Threat Hunting:
Machine-Assisted Incident Investigation

TRIAGINGX

Incident Response Management & Forensics

"Effective Incident Investigation requires speed of deployement and accuracy of the hunting tools. Using TXHunter we were able to establish the scope and severity of the attack on a critical server in our customer's environment in near real-time"

Bill D. Risk Management Solutions

Executive Summary

A major US based Private Wealth Management company with over 500 clients and $250 million in managed assets, suspected a potential cyber breach had occurred in their environment and called in one of the industries leading incident response management and forensics companies to investigate. The Incident Response (IR) team deployed an industry endpoint detection and response (EDR) solution across the network to identify and stop the potential breach, however as they battled to properly identify the scope and severity of the attack, they suspected that they were missing key pockets of the attack and were still suffering data leakage.

By leveraging the TXHunter solution, the incident response team were able to quickly deploy the disposable client to those suspect systems and identified the presence of Win32/Emotet banking trojan on a critical production windows server. This helped set the extent and severity of the incident for risk analysis and remediation.

Challenges

The standard procedure was to deploy endpoint detection response (EDR) sensors across the network environment to try and pick up evidence of system breaches or data exposure. This is the equivalent of casting a wide net to try and collect as many fish as possible, but not knowing exactly where they are or what they are.

The problem was that the IR team could not be completely certain that the EDR solution was deployed in all the right locations, and whether it could identify the threat. They needed to establish scope and severity quickly.

The Win32/Emotet banking trojan typically spreads via fake invoice emails with Microsoft Word attachments. Executing that document, leads to the downloading of payloads from the attacker's command and control servers. When one machine is infected the malware moves laterally through a network by using the default $admin SMB file share across Windows machines. Depending on the infected user's permission level, persistence can be gained through registry run keys or a service. It evades detection by using randomly generated file names by victim asset and altering its file composition on disk at regular intervals to evade detection based on file hash. The level of code obfuscation and encryption used to hide the code is quite complex, well-executed and actively maintained by the attackers.

How TXHunter Helped

TXHunter is a new generation of machine-assisted Hunters used for conducting threat incident investigations remotely. You only need to tell TXHunter which endpoint you want to investigate, download the disposable run-time agent to gather the data and wait for the analysis.

The agent takes a snapshot of the suspicious system and automatically conduct an incident investigation. If the investigation process identifies suspicious files or URL links, it will automatically launch the built-in sandbox capabilities for a behavior analysis. It is also integrated with third party engines and intelligence, to provide additional context on the detected objects. In about 5 to 10 minutes, TXHunter provides a straight and clear answer whether the endpoint has been infected or hacked, the severity level of that action and all supporting data.

Results, Return on Investment and Future Plans

TXHunter was quickly able to identify that the windows server was still compromised by Win32/Emotet even though the EDR solution had been deployed. This insight was used to quickly reset the scope of the investigation, helped eradicate the remaining pockets of infection across the enterprise and identify a new avenue of data exfiltration.

- Detected suspicious process that tried to connect to outside IP Address
- Detected and analyzed suspicious files which were collected from the system