aDvens

Security for the greater good

Monthly Cyber Threat Intelligence report
February 2024

2024-02-29 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

1. Executive summary

This month, CERT aDvens brings you five noteworthy vulnerabilities in addition to those already published.

Through two articles, CERT analysts provide :

- the malware Troll Stealer was employed by Kimsuky in January, targeting South Korean government agencies during orchestrated attack campaigns.
- an examination of spear-phishing campaigns conducted by the APT group Charming Kitten.

2. Vulnerabilities

This month, the CERT aDvens highlights **three** vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (availability of proofs of concept, exploitation…). Applying their patches or workarounds is highly recommended.

2.1. WordPress Ultimate Member - CVE-2024-1071

On 23 February 2024, Wordfence published in their database the critical vulnerability CVE-2024-1071 affecting the WordPress plugin *Ultimate Member* used to manage the creation of memberships and communities. This plugin is installed on more than 200 000 websites.

This SQL injection flaw is due to an improper check of the "sorting" parameter in a user request. This vulnerability allows an unauthenticated attacker to add malicious SQL requests to existing ones in order to manipulate and extract sensitive data from the database.

This vulnerability is exploited.

2.1.1. Risks

- Sensitive data theft
- Database manipulation

2.1.2. Type of vulnerability

- **CWE-89**: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

2.1.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Affected products

- Ultimate Member versions 2.1.3 to 2.8.2

2.1.5. Recommendations

- Update WordPress's Ultimate Member plugin to version 2.8.3 or later.

2.1.6. Proof of concept

No proof of concept is currently available.

2.2. Zoom - CVE-2024-24691

On 13 February 2024, Zoom reported in their security advisory, a critical vulnerability (CVE-2024-24691) affecting *Zoom Desktop Client for Windows*, *Zoom VDI Client for Windows* and *Zoom Meeting SDK for Windows*.

An improper input validation in Zoom products allows an unauthenticated attacker to escalate their privileges via network access.

Zoom also disclosed six other vulnerabilities with medium and high severity for these clients. Affected versions are taken into account in the recommendations.

2.2.1. Risk

- Privilege escalation

2.2.2. Type of vulnerability

- **CWE-20**: Improper Input Validation

2.2.3. Severity

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	Required	Impact on availability	High

2.2.4. Affected products

- Zoom Desktop Client for Windows versions prior to 5.16.5
- Zoom VDI Client for Windows versions prior to 5.16.10 (excluding 5.14.14 and 5.15.12)
- Zoom Rooms Client for Windows versions prior to 5.17.0
- Zoom Meeting SDK for Windows versions prior to 5.16.5

2.2.5. Recommendations

- Update Zoom Desktop Client for Windows to version 5.17.0 or later.
- Update Zoom VDI Client for Windows to version 5.17.5 or later.
- Update Zoom Rooms Client for Windows to version 5.17.0 or later.
- Update Zoom Meeting SDK for Windows to version 5.17.0 or later.
- Additional information is available in Zoom's advisory.

2.2.6. Proof of concept

No proof of concept is currently available.

2.3. runc - CVE-2024-21626

On 31 January 2024, Open Container Initiative published a security advisory concerning a vulnerability CVE-2024-21626 affecting the runc tool.

This weakness is caused by a file descriptor leak and a lack of control of the container's working directory. This can allow an unauthenticated attacker, by convincing a user to build or execute a malicious image, to escape from a container and access the host's filesystem.

Solutions using runc usually have root privileges, making it possible to obtain a remote code execution on the host from this disk access.

2.3.1. Risks

- Container breakout
- Privilege escalation
- Remote code execution

2.3.2. Type of vulnerability

- **CWE-403**: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')

2.3.3. Severity

Attack vector	Local	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	Required	Impact on availability	High

2.3.4. Affected products

- runc versions 1.0.0-rc93 to 1.1.11

2.3.5. Recommendations

- Update runc and by extension, all solutions that depend on it, to version 1.1.12 or later.
- Vendors also published their own security advisories:
  - Docker
  - containerd
  - Kubernetes
  - AWS
  - GCP
  - Azure
  - RedHat
- Allow users to only run trusted images.

2.3.6. Proof of concept

A proof of concept is available in open sources.

3. Virology: analysis of a Troll Stealer sample (APT Kimsuky)

3.1. A sophisticated spyware

Troll Stealer is sophisticated spyware / infostealer used by APT Kimsuky (North Korea) to **steal information**.

The malware was discovered at the beginning of 2024 during a cyberespionage campaign targeting administrative institutions located in South Korea.

Analysis of Troll Stealer reveals that it shares similarities with Apple Seed and Alpha Seed, two backdoors known to belong to the arsenal of APT Kimsuky.

3.2. Features

Below are the main features of the Troll Stealer malware:

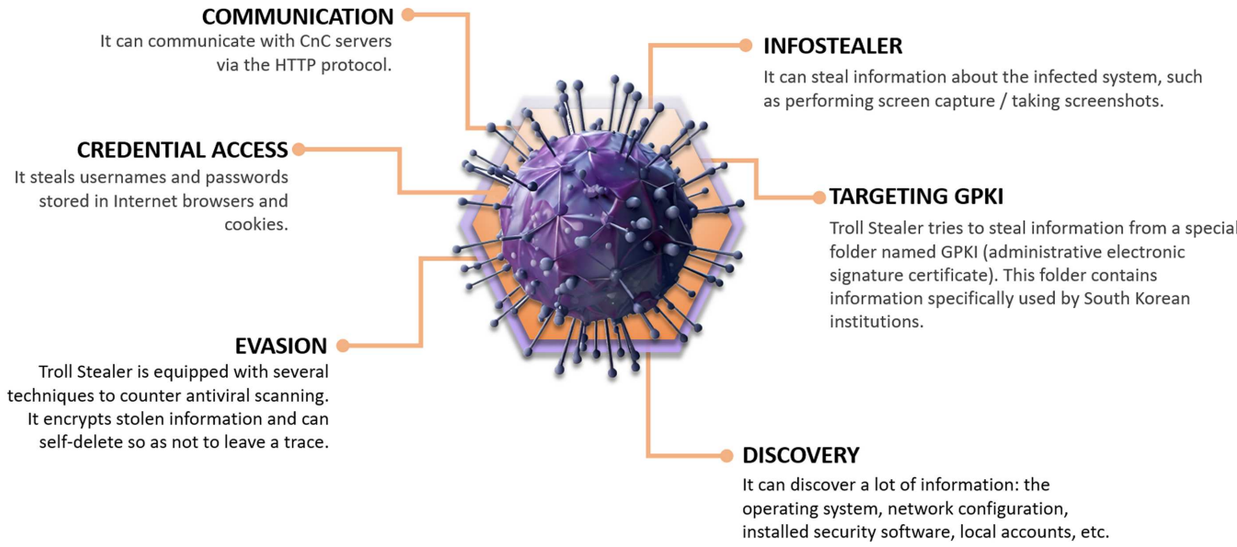


Figure 1. The features of Troll Stealer: information stealing agent.

3.3. Victimology

The attackers used Troll Stealer against **administrative institutions** located in South Korea.

3.4. Infectiology

3.4.1. Infection chain: a synthesis

Below, the six main stages of the infection chain.

