Beyond ValleyRAT: Technical annex

This annex is a companion to the report "Beyond ValleyRAT: Inside a China-Nexus Silver Fox Operation". It holds the supporting tables, lists and evidence detail for the report body. The annex is ordered by topic: A1 names, A2 method, A3 the kit, A4 infrastructure, A5 registrants and accounts, A6 public reporting and attribution. Section, table and figure numbers without the word Annex refer to the report. Citation numbers refer to the reference list at the end of this annex. Indicator values are defanged.

A1 Names used in this report

Name	What it is	Where it appears
ValleyRAT (Winos 4.0)	A backdoor family first reported in early 2023; its builder has been public since March 2025	A2, 3, 6
Silver Fox	An intrusion set, a cluster of activity that vendors track as one. Several vendors track it by its ValleyRAT campaigns and infrastructure and place it in China; we use it as an umbrella for more than one team	A2, 6
China-nexus	Run from a Chinese-speaking environment; no claim of state direction	6.2
HDP loader kit	Our name for the toolkit behind all 44 loaders, after `hdp.dll`, a library name it borrows from a Hithink RoyalFlush program	3, A3
The operation	The 25 loaders that call five C2 servers, and their delivery	2
B1 to B9, F1, F2, C15, C17	Build IDs: B1 to B9, F1 and F2 are the eleven loaders we have as single files; C15 and C17 are two of the 33 builds we extracted from 97 archives	Table 4, Annex Tables 4 and 5
KANGYINGJIE, ZHENGJUNHUA, CENGCHAO	Registrant names: KANGYINGJIE in the records of four C2 domains and, in one listing outside our own records, of auk218[.]club; ZHENGJUNHUA in those of usdt888[.]club, oswin[.]club and 11 other domains; CENGCHAO in those of shyda6317[.]club and six other names; a registrant entry is one such name with its own hashed value and province	4.1, A4.8, A5.4, A5.5
574849-1923	Registrar account (a customer number) at Gname, printed on 243 domains	5, 6, A5.6
The delivery host	kaiwyrey[.]eu[.]cc, a file-sharing site whose four main download links nearly always served the same file as one another	4, A4.2
The auk218[.]club loaders	16 earlier loaders from the delivery host that call auk218[.]club	4.4, A6.3
The padded x64 loaders	Loaders of another family on nearby delivery domains, padded with 138 to 502 MB of filler	A4.6, A4.7
The October re-packed copies	Protector-wrapped copies of the 2026-08-19 compile, seen from 2026-10-05	A3.2, A4.1

Annex Table 1: Names used in this report.

A2 Method

Where the research began

The research began with one file (B1), a library that presents itself as NVIDIA Telemetry, from the VMRay UniqueSignal Threat Intelligence feed. In VMRay's run of 2026-08-21, B1 contacted the C2 server taku788[.]club, received a 339,077 byte stage from 202.61.85[.]104 and installed a scheduled task and a watchdog.

Domain registration records and what they name

A domain registration record is the public record created when someone registers a domain with a registrar. It lists the registrar, the creation date and the registrant, the person or company entered as the owner, often with an organisation, province and email address. The registrant types these fields, so they are claims, not verified facts. KANGYINGJIE, ZHENGJUNHUA and CENGCHAO are registrant names in the organisation field at the registrar 22net, a field we call the registrant organisation. A registrar account is the customer number that a registrar prints in place of contact details, as Gname prints the account 574849-1923 on 243 domains.

Many records hide the registrant behind privacy protection (redaction). Historical copies of some records also replace each contact value except the country, redacted or not, with a fixed code, so two records with the same code share that value. We call the code that stands for the registrant organisation the hashed registrant value. We use registrant names, hashed values and registrar accounts as keys that connect records. A zone serial is the version number of a domain's DNS settings; it changes when the owner edits them.

What is ValleyRAT?

ValleyRAT, also called Winos 4.0, is a remote access tool (RAT): a backdoor that gives an attacker interactive control of a Windows computer. Its core is a library named `登录模块.dll` ("Login Module"), built in 32 and 64 bit forms [1]. The ValleyRAT builder turns the loader code into configured builds and has been publicly available since March 2025 [1]. The family alone therefore names no operator (section A6.4 gives the scale of ValleyRAT use). Here the builder configures the HDP loader kit one precompiled loader at a time (section A5.2).

What is Silver Fox?

Silver Fox is a name that several vendors give to an intrusion set they track by its ValleyRAT campaigns and infrastructure and place in China [3] [4]. China-nexus here means run from a Chinese-speaking environment, with no claim of state direction. The name covers more than one team. CloudSEK describes a Silver Fox tax notice campaign against India [3]. Kaspersky dates Silver Fox tax emails to India from December 2025 and to Russia from January 2026 [19]. Sekoia describes Silver Fox tax audit lures from mid December 2025 [4]. Proofpoint claims only an overlap between its TA4922 and activity others call Silver Fox [6]. We use the name in that umbrella sense and place the operation inside the umbrella rather than in any one team (section 6.1).

How we grade connections and judgments

A shared value alone does not prove one party controls two domains, IP addresses or accounts, so we grade every connection between them by the rule in Table 3.

Values that many unrelated parties share carry no weight. They include registrars, default name servers, privacy values, autonomous system numbers (ASNs), shared IP address ranges such as a /24 block of 256 IP addresses, dates, top-level domains and lure themes. They also include toolkit facts such as a shared builder, compile, cipher, port profile (the set of C2 ports a build uses), template or archive naming habit. Section 6 weighs lure themes, registrars and host vendors only as markers of tradecraft and environment.

Each judgment has two parts, in separate sentences. The likelihood uses the terms of Intelligence Community Directive 203 (ICD 203), each of which stands for a range of chance [20]. The confidence says how solid the evidence is: high when several independent kinds of evidence agree, moderate when it is credible but has gaps, low when it is thin or indirect. We always give its reason.

Facts we observed directly, such as a compile time, need no likelihood term; the text names where each one comes from.

A3.1 How the loaders reach victims

Chain	Package and the name the victim sees	Signed program (signer)	Loader file	Build
A. Three RAR droppers	RAR5; `Notice from Tax Departmen.exe` and two hex names (a)	none; unsigned droppers, one in Rust	none; one drops a `vulkan-1.dll` proxy	not kit loaders
B. VHDX	VHDX `02a39ca8`; `3625132209.EXE`	Alibaba arphasdk `arphaCrashReport.exe` (Guangzhou Ningjinghai)	`ARPHADUMP.Dll`	B9
C. VHDX	VHDX `33d5170d`; `CERT-In5605112305.EXE`	`hxdaemonprocess.exe` (Hithink RoyalFlush)	`hdp.dLL`	B7
D. ISO in ZIP	`Tax-Number852694.zip`; `INT-Number.20260820113657.EXE` (b)	`hxdaemonprocess.exe` (Hithink RoyalFlush)	`hdp.dLL`; `hdpGmS.DlL` (C15)	B4, C15, C17
E. ISO in ZIP	ZIP `d4a8b9d3`; `Num.20021504092026.EXE`	ShadowBot `debugger.host.exe` (Hangzhou Fencha)	`RPABUILDER.DLL`	F2
F. VHD in ZIP	`20260902110114-0AFC3F174BAD.zip`; `_T.0902110038.EXE`	`WeChatAppEx.exe` (Tencent)	`xwEB_eLF.dLl`, hidden	F1
G. Loose library	B8 on its own	`NVDisplay.Container.OverClockingNvc.exe` (NVIDIA), named by the loader	fake `libcef.dll` (`GfeXCode.dll`)	B8
auk218[.]club loaders (c)	ZIPs named `<stamp>.<12 hex>.zip` or `Tax PenaltyN0.<date>` holding ISOs; inner tax or VAT notice names (d)	`ConvertToPDF.exe` (ZEON Corporation)	`pdfCoRe8.dll` in mixed case, hidden	16 loaders
October re-packed copies	7-Zip self extracting archive; ZIPs named `Account_Statement_PC_Version`	none; run through `rundll32.exe`	`hdp.dll`, wrapped by Themida or Enigma	25 copies

Annex Table 2: Delivery chains we observed.

Notes to Annex Table 2:

- (a) `E37F81F5B2C901FE1ADBCF1746E5F6268.exe`, packaged 2026-09-24, and the Rust dropper `D43F785B2C901_2026092412841.exe`.
- (b) C15 and C17 came in `Tax-Number852690.zip` and `Tax-Number852693.zip`, inside the disk image files `INV-No.20260817164222.IMG` and `TI.Number-20260819145147.IMG`.
- (c) Outside the operation.
- (d) Inner names such as `Vat.N0.`, `VATNo.` or `T.No.` followed by a UTC+8 stamp.
- Hex labels such as `02a39ca8` start the package's SHA-256 (Table C of the indicator file).

The RAR droppers of chain A carry no kit loader, but one shared IP address puts them near the operation. Under the rule of section 2, one shared value of this kind is a weak connection. In a late September VMRay run the tax dropper, `Notice from Tax Departmen.exe`, tried to post to 202.61.85[.]50 on port 2222. The operation's C2 domain taku788[.]club used that IP address on 2026-09-23 (Annex Table 10). The other two dropper names echo the

VHDX name of chain C, `D33F785B2C901FE1ADBCF1746E5F6268.vhdx`, but that is a packaging trait and carries no weight.

That file led us to a loader toolkit that we call the HDP loader kit. The name comes from `hdp.dll`, the file name its loaders often travel under, in mixed case such as `hdp.dLL` (Table 4). The file `hdp.dll` is the library that `hxdaemonprocess.exe`, a program of the Chinese stock trading software maker Hithink RoyalFlush, loads from its own folder. The loader packages rename that program as a tax notice and place a loader beside it under that library's name. Hithink RoyalFlush is an abused vendor: its program is unmodified and validly signed, and the loader is unsigned (section A3.7).

Each August and September loader we can place in a package travels beside a genuine signed program renamed with a number, most often a VAT or other tax number, or as an advisory. The pair sits inside a VHDX, ISO or VHD disk image, often in a ZIP. The program loads a library of a fixed name from its own folder, so the loader runs inside a trusted process. This is DLL side-loading (Figure 3). Disk images are also a common way to shed the Mark of the Web, the tag Windows puts on downloaded files. No package held a decoy document (Table 4).

The package names also carry the packing time. In chain D, the name `INT-Number.20260820113657` matches the file times of the ISO at UTC+8. In the delivery host's August ISO packages we analysed, the file times of their disk image files are stored at UTC+8, eight hours ahead of UTC. The packing clock therefore runs at UTC+8, which covers China but also Hong Kong, Taiwan, Singapore and Malaysia.

A3.2 The builds: compiles, C2 servers and cover applications

Builds of one compile differ only in the `.data` section that holds the configuration. The six builds of the 2026-08-19 12:39:19 UTC compile are B1 to B6. They call five C2 servers (Annex Table 3), so a shared compile is no evidence of one operator. Below we call this compile the 2026-08-19 compile. C17 is a separate compile of 02:14:08 UTC that day. B1 to B6 present themselves as NVIDIA Telemetry (`NvTelemetry.dll`), and B7 and B9 as Tencent software. B8 and F1 present themselves as NVIDIA components, and F2 as `NvLocalizedConfig`. The PE time is the compile time in each file's header.

Build	SHA-256 prefix	Arch and size (bytes)	PE time (UTC)	Group ID	C2 server
B1	`5b896138`	x86, 6,074,880	2026-08-19 12:39:19	`D2CCF5010C42A9ADDFB`	taku788[.]club
B2	`d9179153`	x86	2026-08-19 12:39:19	`E00AB0FD05C389654DA`	moik77a[.]club
B3	`3dc4d9df`	x86	2026-08-19 12:39:19	`BAEAF54DA4790C5DF14`	fuoe333[.]club
B4	`a0160e1f`	x86	2026-08-19 12:39:19	`EE7E8CF6AEE6D21B33B`	192.252.183[.]157
B5	`f42c77fc`	x86	2026-08-19 12:39:19	`EFF5A25F278EACE2B90`	usdt888[.]club (a)
B6	`bf503421`	x86	2026-08-19 12:39:19	`C54B8B9C1FD48DC2319`	usdt888[.]club (a)
B7	`a5bab855`	x86, 9,710,080	2026-09-22 21:42:52	`E3EFA9C39EFB93358FF`	taku788[.]club
B8	`2ff861c4`	x86, 5,747,200	2026-09-16 02:05:32	`E401B34ACF61476EEE8`	taku788[.]club
B9	`60243bb5`	x86, 9,570,816	2026-09-21 20:02:04	`6C4C1D842DE25C81A17`	taku788[.]club
F1	`faac737c`	x64, 7,571,968	2026-09-01 17:40:17	`0618B8FDAB471F3CFA0`	fddlbh2[.]club
F2	`2960996c`	x64, 10,307,584	2026-09-03 17:18:04	`D34DDB2892EDD5DD63A`	fddlbh2[.]club

Annex Table 3: The eleven configured builds we have as files.

Notes to Annex Table 3:

- Full hashes are in Table C of the indicator file.
- Every build uses one server on ports 7800, 7811 and 9999, except those marked (a).
- (a) B5 and B6 use 6088, 6099 and 9999 and leave the third channel empty.
- VMRay runs showed the configurations of B1 to B7 as well.

The 97 further archives held 33 more configurations (Annex Table 4). The group ID, a 19-character identifier in each configuration, never repeats across the 44 builds, so it marks a build, not a customer.

Builds	Loaders (n)	Compiled (UTC)	C2 server	Delivered by	First observed (UTC)
auk218[.]club loaders	16 (a)	2026-08-02 to 2026-08-11	auk218[.]club	kaiwyrey[.]eu[.]cc	2026-08-03 08:20 to 2026-08-12 05:10
Early fuoe333[.]club builds	4	2026-08-13 to 2026-08-16	fuoe333[.]club	none on record (b)	2026-08-13 12:25 to 2026-08-17 12:42
C15	1	2026-08-16 14:18:35	192.252.183[.]157	`Tax-Number852690.zip`	2026-08-17 14:49
C17	1	2026-08-19 02:14:08	192.252.183[.]157	`Tax-Number852693.zip`	2026-08-20 05:11
x64 builds of 2026-09-01	3	2026-09-01 17:40:17	taku788[.]club (2), moik77a[.]club (1)	none observed	2026-09-02 08:12 to 2026-09-04 00:30

Builds	Loaders (n)	Compiled (UTC)	C2 server	Delivered by	First observed (UTC)
oswin[.]club build	1	2026-09-01 17:40:17	oswin[.]club (c)	none observed	2026-09-02 18:10
x64 builds of 2026-09-03	7	2026-09-03 17:18:04	taku788[.]club (4), fuoe333[.]club (3)	none observed	2026-09-04 23:20 to 2026-09-08 00:22

Annex Table 4: Further builds extracted from the 97 archives we examined on 2026-10-14.

Notes to Annex Table 4:

- C15 and C17 came from the delivery host kaiwyrey[.]eu[.]cc.
- (a) In 17 packages.
- (b) ISO images named `Notice from Tax Departmen.IMG` were seen with fuoe333[.]club in these weeks (section A6.3).
- (c) Ports 6088, 6099 and 9999, third host empty.
- Table D of the indicator file gives every group ID.

The builds also differ in the version of their cover application, the harmless Windows program each loader is built on (section A3.3). The version shows in the file's main icon. Our eleven builds call five .club C2 domains, the four of the operation (section 2) and fddlbh2[.]club, which sits just outside the operation:

- taku788[.]club
- fuoe333[.]club
- moik77a[.]club
- usdt888[.]club
- fddlbh2[.]club

Of 197 files that communicate with these five domains, 195 carry the antivirus family names ValleyRAT, yogi or Winos. Their main icons show six versions of the cover application used over seven weeks.

Four of the six versions followed the other two from 2026-08-24. They are in Chinese Simplified, and we name them after their icons. The six versions cover these files:

- The Spanish version, whose main icon is the DHS seal: 170 files, which between them call all five C2 servers of the operation, its four .club domains and 192.252.183[.]157 (section A3.8).
- The Chinese version of 2026-08-02 to 2026-08-11: 17 files, the 16 auk218[.]club loaders and `67e1ac14` of 2026-08-09 (section A6.3).
- FvSDK: 10 files.
- The stock icon of the Visual Studio application wizard: 22 files, among them B8.
- NVIDIA FrameView art: 23 files.
- The Tencent QQ penguin: 8 files. B7 and B9 carry the same icon but are not among them.

These counts come from a search by main icon, not from the 197 files. They therefore add up to 250 and are not a breakdown of the 197.

Copies of the 2026-08-19 compile were very likely still being distributed on 2026-10-14. Confidence is moderate, because the evidence for these copies is what their protector wrapping leaves visible: file metadata and contact logs. From 2026-10-05, 25 files with the seal as main icon appeared, all wrapped by Themida or Enigma. These are commercial software protectors that wrap a program in an encrypted layer and hide its code until it runs. All 22 whose metadata we analysed keep the PE time and Spanish icons of the August compile. Six also keep its Rich header hash (a fingerprint of the compiler run), exports and version number. Four of those six have icon resources that match the seal byte for byte, and one of the four carries the kit's x86 string key `BC2411DEE9DC` (section A3.3). The other two keep only the full resource template and the compile time. We assess it almost certain that the four are builds of the Spanish cover application, and very likely that the other two are. Confidence in both is moderate, for the same reason: the evidence is what the protector wrapping leaves visible. Seventeen copies contacted usdt888[.]club, in two groups:

- Sixteen copies first seen from 2026-10-05 to 2026-10-12: they share the Themida import hash (a hash of the functions a file imports) `6758435f5f634446e4dc0111d53fd014`. Eleven of them were also seen on 156.245.245[.]222.
- `578b00dd`: it contacted usdt888[.]club on 156.245.245[.]222 on 2026-10-14.

Table D of the indicator file gives the same import hash for 23 Themida-wrapped October files.

A3.3 Inside the loader

Every loader is the code of an ordinary Windows application with malicious code added. The ordinary part, which we call the cover application, is FakeApp, the skeleton program that the Microsoft Foundation Class (MFC) application wizard of Microsoft Visual Studio generates. Its code is unedited; between versions, its language and its main icon change. The cover application is in Spanish from 2026-08-13 to 2026-08-23 and in Chinese

before and after. It makes the file look like ordinary software, and in the 2026-08-19 compile its own code never runs. The malicious code sits in `.00CFG0`, an encrypted section named like the compiler's Control Flow Guard section. The section's strings decrypt under RC4 with `BC2411DEE9DC` in x86 builds and `BC24C35BEEF5C796C7835BBAFD537E8D` in x64 builds.

Each loader exports the function names its host program expects, all leading to one routine, a ValleyRAT shape documented with `NvSmartMax64.dll` under `nvsmartmaxapp64.exe` [17]. For the Hithink program, `hxdaemonprocess.exe`, the loader copies the twelve function names of the software development kit (SDK) that `hdp.dll` provides. Three encrypted resources, `NVAP032V`, `NVAP064V` and `NVAP086V` (`ZH_CN`, `ZH_HK` and `ZH_TW` in x64 builds), hold two kernel drivers (section A3.6) and the watchdog script, the `.CMD` file that restarts the loader. They decrypt under one fixed keystream from a custom generator, which we recovered by known plaintext.

