Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

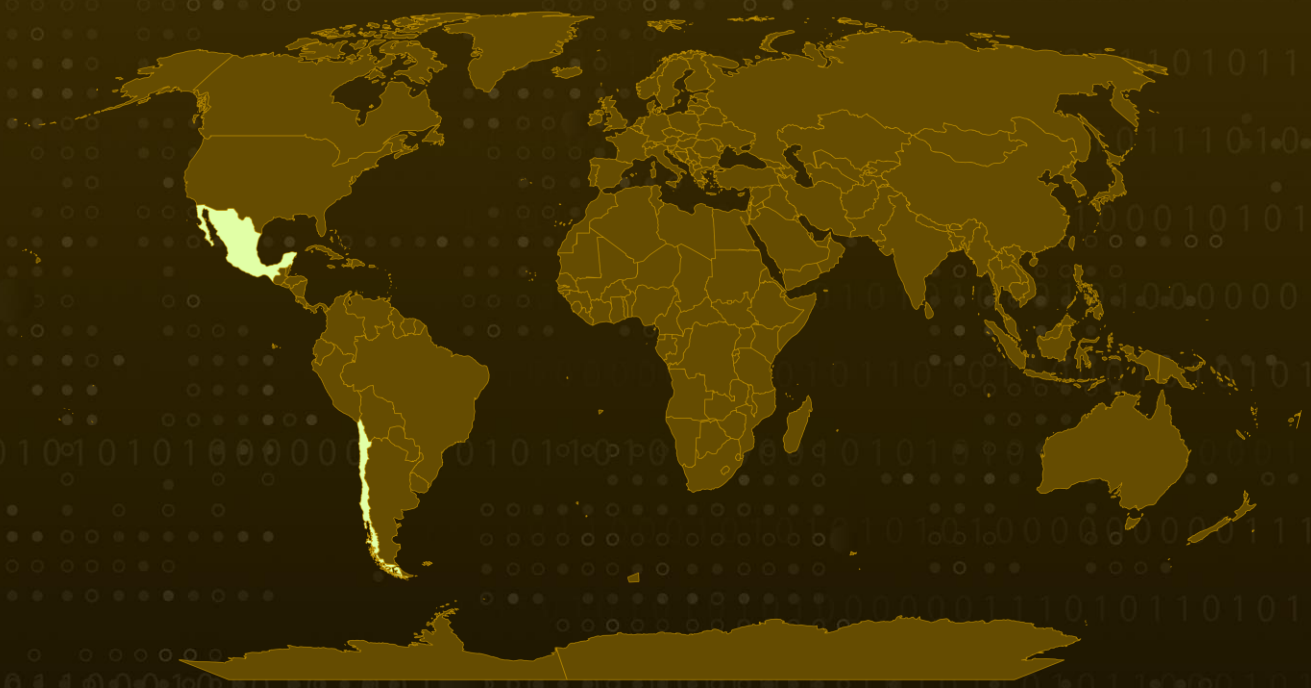
# Fenix Botnet Preys on Mexico and Chile

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| July 27, 2023 | A1 | TA2023315 |

# Summary

**First Seen:** 2022
**Malware:** Fenix Botnet
**Targeted Industry:** Government
**Attack Region:** Mexico and Chile
**Attack:** The Fenix Botnet targets tax-paying individuals in Mexico and Chile, aiming to infiltrate specific networks and pilfer valuable data.

## Attack Regions



# Attack Details

**#1** A Mexico-based cybercrime group has targeted tax-paying individuals in Mexico and Chile, using the Fenix Botnet to breach specific networks and steal valuable data, which they subsequently hand over to sophisticated actor groups. Their initial infection strategy involves using HTTrack Website Copier/3.x to clone official portals and redirect potential victims to these fraudulent sites.

**#2** On these fake websites, users are prompted to download a purported security tool, supposedly enhancing their portal navigation safety. This actor has been active since the last quarter of 2022, and the Fenix botnet capitalizes on the tax season in both countries. Alternatively, it exploits vulnerable WordPress engines to compromise weak websites.

