Quorum Cyber

Threat Intelligence Play Ransomware

TLP Status: White

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version		Date	Summary of Changes
0.1		01/02/2023	Initial Report
1.0		13/05/2023	Final PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

Play Ransomware

Overview

Play ransomware launched in June 2022, since which time organisations across the world have been successfully targeted. The ransomware has notoriously targeted organisations in the Latin American region, mainly Brazil.

The Play ransomware group has previously been observed to have used various infection vectors within their attack chain. Examples include the use of Cobalt Strike for post-compromise operations and SystemBC RAT with regards to target persistence. Play ransomware consistently targets compromised valid accounts or unpatched Fortinet SSL VPN vulnerabilities as a means of establishing a foothold in the target network. As with the majority of modern ransomware[1] variants, Play uses living-off-the-land binaries (LOLBins) to achieve its objective within target systems. These include the use of WinSCP for data exfiltration purposes as well as the Task Manager for Local Security Authority Server Service (LSASS) process dumping.

More recent Play ransomware campaigns have involved the exploitation of the 'ProxyNotShell' vulnerabilities discovered in Microsoft Exchange. Play ransomware is also known to employ similar behavioural trends and tactics as the HIVE and Nokoyawa ransomware variants[2].

Play ransomware has been deployed in prominent attack campaigns, including those against Argentina's Judiciary of Cordoba in August 2022 and more recently against network systems in the City of Oakland in March 2023.

Impact

Successful exploitation by Play ransomware will almost certainly result in the encryption and exfiltration of significant quantities of data held on the compromised system, prior to a ransom of a predetermined value being issued. The ransom amount demanded will almost certainly depend on the estimated value of the compromised organisation. Furthermore, such a compromise of data will also result in the organisation incurring a negative reputational impact. Encrypted data may include private customer data, corporate finance data and system credentials that if released can assist threat actors with future attacks.

Vulnerability Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide effective protection against malware threats including Play ransomware. EDRs can alert system users of potential breaches and stop the malware process during early signs of an attack attempt, therefore limiting the scope of damage.

Affected Products

- Windows OS
- FortiOS

[1] https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
[2] https://explore.avertium.com/resource/an-in-depth-look-at-play-ransomware

Containment, Mitigations & Remediations

As previously stated, one main method of reducing the threat of Play ransomware is to detect it in the early stages, whilst implementing an effective and monitored EDR solution. An effective EDR will increase detection of malicious attempts of Play compromise and halt the malware's progress if detected.

Users are strongly recommended to adhere to the following best practices in order to bolster the network security posture against Play ransomware exploitation[3]:

- 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 the environment
- Minimise 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 back-ups regularly
- Install updates regularly – maintain patch management protocols and keep operating systems and applications up to date. This action will deter threat actors from exploiting software vulnerabilities
- Enforce the multi-factor authentication requirement on all accounts, especially VPNs, webmail, and accounts with access to critical systems to prevent attackers from performing lateral movement inside a network
- Review the security posture of third-party vendors and those interconnected with your organisation. 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 unrecognised accounts
- Segment networks to prevent the spread of ransomware
- Consider adding an email banner to emails received externally to the organisation
- Disable command-line and scripting activities and permissions.

[3] https://explore.avertium.com/resource/an-in-depth-look-at-play-ransomware

Indicators of Compromise

Play Ransomware Associated File Hashes (SHA-256):

- 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55
- d4a0fe56316a2c45b9ba9ac1005363309a3edc7acf9e4df64d326a0ff273e80f
- e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173
- e641b622b1f180fe189e3f39b3466b16ca5040b5a1869e5d30c92cca5727d3f0
- c88b284bac8cd639861c6f364808fac2594f0069208e756d2f66f943a23e3022
- 3e6317229d122073f57264d6f69ae3e145decad3666ddad8173c942e80588e69
- 608e2b023dc8f7e02ae2000fc7dbfc24e47807d1e4264cbd6bb5839c81f91934
- 8962de34e5d63228d5ab037c87262e5b13bb9c17e73e5db7d6be4212d66f1c22
- e4f32fe39ce7f9f293ccbfde30adfdc36caf7cfb6ccc396870527f45534b840b
- 7d14b98cdc1b898bd0d9be80398fc59ab560e8c44e0a9dedac8ad4ece3d450b0
- c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3
- f6072ff57c1cfe74b88f521d70c524bcbbb60c561705e9febe033f51131be408
- f18bc899bcacd28aaa016d220ea8df4db540795e588f8887fe8ee9b697ef819f
- fc2b98c4f03a246f6564cc778c03f1f9057510efb578ed3e9d8e8b0e5516bd49
- 5573cbe13c0dbfd3d0e467b9907f3a89c1c133c774ada906ea256e228ae885d5
- dcaf62ee4637397b2aaa73dbe41cfb514c71565f1d4770944c9b678cd2545087
- 094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde

Play Ransomware Associated File Hashes (SHA-1):

- 8917af3878fa49fe4ec930230b881ff0ae8d19c9
- a996ccd0d58125bf299e89f4c03ff37afdab33fc
- 5f99214d68883e91f586e85d8db96deda5ca54af

Play Ransomware Associated IP Addresses:

- 104[.]21[.]43[.]80
- 172[.]67[.]176[.]244

Play Ransomware Domains:

- sunypoly[.]edu
- hacla[.]org
- siriusshipping[.]eu
- cmvcaridad[.]com
- eds-automotive[.]de

- presco[.]com
- stratacache[.]com
- qut[.]edu[.]au
- www[.]justiciacordoba[.]gob[.]ar

Exploited Vulnerabilities

- **CVE-2022-41080:** Microsoft Exchange Server Elevation of Privilege Vulnerability (CVSSv3 Score 9.8)
- **CVE-2022-41082:** Microsoft Exchange Server Remote Code Execution Vulnerability. (CVSSv3 Score 8.8)

Threat Landscape

Ransomware continues to be one of the prominent threats facing the private sector. Recent attacks and the developing nature of the ransomware threat landscape suggests that the threat is growing as criminal groups are becoming more comfortable demanding ever-increasing ransom quantities.