Every resource the kit adds is tagged Chinese Simplified, while eight of the eleven builds we have name Hindi, Odia or Kannada as their version language. We judge it likely that the ValleyRAT builder sets an Indian locale in that field. Confidence is low, because the judgment rests on the version field of eight builds alone.

A3.4 The configuration and its cipher

The configuration, the settings block inside each loader, decrypts with a key that every build carries in plain sight: its own group ID, reversed.

Each loader stores the configuration as one UTF-16LE hex string in `.data`. Decrypted, it is a list of fields separated by bars and colons, as in this configuration of C17 (Annex Table 5):

```
|1BF1E413B6E0E93047F$@2026-08-24#|A1:192.252.183[.]157|o1:7800|t1:1|S2:192.252.183[.]157|o2:7811|t2:1|p3:192.252.183[.]157|o3:9999|t3:0|dd:10|cl:30|fz:\xac\xc4\xcf\xc8|bb:08191020|bz:2026.08.19|jp:0|bh:0|ll:0|dl:0|sh:0|kl:0|bd:0|
```

Field	Meaning	Values across the builds analysed
group ID	19 hex characters at the head; reversed, the RC4 key	44 distinct IDs, one per build
`$@<date>#`	a date 0 to 7 days on or after `bz`	absent up to 2026-08-13; 2026-08-19 to 2026-09-23 after
`o1`, `o2`, `o3`	the ports of three channels, whose hosts `A1`, `S2` and `p3` are the same	7800, 7811, 9999 (`p3` empty in B5, B6 and the oswin[.]club build); 6088, 6099, 9999 for usdt888[.]club and oswin[.]club; 7880, 7881, 7881 in the TA4922 configuration that Proofpoint published [6]
`fz`	sub group tag	默认 ("default") on the August x86 builds except B5 (`mail`); `MMDD` dates from September; `VHD-0902` on the oswin[.]club build
`bb`	build stamp, `MMDDhhmm` at UTC+8, fixed per compile or builder session	`08031225` to `09230545`; `08100001`, `08170001`, `08200001`; `11171030` in the TA4922 configuration [6]
`bz`	build date	2026.08.03 to 2026.09.23; 2025.11.20 in the TA4922 configuration
`t1` to `t3`, `dd`, `cl`, `jp` to `bd`	channel types, reconnect delay (10 s), heartbeat (30 s), seven startup toggles	the same in every build; every toggle 0

Annex Table 5: The configuration fields and their values across the builds we analysed.

The `fz` value 默认 is stored in the Chinese character encoding GBK, with each character's two bytes swapped. We assess it likely that this value is the builder default, so most August builds were never given their own tag. Confidence is moderate, because every August x86 build except B5 carries the value, while the September builds carry typed `MMDD` dates. The `bb` field is a build stamp: B9's stamp `09220402` equals its PE time to the minute at UTC+8. The decrypted configuration string is also the loader's mutex, a named lock that stops a second copy from running.

The cipher takes four steps: the hex body is reversed and decoded, RC4 decrypts it with the reversed group ID, and the plaintext is reversed again. Our implementation reproduces the runtime configurations of B1 to B7 byte for byte. Proofpoint, in its report on the actor it tracks as TA4922, printed the grammar, called the ID an RC4 key and shared a decryption recipe for one configuration [6]. Beyond that, we write out the reversals, the exact key form and the storage forms.

The delivery archives leak the key: the ZIP of chain F, `20260902110114-0AFC3F174BAD.zip`, ends with the first twelve characters of the reversed group ID of F1, the build inside. We judge it almost certain that the suffix is the key prefix. Confidence is high, because all 16 names we can test match the key of their build. Two name forms carry the suffix: `<14 digit stamp>-<12 hex>.zip`, as in chain F, and `<14 digit stamp>.<12 hex>.zip`, as on the auk218[.]club packages (Annex Table 2). A third form, `ZIP-<14 digits>.<12 hex>.zip`, names `12f496cd`, a package that contacts usdt888[.]club (section A4.7).

A3.5 The backdoor core, its traffic and its persistence

When the loader connects, the C2 server answers with a stage of about 339 KB whose hash changes every session. The stage unpacks to the ValleyRAT Login Module core. Most of its commands are standard remote control. Other commands survey security products and stop the Qihoo 360 and Tencent security programs (360 and QQPC) through the Windows Restart Manager. They also clear the Application, Security and System event logs and store a new configuration under `HKCU\Console\IpDate`.

The core's traffic decrypts with a key that each session derives from a token in its message headers. Each frame starts with `[u32 length][u32 session token][00 00 00 00][CA 00]`, and the key is the ten bytes after the length, each plus 0x36, so only the four token bytes change between sessions. Check Point Research published `363636003797e4383a36` in August 2025 as the XOR key for the traffic between a ValleyRAT downloader and its C2 server [7]. In our builds, where the token changes with every connection, a key of that form fits one session only. Zscaler described single byte XOR 0x36 on shellcode that the C2 server delivers [2]. The per session key and the frame layout are our findings. The scheme decrypts 99.9997 per cent of the bytes in the six live sessions, the VMRay runs in which a C2 server answered.

We assess it likely that the key Check Point published was made the same way as ours, from a message header with 0x36 added to each byte. It follows either this scheme or a slightly different version of it. Confidence is moderate, because four of the five bytes that can be tested match, but the comparison rests on a single published key.

All byte values in this comparison are hexadecimal. Our key is made from the ten header bytes that follow the length field, with 0x36 added to each. Six of those ten header bytes are the same in every message, 00 00 00 00 CA 00, so six key bytes never change: 36 36 36 36 00 36. The 00 appears because 0xCA plus 0x36 is 0x100, one more than the largest value a byte can hold, so the byte rolls over to 00. The other four header bytes are the session token, a value that changes from one connection to the next, so the four key bytes made from it vary with the token.

The ten-byte key is XORed over the message again and again. If its bytes were A to J, the message would be encrypted with ABCDEFGHIJABCDEFGHIJ and so on. Written down from its sixth byte, as FGHIJABCDE, it is still the same key. Check Point wrote theirs down from a different starting byte than we do, so we rotated it before comparing. Their key as published reads 36 36 36 00 37 97 E4 38 3A 36. It has only one 00 byte. We moved its first five bytes to the end, which puts that 00 where our key always has its 00: the position made from CA. In the order the bytes appear in the header, the two keys compare like this:

- Header bytes T1 to T4, the four session token bytes: our key changes with the token; Check Point's key has 97 E4 38 3A.
- Header bytes 00 00 00 00: our key has 36 36 36 36; Check Point's key has 36 36 36 36.
- Header byte CA: our key has 00; Check Point's key has 00.
- Header byte 00 after CA: our key has 36; Check Point's key has 37.

The 00 matches because we used it to line the keys up, so it proves nothing. The four token positions prove nothing either, because a token can be any value. Read as a token, Check Point's 97 E4 38 3A, each minus 0x36, gives 61 AE 02 04. That leaves five fixed bytes as the real test. Four of them match: the bytes made from 00 00 00 00 are 36 in both keys. The last one does not: Check Point's key has 37 where ours has 36.

That last key byte comes from the header byte after CA. In our builds that header byte is 00, which gives 36. To give 37 it would have to be 01, because 37 minus 36 is 01. So if Check Point's key follows this scheme, either their sample uses a slightly different header with 01 in that position, or the published key contains an error.

Check Point presented a single key and said nothing about how it was built or whether it changed between connections. That fits our reading too. If their sample's token never changed, its key would never change either. It would then look like one fixed key, while still being built from the header in the same way.

In the twelve VMRay runs of kit loaders no C2 server sent tasking. In the six runs in which a server answered, the core registered, surveyed the host and waited.

The loader persists through a scheduled task named `NvContainer.NvapiMonitor.{GUID}`, a folder named like a script, `nvpluginnvapimonitor.nvx.vbe`, and a watchdog `.CMD` (Table E of the indicator file). The watchdog restarts the loader every 60 seconds. The loader stores the stage under `HKCU\Console\0` in the value `389126097FFFEF316D35ACD0610E5F31`, the same in all six live sessions. Malwarebytes [12] and CloudSEK [3] published other value names under `HKCU\Console\0` for other ValleyRAT sets. Nextron documented a Silver Fox scheduled task that runs an encoded VBE script in November 2025 [18]. The value name, the task name and the folder name are our findings.

A3.6 Two kernel drivers in the builds we decrypted

Two of the three encrypted resources, `NVAPO32V` and `NVAPO64V`, decrypt to x64 kernel drivers whose certificate tables end exactly at the resource size. We judge it very likely that they are the drivers the core is built to write as `TAOKERNELEX64_AV.SYS` and `TAOACCELERATOREX64_AV.SYS`, because the code beside them builds exactly two drop paths. Confidence is moderate, because this rests on the code: in the VMRay runs the core kept both drivers in its resources. Only bytes inside the certificate tables change between builds, so we assess it likely that the builder changes them to give each build's drivers new hashes. Confidence is moderate, because this rests on the files alone. Annex Table 6 names the drivers by their PE times.

The September builds (B7, B8, B9) carry encrypted resources of other names and sizes, whose content is outside this report. B7 and B9 name the device paths `\\.\xkpsm`, `\\.\ardrv` and `\\.\HWAudioX64` (Annex Table 6).

Item	What the files show
The 2018 driver (`NVAPO32V`, `ZH_CN`)	PE time 2018-01-03 07:15:40; 30,320 bytes, ending with its certificate table (Table D of the indicator file)
The 2023 driver (`NVAPO64V`, `ZH_HK`)	PE time 2023-02-27 20:51:07; 38,816 bytes, ending with its certificate table (Table D of the indicator file)
The watchdog template (`NVAPO86V`, `ZH_TW`)	`.cmd` text with Chinese comments; 1,388 bytes (x86), 1,494 bytes (x64); written in a VMRay run of B4
Drop paths	`%Temp%\TAOKERNELEX64_AV.SYS`, `%Temp%\TAOACCELERATOREX64_AV.SYS` (x86 core); `%LOCALAPPDATA%\Temp\TAOKERNELEX64_EV.SYS<d-h-m>`, `%LOCALAPPDATA%\Temp\TAOACCELERATOREX64_EV.SYS<d-h-m>` (x64)
Device names	`\\.\xkpsm`, `\\.\ardrv`, `\\.\HWAudioX64` (B7, B9); `\\.\BootRepair`, `\\.\Warsaw_PM` (B4, F1)
Privileges and other controls	`SeDebugPrivilege`, `SeLoadDriverPrivilege`, `SeTakeOwnershipPrivilege`, `SeIncreaseBasePriorityPrivilege`, `SeTcbPrivilege`; `RestrictRun` policy lockdown

Annex Table 6: The embedded drivers, drop paths and device names.

Loading a signed but vulnerable driver to gain kernel access, known as bring your own vulnerable driver (BYOVD), is documented for Silver Fox with `amsdk.sys`, `wsftprm.sys` and other drivers [7] [10]. In March 2026 Huntress reported a security tool killer, tied to no actor, that abuses a previously undocumented Huawei audio driver through `\\.\HWAudioX64` [8]. A Zenn write-up analysed it again [9]. Public BYOVD proof of concept tools are collected on GitHub [21]. In July 2026 Cato Networks reported the driver file `BootRepair.sys` as new for Silver Fox, without a device name [10] (section A6.3). The `TAO*` drop names, the resources `NVAPO32V` and `NVAPO64V`, the device names `\\.\xkpsm`, `\\.\ardrv`, `\\.\Warsaw_PM` and `\\.\BootRepair`, and the tie of `\\.\HWAudioX64` to this kit are our findings.

A3.7 The loader hides behind genuine signed programs from five companies

The loaders hide behind genuine programs signed by five companies, four of them Chinese and one Taiwanese. This reuse of signed vendor software is a core technique of the kit. The companies below are not part of the operation.

Every signature in the delivery chains verifies against an unmodified vendor program, and every loader we have is unsigned (Annex Table 7). The five signers are 广州宁静海信息科技有限公司 Guangzhou Ningjinghai Information Technology Co., Ltd., Hithink RoyalFlush, 杭州分叉智能科技有限公司 Hangzhou Fencha Intelligent Technology (ShadowBot), Tencent and ZEON Corporation.

We judge it very likely that the Guangzhou Ningjinghai signature on the 2026 package of chain B is a genuine 2022 vendor signature on a reused host. Confidence is moderate: three facts agree, but all three come from the one signed file. GlobalSign's timestamp authority dated the signature on this Alibaba arphasdk crash reporter, compiled 2021-07-16, to 2022-01-25, inside the certificate's validity, and a timestamp cannot be backdated. The signed file is an unmodified vendor program. No other file we have carries this certificate.

We also judge it very likely that the certificate played no other part in the 2026 packages. Confidence is moderate, because it expired in November 2022 and every loader we have is unsigned (section A3.7). Guangzhou Ningjinghai is a real company and runs the biubiu game accelerator [22] [23]. No public source ties the company to malware. The Hithink certificate expired on 2026-08-02, but the signature's timestamp keeps the signature valid.

Host file (SHA-256 prefix)	Signer	Certificate serial	Validity (UTC)	Signed at (UTC)	Host built	Used with
`arphaCrashReport.exe` (`b2ee510d`)	Guangzhou Ningjinghai, EV	`18C0F9306B46487D00384971`	2021-11-02 to 2022-11-03	2022-01-25 17:52:55	2021-07-16	B9
`hxdaemonprocess.exe` (`53a4e54f`)	Hithink RoyalFlush, EV	`01FEBC8A7743533E070A2A480BF510B5`	2023-08-01 to 2026-08-02	2024-11-18 12:46:46	2024-11-18	B7, B4, C17
`hxdaemonprocess.exe` (`233a7de2`)	Hithink RoyalFlush, same certificate	`01FEBC8A7743533E070A2A480BF510B5`	2023-08-01 to 2026-08-02	2025-02-06	none observed	C15
`debugger.host.exe` (`259ce06b`)	Hangzhou Fencha (ShadowBot), EV	`0E58A7A89AA85656786458595ACEA982`	2024-04-15 to 2027-04-17	2025-06-10 12:46:36	2024-03-07	F2
`WeChatAppEx.exe` (`0fdb6303`)	Tencent	`0EC3880864ADEB96CAFC6AABAFDA1F94`	2025-10-14 to 2028-10-19	2026-08-21 08:20:48	2026-03-02	F1
`ConvertToPDF.exe` (`b869fbdd`)	ZEON Corporation	`085B3F83136C2B622045218988C6BACD`	none observed	2025-09-22	none observed	auk218[.]club loaders
`ConvertToPDF.exe` (`21cf7a17`)	ZEON Corporation	`042C5C97FAEACFEC7115FA1C9229DA9B`	none observed	2023-11-01	none observed	auk218[.]club loaders
`keytool.exe` (`a5fad3d7`)	JetBrains	`083EA13884BDFFCE8E5D9D5CAD2EFBDE`	not listed	2026-03-02 11:15:33	not listed	Padded x64 loaders
`rmiregistry.exe` (`233086e7`)	JetBrains	`083EA13884BDFFCE8E5D9D5CAD2EFBDE`	not listed	2026-03-02 11:14:46	not listed	Padded x64 loaders
`platform_experience_helper.exe` (`1fae7d65`)	Google	`0B50CF246B263EFD85A729315158F3FF`	not listed	2026-06-06 07:12:28	not listed	Padded x64 loaders
GoodSync `LogView.exe` (`0a1fd68a`)	Siber Systems	`84D5733C4181BE468CD04DB03F507188`	not listed	2026-03-07 01:13:35	not listed	Padded x64 loaders
`BugSplatHD.EXE` (`1ffc8bde`)	BugSplat	`F8495E224EFA55D4`	not listed	2020-08-05 14:27:24	not listed	Padded x64 loaders
`LINK.EXE` (`e388eb34`)	Microsoft	`33000004855E99EC0E592FCDD7000000000485`	not listed	not listed	not listed	Padded x64 loaders

Annex Table 7: Signed hosts and their signers.

Notes to Annex Table 7:

- EV means extended validation. Table D of the indicator file repeats the certificate serials.
- The last six rows are the hosts of the padded x64 loaders, another loader family on nearby delivery domains (section A4.7). With them the table lists all ten signers of section A3.7.
- The padded x64 hosts carry genuine vendor signatures; their validity periods and build times are not listed, because the hosts are another family's.

A Sigma rule that Nextron publishes on Valhalla already covers side-loading of `ArphaDump64.DLL` [11]. Our B9 loader travels as `ARPHADUMP.Dll` (Table 4). Ours are the Hithink RoyalFlush program `hxdaemonprocess.exe` as host for `hdp.dll` and the Alibaba `arphaCrashReport.exe` as a host. Ours is also the finding that the Guangzhou Ningjinghai signature on `arphaCrashReport.exe` is very likely a genuine 2022 vendor signature on a reused program (sections 3.1 and A3.7). Three facts agree: a 2022-01-25 timestamp inside the certificate's validity, an unmodified vendor program, and no other file we have with this certificate. Confidence is moderate, because all three come from the one signed file.

We assess it very likely that all ten signer identities on the host programs, the signed programs that side-load the loaders, are genuine. The ten are Guangzhou Ningjinghai, ZEON Corporation, Hithink RoyalFlush, Hangzhou Fencha (ShadowBot), Tencent, JetBrains, Google, Siber Systems, BugSplat and Microsoft. Confidence is high for nine of them, because each signature verifies against the content of its own unmodified vendor file (Annex Table 7). It is moderate for Guangzhou Ningjinghai, because all of its evidence comes from one signed file (section A3.7). A key stolen from a vendor would leave the same signature, which keeps the likelihood below almost certain. The kit's hosts come from Chinese and Taiwanese vendors. The hosts of the padded x64 loaders come from Western developer tools. The difference fits two loader suppliers. Files known by hash that call or carry the operation's C2 domains show eight further signer names in their metadata. They are certificates issued to legitimate companies and developers, among them large software vendors, whose signed software or certificates were reused or abused. A signer name in file metadata says nothing about the certificate owner's involvement. Guangzhou Ningjinghai is not among the eight.

A3.8 The U.S. Department of Homeland Security seal

Our twelve builds compiled from 2026-08-13 to 2026-08-19 carry the seal of the U.S. Department of Homeland Security (DHS) as their main icon. We assess it almost certain that the seal belongs to their Spanish cover application. Confidence is high, because the seal appears only in builds of that version and the code that runs never loads it. The seal is the main icon (`IDR_MAINFRAME`). It comes in ten sizes, the largest a 95,141 byte PNG (`37ff4738`, Table C of the indicator file). In B4 it is icon group 128, the first icon group, so tools that show a file's first icon, VMRay included, display it. The seal is the malware's own icon resource; its mention here implies no involvement or endorsement by DHS.

The seal follows the Spanish cover application whatever the C2 server: twelve builds from five compiles carry it, and no auk218[.]club loader or x64 build does. Of the 170 files with the seal as main icon on 2026-10-14, none was first seen before 2026-08-13. We analysed 47 of them in detail, and all 47 carry the Spanish cover application; none of 63 files with later icons carries the seal. We hold one more, B4, as a file. Of the other 122, 107 are further unwrapped builds first seen from 2026-08-13 to 2026-09-22, six are October wrapped copies, and nine are known to us only by hash. Table C of the indicator file lists a further 138 kit builds and carriers found by the seal or the Spanish cover application.

