CASE STUDY

Evicting Maze

Talos and SecureX stop an active attack cold in its tracks

In the summer of 2020, a manufacturing company received a phishing email containing a malicious attachment. After an employee opened the email, several suspicious activities occurred, including the execution of encoded PowerShell commands to obtain elevated privileges, with indications of use of the penetration-testing tool Cobalt Strike.

In the week that followed, the company received a notification from Cisco SecureX Threat Hunting warning about the PowerShell execution as a potential precursor to a ransomware attack. The company soon contacted CTIR at the behest of their legal counsel.

CTIR provided emergency response services, including incident command, expert guidance on containment and remediation, forensic analysis, threat intelligence and reverse-engineering. CTIR began reviewing data from the Secure Endpoint, SecureX Cloud Edge, and Secure Network Analytics consoles, as well as triage data from affected hosts.

Leveraging threat intelligence from Talos' Threat Intelligence and Interdiction team, CTIR and Talos concluded that the activity Cisco SecureX Threat Hunting alerted on was likely the beginning stages of a Maze ransomware attack. Now allegedly disbanded, Maze was one of the more notorious ransomware families of late, engaging in "big game hunting," or targeting prominent organizations for large ransoms, and innovating the practice of exfiltrating data prior to dropping their ransomware, and then threatening to release the stolen data as another lever to compel victims to pay the ransom.

Maze adversaries typically maintain a long dwell time on the victim network as they search for privileged accounts and sensitive information. CTIR assessed that the adversaries had indeed been on the network several weeks before CTIR was engaged. However, this dwell time provided an opportunity for CTIR to identify the threat actor and thwart the more destructive elements of the attack.

From previous Maze attacks, Talos had developed a playbook that matched typical Maze tactics, techniques and procedures (TTPs) to ATT&CK information, as well as associated search strings in Secure Endpoint.

While reviewing malicious activity in Secure Endpoint data and associated ATT&CK information, CTIR realized that much of the TTPs appearing in this engagement were similar to previous Maze incidents. We discovered similar system information and owner discovery. The attackers also leveraged procdump for credential dumping and used privileged accounts to traverse the network. All of these TTPs looked identical to what was happening at the manufacturing company. The use of Cobalt Strike and a command and control (C2) IP address previously associated with a Maze attack confirmed the likely connection to Maze.

CTIR had additionally drawn up guides for combating Maze attacks and remediation strategies. Because of this, CTIR quickly delivered a plan of action (POA) to the customer the day they were engaged, containing a series of steps to take to prevent the adversary from accessing even more systems, exfiltrating data and dropping their ransomware.

These steps included:

- Preparing an Active Directory Domain password reset.
  - *Changing passwords of accounts in highly privileged groups.*
  - *Rolling Kerberos Ticket Granting Ticket (KRBTGT) twice.*
  - *Changing built-in local admin password.*
  - *Forcing password change on next login for general user accounts.*
  - *Disabling the ability of the Windows operating system to cache credentials on any device where credentials are not needed.*
- Installing and setting up Microsoft Local Administrative Password Solutions (LAPS) to provide management of and strong passwords for all local administrator accounts.
- Ensuring that backups are offline and separated from the impacted machines in network
- Limiting access to PowerShell, PSExec, Windows Management Instrumentation (WMI), Remote Desktop Protocol (RDP), SMB and administrative shares to trusted accounts or systems that have a legitimate access to such tools.

Case Study: Evicting Maze

The customer was very receptive to the plan of action and actively began implementing these recommendations. These actions had an immediate effect on the adversary's ability to move laterally throughout the network. With passwords reset, they had lost their privileged accounts. With access to PowerShell locked down, they could not execute commands. Locking down SMB and RDP prevented them from spreading to more machines on the network, and with backups isolated, the potential for encryption decreased.

The customer also had Secure Endpoint deployed, but in Audit mode so that malicious files would be alerted on but not necessarily quarantined. CTIR worked with the customer to push Secure Endpoint throughout the network and ensure it was running in Protect mode.

With their avenues for lateral movement restricted, the adversaries dropped the ransomware binary on all systems they had previously accessed. The adversaries dropped the malicious DLL file on 130 systems. However, with Secure Endpoint running in Protect mode, the file was successfully quarantined, and the ransomware component of the attack was prevented.

Meanwhile, Talos safely detonated the ransomware file in Secure Malware Analytics. From there, they obtained the ransom note that confirmed the analysts' assessment that this was, in fact, a Maze ransomware attack.

CTIR continued analysis and remediation efforts. Although some NetFlow data indicated potential exfiltration, CTIR found no evidence of data staging and, as opposed to many other Maze victims, had no stolen information posted on the Maze leaks website.

This engagement exemplifies how CTIR leverages Talos-wide resources, past experience and their expertise to deliver quick identification of threats as well as recommendations for remediation. With an active customer, CTIR prevented one of the most dangerous ransomware threat actors from achieving their goal.