MALICIOUS

Classifications: Downloader

Threat Names: C2/Generic-A | Emotet | Mal/HTMLGen-A | Mal/Generic-S

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**9f8b5f5da718fafb98de9b2128cd81fd720a37de6c755b81965ead358aeb912a.xlsx.xls**
ID	#7435904
MD5	ae72f6016f8929c7780693cadfb855ef
SHA1	bda7fd78150a0103f3c2281d90074332ccfa8cde
SHA256	9f8b5f5da718fafb98de9b2128cd81fd720a37de6c755b81965ead358aeb912a
File Size	89.00 KB
Report Created	2023-04-15 19:45 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (19 rules, 155 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Emotet configuration was extracted	1	Downloader
	• A configuration for Emotet was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Downloader
	• Rule "EmotetFunctionStrings" from ruleset "Malware" has matched on the function strings for (process #5) regsvr32.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #4) regsvr32.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Local\ABeIsdLaCr\hsBpWPNj.dll".			
4/5	Network Connection	Downloads executable	1	Downloader
	• (Process #1) excel.exe downloads Windows executable via http from hxxp://www[.]chawkyfrenn[.]com/icon/JtT/.			
4/5	Network Connection	Attempts to connect through HTTP	6	-
	• (Process #1) excel.exe connects to hxxp://chillpassion[.]com/wp-content/nd4wjKgokzKbKH0DQDD/. • (Process #5) regsvr32.exe connects to hxxps://45[.]118[.]115[.]99:8080. • (Process #1) excel.exe connects to hxxp://bruidsfotografie-breda[.]nl/cache/QPk/. • (Process #1) excel.exe connects to hxxp://www[.]chawkyfrenn[.]com/icon/JtT/. • (Process #5) regsvr32.exe connects to hxxps://172[.]105[.]226[.]75:8080. • (Process #5) regsvr32.exe connects to hxxps://206[.]189[.]28[.]199:8080.			
4/5	Network Connection	Attempts to connect through HTTPS	5	-
	• (Process #5) regsvr32.exe connects to hxxps://213[.]239[.]212[.]5. • (Process #5) regsvr32.exe connects to hxxps://144[.]91[.]78[.]55. • (Process #1) excel.exe connects to hxxps://chiptochip[.]es/alojamiento-web/dofwXVVQ3hvsp/. • (Process #5) regsvr32.exe connects to hxxps://135[.]148[.]6[.]80. • (Process #5) regsvr32.exe connects to hxxps://45[.]55[.]191[.]130.			
4/5	Network Connection	Connects to a CMS hoster	1	-
	• (Process #1) excel.exe connects to a hosted Wordpress site at hxxp://chillpassion[.]com/wp-content/nd4wjKgokzKbKH0DQDD/.			
4/5	Execution	Document contains suspicious Office macros which are executed automatically	1	-
	• c:\users\rdhj0cnfevzx\desktop\9f8b5f5da718fafb98de9b2128cd81fd720a37de6c755b81965ead358aeb912a.xlsx.xls contains deprecated Office macros which are executed on AUTO_OPEN.			
4/5	Execution	Document tries to create process	4	-
	• Document creates (process #6) regsvr32.exe. • Document creates (process #7) regsvr32.exe. • Document creates (process #2) regsvr32.exe. • Document creates (process #3) regsvr32.exe.			
4/5	Reputation	Known malicious file	2	-
	• The sample itself is a known malicious file. • Reputation analysis labels embedded file "kq8j1ZAN2Ug.dll" as Mal/Generic-S.			

Score	Category	Operation	Count	Classification
4/5	Reputation	Contacts known malicious URL	11	-

- Reputation analysis labels the URL "hxxp://chillpassion[.]com/wp-content/nd4wjKgokzKbKH0DQDD/" which was contacted by (process #1) excel.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxps://213[.]239[.]212[.]5" which was contacted by (process #5) regsvr32.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxps://45[.]118[.]115[.]99:8080" which was contacted by (process #5) regsvr32.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxps://144[.]91[.]78[.]55" which was contacted by (process #5) regsvr32.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxp://bruidsfotografie-breda[.]nl/cache/QPk/" which was contacted by (process #1) excel.exe as Mal/HTMLGen-A.
- Reputation analysis labels the contacted URL "hxxps://bruidsfotografie-breda[.]nl/cache/QPk/" as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxp://www[.]chawkyfrenn[.]com/icon/JtT/" which was contacted by (process #1) excel.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxps://172[.]105[.]226[.]75:8080" which was contacted by (process #5) regsvr32.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxps://chiptochip[.]es/alojamiento-web/dofwXVVQ3hvsp/" which was contacted by (process #1) excel.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "hxxps://206[.]189[.]28[.]199:8080" which was contacted by (process #5) regsvr32.exe as C2/Generic-A.
- Reputation analysis labels the URL "hxxps://45[.]55[.]191[.]130" which was contacted by (process #5) regsvr32.exe as Mal/HTMLGen-A.

Score	Category	Operation	Count	Classification
4/5	Reputation	Resolves known malicious domain	3	-

- Reputation analysis labels the resolved domain "www.chawkyfrenn.com" as Mal/HTMLGen-A.
- Reputation analysis labels the resolved domain "bruidsfotografie-breda.nl" as Mal/HTMLGen-A.
- Resolved domain "chillpassion.com" is a known malicious domain.

Score	Category	Operation	Count	Classification
4/5	Reputation	File has embedded malicious URL	12	-

- Embedded URL "hxxp://chillpassion[.]com/wp-content/.../bootstrap-front.css?ver=6.0.3" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/wp-content/.../beautiful-taxonomy-filters-base.min.css?ver=2.4.3" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/xmlrpc.php" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/wp-includes/css/dist/block-library/style.min.css?ver=6.0.3" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/wp-content/.../select2.min.css?ver=2.4.3" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/wp-content/.../counter-column.css?ver=6.0.3" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com//wp-includes//js//wp-emoji-release.min.js?ver=6.0.3" is a known malicious URL.
- Embedded URL "hxxps://chillpassion[.]com/comments/feed/" is a known malicious URL.
- Embedded URL "hxxps://chillpassion[.]com/feed/" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/wp-content/plugins/foobox-image-lightbox/free/css/foo" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/wp-content/.../font-awesome.min.css?ver=6.0.3" is a known malicious URL.
- Embedded URL "hxxp://chillpassion[.]com/wp-content/uploads/2019/09/logo.png" is a known malicious URL.

Score	Category	Operation	Count	Classification
3/5	Discovery	Enumerates running processes	2	-

- (Process #4) regsvr32.exe enumerates running processes.
- (Process #5) regsvr32.exe enumerates running processes.

Score	Category	Operation	Count	Classification
2/5	Network Connection	Allows invalid SSL certificates	1	-

- (Process #5) regsvr32.exe allows network connections with an invalid SSL certificate.

Score	Category	Operation	Count	Classification
2/5	Network Connection	URL indicates a CMS hoster	100	-

• URL hxxps://olargo[.]pt/wp-content/.../public-powerkit-coming-soon.css?ver=2.8.6 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-includes/css/dashicons.min.css?ver=6.2 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/.../public-powerkit-lazyload.css?ver=2.8.6 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/.../public-powerkit-basic-elements.js?ver=4.0.0 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2022/01/cropped-favicon-32x32.png embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../media_screen.css?ver=1 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/.../public-powerkit-share-buttons.css?ver=2.8.6 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/up...22-12-16-00-17-46-utc-80x46.jpg embedded in document None is hosted by Wordpress.
• URL hxxp://chillpassion[.]com/wp-content/.../bootstrap-front.css?ver=6.0.3 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/04/Copia-de-o-largo.-_-Livro-de-Estilo-1.png embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/themes/startkit/js/wow.min.js?ver=7a22247de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/plugins/sight/render/css/sight-lightbox.css?ver=1651501830 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-includes/css/classic-themes.min.css?ver=6.2 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../datepicker_smoothness.css?ver=1 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-...7de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/upl...22-10-31-21-30-05-utc-380x220.jpg embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../cookie-law-info-gdpr.css?ver=3.0.8 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-includes/css/dist/block-library/style.min.css?ver=6.2 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/.../public-powerkit-instagram.css?ver=2.8.6 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-i...47de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-includes/css/classic-themes.min.css?ver=7a22247de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2017/07/20519291_kZsYZ1-80x46.png embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-includes//js//wp-emoji-release.min.js?ver=6.2 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/02/tarik-t0NjFdoajx4-unsplash-380x220.jpg embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../date_picker.js?ver=1 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/themes/startkit/js/bootstrap.min.js?ver=4.3.1 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/03/Manteau-credito-Joao-Berberan-jpg-webp-80x46.webp embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/02/unnamed-2-jpg-webp-380x220.webp embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/plugins/post-views-counter/css/frontend.min.css?ver=1.3.12 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2022/01/Design-sem-nome-2-380x220.png embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/themes/startkit/images/404robot.png embedded in document None is hosted by Wordpress.
• URL hxxp://chillpassion[.]com/wp-content/.../beautiful-taxonomy-filters-base.min.css?ver=2.4.3 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../custom-script.js?ver=1 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/04/flag-of-russia-2022-11-16-21-05-41-utc-80x80.jpg embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/plugin....js?ver=7a22247de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/themes/startkit/js/skip-link-focus-fix.js?ver=20151215 embedded in document None is hosted by Wordpress.
• URL hxxp://chillpassion[.]com/wp-includes/css/dist/block-library/style.min.css?ver=6.0.3 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/04/porto-80x80.jpg embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/plugins/widget-options/assets/css/widget-options.css embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../intlTelInput.js?ver=7a22247de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/.../public-powerkit-facebook.css?ver=2.8.6 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/plugins/powerkit/modules/lightbox/public/js/glightbox.min.js?ver=2.8.6 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/03/jana-shnipelson-AUVH9wcQhFU-unsplash-80x46.jpg embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../font-awesome.min.css?ver=7a22247de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/.../glightbox.min.css?ver=2.8.6 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2023/03/Adicionar-um-titulo-jpg-webp-80x46.webp embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/.../1401090723532071026549684-e1679667674870-jpg-webp-80x46.webp embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/uploads/2022/02/21122321_7WSyh-jpeg-webp-200x140.webp embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../swiper.min.js?ver=7a22247de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../style_03.css?ver=1 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../intlTelInput.css?ver=1 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-includes/wlwmanifest.xml embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es//wp-admin//admin-ajax.php embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-content/.../jquery-confirm.min.js?ver=7a22247de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxp://chillpassion[.]com/wp-content/.../select2.min.css?ver=2.4.3 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-c...47de8db3271f3bf8573be10e986 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-content/plugins/searchwp-live-ajax-search/assets/styles/style.css?ver=1.7.4 embedded in document None is hosted by Wordpress.
• URL hxxps://olargo[.]pt/wp-includes/js/imagesloaded.min.js?ver=4.1.4 embedded in document None is hosted by Wordpress.
• URL hxxps://chiptochip[.]es/wp-includes/js/jquery/ui/core.min.js?ver=1.13.2 embedded in document None is hosted by Wordpress.

