



Ransomware | MITRE Techniques Demo Test Drive



Overview:

Ransomware attacks have become increasingly common with attackers targeting organizations with weak security practices. In fact, a recent survey revealed that 85% of organizations have fallen prey to ransomware in the past five years. And this crime pays: The predicted global cost of ransomware attacks has climbed steeply with a more than 4x increase between 2017 and 2022 to an estimated \$20 Billion, and may be up to 265 Billion by 2031.

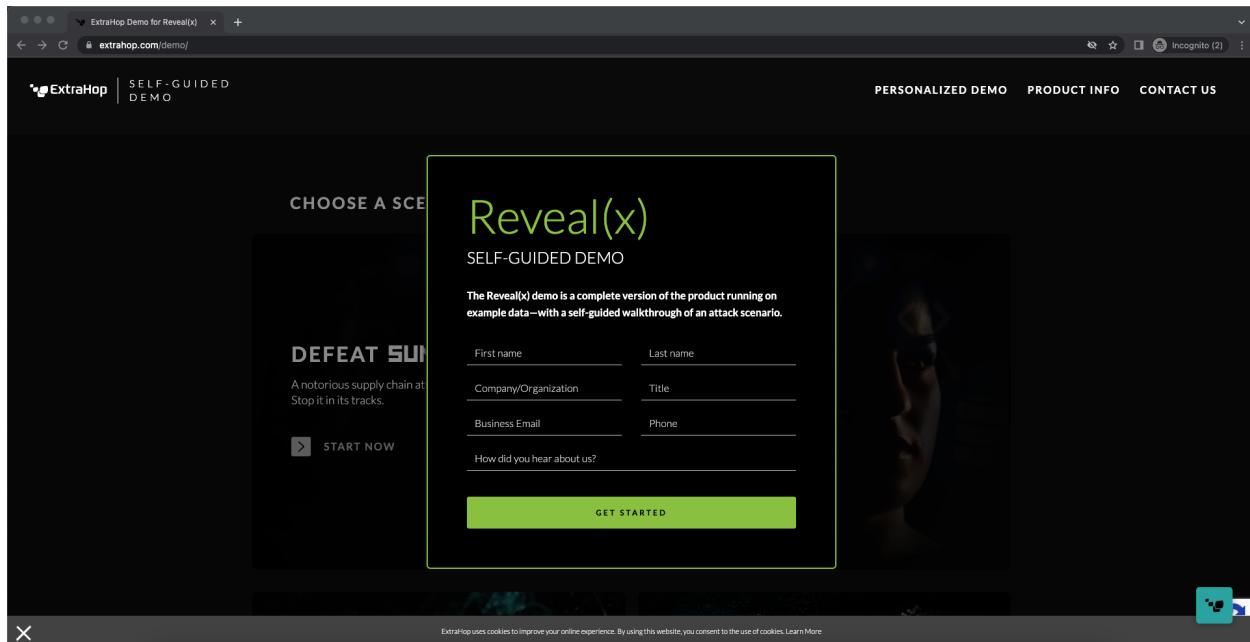
Indeed, modern ransomware attacks are so profitable that criminal groups like Black Basta, Lock Bit, Conti, and formerly REvil are continually developing new and innovative ways to systematically attack organizations while simultaneously increasing the difficulty of detection and prevention. These tactics have included the use of encrypted protocols to obscure actions such as exploitation, data gathering, and the exfiltration of data for the purposes of extortion.

Unlike early ransomware attacks that focused on targets of opportunity, modern ransomware attacks leverage detailed playbooks that rapidly take advantage of new vulnerabilities to gain access to their victims' networks.

One prominent example is the speed with which the BlackByte ransomware gang began leveraging the Proxy-Logon and Proxy-Shell vulnerabilities as part of their standard attack playbook. The adaptability of these criminal groups and their ability to bypass traditional perimeter defenses serves to underscore the necessity of midgame detection techniques.

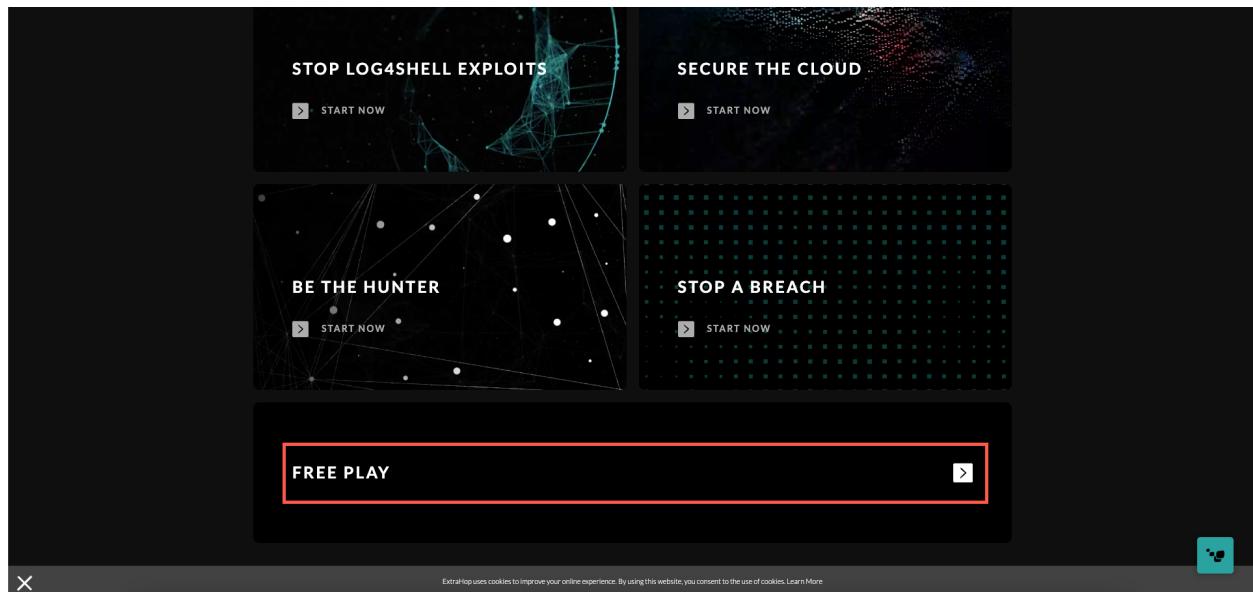
This lab is intended to teach users how to leverage the ExtraHop demo platform to view current detections, alerts, and assets. These environments may be traditional, on-premise, virtual, or cloud. We will show the power of the ExtraHop platform and its ability to passively ingest network data, out-of-band and without the necessity of end-point agents.

1. Login in to the ExtraHop Demo Platform <https://extrahop.com/demo/>
2. You should be prompted with the login info below, please provide your user details and click 'Get Started'.





