TLP:CLEAR

Beyond ValleyRAT: Indicators and Hunting Values

Companion file to the report "Beyond ValleyRAT: Inside a China-Nexus Silver Fox Operation" (as of 2026-10-31, observations to 2026-10-14). It holds the complete, defanged indicator set of the research in five tables (1,391 values): Table A, search keys; Table B, network indicators; Table C, file indicators; Table D, configuration and build values; and Table E, host artefacts. `ChinaNexus_SilverFox_ValleyRAT_IOCs_TLP-CLEAR.csv` carries the same values as one machine readable list.

How to read the action column

"Block" means fit for a blocking control after review. "Block (dated)" marks a rented or shared value that was hostile only on the dates shown. "Hunt" means search for it without blocking on it alone, and "Hunt (dated)" adds the dates. "Hunt (context)" and "Hunt (dated, context)" mark neighbours of the operation, such as the older KANGYINGJIE domains and their IP addresses. "Hunt (page; never block)" marks lure page files. "Never block" marks legitimate files, and "Pivot only" marks search keys. Dates are first and last observations, not deployment dates, and network values change hands within weeks. Artefacts of the VMRay analysis environment, the per session stage and the Microsoft TLS certificate that 156.245.245[.]235 presented are not indicators. Registrant names, hashed values and account numbers are search keys only and identify no person.

A. Search keys

Table A lists the registration values that connect records of the operation and its neighbours (report sections 4.1 and 5.2).

Value	Type	Role	Observed (UTC)	Use
KANGYINGJIE	Registrant organisation	Search key: the registrant organisation of taku788[.]club, fuoe333[.]club and moik77a[.]club (BEIJINGSHI) and of 15 older domains (ANHUISHENG); one listing outside our own records places auk218[.]club under it, and one stored record places fddlbh2[.]club under it; registration data we found lists 121 domains under it at 22net, 2025-04-13 to 2026-10-11	2024-04-22 to 2026-10-14	Pivot only
ab376f4f34801a68	Hashed registrant value	Search key: the organisation code that historical copies of the registration records show for the KANGYINGJIE entry on the four C2 domains, fddlbh2[.]club included	2026-08-11 to 2026-10-09	Pivot only
ZHENGJUNHUA	Registrant organisation	Search key: the registrant organisation of usdt888[.]club, wordtax[.]ink and g00g1e[.]club; registration data we found lists 13 domains under it at 22net, oswin[.]club and winapp[.]work among them, 2026-04-29 to 2026-09-20	2026-04-29 to 2026-10-14	Pivot only
e65ef034ff5b3fab	Hashed registrant value	Search key: the organisation code that historical copies of the registration records show for the ZHENGJUNHUA entry of usdt888[.]club	2026-08-18 to 2026-08-24	Pivot only
CENGCHAO	Registrant organisation	Search key: shyda6317[.]club from 2026-01-29	2026-01-29 to 2026-10-14	Pivot only
574849-1923	Registrar account (Gname)	Search key: the account of the 243 lure and host domains of report section 5.2	2025-09-26 to 2026-10-14	Pivot only
u53630135	Sender account	SendGrid sender whose link led to the delivery host	2026-07-29	Pivot only

Value	Type	Role	Observed (UTC)	Use
u48334250	Sender account	SendGrid sender of a second download path	2026-08-31	Pivot only

Table A: Search keys. Registrant names, hashed registrant values and account numbers identify no person.

B. Network indicators

Table B lists every domain, host, IP address and URL tied to the operation, its delivery and its registrant identities, with the use we advise.

Value (defanged)	Type	Role	Observed (UTC)	Use
taku788[.]club	Domain	C2 server of B1, B7, B8, B9 and six x64 builds; registrant organisation KANGYINGJIE	created 2026-08-14 06:08, expires 2027-08-14; seen 2026-08-16 to 2026-10-13	Block
fuoe333[.]club	Domain	C2 server of B3, four early builds with the DHS seal and three x64 builds; KANGYINGJIE	created 2026-08-09, expires 2027-08-09; seen 2026-08-11 to 2026-10-13	Block
moik77a[.]club	Domain	C2 server of B2 and one x64 build; KANGYINGJIE	created 2026-08-19, expires 2027-08-19; seen 2026-08-19 to 2026-10-13	Block
usdt888[.]club	Domain	C2 server of B5, B6 and 17 October re-packed copies; ZHENGJUNHUA	created 2026-08-18, expires 2027-08-18; seen 2026-08-18 to 2026-10-14	Block
fddlbh2[.]club	Domain	C2 server of F1 and F2; KANGYINGJIE by the organisation code in historical copies of its record, and by name in a stored record of 2026-09-06	created 2026-09-01 12:15, expires 2027-09-01; seen 2026-09-03 to 2026-10-13	Block
www[.]fddlbh2[.]club	Domain	Host of fddlbh2[.]club; on 154.36.188[.]18 from 2026-09-15	2026-09-05 to 2026-10-13	Block
auk218[.]club	Domain	C2 server of the 16 auk218 loaders (HDP kit, outside the operation); KANGYINGJIE in one listing outside our own records (likely the operator of the C2 domains); redacted with province BEIJINGSHI in our own records	created 2026-07-27, expires 2027-07-27; one IP address 2026-07-31 to 2026-10-14	Block
oswin[.]club	Domain	C2 server of one x64 build of 2026-09-01 (outside the operation); ZHENGJUNHUA in two records; likely one party with usdt888[.]club; BEIJINGSHI, redacted in our own records	created 2026-08-31, expires 2027-08-31; seen 2026-09-02 to 2026-10-14	Block
192.252.183[.]157	IPv4	C2 server IP address set directly in B4, C15 and C17; fddlbh2[.]club pointed here	2026-08-17 to 2026-09-03	Block (dated)
202.61.85[.]34	IPv4	taku788[.]club IP address (also atyv788[.]club from 2026-08-14)	2026-08-16	Block (dated)
202.61.85[.]172	IPv4	taku788[.]club IP address	2026-08-18	Block (dated)
202.61.85[.]104	IPv4	taku788[.]club IP address; contacted by B1	2026-08-21	Block (dated)
202.61.85[.]180	IPv4	taku788[.]club IP address	2026-08-31	Block (dated)
202.61.85[.]216	IPv4	taku788[.]club IP address	2026-09-10	Block (dated)
202.61.85[.]153	IPv4	taku788[.]club IP address	2026-09-15	Block (dated)
202.61.85[.]50	IPv4	taku788[.]club IP address; the tax dropper tried to post here	2026-09-23 to 2026-10-13	Block (dated)

Value (defanged)	Type	Role	Observed (UTC)	Use
43.224.224[.]66	IPv4	fuoe333[.]club IP address	2026-08-11 to 2026-08-26	Block (dated)
43.224.224[.]72	IPv4	fuoe333[.]club IP address	2026-09-14	Block (dated)
43.224.224[.]81	IPv4	fuoe333[.]club IP address	2026-09-22 to 2026-10-13	Block (dated)
186.240.201[.]63	IPv4	moik77a[.]club IP address; reverse DNS of 2026-09-09 names a mobile user IP address, likely reassigned to an unrelated subscriber, do not block	2026-08-19 to 2026-08-26	Hunt (dated)
137.220.152[.]244	IPv4	moik77a[.]club IP address	2026-09-17 to 2026-10-13	Block (dated)
64.90.19[.]141	IPv4	usdt888[.]club IP address; contacted by B5	2026-08-18 to 2026-08-20	Block (dated)
103.42.30[.]245	IPv4	usdt888[.]club IP address; contacted by B6; winapp[.]work on 2026-09-22	2026-08-21 to 2026-09-22	Block (dated)
45.203.213[.]231	IPv4	usdt888[.]club IP address	2026-08-24	Block (dated)
122.10.117[.]3	IPv4	usdt888[.]club IP address on 2026-08-24; ManageEngine Endpoint Central server of the RMM deployment; port 8383 named as a C2 server by a researcher (annex reference 29)	2026-07-28 to 2026-10-09	Hunt
156.245.245[.]235	IPv4	usdt888[.]club (2026-09-04) and oswin[.]club (2026-09-02) IP address; presented a borrowed Microsoft certificate	2026-09-02 to 2026-09-04	Block (dated)
156.245.245[.]222	IPv4	usdt888[.]club IP address; contacted by the October copy 578b00dd	2026-10-08 to 2026-10-14	Block (dated)
154.36.188[.]18	IPv4	Later IP address of fddlbh2[.]club (www from 2026-09-15, apex 2026-09-26); shared server with other customers from 2026-04-10	2026-09-15 to 2026-10-13	Hunt
118.107.0[.]196	IPv4	auk218[.]club, its only IP address	2026-07-31 to 2026-10-14	Block
103.42.30[.]140	IPv4	oswin[.]club and winapp[.]work IP address	2026-10-14	Hunt
chusyiorusvo[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; registrant changed to DENGHONGXIN (ZHONGQINGSHI) inside the registration in 2024-08. IP addresses: 172.98.22[.]236 (2024-08-04)	created 2024-04-22; expiry 2025-04-22 (lapsed; unregistered now)	Hunt (context)
shyda6317[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG to 2025; CENGCHAO GUANGDONGSHENG from 2026-01-29. IP addresses: 154.36.188[.]218 (2026-05-07); 202.95.19[.]243 (2026-10-14)	created 2024-11-09; created again 2026-01-29; expiry 2025-11-09; new lifecycle 2027-01-29	Hunt (context)
shyda6318[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; one of the six that moved together. IP addresses: 103.27.79[.]70 (2025-03-26); 45.204.208[.]37 (2026-02-17); 202.95.19[.]243 (2026-10-14)	created 2024-11-09; expiry 2026-11-09	Hunt (context)
shyda6319[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; one of the six that moved together. IP addresses: 103.27.79[.]70 (2025-03-27); 202.95.1[.]227 (2026-02-12); 112.213.120[.]139 (2026-06-21); 202.95.19[.]243 (2026-10-14)	created 2024-11-09; expiry 2026-11-09	Hunt (context)
shyda6320[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE as registrant organisation in historical registration data, with no province. IP addresses: 118.107.5[.]152 (2026-02-15)	created 2025-04-13; expiry 2026-04-13 (lapsed; unregistered now)	Hunt (context)
shyda6321[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG. IP addresses: none printed	created 2025-04-13; expiry 2026-04-13 (lapsed; unregistered now)	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
aeya388[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; C2 server of the configuration Proofpoint published for TA4922 (annex reference 6); one of the six that moved together. IP addresses: 202.95.1[.]227 (2026-02-03); 112.213.120[.]139 (2026-06-13); 202.95.19[.]243 (2026-08-16); 112.213.120[.]167 (2026-10-14)	created 2025-10-30; expiry 2026-10-30	Hunt (context)
shaeyda6328[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; one of the six that moved together. IP addresses: 45.204.208[.]37 (2026-02-03); 112.213.120[.]139 (2026-06-22); 202.95.19[.]243 (2026-10-14)	created 2025-10-30; expiry 2026-10-30	Hunt (context)
aeyd588[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; one of the six that moved together; name servers moved to a Cloudflare pair on 2026-08-10. IP addresses: 202.95.1[.]227 (2026-02-08); no A record now	created 2025-11-16; expiry 2026-11-16	Hunt (context)
aeyh688[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG. IP addresses: 192.229.115[.]159 (2026-10-14)	created 2025-11-18; expiry 2026-11-18	Hunt (context)
atyv788[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; moved to taku788[.]club's IP address 202.61.85[.]34 at 2026-08-14 09:11:59 UTC, three hours after taku788[.]club was registered. IP addresses: 45.192.219[.]19 (2026-02-16); 192.253.224[.]109 (2026-08-01); 202.61.85[.]34 (2026-08-14 to 2026-10-14)	created 2025-12-02; expiry 2026-12-02	Hunt (context)
akyv188[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; sits in the /24 of 192.252.183[.]157 (an IP address range, which carries no weight). IP addresses: 27.50.54[.]151 (2026-02); 192.252.183[.]224 (2026-07-21 to 2026-10-14)	created 2026-01-07; expiry 2027-01-07	Hunt (context)
nta-go[.]work	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG. IP addresses: 103.118.41[.]125 (2026-10-14)	created 2026-01-28; expiry 2027-01-28	Hunt (context)
yscf988[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG. IP addresses: 134.122.163[.]220 (2026-10-14)	created 2026-03-08; expiry 2027-03-08	Hunt (context)
aeda6188[.]club	Domain	Older KANGYINGJIE domain at 22net. KANGYINGJIE ANHUISHENG; one of the six that moved together. IP addresses: 154.36.161[.]80 (2026-03-26); 112.213.120[.]139 (2026-06-12); 202.95.19[.]243 (2026-10-14)	created 2026-03-24; expiry 2027-03-24	Hunt (context)
202.95.19[.]243	IPv4	Shared IP address of the older KANGYINGJIE domains (aeya388, aeda6188, shaeyda6328, shyda6317, shyda6318, shyda6319); in 2026 it carried only names of this set	2026-08-16 to 2026-10-14	Hunt (dated, context)
112.213.120[.]139	IPv4	Shared IP address of the older domains; also carried gambling and other customers before, during and after	2026-04-23 to 2026-06-22	Hunt (dated, context)
112.213.120[.]167	IPv4	IP address of aeya388[.]club; in 2026 it carried only names of the set	2026-10-14	Hunt (dated, context)
45.204.208[.]37	IPv4	Shared IP address of the older domains; also carried other customers	2026-01-28 to 2026-02-17	Hunt (dated, context)
202.95.1[.]227	IPv4	Shared IP address of the older domains; in 2026 it carried only names of the set	2026-02-03 to 2026-02-12	Hunt (dated, context)

Value (defanged)	Type	Role	Observed (UTC)	Use
103.27.79[.]70	IPv4	Earliest wave IP address of the older domains (shyda6318, shyda6319)	2025-03-26 to 2025-03-27	Hunt (dated, context)
192.253.224[.]109	IPv4	IP address of atyv788[.]club before its move to 202.61.85[.]34	2026-08-01	Hunt (dated, context)
45.192.219[.]19	IPv4	IP address of atyv788[.]club	2026-02-16	Hunt (dated, context)
192.252.183[.]224	IPv4	IP address of akyv188[.]club, in the /24 of 192.252.183[.]157	2026-07-21 to 2026-10-14	Hunt (dated, context)
27.50.54[.]151	IPv4	IP address of akyv188[.]club in February 2026	2026-02	Hunt (dated, context)
154.36.188[.]218	IPv4	IP address of shyda6317[.]club (CENGCHAO lifecycle) and earlier of idecald[.]cn	2026-02-07 to 2026-05-07	Hunt (dated, context)
118.107.5[.]152	IPv4	IP address of shyda6320[.]club	2026-02-15	Hunt (dated, context)
192.229.115[.]159	IPv4	IP address of aeyh688[.]club	2026-10-14	Hunt (dated, context)
103.118.41[.]125	IPv4	IP address of nta-go[.]work	2026-10-14	Hunt (dated, context)
134.122.163[.]220	IPv4	IP address of yscf988[.]club	2026-10-14	Hunt (dated, context)
154.36.161[.]80	IPv4	IP address of aeda6188[.]club	2026-03-26	Hunt (dated, context)
172.98.22[.]236	IPv4	IP address of chusyiorusvo[.]club in its KANGYINGJIE period	2024-08-04	Hunt (dated, context)

Value (defanged)	Type	Role	Observed (UTC)	Use
wordtax[.]ink	Domain	ZHENGJUNHUA domain at 22net (organisation printed to 2026-07-24); served the remote management agent package and a copy of the Indian tax lure page	created 2026-05-26, expires 2027-05-26; on hold at the registry (clientHold) from 2026-09-11; seen 2026-06-23 to 2026-09-10	Hunt
www[.]wordtax[.]ink	Domain	Host of wordtax[.]ink, first seen 2026-08-12	2026-08-12 onward	Hunt
mail[.]wordtax[.]ink	Domain	Mail host of wordtax[.]ink (MX from 2026-05-28; inactive 2026-10-03)	2026-05-28 to 2026-10-03	Hunt
g00g1e[.]club	Domain	ZHENGJUNHUA domain at 22net (organisation printed to 2026-08-05)	created 2026-04-29, expires 2027-04-29; seen 2026-05-01 to 2026-10-14	Hunt
mail[.]g00g1e[.]club	Domain	Mail host of g00g1e[.]club	2026-10-14	Hunt
jpword[.]cc	Domain	RMM deployment domain; 22net default name servers, state BeiJing; resolved to 122.10.117[.]3 from 2026-07-28; port 8383 named as a C2 server by a researcher (annex reference 29)	created 2026-04-30, expires 2027-04-30; seen 2026-06-21 to 2026-10-14	Hunt
agent[.]jpword[.]cc	Domain	RMM deployment host on 103.193.172[.]103; served Purchase_Order_31_July_2026.pdf.zip	2026-07-28 to 2026-08-09	Hunt
mail[.]jpword[.]cc	Domain	Mail host of jpword[.]cc, first seen 2026-04-30	2026-04-30 onward	Hunt
vipmail[.]uno	Domain	Name on the wordtax[.]ink certificate group (one server account)	2026-08-12 to 2026-09-16	Hunt
rumail[.]cc	Domain	Name on the wordtax[.]ink certificate group	2026-08-12 to 2026-09-16	Hunt
dnswwt[.]club	Domain	ZHENGJUNHUA domain at 22net (one record); name on the wordtax[.]ink certificate group; served the Indian tax lure body and a 59 MB ZIP on 181.214.250[.]174	created 2026-09-02; seen 2026-09-02 to 2026-09-20	Hunt
downin[.]club	Domain	ZHENGJUNHUA domain at 22net (one record); name on the wordtax[.]ink certificate group	2026-09-02 to 2026-09-16	Hunt
ssmail[.]ink	Domain	ZHENGJUNHUA domain at 22net (one record); name on the wordtax[.]ink certificate group; served the Indian tax lure body	2026-09-16	Hunt
winapp[.]work	Domain	ZHENGJUNHUA domain at 22net (one record; BEIJINGSHI) seen on usdt888[.]club's IP address 103.42.30[.]245; now with oswin[.]club on 103.42.30[.]140	created 2026-09-20, expires 2027-09-20; seen 2026-09-22 to 2026-10-14	Hunt
weburl[.]club	Domain	ZHENGJUNHUA domain at 22net (one record; BEIJINGSHI) on the RMM IP address 103.193.172[.]103	created 2026-08-06, expires 2027-08-06	Hunt
103.193.172[.]103	IPv4	RMM deployment IP address (agent[.]jpword[.]cc; weburl[.]club)	2026-07-30 to 2026-08-09	Hunt
181.214.250[.]206	IPv4	wordtax[.]ink IP address; served setup.aac and setup.appx	2026-08-14 to 2026-08-25	Hunt (dated)
181.214.250[.]174	IPv4	wordtax[.]ink and certificate group IP address; served the Indian tax lure body and dnswwt[.]club's 59 MB ZIP	2026-08-27 to 2026-09-20	Hunt (dated)
166.88.227[.]22	IPv4	IP address of wordtax[.]ink	2026-06-23	Hunt (dated)
194.24.161[.]113	IPv4	IP address of g00g1e[.]club	2026-05-01	Hunt (dated)
185.55.243[.]158	IPv4	IP address of g00g1e[.]club with its mail host	2026-10-14	Hunt (dated)

