#StopRansomware: Play Ransomware | CISA

Published: 2025-06-04 · Archived: 2026-04-06 00:38:23 UTC

Summary

Note: *This joint Cybersecurity Advisory 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.*

Note: Updates to this advisory, originally published December 18, 2023, include:

- **June 4, 2025:** The advisory was updated to reflect new TTPs employed by Play ransomware group, as well as provide current IOCs/remove outdated IOCs for effective threat hunting.

Update June 4, 2025:

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 advisory to disseminate the Play ransomware group's IOCs and TTPs identified through FBI investigations as recently as January 2025.

End Update

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. Play ransomware was among the most active ransomware groups in 2024.

Organizations should take the following actions 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.

Update June 4, 2025:

As of May 2025, FBI was aware of approximately 900 affected entities allegedly exploited by the ransomware actors.

End Update

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

Update June 4, 2025:

Each victim receives a unique `@gmx.de` or `@web[.]de` email for communications. A portion of victims are contacted via telephone and are threatened with the release of the stolen data and encouraged to pay the ransom.

End Update

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.

Download a PDF version of this report:

-
-

For a downloadable copy of IOCs, see:

-

-

For a downloadable copy of historic IOCs, see:

-
-

Technical Details

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 17. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Initial Access

The Play ransomware group gains initial access to victim networks through the abuse of valid accounts, likely purchased on the dark web [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 using external-facing services [T1133] such as Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) for initial access.

Update June 4, 2025:

Multiple ransomware groups, including initial access brokers with ties to Play ransomware operators, exploited CVE-2024-57727 in remote monitoring and management (RMM) tool SimpleHelp [T1190] to conduct remote code execution [T1059.001] at many U.S.-based entities following the vulnerabilities' disclosure on 16 January 2025.

End Update

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,[3] 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

Update June 4, 2025:

The Play ransomware binary is recompiled for every attack, resulting in unique hashes for each deployment, complicating anti-malware and anti-virus program detection of the ransomware [T1027].

End Update

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.[4] **(Note:** System files are skipped during the encryption process.) A `.PLAY` extension is added to file names once encrypted. Within the Windows environment, tools and a ransom note titled `ReadMe[.]txt` are placed in `C:/Users/Public/Music/`.

Impact

Update June 4, 2025:

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` or `@web[.]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).

Play ransomware targets regularly receive phone calls from threat actors encouraging payment and threatening the release of company information. These calls can be routed to a variety of phone numbers within the organization, including those discovered in open source, such as help desks or customer service representatives.

ESXi Variant

The ESXi variant of Play ransomware invokes shell commands specific to the ESXi environment to conduct tasks, including powering off all running Virtual Machines (VMs), listing machines names, and setting the welcome message of the ESXi interface to the campaign-specific ransom note. The ransomware binary supports command line arguments; however, if no command line arguments are passed, the malware powers off all VMs and encrypts files related to VMs using randomly generated per-file keys. The targeted file extensions include `.vmdk` , `.vmem` , `.vmsd` , `.vmsn` , `.vmx` , `.vmxf` , `.vswp` , `.vmss` , `.nvram` , `.vmtx` , and `.log` . The ransomware binary employs AES-256 as its encryption algorithm. The binary creates a copy of the ransom note titled `PLAY_Readme.txt` in the root directory and in the path `/vmfs/volumes/` , as well as the welcome message of the ESXi interface.

Like the Windows variant of Play ransomware, the ESXi variant must be recompiled for each campaign. Through command line flags, the binary supports additional functionality likely used for development and debugging, including exempting specific VMs from encryption, targeting only one file for encryption, or skipping the file extension check and attempting to encrypt all files. Please see below for YARA rules.

End Update

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 antivirus 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.
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.

Name	Description
Process Hacker	Used to enumerate running processes on a system.
Plink	Used to establish persistent SSH tunnels.

Update June 4, 2025:

Indicators of Compromise

See **Table 2** for Play ransomware IOCs obtained from FBI investigations as of January 2025.

