INCIDENT RESPONSE CASE STUDY: HEALTHCARE INDUSTRY

Infogressive
Cybersecurity Solved.

INDUSTRY

- Managed Service Provider's Client Organization
- Large Neurosurgery Practice

ENVIRONMENT

- 150+ Endpoints
- 7 Clinic Locations

THE PROBLEM

- Multiple ransomware attacks
- Hospital servers infected & encrypted
- Proper investigation & recovery was not achieved after first breach, leading to another incident
- Outdated systems & security solutions in place

THE SOLUTION

- Full IR investigation helped uncover security gaps
- Transitioned to bundled security with Infogressive's Nation State solution

EXECUTIVE SUMMARY

A Managed Service Provider's (MSP) client was experiencing a large-scale cyber incident. Through the MSP, the Midwest-based healthcare organization turned to Infogressive after being hit with their second severe ransomware attack in three years. Infogressive's Incident Response (IR) investigation traced the 2019 cyberattack back to the same source of the 2016 attack and uncovered the security gaps that contributed to the attackers' success.

After the breach investigation, the healthcare organization decided to improve the security of their systems for the sake of patient safety. The organization chose Infogressive's most wholistic layered protection, available through the MSP's partnership: the Nation State Bundle.

THE INCIDENT

In 2016, the healthcare organization was hit by a ransomware attack that encrypted multiple workstations. The team felt lucky, however, to have had a robust backup solution in place that allowed them to restore the workstations and continue business as usual without paying the ransom. There appeared to be no impact at the time to the network or the organization's patients and operations.

In the spring of 2019, the subsequent attack revealed a different story.

The organization became the victim of a cyberattack once again, finding workstations and a critical server had been encrypted by a form of ransomware. Although they could restore from backups to recover, as done in 2016, the organization was unsure of how the breach occurred originally or how they had been hit a second time. In addition, the MSP advised an IR investigation to reveal if any personally identifiable information (PII) had been compromised or leaked — an event that would require further legal action and reporting. The organization chose to proceed with an IR before restoring, allowing forensics and investigation to reveal the unknown and provide insight into how to prevent future successful cyberattacks.

Infogressive
Cybersecurity Solved.

Infogressive's Security Operation Center (SOC) was engaged in March 2019. The team deployed Malware Prevention and EDR in the network to aid in the investigation. Just like the 2016 incident, the machines had been encrypted using .Locky ransomware: an infamous malware variant responsible for the 2016 Hollywood Presbyterian Medical Center breach, which is commonly delivered through spear-phishing emails and encrypts all files on a machine, renaming their extension to ".locky". This specific attack paired .locky with other tactics, allowing it to spread from machine-to-machine within the network..

THE OUTCOME

Through Incident Response processes (forensic investigation, data collection), the Infogressive team determined the source of the breach to be an open port. RDP (port 3389) was "wide open" and unsecured to access from the internet. This security vulnerability was initially used to breach the organization in 2016, when the attacker entered the network, planted the .Locky ransomware files, and created a user account titled "New User" which had not been identified by the organization or removed. When the organization restored the infected workstations in 2016, the attacker never lost access because the open port and the user account under the attacker's control were not investigated or remediated.

The attacker maintained access to the organization's network during the entirety of 2016 and 2017, leading up to the following attack in early 2019 at which point the same ransomware approach was deployed again. Infogressive's investigation identified the original vulnerability and user account were the point of access once again in the second incident. Luckily, there were no signs of data exfiltration within the network. The attacker's goal remained focused on payment via bitcoin in exchange for encrypted files. Infogressive assisted the organization in revoking access, securing the open port, and authorized the organization to restore the systems once the investigation was complete.

THE SOLUTION

Post-breach, the organization decided that after suffering multiple attacks, it was time to improve their defenses by implementing the "Nation State" security bundle. Within the first six months of service, the protection was already evident:

5,817

attempted file-based exploits blocked

of incoming email was spam or malicious

200+

viruses blocked from reaching inboxes

Infogressive
Cybersecurity Solved.