Value (defanged)	Type	Role	Observed (UTC)	Use
185.55.240[.]19	IPv4	IP address of jpword[.]cc with its mail host	2026-06-21	Hunt (dated)
hxxps://wordtax[.]ink/down/setup.aac	URL	ManageEngine UEMS agent package fetched by the HTA 27254125	2026-08-25	Block
hxxps://wordtax[.]ink/down/setup.appx	URL	Download of 53,261,960 B on wordtax[.]ink; a researcher traced it to the C2 servers jpword[.]cc:8383 and 122.10.117[.]3:8383 (annex reference 29)	2026-08-18	Block
kaiwyrey[.]eu[.]cc	Domain	The delivery host (file sharing application; links /d/<12 hex>); registry object 134544; every contact field redacted	created 2026-06-29 19:08:33, expires 2027-06-29; files from 2026-07-03, packages from 2026-07-28, last answer 2026-09-26	Block
103.23.172[.]117	IPv4	kaiwyrey[.]eu[.]cc's first IP address (2026-06-30); June lure pages of 574849-1923; eight batch eu.cc names	2026-05-27 to 2026-07-11	Block (dated)
103.23.172[.]118	IPv4	kaiwyrey[.]eu[.]cc from 2026-07-01 and the uploads; 19 other batch eu.cc names	2026-07-01 to 2026-10-13	Block (dated)
103.23.172[.]15	IPv4	Indian tax lure pages of 574849-1923 from mid July; e-tzsgzxyu[.]jp	2026-07-14 to 2026-10-06	Block (dated)
103.23.172[.]230	IPv4	Single eu.cc names; 11 names of 574849-1923; eleven Sekoia-listed Silver Fox phishing names (annex reference 4); vbaesta[.]live panel object	2025-09-04 to 2026-10-09	Hunt
103.23.172[.]25	IPv4	Single eu.cc names; 11 names of 574849-1923 with three Thai government lure hosts	2025-07-09 to 2026-10-14	Hunt
103.23.172[.]14	IPv4	IP address bdgsewa[.]eu[.]cc moved to after leaving 103.23.172[.]118	2026-10-14	Hunt (dated)
hxxps://kaiwyrey[.]eu[.]cc/d/c02aa2c1675e	URL	Download link on the delivery host. July files before the kit packages. Files: c839ae15	first seen 2026-07-03	Block
hxxps://kaiwyrey[.]eu[.]cc/d/898baacd110b	URL	Download link on the delivery host. July files before the kit packages. Files: 84061a94	first seen 2026-07-04	Block
hxxps://kaiwyrey[.]eu[.]cc/d/db8bf07b3cf3	URL	Download link on the delivery host. July files before the kit packages. Files: 1290f83e, e79905ac	first seen 2026-07-10	Block
hxxps://kaiwyrey[.]eu[.]cc/d/60b2d5439aad	URL	Download link on the delivery host. July files before the kit packages. Files: 35a2d6c7, 4a4d17d3	first seen 2026-07-20	Block
hxxps://kaiwyrey[.]eu[.]cc/d/e9f5bab719d8	URL	Download link on the delivery host. Late July packages (3.84 to 4.67 MB). Files: 0d481d10, 6b97957b	first seen 2026-07-28	Block
hxxps://kaiwyrey[.]eu[.]cc/d/6f025f85e3c0	URL	Download link on the delivery host. Main download link (one of four that from 2026-08-03 nearly always served the same file: 45 of 46 pairs of checks made within three minutes agreed); served B4 and then F1. Files: 5fada679, b292de38 (B4), da36a96f (F1)	first seen 2026-07-29	Block
hxxps://kaiwyrey[.]eu[.]cc/d/b9059861159e	URL	Download link on the delivery host. Reached through SendGrid account u53630135 on 2026-07-29; served 20260729104357.zip. Files: 6042e01e	first seen 2026-07-29	Block
hxxps://kaiwyrey[.]eu[.]cc/d/c6a6e346738d	URL	Download link on the delivery host. Late July packages (3.84 to 4.67 MB). Files: aa1b45d0	first seen 2026-07-29	Block
hxxps://kaiwyrey[.]eu[.]cc/d/29fefdc0cc4e	URL	Download link on the delivery host. Late July packages (3.84 to 4.67 MB). Files: b856a8d4	first seen 2026-07-30	Block
hxxps://kaiwyrey[.]eu[.]cc/d/e2691cff481e	URL	Download link on the delivery host. Late July packages (3.84 to 4.67 MB). Files: 8dfe4596	first seen 2026-07-30	Block
hxxps://kaiwyrey[.]eu[.]cc/d/ac516096c285	URL	Download link on the delivery host. Main download link. Files: 45695977, d309fe28	first seen 2026-07-31	Block
hxxps://kaiwyrey[.]eu[.]cc/d/4c0956f0a98a	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 69498883	first seen 2026-08-03	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
hxxps://kaiwyrey[.]eu[.]cc/d/b10f4cab0b43	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: ba2a39fd, f2e5148c	first seen 2026-08-03	Block
hxxps://kaiwyrey[.]eu[.]cc/d/e371fa68af13	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: e41d56c6	first seen 2026-08-04	Block
hxxps://kaiwyrey[.]eu[.]cc/d/ed86198ed307	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 3d53bd10	first seen 2026-08-04	Block
hxxps://kaiwyrey[.]eu[.]cc/d/1dd63a1a7fbc	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 0505f40d, 1a5d19bd	first seen 2026-08-05	Block
hxxps://kaiwyrey[.]eu[.]cc/d/9eceece22fac	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 05e27d19	first seen 2026-08-05	Block
hxxps://kaiwyrey[.]eu[.]cc/d/193338c39726	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 096de423	first seen 2026-08-06	Block
hxxps://kaiwyrey[.]eu[.]cc/d/2806bf9f5858	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 14b0b41d	first seen 2026-08-07	Block
hxxps://kaiwyrey[.]eu[.]cc/d/8b875e8cf101	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 7582528e, a5ae301a, b14ab004	first seen 2026-08-07	Block
hxxps://kaiwyrey[.]eu[.]cc/d/f65c0a1e3963	URL	Download link on the delivery host. Period of the auk218[.]club loader packages. Files: 43c28f6f, 542acfb5, 8375a630, a2cef022	first seen 2026-08-10	Block
hxxps://kaiwyrey[.]eu[.]cc/d/a63179e2fe1a	URL	Download link on the delivery host. Served 2c16aed0 on 2026-08-18 (period of the 192.252.183[.]157 builds). Files: 2c16aed0	first seen 2026-08-18	Block
hxxps://kaiwyrey[.]eu[.]cc/d/863c42ccf5e0	URL	Download link on the delivery host. Served the C17 package feb58c7b from 2026-08-20. Files: feb58c7b	first seen 2026-08-20	Block
hxxps://kaiwyrey[.]eu[.]cc/d/ab8be35731a0	URL	Download link on the delivery host. Link that served F2 (d4a8b9d3) on 2026-09-04 and 6dc6af47 to 2026-09-06. Files: 6dc6af47, d4a8b9d3	first seen 2026-09-04	Block
hxxps://kaiwyrey[.]eu[.]cc/d/52f5a2c0c2e1	URL	Download link on the delivery host. Link that served the 7.5 MB x64 file 28958b5d from 2026-09-08 to 2026-09-15. Files: 28958b5d	first seen 2026-09-08	Block
hxxps://kaiwyrey[.]eu[.]cc/d/0cd07b91456a	URL	Download link on the delivery host. The file sharing application's 403 page on 2026-09-17 and 09-18	first seen 2026-09-17	Block
hxxps://kaiwyrey[.]eu[.]cc/d/0f061f21853b	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/116b24b25c63	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/13475714b3d9	URL	Download link on the delivery host. Linked from the Indian tax lure page kcsueaw[.]xin on 2026-07-31	first seen 2026-07-31	Block
hxxps://kaiwyrey[.]eu[.]cc/d/13fc3e5f75ac	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/1a5fa5b74f9a	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/1fe96b4a6171	URL	Download link on the delivery host. Served 20260804142311.ACC94F70494B.zip (e8409b4f) on 2026-08-04	first seen 2026-08-04	Block
hxxps://kaiwyrey[.]eu[.]cc/d/244d8556d73d	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
hxxps://kaiwyrey[.]eu[.]cc/d/28b6e7c0877b	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/29bfbc09808b	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/33b276dd1c21	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/3f6fda10c779	URL	Download link on the delivery host. First stored panel page (2026-07-28); served 20260728151147.zip	first seen 2026-07-28	Block
hxxps://kaiwyrey[.]eu[.]cc/d/5ef3f302a330	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/70878efbc582	URL	Download link on the delivery host. Main download link	first seen 2026-08-03	Block
hxxps://kaiwyrey[.]eu[.]cc/d/7dbf48f20833	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/9195f8f2c07a	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/9abdb5389166	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/b6e03b8b7194	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/bdc9637e70c2	URL	Download link on the delivery host. Main download link; served from 2026-07-30	first seen 2026-07-30	Block
hxxps://kaiwyrey[.]eu[.]cc/d/d4f46bd3b34b	URL	Download link on the delivery host. Link observed on 2026-08-21	first seen 2026-08-21	Block
hxxps://kaiwyrey[.]eu[.]cc/d/e583e34f9259	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/ec9be9847641	URL	Download link on the delivery host. A URL record of this link code on kaiwyrey[.]eu[.]cc, with no date and no file attached	undated	Block
hxxps://kaiwyrey[.]eu[.]cc/d/fe93220bfecf	URL	Download link on the delivery host. Stale /file?code= link answered with the 403 panel page on 2026-08-03	first seen 2026-08-03	Block
hxxps://<label>[.]eu[.]cc/d/<12 hex>/file?code=<32 hex>	URL pattern	Delivery URL pattern of the file sharing application (302 from /d/<id> to /file?code=, then a 200 attachment)	2026-07-21 onward	Hunt
bdgsewa[.]eu[.]cc	Domain	Batch eu.cc name, registry 149625; moved to 103.23.172[.]14 by 2026-10-14; on 103.23.172[.]118	created 2026-08-06 05:26:51; seen 2026-08-08 to 2026-08-08	Hunt
ddisuyer[.]eu[.]cc	Domain	Batch eu.cc name, registry 128602; served the padded x64 loaders; target of 18 June lure page links; on 103.23.172[.]118	created 2026-06-18 03:28:51; seen 2026-06-21 to 2026-06-21	Block
fuerubuiaie[.]eu[.]cc	Domain	Batch eu.cc name, registry 109453; served the padded x64 loaders; target of 10 June lure page links; on 103.23.172[.]118	created 2026-05-11 11:29:41; seen 2026-08-13 to 2026-10-14	Block
hsaueraw[.]eu[.]cc	Domain	Batch eu.cc name, registry 134660; on 103.23.172[.]118	created 2026-06-30 05:11:28; seen 2026-08-11 to 2026-10-14	Hunt
hsawtse[.]eu[.]cc	Domain	Batch eu.cc name, registry 134541; certificate order of 2026-06-30 with kaiwyrey; on 103.23.172[.]117	created 2026-06-29 19:08:31; seen 2026-08-11 to 2026-10-14	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
idutyarwse[.]eu[.]cc	Domain	Batch eu.cc name, registry 109454; served the padded x64 loaders; target of 2 June lure page links; on 103.23.172[.]118	created 2026-05-11 11:29:41; seen 2026-08-11 to 2026-10-14	Block
isudcnzy[.]eu[.]cc	Domain	Batch eu.cc name, registry 134545; served the padded x64 loaders; shares two files with the delivery host account in July; on 103.23.172[.]118	created 2026-06-29 19:08:35; seen 2026-07-30 to 2026-10-14	Block
iysdzxc[.]eu[.]cc	Domain	Batch eu.cc name, registry 149624; on 103.23.172[.]118	created 2026-08-06 05:26:50; seen 2026-08-08 to 2026-10-14	Hunt
kcjsjyeaw[.]eu[.]cc	Domain	Batch eu.cc name, registry 128603; on 103.23.172[.]118	created 2026-06-18 03:28:51; seen 2026-08-10 to 2026-10-14	Hunt
kksiaueted[.]ec[.]cc	Domain	Batch eu.cc name, registry 135117; on 103.23.172[.]117	created 2026-07-01 03:47:45; seen 2026-07-03 to 2026-07-03	Hunt
ksidxhcte[.]eu[.]cc	Domain	Batch eu.cc name, registry 134664; on 103.23.172[.]118	created 2026-06-30 05:11:30; seen 2026-08-02 to 2026-10-14	Hunt
laiwybstw[.]eu[.]cc	Domain	Batch eu.cc name, registry 134663; certificate order of 2026-07-21 with kaiwyrey; served the padded x64 loaders; on 103.23.172[.]118	created 2026-06-30 05:11:29; seen 2026-08-10 to 2026-10-14	Block
lzsifuiseurtt[.]eu[.]cc	Domain	Batch eu.cc name, registry 109455; target of 7 June lure page links; on 103.23.172[.]118	created 2026-05-11 11:29:41; seen 2026-05-29 to 2026-05-29	Hunt
ncstsruks[.]eu[.]cc	Domain	Batch eu.cc name, registry 128601; on 103.23.172[.]118	created 2026-06-18 03:28:50; seen 2026-06-21 to 2026-06-21	Hunt
oaiwuyda[.]eu[.]cc	Domain	Batch eu.cc name, registry 134661; on 103.23.172[.]118	created 2026-06-30 05:11:28; seen 2026-08-11 to 2026-10-14	Hunt
oaosifytaw[.]eu[.]cc	Domain	Batch eu.cc name, registry 128600; on 103.23.172[.]118	created 2026-06-18 03:28:50; seen 2026-08-08 to 2026-10-14	Hunt
psiawute[.]eu[.]cc	Domain	Batch eu.cc name, registry 134542; on 103.23.172[.]117	created 2026-06-29 19:08:31; seen 2026-08-10 to 2026-10-14	Hunt
pzidiauwytsd[.]eu[.]cc	Domain	Batch eu.cc name, registry 109457; target of 8 June lure page links; on 103.23.172[.]118	created 2026-05-11 11:29:45; seen 2026-08-12 to 2026-10-14	Hunt
qaywtfse[.]eu[.]cc	Domain	Batch eu.cc name, registry 134538; on 103.23.172[.]117	created 2026-06-29 19:08:31; seen 2026-08-10 to 2026-10-14	Hunt
rcyawday[.]eu[.]cc	Domain	Batch eu.cc name, registry 134662; certificate order of 2026-07-21 with kaiwyrey; on 103.23.172[.]118	created 2026-06-30 05:11:28; seen 2026-08-12 to 2026-10-14	Block
suawytde[.]eu[.]cc	Domain	Batch eu.cc name, registry 134539; on 103.23.172[.]117	created 2026-06-29 19:08:31; seen 2026-08-08 to 2026-10-14	Hunt
vcxetknsbe[.]ec[.]cc	Domain	Batch eu.cc name, registry 135116; on 103.23.172[.]117	created 2026-07-01 03:47:45; seen 2026-08-01 to 2026-10-14	Hunt
xciwuerse[.]eu[.]cc	Domain	Batch eu.cc name, registry 134540; on 103.23.172[.]117	created 2026-06-29 19:08:31; seen 2026-08-08 to 2026-10-14	Hunt
xkcisetr[.]eu[.]cc	Domain	Batch eu.cc name, registry 134665; on 103.23.172[.]118	created 2026-06-30 05:11:30; seen 2026-08-02 to 2026-10-14	Hunt
xzsdiiaeugs[.]eu[.]cc	Domain	Batch eu.cc name, registry 109458; served the padded x64 loaders; target of 11 June lure page links; on 103.23.172[.]118	created 2026-05-11 11:29:45; seen 2026-08-01 to 2026-10-14	Block
zuxyegea[.]eu[.]cc	Domain	Batch eu.cc name, registry 134659; on 103.23.172[.]118	created 2026-06-30 05:11:28; seen 2026-08-02 to 2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
zxysevre[.]eu[.]cc	Domain	Batch eu.cc name, registry 134543; on 103.23.172[.]117	created 2026-06-29 19:08:33; seen 2026-08-10 to 2026-10-14	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/00f6ccb8a058	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc. Files: e329a261	first seen 2026-06-19	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/5030962e6cf3	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc. Files: 432e225c	first seen 2026-06-23	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/675d35b0cefd	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc. Files: 69de3198	first seen 2026-06-23	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/56173a63cdd6	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc. Files: 7e01626c	first seen 2026-06-24	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/cf6615384394	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc. Files: 82c0617c	first seen 2026-06-24	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/109430a6d909	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc. Files: 15ed0bb5	first seen 2026-06-25	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/ca9a0c4054f2	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc. Files: c8d02395	first seen 2026-06-25	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/2f7d9b9e549b	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc	undated	Hunt
hxxps://ddisuyer[.]eu[.]cc/d/b29b5390c201	URL	Download link on batch eu.cc name ddisuyer[.]eu[.]cc	undated	Hunt
hxxps://fuerubuiaie[.]eu[.]cc/d/dbcb05dac572	URL	Download link on batch eu.cc name fuerubuiaie[.]eu[.]cc. Files: db40ca5c	first seen 2026-06-02	Hunt
hxxps://fuerubuiaie[.]eu[.]cc/d/0295208197a2	URL	Download link on batch eu.cc name fuerubuiaie[.]eu[.]cc. Files: 67631fba	first seen 2026-06-05	Hunt
hxxps://fuerubuiaie[.]eu[.]cc/d/0968c3e17581	URL	Download link on batch eu.cc name fuerubuiaie[.]eu[.]cc	undated	Hunt
hxxps://fuerubuiaie[.]eu[.]cc/d/e89636c887a3	URL	Download link on batch eu.cc name fuerubuiaie[.]eu[.]cc	undated	Hunt
hxxps://hsaueraw[.]eu[.]cc/d/e6af2259d500	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc. Files: 11c5ae00	first seen 2026-07-23	Hunt
hxxps://hsaueraw[.]eu[.]cc/d/3368b283d97a	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc. Files: 8805c7f4	first seen 2026-07-28	Hunt
hxxps://hsaueraw[.]eu[.]cc/d/074457b9510d	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc. Files: 74c46708	first seen 2026-07-29	Hunt
hxxps://hsaueraw[.]eu[.]cc/d/2f9332b9f22f	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc. Files: 8b6f5ad8	first seen 2026-08-01	Hunt
hxxps://hsaueraw[.]eu[.]cc/d/201177156384	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc	undated	Hunt
hxxps://hsaueraw[.]eu[.]cc/d/3d515df256e0	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc	undated	Hunt
hxxps://hsaueraw[.]eu[.]cc/d/8f9d8472d399	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc	undated	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
hxxps://hsaueraw[.]eu[.]cc/d/18ca5ed6bfc4	URL	Download link on batch eu.cc name hsaueraw[.]eu[.]cc	undated	Hunt
hxxps://idutyarwse[.]eu[.]cc/d/f1f4d592161d	URL	Download link on batch eu.cc name idutyarwse[.]eu[.]cc. Files: 7c8395cc	first seen 2026-06-05	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/5e54862579f0	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc. Files: 84061a94	first seen 2026-07-04	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/33cb9533b11b	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc. Files: 293d87d9	first seen 2026-07-08	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/c541853be790	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc. Files: 3ab04222	first seen 2026-07-08	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/1b78c105d6b8	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc. Files: 747124f4, 77a03e8d	first seen 2026-07-17	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/68989d373f77	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc	undated	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/9d6385f95218	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc	undated	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/b38042fae927	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc	undated	Hunt
hxxps://isudcnzy[.]eu[.]cc/d/4a28a94fbf3d	URL	Download link on batch eu.cc name isudcnzy[.]eu[.]cc	undated	Hunt
hxxps://iysdzxc[.]eu[.]cc/d/ee2b12fbd661	URL	Download link on batch eu.cc name iysdzxc[.]eu[.]cc. Files: f99a5496	first seen 2026-08-07	Hunt
hxxps://kcjsjyeaw[.]eu[.]cc/d/d11aa82d71f7	URL	Download link on batch eu.cc name kcjsjyeaw[.]eu[.]cc	undated	Hunt
hxxps://kcjsjyeaw[.]eu[.]cc/d/aa0509a6602b	URL	Download link on batch eu.cc name kcjsjyeaw[.]eu[.]cc	undated	Hunt
hxxps://kcjsjyeaw[.]eu[.]cc/d/4c45eaa2b9ac	URL	Download link on batch eu.cc name kcjsjyeaw[.]eu[.]cc	undated	Hunt
hxxps://ksidxhcte[.]eu[.]cc/d/b16074ea4502	URL	Download link on batch eu.cc name ksidxhcte[.]eu[.]cc. Files: 091de589	first seen 2026-08-12	Hunt
hxxps://ksidxhcte[.]eu[.]cc/d/75af6221821a	URL	Download link on batch eu.cc name ksidxhcte[.]eu[.]cc	undated	Hunt
hxxps://laiwybstw[.]eu[.]cc/d/b1f16e9a3d9a	URL	Download link on batch eu.cc name laiwybstw[.]eu[.]cc. Files: 747124f4	first seen 2026-07-23	Hunt
hxxps://laiwybstw[.]eu[.]cc/d/80220b66de2b	URL	Download link on batch eu.cc name laiwybstw[.]eu[.]cc	undated	Hunt
hxxps://laiwybstw[.]eu[.]cc/d/013f990c5183	URL	Download link on batch eu.cc name laiwybstw[.]eu[.]cc	undated	Hunt
hxxps://laiwybstw[.]eu[.]cc/d/20d4213152f7	URL	Download link on batch eu.cc name laiwybstw[.]eu[.]cc	undated	Hunt
hxxps://lzsifuiseurtt[.]eu[.]cc/d/07b3b6c32b8b	URL	Download link on batch eu.cc name lzsifuiseurtt[.]eu[.]cc. Files: 63d39bb5	first seen 2026-05-28	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
hxxps://lzsifuiseurtt[.]eu[.]cc/d/761fc975ba4d	URL	Download link on batch eu.cc name lzsifuiseurtt[.]eu[.]cc. Files: a6fb779b	first seen 2026-05-28	Hunt
hxxps://lzsifuiseurtt[.]eu[.]cc/d/9d57022862c6	URL	Download link on batch eu.cc name lzsifuiseurtt[.]eu[.]cc. Files: 59ad96dd	first seen 2026-05-29	Hunt
hxxps://lzsifuiseurtt[.]eu[.]cc/d/2edb4dfc03bf	URL	Download link on batch eu.cc name lzsifuiseurtt[.]eu[.]cc	undated	Hunt
hxxps://lzsifuiseurtt[.]eu[.]cc/d/c34986984b3f	URL	Download link on batch eu.cc name lzsifuiseurtt[.]eu[.]cc	undated	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/534de9718ba0	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: 4fe38dc2	first seen 2026-07-02	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/e6600cac8ae3	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: 92d34a15	first seen 2026-07-02	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/c8bc03a88702	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: bd495b4c	first seen 2026-07-02	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/55fbb2550be9	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: 7dc5a105	first seen 2026-07-03	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/63fa02e75abc	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: df31e4e7	first seen 2026-07-03	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/efccb6d9a566	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: 0b09b117	first seen 2026-07-06	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/7400f2c1d28e	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: e2ce9f9b	first seen 2026-07-15	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/78bdaf9424d4	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc. Files: fa5df7b0	first seen 2026-07-16	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/1fa3ee0e4948	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc	undated	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/a32b8250817b	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc	undated	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/a66d1c756057	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc	undated	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/b048956ed072	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc	undated	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/3320ac38c0ad	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc	undated	Hunt
hxxps://oaosifytaw[.]eu[.]cc/d/181671de26ae	URL	Download link on batch eu.cc name oaosifytaw[.]eu[.]cc	undated	Hunt
hxxps://pzidiauwytsd[.]eu[.]cc/d/c200ea02fd60	URL	Download link on batch eu.cc name pzidiauwytsd[.]eu[.]cc. Files: 8ab8f771	first seen 2026-06-23	Hunt
hxxps://pzidiauwytsd[.]eu[.]cc/d/bbcbbf698cc1	URL	Download link on batch eu.cc name pzidiauwytsd[.]eu[.]cc. Files: 156bbc56	first seen 2026-06-24	Hunt
hxxps://pzidiauwytsd[.]eu[.]cc/d/df705f68f4e2	URL	Download link on batch eu.cc name pzidiauwytsd[.]eu[.]cc. Files: 6d2313dc	first seen 2026-06-25	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
hxxps://pzidiauwytsd[.]eu[.]cc/d/72d681bc3690	URL	Download link on batch eu.cc name pzidiauwytsd[.]eu[.]cc. Files: d93b3a54	first seen 2026-06-26	Hunt
hxxps://pzidiauwytsd[.]eu[.]cc/d/76bbdcf4299a	URL	Download link on batch eu.cc name pzidiauwytsd[.]eu[.]cc. Files: 1ea0d3cf	first seen 2026-07-02	Hunt
hxxps://pzidiauwytsd[.]eu[.]cc/d/a06c1797e07c	URL	Download link on batch eu.cc name pzidiauwytsd[.]eu[.]cc	undated	Hunt
hxxps://xzsdiiaeugs[.]eu[.]cc/d/3796534db3ed	URL	Download link on batch eu.cc name xzsdiiaeugs[.]eu[.]cc. Files: d0c2f5cc	first seen 2026-06-17	Hunt
hxxps://xzsdiiaeugs[.]eu[.]cc/d/aa86573aa764	URL	Download link on batch eu.cc name xzsdiiaeugs[.]eu[.]cc. Files: f1cf9b97	first seen 2026-06-18	Hunt
hxxps://xzsdiiaeugs[.]eu[.]cc/d/2a358fa67778	URL	Download link on batch eu.cc name xzsdiiaeugs[.]eu[.]cc	undated	Hunt
hxxps://xzsdiiaeugs[.]eu[.]cc/d/9cf52d089568	URL	Download link on batch eu.cc name xzsdiiaeugs[.]eu[.]cc	undated	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/72cfa0d115e8	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: 362f7330	first seen 2026-08-01	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/bd199d1aa929	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: 8becdd83	first seen 2026-08-04	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/21fa5dd9c596	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: 779314ed	first seen 2026-08-06	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/cec66f8cb9ae	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: a47ec01e	first seen 2026-08-08	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/215310b04ae1	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: f14206ab	first seen 2026-08-08	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/7ad8be732033	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: c694a854	first seen 2026-08-11	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/eee736601c59	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: 24d615e3	first seen 2026-08-13	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/cd5817c21ba6	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc. Files: cb55a8b5	first seen 2026-09-16	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/ba62115f7526	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc	undated	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/ce75fa641dab	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc	undated	Hunt
hxxps://zuxyegea[.]eu[.]cc/d/0bf262904027	URL	Download link on batch eu.cc name zuxyegea[.]eu[.]cc	undated	Hunt
bcaisuyer[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-28; seen 2026-08-14 to 2026-10-14	Hunt
bctetagrg[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-02 to 2026-10-14	Hunt
bvbxdse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]118	created 2026-08-09	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
bvdaccs[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2025-12-03	Hunt
bzusdty[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt
bzusydyea[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-26; seen 2026-08-10 to 2026-10-14	Hunt
cksxmviu[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-25; seen 2026-08-08 to 2026-10-14	Hunt
cnxvbsjdy[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
csdfsera[.]live	Domain	Lure host of 574849-1923 on 103.23.172[.]15	created 2026-08-06; seen 2026-08-08 to 2026-08-08; clientHold	Block
cvwbrwrs[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name fuerubuiaie[.]eu[.]cc	created 2026-05-31; seen 2026-08-08 to 2026-10-14	Block
dccawc[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-07; seen 2026-08-09 to 2026-10-14	Hunt
dyrys[.]tasykdwa[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-23; seen 2026-03-02 to 2026-10-14	Hunt
fdcmsjrsw[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
fddrdh[.]ifuaytes[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-23; seen 2026-10-09 to 2026-10-14	Hunt
fdigaifev[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-04; seen 2026-08-16 to 2026-10-14	Hunt
fduaywayst[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name lzsifuiseurtt[.]eu[.]cc	created 2026-05-28; seen 2026-08-11 to 2026-10-14	Block
fghs[.]kzifyakyue[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-04; seen 2026-07-22 to 2026-10-14	Hunt
ficjseytea[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
fisuahwa[.]live	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-08-07; seen 2026-08-09 to 2026-08-09; clientHold	Block
fiusyevr[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name fuerubuiaie[.]eu[.]cc	created 2026-05-31; seen 2026-06-19 to 2026-06-19; clientHold	Block
flsiuety[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name xzsdiiaeugs[.]eu[.]cc	created 2026-06-17; seen 2026-06-20 to 2026-06-20; clientHold	Block
fstawrxvy[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name xzsdiiaeugs[.]eu[.]cc	created 2026-06-22; seen 2026-07-31 to 2026-10-14	Block
fsyahsxd[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-21; seen 2026-07-31 to 2026-07-31; clientHold	Block
fuaytrwese[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name lzsifuiseurtt[.]eu[.]cc	created 2026-05-28; seen 2026-08-09 to 2026-10-14	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
fusaystrbc[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-06-10 to 2026-06-10; clientHold	Hunt
fvxcuvuyte[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name fuerubuiaie[.]eu[.]cc	created 2026-06-02; seen 2026-08-02 to 2026-10-14	Block
fxuawyje[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-06-26 to 2026-06-26; clientHold	Hunt
fxvsgaewz[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-14; seen 2026-08-01 to 2026-10-14	Hunt
fychdstjse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
fysiyr[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-03-26; seen 2026-08-06 to 2026-08-06	Hunt
ghsyse[.]xzdyattte[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-02; seen 2026-07-23 to 2026-10-14	Hunt
gisudyawz[.]ink	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-19; seen 2026-07-21 to 2026-07-21; clientHold	Block
gothds[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-08	Hunt
gothuy[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-08	Hunt
gov[.]bvdaccs[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25; Thai government lure host	created 2025-12-03; seen 2026-06-03 to 2026-10-14	Block
gsawytex[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name pzidiauwytsd[.]eu[.]cc	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Block
gxncjsuefre[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
hauwtcbe[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-06-26 to 2026-06-26; clientHold	Hunt
haywtrbcye[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-07-31 to 2026-10-14	Hunt
hbxauyea[.]win	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-29; seen 2026-07-31 to 2026-07-31; clientHold	Hunt
hduywtt[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-02 to 2026-10-14	Hunt
hsaudxze[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-07-29 to 2026-10-14	Hunt
hsauyeet[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-08-01 to 2026-10-14	Hunt
hsieuygrw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name xzsdiiaeugs[.]eu[.]cc	created 2026-06-17; seen 2026-06-19 to 2026-06-19; clientHold	Block
hsiueteas[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
hsncjdyea[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
hsy[.]iauechte[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-04; seen 2026-06-17 to 2026-10-14	Hunt
httpiaw[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2026-03-25; seen 2026-03-27 to 2026-03-27; clientHold	Hunt
httplai[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2026-03-25; seen 2026-03-27 to 2026-03-27; clientHold	Hunt
httpsuw[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2026-03-26; seen 2026-06-09 to 2026-06-09	Hunt
iauechte[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-04	Hunt
iauishatw[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-21; seen 2026-07-31 to 2026-07-31; clientHold	Hunt
iawu[.]sidigara[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-02; seen 2026-09-15 to 2026-10-14	Hunt
iayueate[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-26; seen 2026-05-28 to 2026-05-28; clientHold	Hunt
ifuaytes[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-23	Hunt
ijshefdse[.]win	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-29; seen 2026-07-31 to 2026-07-31; clientHold	Hunt
isauwtsq[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-06 to 2026-10-14	Hunt
isdhdwhw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name ddisuyer[.]eu[.]cc	created 2026-06-23; seen 2026-08-01 to 2026-10-14	Block
isyawtgxe[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-28; seen 2026-06-30 to 2026-06-30	Hunt
isyraw[.]quidoaehse[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230; listed by Sekoia as Silver Fox phishing (annex reference 4)	created 2025-10-09; seen 2026-05-23 to 2026-10-14	Block
itrydsba[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-09; seen 2026-08-11 to 2026-08-11; clientHold	Hunt
ixufruwig[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-18; seen 2026-08-13 to 2026-10-14	Hunt
jaiehsycres[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
jaiwuydr[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name ddisuyer[.]eu[.]cc	created 2026-06-18; seen 2026-06-20 to 2026-06-20; clientHold	Block
jaiydteds[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name idutyarwse[.]eu[.]cc	created 2026-05-31; seen 2026-08-07 to 2026-10-14	Block
jdfksyaw[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
jdshduyw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-22; seen 2026-06-24 to 2026-06-24; clientHold	Hunt
juxsyena[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-01 to 2026-10-14	Hunt
kairtyayede[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-26; seen 2026-05-28 to 2026-05-28; clientHold	Hunt
kaisufyyte[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-31; seen 2026-08-07 to 2026-10-14	Hunt
kaiwxnyes[.]live	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-15; seen 2026-08-08 to 2026-10-14	Block
kakiwuyder[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
kcbahwtrz[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-07; seen 2026-08-01 to 2026-10-14	Hunt
kcsueaw[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages); on 2026-07-31 its page linked hxxps://kaiwyrey[.]eu[.]cc/d/13475714b3d9	created 2026-07-19; seen 2026-07-21 to 2026-07-21; clientHold	Block
kdsuyrse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-08-12 to 2026-10-14	Hunt
kfuyisulnry[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-02	Hunt
kiafewoey[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-09	Hunt
kidueyrfs[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-29 to 2026-10-14	Hunt
kiuasyxse[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-21; seen 2026-07-31 to 2026-07-31; clientHold	Hunt
kiufusete[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
kixuseteh[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-03 to 2026-10-14	Hunt
kjfuwyce[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; listed by JUMPSEC as documented Silver Fox (annex reference 5)	created 2026-06-23; seen 2026-08-02 to 2026-10-14	Hunt
klseiiuvye[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-14; seen 2026-08-01 to 2026-08-01; clientHold	Hunt
kncjxdhyers[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
ksiduyee[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-22; seen 2026-07-31 to 2026-10-14	Hunt
kudkgoay[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-01 to 2026-10-14	Hunt
kxaussyte[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-13; seen 2026-07-30 to 2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
kxisetcblg[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-03 to 2026-10-14	Hunt
kxjnbsagt[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
kxmnshaw[.]win	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-31; seen 2026-08-02 to 2026-08-02; clientHold	Hunt
kxuaicnvyet[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-05 to 2026-10-14	Hunt
kzifyakyue[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-04	Hunt
laiujsatx[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-08-10 to 2026-08-10; clientHold	Hunt
laiwyfbtw[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-05 to 2026-07-05; clientHold	Hunt
laiwyhvge[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-22; seen 2026-07-31 to 2026-10-14	Hunt
lasdyyterc[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-08-05 to 2026-10-14	Hunt
lasodtetr[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-18; seen 2026-08-04 to 2026-10-14	Hunt
lckawybdy[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt
ldiruttew[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-17; seen 2026-06-19 to 2026-06-19; clientHold	Hunt
licduytrdse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
lisiutegrm[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-31; seen 2026-08-07 to 2026-10-14	Hunt
lisudted[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-06-26 to 2026-06-26; clientHold	Hunt
lodiisuede[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
lvsiurae[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-06; seen 2026-08-08 to 2026-10-14	Hunt
lxcosetrs[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
lxkzsyeqwt[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-07; seen 2026-08-01 to 2026-10-14	Hunt
lzaiwugsa[.]ink	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-19; seen 2026-07-21 to 2026-07-21; clientHold	Block
maietxdea[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-03 to 2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
maiuueytw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-31; seen 2026-08-12 to 2026-10-14	Hunt
maoasiye[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]118	created 2026-05-26; seen 2026-05-28 to 2026-05-28; clientHold	Hunt
mckajwyd[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt
misajwut[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-14; seen 2026-08-01 to 2026-10-14	Hunt
mksfuuerwo[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-31; seen 2026-08-08 to 2026-10-14	Hunt
mxnnshya[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-05 to 2026-10-14	Hunt
mxodsiuuy[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
mxziyuve[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-05 to 2026-07-05; clientHold	Hunt
ncduuyese[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-28; seen 2026-08-14 to 2026-10-14	Hunt
nhdsesd[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-06; seen 2026-08-08 to 2026-08-08; clientHold	Hunt
nsisuyete[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
nxjdfysead[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
nzsjdyzw[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt
oakwusya[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name lzsifuiseurtt[.]eu[.]cc	created 2026-05-28; seen 2026-08-08 to 2026-10-14	Block
paiwudyea[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; its saved June lure page links batch name idutyarwse[.]eu[.]cc	created 2026-05-31; seen 2026-07-30 to 2026-10-14	Block
pawoidutte[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-28; seen 2026-08-10 to 2026-10-14	Hunt
pbcgsrwre[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
pdijcsuet[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-06-26 to 2026-06-26; clientHold	Hunt
pifuytawjne[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-18; seen 2026-08-03 to 2026-10-14	Hunt
piumbtaw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
pixizysaws[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-07; seen 2026-08-09 to 2026-08-09; clientHold	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
posaiyaws[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-19; seen 2026-07-21 to 2026-07-21; clientHold	Hunt
pxjastyha[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-21; seen 2026-07-31 to 2026-07-31; clientHold	Hunt
pxnzsdgre[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-08-04 to 2026-10-14	Hunt
pxoiseyhx[.]live	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-15; seen 2026-08-07 to 2026-10-14	Block
pzisiauywa[.]xin	Domain	Domain of 574849-1923 among the Indian tax lure pages, with no IP address on record	created 2026-07-22; clientHold	Hunt
qaksdiuw[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-19; seen 2026-07-21 to 2026-07-21; clientHold	Block
qeuasytua[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-26; seen 2026-08-11 to 2026-10-14	Hunt
qicxgreae[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
qisdyetvcae[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
qisuawbsw[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-08-15 to 2026-10-14	Hunt
qmcsjeus[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt
qodyeytax[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages; tax word in the label	created 2026-06-02; seen 2026-06-10 to 2026-06-10; clientHold	Hunt
qoisuayws[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-15; seen 2026-08-06 to 2026-10-14	Hunt
quayastgfd[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-21; seen 2026-07-31 to 2026-07-31; clientHold	Hunt
quidoaehse[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-09	Hunt
qwdrfdsgc[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-06; seen 2026-08-08 to 2026-08-08; clientHold	Hunt
qxcddrse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-05 to 2026-07-05; clientHold	Hunt
qzhgsbaw[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-08-08 to 2026-08-08; clientHold	Hunt
qzixudex[.]win	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-29; seen 2026-07-31 to 2026-10-14	Hunt
rctsbetaw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25	Hunt
saiyxsux[.]live	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-08-07; seen 2026-08-09 to 2026-08-09; clientHold	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
scyatwks[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-14; seen 2026-08-01 to 2026-10-14	Hunt
scytatyweg[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
sidigara[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-02	Hunt
siuf[.]kfuyisulnry[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-02; seen 2026-10-12 to 2026-10-14	Hunt
sixzuyzva[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-08-15 to 2026-08-15; clientHold	Hunt
siyuyeaw[.]win	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-31; seen 2026-08-02 to 2026-10-14	Hunt
skjsayeyd[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-06-26 to 2026-06-26; clientHold	Hunt
sueysu[.]ysieiuhaw[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-09; seen 2026-03-02 to 2026-10-14	Hunt
suiyerjser[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-09-26	Hunt
suyczshea[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-22; seen 2026-08-13 to 2026-08-13; clientHold	Block
syfiaydytea[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-28; seen 2026-08-14 to 2026-10-14	Hunt
syxhtejkdr[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-02 to 2026-10-14	Hunt
tasdhwia[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-02 to 2026-10-14	Hunt
tasykdwa[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-23	Hunt
tawuiutfe[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-28; seen 2026-08-05 to 2026-10-14	Hunt
tbckduurs[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-22; seen 2026-06-24 to 2026-06-24	Hunt
tdrw[.]bvbxdse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]118; host of bvbxdse[.]live	created 2026-08-09; seen 2026-09-05 to 2026-10-14	Hunt
thaigov[.]gothds[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25; Thai government lure host	created 2026-02-08; seen 2026-10-09 to 2026-10-14	Block
tsadya[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2026-03-26; seen 2026-06-11 to 2026-06-11	Hunt
tsagwaza[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-13; seen 2026-07-16 to 2026-07-16; clientHold	Hunt
tsbwufyrsw[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
tsgvvzhyse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-15; seen 2026-08-09 to 2026-10-14	Hunt
tycxnedns[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-07; seen 2026-08-01 to 2026-10-14	Hunt
tzawccsw[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-22; seen 2026-07-23 to 2026-07-23; clientHold	Block
uetrsd[.]suiyerjser[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-09-26; seen 2026-02-23 to 2026-10-14	Hunt
usetr[.]uydsecbjyge[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-09-26; seen 2026-07-10 to 2026-10-14	Hunt
uydsecbjyge[.]cyou	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-09-26	Hunt
vbndfge[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-05; seen 2026-08-07 to 2026-10-14	Hunt
vbsefaae[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-09; seen 2026-08-11 to 2026-10-14	Hunt
vnbhaytysw[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
vxiduyga[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-05 to 2026-07-05; clientHold	Hunt
whdusse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-30 to 2026-10-14	Hunt
www[.]thaigov[.]go[.]th[.]gothuy[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25; Thai government lure host	created 2026-02-08; seen 2026-09-03 to 2026-10-14	Block
wyasuda[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-07; seen 2026-08-09 to 2026-10-14	Hunt
wyctridea[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
xacyuiat[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-22; seen 2026-08-12 to 2026-08-12; clientHold	Hunt
xafgdvctw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-02 to 2026-10-14	Hunt
xauqeygar[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-06-10 to 2026-06-10; clientHold	Hunt
xauysfhyte[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-28; seen 2026-08-13 to 2026-10-14	Hunt
xbgsetewt[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
xciuyuas[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-06; seen 2026-08-08 to 2026-08-08; clientHold	Hunt
xcndyteer[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
xcuyeaet[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-25; seen 2026-08-11 to 2026-10-14	Hunt
xcvgyuraw[.]live	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-14; seen 2026-07-30 to 2026-07-30; clientHold	Block
xhastyese[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-28; seen 2026-06-30 to 2026-06-30; clientHold	Hunt
xiawytee[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-28; seen 2026-07-30 to 2026-10-14	Hunt
xiiuxcna[.]ink	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-05; seen 2026-08-07 to 2026-08-07; clientHold	Hunt
xiiuxcna[.]skin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-05; seen 2026-08-07 to 2026-08-07; clientHold	Hunt
xijbdgecr[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
xiusydba[.]live	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-13; seen 2026-08-01 to 2026-10-14	Block
xnbscuya[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-26; seen 2026-07-31 to 2026-10-14	Hunt
xsiyrytttde[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-08-02 to 2026-10-14	Hunt
xstvchfhd[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-30 to 2026-10-14	Hunt
xtaxutfaw[.]ink	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-08-14 to 2026-10-14	Hunt
xtaxutfaw[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-08-15 to 2026-08-15; clientHold	Hunt
xuaidjay[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt
xuastyrdqk[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-31; seen 2026-08-08 to 2026-10-14	Hunt
xuaytedgv[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-05 to 2026-07-05; clientHold	Hunt
xuaywttsa[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-06-26 to 2026-06-26; clientHold	Hunt
xucnvgjte[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-08-02 to 2026-10-14	Hunt
xudysytes[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-31; seen 2026-08-07 to 2026-10-14	Hunt
xusadtraw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-18; seen 2026-08-05 to 2026-10-14	Hunt
xusdtmcdra[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-18; seen 2026-06-20 to 2026-06-20; clientHold	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
xzdyattte[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-02	Hunt
xzystrbvnse[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-02; seen 2026-08-02 to 2026-10-14	Hunt
yasuhdeav[.]win	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-31; seen 2026-08-02 to 2026-08-02; clientHold	Hunt
yasyciuste[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-17; seen 2026-06-19 to 2026-06-19; clientHold	Hunt
ydufwyaxe[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
ysieiuhaw[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-09	Hunt
yswhg[.]kiafewoey[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]230	created 2025-10-09; seen 2026-10-04 to 2026-10-14	Hunt
yzytsrasca[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-26; seen 2026-05-28 to 2026-05-28; clientHold	Hunt
zasudtytw[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-22; seen 2026-07-23 to 2026-07-23; clientHold	Block
zdtrebdhr[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-02; seen 2026-07-04 to 2026-07-04; clientHold	Hunt
zidydrvds[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-30 to 2026-10-14	Hunt
zixhasda[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-21; clientHold	Block
zjkyewe[.]icu	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]25	created 2026-02-04; seen 2026-08-12 to 2026-08-12	Hunt
zlvbvyer[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-25; seen 2026-08-09 to 2026-10-14	Hunt
zocuyuefgd[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
zsucyrgs[.]xin	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-16; seen 2026-07-29 to 2026-07-29; clientHold	Hunt
zsyrtcmke[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-23; seen 2026-06-25 to 2026-06-25; clientHold	Hunt
zsyxmyur[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-03; seen 2026-07-05 to 2026-07-05; clientHold	Hunt
zusyyredrs[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-28; seen 2026-07-30 to 2026-10-14	Hunt
zuszdyyst[.]live	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-08-06; seen 2026-08-08 to 2026-08-08; clientHold	Block
zuxywrjcie[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-02 to 2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
zuytyarws[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-19; seen 2026-07-21 to 2026-07-21; clientHold	Block
zxaiasuye[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-24; seen 2026-08-03 to 2026-10-14	Hunt
zxcjyeahd[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-06-30; seen 2026-07-02 to 2026-07-02; clientHold	Hunt
zxiuusdtx[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-08-07; seen 2026-08-09 to 2026-08-09; clientHold	Hunt
zxizusuy[.]xin	Domain	Indian tax lure page host of July and August (one of the 18 pages)	created 2026-07-22; seen 2026-07-23 to 2026-07-23; clientHold	Block
zysawbbus[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-14; seen 2026-08-01 to 2026-10-14	Hunt
zytsyxbwa[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]15, the IP address of the Indian tax lure pages from mid July	created 2026-07-13; seen 2026-07-16 to 2026-07-16; clientHold	Hunt
zzisudted[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-05-31; seen 2026-08-12 to 2026-10-14	Hunt
zziyyterser[.]live	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117, the IP address of the June Indian tax lure pages	created 2026-07-01; seen 2026-07-03 to 2026-07-03; clientHold	Hunt
pmrravwg[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host; its saved June lure page links batch name ddisuyer[.]eu[.]cc	created 2026-06-19, expires 2027-06-19; clientHold	Block
psufuyvaw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-19, expires 2027-06-19; clientHold	Block
laiwnndye[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host; its saved June lure page links batch name pzidiauwytsd[.]eu[.]cc	created 2026-06-19, expires 2027-06-19; clientHold	Block
bxyawrgr[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host; its saved June lure page links batch name ddisuyer[.]eu[.]cc	created 2026-06-19, expires 2027-06-19	Block
kcetbftaw[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-25, expires 2027-06-25; clientHold	Block
lcvajwyt[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-25, expires 2027-06-25; clientHold	Block
svuatwea[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-05-26, expires 2027-05-26; clientHold	Block
qiawmcue[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-19, expires 2027-06-19	Block
uyfbbnstet[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-19, expires 2027-06-19; clientHold	Block
kisuytbze[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-19, expires 2027-06-19	Block
fuavyexr[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-25, expires 2027-06-25; clientHold	Block
pasoiuewuy[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-05-26, expires 2027-05-26; clientHold	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
vusuydryt[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-05-26, expires 2027-05-26; clientHold	Block
aymdkese[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host; its saved June lure page links batch name pzidiauwytsd[.]eu[.]cc	created 2026-06-19, expires 2027-06-19; clientHold	Block
kasiemmu[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-19, expires 2027-06-19	Block
ysicgtes[.]love	Domain	Domain of registrar account 574849-1923 on 103.23.172[.]117; June Indian tax lure page host	created 2026-06-19, expires 2027-06-19	Block
bvjse[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67978	created 2026-03-13 05:55:35; seen 2026-08-11 to 2026-08-11	Hunt
cuyew[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 67973	created 2026-03-13 05:42:44; seen 2026-08-17 to 2026-10-14	Hunt
cwtsh[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67642	created 2026-03-12 13:17:56; seen 2026-07-31 to 2026-10-14	Hunt
cysta[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65477	created 2026-03-09 06:40:19; seen 2026-08-14 to 2026-08-14	Hunt
dfyue[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67979	created 2026-03-13 05:56:13; seen 2026-08-11 to 2026-08-11	Hunt
dtrar[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67981	created 2026-03-13 05:58:23; seen 2026-08-16 to 2026-10-14	Hunt
duyey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67641	created 2026-03-12 13:17:08; seen 2026-08-16 to 2026-10-14	Hunt
evaet[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 69451	created 2026-03-17 07:57:26; seen 2026-08-12 to 2026-08-12	Hunt
fasytwa[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 87254	created 2026-04-03 04:28:58; seen 2026-08-14 to 2026-08-14	Hunt
fatw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 64433	created 2026-03-08 07:34:00; seen 2026-08-12 to 2026-08-12	Hunt
fegeu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65478	created 2026-03-09 06:41:05; seen 2026-07-30 to 2026-10-14	Hunt
fwiu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 64436	created 2026-03-08 07:37:31; seen 2026-08-06 to 2026-08-06	Hunt
fyaey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 67640	created 2026-03-12 13:15:50; seen 2026-08-14 to 2026-08-14	Hunt
gauteya[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 87256	created 2026-04-03 04:30:32; seen 2026-07-30 to 2026-10-14	Hunt
gdhe[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67997	created 2026-03-13 06:17:15; seen 2026-08-10 to 2026-08-10	Hunt
ghre[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67995	created 2026-03-13 06:16:29; seen 2026-08-12 to 2026-08-12	Hunt
hauwyc[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 87253	created 2026-04-03 04:28:25; seen 2026-08-13 to 2026-08-13	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
hawsu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 81055	created 2026-03-26 23:46:05; seen 2026-08-03 to 2026-08-03	Hunt
hcsyds[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85043	created 2026-04-01 03:43:50; seen 2026-08-09 to 2026-08-09	Hunt
hdsau[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 76016	created 2026-03-24 05:38:12; seen 2026-08-07 to 2026-08-07	Hunt
hdtgr[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67643	created 2026-03-12 13:19:43; seen 2026-09-29 to 2026-10-14	Hunt
heaqw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74893	created 2026-03-23 04:25:34; seen 2026-05-09 to 2026-05-09; clientHold	Hunt
hgsye[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 80536	created 2026-03-26 15:50:16; seen 2026-08-13 to 2026-08-13	Hunt
hiaoei[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85044	created 2026-04-01 03:46:04; seen 2026-08-02 to 2026-10-14	Hunt
hlsdleu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85047	created 2026-04-01 03:48:59; seen 2026-08-03 to 2026-08-03	Hunt
hsutfa[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85045	created 2026-04-01 03:47:17; seen 2026-07-31 to 2026-10-14	Hunt
htawau[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 80524	created 2026-03-26 15:42:14; seen 2026-08-02 to 2026-10-14	Hunt
htdfs[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85592	created 2026-04-01 16:07:18; seen 2026-05-08 to 2026-05-08; clientHold	Hunt
htgsds[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85556	created 2026-04-01 15:45:40; seen 2026-07-31 to 2026-10-14	Hunt
htiauwi[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85037	created 2026-04-01 03:42:00; seen 2026-08-13 to 2026-08-13	Hunt
htpaw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 77462	created 2026-03-25 02:53:44; seen 2026-08-12 to 2026-08-12	Hunt
htpzx[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 77460	created 2026-03-25 02:52:47; seen 2026-08-02 to 2026-10-14	Hunt
htsdjey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85557	created 2026-04-01 15:47:03; seen 2026-05-02 to 2026-05-02; clientHold	Hunt
htsra[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74925	created 2026-03-23 05:20:54; seen 2026-07-30 to 2026-10-14	Hunt
httcay[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85113	created 2026-04-01 07:31:48; seen 2026-08-12 to 2026-08-12	Hunt
httczey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 80475	created 2026-03-26 15:07:37; seen 2026-08-15 to 2026-10-14	Hunt
httdws[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74924	created 2026-03-23 05:19:59; seen 2026-08-08 to 2026-08-08	Hunt
httgasi[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 84164	created 2026-03-30 15:36:49; seen 2026-08-12 to 2026-08-12	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
httpaw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 70564	created 2026-03-20 08:13:38; seen 2026-08-08 to 2026-08-08	Hunt
httpitf[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 80471	created 2026-03-26 15:06:54; seen 2026-08-05 to 2026-08-05	Hunt
httpks[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 70567	created 2026-03-20 08:22:39; seen 2026-08-06 to 2026-08-06	Hunt
httpri[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 77463	created 2026-03-25 02:54:42; seen 2026-08-09 to 2026-08-09	Hunt
httpuay[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 81052	created 2026-03-26 23:43:47; seen 2026-08-09 to 2026-08-09	Hunt
httpyctw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 84166	created 2026-03-30 15:37:41; seen 2026-08-07 to 2026-08-07	Hunt
httpys[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 77469	created 2026-03-25 02:56:45; seen 2026-08-05 to 2026-08-05	Hunt
httpzae[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 77466	created 2026-03-25 02:55:40; seen 2026-08-01 to 2026-10-14	Hunt
httqatc[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 80477	created 2026-03-26 15:09:04; seen 2026-08-15 to 2026-10-14	Hunt
httqays[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 84165	created 2026-03-30 15:37:10; seen 2026-07-30 to 2026-10-14	Hunt
httqfs[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 80531	created 2026-03-26 15:43:25; seen 2026-08-16 to 2026-10-14	Hunt
httre[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74932	created 2026-03-23 05:24:35; seen 2026-08-05 to 2026-08-05	Hunt
httriuyw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 84171	created 2026-03-30 15:39:48; seen 2026-08-12 to 2026-08-12	Hunt
httsy[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74930	created 2026-03-23 05:23:24; seen 2026-08-12 to 2026-08-12	Hunt
httsya[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74906	created 2026-03-23 04:42:33; seen 2026-08-04 to 2026-08-04	Hunt
httvdfr[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85112	created 2026-04-01 07:30:56; seen 2026-08-10 to 2026-08-10	Hunt
httxza[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 74928	created 2026-03-23 05:22:13; seen 2026-08-14 to 2026-08-14	Hunt
httydaut[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85119	created 2026-04-01 07:38:09; seen 2026-04-22 to 2026-04-22; clientHold	Hunt
httysc[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74933	created 2026-03-23 05:26:03; seen 2026-08-04 to 2026-08-04	Hunt
httyust[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85114	created 2026-04-01 07:32:57; seen 2026-08-11 to 2026-08-11	Hunt
httzsx[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74971	created 2026-03-23 06:18:16; seen 2026-08-02 to 2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
htvdaey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85042	created 2026-04-01 03:43:12; seen 2026-08-01 to 2026-10-14	Hunt
htxeat[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 85607	created 2026-04-01 16:12:25; seen 2026-08-05 to 2026-08-05	Hunt
ifey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65473	created 2026-03-09 06:37:29; seen 2026-08-14 to 2026-08-14	Hunt
isfya[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65479	created 2026-03-09 06:41:34; seen 2026-08-14 to 2026-08-14	Hunt
isriy[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 61348	created 2026-03-05 16:28:39; seen 2026-08-06 to 2026-08-06	Hunt
iuwt[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 64430	created 2026-03-08 07:32:43; seen 2026-08-03 to 2026-08-03	Hunt
jrtsw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 69772	created 2026-03-18 05:06:46; seen 2026-08-11 to 2026-08-11	Hunt
ksiey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 69449	created 2026-03-17 07:56:08; seen 2026-08-11 to 2026-08-11	Hunt
ncyea[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 74895	created 2026-03-23 04:27:57; seen 2026-07-31 to 2026-10-14	Hunt
pdsishf[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 87252	created 2026-04-03 04:27:50; seen 2026-08-08 to 2026-08-08	Hunt
psaudr[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry n/a	created n/a; seen 2026-04-22 to 2026-04-22	Hunt
qiat[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 64434	created 2026-03-08 07:34:33; seen 2026-08-07 to 2026-08-07	Hunt
qiuafs[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 87251	created 2026-04-03 04:27:15; seen 2026-04-21 to 2026-04-21; clientHold	Hunt
ratws[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 70164	created 2026-03-19 06:41:29; seen 2026-08-08 to 2026-08-08	Hunt
rdyue[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 87250	created 2026-04-03 04:26:45; seen 2026-08-07 to 2026-08-07	Hunt
rtga[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 64438	created 2026-03-08 07:37:43; seen 2026-08-01 to 2026-10-14	Hunt
sfywe[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 74908	created 2026-03-23 04:45:03; seen 2026-08-14 to 2026-08-14	Hunt
siaw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 61354	created 2026-03-05 16:33:29; seen 2026-08-01 to 2026-10-14	Hunt
soieu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 66971	created 2026-03-11 06:16:29; seen 2026-08-10 to 2026-08-10	Hunt
srtis[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65475	created 2026-03-09 06:38:46; seen 2026-08-13 to 2026-08-13	Hunt
strdi[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65482	created 2026-03-09 06:42:41; seen 2026-07-30 to 2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
syeg[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67607	created 2026-03-12 12:23:19; seen 2026-08-03 to 2026-10-14	Hunt
sytae[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67980	created 2026-03-13 05:57:50; seen 2026-08-06 to 2026-08-06	Hunt
taayt[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 66974	created 2026-03-11 06:17:55; seen 2026-07-31 to 2026-10-14	Hunt
tadwy[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 76014	created 2026-03-24 05:37:19; seen 2026-08-02 to 2026-10-14	Hunt
tarey[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65476	created 2026-03-09 06:40:15; seen 2026-08-05 to 2026-08-05	Hunt
tayzcur[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 87255	created 2026-04-03 04:30:00; seen 2026-08-11 to 2026-08-11	Hunt
uiaef[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65480	created 2026-03-09 06:42:08; seen 2026-08-08 to 2026-08-08	Hunt
vaytw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 66973	created 2026-03-11 06:17:19; seen 2026-08-04 to 2026-08-04	Hunt
vcfdt[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65484	created 2026-03-09 06:43:35; seen 2026-08-02 to 2026-10-14	Hunt
vdfwa[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 69773	created 2026-03-18 05:07:09; seen 2026-07-31 to 2026-10-14	Hunt
vuyat[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67974	created 2026-03-13 05:43:43; seen 2026-08-02 to 2026-08-02	Hunt
xaie[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 64439	created 2026-03-08 07:37:43; seen 2026-07-30 to 2026-10-14	Hunt
xaisu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 76017	created 2026-03-24 05:39:18; seen 2026-08-13 to 2026-08-13	Hunt
xaut[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 61521	created 2026-03-06 04:34:25; seen 2026-08-14 to 2026-08-14	Hunt
xdie[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 64435	created 2026-03-08 07:36:02; seen 2026-08-04 to 2026-08-04	Hunt
xoeyu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 66970	created 2026-03-11 06:15:56; seen 2026-08-09 to 2026-08-09	Hunt
xoqu[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 64431	created 2026-03-08 07:33:23; seen 2026-08-03 to 2026-08-03	Hunt
xsiw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 61350	created 2026-03-05 16:30:09; seen 2026-08-04 to 2026-08-04	Hunt
xteue[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 69450	created 2026-03-17 07:56:41; seen 2026-08-12 to 2026-08-12	Hunt
xyiau[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 70165	created 2026-03-19 06:42:50; seen 2026-08-10 to 2026-08-10	Hunt
yagw[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 61528	created 2026-03-06 04:36:40; seen 2026-07-31 to 2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
yatna[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74894	created 2026-03-23 04:26:54; seen 2026-08-06 to 2026-08-06	Hunt
ydfue[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 67994	created 2026-03-13 06:15:50; seen 2026-08-11 to 2026-08-11	Hunt
ydtew[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]25, registry 67976	created 2026-03-13 05:54:29; seen 2026-07-31 to 2026-10-14	Hunt
ytahf[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 67998	created 2026-03-13 06:17:51; seen 2026-08-08 to 2026-08-08	Hunt
ytrud[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 65474	created 2026-03-09 06:38:10; seen 2026-07-30 to 2026-10-14	Hunt
yudts[.]eu[.]cc	Domain	Single eu.cc name on 103.23.172[.]230, registry 74907	created 2026-03-23 04:43:39; seen 2026-08-07 to 2026-08-07	Hunt
e-tzxarw[.]jp	Domain	Japanese e-Tax lookalike on 103.23.172[.]118; contact is a privacy relay shared with e-tzsgzxyu[.]jp	created 2026-09-14; seen 2026-09-17 to 2026-10-14	Hunt
e-tzsgzxyu[.]jp	Domain	Japanese e-Tax lookalike on 103.23.172[.]15; same privacy relay contact	created 2026-09-14; seen 2026-09-17 to 2026-10-14	Hunt
vbaesta[.]live	Domain	Served one object of the file sharing application on 103.23.172[.]230	2026-09-08	Hunt
cao[.]tedboscomwe[.]com	Domain	Served ZIP-20260824011202.92B2DAACC45A.zip (12f496cd), which contacts usdt888[.]club	2026-08-27	Block
hxxps://cao[.]tedboscomwe[.]com/ZIP-20260824011202.92B2DAACC45A.zip	URL	Download of the usdt888[.]club package 12f496cd	2026-08-27	Block
72.11.130[.]248	IPv4	IP address of cao[.]tedboscomwe[.]com	2026-08-27	Hunt
gzsgdn[.]com	Domain	Click tracker chain; served 20260810124517.A8F39C2D71BE.zip (c949596a)	2026-08-10	Hunt
dianji[.]gzsgdn[.]com	Domain	Click tracker host of gzsgdn[.]com	2026-08-10	Hunt
hxxps://gzsgdn[.]com/20260810124517.A8F39C2D71BE.zip	URL	Download in the kit archive naming	2026-08-10	Block
dltwum[.]com	Domain	Click tracker chain to an Alibaba Cloud OSS bucket	2026-08-10	Hunt
tongji[.]dltwum[.]com	Domain	Click tracker host of dltwum[.]com	2026-08-10	Hunt
8.211.182[.]27	IPv4	IP address of gzsgdn[.]com and dltwum[.]com on one day	2026-08-10	Hunt (dated)
kiuwjeq0810[.]oss-ap-northeast-1[.]aliyuncs[.]com	Domain	Cloud storage bucket that served 20260810134755.B7D42E8C91AF.zip (293c05f0)	2026-08-10	Hunt
hxxps://kiuwjeq0810[.]oss-ap-northeast-1[.]aliyuncs[.]com/20260810134755.B7D42E8C91AF.zip	URL	Download in the kit archive naming	2026-08-10	Block
gjtuerqw-1433552157[.]cos[.]ap-hongkong[.]myqcloud[.]com	Domain	Tencent Cloud COS bucket reached from SendGrid u48334250; served 20260830213443-BECCD7053B19.zip (85a0a2e4)	2026-08-31	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
gin[.]gl/RQ4Bq	URL path	Short link in the SendGrid u48334250 chain	2026-08-31	Hunt
divsoftware[.]nl/s/techn	URL path	Redirect step in the SendGrid u48334250 chain; the site may be compromised, so hunt on the full path only	2026-08-31	Hunt
hckjnkjnaxanxdmdjp[.]pages[.]dev	Domain	Cloudflare Pages front of the hcnaxnkxankknjp[.]com download path (technical annex section A4.7)	2026-09-01 to 2026-09-11	Hunt
hcnaxnkxankknjp[.]com	Domain	Served 20260901014335-71359EDFC0A5.zip (a2fd0212) and 20260902114342-063801A8ED70.zip (709ba0d9) through icloud.php	2026-09-01 to 2026-09-11	Hunt
hxxps://hcnaxnkxankknjp[.]com/icloud.php	URL	Download script of the hcnaxnkxankknjp[.]com download path (technical annex section A4.7; token parameter varies)	2026-09-01 to 2026-09-11	Hunt
103.118.42[.]40	IPv4	IP address of hcnaxnkxankknjp[.]com	2026-09-01 to 2026-09-11	Hunt (dated)
floral-tree-1723[.]robertsmayer5182189[.]workers[.]dev	Domain	Worker host listed with the hcnaxnkxankknjp[.]com download path (technical annex section A4.7)	2026-09	Hunt
u53630135[.]ct[.]sendgrid[.]net	Domain	SendGrid click host whose link led to the delivery host	2026-07-29	Hunt
guaolheru[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-07-27	Hunt (context)
chiulmrtvuk[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-07-29	Hunt (context)
actv666[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-04	Hunt (context)
apcv207[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-07	Hunt (context)
acms555[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-09	Hunt (context)
acuf444[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-09	Hunt (context)
cheulmri[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-09	Hunt (context)
wheiulmra[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-09	Hunt (context)
at77712[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-10	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
baieoaze[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-10	Hunt (context)
bwobek[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-10	Hunt (context)
geco249[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-10	Hunt (context)
accfe01[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-11	Hunt (context)
biaoisdiu[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-11	Hunt (context)
chaaeeuro[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-11	Hunt (context)
qzqy688[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-11	Hunt (context)
weqt588[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-11	Hunt (context)
zhatv663[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-11	Hunt (context)
juea802[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-12	Hunt (context)
bbtsoe[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-13	Hunt (context)
incometaxind[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); Indian tax lookalike name	created 2026-08-14	Hunt
caiyun1[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24 at 202.61.85[.]181 (IP address range carries no weight)	created 2026-08-18	Hunt (context)
fattoea[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-19	Hunt (context)
hevk66b[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-19	Hunt (context)
wheulmuv[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-19	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
wheulmuv[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-19	Hunt (context)
incumetaxineia[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); Indian tax lookalike name	created 2026-08-20	Hunt
incumetaxineia[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); Indian tax lookalike name	created 2026-08-20	Hunt
awlxeu9[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-23	Hunt (context)
bokzcc8[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-23	Hunt (context)
incogtaxbbo[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); Indian tax lookalike name	created 2026-08-23	Hunt
vvazwc1[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-23	Hunt (context)
ct4vk1d[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24, on 202.61.85[.]114 from 2026-08-27	created 2026-08-24	Hunt (context)
baouie2[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-26	Hunt (context)
bshysofkt[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-27	Hunt (context)
evubt8z[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-30	Hunt (context)
ayowo8b[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-08-31	Hunt (context)
e1gbthu[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-01	Hunt (context)
iedgc4z[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-01	Hunt (context)
rezmv3s[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-01	Hunt (context)
baieoa1[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-03	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
fwnjz[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-03	Hunt (context)
baieoc2[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-05	Hunt (context)
btimve4[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-05	Hunt (context)
buieve3[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-05	Hunt (context)
irddov[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-06	Hunt (context)
dbc3do8[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-10	Hunt (context)
e7k3vw5[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-10	Hunt (context)
qztt688[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24 at 202.61.85[.]168 (IP address range carries no weight)	created 2026-09-10	Hunt (context)
ackp1o5[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24, on 202.61.85[.]190 from 2026-09-15	created 2026-09-13	Hunt (context)
mfn2uau[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-14	Hunt (context)
kvqunru[.]work	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-15	Hunt (context)
o2ycefv[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-16	Hunt (context)
bsotfo2[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-20	Hunt (context)
qemf4e[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-20	Hunt (context)
rencsu1[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-20	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
zrbhfn3[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-20	Hunt (context)
avmd2t[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-21	Hunt (context)
bbdw3c[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-21	Hunt (context)
bisuroa[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-21	Hunt (context)
eabiur6[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24 at 202.61.85[.]116 (IP address range carries no weight)	created 2026-09-21	Hunt (context)
nnkkbk7[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-21	Hunt (context)
rumrwe8[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-21	Hunt (context)
uddxse1[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-21	Hunt (context)
yqfoke9[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-21	Hunt (context)
b5dwvc[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-22	Hunt (context)
pnoy6u[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-23	Hunt (context)
rqew7o[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-09-23	Hunt (context)
arum21[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
bfax7[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
cmrv25[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
dtfva6[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
gntr30[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
htif12[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
hurt5[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
hzdv29[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
ixee18[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); served a fake software download page on 156.251.11[.]56	created 2026-10-04	Hunt
khltt1[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24 at 202.61.85[.]151 (IP address range carries no weight)	created 2026-10-04	Hunt (context)
khst2[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
kufp16[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24 at 202.61.85[.]233, now 23.226.57[.]52 (IP address range carries no weight)	created 2026-10-04	Hunt (context)
kyvs17[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
pmae14[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
pzfy4[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
rkke24[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
rtce11[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
scnk3[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
suvh9[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
tidm15[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
trzv23[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
tvft28[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
usod22[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); in 202.61.85[.]0/24 at 202.61.85[.]170 (IP address range carries no weight)	created 2026-10-04	Hunt (context)
utjs27[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
uvmz26[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
uykb10[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
wvlh8[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
wvxl19[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
yac13[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
yfth20[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-04	Hunt (context)
chaieo[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-06	Hunt (context)
podnline[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-06	Hunt (context)
1euwwn[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-11	Hunt (context)
3d22cx[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-11	Hunt (context)

