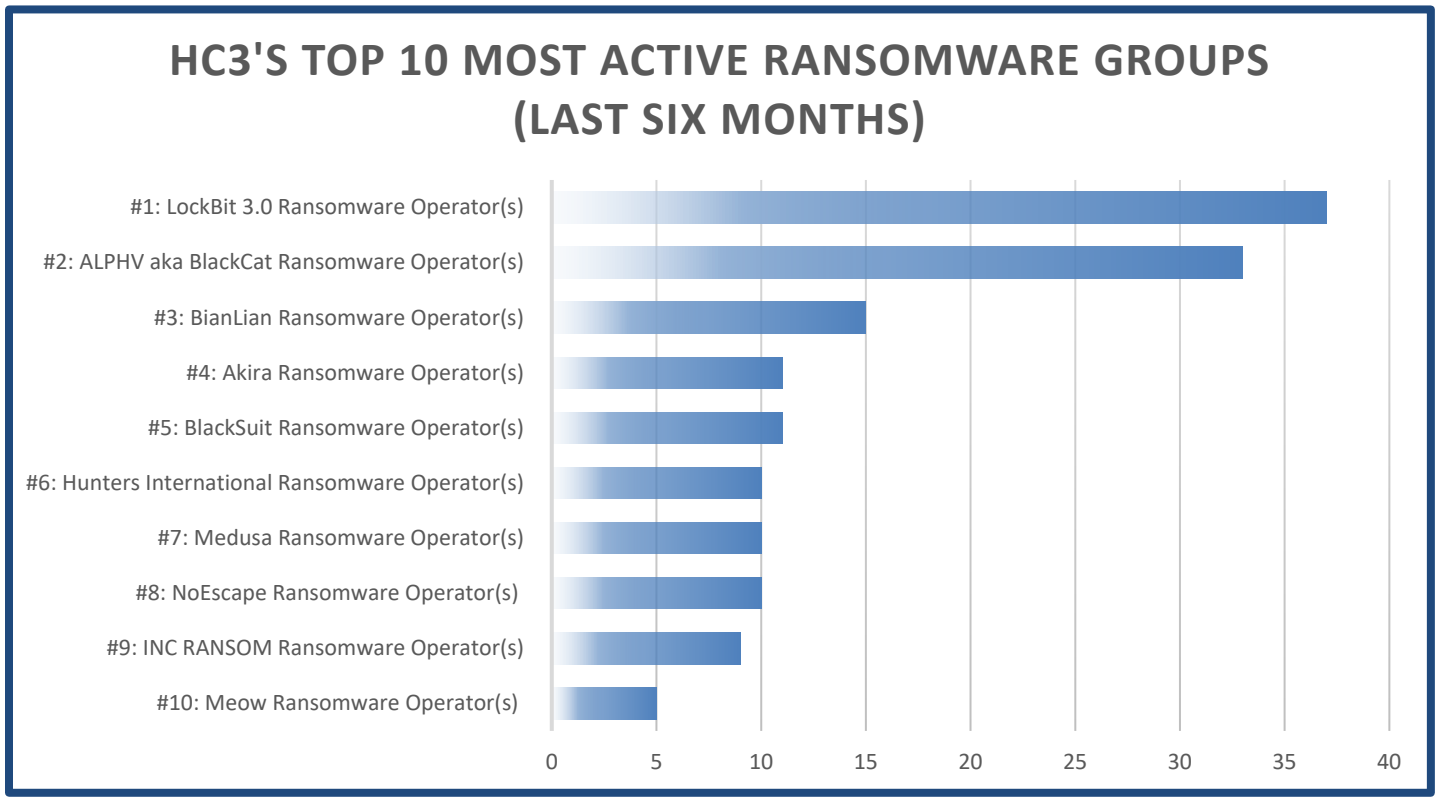
HC3: Analyst Note
April 5, 2024 TLP:CLEAR Report: 202404051700

HC3's Top 10 Most Active Ransomware Groups

Executive Summary
HC3 monitors and tracks healthcare incidents across multiple platforms, including proprietary and open-source intelligence. As of mid-March 2024, in the last six months HC3 has tracked 730 attacks against the Healthcare and Public Health (HPH) sector worldwide. Of these attacks, more than 530 affected the U.S. HPH, and of those attacks, nearly half were ransomware related. This report provides high-level insight into the top ten ransomware groups HC3 has seen targeting the healthcare sector.

