Real-Time Ransomware Detection and Response

Stop Ransomware Before It Becomes Catastrophic

ExtraHop offers a simple way for IT departments to detect, investigate, and mitigate many types of ransomware attacks in minutes. This real-time detection for the entire environment has never been possible before.

At-a-glance

Know before you go

- The ExtraHop solution for ransomware is unique—no other product can detect ransomware activity across all NAS systems, file shares, or shared drives
- ExtraHop notifies IT departments of ransomware attacks within minutes when they are observed on the network
- IT teams can not only detect ransomware, but see and search on who received malicious files and the IP addresses hosting malware
- By detecting and stopping attacks within minutes, organizations can prevent disruption of operations and financial costs

Did You Know?

- 70 percent of businesses infected with ransomware paid the ransom, according to an IBM survey.
- The FBI estimates that ransomware brought in more than $1 billion for criminals in 2016.
- The average ransom demand in 2016 was $679, more than double the demand at the end of 2015, according Symantec.
- Ransomware makes up about 60 percent of malware infections encountered by Malwarebytes anti-virus software.

Learn more by downloading the whitepaper:

Detect and Stop Ransomware with a New Mitigation Approach

Ransomware has taken off as a low-risk, high-reward way for hackers to make money. Increasingly, hackers are targeting businesses. ExtraHop analyzes all data in flight so that IT organizations have full network visibility. In the case of ransomware, the ExtraHop platform enables incident response teams to know about an attack within minutes and take quick action to mitigate the impact.

Detect

Detect threats faster inside your environment

The ExtraHop platform detects anomalies on the network, including the unique storage WRITE operations and file changes that are associated with ransomware. Incident response teams can set up an alert and be notified within minutes of a ransomware infection.

Investigate

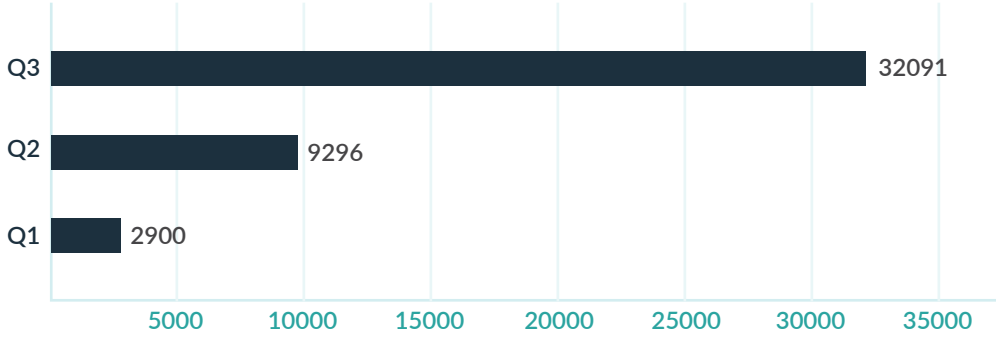
Track down all infected machines and malicious IPs

Ransomware takes some time to overwrite files, making it crucial that incident response teams can pinpoint attacks within minutes. The ExtraHop platform enables teams to rapidly identify attacks in progress on NAS systems and shared file infrastructure. ExtraHop also enables response teams to rapidly identify users who received malicious files and which IP addresses are hosting the malware.

Stop

Integrate with firewalls and network access control

With the specific data provided by ExtraHop, incident response teams can disconnect infected computers, block malicious IP addresses, and begin restoring files from backup.



According to Kaspersky Labs, the number of new cryptor modifications grew more than three times from Q2 to Q3 in 2016. ExtraHop works for all variants of crypto-ransomware because it detects ransomware by observing behaviors.

