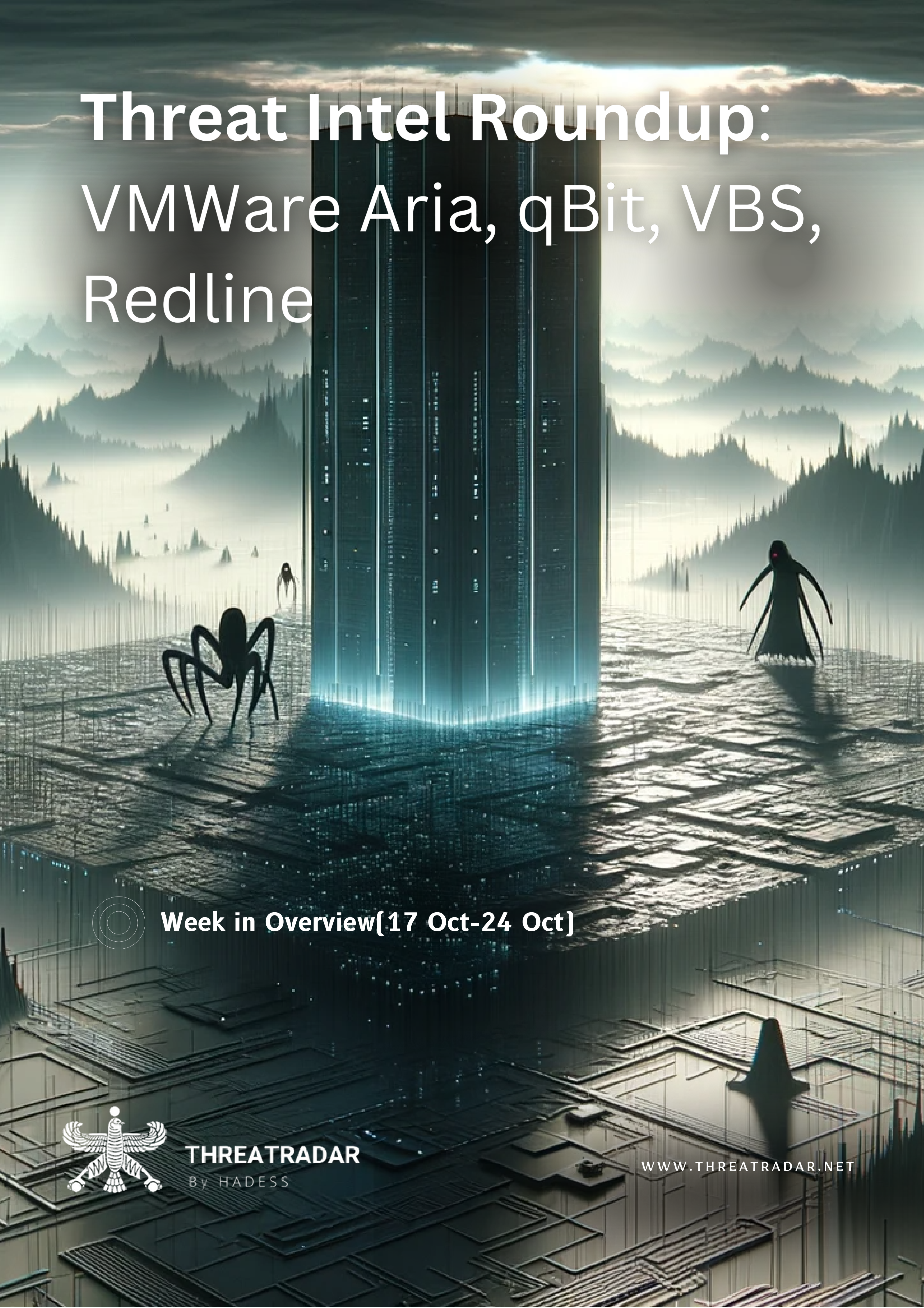


Threat Intel Roundup: VMWare Aria, qBit, VBS, Redline

Week in Overview(17 Oct-24 Oct)

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

Recent cybersecurity analyses have unearthed a variety of threats and vulnerabilities across different platforms and applications. Among them, the RedLine Stealer emerges as a potent threat, exemplifying the need for robust cybersecurity measures. A notable vulnerability, CVE-2023-36745, in Microsoft Exchange Server further accentuates the critical necessity for timely patch management. Concurrently, the distribution of CobaltStrike beacons by Pikabot and the vulnerability CVE-2023-34051 in VMware Aria Operations for Logs underline the multiplicity of threat vectors organizations are facing.

The advent of qBit, a new threat being promoted on the RansomedForum by a user named "qBitSupp," demonstrates the continuous evolution of malware. Meanwhile, a manual decoding of a complex .vbs script used for loading Cobalt Strike Shellcode elucidates the intricate methodologies employed by adversaries to obfuscate malicious code. The exploitation of Cisco IOS XE Software Web UI vulnerabilities delves deeper into the indicators of compromise, providing a glimpse into the nefarious activities surrounding Cisco devices.

In a case of deception, an incident of a victim's token approval being mistakenly granted to a scammer through an "increaseAllowance" transaction was reported, showcasing the sophisticated social engineering tactics at play. On another front, a stealthy malicious Excel file managed to evade detection by a majority of antivirus solutions, accentuating the limitations of existing defensive measures against evolving malware strains.