Score	Category	Operation	Count	Classification
2/5	Defense Evasion	Loads a dropped DLL	1	-
	• (Process #4) regsvr32.exe loads dropped DLL phdg2.ocx.			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a macro in legacy format.			
1/5	YARA	Content matched by YARA rules	1	-
	• Rule "JS_Unicode_escaped_bytes" from ruleset "Generic" has matched on script.			

Malware Configuration: Emotet

	Url	https://172.104.251.154:8080
	Url	https://51.161.73.194:443
	Url	https://101.50.0.91:8080
	Url	https://91.207.28.33:8080
	Url	https://119.193.124.41:7080
	Url	https://150.95.66.124:8080
	Url	https://103.132.242.26:8080
	Url	https://37.187.115.122:8080
	Url	https://172.105.226.75:8080
	Url	https://131.100.24.231:80
	Url	https://196.218.30.83:443
	Url	https://79.137.35.198:8080
	Url	https://103.75.201.2:443
	Url	https://82.223.21.224:8080
	Url	https://153.126.146.25:7080
	Url	https://146.59.226.45:443
	Url	https://209.97.163.214:443
	Url	https://186.194.240.217:443
	Url	https://197.242.150.244:8080
	Url	https://45.118.115.99:8080
	Url	https://201.94.166.162:443
	Url	https://159.65.88.10:8080
	Url	https://213.239.212.5:443
	Url	https://167.172.253.162:8080
	Url	https://183.111.227.137:8080
	Url	https://207.148.79.14:8080
	Url	https://188.44.20.25:443
	Url	https://185.4.135.165:8080
	Url	https://82.165.152.127:8080
	Url	https://64.227.100.222:8080
	Url	https://163.44.196.120:8080
URL	Url	https://173.212.193.249:8080
	Url	https://115.68.227.76:8080
	Url	https://107.170.39.149:8080
	Url	https://72.15.201.15:8080
	Url	https://51.254.140.238:7080
	Url	https://206.189.28.199:8080
	Url	https://45.176.232.124:443
	Url	https://144.91.78.55:443
	Url	https://159.65.140.115:443
	Url	https://160.16.142.56:8080
	Url	https://51.91.76.89:8080
	Url	https://103.43.75.120:443
	Url	https://46.55.222.11:443
	Url	https://94.23.45.86:4143
	Url	https://149.56.131.28:8080
	Url	https://213.241.20.155:443
	Url	https://164.68.99.3:8080
	Url	https://209.126.98.206:8080
	Url	https://129.232.188.93:443
	Url	https://45.55.191.130:443
	Url	https://103.70.28.102:8080
	Url	https://5.9.116.246:8080
	Url	https://139.59.126.41:443
	Url	https://151.106.112.196:8080
	Url	https://134.122.66.193:8080
	Url	https://212.24.98.99:8080

Mitre ATT&CK Matrix

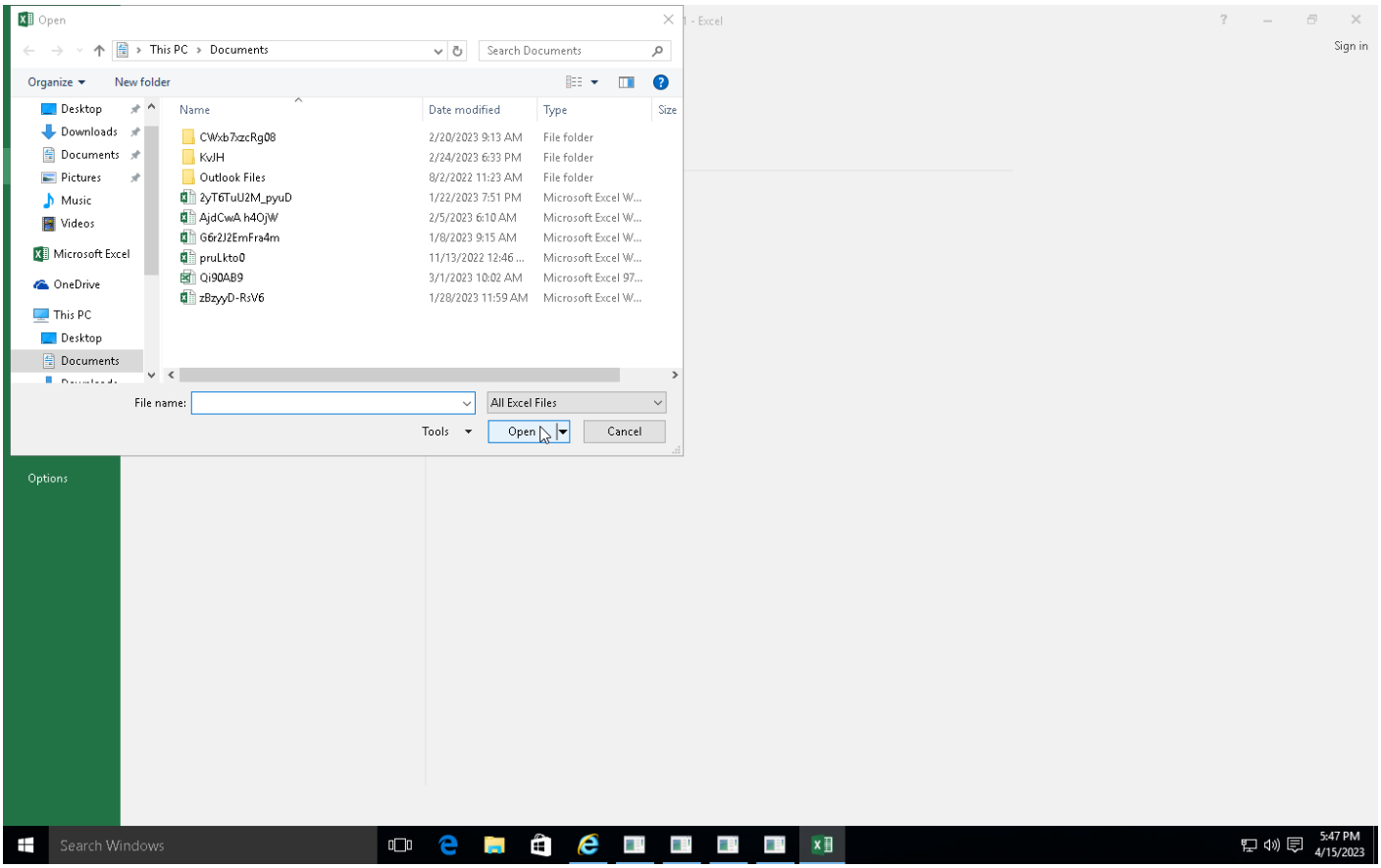
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1096 NTFS File Attributes		#T1057 Process Discovery	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
	#T1204 User Execution			#T1064 Scripting					#T1105 Remote File Copy		
	#T1059 Command-Line Interface								#T1032 Standard Cryptographic Protocol		

