aDvens

Security for the greater good

Monthly Cyber Threat Intelligence report
July 2024

2024-08-08 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 38 rue des Jeuneurs - 75002 Paris

Table of content

1. Executive summary

This month, the CERT aDvens presents four noteworthy vulnerabilities, in addition to those already published.

In two articles, the CERT analysts discuss:

- The modus operandi for deploying a HijackLoader via the Driver Booster executable from IObit.
- The necessity of a vulnerability management policy, illustrated through an attack campaign attributed to the Estate ransomware group.

2. Vulnerabilities

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

2.1. ServiceNow - CVE-2024-4879 and CVE-2024-5217

On 10 July 2024, ServiceNow published two vulnerabilities affecting their Utah, Vancouver and Washington DC platforms.

These vulnerabilities are caused by user input control flaws and allow an attacker to execute arbitrary code with the platform's privileges.

These vulnerabilities are actively exploited.

2.1.1. Type of vulnerability

For CVE-2024-4879

- CWE-1287: Improper Validation of Specified Type of Input

For CVE-2024-5217

- CWE-697: Incorrect Comparison
- CWE-184: Incomplete List of Disallowed Inputs

2.1.2. Risk

- Remote code execution

2.1.3. Severity (base score CVSS 3.1)

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. Impacted Products

- Now Platform versions Utah, Vancouver and Washington DC

2.1.5. Recommendations

Update ServiceNow to the following versions:

- **Utah**
  - Utah Patch 10 Hot Fix 3

    - Utah Patch 10a Hot Fix 2
- **Vancouver**
    - Vancouver Patch 6 Hot Fix 2
    - Vancouver Patch 7 Hot Fix 3b
    - Vancouver Patch 8 Hot Fix 4
    - Vancouver Patch 9
    - Vancouver Patch 10
- **Washington DC**
    - Washington DC Patch 1 Hot Fix 2b
    - Washington DC Patch 2 Hot Fix 2
    - Washington DC Patch 3 Hot Fix 1
    - Washington DC Patch 4

Additional information is available in ServiceNow's advisory.

2.1.6. Proof of concept

A proof of concept is available in open source.

2.2. Palo Alto - CVE-2024-5910

An authentication control flaw in a critical function of Palo Alto Networks Expedition allows an attacker to take control of Expedition administrator account.

2.2.1. Type of vulnerability

- CWE-306: Missing Authentication for Critical Function

2.2.2. Risk

- Account compromise

2.2.3. Severity (base score CVSS 3.1)

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

2.2.4. Impacted Products

- Expedition versions prior to 1.2.92

2.2.5. Recommendations

- Update Expedition to version 1.2.92 or later.
- Additional information is available in Palo Alto's advisory.

2.2.6. Proof of concept

To date, no proof of concept is available in open source.

2.3. Progress Telerik - CVE-2024-6327

An insecure deserialisation vulnerability in Progress Telerik allows an attacker to execute arbitrary code.

2.3.1. Type of vulnerability

- CWE-502: Deserialization of Untrusted Data

2.3.2. Risk

- Remote code execution

2.3.3. Severity (base score CVSS 3.1)

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

2.3.4. Impacted Products

- Telerik Report Server versions prior to 10.1.24.709

2.3.5. Recommendations

- Update Telerik Report Server to version 10.1.24.709 or later.
- Additional information is available in Progress' advisory.

2.3.6. Proof of concept

To date, no proof of concept is available in open source.

3. Distribution of HijackLoader with IObit's Driver Booster executable

In May and June 2024, security researchers from *Lab52* and *Kroll* observed the use of HijackLoader malware in attacks to install infostealer payloads. *Lab52* detailed a phishing campaign led by APT-C-36's targeting Colombia where AsyncRAT malware was deployed. For their part, *Kroll* documented a "drive-by download" attack campaign through a Bollywood pirated film download website.

During these two campaigns, the attackers used a ZIP archive containing multiple files, including a legitimate executable signed by IObit RttHlp.exe, Borland Package Library (BPL) files and several other malicious files. This deployment of HijackLoader also makes use of new obfuscations techniques to hide the malicious code and to prevent detection by security solutions based on signature databases.

3.1. HijackLoader

HijackLoader (aka IDAT Loader, DOILoader) is a **malicious loader** malware observed for the first time in **July 2023** by *Zscaler ThreatLabz*. This malware uses system calls to evade detection by security solutions, detects several specific processes based on a blocklist and delays code execution at different steps of its deployment. It also includes multiple embedded modules to simplify malicious code injection and execution.

HijackLoader is used as a vector to deploy **infostealer** payloads such as Lumma, Redline, Amadey, Vidar, Raccoon, StealC but also **remote access tools** such as AsyncRAT or Remcos.

3.1.1. Attack chain

The modus operandi detailed below is based on the drive-by download campaign observed by *Kroll*. The attacker lures its victims through a pirated film download website. When a user tries to download a video, he is redirected to a web page hosted on the content delivery network (CDN) Bunny that provides a short link bit[.]ly so that he downloads a ZIP file.