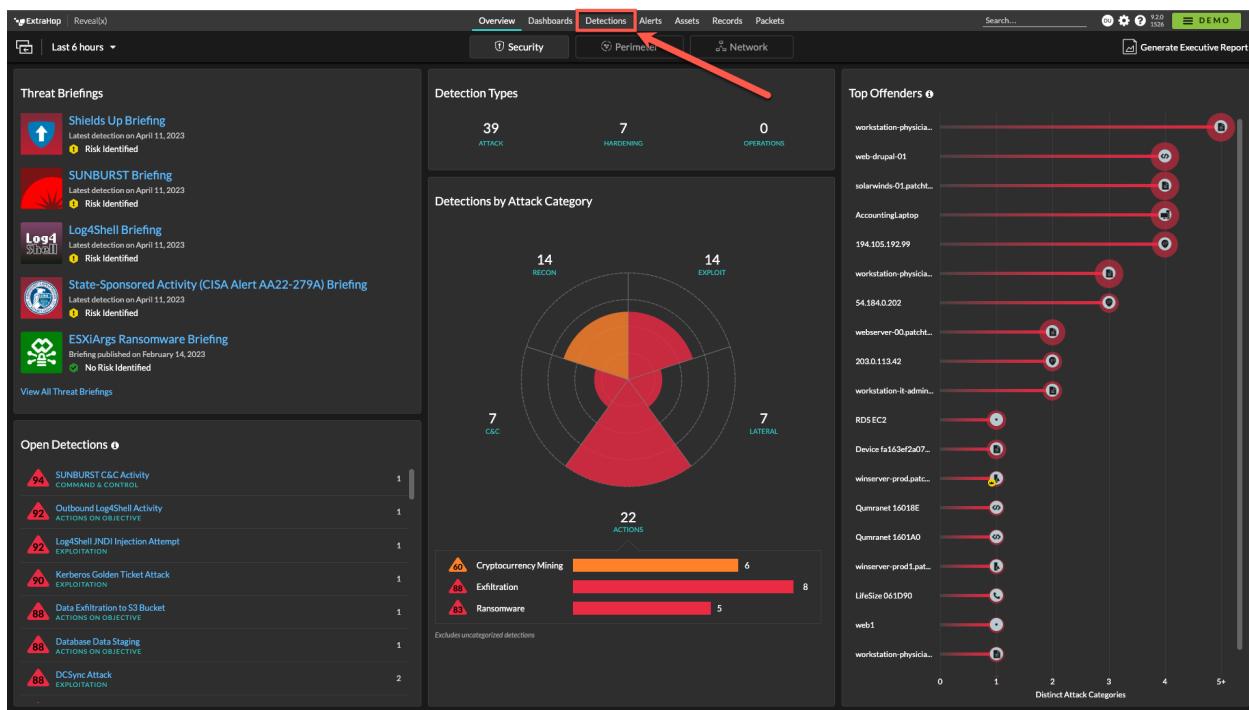
3. There are several guided scenarios listed that you could use at your leisure to walk through the platform capabilities. Please scroll down to the bottom of the page and click on 'FREE PLAY'. This provides you with unscripted access and you will follow the steps below.



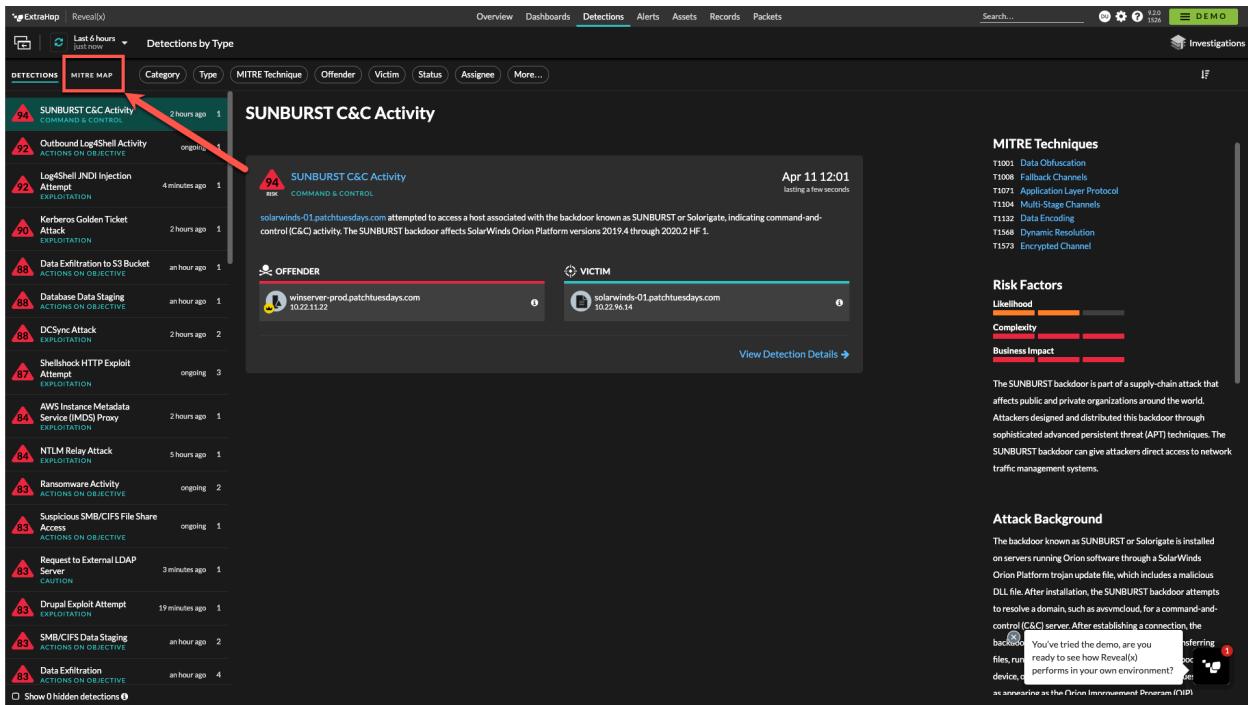
As you can see, once you're logged in, there are several different charts that highlight rich detail in the Overview pane. The separate panes located within here include:

- Threat Briefings: These include details on current threats including an overview of your environment in a quick and easy overview.
- Detections: These are the current open detections within the platform and will provide Detection Card detail.
- Detection Types: Are summarized overview of each type.
- Detection by Attack Category: Maps these to a heat map of the common categories, as defined within the platform.
- Top Offenders: Covers the endpoints in your environment and the distinct number of categories found for each.

1. Click on the top-level Detections tab, as shown below to go to the detections page.

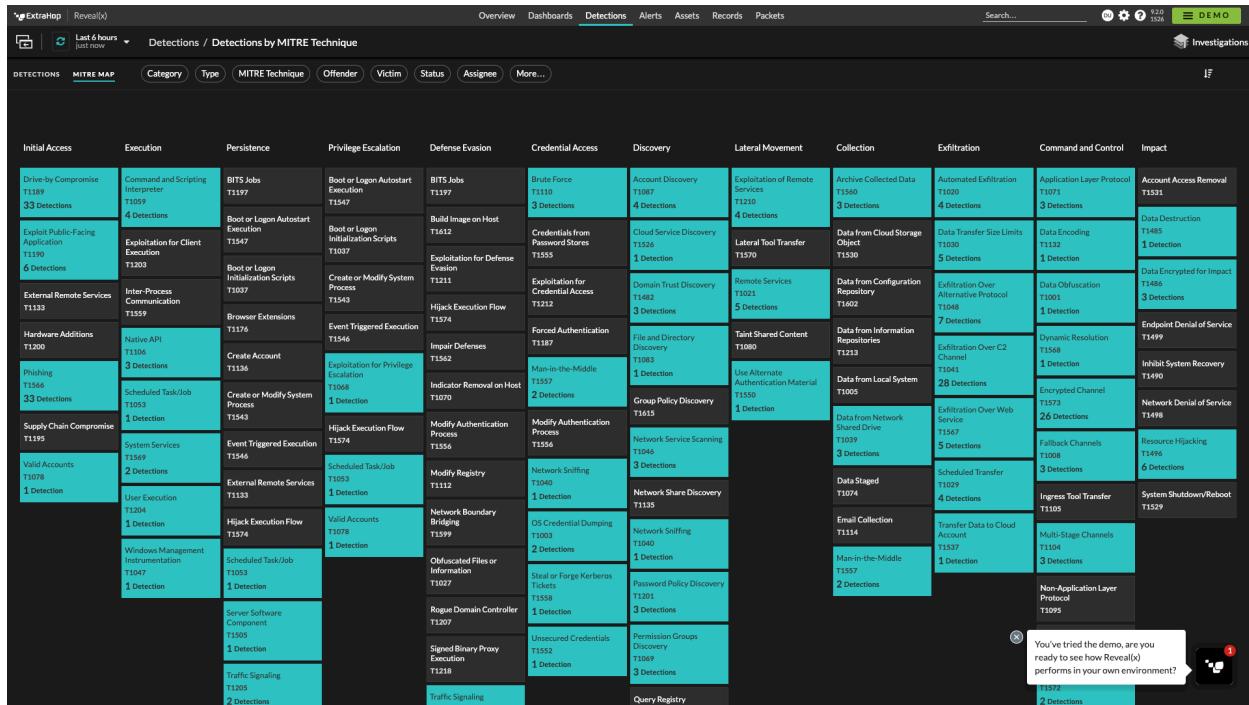


2. From here, we see all of the detections and some additional detail as each are highlighted, including time of the detection, offender and the victim, a brief overview the detection and the associated risk score as assigned by the platform.
3. Feel free to click on a few others to explore the Detections found in the network.
4. From here, click on the 'MITRE MAP', as noted below to go the mapping of the detections to the MITRE ATT&CK framework.



