

How Play Achieves Encryption

 guidepointsecurity.com/blog/how-play-achieves-encryption

Jean-Pierre Mouton

August 25, 2026



Background

GuidePoint Security analysts are often called to support and consult on Digital Forensics and Incident Response (DFIR) efforts in remediation, recovery and forensic analysis of ransomware events. Play (also tracked as PlayCrypt) is a ransomware group that has been active since June 2022. Thus far, Play has claimed hundreds of victims across North America, South America and Europe. It usually targets organizations across healthcare, critical infrastructure, manufacturing and education. According to our internal tracking of ransomware trends, as of August 2026, at least 1,200 organizations have been allegedly impacted by the group. This places Play among the most prolific ransomware operations of the past several years.

Play operates under what it characterizes as a “closed” model, a posture the group has explicitly stated on its own data leak site as a means to “guarantee the secrecy of deals.” Unlike the prevailing Ransomware-as-a-Service (RaaS) model, in which a core development team licenses their encryptor to external affiliates who conduct intrusions independently, Play is assessed to conduct its own operations without an external affiliate population. This produces a more consistent and predictable Tactic, Techniques and Procedures (TTP) profile across cases. The group employs a double extortion model, encrypting systems after exfiltrating data and threatening to publish stolen data on their Tor-hosted leak site if ransom is not paid. Ransom notes do not include a payment amount or instructions. Instead, victims are directed to contact the group via a victim-specific @gmx[.]de or @web[.]de email address and a portion of victims subsequently receive telephone calls from threat actors encouraging payment.

An early 2026 digital forensics and incident response (DFIR) case reflects the group’s documented playbook with notable fidelity. It is notable both for confirming what defenders

should expect from Play and for the forensic artifact detail it provides that is rarely available in public reporting.

Attack Overview

The first indications of the attack, from the defender's perspective, were widespread encryption of files across the environment and the discovery of ransom notes dropped in affected directories. Encrypted files bore the .PLAY extension characteristic of Play ransomware. Additionally, ReadMe.txt ransom notes were discovered on multiple compromised systems. A Windows Defender detection, Behavior:Win32/GenRansom.SA!rsm, fired on a domain controller during the encryption event, which is an indication that endpoint protection had not been fully neutralized across all hosts at the time of execution. Shortly before encryption began, the Security event log on web servers had been cleared. This is a deliberate anti-forensic measure designed to complicate the reconstruction of attacker activity and a hallmark of a sophisticated operator seeking to limit defenders' ability to reverse their tactics post-incident.

In this case, Play followed its documented playbook closely. The threat actor gained initial access via a compromised SonicWall VPN, consistent with the group's well-documented pattern of exploiting external remote services. What makes this case particularly instructive for defenders is the combination of three specific behaviors:

1. Domain-wide tool staging via the SYSVOL share rather than per-host delivery,
2. EDR removal using the victim's own SentinelOne uninstallation utility rather than a kernel-level driver exploit and
3. The recovery of a crash dump from a host where the encryptor failed to complete, an artifact that provides a rare forensic window into the encryption execution itself.

Together, these details offer defenders concrete, behavioral detection opportunities that extend beyond file hashes.

Initial Access

Forensic analysis revealed that the initial point of entry was a SonicWall VPN. The presence of SonicWall software was confirmed on the web server via Shellbag artifacts, which showed the attacker browsing the path \\[redactedIP][redactedDirectory]\$ -> Program Files -> SonicWall on a compromised workstation. The earliest attacker-attributed logon was observed two and half months prior to encryption. It originated from a host identified as WINNITHERLANDS, which is an attacker-controlled Windows machine. A Linux-based attack platform identified as kali was also observed in logon artifacts, consistent with the use of dual

operating environments commonly seen in hands-on-keyboard intrusions. We have observed a pattern of Play exploiting externally facing network appliances and remote access solutions for initial access, making the SonicWall VPN a credible and consistent entry point for this group.

Persistence and Command and Control

After gaining access to the victim's environment, the threat actor deployed SystemBC as the primary Command and Control (C2) backdoor. SystemBC is a proxy-based malware that uses an encrypted SOCKS5 tunnel to route communications, allowing the threat actor to maintain persistent access while obscuring the origin of their traffic. It has been documented in Play ransomware campaigns by both [CISA](#) and Symantec and its use here is consistent with the group's established toolkit. SystemBC was installed as a .DLL within the Windows Tasks directory, a location that benefits from lower monitoring scrutiny than more commonly targeted paths: It is worth noting that SystemBC is not exclusive to Play. It has been observed in campaigns attributed to Conti, ALPHV/BlackCat and other groups, but its consistent presence in Play intrusions is specifically documented by both CISA and Symantec and serves as a reliable behavioral indicator when observed alongside other Play TTPs.

C:\Windows\Tasks\4.dll

SHA256: 5717e8064affa943e6ed5476e8616ac2b295c3a4513b3f4d941001f4db283a1c

C:\Windows\Tasks\svhost.dll

C:\Windows\Tasks\svhost_V1.dll

C2: 45.32.78[.]243 (Vultr Holdings)

A PowerShell script, vu1fijb0.on3.ps1, was also identified under C:\Windows\Temp\, likely used for payload staging or lateral movement setup. Separately, WinSCP was staged at C:\PerfLogs\WinSCP.exe in preparation for the data exfiltration phase discussed below. The use of C:\PerfLogs\ as a staging directory is a recurring behavior in Play intrusions. The directory is a low-traffic location that is rarely subject to file creation alerting and is not cleared by default Windows maintenance processes, making it an effective staging ground that may persist unnoticed for extended periods.

Reconnaissance and Lateral Movement

With a stable C2 channel established, Play pivoted to credential access and lateral movement. It follows the methodical staging pattern consistent with Play's documented intrusion template. Mimikatz was deployed at C:\Users\

[redacted]\AppData\Local\Temp\mimikatz.exe to dump credentials from memory, providing the threat actor with the credentials needed to move freely across the environment under the guise of legitimate user accounts. Notably, the Mimikatz binary was deployed under its original filename rather than a renamed variant. Most sophisticated operators rename credential dumping tools in an effort to evade process-name-based detection, making the unmodified filename a useful hunt signal in this case. Forensic artifacts on web servers showed the compromised account conducting extensive enumeration of the environment's Hyper-V infrastructure . This activity indicated the attacker was actively mapping virtual machine inventory as well as browsing network shares across multiple servers.

The tool PsExec was then used to facilitate lateral movement and, ultimately, encryptor distribution. Rather than deploying PsExec on a per-host basis, the threat actor distributed it via the domain's SYSVOL share, a domain-wide accessible path that allowed a single staging action to make the tooling available to all domain-joined systems simultaneously. MFT and Prefetch artifacts on an end-user device confirmed the execution of multiple PsExec variants (see Technical Details). The attacker's activity was observed across multiple hosts indicating broad lateral movement prior to the encryption event.

C:\Users\[redacted]\AppData\Local\Temp\mimikatz.exe

C:\Windows\PSEXESVC.exe — created 05:28:00Z

SYSVOL\PerfLogs\PSEXEC.exe — ShimCache

SYSVOL\PerfLogs\PSEXEC64.exe — ShimCache

SHA1 PsExec.exe: a0ee0761602470e24bcea5f403e8d1e8bfa29832

SHA1 PsExec64.exe: 0098c79e1404b4399bf0e686d88dbf052269a302

SHA1 PSEXESVC.exe: 2c27a865b3ab1f0bd2ea1e8f7298b5ef9348c5ac

SHA256 PsExec64:

5910b49c041b80f6e8d2e8e10752a9062febe4a2edd15f07c6b1961b3c79c129

Data Exfiltration

Prior to initiating encryption, the TA conducted a systematic data staging and exfiltration operation. Play used WinSCP, a legitimate SFTP/SCP/FTP client widely used in IT administration, to transfer data to an attacker-controlled server. UserAssist artifacts on a web server confirmed that WinSCP was executed by the compromised account at 04:51:32Z on the day of the incident and Shellbag artifacts on a separate server showed WinSCP had also

been distributed to \\[redactedIP]\redactedDirectory]\PerfLogs\, indicating the tool was pushed to multiple hosts via PsExec or SYSVOL in preparation for a coordinated exfiltration effort across the environment.

Data was archived using WinRAR. It was installed via C:\PerfLogs\winrar-x64-611.exe, and staged in the C:\PerfLogs\ and F:\PerfLogs\ directories. LNK and JumpList artifacts on the web server confirmed the attacker's access to and staging of a broad range of sensitive data, including archives corresponding to financial records, human resources data, client data, bank statements and corporate documentation. Multi-part RAR archives observed on the web server included:

F:\PerfLogs\Accounting.part12.rar

F:\PerfLogs\HR.part2.rar – HR.part6.rar

F:\PerfLogs\CLIENTS.part07.rar, CLIENTS.part09.rar, CLIENTS.part10.rar

F:\PerfLogs\[redacted] Document Libraries.rar

F:\PerfLogs\[redacted].rar

C:\PerfLogs\Accounting.rar

C:\PerfLogs\Budget.rar

C:\PerfLogs\Bank Statements.rar

C:\PerfLogs\[redacted] Financial Audit Reports.rar

C:\PerfLogs\HR.rar

C:\PerfLogs\CLIENTS.rar

Exfiltrated data serves as independent leverage, ensuring that even organizations capable of recovering from backups face pressure to comply with ransom demands to prevent public data disclosure. Play maintains a public-facing data leak site on which non-paying victims are posted alongside proof-of-exfiltration samples. Play is assessed to operate under a closed model, which is distinct from the Ransomware-as-a-Service (RaaS) structure in which a core developer team licenses their encryptor to external affiliates who conduct intrusions independently. A closed model means the group conducts its own operations, which in practice produces a more consistent and predictable TTP profile. Because Play does not rely on a rotating pool of affiliates with varying techniques and tooling preferences, the group's intrusions tend to follow a repeatable playbook. This makes behavioral detection more reliable

as a primary hunting hypothesis than signature-based detection alone. Defenders familiar with Play's patterns can generate high-confidence rules around specific behaviors (for example, SYSVOL-based tool staging, C:\PerfLogs\ as a staging directory, SystemBC in the Tasks directory) rather than chasing individual file hashes.

It is also worth noting that open-source reporting has identified a possible relationship between Play ransomware and Jumpy Pisces (also tracked as Andariel and Onyx Sleet), a threat actor attributed to North Korea's Reconnaissance General Bureau. [Unit 42 documented](#) this connection in September 2024, assessing it as the first known instance of a DPRK-nexus actor acting as an affiliate of or in collaboration with, a non-DPRK ransomware group. Whether Jumpy Pisces operated as a full affiliate or leveraged Play's encryptor as a financial instrument, the precise nature of this relationship remains an active area of research. Its existence complicates the closed-group narrative and warrants continued monitoring.

Defense Evasion

With lateral movement complete and data staged for exfiltration, Play moved to neutralize endpoint protection and eliminate forensic evidence before detonating the encryptor. This pre-encryption cleanup sequence is characteristic of Play operations. The SentinelOne security platform was disabled using a tool identified as SentinelCleaner.exe. The victim organization's own SentinelOne uninstallation utility, which was repurposed as an Endpoint Detection and Response (EDR) "killer." This technique of using a vendor's own legitimate tooling to remove their product is distinct from Bring Your Own Vulnerable Driver (BYOVD) attacks, which weaponize a signed but vulnerable kernel driver to terminate security processes from the kernel level. Here, the attackers did not require a driver or kernel exploit. Instead, they obtained and executed the vendor's own removal tool, which by design has the necessary privileges to cleanly uninstall the product. This reflects an increasing trend in which threat actors research and leverage vendor-specific removal utilities as a more reliable and less detectable alternative to BYOVD or direct process termination. This technique, of abusing legitimate vendor tools to remove the EDR, has been observed in campaigns linked to other ransomware groups including Akira, but its presence in Play intrusions is particularly consistent and warrants specific defensive attention: enabling vendor-authenticated tamper protection, a setting that requires authentication with the security vendor before uninstallation is permitted, would have prevented this evasion path entirely.

C:\Windows\Temp\S1_3188D2ADBF43458B98D8018E4F44D92D\temp_content\SentinelCleaner.exe

SHA256: e81ca38e710a63bb68d2bc7bf1a7b0f0f9f30d141afa9c38a9fb8a161e23b1bb

Following EDR removal, Play cleared the Windows Security event log on the web server (EventID 1101), approximately twelve minutes after the first confirmed encryptor execution on an user workstation`. Event log clearing immediately prior to or during encryption deployment is a deliberate anti-forensic measure that limits an incident response team's ability to reconstruct the attack timeline and identify the full scope of lateral movement. The presence of EventID 1102 is itself a high-fidelity indicator of pre-encryption activity and should be treated as a critical alert in any environment where it fires outside of routine administrative operations.

