telelink
business
services

Monthly Security Bulletin

MAY/24

Advanced Security
Operations Center

tbs.tech | simplify the complex

This security bulletin is powered by

Telelink Business Services'

Advanced Security Operations Center

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

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

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

Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!

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

⬛ Lite Plan

🟦 Professional Plan (incl. all from Lite)

🟧 Advanced Plan (incl. all from Professional)

What is inside:

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

Table of Contents

1. New XZ backdoor scanner detects implant in any Linux binary

Firmware security firm Binarly has released a free online scanner to detect Linux executables impacted by the XZ Utils supply chain attack, tracked as CVE-2024-3094.

CVE-2024-3094 is a supply chain compromise in XZ Utils, a set of data compression tools and libraries used in many major Linux distributions.

Late last month, Microsoft engineer Andres Freud discovered the backdoor in the latest version of the XZ Utils package while investigating unusually slow SSH logins on Debian Sid, a rolling release of the Linux distribution.

The backdoor was introduced by a pseudonymous contributor to XZ version 5.6.0, which remained present in 5.6.1. However, only a few Linux distributions and versions following a "bleeding edge" upgrading approach were impacted, with most using an earlier, safe library version.

Following the discovery of the backdoor, a detection and remediation effort was started, with CISA proposing downgrading the XZ Utils 5.4.6 Stable and hunting for and reporting any malicious activity.

The XZ scanner

Binarly says the approach taken so far in the threat mitigation efforts relies on simple checks such as byte string matching, file hash blocklisting, and YARA rules, which could lead to false positives.

This approach can trigger significant alert fatigue and doesn't help detect similar backdoors on other projects.

To address this problem, Binarly developed a dedicated scanner that would work for the particular library and any file carrying the same backdoor.

> *"Such a complex and professionally designed comprehensive implantation framework is not developed for a one-shot operation. It could already be deployed elsewhere or partially reused in other operations. That's exactly why we started focusing on more generic detection for this complex backdoor."*
>
> *- Binarly*

Binarly's detection method employs static analysis of binaries to identify tampering of transitions in GNU Indirect Function (IFUNC).

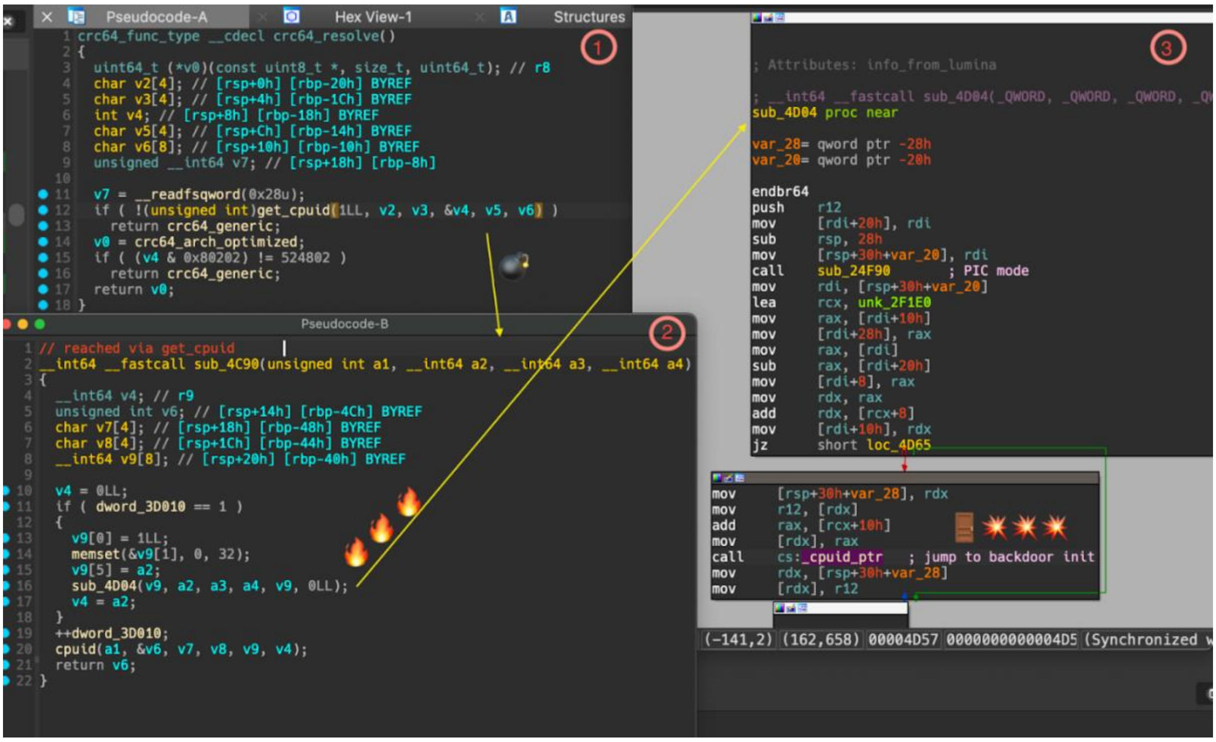
Specifically, the scanner examines the transitions marked as suspicious during the implantation of malicious IFUNC resolvers. The GCC compiler's IFUNC attribute allows developers to create multiple versions of the same function that are then selected at runtime based on various criteria, such as the processor type.

"One of the core techniques used by the XZ backdoor to gain initial control during execution is the GNU Indirect Function (ifunc) attribute for the GCC compiler to resolve indirect function calls in runtime," explains Binarly.

"The implanted backdoor code initially intercepts or hooks execution.

"It modifies ifunc calls to replace a check "is_arch_extension_supported" which should simply invoke "cpuid" to insert a call to "_get_cpuid" which is exported by the payload object file (i.e., liblzma_la-crc64-fast.o) and which calls malformed _get_cpuid() which is implanted into the code shown in the figure below."

The backdoor exploits this mechanism by modifying IFUNC calls to intercept or hook execution, resulting in the insertion of malicious code.


Pseudocode-A
Hex View-1
Structures
1
Pseudocode-B
2
3
(-141,2) (162,658) 00004D57 00000000000004D5 (Synchronized w

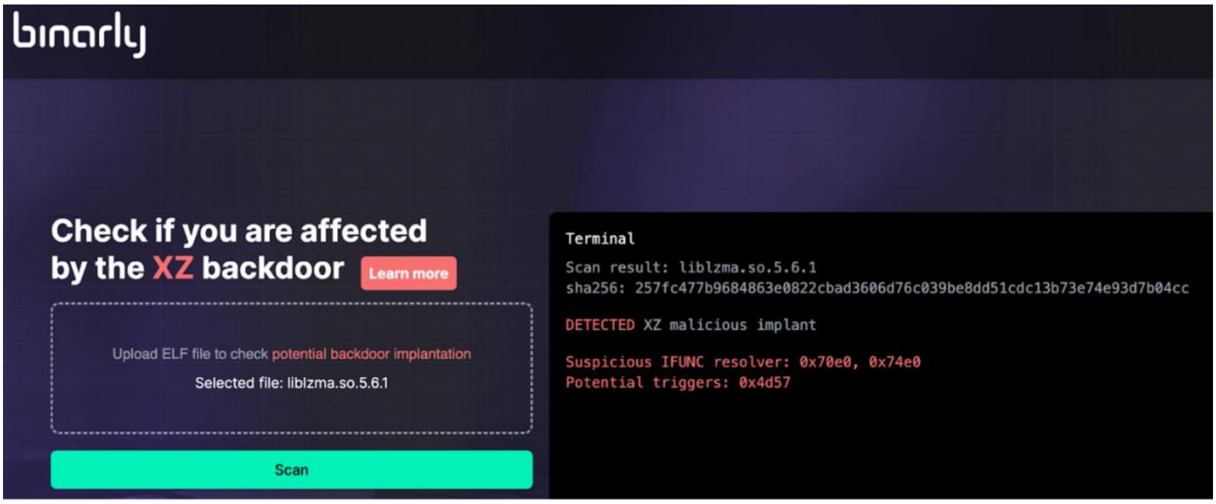
```
crc64_func_type __cdecl crc64_resolve()
{
  uint64_t (*v0)(const uint8_t *, size_t, uint64_t); // r8
  char v2[4]; // [rsp+0h] [rbp-20h] BYREF
  char v3[4]; // [rsp+4h] [rbp-1Ch] BYREF
  int v4; // [rsp+8h] [rbp-18h] BYREF
  char v5[4]; // [rsp+Ch] [rbp-14h] BYREF
  char v6[8]; // [rsp+10h] [rbp-10h] BYREF
  unsigned __int64 v7; // [rsp+18h] [rbp-8h]

  v7 = __readfsqword(0x28u);
  if ( !(unsigned int)get_cpuid(1LL, v2, v3, &v4, v5, v6) )
    return crc64_generic;
  v0 = crc64_arch_optimized;
  if ( (v4 & 0x80202) != 524802 )
    return crc64_generic;
  return v0;
}
```

```
// reached via get_cpuid
__int64 __fastcall sub_4C90(unsigned int a1, __int64 a2, __int64 a3, __int64 a4)
{
  __int64 v4; // r9
  unsigned int v6; // [rsp+14h] [rbp-4Ch] BYREF
  char v7[4]; // [rsp+18h] [rbp-48h] BYREF
  char v8[4]; // [rsp+1Ch] [rbp-44h] BYREF
  __int64 v9[8]; // [rsp+20h] [rbp-40h] BYREF

  v4 = 0LL;
  if ( dword_3D010 == 1 )
  {
    v9[0] = 1LL;
    memset(&v9[1], 0, 32);
    v9[5] = a2;
    sub_4D04(v9, a2, a3, a4, v9, 0LL);
    v4 = a2;
  }
  ++dword_3D010;
  cpuid(a1, &v6, v7, v8, v9, v4);
  return v6;
}
```

```
; Attributes: info_from_lumina

; __int64 __fastcall sub_4D04(_QWORD, _QWORD, _QWORD, _QW
sub_4D04 proc near

var_28= qword ptr -28h
var_20= qword ptr -20h

endbr64
push    r12
mov     [rdi+20h], rdi
sub     rsp, 28h
mov     [rsp+30h+var_20], rdi
call    sub_24F90       ; PIC mode
mov     rdi, [rsp+30h+var_20]
lea     rcx, unk_2F1E0
mov     rax, [rdi+10h]
mov     [rdi+28h], rax
mov     rax, [rdi]
sub     rax, [rdi+20h]
mov     [rdi+8], rax
mov     rdx, rax
add     rdx, [rcx+8]
mov     [rdi+10h], rdx
jz      short loc_4D65

mov     [rsp+30h+var_28], rdx
mov     r12, [rdx]
add     rax, [rcx+10h]
mov     [rdx], rax
call    cs:_cpuid_ptr    ; jump to backdoor init
mov     rdx, [rsp+30h+var_28]
mov     [rdx], r12
```

Analysis steps to detect execution flow anomalies (Binarly)

Binarly's scanner increases detection as it scans for various supply chain points beyond just the XZ Utils project, and the results are of much higher confidence.



Check if you are affected by the XZ backdoor

Upload ELF file to check potential backdoor implantation

Selected file: liblzma.so.5.6.1

```
Terminal
Scan result: liblzma.so.5.6.1
sha256: 257fc477b9684863e0822cbad3606d76c039be8dd51cdc13b73e74e93d7b04cc

DETECTED XZ malicious implant

Suspicious IFUNC resolver: 0x70e0, 0x74e0
Potential triggers: 0x4d57
```

Online scanner in action

"This detection is based on behavioral analysis and can detect any variants automatically if a similar backdoor is implanted somewhere else," Binarly's lead security researcher and CEO, Alex Matrosov, told BleepingComputer.

"Even after recompilation or code changes, we will detect it," Matrosov further told BleepingComputer.

The backdoor scanner is available online at xz.fail, where people can upload their binary files for unlimited free checks.

Update 4/2 - Binarly has made a free API available to accomodate bulk scans for those who need it.

Source: https://www.bleepingcomputer.com/news/security/new-xz-backdoor-scanner-detects-implant-in-any-linux-binary/

2. Surveillance by the New Microsoft Outlook App

The ProtonMail people are accusing Microsoft's new Outlook for Windows app of conducting extensive surveillance on its users. It shares data with advertisers, a lot of data:

The window informs users that Microsoft and those 801 third parties use their data for a number of purposes, including to:

- Store and/or access information on the user's device
- Develop and improve products
- Personalize ads and content
- Measure ads and content
- Derive audience insights
- Obtain precise geolocation data
- Identify users through device scanning

Commentary.

Source: https://www.schneier.com/blog/archives/2024/04/surveillance-by-the-new-microsoft-outlook-app.html

3. Notepad++ needs your help in "parasite website" shutdown

The Notepad++ project is seeking the public's help in taking down a copycat website that closely impersonates Notepad++ but is not affiliated with the project.