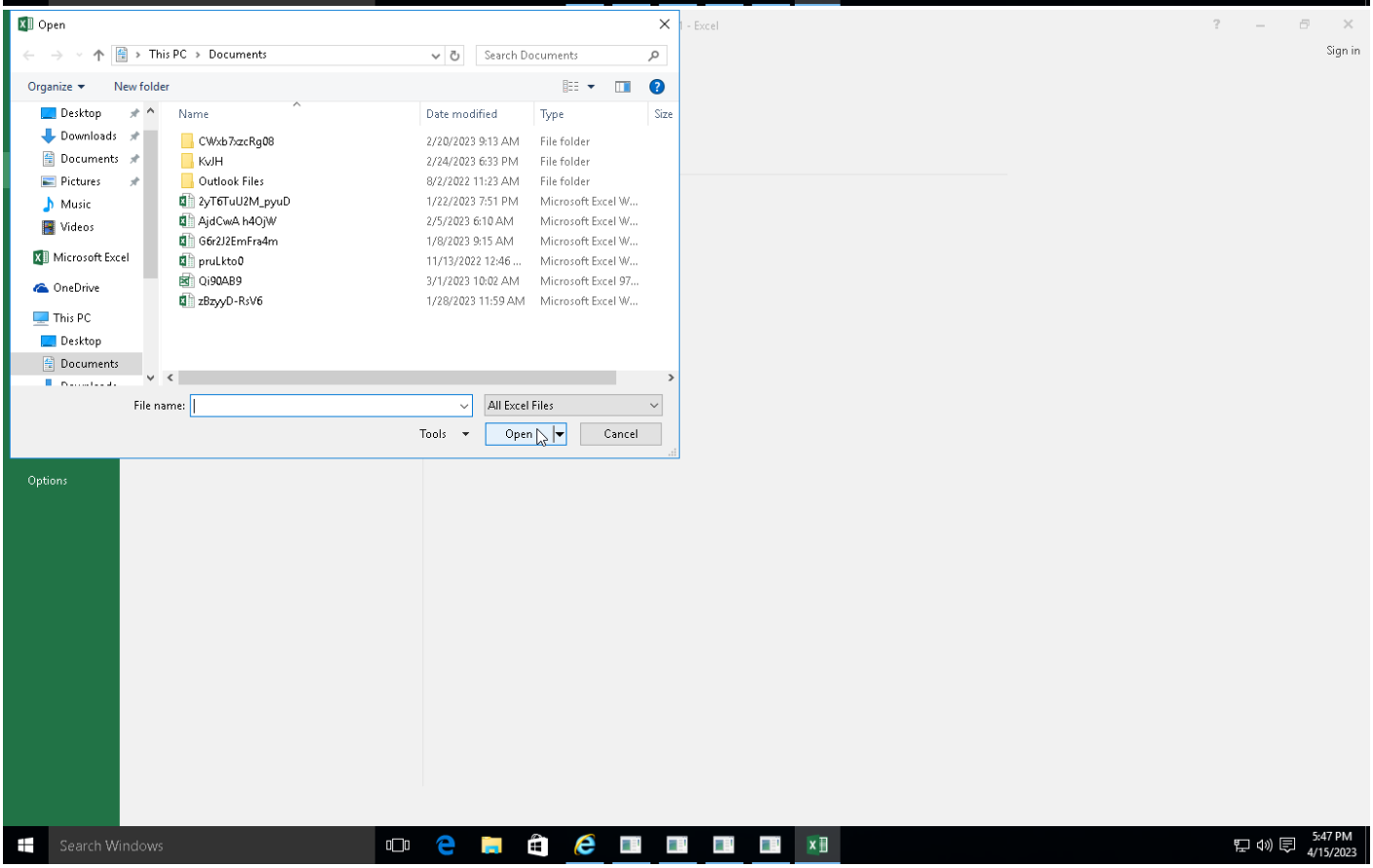
Sample Information

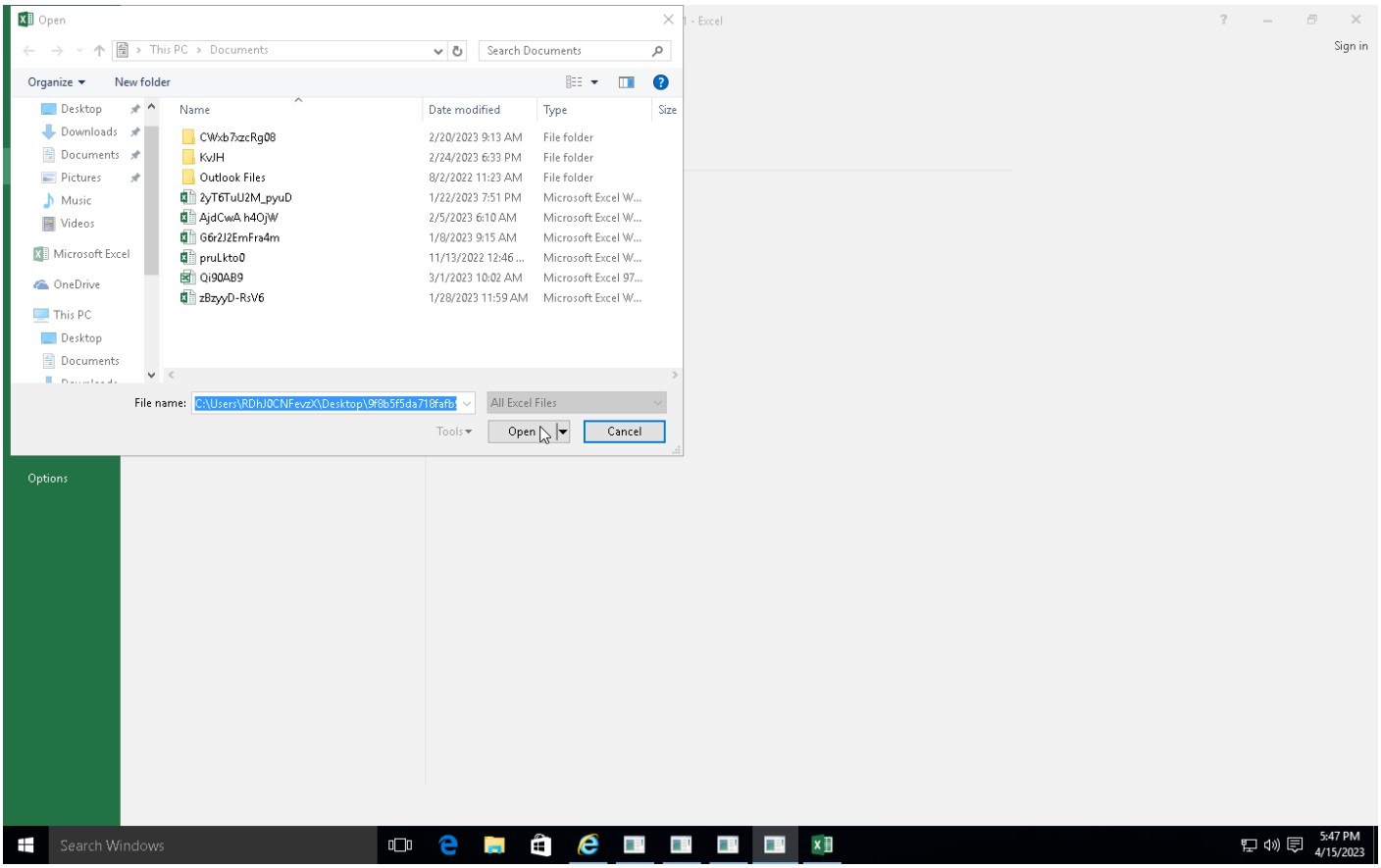
ID	#7435904
MD5	ae72f6016f8929c7780693cadfb855ef
SHA1	bda7fd78150a0103f3c2281d90074332ccfa8cde
SHA256	9f8b5f5da718fafb98de9b2128cd81fd720a37de6c755b81965ead358aeb912a
SSDeep	1536:n6k3hOdsylKlgxopeiBNhZFGzE+cL2kdAdHuS4lcTO9Tv7UYdEJi9a2:6k3hOdsylKlgxopeiBNhZFGzE+cL2kd7
File Name	9f8b5f5da718fafb98de9b2128cd81fd720a37de6c755b81965ead358aeb912a.xlsx.xls
File Size	89.00 KB
Sample Type	Excel Document
Has Macros	✔

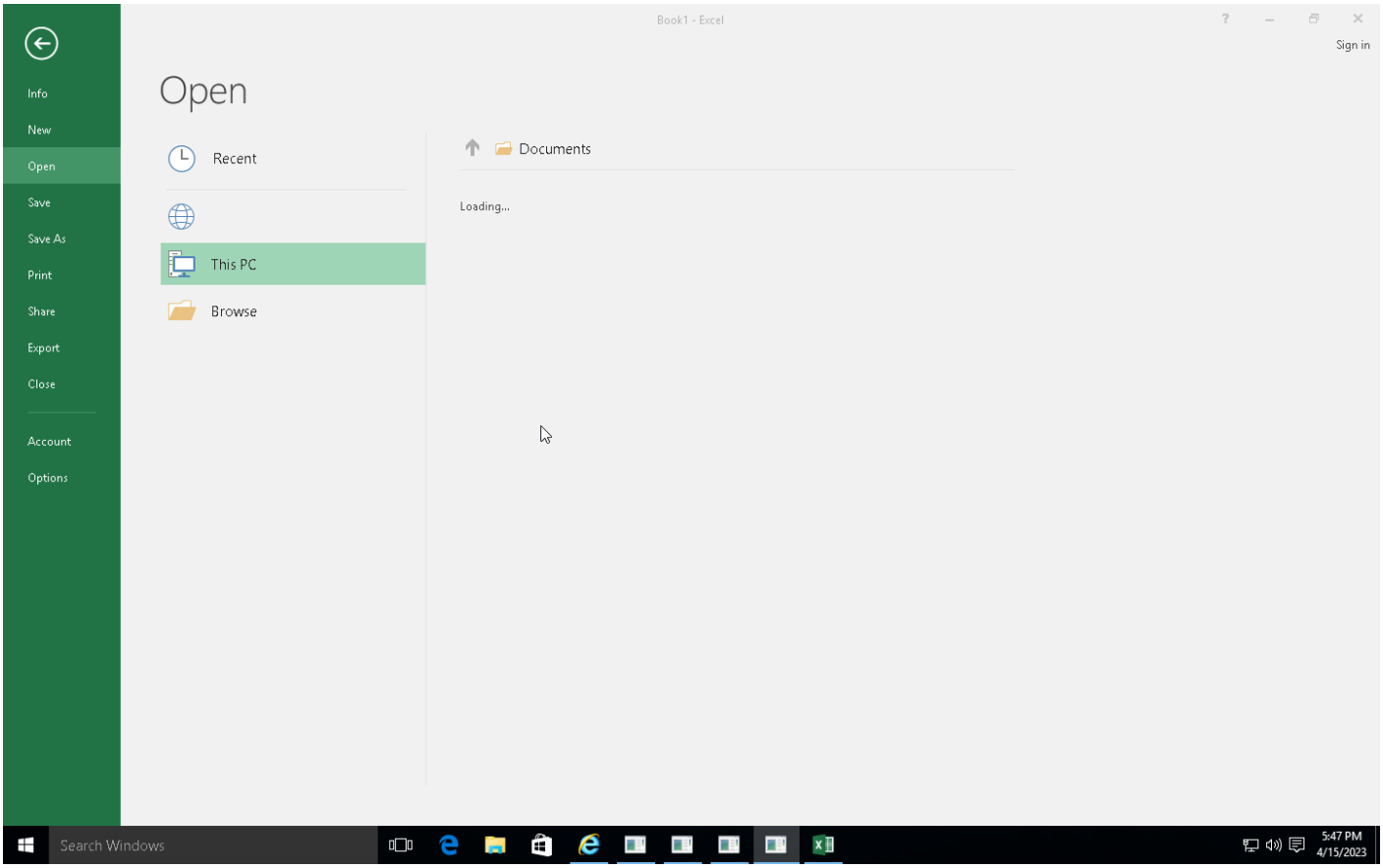
Analysis Information

Creation Time	2023-04-15 19:45 (UTC+2)
Analysis Duration	00:03:04
Termination Reason	Timeout
Number of Monitored Processes	7
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	3