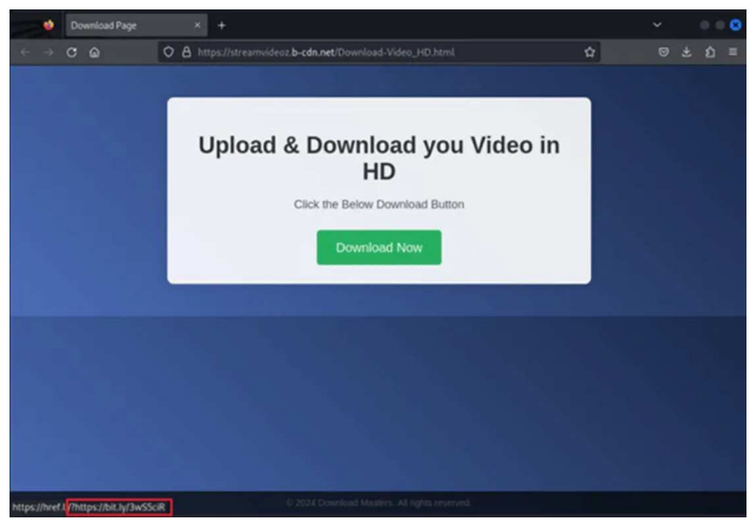

Figure 1. Download page providing the link to the ZIP file - Source: Kroll

This ZIP archive itself contains a ZIP file protected by password and a TXT file providing the password. Once unzipped, the password protected archive contains an LNK file of 192 MB and a decoy file with the "trailer" video.

The malicious LNK file uses Microsoft's executable mshta.exe to download an **OpenPGP secret key** hosted on Bunny CDN. This key is in fact specifically crafted content containing an **HTML Application (HTA)** script, Microsoft's legitimate executable calc.exe and additional **junk bytes**, including the first two bytes corresponding to the Magic bytes of an OpenPGP secret key. This setup is used to escape protective measures based on AI, resulting in an extremely low detection rate on VirusTotal with only one detection among 64 security products at the time of *Kroll*'s analysis.

Mshta.exe then runs the HTA malicious code, even if it is not compliant with HTML standard. Web browsers always try to render an

HTML page even if there are errors, due to inconsistencies between different browsers, poor coding practices or the lack of testing of millions of websites. The mshta.exe process is not an exception to this rule. However, unlike browsers that are often protected by sandboxed execution, stopping scripts from interacting with the underlying system, HTA scripts executed through mshta.exe can interact with the host system without these restrictions.

This technique allows a malicious script to potentially mimic any type of file, the latter being analysed differently according to the security solutions used, which makes it easier to bypass them. The attacker takes advantage of this behavior to distribute HijackLoader.

The HTA code contained in the crafted file also has **four layers of obfuscation**, making the code invalid for HTML. Fully deobfuscated, the code downloads two separates ZIP archives. The script contains an unzip function that will drop the content of the archive in *%AppData%* and try to use the content as a command to be executed. If the ZIP file contains multiple files or a file that is not executable, the code fails. However, if the archive contains only one executable file, the code is executed.

The analysis of the two archives K1.zip and K2.zip by *Kroll* shows that the first one contains several files while the second one contains only the IOBit's legitimate binary RttHlp.exe renamed jdekl.exe.

Figure 2. Content of downloaded zip files - Source: Kroll

The hydrogeology.wmv file contains encrypted parts of HijackLoader's code. It is decrypted and executed by the loader.

The executable jdekl.exe is written and compiled in **Delphi**. It imports **Borland Package Library (BPL)** files rtl120.bpl and vcl120.bpl which are **DLL** type files created by **Borland** to be used with their compilation tools, especially **Delphi**. Thus, instead of being a common DLL side-loading, it is a BPL side-loading with the executable. This sub-technique does not exist for now in the **MITRE** framework. Its creation was requested by *Kroll*.

The library vcl120.bpl contains code accessing the encrypted data file hydrogeology.wav, which confirms that the file contains the malicious code of HijackLoader.