**#3** The cybercriminal group establishes new domains for launching phishing campaigns, tricking users through typosquatted domains that resemble legitimate apps such as AnyDesk, WhatsApp, and others. The infiltrated website masquerades a ZIP file containing the software and serves as a launchpad for initiating an infection sequence.

**#4** This sequence involves executing a concealed PowerShell script, which, in turn, loads and runs a .NET binary. This process establishes persistence on the compromised host and deploys the Fenix botnet malware. The Fenix botnet is designed to execute commands received from a remote server, and it can also activate a stealer module responsible for extracting credentials stored in web browsers and crypto wallets.

# Recommendations

**Verify the Domain:** To safeguard against typosquatting, diligently verify website domains for spelling accuracy, use of URL shortener, and legitimacy. Utilize online tools, check domain ownership details, and exercise caution when encountering phishing attempts or unfamiliar domain extensions.

**Exercise caution when installing third-party apps:** Stick to trusted sources and thoroughly review app permissions. Unauthorized or poorly vetted apps may gain access to your data, compromising your security.

**Enhance Intrusion Detection Systems:** Implement robust intrusion detection systems to promptly identify and respond to obfuscated PowerShell scripts and .NET binaries. This enhancement will significantly improve your ability to detect and neutralize potential threats effectively.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0006<br>Credential Access | TA0007<br>Discovery | TA0009<br>Collection |
| TA0010<br>Exfiltration | TA0011<br>Command and Control | T1566<br>Phishing | T1059<br>Command and Scripting Interpreter |
| T1059.007<br>JavaScript | T1059.001<br>PowerShell | T1204.002<br>Malicious File | T1547.001<br>Registry Run Keys / Startup Folder |
| T1543<br>Create or Modify System Process | T1055<br>Process Injection | T1557<br>Adversary-in-the-Middle | T1056<br>Input Capture |
| T1620<br>Reflective Code Loading | T1497<br>Virtualization/Sandbox Evasion | T1010<br>Application Window Discovery | T1057<br>Process Discovery |
| T1071.001<br>Web Protocols | T1573<br>Encrypted Channel | T1090.001<br>Internal Proxy | T1041<br>Exfiltration Over C2 Channel |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | b10b9f1f286f7ae29d9e87c5391d3653,<br>500b1c312163009fefec3f8fe7861258,<br>594804aa21887ee9d7b1b888f482d60c,<br>1c50c6d0aeaf8071f528b76b1ab242fe,<br>d80f1780bb24e7ecdab8a262744bccb7, |

| TYPE | VALUE |
| --- | --- |
| MD5 | 1be0606640d645ddbfb2fbdff53ca918,<br>7631660bdcf74b95b5806328a7668cab,<br>eaff13d6c89ce0e2a7632bd811045c35,<br>ea68e0cc90a88315526704bae1ca8b4a,<br>b262b36c3b09ebeab66c95e121be4c73,<br>6f0b4018da4aa0887b5aa879ce315543,<br>7fe97d4e29e17f39e343a9ef5fde03ca |
| URLs | file[:]\\139[.]162[.]73[.]58@80\SuECWRPQ\SAT_Herramienta_Seguridad[.]jse,<br>file[:]\\139[.]162[.]73[.]58@80\YtmpEoBw\Herramienta_de_Seguridad_SII[.]jse,<br>hxxps[:]//fja[.]com[.]mx/wp-contents/execution[.]php?tag=russian,<br>hxxps[:]//fja[.]com[.]mx/wp-contents/init[.]php?id=1,<br>hxxps[:]//www[.]grafoce[.]com/scripts/index[.]php?id=2,<br>hxxps[:]//www[.]grafoce[.]com/wp-contents/execution[.]php?tag=russian,<br>hxxps[:]//russiancl[.]top/bramx/7684jasdtg[.]xls,<br>hxxps[:]//russiancl[.]top/bramx/post[.]php,<br>hxxps[:]//russiancl[.]top/bramx/ot[.]crypt,<br>hxxps[:]//russiancl[.]top/bramx/proxy[.]crypt,<br>hxxps[:]//russiancl[.]top/bramx/steal[.]crypt |
| Domains | 2repuvegobmx[.]com.mx,<br>annydesk.website,<br>citasatmx2023[.]lat,<br>citas-sat2023[.]com.mx,<br>citas-satmx[.]com,<br>citas-sregob-mexico[.]com,<br>consultacurp-gobmx[.]com.mx,<br>consultacurp-gobmx[.]com[.]mx,<br>fja[.]com[.]mx,<br>grafoce[.]com,<br>lbci-seguro[.]com,<br>mexico-curp[.]com,<br>russiancl[.]top,<br>siii-chile[.]com,<br>sre-curpmexico[.]com,<br>tramites-sat[.]com.mx,<br>whatsapp.website |
| IPv4 | 207.210.228[.]67,<br>139.162.73[.]58,<br>80.66.64[.]154 |

