# An In-Depth Look at Play Ransomware

avertium.com/resources/threat-reports/an-in-depth-look-at-play-ransomware


Executive Summary

Play ransomware (also known as PlayCrypt) is a new ransomware operation that launched in June 2022. The operation has amassed a steady stream of victims across the world. Play has recently been in the news for attacking Argentina's Judiciary of Cordoba and the German hotel chain "H-Hotels". Play's attacks focus on organizations in the Latin American region – Brazil being their primary target. They have also been observed deploying attacks on India, Hungary, Spain, and the Netherlands.

Play is known for their big game hunting tactics, such as using Cobalt Strike for post-compromise and SystemBC RAT for persistence. They have recently started exploiting the ProxyNotShell vulnerabilities in Microsoft Exchange. The group also has similar tactics and techniques to the ransomware groups Hive and Nokoyawa, leading researchers to believe Play is operated by the same people. Let's take a look at Play ransomware, their tactics and techniques, as well as how organizations can protect themselves from this kind of threat actor.

**TIR Snapshot**

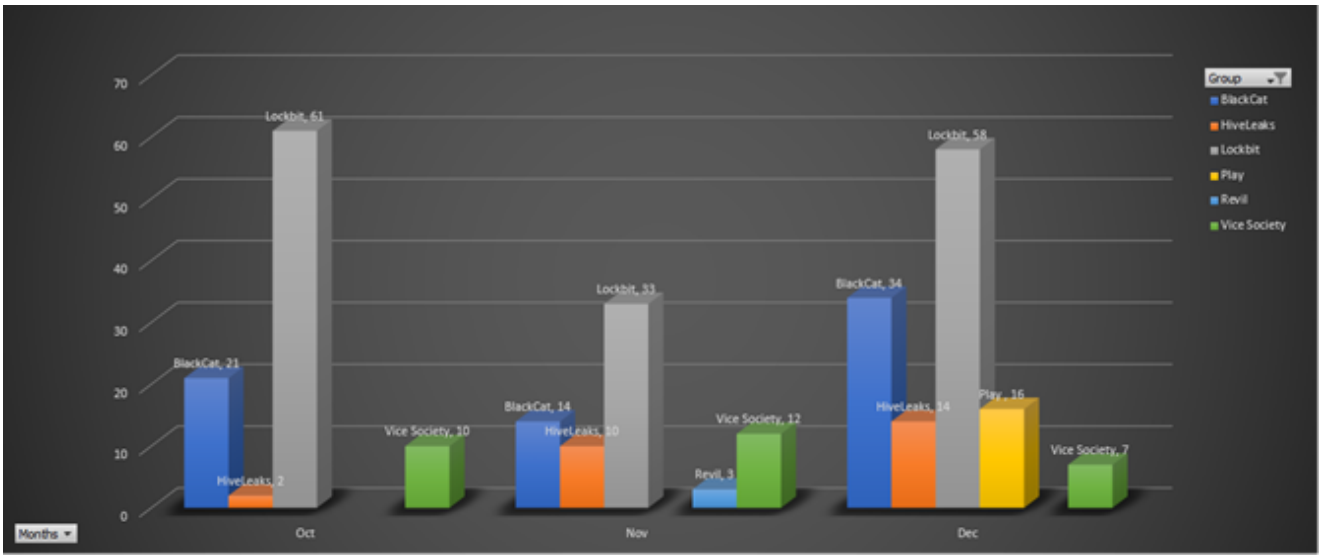
- Play was discovered in June 2022 after several victims of their ransomware attacks appeared in Bleeping Computer forums.
- Not long after victims started reporting attacks in Bleeping Computer forums, Play targeted Argentina's Judiciary of Cordoba.
- Towards the end of December 2022, Play was observed using a method to exploit two ProxyNotShell vulnerabilities in Microsoft exchange to gain initial access in environments.
- Play has similar behavior and tactics to HIVE and Nokoyawa ransomware. The threat actor was observed using similar file names and file paths of their respective tools and payloads.
- Play's infection chain includes using compromised valid accounts or unpatched Fortinet SSL VPN vulnerabilities to gain access to organization's networks.
- There are some best practices that can help protect organizations and end users from Play, including: securing backups, minimizing the use of administrator accounts, and blocking or restricting the use of psexec within your environment.

