Threat Brief: Maze Ransomware

By Brittany Barbehenn, Doel Santos

Published: 2020-05-08 · Archived: 2026-04-05 17:08:21 UTC

Several adversarial techniques were observed in this activity.

The following measures are suggested within Palo Alto Networks products and services for Maze ransomware:

Tactic	Technique (Mitre ATT&CK ID)	Product/Service	Course of Action
Initial Access	External Remote Services (T1133)	NGFW	Configure Interfaces and Zone segmentation
		Threat Prevention†	Deploy Vulnerability Protection Profile for all low and high severity threats with block action
		Cortex XDR	Configure Host Firewall Profile
Initial Access	Spear-Phishing Attachment (T1193)	NGFW	Configure a File Blocking Profile
		Threat Prevention†	Enable Anti-Virus profile with reset-both action
		WildFire	Forward files for WildFire Analysis
		Cortex XDR	Configure Malware Security Profile
Initial Access	Drive-by Compromise (T1189)	NGFW	Block all unknown and unauthorized applications
		Threat Prevention†	Deploy Vulnerability Protection Profile for all low and high severity threats with block action
		DNS Security†	Enable DNS Security in Anti-Spyware profile
		URL Filtering†	Control web access based on URL Category
		WildFire	Forward Files for WildFire Analysis
Initial Access	Trusted Relationship (T1199)	NGFW	Configure Interfaces and Zones segmentation
Initial Access Privilege Escalation Persistence	Valid Accounts (T1078)	NGFW	Configure Multi-Factor Authentication
		Threat Prevention†	Enable Credential Phishing protection

Defense Evasion		Cortex XSOAR	Deploy Cortex XSOAR Playbook - Access Investigation
Execution Defense Evasion	Scripting (T1064)	WildFire	Forward Files for WildFire Analysis
		Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
Execution	Powershell (T1086)	Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
Execution	Command-Line Interface (T1059)	Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
Execution	Service Execution (T1035)	Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile
Persistence	Modify Existing Service (T1031)	Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile
Persistence	Registry Run Keys / Startup Folder (T1060)	Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile
Persistence	New Service (T1050)	Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
Defense Evasion	NTFS File Attributes (T1096)	NGFW	Block all unknown and unauthorized applications
		WildFire	Forward files for WildFire Analysis
		Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile
Defense Evasion	Obfuscated Files or Information (T1027)	WildFire	Forward files for WildFire Analysis
		Cortex XDR	Enable Anti-Exploit and Anti-Malware Protection
Defense Evasion	Disabling Security Tools (T1089)	Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile

Credential Access	Brute Force (T1110)	NGFW	Create a rule to modify the default action for all signatures in the brute force category to block-ip address action
Credential Access	Credential Dumping (T1003)	Cortex XDR	Cortex XDR monitors for behavioral events and files associated with credential access and exfiltration
Lateral Movement	Remote Desktop Protocol (T1076)	NGFW	Configure Multi Factor Authentication,Create User Group for Limited Access to Allow List Applications,Configure Interfaces and Zones segmentation
		Cortex XDR	Configure Host Firewall Profile
Collection	Data from Local System (T1005)	Cortex XDR	Cortex XDR monitors for behavioral events and files associated with collection activities
Command and Control	Standard Application Layer Protocol (T1071)	NGFW	Block all unknown and unauthorized applications
		DNS Security†	Deploy Anti-Spyware profiles with block action
		Cortex XDR	Cortex XDR monitors for behavioral events indicative of command and control activity
Command and Control	Remote File Copy (T1105)	NGFW	Block all unknown and unauthorized applications
		WildFire	Forward files for WildFire Analysis
		Cortex XDR	Cortex XDR monitors for behavioral events associated with file creation, staging, and exfiltration
Command and Control	Standard Cryptographic Protocol (T1032)	NGFW	Block all unknown and unauthorized applications, Enable SSL decryption
		DNS Security†	Enable DNS Security in Anti-Spyware profile
		WildFire	Forward SSL decrypted files to WildFire
Discovery	File and Directory Discovery (T1083)	Cortex XDR	Cortex XDR monitors for behavioral events along a causality chain to identify discovery behaviors

Discovery	Network Share Discovery (T1135)	Cortex XDR	Cortex XDR monitors for behavioral events along a causality chain to identify discovery behaviors
Discovery	Process Discovery (T1057)	Cortex XDR	Cortex XDR monitors for behavioral events along a causality chain to identify discovery behaviors
Discovery	Software Discovery (T1518)	Cortex XDR	Cortex XDR monitors for behavioral events along a causality chain to identify discovery behaviors
Discovery	System Information Discovery (T1082)	Cortex XDR	Cortex XDR monitors for behavioral events along a causality chain to identify discovery behaviors
Exfiltration	Data Encrypted (T1022)	Cortex XDR	Configure Behavioral Threat Protection under the Malware Security Profile
Exfiltration	Exfiltration Over Alternative Protocol (T1048)	NGFW	Block all unknown and unauthorized applications. profile
		DNS Security†	Enable DNS Security in Anti-Spyware
Exfiltration	Exfiltration Over Command and Control (T1041)	NGFW	Block all unknown and unauthorized applications
		DNS Security†	Enable DNS Security in the Anti-Spyware profile
		Threat Prevention†	Enable Anti-Spyware Profile with Block Action
Impact	Data Encrypted for Impact (T1486)	Cortex XSOAR	Deploy Cortex XSOAR Playbook - Ransomware Manual for incident response

Table 1. Course of Action for Maze Ransomware

† These capabilities are part of the NGFW security subscriptions service

Recently, malicious operators behind the Maze ransomware activities compromised multiple IT service providers. These operators were also able to establish a foothold within another victim's network through insecure Remote Desktop Protocol and other remote service connections or by brute-forcing the local administrator account. Organizations should be mindful of potential compromises through third-party sources and ensure strong passwords are used for all systems capable of remote access.

It was also reported that Maze operators pay special attention to cloud backups on the compromised network. If the operators were to obtain login credentials, they are then able to download all backup data to an actor controlled server. Organizations should ensure that all cloud backup files are properly stored and protected.

Ransomware is a criminal business model that uses malicious software to hold valuable files and other data for ransom. Victims of ransomware attacks may have their operations degraded or shut down entirely.

Palo Alto Networks customers can review activity associated with this Threat Brief via AutoFocus using the following tag: *Maze*, SpelevoEKFlashContainer

Palo Alto Networks Cortex XDR contains an Anti-Ransomware Protection module. This module targets encryption-based activity associated with ransomware. Cortex XDR contains defined behavioral indicators of compromise designed to detect anomalies within your network.

The suggested courses of action in this report are based on the information currently available to Palo Alto Networks and the capabilities within Palo Alto Networks products and services.