Play ransomware attacks mainly focus on organisations in the Latin American region, Brazil and Argentina being their primary targets. They have also been observed deploying attacks on India, Hungary, Spain and the Netherlands.

Threat Group

The Play ransomware group operates on the basis of a double extortion technique. Not only does the group encrypt the private data of the victim and demand ransom for the keys, but they also threaten the victims with the publishing of the data on their own dark web site. This is likely designed to increase pressure on the victim and increase the likelihood of securing the desired payment.

Mitre Methodologies

Resource Development
T1584.005 - Botnet[4]
T1588.002 - Tool[5]

Initial Access
T1133 - External Remote Services[6]
T1190 - Exploit Public-Facing Application[7]

Execution
T1059 - Command and Scripting Interpreter[8]
T1072 - Software Deployment Tools[9]

Persistence
T1098 - Account Manipulation[10]
T1133 - External Remote Services[11]

Defence Evasion
T1497 - Virtualization/Sandbox Evasion[12]

Credential Access
T1056.001 - Keylogging[13]

Discovery
T1082 - System Information Discovery[14]
T1083 - File and Directory Discovery[15]
T1497 - Virtualization/Sandbox Evasion[16]

Lateral Movement
T1072 - Software Deployment Tools[17]

Collection
T1005 - Data from Local System[18]
T1056.001 - Keylogging[19]

Command and Control
T1105 - Ingress Tool Transfer[20]

[4] https://attack.mitre.org/techniques/T1584/005/
[5] https://attack.mitre.org/techniques/T1588/002/
[6] https://attack.mitre.org/techniques/T1133/
[7] https://attack.mitre.org/techniques/T1190/
[8] https://attack.mitre.org/techniques/T1059/
[9] https://attack.mitre.org/techniques/T1072/
[10] https://attack.mitre.org/techniques/T1098/
[11] https://attack.mitre.org/techniques/T1133/
[1212] https://attack.mitre.org/techniques/T1497/
[13] https://attack.mitre.org/techniques/T1056/001/
[14] https://attack.mitre.org/techniques/T1082/
[15] https://attack.mitre.org/techniques/T1083/
[1616] https://attack.mitre.org/techniques/T1497/
[17] https://attack.mitre.org/techniques/T1072/
[18] https://attack.mitre.org/techniques/T1005/
[19] https://attack.mitre.org/techniques/T1056/001/
[20] https://attack.mitre.org/techniques/T1105/

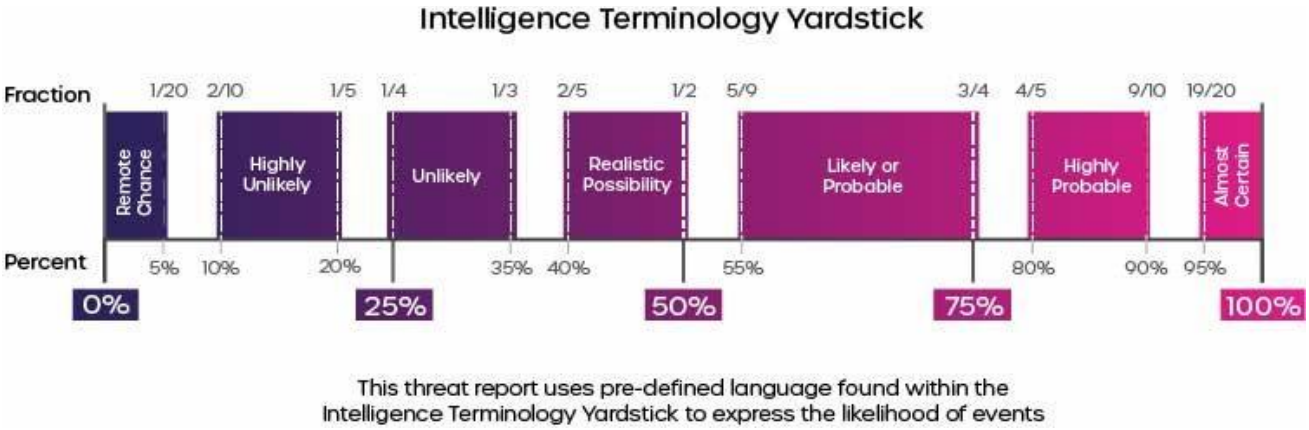
Exfiltration
T1030 - Data Transfer Size Limits[21]

Impact
T1486 - Data Encrypted for Impact[22]
T1565 - Data Manipulation[23]

Further Information

- Avertium Report
- Trend Micro Report

Intelligence Cut-off Date (ICoD): 08/03/2023 10:00 GMT



[21] https://attack.mitre.org/techniques/T1030/
[22] https://attack.mitre.org/techniques/T1486/
[23] https://attack.mitre.org/techniques/T1565/