Value (defanged)	Type	Role	Observed (UTC)	Use
8ozrdoi[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-11	Hunt (context)
pm3c4y[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found); scanned on port 6803	created 2026-10-11	Hunt (context)
u1km69[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-11	Hunt (context)
v3ndpr[.]club	Domain	KANGYINGJIE domain at 22net (one record in registration data we found)	created 2026-10-11	Hunt (context)
mailio[.]club	Domain	ZHENGJUNHUA domain at 22net (one record in registration data we found)	created 2026-08-25	Hunt (context)
inword[.]club	Domain	ZHENGJUNHUA domain at 22net (one record in registration data we found)	created 2026-09-01	Hunt (context)
ceoword[.]club	Domain	ZHENGJUNHUA domain at 22net (one record in registration data we found)	created 2026-09-02	Hunt (context)
log1n[.]work	Domain	ZHENGJUNHUA domain at 22net (one record in registration data we found); served a Japanese Proton Mail phishing page on 198.44.182[.]48	created 2026-09-20; seen 2026-09-30	Hunt
hxxps://dnswwt[.]club/down/file.zip	URL	ZIP of 59 MB on dnswwt[.]club (181.214.250[.]174)	2026-09-20	Hunt
hxxps://dnswwt[.]club/down/setup.aac	URL	Download path on dnswwt[.]club (181.214.250[.]174)	2026-09-20	Hunt
156.251.11[.]56	IPv4	IP address of ixee18[.]club with a fake software download page	after 2026-10-04	Hunt (dated)
198.44.182[.]48	IPv4	IP address of log1n[.]work with a Japanese Proton Mail phishing page	2026-09-30	Hunt (dated)
homeysion[.]work	Domain	CENGCHAO domain at 22net; Hong Kong lottery page on 121.127.254[.]69	created 2026-03-24, expires 2027-03-24; seen 2026-10-07	Hunt (context)
121.127.254[.]69	IPv4	IP address of homeysion[.]work with a Hong Kong lottery page	2026-10-07	Hunt (dated, context)
23.226.57[.]52	IPv4	Later IP address of kufp16[.]club, a KANGYINGJIE domain	after 2026-10-04	Hunt (dated, context)

Table B: Network indicators of the operation, its delivery and its registrant identities. clientHold means that the registrar has put the domain on hold at the registry.

C. File indicators

Table C lists every file by SHA-256. It includes 138 further kit builds and carriers found by the DHS seal or the Spanish cover application, 107 of them further unwrapped builds with the seal, first seen from 2026-08-13 to 2026-09-22 (report section 3.3 and Annex section A3.8). Rows marked Never block are genuine signed vendor programs.

Value (defanged)	Type	Role	Observed (UTC)	Use
37ff47383d607b4f33db8e6aec817cecff5c1af729628031f7a113fdd1a2f1a0	Icon resource hash	Icon resource: the U.S. Department of Homeland Security seal (RT_ICON 10, 256 px PNG, 95,141 B); hunt on carved resources only		Hunt
1dd6a5e79412c48bbe5920ab491c28d2	Icon resource hash	Icon resource: 48 px member of the seal icon group		Hunt
5b896138d41d4662a93a7ebaf6e15cebdc5a2850e9343da05c2ab1862ec31a3f	SHA-256	Loader B1 (first sample), the operation	2026-08-19	Block
d917915320d87f797ca7a86492af54f8ea9004987bb9ccb83eed0e72d66ed96	SHA-256	Loader B2, the operation	2026-08-24	Block
3dc4d9df6532fdb7b1e69242ecd59700704a9cb77cbb9af9e49469a351d47277	SHA-256	Loader B3, the operation	2026-08-21	Block
a0160e1fb98ba8d27b0849bf68eadbfc3919a12207fbd329aa11efa41e16a5f4	SHA-256	Loader B4 (hdp.dLL), the operation	2026-08-20	Block
f42c77fc05af60b8e702ab357714890d2ce17419d63bcc108f00be7733e8c7c5	SHA-256	Loader B5, the operation	2026-08-19	Block
bf5034213ac74e8cd279b1a5edaeab194fb7192e449f0b7d29bc0b8e339b2b80	SHA-256	Loader B6, the operation	2026-09-22	Block
a5bab85507e9ce4f56dfe8412a1f46612aec23fa42c86cea089d5ac12c5e4e2f	SHA-256	Loader B7 (hdp.dLL), the operation		Block
2ff861c4916c289ad474c7d8cbcc78c495c5f5638a78d567cd25783e9eee2591	SHA-256	Loader B8 (fake libcef.dll / GfeXCode.dll), the operation	2026-09-18	Block
60243bb550ac179742f6e22a1819c02092ba9d03b888cf7be241b473b5adeb3c	SHA-256	Loader B9 (ARPHADUMP.Dll), the operation		Block
faac737c6d575b1f5be3d0391d8bb34354010cb6de6dbfa84c3131cf5ef1ea82	SHA-256	Loader F1 (xwEB_eLF.dLl)	2026-09-02	Block
2960996c578dbe3f11016420220fe42967a9554fef0a1de67ad718e04660a36a	SHA-256	Loader F2 (RPABUILDER.DLL)	2026-09-04	Block
1850e93db051b17becfea9775f0a0241d565de30b9059e5122589fce0e31725a	SHA-256	Loader of C15 (hdpGmS.DlL), the operation	2026-08-17	Block
d7b7cec28ea90b651e77450011864e756baf721e226827727fe67f7d2502a9ce	SHA-256	Loader of C17 (hdp.dLL), the operation	2026-08-20	Block
6620e9ad75919ff168183d2c6bb4fc13870cbf4573da45b859bdd031227d790c	SHA-256	Delivery package of C15 (Tax-Number852690.zip), the operation	2026-08-17	Block
feb58c7b63cdd7b1a4300f43646914f3e8cb92bd0f061113997ed5bd4f892582	SHA-256	Delivery package of C17 (Tax-Number852693.zip), the operation	2026-08-20 to 2026-08-29	Block
b292de38fda529070124638f89b6b6299553250aa56aadf3f59d3c98c3e8b15e	SHA-256	Delivery package of B4 (Tax-Number852694.zip), the operation	2026-08-20 to 2026-08-31	Block
e057dd3f53c140ef1f6f90c7d539782ca8308a9a0154a5f27d659b66aac9f3a4	SHA-256	Carrier of B4 (INT-Number.20260820113657.IMG), the operation		Block
02a39ca8ca9c8afe3d6082901d4feeec3ccb98650c76fc010a77b149d092c76a	SHA-256	Carrier of B9 (first VHDX kit, 36251322092026.71A.vhdx), the operation	2026-09-22	Block
33d5170dbbaba3b5ffb6f477a1a41ab2a8c9aea82783d63c50ba7266e77202e4	SHA-256	Carrier of B7 (second VHDX kit, D33F785B2C901FE1ADBCF1746E5F6268.vhdx), the operation	2026-09-23	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
da36a96f05040e462650fd8feb8e409716675aeb8886fd6f4b007afe806745e7	SHA-256	Delivery package of F1 (20260902110114-0AFC3F174BAD.zip)	2026-09-02	Block
ddd7c0e176f2d1a9f7e05df7d6ae27ea9e7397fae400b88fbbddcb75f6143dd8	SHA-256	Carrier of F1 (_T.0902110038.VHD)		Block
d4a8b9d3df24f8bc11370d4c77507897d4ba09709755f044dec5503e6b057e29	SHA-256	Delivery package of F2	2026-09-04	Block
11661437d7e37cf86acfdbb4edfcbbacc9b17ff08594b99b513c8d2aee535025	SHA-256	Carrier of F2 (ITD-2002150409.img)	2026-09-04	Block
9e05ace962019dc7796d0abb3bee9f5ab453c5753cb140d7d52177b67d8c5fb1	SHA-256	Carrier of the tax dropper (RAR5)		Block
8d4c7a2f613ccf013e61a82307a63b06792c206b9c35b516ad8fbc819aca2b57	SHA-256	Carrier of the tax dropper twin (RAR5)	2026-09-24	Block
c977a12d91331ddcc0bc71692ab423344cfac9eef252c8f6e019bae1b777206e	SHA-256	Carrier of the Rust dropper (RAR5)		Block
6c3d59d82c2ab7392d793f39de3250605a9bb913890534a20f23f2f04de5e584	SHA-256	Carrier of 67e1ac14 (Notice from Tax Departmen.IMG)	2026-08-11	Block
8ad0f9b60c16107a4c71f9d3dff024299cef429efe5ca0bee982a8346aebee02	SHA-256	Carrier with a Spanish tax lure (Notificación del Departamento de Impuestos.img)	2026-08-18	Block
e0e1ffe72e09c0fa065cc0323cadddd8b01203ee1e4ccf770678099a1f0ca61f	SHA-256	Carrier with a Portuguese tax lure (Penalidade fiscal.img)	2026-08-19	Block
12f496cdcf357d55002675e562864d201ecb9cd5956f76958da855ca9bf299d7	SHA-256	Delivery package (ZIP-20260824011202.92B2DAACC45A.zip), the operation, usdt888[.]club line	2026-08-24 to 2026-08-27	Block
e80a531506184d0df8e31e6534fdc3d00965109b1a4ca731dee007d4329da40c	SHA-256	Tax dropper (Notice from Tax Departmen.exe)		Block
38955b79b40bcbfc1bd07e97cba0d7ba700e2f0c46e4b6f944dcf759d37f6edd	SHA-256	Tax dropper twin (E37F81F5B2C901FE1ADBCF1746E5F6268.exe)	2026-09-24	Block
ce79c9f299c88c7bff93aa9d3116c0496352b1ef820176e290936e7f64635abf	SHA-256	Rust dropper (D43F785B2C901_20260924128 41.exe)		Block
d93d51320f9a206bdf0af70669763ac34fcfdaa3e6d66b711289fd62713dc486	SHA-256	Vulkan proxy (vulkan-1.dll)		Block
67e1ac1423eabe185f870744acc9ad7526ee716c60e552fdfa6976aad9bdf453	SHA-256	Pre seal build 67e1ac14 (NvSmartMaxapp.dll, side loaded as pdfcoRE8.DlL)	2026-08-11	Block
cc9dd67664c7aeace554d70bdf08ba06005dc48a32f44245e7a0a4feb7ca4b25	SHA-256	Build with the DHS seal (InstallerExtension.dll)	2026-08-13	Block
66f1eb688e731d181e93726de47fa3df33dad5a80d1445b2b2e747615034f7c8	SHA-256	October re-packed copy (BugSplatNative.dll / hdp.dll)	2026-10-14	Block
7cc3884de68377d36601d5802b37e1cf8ae9a6cf64659619919328eeccd0461b	SHA-256	October re-packed copy (BugSplatNative.dll, 24.86 MB)	2026-10-14	Block
9b70faebdf93666f395f2d478db889df0f4198cd6ad2bd80ac76888077a3f15f	SHA-256	October re-packed copy (hdp.dll)	2026-10-14	Block
67641302fd91d61ca60f610df0dee58cb8564ec3e7081a62ade88cb68b2a4e45	SHA-256	October re-packed copy (hdp.dll)	2026-10-14	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
578b00dd0e48215aacaf97c8e9d90ee34562b745df0ddb333a8cdf383a072506	SHA-256	October re-packed copy (hdp.dll)	2026-10-14	Block
29d7b3d3a47cca1f0778702b17e03df31dab89cda667a20ca0f84485baf85ebe	SHA-256	October re-packed copy (hdp.dll)	2026-10-12	Block
6dc6af4769d61080ec154d98c19a8c8b6fc98d0be8c045d1e940906e655df4fe	SHA-256	File served by the delivery host kaiwyrey[.]eu[.]cc after F2	2026-09-04 to 2026-09-06	Hunt
28958b5dd326237001073e233e255b3cfd94ee752fa78143fff650b1ac09e608	SHA-256	File served by the delivery host kaiwyrey[.]eu[.]cc	2026-09-08 to 2026-09-15	Hunt
2c16aed029639d620cec9ac212ec3ce3118ac8ad403eb324826ae503ab7313a0	SHA-256	File served by the delivery host kaiwyrey[.]eu[.]cc	2026-08-18	Hunt
4f0850345944e0d0795501c107e3cf6855814c07e679f4095ac45cb80064afd5	SHA-256	Delivery package served by the delivery host kaiwyrey[.]eu[.]cc (Tax-Number852691.zip)	2026-08-18	Hunt
6b97957b0698446932f14c5d6d74a425b9732b8aaef9e4925ecb5348c01a437e	SHA-256	Package served by the delivery host kaiwyrey[.]eu[.]cc (20260728151147.zip)	2026-07-28	Hunt
aa1b45d0c5384d740c625c907b3f44ada18b0230f6e8dea33935ebd3db3ac72c	SHA-256	Package served by the delivery host after an email click (20260729104357.zip)	2026-07-29	Hunt
c5c138b5742de7018cca4d905d3d56c82ae4040983f1d1ec4ad0e4fe9793e524	SHA-256	x64 kit build of a third x64 compile that contacts 156.245.245[.]235		Hunt
6a70b0d468d9dbe370be7e410a1d59f4e645447c26a58e047c2fd51c214bdfcc	SHA-256	Encrypted stage resource ZH_TW (watchdog template) of F1 and F2		Hunt
10ced9fa6a38ad4c713b8e967b9d2672008a2b8ab8da1fb226c4d7bc1389e9b6	SHA-256	Encrypted stage resource ZH_CN or ZH_HK (embedded x64 driver) of F2		Hunt
cb870d5980a836f886ffa6e8df64ed2b83755963e7071dcbb8c186fbb749a92f	SHA-256	Encrypted stage resource ZH_CN or ZH_HK (embedded x64 driver) of F2		Hunt
7ceaf1c25c20f2794473149fc6099e49e0a11366c1acf9136c49066b9f5f290c	SHA-256	Encrypted stage resource ZH_CN or ZH_HK (embedded x64 driver) of F1		Hunt
97553afaccaa7e29034243dfba417a00f3d4519c61efdaae15364b11476c4678	SHA-256	Encrypted stage resource ZH_CN or ZH_HK (embedded x64 driver) of F1		Hunt
363e5db207bcc5702a61917991a1647e5a0cab822ae19440248bacc8c52791b8	SHA-256	Decrypted watchdog .cmd template (from NVAPO86V)		Hunt
b2ee510d0b5012487dee143b459e4e2fcfb758960d3fe7ec4743552bc91be9e2	SHA-256 (legitimate signed host)	Legitimate signed host abused for side-loading (arphaCrashReport.exe); not an indicator		Never block
53a4e54f23228c129e2f3d6f34ac457878e49ed2bb5ac13f05c10a55693d2dd8	SHA-256 (legitimate signed host)	Legitimate signed host abused for side-loading (hxdaemonprocess.exe); not an indicator		Never block
233a7de23438d09cbb277a0ebb11f71a2af9c53d2cf5ac9e4af368de0bf20a3f	SHA-256 (legitimate signed host)	Legitimate signed host abused for side-loading (hxdaemonprocess.exe); not an indicator		Never block
259ce06bf148c971334414bb77fe26a839ebf7098603c11b763ef0bbf2b298e7	SHA-256 (legitimate signed host)	Legitimate signed host abused for side-loading (ShadowBot debugger.host.exe); not an indicator		Never block
0fdb63034c7c655e05b3a7725d5e2776606c323ae534bf6f30cd9eeadb3a879d	SHA-256 (legitimate signed host)	Legitimate signed host abused for side-loading (Tencent WeChatAppEx.exe 2.5.6.25506); not an indicator		Never block
b869fbddbda07a9b4e511f533b4b7ac2a161cc88dae0519e0e55347c74db94a8	SHA-256 (legitimate signed host)	Legitimate signed host abused for side-loading (ZEON ConvertToPDF.exe); not an indicator		Never block

