aDvens

Security for the greater good

May Cyber Threat Intelligence monthly report

2024-06-06 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 38 rue des Jeuneurs - 75002 Paris

Table of content

1. Executive summary

This month, aDvens' CERT presents three noteworthy vulnerabilities, in addition to those already published.

Through two articles, the CERT's analysts discuss:

- the LATRODECTUS malware with similarities to IcedID.
- the KINSING cryptominer, which can be used to gain persistent access to compromised machines.

2. Vulnerabilities

This month, the CERT aDvens highlights **three** 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. CVE-2024-29212

On 7 May 2024, Veeam issued a security bulletin regarding a critical vulnerability in Veeam Service Provider Console and released appropriate patches. These were examined further and the advisory was updated on 28 May 2024.

Insecure deserialisation in the Veeam Service Provider Console (VSPC) server allows an authenticated attacker, by sending specially crafted requests, to execute arbitrary code.

2.1.1. Type of vulnerability

- CWE-502: Deserialization of Untrusted Data

2.1.2. Risks

- Remote code execution

2.1.3. Criticity (base score CVSS v3.1)

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

2.1.4. Impacted Products

- Veeam Service Provider Console versions 4, 5, 6, 7 and 8

2.1.5. Recommandations

- Update Service Provider Console version 7.x to version 7.0.0.19551 or later.
- Update Service Provider Console version 8.x to version 8.0.0.19552 or later.
- Versions 4, 5 and 6 have reached End of Life and are therefore unsupported.
- Additional information is available in Veeam's advisory.

2.1.6. Proof of concept

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

2.2. CVE-2024-26289

On 22 May 2024, the European Union Cybersecurity Agency (ENISA) published an alert concerning a critical vulnerability affecting several versions of the PMB software. PMB is an integrated library management system, with a free version. This tool is widely used in many public libraries, research libraries, schools and documentation centres in companies or associations.

Insecure data deserialisation in PMB allows an unauthenticated attacker, by sending specifically crafted requests, to execute arbitrary code.

2.2.1. Type of vulnerability

- CWE-502: Deserialization of Untrusted Data

2.2.2. Risks

- Remote code execution

2.2.3. Criticity (base score CVSS v3.1)

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

- PMB :
  - Versions from 7.3.1 before 7.3.18,
  - Versions from 7.4.1 before 7.4.9,
  - Versions from 7.5.1 before 7.5.6-2

2.2.5. Recommandations

- Update PMB to version 7.3.18, 7.4.9, 7.5.6-2, 7.5.7 or later.
- Additional information is available in ENISA's advisory.

2.2.6. Proof of concept

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

2.3. CVE-2024-25641

On 14 May 2024, Cacti published a security bulletin to address the CVE-2024-25641 vulnerability. This advisory also contained a proof of concept.

A handling of special characters flaw in the */lib/import.php* library in Cacti's *Package Import* component allows an authenticated attacker with *Import Templates* permission to execute arbitrary PHP code on the web server.

2.3.1. Type of vulnerability

- CWE-20: Improper Input Validation

2.3.2. Risks

- Remote code execution

2.3.3. Criticity (base score CVSS v3.1)

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

2.3.4. Impacted Products

- Cacti version 1.2.26 and prior

2.3.5. Recommandations

- Update Cacti to version 1.2.27 or later.
- Additional information is available in Cacti's bulletin.

2.3.6. Proof of concept

A proof of concept is available in open source.

3. LATRODECTUS, the new IcedID ?

3.1. Context

LATRODECTUS is a malware first discovered in **2023** by *Walmart* researchers while investigating an IcedID campaign.

They noticed that the hash (imphash) of the sample studied showed an **overlap** with another executable. This group uses similar **techniques** and **tools** to those used in historical IcedID campaigns, suggesting a **connection** between these operators.

LATRODECTUS stands out for its ability to **evolve** and **adapt** its methods, making it a **persistent** and **sophisticated** threat.

The malware acts as a **loader**, installing additional payloads. It also offers **standard features** after the initial compromise, such as process discovery, file listing and deletion of running files. This type of malware is often used to deploy **ransomware**. In the context of LATRODECTUS campaigns, this has not yet been observed.

The **victimology** is currently **not known**, LATRODECTUS operations have been observed on **various organisations** without them being specified.

Operators mainly use **phishing** e-mails to distribute LATRODECTUS. These campaigns are **designed** to circumvent traditional security measures, using techniques such as identity theft and domains resembling legitimate entities to fool victims. The e-mails may contain **Word** or **Excel** documents with malicious macros which, once activated, install malware on the victim's computer.

3.2. Attribution

According to *ProofPoint*, this malware was first observed when it was distributed by TA577, a group of malicious actors already known for its extensive distribution of Qbot before the malware was disrupted in 2023. TA577 used LATRODECTUS in at least three campaigns in November 2023 before switching back to Pikabot. Since mid-January 2024, researchers have observed it being used almost exclusively by TA578 in threat e-mail campaigns. This actor typically uses contact forms to initiate a conversation with a target. In a campaign observed on 15 December 2023, *Proofpoint* found that TA578 distributed LATRODECTUS via a DanaBot infection.

3.3. Latest campaigns

In early March 2024, researchers at *Elastic Security Labs* observed an **increase** in e-mail campaigns distributing LATRODECTUS. The malware is distributed via phishing campaigns using *Microsoft* and *Cloudflare* themes to appear legitimate. These e-mails contained **PDF attachments** or embedded **URLs**, leading to a fake *Cloudflare* captcha. Once the captcha is resolved, a **JavaScript** is downloaded. This oversized JavaScript file uses WMI's ability to invoke msiexec.exe and install a remotely-hosted MSI file on a WEBDAV share to **deploy the DLL** TRUFOS.DLL corresponding to LATRODECTUS.