Lastly, the unveiling of the IRATA Family Attack Vector outlines the organized and well-structured approach of modern-day threat actors. The wide array of threats and vulnerabilities discussed here underscores the critical importance of employing comprehensive cybersecurity strategies, staying updated with the latest threat intelligence, and fostering a culture of continuous learning and adaptation to stay ahead in the ever-evolving cybersecurity landscape.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- Catching the RedLine Stealer
- CVE-2023-36745 sheds light on a vulnerability in Microsoft Exchange Server
- Pikabot distributing a CobaltStrike beacon
- CVE-2023-34051 in VMware Aria Operations for Logs
- qBit has emerged, promoted on the RansomedForum by a user named "qBitSupp."
- Manual Decoding of Complex .vbs Script for Loading Cobalt Strike Shellcode
- Active Exploitation of Cisco IOS XE Software Web UI Vulnerabilities
- Scammer through an "increaseAllowance" Transaction
- Stealthy Malicious Excel File Bypasses Majority of Antivirus Solutions
- Malware Alert: Unveiling the IRATA Family Attack Vector

🚨 Vulnerability of the Week

VMWare Aria

CVE-2023-34051

The vulnerability identified as CVE-2023-34051 exists in VMware Aria Operations for Logs and allows an unauthenticated malicious actor to bypass authentication mechanisms. This can lead to unauthorized file injection into the operating system of the impacted appliance, and subsequently, remote code execution.

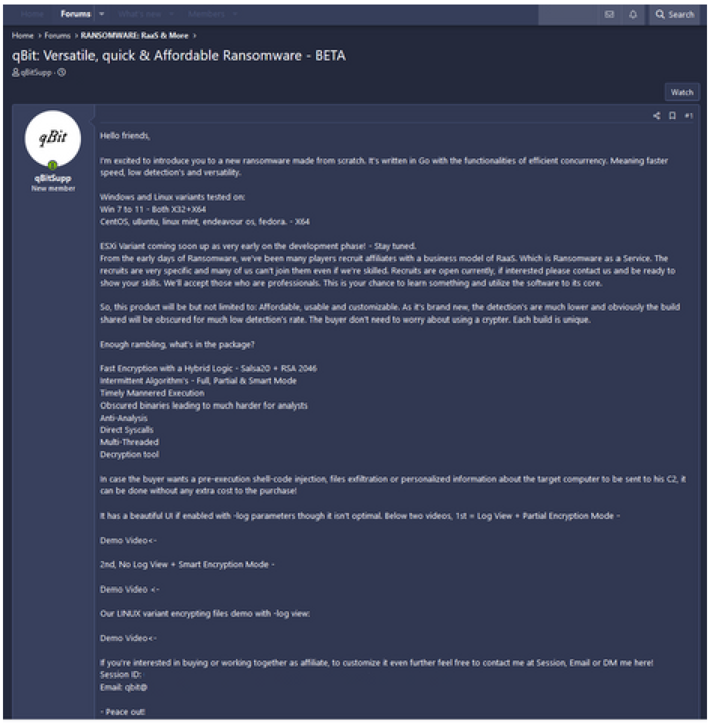
Details:
The flaw stems from inadequate authentication checks in the application, permitting an attacker without authentic credentials to inject files into the operating system of the targeted appliance. Once the files are injected, the attacker can execute arbitrary code remotely on the affected system. The vulnerability is critical and has been assigned a score of 9.8 out of 10 on the CVSS scale1.

Proof of Concept (PoC):
A proof of concept demonstrating the exploitation of this vulnerability is available at https://github.com/horizon3ai/CVE-2023-34051.
Affected Versions:
The advisory did not specify the affected versions. It's recommended to refer to the official VMware advisory for this information.

Mitigations:
It's recommended to apply the necessary patches or updates provided by VMware to remediate this vulnerability. Additionally, adhering to best practices such as restricting network access, employing strong authentication mechanisms, and regularly monitoring system logs can help mitigate the risks associated with this vulnerability.
References:

Official VMware Advisory: Link (Note: The page could not be accessed for further details)
Technical Deep Dive: Horizon3.ai
Vulnerability Details: CVE Details, Tenable, Vulners

🥵 Malware or Ransomware



Home › Forums › RANSOMWARE: RaaS & More ›

qBit: Versatile, quick & Affordable Ransomware - BETA

qBitSupp ·

qBitSupp
New member

Hello friends,

I'm excited to introduce you to a new ransomware made from scratch. It's written in Go with the functionalities of efficient concurrency. Meaning faster speed, low detection's and versatility.

Windows and Linux variants tested on:
Win 7 to 11 - Both X32+X64
CentOS, ubuntu, linux mint, endeavour os, fedora. - X64

ESXi Variant coming soon up as very early on the development phase! - Stay tuned.
From the early days of Ransomware, we've been many players recruit affiliates with a business model of RaaS. Which is Ransomware as a Service. The recruits are very specific and many of us can't join them even if we're skilled. Recruits are open currently, if interested please contact us and be ready to show your skills. We'll accept those who are professionals. This is your chance to learn something and utilize the software to its core.

So, this product will be but not limited to: Affordable, usable and customizable. As it's brand new, the detection's are much lower and obviously the build shared will be obscured for much low detection's rate. The buyer don't need to worry about using a crypter. Each build is unique.

Enough rambling, what's in the package?

Fast Encryption with a Hybrid Logic - Salsa20 + RSA 2046
Intermittent Algorithm's - Full, Partial & Smart Mode
Timely Mannered Execution
Obscured binaries leading to much harder for analysts
Anti-Analysis
Direct Syscalls
Multi-Threaded
Decryption tool

In case the buyer wants a pre-execution shell-code injection, files exfiltration or personalized information about the target computer to be sent to his C2, it can be done without any extra cost to the purchase!