Report
This chart shows the top 10 most active ransomware groups HC3 has seen targeting the U.S. HPH:



#1: LockBit 3.0 Ransomware Operator(s)
As of July 2022, LockBit 3.0 is a ransomware-as-a-service (RaaS) group that continues the legacy of LockBit and LockBit 2.0. They are also the most active RaaS group targeting the U.S. HPH. One of the key differences from its predecessors is the ability to customize both the compilation and execution of the payload. LockBit 3.0 utilizes a modular approach and encrypts the payload until execution, which presents significant obstacles to malware analysis and detection.

LockBit 3.0 uses multiple methods for initial access, including exploiting Remote Desktop Protocol (RDP), phishing campaigns, and exploiting vulnerabilities in public-facing applications. Using an open-source package installer known as Chocolatey to install and execute malicious payloads is a recurring feature in LockBit 3.0 attacks, likely employed to evade detection. LockBit 3.0 uses hardcoded credentials or

compromised local accounts with elevated privileges to spread through a victim network. Using the Server Message Block (SMB) protocol, it can also spread via Group Policy Objects and PsExec.

MITRE ATT&CK TTPs Used by LockBit 3.0

TACTIC	TECHNIQUE	ID
Initial Access	Phishing	T1566
	External Remote Services	T1133
	Valid Accounts	T1078
	Drive-by Compromise	T1189
	Exploit Public-Facing Application	T1190
Privilege Escalation	Boot or Logo AutoStart Execution	T1547
Execution	Software Deployment Tools	T1072
Persistence	Valid Accounts	T1078
	Boot or Logo AutoStart Execution	T1547
Defense Evasion	Obfuscated Files or Information	T1027
	Indicator Removal: File Deletion	T1070.004
	Execution Guardrails: Environmental Keying	T1480.001
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001
Discovery	Network Service Discovery	T1046
	System Information Discovery	T1082
	System Location Discovery: System Language Discovery	T1614.001
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001
Command And Control	Application Layer Protocol: File Transfer Protocols	T1071.002
	Protocol Tunnel	T1572
Exfiltration	Exfiltration Over Web Service	T1567
	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
Impact	Data Destruction	T1485
	Data Encrypted for Impact	T1486
	Service Stop	T1489
	Inhibit System Recovery	T1490
	Defacement: Internal Defacement	T1491.001

#2: ALPHV aka BlackCat Ransomware Operator(s)

BlackCat, or ALPHV, is a ransomware group known for being the first to use the Rust programming language, which allows for easy malware customization for different operating systems—such as Windows and Linux—and bypassing security controls that are not designed to analyze malware written in Rust. The

group has been operating since approximately December 2021 and uses a lucrative ransomware-as-a-service (RaaS) model, which could make it more attractive to potential affiliates.

The group gains initial access to targeted systems by using stolen user credentials or exploiting known Microsoft Exchange vulnerabilities. Once they have access, they compromise user and administrator accounts within the Active Directory. This allows them to set up malicious Group Policy Objects (GPOs) using the Windows Task Scheduler, enabling them to deploy the ransomware payload. Once the threat actor accesses the network, it disables the security measures of a target organization by removing antivirus software. After that, the actor obtains domain accounts using AdFind and ADRecon tools, and gathers information about the victim network using SoftPerfect. Finally, the attacker uses Process Hacker and Mimikatz to obtain and extract the victim's login credentials.

MITRE ATT&CK TTPs Used by ALPHV aka BlackCat

TACTIC	TECHNIQUE	ID
Execution	Malicious File	T1204.002
	Windows Command Shell	T1059.003
Privilege Escalation	Process Injection	T1055
Defense Evasion	Disable or Modify Tools	T1562.001
Discovery	Query Registry	T1012
	System Information Discovery	T1082
Impact	Inhibit System Recovery	T1490
	Defacement	T1491
	Data Encrypted for Impact	T1486

#3: BianLian Ransomware Operator(s)

BianLian (变脸), which is a reference to the traditional Chinese art of "face-changing", is a shape-shifting cyber threat actor known for its agile adaptation and rapid evolution in its tactics, techniques, and procedures (TTPs). It first appeared as an Android banking trojan in 2019, but shifted its operations to focus on ransomware attacks, becoming a ransomware strain first observed in July 2022.