Value (defanged)	Type	Role	Observed (UTC)	Use
21cf7a17569852a7a4c93ea9faf1478b0a08b9695acf56f10d597e86cac8aed9	SHA-256 (legitimate signed host)	Legitimate signed host abused for side-loading (ZEON ConvertToPDF.exe); not an indicator		Never block
a5fad3d78a6c7592176718cb852aa46839dc72d131400f00e534dcb2b1d525ee	SHA-256 (legitimate signed host)	Legitimate signed host (JetBrains keytool.exe) in the padded x64 loaders; not an indicator		Never block
233086e7d57e16523ac3463df306cfc497a9ba3c3e8268f62c8625ef56b2380e	SHA-256 (legitimate signed host)	Legitimate signed host (JetBrains rmiregistry.exe) in the padded x64 loaders; not an indicator		Never block
1fae7d654695f7c4e0f4bb8a42a4c33137652effc360b998708c6ffcac1380e6	SHA-256 (legitimate signed host)	Legitimate signed host (Google platform_experience_helper.exe) in the padded x64 loaders; not an indicator		Never block
0a1fd68a1fbab226ed926977f89df6621713aac36da7ee076a30db99d8be4c5c	SHA-256 (legitimate signed host)	Legitimate signed host (Siber Systems GoodSync LogView.exe) in the padded x64 loaders; not an indicator		Never block
1ffc8bde92758bc0d2ddcc5a6bb78c73b6409429e52d62191f25afa8ebfad84a	SHA-256 (legitimate signed host)	Legitimate signed host (BugSplatHD.EXE) in the padded x64 loaders; not an indicator		Never block
e388eb34fe4d280633609f6acec12a3e73c288f8b69ce402c3d24c0d0f5524f3	SHA-256 (legitimate signed host)	Legitimate signed host (Microsoft LINK.EXE) in the padded x64 loaders; not an indicator		Never block
77a03e8d48a0dca9c736d04dc6a6ab9aa74dc7445bea203937506da1edc03b44	SHA-256	Package of the padded x64 loaders (Tax-Number635863.zip); not tied to the operation	2026-07-17 to 2026-07-21	Hunt
747124f46aeb58132a904be14c9839bc167b8a58051f7e946dc41fe6a625703d	SHA-256	Package of the padded x64 loaders (Tax-Number735863.zip); not tied to the operation	2026-07-23	Hunt
f1b311418d6ccfe5564ffe2789e446974be55498ee22b133ffc9725ba25adfb2	SHA-256	Padded proxy DLL of the padded x64 loaders (jli.dll); not tied to the operation	2026-07-17	Hunt
5c373876a8809d503a329b528f44ec6cbaa2eae834b560be0ea819ce532dc4e6	SHA-256	Padded proxy DLL of the padded x64 loaders (Secur32.dll); not tied to the operation	2026-07-23	Hunt
67631fba728076b90ace6786d9eacfb46d5c06548054980667227f2666911b94	SHA-256	Image of the padded x64 loaders (Tax-Number723863); not tied to the operation	2026-06-05 to 2026-06-07	Hunt
7c8395ccb094b133c8a035bfb0bd08480073237b7e49f24a05e23fccffa14b46	SHA-256	Image of the padded x64 loaders (Tax-Number223863); not tied to the operation	2026-06-05	Hunt
d0c2f5ccb846ddc425e154f3d0d5ef350dc0b609790d315072484804ebc40f8c	SHA-256	Image of the padded x64 loaders (Tax-Number119863); not tied to the operation	2026-06-17	Hunt
e329a261e98d890fb4184ac6ccbaf4a2b39335f87d20e1f383cfa89394bc32d2	SHA-256	Image of the padded x64 loaders (Tax-Number919863); not tied to the operation	2026-06-19 to 2026-06-20	Hunt
12193e11ce3ac232aeccc85f5b05c0b6e36dee3f02c8ce45888de1188db8a3cb	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
01ecdfb680f9abb5929b35d89ee63de83e2b3ef6e38d8a04d3916955c12ee140	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-12	Block
45f45a4cde28dc659d3de0e5a4a94ad16cc7063e5bd827fdefdc89d0c76a1818	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
0505f40d42a00fea1cc43f5c6c57ac57a1f0cdad95c3126963e02acae8cbc6af	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-06	Block
bae6976823c2f44fd6043fdcafb62fc031dcf883d362b37e2177f6cb2bf75229	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
05e27d19390174e3984263f08f5298ac01df16479dab7def7bca3ee2ed485c60	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-05	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
0b7ad10b3157c88837d5b101675cdeae63bd315abb6e17dfd928ced7c9e1b9c3	SHA-256	Loader of an early build with the DHS seal, the operation	2026-08-13	Block
29c3b1212795dc85daa518a93691a21308781b24c87d921f2fb286752c8a47c9	SHA-256	Loader of the oswin build (outside the operation)	2026-09-02	Block
2df75ca7f44c3fc5b6b7d27ddbf9860d654c1b000e3fd6bfc2d181ccc92a5a24	SHA-256	Loader of an x64 build of the 2026-09-03 compile, the operation	2026-09-07	Block
31cb9374093e54220d67f266e19da27468f664e0be2bf674b764041756393ce4	SHA-256	Loader of an x64 build of the 2026-09-03 compile, the operation	2026-09-04	Block
323f6232ce475bf0fd9812a5fbdef194aaf7c4eb01854749500a9bc0bb09c02a	SHA-256	Loader of an x64 build of the 2026-09-03 compile, the operation	2026-09-05	Block
e4e94604d0c73e1d5e4bd6855f2dd0c91d7e884512aa4eed8b63fa69e2a91391	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
397b72923f2bf9eae7d9eeb9f576889e5048bd1c5ca9a923bead1d1e975131fe	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-03	Block
c7d77add01e19ac3a47386d563d9cabacb72bcab4359f9e7200188396e334df3	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
43c28f6f7aa498ef0e76c8e338c2942d5e62696c73d65de3e1a0d63fc6780f1e	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-10	Block
6d76680c3319eb999bbbb776437a39b7c6d2c6ab0be776b431e061e6723fd4ca	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
50f667b15dbcbe8068f55f87e5e62fce7d3f6c4c6cbe60931193815eb1b07763	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-09	Block
854708d8856210aa230479ebf70d77bae9ba9fa63404c1d3de1081c8fdb89220	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
52f3736ca57fd547f8360ad3f07b9e7ce5f62adbbc95b1d7df95b547d648b097	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-11	Block
56b7cbf67984610d0b1291eba7e137ce1cfbe6abf6268cd497d0f543ef727709	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-06	Block
3cdf7e3999c68e837b015e63240ae73961da2cd583306dd988980f1499dd74ef	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
7582528e3cd907d509f6478f2a19c2ee642dd5f79f006b45bde26f607d8f3f3a	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-07 to 2026-08-08	Block
7bcede88b2917a631bc7995fae8a6765ee8071f387c2dc48e3b0469cf5a9fbf9	SHA-256	Loader of an x64 build of the 2026-09-03 compile, the operation	2026-09-04	Block
8bd0b996bc98df0cf3e9fffb12e6b131e219dfcc1a16f26be53b72615f16aef3	SHA-256	Loader of an x64 build of the 2026-09-03 compile, the operation	2026-09-04	Block
5b4acaf5006310cadac78c9de2feb7083fb7422b59101c1843038862f714d357	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
8d26fb812e3f80d44c3c10a7eb67fa9543d4f1f6d0975f898e085623f9565856	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-08	Block
92a70bc78c69b729fb3e4fb08e2f125a81d0606bba560cb173053e5c5553ee80	SHA-256	Loader of an x64 build of the 2026-09-01 compile, the operation	2026-09-02	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
9f6daad5d0d0330a69bd5022f570096990bc924a15d918681ddba380cc10e444	SHA-256	Loader of an x64 build of the 2026-09-03 compile, the operation	2026-09-04	Block
a594eb76744c835b7e1efa6c0993b8c38254127b413cc2afbfc2f6aa150638be	SHA-256	Loader of an x64 build of the 2026-09-03 compile, the operation	2026-09-04	Block
40dfb3e645b4b97de269d83463f23d2eeecdac4e5ef3a8fd3f7c65a29e651faa	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
a5ae301ad6b736229f485d140c80cddd83af13ed7aa0e4e35f943dff7e2990bd	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-07	Block
b1159a9db84d8aa7c73e47da28fa880d4214956213ead4f93e00ae938958640c	SHA-256	Loader of an x64 build of the 2026-09-01 compile, the operation	2026-09-02	Block
49e756b83cc0daf9834b7be170353634861034ccd4892497e99330ba91b03a41	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
b14ab00411c35ae382a426a2fe80197c56e48e44b8c6d95da1e38b5ebde460f9	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-07	Block
b8f5ae180e8d6702c28de167a52a7f4f657afa4eec361577ddbf4ae30d35017b	SHA-256	Loader of an x64 build of the 2026-09-01 compile, the operation	2026-09-03	Block
62b4dab833c0ea54fe9d4a65ecb1e705791bfe47b61398c0ea155d2445fffce5	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
ba2a39fdfb2c77a831f34664350f2e018b01e42c48f9518f050a1671c1f81064	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-04 to 2026-08-05	Block
c1aff663839e5d36b8e43a2886d1d97b1583f8a0fc325dd64af8144b77eeaee5	SHA-256	Loader of an early build with the DHS seal, the operation	2026-08-17	Block
3807ef43f7cbed1b210b64ddf532f9646482d4f4366b060a692c8598ab01e3aa	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
e8409b4f985f9a499e478fe6e7d2cdd2d41346ce34aaf2c79fe8c8181d69de8d	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-04	Block
bbc90b449d5248619ef8bf6d55436cd382b3bd7dea4c18c9666da84e41c199c1	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
ef3a41cab8b104230f2fe5348108ed68428225a41dab3b5a82892574da58eb96	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-11	Block
8d21224a16afafd6f04bacf2e733acaf798c5354cda049f4cabf2e938cb814ee	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
f2e5148c34c57ffabc944680f6c4492c65f8510426fcebb475c20e7c4b40fdd7	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-03	Block
d76448edc2cebaada0e477832e0932dff2a37b4dd4713e6f3f6cfda9d225268d	SHA-256	Loader of the auk218[.]club loaders (HDP kit, outside the operation)		Block
f6a97ffa1d4b739b8c7973c46713c3a08701438d3cff7ce9a581658374a1f6bd	SHA-256	Delivery package of the auk218[.]club loaders (HDP kit, outside the operation)	2026-08-05	Block
3e4204dfc05f7d98d882477e759a27a5f21abbf26bc3e33e90c7279a242bf0d6	SHA-256	Loader of an early build with the DHS seal, the operation	2026-08-15	Block
754c52330d3a560cad89314d7ec652dfb239f2ba1610734261195f3cd64c298b	SHA-256	Loader of an early build with the DHS seal, the operation	2026-08-13	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
0187eeeb04329241871412d76d9480f1194499f5100ebe6754644904388329 62	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-23	Block
04e74b215c2420a012b91fe16efdda25845633e36c1ad3095ca850738597b647	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-24	Block
06604538283f2ab4de8515a97918c20ba0062e8e7bf6b6594a06c02553c49bb0	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-22 to 2026-08-31	Block
07ee7405d967ed2967b840998f0b6b0d94325828515bd07d1bbe7f7771feddbf	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-17	Block
0dda73e626903fc2da21902d4638f9e30598425dc3a4230f7fec953a15236414	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-27 to 2026-09-11	Block
0f4346c4c1cac1adda16105f080596e19f2b5c9e5eda62de2ada2d339b8ad938	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-31 to 2026-09-12	Block
16b52440af15755eb40e8e873ee5396da98df11645f65d36870360cc77624f3d	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-19 to 2026-08-20	Block
1c1d4382c12d7605e211610b815e16a0dfa21ac2e7ee466b4d6dfc8835833ec1	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-30 to 2026-10-01	Block
1cd7d58df3390b3262c08f27ef90161d3bd217fa13d3e83890d563d4a6eb5819	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-22 to 2026-09-23	Block
1f91efc2da6cdded49e318a6c3f97b0b74190f6776fdaba4faf93be550067475	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-14 to 2026-09-30	Block
225b6e184c432cbb26b287747e56c7a78d83e52dd164002df5ca2730f989ce54	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-19 to 2026-08-21	Block
24e9574173aa0451026921df69f5327e07742897df7e6afe935fa6d2332b4de2	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-22 to 2026-08-26	Block
2518264301be19b814d43a19092107526db7f32709b97dc2865cdcf00cf0e6d4	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-10 to 2026-10-02	Block
3cf97f3e4709086ddaea10ba0d8744d0229f6c13ca831e1c8fd10079f7cbc136	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-04 to 2026-09-05	Block
48ab0a4bf8e295df7a8057a9a27b15b60db7874ded2ab0d99f6dc02aa6766930	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-11 to 2026-10-02	Block
536e05cbcc288f6d5044d3bc3a995e8062be872173377 85127c5bf81013cd75d	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-25 to 2026-08-28	Block
64806a19416d12e4d62d425ad163b5c3f767b157920f3a3918918bcff8fa28ea	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-24	Block
66a46bb960b757df1f1a2b33fbf03620b9cb7eabcbdd379f179ad39e7b573247	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-18 to 2026-10-10	Block
6bab63f86925a5ab2343a9f65420907b0905e7c35fa2422973887befc78aae61	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-25 to 2026-09-09	Block
72539b454897ea9f1f7e487e69edef2f879312d30ed0a0fc7cada1f47eb87f15	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-17 to 2026-10-10	Block
740fe5264efe8ad2fab97905c62e5ee6b712fc05a3089183085230ceab3c698b	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-01 to 2026-09-12	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
763bc04263e049420e318ebf1fc64bf649bc89cbac4051bd8a0347a6cf452de1	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-28 to 2026-09-07	Block
792ef0e7518ac51196ce515ea948d2c921bbe7bb17286a62020874230c0ba71f	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-20	Block
7dece88eefef854c961d8d49cb836d63e0a1224aedf953691b756fc16b1f93fa	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-19 to 2026-08-21	Block
7e035e7e5af2dfb696aa189a0389af833f60ba5611a5fd07c23959c132537948	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-21 to 2026-09-22	Block
863e22cb4c7aedd5fd6be69ca584a1867320cbd2ff7c9aa335ff991aab8116be	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-19 to 2026-09-29	Block
87fbbb20904003630db2f82a7053ca4bdc77a7bcd68dbd3def0677cbc4d15f1c	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-27 to 2026-09-01	Block
8ad984f47871496bfae879f9b6616f8cea7d5cf4f6a0f7e79a8a0f615a732dba	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-27 to 2026-09-02	Block
8d68655d14fd21e6cf221a7a10ccd6bf7b36f8e53dd83235fe02f80f8f77457d	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-24 to 2026-09-10	Block
96acfb741a79711e4856da4942740e4b773d2dbc7e14d060211c0f3179fd4a49	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-02 to 2026-09-12	Block
99015ded3f34be63dd409057646b8df312a422d050083b02defafad8e41985bc	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-27 to 2026-09-04	Block
a55764b3eca51d90c8f0f5ba4ce9f717a26febccd91ffe55a550b131db0166ac	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-04 to 2026-09-05	Block
b1840e2f639f80ed869e38b1f52a659a38ce5f967c350a16bbbdbd69a936c81f	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-19 to 2026-08-26	Block
b7a023ad2f0917d9c11af78bb8d84407927ce95ad3d8a0f303c253ee6e5da9a8	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-24 to 2026-09-26	Block
b89d05e014cc1e17e16d843f2b0741887a9752aa831645fbdb2ab5cee5156db7	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-21 to 2026-10-10	Block
bba34e8c07d753b7b8083a108f86cb0c3bd7eacf97ca83fd50bfe981b268252c	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-13	Block
c29e5943a76ec47c3f818e9544013568f7a99a23002ea6e89a756e14f5c203ba	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-21 to 2026-08-26	Block
c44a102ce226dd02cf26eb496f302a2e661ce9e59b86dc3d222f1d4c389aa70b	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-28 to 2026-08-30	Block
c65b23d90ff8c0a8042b6a1de200b207004741fc8f5d807b7a995c601f2afc61	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-18 to 2026-09-26	Block
c6f219b90f5fe01a63967815e9ef242e61bccf8fd713ffcd0331ca394cb87373	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-14 to 2026-10-12	Block
c9f3b8739ee4f7cb6b90b5248cd581c4e3470290df4f37778f90b6ab159e5626	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-27 to 2026-09-11	Block
c9fdb65ae80899bb24b7620be7bd5c69de32c850e382053d9c1fe0c8dec5a697	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-04 to 2026-09-29	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
ced28128f5f79c16577f0d46b7faf8abe2175db3cc03558c2d039a1cf3bfa763	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-19 to 2026-08-31	Block
d129dcf3278fb614ca2f760d06efa91e3e7c378969c1b6f604d82d24c4c7839b	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-15 to 2026-09-25	Block
defeb0740dbd9e084d862a425c8ec0c7f198dcd65687d73683098152160a7e86	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-20 to 2026-10-10	Block
ec0a5d5fe2ddc9acfbd6fa4ca066021e1343b300110da28abfb6b58aab193919	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-27 to 2026-09-02	Block
f5b713c3d247d3ad387dba54f5eeaec7aabe644482075066b55a880ef7e196f5	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-08-13 to 2026-08-28	Block
f8df5f53e76c79b0ae4c74229ae414107b3f0ba00363929fc6b53c278b212a92	SHA-256	File that contacts a C2 server of the operation (fuoe333[.]club)	2026-09-15 to 2026-09-30	Block
0084eb27db41425f2c24118cad51520f0740710a078938799e99edbcbc65a7de	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-24 to 2026-08-26	Block
04baed3dadd15e82d9b0e32f92fbd5c2ba32f8f5e25414889d86b504cc1c278b	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-15 to 2026-09-25	Block
053deca10c9f685d60affa84e16e38506727a592610b37ce99ac5606fb82988a	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-10 to 2026-09-25	Block
14d2dcbed2bba2414e7da2ebbf151a2676b43ee12153374a458df05aee2a9bb0	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-15 to 2026-09-25	Block
14d9c3854c08f0bc09b1109e8203732d7ed0c2088f54e58542aec0771ac82c34	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-20 to 2026-10-10	Block
1c427bb0e21993ea242ad69e04979dbf51020e4fa963efbc5a285f5c7c7fae87	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-19 to 2026-08-31	Block
1fda6926c3bf7ba9163bb1434bb3f2ef66de2bb3f9558374a1a4b4c79cb14c3e	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-21 to 2026-09-27	Block
23086607cc8ec2c2d41ee01c064951e2bc20e9617b6efaacf2809b6da8ab6f80	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-24	Block
2cca35238fe3a3136634d488df4ee07f115ab8e43bc9e36e3334254ebdd315cd	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-20 to 2026-08-29	Block
2f69d8816359b2edff0f9276a344c055a3ead4bad8130ffd6181ed7a2fd76752	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-24 to 2026-08-31	Block
2f7a3301b4969aa0f55cf05c862d120723c7787694198496e3915d036191a26d	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-24 to 2026-09-01	Block
394c4a9a0ad0dca5d5cbc4f2ce52dc8edcff67288344c76a81b7c79f5cfd1d2d	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-24	Block
3e05968378085975f2961112a2ac6949f68f02024dc9cc17de09cce3aa6c2237	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-20 to 2026-08-25	Block
3f5e2fec30cd06463d2dd38689b534afdec521f6e043910ecb69309fa9437ac5	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-17 to 2026-10-10	Block
92967060aabe7b493ba04aec84849e5f619b5147b8b1254c8069f6d71b66db12	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-24	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
92dced9c7094caf199b23deb6dcf4345f7db02bcfb68e3addecf108a1ce31466	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-15 to 2026-09-25	Block
b0823b51994d814844cd00813700500fe008b59cbf4de47501a093c33391f472	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-24 to 2026-09-08	Block
b94f3dddf9d35bfb98f23994131c638041f783be9402426ea141c3d09f6d8d55	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-25 to 2026-09-02	Block
c3ea27ba1820bcf9ca0059fbb636ed9565ffe42423173738ad701a808b261ec0	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-20 to 2026-08-26	Block
cc816e454906758bfcae14ef41ede98cfdf09b26d6e32d65422fe0c67da125e9	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-25 to 2026-08-29	Block
d1e7ce49e70342b622249cfd1572f76d284d2b01cf124d4a36792441b374f69c	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-20 to 2026-08-24	Block
d4129273997be14d4c8e9322d95302d264852e871d274e2519502767d389fd19	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-10 to 2026-10-01	Block
d6ce323510b37dfb54480b446975d6089c748a5aa19529cc73d275debbbabba7	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-10 to 2026-10-12	Block
dbe3a51a49d48c5d8efa6f5f3fd5524e48da1cfea59da72207ebbec3d3918837	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-16 to 2026-09-25	Block
e192514ae23601ea993ebd0b2f8b7a6f129b1198e67c3d1386c28aaa7c632f3a	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-09-04 to 2026-09-12	Block
f68f891d38b2fcf5e55841bb985e2b143c717207ac0db644c12d432af7eced24	SHA-256	File that contacts a C2 server of the operation (moik77a[.]club)	2026-08-25 to 2026-09-14	Block
00bc3e3faf923b6b694bed11f0dab8431303fce85c27bce65df0a07a620c5ef6	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-05	Block
0a509d784b7c20226e5d27d6a7039b3fcf8d6c0db96c96b552c8fb97338df874	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-03	Block
0a85faeb2057b0a43d9d503af90957e5ac65c3e02fdedbd101166c3472ad4166	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-05	Block
1bb87e5c60f4a2cf0d9cef8761ad1ab56dc0b81ed310cc738b36d3836ce4f950	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-03 to 2026-09-05	Block
21e19b834f6ff5577c27ffd55f3ee61ca6a21cca6bc9d9193798eacae33c212b	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-12 to 2026-09-28	Block
27beac85107f685ed0002d0778ef8a93824a2da1c0afd871b4d534d6e10c3479	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-29 to 2026-09-06	Block
28c3beecdc54c75f29365f11cf1f187bf8ca776bd98e8818a9f37798e533bb86	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-17 to 2026-10-10	Block
2faf35c81460f594d5471186c8a9be65c004c92c5f3968a67e8e88c11a35d347	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-31 to 2026-09-16	Block
3a02874ada8b9a734923d6d6ffce27edbc3a54cbb346a2ac2fafa09076beeba6	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-13 to 2026-09-25	Block
3bde2f5408524eca397d51626cf38a9e0d41d1bf17b090cbb6ebf539ab673a76	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-19 to 2026-10-13	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
3c253d2d70c27823e34b457f786443e40053bed57873f6cacca10ca331462acf	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-02 to 2026-09-09	Block
3f780c9fc89a45576e2ff1b27175d0e9f530653adcb2a7932341629a527088fe	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-02 to 2026-09-04	Block
4b17f808fc2106166e911e0db6bc2941095c9c9b231aa6a79004f756640741d2	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-03 to 2026-09-12	Block
4cb79cee3ff868c4217839befd927060b8cece22b11045425e3cfe83e447977e	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-12	Block
4e6a4fee8ae9162d193b0c8314c437c27aff13578922c698647d2038c7af784d	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-10 to 2026-10-12	Block
56684f6ee5490d628bf3c9ea94be47a6ea471a63a6514500ee73f220f4698141	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-18 to 2026-08-22	Block
68349c42d5f7ad25c7bc0186053942ebd2cade6c5af71d28d42049243a927aac	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-06	Block
6e94f503d02d7eb6fd7f768164526c2dcab0407e8b085999b59796400ccaf349	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-15 to 2026-09-25	Block
6eea260ad32653938205496fdb8fc4e50a0fd05bf70d9aed44b6492987640c1e	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-03 to 2026-09-12	Block
772e1cc4429df970ac49ae00ad679c61d30766a3dd9d5f74e7e57c605f622bbd	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-03	Block
77aad50c70e4505f4a8ce695450a2015253f9271387cfcfddec3f54be6aea010	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-12	Block
78d9d70921c1b880164d9d125d285358a7a57a1fa99a73c99e2d559b04202059	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-17 to 2026-10-13	Block
798f1ff9a0aef2039663e331783075dfa4bc87b2764aa4f8f6c5c5f5dc86596f	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-29 to 2026-09-06	Block
7b18defe0585870394f5d3bdc09f664cbaec2771e41ee9dc11becb1b1c39f62f	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-02 to 2026-09-04	Block
7bd4043fbcc91e4c9aec01982207e2518fdcd4ed1b5dec58bcf834f879ae8db2	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-15 to 2026-09-25	Block
7d660650ba143558d21b4f05f31412e0ab735b855677a94a9efcd3ce2f6b967e	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-24	Block
8cb5bd08804eabc315b224c6deb21e2fcf24547237aba6da32199cc8ea6f1e34	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-20	Block
a2fadfbed949d378ef7ce1316e92152f869477f6e09a961726b9afae4ec5f878	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-11 to 2026-10-13	Block
a4899c2169be9ad8285173d1e6d12e8471e26e583b79cac54749e81308006598	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-21	Block
ab38d2a19e63759e3102dfcb4c1b04af08f7307c4f6022daa650144733fdc5cb	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-06	Block
b461ee54cecbee799a8e6d20a0d30234aafe25ee44e4293c2ab3e506787f99bd	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-24 to 2026-08-26	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
b4790764968dce129c5eb48710e039d65bd5c72c77e2160b2f3f50b1f8ba560a	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-25 to 2026-09-01	Block
c01759d70ea22c4be6e4bfdfa02feb948b1b5fdeb0de7cc30b4673d38d3b160e	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-31 to 2026-09-13	Block
c8213b675f90128b73ad394e7028ed622e63e8baf3d78758994888ee137ec325	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-24	Block
d0537219f73e304a800ade313313bc82d0130a559aad20f1f0e187f38eec0c19	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-21 to 2026-08-29	Block
d793f5b98883fc61a3643cbe0414e1dda28ffc666bd5451ad887757ac6314174	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-18 to 2026-08-20	Block
dc2649a3a477bd342b8cfc331a5151077ff2c6554f7066f92d8a977fce39a512	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-05	Block
dd5ef802f176a35702b0fa4daa36fe1481aef21ab756ce82a2f8d01c83d25585	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-11 to 2026-09-27	Block
ef25b25888922a7bb98f44bf94cb10a2307d7cf03570ad52ef6297ea95a36c5e	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-10 to 2026-09-29	Block
f0d2b08b22f0c6177cc5dcded89d64f233e59d8f2246703aacdd6d4317442d47	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-21	Block
f17bf9d326446b0e72bf00408883f3683515a98d1e89387ce5fff11fc180bcf4	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-21 to 2026-08-29	Block
f5694bfc987066e0c6607f1f433c18a7ef15eafa44846269660ff53b5f961fef	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-25 to 2026-08-28	Block
f715b63636e4dfe34ef86aeb1378b153564da0bb7dbe5022019d51ea246c0b5e	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-10 to 2026-09-29	Block
f7e44ff3d9bc2534a62f7644758e5368d6b0bcda0f368afa151027762609f09e	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-16	Block
fa11fe5b59145b69d29ce92a86ed7f3267c9c7407da21341d0b110ee9e5a58fd	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-08-25 to 2026-09-01	Block
fbb65f96bfc29eaa706a7fc25cbfaeb9b19a367fc80ef46689f45b2b3f0a592a	SHA-256	File that contacts a C2 server of the operation (taku788[.]club)	2026-09-04 to 2026-09-05	Block
042030db768e7af317a15fe0b2ccf630663a139d7f1a646693f886e62a2176c4	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-08 to 2026-10-09	Block
0f78a68d6c371e7e1d12768bc3fe56ca1007086ec258cfc7c8a2c1ae56e93819	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-11 to 2026-10-12	Block
18f4cf31f79eb5186f25232b84503263d6ed0e30d780b620a217d29bdba275f2	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-08 to 2026-10-12	Block
1a23f4f94aed79dbf7b64afc82ce73dec69d9ffe2e8a8b061ada42f14ef78254	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-08 to 2026-10-11	Block
21880ecd057deb58813dcd973c459c950f4d434764b25ff3a1bba3df31965faa	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12 to 2026-10-13	Block
2302971761d996b310dd30a42b3883407f693c9f84d73831e22afbbc8f939aec	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-19 to 2026-08-21	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
2e765a14b583740eedeb7cb37066b596d39a902a53e46ba9d24f2fe7c02498cd	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-10	Hunt
31ce7dafca1d024fc9b96a84fe5cbe4d746059d273312eb87065e6716aa8673e	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12 to 2026-10-13	Block
34bed9911940ab04419e526db4c36f9206130c4f72f98a379c873fbb8e612bf4	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-11	Block
34ed04fe3d98779b985d2733dbc7de63087d184f6b9be6c9eaa1893829810d4e	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-05 to 2026-10-08	Block
3a089af390ad39c4dd0c1bdfe45fff8b14e8c6b544a311a988b231fd3f38eb84	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12 to 2026-10-13	Block
3ef77fdd2f9abb7e51a8fd8e2e942ce48e66058815ea9b81d6bdc133da7d2f6d	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-29 to 2026-09-09	Block
50a16a136a0a504d36cc105f5115babe436667c9965cd15f816251cad81f50b1	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-08 to 2026-10-09	Block
54abeb1cc8d3f834e973d5c3bd71782e28f0bec49a7e824fee17a7694a65c0ea	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-05 to 2026-10-10	Block
5748e3e60ba2f8da9cd598387953db279009026071e2d0feeb7846c534f0572c	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-24 to 2026-09-08	Block
5efa15938fb8b71fd1d13ec89fce498c39713dcaf0005a79e4f4408371065748	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12	Block
61cac6ba26a633f5347d4408b4bb8b1d72f565334a751ae652baae7c54d050ba	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-13	Block
6bd6fb90cbd657d5f056da40d12e1bf1426215675a7b4eddb2c1fa709ac6e61f	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-08 to 2026-10-13	Block
6cf0be9b52191f7f1a640919c22d712da7f36b9c889b24c674437b140dc0c4ae	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-10	Block
6e29c9f5f042a5b9c2a9bba12442795344b41ffcd990ee12e5597b2d8bb466d9	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-18 to 2026-08-24	Block
70b65d3f347d7e965bc67f3f7d7d8e4f1696bfaa79f3673255a5946e5a8cb47a	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-10	Block
786b54c96639d44d5f06cd2c7af57498d32a27b3d918d69f41f80f8129b42b19	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-05 to 2026-10-12	Block
7d6d8dfe748cd1e59308ee4bc591c438eaee40e955fcffbc838fda5d10d7af5b	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-05	Hunt
878d0b3df7f28d198776b22df1e7563d481e50cdffbb7d2c562af402d170e6fb	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12 to 2026-10-14	Block
8a0d92c1ca60ca27d01aabf14b878458d223c80a3100d28518a380a7cbc5bd3c	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12 to 2026-10-13	Block
8a5f0b02aff219b92257283f3d4f841347857c1354ce9abfa52be5e283476599	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-13	Block
8de938d7e7412d445e7c243f53b81ee0866d059188255b4d7936cd73f86fa5a8	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-11	Block