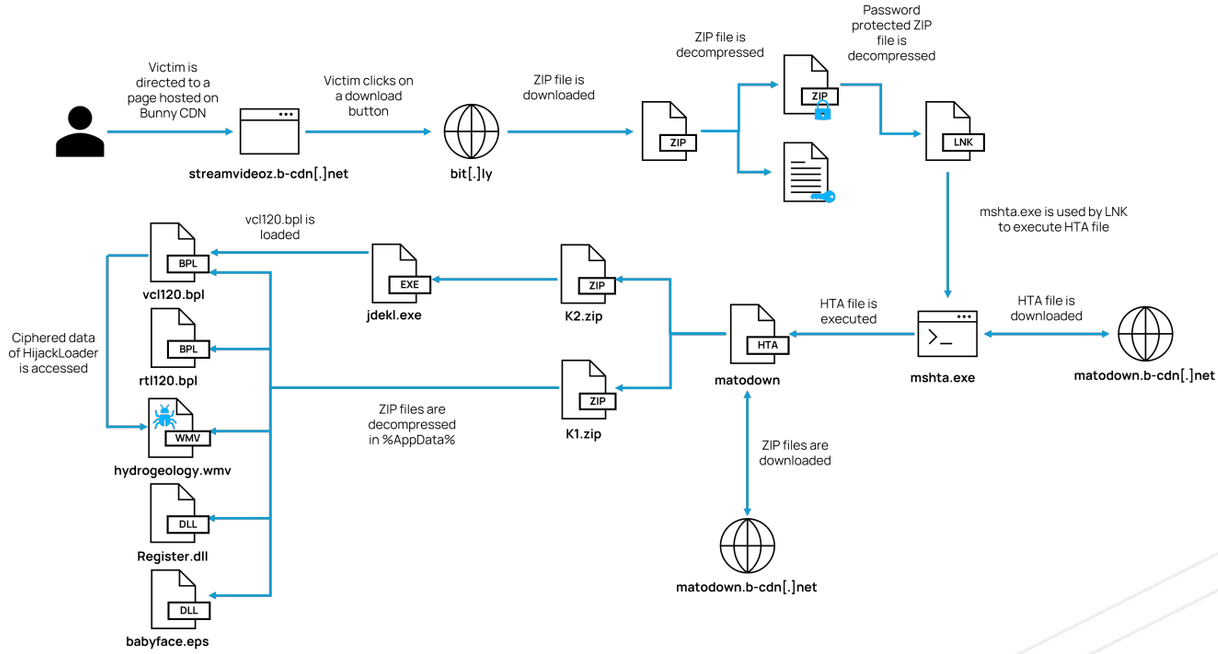

Figure 3. HijackLoader's attack chain

3.1.2. Exploitation of CVE-2024-21412

In more recent campaigns observed in July of infostealer deployment via HijackLoader, CVE-2024-21412 is exploited. This **security bypass** vulnerability in Microsoft's Windows SmartScreen allows an attacker to prevent the appearance of a SmartScreen warning window to deliver malicious files.

By persuading a user to click on a specially crafted URL file, the attacker deploys a malicious LNK file hosted on a **WebDAV** share to the victim's machine.

Figure 4. Content of a URL file - Source: Cyble

The LNK file retrieved uses the legitimate Windows forfiles.exe executable to launch PowerShell, run mshta.exe and download the HTA script. In the campaign detailed by *Cyble*, the HTA file is put together with the legitimate executable dialer.exe to bypass security. The obfuscation of this file is similar to that already observed by *Kroll*.

3.1.3. MITRE ATT&CK

INITIAL ACCESS

T1189 Drive-by Compromise T1566.001 Phishing: Spearphishing Attachment T1566.002 Phishing: Spearphishing Link

EXECUTION

T1204.002 User Execution: Malicious File T1059.001 Command and Scripting Interpreter: PowerShell

PRIVILEGE ESCALATION

T1055 Process Injection

DEFENSE EVASION

T1202 Indirect Command Execution T1218.005 System Binary Proxy Execution: Mshta T1574 Hijack Execution Flow: BPL Sideloading T1564.003 Hide Artifacts: Hidden Windows T1036.003 Masquerading: Rename System Utilities T1036.005 Masquerading: Match Legitimate Name or Location T1036.007 Masquerading: Double File Extension T1562.002 Impair Defenses: Disable Windows Event Logging T1027 Obfuscated Files or Information T1553.004 Subvert Trust Controls: Install Root Certificate

DISCOVERY

T1082 System Information Discovery T1012 Query Registry

LATERAL MOVEMENT

T1021.002 Remote Services: SMB/Windows Admin Shares

COMMAND AND CONTROL

T1071 Application Layer Protocol

Figure 5. MITRE ATT&CK HijackLoader

3.1.4. Detection

Sigma:

```
title: Remotely Hosted HTA File Executed Via Mshta.EXE
id: b98d0db6-511d-45de-ad02-e82a98729620
status: test
description: Detects execution of the "mshta" utility with an argument containing the "http" keyword, which
could indicate that an attacker is executing a remotely hosted malicious hta file
references:
    - https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-
disable-anti-Virus-scans-log4shell.html
author: Nasreddine Bencherchali (Nextron Systems)
date: 2022/08/08
modified: 2023/02/06
tags:
    - attack.defense_evasion
    - attack.execution
    - attack.t1218.005
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        - Image|endswith: '\mshta.exe'
        - OriginalFileName: 'MSHTA.EXE'
    selection_cli:
        CommandLine|contains:
            - 'http://'
            - 'https://'
            - 'ftp://'
    condition: all of selection_*
falsepositives:
    - Unknown
level: high
```

Yara:

```
rule MAL_Loader_IDAT_August_2023
{
    meta:
        description = "IDAT Loader August 2023"
        author = "Natalie Zargarov"
    strings:
        $trait_0 = {C6 A5 79 EA F4 B4 07 9A}
        $trait_1 = {3D ED C0 D3}
        $trait_2 = {C6 45 FC 4D C6 45 FD 5A}
        $trait_3 = {68 77 94 91 2C 8B 45 ?? 50 E8}
    condition:
        2 of ($trait_*)
}
```

```
rule MAL_Loader_IDAT_Shellcode_Dec_2023
{
     meta:
        author = "Thomas Elkins - Rapid7"
        description = "Yara detects in memory IDAT Loader shellcode"
        date = "20-12-2023"
    strings:
        $stage1_32_1 = { 8B D1 8D 04 09 D1 EA 33 D0 8D 04 09 56 81 E2 55 55 55 55 33 D0 8B F2 8B C2 C1 E0 02
C1 EE 02 33 } // function from IDAT API Hashing Routine
        $stage1_32_2 = { 8A 44 0D 08 30 04 32 8D 41 01 83 E9 03 42 F7 D9 1B C9 23 C8 3B D7 72 E8 } // XOR
encrpytion routine for creation of encrypted temp file
        $stage1_64_1 = { 8B 44 24 08 25 55 55 55 55 D1 E0 8B 4C 24 08 D1 E9 81 E1 55 55 55 55 0B C1 89 44 24
08 } // function from IDAT API Hashing Routine
        $stage1_64_2 = { 8B 04 24 8B 4C 24 04 0F B6 4C 0C 08 48 8B 54 24 20 0F B6 04 02 33 C1 8B 0C 24 48 8B
54 24 20 88 } // XOR encryption for creation of encrypted temp file
        $stage2_1 = { FF 57 0C 33 D2 6A 1A 59 F7 F1 66 0F BE 44 15 DC 66 89 04 73 46 3B 75 FC 72 E6 } //
Function turns computer name into UpperCase only characters using srand function
        $stage2_2 = { 8B 00 33 04 8A 8B 4D E8 89 01 8B 55 E4 83 EA 01 39 55 F4 75 } // decryption loop for
final payload
    condition:
        2 of ($stage1_32_*) or 2 of ($stage1_64_*) or 2 of ($stage2_*)
}
```

```
rule Malicious_LNK
{
    meta:
        author = "CRIL"
        description = "Yara Rule to Identify Malicious LNK Files"
    strings:
        $str1 = "C:\\Windows /m win.ini /c" wide ascii
        $str2 = "C:\\Windows\\System32\\forfiles.exe" wide ascii
        $str3 = "powershell . mshta http" wide ascii
    condition:
        (uint32(0) == 0x0000004C) and all of ($str*)
}
```