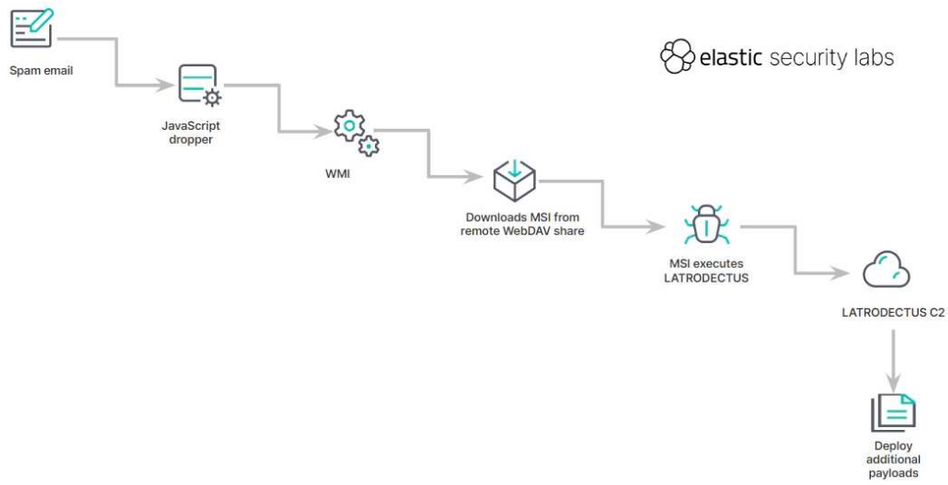
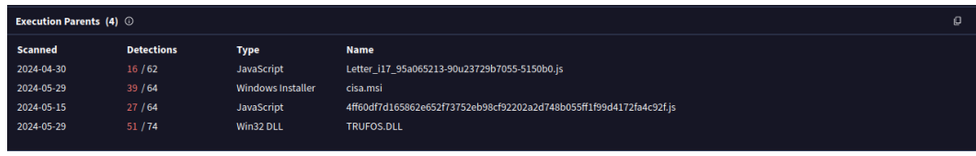


Figure 1. LATRODECTUS kill chain

Researching the malicious file analysed by *Elastic Security Labs*, it's possible to trace this campaign back to March 2024.



Execution Parents (4)

Scanned	Detections	Type	Name
2024-04-30	16 / 62	JavaScript	Letter_i17_95a065213-90u23729b7055-5150b0.js
2024-05-29	39 / 64	Windows Installer	cisa.msi
2024-05-15	27 / 64	JavaScript	4ff60df7d165862e652f73752eb98cf92202a2d748b055ff1f99d4172fa4c92f.js
2024-05-29	51 / 74	Win32 DLL	TRUFOS.DLL

Figure 2. VirusTotal TRUFOS.DLL

The file TRUFOS.DLL was executed by the parent file Letter_i17_95a065213-90u23729b7055-5150b0.js.

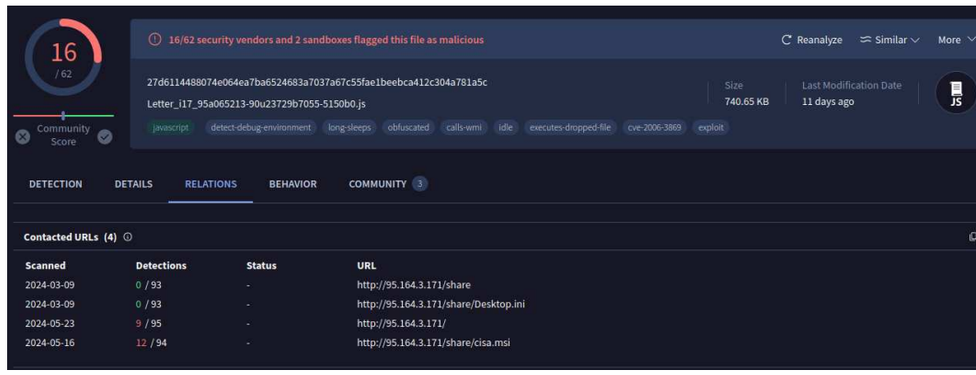
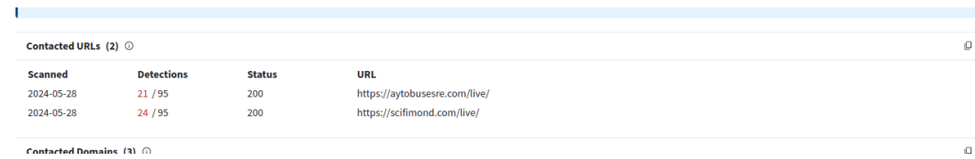


Figure 3. VirusTotal Letter_i17_95a065213-90u23729b7055-5150b0.js

This malicious file, associated with LATRODECTUS, is also linked to C2s hxxps://scifimond[.]com/live/ and hxxps://aytobusesre[.]com/live/.



Contacted URLs (2)

Scanned	Detections	Status	URL
2024-05-28	21 / 95	200	https://aytobusesre.com/live/
2024-05-28	24 / 95	200	https://scifimond.com/live/

Contacted Domains (3)

Figure 4. VirusTotal TRUFOS.DLL

3.4. Infrastructure, techniques, tactics and procedures

Infrastructure

The infrastructure of the LATRODECTUS operators is **similar** for each campaign. The group uses **CloudFlare domains**, created to be used as C2 servers. The names seem to be **randomly generated**, with different extensions. However, there's one thing these C2s have in common: the **directory *"live"*** seems to be used in every campaign.

These domains are not only used for a single campaign, but also for **different periods**. For example, the hxxps://scifimond[.]com/live/ domain was first observed on March 4, 2024, and appears to be **still active** on May 28, 2024.

Initial Access

Phishing e-mails, either through malicious attachments or specifically crafted links, are used to deploy the malware. Initially, an oversized Javascript file containing random text is installed on the compromised machine.

Execution

The JavaScript dropper uses WMI to mount a WEBDAV share and calls msiexec to install a remote MSI file.

Once executed, it drops the LATRODECTUS DLL and launches rundll32 to load it via the Advanced Installer viewer.exe binary.

Defense Evasion

Rundll32 loads the LATRODECTUS DLL from AppData and starts injecting code. When not loaded from AppData, it deletes itself while still running, then restarts from the new path.

To avoid sandbox or virtual machines that may have a reduced number of active processes, checks are used to combine the number of running processes with the operating system product version.

LATRODECTUS uses the file information of a BitDefender component (TRUFOS.SYS), pretending to be it.

Persistence

Rundll32 will be used to create scheduled tasks, using Windows Component Object Model (COM), to establish persistence on the compromised system.

Collect

The malware uses a list of Shell commands to collect information from the compromised system:

```
&ipconfig=
&systeminfo=
&domain_trusts=
&domain_trusts_all=
&net_view_all_domain=
&net_view_all=
&net_group=
&wmic=
&net_config_ws=
&net_wmic_av=
&whoami_group=
```

Command and Control

LATRODECTUS communicates with command and control (C2) servers to download new payloads.

The malware encrypts its requests, encoded in Base64, using RC4 and a hard-coded password “12345”. The first POST request via HTTPS includes victim information and configuration details, registering the infected system.