Table 2: Hashes Associated with Play Ransomware Actors

Hashes (SHA 256 and SHA 1)	Description
47B7B2DD88959CD7224A5542AE8D5BCE928BFC986BF0D0321532A7515C244A1E	SVCHost.dll Backdoor
75B525B220169F07AECFB3B1991702FBD9A1E170CAF0040D1FCB07C3E819F54A 453257C3494ADDAFB39CB6815862403E827947A1E7737EB8168CD10522465DEB C59F3C8D61D940B56436C14BC148C1FE98862921B8F7BAD97FBC96B31D71193C	GRIXBA Gt_net.exe Custom data gathering tool
1409E010675BF4A40DB0A845B60DB3AAE5B302834E80ADEEC884AEBC55ECCBF7	PSexesvc.exe Custom Play “psexesvc”
0E408AED1ACF902A9F97ABF71CF0DD354024109C5D52A79054C421BE35D93549	HRsword.exe Disables endpoint protection
90040340EE101CAC7831D7035230AC8AD4224D432E5636F34F13AA1C4A0C2041	Usysdiag.exe Associated with HRsword; changes settings of System certificates
3D86555ACAA19AEDDB5896071D1E3711B062EDBE	fThe9C.exe
6DE8DD5757F9A3AC5E2AC28E8A77682D7A29BE25C106F785A061DCF582A20DC6	Hi.exe Associated with ransomware
75404543DE25513B376F097CEB383E8EFB9C9B95DA8945FD4AA37C7B2F226212	SystemBC Malware EXE
7A42F96599DF8090CF89D6E3CE4316D24C6C00E499C8557A2E09D61C00C11986 7DEA671BE77A2CA5772B86CF8831B02BFF0567BCE6A3AE023825AA40354F8ACA	SystemBC malware DLL
967DAFF362E63FF45526F585B7944488ACE1BB5BB5B30FA40D56557F1C538D09	SHA256 Hash of public ECDSA key

Hashes (SHA 256 and SHA 1)	Description
859165041D75FBA3759C5533E324225F355C8A07B4645B984192AD6BEF06DB1A	SHA-256 Hash of public ED25519 Key for WinSCP Server
511F63455CA4F83B0347B65DDA17585AD02591A9F23D8E234E5CE1321AA3381A	SHA-256 Hash of public ED25519 Key WinSCP Server
372F7B45A141BB0709D578BC716CBCA03104258822C4290CCBEB600223850158	SHA-256 Hash of public ED25519 Key WinSCP Server

End Update

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.
Update June 4, 2025: Command and Scripting Interpreter: PowerShell	T1059.001	Play ransomware actors leveraged PowerShell commands to achieve RCE with a newly disclosed vulnerability. **End Update**

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 antivirus 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 antivirus 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 insecurely 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.

Update June 4, 2025:

Below is a copy of YARA rules related to the ESXi variant:

```
rule PlayForESXi
{
    meta:
        description = "Detects PLAY ransomware targeting ESXi Hypervisors"
        date = "2025-01"
        filetype = "elf"
        maltype = "ransomware"
    strings:
        $encrypt_str = "encrypt:"
        $first_step_str = "First step is done."
        $vmfs_path_str = "/vmfs/volumes"
        $PLAY_ext_str = ".PLAY" fullword
        $stop_list_mode_str = "stop list mode"
        $hosts_in_exclusion_str = "hosts in exclusion:"
        $error_in_stop_list_str = "Error, check stop list file, exit."
        $complete_str = "Complete."
        $dev_urandom_path_str = "/dev/urandom"
        $targeted_ext_vmdk = ".vmdk" fullword
        $targeted_ext_vmem = ".vmem" fullword
        $targeted_ext_vmsd = ".vmsd" fullword
```

```
        $targeted_ext_vmsn = ".vmsn" fullword
        $targeted_ext_vmx = ".vmx" fullword
        $targeted_ext_vmxf = ".vmxf" fullword
        $targeted_ext_vswp = ".vswp" fullword
        $targeted_ext_vmss = ".vmss" fullword
        $targeted_ext_nvram = ".nvram" fullword
        $targeted_ext_vmtx = ".vmtx" fullword
        $targeted_ext_log = ".log" fullword
        $vim_cmd_power_off_vms_str = "vim-cmd vmsvc/power.off"
        $get_storage_shell_cmd_str = "esxcli storage filesystem list > storage"
        $get_machines_shell_cmd_str = "vim-cmd vmsvc/getallvms > machines"
    condition:
        all of them
}
```