## play ransomware

Play was discovered in June 2022 after several victims of their ransomware attacks appeared in Bleeping Computer forums. Play's ransomware name stems from its behavior, as the extension **.play** is added after file encryption. The ransomware note left behind also contains the single word **PLAY**, as well as the group's contact email address.

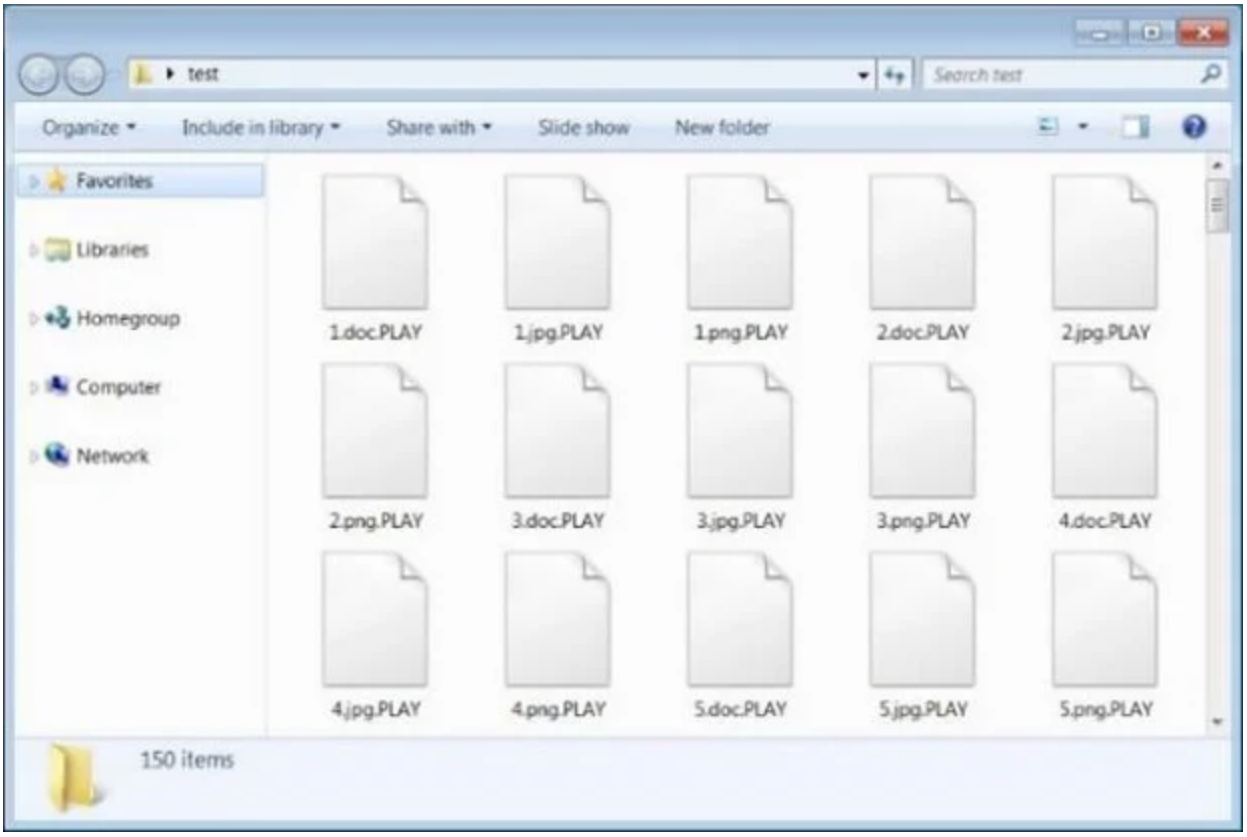
Not long after victims started reporting attacks in Bleeping Computer forums, Play targeted Argentina's Judiciary of Cordoba. The attack took place in August 2022 and the Judiciary had to shut down their IT systems, as well as their online portal as a result. The Judiciary was forced to use pen and paper for submitting official documents. The Argentinian publication, ***Clarin,*** reported that the attack was the "worst attack on public institutions in history."