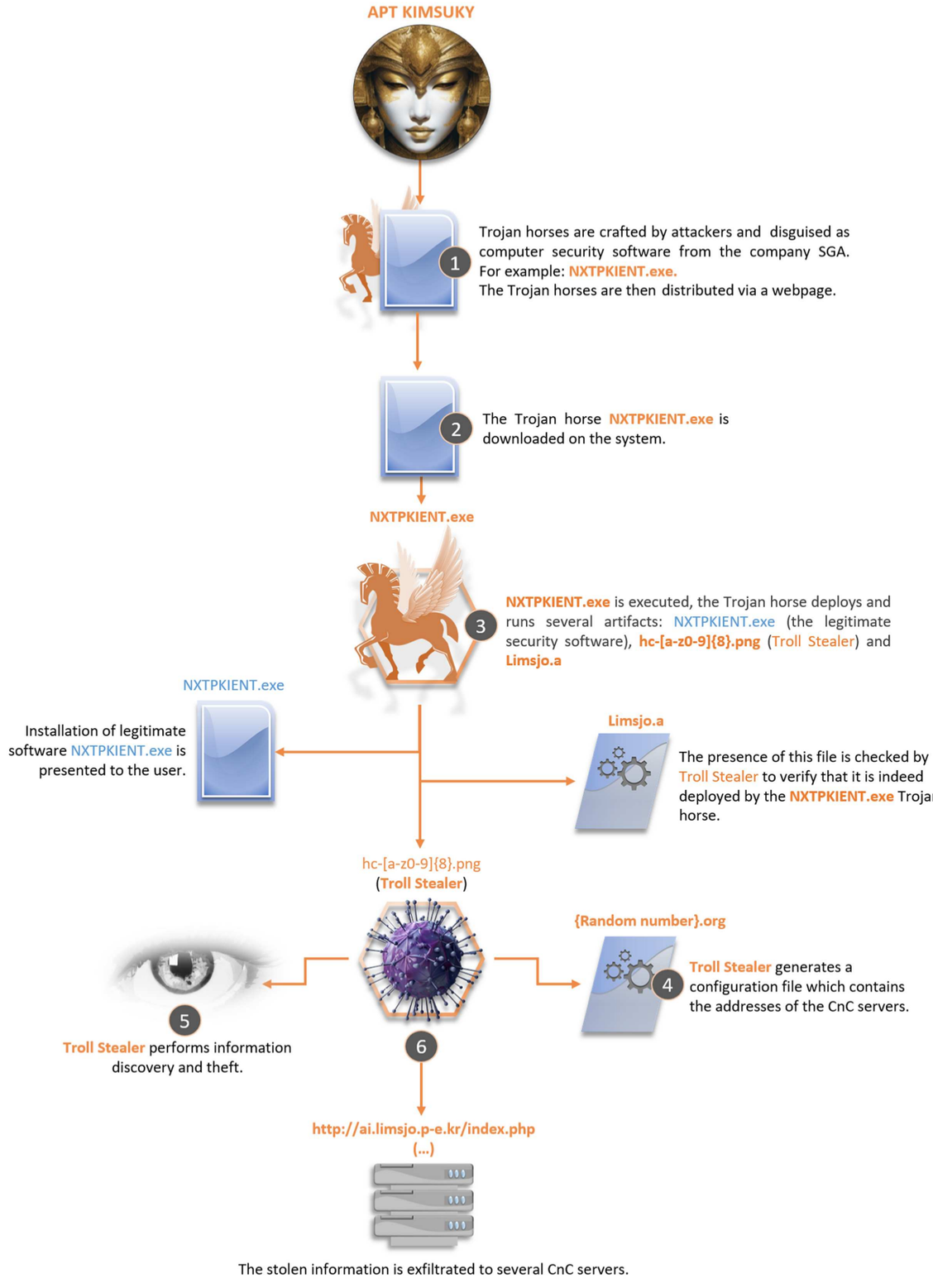


Figure 2. Infographic summary of the infection chain.

3.4.2. Infection chain: a detailed analysis

Infection vector

The attackers used a web page to share their Trojan Horses disguised as security software from the company **SGA Solutions**. For example: TrustPKI and NX_PRNMAN.

Figure 3. Malicious Korean Web Page (Original Korean Version).

Below is an English translated version:

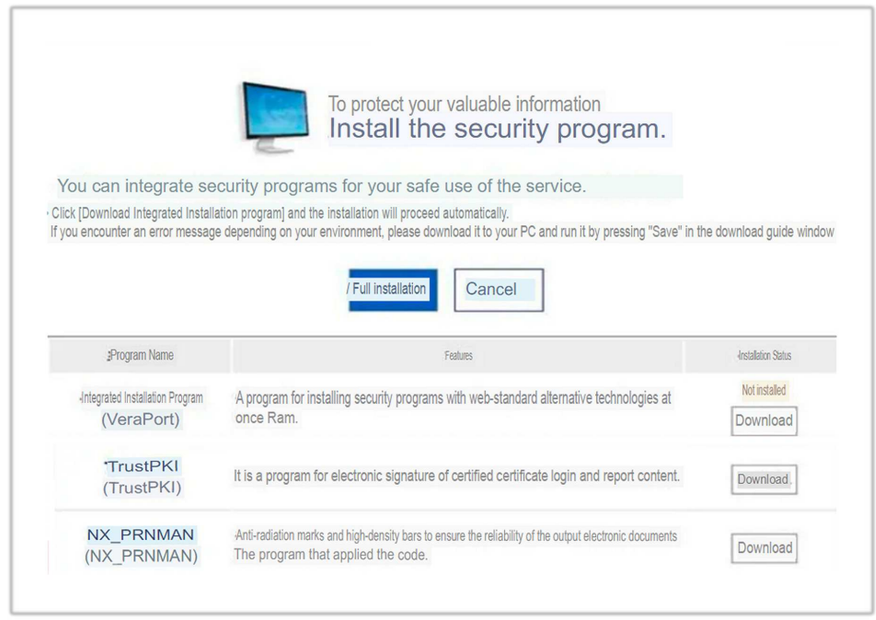


Figure 4. Malicious Korean web page (translated version).

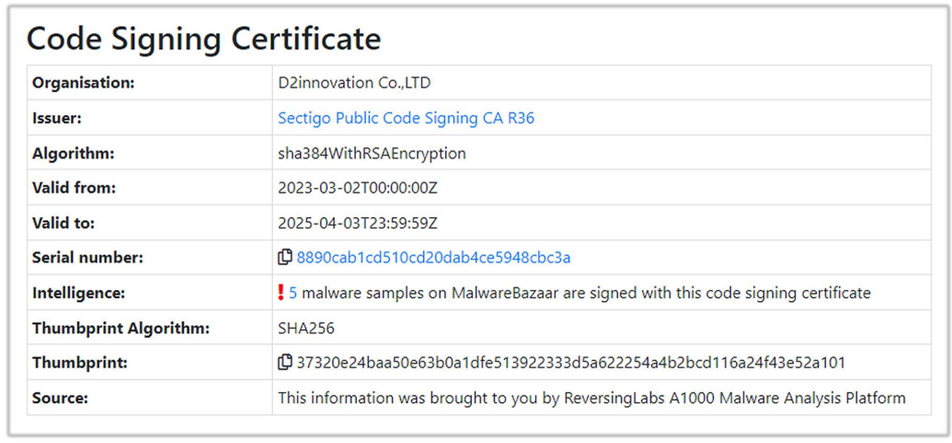
Downloading of the Trojan horse

Suspicious certificates

When downloaded, the Trojan malware is a binary signed with the **D2innovation Co.,LTD** certificate. For example, NXTPKIENT.exe has the following certificate:

Figure 5. Certificat D2innovation.

The certificate is reported on *Malware Bazaar* as being used by five malware.



Code Signing Certificate

Organisation:	D2innovation Co.,LTD
Issuer:	Sectigo Public Code Signing CA R36
Algorithm:	sha384WithRSAEncryption
Valid from:	2023-03-02T00:00:00Z
Valid to:	2025-04-03T23:59:59Z
Serial number:	8890cab1cd510cd20dab4ce5948cbc3a
Intelligence:	! 5 malware samples on MalwareBazaar are signed with this code signing certificate
Thumbprint Algorithm:	SHA256
Thumbprint:	37320e24baa50e63b0a1dfe513922333d5a622254a4b2bcd116a24f43e52a101
Source:	This information was brought to you by ReversingLabs A1000 Malware Analysis Platform

Figure 6. Malware Bazaar : Analysis.

IT security software from **SGA Solutions** are normally signed with the **SGA** certificate. However, NXTPKIENT.exe appears to be signed by a certificate stolen from the company **D2innovation**.

Mutex creation

When executed, NXTPKIENT.exe creates the following mutex:

```
\Sessions\1\BaseNamedObjects\windows update {2024-1020-02A}
```

Defense evasion: indicator removal

After creating the mutex, NXTPKIENT.exe creates a BAT script at the location %Temp%\\[A-Z0-9]{4}.tmp.bat.

File Path	Offset	Length	Value	Ascii
C:\Users\user\AppData\Local\Temp\2675.tmp.bat	0	223	3a 67 6f 74 6f 5f 72 65 64 65 6c 0d 0a 72 64 20 2f 73 20 2f 71 20 22 43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 44 65 73 6b 74 6f 70 5c 4e 58 54 50 4b 49 45 4e 54 2e 65 78 65 22 0d 0a 64 65 6c 20 22 43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 44 65 73 6b 74 6f 70 5c 4e 58 54 50 4b 49 45 4e 54 2e 65 78 65 22 0d 0a 69 66 20 65 78 69 73 74 20 22 43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 44 65 73 6b 74 6f 70 5c 4e 58 54 50 4b 49 45 4e 54 2e 65 78 65 22 20 67 6f 74 6f 20 67 6f 74 6f 5f 72 65 64 65 6c 0d 0a 64 65 6c 20 22 43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 32 36 37 35 2e 74 6d 70 2e 62 61 74 22	:goto_redelrd /s /q "C:\Users\ user\Desktop\NXTPKIENT.exe"del "C:\Users\user\Desktop\NXTPKI ENT.exe"if exist "C:\Users\use r\Desktop\NXTPKIENT.exe" goto goto_redeldel "C:\Users\user\A ppData\Local\Temp\2675.tmp.bat"

Figure 7. JoeSandBox : Analysis.