The screenshot shows the ExtraHop interface with the 'Detections' tab selected. The main pane displays a list of detections, with the first one expanded to show more details. The expanded detection is for 'SUNBURST C&C Activity' and includes fields for Offender (winserver-prod.patchtuadays.com), Victim (solarwinds-01.patchtuadays.com), and a timestamp (Apr 11 12:01). The sidebar on the right contains sections for 'MITRE Techniques' (listing T1001 through T1573), 'Risk Factors' (Likelihood, Complexity, Business Impact), and 'Attack Background' (describing the SUNBURST backdoor and its impact on traffic management systems).

5. From here, you can see the MITRE ATT&CK matrix and the mapping of the detections from the previous page. These are also all clickable to get the MITRE subcategory ID and associated detections found by the platform.
6. ExtraHop has an extensive listing and industry leading detection capability with 123 of the total MITRE ATT&CK Techniques covered and 86% of coverage of all network addressable techniques covered.
7. Click on the Detections tab, listed next to the MITRE MAP in the upper left corner to return to the Detections tab.



The screenshot shows the ExtraHop interface for 'Detections / Detections by MITRE Technique'. The top navigation bar includes 'Overview', 'Dashboards', 'Detections' (which is selected), 'Alerts', 'Assets', 'Records', and 'Packets'. A search bar and various filter options like 'Category', 'Type', 'MITRE Technique', 'Offender', 'Victim', 'Status', 'Assignee', and 'More...' are available. The main content area displays a grid of MITRE ATT&CK techniques categorized into columns: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, Command and Control, and Impact. Each cell in the grid contains a specific technique ID (e.g., T1109, T1547) and a count of detections (e.g., 33 Detections, 4 Detections). A tooltip at the bottom right of the grid asks if the user wants to try the demo.

8. As we'll be focusing methods to detect Ransomware and the initial attack vectors, adversary tactics and techniques used by bad actors, scroll down on the left to Ransomware to bring up the Ransomware we've detected in the environment.

SUNBURST C&C Activity

94 RISK SUNBURST C&C Activity

Apr 11 12:01 lasting a few seconds

Actions on Objective: ongoing 2

Offender: winserver-prod.patchtuesdays.com (10.22.11.22)

Victim: solarwinds-01.patchtuesdays.com (10.22.16.14)

[View Detection Details](#)

Risk Factors

- Likelihood:
- Complexity:
- Business Impact:

The SUNBURST backdoor is part of a supply-chain attack that affects public and private organizations around the world. Attackers designed and distributed this backdoor through sophisticated advanced persistent threat (APT) techniques. The SUNBURST backdoor can give attackers direct access to network traffic management systems.

Attack Background

The backdoor known as SUNBURST or Solorigate is installed on servers running Orion software through a SolarWinds Orion Platform update file, which includes a malicious DLL file. After installation, the SUNBURST backdoor attempts to resolve a domain, such as avsmvcloud, for a command-and-control (C&C) server. After establishing a connection, the backdoor performs its malicious activities, such as stealing files, running processes, and so on.

9. You should now see the pane below. Please click on View Detection Details as show below.

Ransomware Activity

83 RISK Ransomware, ACTIONS ON OBJECTIVE

Apr 11 12:00 Ongoing

Actions on Objective: ongoing 2

Offender: Device fa163ef2a0730000 (192.168.0.33)

Victim: Device fa163ef7be540000 (192.168.0.25)

[View Detection Details](#)

MITRE Techniques

- T1486 Data Encrypted for Impact

Risk Factors

- Likelihood:
- Complexity:
- Business Impact:

Ransomware attacks are increasingly common because they provide attackers with a high return on their investment. Different strains of ransomware malware are easily acquired or created in multiple programming languages. The impact of ransomware on a business can be devastating, especially if sensitive or business-critical data is lost through encryption, or if a ransom is paid.

The system might change the risk score for this detection.

Attack Background

Ransomware is a type of malware that encrypts files on a victim machine, which makes those files inaccessible until the victim pays a ransom for the decryption key. Ransomware attacks can originate from phishing emails, exploited network services, or large-scale attack campaigns. After the ransomware encryption begins, the encryption process can quickly spread throughout the network and across file shares on critical assets.

View Detection Details

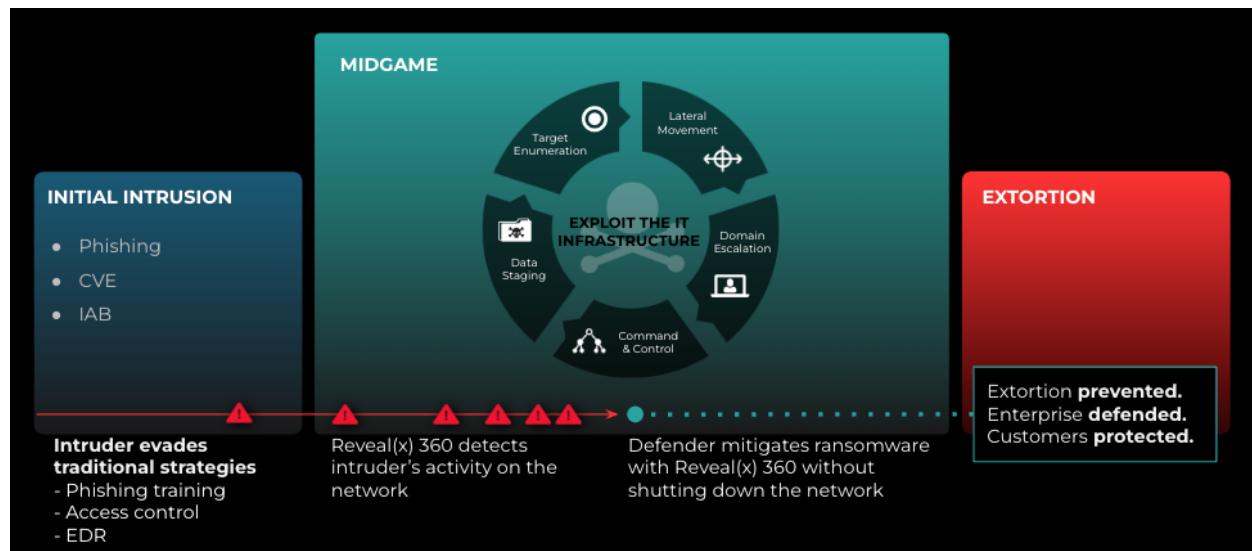
You've tried the demo, are you ready to see how Reveal(x) performs in your own environment? [Get Started](#)

THE MIDGAME:

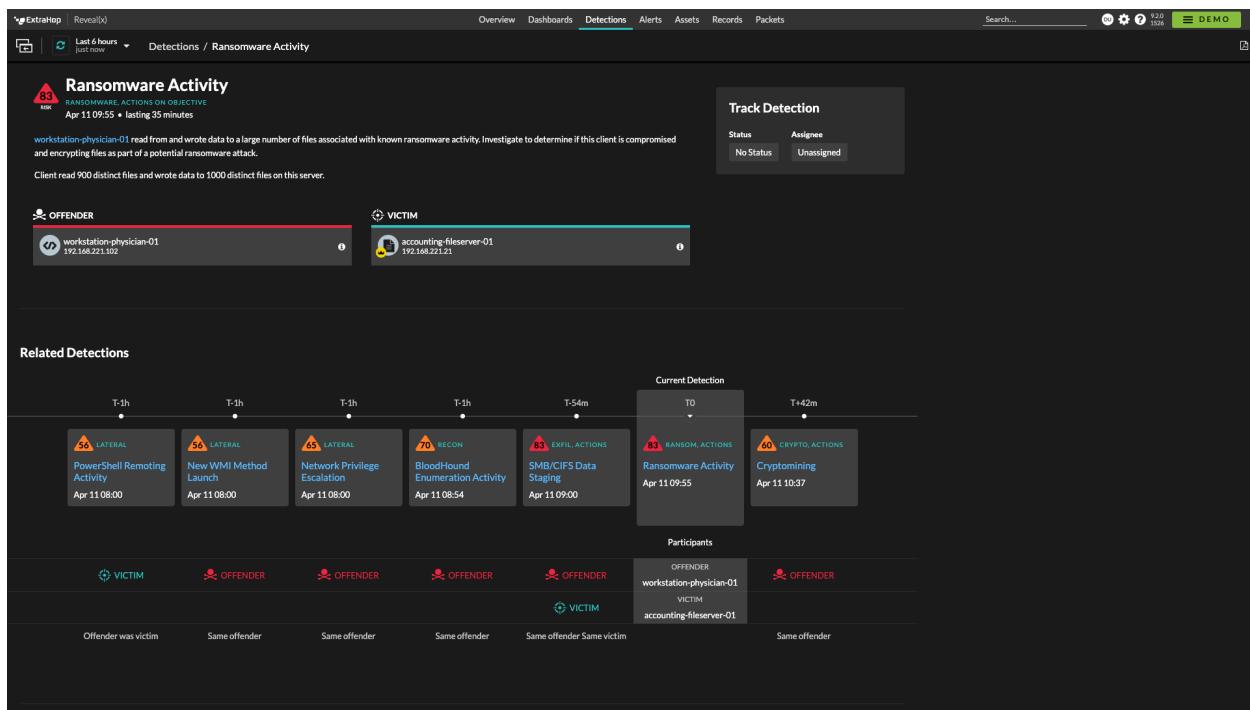
Preventing initial access may not be possible, but with [ExtraHop Reveal\(x\) 360](#), defenders can detect and stop ransomware in the midgame before they achieve real damage.

Using machine learning, you can detect behaviors that signal a ransomware attack in progress, with alerts that flag attackers as they enumerate targets, escalate domain privileges, and send C2 over noisy channels like DNS. It also spots data staging before encryption starts, allowing your business to avert the massive operational, reputational, and financial loss that accompanies a ransomware attack.

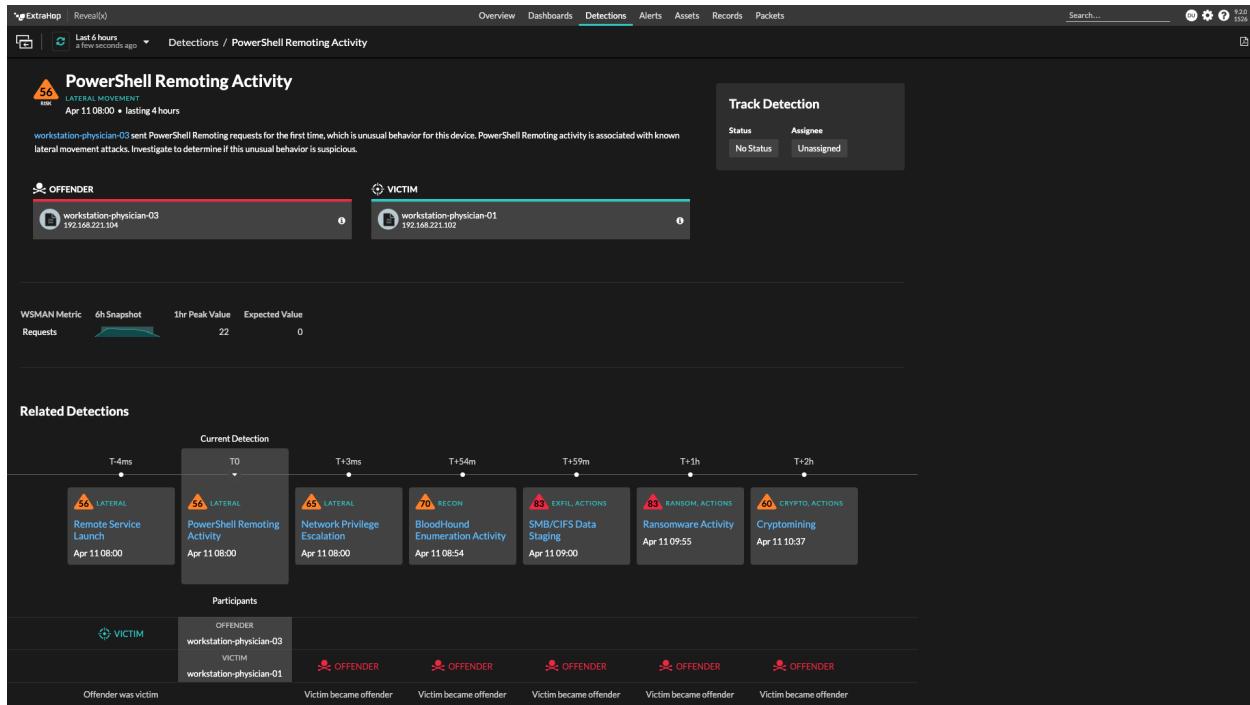
Ransomware gangs have adopted advanced tactics in the east-west corridor to make victims more likely to pay the ransom. They exploit existing IT infrastructure (a tactic known as living-off-the-land) like remote desktop protocol (RDP) to move stealthily and persist for longer periods of time before springing their trap, putting security and IT at a disadvantage to prevent large-scale ransomware incidents.



1. The Detection card below has a great deal of information located on it. As you can see, it also displays related detections to the ransomware detection that we first noted.
2. From here, we can see the offender and victim in this specific detection. It lists the related detections both prior and post ransomware encryption, even with the bad actor having installed Cryptomining software transferred over the Stratum protocol and connecting to the mining pool at pool.tupportxmr.com.



3. As we look to investigate this attack, we can see that the bad actor has executed a number of methods in their playbook.
4. In the summary above, you can note that the summary and time required to execute.
5. We can see that there are a number of methods utilized here, including Remote PowerShell to Privilege Escalation, to BloodHound enumeration, etc.



6. As you return to the Ransomware Detection Card, please scroll down to note additional details that the platform has included for Incident Response, as well as understanding the 'blast-radius' of the attack, as shown below.

7. We can see the files that have been encrypted when accessed from the ‘workstations-physician-01’ PC to the ‘accounting-fileserver-01’.

