Leading Health Services Provider Thwarts Ransomware Attack with ExtraHop

CHALLENGE

A ransomware attack threatened to hold the company's sensitive, business-critical files hostage.

SOLUTION

With the ExtraHop platform, the health services provider was able to quickly pin down how ransomware had infiltrated the client machine and track its movements in real-time in order to quarantine all infected hosts—not by signatures, but by pattern-based behavioral analysis—before it could do significant harm. They now have ExtraHop monitoring all critical file systems to analyze any anomalous behavior and activity, something that previously wasn't possible.

BENEFITS

- **Rapidly isolated the source of the malicious code**
- **Quickly and efficiently quarantined impacted hosts and resources stopping the spread of the ransomware**
- **Created alerts on anomalous file activity to rapidly detect and prevent future attacks**

CHALLENGE

Early in 2016, an employee of a large health services provider was experiencing performance problems with his client machine. He opened a ticket with the organization's IT department. What they found came as a surprise—and a wake-up call—to everyone involved.

The slowness and performance problems that seemed innocuous turned out to be much more insidious. The client machine had been infected with ransomware, and it was already working to encrypt local and remote files to which the employee had access.

Because ransomware relies on the permissions of the infected user or machine to access and encrypt files on any shared volumes on the NAS, the IT team first needed to understand what was happening on the employee's machine.

SOLUTION

In order to prevent a large-scale data hostage situation like that experienced at a major hospital earlier the same week, the IT and security teams at the health services provider leveraged their existing deployment of ExtraHop. The service provider needed a way to determine how and when the employee's machine had become infected with ransomware, determine which files and systems had been impacted, and quickly alert on any activity associated with the ransomware. In this case, the ransomware used file extensions that were not used within their NAS, so they created an alert for activities of that type to serve as an early warning for current as well as future attacks.

Using ExtraHop to monitor and analyze East-West traffic, they were able to monitor the client machine and watch, in real-time, each file that the ransomware was reading and writing. In turn, they were able to quickly isolate impacted assets and stop the attack from progressing.

CSI: Network

While the most critical step in thwarting a ransomware attack is blocking its access to NAS resources, it's also crucial to understand when and how the client machine or user was infected in the first place so an organization can discover all potentially impacted machines.

Using the look-back functionality in ExtraHop, the security team for the health services provider was able to identify and investigate the employee's transaction activity, looking specifically at the 10 minutes leading up to when the attack started.

In this particular case, the IT and security teams were able to use ExtraHop to determine that the ransomware came not from a PDF or executable file the user had downloaded, but from a URI on which the employee had clicked. With ExtraHop, they could now easily search and see any other client that had accessed similar URIs and quarantine those preventing a widespread infection across their environment. They also set a policy in their web filtering proxy blocking all future access to that same URI.

DEFEATING RANSOMWARE WITH PROACTIVE SECURITY MONITORING

Between 2013 & 2014

250%
increase in new crypto ransomware families on the threat landscape.[1]

2015

48.3%
increase in number of users attacked by encryption ransomware.[2]

In Q1 2015

165%
YoY increase in ransomware attacks.[3]

2015

FIRST
ransomware for Linux appears.[4]

753,684
number of computers of unique users where ransomware programs were detected.[5]

179,209
number of computers targeted by encryption ransomware.[4]

[1] Symantec; [2,4,5] Kaspersky Labs; [3] McAfee Labs

ExtraHop

EXTRAHOP = POSITIVE + PROACTIVE SECURITY

1. Detect ransomware infections *in real time* based on observed anomalous file activity
2. Investigate details easily, including all infected clients and malware source
3. Mitigate risk by blocking malware hosts and infected client access to network shares

BENEFITS

Security Beyond the Perimeter

Ransomware attacks are yet another example of why traditional perimeter-based security solutions, virus scanning, and log file analysis are no longer sufficient to address today's sophisticated real-time threats.

ExtraHop provides real-time visibility into all North-South and East-West traffic, empowering IT and security teams to detect anomalous behavior—such as irregular NAS activity—and track that behavior from the client machine or user through the entire environment. This rapid detection and correlated, cross-tier investigation based on observed file activity and behavior is something that neither next generation firewalls nor log analysis systems support. With that insight, IT and security teams can spot potential breaches early, and proactively block off sensitive assets before they are attacked.

Fast Quarantine + Proactive Alerting

For the health services provider, one of the most critical steps in curtailing the ransomware attack was quarantining systems to prevent further spread. Using the ExtraHop ransomware solution, the organization's information security team was able to rapidly identify the behavior and affected host preventing a bad situation from becoming catastrophic. The InfoSec team is now planning to expand the use of ExtraHop beyond IT Operations using the platform as the foundation for its next-generation real-time security analytics architecture.

ABOUT EXTRAHOP NETWORKS

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop platform analyzes all L2-L7 communications, including full bidirectional transactional payloads. This provides the correlated, cross-tier visibility essential for today's complex and dynamic IT environments. The ExtraHop platform scales up to 40 Gbps in a single appliance, deploys without agents, and delivers tangible value immediately upon deployment.

ExtraHop

ExtraHop Networks, Inc.
520 Pike Street, Suite 1700
Seattle, WA 98101 USA

www.extrahop.com
info@extrahop.com

T 877-333-9872
F 206-274-6393

Customer Support
support@extrahop.com
877-333-9872 (US)
+44 (0)845 5199150 (EMEA)