It has a beautiful UI if enabled with -log parameters though it isn't optimal. Below two videos, 1st = Log View + Partial Encryption Mode -

Demo Video<-

2nd, No Log View + Smart Encryption Mode -

Demo Video <-

Our LINUX variant encrypting files demo with -log view:

Demo Video<-

If you're interested in buying or working together as affiliate, to customize it even further feel free to contact me at Session, Email or DM me here!
Session ID:
Email: qbit@

- Peace out!

https://twitter.com/azalsecurity/status/1716249809374314718

The new ransomware named qBit has been advertised on the Ransomed cybercrime forum by a threat actor using the pseudonym qBitSupp. This ransomware is currently in its Beta stage and is claimed to be written from scratch in Go, making it a fresh addition to the growing list of ransomware variants. The ransomware operates on a Ransomware as a Service (RaaS) model, offering many features to potential affiliates. The threat actor behind qBit advertises faster encryption speed, a low detection rate, and remarkable versatility with both Windows and Linux variants available. There's also mention of the development of an ESXi version. qBitSupp aims to make qBit an affordable and accessible choice for newcomers to cybercrime, offering a 85/15 profit-sharing arrangement to affiliates1.

Moreover, qBitSupp has shared demo videos showcasing the potential harm this ransomware could inflict, adding to the growing concerns within the cybersecurity community regarding the proliferating nature of ransomware threats1.

Interestingly, the mention of qBitSupp comes a week after the coverage of qBit Stealer malware by @pcrisk, suggesting that both the Stealer and Ransomware variants are managed and developed by qBitSupp. Although there isn't a direct correlation established between qBit Stealer and qBit ransomware, the common pseudonym qBitSupp used in the promotion of both malicious software suggests a possible link between the two.

The emergence of qBit and its advertisement on the Ransomed forum indicates a continuous evolution in the ransomware landscape, with threat actors developing and promoting new tools to commit cyber extortion. The RaaS model, which qBit operates under, continues to provide a platform for cyber criminals to easily deploy ransomware attacks, even for those with lesser technical skills, thus broadening the scope and scale of potential cyber threats.

Malware Distribution Sites

https://twitter.com/Threatlabz/status/1716492689036951591

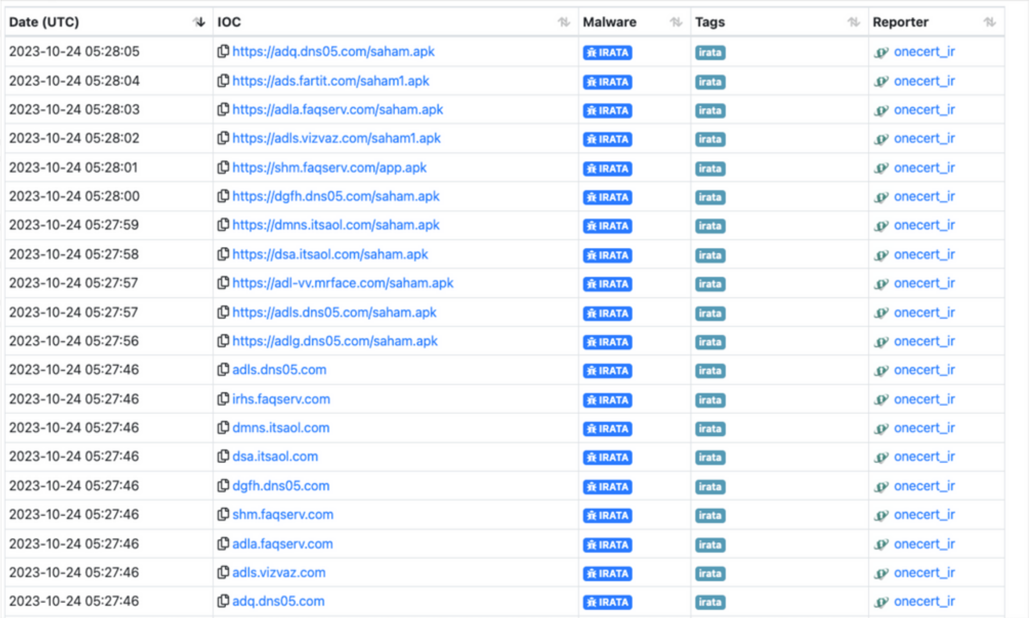
The report on Pikabot distributing a CobaltStrike beacon through the URL hxxps://173.44.141.113/Create/v10.58/RTYZC2PY and the mentioned Command and Control servers (C2s) is as follows:
Pikabot has been identified to distribute CobaltStrike beacons, which are typically used for establishing persistent connections to infiltrated networks, allowing attackers to control compromised systems remotely. The distribution is carried out through malicious URLs, with the specified URL being one of the mediums. The technical analysis reveals that the malicious URL hxxps://173.44.141.113/Create/v10.58/RTYZC2PY is associated with a CobaltStrike beacon, indicating that it's part of a malicious campaign orchestrated by Pikabot1.

Moreover, the listed Pikabot C2s (Command and Control servers) are essentially remote servers controlled by cyber attackers to manage malware or receive stolen data from compromised systems. The IP addresses and ports mentioned:

- 139.99.216[.]90:13720
- 156.251.137[.]134:5000
- 154.12.252[.]84:23399
- 85.215.218[.]128:5243
- 103.231.93[.]15:5631
- 196.218.123[.]202:13783

are part of this malicious network infrastructure utilized by Pikabot for its nefarious activities. Each of these IP addresses corresponds to a server that can potentially control malware, send commands, or exfiltrate data from victimized networks.
A deeper understanding of Pikabot's mechanisms can be gleaned from technical analyses and deep dives into its cyber threat tactics, techniques, and procedures (TTPs)23. Additionally, the detection of Cobalt Strike beacons and the mitigation of associated threats are critical aspects that cybersecurity professionals are continually working on, as evidenced by resources and guides available online4.
While the specific Twitter post by Threatlabz was not directly accessible in the searched resources, the information gathered provides a substantial understanding of the cyber threat posed by Pikabot and its use of CobaltStrike beacons distributed through malicious URLs and controlled via the specified C2 servers.

Mobile Malware



Date (UTC)	IOC	Malware	Tags	Reporter
2023-10-24 05:28:05	https://adq.dns05.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:28:04	https://ads.fartit.com/saham1.apk	IRATA	irata	onecert_ir
2023-10-24 05:28:03	https://adla.faqserv.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:28:02	https://adls.vizvaz.com/saham1.apk	IRATA	irata	onecert_ir
2023-10-24 05:28:01	https://shm.faqserv.com/app.apk	IRATA	irata	onecert_ir
2023-10-24 05:28:00	https://dgfh.dns05.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:27:59	https://dmns.itsaol.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:27:58	https://dsa.itsaol.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:27:57	https://adl-vv.mrface.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:27:57	https://adls.dns05.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:27:56	https://adlg.dns05.com/saham.apk	IRATA	irata	onecert_ir
2023-10-24 05:27:46	adls.dns05.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	irhs.faqserv.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	dmns.itsaol.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	dsa.itsaol.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	dgfh.dns05.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	shm.faqserv.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	adla.faqserv.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	adls.vizvaz.com	IRATA	irata	onecert_ir
2023-10-24 05:27:46	adq.dns05.com	IRATA	irata	onecert_ir

https://twitter.com/onecert_ir/status/1715660317689073868

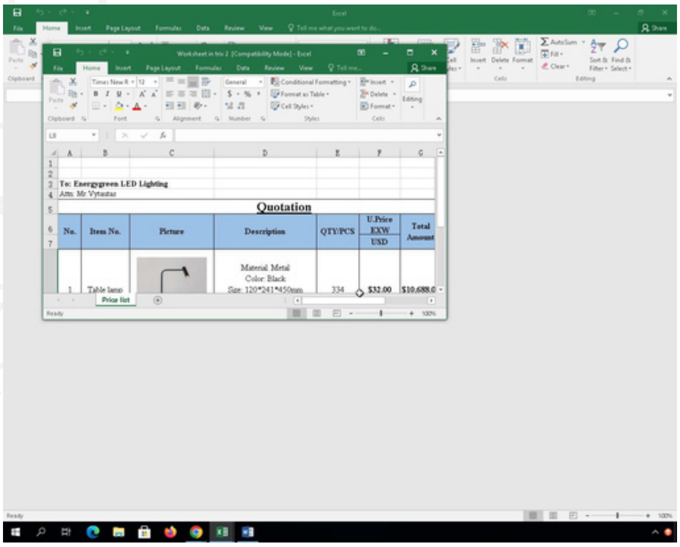
A new malware threat identified as the IRATA family has emerged in the cybersecurity landscape, exhibiting an orchestrated attack pattern. This malicious software is distributed via certain payload URLs, with one such URL being highlighted by URLhaus: https://urlhaus.abuse.ch/url/2722813/. The payload linked to this URL was found to be hosted on Bazaar's platform, showcasing a distinct malware sample with the hash: 6993d0ce074816c4f58761aa1579104aa5b95f1dbbf32ea70a67f904f6023fc6. The threat actors behind the IRATA family have operationalized this malware to execute malicious activities upon successful infiltration.

The IRATA malware communicates with its command and control servers (C2) to receive instructions and exfiltrate sensitive data. Two particular IoCs (Indicators of Compromise) linked with this C2 communication have been noted on ThreatFox: https://threatfox.abuse.ch/ioc/1191454/ and https://threatfox.abuse.ch/ioc/1191455/. Furthermore, a domain associated with this malware campaign, tedalat[.]hair, has been identified, which further unveils the infrastructure used by the attackers to perpetrate their malicious intents.

The infrastructure supporting this malware campaign is leveraged through services provided by Cloudflare (ISP) and the domain is registered with Namecheap (Registrar). These platforms inadvertently play a part in hosting and facilitating the malware's network, underlining the significant role of third-party service providers in the malware distribution chain. The use of reputable service providers aids in masking the malicious activities, thereby increasing the chances of the malware evading detection and prolonging its operational lifespan.

The emergence of the IRATA family exemplifies the continuous evolution of malware threats. The modus operandi involving the use of legitimate service providers and a multi-tier communication infrastructure underscores the sophisticated techniques employed by modern-day threat actors. It's imperative for organizations to remain vigilant, employ robust cybersecurity measures, and collaborate with external threat intelligence platforms to stay ahead of such evolving threats. The insights provided by platforms like URLhaus, Bazaar, and ThreatFox are invaluable in understanding the threat landscape and preparing defenses against such nuanced malware campaigns.

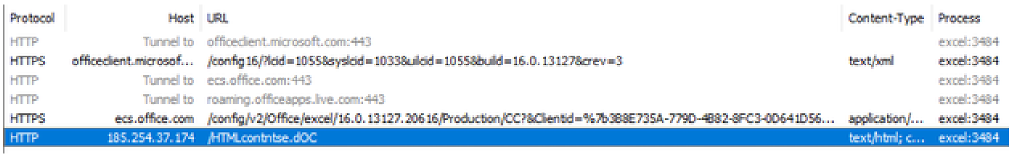
Proxylife



To: Energygreen LED Lighting
Attn: Mr Vytautas

Quotation

No.	Item No.	Picture	Description	QTY/PCS	U.Price EXW USD	Total Amount
1	Table lamp		Material: Metal Color: Black Size: 120*241*450mm	334	$32.00	$10,688.0



Protocol	Host	URL	Content-Type	Process
HTTP	Tunnel to	officeclient.microsoft.com:443		excel:3484
HTTPS	officeclient.microsof...	/config16/?lcid=1055&syslcid=1033&uilcid=1055&build=16.0.13127&crev=3	text/xml	excel:3484
HTTP	Tunnel to	ecs.office.com:443		excel:3484
HTTP	Tunnel to	roaming.officeapps.live.com:443		excel:3484
HTTPS	ecs.office.com	/config/v2/Office/excel/16.0.13127.20616/Production/CC?&Clientid=%7b3B8E735A-779D-4B82-8FC3-0D641D56...	application/...	excel:3484
HTTP	185.254.37.174	/HTMLcontntse.dOC	text/html; c...	excel:3484

https://twitter.com/doc_guard/status/1716463458156228993

In a recent security incident, a malicious Excel file has managed to slip past the detection mechanisms of a majority of antivirus solutions, signaling a potential rise in the sophistication of malware delivery techniques. The malicious file, named "solicitud de cotización.xla", exhibited a complex multi-step infection flow that involved multiple Microsoft applications and processes to ultimately execute malicious code on the victim's system. With a low detection rate of 9 out of 62 on VirusTotal (VT), this file poses a significant threat to users and networks unprepared for such advanced evasion tactics.

The infection chain commenced with the malicious Excel file, which upon being opened, triggered a cascade of actions involving Word, the Equation Editor (eqnedt32.exe), Windows Script Host (wscript.exe), and subsequently multiple instances of PowerShell, ultimately leading to the execution of regasm.exe. This elaborate sequence of actions serves as a means to evade detection, by leveraging legitimate processes to carry out malicious activities stealthily. The multi-stage attack vector not only demonstrates the attacker's in-depth understanding of Microsoft's suite of applications but also their ability to manipulate these interconnected processes to fulfill malicious intents.

The MD5 hash value of the malicious file is identified as 2ca17c363987979bbbee80b08f3f97be, and it has been reported to communicate with a malicious IP address 185.254.37.174, which is suspected to be a command and control server (C2) for the malware. The detailed analysis provided by DOCGuard in their report highlights the intricacies of the attack and the stealthy nature of the malicious Excel file. The evasion of nearly all antivirus solutions is alarming and underscores the necessity for advanced detection mechanisms capable of identifying and mitigating multi-stage, obfuscated attack vectors.

As malicious actors continue to refine their evasion techniques and employ multi-stage attack vectors, the onus falls on security solutions to evolve and adapt to these emerging threats. This incident emphasizes the importance of employing a multi-layered security approach, encompassing not just antivirus solutions but also employing behavior analysis, heuristic detection, and robust incident response procedures to detect and mitigate such sophisticated threats. Additionally, educating end-users on the risks associated with opening unsolicited attachments and promoting a culture of cybersecurity awareness can significantly contribute to minimizing the risk posed by such stealthy malicious files.

🥷 TTP Analysis

A complex .vbs script has been identified which is designed to load Cobalt Strike shellcode into memory. The script utilizes heavy text-based obfuscation which can be decoded manually using CyberChef and Regex. Post-obfuscation, some "malformed" shellcode is identified, which is then manually fixed before being emulated with the SpeakEasy emulator.

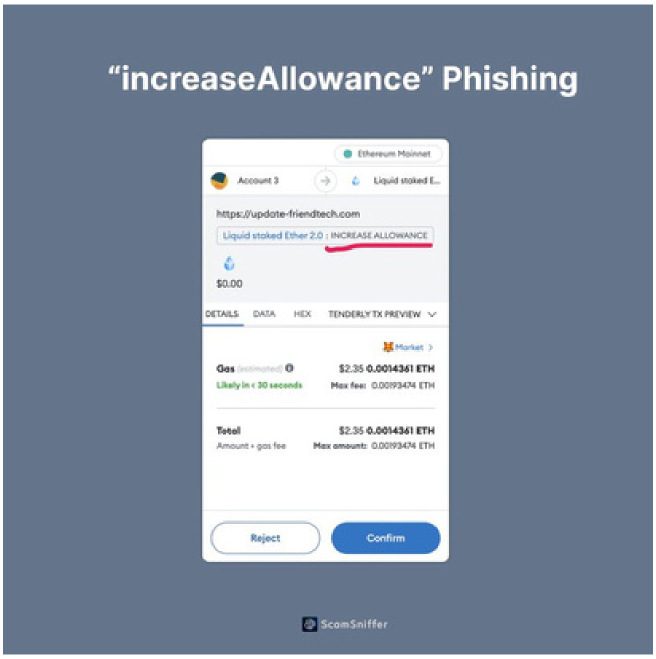
Methods:

1. **Initial Analysis**:
   - Save and unzip the script using the password 'infected'.
   - Open the file using a text editor like Notepad++ to observe references to Excel objects and Wscript.Shell, hinting at the use of Excel and Wscript to execute obfuscated code.
2. **Overview of Obfuscation Techniques**:
   - Identify obfuscation techniques:
     - Script broken into small strings.
     - Utilization of decimal encoded values decoded using Chr.
     - Lines ending with an underscore _.
3. **Removing Obfuscation**:
   - Utilize regex to remove the identified obfuscations.
   - Remove string split obfuscation using a search/replace for "&" with an empty replace value.
   - Use CyberChef to identify and remove Chr(10) style obfuscation using regex to hone in on the decimal encoded values and decode them.
4. **Further Cleanup**:
   - Remove remaining ampersands and underscores using regex.
   - Remove unnecessary quotes from the script.
5. **Analyzing the Cleaned-Up Script**:
   - Identify references to APIs commonly used in process injection.
   - Locate a blob of hex bytes and a process name, suggesting an injection into rundll32.exe.
   - Assume the bytes to be shellcode due to its short length.
6. **Fixing Negative Decimal Values**:
   - Identify negative values in the shellcode, subtracting them from 256 using CyberChef or Python.
7. **Validation and Emulation**:
   - Use the SpeakEasy emulator to confirm the bytes as shellcode and emulate its function.
   - Identify the shellcode as a http-based downloader from the IP 47.98.41[.]47.

Results: Upon successful decoding and emulation, the script is revealed to load a Cobalt Strike shellcode into memory which acts as an HTTP-based downloader from a specified IP address. The manual decoding process unveiled the underlying malicious activity hidden behind multiple layers of obfuscation in the .vbs script.

https://twitter.com/embee_research/status/1716339955314897326

👹 Scam Contract



"increaseAllowance" Phishing

Ethereum Mainnet

Account 3 → Liquid staked E...

https://update-friendtech.com

Liquid staked Ether 2.0 : INCREASE ALLOWANCE

$0.00

Gas (estimated) $2.35 0.0014361 ETH
Likely in < 30 seconds Max fee: 0.00193474 ETH

Total $2.35 0.0014361 ETH
Amount + gas fee Max amount: 0.00193474 ETH

https://twitter.com/realScamSniffer/status/1715809311904207246

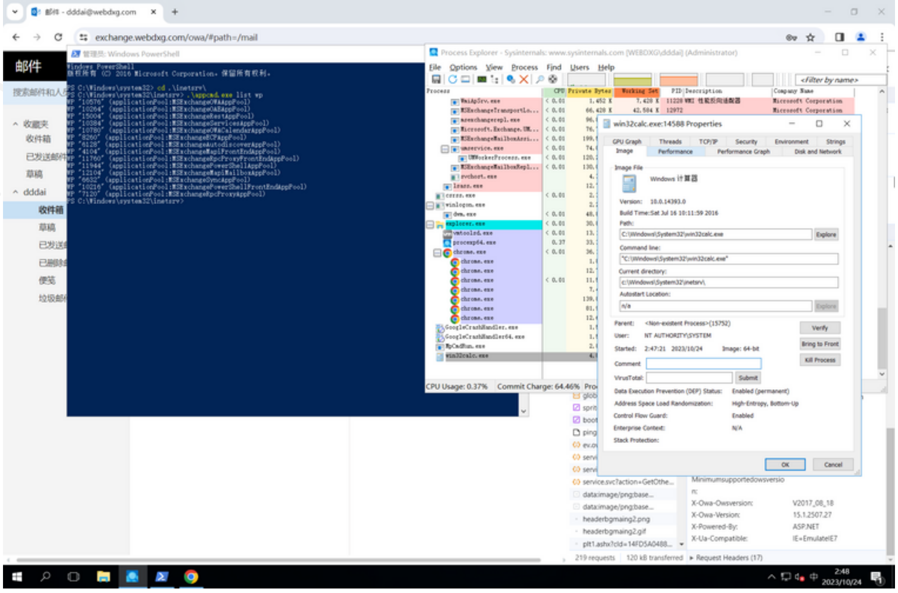
In the ever-evolving space of digital transactions, security has become the centerpiece of concerns, especially with the increasing sophistication of scams. A particularly concerning scenario unfolded recently when a victim mistakenly approved a token allowance to a scammer by signing an "increaseAllowance" transaction. The "increaseAllowance" function is a part of the ERC-20 token standard in the Ethereum blockchain, which allows a specified address to spend tokens on behalf of the owner up to a certain amount. Unwittingly, the victim authorized the scammer to access and manage their tokens by executing this function, which set off a series of unauthorized transactions.

This unfortunate event underscores the critical importance of understanding the implications of the transactions one is signing on the blockchain. The deceptive request for an "increaseAllowance" transaction might have appeared benign or routine to the victim, masking the malicious intent of the scammer. Furthermore, the scammer could have employed social engineering techniques to gain the trust of the victim or exploit their lack of understanding regarding the functionalities associated with such transactions. In essence, the scammer's ability to mislead the victim into signing the transaction accentuates the emerging sophisticated tactics employed by malicious actors in the blockchain space.

The aftermath of this incident holds substantial financial ramifications for the victim, alongside a breach of their digital trust. Once the scammer received the misguided approval, they gained the ability to initiate transactions with the victim's tokens up to the approved limit. Without immediate corrective measures, such as revoking the allowance using the "decreaseAllowance" function or transferring the tokens to a secure address, the victim stood to lose a significant portion, if not all, of their digital assets. The scenario sheds light on the potentially catastrophic impacts that a single misguided transaction approval could entail in the blockchain ecosystem.

Moving forward, this incident serves as a stark reminder for individuals and entities interacting with blockchain technologies to exercise utmost caution. It's imperative to have a solid understanding of the transactions one is engaging in, especially when authorizing allowances for token transactions. Employing additional security measures such as multi-signature approvals, utilizing secure and reputable platforms, and seeking advice from knowledgeable sources before executing sensitive transactions can act as deterrents against falling victim to such scams. The blockchain community must also ramp up efforts in educating users on the security aspects and potential risks associated with token transactions to foster a safer digital transaction environment.

NDay



```
Windows PowerShell
版权所有 (C) 2016 Microsoft Corporation。保留所有权利。

PS C:\Windows\system32> cd .\inetsrv\
PS C:\Windows\system32\inetsrv> .\appcmd.exe list wp
WP "10576" (applicationPool:MSExchangeOWAAppPool)
WP "10264" (applicationPool:MSExchangeOABAppPool)
WP "15004" (applicationPool:MSExchangeRestAppPool)
WP "10384" (applicationPool:MSExchangeServicesAppPool)
WP "10780" (applicationPool:MSExchangeOWACalendarAppPool)
WP "8260" (applicationPool:MSExchangeECPAppPool)
WP "6128" (applicationPool:MSExchangeAutodiscoverAppPool)
WP "4104" (applicationPool:MSExchangeMapiFrontEndAppPool)
WP "11760" (applicationPool:MSExchangeRpcProxyFrontEndAppPool)
WP "11944" (applicationPool:MSExchangePowerShellAppPool)
WP "12104" (applicationPool:MSExchangeMapiMailboxAppPool)
WP "6632" (applicationPool:MSExchangeSyncAppPool)
WP "10216" (applicationPool:MSExchangePowerShellFrontEndAppPool)
WP "7120" (applicationPool:MSExchangeRpcProxyAppPool)
PS C:\Windows\system32\inetsrv>
```

win32calc.exe:14588 Properties

Windows 计算器

Version: 10.0.14393.0

Build Time:Sat Jul 16 10:11:59 2016

Path: C:\Windows\System32\win32calc.exe

Command line: "C:\Windows\System32\win32calc.exe"

Current directory: c:\Windows\System32\inetsrv\

Autostart Location: n/a

Parent: <Non-existent Process>(15752)

User: NT AUTHORITY\SYSTEM

Started: 2:47:21 2023/10/24 Image: 64-bit

Data Execution Prevention (DEP) Status: Enabled (permanent)

Address Space Load Randomization: High-Entropy, Bottom-Up

Control Flow Guard: Enabled

Enterprise Context: N/A

Stack Protection:

X-Owa-Owsversion: V2017_08_18

X-Owa-Version: 15.1.2507.27

X-Powered-By: ASP.NET

X-Ua-Compatible: IE=EmulateIE7

https://n1k0la-t.github.io/2023/10/24/Microsoft-Exchange-Server-CVE-2023-36745/

The report on CVE-2023-36745 sheds light on a vulnerability in Microsoft Exchange Server, identified as a variant of CVE-2022-41082. This vulnerability surfaced after the release of a report by Trend Micro Zero Day Initiative regarding remote code execution in Exchange PowerShell Backend. It has a lineage of deserialization bypass vulnerabilities, specifically in the PowerShell endpoint of Microsoft Exchange Server, like CVE-2023-21707 and CVE-2023-32031 demonstrated at Hexacon 2023 by chudyPB.

The crux of CVE-2023-36745 lies in bypassing via the **Microsoft.Exchange.DxStore.Common.DxSerializationUtil.SharedTypeResolver** class, wherein its single-argument constructor calls **Assembly.LoadFrom** to load assemblies.

The **Microsoft.Exchange.Diagnostics.ChainedSerializationBinder** class has a **LoadType** method which loads classes from the assemblies in the current application context.

The exploitation process involves leveraging deserialization type conversion to invoke the single-argument constructor of **Microsoft.Exchange.DxStore.Common.DxSerializationUtil.SharedTypeResolver** class to load a custom assembly introducing malicious classes. Thereafter, utilizing deserialization type conversion to invoke the single-argument constructor of the malicious class enables Remote Code Execution (RCE).

However, there's a caveat since the .NET Framework 4 and onwards has disabled the ability to execute code in assemblies loaded from remote locations by default, which could lead to a **FileLoadException** being thrown when calling the **LoadFrom** method. A workaround is mentioned using SMB share to load assemblies from other machines.

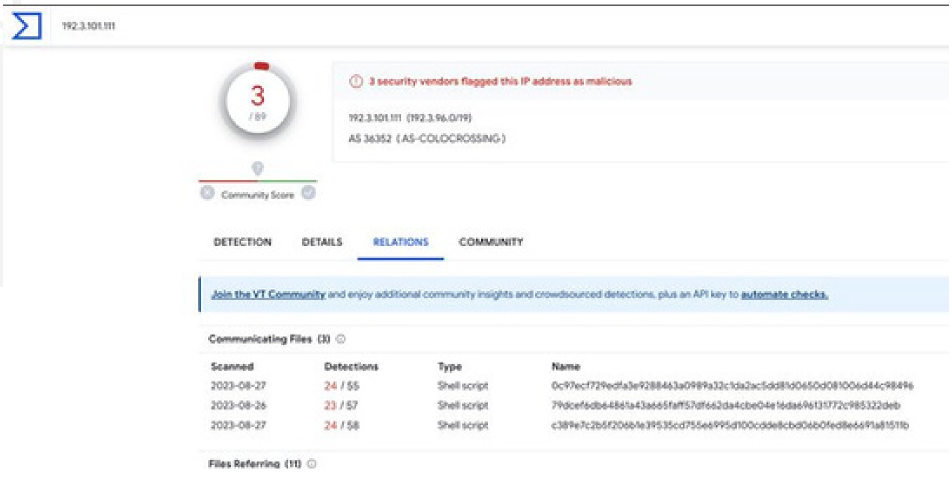
In order to bypass the whitelist of allowed classes for deserialization, the exploitation process requires to be paired with CVE-2023-21529 to utilize the generic class **Microsoft.Exchange.Data.MultiValuedProperty**.

The Proof of Concept (PoC) section provides XML snippets showing how to construct malicious objects to exploit this vulnerability, by setting the **TargetTypeForDeserialization** to a malicious value and providing an SMB path to load assemblies from or executing a malicious command like **calc.exe**.

This report represents a deep technical analysis of the CVE-2023-36745 vulnerability, providing insights into how it can be exploited to achieve remote code execution on a target Microsoft Exchange Server, by bypassing deserialization protections.

You can read the full report here.

🌶️ Trending Exploit



192.3.101.111

3 / 89

ⓘ 3 security vendors flagged this IP address as malicious

192.3.101.111 (192.3.96.0/19)
AS 36352 (AS-COLOCROSSING)

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Communicating Files (3)

Scanned	Detections	Type	Name
2023-08-27	24 / 55	Shell script	0c97ecf729edfa3e9288463a0989a32c1da2ac5dd81d0650d081006d44c98496
2023-08-26	23 / 57	Shell script	79dcef6db64861a43a665faff57df662da4cbe04e16da696131772c985322deb
2023-08-27	24 / 58	Shell script	c389e7c2b5f206b1e39535cd755e6995d100cdde8cbd06b0fed8e6691a81511b

Files Referring (11)

https://twitter.com/TLP_R3D/status/1716479835411714198

Cisco IOS XE Software Web UI has been identified to have vulnerabilities that are actively being exploited. A deeper look into the Indicators of Compromise (IoCs) provided shows a pattern of exploitation originating from specific IP addresses which share a unique HTML page. This report explores the identified IoCs and advises on the necessary vigilance to mitigate the risks associated with this exploitation.

Methods:

1. **Analysis of Provided IoCs**:
    - Investigated the list of IP addresses provided in relation to the active exploitation of Cisco IOS XE Software Web UI vulnerabilities.
    - Discovered that these IPs share an identical unique HTML page, which is a significant indicator of coordinated exploitation.
2. **Pivoting for Additional Indicators**:
    - Conducted a pivot analysis to uncover more indicators that could shed light on the exploitation activity.
    - The pivot revealed more indicators reinforcing the active exploitation of the said vulnerabilities.
3. **Monitoring and Alertness**:
    - Recommended a heightened level of alertness to monitor and mitigate potential exploitation from the identified IP addresses.
4. **Consultation of External Resources**:
    - Referred to the detailed information provided on the Talos Intelligence Blog regarding the active exploitation of Cisco IOS XE Software Web UI vulnerabilities.

Identified IoCs: Below are the IP addresses identified to be sharing an identical unique HTML page, which is a significant indicator of the ongoing exploitation:

- 205.185.123.17
- 209.141.34.83
- 154.53.63.93
- 192.3.101.111
- 92.223.30.129
- 95.168.191.172
- 192.227.196.186
- 108.177.235.177
- 92.38.132.181
- 92.38.169.180
- 192.109.119.29
- 154.53.56.231

🕯️ The Topic of the Week

```
user@SarlackLab:~/Catching-RedLine-Stealer$ ngrep RedLine-Stealer
```

https://twitter.com/Abjuri5t/status/1716512467650580903

RedLine Stealer is a notorious malware that operates by pilfering sensitive data from infected computers. It is typically classified as an "infostealer" due to its data theft capabilities. The malware is often utilized by cyber criminals for reconnaissance and initial access to networks. RedLine Stealer extracts a variety of data, including login credentials, session cookies, cryptocurrency keys, and system details. A notable breach attributable to RedLine Stealer is the 2023 hack of the Linus Tech Tips YouTube channel. In the face of its growing infamy, devising measures to catch and curb RedLine Stealer's activities is imperative.

Data Exfiltration Protocol: RedLine Stealer's data exfiltration mechanism initiates with communication to a hard-coded Command-and-Control (C2) server using a unique cleartext protocol. This protocol outlines a structured format for data transmission, including connection initiation, call classification, authorization, and data sending. Each communication is tagged with specific 'Id numbers', providing a well-organized structure for data exfiltration. A specific pattern observed is the use of a string "http://tempuri.org/" before an entity's classification, a remnant of improperly implemented ASP.Net web services. This pattern can be employed to create network signatures for detecting RedLine Stealer data exfiltration.

Command-and-Control Meta-Analysis: RedLine Stealer's C2 infrastructure presents a blend of domain names and hard-coded IP addresses for establishing connections. Notably, about two-thirds of the domain names are registered under *.xyz and *.top top-level domains, often leveraging Dynamic DNS (DDNS) services. However, a majority of RedLine payloads, around 80%, directly connect to hard-coded IP addresses, which are often hosted on bulletproof hosting providers or compromised infrastructure.

Catching the RedLine: Efficient strategies to mitigate the RedLine Stealer include:

- **Protect:** Employ DNS sinkholes to redirect domain resolution to benign servers, particularly targeting domains such as *.xyz, *.top, *.duckdns.org, and *.ddns.net which are commonly used by RedLine Stealer. Utilizing IP lists from reliable threat intelligence platforms like ThreatFox can also help in detecting and blocking RedLine C2 connections.
- **Detect:** Layer defenses with detection capabilities to alert on potential RedLine communications to known servers. Utilizing network signatures to exploit patterns in RedLine's custom protocol can provide a viable detection mechanism.

HADESS

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:

WWW.HADESS.IO

Threat Radar

WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.