Malware-as-a-Service: Redline Stealer Variants Demonstrate a Low-Barrier-to-Entry Threat

Intelligence Center

Curated Feeds

Learn how EclecticIQ can help you address your specific challenges – by team and by need – and improve your overall security posture.

Solutions overview

For CTI Teams

Provide your CTI team with the automation, performance, flexibility, and integrations needed to supercharge their CTI operations with our range of analyst-centric products and services.

For SOC Teams

Enable your SOC team to better operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.

For Situational Awareness

Improve your situational awareness and mitigate risk with our collection of analyst-centric threat intelligence products and services.

For Collaboration & Dissemination

Operationalize threat intelligence for more effective and efficient incident response with our range of analyst-centric management products and services.

Our Ecosystem

An ecosystem supporting our customers' intelligence-led proactive cybersecurity needs with collaborative partner programs delivering world-class joint solutions.

Partner Program

Partner with EclecticIQ to bring valuable and innovative security solutions and services to end users. Open to all partner types, including technology developers, service providers, resellers, and community.

Become a Partner

Our Partnerships

We partner with the world's premier technology and solution providers to support all phases of your cybersecurity needs. Explore all our partners' solutions and offerings to build and extend your cyber defense ecosystem.

About Our Partners

Open Source Projects

We are proud to be an active member in the open source community and to help develop and advance progress of security technology. Learn more about contributions or go directly to our GitHub page.

Open Source Projects EclecticIQ on GitHub

EclecticIQ analysts collected samples from a RedLine stealer spam campaign between April and August 2023. The campaign has been successful through shifting command and control among recently created domains hosted on IP addresses with legitimate traffic. Redline developers provide minor iterations to previous variants. Disrupting the malware’s living off the land tactics is the best practice for security teams.

Aleksander W. Jarosz – August 23, 2023

Multiple New Campaigns in 2023 Demonstrate The Malware Family Has Been Redeveloped to Remain a Popular And Prominent Threat

EclecticIQ analysts observe the malware family targeting financial information to be used for immediate gain as well as reconnaissance functions to perform initial information gathering and establish persistence. RedLine stealer is almost always accompanied by other malware; either preceded by a loader to install it or succeeded by further malware.

In the last major iteration of RedLine stealer in 2022, variants were almost always configured to rely on exploit kits for infection. At some point in 2022 infections saw a relative break in traffic as developers retooled, but in 2023 the malware has re-emerged as a prominent threat and is now reliant on other malware to act as the loader. [1] Most recently, Trend Micro identified a campaign that leveraged trojanized large-language model software to trick users into installing RedLine. [2]

Campaign variants emerge in VirusTotal starting the last week of April. [3] Samples very likely undergo initial testing in late April. This is supported by evidence from command and control infrastructure, discussed below. A small initial cluster of RedLine peaks approximately mid-July before tapering off significantly by the beginning of August. Sample volume then resumes in higher volume the second week of August.

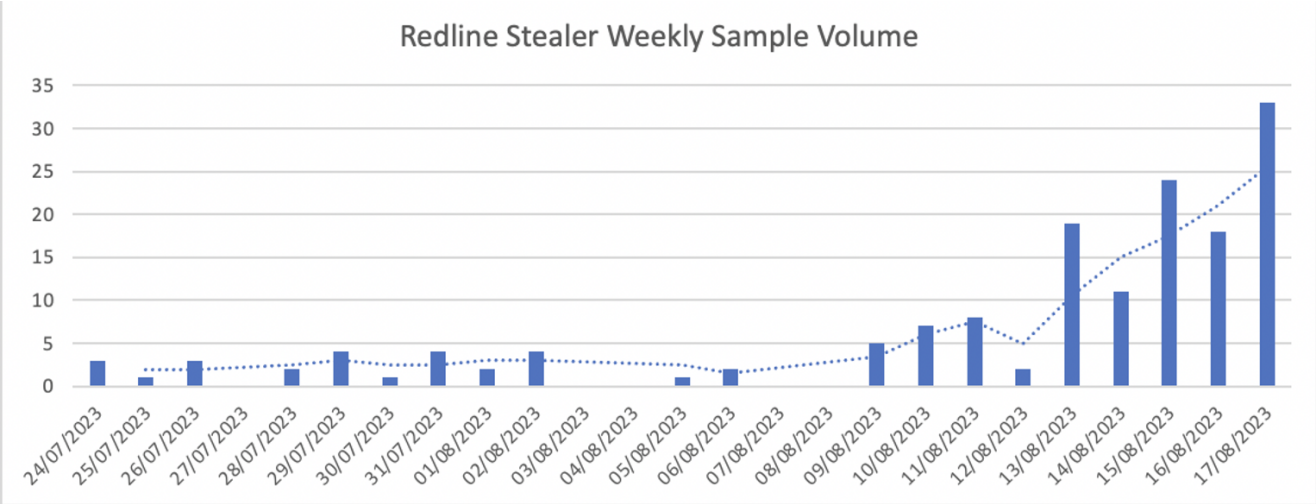


Figure 1 - Redline sample volumes collected through VirusTotal
(click on image to open in separate tab).