8. Note that we can see the bad actor has encrypted 2,000 total files.

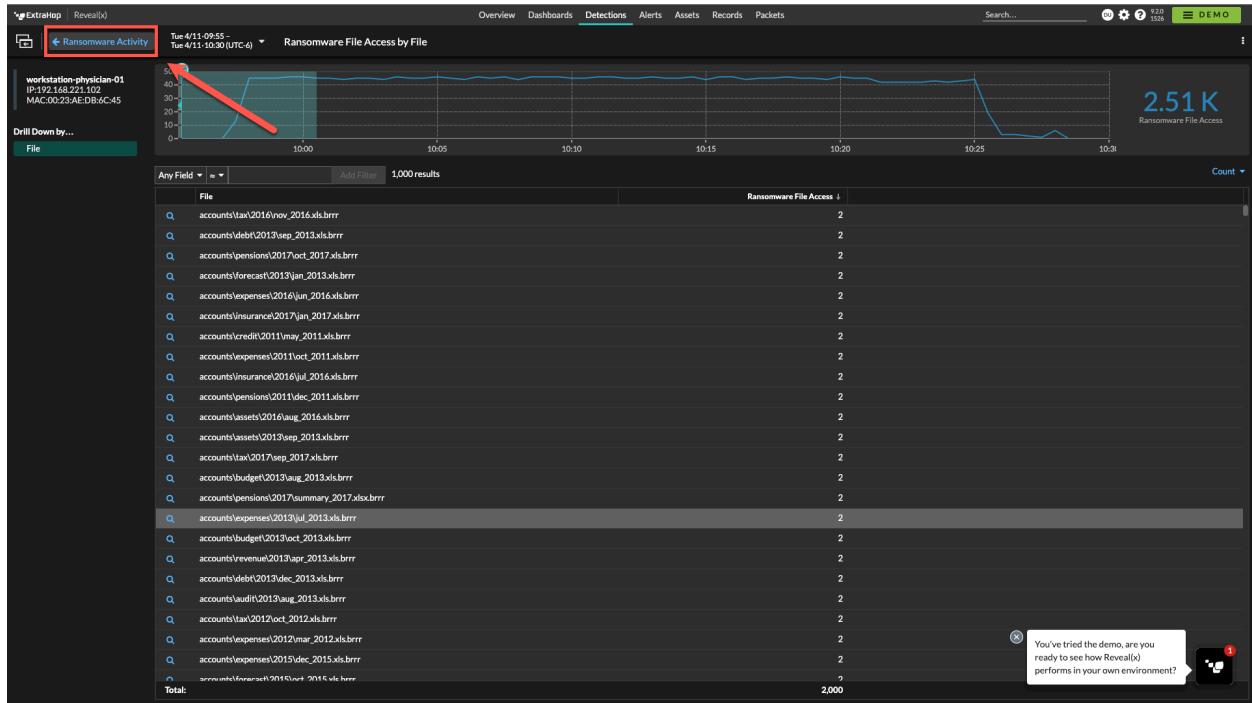
9. For additional detail, click on ‘Go to Metric Details as noted below’.

Files	
View the files with ransomware extensions	
File	Ransomware File Access ↓
accounts\expenses\2016\oct_2016.xls.brrr	2
accounts\tax\2015\mar_2015.xls.brrr	2
accounts\insurance\2015\nov_2015.xls.brrr	2
accounts\credit\2015\dec_2015.xls.brrr	2
accounts\revenue\2012\feb_2012.xls.brrr	2
accounts\insurance\2010\oct_2010.xls.brrr	2
accounts\revenue\2016\jan_2016.xls.brrr	2
accounts\budget\2011\feb_2011.xls.brrr	2
accounts\credit\2017\jan_2017.xls.brrr	2
accounts\payroll\2017\jun_2017.xls.brrr	2
accounts\credit\2013\aug_2013.xls.brrr	2
accounts\insurance\2013\sep_2013.xls.brrr	2
accounts\forecast\2014\jul_2014.xls.brrr	2
accounts\insurance\2012\aug_2012.xls.brrr	2
Total:	2,000

[Go to Metric Details](#)

10. From here we can drill down and visualize the timeframe, and encrypted files. Click on the magnifying glass for additional detail for methods, time, and our record detail for each.

11. Once done, please click in the upper left-hand corner on ‘Ransomware Activity’ as noted below to return to the detection card.

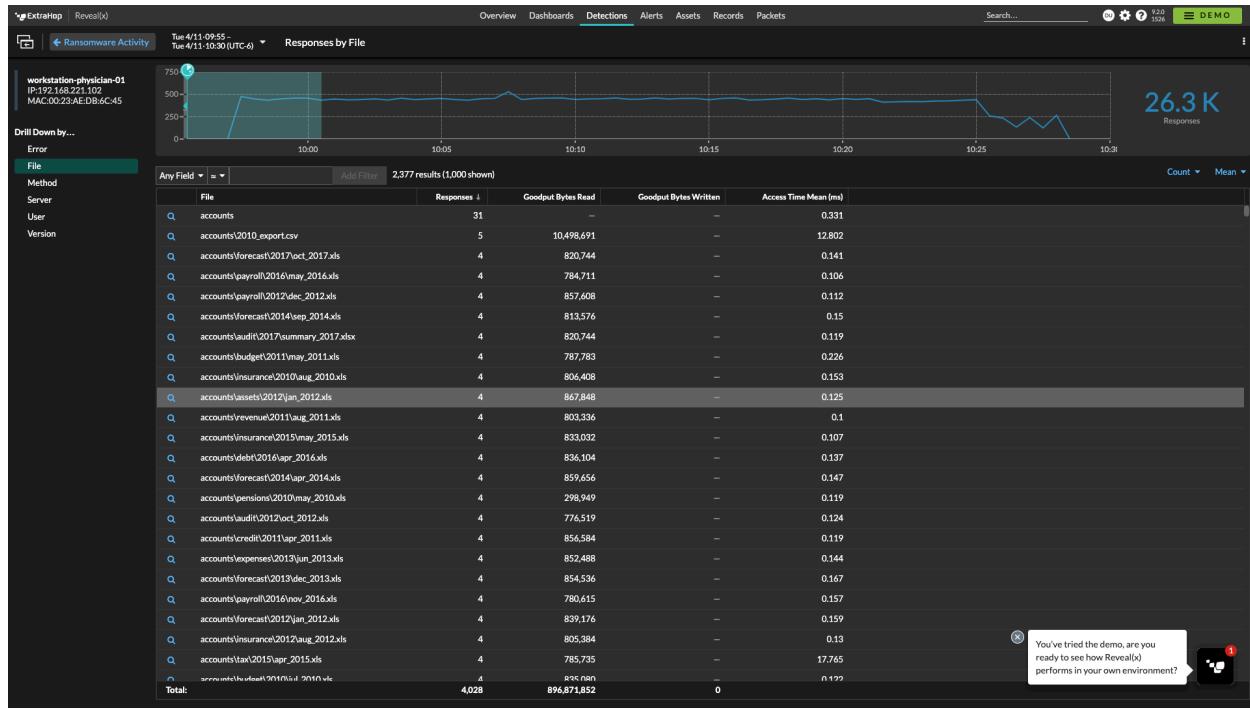


12. As you continue to scroll, you can see files accessed, but not encrypted. This may be important to understand the data accessed when evaluating other post breach items, such as Impact to the Brand, PII, Intellectual Property, etc.