Image 1: Play Ransomware Activity Compared to Other Ransomware Groups




Although the Judiciary did not go into detail, journalist Luis Ernest Zegarra confirmed via Twitter that the Judiciary was hit by ransomware that appends the **.play** extension to encrypted files. The ransomware note that Play leaves behind is not lengthy and is unusually simple. The note is only made at the root of a hard dive (C:\) and only contains the word **PLAY** and an email address for victims to contact. This kind of simplicity is not usual for ransomware operators.

Image 2: Encrypted Files




*Source: Bleeping Computer*

Although not confirmed, researchers suspect that Play was able to breach the Judiciary via a list of leaked Globant employee email addresses. The attack on Globant took place in March 2022 and the leaked email addresses may have allowed Play to launch a phishing attack to steal credentials.

Image 3: Globant's Breach


*Source: Twitter*

## tactics & techniques

### PROXYNOTSHELL

Towards the end of December 2022, Play was observed using a method to exploit two ProxyNotShell vulnerabilities in Microsoft exchange to gain initial access in environments. The ProxyNotShell flaws are:

- **CVE-2022-41040** – Microsoft Exchange Server Elevation of Privilege Vulnerability

- **CVE-2022-41082** – Microsoft Exchange Server Remote Code Execution Vulnerability

The flaws impact Exchange Server 2013, 2016, and 2019. If successful, an attacker could exploit ProxyNotShell to elevate privileges to run PowerShell in the context of the system, gaining arbitrary or remote code execution on vulnerable servers. Although the vulnerabilities were patched by Microsoft in November 2022, Play was able to bypass URL rewrite mitigations for the Autodiscover endpoint implemented by Microsoft.

Next, Play was able to leverage legitimate Plink and AnyDesk executables to maintain access. They also performed anti-forensics techniques on the server, attempting to hide their activity. The security researchers at CrowdStrike investigated several Play ransomware intrusions where they suspected the threat actors used ProxyNotShell as their entry vector. However, after analyzing and after reviewing their logs, they determined that there was no evidence of exploitation of CVE-2022-41040 for initial access but "corresponding requests were made directly through the Outlook Web Application (OWA) endpoint - signifying a previously undisclosed exploit method for Exchange."

According to Security Affairs, a security researcher from Huntress Labs discovered Play's tool set and shared it through MegaUpload. The tools include a Python script "**poc.py**" (which led CrowdStrike to replicate the logs generated in recent Play ransomware attacks).