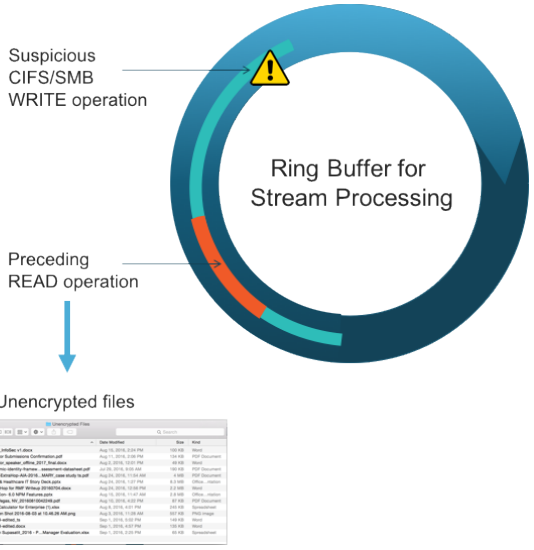
Ransomware Detection with ExtraHop

The ExtraHop platform analyzes all data in flight—all client, network, application, and infrastructure activity—providing the richest source of real-time security insights.

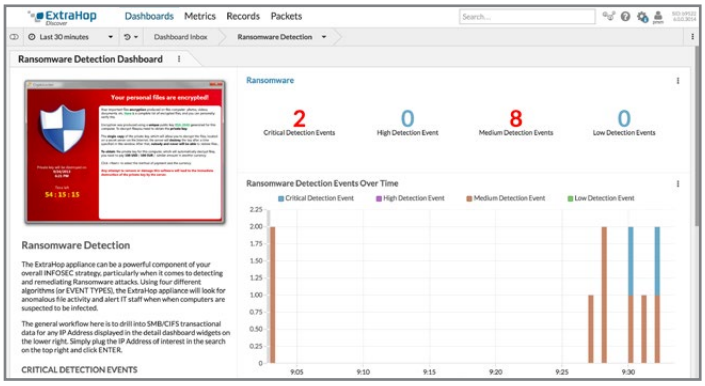
The ExtraHop solution for detecting ransomware identifies suspicious CIFS/SMB WRITE operations using malformed file extensions, for example. Ransomware variants such as Cryptowall change the file names and extensions as those files are encrypted so that they read, for example, “asksdf.ui4” or “sdffdfeerr.u8i3.”

The screens below shows a Cryptowall infection propagating through several sandboxed workstations. This solution has also successfully detected ransomware in the environments of ExtraHop customers.

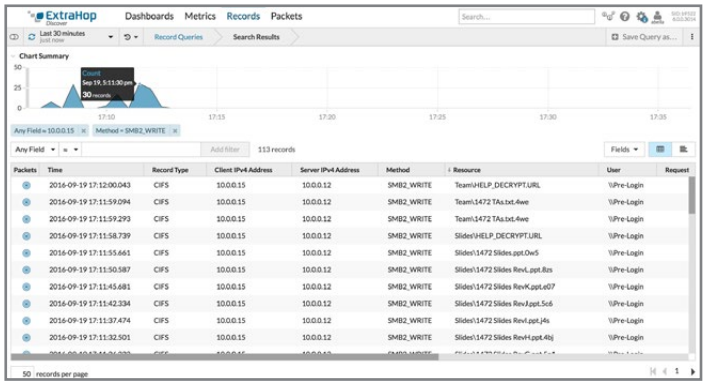
Beyond detection, the ExtraHop platform offers excellent investigation capabilities. You can easily drill down to see which clients received the malicious file and the IP address from which the malware is downloaded. The platform makes it possible for you to automate firewall or network access control actions, so that you can block communications or quarantine infected machines. You can also reconstruct files from packet captures of just the READ operations (see illustration at right).



Back-up on the wire! ExtraHop can precisely capture the packets of the READ operations that precede suspicious WRITE operations so that you can reconstruct unencrypted files.



The ExtraHop ransomware solution includes two dashboards for a high-level view of suspicious CIFS/SMB file activity.



From the dashboard, you can easily explore transaction records to understand the extent of the infection and the origin.

Try the Online Demo!

See what the ExtraHop platform can do for security use cases in our online demo. You can explore the interface for yourself or follow guided tours, including for ransomware detection and threat detection.

www.extrahop.com/demo