3.1.5. Indicators of compromise

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	SHA256	6cede3165d85ab681491f4ff7f2362e6f4d332b2c385037a2390bcea423ab70f	Video HD (1080p).lnk
TLP:CLEAR	SHA256	7c78c287bbd93eaa79a792d5be6a2ef1522ff377a1fcd8daaebf152df5f174b7	matodown
TLP:CLEAR	SHA256	97db294fe0daf6c8dd581ca8f7eacd573ff00416d00839fad252cfb0b127e462	K1.zip
TLP:CLEAR	SHA256	372b14fce2eb35b264f6d4aeef7987da56d951d3a09ef866cf55ed72763caa12	Register.dll
TLP:CLEAR	SHA256	24d7ac3a5e97c764b1607b45e04545a311b3155887bf0a79dd6b79adad042e90	babyface.eps
TLP:CLEAR	SHA256	1da4ed3380f7477e728f6881129a20e33efcaa21191043eda902cf923332f924	hydrogeology.wmv
TLP:CLEAR	SHA256	d6dd7a4f46f2cfde9c4eb9463b79d5ff90fc690da14672ba1da39708ee1b9b50	rtl120.bpl
TLP:CLEAR	SHA256	7d0f90081a1b3500d724731a5c2f1bf120267a4803a59e59c734bcaff291220b	vcl120.bpl
TLP:CLEAR	SHA256	2f4f9fae763b5c99421a845449240b305ecdc288804268e2a411db2cce8035c3	K2.zip
TLP:CLEAR	SHA256	8aed681ad8d660257c10d2f0e85ae673184055a341901643f27afc38e5ef8473	jdekl.exe (RttHlp.exe)
TLP:CLEAR	URL	hxxps://streamvideoz[.]b-cdn[.]com/Download-Video_HD.html	Initial download
TLP:CLEAR	URL	hxxps://matodown[.]b-cdn.net/matodown	HTA file masquerading as a secret OpenPGP key download
TLP:CLEAR	URL	hxxps://vidstreemz[.]b-cdn.net/matodown	HTA file masquerading as a secret OpenPGP key download
TLP:CLEAR	URL	hxxps://mato2[.]b-cdn.net/matodown	HTA file masquerading as a secret OpenPGP key download
TLP:CLEAR	URL	hxxps://matodown[.]b-cdn[.]com/K1.zip	Second stage download
TLP:CLEAR	URL	hxxps://matodown[.]b-cdn[.]com/K2.zip	Second stage download
TLP:CLEAR	SHA256	4a3bbdb727e0e8fc2b41d5ebb8f7887defd468af19ac76e94b7f452e668555cd	08 CITACION DEMANDA.zip
TLP:CLEAR	SHA256	8aed681ad8d660257c10d2f0e85ae673184055a341901643f27afc38e5ef8473	08 CITACION DEMANDA.exe (RttHlp.exe)
TLP:CLEAR	SHA256	1dd7ae853911217095d2254337bedecee7267eea1ac9d0840eaf13506f40c9ab	vcl120.bpl
TLP:CLEAR	SHA256	0f6b87db9f0ae16d439b92514b3a63ae294ab5232901bbd8d87f14be47f7a67c	dreamland.m4a
TLP:CLEAR	SHA256	bb83ecbdd3c3dd6ec0a63b4c0cb480edb748165ed3a4a8720cb6605ac7173a6c	cutcherry.vcf
TLP:CLEAR	SHA256	c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2	Crowdstrike-hotfix.zip
TLP:CLEAR	SHA256	2bdf023c439010ce0a786ec75d943a80a8f01363712bbf69afc29d3e2b5306ed	vclx120.bpl
TLP:CLEAR	SHA256	4f450abaa4daf72d974a830b16f91deed77ba62412804dca41a6d42a7d8b6fd0	instrucciones.txt