WMI Abuse Continues to Provide Core Information Gathering Capabilities

Notable capabilities within the Kill-Chain that are shared by these variants include:

- Code obfuscation using XOR and RC4 algorithms and future timestamps to bypass security systems.
- The use of registry keys via modification to establish persistence.
- WMI to drive local system queries and fingerprinting.
- The ability to delete files the malware creates to help conceal cyberattacks.

The first three capabilities were present in previous reporting by security researchers. [4] New variants use a new code obfuscation tactic; using XOR and RC4 encryption for payloads. PowerShell modules present in previous campaigns are absent in these versions of Redline stealer. [3, 4]

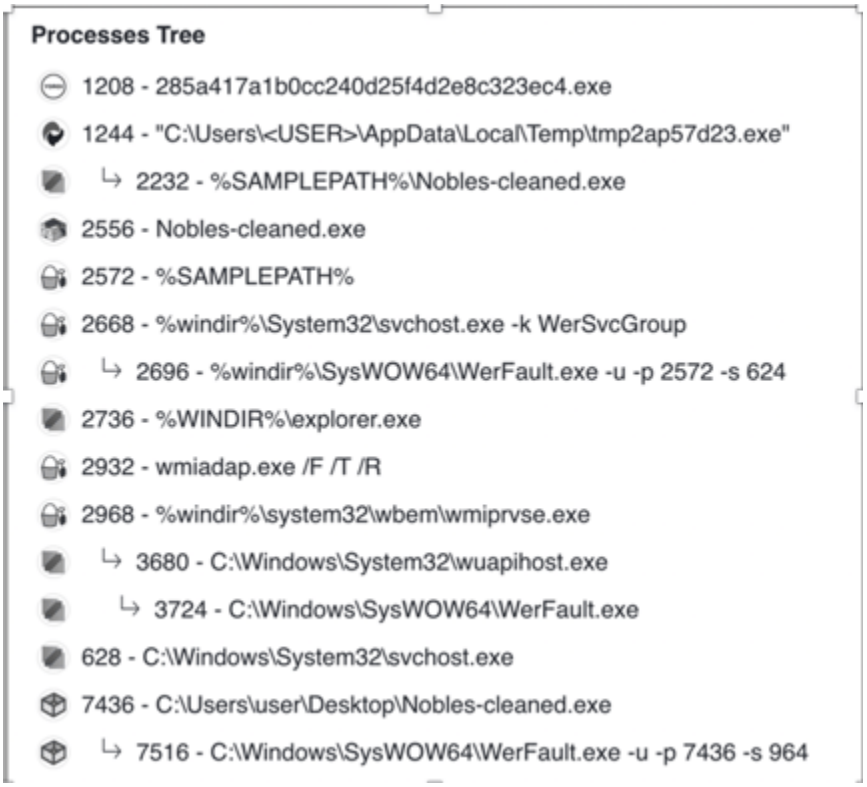


Figure 2 - The variants analyzed do not invoke PowerShell, but continue to leverage Windows Management Instrumentation heavily for core information gathering capabilities from local systems.

Variants analyzed are capable of targeting browsers; Firefox, Edge, Chrome, Iridium, Cent, Coowon, and Brave. Other browsers are not targeted; previous versions targeted many more browsers and crypto wallets [4] It also logs keystrokes, targets Coinomi crypto-wallets, and provides thorough fingerprinting of the local system.