This script will be run later to remove traces of the Trojan malware dropper (NXTPKIENT.exe) and the BAT script itself. Below is the content of the script:

```
:goto_redel
rd /s /q [File path]
del [File path]
if exist [File path] goto goto_redel
del %Temp%\\[A-Z0-9]{4}.tmp.bat
```

Drop of artifacts

When the BAT script is created, NXTPKIENT.exe deploys three artifacts:

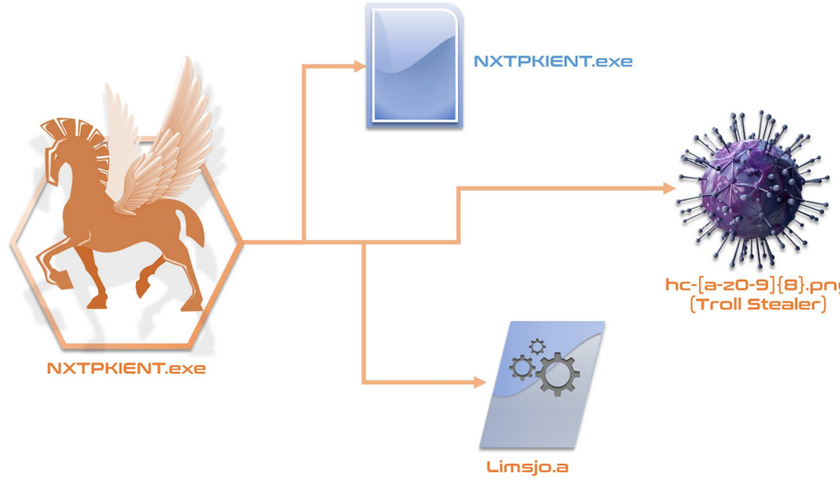


Figure 8. Artifacts dropped.

- NXTPKIENT.exe: This is the legitimate binary crafted by the company **SGA Solutions**. It is executed to trigger the installation of the security software. Location: %USERPROFILE%\Desktop\NXTPKIENTS.exe

- hc-[a-z0-9]{8}.png (Troll Stealer): the spyware, a malware specially crafted to steal data. The file and folder name may vary. Location: %USERPROFILE%\Hancom\hc-[a-z0-9]{8}.png

- limsjo.a: a small file used by attackers to check the authenticity of the infection chain. The file and folder name may vary. Location: %ProgramData%\limsjo.a

Troll Stealer

Drop and execution

The malware hc-[a-z0-9]{8}.png (Troll Stealer) is dropped by NXTPKIENT.exe. Below is a *JoeSandBox* analysis, Troll Stealer is dropped in C:\Users\user\AppData\Roaming\Hancom\ with the name hc-89c9a0b9.png:

File Path	Offset	Length	Value	Ascii
C:\Users\user\AppData\Roaming\Hancom\hc-89c9a0b9.png	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0d 00 29 4b fd 65 00 00 00 00 00 00 00 00 fd 00 2e 22 0b 02 02 24 00 18 4e 00 00 26 fd 00 00 28 06 00 7e 2e fd 00 00 10 00 00 00 00 fd 34 02 00 00 00 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 5e 01 00 04 00 00 fd 54 fd 00 03 00 60 fd 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd)Ke."$N&(~.4^T`

Figure 9. JoeSandBox: Troll Stealer Deployment.

Troll Stealer is run by NXTPKIENT.exe via rundll32.exe.

```
C:\Windows\system32\rundll32.exe C:\Users\user\AppData\Roaming\Hancom\hc-89c9a0b9.png
```

Deleting a scheduled task

Upon execution, Troll Stealer deletes a scheduled task from the *Chrome* browser.

```
schtasks /delete /f /tn "ChromeUpdateTaskMachineUAC"
```

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules	
Source: C:\Windows\System32\rundll32.exe	Process created: C:\Windows\System32\schtasks.exe schtasks /delete /f /tn "ChromeUpdateTaskMachineUAC"

Figure 10. JoeSandBox : Boot Survival.

Infection verification

After deleting the Chrome scheduled task, Troll Stealer checks for the presence of the file:

```
%ProgramData%\limsjo.a
```

If the file is present, Troll Stealer considers that it comes from the Trojan horse NXTPKIENT.exe. If the limsjo.a file is not present, then the system infection is halted.

Mutex

Troll Stealer creates the following mutex.

```
chrome development kit 1.0
```

Configuration

A configuration file is created by Troll Stealer at the location:

```
%UserProfile%\.tmp\{nombre aléatoire}.org
```

This file is completed by Troll Stealer with information about the infected system and the addresses of the CnC servers which will be used to exfiltrate the stolen data.

```
{
"ServerID": 0,
"ObjectID": 0,
"GtType": 2111,
"GtID": [sha1_hash(little_endian(mac_addr[:8]))],
"GtVer": "gt@2.0",
"Interval": 0,
"LocalPath": "%AppData%\\local\\",
"MacAddr": [Adresse MAC],
"ProxyNum": 5,
"ProxyUrl": [
"",
"",
"",
"hxxp://qi.limsjo.p-e.kr/index.php",
"hxxp://ai.limsjo.p-e.kr/index.php"
]
}
```

CnC Addresses:

```
Server CnC: hxxp[:]//qi.limsjo.p-e[.]kr/index.php
Server CnC: hxxp[:]//ai.limsjo.p-e[.]kr/index.php
```

When Troll Stealer has finished filling its configuration file, it is encrypted and saved to the location:

```
%AppData%\local\gcfg@{YYMMDD}(HH.MM.SS-000).gte1
```

As soon as the file is sent to the CnC servers, it is deleted locally so as not to leave traces on the infected system.

Stealing and exfiltrating data

Data theft: SSH

Troll Stealer checks the presence of the *.ssh* folder on the infected system:

```
%USERPROFILE%\.ssh
```

If the *.ssh* folder is present on the system, Troll Stealer makes an encrypted copy of it and saves it in the location:

```
%AppData%\local\tsd@{YYMMDD}(HH.MM.SS-000).gte1
```

This file is then uploaded to the CnC servers.

Data theft: FileZilla

Troll Stealer targets *FileZilla* software located in:

```
%AppData%\filezilla
```

The entire *FileZilla* software folder is copied, encrypted and saved by Troll Stealer to the location:

```
%AppData%\local\tfd@{YYMMDD}(HH.MM.SS-000).gte1
```

This copy is then uploaded to the CnC servers.

Data theft: Microsoft Sticky Note

The *localstate* folder of *Microsoft Sticky Notes* is also targeted:

```
%USERPROFILE%\AppData\Local\packages\microsoft.microsoftstickynotes_8wekyb3d8bbwe\localstate
```

The entire *localstate* software folder is copied, encrypted and saved by Troll Stealer at the location:

```
%AppData%\local\tnd@{YYMMDD}(HH.MM.SS-000).gte1
```

This copy is then uploaded to the CnC servers.

Data theft: GPKI

Troll Stealer also collects information about files and folders present on the **C** drive of the infected system. One folder in particular is sought by the malware: *GPKI*. This is a special folder (*administrative electronic signature certificate*) used by administrative institutions located in South Korea. Important note: this folder is present on workstations of South Korean **public infrastructure**. This folder is not found on personal computers.

When the *GPKI* folder is identified on the infected system, Troll Stealer will then targets specific files and retrieves their titles, for example "GPKI". When the title is retrieved, character strings are generated before and after the title:

```
aaxxyyzz + GPKI + zzyyxxaa
```

A SHA512 is generated from this character string. Troll Stealer checks if this SHA512 matches one of its hardcoded ones. Below is a hardcoded SHA512 fingerprint in Troll Stealer:

```
7ccb0832c3382b5f9e86236e035d899a351c98f3871080c138d4494218cbbc2b6f9dc43705ed97e8b0b09f25752302094e0d297151f6
7b22328af95610f72f1
```

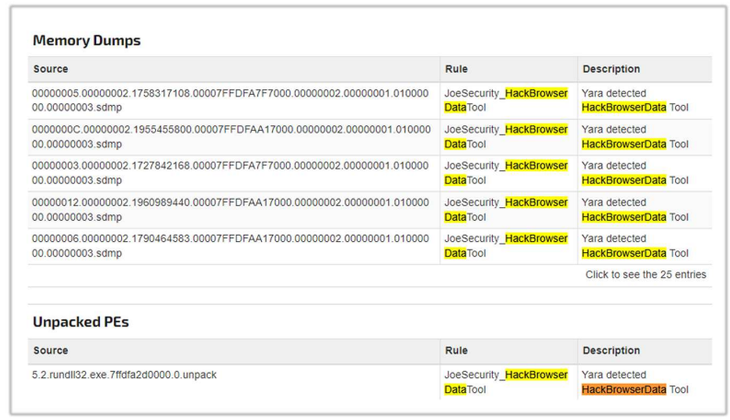
If the generated SHA512 matches a hardcoded hash, then the targeted file is copied, encrypted and saved to the location:

```
%AppData%\local\tcd@{YYMMDD}(HH.MM.SS-000).gte1
```

This copy is then uploaded to the CnC servers.