Open
This PC › Documents
Search Documents
Organize
New folder
Desktop
Downloads
Documents
Pictures
Music
Videos
Microsoft Excel
OneDrive
This PC
Desktop
Documents
Name
Date modified
Type
Size
CWxb7vzcRg08 2/20/2023 9:13 AM File folder
KvJH 2/24/2023 6:33 PM File folder
Outlook Files 8/2/2022 11:23 AM File folder
2yT6TuU2M_pyuD 1/22/2023 7:51 PM Microsoft Excel W...
AjdCwA h4OjW 2/5/2023 6:10 AM Microsoft Excel W...
G6r2J2EmFra4m 1/8/2023 9:15 AM Microsoft Excel W...
pruLkto0 11/13/2022 12:46 ... Microsoft Excel W...
Qi90AB9 3/1/2023 10:02 AM Microsoft Excel 97...
zBzyyD-RsV6 1/28/2023 11:59 AM Microsoft Excel W...
File name:
All Excel Files
Tools
Open
Cancel
Options
Sign in
Search Windows
5:47 PM
4/15/2023


Open
This PC › Documents
Search Documents
Organize
New folder
Desktop
Downloads
Documents
Pictures
Music
Videos
Microsoft Excel
OneDrive
This PC
Desktop
Documents
Name
Date modified
Type
Size
CWxb7vzcRg08 2/20/2023 9:13 AM File folder
KvJH 2/24/2023 6:33 PM File folder
Outlook Files 8/2/2022 11:23 AM File folder
2yT6TuU2M_pyuD 1/22/2023 7:51 PM Microsoft Excel W...
AjdCwA h4OjW 2/5/2023 6:10 AM Microsoft Excel W...
G6r2J2EmFra4m 1/8/2023 9:15 AM Microsoft Excel W...
pruLkto0 11/13/2022 12:46 ... Microsoft Excel W...
Qi90AB9 3/1/2023 10:02 AM Microsoft Excel 97...
zBzyyD-RsV6 1/28/2023 11:59 AM Microsoft Excel W...
File name:
All Excel Files
Tools
Open
Cancel
Options
Sign in
Search Windows
5:47 PM
4/15/2023





Screenshots truncated

NETWORK

General

11.73 KB total sent

741.29 KB total received

4 ports 80, 8080, 443, 53

13 contacted IP addresses

415 URLs extracted

7 files downloaded

0 malicious hosts detected

DNS

5 DNS requests for 5 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

9 URLs contacted, 8 servers

9 sessions, 8.98 KB sent, 737.11 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://www[.]chawkyfrenn[.]com/icon/JtT/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]googletagmanager[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://chillpassion[.]com//wp-includes//js//wp-emoji-release.min.js?ver=6.0.3	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/xmlrpc.php	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/nd4wjKgokzKbKH0DQDD/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/plugins/counter-number-showcase/assets/css/bootstrap-front.css?ver=6.0.3	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/plugins/counter-number-showcase/assets/css/font-awesome/css/font-awesome.min.css?ver=6.0.3	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-includes/css/dist/block-library/style.min.css?ver=6.0.3	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/plugins/counter-number-showcase/assets/css/counter-column.css?ver=6.0.3	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/plugins/beautiful-taxonomy-filters/public/css/select2.min.css?ver=2.4.3	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/plugins/beautiful-taxonomy-filters/public/css/beautiful-taxonomy-filters-base.min.css?ver=2.4.3	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/uploads/2019/09/logo.png	-	-	-	0 bytes	MALICIOUS
GET	hxxp://chillpassion[.]com/wp-content/plugins/foobox-image-lightbox/free/css/foo	-	-	-	0 bytes	MALICIOUS
GET	hxxp://s[.]w[.]org	-	-	-	0 bytes	CLEAN
GET	hxxp://use[.]fontawesome[.]com	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://secure[.]gravatar[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://assets[.]pinterest[.]com/js/pinit.js?ver=6.2	-	-	-	0 bytes	CLEAN
GET	hxxp://i0[.]wp[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://pagead2[.]googlesyndication[.]com/pagead/js/adsbygoogle.js?ver=6.2	-	-	-	0 bytes	CLEAN
GET	hxxp://pagead2[.]googlesyndication[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://bruidsfotografie-breda[.]nl/cache/QPk/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://v0[.]wordpress[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://gmpg[.]org/xfn/11	-	-	-	0 bytes	CLEAN
GET	hxxp://fonts[.]googleapis[.]com/css?family=Open+Sans%3A300%2C400%2C600%2C700%2C800%7CRaleway%3A400%2C700&subset=latin%2Clatin-ext	-	-	-	0 bytes	CLEAN
GET	hxxp://fonts[.]googleapis[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es//wp-admin//admin.php?page=twb_form-maker	-	-	-	0 bytes	CLEAN
GET	hxxps://facebook[.]com/olargopt	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=O%20OpenAI%20%C3%A9%20preconceituoso%3F%20N%C3%B3s%20fomos%20verificar&via=olargopt&url=https://olargo.pt/2023/03/o-openai-e-preconceituoso-nos-fomos-verificar/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=Manteau%20lan%C3%A7a%20single%20%E2%80%9CFunny%20Hand%E2%80%9D&via=olargopt&url=https://olargo.pt/2023/03/manteau-lanca-single-funny-hand/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=Jornalista%20bielorrusso%20da%20RFE%2FRL%20Ihar%20Losik%C2%A0pode%20estar%20na%20solit%C3%A1ria&via=olargopt&url=https://olargo.pt/2023/03/jornalista-bielorrusso-da-rfe-rl-ihar-losik-pode-estar-na-solitaria/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=Boa%20P%C3%A1scoa%21&via=olargopt&url=https://olargo.pt/2023/04/boa-pascoa/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=Arcos%20de%20Valdevez%3A%20%E2%80%9CBois%20da%20P%C3%A1scoa%E2%80%9D%20est%C3%A3o%20de%20regresso&via=olargopt&url=https://olargo.pt/2023/03/arcos-de-valdevez-bois-da-pascoa-estao-de-regresso/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=CNID%20considera%20%E2%80%9Csem%20sentido%E2%80%9D%20atitude%20de%20Cristiano%20Ronaldo%20de%20n... ...argopt&url=https://olargo.pt/2023/03/cnid-considera-sem-sentido-atitude-de-cristiano-ronaldo-de-nao-responder-a-perguntas-da-cmtv/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=Ge%C3%B3rgia%20debate%20uma%20lei%20de%20agente%20estrangeiro%2C%20que%20os%20cr%C3%ADticos%20di... ...l=https://olargo.pt/2023/03/georgia-debate-uma-lei-de-agente-estrangeiro-que-os-criticos-dizem-estabelecer-um-precedente-perigoso/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/olargopt	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=Diogo%20Pi%C3%A7arra%20disponibiliza%20concerto%20no%20YouTube&via=olargopt&url=https://olargo.pt/2023/03/diogo-picarra-disponibiliza-concerto-no-youtube/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=IPCA%20assinala%20dia%20do%20Estudante%20com%20emiss%C3%A3o%20experimental%20de%20televis%C3%A3o&via=olargopt&url=https://olargo.pt/2023/03/ipca-assinala-dia-do-estudante-com-emissao-experimental-de-televisao/	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://twitter[.]com/share?&text=Intelig%C3%AAncia%20Intergeracional&via=olargopt&url=https://olargo.pt/2023/03/inteligencia-intergeracional/	-	-	-	0 bytes	CLEAN
GET	hxxps://twitter[.]com/share?&text=o%20largo.%20lan%C3%A7a%20iniciativa%20%E2%80%9CFake%20News%20n%C3%A3o%20s%C3%A3o%20uma%20mentirinha%E2%80%9D&via=olargopt&url=https://olargo.pt/2023/04/o-largo-lanca-iniciativa-fake-news-nao-sao-uma-mentirinha/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]googletagmanager[.]com/gtag/js?id=UA-188584285-1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es//wp-admin//admin-ajax.php	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es//wp-json//	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/diogo-picarra-disponibiliza-concerto-no-youtube/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/georgia-debate-uma-lei-de-agente-estrangeiro-que-os-criticos-dizem-estabelecer-um-precedente-perigoso/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/inteligencia-intergeracional/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/arcos-de-valdevez-bois-da-pascoa-estao-de-regresso/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/04/o-largo-lanca-iniciativa-fake-news-nao-sao-uma-mentirinha/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/04/boa-pascoa/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/ipca-assinala-dia-do-estudante-com-emissao-experimental-de-televisao/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/jornalista-bielorrusso-da-rfe-rl-ihar-losik-pode-estar-na-solitaria/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/o-openai-e-preconceituoso-nos-fomos-verificar/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/manteau-lanca-single-funny-hand/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/ChipToChipRuzafa/	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]facebook[.]com/sharer.php?u=https://olargo.pt/2023/03/cnid-considera-sem-sentido-atitude-de-cristiano-ronaldo-de-nao-responder-a-perguntas-da-cmtv/	-	-	-	0 bytes	CLEAN
GET	hxxps://chillpassion[.]com/feed/	-	-	-	0 bytes	MALICIOUS
GET	hxxps://chillpassion[.]com/comments/feed/	-	-	-	0 bytes	MALICIOUS
GET	hxxps://cdnjs[.]cloudflare[.]com/ajax/libs/animate.css/4.1.1/animate.min.css	-	-	-	0 bytes	CLEAN
GET	hxxps://cdnjs[.]cloudflare[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://www[.]viralagenda[.]com/pt/w/?theme=1&color=444444&font=5&preview=1	-	-	-	0 bytes	CLEAN
GET	hxxps://sobescuta[.]olargo[.]pt	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/feed/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/wp-test.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/media_screen.css?ver=1	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://chiptochip[.]es/gestion-copias-de-seguridad/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=5.7.5.1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/servicios-informaticos/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/bootstrap.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/datepicker_smoothness.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/form-maker/booster/assets/css/global.css?ver=1.0.0	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/font-awesome.min.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar/shortcode/frontend/contact/intlTelInput.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?ver=5.7.5.1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/form-maker/booster/assets/js/circle-progress.js?ver=1.2.2	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/reparacion-de-ordenadores/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/colors/default.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/cookie-law-info/legacy/public/css/cookie-law-info-public.css?ver=3.0.8	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/jquery/jquery.min.js?ver=3.6.3	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/xmlrpc.php?rsd	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/contact/intlTelInput.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.7.5.1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/fonts/font-awesome/css/font-awesome.min.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/form-maker/booster/assets/js/global.js?ver=1.0.0	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/jetpack/css/jetpack.css?ver=12.0	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/js/jquery-migrate-1.4.1.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/swiper.min.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.11	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/cookie-law-info/legacy/public/css/cookie-law-info-gdpr.css?ver=3.0.8	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/style.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://chiptochip[.]es/mantenimiento-informatico-empresas/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/js/jquery.sticky.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/widget.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/jquery.preloader.min.js?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/jquery/ui/core.min.js?ver=1.13.2	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/posicionamiento-web/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-json/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/bootstrap.min.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/jetpack/_inc/build/photon/photon.min.js?ver=20191001	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//js/confirmation/jquery-confirm.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//js/confirmation/jquery-confirm.min.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/responsive.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/meanmenu.min.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/menu.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/animate.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/js/skip-link-focus-fix.js?ver=20151215	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/style_03.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/adaptacion-lopd-lssice/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/css/gutenberg.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/js/jquery.meanmenu.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/alojamiento-web-o-hosting/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/mediaelement/mediaelementplayer-legacy.min.css?ver=4.2.17	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/css/dist/block-library/style.min.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/asistencia-tecnica-remota/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/custom-script.js?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/js/custom.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.0	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/css/classic-themes.min.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/examples.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/images/404robot.png	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/alertbox/notify.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/mantenimiento-web/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/comments/feed/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/swiper.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.7.5.1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/clever-fox//inc/assets/css/owl.carousel.min.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/mediaelement/wp-mediaelement.min.css?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/diseno-desarrollo-de-software/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-includes/js/dist/vendor/wp-polyfill-inert.min.js?ver=3.1.2	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/js/bootstrap.min.js?ver=4.3.1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/clever-fox/inc/assets/js/owl.carousel.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/cookie-law-info/legacy/public/js/cookie-law-info-public.js?ver=3.0.8	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/themes/startkit/js/wow.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/bootstrap.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/blog/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/alojamiento-web/dofwXVVQ3hvsp/	-	-	-	0 bytes	MALICIOUS
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/alertbox/notify.css?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/contacto/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/traducciones-de-paginas-web/	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/como-configurar	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/date_picker.js?ver=1	-	-	-	0 bytes	CLEAN
GET	hxxps://olrg[.]pt/N2bFc	-	-	-	0 bytes	CLEAN
GET	hxxps://bilheteira[.]olargo[.]pt	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es//wp-content//plugins//form-maker//booster	-	-	-	0 bytes	CLEAN
GET	hxxps://stats[.]wp[.]com/e-202315.js	-	-	-	0 bytes	CLEAN
GET	hxxps://206[.]189[.]28[.]199:8080	-	-	-	0 bytes	MALICIOUS