Below are copies of YARA and Suricata rules related to Play's custom data gathering tool, Grixba:

```
rule GRXBA
{
    meta:
        description = "Detects the infostealer GRXBA version 1.1.3.0"
        date = "2025-01"
        filetype = "pe"
        maltype = "infostealer"
    strings:
        $GRB_NET_hex = { 47 52 42 5F 4E 45 54 }
        $GRB_NET_exe_hex = { 47 52 42 5F 4E 45 54 2E 65 78 65 00 }
        $Copyright_Zabbix_2023_hex = { 43 6F 70 79 72 69 67 68 74 20 5A 61 62 62 69 78 20 32 30 32 33 00 }
        $GRB_NT_hex = { 47 52 42 5F 4E 54 00 }
        $help_string_1_hex = { 48 65 6C 70 54 65 78 74 2B 46 69 6C 65 2E 74 78 74 2F 31 32 37 2E 30 2E 30 2E
31 2D 31 32 37 2E 30 2E 30 2E 32 35 35 2F 31 32 37 2E 30 2E 30 2E 31 2D 32 34 }
        $help_string_2_hex = { 48 65 6C 70 54 65 78 74 5E 44 6F 6D 61 69 6E 20 6E 61 6D 65 20 66 6F 72 20 55
73 65 72 73 20 61 6E 64 20 43 6F 6D 70 75 74 65 72 73 20 67 61 74 68 65 72 69 6E 67 2E 20 49 66 20 6E 6F 74 20
73 65 74 20 77 69 6C 6C 20 62 65 20 75 73 65 64 20 64 6F 6D 61 69 6E 20 6F 66 20 63 75 72 72 65 6E 74 20 75 73
65 72 }
        $help_string_3_hex = { 48 65 6C 70 54 65 78 74 62 47 52 42 20 6D 6F 64 65 2E 20 73 63 61 6E 2F 73 63
61 6E 61 6C 6C 2F 63 6C 72 2E 20 73 63 61 6E 20 2D 20 6E 65 74 77 6F 72 6B 20 73 63 61 6E 6E 65 72 2E 20 73 63
61 6E 61 6C 6C 20 2D 20 67 72 61 62 20 61 6C 6C 2E 20 20 63 6C 72 20 2D 20 65 76 65 6E 74 20 6C 6F 67 73 20 63
6C 65 61 6E 65 72 }
        $help_string_4_hex = { 48 65 6C 70 54 65 78 74 3A 49 6E 70 75 74 3A 20 66 2F 72 2F 73 2E 20 66 20 2D
20 66 69 6C 65 2C 20 72 20 2D 20 72 61 6E 67 65 2C 20 73 20 2D 20 73 75 62 6E 65 74 2C 20 64 20 2D 20 64 6F 6D
61 69 6E }
    condition:
        all of them
}
```

```
Rule Suricataalert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 6c 00 20 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 5c 00 57 00 65 00 62 00 43 00 61 00 63 00 68 00 65 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_1_detected ;sid:1900002; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 6c 00 20 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 52 00 6f 00 61 00 6d 00 69 00 6e 00 67 00 5c 00 4d 00 6f 00 6f 00 6e 00 63 00 68 00 69 00 6c 00 64 00 20 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 69 00 6f 00 6e 00 73 00 5c 00 50 00 61 00 6c 00 65 00 20 00 4d 00 6f 00 6f 00 6e 00 5c 00 50 00 72 00 6f 00 66 00 69 00 6c 00 65 00 73 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_2_detected ;sid:1900003; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 6c 00 20 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 52 00 6f 00 61 00 6d 00 69 00 6e 00 67 00 5c 00 43 00 6f 00 6d 00 6f 00 64 00 6f 00 5c 00 49 00 63 00 65 00 44 00 72 00 61 00 67 00 6f 00 6e 00 5c 00 50 00 72 00 6f 00 66 00 69 00 6c 00 65 00 73 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_3_detected ;sid:1900004; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 6c 00 20 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 54 00 65 00 6e 00 63 00 65 00 6e 00 74 00 5c 00 51 00 51 00 42 00 72 00 6f 00 77 00 73 00 65 00 72 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_4_detected ;sid:1900005; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 6c 00 20 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 56 00 69 00 76 00 61 00 6c 00 64 00 69 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_5_detected ;sid:1900006; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 6c 00 20 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 43 00 6f 00 63 00 43 00 6f 00 63 00 5c 00 42 00 72 00 6f 00 77 00 73 00 65 00 72 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_6_detected ;sid:1900007; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 41 00 6c 00 6c 00 20 00 55 00 73 00 65 00 72 00 73 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 53 00 6f 00 67 00 6f 00 75 00 45 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 5c 00 57 00 65 00 62 00 6b 00 69 00 74 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_7_detected ;sid:1900008; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 4c 00 6f 00 63 00 61 00 6c 00 5c 00 56 00 69 00 76 00 61 00 6c 00 64 00 69 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_8_detected; sid:1900009; rev:1;)

alert smb any any -> any any (noalert; content:"|55 00 73 00 65 00 72 00 73 00 5c 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 20 00 55 00 73 00 65 00 72 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 52 00 6f 00 61 00 6d 00 69 00 6e 00 67 00 5c 00 4f 00 70 00 65 00 72 00 61 00 20 00 53 00 6f 00 66 00 74 00 77 00 61 00 72 00 65 00 5c 00 4f 00 70 00 65 00 72 00 61 00 20 00 53 00 74 00 61 00 62 00 6c 00 65 00|"; flow:to_server; flowbits:set,GRXBA_webhist_path_9_detected ;sid:1900010; rev:1;)

alert smb any any -> any any (msg:"GRIXBA web history scanning detected - potential indicator of imminent PLAY Ransomware attack"; flowbits:isset,GRXBA_webhist_path_1_detected; flowbits:isset,GRXBA_webhist_path_2_detected; flowbits:isset,GRXBA_webhist_path_3_detected; flowbits:isset,GRXBA_webhist_path_4_detected; flowbits:isset,GRXBA_webhist_path_5_detected;flowbits:isset,GRXBA_webhist_path_6_detected; flowbits:isset,GRXBA_webhist_path_7_detected; flowbits:isset,GRXBA_webhist_path_8_detected; flowbits:isset,GRXBA_webhist_path_9_detected; flowbits:set,GRXBA_hit_found; classtype:attempted-recon; sid:1900011; rev:1;)

alert smb any any -> any any (noalert; flowbits:isset,GRXBA_hit_found; flowbits:unset,GRXBA_webhist_path_1_detected;flowbits:unset,GRXBA_webhist_path_2_detected;flowbits:unset,GRXBA_webhist_path_3_detected;fl sid:1900012; rev:1;)
```