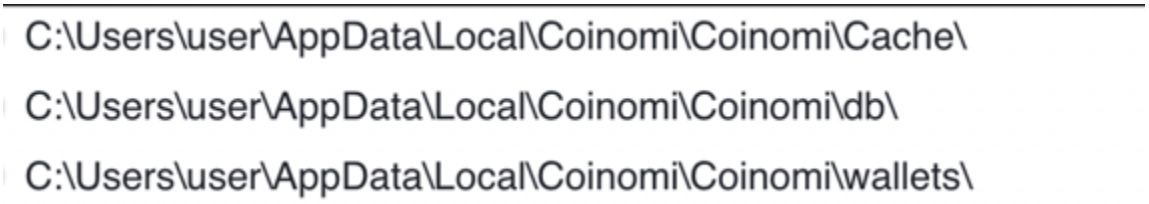


Figure 3 - Variants configured to access Coinomi wallets.

Command and Control Infrastructure Leverages New Domains to Circumvent a Majority of Blacklists

Infrastructure located in Austria and Finland are involved in this campaign. One Finland-based IP address 77.91.68.141, one Austrian IP address 78.153.130.209 serve as the primary command and control nodes. The malware is served from recently registered domains that are marked malicious, but hosted on IP addresses with other domains and legitimate traffic; a very common technique among threat actors.

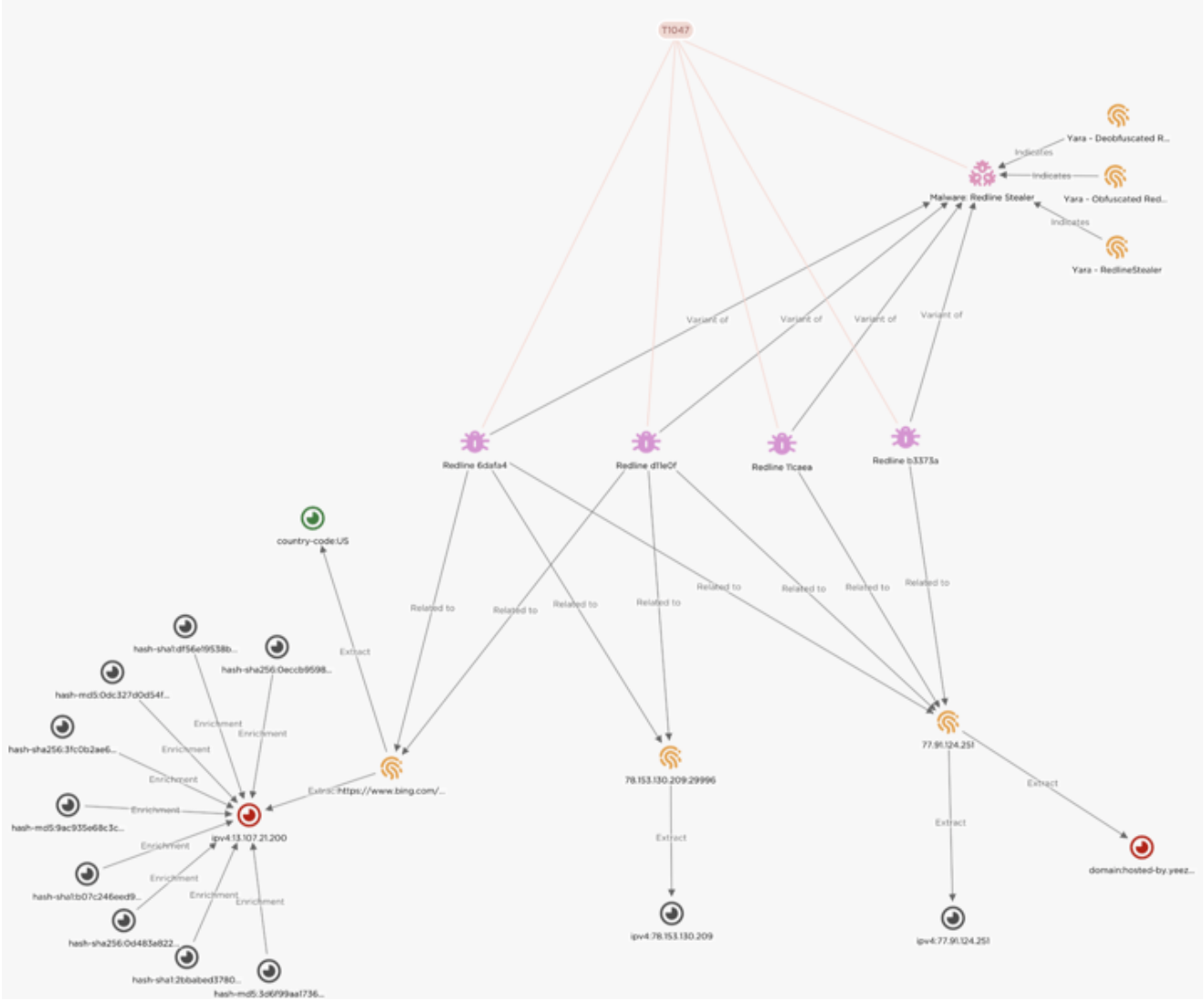


Figure 4 – A partial representation of this campaign in EclecticIQ Threat Intelligence Center. In this case the variants all share TTPs, to which security response and mitigation can be best directed.