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	SHA256	52019f47f96ca868fa4e747c3b99cba1b7aa57317bf8ebf9fcbf09aa576fe006	maddisAsm_.bpl
TLP:CLEAR	SHA256	835f1141ece59c36b18e76927572d229136aeb12eff44cb4ba98d7808257c299	madexcept_.bpl
TLP:CLEAR	SHA256	931308cfe733376e19d6cd2401e27f8b2945cec0b9c696aebe7029ea76d45bf6	maidenhair.cfg
TLP:CLEAR	SHA256	b1fcb0339b9ef4860bb1ed1e5ba0e148321be64696af64f3b1643d1311028cb3	rtl120.bpl
TLP:CLEAR	SHA256	b6f321a48812dc922b26953020c9a60949ec429a921033cfaf1e9f7d088ee628	vcl120.bpl
TLP:CLEAR	SHA256	be074196291ccf74b3c4c8bd292f92da99ec37a25dc8af651bd0ba3f0d020349	battuta.flv
TLP:CLEAR	SHA256	d6d5ff8e9dc6d2b195a6715280c2f1ba471048a7ce68d256040672b801fda0ea	madBasic_.bpl
TLP:CLEAR	SHA256	58e2b766dec37cc5fcfb63bc16d69627cd87e7e46f0b9f48899889479f12611e	Malicious LNK
TLP:CLEAR	SHA256	268a0de2468726a106fd92563a846e764f2ba313e37b5fc0cf76171b0a363f6f	Malicious LNK
TLP:CLEAR	SHA256	aceee450c55d61671c2d3d154b5f77e7f99688b6da8a8f3256a4bae2cdb76a4c	Malicious LNK
TLP:CLEAR	SHA256	2460e7590e09af09ced6f75c001a9066c18629d956edbe8041f08cd21b7528b2	Malicious LNK
TLP:CLEAR	SHA256	4eccb7813cee8c8039424aebf69f4269d4a6c2c72d81a001254bcdce80034555	Malicious LNK
TLP:CLEAR	SHA256	6481462f15ad4213f83a3d28304f14496bae1feb8580056959a657d0ee8981db	Malicious LNK
TLP:CLEAR	SHA256	7ee31fa89e9e68f20004bdc31f8f05a95861b6c678bfa3b57f09fdfad9ef5290	Malicious LNK
TLP:CLEAR	SHA256	81e89754ae2324c684fce71acafc30f8085870be947e7a76971b4fec1b24b5d1	Malicious LNK
TLP:CLEAR	SHA256	473abb2c272295473e5556ec7dec06f2018c0a67f208d8ab33de1fb6d40895f5	Malicious LNK
TLP:CLEAR	URL	hxxps://lajollaautorepairs[.]com/cart/ionama	Malicious HTA file download
TLP:CLEAR	URL	hxxps://lajollaautorepairs[.]com/ext/paola	Malicious HTA file download
TLP:CLEAR	URL	hxxps://offshorenergytoday[.]com/shop/gklakdgasd	Malicious HTA file download
TLP:CLEAR	URL	hxxp://172.233.43.[]49/testone	Malicious HTA file download
TLP:CLEAR	URL	hxxps://21centuryart[.]com/arc/msncjsudh	Malicious HTA file download
TLP:CLEAR	URL	hxxps://offshorenergytoday[.]com/mod/mvnashd	Malicious HTA file download
TLP:CLEAR	URL	hxxps://21centuryart[.]com/au/okasjhdd	Malicious HTA file download
TLP:CLEAR	IP	62.133.61[.]26	WebDAV sharing
TLP:CLEAR	IP	62.133.61[.]43	WebDAV sharing
TLP:CLEAR	IP	5.42.107[.]78	WebDAV sharing
TLP:CLEAR	Domain	scratchedcards[.]com	Malicious HTA file download
TLP:CLEAR	Domain	proffyrobharborye[.]xyz	Malicious HTA file download
TLP:CLEAR	Domain	answerrsdo[.]shop	Malicious HTA file download
TLP:CLEAR	SHA256	e15b200048fdddaedb24a84e99d6d7b950be020692c02b46902bf5af8fb50949	DR_Mod_180_2023.pdf
TLP:CLEAR	SHA256	547b6e08b0142b4f8d024bac78eb1ff399198a8d8505ce365b352e181fc4a544	DR_Mod_200_2023.PDF.lnk

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	SHA256	bd823f525c128149d70f633e524a06a0c5dc1ca14dd56ca7d2a8404e5a573078	ES_Mod_180_2023.PDF.url
TLP:CLEAR	SHA256	bc6933a8fc324b907e6cf3ded3f76adc27a6ad2445b4f5db1723ac3ec86ed10d	package_full.pdf.lnk
TLP:CLEAR	SHA256	59d2c2ca389ab1ba1fefa4a06b14ae18a8f5b70644158d5ec4fb7a7eac4c0a08	DIALER.EXE
TLP:CLEAR	SHA256	8568226767ac2748eccc7b9832fac33e8aa6bfdc03eafa6a34fb5d81e5992497	DIALER.EXE
TLP:CLEAR	SHA256	4043aa37b5ba577dd99f6ca35c644246094f4f579415652895e6750fb9823bd9	DIALER.EXE
TLP:CLEAR	SHA256	0604e7f0b4f7790053991c33359ad427c9bf74c62bec3e2d16984956d0fb9c19	DIALER.EXE
TLP:CLEAR	SHA256	8c6d355a987bb09307e0af6ac8c3373c1c4cbfbceeeb1159a96a75f19230ede6	flutter_windows.dll
TLP:CLEAR	SHA256	de6960d51247844587a21cc0685276f966747e324eb444e6e975b0791556f34f	IDMan.exe
TLP:CLEAR	SHA256	6c779e427b8d861896eacdeb812f9f388ebd43f587c84a243c7dab9ef65d151c	docpad.exe
TLP:CLEAR	SHA256	08c75c6a9582d49ea3fe780509b6f0c9371cfcd0be130bc561fae658b055a671	Invoice.pdf.lnk
TLP:CLEAR	SHA256	abc54ff9f6823359071d755b151233c08bc2ed1996148ac61cfb99c7e8392bfe	DIALER.EXE
TLP:CLEAR	SHA256	643dde3f461907a94f145b3cd8fe37dbad63aec85a4e5ed759fe843b9214a8d2	mr_0x0003B03B43F6EE12.exe

4. Vulnerability management, a pillar of security: an example with Estate ransomware

Monitoring and managing vulnerabilities affecting an organisation's information system is a daily challenge for security teams, with over fifty new vulnerabilities published every day.

