CASE STUDY

Cobalt Strikes Out

Cisco Talos IR and SecureX team up with client to repel attack

In 2020, an employee at a publicly traded company with more than $8 billion in revenue going through a merger and acquisition downloaded a malicious document containing the commodity banking trojan Qakbot. Unfortunately, the host was configured to trust and enable macros on all Excel documents on the internet. Therefore, there was no warning of the macros' existence before they were automatically executed. Shortly after downloading the maldoc, a user opened it and a macro attempted to download a payload from an actor-controlled URL. It was saved to the victim machine and executed using a legitimate Windows component: rundll32.exe.

Shortly afterward, the adversary used PowerShell to download penetration-testing tool Cobalt Strike onto the victim machine. CTIR observed the adversary executing multiple Cobalt Strike-encoded commands reaching out to their command and control (C2) over ports 80, 443 and 8080. The adversary also engaged in some initial profiling and system discovery, using PowerShell to enumerate Domain Controllers on the domain, and the open-source Active Directory profiling tool Bloodhound to identify users and systems within the domain.

Shortly after Bloodhound was downloaded, a .JSON file was created in a user's Downloads folder, likely containing the output of information about the users within the domain from the Bloodhound execution. The adversaries then dropped a Cobalt Strike executable on two Domain Controllers and used open-source Active Directory profiling tool ADFind to enumerate other hosts. Similar to the Bloodhound .JSON output file, the adversary also directed the output of their AdFind enumeration commands into a .CSV file. The adversary later deleted this file.

Analysis of the Cobalt Strike beacons revealed they were executed from the ADMIN$ share, such as "\ADMIN$\9b0c536.exe," suggesting this executable was executed remotely from another system. One of the Cobalt Strike payloads was also installed on a host as a service and executed – additional evidence of the adversary's ability to execute payloads remotely.

CTIR observed the suspicious PowerShell activity in their SecureX telemetry, and sent a notification to the customer warning that the TTPs were consistent with pre-ransomware activity. This alert contained the specific hostname and indicators observed in SecureX that indicated a Cobalt Strike beacon reaching out to a C2.

After notification, CTIR began forensic analysis focusing on three key systems including patient zero and the two compromised Domain Controllers. CTIR was given access to the customer's Cisco Secure Endpoint console to search for malicious activity in the environment. CTIR then notified the customer of the affected hosts which had activity related to this incident. All of the affected hosts had already been found and remediated by the customer's team.

This customer had an existing IR Retainer with CTIR and a strong relationship that was formed over extensive pre-incident engagements and drills. Similar to the case above, the customer's alacrity in implementing CTIR recommendations avoided a disastrous outcome. CTIR recommendations included:

- Reimaging the patient zero endpoint to a known good image with up-to-date patches installed, placed on a VLAN that cannot route to the infected VLAN to prevent reinfection.
- Credential reset, similar to the case above, to prevent reinfection of affected hosts.
- Issuing a Group Policy Object limiting macro execution in Microsoft Office documents, which would prevent a similar attack from leveraging that infection vector.
- Instituting multi-factor authentication for all critical services to prevent remote-based compromise and post-compromise lateral movement.
- Issuing a Group Policy Object limiting the use of Windows utilities, such as PowerShell PSExec and Remote Desktop, to trusted accounts.

The collaborative, joint incident response between the customer's IR team and CTIR led to a quick containment and full eradication of the active adversary in the enterprise IT environment that had the capability to deploy ransomware to complete actions on objective.