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://use[.]fontawesome[.]com/releases/v6.2.1/css/v4-shims.css	-	-	-	0 bytes	CLEAN
GET	hxxps://use[.]fontawesome[.]com/releases/v6.2.1/css/all.css	-	-	-	0 bytes	CLEAN
GET	hxxps://secure[.]gravatar[.]com/avatar/8a4c0723d207b4e04d16c2fc69f90040?s=40&d=mm&r=g	-	-	-	0 bytes	CLEAN
GET	hxxps://chiptochip[.]es//wp-includes//js//wp-emoji-release.min.js?ver=7a22247de8db3271f3bf8573be10e986	-	-	-	0 bytes	CLEAN

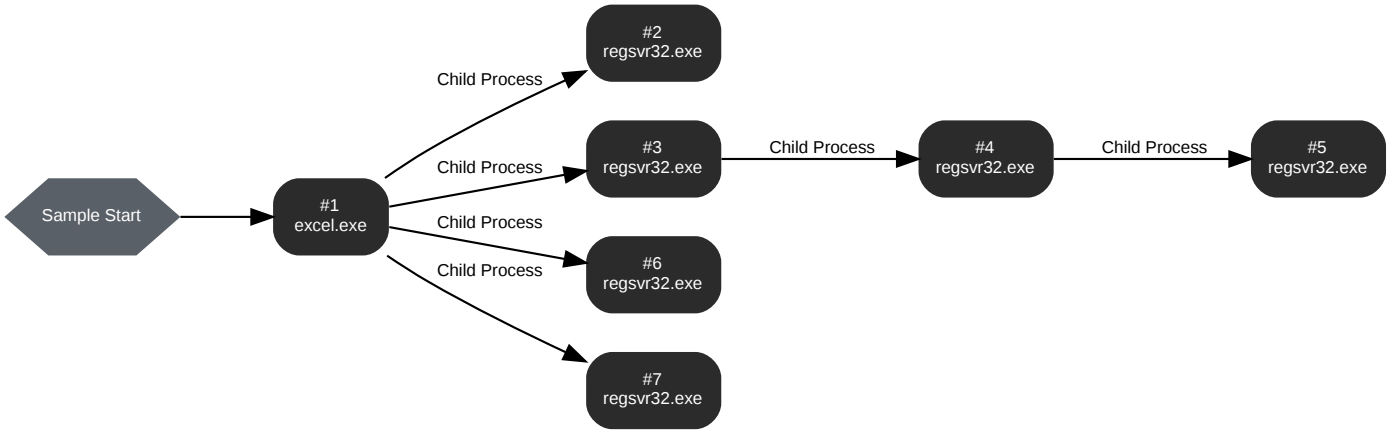
Reduced dataset

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www[.]chawkyfrenn[.]com	NO_ERROR	50.116.62.25	-	MALICIOUS
A	olargo[.]pt	NO_ERROR	172.67.149.202, 104.21.29.205	-	CLEAN
A	chiptochip[.]es	NO_ERROR	185.186.169.202	-	CLEAN
A	bruidsfotografie-breda[.]nl	NO_ERROR	141.138.168.131	-	MALICIOUS
A	chillpassion[.]com	NO_ERROR	172.81.116.81	-	MALICIOUS

BEHAVIOR

Process Graph



Process #1: excel.exe

ID	1
File Name	c:\program files (x86)\microsoft office\office16\excel.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 139157, Reason: Analysis Target
Unmonitor End Time	End Time: 317019, Reason: Terminated by timeout
Monitor duration	177.86s
Return Code	Unknown
PID	4368
Parent PID	1900
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	425.00 KB	4d7ccf2bba4cbce46dc8d694eed0894985fd494e47f846e88fe23e714aa42e59	✖

Host Behavior

Type	Count
File	4
Process	8

Network Behavior

Type	Count
HTTP	3
HTTPS	1

Process #2: regsvr32.exe

ID	2
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	C:\Windows\System32\regsvr32.exe /S ..\phdg1.ocx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 171072, Reason: Child Process
Unmonitor End Time	End Time: 173171, Reason: Terminated
Monitor duration	2.10s
Return Code	3
PID	2924
Parent PID	4368
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
Registry	4

Process #3: regsvr32.exe

ID	3
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	C:\Windows\System32\regsvr32.exe /S ..\phdg2.ocx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 172742, Reason: Child Process
Unmonitor End Time	End Time: 180576, Reason: Terminated
Monitor duration	7.83s
Return Code	0
PID	4336
Parent PID	4368
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
Registry	4
File	3
System	2
Process	2

Process #4: regsvr32.exe

ID	4
File Name	c:\windows\system32\regsvr32.exe
Command Line	/S ..\phdg2.ocx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 173172, Reason: Child Process
Unmonitor End Time	End Time: 180141, Reason: Terminated
Monitor duration	6.97s
Return Code	0
PID	4296
Parent PID	4336
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\ABeIsdLaCr\hsBpWPNj.dll	425.00 KB	4d7ccf2bba4cbce46dc8d694eed0894985fd494e47f846e88fe23e714aa42e59	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	63
Registry	4
Environment	1
File	5
System	1
-	1
Process	110