Data theft: Internet browsers

The tool HackBrowserData is embedded into Troll Stealer. This tool is written in Go and is used to steal information stored by *Chrome* and *Firefox* Internet browsers.



Memory Dumps

Source	Rule	Description
00000005.00000002.1758317108.00007FFDFA7F7000.00000002.00000001.010000 00.00000003.sdmp	JoeSecurity_HackBrowser DataTool	Yara detected HackBrowserData Tool
0000000C.00000002.1955455800.00007FFDFAA17000.00000002.00000001.010000 00.00000003.sdmp	JoeSecurity_HackBrowser DataTool	Yara detected HackBrowserData Tool
00000003.00000002.1727842168.00007FFDFA7F7000.00000002.00000001.010000 00.00000003.sdmp	JoeSecurity_HackBrowser DataTool	Yara detected HackBrowserData Tool
00000012.00000002.1960989440.00007FFDFAA17000.00000002.00000001.010000 00.00000003.sdmp	JoeSecurity_HackBrowser DataTool	Yara detected HackBrowserData Tool
00000006.00000002.1790464583.00007FFDFAA17000.00000002.00000001.010000 00.00000003.sdmp	JoeSecurity_HackBrowser DataTool	Yara detected HackBrowserData Tool
		Click to see the 25 entries

Unpacked PEs

Source	Rule	Description
5.2.rundll32.exe.7ffdfa2d0000.0.unpack	JoeSecurity_HackBrowser DataTool	Yara detected HackBrowserData Tool

Figure 11. JoeSandBox : Analysis - detection of HackBrowserData portable executable (PE) when Troll Stealer infects the system.

The tool retrieves multiple pieces of information including history, downloads, cookies and backups. All this information is saved in a JSON file in the browsers folder. Troll Stealer compresses the JSON file, encrypts it and saves it to the location:

```
%AppData%\local\tbd@{YYMMDD}(HH.MM.SS-000).gte1
```

This copy is then uploaded to the CnC servers.

Data theft: System information

A lot of system information is retrieved by Troll Stealer via the following instruction list:

```
systeminfo &
net user &
query user &
powershell Get-CimInstance -Namespace root/SecurityCenter2 -Classname AntivirusProduct &
wmic qfe &
wmic startup get &
wmic logicaldisk get &
ipconfig /all &
arp -a &
route print &
tasklist &
wmic process get Caption, Commandline &
dir "%programfiles%" &
dir "%programfiles% (x86)" &
dir "%programdata%\Microsoft\Windows\Start Menu\Programs" &
dir "%appdata%\Microsoft\Windows\Recent" &
dir /s "%userprofile%\desktop" &
dir /s "%userprofile%\downloads" &
```

```
dir /s "%userprofile%\documents"
```

In short, Troll Stealer focuses on the following data: user information, installed security software, configuration of IP address, list of processes, installed programs, recently used files, system desktop, downloads and documents.

All retrieved information is saved in an encrypted file at the location:

```
%AppData%\local\ccmd@{YYMMDD}(HH.MM.SS-000).gte1
```

This file is then uploaded to the CnC servers.

Screen capture

Troll Stealer uses a screen capture tool developed by the *Github* user kbinani.

Screenshots are saved and encrypted at the location:

```
%AppData%\local\ssht@{YYMMDD}(HH.MM.SS-000).gte1
```

They are then uploaded to the CnC servers.

Defense evasion : Troll Stealer's indicator removal

To avoid leaving any traces, Troll Stealer is deleted via a PowerShell script generated by the Trojan NXTPKIENT.exe

C:\Users\user\.tmp\1306257149.ps1	
Process:	C:\Windows\System32\rundll32.exe
File Type:	Unicode text, UTF-8 (with BOM) text
Category:	dropped
Size (bytes):	266
Entropy (8bit):	5.238471490498416
Encrypted:	false
SSDEEP:	6:6701PPaZ5mlul7uvDOCuKDOtzKT9MbDOYyc2cl:670MHGI7gDb97el
MD5:	787E9263F7E7A9F3F4AE33EBACB17D02
SHA1:	5D2D363D72FCBAA1DAE5BC9F1F614EDA5467AD65
SHA-256:	76A27E353F324CC1FCAEE62BFBE8A5366C3B5A4069927F1B5EF96C5BCB47C43C
SHA-512:	F84D10922D86DB827B24E736981BF50783C7A7DC68FCA60B97AE0BDC1BE133275E83FD72BD36E690947A34D312993E93D91C919D737BD3D9FDA50B4557978316
Malicious:	true
Preview:	..$target = "C:\Users\user\AppData\Roaming\Hancom\hc-89c9a0b9.png".for ($i = 0; $i -lt 50; $i++).{..Remove-Item $target -Force..Remove-Item $PSCommandPath -Force..if (!(Test-Path $target) -and !(Test-Path $PSCommandPath))..{...break..}..Start-Sleep -Seconds 2.}..

Figure 12. JoeSandBox : PowerShell

Below is the PowerShell code:

```
$target = {path Troll Stealer}
for ($i = 0; $i -lt 50; $i++)
{
Remove-Item $target -Force
Remove-Item $PSCommandPath -Force
if (!(Test-Path $target) -and !(Test-Path $PSCommandPath))
{
break
}
Start-Sleep -Seconds 2
}
```

3.5. APT KIMSUKY attribution

Several details allow us to attribute this cyber-espionage campaign to APT Kimsuky.

3.5.1. A well-known target : South Korea

South Korea is regularly targeted by APT Kimsuky. For example, in 2022 South Korea was targeted by the GoldDragon cyber-espionnage campaign.

3.5.2. Similarity with APT Kimsuky's arsenal

Troll Stealer shares many similarities with Alpha Seed and Apple Seed.

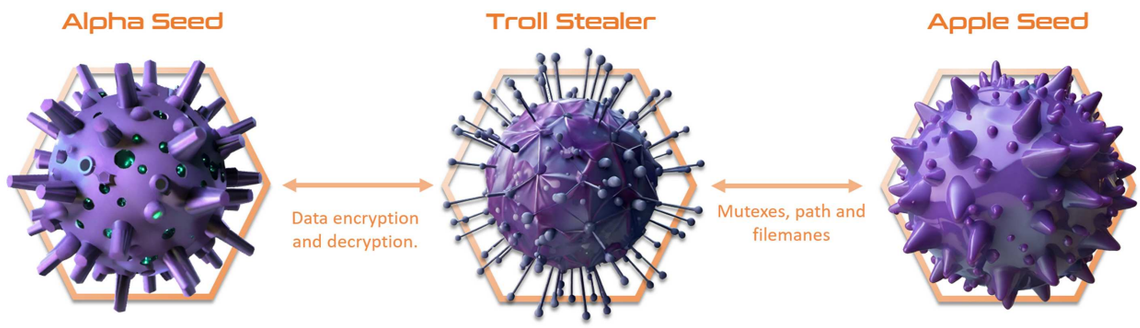


Figure 13. Troll Stealer and its main similarities with Alpha Seed and Apple Seed

Troll Stealer and Apple Seed

Apple Seed is a backdoor used by APT Kimsuky, it shares several similarities with Troll Stealer. For example, the location and name of the malware strain are very similar.

Apple Seed

- Path: %APPDATA%\Media
- Filename: wmi-ui-[random].db

Troll Stealer

- Path: %APPDATA%\Media or %APPDATA%\Hancom
- Filename: hc-[a-z0-9]{8}.png or win-[a-z0-9]{8}.db

Additionally, open source analysis show identical instructions executed by Apple Seed and Troll Stealer to collect information about the infected system. An example of an identical instruction:

```
c:\windows\system32\cmd.exe /c systeminfo & powershell Get-CimInstance -Namespace root/SecurityCenter2
-Classname AntivirusProduct & ipconfig /all & arp -a & dir"%programfiles%" & dir "%proramfiles% (x86)" & dir
"%programdata%\Microsoft\Windows\StartMenu\Programs" /s dir %appdata%\Microsoft\Windows\Recent" & dir
"%userprofile%\desktop" /s & dir "%userprofile%\downloads" /s & dir "%userprofile%\documents" /s
```

The Mutex's names are exactly the same.