3.5. IcedID et LATRODECTUS

3.5.1. Technical similarities

Both groups use **phishing e-mails** to reach their victims. These e-mails are often highly **sophisticated**, using social engineering techniques to appear legitimate and entice users to open attachments or click on malicious links. Documents attached to e-mails, such as Word and Excel files, contain malicious macros. Once activated, these macros download and run malware on the victim’s system.

3.5.2. Shared infrastructure and tools

The two groups appear to **share similar or even identical infrastructures**. This includes the servers used to control malware after it has been installed on infected systems. This shared infrastructure suggests either direct collaboration between the two groups, or common use of third-party criminal services.

Security researchers found **similarities in the code** of the malware used by LATRODECTUS and IcedID. These similarities may indicate that LATRODECTUS is using variants or modified versions of IcedID's tools, which is common in cybercrime circles where malicious code is often exchanged or sold between groups.

3.6. Conclusion

It is possible that LATRODECTUS is an **evolution** or **reorganisation of IcedID's' operations**. Cybercriminal groups regularly change their name and structure to evade investigation and enforcement. LATRODECTUS could therefore be a **continuation of activities** of IcedID under a new name and with a few modifications to improve their effectiveness and evade detection. However, it seems that IcedID's capabilities are, for now, more developed.

An operation, named *EndGame* and led by Europol, is currently underway to hinder services used by cybercriminals. Four malware programs, including IcedID, are involved. To date, four people have been arrested and over 100 servers have been taken offline.

3.7. Detection rule

```
rule Windows_Trojan_LATRODECTUS_841ff697 {
    meta:
        author = "Elastic Security"
        creation_date = "2024-03-13"
        last_modified = "2024-04-05"
        license = "Elastic License v2"
        os = "Windows"
        arch = "x86"
        threat_name = "Windows.Trojan.LATRODECTUS"
        reference_sample = "aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c"
    strings:
        $Str1 = { 48 83 EC 38 C6 44 24 20 73 C6 44 24 21 63 C6 44 24 22 75 C6 44 24 23 62 C6 44 24 24 }
        $crc32_loadlibrary = { 48 89 44 24 40 EB 02 EB 90 48 8B 4C 24 20 E8 ?? ?? FF FF 48 8B 44 24 40 48 81
C4 E8 02 00 00 C3 }
        $delete_self = { 44 24 68 BA 03 00 00 00 48 8B 4C 24 48 FF 15 ED D1 00 00 85 C0 75 14 48 8B 4C 24 50
E8 ?? ?? 00 00 B8 FF FF FF FF E9 A6 00 }
        $Str4 = { 89 44 24 44 EB 1F C7 44 24 20 00 00 00 00 45 33 C9 45 33 C0 33 D2 48 8B 4C 24 48 FF 15 7E
BB 00 00 89 44 24 44 83 7C 24 44 00 75 02 EB 11 48 8B 44 24 48 EB 0C 33 C0 85 C0 0F 85 10 FE FF FF 33 }
        $handler_check = { 83 BC 24 D8 01 00 00 12 74 36 83 BC 24 D8 01 00 00 0E 74 2C 83 BC 24 D8 01 00 00
0C 74 22 83 BC 24 D8 01 00 00 0D 74 18 83 BC 24 D8 01 00 00 0F 74 0E 83 BC 24 D8 01 00 00 04 0F 85 44 02 00
00 }
        $hwid_calc = { 48 89 4C 24 08 48 8B 44 24 08 69 00 0D 66 19 00 48 8B 4C 24 08 89 01 48 8B 44 24 08
8B 00 C3 }
        $string_decrypt = { 89 44 24 ?? 48 8B 44 24 ?? 0F B7 40 ?? 8B 4C 24 ?? 33 C8 8B C1 66 89 44 24 ?? 48
8B 44 24 ?? 48 83 C0 ?? 48 89 44 24 ?? 33 C0 66 89 44 24 ?? EB ?? }
        $campaign_fnv = { 48 03 C8 48 8B C1 48 39 44 24 08 73 1E 48 8B 44 24 08 0F BE 00 8B 0C 24 33 C8 8B
C1 89 04 24 69 04 24 93 01 00 01 89 04 24 EB BE }
    condition:
        2 of them
}
```

3.8. MITRE ATT&CK

RESOURCE DEVELOPMENT

T1583.001 Compromise Infrastructure: Domains T1587.001 Develop Capabilities: Malware

INITIAL ACCESS

T1566 Phishing T1566.001 Phishing: Spearphishing Attachment

EXECUTION

T1059.003 Command and Scripting Interpreter: Windows Command Shell T1047 Windows Management Instrumentation T1204 User Execution T1559.007 Command and Scripting Interpreter: JavaScript

PERSISTENCE

T1053.005 Scheduled Task/Job: Scheduled Task

PRIVILEGE ESCALATION

T1068 Exploitation for Privilege Escalation

DEFENSE EVASION

T1027 Obfuscated Filed or Information T1070.004 Indicator Removal: File Deletion T1036 Masquerading T1055 Process Injection T1218.007 System Binary Proxy Execution: Msiexec T1218.007 System Binary Proxy Execution: Rundll32

CREDENTIAL ACCESS

T1003 OS Credential Dumping

DISCOVERY

T1082 System Information Discovery

COLLECTION

T1005 Data from Local System

COMMAND AND CONTROL

T1105 Ingress Tool Transfer T1132 Data Encoding T1001 Data Obfuscation

EXFILTRATION

T1567 Exfiltration Over Web Service

Figure 5. TTPS LATRODECTUS

3.9. IOCs

TLP	TYPE	VALUE	COMMENT	DATE
TLP:CLEAR	SHA256	db03a34684feab7475862080f59d4d99b32c74d3a152a53b257fd1a443e8ee77	LNK Payload	27 November 2023
TLP:CLEAR	SHA256	e99f3517a36a9f7a55335699cfb4d84d08b042d47146119156f7f3bab580b4d7	DLL Payload	27 November 2023
TLP:CLEAR	URL	hxxps://mazdakrichest[.]com/live/	Latrodectus C2	27 November 2023
TLP:CLEAR	URL	hxxps://riverhasus[.]com/live/	Latrodectus C2	27 November 2023
TLP:CLEAR	SHA256	bb525dc6b7a7ebefd040e01fd48d7d4e178f8d9e5dec9033078ced4e9aa4e241	JavaScript Payload	28 November 2023
TLP:CLEAR	SHA256	b97e093f2e0bf6dec8392618722dd6b4411088fe752bedece910d11fffe0288a2	DLL Payload	28 November 2023
TLP:CLEAR	URL	hxxp://162[.]55[.]217[.]30/gRMS/0[.]6395541546258323[.]dat	JavaScript Payload	28 November 2023
TLP:CLEAR	URL	hxxp://157[.]90[.]166[.]88/O3ZIYNW/0[.]7797109211833805[.]dat	JavaScript Payload	28 November 2023
TLP:CLEAR	URL	hxxp://128[.]140[.]36[.]37/cQtDlo/0[.]43650426987684443[.]dat	JavaScript Payload	28 November 2023
TLP:CLEAR	URL	hxxps://peermangoz[.]me/live/	Latrodectus C2	28 November 2023
TLP:CLEAR	URL	hxxps://aprettopizza[.]world/live/	Latrodectus C2	28 November 2023
TLP:CLEAR	URL	hxxps://nimeklroboti[.]info/live/	Latrodectus C2	28 November 2023
TLP:CLEAR	URL	hxxps://frotneels[.]shop/live/	Latrodectus C2	28 November 2023
TLP:CLEAR	SHA256	f9c69e79e7799df31d6516df70148d7832b121d330beebe52cff6606f0724c62	JavaScript Payload	28 November 2023
TLP:CLEAR	SHA256	d9471b038c44619739176381815bfa9a13b5ff77021007a4ede9b146ed2e04ec	DLL Payload	24 November 2023
TLP:CLEAR	URL	hxxps://hukosafaris[.]com/elearning/f/q/daas-area/chief/index[.]php	JavaScript Payload	24 November 2023
TLP:CLEAR	SHA256	d98cd810d568f338f16c4637e8a9cb01ff69ee1967f4cfc004de3f283d61ba81	DLL Payload	14 December 2023
TLP:CLEAR	SHA256	47d66c576393a4256d94f5ed1e77adc28426dea027f7a23e2dbf41b93b87bd78	EXE Payload	14 December 2023
TLP:CLEAR	IP	77[.]91[.]73[.]187:443	DanaBot C2	14 December 2023
TLP:CLEAR	IP	74[.]119[.]193[.]200:443	DanaBot C2	14 December 2023
TLP:CLEAR	URL	hxxps://arsimonopa[.]com/live	Latrodectus C2	14 December 2023
TLP:CLEAR	URL	hxxps://lemonimonakio[.]com/live	Latrodectus C2	14 December 2023
TLP:CLEAR	SHA256	bb525dc6b7a7ebefd040e01fd48d7d4e178f8d9e5dec9033078ced4e9aa4e241	JavaScript Payload	1 February 2024
TLP:CLEAR	SHA256	5d881d14d2336273e531b1b3d6f2d907539fe8489cbe80533280c9c72efa2273	DLL Payload	1 February 2024
TLP:CLEAR	URL	hxxp://superior-coin[.]com/ga/index[.]php	JavaScript Payload	1 February 2024
TLP:CLEAR	URL	hxxp://superior-coin[.]com/ga/m/6[.]dll	JavaScript Payload	1 February 2024
TLP:CLEAR	URL	hxxps://fluraresto[.]me/live/	Latrodectus C2	1 February 2024
TLP:CLEAR	URL	hxxps://mastralakkot[.]live/live/	Latrodectus C2	1 February 2024
TLP:CLEAR	URL	hxxps://postolwepok[.]tech/live/	Latrodectus Update	1 February 2024
TLP:CLEAR	URL	hxxps://trasenanoyr[.]best/live/	Latrodectus Update	1 February 2024
TLP:CLEAR	SHA256	10c129e2310342a55df5fa88331f338452835790a379d5230ee8de7d5f28ea1a	JavaScript Payload	5 February 2024

TLP	TYPE	VALUE	COMMENT	DATE
TLP:CLEAR	SHA256	781c63cf4981fa6aff002188307b278fac9785ca66f0b6dfcf68adbe7512e491	MSI Payload	5 February 2024
TLP:CLEAR	SHA256	aa29a8af8d615b1dd9f52fd49d42563fbeafa35ff0ab1b4afc4cb2b2fa54a119	DLL Payload	5 February 2024
TLP:CLEAR	SHA256	0ac5030e2171914f43e0769cb10b602683ccc9da09369bcd4b80da6edb8be80e	JavaScript Payload	9 February 2024
TLP:CLEAR	SHA256	0e96cf6166b7cc279f99d6977ab0f45e9f47e827b8a24d6665ac4c29e18b5ce0	MSI Payload	9 February 2024
TLP:CLEAR	SHA256	77270e13d01b2318a3f27a9a477b8386f1a0ebc6d44a2c7e185cfbe55aac8017	DLL Payload	9 February 2024
TLP:CLEAR	URL	hxxps://miistoria[.]com/live	Latrodectus C2	9 February 2024
TLP:CLEAR	URL	hxxps://plwskoret[.]top/live	Latrodectus C2	9 February 2024
TLP:CLEAR	SHA256	e7ff6a7ac5bfb0bb29547d413591abc7628c7d5576a3b43f6d8e5d95769e553a	JavaScript Payload	13 February 2024
TLP:CLEAR	SHA256	dedbc21afc768d749405de535f9b415baaf96f7664ded55d54829a425fc61d7e	MSI Payload	13 February 2024
TLP:CLEAR	SHA256	378d220bc863a527c2bca204daba36f10358e058df49ef088f8b1045604d9d05	DLL Payload	13 February 2024
TLP:CLEAR	SHA256	edeacd49aff3cfea35d593e455f7caca35ac877ad6dc19054458d41021e0e13a	JavaScript Payload	20 February 2024
TLP:CLEAR	SHA256	9c27405cf926d36ed8e247c17e6743ac00912789efe0c530914d7495de1e21ec	MSI Payload	20 February 2024
TLP:CLEAR	SHA256	9a8847168fa869331faf08db71690f24e567c5cdf1f01cc5e2a8d08c93d282c9	DLL Payload	20 February 2024
TLP:CLEAR	URL	hxxp://178[.]23[.]190[.]199:80/share/gsm[.]msi	JavaScript WebDAV Payload	20 February 2024
TLP:CLEAR	URL	hxxps://sluitionsbad[.]tech/live/	Latrodectus C2	20 February 2024
TLP:CLEAR	URL	hxxps://grebiunti[.]top/live/	Latrodectus C2	20 February 2024
TLP:CLEAR	SHA256	856dfa74e0f3b5b7d6f79491a94560dbf3eacacc4a8d8a3238696fa38a4883ea	JavaScript Payload	23 February 2024
TLP:CLEAR	SHA256	88573297f17589963706d9da6ced7893eacbdc7d6bc43780e4c509b88ccd2aef	MSI Payload	23 February 2024
TLP:CLEAR	SHA256	97e08d1c7970c1c12284c4644e2321ce41e40cdaac941e451db4d334cb9c5492	DLL Payload	23 February 2024
TLP:CLEAR	URL	hxxp://5[.]252[.]21[.]207@80/share/escape[.]msi	JavaScript WebDAV Payload	23 February 2024
TLP:CLEAR	URL	hxxps://zumkoshapsret[.]com/live/	Latrodectus C2	23 February 2024
TLP:CLEAR	URL	hxxps://jertacco[.]com/live/	Latrodectus C2	23 February 2024
TLP:CLEAR	SHA256	60c4b6c230a40c80381ce283f64603cac08d3a69ceea91e257c17282f66ceddc	JavaScript Payload	27 February 2024
TLP:CLEAR	SHA256	88573297f17589963706d9da6ced7893eacbdc7d6bc43780e4c509b88ccd2aef	MSI Payload	27 February 2024
TLP:CLEAR	SHA256	97e08d1c7970c1c12284c4644e2321ce41e40cdaac941e451db4d334cb9c5492	DLL Payload	27 February 2024
TLP:CLEAR	URL	hxxp://5[.]252[.]21[.]207/share/escape[.]msi	JavaScript WebDAV	27 February 2024
TLP:CLEAR	SHA256	a189963ff252f547fddfc394c81f6e9d49eac403c32154eebe06f4cddb5a2a22	JavaScript Payload	4 March 2024
TLP:CLEAR	SHA256	aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c	DLL Payload	4 March 2024
TLP:CLEAR	URL	hxxp://95[.]164[.]3[.]171/share/cisa[.]msi	WebDAV Payload	4 March 2024
TLP:CLEAR	URL	hxxps://scifimond[.]com/live/	Latrodectus C2	4 March 2024

TLP	TYPE	VALUE	COMMENT	DATE
TLP:CLEAR	URL	hxxps://aytobusesre[.]com/live/	Latrodectus C2	4 March 2024
TLP:CLEAR	SHA256	4416b8c36cb9d7cc261ff6612e105463eb2ccd4681930ca8e277a6387cb98794	JavaScript Payload	7 March 2024
TLP:CLEAR	SHA256	aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c	DLL Payload	7 March 2024
TLP:CLEAR	URL	hxxps://popfealt[.]one/live/	Latrodectus Update	7 March 2024
TLP:CLEAR	URL	hxxps://ginzbargatey[.]tech/live/	Latrodectus Update	7 March 2024
TLP:CLEAR	URL	hxxps://minndarespo[.]icu/live/	Latrodectus Update	7 March 2024
TLP:CLEAR	SHA256	090f2c5abb85a7b115dc25ae070153e4e958ae4e1bc2310226c05cd3e9429446	JavaScript Payload	11 March 2024
TLP:CLEAR	SHA256	ee1e5b80a1d3d47c7703ea2b6b64ee96283ab3628ee4fa1fef6d35d1d9051e9f	MSI Payload	11 March 2024
TLP:CLEAR	SHA256	3b63ea8b6f9b2aa847faa11f6cd3eb281abd9b9cceedb570713c4d78a47de567	DLL Payload	11 March 2024
TLP:CLEAR	URL	hxxps://drifajizo[.]fun/live/	Latrodectus C2	11 March 2024
TLP:CLEAR	URL	hxxps://scifimond[.]com/live/	Latrodectus C2	11 March 2024
TLP:CLEAR	URL	hxxps://minndarespo[.]icu/live/	Latrodectus C2	11 March 2024
TLP:CLEAR	SHA256	6904d382bc045eb9a4899a403a8ba8a417d9ccb764f6e0b462bc0232d3b7e7ea	JavaScript Payload	18 March 2024
TLP:CLEAR	SHA256	71fb25cc4c05ce9dd94614ed781d85a50dccf69042521abc6782d48df85e6de9	DLL Payload	18 March 2024
TLP:CLEAR	URL	hxxp://sokingscrosshotel[.]com/share/upd[.]msi	WebDAV Payload	18 March 2024
TLP:CLEAR	URL	hxxps://titnovacrion[.]top/live/	Latrodectus C2	18 March 2024

4. Kinsing Malware

With the rise of the cloud, more and more systems are reachable to anyone, giving cyber-criminals access to a new set of systems, often badly protected. One of the more common but less looked at threats is that of cryptomining. This type of malware uses the system's ressources to try and gain cryptocurrency whilst also allowing the attacker to maintain a foot in the victim's system.

Kinsing, also known as h2Miner, is a threat that has been profiting of this for 5 years. This malware was discovered in January 2020 but its first activities were observed in December 2019. It is operated by a group with the same name. The group mainly targets the Cloud and Linux servers in order to deploy a *rootkit* as well as a cryptocurrency miner. 4 years after its discovery, the group continues to be successful in their campaigns by keeping an almost unchanged modus operandi.

4.1. The malware

Kinsing is a software coded in the Go language (Golang). It presents itself as an ELF file and is used as a Remote Access Trojan (RAT) to deploy a cryptominer. It has been used in multiple campaigns since 2019, mainly in opportunistic attacks. The cybercriminals behind this malware often obtain their initial access via vulnerabilities or misconfigurations in Cloud environments.

When Kinsing was first discovered in 2020, the malware's operators targeted misconfigured Docker APIs. Since then, their modus operandi has evolved to quickly integrate vulnerability exploitation scripts after the disclosure of proofs of concept. A (non-exhaustive) list of exploited vulnerabilities is available in the appendix.

Once the primary infection has been obtained, the attackers download the Kinsing malware, which installs itself and establishes persistence on the system. This malware also has a module, called Masscan, which helps it discover if it can lateralise itself. Subsequently, Kinsing communicates with C2 servers and installs a cryptominer: XMrig. The latter is an open-source miner that seeks to obtain Monero cryptocurrency. The associated process is often named *kdevtmpfsi*.

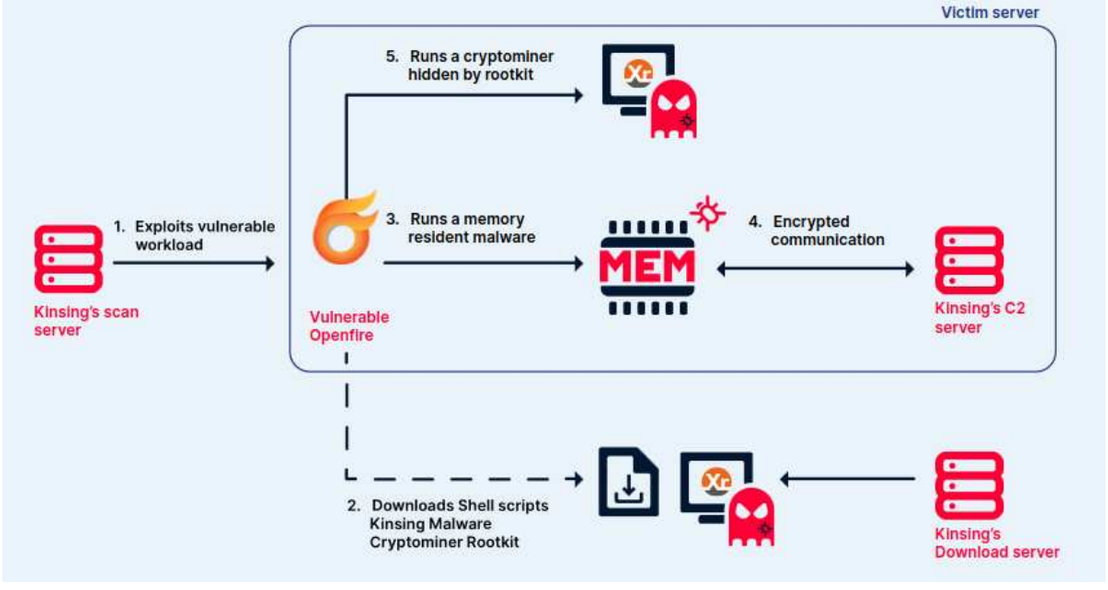


Figure 6. Openfire campaign. Source: Aqua Nautilus

In the scenario presented by Aqua Nautilus' researchers, the malware operators will exploit CVE-2023-32315 in Openfire to gain the initial access.

4.2. Defence evasion

Kinsing stands out for its defence evasion methods, combining commonly used techniques with more original ones. To ensure the effectiveness of these evasion methods, several installation scripts for Kinsing and the malware itself exist, depending on the targeted architecture. In their report, Aqua Nautilus' security researchers identified two categories of installation scripts: Type I and Type II.

- Type I scripts are more substantial (approximately 825 lines) and essentially seek to eliminate the competition (76% of the lines are devoted to this). These files are approximately 14 MB in size.

- Type II scripts are lighter (approximately 454 lines) and focus on defence evasion by installing a *rootkit* (a persistence tool that can hide its existence and that of other software). These are about 6 MB in size.

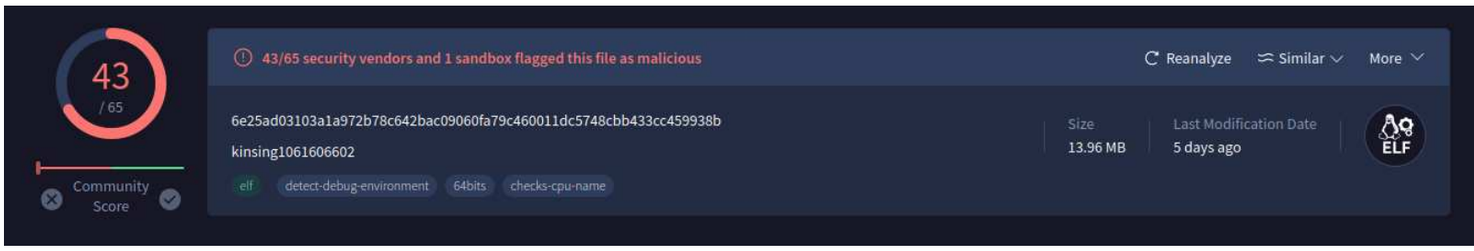


Figure 7. Script Type I

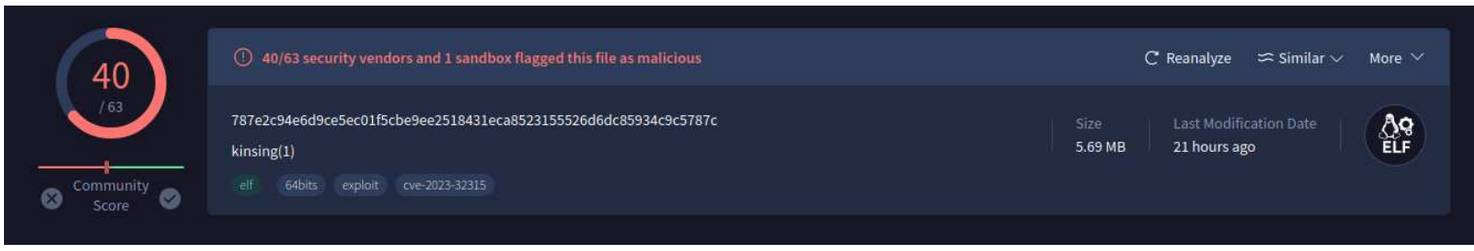


Figure 8. Script Type II

Removal of defence tools

When Type I scripts are run, certain security tools (such as selinux, aegis, apparmor, etc.) are stopped and removed. The script also disables *UFW* firewall protection (via the *ufw disable* command) and flushes the iptables rules (*iptables -f*).

The Type II script installs a *rootkit* in the "*/etc/libsystem.so*" directory.

Eliminating other malware.

Both types of installation scripts list the processes present in the */proc* directory and terminate certain specific processes belonging to competitors. These processes are detected by searching for specific process names, certain strings or IP addresses.

pkger

A distinguishing feature of Kinsing is the presence of Shakespeare's entire play *Hamlet* in some versions of the malware. Cyberark researchers have found the source of this text. The 0.12.8 version of the markbates/pkger opensource tool available on Github, and integrated into Kinsing, uses this text.

The purpose of this text is to increase the size of the binary and to avoid detection by static detection engines.

Man pages

In campaigns as recent as April 2024, Tenable discovered Kinsing installed in the "*man*" pages of Linux systems. The malware was installed in the "*var/cache/man/zh_TW/cat8/*", "*/var/cache/man/cs/cat1/*" and "*/var/cache/man/cs/cat3/*" locations. These locations are used because they are not often checked for malware.

4.3. Comparison with NSPPS

In 2021, Cyberark investigated the Kinsing malware and found that it shares many similarities with another malware called NSPPS.

NSPPS is a Trojan horse also written in Go. Like Kinsing, this malware incorporates the Masscan tool. To use it, both contain a bash script called *firewire.sh* which is executed by the *main.masscan* function. The *firewire.sh* files remain identical, but the *main.masscan* files differ slightly. Cyberark believes that this difference is due to compilation. At the time of the study, the researchers claim that these files were not available in open source.

An analysis of the code shows that the structure used is very similar for both malwares. The biggest difference being the presence of cryptomining features in Kinsing and not in NSPPS.

Figure 9. main.main function

Figure 10. main.doTask function

Code comparison between NSPPS (left) and Kinsing (right). Source : Cyberark

IronNet's researchers also discovered an *RC4* key used by NSPPS as well as Kinsing.

```
000000000088230E RC4_Key_Kinsing db 37h, 36h, 34h, 31h, 35h, 33h, 34h, 34h, 36h, 62h, 36h
000000000088230E                                        ; DATA XREF: .data:RC4_Key_off↓o
```

Figure N. 14: Kinsing RC4 key

```
00000000007B3F79 RC4_Key_NSPPS   db 37h, 36h, 34h, 31h, 35h, 33h, 34h, 34h, 36h, 62h, 36h
00000000007B3F79                                        ; DATA XREF: .data:RC4_Key_off↓o
```

Figure N. 15: NSPPS RC4 key

Figure 11. RC4 key. Source : CyberArk

Their last study focused on function names. NSPPS contains 63 functions whereas Kinsing only contains 59. Of these functions, 51 have the same name, i.e. 84% of the functions. The 8 that differ in Kinsing are related to cryptomining activities and the 12 in NSPPS are related to trojan activities.

The similarities between Kinsing and NSPPS give rise to several hypotheses:

- These tools are operated by the same operators for different purposes.
- One of the two tools is the result of collaboration between operators.
- The first malware was reused and modified by an actor to make their own tool.

4.4. Conclusion

Although Kinsing is not a newmalware, it is still very effective, especially against Cloud environments. Operators continue to maintain and develop it, in particular by improving its performance and evasion techniques.

The risk of cryptomining is often overlooked, but these malwares allow attackers to maintain access to systems and can cause financial losses to victim companies.

4.5. Appendices

4.5.1. Mitre Att&ck

DISCOVERY

T1595.002 Active Scanning: Vulnerability Scanning. T1087.001 Account Discovery: Local Account. T1083 File and Directory Discovery. T1057 Process Discovery. T1018 Remote System Discovery.

INITIAL ACCESS

T1190 Exploit Public-Facing Application. T1133 External Remote Services. T1078 Valid Accounts.

EXECUTION

T1059.004 Command & Scripting Interpréter: Unix Shell. T1106 Native API. T1204.002 User Execution: Malicious File. T1569.002 System Services: Service Stop. T1609 Container Administration Command.

PERSISTENCE

T1546.004 Event Triggered Execution: Unix Shell Configuration Modification. T1543.002 Create or Modify System Process: Systemd Service. T1053.005 Scheduled Task/Job: Scheduled Task. T1053.003 Scheduled Task/Job: Cron.

DEFENSE EVASION

T1222.002 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification. T1562.001/4 Impair Defenses: Disable or Modify Tools/System Firewall. T1070.004 Indicator Removal: File Deletion. T1027.002 Obfuscated Files or Information: Software Packing. T1140 Deobfuscate/Decode Files or Information. T1014 Rootkit.

DISCOVERY

T1595.002 Active Scanning: Vulnerability Scanning. T1087.001 Account Discovery: Local Account. T1083 File and Directory Discovery. T1057 Process Discovery. T1018 Remote System Discovery.

CREDENTIAL ACCESS

T1552.003 Unsecured Credentials: Bash History. T1552.004 Unsecured Credentials: Private Keys. T1110.001 Brute Force: Password Guessing.

COMMAND & CONTROL

T1071.001/2/4 Application Layer Protocol: Web Protocols/Proxy/DNS. T1105 Ingress Tool Transfer.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

IMPACT

T1496 Resource Hijacking. T1490 Inhibit System Recovery. T1485 Data Destruction.

Figure 12. Mitre Att&ck Matrix.

4.5.2. Detection

YARA rule :

```
import "elf"
```

```
rule Kinsing_Malware
{
  meta:
    author = "Aluma Lavi, CyberArk"
    date = "22-01-2021"
    version = "1.0"
    hash = "d247687e9bdb8c4189ac54d10efd29aee12ca2af78b94a693113f382619a175b"
    description = "Kinsing/NSPPS malware"
  strings:
    $rc4_key = { 37 36 34 31 35 33 34 34 36 62 36 31 }
    $firewire = "./firewire -iL $INPUT --rate $RATE -p$PORT -oL $OUTPUT"
    $packa1 = "google/btree" ascii wide
    $packa2 = "kardianos/osext" ascii wide
    $packa3 = "kelseyhightower/envconfig" ascii wide
    $packa4 = "markbates/pkger" ascii wide
    $packa5 = "nu7hatch/gouuid" ascii wide
    $packa6 = "paulbellamy/ratecounter" ascii wide
    $packa7 = "peterbourgon/diskv" ascii wide
    $func1 = "main.RC4" ascii wide
    $func2 = "main.runTaskWithScan" ascii wide
    $func3 = "main.backconnect" ascii wide
    $func4 = "main.downloadAndExecute" ascii wide
    $func5 = "main.startCmd" ascii wide
    $func6 = "main.execTaskOut" ascii wide
    $func7 = "main.minerRunningCheck" ascii wide
  condition:
    (uint16(0) == 0x457F
    and not (elf.sections[0].size + elf.sections[1].size + elf.sections[2].size + elf.sections[3].size +
elf.sections[4].size + elf.sections[5].size + elf.sections[6].size + elf.sections[7].size > filesize))
    and ($rc4_key
    or $firewire
    or all of ($packa*)
    or 4 of ($func*)
    )
}
```

4.5.3. Indicators of Compromise

TLP	TYPE	VALUE	COMMENT	DATE
TLP:CLEAR	Sha256	0b0aa978c061628ec7cd611edeec3373d4742cbda533b07a2b3eb84a9dd2cb8a	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	0c811140be9f59d69da925a4e15eb630352fa8ad4f931730aec9ae80a624d584	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	2132d7bed60fda38adda28efdbbd2df2c9379fed5de2e68fc6801f5621b596b0	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	4b0138c12e3209d8f9250c591fcc825ee6bff5f57f87ed9c661df6d14500e993	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	4f4e69abb2e155a712df9b3d0387f9fb2d6db8f3a2c88d7bbe199251ec08683f	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	5059d67cd24eb4b0b4a174a072ceac6a47e14c3302da2c6581f81c39d8a076c6	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	511de8dd7f3cb4c5d88cd5a62150e6826cb2f825fa60607a201a8542524442e2	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	554c233d0e034b8bb3560b010f99f70598f0e419e77b9ce39d5df0dd3bc25728	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	655ee9ddd6956af8c040f3dce6b6c845680a621e463450b22d31c3a0907727e4	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	6814d22be80e1475e47e8103b11a0ec0daa3a9fdd5caa3a0558d13dc16c143d9	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	681f88d79c3ecab8683b39f8107b29258deb2d58fcea7b0c008bab76e18aa607	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	6e8c96f9e9a886fd6c51cce7f6c50d1368ca5b48a398cc1fedc63c1de1576c1e	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	7727a0b47b7fd56275fa3c1c4468db7fa201c788d1e56597c87deaff45aad634	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	7f9f8209dc619d686b32d408fed0beb3a802aa600ddceb5c8d2a9555cdb3b5e0	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	8c9b621ba8911350253efc15ab3c761b06f70f503096279f2a173c006a393ee1	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	98d3fd460e56eff5182d5abe2f1cd7f042ea24105d0e25ea5ec78fedc25bac7c	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	9fbb49edad10ad9d096b548e801c39c47b74190e8745f680d3e3bcd9b456aafc	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	a0363f3caad5feb8fc5c43e589117b8053cbf5bc82fc0034346ea3e3984e37e8	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	a5b010a5dd29d2f68ac9d5463eb8a29195f40f5103e1cc3353be2e9da6859dc6	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	b44dae9d1ce0ebec7a40e9aa49ac01e2c775fa9e354477a45b723c090b5a28f2	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	b70d14a7c069c2a88a8a55a6a2088aea184f84c0e110678e6a4afa2eb377649f	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	c44b63b1b53cbd9852c71de84ce8ad75f623935f235484547e9d94a7bdf8aa76	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	c9932ca45e952668238960dbba7f01ce699357bedc594495c0ace512706dd0ac	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	ccfda7239b2ac474e42ad324519f805171e7c69d37ad29265c0a8ba54096033d	source:Cyberark	3 september 2021

TLP	TYPE	VALUE	COMMENT	DATE
TLP:CLEAR	Sha256	d247687e9bdb8c4189ac54d10efd29aee12ca2af78b94a693113f382619a175b	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	db3b9622c81528ef2e7dbefb4e8e9c8c046b21ce2b021324739a195c966ae0b7	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	f2e7244e2a7d6b28b1040259855aeac956e56228c41808bccb8e37d87c164570	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b	source:Lacework	12 december 2021
TLP:CLEAR	Sha256	c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	b9e79bb09995a9dd2f5a22dc2e59738696e2be2204ec92a2881fb3fa70e0160f	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	93fb80086c152179bfec7f19f5060758139828ef6938bac51ba8fbb673fc7b91	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	c6fbd6896d162a12d9c900056781eb82f44649945808b7b009646b5397bcf6bf	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	063f80c2c5accaecd8c9e6b6815ae80e372477f9df1113dafc72a2a0703aaa68	XMRig source:Tenable	16 may 2024

4.5.4. List of exploited vulnerabilities

Product	CVE identifier	Risk	CVSSv3 score
Citrix	CVE-2019-19781	Remote code execution	9.8
Kibana	CVE-2019-7609	Remote code execution	10
Oracle WebLogic	CVE-2020-14883	Server compromise	7.2
SaltStack	CVE-2020-11651	Remote code execution	9.8
SaltStack	CVE-2020-11652	Confidentiality breach	6.5
Liferay	CVE-2020-7961	Remote code execution	9.8
WordPress File Manager	CVE-2020-25213	Remote code execution	9.8
Apache HTTP Server	CVE-2021-41773	Remote code execution	7.5
Log4j	CVE-2021-44228	Remote code execution	10
Atlassian Confluence	CVE-2021-26084	Remote code execution	9.8
Atlassian Confluence	CVE-2022-26134	Remote code execution	9.8
WSO2	CVE-2022-29464	Remote code execution	9.8
glibc	CVE-2023-4911	Remote code execution	7.8
Apache ActiveMQ	CVE-2023-46604	Remote code execution	9.8
Apache Openfire	CVE-2023-32315	Confidentiality breach	7.5

5. Sources

CVEs

- https://nvd.nist.gov/vuln/detail/CVE-2024-29212
- https://www.veeam.com/kb4575
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0374/
- https://www.helpnetsecurity.com/2024/05/08/cve-2024-29212/
- https://nvd.nist.gov/vuln/detail/CVE-2024-25641
- https://github.com/Cacti/cacti/security/advisories/GHSA-7cmj-g5qc-pj88
- https://thehackernews.com/2024/05/critical-flaws-in-cacti-framework-could.html
- https://nvd.nist.gov/vuln/detail/CVE-2024-26289
- https://github.com/enisaeu/CNW/blob/main/advisories/2024/CNW-2024-A-12.md
- https://cert.be/en/advisory/warning-remote-code-inclusion-vulnerability-multiple-versions-pmb-library-software-patch

Latrodectus, the new IcedID?

- https://medium.com/walmartglobaltech/icedid-gets-loaded-af073b7b6d39
- https://www.elastic.co/security-labs/spring-cleaning-with-latrodectus
- https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice
- https://github.com/pr0xylife/latrodectus/
- https://x.com/embee_research/status/1792826263738208343

The Kinsing malware

- https://1665891.fs1.hubspotusercontent-na1.net/hubfs/1665891/Threat%20reports/AquaSecurity_Kinsing_Demystified_Technical_Guide.pdf
- https://www.cyberark.com/resources/threat-research-blog/kinsing-the-malware-with-two-faces
- https://redcanary.com/blog/threat-intelligence/kinsing-malware-citrix-saltstack/
- https://blog.sekoia.io/activemq-cve-2023-46604-exploited-by-kinsing-and-overview-of-this-threat/#h-iocs
- https://www.tenable.com/blog/kinsing-malware-hides-itself-as-a-manual-page-and-targets-cloud-servers
- https://www.trendmicro.com/vinfo/ph/security/news/virtualization-and-cloud/misconfigured-docker-daemon-api-ports-attacked-for-kinsing-malware-campaign
- https://sysdig.com/blog/cloud-defense-in-depth/
- https://www.ironnet.com/blog/malware-analysis-nspps-a-go-rat-backdoor