| TYPE | VALUE |
| --- | --- |
| FileNames | SII_Seguro_XXXXXX.zip,<br>Herramienta Seguridad SII.url,<br>AT_herramienta_XXXXXX.zip,<br>SAT_Herramienta_Seguridad.jse,<br>7684jasdtg.xls,<br>ot.crypt,<br>proxy.crypt,<br>steal.crypt,<br>pay.txt |

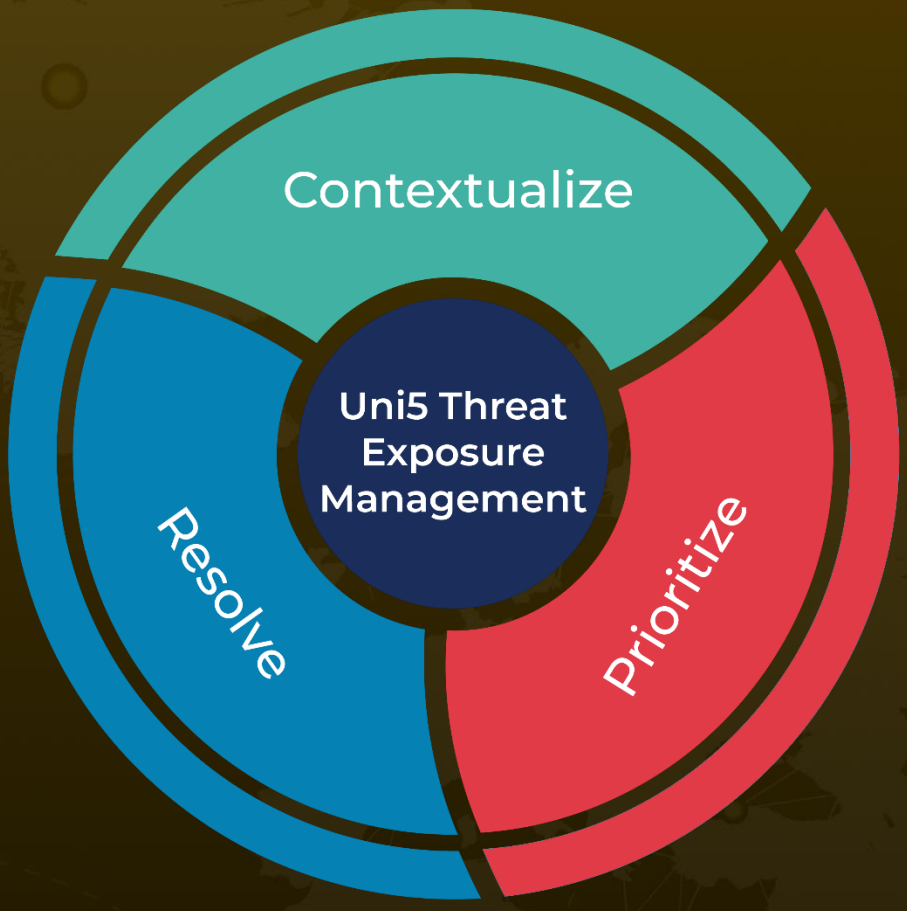
## References

https://web.archive.org/web/20230726140920/https://www.metabaseq.com/fenix-botnet/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**July 27, 2023 • 5:00 AM**



More at www.hivepro.com