The earliest IP address tracked is the Finnish IP. It is registered to STARK INDUSTRIES. The ASN is registered to a “Daniil Yevchenko” and includes further Ukrainian-based registration information. The current domain hosted on that IP address, “hosted-by.yeezyhost.net” was created in late 2022 and is used by RedLine Stealer variants analyzed. The IP address is marked clean by all antivirus vendors. Only a handful of service providers currently recognizes the IP address as malicious.

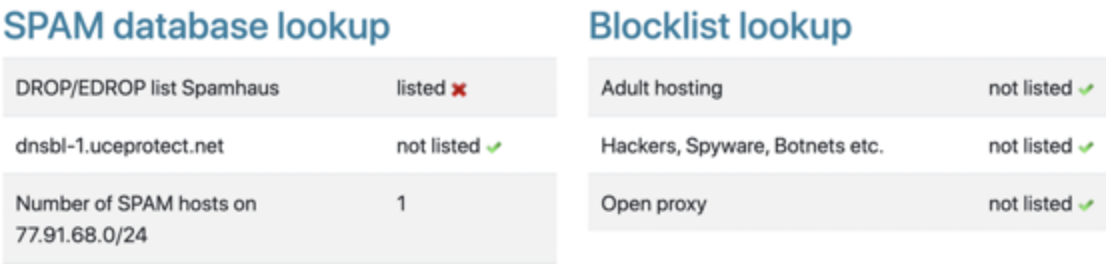


Figure 5 - The current infrastructure arrangement likely helps this RedLine Stealer campaign increase success.

The IP address hosts 40 unrelated domains. A snapshot of the first 10 below shows they are mostly legitimate and spam domains (obtained from dnslytics.com).

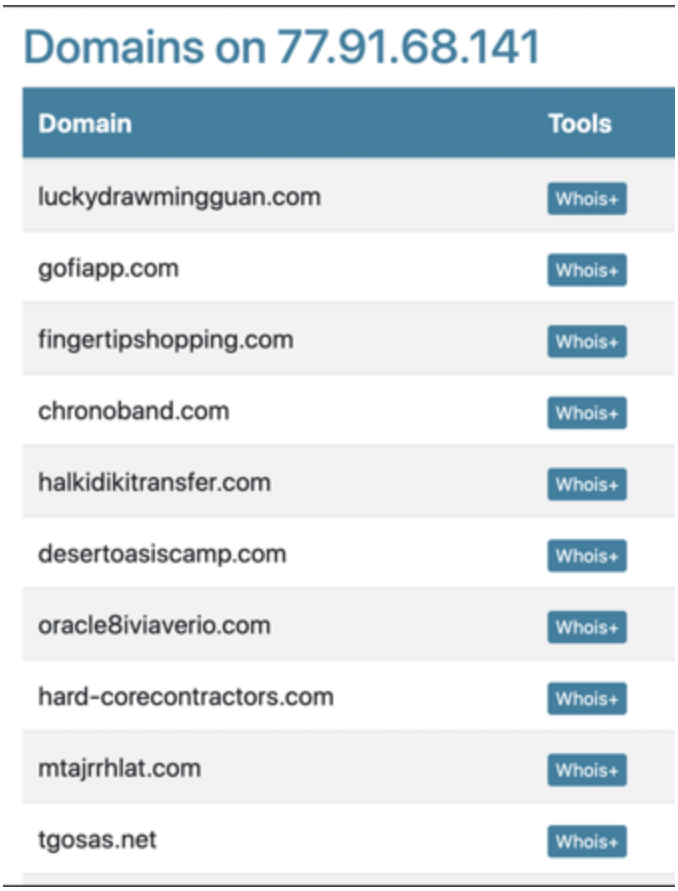


Figure 6 – An example of 10 domains (of 40) currently hosted.