End Update

Mitigations

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. 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 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, CPG 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 15 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.[5]
- **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. [6]
- **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. [7]
- **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 – MITRE.
- **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, 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. 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 **Table 3** through **Table 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.

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

FBI, CISA, and ASD's ACSC do not encourage paying a 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, FBI and CISA urge you to promptly report ransomware incidents to a local FBI Field Office, FBI's Internet Crime Complaint Center (IC3), or CISA via CISA's 24/7 Operations Center (report@cisa.gov or 1-844-Say-CISA).

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 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 FBI.

References

[1] Threat Hunter Team, "Play Ransomware Group Using New Custom Data-Gathering Tools," *Symantec Enterprise Blogs*, *Symantec*, April 19, 2023, https://www.security.com/threat-intelligence/play-ransomware-volume-shadow-copy.

[2] Trend Micro Research, "Play," Trend Micro, July 21, 2023, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play.

[3] Trend Micro Research, "Play."

[4] Aleksandar Milenkoski, "Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection," SentinelLabs, September 8, 2022, https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/.

[5] See also Protect Yourself: Multi-Factor Authentication – Cyber.gov.au.

[6] See also Patching Applications and Operating Systems – Cyber.gov.au .

[7] See also Implementing Network Segmentation and Segregation – Cyber.gov.au .