Some of these newly disclosed vulnerabilities may already be exploited, requiring a rapid and appropriate response to mitigate the risk to the organisation's infrastructure. This risk is exacerbated by the disclosure of open source proofs of concept (PoCs). While these PoCs make it easier to understand a vulnerability and adjust detection strategies and workarounds, they can also be exploited by malicious actors.

It is important to prioritise these vulnerabilities as part of a patch management policy. However, it is also important not to overlook vulnerabilities with a low CVSS score or those for which there is not yet a PoC or known exploitation. Delays in patch deployment can provide opportunities for attackers, underlining the need for a proactive and rigorous approach to security risk management.

4.1. CVE-2023-27532

On 7 March 2023, *Veeam* published a security advisory regarding the CVE-2023-27532 vulnerability affecting the **Veeam Backup & Replication** and **Veeam Cloud Connect** products. This vulnerability allows an unauthenticated attacker to **obtain credentials**, by sending specially crafted requests to port 9401 of the vulnerable process.

In April 2023, researchers from *WithSecure*, revealed that the cybercriminal group FIN7 was targeting backup servers using *Veeam* solutions affected by this vulnerability. The aim of these attacks was to compromise backup servers in order to **delete sensitive data** or **disrupt backup operations**.

Following the disclosure of the vulnerability, proofs of concept were quickly released, which simplified and accelerated its exploitation, considerably increasing its danger.

More than a year later, CVE-2023-27532 is still being exploited by attackers, including the Estate Ransomware group. According to researchers at *Groupe-IB*, the operators of this new ransomware exploited this vulnerability in April 2024 to steal **valid credentials** and **move laterally** into the compromised system.

4.2. Estate Ransomware

Estate Ransomware was first observed in April 2024. Several victims have been identified in **France**, the **United Arab Emirates**, **Hong Kong**, **Malaysia** and the **United States of America**, although the areas affected are not known.

4.2.1. Diamond Model

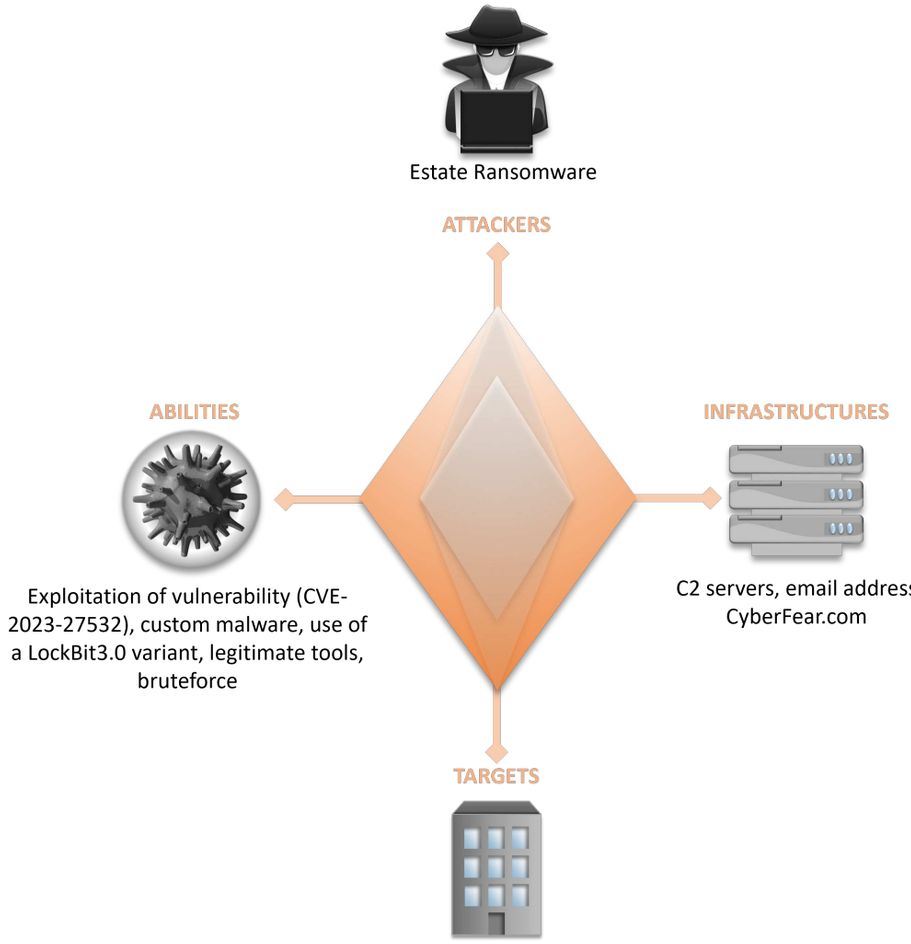

Figure 6. Diamond Model.

4.2.2. Attack chain

The **first manifestation of intrusion** occurred in April 2024 when the threat actor used the **SSL VPN service of a *FortiGate*** firewall to access the compromised system. Prior to the ransomware attack, **brute force attempts** via VPN were observed using a dormant account, **'Acc1'**. A few days later, a successful VPN connection using this account was linked to the IP address 149.28.106[.]252.

In April 2024, several VPN connections using 'Acc1' were observed from IP addresses in the US (149.28.106[.]252, 149.28.99[.]61 and 45.76.232[.]205). Shortly afterwards, RDP connections were established from the firewall to the compromised server. The IP addresses share the same autonomous system: AS-CHOOPA. The attackers probably selected these addresses to bypass security devices, due to their geolocation and the mutualisation of hosted services, which can lead to legitimate services being blocked.

Figure 7. Virus Total.

Figure 8. Virus Total.

