blackpoint

THREAT PROFILE:

Play Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2022

Operation style:
Debated - reports indicate the group likely operates as a ransomware-as-a-service (RaaS); however, the group maintains they are a private operation.

Extortion method:
Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:
- North America

Known Associations:
- Andariel
- Balloonfly
- Fiddling Scorpius
- Prolific Panda
- QuadSwitcher
- Quantum Ransomware

INITIAL ACCESS	PERSISTENCE	LATERAL MOVEMENT
Valid accounts, exploitation of external remote services, vulnerability exploitation, phishing (MITRE ATT&CK: T1078, T1133, T1190, T1566)	Scheduled tasks, valid accounts, create or modify system process (MITRE ATT&CK: T1053, T1078, T1543)	Exploitation of remote services, lateral tool transfer (MITRE ATT&CK: T1021, T1570)

Diamond Model

Description

Play (AKA PlayCrypt) ransomware is a private ransomware operation that has been active since, at least, June 2022. The group operates in a double extortion method, where the victim data is stolen and leaked via a data leak site if the ransom demand is not paid. According to the group's data leak site, the operation remains a closed operation that is designed to "guarantee the secrecy of deals." Despite reports that the group opened their operations to a RaaS in late 2023, the group's data leak site contains a statement that they are private and have not, and do not plan to, open their operation.

Play ransomware operators gain initial access through a variety of methods, including the abuse of valid accounts, exploiting vulnerabilities, specifically FortiOS and Microsoft Exchange instances, social engineering attacks, and abusing external facing services, including RDP and VPN.

Play ransomware has been assessed to operate in a similar manner to Hive and Nokoyawa ransomware operations; however, as many ransomware operations follow similar behaviors, it is not known the extent of the relationship between these operations. Play and Quantum ransomware operations partly share the same infrastructure, in that Cobalt Strike beacons observed in Play attacks contain the same watermarks as those that had been dropped by Emotet and SVCReady botnets in Quantum ransomware attacks.

Play ransomware is written in C++ and contains several anti-debugging and anti-analysis features to slow investigations into the behaviors of the ransomware, including garbage code and function returns that drive execution into a dead end.

Play has been reported as a RaaS; however, the group maintains they are a completely private operation via their data leak site.

In 2025, it was reported that the Play binary is recompiled for every attack. This results in unique hashes for each deployment, making anti-malware and anti-virus program detection of the malware more difficult.

The group utilizes the public music folder to hide their malicious files and creates new, high-privilege accounts, on victim machines. The Play ransomware group uses intermittent encryption that encrypts chunks of 0x10000 bytes. The observed samples encrypt every other 0x10000 byte chunk until the end of the file.

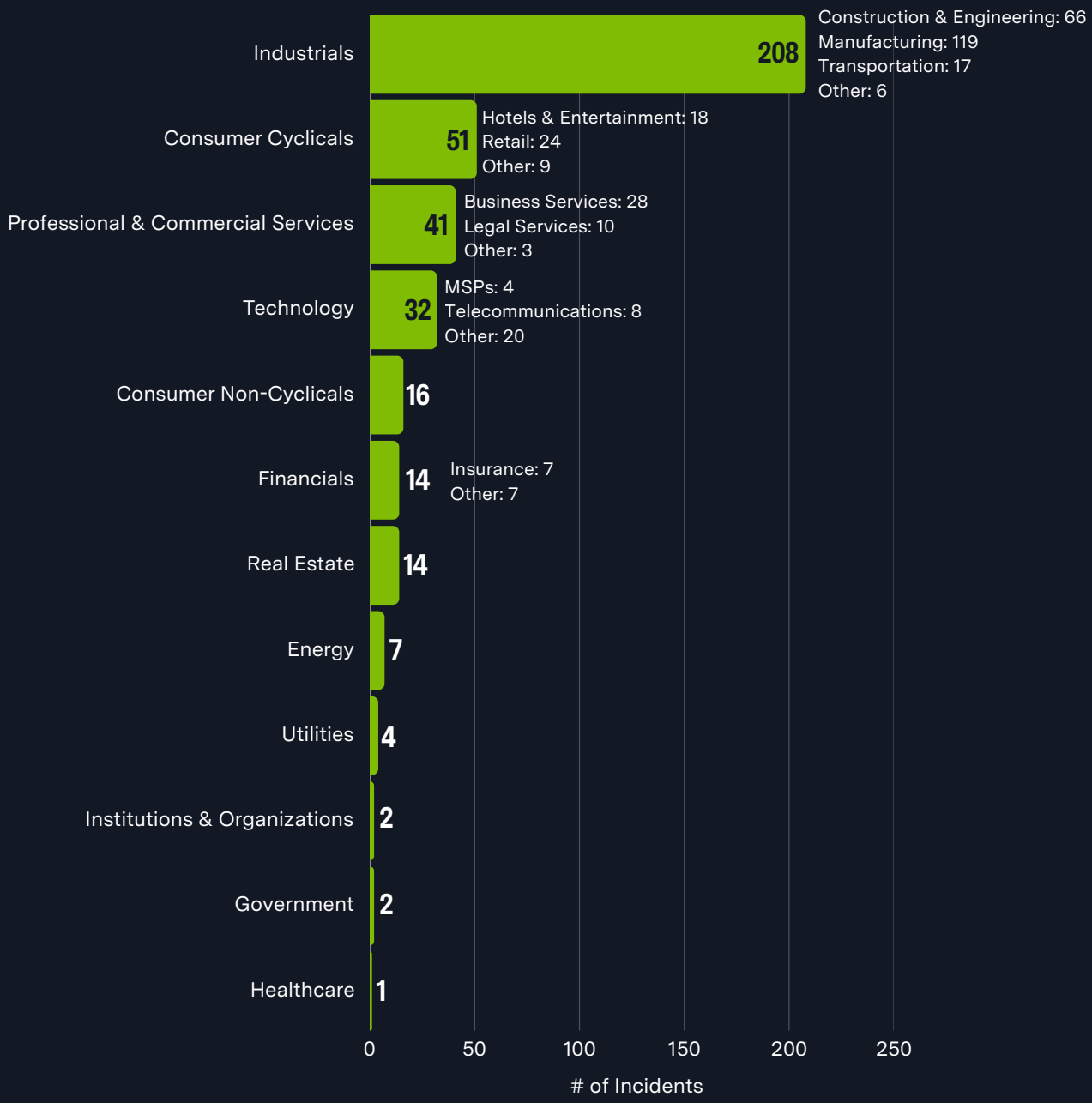
In 2024, Trend Micro security researchers reported that Play ransomware operators had developed and began deploying a Linux variant of the ransomware. The variant only encrypts files when running in a VMware ESXi environment. The identification of a Linux version indicates that the group is likely attempting to expand their operations.

Additionally, the researchers reported that a URL used to host the Play ransomware payload and its tools is related to another threat actor, Prolific Puma. This indicates that the two groups are likely related in some capacity.

In ransom notes, Play operators have been observed providing emails ending in "gmx[.]de" or web[.]de" for victims to contact the group.

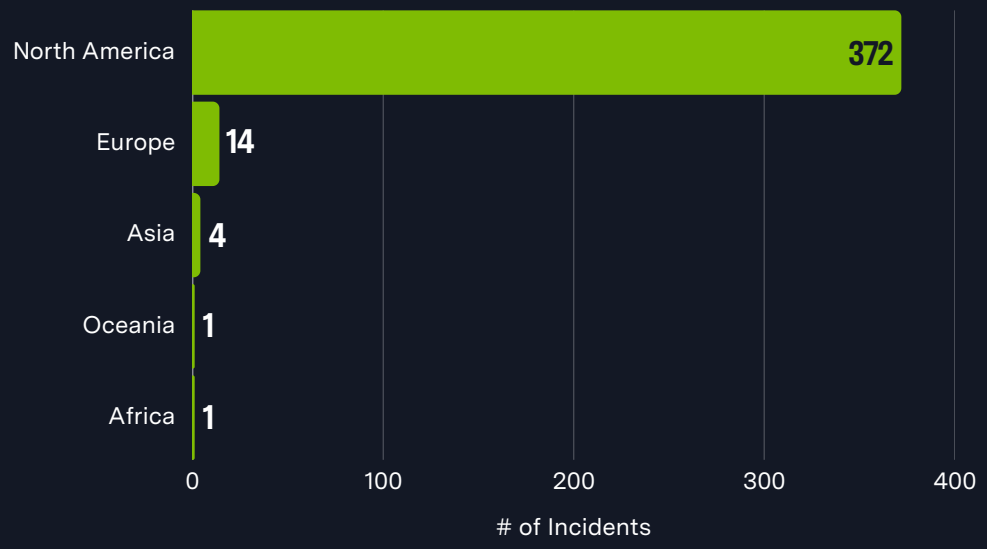
Previous Targets

Previous Industry Targets from 01 Jan 2025 to 31 Dec 2025

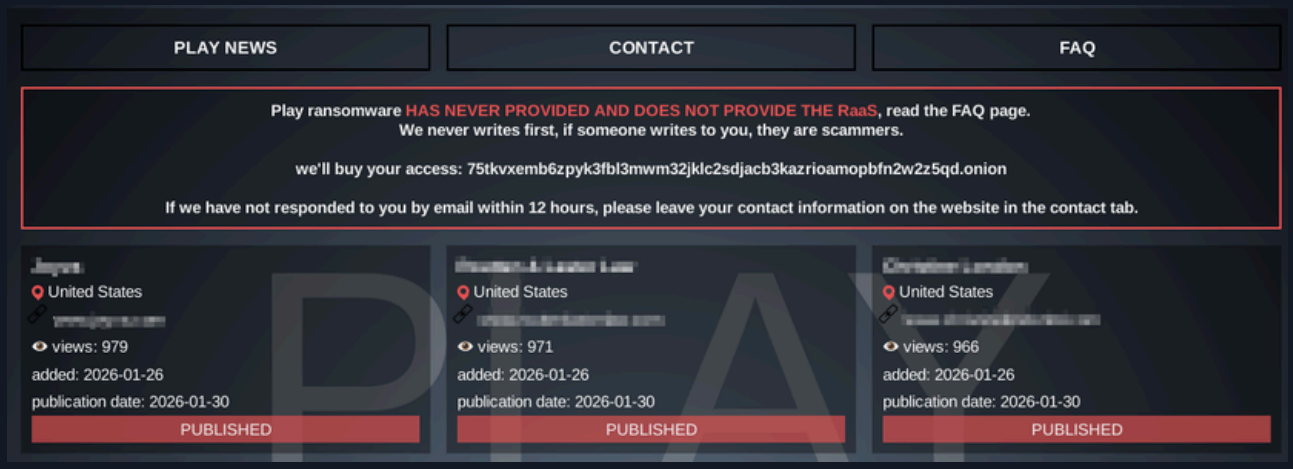


Previous Targets

Previous Victim HQ Regions from 01 Jan 2025 to 31 Dec 2025



Data Leak Site



hxxp://k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd[.]onion/
hxxp://mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd[.]onion/

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2014-7169	Arbitrary Code Execution Vulnerability	GNU Bourne-Again Shell (Bash)	9.8
CVE-2016-6662	RCE Vulnerability	Oracle MySQL, MariaDB, and Percona Server	9.8
CVE-2018-13379	Credential Exposure Vulnerability	Fortinet FortiOS SSL VPN	9.8
CVE-2020-12812	2FA Authentication Vulnerability	Fortinet FortiOS SSL VPN	9.8
CVE-2024-57727	Path Traversal Vulnerability	SimpleHelp	7.5
OWASSRF (CVE-2022-41080)	SSRF Vulnerability	Microsoft Exchange	9.8
ProxyNotShell (CVE-2022-41040; CVE-2022-41082)	Privilege Escalation Vulnerability/RCE Vulnerability	Microsoft Exchange	8.8, 8.8
ZeroLogon (CVE-2020-1472)	Privilege Escalation Vulnerability	Netlogon	10

Associations

Andariel

AKA APT45, Nickel Hyatt, Onyx Sleet, Jumpy Pisces. Security researchers with Palo Alto reported an Andariel intrusion that resulted in the deployment of the Play Ransomware variant. As Play claims to not operate as an RaaS, there is an even chance that Andariel acted as an initial access broker, providing access to Play operators after gain persistence and collecting sensitive data.

Balloonfly

A threat group tracked by Symantec, attributed with the development of the Play ransomware variant.

Fiddling Scorpius

Threat group behind the Play Ransomware operation as tracked by Palo Alto.

Prolific Puma

A threat group that has been reported to provide an underground link shortening service to other cybercriminals. Trend Micro security researchers reported that a Play ransomware encryptor and tools were hosted on a URL linked to the Prolific Puma.

QuadSwitcher

An affiliate that has been linked to multiple groups, including Play and Ransomhub. The affiliate was attributed with targeting a Manufacturing company in 2024. Play has announced, via their data leak site, that they have never operated as an RaaS, indicating that a trusted member of the Play operation has a cooperative relationship with other ransomware operations.

Quantum Ransomware

Security researchers have reported that Cobalt Strike beacons in Play's attacks have the same watermark that was dropped by the Emotet and SVCReady botnets observed in Quantum ransomware attacks. The extent of the connection between Play and Quantum remains unknown.

Known Tools

Function	Tool	Description
Execution	cmd	Utility used to execute commands on Windows systems.
	PowerShell	Command line shell, scripting language, and automation framework utilized to execute scripts and payloads.
	WMI	Microsoft's framework for managing data and operations used to execute commands and queries remotely.
Persistence	AnyDesk	Remote access tool abused for persistent access.
	SimpleHelp	RMM tool abused to maintain access.
Privilege Escalation	Nekto/PriviCMD	Tool used to elevate privileges on a compromised host.
	PowerTool	Tool used to enable Kernel-level manipulation of security services.
	TokenPlayer	Tool used to manipulate and abuse Windows access tokens
	WinPEAS	Utility used to enumerate Windows privilege escalation paths
	WKTools	Collection of tools used to modify Windows Kernel.
Defense Evasion	AlphvVSS	.NET class library used to interact with Volume Shadow Copies (VSS).
	GMER	Rootkit detection tool abused to kill AV/EDR
	HRSword	Tool used to obfuscate payloads to hinder analysis.
	IOBit Uninstaller	Tool used to force uninstall software to evade detection.
	Process Hacker	Tool used to terminate or manipulate protected processes.
	Rundll32	Windows utility used to load DLLs that lack an executable; used to bypass security controls.
	Taskkill	Windows utility used to terminate security processes
	wevutil	Windows utility used to manipulate and query Windows event logs

Known Tools

Function	Tool	Description
Credential Access	LSASS	Windows process frequently targeted as it stores credentials in memory.
	Mimikatz	Hacktool used to extract Windows passwords in plain-text from memory.
	Rubeus	Toolset for Kerberos interaction and abuse.
Discovery	AdFind	Tool used to query Active Directory for domain information.
	BloodHound	Tool used to map Active Directory relationships and attack paths.
	Dtrack	AKA LeadLift, Preft, Valefor. Remote access trojan used to identify sensitive information.
	Grixba	Tool used to enumerate users and computers within a domain.
	ipconfig	Windows utility that enumerates network configurations.
	netsh	Windows utility used to enumerate and modify network configuration.
	Ping	Windows utility used to check host reachability.
	SoftPerfect Network Scanner	Tool that scans networks for connected devices, shared folders, and open ports.
	Windows Task Manager	Windows utility used to enumerate processes and performance
Lateral Movement	Impacket	Tool for working with network protocols; frequently abused for lateral movement.
	nltest	Windows utility used to enumerate domain trusts and domain controllers.
	Plink	Tool used to tunnel RDP and SSH traffic.
	PsExec	Command line tool abused to execute a program on another computer.

Known Tools

Function	Tool	Description
Lateral Movement	RDP	Microsoft protocol used to remotely connect to a Windows computer.
Command and Control	Cobalt Strike	Commercial C2 framework abused for post-exploitation
	Empire	PowerShell/Python post-exploitation framework
	Sliver	Cross-platform adversary emulation framework
	SystemBC	AKA Coroxy. Malware used to turn infected computers into SOCKS5 proxies.
Exfiltration	TeraCopy	Free utility used to copy files, which can be abused to steal sensitive data.
	WinRAR	File archiver utility that can backup data, open and unpack RAR, ZIP, and other files from the internet; often used for exfiltrating sensitive data.
	WinSCP	Windows utility abused to transfer files over SFTP/FTP
Impact	VSS Copy Tool	Custom tool for interacting with Windows Volume Shadow Copy Service (VSS).
Infrastructure	GMX	Free email service from Germany often abused for victim negotiation and ransomware operator contacts.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	Execution of ransomware payload via Play.exe / PlayCrypt.exe
		Execution via cmd.exe and powershell.exe
		Remote execution via PsExec.exe
		Abuse of Windows Management Instrumentation (WMI) for process execution
Persistence	Configuration Change	Creation or modification of scheduled tasks
		Service creation for tool or payload execution
Privilege Escalation	Command Execution	Token abuse via SeDebugPrivilege
		Credential reuse to access privileged accounts
		Execution under SYSTEM context via service abuse
Defense Evasion	Command Execution	Shadow copy deletion via vssadmin delete shadows /all /quiet
		Shadow copy deletion via WMI
		Disabling endpoint security services
		Event log clearing via wevtutil
	Configuration Change	Modification of registry keys to weaken security controls
Credential Access	Command Execution	LSASS memory dumping
		Credential harvesting via post-exploitation tooling
	Output/Artifact	LSASS dump files recovered from disk
Discovery	Command Execution	Domain enumeration via nltest
		Account discovery via net user /domain
		Group enumeration via net group /domain

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Discovery	Command Execution	Host discovery via ping and network scanning
		Service and process enumeration
Lateral Movement	Command Execution	Remote execution via PsExec.exe
		SMB administrative share abuse (C$, ADMIN$)
		WMI-based remote process creation
		RDP used for interactive lateral movement
Collection	Command Execution	Data staging using WinRAR.exe or 7zip.exe
		Collection of sensitive files prior to encryption
	Output/Artifact	Staged archives containing business data
Command and Control	Command Execution	Use of Cobalt Strike beacons
		HTTPS-based C2 communications
		Use of commodity remote access tooling
Impact	Command Execution	File encryption across local and network shares
		Deletion of backups and recovery artifacts
	Configuration Change	Disabling system recovery features
	Output/Artifact	Credential harvesting via post-exploitation tooling

Kill Chain

Initial Access

- Exposed RDP and VPN
- Valid Stolen Credentials
- Previously Compromised Environments

Persistence

- New Accounts
- Scheduled Tasks
- Registry Key Changes
- Legitimate Admin Tools

Defense Evasion

- Disable Security Tools
- LOLBins
- Clearing/Suppressing Windows Event Logs

Lateral Movement

- Credential Harvesting
- SMB, RDP, Admin Tools
- Rapid Movement to Active Directory

Exfiltration

- Data Staged Locally
- Legitimate Tool & Cloud Service Abuse
- Sensitive Business Data, Financials, Legal Data

Impact

- Recompiled Binary for Each Attack
- Phone Calls to Victims
- TOR-based Data Leak Sites

MITRE ATT&CK® Mappings

Resource Development	
T1584: Compromise Infrastructure	.005: Botnet
T1587: Develop Capabilities	.001: Malware
T1588: Obtain Capabilities	.002: Tool
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell .004: Unix Shell
T1072: Software Deployment Tools	
T1106: Native API	
T1203: Exploitation for Client Execution	
T1569: System Services	.002: Service Execution

MITRE ATT&CK® Mappings

Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Account	
T1543: Create or Modify System Process	
Privilege Escalation	
T1055: Process Injection	
Defense Evasion	
T1027: Obfuscated Files or Information	.010: Command Obfuscation
T1055: Process Injection	
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1134: Access Token Manipulation	
T1140: Deobfuscate/Decode Files or Information	
T1484: Domain Policy Modification	.001: Group Policy Modification
T1497: Virtualization/Sandbox Evasion	
T1562: Impair Defenses	.001: Disable or Modify Tools
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1056: Input Capture	.001: Keylogging
T1552: Unsecured Credentials	

MITRE ATT&CK® Mappings

Discovery	
T1007: System Service Discovery	
T1012: Query Registry	
T1016: System Network Configurations Discovery	
T1018: Remote System Discovery	
T1033: System Owner/User Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.001: Local Groups .002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.001: Local Account .002: Domain Account
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	.001: Security Software Discovery
T1615: Group Policy Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares

MITRE ATT&CK® Mappings

Lateral Movement	
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1056: Input Capture	.001: Keylogging
T1560: Archive Collected Data	.001: Archive via Utility
Command and Control	
T1071: Application Layer Protocol	
T1090: Proxy	
T1105: Ingress Tool Transfer	
T1219: Remote Access Software	.002: Remote Desktop Software
T1568: Dynamic Resolution	.002: Domain Generation Algorithms
T1572: Protocol Tunneling	
Exfiltration	
T1030: Data Transfer Size Limits	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	.003: Exfiltration Over Unencrypted Non-C2 Protocol
Impact	
T1486: Data Encrypted for Impact	

MITRE ATT&CK® Mappings

Impact
T1489: Service Stop
T1490: Inhibit System Recovery
T1565: Data Manipulation
T1657: Financial Theft

References

- AhnLab (2025, January 02) “Play Ransomware Attack Cases Detected by AhnLab EDR.” https://asec.ahnlab.com/en/85580/
- CISA (2025, June 04) “#StopRansomware: Play Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
- Mateo, Cj Arsley; Virtusio, Darrel Tristan; et. al. (2024, July 19) Trend Micro: “Play Ransomware Group’s New Linux Variant Targets ESXi, Shows Ties With Prolific Puma.” https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html
- Montini, Heloise (2024, January 26) Proven Data: “Play Ransomware: What You Need to Know.” https://www.provendata.com/blog/play-ransomware/
- Souček, Jakub; Holman, Jan (2025, March 26) ESET: “Shifting the sands of Ransomhub’s EDRKillShifter.” https://www.welivesecurity.com/en/eset-research/shifting-sands-ransomhub-edrkillshifter/
- Unit 42 (2024, October 31) “Jumpy Pisces Engages in Play Ransomware.” https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

Adversary Pursuit Group

blackpoint