## CONNECTIONS TO OTHER GROUPS

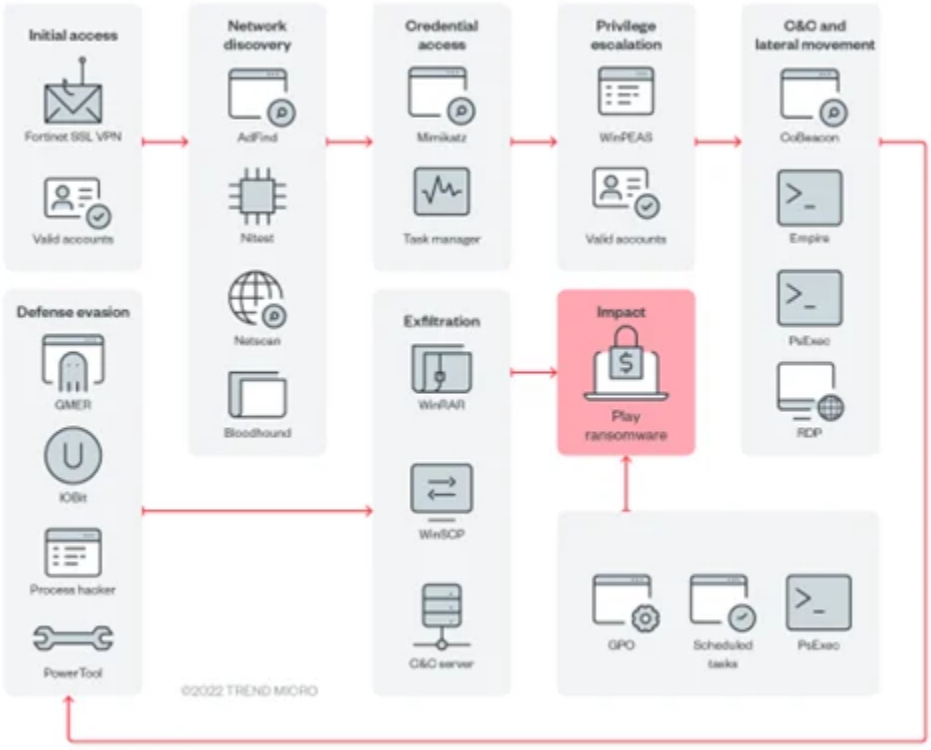
As previously stated, Play's name originated from the **.play** extension that is added after encrypting files. The threat actors have similar behavior and tactics to HIVE and Nokoyawa ransomware. The threat actor was observed using similar file names and file paths of their respective tools and payloads. Trend Micro also found evidence hinting that the operators behind Nokoyawa are associated with the operators behind HIVE, as there are many similarities between their attack chains.

One of the ways that Play is set apart from HIVE and Nokoyawa is through their use of AdFind – a command-line query tool which collects information from Active Directory (AD). HIVE has been observed using tools such as the TrojanSpy.DATASPY trojan to gather victim information. Play, HIVE, and Nokoyawa may not share all the same indicators, but their shared tactics and tools indicate that they are affiliated in some way.

Trend Micro also found evidence of a possible connection between Play and Quantum ransomware. Quantum is known for being a splinter group of Conti. The ransomware operation was taken over by Conti Team Two in April 2022, but the group kept Quantum's original name. Quantum is also known for employing their version of BazarCall, called Jormungandr, and hiring people who specialize in OSINT, spamming, design, and call center operations.

Trend Micro's researchers stated that the Cobalt Strike beacons used in Play's attacks, have the same watermark that was dropped by the Emotet and SVCReady botnets – two botnets that have been observed in Quantum ransomware attacks.

Image 4: Play Infection Train




*Source: Trend Micro*

As you can see above, Play's infection chain includes using compromised valid accounts or unpatched Fortinet SSL VPN vulnerabilities to gain access to organization's networks. They use living-off-the-land binaries (LOLBins) during their attacks (i.e., using WinSCP for data exfiltration and Task Manger for Local Security Authority Server Service for dumping and credential cracking). Like other ransomware gangs, Play uses the double extortion model against their victims. The threat actor exfiltrates data before deploying their ransomware and archives the victim's files using WinRAR before uploading them to sharing sites.

Regarding execution, Trend Micro observed Play using scheduled tasks and PsExec during execution. The ransomware gang also creates a GPO, which can control user and machine settings in the AD. Play uses batch files to execute PsExec, which executes processes on other systems and allows the spread of the ransomware. This also assists Play in its reconnaissance activities.

After gaining access to accounts, Play uses the accounts as a persistence mechanism. If Remote Desktop Protocol (RDP) is disabled on their victim's system, Play will enable it by executing "**netsh**" commands – establishing inbound connects within the victim's system. Next Mimikatz is used to extract high privilege credentials from memory. To avoid detection, GMER, IOBit, Process Hacker, and PowerTool is used to disable antivirus tools and monitoring solutions. Wevtutil or a batch script is used to remove indicators that show Play was present in a system, while Windows Defender is disabled through PowerShell or command script.

Play uses the following tools to move laterally across a victim's system:

- Cobalt Strike SMB beacon
- SystemBC
- Empire
- Mimikatz

To avoid triggering network data transfer, Play splits victim data into chunks before exfiltration. To compress the files in **.RAR** format, they use WinRaR.

## what organization's can do

here are some best practices that can help protect organizations and end users from ransomware operators such as Play, those best practices include:

- If running Exchange servers, ensure they are fully patched and running on Windows Server 2019. Or move to M365 and a fully hosted environment.
- Block or restrict the use of **psexec** within your environment.
- Minimize the use of administrator accounts (at both the local and domain level). All domain administrators should have standard accounts for day-to-day use and additional administrator accounts that are only used when required.
- Use Data Loss Prevention (DLP) software to detect and block aggregation and exfiltration of sensitive data.
- Where possible disable the use of Remote Desktop Protocol via GPO and do not allow users to install other remote access software.
- Back up all data and test those backups regularly. Even if you become the victim of a ransomware attack, your business operations won't be severely interrupted, and your data will be retrievable.
- Install updates regularly – maintain patch management protocols and keep your operating systems and applications up to date. This action will deter threat actors from exploiting software vulnerabilities.
- Using phishing resistant MFA on all accounts, especially VPNs, webmail, and accounts with access to critical systems will prevent attackers from performing lateral movement inside a network.

- Deploy and monitor Endpoint Detection and Response or antivirus software and ensure that your analysts are trained to determine at what point of the cyber attack the detection relates to.

Remember, relying on outdated tools and point solutions will only compromise your network or system. Organizations should rely on modern technology to detect complex attacks.

## How Avertium is Protecting Our CUSTOMERS

Because the cyber landscape is always changing, it is imperative to be aware of new cyber attack strategies and techniques. Avertium is here to keep you informed and to keep your organization safe. **We recommend the following services for the best protection against ransomware attacks:**

Avertium offers VMaaS to provide a deeper understanding and control over organizational information security risks. If your enterprise is facing challenges with the scope, resources, or skills required to implement a vulnerability management program with your team, outsourced solutions can help you bridge the gap.

- Fusion MXDR is the first MDR offering that fuses together all aspects of security operations into a living, breathing, threat-resistant XDR solution. By fusing insights from threat intelligence, security assessments, and vulnerability management into our MDR approach, Fusion MXDR offers a more informed, robust, and cost-effective approach to cybersecurity – one that is greater than the sum of its parts.

- Avertium offers Zero Trust Architecture, like AppGate, to stop malware lateral movement.

- It is also recommended by **Avertium and the FBI** that your business require multi-factor authentication (MFA) to remotely access networks.
  Implementing network segmentation and filtering network traffic to stop phishing emails from reaching victims is also helpful.

Reach out to your **Service Delivery Manager or Account Executive** if you need assistance applying any of the above recommendations.

## avertium's recommendations

**The FBI and CISA urge all organizations to apply the following recommendations to prepare for, mitigate/prevent, and respond to ransomware incidents:**

- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).

- Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.

- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.

- Segment networks to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.

- Consider adding an email banner to emails received from outside your organization.

- Disable command-line and scripting activities and permissions. Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.

## MITRE Map

| Execution | Defense Evasion | Collection | Command and Control | Exfiltration |
|---|---|---|---|---|
| T1106: Native API | T1027: Obfuscated Files or Information | T1056: Input Capture | T1090: Proxy | T1030: Data Transfer Size Limits |
| | T1140: Deobfuscate/Decode Files or Information | | | |
| | T1055: Process Injection | | | |

## Indicators of Compromise (IoCs)

**Hashes**

- 223eff1610b432a1f1aa06c60bd7b9a6
- 14177730443c65aefeeda3162b324fdedf9cf9e0
- 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55
- 0ba1d5a26f15f5f7942d0435fa63947e
- 223eff1610b432a1f1aa06c60bd7b9a6
- b8a152a840702e5d5707aa425da1f70e
- e9dc058440d321aa17d0600b3ca0ab04
- fb8535e2bd80cc8044c52a3ed82d390d
- 0c7ff504e91f28a5d8adfc0e9aaf6cfb53fdc749
- 14177730443c65aefeeda3162b324fdedf9cf9e0
- 4b9b2d86bbd1c67a582ac6042dd93e42df601517
- 539c228b6b332f5aa523e5ce358c16647d8bbe57
- 92284cdbefe3fe21a57aa1b0fba23dbca16069eb
- 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55
- 094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde
- 3e6317229d122073f57264d6f69ae3e145decad3666ddad8173c942e80588e69
- 5573cbe13c0dbfd3d0e467b9907f3a89c1c133c774ada906ea256e228ae885d5
- 608e2b023dc8f7e02ae2000fc7dbfc24e47807d1e4264cbd6bb5839c81f91934
- 7d14b98cdc1b898bd0d9be80398fc59ab560e8c44e0a9dedac8ad4ece3d450b0
- 8962de34e5d63228d5ab037c87262e5b13bb9c17e73e5db7d6be4212d66f1c22
- c316627897a78558356662a6c64621ae25c3c3893f4b363a4b3f27086246038d
- c88b284bac8cd639861c6f364808fac2594f0069208e756d2f66f943a23e3022
- dcaf62ee4637397b2aaa73dbe41cfb514c71565f1d4770944c9b678cd2545087
- e1c75f863749a522b244bfa09fb694b0cc2ae0048b4ab72cb74fcf73d971777b
- e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173
- f5c2391dbd7ebb28d36d7089ef04f1bd9d366a31e3902abed1755708207498c0

**IP Address**

- 84[.]32[.]190[.]37
- 185[.]150[.]117[.]186

**URLs**

- hxxp://185[.]150[.]117[.]186:80/asdfgsdhsdfgsdfg'
- hxxp://84[.]32[.]190[.]37:80/ahgffxvbghgfv
- hxxp://84[.]32[.]190[.]37:80/ahgffxvbghgfv'
- hxxp://newspraize[.]com
- newspraize[.]com
- realmacnow[.]com
- hacktool[.]win32[.]toolpow[.]sm
- hxxp://realmacnow[.]com

## Supporting Documentation

Acuerdo Reglamentario 1778 A 15 08 2022 Plan de Contigencia Ciberatque PJ | PDF | Justicia | Crimen y violencia (scribd.com)

Argentina's Judiciary of Córdoba hit by PLAY ransomware attack (bleepingcomputer.com)

Play ransomware claims attack on Belgium city of Antwerp (bleepingcomputer.com)

They denounce that they hacked the Judicial Power of Córdoba: it affects the website, the systems and the database (clarin.com)

Play Ransomware Group Using New ProxyNotShell Exploit | Decipher (duo.com)

How to Prevent Ransomware Attacks: Top 10 Best Practices in 2022 | UpGuard

Play ransomware claims attack on German hotel chain H-Hotels (bleepingcomputer.com)

Play Ransomware's Attack Playbook Similar al de Hive, Nokoyawa | (ogdi.org)

An In-Depth Look at Quantum Ransomware (avertium.com)

Play Ransomware Attack Playbook Similar to that of Hive, Nokoyawa - AlienVault - Open Threat Exchange

Play Ransomware Attack Playbook Similar to that of Hive, Nokoyawa (trendmicro.com)

Play ransomware attacks use a new exploit to bypass ProxyNotShell mitigations on Exchange serversSecurity Affairs

OWASSRF: CrowdStrike Identifies New Method for Bypassing ProxyNotShell Mitigations

## APPENDIX II: Disclaimer

*This document and its contents do not constitute, and are not a substitute for, legal advice. The outcome of a Security Risk Assessment should be utilized to ensure that diligent measures are taken to lower the risk of potential weaknesses be exploited to compromise data.*

*Although the Services and this report may provide data that Client can use in its compliance efforts, Client (not Avertium) is ultimately responsible for assessing and meeting Client's own compliance responsibilities. This report does not constitute a guarantee or assurance of Client's compliance with any law, regulation or standard.*


**Related Resource:** 2023 Cybersecurity Landscape: 8 Lessons for Cybersecurity Professionals