Another tool, GoGo.exe, was also identified at both C:\PerfLogs\GoGo.exe and SYSVOL\PerfLogs\GoGo.exe. GRIT assesses that the tool served as an encryptor deployment tool used in conjunction with PsExec to orchestrate execution across domain-joined systems, though it was no longer present on hosts at the time of forensic analysis.

Actions on Objective

Encryptor execution was confirmed via UserAssist artifacts on the web server, which showed a second compromised account interactively executing C:\PerfLogs\mmm.exe. The encryptor was distributed under multiple filenames (mmm.exe, IHDpr3.exe, 8gh2dA.exe and hi.exe) all sharing the same SHA256 hash and file size of 492,544 bytes, confirming they are the same binary. The use of multiple filenames is consistent with a distribution strategy designed to reduce the likelihood of hash-based detection blocking execution on hosts where the binary was deployed under an alternate name.

C:\PerfLogs\mmm.exe

C:\Users\Public\Music\IHDpr3.exe

C:\Users\Public\Music\8gh2dA.exe

C:\PerfLogs\hi.exe

SHA256: c597377f3cd349a07d46483e130952a566c4bda73d9771b54b7ce8a9901c4c76

A crash dump, C:\Users\[redacted]\AppData\Local\CrashDumps\mmm.exe.35408.dmp, indicates the encryptor process crashed on at least one host, which may have partially limited the scope of encryption on that system. The Windows Defender detection Behavior:Win32/GenRansom.SA!rsm firing on the domain controller further suggests that EDR removal was not fully completed across all hosts prior to execution. These unforeseen issues with encryptor execution limited the threat actor's reach, though not sufficiently enough to prevent widespread encryption.

Encrypted files had the .PLAY extension appended and ReadMe.txt ransom notes were created in impacted directories, directing the victim to contact the group via a unique email address. The ransom note is reproduced below:

Ransom Note

Technique	Tool/Activity	ATT&CK ID	Details
External Remote Services	SonicWall VPN exploitation	T1133	Assessed initial access vector based on victim infrastructure and Play TTPs
Valid Accounts	Compromised domain credentials (CWhite, fcampbell)	T1078	TA operated under legitimate accounts throughout the intrusion
OS Credential Dumping: LSASS Memory	Mimikatz	T1003.001	Credential harvesting prior to lateral movement
Proxy / C2	SystemBC (4.dll, svhost.dll)	T1090.001	C2 traffic proxied through 45.32.78[.]243 (Vultr)
Remote Services: PsExec	PsExec.exe / PsExec64.exe	T1021.002	Lateral movement and encryptor distribution
Group Policy Modification	SYSVOL-based tool staging	T1484.001	Domain-wide tool distribution via SYSVOL share
System Information Discovery	Shellbag / Hyper-V enumeration<	T1082	Attacker enumerated VM inventory and network shares

Technique	Tool/Activity	ATT&CK ID	Details
Network Share Discovery	Shellbag artifacts, MountPoints2	T1135	CWhite account used to enumerate network shares
Archive Collected Data	WinRAR	T1560.001	Data staged as multi-part RAR archives in C:\PerfLogs\
Exfiltration Over Alternative Protocol	WinSCP to attacker-controlled server	T1048	Large-volume exfiltration of financial, HR and client data
<u>Disable or Modify Security Tools</u>	SentinelCleaner.exe	T1562.001	SentinelOne uninstall utility leveraged to strip EDR pre-encryption
Clear Windows Event Logs	Security EventID 1102	T1070.001	Audit log cleared on ISTSVWEB08 immediately before encryption
Data Encrypted for Impact	mmm.exe / IHDpr3.exe / 8gh2dA.exe	T1486	Play encryptor deployed across domain-joined systems

[Jean-Pierre Mouton](#)

Jean-Pierre Mouton is a Consultant and GuidePoint University Fellow on GuidePoint Security's Research and Intelligence Team (GRIT), where he engages in incident response investigations and threat intelligence research on behalf of the firm and its clients. His career background includes strategic and tactical intelligence analysis, technical subject matter expertise and intelligence program management in the Department of Defense and the United States Navy.