Process #5: regsvr32.exe

ID	5
File Name	c:\windows\system32\regsvr32.exe
Command Line	C:\Windows\system32\regsvr32.exe "C:\Users\RDhJ0CNFevzX\AppData\Local\ABelsdLaCr\hsBpWPNj.dll"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 178728, Reason: Child Process
Unmonitor End Time	End Time: 317019, Reason: Terminated by timeout
Monitor duration	138.29s
Return Code	Unknown
PID	4512
Parent PID	4296
Bitness	64 Bit

Host Behavior

Type	Count
Module	62
Registry	4
Environment	1
File	3
System	5
-	1
Process	208
-	2
-	3

Network Behavior

Type	Count
HTTPS	7
TCP	4

Process #6: regsvr32.exe

ID	6
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	C:\Windows\System32\regsvr32.exe /S ..\phdg3.ocx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 180539, Reason: Child Process
Unmonitor End Time	End Time: 182656, Reason: Terminated
Monitor duration	2.12s
Return Code	3
PID	4504
Parent PID	4368
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
Registry	4

Process #7: regsvr32.exe

ID	7
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	C:\Windows\System32\regsvr32.exe /S ..\phdg4.ocx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 182765, Reason: Child Process
Unmonitor End Time	End Time: 186277, Reason: Terminated
Monitor duration	3.51s
Return Code	3
PID	4692
Parent PID	4368
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
Registry	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b9aef465af8e18ce913c45694fbbe554dc3b9a458f49b31d42816690cd3667d6	-	Downloaded File	13.67 KB	text/html	-	MALICIOUS
9f8b5f5da718fafb98de9b2128cd81fd720a37de6c755b81965ead358aeb912a	-	Sample File	89.00 KB	application/vnd.ms-excel	-	MALICIOUS
4d7ccf2bba4cbce46dc8d694eed0894985fd494e47f846e88fe23e714aa42e59	..\phdg2.ocx, C:\Users\RDhJ0CNFevzX\phdg2.ocx, C:\Users\RDhJ0CNFevzX\AppData\Local\ABelsdLaCr\hsBpWPNj.dll, C:\Users\RDhJ0CNFevzX\...\...LaCr\hsBpWPNj.dll, kq8j1ZAN2Ug.dll, c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\w3uuzswb\kq8j1zan2ug[1].dll	Downloaded File	425.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	MALICIOUS
88a1fb3ac6c0faa1b9736e5457c7e2de760943c7b80cddb975c08312053320ed	-	Script	2.11 KB	text/javascript	-	MALICIOUS
2a26a6535a92432445939de8c1ff3bfaa13adf7a17aea516329cf7a21a666a0b	-	Downloaded File	1.35 KB	text/html	-	CLEAN
ad2bd75548ce0d24c11e7c32958e9e2895498a201a2a6e07bee97be6ab95f965	-	Downloaded File	258 bytes	text/html	-	CLEAN
6f9159dd495adce554a6e33c55bb68f08443f0bce367abdd0ca4f3febe5c5f2e	-	Script	2.10 KB	text/javascript	-	CLEAN
a96203cccb1fef3241553c27997760690e88f3dcb72c6285ad32a67c08a70ba3	-	Downloaded File	118.26 KB	text/html	-	CLEAN
134db74c5397b3acd1db5c9662beeba7560174480be1209fb8936b3cc77bd384	0.JPG	Extracted File	28.68 KB	image/jpeg	-	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
3c2372105968ad6c9e37bb8e4ddd3b2a53efb3c3bd230a6aaa28dd383144d410	-	Downloaded File	184.64 KB	text/html	-	CLEAN
eb34459a86aa008f87f2c7b56820b15f8e593bb0337badf6f782dea92946ff86	-	Downloaded File	140 bytes	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\9f8b5f5da718fafb98de9b2128cd81fd720a37de6c755b81965ead358aeb912a.xlsx.xls	Sample File	-	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\w3uuzswb\kq8j1zan2ug[1].dll	Downloaded File, Extracted File	-	CLEAN
..\phdg2.ocx	Accessed File, Downloaded File, Extracted File	Access, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\ABelsdLaCr\hsBpWPNj.dll:Zone.Identifier	Accessed File	Access, Delete	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
c:\srvsvc	Dropped File, Modified File	-	CLEAN