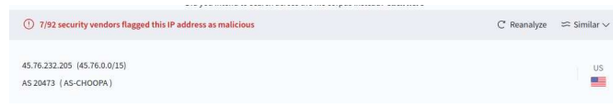

Figure 9. Virus Total.

During a remote session, the Estate ransomware operators deployed a persistent backdoor named "svchost.exe" and configured a scheduled task for its daily execution. By using the name of a legitimate *Windows* process, they sought to remain discreet and evade protection tools. After installing this backdoor, the attackers disconnected from the VPN and no further connections were observed.

This malware allows the attacker to establish **outward communication** with the IP 77.238.245[.]11:30001. The use of port 30001 is not common. It is a Transmission Control Protocol (TCP) port that has already been identified by security researchers during the deployment of Trojan horses. In the case of Estate Ransomware, the svchost.exe file establishes a tunnel using the HTTP protocol to connect to the C2 server in order to **remotely execute commands** on the compromised server.

To date, port 30001 is no longer open, as Estate operators appear to have dismantled this infrastructure.

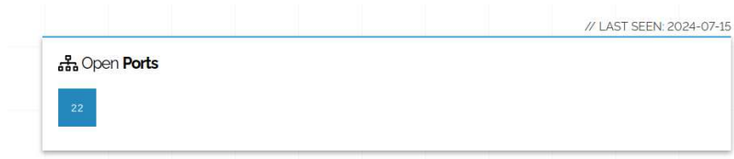

Figure 10. Source: Shodan.

The Dutch IP 77.238.245[.]11 belongs to a Russian host and is used by **several malicious groups**. It has been identified in **Banking Trojan** deployment campaigns. Attackers favour shared **IP** addresses for strategic and technical reasons, as it is difficult to block them without affecting **legitimate** sites sharing the same address. This allows them to carry out their malicious activities without being quickly **detected** or **blocked**.

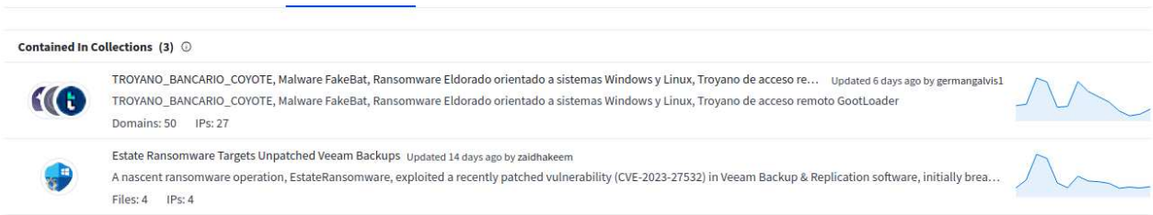

Figure 11. Source: VirusTotal.

The following day, the attacker accessed a file server via RDP and carried out various malicious activities, mainly focusing on exfiltrating credentials and exploiting vulnerabilities in Veeam Backup & Replication. According to Groupe-IB, the group abused a proof of concept published by Horizon3 and sfewer-R7 on GitHub for CVE-2023-27532 vulnerability, which has been available for over a year.

The malicious actor used SoftPerfect Netscan and password recovery tools from Nirsoft to scan the network and harvest information and credentials. Additional information was extracted from the backup server via the 'VeeamBkp' account, enabling it to be lateralised to the Active Directory (AD) server via RDP.

From the AD server, AdFind was downloaded and executed to enumerate users in the domain. Once enough information had been gathered, the attacker moved to other servers and workstations using compromised domain accounts.

The ransomware was deployed using three binaries: DC.exe, LB3.exe and PsExec.exe. On each host, Windows Defender was disabled with Defender Control (DC.exe), a tool widely used in attacks. Next, PsExec was used to connect to the host and execute the ransomware file LB3.exe, followed by the creation of the first ransom note. To avoid detection and hamper investigations, the ransomware erased Windows event logs on all compromised systems.

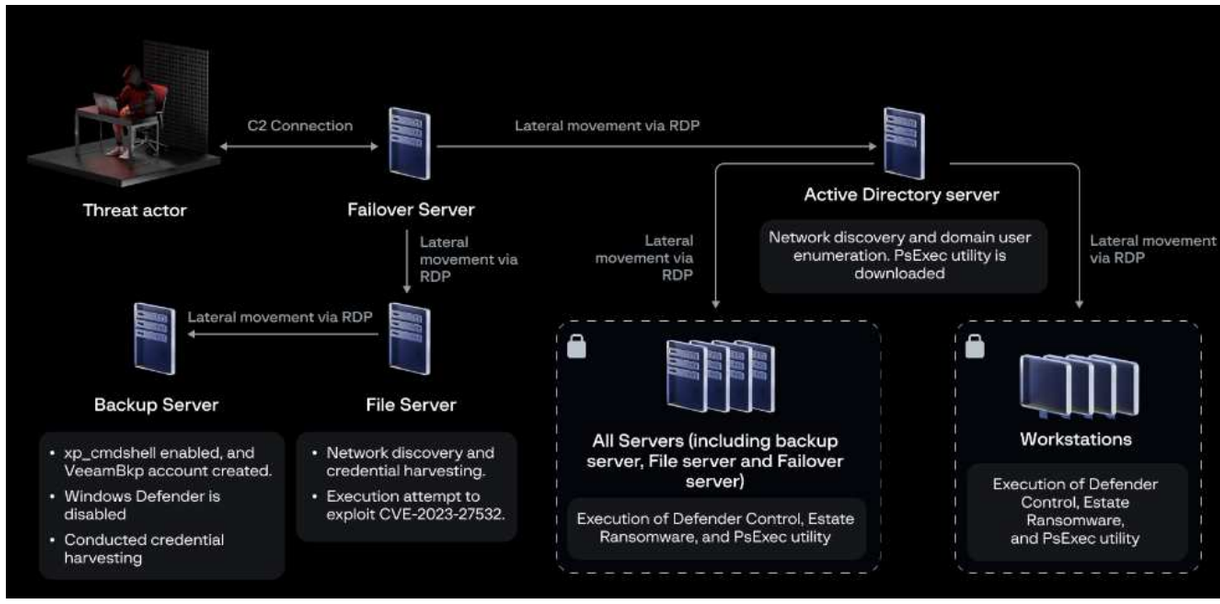

Figure 12. Killchain. Source: Groupe-IB.