Value (defanged)	Type	Role	Observed (UTC)	Use
954462f2b44d7c18fa0ababa90f7e705422cbf75b5f49456b1d6e2b31c8b5efa	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-18 to 2026-08-21	Block
95f830eff058463a6ba343e828f8697532d9ec88b4c81f234a2d13e4f89d4f3a	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-11	Block
96c77b9265c7bd73cf0efab694734d8ec5b9e2bfad3bc6b18a86f2fc0a35f4e8	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12 to 2026-10-13	Block
9bd3aa52a05b76ca773c6ea0e766fb916cf63171d3dcd7c9b77c1db605706be1	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-13	Block
9cda6ae687c538780e7ceda2b5d18554187463b7fdd0f95c17d7ead85c758c79	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-24 to 2026-08-29	Block
9daecd525772866982b16d7bbde6d3f23822766ad0ce9a3c20b68615dae5ed22	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-10	Block
9ef75888f590cd3b7a53caa682be8311cb8704a46aba31e71a03a4b4b8120056	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-08 to 2026-10-10	Block
a4873208b6719323cdc0417436531c184d3cbd234847c9beff7f02e95a833d1d	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-19 to 2026-09-05	Block
b971cccbcd0d6485a12b826359dd8d9c121110e103ad267144eabf2312dbe9b7	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-24 to 2026-08-28	Block
c275ee3b3dffff189fc1333dc2aa4718cff12a68d255f4c6a67fea7b34325931	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12	Block
d9972d4b8190fe46265db0c4c9bd3f3a1a132e0b591cbd2b0a48f86d7ec1d875	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-12 to 2026-10-13	Block
d9a76cc9a69d98fa3f8b06fa6cf6bc0e7b4324c9848cac00b7cae1414c3eec36	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-13	Block
e0010ecfc238f0d52030115f1b084bd2e96513600b5e4ad6d31756c5a9372582	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-11	Block
e4b5cc63850cfe7d4e4518497c5aa74f3abc954ce64f0a4ce5a675f0b66130ba	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-19 to 2026-09-23	Block
ed7ddd1c0ea46783133b1b482b8016fffd8f7aceacd332a7131fda4c14d7f953	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09	Block
f2f9f7d96753cab149bdd40022113ac2b0a186eef58021667b35e5055192af52	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-10	Block
f70856545c15e9e4a38244d99f9c0fd40acb0e54d93d83be08f6fe1beec601e4	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-10	Block
f85e47a13b5c87ef975d6722f41a49b11c0e8b3e8c856dc2888999b225c83d16	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-10-09 to 2026-10-11	Block
f93eda939749ae2d52efddcd676891a97ac3fb842efa6659d09303bc1e51b95f	SHA-256	File that contacts a C2 server of the operation (usdt888[.]club)	2026-08-19 to 2026-08-30	Block
091de5894a170b40f92269f20585b38a61662da16e638146378557f04fcc8923	SHA-256	Archive served by batch eu.cc name ksidxhcte[.]eu[.]cc (link b16074ea4502); 1,944,809 B; detected as Win64.Malware.Yogi	2026-08-12	Hunt
096de423fcc4a3ca73c31ab96d47ca91a9b1ea2b506b74de68ee917be8364769	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 193338c39726); period of the auk218[.]club loader packages; 4,984,880 B; detected as Win32.Trojan.DllHijack	2026-08-06	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
0b09b1171c20f78d038451f128a8964724a2cbfa0972a286cd25baafdc1c9f48	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link efccb6d9a566); 2,424,268 B; not flagged as malware	2026-07-06	Hunt
0d481d105cfcbf4ad7b99d6af236e27720075125863e1d1b92a95109ae68522a	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link e9f5bab719d8); late July packages of 3.84 to 4.67 MB; 4,176,648 B; detected as Win32.Trojan.DllHijack	2026-07-29	Hunt
11c5ae00f884a099940522c246e51a4175a90a5c8c28681983db2b76cc1395da	SHA-256	Archive served by batch eu.cc name hsaueraw[.]eu[.]cc (link e6af2259d500); 2,449,430 B; not flagged as malware	2026-07-23	Hunt
11c619e868bbaf4991097e29a244cfeb0159a8b218b6d6413cc52cdf4a67e6b7	SHA-256	Archive served by maoasiye[.]live, a 574849-1923 domain on 103.23.172[.]118; 10,164,365 B; not flagged as malware	2026-05-27	Hunt
1290f83ecc6e7277641400c265ba03d850e7007c68437e5799f6f483af567f2e	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link db8bf07b3cf3); July files before the kit packages; 269,194 B; detected as Win64.Backdoor.ValleyRAT	2026-07-15	Hunt
14b0b41d11793273c6358d34391eaa52e54bb2fbc563d8055722c0a0a551f892	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 2806bf9f5858); period of the auk218[.]club loader packages; 5,000,562 B; detected as Win32.Trojan.DllHijack	2026-08-07	Hunt
156bbc560dc0cefe309444f05850e38363bd699c28bbcb10b3238ad588b14246	SHA-256	Archive served by batch eu.cc name pzidiauwytsd[.]eu[.]cc (link bbcbbf698cc1); 1,247,538 B; not flagged as malware	2026-06-24	Hunt
15ed0bb5b23dcc9ea42344b7d6bfa991428876975fed99121cab37fa20ebcf2a	SHA-256	Archive served by batch eu.cc name ddisuyer[.]eu[.]cc (link 109430a6d909); 1,261,307 B; not flagged as malware	2026-06-25	Hunt
1a5d19bd62c7650514d86b7bde9a57e3180e77f34649117ec910420f04b21532	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 1dd63a1a7fbc); period of the auk218[.]club loader packages; 3,992,751 B; detected as Win32.Trojan.DllHijack	2026-08-05	Hunt
1ea0d3cfcc5cc27d5218d8aa5e90c0611b8be9ef6dc9c5b9363b0cb738ce5c74	SHA-256	Archive served by batch eu.cc name pzidiauwytsd[.]eu[.]cc (link 76bbdcf4299a); 1,308,983 B; not flagged as malware	2026-07-02	Hunt
24d615e3e3cbbaf218411f00f20ca42879d6a0c5b65e1eab88e4770e5cf9a31d	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link eee736601c59); 1,944,794 B; detected as Win64.Dropper.Yogi	2026-08-13	Hunt
293d87d989c8a11f3a763d6546b811b190dd4ca34c41a31b68d97bc70a46b529	SHA-256	Archive served by batch eu.cc name isudcnzy[.]eu[.]cc (link 33cb9533b11b); 2,342,076 B; detected as Win64.Trojan.Generic	2026-07-08	Hunt
35a2d6c73b7ce7d9fd2b7746071f5e186c12a3947701d3bd118ec110f16899ac	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 60b2d5439aad); July files before the kit packages; 5,470,316 B; not flagged as malware	2026-07-22	Hunt
362f733046c001838e6b5dd28f5702b3fb64fb9eb12acc9ae649f2cd88457530	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link 72cfa0d115e8); 10,633,879 B; detected as Win64.Malware.Generic	2026-08-01	Hunt
3ab04222fac68a1498508bd4d8002b63a2074048e62b448e214bec3ba5b577a3	SHA-256	Archive served by batch eu.cc name isudcnzy[.]eu[.]cc (link c541853be790); 6,414,081 B; detected as Win32.Backdoor.Myncsom	2026-07-08	Hunt
3d53bd1007b12be7fd95081037d1a63b0091cc05da819ecb3a1cf352089dd4f4	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link ed86198ed307); period of the auk218[.]club loader packages; 4,150,473 B; detected as Win32.Trojan.DllHijack	2026-08-04	Hunt
432e225cc7607eb7e49826c6e0e9557b8192e05247e222ef6ea5054f2c91360e	SHA-256	Archive served by batch eu.cc name ddisuyer[.]eu[.]cc (link 5030962e6cf3); 1,230,133 B; not flagged as malware	2026-06-23	Hunt
4624a18e994fee1f2363c7df48b7ea62a7f443f762c9e4aa289a0444a60d5984	SHA-256	Object of the file sharing application (3,036 B) on 103.23.172[.]230	2026-09-03	Hunt
4a4d17d3dd05ed103e76b0906a5dfefd8d3e9e496b04418f02f1db7ecbba0cb3	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 60b2d5439aad); July files before the kit packages; 1,769,848 B; detected as Win64.Trojan.ValleyRAT	2026-07-20	Hunt
4fe38dc20cb2ab147dfe932249ce1626740eca83152902dafbfa7308664a32c6	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link 534de9718ba0); 3,335,548 B; not flagged as malware	2026-07-02	Hunt
542acfb55e54ab8c4190fe19359efa4db21f63968ec694bca4f4dbaeb76c921d	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link f65c0a1e3963); period of the auk218[.]club loader packages; 4,920,322 B; detected as Win32.Trojan.ValleyRat	2026-08-12	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
59ad96dd3b4d5f10a5c53bbd465446e52dc7701a4ac633632f762bf1336d3347	SHA-256	Archive served by batch eu.cc name lzsifuiseurtt[.]eu[.]cc (link 9d57022862c6); 10,552,908 B; detected as Win64.Trojan.DllHijack	2026-05-29	Hunt
5fada6799140d07851d834506f6cce88304f312582eccc7c9cc3150e253c0b42	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 6f025f85e3c0); late July packages of 3.84 to 4.67 MB; 4,176,658 B; detected as Win32.Trojan.DllHijack	2026-07-29	Hunt
6042e01e3670bad16131f4f2d932cfdb9c9d01a9838447ff2a006a09d409adfa	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link b9059861159e); late July packages of 3.84 to 4.67 MB; 4,176,665 B; detected as Win32.Trojan.DllHijack	2026-07-29	Hunt
63d39bb548946f3aeec76ffba574e7963f65e219042d35cb9d05df97203efdc1	SHA-256	Archive served by batch eu.cc name lzsifuiseurtt[.]eu[.]cc (link 07b3b6c32b8b); 8,696,924 B; not flagged as malware	2026-05-28	Hunt
69de31986a0d8206a1788f8097f9176569ca04836efafb129467e4b6fd6d22e2	SHA-256	Archive served by batch eu.cc name ddisuyer[.]eu[.]cc (link 675d35b0cefd); 1,271,928 B; not flagged as malware	2026-06-23	Hunt
6d2313dc89baa6e441ce951f20201ed91355d22865fe7d85bfa5ffdcd059095c	SHA-256	Archive served by batch eu.cc name pzidiauwytsd[.]eu[.]cc (link df705f68f4e2); 2,721,788 B; not flagged as malware	2026-06-25	Hunt
74c46708b0d9338bd7a895f2ef2be18f5190cb52f63cc78876dc6ff05c5a7255	SHA-256	Archive served by batch eu.cc name hsaueraw[.]eu[.]cc (link 074457b9510d); 229,153 B; detected as Win64.Trojan.Generic	2026-07-29	Hunt
779314ede676f82cf91b4b903cfd479ec7331f98b5debd67a0df3e53afb79cce	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link 21fa5dd9c596); 111,973 B; detected as Win64.Dropper.Yogi	2026-08-06	Hunt
7dc5a105620a8d441d5e55c0a099577a3b19f60c74bd6deffe9732147a6e7e14	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link 55fbb2550be9); 2,409,435 B; not flagged as malware	2026-07-03	Hunt
7e01626c9407e835342589cb7207dd1a9eafe3ac66f7dfc93184404d52dc3214	SHA-256	Archive served by batch eu.cc name ddisuyer[.]eu[.]cc (link 56173a63cdd6); 1,201,977 B; not flagged as malware	2026-06-24	Hunt
82c0617cd6d88d1d2a56051aff61614dc1679dae6026b1f26924aff1c973b168	SHA-256	Archive served by batch eu.cc name ddisuyer[.]eu[.]cc (link cf6615384394); 286,910 B; not flagged as malware	2026-06-24	Hunt
8375a630067fefa98230d061e676eed21b1d3f9e3af3dfeef6603f1cb71db5f6	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link f65c0a1e3963); period of the auk218[.]club loader packages; 4,786,733 B; detected as Win32.Trojan.Yogi	2026-08-13	Hunt
84061a9402d2a65454618ddd238df18ecb220c21cac68e357bcc371dfb1d84a4	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 5e54862579f0, 898baacd110b); July files before the kit packages; 2,267,632 B; not flagged as malware; also served by isudcnzy[.]eu[.]cc	2026-07-04	Hunt
8805c7f4ae9e7dc8ba3cfd41cf9cd796ed0efc798b7cea87d503971bcf93908e	SHA-256	Archive served by batch eu.cc name hsaueraw[.]eu[.]cc (link 3368b283d97a); 4,182,519 B; not flagged as malware	2026-07-28	Hunt
8ab8f771858839786871e679b6fda2642e2492e8433d01720204b0b2a4ae4edc	SHA-256	Archive served by batch eu.cc name pzidiauwytsd[.]eu[.]cc (link c200ea02fd60); 1,480,236 B; not flagged as malware	2026-06-23	Hunt
8b6f5ad868c3256c246ef532e807b0a21893de072d66705f23a64c4689f330f1	SHA-256	Archive served by batch eu.cc name hsaueraw[.]eu[.]cc (link 2f9332b9f22f); 2,829,832 B; not flagged as malware	2026-08-01	Hunt
8becdd83d85912cf14cc5bf3f324ddc0cfe5b7d51fe7b70364398f90b5623726	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link bd199d1aa929); 294,305 B; not flagged as malware	2026-08-04	Hunt
8dfe45965bd25d8d2b01601b0902d9601952f604aff42ecdfe07cae06b70b45b	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link e2691cff481e); late July packages of 3.84 to 4.67 MB; 4,176,662 B; detected as Win32.Trojan.DllHijack	2026-07-30	Hunt
92d34a1517e7272d7cf377a8f9b74fd6a14ddca28cdff8c732a60d13cc5818c6	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link e6600cac8ae3); 3,409,833 B; not flagged as malware	2026-07-02	Hunt
a2cef022d58ff7ceb26b80fc193361ece968dd76c8bce7c523067121fcd3df13	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link f65c0a1e3963); period of the auk218[.]club loader packages; 4,962,672 B; detected as Win32.Trojan.DllHijack	2026-08-10	Hunt
a47ec01e94f36e42e594aeaef52fc20089f8939a34a1f4b69eafbe22bf7b0a01	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link cec66f8cb9ae); 64,293 B; not flagged as malware	2026-08-08	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
a6fb779be35592fb0ff624a8f8e12ab3cafe7bcfc312cd98263814db7fb01e02	SHA-256	Archive served by batch eu.cc name lzsifuiseurtt[.]eu[.]cc (link 761fc975ba4d); 10,267,404 B; not flagged as malware	2026-05-28	Hunt
b3e63353a857dffc2d4975d675c133c136c3a1080ca6df76975eb6e599a412e1	SHA-256	Package served by wordtax[.]ink (RMM deployment); 53,261,960 B; not flagged as malware	2026-08-17	Hunt
bd495b4c2851819a15b9dcdbdf92d9fb443cf3fbe76c1abcb7f955240440f5d8	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link c8bc03a88702); 3,203,183 B; not flagged as malware	2026-07-02	Hunt
c694a8541c7d653eff4c0ac5d771f49a487836e4fe62fd85cfce15ec0572056e	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link 7ad8be732033); 1,944,309 B; detected as Win64.Dropper.Generic	2026-08-11	Hunt
c839ae158e98777d61689c14c017186e842deb34b49399933d821fcb5d9d7292	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link c02aa2c1675e); July files before the kit packages; 2,254,911 B; detected as Win64.Trojan.Generic	2026-07-03	Hunt
c8d0239521c4d27b45245fc5cbacf52ecf7de96ff6f74fb165bc928a5c87f9de	SHA-256	Archive served by batch eu.cc name ddisuyer[.]eu[.]cc (link ca9a0c4054f2); 2,577,257 B; not flagged as malware	2026-06-25	Hunt
cb55a8b5564d28e4ffe001c7696eedc2de1dc37d84380b1dcebd9b5f364694ff	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link cd5817c21ba6); 3,985,337 B; detected as Binary.Trojan.Generic	2026-09-16	Hunt
d309fe28d0ea7d68fbef7eef6ca7205b937d1f2f0d660aaad0a198b5ba35739f	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link ac516096c285); period of the auk218[.]club loader packages; 4,150,475 B; detected as Win32.Trojan.DllHijack	2026-08-03	Hunt
d4252da8242cf44ecfaad45a78a350fe602613a8c38eaa36812a6eaac4bb7e6a	SHA-256	Package served by wordtax[.]ink (RMM deployment); 52,427,669 B; not flagged as malware	2026-07-31	Hunt
d93b3a5431953b2f99ce24bd9b2d81101fec2645ff722ec593fe1f3c039fc5f6	SHA-256	Archive served by batch eu.cc name pzidiauwytsd[.]eu[.]cc (link 72d681bc3690); 2,742,212 B; not flagged as malware	2026-06-26	Hunt
db40ca5c57e2b0d1df2485bb045f438922ee1e38e5e82fd6d0e27a80674c945c	SHA-256	Archive served by batch eu.cc name fuerubuiaie[.]eu[.]cc (link dbcb05dac572); 10,069,056 B; not flagged as malware	2026-06-02	Hunt
df31e4e790060fa059736d523a4c97d02717c7aa45f29f0a614b44f071d2f2ff	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link 63fa02e75abc); 2,377,896 B; not flagged as malware	2026-07-03	Hunt
e2ce9f9bdf463f0346d3d7069b49df05a978a7a6132a7c9016ca0aa35aefebb1	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link 7400f2c1d28e); 3,177,324 B; not flagged as malware	2026-07-15	Hunt
e41d56c64bd181abeaa5951b3be61209c0508bdcdb36000158fe7610dc3dccd9	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link e371fa68af13); period of the auk218[.]club loader packages; 4,150,471 B; detected as Win32.Trojan.Malgent	2026-08-04	Hunt
e79905ac30bbb0831551410f19dfc4b6f89cc706f79eb0aa35f798eaa1934f8f	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link db8bf07b3cf3); July files before the kit packages; 52,479 B; detected as Win32.Trojan.ValleyRat	2026-07-10	Hunt
f14206abae6aefd3b5f01d65a0074f1c1e89827432bcfa6dc1392f5e83b92b30	SHA-256	Archive served by batch eu.cc name zuxyegea[.]eu[.]cc (link 215310b04ae1); 64,332 B; not flagged as malware	2026-08-08	Hunt
f1cf9b973562a4ed33a97d10afb139d1705f20b7c9640dd748d5afb262a903e5	SHA-256	Archive served by batch eu.cc name xzsdiiaeugs[.]eu[.]cc (link aa86573aa764); 1,216,190 B; not flagged as malware	2026-06-18	Hunt
f99a5496f35346d5ff12183d5f3b842313d7f277e75b95d4537b81476be45893	SHA-256	Archive served by batch eu.cc name iysdzxc[.]eu[.]cc (link ee2b12fbd661); 3,036 B; not flagged as malware	2026-08-07	Hunt
fa5df7b02663782c0b32696bc4bebe80f6cb354e55d526bc6b198d91bb234436	SHA-256	Archive served by batch eu.cc name oaosifytaw[.]eu[.]cc (link 78bdaf9424d4); 4,676,169 B; not flagged as malware	2026-07-16	Hunt
45695977abd063060ab8e85abf3c42aeb073377f50325090694e724fa3d3ebc5	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link ac516096c285); late July packages of 3.84 to 4.67 MB; 3,842,666 B; detected as Win32.Trojan.DllHijack	2026-07-31	Hunt
6949888348b68d1dcd1aaf6f26ff3231d8f1435302198111d4051385c46b7ac45	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 4c0956f0a98a); period of the auk218[.]club loader packages; 4,197,636 B; detected as Win32.Trojan.DllHijack	2026-08-03	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
69d3ed3a241b17bb40112b72e4ce9841a6c78f133b7760a97374528ff9560ce5	SHA-256	Package served by wordtax[.]ink (RMM deployment); 52,726,622 B; not flagged as malware	2026-08-24	Hunt
b856a8d469bae6f192b89f05c09a91b89682688a99a6c2bb8381d7d7cd28aab6	SHA-256	Archive served by the delivery host kaiwyrey[.]eu[.]cc (link 29fefdc0cc4e); late July packages of 3.84 to 4.67 MB; 3,842,587 B; detected as Win32.Trojan.DllHijack	2026-07-30	Hunt
c8cb42ad507e0c2135ae3569217ceb6bdfd000aeba9c9073d48827aa88d548c0	SHA-256	ISO9660 image T.No.20260812111446.IMG inside 20260812111459.A86E3055B7FA.zip (D-r27, outer 01ecdfb6); 9,216,000 B		Block
d3b0bd3fc1a41e3d2df9a9da1599859308fb396d466186907ed560e4e0076d54	SHA-256	ISO9660 image Vat_N0.20260805114009.IMG inside 20260805114035.4EAB026E9B55.zip (Dt-r20b, outer 05e27d19); 7,528,448 B		Block
2ffbb43a3cc95b2f03f01a3588392a001aed9b9fbae97e455d258bf54fd56cff	SHA-256	ISO9660 image Vat.N0.20260803122837.IMG inside 20260803122904.0CDDE8D5F31F.zip (D-r18, outer 397b7292); 7,733,248 B		Block
3efd4f8c9dfe95cd33060f312c3a0d7c958c2bd70562802abdff3c77c90c2fac	SHA-256	ISO9660 image VATNo.20260810223945.IMG inside 20260810224021.4628EE8AC9D6.zip (Dt-r25, outer 43c28f6f); 9,996,288 B		Block
f681e386bb77530344ee81e51c36c6a8a55ef4d0234ee4a32ea45b61ac68c128	SHA-256	ISO9660 image VATNo.20260809224851.IMG inside 20260809224916.A22CCFC936E7.zip (D-r24, outer 50f667b1); 9,123,840 B		Block
75942367fdd5365c90e845a2513afb43cdb24b352b1a042df2acd4e5d44c81dd	SHA-256	ISO9660 image No.20260811113519.IMG inside 20260811113526.13D9EF7DBCBC.zip (D-r26, outer 52f3736c); 9,592,832 B		Block
3bf844266f8a3af21b3f2babf438c40e82952711e61931900192e72ca6f02aab	SHA-256	ISO9660 image INV-No.20260817164222.IMG inside Tax-Number852690.zip (outer 6620e9ad); 7,260,160 B		Block
9d83227dbd79f8b1ff499312f437ca523cf88eba131a3409dacffa049d8a27f6	SHA-256	UDF image Tax-Number723863.img of the padded x64 loaders, inside its package; 437,780,480 B		Hunt
725c23f3466bd905259557f5a328bdea9b78b8efee1867127fdf10b7a80dfbb7	SHA-256	UDF image Tax-Number735863.img of the padded x64 loaders, inside Tax-Number735863.zip; 511,311,872 B		Hunt
89b1b83b6a42a100861256ed235786d499374df02d9e7f4cd1d8929cc2b2f294	SHA-256	ISO9660 image VAT-N0.20260807142129.IMG inside 20260807142214.FA7F5B5F6E7C.zip (outer 7582528e); 9,148,416 B		Block
138ec0c1553c077267952cc261de5a99a19cf15b2eb0c4e21fccff630fb2c5f9	SHA-256	UDF image Tax-Number635863.img of the padded x64 loaders, inside Tax-Number635863.zip; 401,342,464 B		Hunt
212873eb2d9e36df29714242b9cf7ca9ccf27dad6197feaa0a286af22a858162	SHA-256	UDF image Tax-Number223863.img of the padded x64 loaders, inside its package; 244,318,208 B		Hunt
f695407e07d77ebd814be59edf069dad14d658b318f101b02047bfcd54998c54	SHA-256	ISO9660 image VAT-N0.20260807142129.IMG inside Tax PenaltyN0.20260807.zip (D-r23, outer 8d26fb81); 9,148,416 B		Block
b28ba5d7aa04a20777a3cb47b7140e6446c9757cbf718634c4e94208cfaf3434	SHA-256	ISO9660 image VAT-N0.20260807142129.IMG inside 20260807142208.24595BD28C81.zip (Dt-r23b, outer a5ae301a); 9,148,416 B		Block
d106499294ed5bad27d4779e37285e0a36e0250614d25dfcc9074d99b58c9107	SHA-256	ISO9660 image VAT-N0.20260807142129.IMG inside 20260807142201.C18AA1EC4135.zip (Dt-r23a, outer b14ab004); 9,148,416 B		Block
bd5ddd01879db700bdbc5fa8f42404e7072c847ebe9efd53d7f8eff78d1c1271	SHA-256	ISO9660 image Vat.N0.20260804142245.IMG inside 20260804142250.A7EABE4E1BAE.zip (D-r19, outer ba2a39fd); 7,624,704 B		Block
9d5ca1924eb50171627ea1e1ae49cbc075f1030147becb9acdde8c587a8ec66b	SHA-256	UDF image Tax-Number119863.img of the padded x64 loaders, inside its package; 144,375,808 B		Hunt
03a0ca970508e5ee765d3c7d465d6ec922abde4e95e18248b1192df0646c2b89	SHA-256	UDF image Tax-Number919863.img of the padded x64 loaders, inside its package; 381,091,840 B		Hunt
bd35b1cd4412add4f77322763dedfa49f27a06d7a7b1d2b283a25832c2f1a432	SHA-256	ISO9660 image Vat.N0.20260804142245.IMG inside 20260804142311.ACC94F70494B.zip (Dt-r19, outer e8409b4f); 7,624,704 B		Block