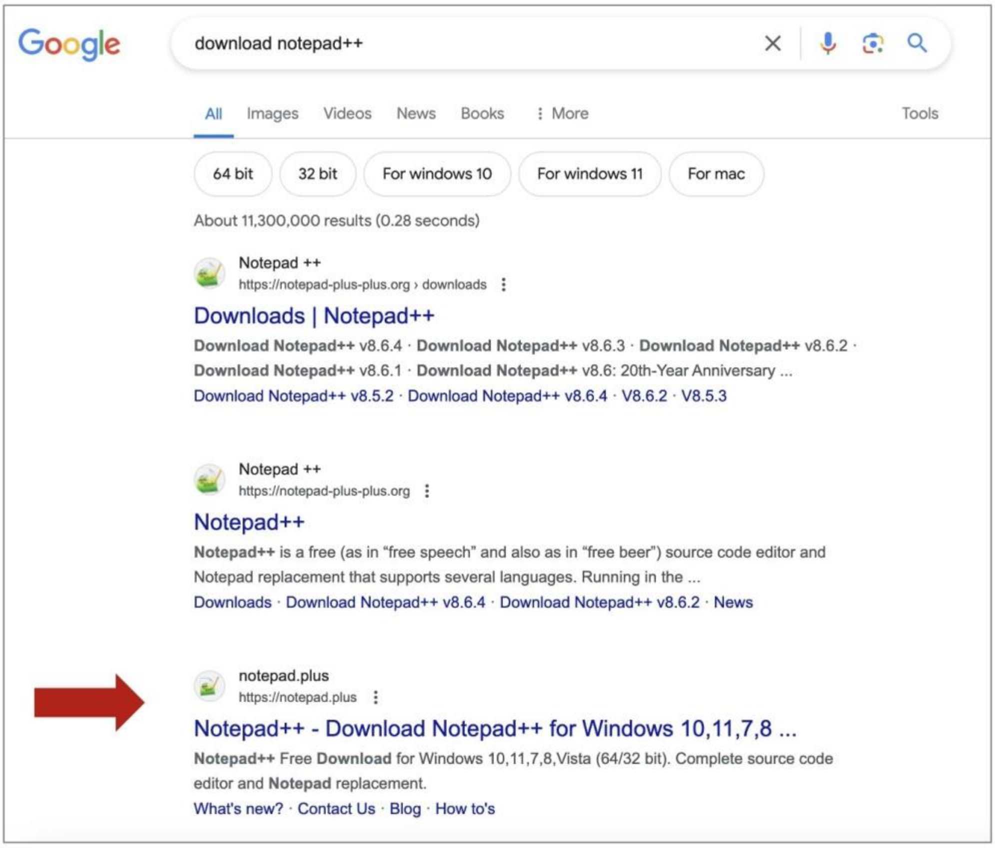
Although, at the time of writing, the lookalike website takes visitors to the official Notepad++ downloads page, there is some concern that it could pose security threats—for example, if it starts pushing malicious releases or spam someday either deliberately or as a result of a hijack.

"Help us to take down the parasite website"

Notepad++, the free and open-source text and source code editor project has appealed to everyone to help shut down a lookalike website, **notepad[.]plus** that uses the project's branding, and even manages to rank high in search engine results alongside the official website, **notepad-plus-plus.org**.

"I've received numerous complaints via email, social media, and forums regarding a website that poses a significant threat to our community," writes Don Ho, the original developer of Notepad++.

The site in question **notepad[.]plus,** according to Ho, comes up prominently in search results when users look up "download Notepad++", as confirmed by BleepingComputer:



About 11,300,000 results (0.28 seconds)

Notepad ++
https://notepad-plus-plus.org › downloads

Downloads | Notepad++

Download Notepad++ v8.6.4 · **Download Notepad++** v8.6.3 · **Download Notepad++** v8.6.2 · **Download Notepad++** v8.6.1 · **Download Notepad++** v8.6: 20th-Year Anniversary ...

Download Notepad++ v8.5.2 · Download Notepad++ v8.6.4 · V8.6.2 · V8.5.3

Notepad ++
https://notepad-plus-plus.org

Notepad++

Notepad++ is a free (as in "free speech" and also as in "free beer") source code editor and Notepad replacement that supports several languages. Running in the ...

Downloads · Download Notepad++ v8.6.4 · Download Notepad++ v8.6.2 · News

notepad.plus
https://notepad.plus

Notepad++ - Download Notepad++ for Windows 10,11,7,8 ...

Notepad++ Free **Download** for Windows 10,11,7,8,Vista (64/32 bit). Complete source code editor and **Notepad** replacement.

What's new? · Contact Us · Blog · How to's

The lookalike website appears prominently in search results
(BleepingComputer)

"Some users have mistakenly believed that [it] is the official Notepad++ website. This confusion has led to frustration and potential security risks," states the dev.

The website in question does contain a clear disclaimer at the bottom spelling out that it's "an unofficial fan website" and "not affiliated" with the project.

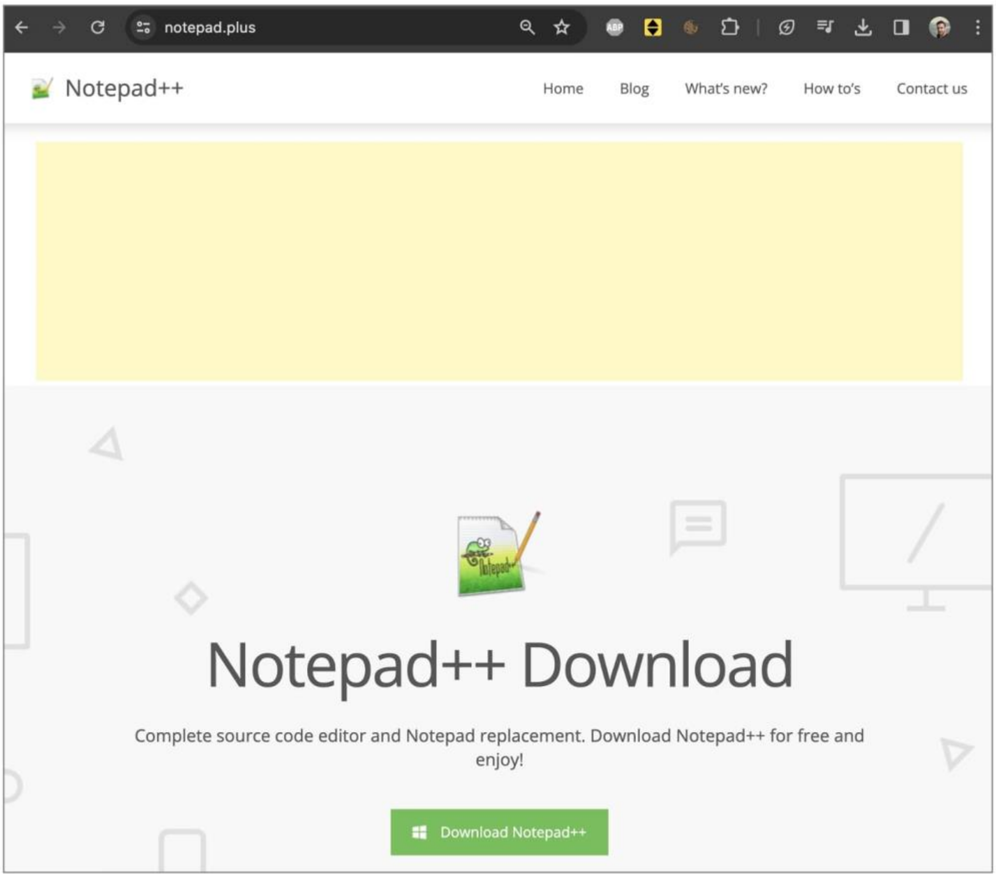
> *Notepad++ is a trademark of Don HO. Notepad[.]plus is not affiliated, sponsored or endorsed by Don HO in any ways. This is an unofficial fan website created for general information/educational purpose only. Any context found in this website is our personal opinions and do not purport to reflect the opinions or views of Don HO or its representatives. All other trademarks are the property of their respective owners.*

Fan site presently **redirects to official releases**

It is worth noting the fan site directs visitors to the official Notepad++ releases downloads page hosted on **notepad-plus-plus.org**.

Despite this, Ho alleges that "this site harbors a hidden agenda" and is "is riddled with malicious advertisements on every page."

Such ads, according to Ho, could deceive unsuspecting Notepad++ users into clicking on links that generate revenue for admins of the unofficial website.



Notepad++ Download

Complete source code editor and Notepad replacement. Download Notepad++ for free and enjoy!

Unofficial Notepad++ fan site *(BleepingComputer)*

"The true purpose" of, what Ho has called a "parasite website" is, according to him, "to divert traffic away from the legitimate Notepad++ website, notepad-plus-plus.org" which potentially "compromises user safety and undermines the integrity of our community."

BleepingComputer checked both the latest version of the **notepad[.]plus** website and archived copies from the past.

While the site's home page does contain an area at the top that appears to be purposed for hosting ad banners, we did not find an active ad running in that space or any other promotional links on the website. We did notice multiple educational and how-to blog posts on using Notepad++.

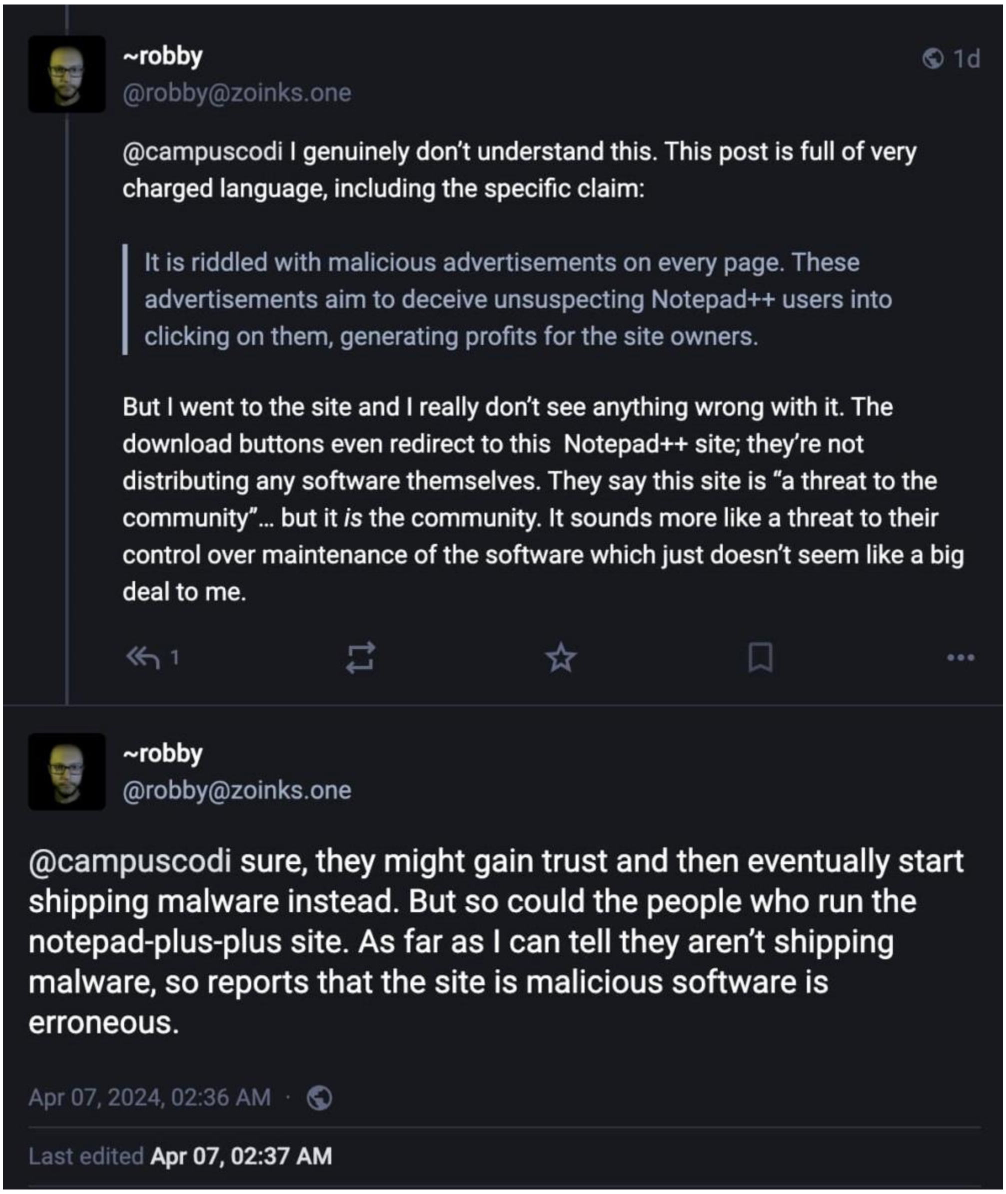
The developer urges everyone to report the website via Google Safebrowsing's "report malicious software" web form.

Such an approach, however, may not be fruitful given that presently **no malicious software releases** are being pushed by the unofficial site, or anything that warrants it to be classified as blatantly unsafe. Moreover, the aforementioned disclaimer put in place by the website may safeguard it against such accusations.

The Notepad++ logo and branding used by the website, on the other hand, could still fall afoul of trademark rules.

Technology reporter Catalin Cimpanu shared Notepad++'s blog post in a Mastodon thread.

Many community members began reporting the unofficial website, although, one developer echoed that reporting the site for shipping malicious software may be "erroneous."



~robby
@robby@zoinks.one
1d

@campuscodi I genuinely don't understand this. This post is full of very charged language, including the specific claim:

> It is riddled with malicious advertisements on every page. These advertisements aim to deceive unsuspecting Notepad++ users into clicking on them, generating profits for the site owners.

But I went to the site and I really don't see anything wrong with it. The download buttons even redirect to this Notepad++ site; they're not distributing any software themselves. They say this site is "a threat to the community"… but it *is* the community. It sounds more like a threat to their control over maintenance of the software which just doesn't seem like a big deal to me.

~robby
@robby@zoinks.one

@campuscodi sure, they might gain trust and then eventually start shipping malware instead. But so could the people who run the notepad-plus-plus site. As far as I can tell they aren't shipping malware, so reports that the site is malicious software is erroneous.

Apr 07, 2024, 02:36 AM ·

Last edited Apr 07, 02:37 AM

A developer disagrees that lookalike site poses risks *(Mastodon)*

"I genuinely don't understand this. This post is full of very charged language... But I went to the site and I really don't see anything wrong with it," writes Robby Zambito.

"The download buttons even redirect to this Notepad++ site; they're not distributing any software themselves. They say this site is "a threat to the community"... but it **is** the community. It sounds more like a threat to their control over maintenance of the software which just doesn't seem like a big deal to me."

"Sure, they might gain trust and then eventually start shipping malware instead. But so could the people who run the notepad-plus-plus site," states Zambito.

The observation is especially relevant at a time when large-scale open-source projects, such as the XZ utility, had a backdoor injected in it by a developer who gained the trust of official project maintainers but went rogue. Similar stories of "vetted" researchers contributing malicious code to official projects aren't unheard of.

Such cases of wrongdoing are eventually caught, thanks to the numerous sharp-eyed community members who constantly scrutinize the open source ecosystem.

Given the popularity of Notepad++, its users are also frequently targeted with counterfeit trojanized versions by threat actors. As such, consuming open source projects like Notepad++ from their official websites and repositories remains a much safer approach than otherwise.

Source: https://www.bleepingcomputer.com/news/security/notepad-plus-plus-needs-your-help-in-parasite-website-shutdown/

4. Security Vulnerability of HTML Emails

A This is a newly discovered email vulnerability:

> The email your manager received and forwarded to you was something completely innocent, such as a potential customer asking a few questions. All that email was supposed to achieve was being forwarded to you. However, the moment the email appeared in your inbox, it changed. The innocent pretext disappeared and the real phishing email became visible. A phishing email you *had* to trust because you knew the sender and they even confirmed that they had forwarded it to you.
>
> This attack is possible because most email clients allow CSS to be used to style HTML emails. When an email is forwarded, the position of the original email in the DOM usually changes, allowing for CSS rules to be selectively applied only when an email has been forwarded.
>
> An attacker can use this to include elements in the email that appear or disappear depending on the context in which the email is viewed. Because they are usually invisible, only appear in certain circumstances, and can be used for all sorts of mischief, I'll refer to these elements as *kobold letters*, after the elusive sprites of mythology.

I can certainly imagine the possibilities.

Source: https://www.schneier.com/blog/archives/2024/04/security-vulnerability-of-html-emails.html

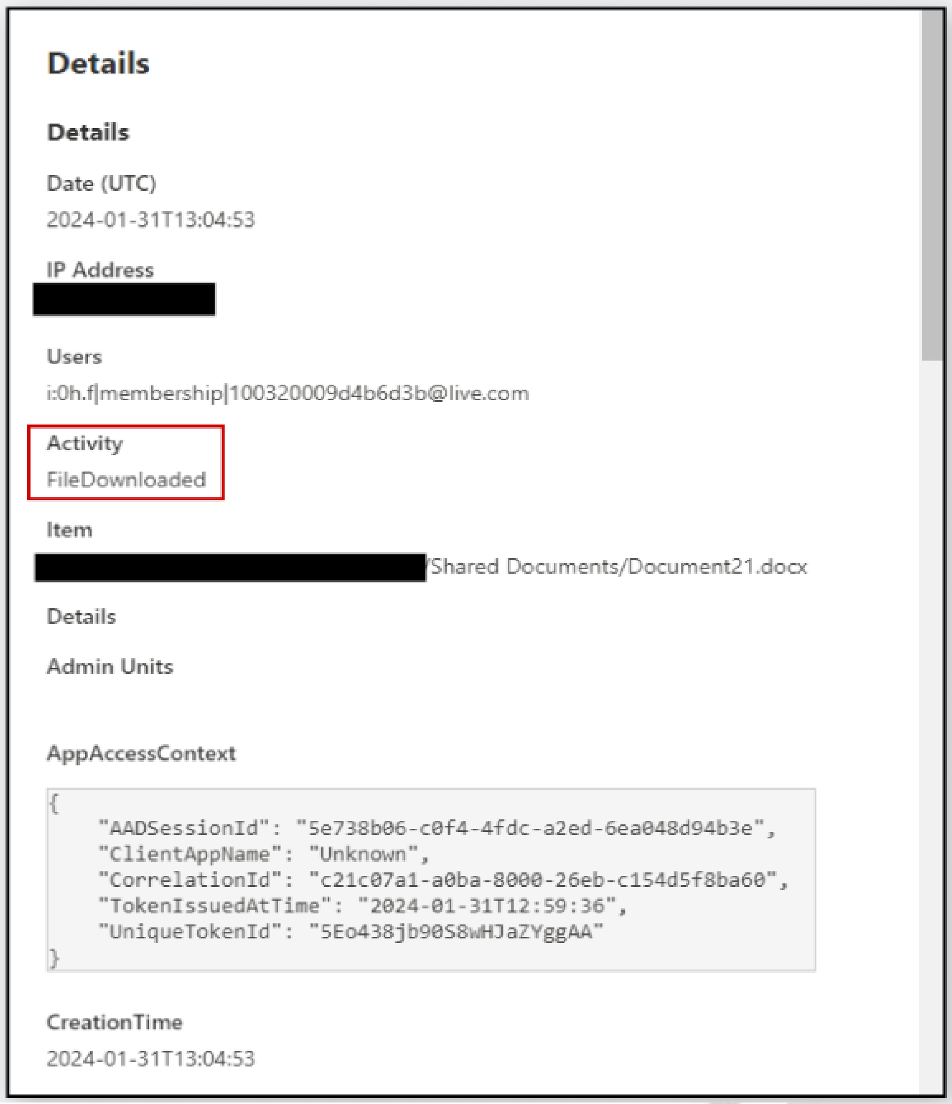
5. New SharePoint flaws help hackers evade detection when stealing files

Researchers have discovered two techniques that could enable attackers to bypass audit logs or generate less severe entries when downloading files from SharePoint.

Microsoft SharePoint is a web-based collaborative platform that integrates with Microsoft Office and 365, primarily as a document management and data storage system.

Many companies use it for document management and collaboration, creating websites and corporate intranets, automating complex workflows, and enterprise content management applications.

Due to the sensitivity of SharePoint data, many companies audit sensitive events, like the downloading of data, to trigger alerts in cloud access security tools, data loss prevention tools, and security information and event management platforms (SIEMs).



Details

Details

Date (UTC)
2024-01-31T13:04:53

IP Address
[redacted]

Users
i:0h.f|membership|100320009d4b6d3b@live.com

Activity
FileDownloaded

Item
[redacted]/Shared Documents/Document21.docx

Details

Admin Units

AppAccessContext

```
{
    "AADSessionId": "5e738b06-c0f4-4fdc-a2ed-6ea048d94b3e",
    "ClientAppName": "Unknown",
    "CorrelationId": "c21c07a1-a0ba-8000-26eb-c154d5f8ba60",
    "TokenIssuedAtTime": "2024-01-31T12:59:36",
    "UniqueTokenId": "5Eo438jb90S8wHJaZYggAA"
}
```

CreationTime
2024-01-31T13:04:53

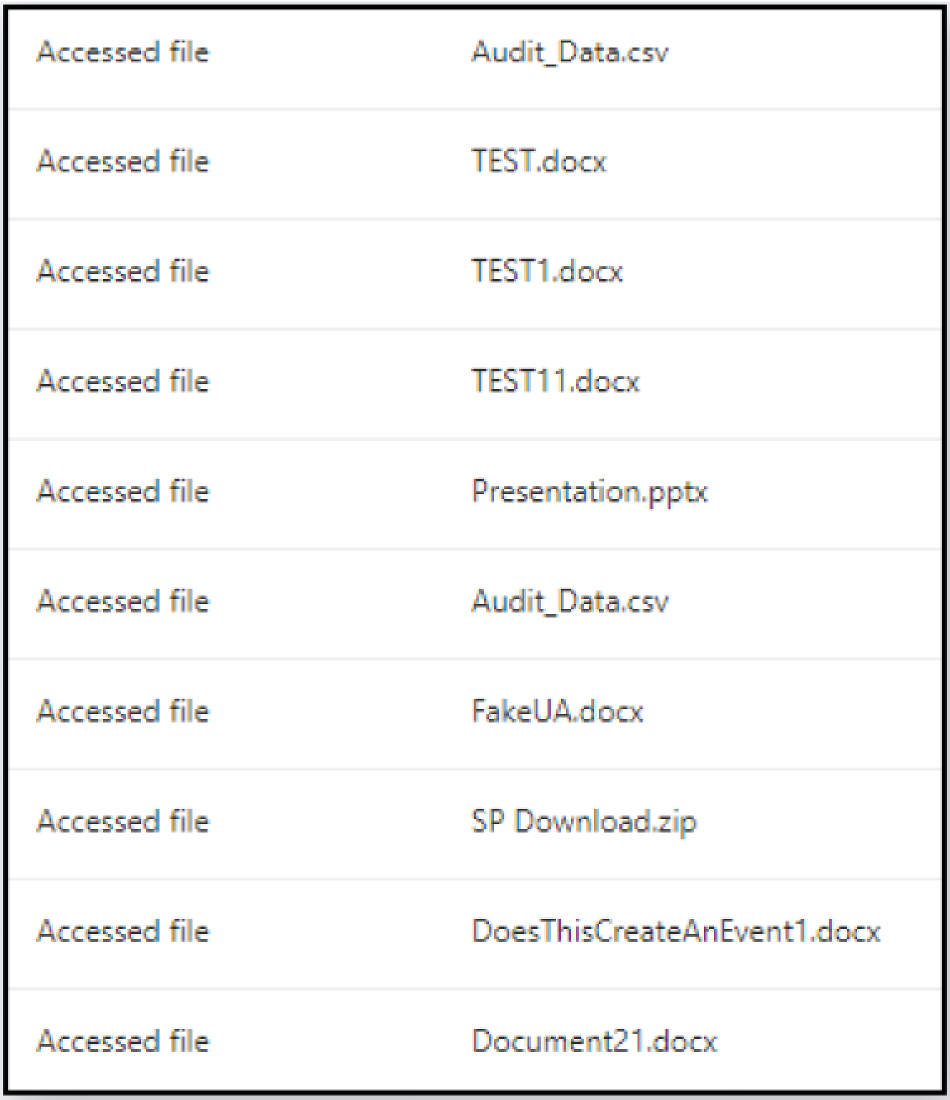
A file download event in SharePoint logs
Source: Varonis

Researchers at the Varonis Threat Labs have devised two simple techniques that enable users to bypass audit logs or generate less sensitive events by downloading data a certain way or disguising it as data syncing actions.

Silent data exfiltration

The first technique described in Varonis' report takes advantage of SharePoint's "Open in App" feature, which allows users to open documents with applications like Microsoft Word instead of using the web browser, which is the default option.

Utilizing this feature does not generate a "FileDownloaded" event in SharePoint's audit logs but instead creates an "Access" event that administrators may ignore.

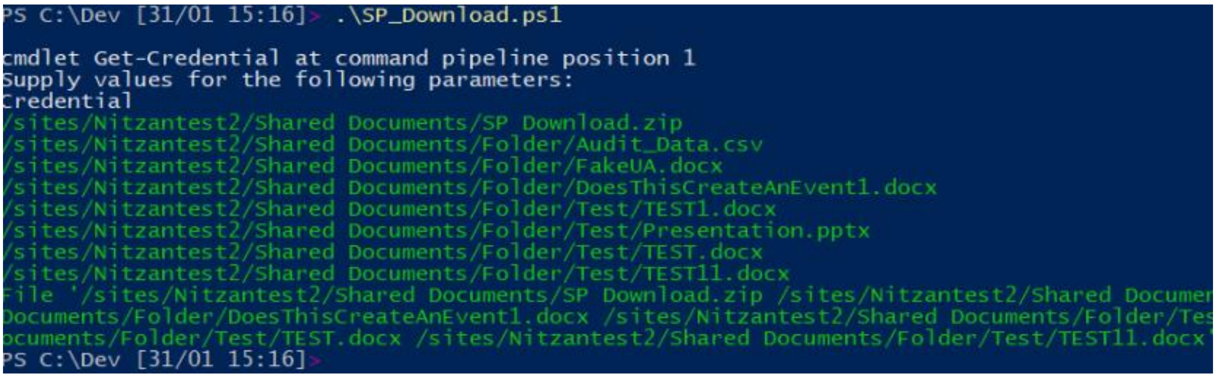


Accessed file	Audit_Data.csv
Accessed file	TEST.docx
Accessed file	TEST1.docx
Accessed file	TEST11.docx
Accessed file	Presentation.pptx
Accessed file	Audit_Data.csv
Accessed file	FakeUA.docx
Accessed file	SP Download.zip
Accessed file	DoesThisCreateAnEvent1.docx
Accessed file	Document21.docx

Multiple access events created from a series of file exfiltrations
Source: Varonis

Opening the file from a cloud location creates a shell command with the non-expiring URL from the file's location on the cloud endpoint, which someone can use to download the file without restrictions.

Varonis also notes that misuse of "Open in App" can be both manual and automated, using a custom PowerShell script that could enable someone to exfiltrate large lists of files quickly.



```
PS C:\Dev [31/01 15:16]> .\SP_Download.ps1

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
/sites/Nitzantest2/Shared Documents/SP Download.zip
/sites/Nitzantest2/Shared Documents/Folder/Audit_Data.csv
/sites/Nitzantest2/Shared Documents/Folder/FakeUA.docx
/sites/Nitzantest2/Shared Documents/Folder/DoesThisCreateAnEvent1.docx
/sites/Nitzantest2/Shared Documents/Folder/Test/TEST1.docx
/sites/Nitzantest2/Shared Documents/Folder/Test/Presentation.pptx
/sites/Nitzantest2/Shared Documents/Folder/Test/TEST.docx
/sites/Nitzantest2/Shared Documents/Folder/Test/TEST11.docx
File '/sites/Nitzantest2/Shared Documents/SP Download.zip /sites/Nitzantest2/Shared Documer
Documents/Folder/DoesThisCreateAnEvent1.docx /sites/Nitzantest2/Shared Documents/Folder/Tes
ocuments/Folder/Test/TEST.docx /sites/Nitzantest2/Shared Documents/Folder/Test/TEST11.docx'
PS C:\Dev [31/01 15:16]>
```

PowerShell script automating the file exfiltration

Source: Varonis

The second technique involves spoofing the User-Agent string of the file access requests to mimic Microsoft SkyDriveSync, a service used for file synchronization between SharePoint and a user's local computer.

This trick makes the file downloads performed via the browser or Microsoft Graph API appear in the logs as data syncing events ("FileSyncDownloadedFull"), reducing the likelihood of scrutiny by security teams.

In this case, too, the alteration of the User-Agent string and subsequent file exfiltration can be done manually or via a PowerShell script to automate the process.

Mitigation

Varonis disclosed these bugs in November 2023, and Microsoft added the flaws to a patch backlog for future fixing.

However, the issues were rated as moderate severity, so they won't receive immediate fixes. Therefore, SharePoint admins should be aware of these risks and learn to identify and mitigate them until patches become available.

Varonis recommends monitoring for high volumes of access activity within a short timeframe and the introduction of new devices from unusual locations, which could be signs of unauthorized data exfiltration.

Moreover, security teams are recommended to scrutinize sync events for anomalies in frequency and data volumes and try to identify unusual activity patterns.

BleepingComputer has reached out to Microsoft to learn more about their plans for addressing the issues presented by Varonis, and a spokesperson has sent the following statement:

> *We're aware of this report and our customers do not need to take action. We have confirmed that the product is performing as expected, by detecting a file accessed and reporting that through the audit log.*

Security products and vendors should be using FileAccessed, FileDownloaded, plus two potential sync-related signals, FileSyncDownloadedFull and FileSyncDownloadedPartial audit events to monitor for file access. - Microsoft spokesperson

Update 4/10 - Added Microsoft statement

Source: https://www.bleepingcomputer.com/news/security/new-sharepoint-flaws-help-hackers-evade-detection-when-stealing-files/

6. New Spectre v2 attack impacts Linux systems on Intel CPUs

Researchers have demonstrated the "first native Spectre v2 exploit" for a new speculative execution side-channel flaw that impacts Linux systems running on many modern Intel processors.

Spectre V2 is a new variant of the original Spectre attack discovered by a team of researchers at the VUSec group from VU Amsterdam.

The researchers also released a tool that uses symbolic execution to identify exploitable code segments within the Linux kernel to help with mitigation.

The new finding underscores the challenges in balancing performance optimization with security, which makes addressing fundamental CPU flaws complicated even six years after the discovery of the original Spectre.

Spectre spooks Linux

Speculative execution is a performance optimization technique where modern processors guess what instructions will be executed next and start implementing them before they know they are needed. As modern processors are extremely powerful, they can predict multiple paths a program may take and execute them simultaneously.

If one of the guesses is correct, there is an increase in application performance. If the guesses are wrong, the CPU throws away the previous work and proceeds as usual without changing performance.

However, while this feature improves performance, it also introduces security risks by leaving traces of privileged data in CPU caches, which attackers can potentially access.

This data can include account passwords, encryption keys, sensitive personal or corporate information, software code, and more.

Two attack methods are Branch Target Injection (BTI), which involves manipulating the CPU's branch prediction to execute unauthorized code paths, and Branch History Injection (BHI), which manipulates branch history to cause speculative execution of chosen gadgets (code paths), leading to data leakage.

Intel has already assigned CVE-2022-0001 and CVE-2022-0002 to BTI and BHI, respectively, while CVE-2024-2201 involves a new Spectre v2 exploit that works against the Linux kernel.

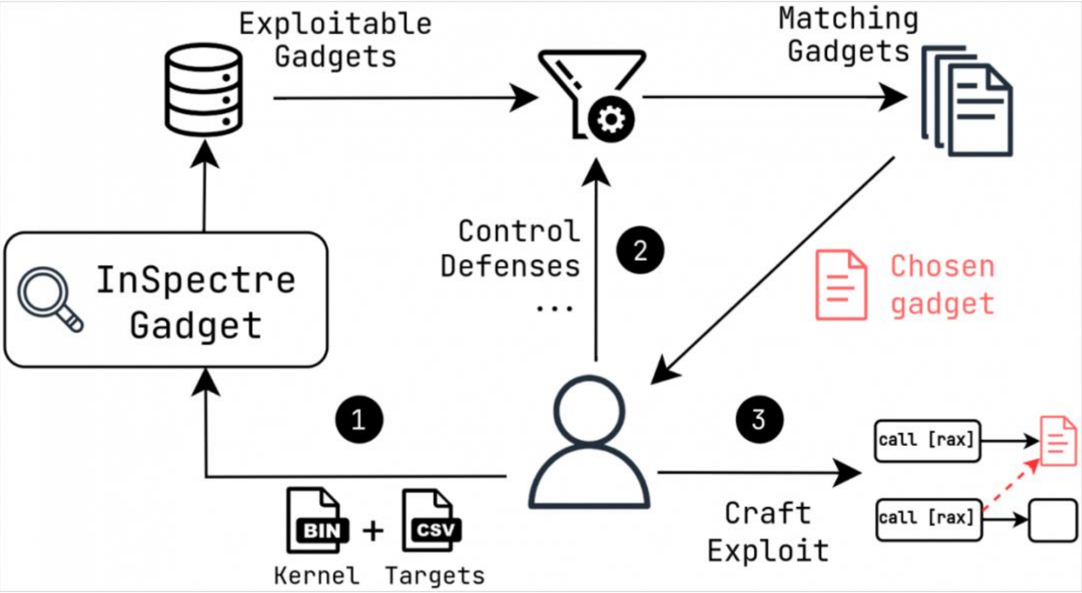
As the CERT Coordination Center (CERT/CC) disclosed yesterday, the new flaw, tracked as CVE-2024-2201, allows unauthenticated attackers to read arbitrary memory data by leveraging speculative execution, bypassing present security mechanisms designed to isolate privilege levels.

"An unauthenticated attacker can exploit this vulnerability to leak privileged memory from the CPU by speculatively jumping to a chosen gadget," reads the CERT/CC announcement.

"Current research shows that existing mitigation techniques of disabling privileged eBPF and enabling (Fine)IBT are insufficient in stopping BHI exploitation against the kernel/hypervisor."

An exploit demonstrating the new Spectre V2 flaw can be seen in the video below.

Current mitigations are designed around isolating exploitable gadgets to remove the attack surface. However, the VUSec researchers, through their custom 'InSpectre Gadget' analysis tool, demonstrated that exploitable gadgets in the Linux kernel remain.



InSpectreGadget function overview (VUSec)

Microsoft has released updated guidance to mitigate CVE-2024-2201 as part of the April Patch Tuesday security updates, but the mitigations are disabled by default to allow users and admins to evaluate performance results.

However, the risk remains for Linux distributions, with the following impacted entities responding to the situation:

- **Illumos** – Planning to add BHI mitigations this week.
- **Linux Foundation** – Issue to be handled by the standard hardware vulnerability procedure followed by the Linux kernel development team.
- **Red Hat** – Unprivileged eBPF is disabled by default on RHEL, so the issue isn't exploitable in standard configurations.

- **SUSE Linux** – Confirmed impact.
- **Triton Data Center** – Recommended updating to SmartOS 20240418.
- **Xen** – CERT/CC independently verified impact.

Intel has also updated its mitigation recommendations for Spectre v2 and now proposes disabling unprivileged Extended Berkeley Packet Filter (eBPF) functionality, enabling Enhanced Indirect Branch Restricted Speculation (eIBRS), and enabling Supervisor Mode Execution Protection (SMEP).

Moreover, Intel recommends adding LFENCE (Load Fence) instructions to specific locations in the code to serve as serialization points and implementing software sequences that clear the Branch History Buffer (BHB) for transitions between different security domains.

The hardware vendor has indicated that future processors will include mitigations for BHI and potentially other speculative execution vulnerabilities.

For a complete list of impacted Intel processors to the various speculative execution side-channel flaws, check this page updated by the vendor.

Source: https://www.bleepingcomputer.com/news/security/new-spectre-v2-attack-impacts-linux-systems-on-intel-cpus/

7. Vulnerability in some TP-Link routers could lead to factory reset

Cisco Talos' Vulnerability Research team has disclosed 10 vulnerabilities over the past three weeks, including four in a line of TP-Link routers, one of which could allow an attacker to reset the devices' settings back to the factory default.

A popular open-source software for internet-of-things (IoT) and industrial control systems (ICS) networks also contains multiple vulnerabilities that could be used to arbitrarily create new files on the affected systems or overwrite existing ones.

For Snort coverage that can detect the exploitation of these vulnerabilities, download the latest rule sets from Snort.org, and our latest Vulnerability Advisories are always posted on Talos Intelligence's website.

Denial-of-service, remote code execution vulnerabilities in TP-Link AC1350 router

Talos researchers recently discovered four vulnerabilities in the TP-Link AC1350 wireless router. The AC1350 is one of many routers TP-Link produces and is designed to be used on home networks.

TALOS-2023-1861 (CVE-2023-49074) is a denial-of-service vulnerability in the TP-Link Device Debug Protocol (TDDP). An attacker could exploit this vulnerability by sending a series of unauthenticated packets to the router, potentially causing a denial of service and forcing the device to reset to its factory settings.

However, the TDDP protocol is only ~~denial of service~~available for roughly 15 minutes after a device reboot.

The TDDP protocol is also vulnerable to TALOS-2023-1862 (CVE-2023-49134 and CVE-2023-49133), a command execution vulnerability that could allow an attacker to execute arbitrary code on the targeted device.

There is another remote code execution vulnerability, TALOS-2023-1888 (CVE-2023-49912, CVE-2023-49909, CVE-2023-49907, CVE-2023-49908, CVE-2023-49910, CVE-2023-49906, CVE-2023-49913, CVE-2023-49911) that is triggered if an attacker sends an authenticated HTTP request to the targeted device. This exploit includes multiple CVEs because an attacker could overflow multiple buffers to cause this condition.

TALOS-2023-1864 (CVE-2023-48724) also exists in the device's web interface functionality. An adversary could exploit this vulnerability by sending an unauthenticated HTTP request to the targeted device, thus causing a denial of service.

Multiple vulnerabilities in OAS Platform

Discovered by Jared Rittle.

Open Automation Software's OAS Platform is an IoT gateway and protocol bus. It allows administrators to connect PLCs, devices, databases and custom apps.

There are two vulnerabilities — TALOS-2024-1950 (CVE-2024-21870) and TALOS-2024-1951 (CVE-2024-22178) — that exist in the platform that can lead to arbitrary file creation or overwrite. An attacker can send a sequence of requests to trigger these vulnerabilities.

An adversary could also send a series of requests to exploit TALOS-2024-1948 (CVE-2024-24976), but in this case, the vulnerability leads to a denial of service.

An improper input validation vulnerability (TALOS-2024-1949/CVE-2024-27201) also exists in the OAS Engine User Configuration functionality that could lead to unexpected data in the configuration, including possible decoy usernames that contain characters not usually allowed by the software's configuration.

Arbitrary write vulnerabilities in AMD graphics driver

Discovered by Piotr Bania.

There are two out-of-bounds write vulnerabilities in the AMD Radeon user mode driver for DirectX 11. TALOS-2023-1847 and TALOS-2023-1848 could allow an attacker with access to a malformed shader to potentially achieve arbitrary code execution after causing an out-of-bounds write.

AMD graphics drivers are software that allows graphics processing units (GPUs) to communicate with the operating system.

These vulnerabilities could be triggered from guest machines running virtualization environments to perform guest-to-host escape. Theoretically, an adversary could also exploit these issues from a web browser. Talos has demonstrated with past, similar, vulnerabilities that they could be triggered from HYPER-V guest using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host.

Source: https://blog.talosintelligence.com/vulnerability-roundup-april-10-2024/

8. Apple: Mercenary spyware attacks target iPhone users in 92 countries

Apple has been notifying iPhone users in 92 countries about a "mercenary spyware attack" attempting to remotely compromise their device.

In a sample notification the company shared with BleepingComputer, Apple says that it has high confidence in the warning and urges the recipient to take seriously.

"Apple detected that you are being targeted by a mercenary spyware attack that is trying to remotely compromise the iPhone associated with your Apple ID -xxx-," reads the notification.

> *This attack is likely targeting you specifically because of who you are or what you do. Although it's never possible to achieve absolute certainty when detecting such attacks, Apple has high confidence in this warning — please take it seriously. - Apple's warning*

To protect against such attacks, Apple recommends a set of immediate actions that include enabling lockdown mode on the device, updating the iPhone and any other Apple products to the latest software version, and seeking expert assistance such as that from the Digital Security Helpline - a non-profit that provides technical support at no cost for journalists, activists, and human rights defenders.

When describing mercenary spyware attacks, the notification highlights NSO Group's Pegasus kit and says that they are exceptionally well-funded, sophisticated, and target a very small number of individuals.

Apple also updated its support page on spyware protection yesterday replacing the term "state-sponsored" with "mercenary spyware," noting that these attacks are ongoing and global and sometimes involve private companies that develop spying tools for state actors.

Primary targets of these attacks typically include journalists, activists, politicians, and diplomats due to their roles or the sensitive information they may possess.

Despite the sophistication of these attacks, Apple assures users it's doing everything in its power to detect them, alert users, and assist them in taking the necessary action.

"Mercenary spyware attacks cost millions of dollars and often have a short shelf life, making them much harder to detect and prevent," reads the updated support page.

"Since 2021, we have sent Apple threat notifications multiple times a year as we have detected these attacks, and to date, we have notified users in over 150 countries in total," Apple informs.

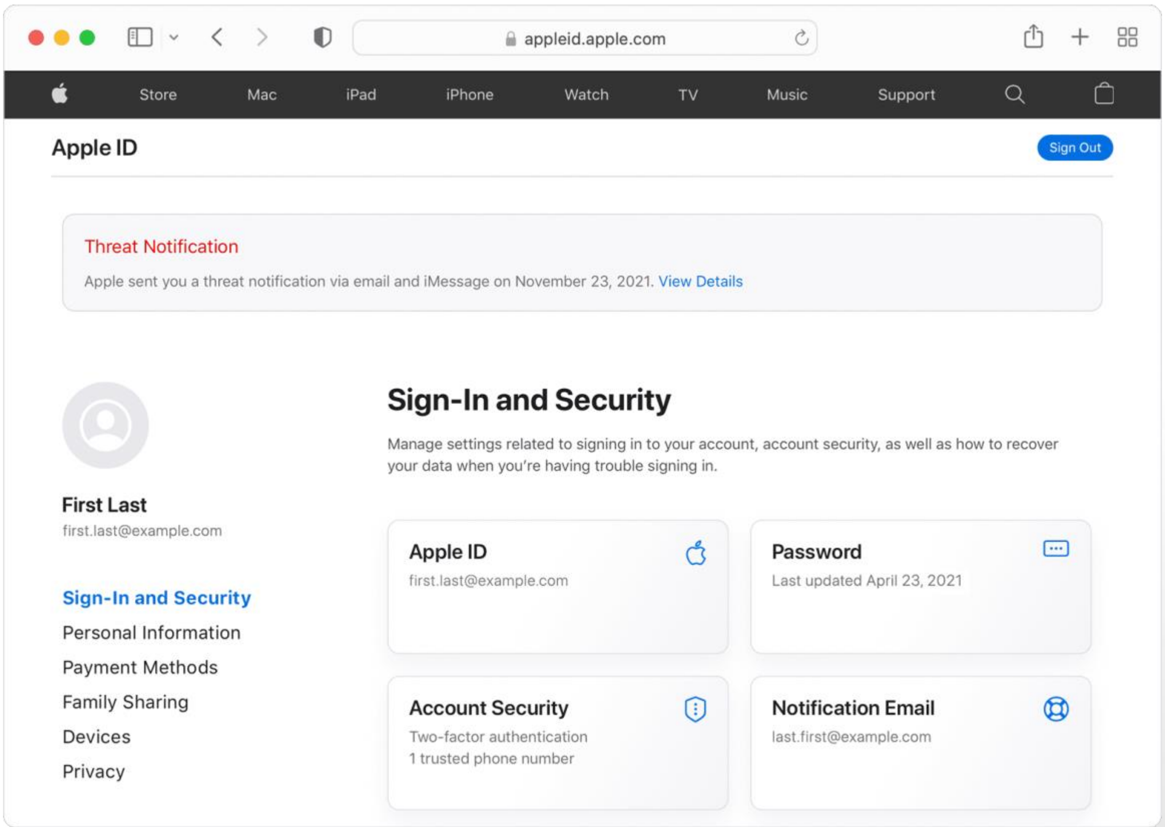
BleepingComputer asked Apple to comment on the targeting scope of the latest campaign it detected, but a spokesperson declined to provide clarifications.

On a related note, in the updated support page, Apple says that the "extreme cost, sophistication, and worldwide nature of mercenary spyware attacks makes them some of the most advanced digital threats in existence today.

Because of this, the company does not attribute the attacks to a specific attacker or or geographical regions.

What to do if targeted

If you're targeted by mercenary spyware attacks, you will get an email and iMessage notification at the numbers registered with your Apple ID, while a threat notification will also be displayed on the Apple ID portal after login, as a way to confirm authenticity.



Threat Notification

Apple sent you a threat notification via email and iMessage on November 23, 2021. View Details

First Last
first.last@example.com

Sign-In and Security

Manage settings related to signing in to your account, account security, as well as how to recover your data when you're having trouble signing in.

Apple ID
first.last@example.com

Password
Last updated April 23, 2021

Account Security
Two-factor authentication
1 trusted phone number

Notification Email
last.first@example.com

Notification of active spyware attack (Apple)

The actions Apple recommends that people take in that case are the following:

- Contact the Digital Security Helpline at Access Now for emergency security help and advice.
- Turn on Lockdown Mode for added protection against spyware, significantly reducing the attack surface.
- Update messaging and cloud apps to the latest available versions.
- Update all other Apple devices (Mac, iPad) you use and enable Lockdown Mode on those too.
- Follow general good practices like applying the latest updates, using passcodes, enabling two-factor authentication, downloading apps only from the App Store, using strong and unique passwords, and avoiding opening suspicious links or attachments.

Apple cannot detect all spyware attacks, so if you suspect you're being targeted, it's advisable to enable Lockdown Mode even if you have received no notifications from the company.

Source: https://www.bleepingcomputer.com/news/security/apple-mercenary-spyware-attacks-target-iphone-users-in-92-countries/

9. PuTTY SSH client flaw allows recovery of cryptographic private keys

A vulnerability tracked as CVE-2024-31497 in PuTTY 0.68 through 0.80 could potentially allow attackers with access to 60 cryptographic signatures to recover the private key used for their generation.

PuTTY is a popular open-source terminal emulator, serial console, and network file transfer application that supports SSH (Secure Shell), Telnet, SCP (Secure Copy Protocol), and SFTP (SSH File Transfer Protocol).

System administrators and developers predominantly use the software to remotely access and manage servers and other networked devices over SSH from a Windows-based client.

The vulnerability tracked as CVE-2024-31497 was discovered by Fabian Bäumer and Marcus Brinkmann of the Ruhr University Bochum and is caused by how PuTTY generates ECDSA nonces (temporary unique cryptographic numbers) for the NIST P-521 curve used for SSH authentication.

Specifically, there's a bias due to PuTYY's use of a deterministic way to generate these numbers to compensate for the lack of a robust cryptographic random number generator on specific Windows versions.

> *"PuTTY's technique worked by making a SHA-512 hash and then reducing it mod q, where q is the order of the group used in the DSA system. For integer DSA (for which PuTTY's technique was originally developed), q is about 160*

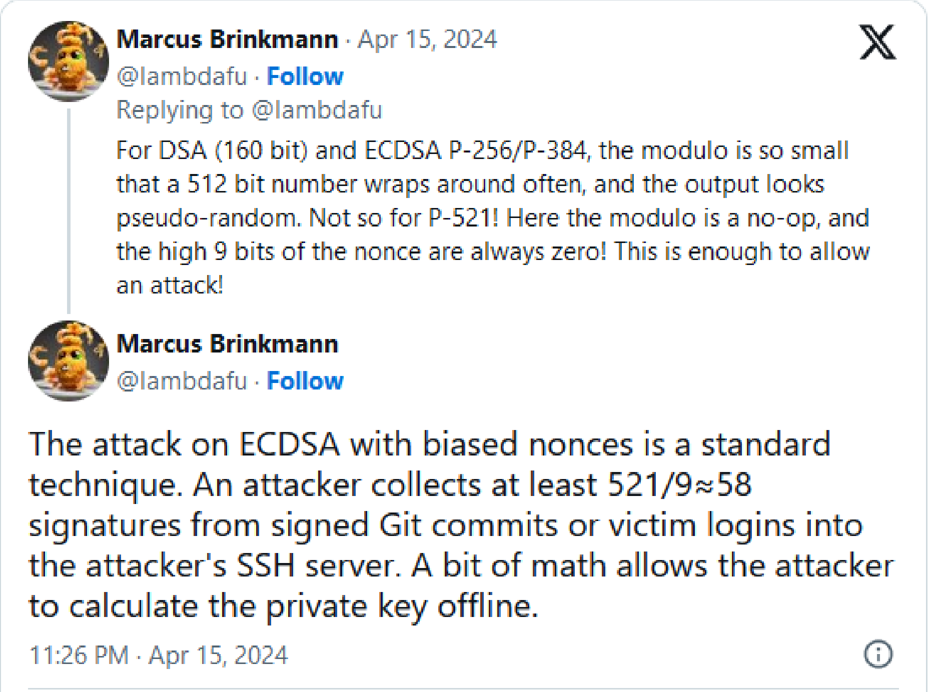
> *bits; for elliptic-curve DSA (which came later), it has about the same number of bits as the curve modulus, so 256 or 384 or 521 bits for the NIST curves."*
>
> *"In all of those cases except P521, the bias introduced by reducing a 512-bit number mod q is negligible. But in the case of P521, where q has 521 bits (i.e. more than 512), reducing a 512-bit number mod q has no effect at all – you get a value of k whose top 9 bits are always zero." - PuTTY security advisory.*

The main repercussion of recovering the private key is that it allows unauthorized access to SSH servers or sign commits as the developer, potentially even achieving supply chain attacks on impacted software projects.

Exploiting CVE-2024-31497

A digital signature is created using a user's private key and verified by the corresponding public key on the server, ensuring the user's identity and the communication's security.

Brinkmann explained on X that attackers require 58 signatures to calculate a target's private key, which they can acquire either by collecting them from logins to an SSH server they control or is compromised, or from signed Git commits.



Marcus Brinkmann · Apr 15, 2024
@lambdafu · **Follow**
Replying to @lambdafu

For DSA (160 bit) and ECDSA P-256/P-384, the modulo is so small that a 512 bit number wraps around often, and the output looks pseudo-random. Not so for P-521! Here the modulo is a no-op, and the high 9 bits of the nonce are always zero! This is enough to allow an attack!

Marcus Brinkmann
@lambdafu · **Follow**

The attack on ECDSA with biased nonces is a standard technique. An attacker collects at least 521/9≈58 signatures from signed Git commits or victim logins into the attacker's SSH server. A bit of math allows the attacker to calculate the private key offline.