The last compile of the Chinese version is dated 2026-08-11 17:44:29 UTC. The first sighting of a seal file came at 2026-08-13 01:49:27 UTC. We judge it likely that the switch from the Chinese to the Spanish version came between these two times. Confidence is moderate, because an earlier seal build made for another builder user would also fit.

On the delivery paths we observed, the seal never reaches the screen. The loaders are libraries, which Windows Explorer draws with a generic icon, and the ISO of chain D showed the signed Hithink program with its own icon. Only the cover application's own code, which nothing calls, would load the seal. We assess it almost certain that the side-loading path never loads or draws the seal. Confidence is high, because the code that runs calls no icon routine, and the nine VMRay run logs of B1 to B6 record no icon load.

Every lure we found for these builds is a tax notice in English, Spanish or Portuguese. None of the lure pages or package names we recorded is themed on Homeland Security. Annex Table 8 grades five explanations for the seal in the cover application.

Explanation	Main evidence	Grade
A leftover of a US-themed use of the cover application	No US-themed file, string or lure	Unlikely; low
A deliberate official-looking icon for victims	Libraries never show it, and it left with the Spanish version on 2026-08-24	Very unlikely; moderate
Part of a resource pack the kit author ships	Kept in the October copies, but each later version has its own icon	Roughly even chance; low
A decoy for a later DHS-themed lure	B4 travelled as a tax document, and the seal was never rendered	Very unlikely (a); low
A test or placeholder	An unedited cover, but a ten size icon kept for two months	Roughly even chance; low

Annex Table 8: Five explanations for the seal.

Notes to Annex Table 8:

- They overlap, so their likelihoods do not add up to 100 per cent.
- (a) For the builds analysed; unlikely for the Spanish version as a whole.

A4.1 The C2 servers

The 44 builds call eight C2 servers, seven domains and one IP address, and each build repeats one server in every connection channel of its configuration (Table 5). Every domain was registered at 22net between about six days and five hours before the earliest compile of a build that calls it. Four of the operation's domains were created from 2026-08-09 to 2026-08-19. fddlbh2[.]club followed on 2026-09-01 at 12:15 UTC, about five and a half hours before its first x64 compile at 17:40 UTC that day. All of them use 22net's default name servers, ns1[.]22[.]cn and ns2[.]22[.]cn, which every 22net customer shares. Dates alone never connect two domains.

Two port profiles split the domains. A port profile is a builder setting, so it says nothing about who runs a server. No two of the operation's domains shared an IP address (Annex Table 10). taku788[.]club moved through seven IP addresses in 202.61.85[.]0/24, a range of the network COMING-HK. Four domains, three of the operation's and fddlbh2[.]club, trace to one registrant name, KANGYINGJIE, and share none of their IP addresses.

Most C2 server IP addresses are small rented servers with other customers. Three IP addresses need a note:

- 192.252.183[.]157, the C2 server IP address of B4, C15 and C17: in 2026 it hosted fddlbh2[.]club and four hosts of spbo[.]cc, a domain registered in 2019. The four hosts are spbo[.]cc, www[.]spbo[.]cc, bf[.]spbo[.]cc and live[.]spbo[.]cc. We judge it likely that spbo[.]cc belongs to another customer of the rented server. Confidence is low, because the only evidence is the hosting history of the IP address, whose spbo[.]cc hosts predate the operation.

Three other malware files contacted 43.224.224[.]81 on 2026-09-23, the day after fuoe333[.]club used that IP address. Each is listed with the antivirus family name it carries:

- `3c6f5a7b`: trojan.lazy
- `acba1b70`: trojan.silverfox

- `d99f5efc`: trojan.abtrojan

We judge it likely that they belong to other customers of the IP address. Confidence is low, because the only evidence is that the IP address is a small rented server with other customers.

usdt888[.]club was still in use in October and very likely served as the C2 server of the October re-packed copies (section A3.2). Confidence is moderate, because their configurations sit inside protector wrapping, so the judgment rests on the contact logs of 17 copies.

C2 server	Created (UTC)	Expires	Registrant organisation	Port profile	Builds (n)
taku788[.]club	2026-08-14 06:08	2027-08-14	KANGYINGJIE	1	10
fuoe333[.]club	2026-08-09	2027-08-09	KANGYINGJIE	1	8
moik77a[.]club	2026-08-19	2027-08-19	KANGYINGJIE	1	2
usdt888[.]club	2026-08-18	2027-08-18	ZHENGJUNHUA	2	2
192.252.183[.]157	n/a (IP address)	n/a	n/a	1	3
fddlbh2[.]club	2026-09-01 12:15	2027-09-01	KANGYINGJIE (hashed value in our records; printed in one stored record, section A5.4)	1	2
auk218[.]club	2026-07-27	2027-07-27	Redacted; KANGYINGJIE in one listing	1	16
oswin[.]club	2026-08-31	2027-08-31	Redacted; ZHENGJUNHUA in two records	2	1

Annex Table 9: The C2 servers that the 44 builds call.

Notes to Annex Table 9:

- Port profile 1 is ports 7800, 7811 and 9999; profile 2 is 6088, 6099 and 9999 with an empty third host.
- taku788[.]club: B1, B7, B8, B9 and six x64 builds, grouped by compile:
  - `92a70bc7` and `b1159a9d`: compile of 2026-09-01
  - `2df75ca7`, `323f6232`, `8bd0b996` and `a594eb76`: compile of 2026-09-03
- fuoe333[.]club: B3, the four early builds with the DHS seal and three x64 builds, grouped by compile:
  - `0b7ad10b`, `754c5233` and `3e4204df`: early builds with the DHS seal, 2026-08-13
  - `c1aff663`: early build with the DHS seal, 2026-08-16
  - `31cb9374`, `7bcede88` and `9f6daad5`: x64 builds, 2026-09-03
- moik77a[.]club: B2 and `b8f5ae18` (2026-09-01).
- usdt888[.]club: B5 and B6; 17 of the October re-packed copies also contacted it.
- 192.252.183[.]157: B4, C15 and C17.
- fddlbh2[.]club: F1 `faac737c` (2026-09-01) and F2 `2960996c` (2026-09-03).
- auk218[.]club: the 16 auk218[.]club loaders (section 4.1).
- oswin[.]club: `29c3b121` (2026-09-01).
- auk218[.]club and oswin[.]club are outside the operation, and fddlbh2[.]club sits just outside it, tied to it by a shared server and download link (section 4.3).
- Table C of the indicator file gives every hash in full.

C2 server	IP address	Observed (2026)	Note
taku788[.]club	202.61.85[.]34	08-16	atyv788[.]club moved here on 08-14 (section A5.4)
taku788[.]club	202.61.85[.]172	08-18	none
taku788[.]club	202.61.85[.]104	08-21	B1 contacted it
taku788[.]club	202.61.85[.]180	08-31	none
taku788[.]club	202.61.85[.]216	09-10	none
taku788[.]club	202.61.85[.]153	09-15	none
taku788[.]club	202.61.85[.]50	09-23	The tax dropper tried to post here
fuoe333[.]club	43.224.224[.]66	08-11	none
fuoe333[.]club	43.224.224[.]72	09-14	none
fuoe333[.]club	43.224.224[.]81	09-22	none

C2 server	IP address	Observed (2026)	Note
moik77a[.]club	186.240.201[.]63	from 08-19	A mobile user IP address
moik77a[.]club	137.220.152[.]244	from 09-17	none
usdt888[.]club	64.90.19[.]141	08-18 to 08-20	B5 contacted it
usdt888[.]club	103.42.30[.]245	08-21 to 08-26	B6 contacted it; seen again 09-22
usdt888[.]club	45.203.213[.]231	08-24	none
usdt888[.]club	122.10.117[.]3	08-24	The remote management server (section A4.8)
usdt888[.]club	156.245.245[.]235	09-04	oswin[.]club here on 09-02
usdt888[.]club	156.245.245[.]222	10-08	October copies contacted it to 10-14
fddlbh2[.]club	192.252.183[.]157	from 09-01	Seen 09-03
fddlbh2[.]club	154.36.188[.]18	www 09-15	The domain itself 09-26
auk218[.]club	118.107.0[.]196	07-31 to 10-14	none
oswin[.]club	156.245.245[.]235	09-02	none
oswin[.]club	103.42.30[.]140	10-14	Shared with winapp[.]work

Annex Table 10: Dated IP addresses of the C2 domains.

Notes to Annex Table 10:

- The 09-01 date for fddlbh2[.]club assumes that the zone serial records the time of the last edit (section A2).

If 22net zone serials record the time of the last edit, the four domains under the registrant name KANGYINGJIE were last edited between 2026-09-13 and 2026-09-22. That fits one party maintaining them, but a date alone connects nothing.

The notes on the other two are:

- 43.224.224[.]66, the first IP address of fuoe333[.]club: it carried 106 names from bulk registrations of 2025 and February 2026, the last of them dated 2026-03-22. After that date the only name printed on it is fuoe333[.]club, from 2026-08-11.
- 186.240.201[.]63, the first IP address of moik77a[.]club: it is a Brazilian mobile user IP address according to its reverse DNS record of 2026-09-09. Blocking this IP address after August therefore risks hitting an unrelated user.

Of the 44 builds, every one whose delivery host is on record came from the delivery host kaiwyrey[.]eu[.]cc (section 4.2). The other builds are known by their carriers. Two September builds (B7, B9) came in VHDX disk images. ISO disk images named `Notice from Tax Departmen.IMG` carried further builds seen with fuoe333[.]club, among them `67e1ac14` (section A6.3). The October copies came in ZIP and 7-Zip archives. One more package tied to an operation C2 server, `12f496cd`, came from cao[.]tedboscomwe[.]com on 2026-08-27 and contacts usdt888[.]club (section A4.7).

A4.2 One delivery host, three C2 servers in turn

One delivery host, kaiwyrey[.]eu[.]cc, served loaders for three C2 servers in turn. We assess it very likely that one account of its file-sharing application shipped them all. Confidence is moderate. When two of the delivery host's four main download links were checked within three minutes of each other, both served the same file in 45 of 46 cases, which points to one account, but one account run by a delivery service for several customers would leave the same trace. This judgment therefore does not settle whether one customer used the delivery host (sections 4.3 and 5.2).

kaiwyrey[.]eu[.]cc was created at Gname on 2026-06-29 at 19:08:33 UTC as registry ID 134544, and its registration record redacts every contact field. The domain runs a file-sharing web application whose links take the form hxxps://kaiwyrey[.]eu[.]cc/d/<12 hex>, where the 12 character code is the download link code. From 2026-08-03 four main download links, `6f025f85e3c0`, `70878efbc582`, `bdc9637e70c2` and `ac516096c285`, nearly always served the same files as one another. When two of them were checked within three minutes of each other, both returned the same file in 45 of 46 cases, though the file itself changed over time, sometimes within minutes, and from 2026-08-20 to 2026-08-29 the links alternated between the C17 and B4 packages. We therefore treat the four links as one. Table B of the indicator file lists all 48 download links on record.

The C2 servers followed one another without overlap: auk218[.]club from 2026-08-03, 192.252.183[.]157 from 2026-08-17 and fddlbh2[.]club from 2026-09-02 (Figure 6, Annex Table 11).

On 2026-09-02 the download link `6f025f85e3c0`, which had served the ZIP of a build for 192.252.183[.]157 (B4), served the ZIP of a build for fddlbh2[.]club (F1). The builds for 192.252.183[.]157 began before B4. C15, which calls the same C2 server, was compiled on 2026-08-16 and served on 2026-08-17, two days before B4's compile of 2026-08-19.

Annex Table 12 dates the delivery host's last weeks. The main links went dark on 2026-09-04, new links served the x64 files, and the server stopped answering after 2026-09-26.

Of 33 packing stamps on the delivery host's packages, read at UTC+8, 27 fall on a weekday between 10:00 and 17:00. Of the 33, 32 fall on a weekday. We judge it likely that whoever packed the packages works a weekday office schedule in a UTC+8 zone. Confidence is moderate, because the schedule rests on 33 stamps from one delivery host.

Period (2026)	What it served	Analysed (n)	Seen (n)	Example name
07-03 to 07-22	Other files, 52 KB to 5.5 MB (a)	0	6	No name on record
07-28 to 07-31	Packages of 3.84 to 4.67 MB (b)	0	8	`20260729104357.zip`
08-03 to 08-13	auk218[.]club loaders (c)	17	31	`Tax PenaltyN0.20260806.IMG`
08-17 to 08-31	192.252.183[.]157: C15, B4, C17 (d)	3	5	`Tax-Number852694.zip`
09-02 to 09-06	fddlbh2[.]club: F1, F2 (e)	2	3	`20260902110114-0AFC3F174BAD.zip`
09-08 to 09-15	One 7.5 MB x64 file, `28958b5d`	0	1	No name on record

Annex Table 11: What the delivery host kaiwyrey[.]eu[.]cc served, by period.

Notes to Annex Table 11:

- (a) Four ValleyRAT or generic x64 files and two files that no detection flagged. Dates are month and day in 2026:
  - `c839ae15` (07-03), `e79905ac` (07-10), `1290f83e` (07-15) and `4a4d17d3` (07-20): ValleyRAT or generic x64
  - `84061a94` (07-04, also served by isudcnzy[.]eu[.]cc) and `35a2d6c7` (07-22): no detection
- (b) Eight files, listed below. A SendGrid link of 2026-07-29 led to the download link `b9059861159e` and delivered `20260729104357.zip`.
  - `6b97957b`
  - `aa1b45d0`
  - `0d481d10`
  - `6042e01e`
  - `5fada679`
  - `8dfe4596`
  - `b856a8d4`
  - `45695977`
- (c) The 17 packages that hold the 16 auk218[.]club loaders and 14 further packages; one more package followed on 08-14.
  - Other names from 08-03: `<14 digit stamp>.<12 hex>.zip` and images `Vat.N0.`, `VAT-N0.`, `VATNo.`, `No.`, `T.No.`
- (d) Three packages we analysed and two more we saw. Dates are month and day in 2026, and a link is the download link code:
  - `6620e9ad`: package of C15, analysed
  - `b292de38`: package of B4, analysed
  - `feb58c7b`: package of C17, analysed
  - `2c16aed0`: seen, 08-18, link `a63179e2fe1a`
  - `4f085034`: seen, `Tax-Number852691.zip`, 08-18
  - Other names from 08-17: `Tax-Number852690.zip`, `Tax-Number852693.zip` and images `INV-No.`, `TI.Number-`, `INT-Number.`
- (e) The packages and file names of this period. Dates are month and day in 2026, and a link is the download link code. Table C of the indicator file lists every file by hash.
  - `da36a96f`: package of F1, link `6f025f85e3c0`
  - `d4a8b9d3`: package of F2, which came as `ITD-2002150409.img`, link `ab8be35731a0`, 09-04
  - `6dc6af47`: the same link `ab8be35731a0`, 09-04 to 09-06

Date (2026, UTC)	Event
07-29	SendGrid account `u53630135` links to the delivery host
09-04 01:20	Main links answer 404 from this time
09-04, ten hours later	The new link `ab8be35731a0` serves F2
09-08 to 09-15	The link `52f5a2c0c2e1` serves `28958b5d`
09-17 and 09-18	The link `0cd07b91456a` answers with the application's 403 page, titled 文件下载 ("file download")
after 09-26	The server at 103.23.172[.]118 gives no answer

Annex Table 12: The last weeks of the delivery host.

A4.3 Who controlled fddlbh2[.]club

We assess it likely that the operator of the server at 192.252.183[.]157 also controls fddlbh2[.]club. Confidence is low for two reasons. First, the connection holds only if one customer used the delivery host. Second, the only source that places the delivery host's other C2 server, auk218[.]club, under KANGYINGJIE, the registrant name of fddlbh2[.]club, is one listing outside our own records (section 4.1). Here the operator of 192.252.183[.]157 means whoever controls that IP address and the three builds that call it (B4, C15 and C17).

Thirteen and a half hours after the last download of B4's package, fddlbh2[.]club was registered. Within two days a build that calls fddlbh2[.]club was served from B4's download link (Annex Table 13).

Time (UTC unless marked)	Event
2026-08-31 22:40	B4's ZIP last seen served
2026-09-01 12:15	fddlbh2[.]club registered under KANGYINGJIE (hashed value in our records; printed in one stored record of 2026-09-06)
2026-09-01 12:30	fddlbh2[.]club points at 192.252.183[.]157 (zone serial)
2026-09-02 (10:50 at UTC+8)	Build stamp of all five x64 builds of the 2026-09-01 compile
2026-09-02 03:01	F1 packed, about 15 hours after the registration
2026-09-02 evening	F1 served from B4's download link
2026-09-03	fddlbh2[.]club first seen on 192.252.183[.]157
2026-09-04	F2 served

Annex Table 13: From B4's last download to F2.

Notes to Annex Table 13:

- The 12:30 UTC entry assumes that a zone serial records the time of the last edit.

Two independent shared values from different suppliers connect fddlbh2[.]club to the build for 192.252.183[.]157 (B4) in one period: the IP address and the delivery host. Under our grading rule that is a strong connection, and it applies only if the delivery host belongs to one customer.

The main alternative is a service that hosts C2 servers on 192.252.183[.]157 and runs the delivery host for several customers. That service fits the IP address and the delivery host, but it explains auk218[.]club less well. One listing of 22net registrations outside our own records places auk218[.]club, the delivery host's earlier C2 server, under KANGYINGJIE, so the delivery host's C2 servers likely share one registrant (section 4.1). From 2026-08-17 to 2026-08-31 every package we read from the delivery host (three of the five seen) calls 192.252.183[.]157. A second alternative, another user of the public builder, explains the evidence less well, because that buyer would have had to pick 192.252.183[.]157 and the delivery host within days. The eleven other builds of the x64 compiles of 2026-09-01 and 2026-09-03, the compiles that also produced F1 and F2, all call other servers (Annex Table 9).

fddlbh2[.]club's later IP address, 154.36.188[.]18, had other customers from 2026-04-10, among them keep-cos[.]yanshi-eyucode[.]biz with its api, pc, demo and sq hosts. We judge it likely that the IP address carried other customers' traffic rather than this operator's. Confidence is low, because the hosting history of the IP address is the only evidence.

F1, the first fddlbh2[.]club build, carries a build stamp, a time at UTC+8 written into its configuration. That stamp falls ten minutes before F1's disk image was named and eleven minutes before F1 was packed at 03:01 UTC. If the build stamp records the builder session, that build was configured and packed in one sitting. Timing alone connects nothing, but the sequence from B4's last download to F1 leaves another customer only two days to take over both the IP address and the delivery host. By 2026-09-15 fddlbh2[.]club had been repointed: its www host was on 154.36.188[.]18 that day and the domain itself on 2026-09-26.