This ransomware uses the *CyberFear* messaging service to communicate with its victims, encouraging them to use a ProtonMail address. This service, which is reputed to be secure, end-to-end encrypted and log-free, with offshore servers, is also used by other ransomware groups such as Worry.

In the Estate ransomware attack, the only custom tool was the "Svchost.exe" backdoor, with the rest of the attack relying on known, publicly available tools. The encryption executable was a variant of the LockBit3.0 ransomware whose source code was leaked in 2023. This shows that the group is currently not very sophisticated and is using common means. However, given the novelty of this ransomware, it is likely that the attacks will be personalised and improved over time.

4.2.3. Mitre Att&ck

INITIAL ACCESS

T1078 Valid Accounts. T1133 External Remote Services.

EXECUTION

T1204.002 User Execution: Malicious File. T1569.002 System Services: Service Execution.

PERSISTENCE

T1053.005 Scheduled Task/Job: Scheduled Task. T1136.001 Create Account: Local Account. T1505.001 Server Software Component: SQL Stored Procedures.

DEFENSE EVASION

T1070.001 Indicator Removal: Clear Windows Event Logs. T1070.004 Indicator Removal: File Deletion. T1562.001 Impair Defenses: Disable or Modify Tools.

CREDENTIAL ACCESS

T1555 Credentials from Password Stores.

DISCOVERY

T1018 Remote System Discovery. T1087.002 Account Discovery: Domain Account.

LATERAL MOVEMENT

T1021.001 Remote Services: Remote Desktop Protocol.

COMMAND & CONTROL

T1571 Non-Standard Port. T1071.001 Application Layer Protocol: Web Protocols.

IMPACT

T1486 Data Encrypted for Impact.

Figure 13. Kill Chain. Source : Groupe-IB.

4.2.4. IoC

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	IP	149.28.106[.]252	Bruteforce
TLP:CLEAR	IP	149.28.99[.]61	Bruteforce
TLP:CLEAR	IP	45.76.232[.]205	Bruteforce
TLP:CLEAR	IP	77.238.245[.]11:30001	C2 from Svchost.exe
TLP:CLEAR	SHA1	CB704D2E8DF80FD3500A5B817966DC262D80DDB8	CD.exe
TLP:CLEAR	SHA1	2C56E9BEEA9F0801E0110A7DC5549B4FA0661362	DC.ini
TLP:CLEAR	SHA1	5E460A517F0579B831B09EC99EF158AC0DD3D4FA	Svchost.exe
TLP:CLEAR	SHA1	107EC3A7ED7AD908774AD18E3E03D4B999D4690C	LB3.exe
TLP:CLEAR	File	netscan.exe	
TLP:CLEAR	File	veeam-creds-main	
TLP:CLEAR	File	CVE-2023-27532.exe	
TLP:CLEAR	File	VeeamHax	
TLP:CLEAR	File	BulletsPassView64.exe	
TLP:CLEAR	File	netpass64.exe	
TLP:CLEAR	File	PasswordFox64.exe	
TLP:CLEAR	File	ChromePass.exe	
TLP:CLEAR	File	WirelessKeyView64.exe	
TLP:CLEAR	File	mspass.exe	
TLP:CLEAR	File	VNCPassView.exe	
TLP:CLEAR	File	WebBrowserPassView.exe	
TLP:CLEAR	File	mailpv.exe	
TLP:CLEAR	File	RouterPassView.exe	
TLP:CLEAR	File	PstPassword.exe	
TLP:CLEAR	File	OperaPassView.exe	
TLP:CLEAR	File	Dialupass.exe	
TLP:CLEAR	File	BulletsPassView64.exe	
TLP:CLEAR	File	ExtPassword.exe	
TLP:CLEAR	File	pspv.exe	
TLP:CLEAR	File	iepv.exe	
TLP:CLEAR	File	SniffPass64.exe	
TLP:CLEAR	File	rdpv.exe	

5. Sources

Distribution of HijackLoader with IObit's Driver Booster executable

- https://lab52.io/blog/dll-side-loading-through-iobit-against-colombia/
- https://www.kroll.com/en/insights/publications/cyber/idatloader-distribution
- https://www.crowdstrike.com/blog/likely-ecrime-actor-capitalizing-on-falcon-sensor-issues/
- https://cyble.com/blog/increase-in-the-exploitation-of-microsoft-smartscreen-vulnerability-cve-2024-21412/
- https://www.fortinet.com/blog/threat-research/exploiting-cve-2024-21412-stealer-campaign-unleashed

Vulnerability management, a pillar of security: an example with Estate ransomware

- https://www.group-ib.com/blog/estate-ransomware/
- https://www.mycert.org.my/portal/advisory?id=MA-1076.052024
- https://www.pcrisk.com/removal-guides/25608-worry-ransomware