11:26 PM · Apr 15, 2024

Collecting signatures from an SSH server is not as critical as it would mean the server itself is already compromised, and thus, the threat actor has broad access to the operating system.

However, Bäumer told BleepingComputer that the second method of harvesting signatures from public commits is far more practical for attackers.

> *There are instances where this vulnerability can be exploited without the need to compromise a server in advance.*

> *One such case is the use of SSH keys for signing Git commits. A common setup involves using Pageant, the ssh-agent of PuTTY, locally and forwarding the agent to a development host.*
>
> *Here, you configure Git to use OpenSSH to sign Git commits with the SSH key provided by Pageant. The signature is then generated by Pageant, making it susceptible to private key recovery.*
>
> *This is particularly concerning as git signatures may be publicly accessible, for example, if the commit is pushed to a public repository on GitHub.*
>
> ❖ *Fabian Bäumer*

Flaw fixed, other software impacted

The developers fixed the vulnerability in PuTTY version 0.81, which abandons the previous k-generation method and switches to the RFC 6979 technique for all DSA and ECDSA keys.

However, it is noted that any P521 private keys generated using the vulnerable version of the tool should be considered unsafe and replaced by new, secure keys.

The following software that uses the vulnerable PuTTY is confirmed as impacted:

- FileZilla 3.24.1 – 3.66.5 (fixed in 3.67.0)
- WinSCP 5.9.5 – 6.3.2 (fixed in 6.3.3)
- TortoiseGit 2.4.0.2 – 2.15.0 (fixed in 2.15.0.1)
- TortoiseSVN 1.10.0 – 1.14.6 (mitigation possible by configuring TortoiseSVN to use Plink from the latest PuTTY 0.81 release)

There are likely more software tools impacted by CVE-2024-31497, depending on which PuTTY version they incorporate. Therefore, users are advised to check their tools and take preventive action as needed.

Source: https://www.bleepingcomputer.com/news/security/putty-ssh-client-flaw-allows-recovery-of-cryptographic-private-keys/

10. Ivanti warns of critical flaws in its Avalanche MDM solution

Ivanti has released security updates to fix 27 vulnerabilities in its Avalanche mobile device management (MDM) solution, two of them critical heap overflows that can be exploited for remote command execution.

Avalanche is used by enterprise admins to remotely manage, deploy software, and schedule updates across large fleets of over 100,000 mobile devices from a single central location.

As the company explained on Wednesday, the two critical security flaws (CVE-2024-24996 and CVE-2024-29204) were found in Avalanche's WLInfoRailService and WLAvalancheService components.

They are both caused by heap-based buffer overflow weaknesses, which can let unauthenticated remote attackers execute arbitrary commands on vulnerable systems in low-complexity attacks that don't require user interaction.

Today, Ivanti also patched 25 medium and high-severity bugs that remote attackers could exploit to trigger denial-of-service attacks, execute arbitrary commands as SYSTEM, read sensitive information from memory, and remote code execution attacks.

"We are not aware of any customers being exploited by these vulnerabilities prior to public disclosure. These vulnerabilities were disclosed through our responsible disclosure program," the company said in a security advisory published on Tuesday.

"To address the security vulnerabilities listed below, it is highly recommended to download the Avalanche installer and update to the latest Avalanche 6.4.3."

Customers can find the latest Avalanche 6.4.3 release here and more information regarding upgrade steps in this support article.

Ivanti patched 13 more critical-severity remote code execution vulnerabilities in the Avalanche MDM solution in December after fixing two other critical Avalanche buffer overflows collectively tracked as CVE-2023-32560 in August.

State-affiliated hackers used two zero-day flaws (CVE-2023-35078 and CVE-2023-35081) in Ivanti's Endpoint Manager Mobile (EPMM), formerly known as MobileIron Core, to breach the networks of multiple Norwegian government organizations one year ago.

Months later, attackers chained a third MobileIron Core zero-day (CVE-2023-35081) with CVE-2023-35078 to also hack into the IT systems of a dozen Norwegian ministries.

"Mobile device management (MDM) systems are attractive targets for threat actors because they provide elevated access to thousands of mobile devices, and APT actors have exploited a previous MobileIron vulnerability," CISA warned last August.

"Consequently, CISA and NCSC-NO are concerned about the potential for widespread exploitation in government and private sector networks."

Source: https://www.bleepingcomputer.com/news/security/ivanti-warns-of-critical-flaws-in-its-avalanche-mdm-solution/

11. Microsoft: Copilot 'app' on Windows Server mistakenly added by Edge

Microsoft says the new Copilot app, mistakenly added to the list of installed Windows apps by recent Edge updates, doesn't collect or relay data to its servers.

The company began testing Microsoft Copilot in Windows Server 2025 preview builds earlier this year. However, after facing backlash from Windows admins, Microsoft removed Copilot from those builds.

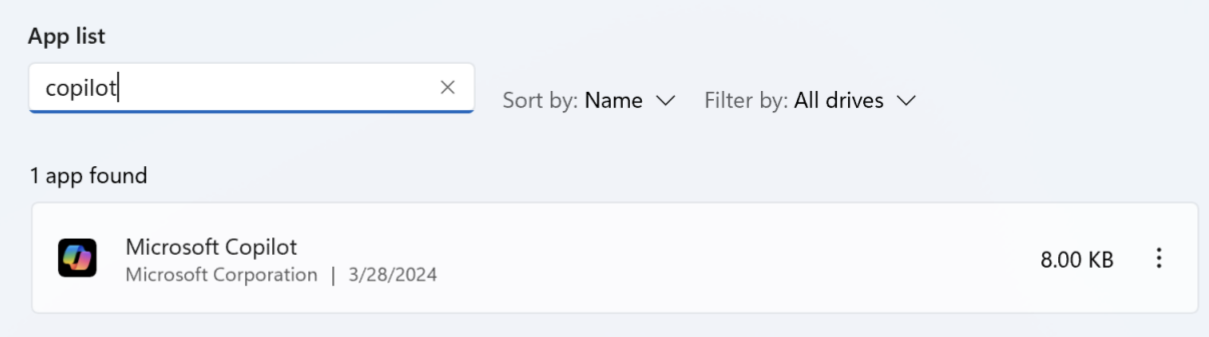
For this reason, they were surprised to see a new 8KB Microsoft Copilot app added to the list of installed programs on live production builds of Windows Server 2022.

As the company revealed on Tuesday, this known issue also affected systems running Windows 10 22H2 and Windows 11 21H2 or later.

"Updates to Edge browser version 123.0.2420.65, released on March 28, 2024 and later, might incorrectly install a new package (MSIX) called 'Microsoft chat provider for Copilot in Windows' on Windows devices. Resulting from this, the Microsoft Copilot app might appear in the Installed apps in Settings menu," Redmond said.

Microsoft also says that the Copilot app these recent Edge updates add on impacted devices can't actually be used to launch Copilot and does not collect any user or system data.

"It is important to note that the Microsoft chat provider for Copilot in Windows does not execute any code or process, and does not acquire, analyze, or transmit device or environment data in any capacity," Microsoft explains.


App list

copilot

Sort by: Name

Filter by: All drives

1 app found

Microsoft Copilot
Microsoft Corporation | 3/28/2024
8.00 KB

Copilot app added by recent Edge update (BleepingComputer)

The package is intended solely to prepare some Windows devices for future Windows Copilot enablement and will not be visible on all Windows devices.

Moreover, according to Microsoft, even if the installed component causes a Copilot app to display as installed on the system, it won't fully install or enable Windows Copilot.

"As part of the upcoming resolution of this issue, the chat provider for Copilot in Windows component will be removed from devices where Microsoft Copilot is not intended to be enabled or installed. This includes most Windows Server devices," Microsoft said.

"We are working on a resolution and will provide an update in an upcoming release of Microsoft Edge."

The company is now also testing ads in the Windows 11 Start menu as part of a new experiment to help users "discover great apps from the Microsoft Store."

This is part of a trial rolling out in the Beta Channel to a "small set of Insiders" who have installed Windows 11 Insider Preview Build 22635.3495.

Two years ago, Redmond promoted its Edge web browser in the Windows 10 Start Menu and accidentally broke both the Taskbar and the Start Menu while testing Microsoft Teams ads on some Windows Insider builds.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-copilot-app-on-windows-server-mistakenly-added-by-edge/

12. Cisco discloses root escalation flaw with public exploit code

Cisco has released patches for a high-severity Integrated Management Controller (IMC) vulnerability with public exploit code that can let local attackers escalate privileges to root.

Cisco IMC is a baseboard management controller for managing UCS C-Series Rack and UCS S-Series Storage servers via multiple interfaces, including XML API, web (WebUI), and command-line (CLI) interfaces.

"A vulnerability in the CLI of the Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root," the company explains.

"To exploit this vulnerability, the attacker must have read-only or higher privileges on an affected device."

Tracked as CVE-2024-20295, this security flaw is caused by insufficient validation of user-supplied input, a weakness that can be exploited using crafted CLI commands as part of low-complexity attacks.

The vulnerability impacts the following Cisco devices running vulnerable IMC versions in default configurations:

- 5000 Series Enterprise Network Compute Systems (ENCS)
- Catalyst 8300 Series Edge uCPE
- UCS C-Series Rack Servers in standalone mode
- UCS E-Series Servers

However, it also exposes a long list of other products to attacks if they're configured to provide access to the vulnerable Cisco IMC CLI.

Cisco's Product Security Incident Response Team (PSIRT) also warned in today's advisory that proof-of-concept exploit code is already available, but luckily, threat actors have yet to start targeting the vulnerability in attacks.

In October, the company released security patches for two zero-days, which were used to breach over 50,000 IOS XE devices within a week.

Attackers also exploited a second IOS and IOS XE zero-day last year, allowing them to hijack vulnerable devices via remote code execution.

More recently, Cisco warned of a large-scale and ongoing credential brute-forcing campaign targeting VPN and SSH services on Cisco, CheckPoint, Fortinet, SonicWall, and Ubiquiti devices after urging customers to mitigate password-spraying attacks against Remote Access VPN (RAVPN) services configured on Cisco Secure Firewall devices.

Source: https://www.bleepingcomputer.com/news/security/cisco-discloses-root-escalation-flaw-with-public-exploit-code/

13. Cybercriminals pose as LastPass staff to hack password vaults

LastPass is warning of a malicious campaign targeting its users with the CryptoChameleon phishing kit that is associated with cryptocurrency theft.

CryptoChameleon is an advanced phishing kit that was spotted earlier this year, targeting Federal Communications Commission (FCC) employees using custom-crafted Okta single sign-on (SSO) pages.

According to researchers at mobile security company Lookout, campaigns using this phishing kit also targeted cryptocurrency platforms Binance, Coinbase, Kraken, and Gemini, using pages that impersonated Okta, Gmail, iCloud, Outlook, Twitter, Yahoo, and AOL.

During its investigations, LastPass discovered that its service was recently added to the CryptoChameleon kit, and a phishing site was hosted at at the "help-lastpass[.]com" domain.

The attacker combines multiple social engineering techniques that involve contacting the potential victim (voice phishing) and pretending to be a LastPass employee trying to help with securing the account following unauthorized access.

Below are the tactics LastPass observed in this campaign:

1. Victims receive a call from an 888 number claiming unauthorized access to their LastPass account and are prompted to allow or block the access by pressing "1" or "2".
2. If they choose to block the access, they're told they will get a follow-up call to resolve the issue.
3. A second call comes from a spoofed number, where the caller, posing as a LastPass employee, sends a phishing email from "support@lastpass" with a link to the fake LastPass site.

4. Entering the master password on this site allows the attacker to change account settings and lock out the legitimate user.

The malicious website is now offline but it is very likely that other campaigns will follow and threat actors will rely on new domains.

Users of the popular password management service are recommended to beware of suspicious phone calls, messages, or emails claiming to come from LastPass and urging immediate action.

Some indicators of suspicious communication from this campaign include emails with the subject "We're here for you" and the use of a shortened URL service for links in the message. Users should report these attempts to LastPass at **abuse@lastpass.com**.

Regardless of the sevice, the master password should not be shared with anyone since it is the key to all your sensitive information.

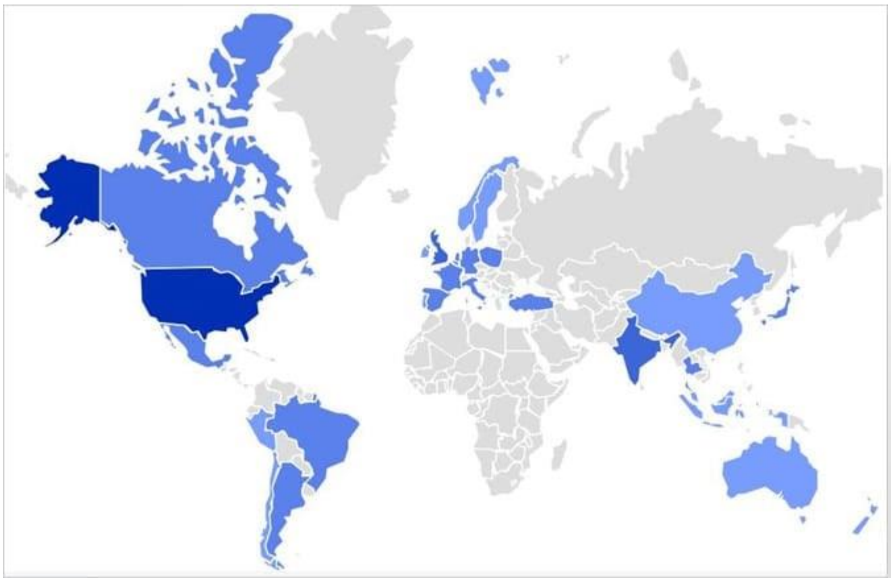
Source: https://www.bleepingcomputer.com/news/security/cybercriminals-pose-as-lastpass-staff-to-hack-password-vaults/

14. Fake cheat lures gamers into spreading infostealer malware

A new info-stealing malware linked to Redline poses as a game cheat called 'Cheat Lab,' promising downloaders a free copy if they convince their friends to install it too.

Redline is a powerful information-stealing malware capable of harvesting sensitive information from infected computers, including passwords, cookies, autofill information, and cryptocurrency wallet information.

The malware is very popular among cybercriminals and is spread worldwide using diverse distribution channels.



Redline victims heatmap (McAfee)

McAfee threat researchers reported that the new information stealer leverages Lua bytecode to evade detection, allowing the malware to inject into legitimate processes for stealth and also take advantage of Just-In-Time (JIT) compilation performance.

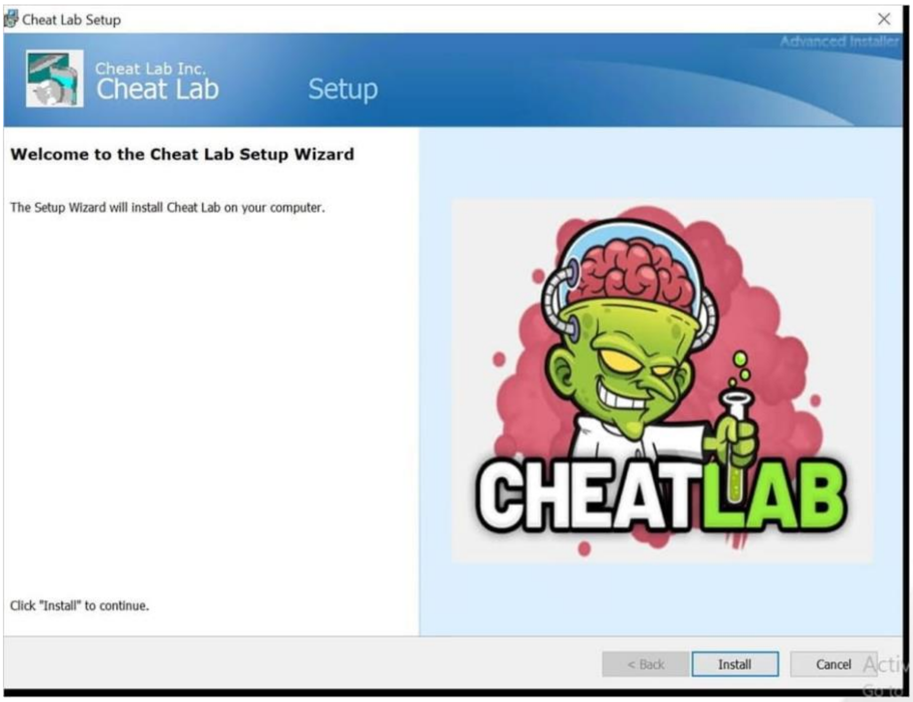
The researchers link this variant to Redline as it uses a command and control server previously associated with the malware.

However, according to BleepingComputer's tests, the malware does not exhibit behavior typically associated with Redline, such as stealing browser information, saving passwords, and cookies.

Wants you to infect your friends too!

The malicious Redline payloads impersonate demos of cheating tools called "Cheat Lab" and "Cheater Pro" through URLs linked to Microsoft's 'vcpkg' GitHub repository.

The malware is distributed as ZIP files containing an MSI installer that unpacks two files, compiler.exe and lua51.dll, when launched. It also drops a 'readme.txt' file containing the malicious Lua bytecode.



Cheat Lab Setup

Welcome to the Cheat Lab Setup Wizard

The Setup Wizard will install Cheat Lab on your computer.

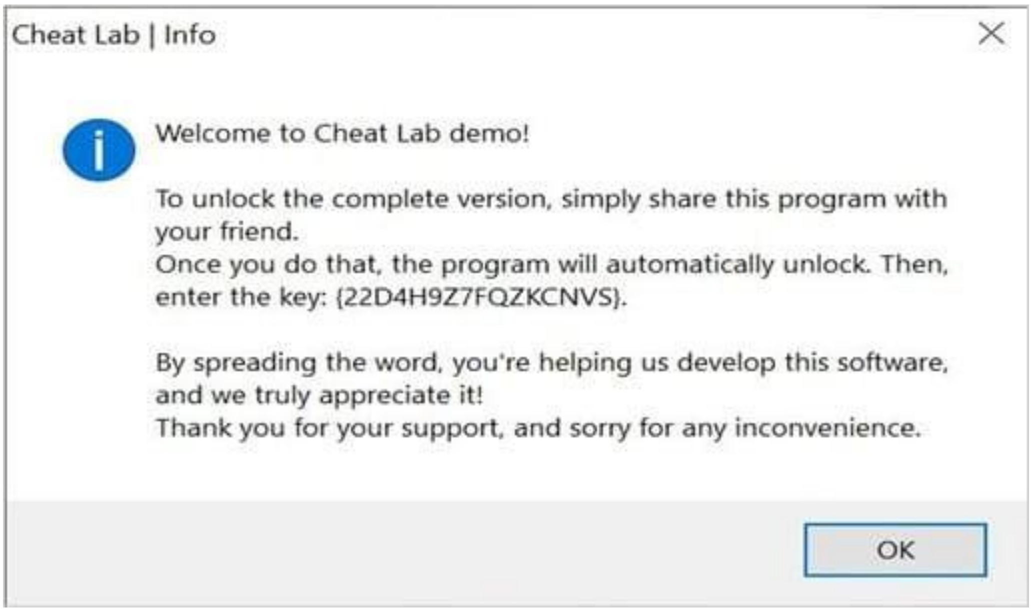
Click "Install" to continue.

The fake CheatLab installer
Source:McAfee

This campaign uses an interesting lure to further distribute the malware by telling victims they can get a free, fully licensed copy of the cheating program if they convince their friends to install it, too.

The message also contains an activation key for added legitimacy.

"To unlock the complete version, simply share this program with your friend. Once you do that, the program will automatically unlock," reads the installation prompt shown below.



Cheat Lab | Info

Welcome to Cheat Lab demo!

To unlock the complete version, simply share this program with your friend.
Once you do that, the program will automatically unlock. Then, enter the key: {22D4H9Z7FQZKCNVS}.

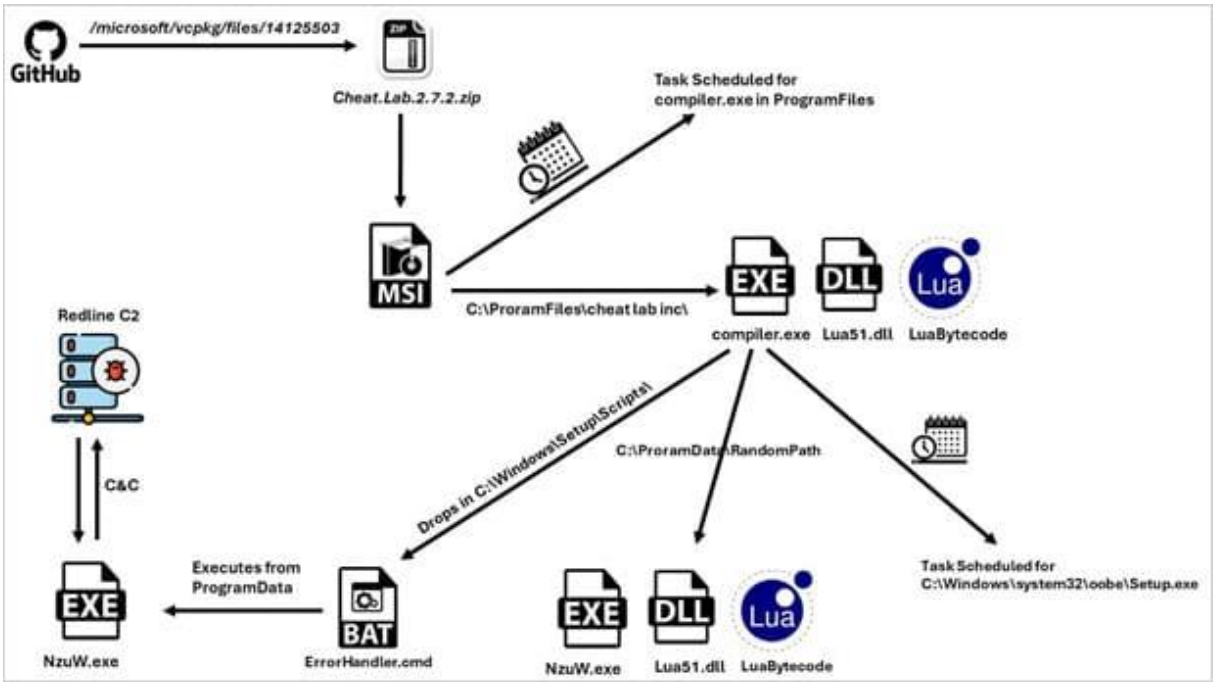
By spreading the word, you're helping us develop this software, and we truly appreciate it!
Thank you for your support, and sorry for any inconvenience.

Prompt to spread the malware
Source:McAfee

To evade detection, the malware payload is not distributed as an executable but rather as uncompiled bytecode.

When installed, the compiler.exe program compiles the Lua bytecode stored in the readme.txt file and executes it. The same executable also sets up persistence by creating scheduled tasks that execute during system startup.

McAfee reports that the malware uses a fallback mechanism for persistence, copying the three files to a long random path under program data.


GitHub
/microsoft/vcpkg/files/14125503
Cheat.Lab.2.7.2.zip
MSI
Task Scheduled for compiler.exe in ProgramFiles
C:\ProramFiles\cheat lab inc\
EXE
DLL
Lua
compiler.exe
Lua51.dll
LuaBytecode
Redline C2
C&C
Drops in C:\Windows\Setup\Scripts\
C:\ProramData\RandomPath
Task Scheduled for C:\Windows\system32\oobe\Setup.exe
EXE
NzuW.exe
Executes from ProgramData
BAT
ErrorHandler.cmd
NzuW.exe
Lua51.dll
LuaBytecode

Infection diagram
Source:McAfee

Once active on the infected system, the malware communicates with a C2 server, sending screenshots of the active windows and system information and waiting for commands to execute on the host.

The exact method used for initial infection hasn't been determined, but information-stealers are typically spread via malvertising, YouTube video descriptions, P2P downloads, and deceptive software download sites.

Users are advised to avoid unsigned executables and files downloaded from shady websites.

This attack shows that even installing programs from seemingly trustworthy locations like Microsoft's GitHub can set people up for a Redline infection.

BleepingComputer contacted Microsoft about the executables distributed through its GitHub URLs but did not receive a response by the time of publication.

Update 4/20: McAfee confirmed to BleepingComputer that it has informed Microsoft of the abuse.

McAfee is in direct communication with the Microsoft Security Response Team. - McAfee spokesperson

Source: https://www.bleepingcomputer.com/news/security/fake-cheat-lures-gamers-into-spreading-infostealer-malware/

15. MITRE says state hackers breached its network via Ivanti zero-days

The MITRE Corporation says that a state-backed hacking group breached its systems in January 2024 by chaining two Ivanti VPN zero-days.

The incident was discovered after suspicious activity was detected on MITRE's Networked Experimentation, Research, and Virtualization Environment (NERVE), an unclassified collaborative network used for research and development.

MITRE has since notified affected parties of the breach, contacted relevant authorities, and is now working on restoring "operational alternatives."

Evidence collected during the investigation so far shows that this breach did not affect the organization's core enterprise network or its partners' systems.

"No organization is immune from this type of cyber attack, not even one that strives to maintain the highest cybersecurity possible," said MITRE CEO Jason Providakes on Friday.

"We are disclosing this incident in a timely manner because of our commitment to operate in the public interest and to advocate for best practices that enhance enterprise security as well necessary measures to improve the industry's current cyber defense posture."

MITRE CTO Charles Clancy and Cybersecurity Engineer Lex Crumpton also explained in a separate advisory that the threat actors compromised one of MITRE's Virtual Private Networks (VPNs) by chaining two Ivanti Connect Secure zero-days.

They could also bypass multi-factor authentication (MFA) defenses by using session hijacking, which allowed them to move laterally through the breached network's VMware infrastructure using a hijacked administrator account.

Throughout the incident, the hackers used a combination of sophisticated webshells and backdoors to maintain access to hacked systems and harvest credentials.

Since early December, the two security vulnerabilities, an auth bypass (CVE-2023-46805) and a command injection (CVE-2024-21887), have been exploited to deploy multiple malware families for espionage purposes.

Mandiant has linked these attacks to an advanced persistent threat (APT) it tracks as UNC5221, while Volexity reported seeing signs that Chinese state-sponsored threat actors were exploiting the two zero-days.

Volexity said the Chinese hackers backdoored over 2,100 Ivanti appliances, harvesting and stealing account and session data from breached networks. The victims ranged in size from small businesses to some of the largest organizations worldwide, including Fortune 500 companies from various industry verticals.

Due to their mass exploitation and the vast attack surface, CISA issued this year's first emergency directive on January 19, ordering federal agencies to mitigate the Ivanti zero-days immediately.

Source: https://www.bleepingcomputer.com/news/security/mitre-says-state-hackers-breached-its-network-via-ivanti-zero-days/

16. GitHub comments abused to push malware via Microsoft repo URLs

A GitHub flaw, or possibly a design decision, is being abused by threat actors to distribute malware using URLs associated with Microsoft repositories, making the files appear trustworthy.

While most of the malware activity has been based around the Microsoft GitHub URLs, this "flaw" could be abused with any public repository on GitHub, allowing threat actors to create very convincing lures.

Abusing GitHub's file upload feature

Yesterday, McAfee released a report on a new LUA malware loader distributed through what appeared to be a legitimate Microsoft GitHub repositories for the "C++ Library Manager for Windows, Linux, and MacOS," known as vcpkg, and the STL library.

The URLs for the malware installers, shown below, clearly indicate that they belong to the Microsoft repo, but we could not find any reference to the files in the project's source code.

```
https://github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip
```

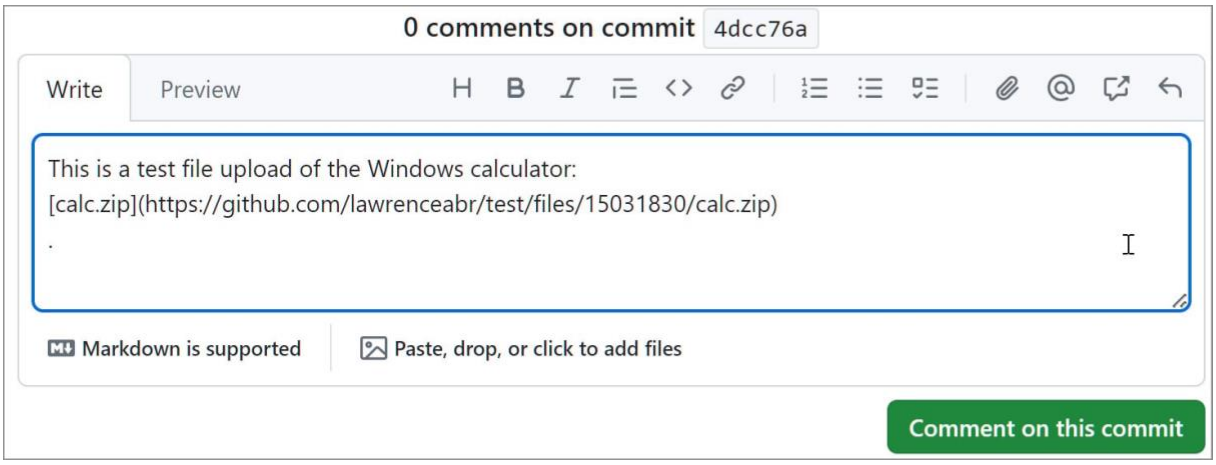
```
https://github[.]com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip
```

Finding it strange that a Microsoft repo would be distributing malware since February, BleepingComputer looked into it and found that the files are not part of **vcpkg** but were uploaded as part of a comment left on a commit or issue in the project.

When leaving a comment, a GitHub user can attach a file (archives, documents, etc), which will be uploaded to GitHub's CDN and associated with the related project using a unique URL in this format: '**https://www.github.com/{project_user}/{repo_name}/files/{file_id}/{file_name}.**'

For videos and images, the files will be stored under the `/assets/` path instead.

Instead of generating the URL after a comment is posted, GitHub automatically generates the download link after you add the file to an unsaved comment, as shown below. This allows threat actors to attach their malware to any repository without them knowing.


0 comments on commit 4dcc76a
Write
Preview
Markdown is supported
Paste, drop, or click to add files
Comment on this commit

This is a test file upload of the Windows calculator:
[calc.zip](https://github.com/lawrenceabr/test/files/15031830/calc.zip)
.

Download link auto-generated when adding a file to a comment
Source: BleepingComputer

Even if you decide not to post the comment or delete it after it is posted, the files are not deleted from GitHub's CDN, and the download URLs continue to work forever.

As the file's URL contains the name of the repository the comment was created in, and as almost every software company uses GitHub, this flaw can allow threat actors to develop extraordinarily crafty and trustworthy lures.

For example, a threat actor could upload a malware executable in NVIDIA's driver installer repo that pretends to be a new driver fixing issues in a popular game. Or a threat actor could upload a file in a comment to the Google Chromium source code and pretend it's a new test version of the web browser.

These URLs would also appear to belong to the company's repositories, making them far more trustworthy.

Unfortunately, even if a company learns their repos are abused to distribute malware, BleepingComputer could not find any settings that allow you to manage files attached to your projects.

Furthermore, you can only protect a GitHub account from being abused in this way and tarnishing your reputation by disabling comments. According to this GitHub support document, you can only temporarily disable comments for a maximum of six months at a time.

However, restricting comments can significantly impact a project's development as it will not allow users to report bugs or suggestions.

Sergei Frankoff, of automated malware analysis service UNPACME, did a livestream on Twitch about this bug just last month, saying that threat actors were actively abusing it.

As part of our research into this bug, BleepingComputer could only find one other repo, httprouter, abused to distribute malware in this way, and it was the same 'Cheater.Pro.1.6.0.zip' as seen in Microsoft's URLs.

However, Frankoff told BleepingComputer that they discovered a similar campaign in March that utilizes the same LUA loader malware, which is called SmartLoader, disguised as the Aimmy cheat software.

Frankoff told BleepingComputer that SmartLoader is commonly installed alongside other payloads, such as the RedLine information-stealing malware.

BleepingComputer contacted both GitHub and Microsoft on Thursday about this abuse but did not receive a response.

At the time of this publication, the information-stealing malware is still being distributed through links associated with Microsoft' GitHub repository.

Update 4/21/24: GitHub has removed the malware linked to Microsoft's repositories. However, the malware associated with httprouter and Aimmy are still accessible.

Source: https://www.bleepingcomputer.com/news/security/github-comments-abused-to-push-malware-via-microsoft-repo-urls/

17. Using Legitimate GitHub URLs for Malware

Interesting social-engineering attack vector:

> McAfee released a report on a new LUA malware loader distributed through what appeared to be a legitimate Microsoft GitHub repository for the "C++ Library Manager for Windows, Linux, and MacOS," known as vcpkg.

The attacker is exploiting a property of GitHub: comments to a particular repo can contain files, and those files will be associated with the project in the URL.

What this means is that someone can upload malware and "attach" it to a legitimate and trusted project.

> As the file's URL contains the name of the repository the comment was created in, and as almost every software company uses GitHub, this flaw can allow threat actors to develop extraordinarily crafty and trustworthy lures.
>
> For example, a threat actor could upload a malware executable in NVIDIA's driver installer repo that pretends to be a new driver fixing issues in a popular game. Or a threat actor could upload a file in a comment to the Google Chromium source code and pretend it's a new test version of the web browser.
>
> These URLs would also appear to belong to the company's repositories, making them far more trustworthy.

Source: https://www.schneier.com/blog/archives/2024/04/using-legitimate-github-urls-for-malware.html

18. Microsoft: APT28 hackers exploit Windows flaw reported by NSA

Microsoft warns that the Russian APT28 threat group exploits a Windows Print Spooler vulnerability to escalate privileges and steal credentials and data using a previously unknown hacking tool called GooseEgg.

APT28 has been using this tool to exploit the CVE-2022-38028 vulnerability "since at least June 2020 and possibly as early as April 2019."

Redmond fixed the vulnerability reported by the U.S. National Security Agency during the Microsoft October 2022 Patch Tuesday but has yet to tag it as actively exploited in its advisory.

The military hackers, part of Military Unit 26165 of Russia's Main Intelligence Directorate of the General Staff (GRU), use GooseEgg to launch and deploy additional malicious payloads and run various commands with SYSTEM-level privileges.

Microsoft has seen the attackers drop this post-compromise tool as a Windows batch script named 'execute.bat' or 'doit.bat,' which launches a GooseEgg executable and gains persistence on the compromised system by adding a scheduled task that launches 'servtask.bat,' a second batch script written to the disk.

They also use GooseEgg to drop an embedded malicious DLL file (in some cases dubbed 'wayzgoose23.dll') in the context of the PrintSpooler service with SYSTEM permissions.

This DLL is actually an app launcher that can execute other payloads with SYSTEM-level permissions and lets attackers deploy backdoors, move laterally through victims' networks, and run remote code on breached systems.

"Microsoft has observed Forest Blizzard using GooseEgg as part of post-compromise activities against targets including Ukrainian, Western European, and North American government, non-governmental, education, and transportation sector organizations," Microsoft explains.

"While a simple launcher application, GooseEgg is capable of spawning other applications specified at the command line with elevated permissions, allowing threat actors to support any follow-on objectives such as remote code execution, installing a backdoor, and moving laterally through compromised networks."

History of high-profile cyberattacks

APT28, a prominent Russian hacking group, has been responsible for many high-profile cyber attacks since it first surfaced in the mid-2000s.

For instance, one year ago, U.S. and U.K. intelligence services warned about APT28 exploiting a Cisco router zero-day to deploy Jaguar Tooth malware, which allowed it to harvest sensitive information from targets in the U.S. and EU.

More recently, in February, a joint advisory issued by the FBI, the NSA, and international partners warned that APT28 used hacked Ubiquiti EdgeRouters to evade detection in attacks.

They were also linked in the past with the breach of the German Federal Parliament (Deutscher Bundestag) and hacks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) ahead of the 2016 U.S. Presidential Election.

Two years later, the U.S. charged APT28 members for their involvement in the DNC and DCCC attacks, while the Council of the European Union also sanctioned APT28 members in October 2020 for the German Federal Parliament hack.

Source: https://www.bleepingcomputer.com/news/security/microsoft-apt28-hackers-exploit-windows-flaw-reported-by-nsa/

19. WP Automatic WordPress plugin hit by millions of SQL injection attacks

Hackers have started to target a critical severity vulnerability in the WP Automatic plugin for WordPress to create user accounts with administrative privileges and to plant backdoors for long-term access.

Currently installed on more than 30,000 websites, WP Automatic lets administrators automate content importing (e.g. text, images, video) from various online sources and publishing on their WordPress site.

The exploited vulnerability is identified as as CVE-2024-27956 and received a severity score of 9.9/10.

It was disclosed publicly by researchers at PatchStack vulnerability mitigation service on March 13 and described as an SQL injection issue that impacts affecting WP Automatic versions before 3.9.2.0.

The issus is in the plugin’s user authentication mechanism, which can be bypassed to submit SQL queries to the site’s database. Hackers can use specially crafted queries to create administrator accounts on the target website.

Over 5.5 million attack attempts

Since PatchStack disclosed the security issue, Automattic's WPScan observed more than 5.5 million attacks trying to leverage the vulnerability, most of them being recorded on March 31st.

WPScan reports that after obtaining admin access to the target website, attackers create backdoors and obfuscate the code to make it more difficult to find.

“Once a WordPress site is compromised, attackers ensure the longevity of their access by creating backdoors and obfuscating the code,” reads WPScan’s report.

To prevent other hackers from compromising the website by exploiting the same issue and to avoid detection, the hackers also rename the vulnerable file “csv.php.”

Once they get control of the website, the threat actor often installs additional plugins that allow uploading files and code editing.

WPScan provides a set of indicators of compromise that can help admins determine if their website was hacked.

Administrators can check for signs that hackers took over the website by looking for the presense of an admin account starting with "xtw" and files named **web.php** and **index.php**, which are the backdoors planted in the recent campaign.

To mitigate the risk of being breached, researchers recommend WordPress site administrators to update the WP Automatic plugin to version 3.92.1 or later.

WPScan also recommends that website owners frequently create backups of their site so they can install clean copies quickly in case of a compromise.

Source: https://www.bleepingcomputer.com/news/security/wp-automatic-wordpress-plugin-hit-by-millions-of-sql-injection-attacks/

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

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

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

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