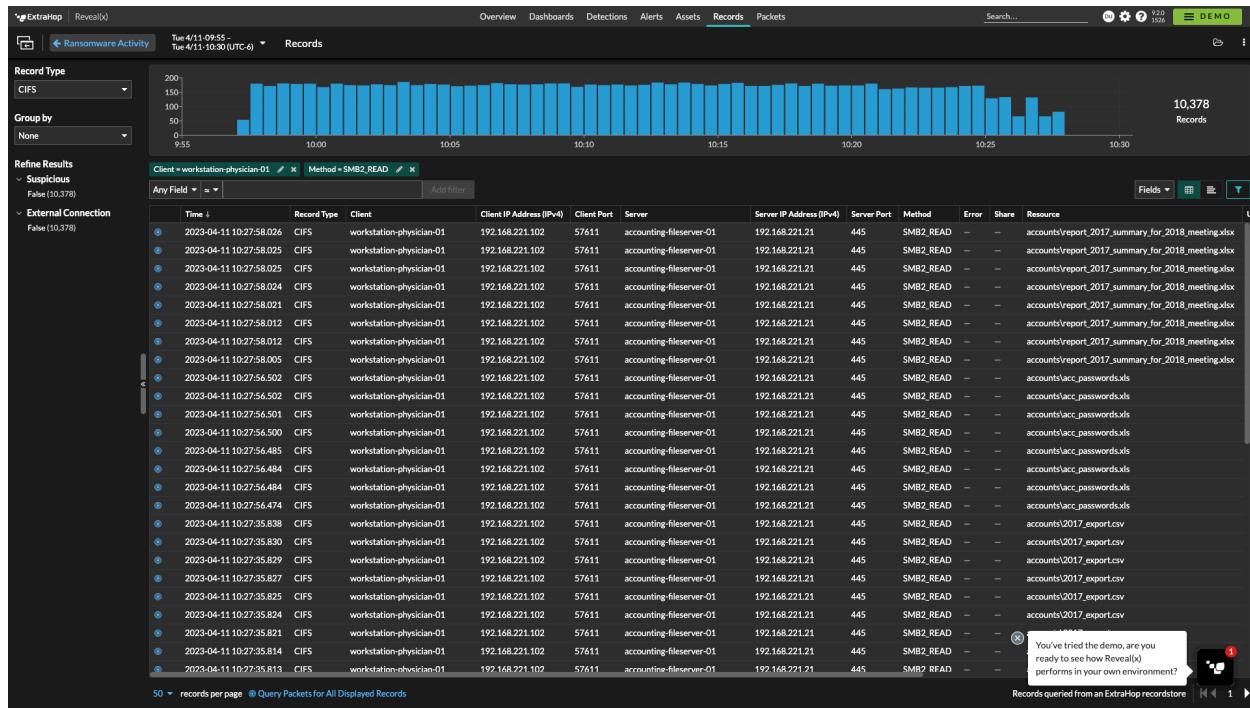
Files					
View the files accessed					
	File	Responses ↓	Goodput Bytes Read	Goodput Bytes Written	Access Time Mean (ms)
Q	accounts	31	—	—	0.331
Q	accounts\2010_export.csv	5	10,498,691	—	12.802
Q	accounts\forecast\2017\oct_2017.xls	4	820,744	—	0.141
Q	accounts\payroll\2016\may_2016.xls	4	784,711	—	0.106
Q	accounts\payroll\2012\dec_2012.xls	4	857,608	—	0.112
Q	accounts\forecast\2014\sep_2014.xls	4	813,576	—	0.15
Q	accounts\audit\2017\summary_2017.xlsx	4	820,744	—	0.119
Q	accounts\budget\2011\may_2011.xls	4	787,783	—	0.226
Q	accounts\insurance\2010\aug_2010.xls	4	806,408	—	0.153
Q	accounts\assets\2012\jan_2012.xls	4	867,848	—	0.125
Q	accounts\revenue\2011\aug_2011.xls	4	803,336	—	0.1
Q	accounts\insurance\2015\may_2015.xls	4	833,032	—	0.107
Q	accounts\debt\2016\apr_2016.xls	4	836,104	—	0.137
Q	accounts\forecast\2014\apr_2014.xls	4	859,656	—	0.147
Total:		4,028	896,871,852	0	
Go to Metric Details					

13. Again, you now see that while over 4,000 files were accessed, just 2,000 were encrypted with the ransomware. As you click on the ‘Metric Details’ again, you can now drill down on the left-hand pane by:

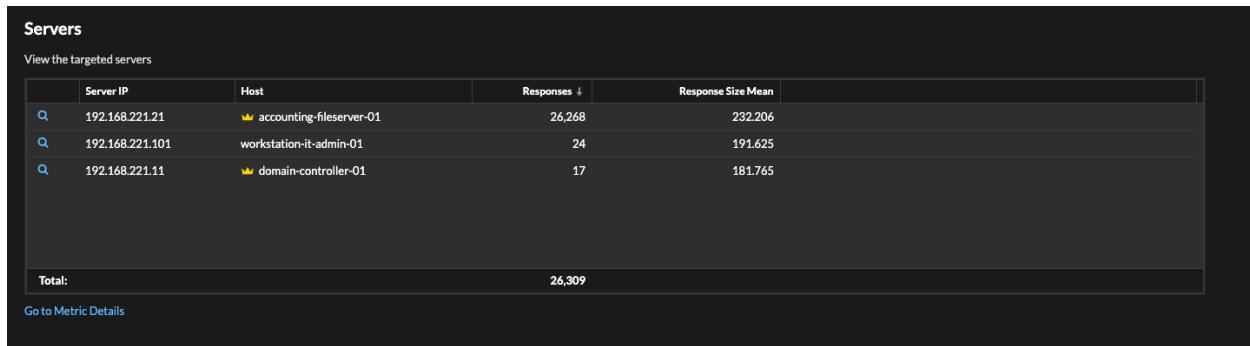
- a. Error
- b. File
- c. Method
- d. Server
- e. User
- f. Version



14. Additional drill down detail and associated metrics can be seen in the screen show below.



15. If we click in the upper left again on the ‘Ransomware Activity’ button and continue to scroll down, as we note the servers that were compromised during the breach.



Servers

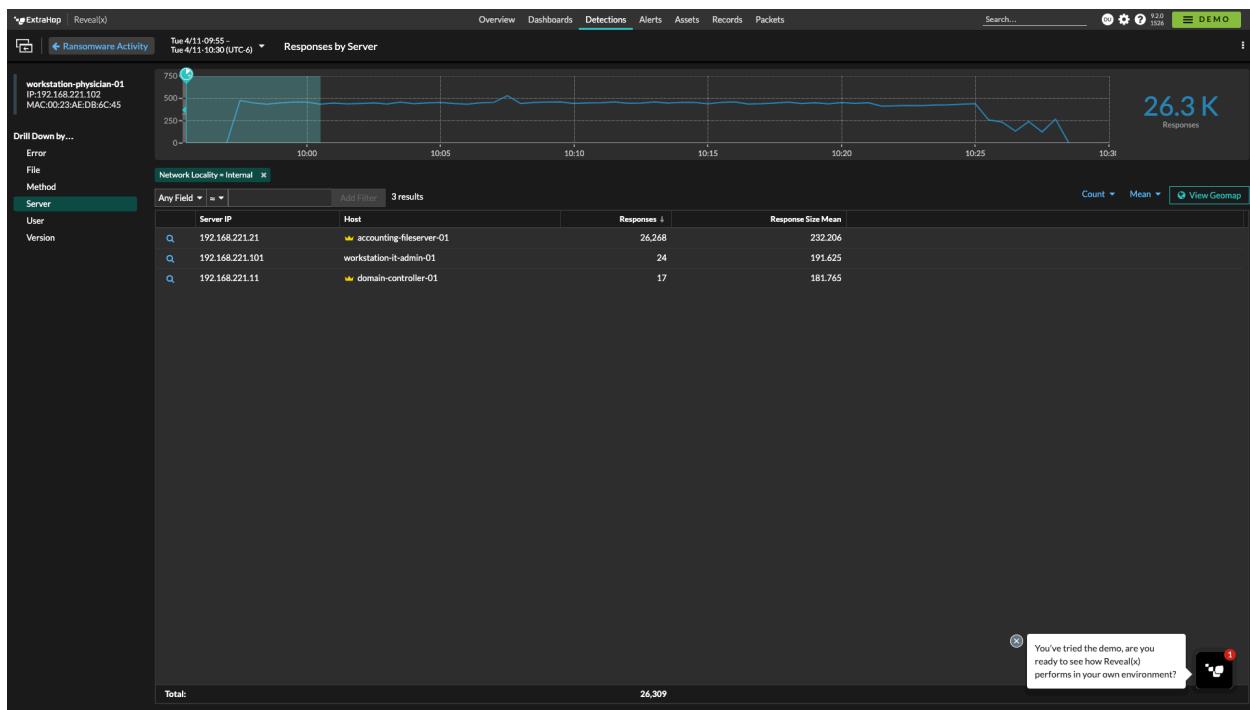
View the targeted servers

Server IP	Host	Responses ↓	Response Size Mean
192.168.221.21	accounting-fileserver-01	26,268	232.206
192.168.221.101	workstation-it-admin-01	24	191.625
192.168.221.11	domain-controller-01	17	181.765

Total: 26,309

[Go to Metric Details](#)

16. Again, going to the ‘Metrics Details’ provides us additional detail on the Servers, as shown below.



Ransomware Activity

Tue 4/11 09:55 | Tue 4/11 10:30 (UTC-4) | Responses by Server

workstation-physician-01
IP: 192.168.221.102
MAC: 00:23:AE:DB:6C:45

Drill down by...
Error
File
Method
Server
User
Version

Network Locality = Internal

Any Field ▾ = ▾ Add Filter 3 results

Server IP	Host	Responses ↓	Response Size Mean
192.168.221.21	accounting-fileserver-01	26,268	232.206
192.168.221.101	workstation-it-admin-01	24	191.625
192.168.221.11	domain-controller-01	17	181.765

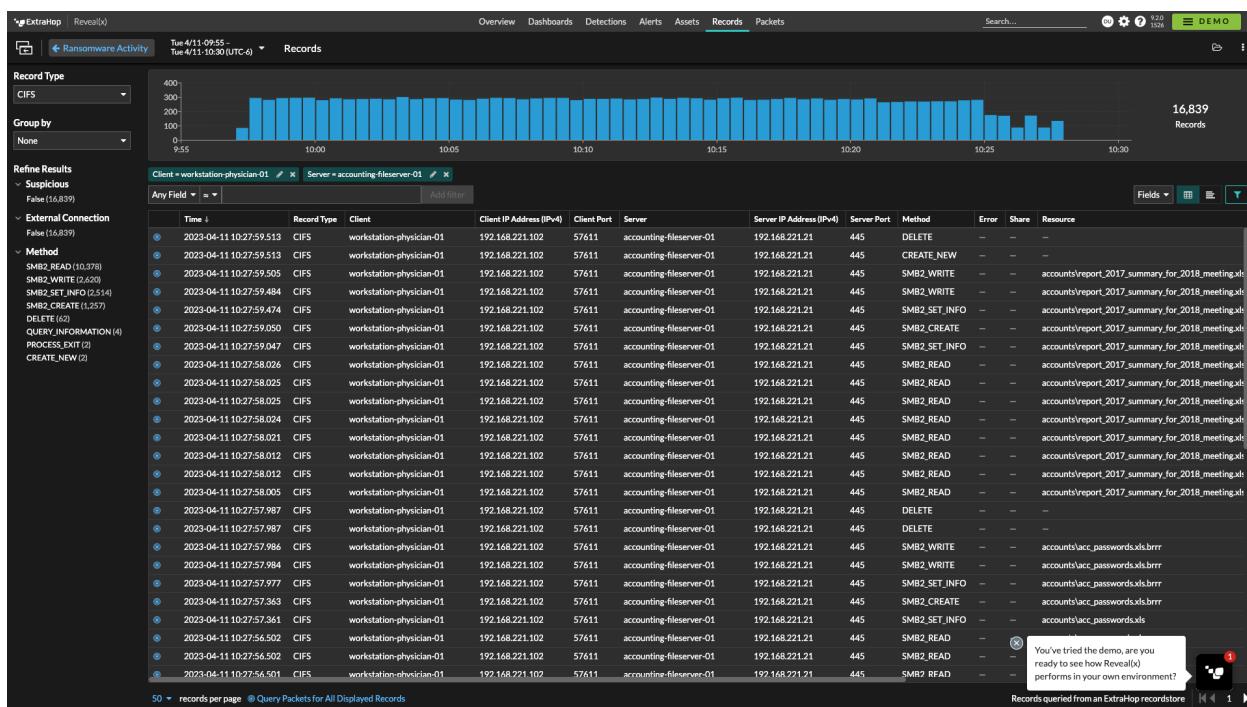
26.3 K Responses

Total: 26,309

You've tried the demo, are you ready to see how Reveal(x) performs in your own environment? [Get Started](#)



17. Clicking on the magnifying glass for the ‘accounting-fileserver-01’ will now show us all metric detail for that server, including all files, methods, timelines and resources accessed.
 18. Note the Methods column and the different ones listed.



19. Clicking on the bullseye on the left of each record will take us to the packet capture that the platform stored during the breach. See below for details.



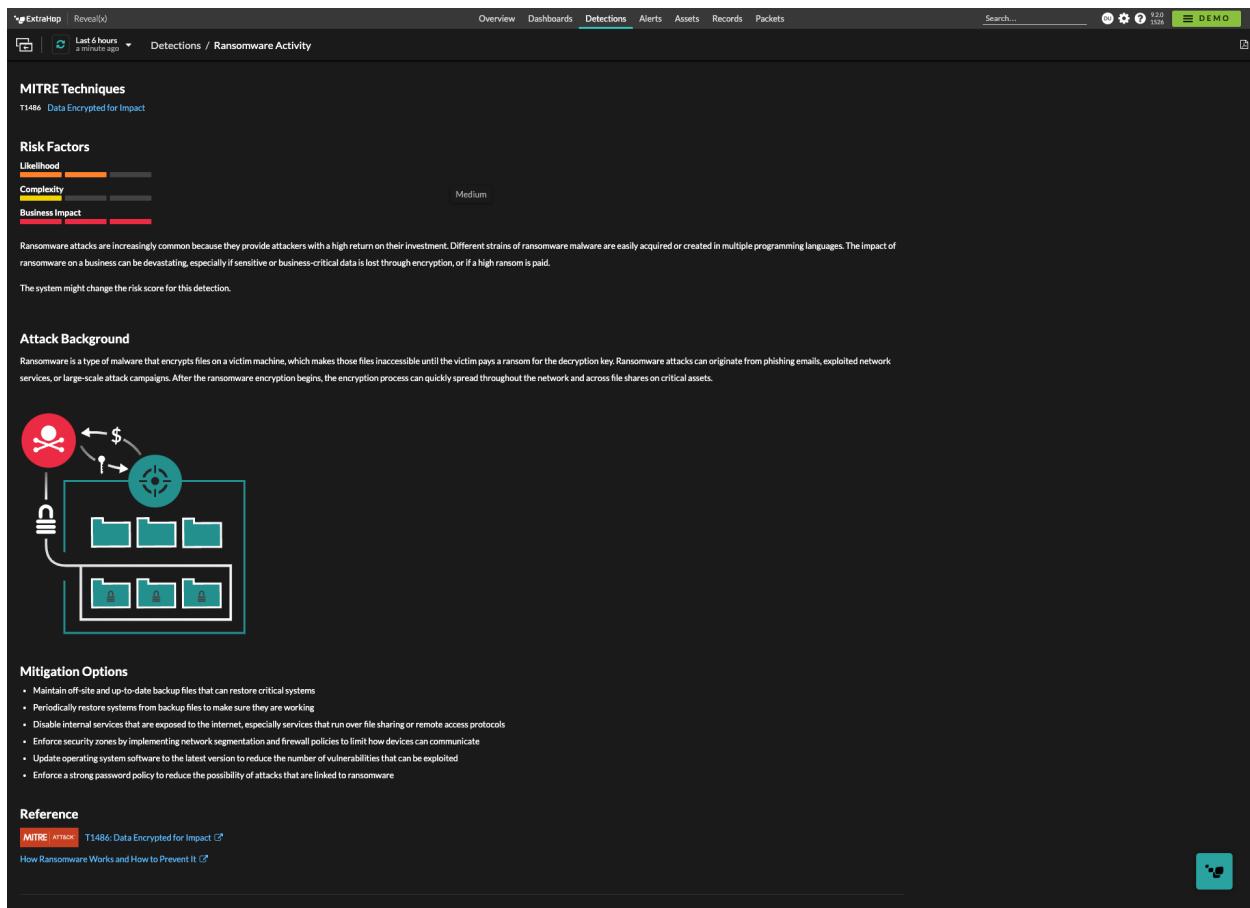
20. Here you can see the full transaction of each record as noted in the previous screen. We've also included the ability to download the PCAP for this specific record.

The screenshot shows the ExtraHop Reveal(x) interface with the following details:

- Header:** ExtraHop Reveal(x), Tue 4/11 09:55 - Tue 4/11 10:30 (UTC-6), Overview, Dashboards, Detections, Alerts, Assets, Records, Packets, Search..., Demo.
- Ransomware Activity:** 204,624 packets captured.
- Packet Query Results:** BPF = (host 192.168.221.102) and (host 192.168.221.21) and (port 445) x
- Table Headers:** Time, Src IP, Dst IP, IP Proto, Src Port, Dst Port, Flags, Bytes, Src MAC, Dst MAC, Ether/Type, VLAN ID.
- Data Preview:** Previewing 100 packets around Apr 11, 10:28:59.125 am. The table lists numerous TCP connections between 192.168.221.102 and 192.168.221.21, mostly on port 445, with ACK and ACK FRAG flags.
- Annotations:** A red arrow points from the "Until Apr 11, 10:30:01 am" button to the "Download PCAP" button. A callout bubble says "You've tried the demo, are you ready to see how Reveal(x) performs in your own environment?".

21. Opening the downloaded PCAP in Wireshark now shows us the full packet detail.

22. Again, click on the upper left corner on ‘Ransomware Activity’ and scroll down and you’ll see the MITRE ATT&CK Techniques used, background and additional mitigation options listed to recover from the breach.



MITRE Techniques

T1486: Data Encrypted for Impact

Risk Factors

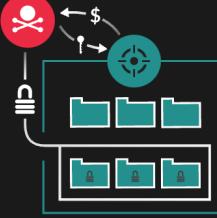
- Likelihood: High
- Complexity: Low
- Business Impact: Medium

Ransomware attacks are increasingly common because they provide attackers with a high return on their investment. Different strains of ransomware malware are easily acquired or created in multiple programming languages. The impact of ransomware on a business can be devastating, especially if sensitive or business-critical data is lost through encryption, or if a high ransom is paid.

The system might change the risk score for this detection.

Attack Background

Ransomware is a type of malware that encrypts files on a victim machine, which makes those files inaccessible until the victim pays a ransom for the decryption key. Ransomware attacks can originate from phishing emails, exploited network services, or large-scale attack campaigns. After the ransomware encryption begins, the encryption process can quickly spread throughout the network and across file shares on critical assets.



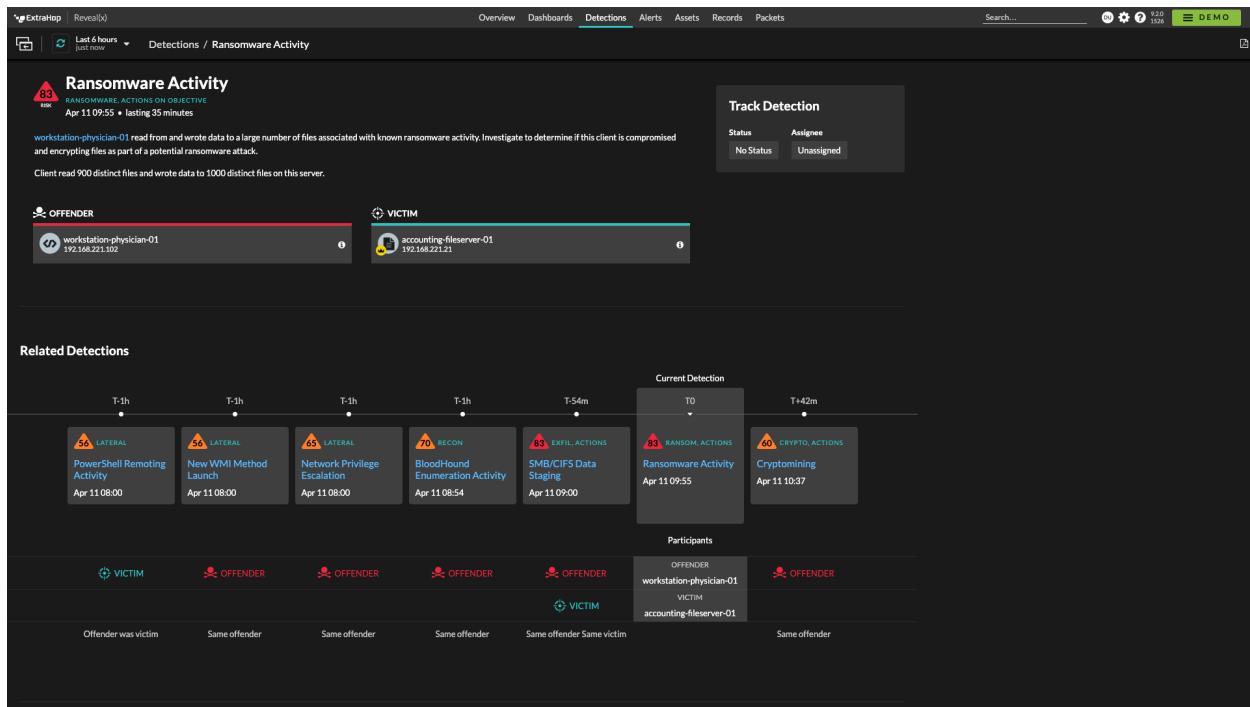
Mitigation Options

- Maintain off-site and up-to-date backup files that can restore critical systems
- Periodically restore systems from backup files to make sure they are working
- Disable internal services that are exposed to the internet, especially services that run over file sharing or remote access protocols
- Enforce security zones by implementing network segmentation and firewall policies to limit how devices can communicate
- Update operating system software to the latest version to reduce the number of vulnerabilities that can be exploited
- Enforce a strong password policy to reduce the possibility of attacks that are linked to ransomware

Reference

MITRE ATT&CK T1486: Data Encrypted for Impact ⓘ
How Ransomware Works and How to Prevent It ⓘ

23. Finally scrolling back up, you can now see how ExtraHop Reveal (x)360 is able to help gain visibility into a breach and provide better alerting prior to a full exfiltration of data or ransomware encryption.



The screenshot shows the ExtraHop Reveal (x)360 interface with the following details:

- Ransomware Activity:** 83 actions on objective, last 6 hours ago. Offender: workstation-physician-01 (192.168.221.102). Victim: accounting-fileserver-01 (192.168.221.21).
- Track Detection:** Status: No Status, Assignee: Unsigned.
- Related Detections:**
 - T-1h: 56 LATERAL PowerShell Remoting Activity (Apr 11 08:00)
 - T-1h: 56 LATERAL New WMI Method Launch (Apr 11 08:00)
 - T-1h: 65 LATERAL Network Privilege Escalation (Apr 11 08:00)
 - T-1h: 70 RECON Blood-Hound Enumeration Activity (Apr 11 08:54)
 - T-54m: 83 EXFIL ACTIONS SMB/CIFS Data Staging (Apr 11 09:00)
 - T0: 83 RANSOM ACTIONS Ransomware Activity (Apr 11 09:55)
 - T+42m: 60 CRYPTO ACTIONS Cryptomining (Apr 11 10:37)
- Participants:** Offender: workstation-physician-01; Victim: accounting-fileserver-01.
- Offender was victim:** Same offender.
- Same offender:** Same offender.
- Same offender:** Same offender.
- Same offender:** Same victim.
- Same offender:** Same offender.