CASE STUDY

Attivo NETWORKS®

DECEPTION TECHNOLOGY DERAILS RANSOMWARE ATTACK ON REGIONAL HEALTHCARE PROVIDER

COMPANY

Regional healthcare provider

SITUATION

A phishing email attack delivered a new strain of Locky ransomware.

SOLUTION

The team protected the enterprise by using detailed attack forensics provided by the BOTsink® deception server's malware analysis capabilities.

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 that contained an encrypted, password-protected file. The user unlocked the file, "detonating" the malware, which encrypted the system's local drives and network shares, ultimately spreading ransomware through the network. As the ransomware spread, it contacted its Command-and-Control servers (C2) 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 decrypt 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 especially resource-intensive as the team had 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 analyze the malware quickly 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 entirely stopped it.

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.

SOLUTION

The customer used the Attivo ThreatDefend® platform BOTsink® deception server's attack analysis capabilities 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, collecting and correlating the resulting forensic information. The security team identified the processes the malware dropped, the C2 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 ThreatDefend platform provided information that other security solutions could not. The Attivo BOTsink server's analysis engine provided detailed attack forensics and substantiated, actionable alerts that allowed the customer to secure their enterprise by blocking the C2 IPs and applying group policies to shut down the malware's method of east-west movement. They also flagged the 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 valuable 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. These improvements avoided any additional operational costs they would have 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 platform's BOTsink server, the security team understood and stopped the current ransomware infection and prevented an attack from similar strains in the future. Additionally, the team is now significantly more prepared for future incidents 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

ATTIVO PRODUCTS

ThreatDefend Detection and Response Platform

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Data concealment technology hides critical AD objects, data, and credentials, eliminating attacker theft and misuse, particularly useful in a Zero Trust architecture. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys obfuscate the attack surface to derail attacks. Forensic data, automated attack analysis, and automation with third-party integrations serve to speed threat detection and streamline incident response. ThreatDefend capabilities tightly align to the MITRE ATT&CK Framework and deception and denial are now integral parts of NIST Special Publications and MITRE Shield active defense strategies. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com