File Name	Category	Operations	Verdict
..\phdg1.ocx	Accessed File	Access, Create	CLEAN
..\phdg3.ocx	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\ABeIsdLaCr\hsBpWPNj.dll	Miscellaneous File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\ABeIsdLaCr\hsBpWPNj.dll	Accessed File, Downloaded File, Extracted File	Access, Create, Write	CLEAN
C:\Windows\system32\regsvr32.exe	Accessed File	Access	CLEAN
..\phdg4.ocx	Accessed File	Access, Create	CLEAN
kq8j1ZAN2Ug.dll	Downloaded File	-	CLEAN
0.JPG	Miscellaneous File	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://201[.]94[.]166[.]162	Extracted	201.94.166.162	-	-	MALICIOUS
hxxps://209[.]97[.]163[.]214	Extracted	209.97.163.214	-	-	MALICIOUS
hxxps://37[.]187[.]115[.]122:8080	Extracted	37.187.115.122	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/plugins/counter-number-showcase/assets/css/bootstrap-front.css?ver=6.0.3	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://150[.]95[.]66[.]124:8080	Extracted	150.95.66.124	-	-	MALICIOUS
hxxps://167[.]172[.]253[.]162:8080	Extracted	167.172.253.162	-	-	MALICIOUS
hxxps://134[.]122[.]66[.]193:8080	Extracted	134.122.66.193	-	-	MALICIOUS
hxxps://115[.]68[.]227[.]76:8080	Extracted	115.68.227.76	-	-	MALICIOUS
hxxps://101[.]50[.]0[.]91:8080	Extracted	101.50.0.91	-	-	MALICIOUS
hxxps://158[.]69[.]222[.]101	Extracted	158.69.222.101	-	-	MALICIOUS
hxxps://51[.]91[.]76[.]89:8080	Extracted	51.91.76.89	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/nd4wjKgokzKbKH0DQDD/	Extracted, Contacted	172.81.116.81	United States	GET	MALICIOUS
hxxps://196[.]218[.]30[.]83	Extracted	196.218.30.83	-	-	MALICIOUS
hxxps://139[.]59[.]126[.]41	Extracted	139.59.126.41	-	-	MALICIOUS
hxxps://149[.]56[.]131[.]28:8080	Extracted	149.56.131.28	-	-	MALICIOUS
hxxps://153[.]126[.]146[.]25:7080	Extracted	153.126.146.25	-	-	MALICIOUS
hxxps://172[.]105[.]226[.]75:8080	Extracted	172.105.226.75	Japan	-	MALICIOUS
hxxps://209[.]126[.]98[.]206:8080	Extracted	209.126.98.206	-	-	MALICIOUS
hxxps://164[.]68[.]99[.]3:8080	Extracted	164.68.99.3	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/plugins/beautiful-taxonomy-filters/public/css/beautiful-taxonomy-filters-base.min.css?ver=2.4.3	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxp://chillpassion[.]com/xmlrpc.php	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://151[.]106[.]112[.]196:8080	Extracted	151.106.112.196	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-includes/css/dist/block-library/style.min.css?ver=6.0.3	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://82[.]223[.]21[.]224:8080	Extracted	82.223.21.224	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://183[.]111[.]227[.]137:8080	Extracted	183.111.227.137	-	-	MALICIOUS
hxxps://103[.]43[.]75[.]120	Extracted	103.43.75.120	-	-	MALICIOUS
hxxps://45[.]235[.]8[.]30:8080	Extracted	45.235.8.30	-	-	MALICIOUS
hxxps://110[.]232[.]117[.]186:8080	Extracted	110.232.117.186	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/plugins/beautiful-taxonomy-filters/public/css/select2.min.css?ver=2.4.3	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://82[.]165[.]152[.]127:8080	Extracted	82.165.152.127	-	-	MALICIOUS
hxxps://119[.]193[.]124[.]41:7080	Extracted	119.193.124.41	-	-	MALICIOUS
hxxps://144[.]91[.]78[.]55	Extracted, Contacted	144.91.78.55	Germany	GET	MALICIOUS
hxxps://159[.]65[.]140[.]115	Extracted	159.65.140.115	-	-	MALICIOUS
hxxps://72[.]15[.]201[.]15:8080	Extracted	72.15.201.15	-	-	MALICIOUS
hxxps://146[.]59[.]226[.]45	Extracted	146.59.226.45	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/plugins/counter-number-showcase/assets/css/counter-column.css?ver=6.0.3	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://163[.]44[.]196[.]120:8080	Extracted	163.44.196.120	-	-	MALICIOUS
hxxp://chillpassion[.]com//wp-includes//js//wp-emoji-release.min.js?ver=6.0.3	Extracted	-	-	-	MALICIOUS
hxxp://bruidsfotografie-breda[.]nl/cache/QPk/	Extracted, Contacted	141.138.168.131	Netherlands	GET	MALICIOUS
hxxps://207[.]148[.]79[.]14:8080	Extracted	207.148.79.14	-	-	MALICIOUS
hxxps://188[.]44[.]20[.]25	Extracted	188.44.20.25	-	-	MALICIOUS
hxxps://1[.]234[.]2[.]232:8080	Extracted	1.234.2.232	-	-	MALICIOUS
hxxps://bruidsfotografie-breda[.]nl/cache/QPk/	Extracted, Contacted	141.138.168.131	Netherlands	GET	MALICIOUS
hxxps://131[.]100[.]24[.]231:80	Extracted	131.100.24.231	-	-	MALICIOUS
hxxps://159[.]89[.]202[.]34	Extracted	159.89.202.34	-	-	MALICIOUS
hxxps://chillpassion[.]com/comments/feed/	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxp://www[.]chawkyfrenn[.]com/icon/JtT/	Extracted, Contacted	50.116.62.25	United States	GET	MALICIOUS
hxxps://45[.]118[.]115[.]99:8080	Extracted	45.118.115.99	Indonesia	-	MALICIOUS
hxxps://186[.]194[.]240[.]217	Extracted	186.194.240.217	-	-	MALICIOUS
hxxps://160[.]16[.]142[.]56:8080	Extracted	160.16.142.56	-	-	MALICIOUS
hxxps://213[.]239[.]212[.]5	Extracted, Contacted	213.239.212.5	Germany	GET	MALICIOUS
hxxps://213[.]241[.]20[.]155	Extracted	213.241.20.155	-	-	MALICIOUS
hxxps://79[.]137[.]35[.]198:8080	Extracted	79.137.35.198	-	-	MALICIOUS
hxxps://103[.]75[.]201[.]2	Extracted	103.75.201.2	-	-	MALICIOUS
hxxps://103[.]70[.]28[.]102:8080	Extracted	103.70.28.102	-	-	MALICIOUS
hxxps://172[.]104[.]251[.]154:8080	Extracted	172.104.251.154	-	-	MALICIOUS
hxxps://5[.]9[.]116[.]246:8080	Extracted	5.9.116.246	-	-	MALICIOUS
hxxps://197[.]242[.]150[.]244:8080	Extracted	197.242.150.244	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://103[.]132[.]242[.]26:8080	Extracted	103.132.242.26	-	-	MALICIOUS
hxxps://129[.]232[.]188[.]93	Extracted	129.232.188.93	-	-	MALICIOUS
hxxps://chiptochip[.]es/alojamiento-web/dofwXVVQ3hvsp/	Extracted, Contacted	185.186.169.202	Spain	GET	MALICIOUS
hxxps://chillpassion[.]com/feed/	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/plugins/foobox-image-lightbox/free/css/foo	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://51[.]161[.]73[.]194	Extracted	51.161.73.194	-	-	MALICIOUS
hxxps://64[.]227[.]100[.]222:8080	Extracted	64.227.100.222	-	-	MALICIOUS
hxxps://212[.]24[.]98[.]99:8080	Extracted	212.24.98.99	-	-	MALICIOUS
hxxps://185[.]4[.]135[.]165:8080	Extracted	185.4.135.165	-	-	MALICIOUS
hxxps://94[.]23[.]45[.]86:4143	Extracted	94.23.45.86	-	-	MALICIOUS
hxxps://159[.]65[.]88[.]10:8080	Extracted	159.65.88.10	-	-	MALICIOUS
hxxps://107[.]170[.]39[.]149:8080	Extracted	107.170.39.149	-	-	MALICIOUS
hxxps://51[.]254[.]140[.]238:7080	Extracted	51.254.140.238	-	-	MALICIOUS
hxxps://45[.]176[.]232[.]124	Extracted	45.176.232.124	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/plugins/counter-number-showcase/assets/css/font-awesome/css/font-awesome.min.css?ver=6.0.3	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://173[.]212[.]193[.]249:8080	Extracted	173.212.193.249	-	-	MALICIOUS
hxxps://46[.]55[.]222[.]11	Extracted	46.55.222.11	-	-	MALICIOUS
hxxp://chillpassion[.]com/wp-content/uploads/2019/09/logo.png	Extracted	172.81.116.81	United States	-	MALICIOUS
hxxps://91[.]207[.]28[.]33:8080	Extracted	91.207.28.33	-	-	MALICIOUS
hxxps://45[.]55[.]191[.]130	Extracted	45.55.191.130	United States	-	MALICIOUS
hxxps://206[.]189[.]28[.]199:8080	Extracted	206.189.28.199	United Kingdom	-	MALICIOUS
hxxps://www[.]instagram[.]com/chiptochip	Extracted	-	-	-	CLEAN
hxxps://olargo[.]pt/wp-content/plugins/powerkit/modules/coming-soon/public/css/public-powerkit-coming-soon.css?ver=2.8.6	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxp://fonts[.]googleapis[.]com/css?family=Open+Sans%3A300%2C400%2C600%2C700%2C800%7CRaleway%3A400%2C700&subset=latin%2Clatin-ext	Extracted	-	-	-	CLEAN
hxxp://www[.]googletagmanager[.]com	Extracted	-	-	-	CLEAN
hxxps://olargo[.]pt/radio/airplay40-chart/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/temas/institucional/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-includes/css/dashicons.min.css?ver=6.2	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/page/33/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/plugins/powerkit/modules/lazyload/public/css/public-powerkit-lazyload.css?ver=2.8.6	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/2023/03/inteligencia-intergeracional/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://olargo[.]pt/wp-content/plugins/powerkit/modules/basic-elements/public/js/public-powerkit-basic-elements.js?ver=4.0.0	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2022/01/cropped-favicon-32x32.png	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/media_screen.css?ver=1	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://chiptochip[.]es/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://olargo[.]pt/wp-content/plugins/powerkit/modules/share-buttons/public/css/public-powerkit-share-buttons.css?ver=2.8.6	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/author/brunomicaelfernandes/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/03/family-generation-green-eyes-genetics-concept-2022-12-16-00-17-46-utc-80x46.jpg	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/2023/04/o-largo-lanca-iniciativa-fake-news-nao-sao-uma-mentirinha/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/sobre/comentarios/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/04/Copia-de-o-largo.-_-Livro-de-Estilo-1.png	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-content/themes/startkit/js/wow.min.js?ver=7a22247de8db3271f3bf8573be10e986	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://twitter[.]com/share?&text=Arcos%20de%20Valdevez%3A%20%E2%80%9CBois%20da%20P%C3%A1scoa%E2%80%9D%20est%C3%A3o%20de%20regresso&via=olargopt&url=https://olargo.pt/2023/03/arcos-de-valdevez-bois-da-pascoa-estao-de-regresso/	Extracted	-	-	-	CLEAN
hxxps://olargo[.]pt/wp-content/plugins/sight/render/css/sight-lightbox.css?ver=1651501830	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/2023/03/arcos-de-valdevez-bois-da-pascoa-estao-de-regresso/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-includes/css/classic-themes.min.css?ver=6.2	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/datepicker_smoothness.css?ver=1	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://www[.]instagram[.]com/p/Cqfrqfco4zR/	Extracted	-	-	-	CLEAN
hxxps://chiptochip[.]es/wp-content/themes/startkit/css/gutenberg.css?ver=7a22247de8db3271f3bf8573be10e986	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://chiptochip[.]es/comments/feed/	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://twitter[.]com/share?&text=Boa%20P%C3%A1scoa%21&via=olargopt&url=https://olargo.pt/2023/04/boa-pascoa/	Extracted	-	-	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/01/smiling-robot-assistant-with-artificial-intelligen-2022-10-31-21-30-05-utc-380x220.jpg	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-content/plugins/cookie-law-info/legacy/public/css/cookie-law-info-gdpr.css?ver=3.0.8	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://olargo[.]pt/2023/04/alijo-recria-via-dolorosa/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/temas/artes-palcos/cinema/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-includes/css/dist/block-library/style.min.css?ver=6.2	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://assets[.]pinterest[.]com/js/pinit.js?ver=6.2	Extracted	-	-	-	CLEAN
hxxps://olargo[.]pt/wp-content/plugins/powerkit/modules/instagram/public/css/public-powerkit-instagram.css?ver=2.8.6	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-includes/css/dist/block-library/style.min.css?ver=7a22247de8db3271f3bf8573be10e986	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://olargo[.]pt/author/webmasterolargo-pt/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-includes/css/classic-themes.min.css?ver=7a22247de8db3271f3bf8573be10e986	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://olargo[.]pt/author/marta-pimenta-de-brito/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2017/07/20519291_kZsYZ1-80x46.png	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt//wp-includes//js//wp-emoji-release.min.js?ver=6.2	Extracted	-	-	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/02/tarik-t0NjFdoajx4-unsplash-380x220.jpg	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt	Extracted, Contacted	172.67.149.202, 104.21.29.205	United States	GET	CLEAN
hxxps://www[.]linkedin[.]com/company/chip-to-chip	Extracted	-	-	-	CLEAN
hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/date_picker.js?ver=1	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://www[.]instagram[.]com/p/CpezAZLIFhh/	Extracted	-	-	-	CLEAN
hxxps://chiptochip[.]es/wp-content/themes/startkit/js/bootstrap.min.js?ver=4.3.1	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://olargo[.]pt/temas/especiais/cultura-ciencia-e-tecnologia-na-imprensa/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/2023/01/chatgpt-e-trendy-e-viral-quero/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/03/Manteau-credito-Joao-Berberan-jpg-webp-80x46.webp	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/02/unnamed-2-jpg-webp-380x220.webp	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/temas/media/televisao/streaming/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/plugins/post-views-counter/css/frontend.min.css?ver=1.3.12	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/2023/02/tvi-ficcao-e-tvi-reality-chegam-a-vodafone/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2022/01/Design-sem-nome-2-380x220.png	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/sobre/privacidade/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/mantenimiento-informatico-empresas/	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://chiptochip[.]es/wp-content/themes/startkit/images/404robot.png	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/custom-script.js?ver=1	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/04/flag-of-russia-2022-11-16-21-05-41-utc-80x80.jpg	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/js/jquery-migrate-1.4.1.min.js?ver=7a22247de8db3271f3bf8573be10e986	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://www[.]instagram[.]com/p/CphXNYQonEH/	Extracted	-	-	-	CLEAN
hxxps://olargo[.]pt/temas/especiais/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/sobre/fichatecnica/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-content/themes/startkit/js/skip-link-focus-fix.js?ver=20151215	Extracted	185.186.169.202	Spain	-	CLEAN
hxxps://olargo[.]pt/wp-content/uploads/2023/04/porto-80x80.jpg	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/wp-content/plugins/widget-options/assets/css/widget-options.css	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://olargo[.]pt/temas/artes-palcos/congressos-eventos/	Extracted	172.67.149.202, 104.21.29.205	United States	-	CLEAN
hxxps://chiptochip[.]es/wp-content/plugins/appointment-scheduler-weblizar//shortcode/frontend/contact/intlTelInput.js?ver=7a22247de8db3271f3bf8573be10e986	Extracted	185.186.169.202	Spain	-	CLEAN