Value (defanged)	Type	Role	Observed (UTC)	Use
084c7711a6ecc74fcc70642d160443b3d8371c6fed2515849c902ae299b76516	SHA-256	ISO9660 image No.20260811113519.IMG inside 20260811113533.4CEB7C05AACF.zip (Dt-r26, outer ef3a41ca); 9,592,832 B		Block
0ba8cd6fcbffa98179314fa8cf89f64b0d533dbb918c2817e140c81ec7dad269	SHA-256	ISO9660 image Vat.N0.20260803122837.IMG inside 20260803122910.C6375C5AB9F9.zip (Dt-r18, outer f2e5148c); 7,733,248 B		Block
bb7397a8fb6f4d93d4696e7da4a352980908457e77e879bc4316bd8ee0f6a593	SHA-256	ISO9660 image Vat_N0.20260805114009.IMG inside 20260805114029.D42518EF0FDC.zip (Dt-r20a, outer f6a97ffa); 7,528,448 B		Block
4612b85c223d7952ff9b21199466d16579b8c97c7753ec5189bbf9d8b7367607	SHA-256	ISO9660 image TI.Number-20260819145147.IMG inside Tax-Number852693.zip (C-r17, outer feb58c7b); 9,125,888 B		Block
3c6f5a7b0079d3a2e024506799381cafa6b75f40b42766aa55590d8de3b4df1e	SHA-256	File that contacted 43.224.224[.]81 on 2026-09-23, the day after fuoe333[.]club used the IP address; detected as trojan.lazy	2026-09-23	Hunt
acba1b70f64fa0d55dc8162dd8078df55c40e55be734b9741db22029f5f3804d	SHA-256	File that contacted 43.224.224[.]81 on 2026-09-23; detected as trojan.silverfox	2026-09-23	Hunt
d99f5efc60b7920862bfd90cb59f754d5665cb88547db2d797085b8acf174921	SHA-256	File that contacted 43.224.224[.]81 on 2026-09-23; detected as trojan.abtrojan	2026-09-23	Hunt
27254125e70df5045dc8f2ed6234c36122198012ebe9c3e7d05ccd994e6d56cd	SHA-256	HTA 123.pdf.hta that fetches hxxps://wordtax[.]ink/down/setup.aac and silently installs a ManageEngine UEMS agent reporting to 122.10.117[.]3	2026-08-25	Block
02e16c3fe5d9c35090201b77ad5ae85f7aa9b0ac0be0d2b13b8642149fffd180	SHA-256	145.vbs; contacted 122.10.117[.]3 and 181.214.250[.]206:443	2026-08-05	Hunt
e89bc9123c8d8bd189cb121b01cad5c4dc9ef87c04c060ded6035402024e0eae	SHA-256	Purchase_Order_Details_and_Quotation_Sheet.vbs; traffic with 103.193.172[.]103 and 122.10.117[.]3	2026-08-05	Hunt
29453368a7c14218e8cdbacd177c6b82e30a8642e9aa5bfec4b48067219d9214	SHA-256	Click to open the file.vbs; traffic with 103.193.172[.]103 and 122.10.117[.]3	2026-08-06	Hunt
9f6600c5df3ef874293a9eb0d331c2ccfffee9f4a350762559745fc011c4dcfe	SHA-256	Purchase_Order_31_July_2026.pdf.zip (3,806 B) served by agent[.]jpword[.]cc	2026-07-30	Hunt
c949596ac7491216ee1b13c3e10c9b31313bbd5c15b7d8ebb972cd8a0b738d63	SHA-256	20260810124517.A8F39C2D71BE.zip served by gzsgdn[.]com in the kit archive naming	2026-08-10	Hunt
293c05f0b119de8d3ffc974c9d58480374e7a69b6b15c067431bd40e09d2cc24	SHA-256	20260810134755.B7D42E8C91AF.zip served by an OSS bucket behind dltwum[.]com	2026-08-10	Hunt
85a0a2e49cab23121660a37e92e5dfd9b28c78b26f0264941d1865a2f76d2b37	SHA-256	20260830213443-BECCD7053B19.zip served by a COS bucket behind SendGrid u48334250	2026-08-31	Hunt
a2fd0212968cd44dc5f2fbeca9929c8cfda733aefb29efb501a484a040bfa70f	SHA-256	20260901014335-71359EDFC0A5.zip served by hcnaxnkxankknjp[.]com	2026-09-01	Hunt
709ba0d93184a3c1d6e98d6dd0033bf9daa4e5b48f930ea5e2be9a830ef2f65d	SHA-256	20260902114342-063801A8ED70.zip served by hcnaxnkxankknjp[.]com	2026-09-11	Hunt
97ce1eaa60d412824875576c101605cfc855f42aa769ce7bc0dbde707e938493	SHA-256	20260805114016.210116888AF0.zip served by the delivery host; detected as Win32.Trojan.Yogi	2026-08-05	Hunt
f9d511941b2da041689d05dcea00d500391251f333229a1acae34a4a9b6253bf	SHA-256	20260810224007.694275DBF34E.zip served by the delivery host	2026-08-10	Hunt
58b8e90d55b075509443dc080d427466c3f4faffaa70c13a78a9e7e99ea2f7e9	SHA-256	20260814184103.77410DFDD4F7.zip served by the delivery host on all four main links	2026-08-14	Hunt
e071b99af0ff1066b31f004f523c346b11abaa7b969b62534809189f01051e4e	SHA-256	File dropped by the October copy 9b70faeb	2026-10-14	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
1c4270f5a1eb9e40f4e9cfeb97bad5ddc7f57ca907a81f501008d39e3c8a230c	SHA-256	File dropped by the October copy 578b00dd	2026-10-14	Hunt
cb79900f2d49dd2b3d2b9ada5b75122c8167428b612e836037b03cfb975b206a	SHA-256	File dropped by the October copy 578b00dd	2026-10-14	Hunt
5cd15848d52a5b31a72a4ece24ad05a43378d5f136ebd86ffea15af49786e1a3	SHA-256	File dropped by the October copy 29d7b3d3	2026-10-12	Hunt
28380792ec5dbdca1f9be25644eba2d7c6e81c526aaec7ccb1a64691fd1465ce	SHA-256	Body of the Indian tax lure page as served by wordtax[.]ink and its certificate group	2026-08-27 to 2026-09-16	Hunt (page; never block)
7efd55bcb112e63241cc3436c4405313ae4e3c58722531398f599195a17068a7	SHA-256	The Cloud-based Loading page on 181.214.250[.]206	2026-08-25	Hunt (page; never block)
ef93712576cb347b85bc8758a0e1a1a524f97238487f91206a7a1452b85bbd5a	SHA-256	The 31,006 B PNG embedded in the Indian tax lure template (36 hosts)	2026-07-15 to 2026-10-14	Hunt (page; never block)
1084db6a4f3a68b1b5f0a5fc907d513c7d4aeacced54c2c895e818c5553172f9	SHA-256	The 27,464 B JPEG of the 103.23.172[.]15 lure pages	2026-07 to 2026-10	Hunt (page; never block)
b374c49c6e7fbc72fa76c7bedc094cb7ef54386ad89395be0d058d3fd191e298	SHA-256	403 page of the file sharing application, titled 文件下载	2026-07-28 to 2026-09-18	Hunt (page; never block)
8d1e5f80a54df45e67585513f09b616a0dbe17c313cb321492e56c90b2abd5d5	SHA-256	HDP loader kit build with the DHS seal, first seen 2026-08-13	2026-08-13	Hunt
52a20a5b0dd433fc05d5e5d34367955a06174a6485a920b83626a1fe71d30eff	SHA-256	HDP loader kit build with the DHS seal, first seen 2026-08-13	2026-08-13	Hunt
b4dfb2b3cf5bfa574191e3c9ac50394fa5be19fe921141c13b842d3552f7bc3d	SHA-256	HDP loader kit build with the DHS seal, first seen 2026-08-13	2026-08-13	Hunt
84cb61ac98670cc49f919940bc54461c00223ac74fc5b01581b450d89cfe5ab1	SHA-256	HDP loader kit build with the DHS seal, first seen 2026-08-13	2026-08-13	Hunt
bb9950527aae5ccf6edf08846b073ca33bcef82dc0984f8cc9eaabc5eb3b2a17	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
6067e4976a57eddfd7a20dbcfa7ccafce22891eb5e587cd5c7959f07d7375a46	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
06ea5bbd958ec182dd8f138d523937d36779919dd0ccd832c107c67c9db0543c	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
c29cbbfa04100329eb6daa34b03d5369fac8b96c8819b3545accbdfefe4627ae	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
a09b88c39748a23d8bdc088c419f860b52761fa70524a861604ac791bee9ce76	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
7240a308c706371cfa2a8973091e9a1c624a46bb7fd67bb94d3ea5a473d82a33	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
fb92374d66b5fb972df195c81f6700f2cf336b9f43369981f91ddf5b5c19f034	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
c996442832306d1318826c9918d1f3b173964a1eb50d743bbb26aa4514357e70	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
a53aeb3862d828f370a0df799cddcdd81d5e79896c9129d1dfdcfa38c3a54592	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
a5123adc26985c8b67400b4a585a8e1a4244869dd76b5dd42fa9cf983c073149	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
d408bcd61bc022430cfed065cee3418a057d4ae6d3119dca6ab044836651ef7c	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
5994a54a3d307af86419b615404ec058a3d0e51a0e40163920be112bee0a6cee	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
0f1249768e2fe6e2e98146d70dc0d65eda396f6d6cfadea3d1a11f7838005ebe	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
a401af6054995043570bbed66da4d867ffa8bcbb2d76cf503879a4241e1b03c2	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
4632c24ea5c20a3e18d574e4160169186b7b29d8ccc2ffda7603229155134559	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
056227a297f73f0af39e42f606c5ed2295607d60e9674c8ca12e0f8980f18605	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
c3a18392d61f34806c15294e1199a4036d4b94978fbf276695ecd8ed0bef650a	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
2975e5e9190c87ad497c841fa49b9501a64e69525166c139c3043d720ddfcd4b	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
05cce219ba84d0e650fb310b42a1734c86fe8a51b0cee199c645fb9e1c59f5d0	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
a2407ba5ae4b21a1a6dede9ee67c814fdecd4d86d8c47be93d235e8a8a949c2e	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
133c57a70cf0ed37340349ff12fc4a5944f8d9a941183f4186f2fc047e1e6f45	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
36df84a18a1e09e7fa3ccc26ef2c07c4ec3ce149593c01454b4648e215d8a4bd	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
c3a0d61a8d0fc7f922550fcede44abea76c257fb3e6ca4b23e492f502453e1bd	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
0c420e1b16861132cf612874db93c5ed1b1f9085ebbcc1c8efef2add96c413d2	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
f975297ca50a0242340d59bd3fe2aa2118caecf08ea0fa278cc7ea067bddb3f8	SHA-256	Carrier or DLL of the Spanish cover application without the seal icon (HDP loader kit)		Hunt
07382623c126d7d355f6fcdaefc39eb27e96f4d9a1ae44d4af7b514b56326ec7	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
044685cec0e984f25a603d17870ee1c297842146bca86c2827fea078a3730fbc	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
1bd95bfb94c081d0864196c17c60b536f4d7599690b34b9772afc9746fc59eff	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
66e549d7e9722ceeea0b2193cd81457e406a5ecddf1f0382a268c0456d52b034	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
cf0fd4fc3bfc0aeeec5af236454c02c30faf264980e930397c3ef669487f6479	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
9d3fdbc176111e75ddc725879702794b484daf3a45e4903d65a673fb8a28153a	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
4d9a9a1a347b39365dc19b7697f76c7be3ee02b99adfcd588221ac52eae0f358	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
ff2dfa05c6a86a07406db5a731e1f5e35218fffa9b89538cb6c71ea59746a6f4	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
aac419863dbdc545c8edd946ea7c6ae99d4c42e05bc36520adad817ca70f7ef6	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
51307cb85f159a0ccd4cd31efb33bf3aca0c56f612b667d801698fdd6656e775	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
d590578aa191ab07f61067b1ed18160061daed4b5bec15550adcf47bad25dc9d	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
52d76a4f05b2642486ebfcfcb778643d4d7c377536685ca781818a5663945f76	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
0a857187496e9d6b6ded72c0e281ff77eb6506791bb86450d4e5ef8b9746e5b4	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
0d5190f665ece87e626812a03e4e0501bebe2284cacce49071974c9a9b39b743	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
e8b8e31d10d997d68e3517d70c60cf50788b6f00fc21ec5782f5a8d28407c218	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
749d02aacf954ce95077efc5084679a11ee474799b9961c069413f60278ab854	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
a7433d27d894758ed66fb675e5b0e194a9b5ef724c5f574c3ac5f5958bcd9349	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
9e00b1e4432e819d2ffb69f0dbe20536250f8bcd5fc48d28d281b1544962509a	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
437e2d1f194290ef7535e38d41024eb6f3cb93bebfafd4a3032294bc8d29893a	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
4f2549f7565942f86c4f3ac35f8ccff8b3b65e44ae2ad5511fc8ffcc78dfadbb	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
953af333dc71774ef38826955333e28b7912caa273466739bba5c84b6004d543	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
544c18e680027dc6ce8856e57525a3978cba9a97ca8adb9fd2174db715e6ed6a	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
12e69c188c8b9b428dab8fd73cdf3ce6ac0ea33309e00907f45afc8401afee2d	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
da33a95b2ed28e2c50da002584eb81e4e94fe4a55e98945146842ed9e23be066	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
60507a4f30c4b1f8667be1b809caa854f65661b3741054fa73e133d3944a402e	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
11974ece6c707759b83574eaf844a6fbeebb55c16ac2b5b81d89d7200905733e	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
755b59727fa54b89a9e48fe04cc9004a63bfd43d8e55aefc25ce0c825ca6ab6c	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
e63dc60b24b94658992abec4e5819be35bc0ed5bfc3fe65a89f320539236a181	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
0054331717c89f8088ca578d86e621f6bb30bd31effb0d14ebff02b86713e079	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
8374aa8b2f3cd53fa14ae91383deee561e287fd227efac1b3e84d99c9b1e6d05	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
3cf1559a69676e5c024a865e459b1776645a86e23af7490ab8a3987951c98445	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
28e0c3df894780a78cb33abcc1ab539c28098b57821bd63bac404249624249bf	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
d93b8f420b4f7b912db5e45d6c19f900896a80027d16efce5023764ef6a49396	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
ebff816d0db90e8d7d939b34a0494784cc90baa4d0a76f319edf0c1056b41bb4	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
d56b68edaea946a39509c7a8c1a9178f373473b516e98b8a9e32ebdb6c29fe63	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
d0354ce346b11f9874a63d5a02f05fe4b3afbc762710c9c802c46fa546fdbe3b	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
396a568d2a3002d9e9747a1d3828b0a558b3466e1ee9679bc21296eaf480608c	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
3c23cfbd2585d3ce29525ab74a2ab6258583d3896a69fc3df2c598f2f261fa2f	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
0b6124e5013faa3c836d478ceea1634a42430448a3a2046c9864f727310044f2	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
7441c8aef0fc20a5d4feb31c7167df6bc63c64767528802b1377591d90d24282	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
24737e4a3f8f2e66bf3f437a2af4060277c69f9e796afd8712c10b47a6286ca6	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
5fe95d27ab5df2a92778beff3c2baca988e0ffce0b32ce59190ae51c5d287290	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
33e2a5407e8e46d353aa1ea1970fa374dce41cd21b7840140a9eefcaa6ac48fb	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
3c862fab92e39f8fcd1b9127af00a663b45574c51d43ed835c7cecfb28dc59ff	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
b658fdb91cc66e571b36c9f75e9af7f9aed1b85f500c2d4656d6173bfe1f5bd1	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
620c90c9a87fbe6fe654486cb6fd0f9bc7e71b3c468d8d475f5127fddafd0971	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
42d6551cb401fce5d972773294c2e5cb8383207cce87f88bcfabda45234f285c	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
e51521ec52d5e1fe799f5c81b360cd4bc84b0fe5331c692cb43177e708a6dd5a	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
506f5ba8bbbfe34a4d59a99f5b0e55fe7c4bf41650dddbfb6a87e22c55700d61	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
f9cbf803fc66b822743babee996c1cca18535a699725d97b540559965474a530	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
b240cbc7d9918f78855277131b19a6fcfa950e80bf9ae0b53b5bfffad98a97d4	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
a62357b92b33d1aa598f11c950a6fbdcbcf5ee6b66a7e641504461299e011553	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
7162332a1fcabc7e0f58cf426903fda6179d69db229d05fc645084de875b4e1b	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
056dd24538084987a5119b4c33b15a43c056a6d1a344b730299971f37e0cc2c6	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
408e81e7a1bef7e93fe2ab2640012930c18bcd84ec7117f52cf29bd5b0c75cee	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
9389c737b78963cd2fe5ae87972b37a23998938d376be001ab8eb348169f4bbc	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
5f187f6d3b145641d96b0a74ced673d7b53530045f062a25069eb687f43ab40d	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
5631aa6690d57d83d4a12df2b69f73312b29c2ab625a2bf4e7591a6ec9c52865	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
b6ec8cfa9b0f385de64913a934266c3f6311d742d014565d4fd2f3bb02cac6fe	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
03ffb4229cab1bd0a2fd92fd4425c0f2928e252ade1086f6507c9d5cfee95b44	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
279331759f04cbfb50ac0a12945b94c7aacb734df474f3376607c81584d6e163	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
82219b5a553e738d112f284da60fe7ba91b34d368dc3d155e6d6af6386711304	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
5f8305e0db90315b032829cd450afa1e9dcd4c1ee8f07bce04439345946d5da3	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
b3d6811f6555181d1c64dc5f1497f02b7b29fd065df0c7bdc2c0abdd54540c5e	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
76e76847139a485f85564f29268936185b65dfecaa783ef86144e3e50210bc4c	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
4944cbe859c447d8484fb1d7821c9c3216f5f80284126b7f503a8627b747925b	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
bc6e3153fb28928f6aff28a99eae4c7da730ac085f3bd6eceee4f81ed6fcd71b	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
2edc5a1438a0e4592234cb536dd5e083ffa2e1f96565c63f2b94be8b15d2aade	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
46ce2eaa32c4745dec308101d853e1fcc55aa899501d5a8e7640d686fc91183c	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
d91355fe4abb6c08555964c31eb74384f4a37d0177f9bcff5d176b1472dbe1de	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
7dcba49f48a23b69802b8e4daeb47617d1692a3cb6d1e081c6a80d297cba4dbb	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
0f5e09cbca892269687a147242a1dc669c9824f79f11e29f61afd2d89ddd4bb7	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
bec0b42290927d2a645df1a9de27a4ef1b7408b7935d360251439da34aa53a16	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
fb0da935191df5aefd566e0fef45eef5473d0da5a6ff1a9f1cba94f5260f635c	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
4b9a1f52ae83a0f9020fb580eca0f4d7352a326a7a36b9381aec46f2090e0999	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
c5e82fca91a7b8140781eecbe9f709e96eed638deea3acd5f0ca35ef79a221c0	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
ff5d448c4d1134a2457eff09633e97cd4b88e0780063e1ca0d33d8d07b678dee	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
7e78d45368bc3914cc4486d9e0b23e2bbd67131ba466468d7cf1afb7665cd893	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
849598bcfa56aa4d25eaa1f44dbf33c7f536da0d440cd784ed750f526ab64e40	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
60838c66a43202268f44323a48ad3bd8f8da6787bd808856631f55179ac50b05	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
454d333f979dc6597b47ec662dd9cb32fa2db9da6f971402178499be9f73ae47	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
86a894fe150c8f706c6bd428e391c98259bc1153d99920d5cc0b84b8db688b0a	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
6a16c450dd6801bd1d62aace71f4f800cabb2cfbed39c9dc41099b5b2f4ba909	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
82f9e54914b834dec815cbbaa056742d4a5ac07b43ff9885105f2cb254132493	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
6bb63fa4d331abfbf03c42d9707a0bea48e9829df47237392a89297ef0edbfd1	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
d8e2cdff227e5174c00467e0fd7b0f466bf7e389c11c0cc79a70276c21efa48e	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
d71e41acff208ab175d19c8ceb0cac8e62aeed03b4c81b6899eeab7341847a23	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
18eab3bcdfa609a2cf1607dbb202d99566cfc5d11766f4d2143ca4824e99056e	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
7ed71269e552cb42ad20d2f968613b415f04004a8afb6bb9f19b77e75f2c7163	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt

Value (defanged)	Type	Role	Observed (UTC)	Use
9df49e9a905999b066c1994261c2aefa40bbfe54ff978ea75c131dc7e1a573b9	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
06633543b9d0246d819c76e522c86c3da8643756bcbb6a5860065f48fab78295	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
690582b80494b16b84e84e4aabd11884549ad6eef11808e2c47cd39343c200cd	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
72c0340309269393098 7f5b1c7795df0448c0d8be2d7faa648a860dc4bb8d707	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
0bb39d8f96c9bbff21e64c685e2181122ae0e565c45fe0abde5156d8cd41a89b	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
134f8bfb18284ade87d7cf77e08510701c10d2a4a1e4f1d43030acef7298dcdf	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
39cdc5994f3fea1f717ae7e7c16fccae5b89bc6efe98568c29fe87fb4887ed80	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
54901fc6fb3709bce5d42302c8a5cffc1b7bb53bf1bddd2b73828e6a2c98e01d	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
323fb94a0e3bf79b41824385b0b65af48db83ac84c0fc8d041597bd8824cbbf7	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
02a97b438854101f396a32e95b69b463ce19b327ccbf4d700a5a982cf3575d39	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
cf8917e255209f5362b852ad019d53b21b9325df27eb7ef3d7e2d507776d2afe	SHA-256	Unwrapped HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
3fa64a90d133841ebbb3ccf76cd4554510531f18f65e29d7529f454219abccf8	SHA-256	October protector-wrapped build with the DHS seal	2026-10	Hunt
616cadcb52150fd1746815ae1812730ff254fbba258d24b2e017ff946e66946d	SHA-256	October protector-wrapped build with the DHS seal	2026-10	Hunt
7918f4eb7f2025d3449810c5b20a5a40f7ca401224bfb9eb771675e527ad1b91	SHA-256	October protector-wrapped build with the DHS seal	2026-10	Hunt
806b65c34b886601f1952ed56a6920f53923474bafca99434c4cbf2b777c5c60	SHA-256	HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
e0834dd52ce49221160f866f4c9106d69b54e47bf0dc0e3480c829a4873363da	SHA-256	HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
16c3df59b7f250ee5cafc4c775b386aa0822af8cf7765158e160c3e585c4275c	SHA-256	HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
fe60c7241c2c58edceef60bd4931cc1eb9e4a445292c63e3478c8abb6eab3461	SHA-256	HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
547f66e78a1e1fd42a6d9280dad7fd2c3c83342e77c4bf11475fd2afcba30405	SHA-256	HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt
492de970332b2783fd87ffa70da595ffe1e708d321205a1d5085d06e5dc53d9e	SHA-256	HDP loader kit build with the DHS seal	2026-08 to 2026-09	Hunt

Table C: File indicators. Rows marked Never block are legitimate signed hosts and must not be imported as indicators.

The lure page files are three further groups of hashes to hunt as pages and never block: 146 page files on 103.23.172[.]117, 139 of them one Indian tax lure page of 48,255 to 48,260 bytes; 66 page files on 103.23.172[.]15 from 2026-07-14; and 29 files on g00g1e[.]club.

D. Configuration and build values

Table D lists the group IDs configured in the builds, the import and Rich header hashes of the builds, the certificate serials of the signed hosts (Annex Table 7 of the technical annex) and two structure values of the embedded drivers (Annex Table 6 of the technical annex). A group ID is the head of the build's mutex string, and written backwards it is the build's RC4 configuration key (report section 3.2).

Value	Type	Role	Use
f83b5c8d017e806c948851bffc6e9b0e	Rich header hash	Rich header hash of the 2026-08-19 compile and its October rewraps	Hunt
a8254a46e2df6d8e6e6a9b787294c60c	Rich header hash	Rich header hash of `67e1ac14`	Hunt
6758435f5f634446e4dc0111d53fd014	Import hash	Import hash of the Themida-wrapped October builds; 23 files, first seen 2026-10-05 to 2026-10-14	Hunt
946a45c962a4e1c30f9ec7584793a05e	Import hash	Import hash of the Enigma-wrapped October build `66f1eb68`	Hunt
e7ff6484a786eddc25685621265659b5	Import hash	Import hash of the 2026-08-09 compile of the Chinese cover application; `67e1ac14` and one auk218[.]club loader	Hunt
39a6d9af7f2cbb3fba9783c078108f4a	Import hash	Import hash of x64 loader template 1; other tools compute other values	Hunt
c8f3a8a596607b984628e8e421d68c8c	Import hash	Import hash of x64 loader template 2	Hunt
3ce64bc832f0f365a142d024185cf8ee	Import hash	Import hash of x64 loader template 3	Hunt
0d377d85bcc8f6f453462860ce72dee6	Import hash	Import hash of x64 loader template 4; another tool gives 4d1e5f8e59a559b93f8ed9e4f6adcf73	Hunt
10ba571927e07217a4fa2772d771cee2	Import hash	Import hash of x64 loader template 5	Hunt
3e9a836347ce9228c681791f8d38dfa1	Import hash	Import hash of x64 loader template 6; another tool gives ae019a919d51465bf2685b38bc059a61	Hunt
D2CCF5010C42A9ADDFB	Group ID	Group ID of build B1	Hunt
E00AB0FD05C389654DA	Group ID	Group ID of build B2	Hunt
BAEAF54DA4790C5DF14	Group ID	Group ID of build B3	Hunt
EE7E8CF6AEE6D21B33B	Group ID	Group ID of build B4	Hunt
EFF5A25F278EACE2B90	Group ID	Group ID of build B5	Hunt
C54B8B9C1FD48DC2319	Group ID	Group ID of build B6	Hunt
E3EFA9C39EFB93358FF	Group ID	Group ID of build B7	Hunt
E401B34ACF61476EEE8	Group ID	Group ID of build B8	Hunt
6C4C1D842DE25C81A17	Group ID	Group ID of build B9	Hunt
0618B8FDAB471F3CFA0	Group ID	Group ID of build F1	Hunt
D34DDB2892EDD5DD63A	Group ID	Group ID of build F2	Hunt
7E8DE44AF7B5503E68A	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
58F5DC377BF14CBA6EE	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
EBC35E655B9E620BAE4	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
FE9F200028436673AB9	Group ID	Group ID, early build with the DHS seal, the operation, configured to fuoe333[.]club	Hunt
AEF8911293BCD0316CE	Group ID	Group ID, x64 build outside the operation, configured to oswin[.]club	Hunt
DDFABED821E9AEC49D2	Group ID	Group ID, x64 build of the operation, configured to taku788[.]club	Hunt
5EF0AA741CEB7263FD2	Group ID	Group ID, x64 build of the operation, configured to fuoe333[.]club	Hunt
3E27157771EC918C409	Group ID	Group ID, x64 build of the operation, configured to taku788[.]club	Hunt
FFBFABEF13F5D8EDDC0	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt

Value	Type	Role	Use
DB38E656D9CA8EE8264	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
D70F24D7E639CFCC22A	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
B9ADFCBCBCBD7FE9D31	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
AC59D7E7F6F4F42F6B9	Group ID	Group ID, C15, configured to 192.252.183[.]157	Hunt
71F27E5C7E6F5B5F7AF	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
2C58AFEB61BAE050360	Group ID	Group ID, x64 build of the operation, configured to fuoe333[.]club	Hunt
730F597C42E6B7AE38B	Group ID	Group ID, x64 build of the operation, configured to taku788[.]club	Hunt
CB240DFEF108C40DE17	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
BDE82AEE5CC03BBA077	Group ID	Group ID, x64 build of the operation, configured to taku788[.]club	Hunt
A5D86FEDCBFE6FFBDF2	Group ID	Group ID, x64 build of the operation, configured to fuoe333[.]club	Hunt
DF2D3B53EFA6555F37C	Group ID	Group ID, x64 build of the operation, configured to taku788[.]club	Hunt
C8BE92718C82DB59542	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
3E1CFC5C37EFB77914F	Group ID	Group ID, x64 build of the operation, configured to taku788[.]club	Hunt
AE79B5D5314CE1AA81C	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
E3EA13BC19EAEC3A6A5	Group ID	Group ID, x64 build of the operation, configured to moik77a[.]club	Hunt
A18AA22EAB1E4EBAE7A	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
E008558557E5EC845BA	Group ID	Group ID, early build with the DHS seal, the operation, configured to fuoe333[.]club	Hunt
8A3CCDFB49407F49CCA	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
E8668A6FCAA50C7BEC4	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
6CFCE5F9F9BA5C5736C	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
2CF4C69CDF0FE81524D	Group ID	Group ID, auk218[.]club loader (HDP loader kit, outside the operation), configured to auk218[.]club	Hunt
1BF1E413B6E0E93047F	Group ID	Group ID, C17, configured to 192.252.183[.]157	Hunt
C2F416B4ECC0BB743C9	Group ID	Group ID, early build with the DHS seal, the operation, configured to fuoe333[.]club	Hunt
73218D10CB4054294D6	Group ID	Group ID, early build with the DHS seal, the operation, configured to fuoe333[.]club	Hunt
18C0F9306B46487D00384971	Certificate serial	Guangzhou Ningjinghai EV certificate on `arphaCrashReport.exe` (genuine vendor signature)	Pivot only
01FEBC8A7743533E070A2A480BF510B5	Certificate serial	Hithink RoyalFlush EV certificate on `hxdaemonprocess.exe` (genuine vendor signature)	Pivot only
0E58A7A89AA85656786458595ACEA982	Certificate serial	Hangzhou Fencha (ShadowBot) EV certificate on `debugger.host.exe` (genuine vendor signature)	Pivot only
0EC3880864ADEB96CAFC6AABAFDA1F94	Certificate serial	Tencent certificate on `WeChatAppEx.exe` (genuine vendor signature)	Pivot only
085B3F83136C2B622045218988C6BACD	Certificate serial	ZEON Corporation certificate on `ConvertToPDF.exe` (genuine vendor signature)	Pivot only
042C5C97FAEACFEC7115FA1C9229DA9B	Certificate serial	ZEON Corporation certificate on `ConvertToPDF.exe` (genuine vendor signature)	Pivot only
083EA13884BDFFCE8E5D9D5CAD2EFBDE	Certificate serial	JetBrains certificate on `keytool.exe` and `rmiregistry.exe`, hosts of the padded x64 loaders (genuine vendor signature)	Never block
0B50CF246B263EFD85A729315158F3FF	Certificate serial	Google certificate on `platform_experience_helper.exe`, host of a padded x64 loader (genuine vendor signature)	Never block
84D5733C4181BE468CD04DB03F507188	Certificate serial	Siber Systems certificate on GoodSync `LogView.exe`, host of a padded x64 loader (genuine vendor signature)	Never block
F8495E224EFA55D4	Certificate serial	BugSplat certificate on `BugSplatHD.EXE`, host of a padded x64 loader (genuine vendor signature)	Never block
33000004855E99EC0E592FCDD7000000000485	Certificate serial	Microsoft certificate on `LINK.EXE`, host of a padded x64 loader (genuine vendor signature)	Never block

Value	Type	Role	Use
0x8930	PE checksum	The 2018 driver (`NVAPO32V`, `ZH_CN`); certificate table at 0x3800, 15,984 bytes, ending at the resource size of 30,320 bytes	Pivot only
0xC475	PE checksum	The 2023 driver (`NVAPO64V`, `ZH_HK`); certificate table at 0x4600, 20,896 bytes, ending at the resource size of 38,816 bytes	Pivot only

Table D: Configuration and build values, certificate serials and driver structure.

E. Host artefacts

Table E lists host artefacts. The registry value under `HKCU\Console\0` and the configuration mutex are the most precise to search for.

Artefact	Type	Builds	Note
`NvContainer.NvapiMonitor.{GUID}`	Scheduled task	2026-08-19 compile	GUID random per host
`C:\ProgramData\NvContainer.NvapiMonitor.{GUID}\nvpluginnvapimonitor.nvx.vbe\`	Folder	2026-08-19 compile; October copies	Contains the host copy and `hdp.dll`
`C:\ProgramData\HDAudio.Driver.{GUID}\HDAudio.nvi\HDAudio.NVX.EXE`	File path	67e1ac14	Written with `pdfcORe8.DlL`
`C:\ProgramData\S-1-5-21-<SID>\<SID>.CMD`	Watchdog script	2026-08-19 compile	A 60 second relaunch loop
`HKCU\Console\0`, value `389126097FFFEF316D35ACD0610E5F31`	Registry value	All six live runs	The stage as stored, 338,947 bytes
`HKCU\Console\IpDate`, `HKCU\Console\IpDatespecial`, `HKLM\SOFTWARE\IpDates_i4`, `HKCU\Network\GROUP`, `HKCU\Network\REMARK`	Registry values	Core; 2026-08-19 compile runs	Configuration override and state markers
`|<19 hex group ID>|A1:<host>|...`, or `|<19 hex group ID>$@<YYYY-MM-DD>#|A1:<host>|...` in builds compiled from 2026-08-16	Mutex	Every configuration analysed; also at runtime	The whole configuration string
`%Temp%\TAOKERNELEX64_AV.SYS`, `%Temp%\TAOACCELERATOREX64_AV.SYS`, `%LOCALAPPDATA%\Temp\TAOKERNELEX64_EV.SYS<d-h-m>`, `%LOCALAPPDATA%\Temp\TAOACCELERATOREX64_EV.SYS<d-h-m>`	Driver drop paths	Core; F1, F2	Never written
`\\.\xkpsm`, `\\.\ardrv`, `\\.\HWAudioX64`, `\\.\BootRepair`, `\\.\Warsaw_PM`	Device names	B7, B9; B4, F1	Never opened
`C:\Users\Public\nvlocalizedconfig\<name>\`; `%PUBLIC%\Libraries\NVTELEMETRY\<name>\`	Install paths	F2; F1	Set in the build's code
Random names of six to nine characters under `C:\Windows\`	Dropped executables	October copies, 2026-09-03 x64 builds, one early seal build	From the file metadata of these builds; none in our VMRay runs
`BC2411DEE9DC`; `BC24C35BEEF5C796C7835BBAFD537E8D`	String RC4 keys	x86; x64 loaders	Kit constants
`F:\dd\vctools\vc7libs\ship\atlmfc\src\NvPluginWatchdog\Release\NvPluginWatchdog.pdb`	PDB path	B1 to B6, C17	Grafted onto Microsoft's build tree
`hdp.dLL`, `hdpGmS.DlL`, `xwEB_eLF.dLl`, `ARPHADUMP.Dll`, `RPABUILDER.DLL`, `pdfCoRe8.dll`	Side-loading names	Kit builds	Letter case varies
`<YYYYMMDDhhmmss>.<12 hex>.zip`, also with a hyphen before the suffix (F1) or a `ZIP-` prefix (`12f496cd`)	Archive name scheme	15 of 15 further archives; F1	UTC+8 packing time plus the key prefix; the `ZIP-` form shares the shape

Table E: Host artefacts and strings for hunting.

TLP:CLEAR