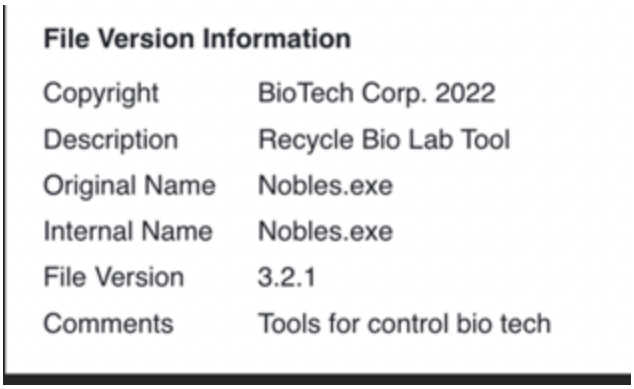
Passive DNS records indicate the campaign likely began April 17. The IP address was associated with the following domains beginning April 17. These were also detected in RedLine Stealer variants. These domains on the IP address have all been registered malicious by multiple AV vendors at some point since April and were very likely used in this campaign:

leatherupcorp.com

kvk-blank-login.mediainsightsgroup.com
mediainsightsgroup.com
grantallarddata.com

Samples Share Meta Data Information

A notable feature shared by all variants identified in this campaign includes the same copyright, description, and comments within their metadata. The copyright is linked to an actual copyright associated to a Malaysian biotech company that recently joined a large consortium of regional biotech partners. [5, 6]



File Version Information	
Copyright	BioTech Corp. 2022
Description	Recycle Bio Lab Tool
Original Name	Nobles.exe
Internal Name	Nobles.exe
File Version	3.2.1
Comments	Tools for control bio tech

Figure 7 - File metadata shared between samples includes copyright, description, similar naming themes, file version, and comments.

The latest variants have been automated via botnets, indicating that a larger campaign is likely underway. The botnet authorization module was absent from versions prior to August.

```
net.tcp://
localhost
d0d4a4bb84cf658744d23264a4da921f
Authorization
HTElByg1JRgiHhcfOzFRGTolDUIfDzkFKCU1XA==
@Hekkimarue
```

Figure 8 - Botnet automation present in the latest samples. The localhost name, authorization token, and botnet (Hekkimarue).

Conclusion and Mitigation

Redline stealer, a popular threat to a variety of organizations, continues to make minor changes to remain a successful and prominent low-barrier-to-entry threat. In lieu of major development changes, latest variants exclude PowerShell, possibly to reduce the malware's

footprint and automate via social media botnets. Command and control relies on new rapidly changing infrastructure that is difficult to mitigate by blocking indicators of compromise. Focusing on core malware development patterns - the use of WMI in this case - and successfully blocking malicious attempts through application whitelisting and process monitoring provide the best way to apply security resources to this and other malware.

Indicator of compromise (IoC)

Hashes:
27e778497f153a8939069c654af632f5bf322e6cc4da39555c818f6e67411782
bf5677548650d278fad6f14ad8b20e4ad4e6a87cf4fe83a47aa5b367f30a3690
a476c972a0ca5ccce58f67b0a51dbde50c915eab506fb1d843e7897f7e785f5e
5561161c347a961a767d0e6994cc89bc831b538e29c508893f9af6bb4678655c
d19dec6cd95aadc361f4c3811b989775a7bf8630c33e455844ae48d8ffcf8a39
06e1920cf81b2106cce759969b30d5ab5e93218c4abfe682e7be2ac11b47726f
0095a2ddc9363c91fc497296555de15fbbc6aeec81e731e0683fc2fca0fd3b06
a951ad91cc7bf9e7507f9ac1c2ff3c2fb80303e5343b87fee1b205233693e6ba
fac496334114561f6f21874bdc003325cba7821c4a294d0ad3a5c23f94a29300
65b00004c90c3d177d400cc52e13c20b489903db211fb91b8216e5fb23d86859
794096f8342c3352f4eb5642acb38241b688608f2026501e1430a70e759fb551
e62ab85547fdf2abe5936b39003db1e5ed3c9b42f35420fac7ea32b3387a0849
32675603ae94c027f4da61496f5e80994a933ae69f51b86c1ce0a8d38672c114
ee37878cc2395bd8872e1d5531b374ddd3da459aaa0e63f74b4c34aa7c7d63dc
4fced2922b13b4a7a9d22ac8c3f78b805ec44e9942e21c8368b45dd092dc1543
a686e9cdf9cc60cc08b5da9e50dd5124f4295f81e5f91222ae77184e190b29f6
7c1666b33638dec6ab6a915dd701a1b6025f2b05d32bad9034f5da4622821b65
07e889ad34a429f3295011d92258f5d43a6e015eeb072695fc81535f82b460c1
cc9625b8d0c1d5e1e04f293737eec2403a7aa8b496abfbfe4421c16de28bcd25
daa609470c4914536118a028e1ebc237fd0b623c776263538cdeaafd57da6068