Apple Seed

- Mutex name: windows update (2021-1020-02-03-A)

Troll Stealer

- Mutex name: windows update (2021-1020-02-03-A)

Troll Stealer and Alpha Seed

Alpha Seed is a backdoor used by APT Kimsuky, which shares several similarities with Troll Stealer. According to open source analyses, data encryption and decryption are identical. Below are the processes:

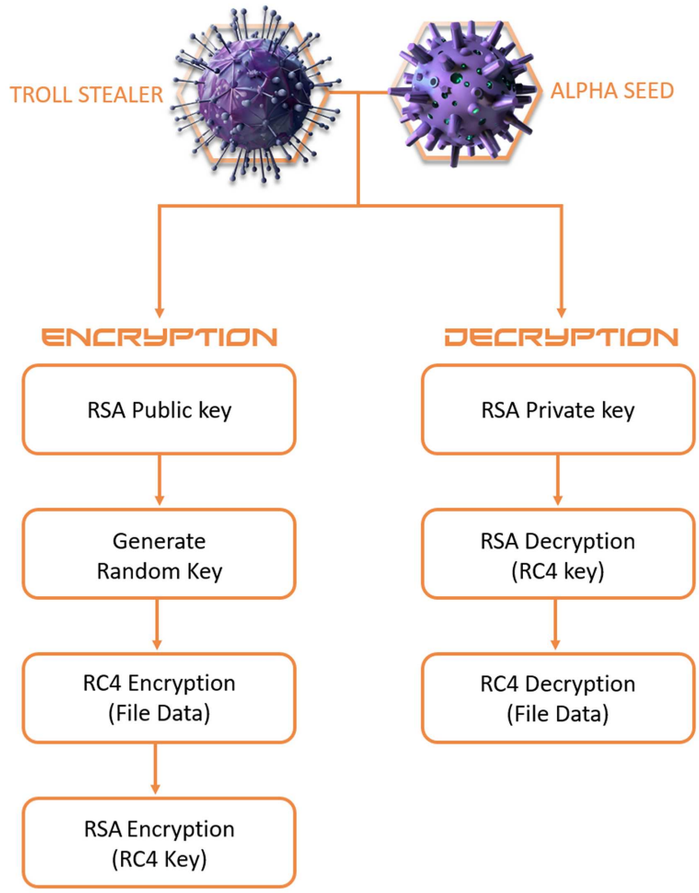


Figure 14. Troll Stealer and Alpha Seed : same encryption and decryption process.

3.6. APT KIMSUKY

APT Kimsuky (aka APT 43, TA406, Thallium, Black Banshee, Velvet Chollima…) is an advanced and persistent threat. It is a state-sponsored threat group from North Korea.

Figure 15. Diamond model of APT Kimsuky.

3.7. Mitre ATT&CK matrix

RESOURCE DEVELOPMENT

T1588.004 Digital Certificates.

EXECUTION

T1204.002 Malicious File. T1059.001 PowerShell. T1059.003 Windows Command Shell.

DEFENSE EVASION

T1027.002 Software Packing

CREDENTIAL ACCESS

T1555.003 Credentials from Web Browsers. T1539 Steal Web Session Cookie.

DISCOVERY

T1057 Process Discovery. T1087.001 Local Account. T1083 File and Directory Discovery.
T1518.001 Security Software Discovery. T1082 System Information Discovery.
T1016 System Network Configuration Discovery.

COLLECTION

T1005 Data from Local System. T1113 Screen Capture.
T1560 Archive Collected Data.

COMMAND and CONTROL

T1071.001 Web Protocol.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

3.8. IOC

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	MD5	19c2decfa7271fa30e48d4750c1d18c1	Dropper NX_PRNMANS.EXE
TLP:CLEAR	SHA1	e6be97ca9e79b45c671c6531908f70b353d47994	Dropper NX_PRNMANS.EXE
TLP:CLEAR	SHA256	6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9	Dropper NX_PRNMANS.EXE
TLP:CLEAR	MD5	7b6d02a459fdaa4caa1a5bf741c4bd42	Dropper NXTPKIENT.exe
TLP:CLEAR	SHA1	4eea45c22881a092ac7a8b0a5379076d5803e83e	Dropper NXTPKIENT.exe
TLP:CLEAR	SHA256	f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3	Dropper NXTPKIENT.exe
TLP:CLEAR	MD5	27ef6917fe32685fdf9b755eb8e97565	Dropper XOWizmxM6U.exe
TLP:CLEAR	SHA1	6d531b021b20febf1dafa730582944eb82d9c6f3	Dropper XOWizmxM6U.exe
TLP:CLEAR	SHA256	2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6d6569a55e	Dropper XOWizmxM6U.exe
TLP:CLEAR	MD5	7457dc037c4a5f3713d9243a0dfb1a2c	Troll Stealer
TLP:CLEAR	SHA1	4c8b7d968806f8108ccde6ac07a37b8174ac44bf	Troll Stealer
TLP:CLEAR	SHA256	ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca	Troll Stealer
TLP:CLEAR	MD5	c8e7b0d3b6afa22e801cacaf16b37355	Troll Stealer
TLP:CLEAR	SHA256	955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b	Troll Stealer
TLP:CLEAR	MD5	88f183304b99c897aacfa321d58e1840	Troll Stealer
TLP:CLEAR	SHA256	bc4c1c869a03045e0b594a258ec3801369b0dcabac193e90f0a684900e9a582d	Troll Stealer
TLP:CLEAR	URL	hxxp(:)//ai.kostin.p-e(.)kr/index.php	
TLP:CLEAR	URL	hxxp(:)//ar.kostin.p-e(.)kr/index.php	
TLP:CLEAR	URL	hxxp(:)//ai.negapa.p-e(.)kr/index.php	
TLP:CLEAR	URL	hxxp(:)//ol.negapa.p-e(.)kr/index.php	
TLP:CLEAR	URL	hxxp(:)//ai.limsjo.p-e(.)kr/index.php	
TLP:CLEAR	URL	hxxp(:)//qi.limsjo.p-e(.)kr/index.php	
TLP:CLEAR	URL	hxxp(:)//coolsystem(.)co.kr/admin/mail/index.php	
TLP:CLEAR	Domain	ai.kostin.p-e(.)kr	
TLP:CLEAR	Domain	ar.kostin.p-e(.)kr	
TLP:CLEAR	Domain	ai.negapa.p-e(.)kr	
TLP:CLEAR	Domain	ol.negapa.p-e(.)kr	
TLP:CLEAR	Domain	ai.limsjo.p-e(.)kr	
TLP:CLEAR	Domain	qi.limsjo.p-e(.)kr	
TLP:CLEAR	IP	216.189.159(.)197	

4. Charming Kitten's advanced spear-phishing

4.1. Context

Charming Kitten, also known as APT35, Phosphorus and Mint Sandstorm, is an **alleged iranian APT** active since 2013. They are known for their large-scale attacks, such as the one against **HBO** in 2017, with the exfiltration of around 1.7 terabytes of sensitive data, and their alleged involvement in **political interference operations**, notably during the 2019 US election campaign.

The organisation is suspected to be related with the **Islamic Revolutionary Guard Corps** (IRGC). It appears that they are seeking intelligence related to IRGC operations and other Iranian intelligence-gathering objectives.

The APT group has been very active in 2023, particularly due to the **intensification of the Israeli-Palestinian conflict**. Lures on this subject have been observed in their **spear-phishing** campaigns.

In their recent attacks, Charming Kitten used advanced social engineering techniques, engaging in prolonged e-mail conversations before sending **malicious links**. In one of their campaign, they even created **fake webinars**, requiring the installation of illegitimate software, to trick their targets.

The aim of this sophisticated phishing is to deploy malware. In campaigns observed between 2023 and 2024, at least 5 malware families were observed: POWERSTAR, POWERLESS, NOKNOK, BASICSTAR, EYEGLASS.

