Deception Technology Derails Ransomware Attack on Regional Healthcare Provider

Company	Situation	Solution
Regional healthcare provider	A phishing email attack delivered new strain of Locky ransomware.	The team inoculated the enterprise by using detailed attack forensics provided by the BOTsink® solution's malware analysis engine.

Overview

A New England healthcare provider, like many healthcare organizations, experienced many ransomware attacks. In this incident, the malware came into the network via a phishing email which contained an encrypted, password-protected file. The user unlocked the file, "detonating" the malware, which encrypted local drives and network shares, ultimately spreading ransomware through the network. As the ransomware spread, it contacted its Command-and-Control servers (C&C) to dynamically mutate the executable file to evade traditional malware detection and remediation tools. The ransomware encrypted the files on endpoints and servers and held them "ransom", forcing the organization to decide either pay to unencrypt the files or lose them altogether.

Challenge

The hospital's existing security controls did not provide enough actionable intelligence or alerts to mitigate current and future attacks. The security team learned of attacks from end users or by seeing ransomware encrypting critical data on their network shares. Responding to this particular attack was very resource intensive as the team was forced to manually quarantine and remediate the individual endpoints and then check the local network shares for encrypted files.

- The team did not obtain the attack forensic information they needed to quickly analyze the malware and deal with its polymorphic nature.
- The security team found manual remediation extremely problematic because it required significant time to gather attack information and respond to the infected systems.
- The incident response approach was resource intensive and reactive, as opposed to a proactive response to an attack
- The security team lacked confidence that when they mitigated an attack, it would not reoccur – they did not know if they had truly stopped it.

Solution

To resolve this challenge, the healthcare provider chose a new approach that provided early attack warning and intelligence on the polymorphic ransomware's different attack methods, including the method of mutation, what C&C hosts the ransomware was contacting, and its lateral movement mechanisms.

The customer used the Attivo BOTsink solution's malware analysis engine to run extensive attack analysis and forensics to understand how the attack was propagating, communicating, and mutating. To gain this information, the security team loaded the malware onto the BOTsink solution's attack analysis engine, which unpacked and detonated the sample inside its secure sandbox. The security team saw the processes the malware dropped, the C&C hosts it contacted, and the methods of lateral movement it used. The team safely and confidently conducted this analysis because the malware analysis sandbox isolated all outbound traffic to a dedicated connection, preventing samples from infecting other machines in the customer's infrastructure. Additionally, since the malware analysis sandbox recorded all network traffic, the security team captured the polymorphic instructions the malware used to change its signature every few hours, using the information to update prevention systems to block infections from occurring within other parts of the network.

Benefits

The Attivo ThreatDefend™ Platform provided information that security devices could not. The Attivo BOTsink solution's analysis engine provided detailed attack forensics and substantiated, actionable alerts that allowed the customer to secure their enterprise by blocking the C&C IPs and applying group policies to shut down the malware's method of east-west movement. They also flagged the files hashes of the original and subsequent mutated files in their endpoint solution, preventing a wide-scale ransomware attack. The organization could now efficiently and quickly know if ransomware surfaces inside their network in the future.

The infosec team was able to drastically reduce their incident response time with their ability to analyze and remediate the ransomware...

ROI

Ransomware, by definition, is designed to force an organization to pay a "ransom" to recover their encrypted files or to forfeit the critical data. If the organization does not pay the ransom, they can lose critical data and suffer damage to their brand reputation.

In a ransomware attack, every second counts. The security team drastically reduced their incident response time with their ability to analyze and remediate the ransomware, as well as improve the posture of other security controls to prevent further infection from the malware. This avoided any additional operational costs that would have been incurred had the ransomware infected additional endpoints. With the ThreatDefend Platform, the healthcare organization saved the ransom they would have needed to pay to recover their critical data.

Outcome

By utilizing the ThreatDefend BOTsink solution, the security team understood and stopped the current ransomware attack and prevented an attack from similar strains in the future. Additionally, the team is now significantly more prepared for future attacks with their ability to use the Attivo ThreatDefend Platform:

- for early detection of a ransomware and other malware attacks
- for attack analysis and forensic reporting
- to detonate sample strains in the analysis engine and open communications with C&C to gain attack IOCs and attacker TTPs
- to accelerate incident response with BOTsink solution engagement server attack findings and automated response actions with prevention systems

Attivo Products

ThreatDefend Deception and Response Platform

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com