IP Addresses:
13.107.21.200
77.91.124.251
78.153.130.209

Mitre ATT&CK Tactics And Techniques Associated to This Collection

TA0002-Execution	
Native API	T1106
Shared Modules	T1129

TA0003-Persistence	
Create or Modify System Process	T1543
Windows Service	T1543.003
Registry Run Keys / Startup Folder	T1547.001
TA0004-Privilege Escalation	
Access Token Manipulation	T1134
Create or Modify System Process	T1543
Windows Service	T1543.003
Bypass User Account Control	T1548.002
TA0005-Defense Evasion	
Masquerading	T1036
Indicator Removal	T1070
Timestomp	T1070.006
Modify Registry	T1112
Access Token Manipulation	T1134
Rundll32	T1218.011
File and Directory	
Permissions Modification	T1222
Virtualization/Sandbox Evasion	T1497
Bypass User Account Control	T1548.002
Impair Defenses	T1562
Disable or Modify Tools	T1562.001
TA0007-Discovery	
Query Registry	T1012
Process Discovery	T1057
System Information Discovery	T1082
File and Directory Discovery	T1083
Security Software Discovery	T1518.001
TA0011-Command and Control	
Application Layer Protocol	T1071
Web Protocols	T1071.001
Non-Standard Port	T1571

Structured Data

Find this and other research in our public TAXII collection for easy use in your security stack: https://cti.eclecticiq.com/taxii/discovery.

Please refer to our **support page** for guidance on how to access the feeds.

About EclecticIQ Intelligence & Research Team

EclecticIQ is a global provider of threat intelligence, hunting, and response technology and services. Headquartered in Amsterdam, the EclecticIQ Intelligence & Research Team is made up of experts from Europe and the U.S. with decades of experience in cyber security and intelligence in industry and government.

We would love to hear from you. Please send us your feedback by emailing us at research@eclecticiq.com.

You might also be interested in:

Black Bersek Malware, Large Language Model Adaption For Offensive Cyber Capabilities

German Embassy Lure: Likely Part of Campaign Against NATO Aligned Ministries of Foreign Affairs

Spearphishing Campaign Targets Zimbra Webmail Portals of Government Organizations

References

[1] Neagu Mihai, “RedLine Stealer Resurfaces in Fresh RIG Exploit Kit Campaign.” Bitdefender. Apr 27, 2022. https://www.bitdefender.com/blog/labs/redline-stealer-resurfaces-in-fresh-rig-exploit-kit-campaign/ (accessed Jun. 28, 2023).

[2] Dela Cruz Junestherry, “Malicious AI Tool Ads Used to Deliver Redline Stealer.” Trend Micro. May 12, 2023. https://www.trendmicro.com/en_us/research/23/e/malicious-ai-tool-ads-used-to-deliver-redline-stealer.html (accessed Jun. 30, 2023).

[3] Jarosz Aleks, “Custom VirusTotal Redline Stealer Query.” VirusTotal. Jun 1, 2023 https://www.virustotal.com/gui/search/metadata%253A%2522Tools%2520for%2520control%2520bio%2520tech%2522%2520and%2520positives%253A2%252B/files (accessed Jun. 1, 2023).

[4] Shrawan Poudel Swachchhanda, Bogati Anish, “RedLine Stealer Malware Outbreak: A Comprehensive Guide to Anatomy, Detection, and Response.” Logpoint. Apr 2023. https://www.logpoint.com/wp-content/uploads/2023/04/etpr-redline-stealer-malware-outbreak.pdf (accessed Jul. 1, 2023).

[5] Life Sciences Asia, “Malaysian Biotechnology Corporation Sdn. Bhd. (BiotechCorp).” Life Sciences Asia. 2023. https://www.life-sciences-asia.com/organisation/malaysian-biotechnology-corporation-sdn-bhd-biotechcorp-malaysia-govt-2001-22671.html (accessed Jul. 31, 2023).

[6] “Digital News Asia, “BiotechCorp rebranded to Malaysian Bioeconomy Development Corp, role expands.” Digital News Asia. Jun 09, 2023. https://www.digitalnewsasia.com/digital-economy/biotechcorp-rebranded-malaysian-bioeconomy-development-corp-role-expands (accessed Jul. 31, 2023).