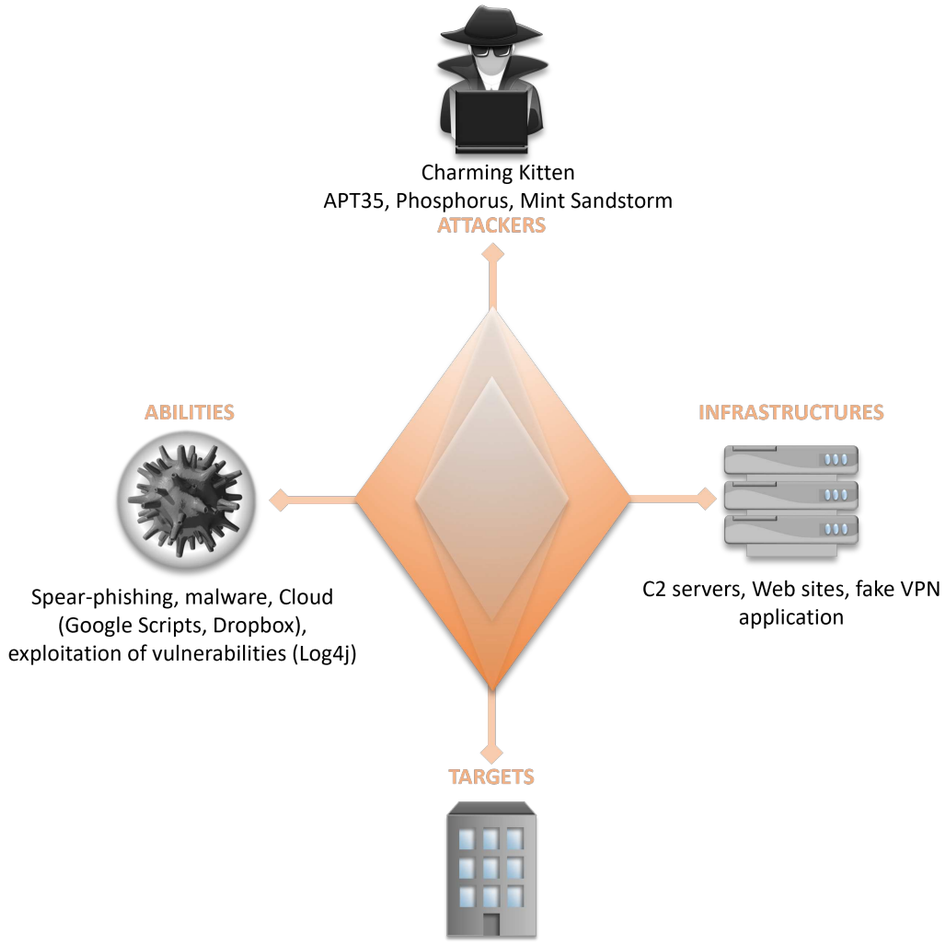
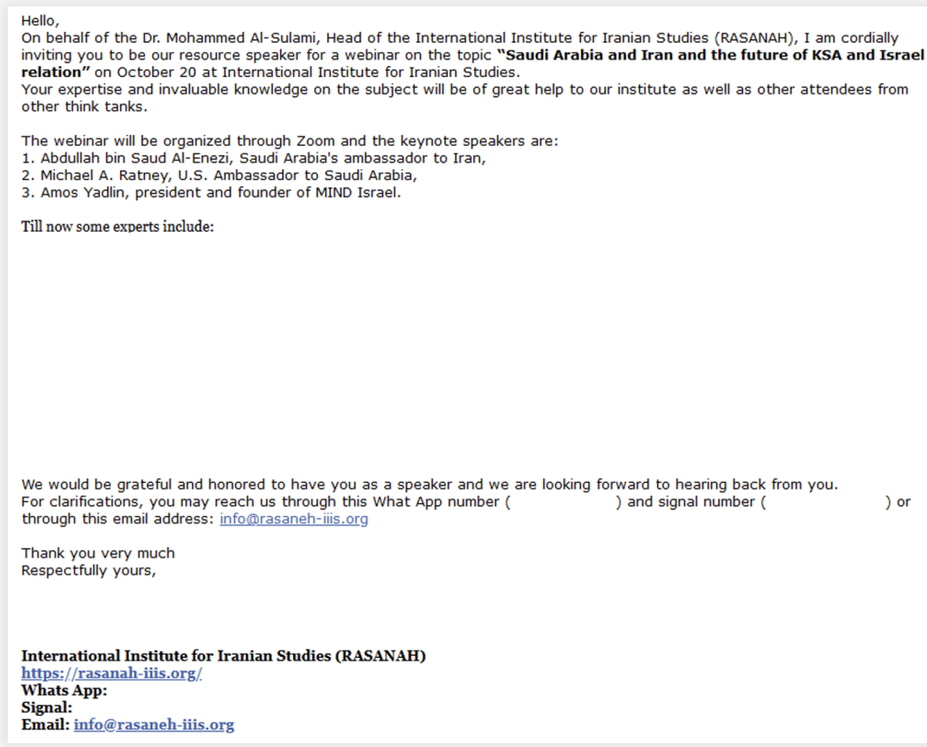


Figure 16. Charming Kitten Diamond Model.

4.2. Spear-Phishing (T1566.002) and its multiple methods

In September and October 2023, Charming Kitten carried out a series of spear-phishing attacks impersonating the **Rasanah International Institute of Iranian Studies** (IIIS). The campaign targeted political experts, inviting them to participate in a webinar.

To achieve this, the attackers registered several typo-squatted domain names similar to that of the organisation, **rasanah-iiis[.]org** to legitimise the e-mails sent to their targets.



Hello,
On behalf of the Dr. Mohammed Al-Sulami, Head of the International Institute for Iranian Studies (RASANAH), I am cordially inviting you to be our resource speaker for a webinar on the topic **"Saudi Arabia and Iran and the future of KSA and Israel relation"** on October 20 at International Institute for Iranian Studies.
Your expertise and invaluable knowledge on the subject will be of great help to our institute as well as other attendees from other think tanks.

The webinar will be organized through Zoom and the keynote speakers are:
1. Abdullah bin Saud Al-Enezi, Saudi Arabia's ambassador to Iran,
2. Michael A. Ratney, U.S. Ambassador to Saudi Arabia,
3. Amos Yadlin, president and founder of MIND Israel.

Till now some experts include:

We would be grateful and honored to have you as a speaker and we are looking forward to hearing back from you.
For clarifications, you may reach us through this What App number ( ) and signal number ( ) or through this email address: info@rasaneh-iiis.org

Thank you very much
Respectfully yours,

International Institute for Iranian Studies (RASANAH)
https://rasanah-iiis.org/
Whats App:
Signal:
Email: info@rasaneh-iiis.org

Figure 17. Phishing email - Source : Volexity.

Furthermore, Charming Kitten deployed an extensive infrastructure to host this fake webinar. They set up a complete website using a legitimate ISSS appearance and offering all the services that a webinar platform could offer.

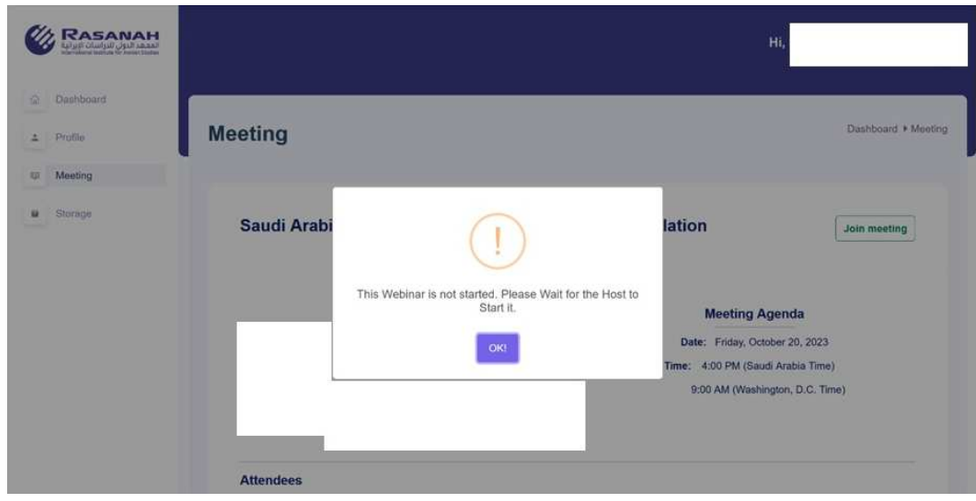


Figure 18. Webinar platform - Source : Volexity.

In addition to creating this highly realistic **decoy**, the attackers forced victims to use a **VPN** they controlled. Targets were invited to download the VPN application, which was then used to deploy the payloads.

In this campaign, victims on a Windows environment received an infection chain to deploy the POWERLESS malware, while the NOKNOK malware was deployed on macOS.

In a second campaign, the attacking group directed victims to a download platform. Charming Kitten took the time to strike up a

conversation with targets, sending successive e-mails to establish a bond of trust and ensure that the victim clicked and downloaded the malicious payload.

The platform hxxps://cloud-document-edit.onrender[.]com/page/jujbMKB[snipped]TpCNvV hosted a password-protected *RAR* file, which contained two *LNK* files: "US strategy in the Middle East is coming into focus - Shortcut.lnk" and "The global consequences of the Israel-Hamas war - Shortcut.lnk". These file names were chosen from recent legitimate articles to attract victims.

The *LNK* files were used to download and execute the malware BASICSTAR and KORKULOADER respectively.

In a third campaign observed in May 2023, Charming Kitten impersonated a **principal researcher at the Royal United Services Institute (RUSI)**. The targets were experts in Middle Eastern affairs and nuclear security. The message solicited comments on a project entitled "Iran in the context of global security" and asked for permission to send a draft for review.

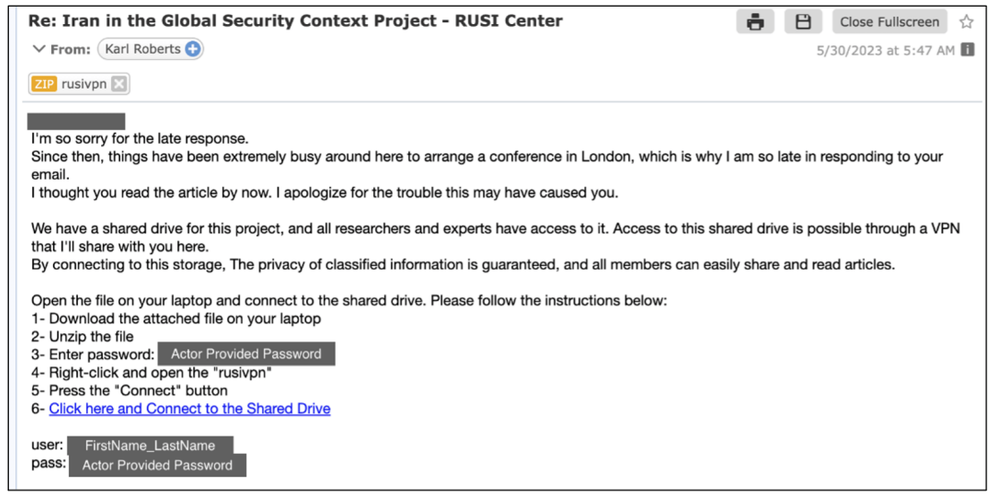


Figure 19. Phishing email - Source : ProofPoint.

The APT group then provided its target with a link that redirected the victim to a DropBox URL. This hosted a password-encrypted .rar file, "Abraham Accords & MENA.rar", which contained a malicious payload.

These different approaches clearly demonstrate the targeted nature of the attacks. The Iranian group has a precise objective in carrying out a campaign, where every **victim is specially selected**, and new infrastructures are deployed.

Unlike opportunistic attacks, this type of campaign is **planned** months or even years in advance, to ensure success.

4.3. Malware deployment

The aim of these **spear-phishing** campaigns is to deploy malware on victims' various devices to establish persistence and harvest **intelligence** on targets over long periods. To achieve this, Charming Kitten uses several families of **malware** that they have **developed** or **customised**.

4.3.1. POWERLESS

Observed in a campaign associated with the group Educated Manticore, this malware also appears to be used by Charming Kitten. Overlaps between the two groups have been reported by *CheckPoint* researchers.

This malware includes the following features and tools:

- Command and Control,
- Command execution,
- A loader for deploying information-stealing malware,
- An audio recorder.

To ensure its persistence, this malware allows its configuration to be updated, including its C2 address.

4.3.2. NOKNOK

NOKNOK is a malware that runs on **macOS**. Its various modules enable the attacker to establish **persistence**, perform **reconnaissance** and **collect information** that can then be exfiltrated to a **Command and Control** server.

Both malwares are based on the POWERSTAR, malware developed by Charming Kitten and first observed in 2022. This highlights the fact that the group continues to evolve and, above all, adapts to its targets. Indeed, variants have been created depending on their victim's environment.

4.4. Yara rules

```
    rule apt_malware_ps1_powerless_b: CharmingCypress
    {
    meta:
        author = "threatintel@volexity.com"
        date = "2023-10-25"
        description = "Detects POWERLESS malware."
        hash1 = "62de7abb39cf4c47ff120c7d765749696a03f4fa4e3e84c08712bb0484306ae1"
        os = "win"
        os_arch = "all"
        reference = "https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-
targeting-israel-via-improved-arsenal-of-tools/"
        report = "TIB-20231027"
        scan_context = "file,memory"
        last_modified = "2023-11-03T15:38Z"
        license = "See license at https://github.com/volexity/threat-intel/blob/main/LICENSE.txt"
        rule_id = 9794
        version = 4
    strings:
        $fun_1 = "function verifyClickStorke"
        $fun_2 = "function ConvertTo-SHA256"
        $fun_3 = "function Convert-Tobase" fullword
        $fun_4 = "function Convert-Frombase" fullword
        $fun_5 = "function Send-Httppacket"
        $fun_6 = "function Generat-FetchCommand"
        $fun_7 = "function Create-Fetchkey"
        $fun_8 = "function Run-Uploader"
        $fun_9 = "function Run-Shot" fullword
        $fun_10 = "function ShotThis("
        $fun_11 = "function File-Manager"
        $fun_12 = "function zip-files"
        $fun_13 = "function Run-Stealer"
        $fun_14 = "function Run-Downloader"
        $fun_15 = "function Run-Stro" fullword
        $fun_16 = "function Run-Tele" fullword
        $fun_17 = "function Run-Voice"
        $s_1 = "if($commandtype -eq \"klg\")"
        $s_2 = "$desrilizedrecievedcommand"
        $s_3 = "$getAsyncKeyProto = @"
        $s_4 = "$Global:BotId ="
        $s_5 = "$targetCLSID = (Get-ScheduledTask | Where-Object TaskName -eq"
        $s_6 = "$burl = \"$Global:HostAddress/"
        $s_7 = "$hashString = [System.BitConverter]::ToString($hash).Replace('-','').ToLower()"
        $s_8 = "$Global:UID = ((gwmi win32_computersystemproduct).uuid -replace '[^0-9a-z]').substring("
        $s_9 = "$rawpacket = \"{`\"MId`\":`\"$Global:MachineID`\",`\"BotId`\":`\"$basebotid`\"}\""
        $s_10 = "$bitmap = New-Object System.Drawing.Bitmap $bounds.Width, $bounds.Height"
        $s_12 = "Runned Without any Error"
        $s_13 = "$commandresponse = (Invoke-Expression $instruction -ErrorAction Stop) | Out-String"
        $s_14 = "Operation started successfuly"
        $s_15 = "$t_path = (Get-WmiObject Win32_Process -Filter \"name = '$process'\" | Select-Object
CommandLine).CommandLine"
        $s_16 = "?{ $_.DisplayName -match \"Telegram Desktop\" } | %{$app_path += $_.InstallLocation }"
        $s_17 = "$chlids = get-ChildItem $t -Recurse -Exclude \"$t\\tdata\\user_data\""
        $s_18 = "if($FirsttimeFlag -eq $True)"
        $s_19 = "Update-Conf -interval $inter -url $url -next_url $next -conf_path $conf_path -key
$config_key"
    condition:
        3 of ($fun_*) or
        any of ($s_*)
}
```

```
    rule apt_malware_noknok_base64_encoded_bash : CharmingCypress
    {
    meta:
        author = "threatintel@volexity.com"
        date = "2023-10-25"
        description = "Detects base64 script execution technique used by CharmingCypress to decode and
execute NOKNOK."
        hash1 = "42477f0236e648f6e981db279406ca5f2a37a26cdf2baf472c41cb7f85f046e8"
        hash2 = "a437876ae60ddeb8a59f88b7a5af82ca95cb16446a3f6aea8b811402da31cd8a"
        hash3 = "ec14d1d4a30a9e11bb7360f46d3154fc4117b5b161a2a87afa8d0a730d017b69"
        hash4 = "dab8a955a8bc3c3fb2643fcde9b184073b104840db8842cf10f755c9e46e0633"
        os = "darwin,linux"
        os_arch = "all"
        report = "TIB-20231027"
        scan_context = "file"
        last_modified = "2023-10-27T16:17Z"
```

```
        license = "See license at https://github.com/volexity/threat-intel/blob/main/LICENSE.txt"
        rule_id = 9792
        version = 3
    strings:
        $start = "bash -c bash -c \"$(base64 -d <<< \"" nocase
        $end = /"\)"; bash "\$@"$/
    condition:
        filesize < 100KB and
        for any i in (0..#start):
            (
                $end in (@start[i]..@start[i]+10240)
            )
}
```

4.5. IOC

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	domain	www[.]defaultbluemarker[.]info	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	IP	144[.]217[.]117[.]74	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	1690cff04de44a26440d4fd15d0a0c11f64d3db670607ef658938690436b6636	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	domain	rasaanah-iiis[.]org	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	37bb42720bfc1cf5d0e9d7b66be134b6431055ed8bdfd384f61ab7ac061d26eb	POWERLESS persistence module
TLP:CLEAR	domain	panel[.]rasaanah-iiis[.]org	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	2d99755d5cd25f857d6d3aa15631b69f570d20f95c6743574f3d3e3e8765f33c	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	35f062f46f42dce06804cc4e7b456c528618d650edcf1cf7f806c016e88b3d19	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	IP	149[.]28[.]133[.]236	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	domain	beginningofgraylife[.]ddns[.]net	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	domain	yellowparallelworld[.]ddns[.]net	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	f1ee5dd179f66f597edfeb4b2c73c6adb4b7b6d4dcfb0bef33ee5c285148d085	POWERLESS browser stealer module
TLP:CLEAR	domain	defaultbluemarker[.]info	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	1feade2bbd4dbc0b2052213d792b83c969928a150dce332746a6b5426ac93e4f	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	a8622dccb40a9fe9c2123f661e32e0a6bc40e95c88c9c2b764e603ce5eccb311	POWERLESS .NET loader
TLP:CLEAR	domain	www[.]rasaaneh-iiis[.]org	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	domain	rasaneh-iiis[.]org	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	domain	rasaaneh-iiis[.]org	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	42477f0236e648f6e981db279406ca5f2a37a26cdf2baf472c41cb7f85f046e8	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	11f0e38d9cf6e78f32fb2d3376badd47189b5c4456937cf382b8a574dc0d262d	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	domain	www[.]panel[.]rasaaneh-iiis[.]org	IOCs associated with CharmingCypress phishing activity distributing POWERLESS and NOKNOK malware via malicious VPN applications.
TLP:CLEAR	sha256	9ef84d6a709adbd6f29813ee145dbf542a69150e5ab4261e0d58de7ee371a8ef	POWERLESS audio recorder module
TLP:CLEAR	domain	coral-polydactyl-dragonfruit[.]glitch[.]me	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	domain	east-healthy-dress[.]glitch[.]me	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	sha256	c6f91e5585c2cbbb8d06b7f239e30b271f04393df4fb81815f6556fa4c793bb0	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	sha256	f6f0f682668f78dbecfc30a0e0c76b6a3d86298869fb44b39adf19fdcdca5762	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	domain	wulpfsrqupnuqorhexiw[.]supabase[.]co	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	domain	cloud-meeting-online[.]onrender[.]com	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	sha256	1ffc0bb577e4605059143a5cca213fbe0762c320c74174fe3c2a8f4878c85fc0	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	sha256	13b659e009577ab7890157ce00cc5c3641049f46135d5be2b1c17ca88a1490f9	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	sha256	fdc5d6caaaa4fb14e62bd42544e8bb8e9b02220e687d5936a6838a7115334c51	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	domain	view-document-online[.]onrender[.]com	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	domain	cloud-document-edit[.]onrender[.]com	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	sha256	07384ab4488ea795affc923851e00ebc2ead3f01b57be6bf8358d7659e9ee407	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	domain	prism-west-candy[.]glitch[.]me	CharmingCypress indicators of compromise related to BASICSTAR and KORKULOADER related phishing.
TLP:CLEAR	sha256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f	CharmingCypress related indicators

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	sha256	1e7d2390a64abf51291d58a4104341664ec3c4f9989e07bdf612ecbe53f1231c	.NET dll likely used as a helper with other unknown malware - provides functionality to read the contents of a sha256 and converts the result to base64
TLP:CLEAR	sha256	b0f0aeded0aa68cfa17353faaf2093d35237758cdb668fff91f915092c9696ed	CharmingCypress related indicators
TLP:CLEAR	IP	185[.]36[.]189[.]81	CharmingCypress related indicators
TLP:CLEAR	sha256	10460becafe4a67b959d9eaa09fb391d4ed46c083843ca3ab28c36e803760e41	CharmingCypress related indicators
TLP:CLEAR	sha256	bd7db9d9617c6108ed363cc2622594e9fd6932ed2c25f403bd1cc83bc9a21a1d	RATHOLE config
TLP:CLEAR	sha256	cfd340b4b4b3698f87acd1bebe8bec3d3ff48bfd6513a73c9aa3975d2cfe84c3	CharmingCypress related indicators
TLP:CLEAR	sha256	ea308c76a2f927b160a143d94072b0dce232e04b751f0c6432a94e05164e716d	Command line 7z
TLP:CLEAR	sha256	a288618325a42a22fc642a73c5f5a39409a229e7f7aedec0043839b1e1483266	Nirsofts' Chrome History Viewer
TLP:CLEAR	domain	editorservices[.]onrender[.]com	CharmingCypress related indicators
TLP:CLEAR	sha256	56cd102b9fc7f3523dad01d632525ff673259dbc9a091be0feff333c931574f7	Command line Winrar
TLP:CLEAR	sha256	e4e7f08d9a9a662b5615e8fcbb6cd3c711ecab6341a60562bbeff9ccca43f7e0	CommandCam utility
TLP:CLEAR	domain	tgtoolsservice[.]onrender[.]com	CharmingCypress related indicators
TLP:CLEAR	domain	ndrrftqrlblfecpupppp[.]supabase[.]co	CharmingCypress related indicators
TLP:CLEAR	sha256	8803b8faa6e6ee4c3cdf31b6d6b4af104be8650e2ff63a9b9818b3e2596fdc5b	CharmingCypress related indicators

5. Sources

CVE-2024-1071

- https://www.cve.org/CVERecord?id=CVE-2024-1071
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ultimate-member/ultimate-member-user-profile-registration-login-member-directory-content-restriction-membership-plugin-213-282-unauthenticated-sql-injection
- https://www.wordfence.com/blog/2024/02/2063-bounty-awarded-for-unauthenticated-sql-injection-vulnerability-patched-in-ultimate-member-wordpress-plugin/

CVE-2024-24691

- https://www.cve.org/CVERecord?id=CVE-2024-24691
- https://www.zoom.com/en/trust/security-bulletin/ZSB-24008/
- https://www.zoom.com/en/trust/security-bulletin/

CVE-2024-21626

- https://www.cve.org/CVERecord?id=CVE-2024-21626
- https://github.com/opencontainers/runc/security/advisories/GHSA-xr7r-f8xq-vfvv
- https://www.docker.com/blog/docker-security-advisory-multiple-vulnerabilities-in-runc-buildkit-and-moby/
- https://github.com/containerd/containerd/releases/tag/v1.7.13
- https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.30.md
- https://aws.amazon.com/security/security-bulletins/AWS-2024-001/
- https://cloud.google.com/anthos/clusters/docs/security-bulletins#gcp-2024-005
- https://github.com/Azure/AKS/issues/4080
- https://access.redhat.com/security/vulnerabilities/RHSB-2024-001

Virology : Troll Stealer (APT KIMSUKY)

- https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2
- https://thehackernews.com/2024/02/kimsukys-new-golang-stealer-troll-and.html
- https://www.virustotal.com/gui/file/f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3/community
- https://www.shouldiremoveit.com/trustpki-kcue-non-activex-client-195964-program.aspx
- https://socprime.com/blog/troll-stealer-detection-novel-malware-actively-leveraged-by-north-korean-kimsuky-apt/
- https://bazaar.abuse.ch/sample/61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92/
- https://bazaar.abuse.ch/sample/ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca/
- https://bazaar.abuse.ch/sample/f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3/
- https://www.joesandbox.com/analysis/1371926/1/html
- https://www.joesandbox.com/analysis/1384316/0/html
- https://www.joesandbox.com/analysis/1384193/1/html
- https://www.joesandbox.com/analysis/1371688/1/html
- https://www.pcrisk.com/removal-guides/29101-troll-stealer
- https://socradar.io/apt-profile-kimsuky/

Charming Kitten's advanced spear-phishing

- https://cybersecuritynews.com/charmingcypress-poisoned-vpn-apps/
- https://www.volexity.com/blog/2024/02/13/charmingcypress-innovating-persistence/
- https://www.proofpoint.com/us/blog/threat-insight/welcome-new-york-exploring-ta453s-foray-lnks-and-mac-malware
- https://www.volexity.com/blog/2023/06/28/charming-kitten-updates-powerstar-with-an-interplanetary-twist/ https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-targeting-israel-via-improved-arsenal-of-tools/
- https://therecord.media/charming-kitten-targeted-israel-cyberattacks

- https://github.com/volexity/threat-intel/blob/main/2024/2024-02-13%20CharmingCypress/rules.yar