Reduced dataset

Domain

Domain	IP Address	Country	Protocols	Verdict
www[.]chawkyfrenn[.]com	50.116.62.25	United States	TCP, DNS, HTTP	MALICIOUS
bruidsfotografie-breda[.]nl	141.138.168.131	Netherlands	TCP, HTTPS, DNS, HTTP	MALICIOUS
chillpassion[.]com	172.81.116.81	United States	TCP, DNS, HTTP	MALICIOUS
bilheteira[.]olargo[.]pt	-	-	-	CLEAN
i0[.]wp[.]com	-	-	-	CLEAN
twitter[.]com	-	-	-	CLEAN
sobescuta[.]olargo[.]pt	-	-	-	CLEAN
chiptochip[.]es	185.186.169.202	Spain	TCP, HTTPS, DNS	CLEAN
www[.]googletagmanager[.]com	-	-	-	CLEAN
fonts[.]googleapis[.]com	-	-	-	CLEAN
open[.]spotify[.]com	-	-	-	CLEAN
www[.]facebook[.]com	-	-	-	CLEAN
secure[.]gravatar[.]com	-	-	-	CLEAN
www[.]linkedin[.]com	-	-	-	CLEAN
cdnjs[.]cloudflare[.]com	-	-	-	CLEAN
www[.]youtube[.]com	-	-	-	CLEAN
assets[.]pinterest[.]com	-	-	-	CLEAN
www[.]viralagenda[.]com	-	-	-	CLEAN
pagead2[.]googlesyndication[.]com	-	-	-	CLEAN
facebook[.]com	-	-	-	CLEAN
use[.]fontawesome[.]com	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www[.]google[.]com	-	-	-	CLEAN
s[.]w[.]org	-	-	-	CLEAN
maps[.]google[.]com	-	-	-	CLEAN
recursos[.]olargo[.]pt	-	-	-	CLEAN
stats[.]wp[.]com	-	-	-	CLEAN
masto[.]pt	-	-	-	CLEAN
ajax[.]googleapis[.]com	-	-	-	CLEAN
breakingnews[.]olargo[.]pt	-	-	-	CLEAN
v0[.]wordpress[.]com	-	-	-	CLEAN
olargo[.]pt	172.67.149.202, 104.21.29.205	United States	TCP, HTTPS, DNS	CLEAN
gmpg[.]org	-	-	-	CLEAN
www[.]instagram[.]com	-	-	-	CLEAN
www[.]feedgrabbr[.]com	-	-	-	CLEAN
olrg[.]pt	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.186.169.202	chiptochip[.]es	Spain	TCP, HTTPS, DNS	CLEAN
103.132.242.26	-	-	-	CLEAN
172.104.251.154	-	-	-	CLEAN
103.70.28.102	-	-	-	CLEAN
0.0.0.0	-	-	-	CLEAN
173.212.193.249	-	-	-	CLEAN
172.67.149.202	olargo[.]pt	United States	TCP, HTTPS, DNS	CLEAN
141.138.168.131	bruidsfotografie-breda[.]nl	Netherlands	TCP, HTTPS, DNS, HTTP	CLEAN
103.75.201.2	-	-	-	CLEAN
64.227.100.222	-	-	-	CLEAN
134.122.66.193	-	-	-	CLEAN
104.21.29.205	olargo[.]pt	-	DNS	CLEAN
129.232.188.93	-	-	-	CLEAN
82.223.21.224	-	-	-	CLEAN
149.56.131.28	-	-	-	CLEAN
51.254.140.238	-	-	-	CLEAN
212.24.98.99	-	-	-	CLEAN
201.94.166.162	-	-	-	CLEAN
110.232.117.186	-	-	-	CLEAN
119.193.124.41	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
158.69.222.101	-	-	-	CLEAN
51.161.73.194	-	-	-	CLEAN
213.239.212.5	-	Germany	TCP, HTTPS	CLEAN
91.207.28.33	-	-	-	CLEAN
151.106.112.196	-	-	-	CLEAN
207.148.79.14	-	-	-	CLEAN
183.111.227.137	-	-	-	CLEAN
209.97.163.214	-	-	-	CLEAN
163.44.196.120	-	-	-	CLEAN
206.189.28.199	-	United Kingdom	TCP, TLS	CLEAN
72.15.201.15	-	-	-	CLEAN
1.234.2.232	-	-	-	CLEAN
79.137.35.198	-	-	-	CLEAN
46.55.222.11	-	-	-	CLEAN
153.126.146.25	-	-	-	CLEAN
115.68.227.76	-	-	-	CLEAN
101.50.0.91	-	-	-	CLEAN
51.91.76.89	-	-	-	CLEAN
167.172.253.162	-	-	-	CLEAN
45.235.8.30	-	-	-	CLEAN
107.170.39.149	-	-	-	CLEAN
45.176.232.124	-	-	-	CLEAN
164.68.99.3	-	-	-	CLEAN
188.44.20.25	-	-	-	CLEAN
103.43.75.120	-	-	-	CLEAN
131.100.24.231	-	-	-	CLEAN
160.16.142.56	-	-	-	CLEAN
185.4.135.165	-	-	-	CLEAN
150.95.66.124	-	-	-	CLEAN
45.118.115.99	-	Indonesia	TCP	CLEAN
186.194.240.217	-	-	-	CLEAN
209.126.98.206	-	-	-	CLEAN
135.148.6.80	-	United States	TCP, HTTPS	CLEAN
37.187.115.122	-	-	-	CLEAN
172.105.226.75	-	Japan	TCP, TLS	CLEAN
50.116.62.25	www[.]chawkyfrenn[.]com	United States	TCP, DNS, HTTP	CLEAN

IP Address	Domains	Country	Protocols	Verdict
45.55.191.130	-	United States	TCP	CLEAN
196.218.30.83	-	-	-	CLEAN
5.9.116.246	-	-	-	CLEAN
94.23.45.86	-	-	-	CLEAN
144.91.78.55	-	Germany	TCP, HTTPS	CLEAN
213.241.20.155	-	-	-	CLEAN
159.89.202.34	-	-	-	CLEAN
139.59.126.41	-	-	-	CLEAN
159.65.88.10	-	-	-	CLEAN
172.81.116.81	chillpassion[.]com	United States	TCP, DNS, HTTP	CLEAN
197.242.150.244	-	-	-	CLEAN
159.65.140.115	-	-	-	CLEAN
146.59.226.45	-	-	-	CLEAN
82.165.152.127	-	-	-	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\ocxfile	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\ocxfile\AutoRegister	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile\AutoRegister	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\dllfile	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\.dll	access, read	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\.ocx	access, read	regsvr32.exe	CLEAN

Process

Process Name	Commandline	Verdict
regsvr32.exe	/S ..\phdg2.ocx	SUSPICIOUS
regsvr32.exe	C:\Windows\system32\regsvr32.exe "C:\Users\RDhJ0CNFevzX\AppData\Local\ABeIsdLaCr\hsBpWPNj.dll"	SUSPICIOUS
excel.exe	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE"	SUSPICIOUS
regsvr32.exe	C:\Windows\System32\regsvr32.exe /S ..\phdg2.ocx	SUSPICIOUS
regsvr32.exe	C:\Windows\System32\regsvr32.exe /S ..\phdg3.ocx	CLEAN
regsvr32.exe	C:\Windows\System32\regsvr32.exe /S ..\phdg4.ocx	CLEAN
regsvr32.exe	C:\Windows\System32\regsvr32.exe /S ..\phdg1.ocx	CLEAN

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	EmotetFunctionStrings	Emotet function strings	Function Strings	-	Downloader	5/5
Generic	JS_Unicode_escaped_bytes	JavaScript contains many unicode-escaped bytes; possible obfuscation	-	-	-	1/5
Generic	JS_Unicode_escaped_bytes	JavaScript contains many unicode-escaped bytes; possible obfuscation	-	-	-	1/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.1.0
Dynamic Engine Version	2023.1.0 / 01/31/2023 04:27
Static Engine Version	2023.1.0.0 / 2023-01-31 03:00:19
AV Exceptions Version	2023.1.1.6 / 2023-02-03 15:34:21
Link Detonation Heuristics Version	2023.1.1.18 / 2023-03-27 12:19:20
Smart Memory Dumping Rules Version	2023.1.1.6 / 2023-02-03 15:34:21
Config Extractors Version	2023.1.1.18 / 2023-03-27 12:19:20
Signature Trust Store Version	2023.1.1.7 / 2023-02-06 18:37:42
VMRay Threat Identifiers Version	2023.1.1.19 / 2023-03-29 15:29:26
YARA Built-in Ruleset Version	2023.1.1.18

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows