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)

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.

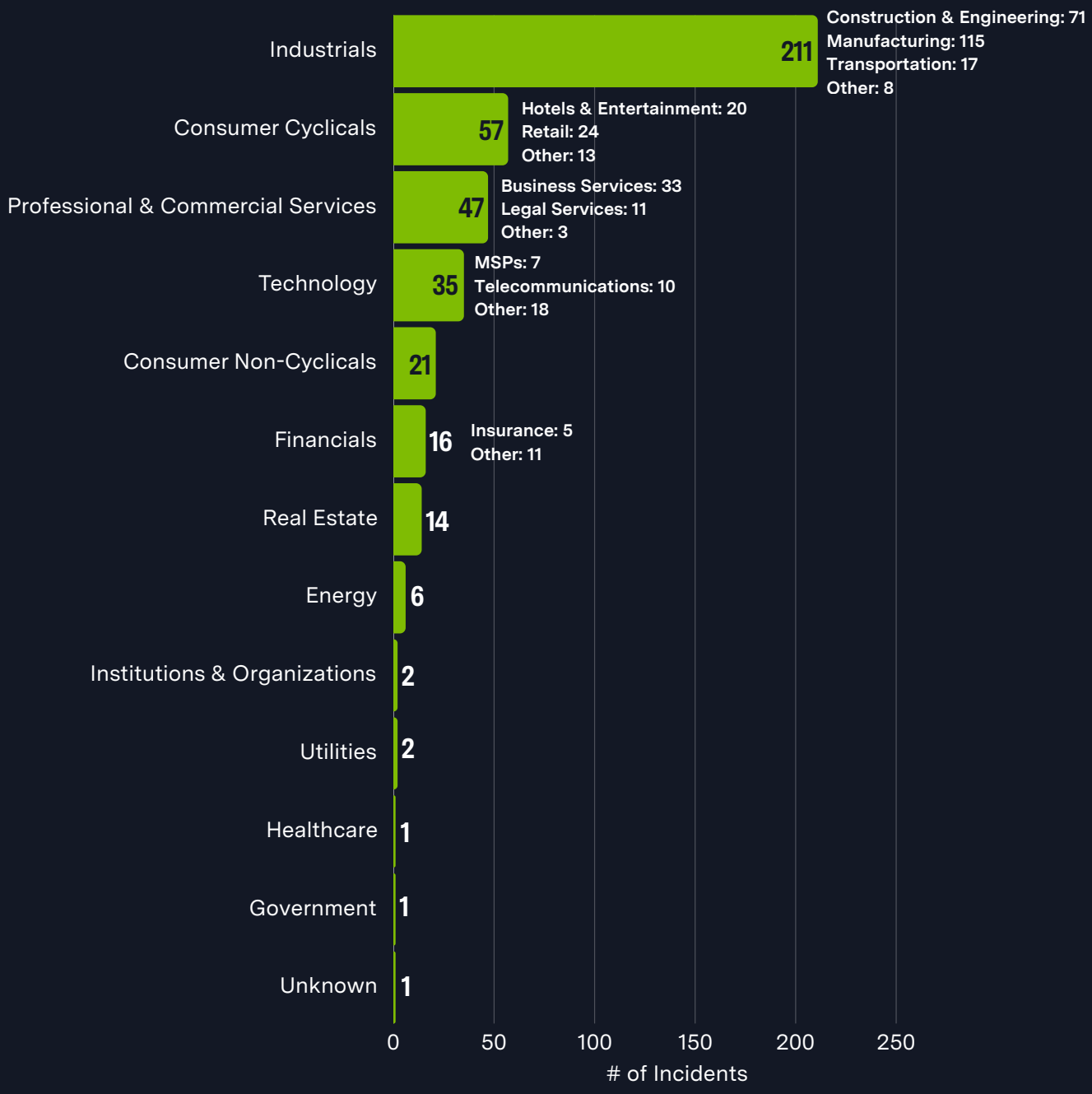
In 2024, Trend Micro security researchers reported that Play ransomware operators had developed and began deploying a Linux variant of the ransomware. The variant only encrypts files when running in a VMware ESXi environment. The identification of a Linux version indicates that the group is likely attempting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

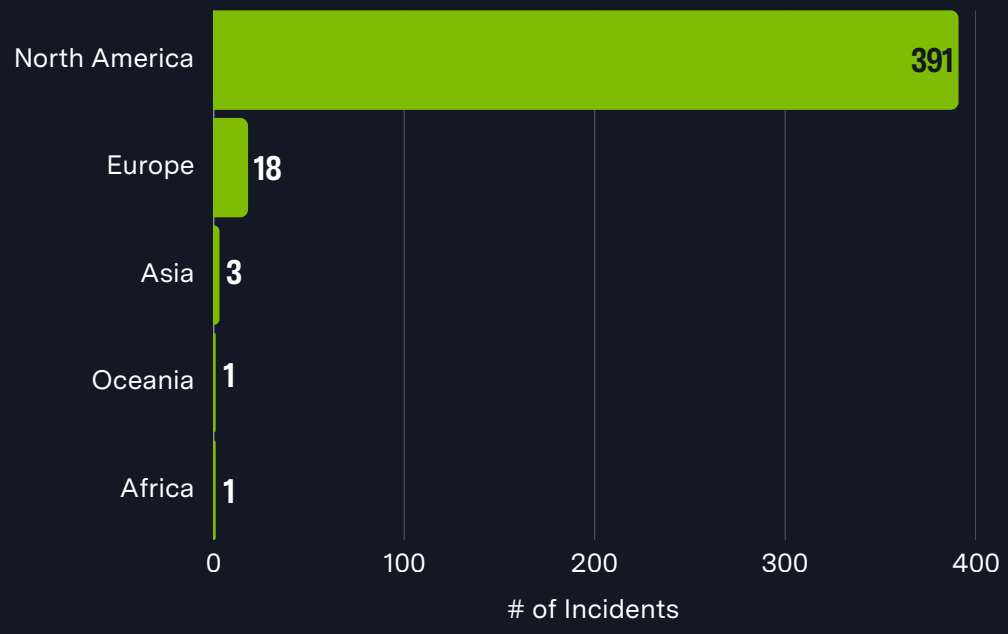
Previous Targets

Previous Industry Targets from 01 Oct 2024 to 30 Sep 2025

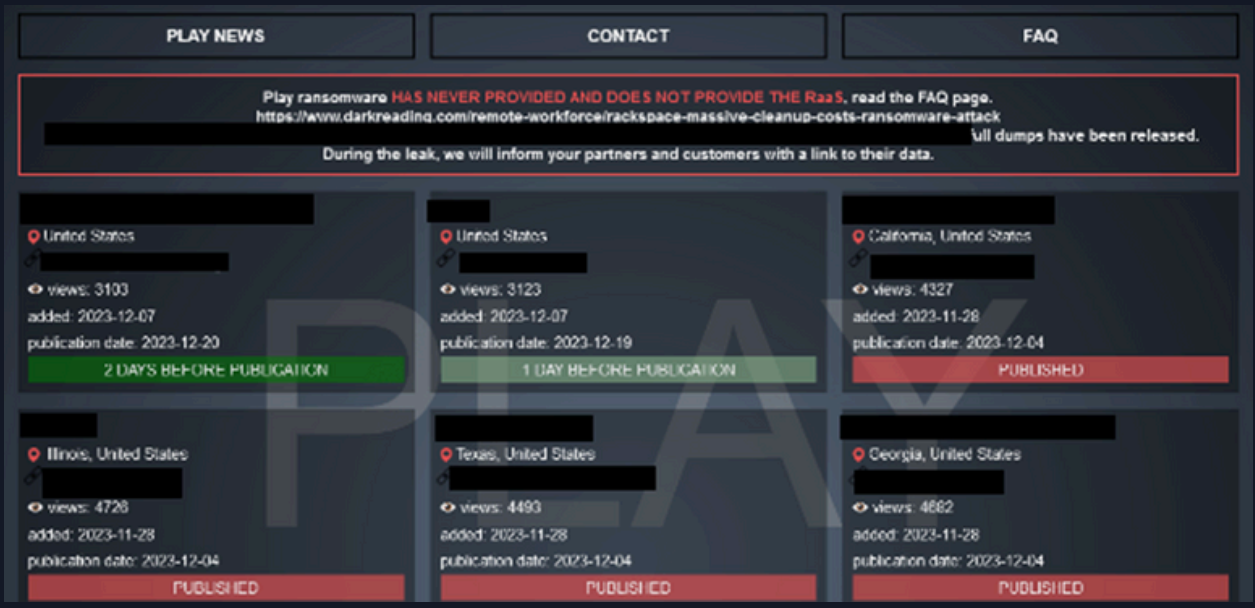


Previous Targets

Previous Victim HQ Regions from 01 Oct 2024 to 30 Sep 2025



Data Leak Site



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

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
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

AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
AlphvVSS	A .NET class library providing a managed API for the Windows Volume Shadow Copy Service (VSS).
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
BloodHound	An Active Directory reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
Cobeacon	A backdoor malware that can execute commands from a remote point and can send and receive information.
Dtrack	AKA LeadLift, Preft, Valefor. A RAT custom created by the Lazarus Group that has been observed in Andariel attacks in 2022. This malware was observed in a Play Ransomware incident reported by Palo Alto.
Empire	An open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure PowerShell for Windows and Python for Linux/macOS.
GMER	A tool used to detect and remove rootkits.
Grixba	A network scanning tool used to enumerate all users and computers in the domain.
HRSword	A security software suite designed to monitor system activity as part of endpoint protection but has previously been abused by ransomware groups to disable endpoint protection systems.

Known Tools

Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
IOBit Uninstaller	A tool used to uninstall software that cannot be uninstalled by Windows or other installers.
ipconfig	A command line utility that is used to display and manage the IP address assigned to the machine.
LSASS	A Windows process that takes care of security policy for the OS.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
Nekto/PriviCMD	A tool used to gain elevated privileges on a compromised network.
NetScan	A utility that scans within a subnet or IP range to check for devices.
netsh	A scripting utility used to interact with networking components on local or remote systems.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.
Ping	A tool used to test whether a particular host is reachable across an IP network.
Plink	A common utility used to tunnel RDP sessions and can be used to establish SSH network connections to other systems using arbitrary source and destination ports.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerTool	A security tool that scans and analyzes files at kernel level; can help threat actors remove and disable security services/software.

Known Tools

Process Hacker	An open-source tool that allows users to see what processes are running on a device and identify network connections that are associated with a process.
PsExec	A utility tool that allows users to control a computer from a remote location.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
Rubeus	A C# toolset for raw Kerberos interaction and abuses.
Rundll32	A command line utility in Microsoft Windows used to run DLLs on the Windows operating system.
SimpleHelp	A RMM software that allows threat actors to maintain remote access to the compromised device.
Sliver	An open source cross-platform adversary emulation/red team framework. It has been increasingly used by threat actors due to the number of tools available, including dynamic code generation, staged and stageless payloads, server C2, and more.
SystemBC	AKA Coroxy. A malware written in C that turns infected computers into SOCKS5 proxies.
Taskkill	A legitimate Windows file that is used by malware to terminate processes on the victims' computer.
TeraCopy	A free utility used to copy files. The tool can also verify copied files to ensure they are identical.
TokenPlayer	A tool used to manipulate and abuse Windows Access Tokens.
VSS Copying Tool	A custom tool that serves as an interface for interacting with Windows Volume Shadow Copy Service ("VSS") over APIs. The tool can enumerate and copy files and folders in a VSS snapshot prior to encryption to serve as backups.

Known Tools

wevutil	A command utility used primarily to register a provider on the computer and can be used to retrieve information about even logs and publishers.
Windows Task Manager	A tool that allows predefined actions to be automatically executed at pre-defined times or after specified time intervals.
WinPEAS	A compilation of local Windows privilege escalation scripts to check for cached credentials, user accounts, access controls, interesting files, registry permissions, service accounts, patch levels, and more.
WinRAR	A trialware file archiver utility for Windows devices that can backup data and reduce the size of email attachments, open and unpack RAR, ZIP and other files downloaded from Internet, and create new archives in RAR and ZIP file format.
WinSCP	A free and open-source SFTP, FTP, WebDAV, S3, and SCP client for Windows that can be used to exfiltrate files to a remote server.
WKTools	A collection of tools that simplify the work with network devices and is often used to explore and modify the Windows Kernel.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Behaviors: Windows

Tactic	Commands Observed
Defense Evasion	SYSTEM\\CurrentControlSet\\services\\eventlog SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\WINEVT\\Channels HKLM\System\ControlSet001\Services\WinDefend DisableRealtimeMonitoring DisableBehaviorMonitoring
Discovery	HKCU\Software\Microsoft\Windows\CurrentVersion whoami users

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	

MITRE ATT&CK® Mappings

Execution	
T1569: System Services	.002: Service Execution
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

MITRE ATT&CK® Mappings

Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1056: Input Capture	.001: Keylogging
T1552: Unsecured Credentials	
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

MITRE ATT&CK® Mappings

Discovery	
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
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	

MITRE ATT&CK® Mappings

Command and Control	
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	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1565: Data Manipulation	
T1657: Financial Theft	

References

- Adlumin (2023, November 21) “PlayCrypt Ransomware-as-a-Service Expands Threat from Script Kiddies and Sophisticated Attackers.” https://adlumin.com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/
- AhnLab (2025, January 02) “Play Ransomware Attack Cases Detected by AhnLab EDR.” https://asec.ahnlab.com/en/85580/
- Avertium (2023, January 04) “AN IN-DEPTH LOOK AT PLAY RANSOMWARE.” https://explore.avertium.com/resource/an-in-depth-look-at-play-ransomware
- CISA (2025, June 04) “#StopRansomware: Play Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
- Guibernau, Francis (2023, December 23) AttackIQ: “Response to CISA Advisory (AA23-352A): #StopRansomware: Play Ransomware.” https://www.attackiq.com/2023/12/23/response-to-cisa-advisory-aa23-352a/
- Imano, Shunichi; Slaughter, James (2022, December 22) Fortinet: “Ransomware Roundup – Play.” https://www.fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware
- Ladores, Don; Silva, Lucas; Burden, Scott; et. al. (2022, September 06) Trend Micro: “Play Ransomware's Attack Playbook Similar to that of Hive, Nokoyawa.” https://www.trendmicro.com/en_za/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
- 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/
- Quorum Cyber (2023, April) “Threat Intelligence Play Ransomware.” https://www.quorumcyber.com/wp-content/uploads/2023/04/QC-Play-Ransomware-Report-TI.pdf
- SOCRadar (2023, June 05) “Dark Web Profile: Play Ransomware.” https://socradar.io/dark-web-profile-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/
- Threat Hunter Team (2023, April 19) Symantec: “Play Ransomware Group Using New Custom Data-Gathering Tools.” https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy
- Trend Micro Research (2023, July 21) “Ransomware Spotlight: Play.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play
- 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