A4.4 auk218[.]club, the earlier C2 server on the same delivery host

auk218[.]club very likely stayed on one IP address, 118.107.0[.]196, throughout the period its 16 loaders were served. Confidence is moderate, because both observations, on 2026-07-31 and 2026-10-14, carry the zone serial set on the creation day. The domain was created at 22net on 2026-07-27. Our own registration records of auk218[.]club are redacted and print the province BEIJINGSHI, which 22net prints on redacted records too. One listing of 22net registrations outside our own records places auk218[.]club under the registrant name KANGYINGJIE, with the same creation day.

auk218[.]club shares two independent values with the KANGYINGJIE C2 domains in one period. The first is the delivery host, which served auk218[.]club's loaders from 2026-08-03, the builds for 192.252.183[.]157 from 2026-08-17 and those for fddlbh2[.]club from 2026-09-02. The second is KANGYINGJIE, which is also the registrant name of taku788[.]club, fuoe333[.]club, moik77a[.]club and fddlbh2[.]club, created from 2026-08-09 to 2026-09-01. Under our grading rule, that is a strong connection. We assess it likely that the operator of the KANGYINGJIE C2 domains also controls auk218[.]club. We therefore judge it likely that one operator, not a service for several customers, runs the KANGYINGJIE C2 domains and the delivery host's account. Confidence in both is low, because the registrant name rests on that single listing, which prints only a name that two registrant entries use. auk218[.]club's IP address appears nowhere else in our evidence. A public DcRAT report names the neighbouring IP address 118.107.0[.]197 [24], a fact about the IP address range only. A second record that prints the name

KANGYINGJIE or its hashed value `ab376f4f34801a68` would raise confidence. The configuration of `67e1ac14`, a build seen with fuoe333[.]club, would show whether one compile carried auk218[.]club and fuoe333[.]club, but that would remain a toolkit fact (section A6.3).

The 16 loaders were compiled from 2026-08-02 to 2026-08-11 in the Chinese version of the cover application, the harmless Windows program each loader is built on. They call auk218[.]club in every channel. Table C of the indicator file lists them with their 17 packages. They side-load as `pdfCoRe8.dll` beside a ZEON Corporation `ConvertToPDF.exe`, a program and library pair that also appears in public reporting (section A6.3).

A4.5 The delivery IP address range and its eu.cc names

The delivery host sat in the IP address range 103.23.172[.]0/24. That range also hosted Indian tax lure pages and, in our DNS records, phishing hosts that Sekoia lists as Silver Fox [4]. Sekoia prints no IP address in this range, so placing those hosts here is our own observation. Under the rule of section A2 the range itself connects nothing to the operation's C2 domains (section A4.10). Gname sells eu.cc names under a second-level zone that it states is not an ICANN-approved top-level domain [25]. The EUCC registry redacts every registration record. From July 2025 to October 2026 the range hosted at least 1,092 names on 131 IP addresses (our DNS records for the range, Figure 8).

We judge it very likely that one buyer or platform account registered the 28 batch eu.cc names (Annex Table 16). Confidence is moderate, because the names came in runs of registry IDs and share IP addresses and certificate orders. The 28 names were created from 2026-05-11 to 2026-08-06 in six runs of registry IDs, one of them of ec.cc names and one that skips 109456. Twenty of them, kaiwyrey[.]eu[.]cc included, sit on 103.23.172[.]118, where they make up 20 of its 23 names, and eight sit on 103.23.172[.]117. kaiwyrey[.]eu[.]cc sat on 103.23.172[.]117 on 2026-06-30 and 2026-07-01 before it moved to 103.23.172[.]118. Sixteen of the 19 other batch names on 103.23.172[.]118 were seen there while kaiwyrey[.]eu[.]cc was in use. The other three were last seen there on these dates:

- lzsifuiseurtt[.]eu[.]cc: 2026-05-29
- ncstsruks[.]eu[.]cc: 2026-06-21
- ddisuyer[.]eu[.]cc: 2026-06-21

We also judge it very likely that hsawtse[.]eu[.]cc, laiwybstw[.]eu[.]cc and rcyawday[.]eu[.]cc were hosted under the same server account as kaiwyrey[.]eu[.]cc. Confidence is moderate. A certificate order of 2026-06-30 covers hsawtse[.]eu[.]cc and kaiwyrey[.]eu[.]cc, and one of 2026-07-21 covers kaiwyrey[.]eu[.]cc, laiwybstw[.]eu[.]cc and rcyawday[.]eu[.]cc. A certificate validated over HTTP, where the issuer checks a file on the web server, binds its names to the server account at the shared IP address, not to one owner. The six payloads we analysed from the other batch names are padded x64 loaders (section A4.7), a family distinct from the HDP loader kit, the toolkit behind all 44 loaders.

Our DNS records first place eleven names on Sekoia's list of Silver Fox phishing websites [4] on 103.23.172[.]230 between 2026-01-09 and 2026-06-13, before the operation's dates. They are:

- ksudeu[.]nanguanglu[.]com
- fghs[.]shlowcarbon[.]com
- swy[.]juanseguros[.]com, with its parent domain juanseguros[.]com
- xueshirencai[.]com
- yigushengjin[.]com
- morecoworking[.]com
- mohaazon[.]com
- host-hunter[.]com
- primetechstocks[.]com
- udste[.]xidyuyedg[.]qpon
- isyraw[.]quidoaehse[.]icu: a host under quidoaehse[.]icu, a domain of 574849-1923 (section 5.2)

Two .qpon names on 103.23.172[.]230, udste[.]xidyuyedg[.]qpon and dyste[.]usdiuasrcvb[.]qpon, print one other Gname handle, C1461784974-CNIC of Shanghai, under parent domains created on 2025-09-10. We assess it likely that one customer controls both. Confidence is low, because the judgment rests on one handle, one creation day and one IP address. These names share only an IP address range with the delivery host, so they are dated context and never a connection.

Apart from the groups in Annex Table 14 they are:

- App download hosts such as app1, app2, oss, dw1 and dw2 under yunshui2025dw[.]store
- 235 numeric names of 2025 on 103.23.172[.]9
- Trading app hosts:
    - mt98[.]pro
    - mt1[.]pro
    - mt28[.]pro
    - cp28[.]pro

    - pionex[.]pro
- Server, proxy and panel customers

None of them shares a value with the operation.

IP address	Names (n)	Registered by	Role	Relation to the builds
103.23.172[.]117	165	Batch eu.cc names; 574849-1923	kaiwyrey[.]eu[.]cc's first IP address; June lure pages	Service that delivered the builds; delivery host account is the C2 server operator's: likely, low (section A5.7)
103.23.172[.]118	23	Batch eu.cc names; 574849-1923	kaiwyrey[.]eu[.]cc from 2026-07-01; the uploads	Service that delivered the builds; delivery host account is the C2 server operator's: likely, low (section A5.7)
103.23.172[.]15	64 to 66	574849-1923	Indian tax lure pages from mid July	Lure page hosts of 574849-1923; the operator's own account: roughly even chance, low (section 5.2)
103.23.172[.]230	151	Single eu.cc names; 574849-1923	Phishing hosts; one object of the same file-sharing application as the delivery host	Hosts of 574849-1923 and of other customers; no value shared with the builds
103.23.172[.]25	45	Single eu.cc names; 574849-1923	Three hosts named after the Thai government	Hosts of 574849-1923 and of other customers; no value shared with the builds
Seven other IP addresses	20	Other hosting customers	They share only a TLS fingerprint with the range	Unrelated

Annex Table 14: The delivery IP address range 103.23.172[.]0/24.

Notes to Annex Table 14:

- Batch eu.cc names are the 28 names of Annex Table 16, two of them under ec.cc.
- Single eu.cc names are the 107 eu.cc names registered one at a time from 2026-03-05 to 2026-04-03. Table B of the indicator file lists them all.
- 574849-1923 is a registrar account (a customer number) at Gname.
- Annex Table 15 lists the names behind each count.

IP address	Group	Names (n)	The names
103.23.172[.]117	Batch eu.cc names	8	hsawtse[.]eu[.]cc, kksiaueted[.]ec[.]cc, psiawute[.]eu[.]cc, qaywtfse[.]eu[.]cc, suawytde[.]eu[.]cc, vcxetknsbe[.]ec[.]cc, xciwuerse[.]eu[.]cc, zxysevre[.]eu[.]cc
103.23.172[.]117	Domains of 574849-1923	156	140 .live and .love names and 16 later .love names (Table B of the indicator file)
103.23.172[.]117	Another hosting customer	1	cy[.]mnss88[.]uk (2026-03-27)
103.23.172[.]118	Delivery host	1	kaiwyrey[.]eu[.]cc
103.23.172[.]118	Batch eu.cc names	19	Annex Table 16
103.23.172[.]118	Domains of 574849-1923	2	maoasiye[.]live, tdrw[.]bvbxdse[.]live
103.23.172[.]118	Japanese e-Tax lookalike	1	e-tzxarw[.]jp
103.23.172[.]15	Domains of 574849-1923	61	17 of the 18 lure page domains of July and August (zixhasda[.]xin has no IP address on record), csdfsera[.]live and the rest in Table B of the indicator file
103.23.172[.]15	Japanese e-Tax lookalike	1	e-tzsgzxyu[.]jp (2026-09-17 to 2026-10-14)
103.23.172[.]15	Older hosting names	3	hk1[.]jks[.]im, hknf[.]jks[.]im, sg[.]80422983[.]xyz (2024 and 2025)
103.23.172[.]230	Single eu.cc names	90	Table B of the indicator file
103.23.172[.]230	Domains of 574849-1923	11	httpiaw[.]icu, httplai[.]icu, httpsuw[.]cyou, ifuaytes[.]icu, kiafewoey[.]icu, quidoaehse[.]icu, suiyerjser[.]cyou, tasykdwa[.]icu, tsadya[.]icu, uydsecbjyge[.]cyou, ysieiuhaw[.]icu
103.23.172[.]230	Hosts under those domains	7	dyrys[.]tasykdwa[.]icu, fddrdh[.]ifuaytes[.]icu, isyraw[.]quidoaehse[.]icu, sueysu[.]ysieiuhaw[.]icu, uetrsd[.]suiyerjser[.]cyou, usetr[.]uydsecbjyge[.]cyou, yswhg[.]kiafewoey[.]icu
103.23.172[.]230	Hosts under the Gname contact handle C1461784974-CNIC	2	Two .qpon hosts
103.23.172[.]230	Other hosting customers	48	Among them the Sekoia-listed names of section A4.5 [4]
103.23.172[.]25	Single eu.cc names	17	Table B of the indicator file
103.23.172[.]25	Domains of 574849-1923	11	bvdaccs[.]cyou, fdigaifev[.]icu, fysiyr[.]icu, gothds[.]cyou, gothuy[.]icu, iauechte[.]cyou, kfuyisulnry[.]icu, kzifyakyue[.]cyou, sidigara[.]icu, xzdyattte[.]icu, zjkyewe[.]icu
103.23.172[.]25	Hosts under those domains	8	fghs[.]kzifyakyue[.]cyou, ghsyse[.]xzdyattte[.]icu, gov[.]bvdaccs[.]cyou, hsy[.]iauechte[.]cyou, iawu[.]sidigara[.]icu, siuf[.]kfuyisulnry[.]icu, thaigov[.]gothds[.]cyou, www[.]thaigov[.]go[.]th[.]gothuy[.]icu
103.23.172[.]25	Other hosting customers	17	Names not tied to the operation
103.23.172[.]27, [.]61, [.]97 and [.]109	Other hosting customers	20	Hosts under maxheap[.]cn and 1950[.]app, among others

IP address	Group	Names (n)	The names
103.23.172[.]3, [.]82 and [.]121	No name in the DNS records	0	None

Annex Table 15: The names behind each count of Annex Table 14.

Notes to Annex Table 15:

- Counts per IP address follow Annex Table 14, where hosts under a domain count with their domain.
- kaiwyrey[.]eu[.]cc sat on 103.23.172[.]117 on 2026-06-30 and had moved to 103.23.172[.]118 by 2026-07-01.
- On 103.23.172[.]230, vbaesta[.]live carried one file of the same file-sharing application as the delivery host (2026-09-08).
- The 103.23.172[.]230 names date from 2025-09-04 to 2026-10-09.

Name	Registry ID	Created (UTC)	IP address	Role
fuerubuiaie[.]eu[.]cc	109453	2026-05-11 11:29:41	103.23.172[.]118	Served the padded x64 loaders; linked from 10 June lure pages
idutyarwse[.]eu[.]cc	109454	2026-05-11 11:29:41	103.23.172[.]118	Served the padded x64 loaders; linked from 2 June lure pages
lzsifuiseurtt[.]eu[.]cc	109455	2026-05-11 11:29:41	103.23.172[.]118	Linked from 7 June lure pages
pzidiauwytsd[.]eu[.]cc	109457	2026-05-11 11:29:45	103.23.172[.]118	Linked from 8 June lure pages
xzsdiiaeugs[.]eu[.]cc	109458	2026-05-11 11:29:45	103.23.172[.]118	Served the padded x64 loaders; linked from 11 June lure pages
oaosifytaw[.]eu[.]cc	128600	2026-06-18 03:28:50	103.23.172[.]118	No payload on record
ncstsruks[.]eu[.]cc	128601	2026-06-18 03:28:50	103.23.172[.]118	No payload on record
ddisuyer[.]eu[.]cc	128602	2026-06-18 03:28:51	103.23.172[.]118	Served the padded x64 loaders; linked from 18 June lure pages
kcjsjyeaw[.]eu[.]cc	128603	2026-06-18 03:28:51	103.23.172[.]118	No payload on record
qaywtfse[.]eu[.]cc	134538	2026-06-29 19:08:31	103.23.172[.]117	No payload on record
suawytde[.]eu[.]cc	134539	2026-06-29 19:08:31	103.23.172[.]117	No payload on record
xciwuerse[.]eu[.]cc	134540	2026-06-29 19:08:31	103.23.172[.]117	No payload on record
hsawtse[.]eu[.]cc	134541	2026-06-29 19:08:31	103.23.172[.]117	Certificate order with kaiwyrey[.]eu[.]cc (2026-06-30)
psiawute[.]eu[.]cc	134542	2026-06-29 19:08:31	103.23.172[.]117	No payload on record
zxysevre[.]eu[.]cc	134543	2026-06-29 19:08:33	103.23.172[.]117	No payload on record
kaiwyrey[.]eu[.]cc	134544	2026-06-29 19:08:33	103.23.172[.]118	The delivery host; on 103.23.172[.]117 on 2026-06-30
isudcnzy[.]eu[.]cc	134545	2026-06-29 19:08:35	103.23.172[.]118	Served the padded x64 loaders; served two files that the delivery host also served in July
zuxyegea[.]eu[.]cc	134659	2026-06-30 05:11:28	103.23.172[.]118	No payload on record
hsaueraw[.]eu[.]cc	134660	2026-06-30 05:11:28	103.23.172[.]118	No payload on record
oaiwuyda[.]eu[.]cc	134661	2026-06-30 05:11:28	103.23.172[.]118	No payload on record
rcyawday[.]eu[.]cc	134662	2026-06-30 05:11:28	103.23.172[.]118	Certificate order with kaiwyrey[.]eu[.]cc (2026-07-21)
laiwybstw[.]eu[.]cc	134663	2026-06-30 05:11:29	103.23.172[.]118	Served the padded x64 loaders; certificate order with kaiwyrey[.]eu[.]cc (2026-07-21)
ksidxhcte[.]eu[.]cc	134664	2026-06-30 05:11:30	103.23.172[.]118	No payload on record
xkcisetr[.]eu[.]cc	134665	2026-06-30 05:11:30	103.23.172[.]118	No payload on record
vcxetknsbe[.]ec[.]cc	135116	2026-07-01 03:47:45	103.23.172[.]117	No payload on record
kksiaueted[.]ec[.]cc	135117	2026-07-01 03:47:45	103.23.172[.]117	No payload on record
iysdzxc[.]eu[.]cc	149624	2026-08-06 05:26:50	103.23.172[.]118	No payload on record
bdgsewa[.]eu[.]cc	149625	2026-08-06 05:26:51	103.23.172[.]118	Moved to 103.23.172[.]14 by 2026-10-14

Annex Table 16: The 28 batch eu.cc names, in registry order.

Notes to Annex Table 16:

- The six runs are these registry IDs (109456 is not among the names we hold):
  - 109453 to 109458 (2026-05-11)
  - 128600 to 128603 (2026-06-18)
  - 134538 to 134545 (2026-06-29)
  - 134659 to 134665 (2026-06-30)
  - 135116 to 135117 (2026-07-01, ec.cc)
  - 149624 to 149625 (2026-08-06)
- "No payload on record" means that we analysed no payload from that name; note (a) to Annex Table 18 counts the files seen from 13 of the 28 names.

The 107 single eu.cc names, those registered one at a time (notes to Annex Table 14), sit on 103.23.172[.]230 (90 names) and 103.23.172[.]25 (17 names), as Annex Table 15 shows. They share only IP addresses with the Gname registrar account 574849-1923, and nothing with the operation.

A4.6 The Indian tax lure pages

We judge it likely that part of the kit's tax package naming targeted India. Confidence is low, because the tie rests on two kinds of file name, and the one lure link to kaiwyrey[.]eu[.]cc (2026-07-31) predates the first loader package we read there. The `Tax PenaltyN0` names on the delivery host, among the package names of the auk218[.]club loaders (Annex Table 2), match the Indian lure page title. The `CERT-In5605112305.EXE` name is that of chain C (Table 4), a September VHDX package that did not come from the delivery host. CERT-In is India's computer emergency response team. Two facts limit the India reading. VAT prefixes such as `VATNo.` are used in many countries, and the IP address range also carried hosts named after the Thai government.

The Indian tax lure pages share one HTML template whose Hindi title reads "tax penalty notice, Government of India". The registrar account 574849-1923 at Gname registered all 18 lure page domains of July and August that we recorded, and the June lure page domains listed below. Of the 18, 17 sat on 103.23.172[.]15, and the 18th, zixhasda[.]xin, has no IP address on record. Copies of the same page also sat on other registrants' domains, as the end of this section shows. The account also registered quidoaehse[.]icu, whose host isyraw[.]quidoaehse[.]icu Sekoia lists as Silver Fox phishing [4], and kjfuwyce[.]love, which JUMPSEC lists as documented Silver Fox infrastructure [5]. The June pages sat on .live and .love names on 103.23.172[.]117, and the July and August pages on .live, .xin, .ink and other names on 103.23.172[.]15. We assess it very likely that the June pages formed one batch of that template. Confidence is moderate. Of the 146 page files on 103.23.172[.]117, 139 are one page of 48,255 to 48,260 bytes. They were first downloaded from 2026-05-27 to 2026-07-09.

Pages on the domains of the June, July and August pages point to files on batch eu.cc names and, once, to the operation's delivery host: kcsueaw[.]xin linked the kaiwyrey[.]eu[.]cc download link code `13475714b3d9` on 2026-07-31.

CloudSEK's report of 2026-07-30 on phishing and malware campaigns against Indian taxpayers lists kcsueaw[.]xin and eleven other domains of the account, and a payload signed with a Certum EV certificate [13]. Among the domains are fsyahsxd[.]xin, gisudyawz[.]ink, qaksdiuw[.]xin, xcvgyuraw[.]live and zytsyxbwa[.]live. CloudSEK does not name the registrar account, so the tie of these domains to 574849-1923 is ours (section 5.2).

We judge it very likely that the June lure pages delivered the padded x64 loaders (section A4.7). Confidence is moderate, because the judgment rests on one kind of evidence: all four lure-linked payloads we analysed, behind June pages, are padded x64 loaders. We assess it unlikely that one operator ran both the lure pages and the delivery of the builds for 192.252.183[.]157. Confidence is low, because the judgment rests on the four lure-linked payloads we analysed, and no record names the C2 server of the padded x64 loaders.

The lure page is a shared template, so it connects no one. The rest sit behind Cloudflare IP addresses. The page's memorandum number `TAX/PEN/2026-142` appears in a DcRAT chain [24], a phishing network [26] [27] and a consumer alert [28]. The same page also sat on wordtax[.]ink, a 22net domain under ZHENGJUNHUA (the registrant name of usdt888[.]club), on 2026-08-27 and 2026-09-10. On 2026-09-18 it sat on dnswwt[.]club, which registration data we found also lists under ZHENGJUNHUA (section A5.5).

Each page's download button points to one file on a batch eu.cc name, addressed by a download link code (section 4.2). Each of the 56 June pages points to a different code, and the codes sit on six batch eu.cc names. The number after each name is how many of the 56 pages point to it:

- ddisuyer[.]eu[.]cc: 18 pages
- xzsdiiaeugs[.]eu[.]cc: 11 pages
- fuerubuiaie[.]eu[.]cc: 10 pages
- pzidiauwytsd[.]eu[.]cc: 8 pages
- lzsifuiseurtt[.]eu[.]cc: 7 pages
- idutyarwse[.]eu[.]cc: 2 pages

The 56 pages were first downloaded from 2026-06-02 to 2026-06-24, and the four payloads we read behind their codes from 2026-06-05 to 2026-06-20. The June pages sat on these domains, among others:

- aymdkese[.]love
- bxyawrgr[.]love
- cvwbrwrs[.]live

- fduaywayst[.]live
- fiusyevr[.]live
- flsiuety[.]love
- fstawrxvy[.]love
- fuaytrwese[.]love
- fvxcuvuyte[.]live
- gsawytex[.]love
- hsieuygrw[.]love
- isdhdwhw[.]love
- jaiwuydr[.]love
- jaiydteds[.]love
- laiwnndye[.]love
- oakwusya[.]love
- paiwudyea[.]love
- pmrravwg[.]love

The 18 lure page domains of July and August are:

- fisuahwa[.]live
- fsyahsxd[.]xin
- gisudyawz[.]ink
- kaiwxnyes[.]live
- kcsueaw[.]xin
- lzaiwugsa[.]ink
- pxoiseyhx[.]live
- qaksdiuw[.]xin
- saiyxsux[.]live
- suyczshea[.]xin
- tzawccsw[.]xin
- xcvgyuraw[.]live
- xiusydba[.]live
- zasudtytw[.]xin
- zixhasda[.]xin
- zuszdyyst[.]live
- zuytyarws[.]xin
- zxizusuy[.]xin

The page's embedded 31,006 byte PNG sat on at least 36 hosts. The hosts named in the records, grouped by IP address, are:

- 181.214.250[.]174: dnswwt[.]club and ssmail[.]ink
- 103.23.172[.]15: zuszdyyst[.]live
- 118.107.13[.]110 and 121.127.232[.]126: taxincomeggov[.]com, jntaiyangneng[.]com and hzkyjc[.]com; the last two may be compromised sites
- 156.245.144[.]92: generated hosts such as www[.]7u[.]apexvertex[.]live, 50[.]syncpulse[.]live and www[.]xm[.]okrate[.]click

A4.7 The padded x64 loaders and other download paths

Six of the batch eu.cc names served a second malware family in June and July, the padded x64 loaders (Annex Table 16).

Each package contains a disk image of 144 to 511 MB in UDF (a standard optical disc format). Inside the image, a genuine host program side-loads an x64 DLL. The DLL is padded with 138 to 502 MB of a repeated pattern and carries no HDP loader kit configuration. Padding of this size pushes a file past the size limits of many scanners and upload services.

The June packages of the padded x64 loaders used the lure name form of the August packages for 192.252.183[.]157: `Tax-Number` and six digits. One pair of examples is `Tax-Number723863.img` and `Tax-Number852694.zip` (B4). A name form is a packaging habit, so it connects nothing, but it is the one packing habit the two loader families share. The shared form fits a delivery service that packs for several customers as well as one operator with two

loader families.

Five other download paths used the kit's archive naming from 2026-08-10 to 2026-09-11, so the naming scheme runs beyond the delivery host (Table B of the indicator file). Two of them are:

- A SendGrid sender account, `u48334250`, the second of two in our evidence (section A5.7 names both sender accounts). Its link of 2026-08-31 ran through the URL shortener gin[.]gl/RQ4Bq and a redirect path on divsoftware[.]nl, a site that may itself be compromised. The path ended at the Tencent Cloud COS bucket (cloud file storage) gjtuerqw-1433552157[.]cos[.]ap-hongkong[.]myqcloud[.]com, which served `20260830213443-BECCD7053B19.zip` (`85a0a2e4`).
- cao[.]tedboscomwe[.]com on 72.11.130[.]248, which served `ZIP-20260824011202.92B2DAACC45A.zip` (`12f496cd`) on 2026-08-27. That ZIP contacts usdt888[.]club, which makes cao[.]tedboscomwe[.]com the only host on record that delivered a package for usdt888[.]club.

The six payloads we analysed are listed with the batch name that served each and, where we have it, the file name:

- `77a03e8d`: isudcnzy
- `747124f4`: isudcnzy and laiwybstw
- `67631fba`: fuerubuiaie, `Tax-Number723863.img`
- `7c8395cc`: idutyarwse, `Tax-Number223863.img`
- `d0c2f5cc`: xzsdiiaeugs, `Tax-Number119863.img`
- `e329a261`: ddisuyer, `Tax-Number919863.img`

The genuine host programs that side-load the DLL are the last six rows of Annex Table 7: JetBrains `keytool.exe` and `rmiregistry.exe`, Google `platform_experience_helper.exe`, Siber Systems GoodSync `LogView.exe`, `BugSplatHD.EXE` and Microsoft `LINK.EXE`.

The other three download paths are:

- Two of the paths are click trackers, dianji[.]gzsgdn[.]com and tongji[.]dltwum[.]com, both on 8.211.182[.]27 on 2026-08-10. gzsgdn[.]com served `20260810124517.A8F39C2D71BE.zip` (`c949596a`). dltwum[.]com handed off to the Alibaba Cloud OSS bucket (cloud file storage) kiuwjeq0810[.]oss-ap-northeast-1[.]aliyuncs[.]com, which served `20260810134755.B7D42E8C91AF.zip` (`293c05f0`).
- A Cloudflare Pages front, hckjnkjnaxanxdmdjp[.]pages[.]dev, listed with a Cloudflare Workers host (Table B of the indicator file). The front fetched from hcnaxnkxankknjp[.]com on 103.118.42[.]40. That domain's script hxxps://hcnaxnkxankknjp[.]com/icloud.php served `20260901014335-71359EDFC0A5.zip` (`a2fd0212`) and `20260902114342-063801A8ED70.zip` (`709ba0d9`) from 2026-09-01 to 2026-09-11.

A4.8 The remote management deployment near usdt888[.]club

On 2026-08-24 usdt888[.]club resolved to 122.10.117[.]3, a server for ManageEngine Endpoint Central, a commercial remote monitoring and management (RMM) product. We judge it very likely that this ManageEngine remote management server and its domains form one deployment. Confidence is moderate, because jpword[.]cc resolved to the server from 2026-07-28 and wordtax[.]ink served the agent that talks to it. An HTML application (HTA) file, `27254125`, fetched hxxps://wordtax[.]ink/down/setup.aac and installed an agent that talks to 122.10.117[.]3. Annex Table 17 lists the deployment and the ZHENGJUNHUA domains around it. ZHENGJUNHUA is the registrant name of usdt888[.]club.

oswin[.]club, the C2 server of one build of the 2026-09-01 x64 compile, is registered under ZHENGJUNHUA in two records in registration data we found. oswin[.]club sat on 156.245.245[.]235 on 2026-09-02, two days before usdt888[.]club did. The registrant name and that IP address are two independent values that oswin[.]club shares with usdt888[.]club in one week, a strong connection.

oswin[.]club now shares 103.42.30[.]140 with winapp[.]work, created on 2026-09-20. One record lists winapp[.]work under ZHENGJUNHUA, and winapp[.]work was seen on usdt888[.]club's IP address 103.42.30[.]245. winapp[.]work thus shares the name and an IP address with each of the other two, a strong connection that rests on one record. We judge it likely that one party controls usdt888[.]club, oswin[.]club and winapp[.]work. Confidence is low, because 156.245.245[.]235 carried other customers and unrelated registrants also use the name ZHENGJUNHUA. The IP address 156.245.245[.]235 also presented Microsoft's own TLS certificate, borrowed by whoever ran the server, and carried panel[.]puppycc[.]fun, another customer. A borrowed certificate connects nothing.

Value	Type	Role	Dates (UTC)
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
www[.]wordtax[.]ink	Domain	Host of wordtax[.]ink, first seen 2026-08-12	2026-08-12 onward
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
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

Value	Type	Role	Dates (UTC)
mail[.]g00g1e[.]club	Domain	Mail host of g00g1e[.]club	2026-10-14
jpword[.]cc	Domain	RMM deployment domain; 22net default name servers, state BeiJing; resolved to 122.10.117[.]3 from 2026-07-28	created 2026-04-30, expires 2027-04-30; seen 2026-06-21 to 2026-10-14
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
mail[.]jpword[.]cc	Domain	Mail host of jpword[.]cc, first seen 2026-04-30	2026-04-30 onward
vipmail[.]uno	Domain	Name on the certificate group of wordtax[.]ink (one server account)	2026-08-12 to 2026-09-16
rumail[.]cc	Domain	Name on the certificate group of wordtax[.]ink	2026-08-12 to 2026-09-16
dnswwt[.]club	Domain	ZHENGJUNHUA domain at 22net (one record); name on the certificate group of wordtax[.]ink; 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
downin[.]club	Domain	ZHENGJUNHUA domain at 22net (one record); name on the certificate group of wordtax[.]ink	2026-09-02 to 2026-09-16
ssmail[.]ink	Domain	ZHENGJUNHUA domain at 22net (one record); name on the certificate group of wordtax[.]ink; served the Indian tax lure body	2026-09-16
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
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
103.193.172[.]103	IPv4	RMM deployment IP address (agent[.]jpword[.]cc; weburl[.]club)	2026-07-30 to 2026-08-09
181.214.250[.]206	IPv4	wordtax[.]ink IP address; served setup.aac and setup.appx	2026-08-14 to 2026-08-25
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
166.88.227[.]22	IPv4	IP address of wordtax[.]ink	2026-06-23
194.24.161[.]113	IPv4	IP address of g00g1e[.]club	2026-05-01
185.55.243[.]158	IPv4	IP address of g00g1e[.]club with its mail host	2026-10-14
185.55.240[.]19	IPv4	IP address of jpword[.]cc with its mail host	2026-06-21
hxxps://wordtax[.]ink/down/setup.aac	URL	ManageEngine Endpoint Central agent package fetched by the HTA 27254125	2026-08-25
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 [29]	2026-08-18

Annex Table 17: The remote management deployment and the ZHENGJUNHUA domains around it.

Notes to Annex Table 17:

- The certificate group is one set of certificates, valid from 2026-08-12, 2026-09-02 and 2026-09-14, on 181.214.250[.]206 and 181.214.250[.]174. It covers six domains:
  - wordtax[.]ink
  - vipmail[.]uno
  - rumail[.]cc
  - dnswwt[.]club
  - downin[.]club
  - ssmail[.]ink

A4.9 Shared suppliers

Several suppliers recur across the operation, and none of them connects two parties. They are the registrars 22net (IANA 1555), Gname (IANA 1923) with the EUCC registry, WebNIC and DNSPod, and the file-sharing application.

A common JARM fingerprint, a hash of how a server answers a TLS handshake, recurs as well. Two public sources list ValleyRAT C2 servers in IP address ranges the operation also used:

- 137.220.152[.]155 and 137.220.152[.]199: NCC Group lists them as suspected ValleyRAT C2 servers, in the /24 range of moik77a[.]club's second IP address [30]
- 154.36.188[.]162 and 154.36.188[.]194: two entries of a public indicator listing give them as ValleyRAT C2 servers, beside 154.36.188[.]18 [31], the later IP address of fddlbh2[.]club

Shared IP address ranges never connect anything.

The name servers that recur are:

- ns1[.]22[.]cn and ns2[.]22[.]cn: 22net's name servers, on every 22net domain
- pk3[.]22[.]cn and pk4[.]22[.]cn: 22net's parking pair
- Gname's default name server pairs and the servers it assigns to expired domains
- Two Cloudflare pairs: on two older KANGYINGJIE domains
- DNSPod: on the unrelated lower case ZHENGJUNHUA domain of section A5.5
- resellerclub ns5 to ns8: on spbo[.]cc

Three of the fixed codes that historical copies of the registration records show in place of contact values recur on all five .club C2 domains of the eleven builds we have as files, B1 to B9, F1 and F2 (section A3.2). Each value is listed with the text it stands for:

- `1f8f4166599d23ee`: "REDACTED FOR PRIVACY"
- `f651612a2f356ad3s@` (as printed): the registrar's standard referral sentence that replaces a hidden field
- `56dfc9b0161500bf`: the province BEIJINGSHI

A4.10 What does not connect

Beyond the delivery host, the infrastructure shares nothing with the delivery range, and most domains near the C2 servers belong to other customers (Annex Table 18).

Item	Why it does not connect
Public sources	Public reporting lists taku788[.]club, fuoe333[.]club, moik77a[.]club and usdt888[.]club as C2 servers [14], but names no group ID, hash, download link code or eu.cc name of the operation, and no registration record that joins its servers
The operation's four C2 domains	No two share an IP address; oswin[.]club, outside the operation, sat on 156.245.245[.]235 two days before usdt888[.]club (section A4.8); none connects to the delivery hosts under the rule of section 2
Other eu.cc names	None of the six payloads of section A4.7 carries an operation C2 server or group ID
Further files	None of 47 files from 13 other batch names equals a file of the operation (a)
Lure-linked payloads	All four we analysed are padded x64 loaders
Homeland Security pages	None of the lure pages or package names we recorded is themed on Homeland Security, USCIS or Seguridad Nacional
22net delivery names	No domain that served a kit build or linked the delivery host is registered at 22net (b)
akyv188[.]club	An older KANGYINGJIE domain on 192.252.183[.]224, in the /24 range of 192.252.183[.]157; the range carries no weight
Other customers on C2 server IP addresses	spbo[.]cc on 192.252.183[.]157; keep-cos[.]yanshi-eyucode[.]biz on 154.36.188[.]18; panel[.]puppycc[.]fun on 156.245.245[.]235; anonchihaya[.]com on 156.245.245[.]222; xz670[.]top, one of 140 names on 202.61.85[.]216
Stale and nearby names	8556vc[.]com, a gambling brand domain with a stale pointer to 202.61.85[.]50 (zone last edited 2025-11-20); hyjjj[.]eu[.]cc in 202.61.85[.]0/24; metamack[.]club on 192.252.183[.]10; 192.252.182[.]61, a shared hosting front beside 192.252.183[.]157
karlost[.]club	A 2024 registration under SUZHAOBIN at 22net, outside the operation; it shares no value with the operation

Annex Table 18: What does not connect in the infrastructure.

Notes to Annex Table 18:

- (a) The 47 further files came from 13 batch names other than kaiwyrey[.]eu[.]cc. One file, `747124f4`, came from two names (isudcnzy[.]eu[.]cc and laiwybstw[.]eu[.]cc), so the numbers below add up to 48. Table C of the indicator file lists each file. The number after each name is how many of the files came from it:
  - oaosifytaw[.]eu[.]cc: 8

    - zuxyegea[.]eu[.]cc: 8
    - ddisuyer[.]eu[.]cc: 7
    - pzidiauwytsd[.]eu[.]cc: 5
    - isudcnzy[.]eu[.]cc: 5
    - hsaueraw[.]eu[.]cc: 4
    - lzsifuiseurtt[.]eu[.]cc: 3
    - fuerubuiaie[.]eu[.]cc: 2
    - xzsdiiaeugs[.]eu[.]cc: 2
    - ksidxhcte[.]eu[.]cc: 1
    - idutyarwse[.]eu[.]cc: 1
    - iysdzxc[.]eu[.]cc: 1
    - laiwybstw[.]eu[.]cc: 1
- (b) The 22net domains wordtax[.]ink and dnswwt[.]club, under ZHENGJUNHUA, served the RMM packages, copies of the Indian tax lure page and a 59 MB ZIP (section A5.5).

A5.1 What the evidence names at each level

Every trail behind the operation ends at a registrant name or a customer account, and none of them identifies a person. Three parties carry the questions that matter:

- the registrant of the C2 domains
- the controller of the delivery host kaiwyrey[.]eu[.]cc, whose four main download links delivered the loader packages
- the customer behind the Gname registrar account 574849-1923, which registered most of the domains around the delivery host

A registrant organisation is the text in the organisation field of a domain registration record. A registrar account is a registrar's customer number, and a hashed registrant value is the fixed code that historical copies of a registration record show in place of the registrant organisation (section A2). We use all three as search keys between records, never as the names of people. We keep five levels apart: the builder, the C2 server owners, the delivery accounts, the bulk registrants and the signers (Annex Table 19). We keep them apart because a connection at one level proves nothing at another. No registrant name or registrar account recurs on two levels in the records we hold, but the records of the eu.cc names, kaiwyrey[.]eu[.]cc among them, print no registrant to compare. Whether one party spans the C2 server and delivery levels is the separate judgment of section 4.4, which finds it likely. Confidence there is low.

Level	Claim	Likelihood	Confidence	What the grade rests on
Builder	One kit, the HDP loader kit, made all 44 configurations	Observed	n/a	One grammar, cipher and key pair in all 44
Builder	One copy of the builder in use made the builds we analysed	Likely	Low	Shared compiles connect seven of eight C2 servers, but a builder can ship one compile to every user
C2 servers	The four KANGYINGJIE C2 domains share one registrant entry (BEIJINGSHI)	Very likely	Moderate	Three print the name in our records; the fourth carries the hashed value, and one stored record prints the name
C2 servers	The operator of the C2 servers registered the 15 older KANGYINGJIE domains	Likely	Low	One exact tie, atyv788[.]club on taku788[.]club's IP address; the moving IP addresses had other customers
Delivery	One account behind the delivery host	Very likely	Moderate	Two main download links checked within three minutes served the same file in 45 of 46 cases
Delivery	One customer behind 574849-1923 and its 243 domains	Very likely	Moderate	One account number in every contact role, on no other Gname domain in our records
Delivery	The C2 server operator runs the delivery host	Likely	Low	One listing outside our own records places auk218[.]club, also served there, under KANGYINGJIE
Bulk registrants	A seller's stock account behind the link domains of a July 2026 lure email (section A5.8)	Very likely	Moderate	84 of its 88 domains passed to other contacts inside one registration
Bulk registrants	A registrant name or account recurs across the levels	Observed: none	n/a	No registrant recurs on two levels; the eu.cc names print none
Signers	Ten vendor identities on reused hosts are genuine signatures	Very likely	High; moderate for Guangzhou Ningjinghai (section A3.7)	Each signature verifies against its file, an unmodified vendor program

Annex Table 19: What the evidence names at each level.

A5.2 One copy of the builder in use

We assess it likely that one copy of the builder in use, a single installation, produced the builds we analysed. Confidence is low, because a builder that ships precompiled loaders gives every user of a release the same compile, so shared compiles leave the number of copies open. Near daily compiles with several C2 servers fit an operator's own copy and a build service equally well, so the judgment points to no single operator.

All 44 configurations share one grammar, one cipher and the same two string keys, across six versions of the cover application. The September builds B7, B8 and B9 carry encrypted resources of other names and sizes (section A3.6). The cover application is the harmless Windows program each loader is built on (section A3.3). One kit, the HDP loader kit, made all 44 configurations. That is a fact about the toolkit, observed in every build.

Shared compiles connect seven of the eight C2 servers, across both registrant names, KANGYINGJIE and ZHENGJUNHUA, and both port profiles, which are builder settings (section 4.1). auk218[.]club alone never shares a compile with another C2 server. Its tie to the rest would run through `67e1ac14`, the build of 2026-08-09, the same compile as an auk218[.]club loader, whose disk image communicates with fuoe333[.]club (section A6.3). That build was made before the Spanish version of the cover application, whose main icon is the U.S. Department of Homeland Security (DHS) seal (section A3.8). Besides the September `MMDD` dates, two `fz` tags were typed in by hand (`fz` is the configuration's sub group tag). One is `mail`, on one usdt888[.]club build (B5). The other is `VHD-0902`, on the build that calls oswin[.]club. It names the carrier, a VHD disk image, and the day, 2026-09-02, of the package of the first fddlbh2[.]club build (F1). One copy of the builder is the minimum, because no build or package requires a second.

Four compiles carry several C2 servers each (Annex Tables 3 and 4): one of 2026-08-16, the 2026-08-19 compile, and the x64 compiles of 2026-09-01 and 2026-09-03. That 2026-08-16 compile carries the build C15, which calls 192.252.183[.]157, and the build `c1aff663`, which calls fuoe333[.]club. The two builds differ only inside the configuration. The 2026-08-19 compile alone carries five C2 servers (Annex Table 3).

A5.3 The registrant identities at a glance

Annex Table 20 profiles every registrant name, hashed value, registrar account and sender account that the registration records attach to the operation or to its neighbours. Sections A5.4 to A5.8 give the evidence for each. Contact fields that would identify private persons stay out of this report.

Identity	What it is	Covers	Connection to the operation	Our assessment
KANGYINGJIE, BEIJINGSHI; hashed value `ab376f4f34801a68`	One registrant entry at 22net	taku788[.]club, fuoe333[.]club, moik77a[.]club, fddlbh2[.]club; 2026-08-09 to 2026-09-01; auk218[.]club (2026-07-27) in one listing	Direct: registrant of C2 domains; strong to auk218[.]club, resting on one listing	One entry: very likely, moderate
KANGYINGJIE, ANHUISHENG	A second entry with the same name at 22net	15 older domains; 2024-04-22 to 2026-03-24	Strong for atyv788[.]club; weak for the rest	Registered by the operator of the C2 servers: likely, low
CENGCHAO, GUANGDONGSHENG	A registrant name at 22net	shyda6317[.]club from 2026-01-29, homeysion[.]work and five older names	Weak: one shared IP address	A second name of the older domains' DNS operator: likely, low
ZHENGJUNHUA, BEIJINGSHI; hashed value `e65ef034ff5b3fab`	A second registrant entry at 22net, under a common romanised name	usdt888[.]club, wordtax[.]ink, g00g1e[.]club in our records; 13 domains, oswin[.]club and winapp[.]work among them, in registration data we found; 2026-04-29 to 2026-09-20	Direct for usdt888[.]club and oswin[.]club; strong between usdt888[.]club, oswin[.]club and winapp[.]work; weak for the others	One operator of the domains and the RMM deployment: roughly even chance, low. One party behind usdt888[.]club, oswin[.]club and winapp[.]work: likely, low
574849-1923	A customer account at Gname, printed in every contact role, with Illinois, United States	243 lure and host domains; 2025-09-26 to 2026-08-09	Strong at account level to the delivery host	One customer: very likely, moderate. The operator's own account: roughly even chance, low
The delivery host account	One account of a file-sharing application on kaiwyrey[.]eu[.]cc	48 download links; files 2026-07-03 to 2026-09-15	Direct for every build it served	One account: very likely, moderate. The C2 server operator's: likely, low
The batch server account and buyer	One server account shown by two certificate orders; one buyer shown by six registry ID runs	kaiwyrey[.]eu[.]cc and three batch names on the account; all 28 batch eu.cc names under the buyer	Strong to the delivery host	One server account for the four: very likely, moderate. One buyer for the 28: very likely, moderate
SendGrid `u53630135` and `u48334250`	Email sender accounts	Links of 2026-07-29 and 2026-08-31	Delivery channels	Owner not graded
C1461784974-CNIC, Shanghai	A Gname contact handle	Two .qpon domains on 103.23.172[.]230	None beyond the IP address range	One customer for both: likely, low
chenxiansheng	A privacy relay contact	e-tzxarw[.]jp and e-tzsgzxyu[.]jp, created 2026-09-14	None; a privacy value	A privacy service value: very likely, moderate

Annex Table 20: The registrant identities and accounts, what they cover and our assessment.

Notes to Annex Table 20:

- The assessment gives the likelihood, then the confidence.
- Section A5.8 covers the registrants that share nothing with the operation.

A5.4 KANGYINGJIE, the registrant of four C2 domains

At the registrar 22net, KANGYINGJIE is the registrant name of taku788[.]club, fuoe333[.]club and moik77a[.]club, three of the operation's four C2 domains. It is also the registrant name of fddlbh2[.]club, the C2 server of two builds just outside the operation (section 4.3). The operation's fourth C2 domain, usdt888[.]club, is under ZHENGJUNHUA (section A5.5). We judge it very likely that taku788[.]club, fuoe333[.]club, moik77a[.]club and

fddlbh2[.]club share one registrant entry, with province BEIJINGSHI. Confidence is moderate, because historical copies of all four records carry the same code for the organisation, the hashed registrant value `ab376f4f34801a68`, and our records of taku788[.]club, fuoe333[.]club and moik77a[.]club print the name. Across the four domains, that value appears in nine dated record rows from 2026-08-11 to 2026-10-09. taku788[.]club's registration record of 2026-08-21 prints `Registrant Organization: KANGYINGJIE` with province BEIJINGSHI. A stored record of fddlbh2[.]club of 2026-09-06, in registration data we found, prints KANGYINGJIE with province BEIJINGSHI in the organisation field, where our own records carry only the hashed value. The four domains share no IP address, so between any two of them the registrant name is one shared value, a weak connection.

Each of the five registrant names at 22net keeps a fixed province (for KANGYINGJIE, one per registrant entry):

- KANGYINGJIE: ANHUISHENG and BEIJINGSHI
- CENGCHAO: GUANGDONGSHENG
- DENGHONGXIN: ZHONGQINGSHI (section A5.8)
- ZHENGJUNHUA: BEIJINGSHI
- SUZHAOBIN: HEBEI (section A5.8)

We therefore judge it almost certain that KANGYINGJIE is a value one customer entered and not one that 22net applies to its customers. Confidence is high. We assess it likely that the entry is the operator's own rather than a name that a reseller gives several customers. Confidence is low, because the judgment rests on the records of this one name; the hashed registrant values of unrelated 22net domains would test it.

The same name heads 15 older domains at 22net, all with province ANHUISHENG, so at least two registrant entries use it (Annex Table 21). The 15 are a floor, because 22net prints the organisation only in records made before a domain switched to redacted output. Eleven remain registered under KANGYINGJIE. chusyiorusvo[.]club, shyda6320[.]club and shyda6321[.]club have lapsed, and shyda6317[.]club lapsed and was registered again under CENGCHAO.

We judge it very likely that one DNS operator points the six domains that moved together:

- aeya388[.]club
- aeyd588[.]club
- aeda6188[.]club
- shaeyda6328[.]club
- shyda6318[.]club
- shyda6319[.]club

Confidence is moderate for two reasons (Annex Table 22). First, two to five of the six sat on each of five IP addresses from March 2025 to October 2026. Second, on four of those IP addresses, those of the six that sat there did so within two weeks of one another. The IP addresses, and what else they hosted, are:

- 202.95.1[.]227 and 202.95.19[.]243: nothing but these domains in 2026, apart from shyda6317[.]club on 202.95.19[.]243 (CENGCHAO, below). The same holds for 112.213.120[.]167, aeya388[.]club's current IP address, which is outside the five.
- 103.27.79[.]70: what else it hosted is not on record
- 112.213.120[.]139 and 45.204.208[.]37: gambling and other customers before, during and after the moves, which keeps confidence at moderate

Two other customers' domains used the older domains' IP addresses first. The first, ze6688[.]cn, sat on 45.204.208[.]37 (2026-01-28) and 112.213.120[.]139 (2026-05-01). KANGYINGJIE domains took both IP addresses within 90 days, a strong connection inside that window only. We assess it a roughly even chance that ze6688[.]cn belongs to the same set as the older KANGYINGJIE domains. The second, idecald[.]cn, sat on 154.36.188[.]218 (2026-02-07) and 112.213.120[.]139 (2026-04-23). Its first IP address, 154.36.188[.]218, pairs it with shyda6317[.]club under CENGCHAO, so it shares only one value with the KANGYINGJIE names, a weak connection. idecald[.]cn and ze6688[.]cn share one registrant contact in records of January and April 2026, a strong connection between the two. We therefore grade them together and judge it a roughly even chance that idecald[.]cn belongs to the set. Confidence in both judgments is low. Separately, one older domain, aeyd588[.]club, moved its name servers to a Cloudflare pair on 2026-08-10.

aeya388[.]club is the C2 server of the configuration that Proofpoint saw in early 2026 and published for its actor TA4922 [6]. An OTX pulse lists aeya388[.]club, aeyh688[.]club, akyv188[.]club and atyv788[.]club beside the operation's C2 servers [14]. A researcher listed aeya388[.]club and shyda6319[.]club as Winos (ValleyRAT) C2 servers in January 2026 [16], and a post of 2026-09-17 names yscf988[.]club [32]. The registration tie between these domains, the shared registrant name KANGYINGJIE, is our own finding. The Proofpoint configuration shares one value with the operation, that registrant name, in another period, a weak connection (section A6.2).

One older KANGYINGJIE domain, atyv788[.]club, forms a pair with taku788[.]club. We judge it likely that the two have one operator. Confidence is low, because a reseller that parks several customers on one leased IP address would leave the same two shared values, the registrant name and the IP address. atyv788[.]club's record prints KANGYINGJIE with province ANHUISHENG. It is not one of the six and has its own IP address history:

- 45.192.219[.]19: February 2026
- 192.253.224[.]109: 2026-08-01
- 202.61.85[.]34: from 2026-08-14 09:11:59 UTC, the time of the move that its live zone serial gives, three hours after taku788[.]club was registered

taku788[.]club was seen on 202.61.85[.]34 on 2026-08-16. An earlier copy of atyv788[.]club's DNS answer carries the creation day serial, which we treat as out of date.

The registrant name and an exact IP address in one period make a strong connection, if a zone serial records the time of the last edit. Three facts weaken it: the IP address is leased and carried 116 names in turn, the two records print different provinces, and taku788[.]club left within two days. Three further judgments rest on this pair, all with low confidence. The operator of the C2 servers likely registered all 15 older domains. KANGYINGJIE likely serves one party rather than a broker that registers for unrelated groups (above). It is a roughly even chance that atyv788[.]club is itself a C2 server; a configuration that calls it would settle its role.

CENGCHAO has been the registrant name of shyda6317[.]club since its second registration on 2026-01-29 (to 2027-01-29), after the KANGYINGJIE registration lapsed. We assess it likely that CENGCHAO is a second name used by the DNS operator of the older KANGYINGJIE domains. Confidence is low, because the two share one IP address, 202.95.19[.]243, where shyda6317[.]club sat with four KANGYINGJIE domains on 2026-10-14, and where a fifth, aeya388[.]club, was seen on 2026-08-16. shyda6317[.]club was on 154.36.188[.]218 on 2026-05-07, an IP address idecald[.]cn had used before. CENGCHAO, always with GUANGDONGSHENG, also heads five older names, the earliest from 2013, and homeysion[.]work (22net, registered 2026-03-24). homeysion[.]work passed inside its registration to two later registrant entries in May and June 2026. None of these six has a tie to the operation.

Domain	Created	Expiry or status	Moved with the six	Latest IP address on record
chusyiorusvo[.]club	2024-04-22	Lapsed 2025-04-22	No	172.98.22[.]236 (2024-08-04)
shyda6317[.]club	2024-11-09	Lapsed 2025-11-09; registered again 2026-01-29	No	202.95.19[.]243 (2026-10-14)
shyda6318[.]club	2024-11-09	Expires 2026-11-09	Yes	202.95.19[.]243 (2026-10-14)
shyda6319[.]club	2024-11-09	Expires 2026-11-09	Yes	202.95.19[.]243 (2026-10-14)
shyda6320[.]club	2025-04-13	Lapsed 2026-04-13	No	118.107.5[.]152 (2026-02-15)
shyda6321[.]club	2025-04-13	Lapsed 2026-04-13	No	None on record
aeya388[.]club	2025-10-30	Expires 2026-10-30	Yes	112.213.120[.]167 (2026-10-14)
shaeyda6328[.]club	2025-10-30	Expires 2026-10-30	Yes	202.95.19[.]243 (2026-10-14)
aeyd588[.]club	2025-11-16	Expires 2026-11-16	Yes	202.95.1[.]227 (2026-02-08); none now
aeyh688[.]club	2025-11-18	Expires 2026-11-18	No	192.229.115[.]159 (2026-10-14)
atyv788[.]club	2025-12-02	Expires 2026-12-02	No	202.61.85[.]34 (2026-08-14 to 2026-10-14)
akyv188[.]club	2026-01-07	Expires 2027-01-07	No	192.252.183[.]224 (2026-07-21 to 2026-10-14)
nta-go[.]work	2026-01-28	Expires 2027-01-28	No	103.118.41[.]125 (2026-10-14)
yscf988[.]club	2026-03-08	Expires 2027-03-08	No	134.122.163[.]220 (2026-10-14)
aeda6188[.]club	2026-03-24	Expires 2027-03-24	Yes	202.95.19[.]243 (2026-10-14)

Annex Table 21: The 15 older KANGYINGJIE domains (province ANHUISHENG), all at 22net.

Notes to Annex Table 21:

- "The six" are the domains that moved between IP addresses together (Annex Table 22).
- Every IP address on record is in Table B of the indicator file. chusyiorusvo[.]club passed to the registrant DENGHONGXIN inside its registration in August 2024 (section A5.8). shyda6317[.]club was registered again under CENGCHAO.

IP address	Observed
103.27.79[.]70	2025-03
202.95.1[.]227	2026-02
45.204.208[.]37	2026-02
112.213.120[.]139	2026-06
202.95.19[.]243	2026-08 to 2026-10-14

Annex Table 22: IP addresses of the six older KANGYINGJIE domains that moved together.

Registration data we found lists 121 domains under KANGYINGJIE at 22net, created from 2025-04-13 to 2026-10-11; it does not include the 2024 domains of Annex Table 21. The registrations continue through the operation's dates (2026-08-09 to 2026-10-14) and past its last compile on 2026-09-22. Of the 121, 66 were created after 2026-09-01, 30 of them on 2026-10-04 and six on 2026-10-11. Table B of the indicator file lists those not named elsewhere in this report. Five domains of 2015 at the registrar Ename under the same string differ in registrar and decade, so we treat them as a name collision. Among the 22net domains are:

- Four Indian tax lookalike domains, created while the kit's builds were being made:

    - incometaxind[.]club: 2026-08-14
    - incumetaxineia[.]club and incumetaxineia[.]work: 2026-08-20
    - incogtaxbbo[.]club: 2026-08-23
- ixee18[.]club, which served a fake software download page on 156.251.11[.]56.
- auk218[.]club, the C2 server of the 16 earlier loaders on the delivery host (section 4.1).
- Eight names in 202.61.85[.]0/24, the range where taku788[.]club moved, each listed with its IP address and the day it was created:
    - caiyun1[.]club: 202.61.85[.]181, 2026-08-18
    - ct4vk1d[.]club: 202.61.85[.]114, 2026-08-24
    - qztt688[.]club: 202.61.85[.]168, 2026-09-10
    - ackp1o5[.]club: 202.61.85[.]190, 2026-09-13
    - eabiur6[.]club: 202.61.85[.]116, 2026-09-21
    - khltt1[.]club: 202.61.85[.]151, 2026-10-04
    - kufp16[.]club: 202.61.85[.]233, now 23.226.57[.]52, 2026-10-04
    - usod22[.]club: 202.61.85[.]170, 2026-10-04

These names, auk218[.]club aside, share only the registrant name with the C2 domains, a weak connection. For the eight in 202.61.85[.]0/24, the IP address range and the creation dates carry no weight. Each of these names rests on one source.

A5.5 ZHENGJUNHUA, usdt888[.]club and the remote management server

ZHENGJUNHUA is the registrant name of usdt888[.]club, the C2 server of two builds (B5, B6) and the server that 17 of the October re-packed copies contacted (section A3.2). Its organisation code in historical copies of the record, the hashed registrant value `e65ef034ff5b3fab`, differs from the KANGYINGJIE value, so usdt888[.]club sits under a second registrant entry. The name is a common romanised one that unrelated registrants also use. Nine unredacted registration records of 2009 to 2015 carry it. From 2010 to 2018, 150 records name it as owner. One domain at DNSPod since 2021 carries it in lower case with the province guang dong sheng. We judge it very likely that the registrant of that domain is unrelated. Confidence is moderate, because its registrar, letter case, province and era all differ.

We assess it a roughly even chance that one operator runs the 2026 ZHENGJUNHUA domains and the ManageEngine remote management deployment (section A4.8). Confidence is low, because the two connect only through the name in the same 2026 record format and one shared IP address. The three ZHENGJUNHUA domains in our own records, each with its registration period, are:

- usdt888[.]club: created 2026-08-18, expires 2027-08-18
- wordtax[.]ink: 2026-05-26 to 2027-05-26, on hold at the registry from 2026-09-11
- g00g1e[.]club: 2026-04-29 to 2027-04-29

wordtax[.]ink's records print ZHENGJUNHUA up to 2026-07-24, and g00g1e[.]club's up to 2026-08-05.

Registration data we found lists 13 ZHENGJUNHUA domains at 22net, created from 2026-04-29 to 2026-09-20, and Table B of the indicator file lists them. A domain of 2018 at the registrar Xin Net under the same string is a name collision. Among the 22net domains are:

- dnswwt[.]club, which served the Hindi tax penalty page of section A4.6 and a 59 MB ZIP, `/down/file.zip`, on 181.214.250[.]174 from 2026-09-18 to 2026-09-20. A researcher post of 2026-09-15 reports a Japanese-language email lure whose PDF links to a page on dnswwt[.]club [33].
- oswin[.]club, the C2 server of one build, and winapp[.]work (section A4.8).

From 2026-07-28 jpword[.]cc resolved to 122.10.117[.]3, the remote management server (section A4.8). A researcher traced hxxps://wordtax[.]ink/down/setup.appx to the C2 servers jpword[.]cc:8383 and 122.10.117[.]3:8383 on 2026-08-18, and saw the same C2 server on 2026-08-05 with a purchase order lure [29]. This fits our finding that wordtax[.]ink served the remote management agent package (section A4.8). Section A5.5 gives further detail on the ZHENGJUNHUA domains.

Registration data we found lists oswin[.]club (two records) and winapp[.]work (one record) under ZHENGJUNHUA. Each of the three domains, usdt888[.]club, oswin[.]club and winapp[.]work, shares an IP address with another of them (section A4.8). With the name, each such pair therefore shares two independent values in one period, a strong connection. We judge it likely that one party controls usdt888[.]club, oswin[.]club and winapp[.]work. Confidence is low, because two of the three IP addresses carried other customers and winapp[.]work's name rests on one record.

Only toolkit facts span the KANGYINGJIE C2 domains and the ZHENGJUNHUA domains: the 2026-08-19 compile and the 2026-09-01 x64 compile. Both names also registered Indian tax themed domains, a lure theme, which carries no weight. Under our grading rule (section 2), nothing connects the two entries. Historical copies of the usdt888[.]club record share the province code `56dfc9b0161500bf` with the four KANGYINGJIE domains, but that code most likely stands for BEIJINGSHI, so it shows only a shared province. We assess it a roughly even chance that one operator runs both. Confidence is low, because only toolkit facts span them (Annex Table 23).

Among the 13 ZHENGJUNHUA domains at 22net of section A5.5 are also:

- log1n[.]work, which served a Japanese Proton Mail phishing page on 198.44.182[.]48 on 2026-09-30.

wordtax[.]ink also served the Indian tax lure page of section A4.6 on 2026-08-27 and 2026-09-10. On 2026-08-24 usdt888[.]club resolved to the remote management server's IP address. Between the ZHENGJUNHUA domains and the remote management deployment, the registrant name and the IP address make two weak connections, since one rented server can serve two groups. wordtax[.]ink's record of 2026-08-22 is redacted; if the name persisted into August, the two values would make a strong connection. The package `12f496cd`, which contacts usdt888[.]club, came through cao[.]tedboscomwe[.]com and not through the delivery host.

A5.6 Registrar account 574849-1923 at Gname

574849-1923 is one customer account at Gname. It registered the Indian tax lure page domains on the delivery IP address range 103.23.172[.]0/24 and two domains on vendors' Silver Fox lists. One is quidoaehse[.]icu, whose host isyraw[.]quidoaehse[.]icu Sekoia lists as Silver Fox phishing [4]. The other is kjfuwyce[.]love, which JUMPSEC lists as documented Silver Fox infrastructure apart from PAPERMILL, the emerging Silver Fox like cluster it tracks [5]. We judge it very likely that one customer controls the account. Confidence is moderate, because the number appears in every contact role of 243 domains and on no other Gname domain in our records. Other Gname domains print 21 other account numbers of the same form as 574849-1923, among them:

- 490943-1923
- 483080-1923
- 575801-1923
- 503494-1923

The suffix 1923 is Gname's IANA registrar number. Every one of the 243 domains prints Illinois, United States, a contact value that nothing else supports.

The account's domains were created from 2025-09-26 to 2026-08-09, and Table B of the indicator file lists all of them with their hosts. They are:

- 156 domains on 103.23.172[.]117, the June Indian tax lure page hosts among them (Annex Table 15 and section A4.6).
- 61 domains on 103.23.172[.]15, among them 17 of the 18 lure page domains of July and August and csdfsera[.]live.
- Two on 103.23.172[.]118, maoasiye[.]live and tdrw[.]bvbxdse[.]live, beside the delivery host.
- 11 on 103.23.172[.]230, quidoaehse[.]icu among them.
- 11 on 103.23.172[.]25, among them three hosts named after the Thai government, www[.]thaigov[.]go[.]th[.]gothuy[.]icu, thaigov[.]gothds[.]cyou and gov[.]bvdaccs[.]cyou.
- Two with no IP address on record, zixhasda[.]xin, one of the 18 lure page domains, and pzisiauywa[.]xin.

On 2026-06-30 the delivery host, kaiwyrey[.]eu[.]cc, and two of the account's domains were recorded on the IP address 103.23.172[.]117; by 2026-07-01 the delivery host had moved to 103.23.172[.]118. On 2026-07-31 the account's lure page kcsueaw[.]xin linked a download link on that host. The shared IP address and, through the lure link, the shared delivery host, within one month, make a strong connection at account level. We assess it likely that one customer account or one service controls both the delivery host and the account's domains. Confidence is low, because the evidence is one IP address shared on one day and one link. We judge it a roughly even chance that the account is the operator's own rather than that of a lure and delivery service that other groups also use. Confidence is low, because no record names the C2 server of the padded x64 loaders, which the same names and IP addresses also carried (section A4.7).

A5.7 The delivery accounts

At the delivery host the evidence names an account, not its owner. One account very likely shipped the builds served there (section 4.2). Confidence is moderate, because when two of the delivery host's four main download links were checked within three minutes of each other, both served the same file in 45 of 46 cases. We assess it likely that this account belongs to the C2 server operator. Confidence is low, because the judgment rests on the one listing outside our own records that places auk218[.]club under KANGYINGJIE (section 4.1).

Of the 28 batch eu.cc names, registered in runs of registry IDs, kaiwyrey[.]eu[.]cc and three others sit on one server account (section A4.5). Every eu.cc registration record is redacted at the registry. Six of the names served the padded x64 loaders. The Gname account 574849-1923 registered almost every domain on 103.23.172[.]117 that is not a batch eu.cc name. Owning the names is a different act from using them. It is a roughly even chance that the owner of the batch names rotates them for its own payloads rather than renting them out. It is unlikely that the batch names are the C2 server operator's own, because every other payload we analysed from them is a padded x64 loader. Confidence in both judgments is low. Finding the C2 server of the padded x64 loaders would change both.

We treat the two SendGrid sender accounts, `u53630135` and `u48334250`, as delivery channels and grade no owner. The link of 2026-07-29 from `u53630135` delivered `20260729104357.zip` from the delivery host, and the link of 2026-08-31 from `u48334250` fed the Tencent Cloud bucket of section A4.7. A rented or compromised sender fits each link as well as the delivery party does.

A5.8 Registrants near the operation that share no value with it

Six registrants or accounts touch the operation's infrastructure, so a pivot from our indicators leads to them. We checked each one and found no value that it shares with the operation. We list them to record that check and to keep them separate from the operation. We judge it likely that each of them is separate from the operation. Confidence is low, because the eu.cc names and redacted 22net records print no registrant to compare.

- DENGHONGXIN, province ZHONGQINGSHI, took chusyiorusvo[.]club from KANGYINGJIE inside its registration (record updated 2024-08-14). Its name is on 119 domains created from 2013-06-14 to 2024-08-12, 102 of them .work company names. We assess it likely that DENGHONGXIN is a separate registrant that acquired one KANGYINGJIE domain. Confidence is low, because the differing province, portfolio and IP addresses are the only evidence.
- SUZHAOBIN, province HEBEI, appears on 1,892 records at 22net, among them a 2024 registration of karlost[.]club (2024-11-17 to 2025-11-17), a domain outside the operation. We judge it likely that SUZHAOBIN is a bulk registration string or a reseller default. Confidence is low, because the size and spread of the portfolio are the only evidence.
- The privacy relay contact chenxiansheng sits on two Japanese e-Tax lookalikes on the delivery IP address range 103.23.172[.]0/24, e-tzxarw[.]jp (103.23.172[.]118) and e-tzsgzxyu[.]jp (103.23.172[.]15), both created on 2026-09-14. We assess it very likely that the contact is a privacy service value. Confidence is moderate. It appears on no third name.
- The link domains of a July 2026 lure email, a Chinese-language email that shares no value with the operation, are a separate cluster. Four of them, with zcgbh[.]cn, came from the stock account of one seller at WebNIC. Of that account's 88 domains, 84 passed to 53 other contacts inside the same registration. We judge it very likely that the account is a seller's stock account. Confidence is moderate. The one outward value is a DNS alias (CNAME) from chboa[.]cn to v1[.]ndjwli[.]cc on 2026-07-05. That alias is a weak connection to a grey market hosting group outside the operation. chboa[.]cn's hosting front, 192.252.182[.]61, sits beside the C2 server IP address 192.252.183[.]157 in a range that carries no weight. The registrants of these domains are private contacts with no tie to the operation, so their names and mailboxes stay out of this report. The names and mailboxes of other bulk portfolio registrants, and of spbo[.]cc and 3668[.]us, domains of other customers, stay out too.
- Two other Gname accounts, 490943-1923 (fsdklhfash[.]cyou and tiktokvis[.]shop, a grey market hosting group) and 483080-1923 (two .vip names of another bulk buyer), share no value with the operation.

The five link domains of that July 2026 lure email are:

- gwsqn[.]cn
- chboa[.]cn
- cawbt[.]cn
- cunlia[.]cn
- zuaem[.]cn

A5.9 How the clusters connect

Six strong connections join groups, two more apply only inside a group, and one applies only within a 90 day window (Annex Table 23). A cluster here is a group of builds, domains or accounts that we treat together because they share values. The two explanations, one operator or a service for several customers, diverge at two gaps. Nothing that carries weight connects the KANGYINGJIE C2 domains to the ZHENGJUNHUA domains, or the padded x64 loaders to any C2 domain. At auk218[.]club, one listing outside our own records points to one operator. The listing places the domain under KANGYINGJIE, and the domain's loaders shared the delivery host with the builds for 192.252.183[.]157 and fddlbh2[.]club (section 4.1). We judge it likely that one operator, not a service for several customers, runs the KANGYINGJIE C2 domains and the delivery host's account. Confidence is low, because the judgment rests on that one listing, which prints only a name that two registrant entries use.

The six strong connections that join groups are the rows of Annex Table 23 graded Strong without the limit "inside the group" or "only within 90 days". Shared IP address ranges, lure themes and signers connect nothing, and Annex Table 23 lists them only where they matter.

Connection	Shared values	Grade	Likelihood; confidence
The kit to the C2 servers it calls	Configured C2 servers	Direct	Almost certain; high
The kit to the 15 older KANGYINGJIE domains	aeya388[.]club in the TA4922 configuration [6]	Weak, through the registrant name only	Not graded
Four KANGYINGJIE C2 domains to the 15 older ones	KANGYINGJIE; atyv788[.]club on 202.61.85[.]34 (a)	Strong, if the zone serial dates the edit	Same registrant: likely; low
Other 22net KANGYINGJIE domains, the eight names in 202.61.85[.]0/24 among them, to the C2 domains	The registrant name only	Weak	Not graded
KANGYINGJIE C2 domains to fddlbh2[.]club	The hashed registrant value and, in one stored record, the name	Weak	Same entry: very likely; moderate
KANGYINGJIE domains to ZHENGJUNHUA domains	Two shared compiles only	Toolkit facts	One operator: roughly even chance; low
The 15 older domains to CENGCHAO	202.95.19[.]243 on one day	Weak	Second name: likely; low
The 15 older domains to ze6688[.]cn	Two IP addresses within 90 days	Strong only within 90 days	In the set: roughly even chance; low
The 15 older domains to idecald[.]cn	One IP address toward the KANGYINGJIE names; one registrant contact shared with ze6688[.]cn	Weak to the set, strong to ze6688[.]cn	In the set: roughly even chance; low
Builds for 192.252.183[.]157 and fddlbh2[.]club to the delivery host	C15, B4, C17, F1 and F2 served there	Direct	Almost certain; high
fddlbh2[.]club to the operator of 192.252.183[.]157	The IP address and the delivery host	Strong, if the delivery host is one customer's	Likely; low
auk218[.]club loaders to the delivery host	16 loaders served there	Direct	Almost certain; high

Connection	Shared values	Grade	Likelihood; confidence
auk218[.]club to the KANGYINGJIE C2 domains	KANGYINGJIE in one listing; the delivery host	Strong, resting on one listing	Same operator: likely; low
ZHENGJUNHUA domains to cao[.]tedboscomwe[.]com	Package `12f496cd` served there (b)	Direct	Almost certain; high
The kit's archive naming to five other download paths	The naming scheme	Toolkit fact	Almost certain; high
usdt888[.]club to oswin[.]club and winapp[.]work	ZHENGJUNHUA (two records for oswin[.]club, one for winapp[.]work) and one shared IP address per pair	Strong; winapp[.]work rests on one record	One party: likely; low
The delivery host to the batch eu.cc names	Certificate orders and the shared IP address	Strong, to one server account	Very likely; moderate
The delivery host to 574849-1923	103.23.172[.]117 on 2026-06-30; a lure link to that host	Strong, at account level	One account or service: likely; low
The six older domains to one another	Shared IP addresses in each period	Strong, inside the group	One DNS operator: very likely; moderate
Domains of 574849-1923 on one IP address	The account and the IP address	Strong, inside the group	One customer: very likely; moderate
574849-1923 to the single eu.cc names	Same two IP addresses	Weak	Not graded
Batch eu.cc names and 574849-1923 to padded loaders	Names served them; lure links fed them	Payload facts	Almost certain; high
Padded loaders to any C2 server	None	None	C2 server operator's: unlikely; low
The link domains of a July 2026 lure email (section A5.8) to v1[.]ndjwli[.]cc	A CNAME	Weak	Not graded

Annex Table 23: How the clusters connect.

Notes to Annex Table 23:

- (a) In 2026-08.
- (b) Graded on the package's contact with usdt888[.]club (section A4.7).

A6.1 The claim, its level and its confidence

We judge it very likely that the operation belongs to the ValleyRAT activity that vendors group as Silver Fox. Confidence is moderate, because two independent kinds of evidence point the same way: the operator's choices place the operation in a Chinese-speaking environment, and the account, which sets Silver Fox apart from other Chinese-speaking ValleyRAT users, is tied to the delivery host (section 6.1). That tie rests on single events, which keeps confidence below high.

Two kinds of evidence carry the judgment. The first is the registrar account 574849-1923, a customer account at Gname (section 5.2). It registered the Indian tax lure page domains on the delivery IP address range, among them 17 of the 18 lure page domains of July and August; the 18th, zixhasda[.]xin, has no IP address on record. It also registered quidoaehse[.]icu, whose host isyraw[.]quidoaehse[.]icu Sekoia lists as Silver Fox phishing infrastructure [4], and kjfuwyce[.]love, which JUMPSEC lists as documented Silver Fox infrastructure [5]. The account's domains also shared an IP address, 103.23.172[.]117, with kaiwyrey[.]eu[.]cc. That host is the operation's delivery host, whose download links delivered the loader packages. One of the account's lure pages linked that host. The IP address and the link make a strong connection at account level, and both came before the first loader package we read there, on 2026-08-03 (sections A4.6 and 5.2):

- 2026-06-30, at the end of June: two of the account's domains and kaiwyrey[.]eu[.]cc, the delivery host, were recorded on 103.23.172[.]117; by 2026-07-01 the delivery host had moved to 103.23.172[.]118.
- 2026-07-31: one of the account's lure pages linked a download link on kaiwyrey[.]eu[.]cc.
- 2026-08-03: the delivery host served the first of its loader packages that we read, a package of the HDP loader kit, the toolkit behind all 44 loaders.

Through that host the account reaches the three builds for 192.252.183[.]157. It reaches the KANGYINGJIE C2 domains only indirectly, through two C2 domains outside the operation whose loaders the delivery host served: fddlbh2[.]club, which shares their hashed registrant value (section A4.3), and auk218[.]club, which one listing places under KANGYINGJIE (section A4.4), and usdt888[.]club not at all, so the judgment is weakest for the two usdt888[.]club builds.

The second is the operator's own choices of servers, packaging and registrations, which do not come with the public builder. They are UTC+8 packing clocks and weekday office hours, Chinese consumer programs as hosts for lures in other languages, and romanised Chinese registrant names at the Chinese registrar 22net (section A6.4). Whoever packed the files and registered the domains made these choices, so they go beyond the builder that anyone can obtain [1]. But vendors partly define Silver Fox by these traits, and they also fit a Chinese-speaking builder user outside Silver Fox, so only the account tells the two apart.

The open questions of sections A4.6 and 5.2 concern who ran each part, not whether the activity belongs to Silver Fox. The first is whether 574849-1923 is one customer's own account or a lure-hosting service. The second is whether one operator ran both the lure pages and the delivery of the builds for 192.252.183[.]157. The second question is graded unlikely (section A4.6), below the roughly even chance of the first (section A5.6). It sits lower because it needs two things at once: the account must be the operator's own, and the pages must have fed the builds. Yet every lure-linked payload we analysed is a padded x64 loader, a loader of another family

(section A4.6). Inside Silver Fox, we judge it likely that one operator, not a service for several customers, runs the KANGYINGJIE C2 domains and the delivery host's account. Confidence is low, because the judgment rests on one registration record (sections 4.3 and 5.2). The attribution rests on that account together with the operator's own choices, not on the account alone.

Three kinds of evidence support the attribution. The family is ValleyRAT. Its core matches Check Point's analysis [1], the configuration fields match CloudSEK and Proofpoint [3] [6], and the fake SDK exports match 0xdelta [17]. Our eleven builds call five .club C2 domains, the operation's four and fddlbh2[.]club. Of the 197 files that communicate with these five domains, 195 carry the antivirus family names ValleyRAT, yogi or Winos (section A3.2). The operation's tax-named packages deliver ValleyRAT, as reports of tax campaigns against India describe [3] [19] [27]. The June lure pages very likely delivered the padded x64 loaders instead (section A4.6). The files carry Chinese-language resources. Any user of the public builder would show the family and kit traits, and lure themes carry no weight. These kinds of evidence therefore support the attribution but leave the weight to the registration evidence and the operator's choices. Two traits of the kit also match Silver Fox reporting. The first is the pair of embedded kernel drivers, consistent with the driver abuse reported for Silver Fox (section A3.6), which the kit carries but never loaded in any run [7] [10]. The second is persistence through a scheduled task [18] and a watchdog script [10].

Among the sources, the claim rests on the two vendor lists that name domains of the account, Sekoia [4] and JUMPSEC [5]. CloudSEK [3], Foresiet [27] and Kaspersky [19] supply the context of Silver Fox tax lure campaigns. Reports [1], [7], [10] and [18] document the family and the kit. We make no judgment on motive, because lure themes and the core's command set fit crime and espionage alike (section A6.4).

A6.2 Public reporting on Silver Fox, ValleyRAT and TA4922

Public reporting touches our evidence in four places. Sekoia and JUMPSEC list a host and a domain of the registrar account 574849-1923 [4] [5]. CloudSEK lists lure page domains of the same account without naming it [13]. Researcher posts and an OTX pulse list C2 servers of the operation and older domains registered under the name KANGYINGJIE [14] [16]. Proofpoint published a configuration of the group it tracks as TA4922, stamped 2025.11.20 and seen in early 2026, that calls aeya388[.]club, one of the older KANGYINGJIE domains [6]. Registering a domain and deploying a configuration that calls it can be the work of different parties. We assess it likely that the operation's C2 server operator registered aeya388[.]club (section A5.4). We assess it unlikely, however, that the operation's C2 server operator and the deployer of that configuration are one operator. Confidence in both judgments is low, because the registrant name is the only value the TA4922 configuration shares with the operation, and its build date is about nine months earlier. The evidence therefore supports attribution to Silver Fox as a whole and to no named team such as TA4922.

Foresiet attributes its fake tax notice chain to Silver Fox, which it describes as a China-nexus operator of ValleyRAT [27]. NCC Group describes Silver Fox search engine optimisation (SEO) poisoning [30], and Forcepoint reports an unattributed India tax chain [34]. Proofpoint tracks TA4922, which uses Winos 4.0 against Japan, Taiwan, India and others [6]. Proofpoint claims only an "overlap in tooling, infrastructure, and social engineering themes" with activity that others report as Silver Fox or Void Arachne, another vendor name for related activity [6]. Annex Table 24 lists what each report shares with the operation.

Report	Date	Attribution as printed	Shared with the operation	Weight
CloudSEK [3]	2025-12-24	ValleyRAT; Silver Fox	Configuration fields; another `HKCU\Console\0` value name; ggwk[.]cc	Toolkit facts
NCC Group [30]	2025-12-18	ValleyRAT; Silver Fox	Two C2 servers near moik77a[.]club's IP address (a)	IP address range only
Sekoia [4]	2026-03-24	ValleyRAT and RMM tools; Silver Fox	A phishing host of 574849-1923	One value, at account level
Kaspersky [19]	2026-04-30	ABCDoor, RustSL, ValleyRAT; Silver Fox	The module name `登录模块.dll_bin`	Toolkit fact
Proofpoint [6]	2026-06-03	Winos 4.0 and others; TA4922	The TA4922 configuration calling aeya388[.]club	Weak
Seqrite [24]	2026-06-26	DcRAT; overlap with Silver Fox	`TAX/PEN/2026-142`; govtop[.]one; 118.107.0[.]197 (b)	Template text and IP address range
Cyderes [35]	2026-07-07	A Gh0st RAT derivative and a Quasar or AsyncRAT family payload; not attributed	Nothing	n/a
Foresiet [26] [27]	2026-07-02 and 2026-07-06	ValleyRAT behind an Overwolf host; Silver Fox in Part II only	`TAX/PEN/2026-142`	Template text
Cato Networks [10]	July 2026	ValleyRAT with a three driver chain; Silver Fox	`ConvertToPDF.exe` with `PDFCORE8.dll`; `BootRepair.sys`	Toolkit facts
TaxGuru [28]	2026-07-20	Not stated	`TAX/PEN/2026-142`	Template text
Forcepoint [34]	2026-08-18	ValleyRAT behind an Overwolf host; not attributed	Nothing	n/a
JUMPSEC [5]	2026-09-15	VenomRAT; PAPERMILL, plus a list of documented Silver Fox domains	kjfuwyce[.]love of 574849-1923, in the Silver Fox list	One value, at account level

Annex Table 24: Public reports reviewed and what they share with the operation.

Notes to Annex Table 24:

- (a) In the /24 range of moik77a[.]club's second IP address.
- (b) Next to auk218[.]club's 118.107.0[.]196, an IP address range fact.
- ggwk[.]cc is the domain that the tax themed PDF of CloudSEK's report opens; JUMPSEC lists it as documented Silver Fox infrastructure [5].

The reports in Annex Table 24 name no C2 server, IP address, group ID or hash of the operation. Researcher posts and an OTX pulse do name C2 servers:

- An OTX pulse named "ValleyRat", created 2026-08-24, lists the operation's four C2 domains, taku788[.]club, fuoe333[.]club, moik77a[.]club and usdt888[.]club [14]. It also lists the older KANGYINGJIE domains aeya388[.]club, aeyh688[.]club, akyv188[.]club and atyv788[.]club [14].
- A researcher named fuoe333[.]club on 2026-08-19, in a reply thread under a post tagged #ValleyRAT [15].
- Another researcher listed aeya388[.]club and shyda6319[.]club as Winos C2 servers on 202.95.1[.]227, port 7881, on 2026-01-27 [16].
- A post of 2026-09-17 names yscf988[.]club [32].
- A researcher traced hxxps://wordtax[.]ink/down/setup.appx to jpword[.]cc:8383 and 122.10.117[.]3:8383 on 2026-08-18 [29] (section A5.5).

None of them names a group ID, hash, download link code or registration record of the operation. The registration analysis that ties these servers to one another, to the delivery host and to auk218[.]club, the delivery host's earlier C2 server, is ours (sections 4.1 and A5.4). Section A6.2 lists a further researcher post.

A6.3 A program and library pair shared with a reported Silver Fox campaign

A program and library pair from a reported Silver Fox campaign appears in builds from the same kit as the operation, served from the operation's delivery host. The pair therefore supports the Silver Fox attribution as a shared tradecraft marker, not as a tie to one operator. Cato Networks reported in July 2026 a Silver Fox campaign against a Japanese industrial manufacturer [10]. The campaign's invoice lure ZIP archive holds a downloader that fetches the side-loading components. Of those components, `ConvertToPDF.exe` or `PDFDirect.exe`, both associated with Zeon Corporation, side-loads a malicious `PDFCORE8.dll`. That library embeds three drivers, `BootRepair.sys`, `EnPortv.sys` and `wsftprm.sys`.

The same pair runs through our August evidence. auk218[.]club is the earlier C2 server on the operation's delivery host. The 16 auk218[.]club loaders, packaged from 2026-08-03 to 2026-08-12, are side-loaded as `pdfCoRe8.dll` by a genuine ZEON Corporation `ConvertToPDF.exe`. Whoever packed the files changed the letter case of that library name every one to three packing days, from `PdfcOrE8.dLL` on 2026-08-03 to `pdfCoRe8.DLL` on 08-12. The build `67e1ac14` was made before the Spanish version of the cover application, the harmless Windows program each loader is built on. That version carries the U.S. Department of Homeland Security (DHS) seal as its main icon. `67e1ac14` travelled as `pdfcoRE8.DlL`, the casing of 08-09 to 08-11. It is the same compile as an auk218[.]club loader that the delivery host served on 2026-08-09. The disk image that carried `67e1ac14`, `Notice from Tax Departmen.IMG` (`6c3d59d8`), communicates with fuoe333[.]club.

The driver names agree on one point only: Cato names a driver file `BootRepair.sys`, and two of the builds we have as files (B4, F1) carry the device name `\\.\BootRepair`. Cato prints no device names or driver hashes, while `EnPortv.sys` and `wsftprm.sys` appear nowhere in our evidence. The kit's own two drivers are known by their drop paths and device names (section A3.6). The shared name is a weak connection, not a match of files.

Anyone who has the kit or copies its packaging can reuse the pair, so it identifies no operator. The library name also appears on two fuoe333[.]club builds with the DHS seal compiled 2026-08-13 03:07:11 UTC (`754c5233`, `0b7ad10b`). On packaging evidence alone, `67e1ac14` sits between the auk218[.]club loaders and fuoe333[.]club, and its configuration would show whether one compile carried both. If the configuration of `67e1ac14` calls fuoe333[.]club, shared compiles would connect all eight C2 servers that the kit's 44 builds call, seven domains and one IP address. That would still be a toolkit fact.

The misspelled lure name `Notice from Tax Departmen` runs through three sets of files:

- The tax dropper of delivery chain A (Annex Table 2), which tried to post to taku788[.]club's IP address of 2026-09-23
- The disk image that carried `67e1ac14`
- Further disk images seen with fuoe333[.]club from 2026-08-17 to 2026-08-25, the weeks of its first builds with the DHS seal (`754c5233`, `0b7ad10b`)

A lure name is a packaging trait and carries no weight, but it is the closest packaging connection between the auk218[.]club compiles and the operation.

A6.4 Where the operation sits among China-nexus threat actors

We judge it very likely that the operation runs from a Chinese-speaking environment in a UTC+8 time zone. Confidence is moderate, because any one of the markers below can be borrowed. Public reporting puts Silver Fox in two frames, crime and espionage. Proofpoint calls TA4922 a suspected Chinese crime group that is Chinese speaking and likely financially motivated, and TA4922 overlaps with activity that others call Silver Fox [6]. Check Point speaks of the "Silver Fox APT" [7]. Seqrite frames a China-nexus campaign that it overlaps with Silver Fox as espionage [24]. The vendors agree on a China nexus and disagree on motive.

Our own evidence on the operator environment comes from the files and the registration records:

- Clocks. Name stamps, the file times of the delivery host's August ISO disk image files and `bb` build stamps all run at UTC+8. All five packages whose packing time we analysed, three from the operation and two from the fddlbh2[.]club builds, were packaged on a weekday between 11:00 and 17:00 local time. Of the 28 other stamps on the delivery host, 27 fall on a weekday and 22 on a weekday between 10:00 and 17:00.
- Language. Every resource added at build time is Chinese Simplified, and five of the six 2026 versions of the cover application are Chinese. The watchdog script carries Chinese comments, and the August x86 builds except B5 carry the GBK string `默认` ("default") as their sub group tag. We assess it likely that this value is the builder default (section A3.4). Confidence is moderate.
- Domain registrations. The C2 domains are registered at the Chinese registrar 22net under registrant names in romanised Chinese. The older KANGYINGJIE domains print the province ANHUISHENG. The 2026 domains print BEIJINGSHI, but 22net also prints that value in redacted records, so it marks no location (sections A4.4 and A4.9).
- Hosts. Four of the five signers of the programs the kit reuses are Chinese companies: Guangzhou Ningjinghai, Hithink RoyalFlush, Hangzhou Fencha and Tencent. The fifth, ZEON Corporation of Taipei, appears beside the auk218[.]club loaders, outside the operation.

The builder markers, such as the tag 默认 and the Chinese Simplified tags on the resources the kit adds, travel with the public builder. The clocks, the host choice and the registrant names stay with the people who packed the files and registered the domains (section 6.1). Three markers point elsewhere, and each has a plainer reading. First, we judge it likely that the Hindi, Odia and Kannada version locales are builder settings (section A3.3). Confidence is low. Second, we assess it almost certain that the DHS seal belongs to the Spanish cover application (section A3.8). Confidence is high. Third, the registrar account 574849-1923 carries Illinois, United States on all 243 of its domains, a contact value that nothing else supports (section 6.2 and section A5.6). In this report China-nexus means only this environment reading and carries no claim of state direction.

The evidence fits crime and espionage alike. The lures are tax, VAT and account statement notices, the core's commands are standard remote control, and the live sessions registered and waited for commands. Scale points to a builder in wide use. Check Point reports that about 85 per cent of the ValleyRAT samples it detected appeared in the last six months of its study window, coinciding with the builder's public release [1]. In our evidence one kit produced 44 configurations in two months. Nothing in the evidence points to state tasking.

References

This list is the reference list of the first version of the report, kept whole so that the citation numbers in this annex stay stable. Each entry names the publisher, the authors where the source names them, the title, the date of publication and the web address, with the date we last accessed it. The one exception is [31], which gives only the entry numbers of a public indicator listing.

[1] Check Point Research, "Cracking ValleyRAT: From Builder Secrets to Kernel Rootkits", 2025-12-10, https://research.checkpoint.com/2025/cracking-valleyrat-from-builder-secrets-to-kernel-rootkits/ (accessed 2026-10-16).

[2] Zscaler ThreatLabz, Muhammed Irfan V A and Manisha Ramcharan Prajapati, "Technical Analysis of the Latest Variant of ValleyRAT", 2024-06-10, https://www.zscaler.com/blogs/security-research/technical-analysis-latest-variant-valleyrat (accessed 2026-10-16).

[3] CloudSEK, Prajwal Awasthi and Koushik Pal, "Silver Fox Targeting India Using Tax Themed Phishing Lures", 2025-12-24, https://www.cloudsek.com/blog/silver-fox-targeting-india-using-tax-themed-phishing-lures (accessed 2026-10-16).

[4] Sekoia, Pierre Le Bourhis and Coline C., "Silver Fox: The Only Tax Audit Where the Fine Print Installs Malware", 2026-03-24, https://www.sekoia.com/blog/silver-fox-the-only-tax-audit-where-the-fine-print-installs-malware (accessed 2026-10-16).

[5] JUMPSEC, Jack Lewis, "PAPERMILL: Tracking an Emerging China-Nexus Malware Factory", 2026-09-15, https://www.jumpsec.com/guides/an-emerging-silver-fox-like-cluster-papermill/ (accessed 2026-10-16).

[6] Proofpoint Threat Research Team, "TA4922: The Suspected Chinese Crime Group is Going Global", 2026-06-03, https://www.proofpoint.com/us/blog/threat-insight/ta4922-suspected-chinese-crime-group-going-global (accessed 2026-10-16).

[7] Check Point Research, "Chasing the Silver Fox: Cat & Mouse in Kernel Shadows", 2025-08-28, https://research.checkpoint.com/2025/silver-fox-apt-vulnerable-drivers/ (accessed 2026-10-16).

[8] Huntress, Anna Pham, "From W-2 to BYOVD: How a Tax Search Leads to Kernel-Mode AV/EDR Kill", 2026-03-19, https://www.huntress.com/blog/w2-malvertising-to-kernel-mode-edr-kill (accessed 2026-10-16).

[9] skybreaker (Zenn), "HwAudKiller: research", 2026-03-27, https://zenn.dev/skybreaker/articles/e2fea6a2e3a62e (accessed 2026-10-16).

[10] Cato Networks (Cato CTRL), Tomer Pugach, Guy Waizel, Zohar Buber, Idan Tarab and Shani Kurtzberg, "Cato CTRL Threat Research: SilverFox Evolves: Abuse of New Drivers and Trusted Software Hijacking Enable Remote Access with ValleyRAT in Japan", 2026-07-28, https://www.catonetworks.com/blog/cato-ctrl-silverfox-evolves/ (accessed 2026-10-31).

[11] Nextron Systems Valhalla, MalGamy, Sigma rule "Potential ArphaDump64.DLL Sideloading", 2025-03-24, https://valhalla.nextron-systems.com/info/sigma-rule/9803ed55-1410-4b61-a370-17f5e8ef7639 (accessed 2026-10-16).

[12] Malwarebytes, Stefan Dasic, blog post, 2026-02-23, https://www.malwarebytes.com/blog/scams/2026/02/huorong (accessed 2026-10-16).

[13] CloudSEK, "Tax Season, Open Season: Phishing and Malware Campaigns Targeting Indian Taxpayers", 2026-07-30, https://www.cloudsek.com/blog/tax-season-open-season-phishing-and-malware-campaigns-targeting-indian-taxpayers (accessed 2026-10-18).

[14] AlienVault OTX, skocherhan, pulse "ValleyRat", 2026-08-24, https://otx.alienvault.com/pulse/6a8ba897394c80ba11a19c90 (accessed 2026-10-20).

[15] ExpectedErr0r, reply on X naming fuoe333[.]club, in a thread under a post tagged #ValleyRAT, 2026-08-19, https://x.com/ExpectedErr0r/status/2090011242547261839 (accessed 2026-10-20).

[16] skocherhan, post on X listing Winos C2 servers, 2026-01-27, https://x.com/skocherhan/status/2015938127060230501 (accessed 2026-10-18).

[17] 0xdelta, Operator 0x_OLYMPUS, "Technical Analysis: ValleyRAT Delivered via Trojanized DingTalk Downloader and NVIDIA DLL Sideloading", undated (logged 2026-07-17), https://0xdelta.org/blog/blue-team/malware-analysis-reverse-engineering/valleyrat/ (accessed 2026-10-16).

[18] Nextron Systems, Maurice Fielenbach, "Thor vs. Silver Fox: Uncovering and Defeating a Sophisticated ValleyRat Campaign", 2025-11-28, https://www.nextron-systems.com/2025/11/28/thor-vs-silver-fox-uncovering-and-defeating-a-sophisticated-valleyrat-campaign/ (accessed 2026-10-16).

[19] Kaspersky Securelist, Anton Kargin, Vladimir Gursky, Victoria Vlasova and Anna Lazaricheva, "Analyzing the Silver Fox tax campaign and the new ABCDoor backdoor", 2026-04-30, https://securelist.com/silver-fox-tax-notification-campaign/119575/ (accessed 2026-10-16).

[20] Office of the Director of National Intelligence, "Intelligence Community Directive 203: Analytic Standards", signed 2015-01-02, with technical amendments of 2022-01-21 and 2023-06-12, https://archive.dni.gov/files/documents/ICD/ICD-203.pdf (accessed 2026-10-16).

[21] BlackSnufkin, "BYOVD", a public GitHub collection of BYOVD proof of concept tools, https://github.com/BlackSnufkin/BYOVD (accessed 2026-10-15).

[22] biubiu, biubiu加速器 official site, https://www.biubiu001.com/?lang=zh-CN (accessed 2026-09-30).

[23] Xiaomi app store, biubiu加速器 (`com.njh.biubiu`), https://app.mi.com/details?id=com.njh.biubiu (accessed 2026-09-30).

[24] Seqrite Labs, Dixit Panchal and Soumen Burma, "Operation DragonReturn: China-Nexus Cyber Espionage Campaign Targeting Govt. of India/MoF Tax Infrastructure via Multi-Stage DcRAT Deployment", 2026-06-26, https://www.seqrite.com/blog/operation-dragonreturn-china-nexus-cyber-espionage-campaign-targeting-govt-of-india-mof-tax-infrastructure-via-multi-stage-dcrat-deployment/ (accessed 2026-10-16).

[25] Gname, the eu.cc registration product page, https://www.gname.com/tld-eu-cc.html (accessed 2026-10-14).

[26] Foresiet, "Fake Tax Notice Phishing: Inside the Multi-Country Network Target" (title as listed), Part I, 2026-07-02, https://foresiet.com/blog/fake-tax-notice-phishing-network/ (accessed 2026-10-16).

[27] Foresiet, "Fake Tax Notice Campaign: ValleyRAT Loader Unmasked (Part II)", 2026-07-06, https://foresiet.com/blog/fake-tax-notice-campaign-valleyrat-unmasked/ (accessed 2026-10-16).

[28] TaxGuru, CA Sandeep Kanoi, "Beware of Fake Income Tax Penalty Notice on Email", 2026-07-20, https://taxguru.in/income-tax/beware-fake-income-tax-penalty-notice-email.html (accessed 2026-10-16).

[29] bomccss, post on X tracing a setup.appx download to its C2 servers, 2026-08-18, https://x.com/bomccss/status/2089549529335140762 (accessed 2026-10-18).

[30] NCC Group, Dillon Ashmore and Asher Glue, "Black Hole of Trust: SEO Poisoning in Silver Fox's Space Odyssey", 2025-12-18, https://www.nccgroup.com/research-blog/black-hole-of-trust-seo-poisoning-in-silver-fox-s-space-odyssey/ (accessed 2026-10-16).

[31] A public indicator listing, IOC entries 1780193 and 1784236 (accessed 2026-10-16).

[32] skocherhan, post on X naming yscf988[.]club, 2026-09-17, https://x.com/skocherhan/status/2100678596784189589 (accessed 2026-10-20).

[33] tdatwja, post on X on a Japanese-language email lure that links to dnswwt[.]club, 2026-09-15, https://x.com/tdatwja/status/2099730099537141922 (accessed 2026-10-20).

[34] Forcepoint X-Labs, Raghu Ram, "Signed Overwolf Binary Sideloads ValleyRAT Malware in India Tax Scam", 2026-08-18, https://www.forcepoint.com/blog/x-labs/valleyrat-overwolf-sideload-tax-scam (accessed 2026-10-16).

[35] Cyderes Howler Cell, Reegun Jayapaul, Baskar M and Rahul Ramesh, "The Tax Trap: From Fake Indian ITR Notice to Dual RAT Deployment in Six Stages", 2026-07-07, https://www.cyderes.com/howler-cell/fake-indian-itr-notice-dual-rat-deployment (accessed 2026-10-16).

TLP:CLEAR