JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-352A

December 18, 2023

#StopRansomware: Play Ransomware

SUMMARY

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

Actions to take today to mitigate cyber threats from Play ransomware:

- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest versions and conduct regular vulnerability assessments.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint CSA to disseminate the Play ransomware group's IOCs and TTPs identified through FBI investigations as recently as October 2023.

Since June 2022, the Play (also known as Playcrypt) ransomware group has impacted a wide range of businesses and critical infrastructure in North America, South America, and Europe. As of October 2023, the FBI was aware of approximately 300 affected entities allegedly exploited by the ransomware actors.

In Australia, the first Play ransomware incident was observed in April 2023, and most recently in November 2023.

The Play ransomware group is presumed to be a closed group, designed to "guarantee the secrecy of deals," according to a statement on the group's data leak website. Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data. Ransom notes do not include an

---

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Report@cisa.dhs.gov.

initial ransom demand or payment instructions, rather, victims are instructed to contact the threat actors via email.

The FBI, CISA, and ASD's ACSC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents. This includes requiring multifactor authentication, maintaining offline backups of data, implementing a recovery plan, and keeping all operating systems, software, and firmware up to date.

For a downloadable copy of IOCs, see:

- AA23-352A (STIX XML, 35KB)
- AA23-352A (STIX JSON, 31KB)

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See the MITRE ATT&CK for Enterprise section for all referenced tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Initial Access

The Play ransomware group gains initial access to victim networks through the abuse of valid accounts [T1078] and exploitation of public-facing applications [T1190], specifically through known FortiOS (CVE-2018-13379 and CVE-2020-12812) and Microsoft Exchange (ProxyNotShell [CVE-2022-41040 and CVE-2022-41082]) vulnerabilities. Play ransomware actors have been observed to use external-facing services [T1133] such as Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) for initial access.

Discovery and Defense Evasion

Play ransomware actors use tools like AdFind to run Active Directory queries [TA0007] and Grixba [1], an information-stealer, to enumerate network information [T1016] and scan for anti-virus software [T1518.001]. Actors also use tools like GMER, IOBit, and PowerTool to disable anti-virus software [T1562.001] and remove log files [T1070.001]. In some instances, cybersecurity researchers have observed Play ransomware actors using PowerShell scripts to target Microsoft Defender.[2]

Lateral Movement and Execution

Play ransomware actors use command and control (C2) applications, including Cobalt Strike and SystemBC, and tools like PsExec, to assist with lateral movement and file execution. Once established on a network, the ransomware actors search for unsecured credentials [T1552] and use the Mimikatz credential dumper to gain domain administrator access [T1003]. According to open source reporting [2], to further enumerate vulnerabilities, Play ransomware actors use Windows Privilege Escalation Awesome Scripts (WinPEAS) [T1059] to search for additional privilege escalation paths. Actors then distribute executables [T1570] via Group Policy Objects [T1484.001].

Exfiltration and Encryption

Play ransomware actors often split compromised data into segments and use tools like WinRAR to compress files [T1560.001] into `.RAR` format for exfiltration. The actors then use WinSCP to transfer data [T1048] from a compromised network to actor-controlled accounts. Following exfiltration, files are encrypted [T1486] with AES-RSA hybrid encryption using intermittent encryption, encrypting every other file portion of 0x100000 bytes. [3] (**Note:** System files are skipped during the encryption process.) A `.play` extension is added to file names and a ransom note titled `ReadMe[.]txt` is placed in file directory `C:`.

Impact

The Play ransomware group uses a double-extortion model [T1657], encrypting systems after exfiltrating data. The ransom note directs victims to contact the Play ransomware group at an email address ending in `@gmx[.]de`. Ransom payments are paid in cryptocurrency to wallet addresses provided by Play actors. If a victim refuses to pay the ransom demand, the ransomware actors threaten to publish exfiltrated data to their leak site on the Tor network (`[.]onion` URL).

Leveraged Tools

Table 1 lists legitimate tools Play ransomware actors have repurposed for their operations. The legitimate tools listed in this product are all publicly available. Use of these tools and applications should not be attributed as malicious without analytical evidence to support they are used at the direction of, or controlled by, threat actors.

Table 1: Tools Leveraged by Play Ransomware Actors

Name	Description
AdFind	Used to query and retrieve information from Active Directory.
Bloodhound	Used to query and retrieve information from Active Directory.
GMER	A software tool intended to be used for detecting and removing rootkits.
IOBit	An anti-malware and anti-virus program for the Microsoft Windows operating system. Play actors have accessed IOBit to disable anti-virus software.
PsExec	A tool designed to run programs and execute commands on remote systems.
PowerTool	A Windows utility designed to improve speed, remove bloatware, protect privacy, and eliminate data collection, among other things.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
Cobalt Strike	A penetration testing tool used by security professionals to test the security of networks and systems. Play ransomware actors have used it to assist with lateral movement and file execution.

Name	Description
Mimikatz	Allows users to view and save authentication credentials such as Kerberos tickets. Play ransomware actors have used it to add accounts to domain controllers.
WinPEAS	Used to search for additional privilege escalation paths.
WinRAR	Used to split compromised data into segments and to compress files into .RAR format for exfiltration.
WinSCP	Windows Secure Copy is a free and open-source Secure Shell (SSH) File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client. Play ransomware actors have used it to transfer data [T1048] from a compromised network to actor-controlled accounts.
Microsoft Nltest	Used by Play ransomware actors for network discovery.
Nekto / PriviCMD	Used by Play ransomware actors for privilege escalation.
Process Hacker	Used to enumerate running processes on a system.
Plink	Used to establish persistent SSH tunnels.

Indicators of Compromise

See Table 2 for Play ransomware IOCs obtained from FBI investigations as of October 2023.

Table 2: Hashes Associated with Play Ransomware Actors

Hashes (SHA256)	Description
453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb	Play ransomware custom data gathering tool
47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57	Play ransomware encryptor
75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7b2f226212	SystemBC malware EXE
7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c00c11986	SystemBC malware DLL
7a6df63d883bbccb315986c2cfb76570335abf84fafbefce047d126b32234af8	Play ransomware binary
7dea671be77a2ca5772b86cf8831b02bff0567bce6a3ae023825aa40354f8aca	SystemBC malware DLL

Hashes (SHA256)	Description
c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b31d71193c	Play network scanner
e652051fe47d784f6f85dc00adca1c15a8c7a40f1e5772e6a95281d8bf3d5c74	Play ransomware binary
e8d5ad0bf292c42a9185bb1251c7e763d16614c180071b01da742972999b95da	Play ransomware binary

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 3–Table 11 for all referenced threat actor tactics and techniques in this advisory.

Table 3: Play ATT&CK Techniques for Enterprise for Initial Access

Technique Title	ID	Use
Valid Accounts	T1078	Play ransomware actors obtain and abuse existing account credentials to gain initial access.
Exploit Public Facing Application	T1190	Play ransomware actors exploit vulnerabilities in internet-facing systems to gain access to networks.
External Remote Services	T1133	Play ransomware actors have used remote access services, such as RDP/VPN connection to gain initial access.

Table 4: Play ATT&CK Techniques for Enterprise for Discovery

Technique Title	ID	Use
System Network Configuration Discovery	T1016	Play ransomware actors use tools like Grixba to identify network configurations and settings.
Software Discovery: Security Software Discovery	T1518.001	Play ransomware actors scan for anti-virus software.

Table 5: Play ATT&CK Techniques for Enterprise for Defense Evasion

Technique Title	ID	Use
Impair Defenses: Disable or Modify Tools	T1562.001	Play ransomware actors use tools like GMER, IOBit, and PowerTool to disable anti-virus software.
Indicator Removal: Clear Windows Event Logs	T1070.001	Play ransomware actors delete logs or other indicators of compromise to hide intrusion activity.

Table 6: Play ATT&CK Techniques for Enterprise for Credential Access

Technique Title	ID	Use
Unsecured Credentials	T1552	Play ransomware actors attempt to identify and exploit credentials stored unsecurely on a compromised network.
OS Credential Dumping	T1003	Play ransomware actors use tools like Mimikatz to dump credentials.

Table 7: Play ATT&CK Techniques for Enterprise for Lateral Movement

Technique Title	ID	Use
Lateral Tool Transfer	T1570	Play ransomware actors distribute executables within the compromised environment.

Table 8: Play ATT&CK Techniques for Enterprise for Command and Control

Technique Title	ID	Use
Domain Policy Modification: Group Policy Modification	T1484.001	Play ransomware actors distribute executables via Group Policy Objects.

Table 9: Play ATT&CK Techniques for Enterprise for Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	T1560.001	Play ransomware actors use tools like WinRAR to compress files.

Table 10: Play ATT&CK Techniques for Enterprise for Exfiltration

Technique Title	ID	Use
Exfiltration Over Alternative Protocol	T1048	Play ransomware actors use file transfer tools like WinSCP to transfer data.

Table 11: Play ATT&CK Techniques for Enterprise for Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Play ransomware actors encrypt data on target systems to interrupt availability to system and network resources.
Financial Theft	T1657	Play ransomware actors use a double-extortion model for financial gain.

MITIGATIONS

The FBI, CISA, and ASD's ACSC recommend organizations apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by Play ransomware. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats and TTPs. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

These mitigations apply to all critical infrastructure organizations and network defenders. The FBI, CISA, and ASD's ACSC recommend that software manufacturers incorporate secure-by-design and -default principles and tactics into their software development practices to limit the impact of ransomware techniques (such as threat actors leveraging backdoor vulnerabilities into remote software systems), thus, strengthening the security posture for their customers.

For more information on secure by design, see CISA's Secure by Design and Default webpage and joint guide.

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers [CPG 2.F, 2.R, 2.S] 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 NIST's standards for developing and managing password policies [CPG 2.C].
  - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length [CPG 2.B];
  - Store passwords in hashed format using industry-recognized password managers;
  - Add password user "salts" to shared login credentials;
  - Avoid reusing passwords;
  - Implement multiple failed login attempt account lockouts [CPG 2.G];
  - Disable password "hints";
  - Refrain from requiring password changes more frequently than once per year.
    Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
  - Require administrator credentials to install software.
- **Require multifactor authentication** [CPG 2.H] for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems. Also see Protect Yourself: Multi-Factor Authentication | Cyber.gov.au.
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing

systems [CPG 1.E]. Organizations are advised to deploy the latest Microsoft Exchange security updates. If unable to patch, then disable Outlook Web Access (OWA) until updates are able to be undertaken. Also see Patching Applications and Operating Systems | Cyber.gov.au.

- **Segment networks** [CPG 2.F] 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. Also see Implementing Network Segmentation and Segregation.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware** with a networking monitoring tool. To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network [CPG 1.E]. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Filter network traffic** by preventing unknown or untrusted origins from accessing remote services on internal systems. This prevents actors from directly connecting to remote access services they have established for persistence. Also see Inbound Traffic Filtering – Technique D3-ITF.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 1.A, 2.O].
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 2.E].
- **Disable unused ports** [CPG 2.V].
- **Consider adding an email banner to emails** [CPG 2.M] received from outside your organization.
- **Disable hyperlinks** in received emails.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the just-in-time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** Privileged 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 [CPG 2.E].

- **Maintain offline backups of data** and regularly maintain backup and restoration [CPG 2.R]. By instituting this practice, an organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the FBI, CISA, and ASD's ACSC recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The FBI, CISA, and ASD's ACSC recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 3-11).
2. Align your security technologies against this technique.
3. Test your technologies against this technique.
4. Analyze your detection and prevention technologies performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The FBI, CISA, and ASD's ACSC recommend continually testing your security program at scale and in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: #StopRansomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Play ransomware actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

The FBI, CISA, and ASD's ACSC do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware,

and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office, the FBI's Internet Crime Complaint Center (IC3), or CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

Australian organizations that have been impacted or require assistance in regard to a ransomware incident can contact ASD's ACSC via 1300 CYBER1 (1300 292 371), or by submitting a report to cyber.gov.au.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and the FBI do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA or the FBI.

REFERENCES

[1] Symantec: Play Ransomware Group Using New Custom Data-Gathering Tools
[2] TrendMicro: Play Ransomware Spotlight
[3] SentinelLabs: Ransomware Developers Turn to Intermittent Encryption to Evade Detection