ExtraHop

WHITE PAPER

Detecting Ransomware in Real Time with Complete East-West Visibility

Abstract

The ransomware epidemic has forced IT organizations to think differently about how they surveil and defend their digital assets. Passive observation of transactions on the network empowers IT departments to detect, investigate, and mitigate crypto-ransomware attacks in minutes. This paper describes how real-time ransomware detection for the entire environment is made possible through analysis of all data in flight.

What We Know

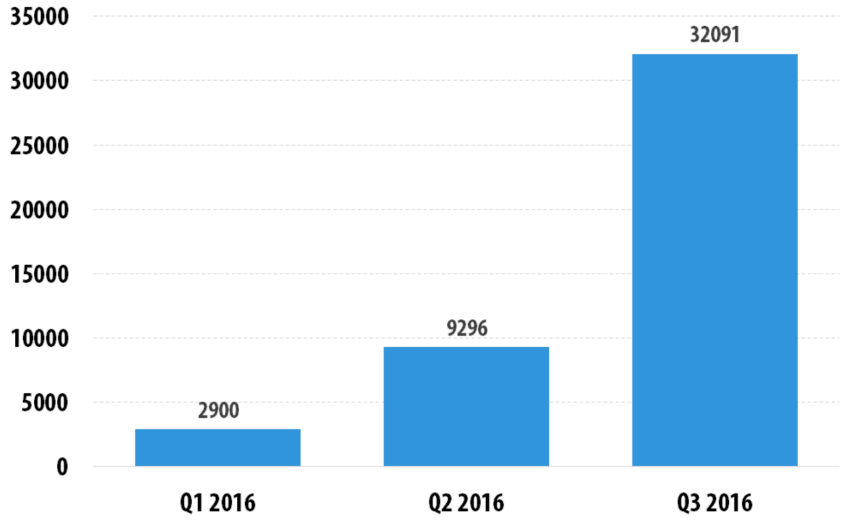
Ransomware is a low-risk, high-reward way for cybercriminals to make money. Increasingly, these criminals are targeting businesses, hoping to hold network shares or even entire file servers ransom for millions of dollars. The FBI has estimated that criminal organizations brought in more than $1 billion in 2016. At the same time, ransomware can shut down operations, costing businesses much more than just the ransom payment. Estimates for the cost of the WannaCry ransomware attack range up to $8 billion globally.

So far, we've learned several things from the ransomware epidemic:

- **Digital files are valuable -** When employees cannot access their documents, spreadsheets, presentations, images, and other files, operations shut down or are forced to revert to paper processes. Ransomware puts a monetary value on these assets that organizations had previously taken for granted.
- **Cybercrime is a business -** Since the primary goal for cybercriminals is making money, they're going to focus their finite resources on the most profitable opportunities. Ransomware has proven to be an easier way to make money than other forms of cybercrime, such as selling stolen credit card data, and thieves are following the money; ransomware now makes up to 60 percent of malware infections observed by Malwarebytes anti-virus software. Unless the IT industry makes this tactic less effective for criminals, we can expect ransomware to be the name of the game for cybercrime for the foreseeable future.
- **We need east-west visibility -** What makes a ransomware infection damaging is when it spreads to network shares, file servers, or even storage backups. Currently, organizations have invested heavily in seeing what traffic is coming into and going out of the environment (so-called "north-south traffic") but have limited visibility for the "east-west" traffic travelling between machines inside of the perimeter. To identify ransomware, organizations need real-time visibility into which devices are accessing network shares and what type of behavior they are exhibiting. As it is, many IT departments fear learning about a ransomware infection from a confused user: "Um … my computer's not working and there's this strange note on my screen."

DID YOU KNOW?

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



Number of new cryptor modifications in 2016, as measured by Kaspersky Labs. Ransomware is rapidly evolving, making signature- or rules-based approaches less effective.

Detecting Ransomware: The Solution Is on the Wire

Traditional security products have not yet tipped the cost-reward balance for cybercriminals. Many of these products focus on the enterprise perimeter, screening for known, bad IP addresses, URLs, emails, and DNS queries. Others aim to protect end-points by scanning payloads for telltale signatures. The problem with these approaches is that the origination vectors and even payloads used in ransomware malware change constantly, even through the course of a single day. So, looking for things that have already been seen has proven unreliable in stopping new variants of ransomware.

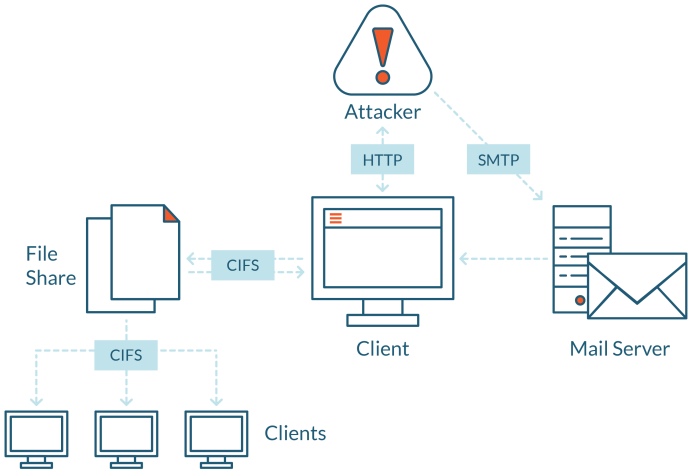
The ExtraHop solution for ransomware detection was designed from the ground up to focus exclusively on the observed behavior of ransomware, not signatures. With comprehensive, real-time visibility of all east-west *and* north-south transactions, IT teams can know about an attack within minutes and take quick action to mitigate the impact.

Detect	Investigate	Stop
The ExtraHop platform detects anomalies on the network, including the unique CIFS/SMB 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.	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.	With the specific data provided by ExtraHop, incident response teams can disconnect infected computers, block malicious IP addresses, and begin restoring files from backup.

Filling the East-West Traffic Visibility Gap

The ExtraHop platform analyzes all data in flight—all client, network, application, and infrastructure activity—providing the richest source of real-time security insights. This approach provides unmatched visibility into all east-west and north-south traffic, filling a gap left by security platforms that only scan for attack signatures or analyze log files.

The ExtraHop solution for detecting ransomware analyzes SMB/CIFS WRITE operations to identify anomalous behavior. For example, crypto-ransomware often progressively encrypts files in your storage, renaming them with something that looks like a random string of characters. The ExtraHop solution will identify these strange file names such as "oweisfhdx.wz" or "awbnidwn.eo" as well as detect unusual levels of activity (i.e. high numbers of WRITE operations).



By analyzing all data in flight, the ExtraHop platform enables organizations to detect ransomware in real time. ExtraHop extracts detailed metrics for protocols involved in ransomware attacks, from mail delivery and malware download, to command and control and file overwrites.

Automating Quarantine or Blocking Actions

The ExtraHop platform automatically detects ransomware; however, it does not take action. To enable automatic remediation, the ExtraHop platform offers a REST API so that you can quarantine a ransomware-infected client with a network access control (NAC) solution or block an IP address through a firewall. The lines of JavaScript code below demonstrate the simplicity of integrating with a NAC solution.

```
var my_path = "/utilities/?quarantine" + "&clientmacaddress=" + Flow.client.device.hwaddr + "
&source="ExtraHop" + "&reason="RANSOMWARE";  Remote.HTTP("my_NAC").get( {path: my_path} );
```

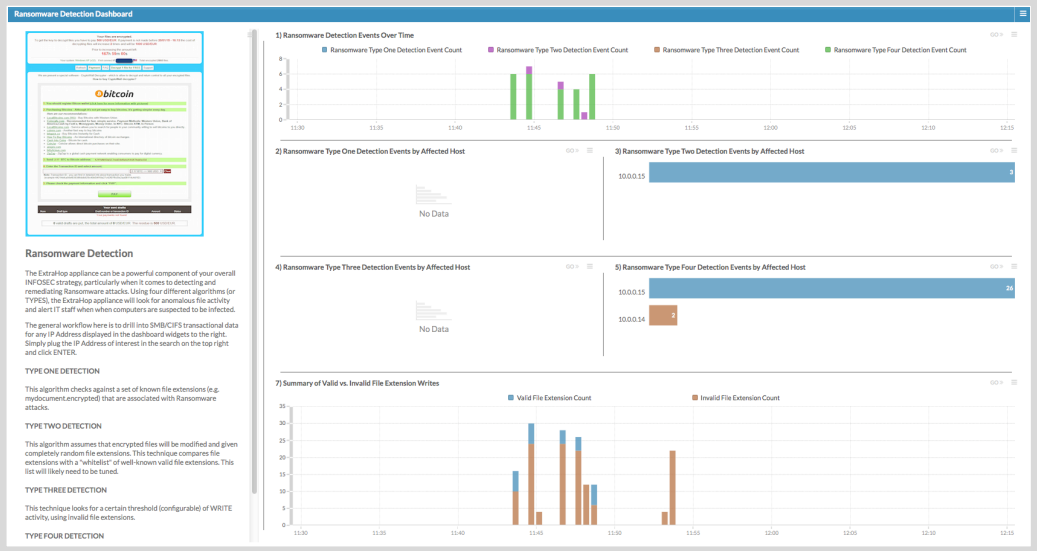
The code snippet above defines a URL path in which to make an outbound REST call, once the ExtraHop platform observes a ransomware infection. The variable `my_NAC` refers to a predefined endpoint for the ExtraHop Open Data Stream, which you would configure through the ExtraHop admin console. Once the NAC platform receives the REST call, it puts the infected workstation in quarantine so that it can no longer encrypt network files.

Controlling the Situation: Rapid Investigation and Response

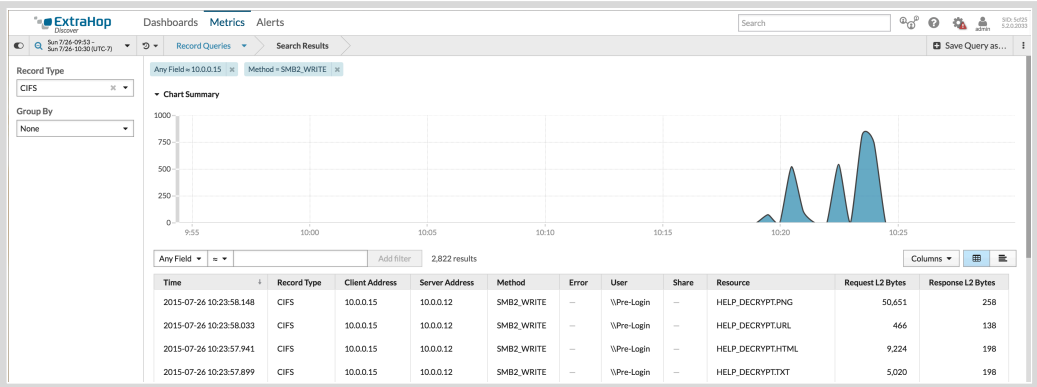
Beyond detection, the ExtraHop platform offers excellent investigation capabilities. You can easily drill down to see which clients received the malicious file and the IP address from which the malware was downloaded. The platform makes it possible for you to detect and respond to a ransomware infection in real time—early enough to minimize damage to your operations.

If you want to automate a response by integrating with your existing firewall infrastructure, you can use the ExtraHop platform's REST API to orchestrate a quarantine of an infected client. By examining which websites the client accessed and which DNS requests the client sent, you can also deploy appropriate perimeter controls to prevent future infections of the same ransomware variant.

This dashboard example shows a CryptoWall infection propagating through several sandboxed workstations. This solution has also successfully detected ransomware in the environments of ExtraHop customers.



ExtraHop enables incident response teams to quickly search through a client machine's past transactions to uncover origination vectors and C&C communications. This screen shows a filtered view of only CIFS WRITE transactions for the infected client at 10.0.0.15. You can see the names of the encrypted files as well as the ransom note.



Real-World Case Study: Health Services Provider

Challenge

Early in 2016, an employee with 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. His machine had been infected with ransomware, and it was already working to encrypt files on network shares to which the employee had access.

In response, the IT and security teams at the health services provider needed to determine which files and systems had been impacted, and find out how and when the employee's machine had become infected.

Solution

Using ExtraHop's analysis of all east-west traffic, including CIFS/SMB WRITE operations from the infected client to the network share, the IT and security teams were able to see which files the ransomware had been overwritten. In turn, they were able to quickly isolate impacted assets and stop the attack from progressing.

While the most critical step in thwarting a ransomware attack is blocking its access to network resources, it's also crucial to understand when and how the client machine or user was infected in the first place. Using the look-back functionality in the ExtraHop platform, the security team for the health services provider was able to investigate the employee's activity on his machine, 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 intentionally downloaded, but from a particular URI on which the employee had clicked.

Benefits

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 platform, the organization's information security team was able to quickly identify and isolate compromised systems, as well as create alerts for the file extensions associated with the ransomware in case they were observed in the future.

Community-Sourced Security Analytics

There is a growing community of IT professionals taking advantage of the open and extensible ExtraHop platform to develop and share security-focused enhancements. Community members have developed ExtraHop bundles to detect and alert on high-profile vulnerabilities such as Heartbleed and Shellshock, as well as specific tasks such as tracking privileged logins. Visit our community forum to see how ExtraHop users are working together to create and improve their security posture at https://forums.extrahop.com.

Some examples of security-related bundles created by the ExtraHop community:

- **Credit cards passed in the clear –** Detects valid credit card numbers passed over unencrypted HTTP. [link]
- **Expiring SSL certificates –** Includes a custom page and alerts for soon-to-expire SSL certificates. [link]
- **Active Directory –** Builds real-time metrics for the following AD Services: User Accounts, Computer Accounts, DNS, LDAP, Global Catalog, and Group Policy loads. [link]
- **Russian DNS queries –** Ties DNS queries for ".ru" domains back to the clients making the query. [link]

Conclusion

The ransomware epidemic is a profit machine for cybercriminals and will continue to spread until the industry builds effective defenses that tip the cost-reward balance and make ransomware more work than it is worth. Traditional approaches that focus on the perimeter and rely on signatures provide insufficient protection and leave IT organizations with zero visibility into east-west traffic.

The ExtraHop solution for ransomware detection focuses on observed behavior on the network. While cybercriminals can get past signature-dependent firewalls and end-point protection products, they cannot hide their activity on the network. Enterprises large and small are using the ExtraHop platform today to detect and shut down ransomware activity in real time. You don't have to wait for the industry to catch up with cybercriminals. You can get the visibility you need *today* to detect and mitigate ransomware attacks on your network and reduce the likelihood of ever needing to pay a ransom.

About ExtraHop

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

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)