BianLian employs a multi-stage attack methodology. Initial access to the target system is often achieved through phishing emails containing malicious attachments or links to compromised websites. Upon successful infiltration, the malware will communicate with its command and control (C2) server, downloading additional modules and tools to escalate its privileges and establish a persistent foothold in the compromised system.

MITRE ATT&CK TTPs Used by BianLian

TACTIC	TECHNIQUE	ID
Resource Development	Develop Capabilities: Malware	T1587.001
Initial Access	External Remote Services	T1133
	Phishing	T1566
Privilege Escalation	Valid Accounts	T1078
Execution	Command and Scripting Interpreter: PowerShell	T1059.001

	Command and Scripting Interpreter: Windows Command Shell	T1059.003
	Scheduled Task/Job	T1053
Persistence	Account Manipulation	T1098
	Create Account: Local Account	T1136.001
Defense Evasion	Modify Registry	T1112
	Impair Defenses: Disable or Modify Tools	T1562.001
	Impair Defenses: Disable or Modify System Firewall	T1562.004
Credential Access	Unsecured Credentials: Credentials in Files	T1552.001
	OS Credential Dumping: LSASS Memory	T1003.001
	OS Credential Dumping: NTDS	T1003.003
Discovery	Account Discovery: Domain Account	T1087.002
	Domain Trust Discovery	T1482
	File and Directory Discovery	T1083
	Network Service Discovery	T1046
	Network Share Discovery	T1135
	Permission Groups Discovery: Domain Groups	T1069.002
	Query Registry	T1012
	Remote System Discovery	T1018
	System Owner/User Discovery	T1033
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001
Collection	Clipboard Data	T1115
Command And Control	Ingress Tool Transfer	T1105
	Remote Access Software	T1219
Exfiltration	Transfer Data to Cloud Account	T1537
	Exfiltration Over Alternative Protocol	T1048
	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
Impact	Data Encrypted for Impact	T1486

#4: Akira Ransomware Operator(s)

Akira ransomware was first identified in May 2023, but there is research suggesting that Akira has connections to the inoperative Conti ransomware gang. The technical details of this include similarities in their exploitation approach, the selection of certain types of files and directories for targeting, their choice

of application for encryption algorithms, their use of ransom payment addresses, and the incorporation of comparable functions. While any formal connection between the two groups has not been confirmed, such a connection could indicate a degree of sophistication to Akira's operations. Akira works as a ransomware group as well as a ransomware-as-a-service (RaaS) group. They conduct double extortion, meaning they charge two fees. The first fee restores the encrypted systems, and the second fee ensures no leaks of stolen data.

They are highly reliant on credential compromise, which provides them initial access into their target networks. In almost all instances of intrusion, the malicious actors capitalized on compromised credentials to gain their initial foothold within the victim's environment. Particularly noteworthy is the fact that most of the targeted organizations had neglected to implement multi-factor authentication (MFA) for their VPNs.

MITRE ATT&CK TTPs Used by Akira

TACTIC	TECHNIQUE	ID
Initial Access	Spear Phishing Attachment	T1566.001
	Spear Phishing Link	T1566.002
	Valid Accounts	T1078
	Exploit Public-Facing Application	T1190
	Supply Chain Compromise	T1195
Privilege Escalation	Valid Accounts	T1078
	Create Account: Domain Account	T1136.002
	Shortcut Modification	T1547.009
	Registry Run Keys / Startup Folder	T1547.001
Persistence	Valid Accounts	T1078
	Shortcut Modification	T1547.009
	Registry Run Keys / Startup Folder	T1547.001
Lateral Movement	Lateral Tool Transfer Data Collection	T1570
Data Collection	Local Email Collection	T1114.001
Data Exfiltration	Exfiltration Over Web Service	T1567
	Exfiltration Over C2 Channel	T1041
	Transfer Data to Cloud Account	T1537
	Scheduled Transfer	T1029
	Automated Exfiltration	T1020
Execution	PowerShell	T1059.001
	Service Execution	T1569.002
	Windows Command Shell	T1059.003
Impact	Data Encrypted for Impact	T1486
Defensive Evasion	Valid Accounts	T1078
	Binary Padding	T1027.001
	Match Legitimate Name or Location	T1036.005
	Impari Defenses: Disable or Modify Tools	T1562.001

#5: BlackSuit Ransomware Operator(s)

Discovered in early May 2023, BlackSuit bares significant similarities to the Royal ransomware family—the

direct successor of the former notorious Russian-linked Conti operation. BlackSuit operates using a double extortion method that steals and encrypts sensitive data on a compromised network.

At this time, not enough is known about BlackSuit ransomware to say which of the below TTPs they rely on the most, but below is a list of TTPs that they have been noted to utilize:

MITRE ATT&CK TTPs Used by BlackSuit

TACTIC	TECHNIQUE	ID
Execution	User Execution	T1204
	Command and Scripting Interpreter	T1059
Discovery	Process Discovery	T1057
	System Information Discovery	T1082
	File and Directory Discovery	T1083
Impact	Data Encrypted for Impact	T1486
	Inhibit System Recovery	T1490

#6: Hunters International Ransomware Operator(s)

Hunters International emerged around the time of the disruption of the Hive ransomware group by law enforcement agencies. This new group, detected in the latter part of 2023, exhibited significant technical overlap with Hive, initially suggesting an evolution or offshoot of the dismantled operation, but the group has stated that they are not simply a new version of Hive, but an independent entity that took over Hive's source code and infrastructure. Their main operational focus is on stealing data rather than encrypting it, distinguishing their approach from Hive's.

The group's focus significantly leans towards stealing data, as evidenced by all known victims experiencing data exfiltration, whereas not every victim's data was encrypted. Hunters International seems to have customized Hive's ransomware to enhance simplicity and efficiency. By reducing command-line options and optimizing encryption key management, they have made their malware less verbose and easier to use for operatives. The switch to Rust, mirroring trends in sophisticated ransomware development, aids in evading detection and facilitates faster encryption. Their approach embeds encryption keys within the encrypted files, a method aimed at streamlining the decryption process for victims who pay the ransom while also complicating security professionals' efforts to counteract the malware.

MITRE ATT&CK TTPs Used by Hunters International

TACTIC	TECHNIQUE	ID
Execution	Native API	T1106
	Shared Modules	T1129
Persistence	Boot or Logon AutoStart Execution	T1547.001
Defense Evasion	Obfuscated Files or Information	T1027
	Impair Defenses	T1562.001
Discovery	Process Discovery	T1057
	System Information Discovery	T1082
	File and Directory Discovery	T1083
Command and Control	Application Layer Protocol	T1071
	Web Protocols	T1071.001

Impact	Data Encrypted for Impact	T1486

#7: Medusa Ransomware Operator(s)

First recorded in June 2021, Medusa (or MedusaLocker) operates under the ransomware-as-a-service (RaaS) model—collaborating with global affiliates and making its reach and impact even more widespread. Due to their using multiple encrypted file extensions (with their signature extension being ".MEDUSA"), it is believed there are multiple variants of Medusa ransomware.

This ransomware predominantly gains access to systems through vulnerable Remote Desktop Protocols (RDP) and phishing campaigns. Once it breaches a system, Medusa employs PowerShell for command execution, systematically erasing shadow copy backups to prevent data restoration. The ransomware then escalates its system privileges, deactivates defense mechanisms, and spreads across the network.

MITRE ATT&CK TTPs Used by Medusa

TACTIC	TECHNIQUE	ID
Initial Access	Valid Accounts	T1078
	Phishing	T1566
	External Remote Services	T1133
Execution	Command and Scripting Interpreter: PowerShell	T1059.001
	Windows Management Instrumentation	T1047
Persistence	Boot or Logon AutoStart Execution	T1547
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002
Defense Evasion	Impair Defenses: Disable or Modify Tools	T1562.001
	Impair Defenses: Safe Mode Boot	T1562.009
Credential Access	Brute Force	T1110
Discovery	File and Directory Discovery	T1083
	Network Share Discovery	T1135
	Query Registry	T1012
Lateral Movement	Remote Services	T1021
Command and Control	Ingress Tool Transfer	T1105
	Application Layer Protocol: Web Protocols	T1071.001
Exfiltration	Exfiltration Over Alternative Protocol	T1048
Impact	Service Stop	T1489

#8: NoEscape Ransomware Operator(s)

NoEscape Ransomware surfaced in May 2023 as a ransomware-as-a-service (RaaS) group. Unlike many of its contemporaries, the developers of NoEscape assert that they have constructed the malware and its associated infrastructure entirely from the ground up, deliberately avoiding the use of source code or leaks

from other established ransomware families. Currently, NoEscape provides affiliates with a comprehensive platform that facilitates the creation and management of payloads tailored for both Windows and Linux operating systems. Furthermore, NoEscape is recognized for its multi-extortion tactics, maintaining a TOR-based blog to publicly list its victims and display the exfiltrated data of those who resist meeting their demands.

NoEscape ransomware supports multiple encryption modes, and it leverages encryption algorithms like RSA and ChaCHA20 for file encryption. The ransomware has features like process termination, safe-mode operation, spreading and encryption over SMB or DFS, and the use of the Windows Restart Manager to bypass any processes that might block encryption. A unique feature is the shared encryption, which allows a single encryption key to be used across all infected files in a network, facilitating efficient encryption and quick decryption if the ransom is paid.

MITRE ATT&CK TTPs Used by NoEscape

TACTIC	TECHNIQUE	ID
Initial Access	External Remote Services	T1133
	Valid Accounts	T1078
Execution	User Execution	T1204.002
	Scheduled Task/Job	T1053.005
Persistence	Registry Run Keys / Startup Folder	T1547.001
	Valid Accounts	T1078
Privilege Escalation	Valid Accounts	T1078
Defense Evasion	Disable or Modify Tools	T1562.001
	Software Packing	T1027.002
	Process Injection	T1055
	Indicator Removal on Host	T1070.004
	Modify Registry	T1112
	Deobfuscate/Decode Files or Information	T1140
	Virtualization/Sandbox Evasion	T1497.001
Credential Access	OS Credential Dumping	T1003
Discovery	Account Discovery	T1078
	Domain Trust Discovery	T1482
	Permissions Groups Discovery	T1069
Lateral Movement	Remote Services	T1021
	Remote Desktop Protocol	T1021.001
Collection	Archive via Utility	T1560.001
Command and Control	Web Protocols	T1071.001

	Exfiltration to Cloud Storage	T1567.002

#9: INC RANSOM Ransomware Operator(s)

INC RANSOM is a relatively new but highly sophisticated cybercriminal group that has rapidly gained notoriety in the realm of digital extortion. This group has distinguished itself through its targeted ransomware attacks, primarily focusing on corporate and organizational networks. Unlike many opportunistic ransomware operators, INC RANSOM appears to carefully select its targets, often aiming at entities with substantial financial resources and sensitive data, which makes the potential payoff from their ransom demands significantly higher.

The group's modus operandi involves a combination of advanced techniques, including spear phishing campaigns to gain initial access, exploitation of known vulnerabilities, and the use of both Commercial Off-The-Shelf (COTS) softwares and legitimate system tools (LOLBINs) for reconnaissance and lateral movement within a network. This approach not only demonstrates their technical prowess, but also their ability to stay under the radar, making detection and prevention more challenging. INC RANSOM utilizes double extortion, meaning that they do not not simply encrypt and ransom data, but they also steal it and threaten to release it publicly.

MITRE ATT&CK TTPs Used by INC RANSOM

TACTIC	TECHNIQUE	ID
Initial Access	Spear Phishing	T1566
	Exploitation of Public-Facing Application	T1190
Execution	Command and Scripting Interpreter	T1059
Persistence	Valid Accounts	T1078
Privilege Escalation	Exploitation for Privilege Escalation	T1068
Defense Evasion	Obfuscated Files or Information	T1027
Credential Access	Credential Dumping	T1003
Discovery	System Network Configuration Discovery	T1016
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001
Collection	Data Staged	T1074
Exfiltration	Data Encrypted for Impact	T1486
Command and Control	Ingress Tool Transfer	T1105
Impact	Data Destruction	T1485

#10: Meow Ransomware Operator(s)

Initially identified in August 2022, Meow ransomware (associated with the Conti v2 variant) disappeared after March 2023 for a time, before a similarly named group resurfaced in late 2023. Their dark web presence displays a limited roster of victims, but only those who have not paid the ransom are shown. Once operating under different names such as MeowCorp, MeowLeaks, or simply Meow, this ransomware employs the ChaCha20 algorithm to encrypt data on compromised servers. Victims are then instructed to contact the extortionists through email or Telegram to receive instructions on paying the ransom and recovering their files.

Not enough is known about the current iteration of Meow ransomware to say for sure, but below is a list of TTPs it is believed they utilize:

HC3: Analyst Note

April 5, 2024 TLP:CLEAR Report: 202404051700

MITRE ATT&CK TTPs of Meow

TACTIC	TECHNIQUE	ID
Initial Access	Exploit Public-Facing Application	T1190
	External Remote Services	T1133
	Phishing	T1566
Execution	Shared Modules	T1129
Defense Evasion	Obfuscated Files or Information	T1027
	Indicator Removal from Tools	T1027.005
	Masquerading	T1036
	Virtualization/Sandbox Evasion	T1497
Credential Access	Input Capture	T1056
Discovery	Process Discovery	T1057
	System Information Discovery	T1082
	File and Directory Discovery	T1083
	Virtualization/Sandbox Evasion	T1497
	Security Software Discovery	T1518.001
Lateral Movement	Taint Shared Content	T1080
Collection	Input Capture	T1056
Command and Control	Application Layer Protocol	T1071
	Encrypted Channel	T1573
Exfiltration	Exfiltration Over C2 Channel	T1041
Impact	Data Encrypted for Impact	T1486

Analyst Comment

An interesting takeaway is that almost every single threat actor in this report utilized some type of phishing as an initial access vector. Organizations should train their employees and take active measures against this form of attack. More information on phishing and how to mitgate against it can be found here.

Observations in the graph are based on a variety of sources, but are not the full picture. HC3 would like to stress how helpful it is that incidents are reported properly to the government, as it enables a more comprehensive picture of the cyber threats that the sector is facing. Cybersecurity incidents can be reported here.

Relevant HHS Reports

For more information on several of the most active ransomware groups, please see our previously published resources:

- #1: LockBit 3.0 Ransomware Operator(s)
  - 20231122 - LockBit 3.0 Exploiting Citrix Bleed Sector Alert
  - 20230428 - New Data Breaches from Cl0p and LockBit Ransomware Groups Sector Alert
  - 20221212 - LockBit 3.0 Ransomware Analyst Note
- #2: ALPHV aka BlackCat Ransomware Operator(s)
  - 20240227 - ALPHV Blackcat Joint Cybersecurity Advisory
  - 20220426 - BlackCat/ALPHV Ransomware Indicators of Compromise Sector Alert

- #4: Akira Ransomware Operator(s)
  - 20240207 - Akira Ransomware Analyst Note
  - 20230912 - Akira Ransomware Sector Alert
- #5: BlackSuit Ransomware Operator(s)
  - 20231106 - BlackSuit Ransomware Analyst Note
- #8: NoEscape Ransomware Operator(s)
  - 20231012 - NoEscape Ransomware Analyst Note

References

Akira Ransomware: What SOC Teams Need to Know
https://cyberint.com/blog/research/akira-ransomware-what-soc-teams-need-to-know/

Dark Web Profile: BlackCat (ALPHV)
https://socradar.io/dark-web-profile-blackcat-alphv/

Dark Web Profile: Hunters International
https://socradar.io/dark-web-profile-hunters-international/

Dark Web Profile: INC Ransom
https://socradar.io/dark-web-profile-inc-ransom/

Dark Web Profile: LockBit 3.0 Ransomware
https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/

Dark Web Profile: Medusa Ransomware (MedusaLocker)
https://socradar.io/dark-web-profile-medusa-ransomware-medusalocker/

Dark Web Profile: Meow Ransomware
https://socradar.io/dark-web-profile-meow-ransomware/

Dark Web Profile: NoEscape Ransomware
https://socradar.io/dark-web-profile-noescape-ransomware/

Threat Actor Profile: BianLian, The Shape-Shifting Ransomware Group
https://socradar.io/threat-actor-profile-bianlian-the-shape-shifting-ransomware-group/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback