

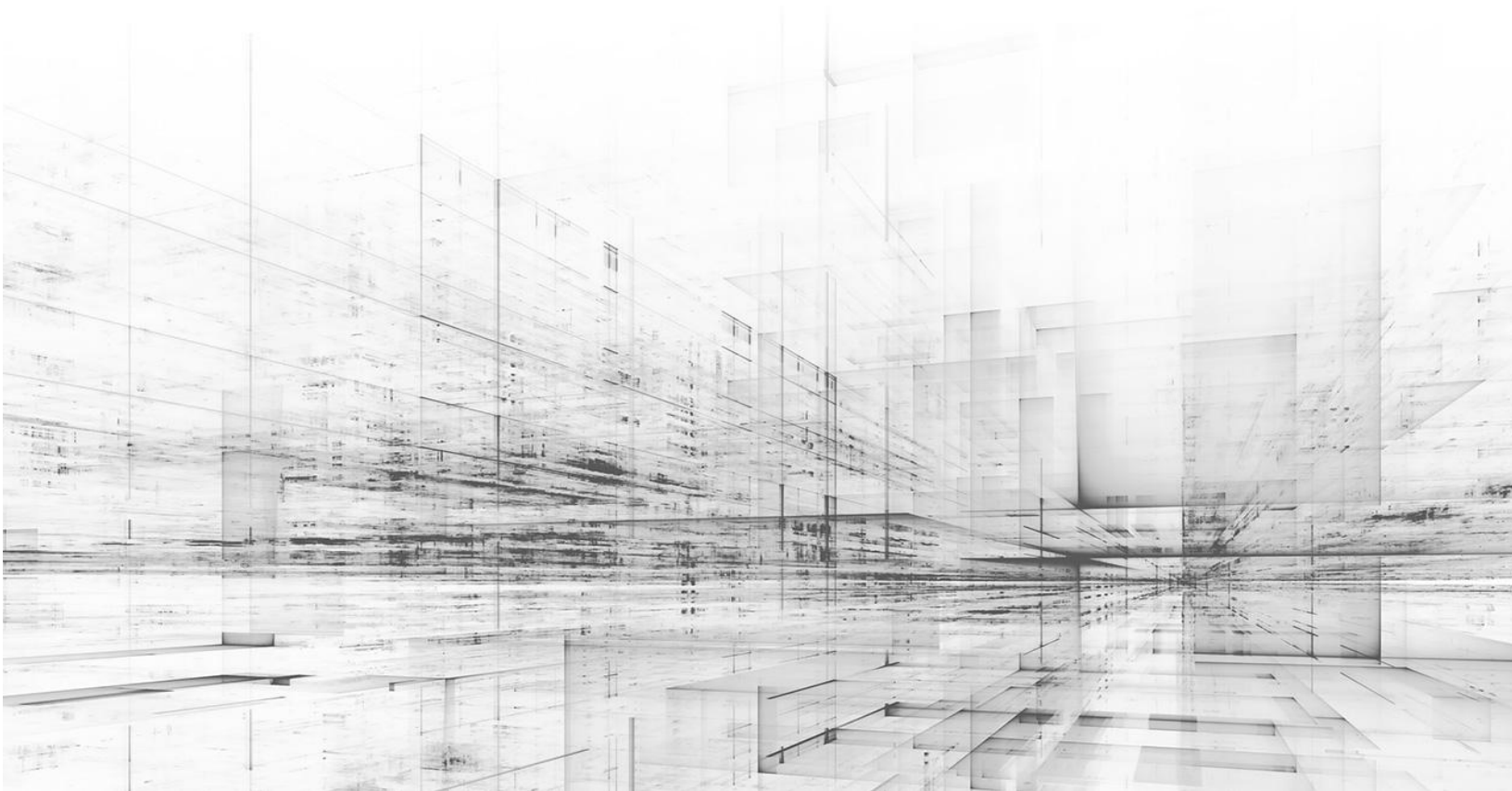
EXTRAHOP

Ransomware Mitigation

Lab Guide | July 2025

Modern ransomware is no longer just encrypting data. Attackers get their claws into your network infrastructure to amplify damage and halt your business operations. Stop them before they set their extortion trap.

In this lab, stop ransomware and other attacks, analyze network traffic and packet queries, discover security hygiene issues, and troubleshoot performance problems.



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.

Lab Introduction

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'.

ExtraHop SELF-GUIDED DEMO

PERSONALIZED DEMO PRODUCT INFO CONTACT US

CHOOSE A SCENARIO

Reveal(x)
SELF-GUIDED DEMO

The Reveal(x) demo is a complete version of the product running on example data—with a self-guided walkthrough of an attack scenario.

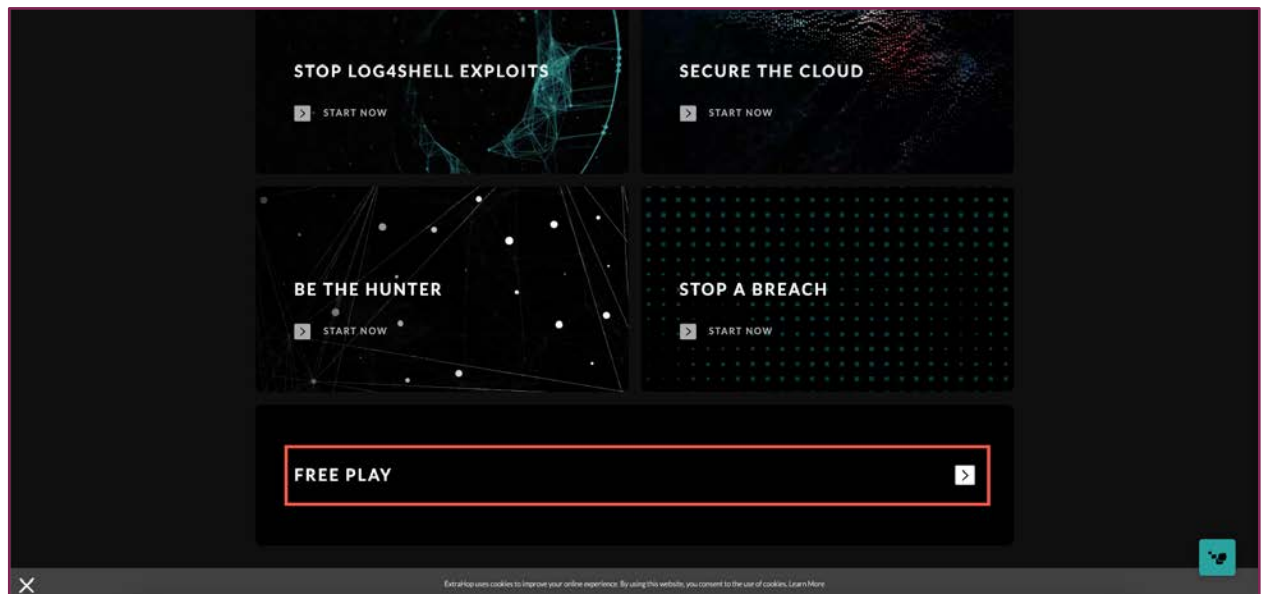
First name Last name
Company/Organization Title
Business Email Phone
How did you hear about us?

GET STARTED

DEFEAT SUN
A notorious supply chain attack. Stop it in its tracks.
START NOW

ExtraHop uses cookies to improve your online experience. By using this website, you consent to the use of cookies. Learn More

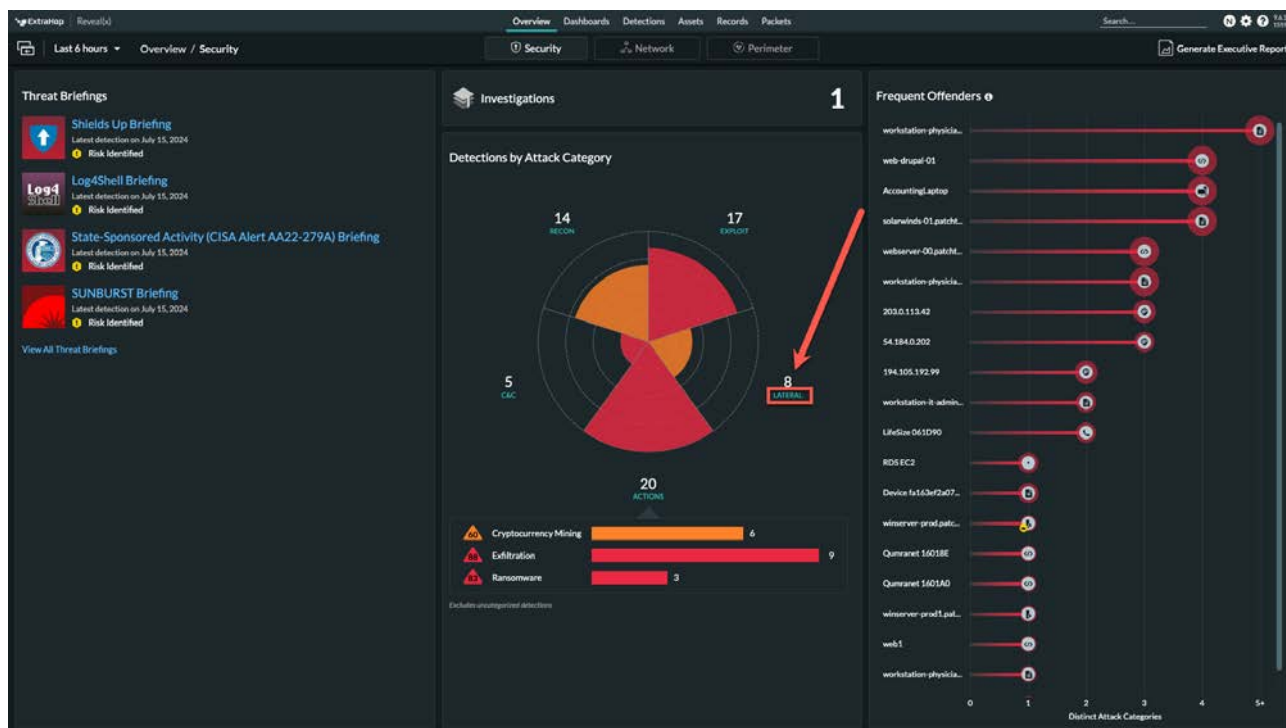
- There are several guided scenarios listed that you could use at your leisure to walk through the platform capabilities. Please scroll down to the bottom of the page and click on 'FREE PLAY'. This provides you with unscripted access and you will follow the steps below.



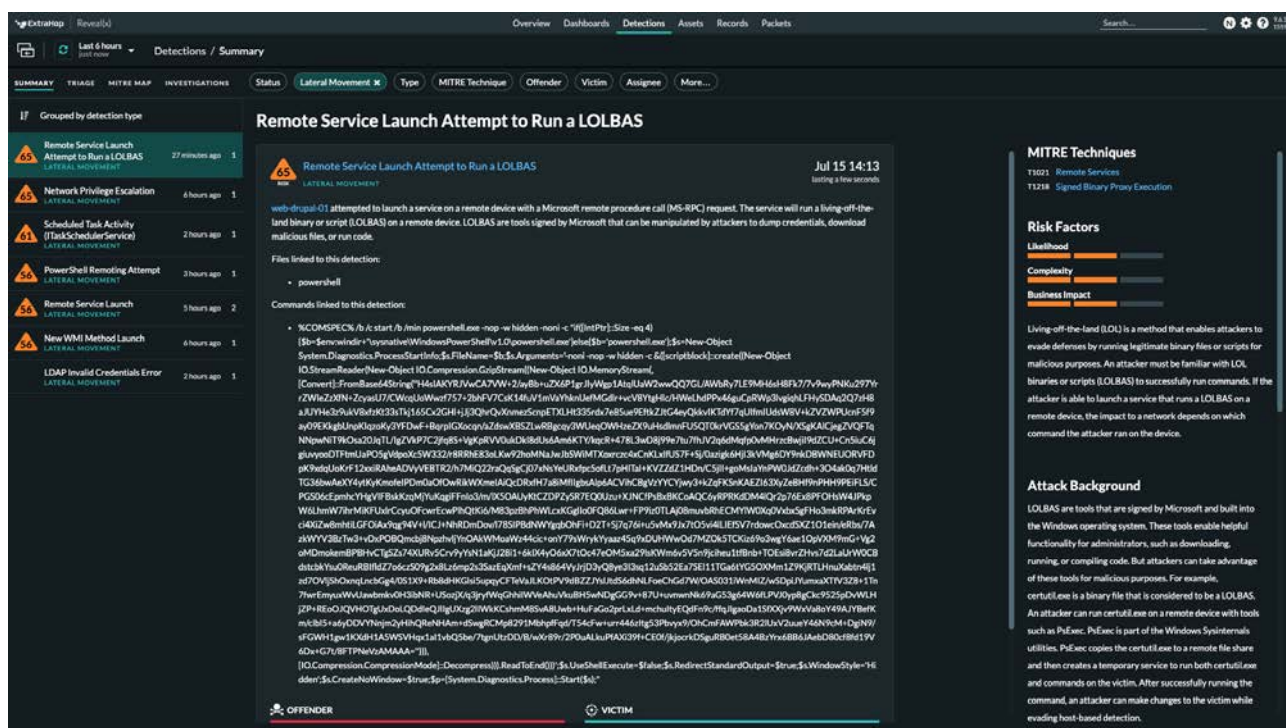
As you can see, once you're logged in, there are a number of different charts that highlight rich detail in the Overview pane. The separate panes located within here include:

- **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.

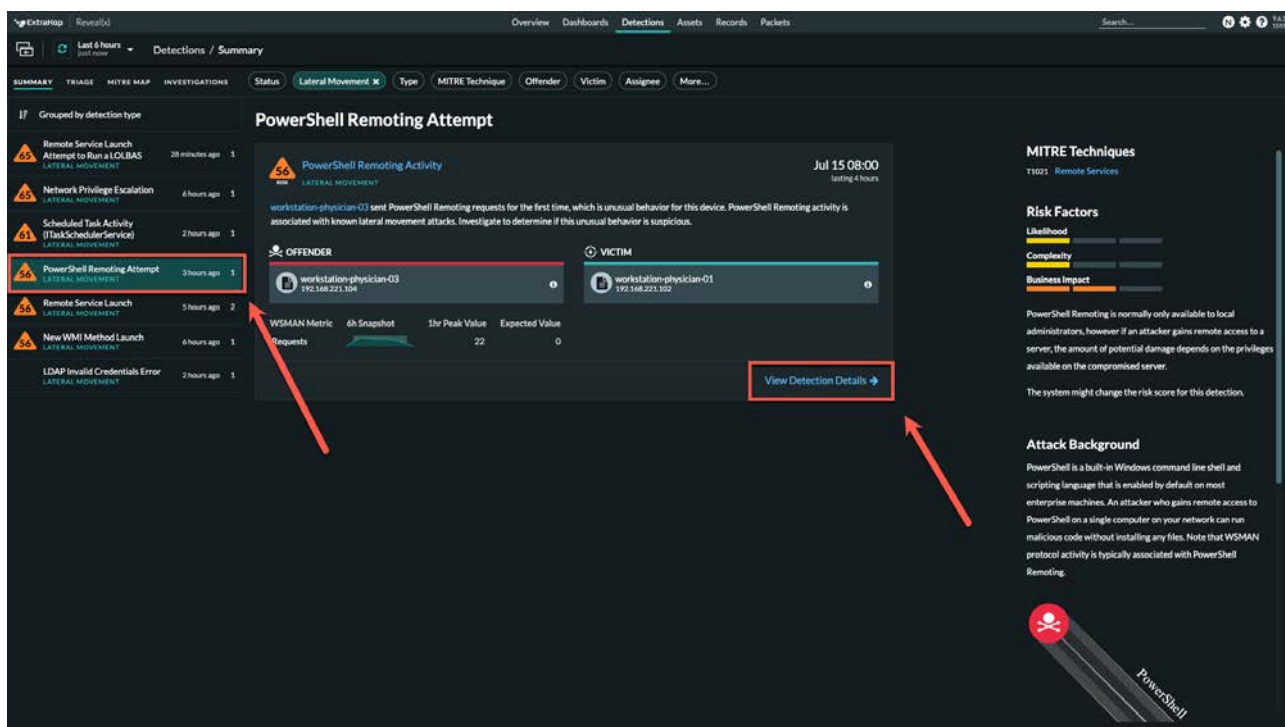
We will start from the overview screen of ExtraHop RevealX. When we're looking at the overview screen of ExtraHop RevealX) platform one of the things I would like to bring your attention to is the lateral movement. Click on Lateral Movement.



1. Lateral movement is one of the techniques that attackers will use to move inside the network to get access to high privilege assets and data. When looking at Ransomware, one of the use cases to see this is Lateral Movement. One of the reasons that we start here is that lateral movement tends to happen on Microsoft Protocols, RPC, WinRM, SMB, etc. And because ExtraHop is the only NDR that can decrypt Microsoft Protocols, we have a much deeper understanding of lateral movement and the normal operations of the protocols.



As you can see, there are six different lateral movement activities listed here. We're going to start on the PowerShell Remoting Attempt, as that's of interest here today. Go ahead click on that attempt on the left and then the View Detection Details as shown below. We're going to jump around a little bit but there some key points to make here.



Detection Details are shown below. We can see that this is a ML based detection based on the graph highlighted below and because of the peak value and expected value under the Detection Summary. We can see that Physician Workstatio-03 has never used the WSMAN (or Remote Powershell) to speak with Physician Workstation-01.

We also see the username that is being used to authenticate between the two systems listed as ([exubuse@AD.V2.INT.EH](#)) and is being used to execute remote PowerShell requests across the network.

They have also never used WSMAN protocol to speak to each other, so this is interesting and warrants some additional investigation. Let's drill down a little.

PowerShell Remoting Activity
LATERAL MOVEMENT
Jul 15 08:00 • lasting 4 hours

workstation-physician-03 sent PowerShell Remoting requests for the first time, which is unusual behavior for this device. PowerShell Remoting activity is associated with known lateral movement attacks. Investigate to determine if this unusual behavior is suspicious.

OFFENDER
workstation-physician-03
192.168.221.104

VICTIM
workstation-physician-01
192.168.221.102

WSMAN Metric

WSMAN Metric	6h Snapshot	1hr Peak Value	Expected Value
Requests		22	0

Users
View the Users

Records	User	Requests
	ecubon@ADV2/NTLM	73

Total: 73

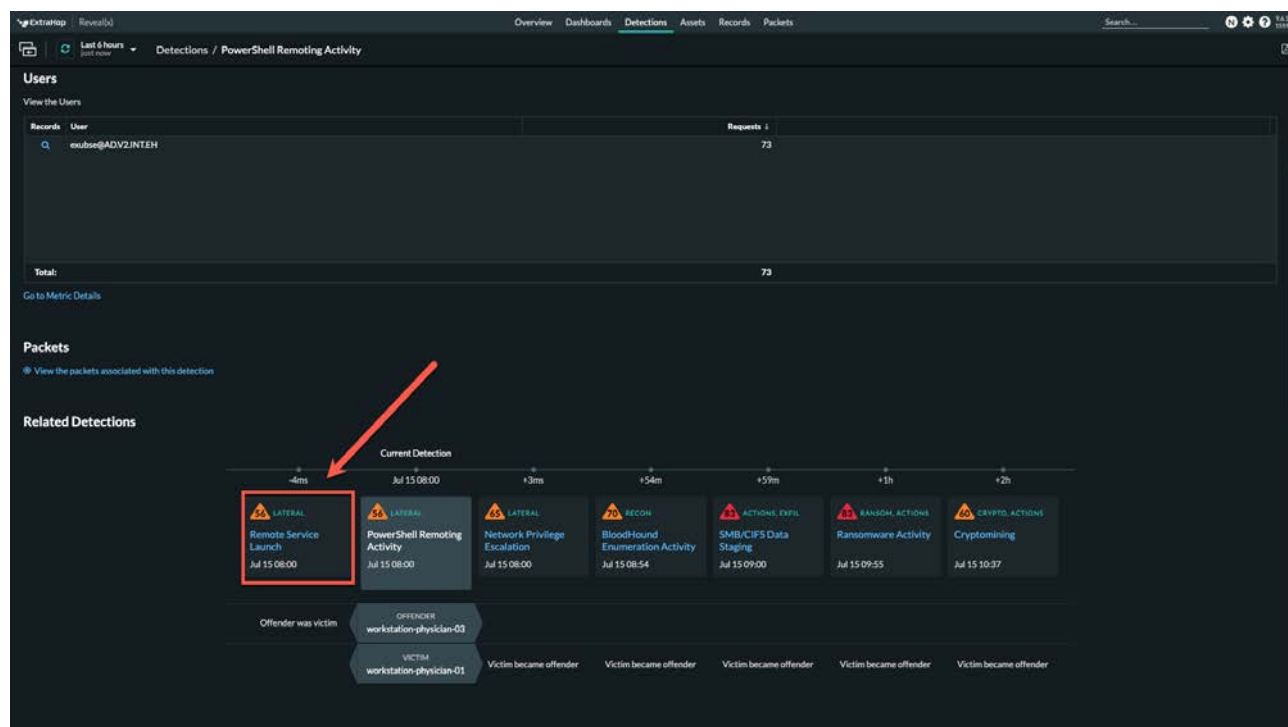
Packets
View the packets associated with this detection

Related Detections

If we scroll down some, we can see related detection timeline and it starts to expand the story.

We can see that there's much more happening here than we initially started to look at. This is because lateral movement caught our eye as an investigator, but in fact this is just a small part of a much larger story. We can see there are things ranging from full Ransomware activity, sata staging, perhaps for data exfil later, but we can also see an earlier attack for a remote service launch. Bad news for sure, but let's see what we can reveal.

Click on the remote service launch icon highlighted below.



We can see below that this is also a ML attack. Now, it's important to note again, that the only reason we can see this is because we can perform Microsoft protocol decryption, including MSRPC in this case. We can even view the commands that were sent over the MSRPC protocol if you hover above the Command selection highlighted below. This is incredibly valuable for the investigator as they continue to work to understand what commands were sent where and exactly how this bad actor gained access and what that blast radius really looks like.

Remote Service Launch
LATERAL MOVEMENT
Jul 15 08:00 • lasting an hour

web-drupal-01 sent a request to launch a service on a remote device. This is the first time web-drupal-01 sent this type of request. Specific tools, such as PsExec, create a temporary service that enables a remote attacker to run commands or launch executable files.

OFFENDER
web-drupal-01
192.168.223.22

VICTIM
workstation-physician-03
192.168.223.104

MSRPC Responses by Interface:Operation

6h Snapshot	1hr Peak Value	Expected Value
svch.CreateServiceW	1	0

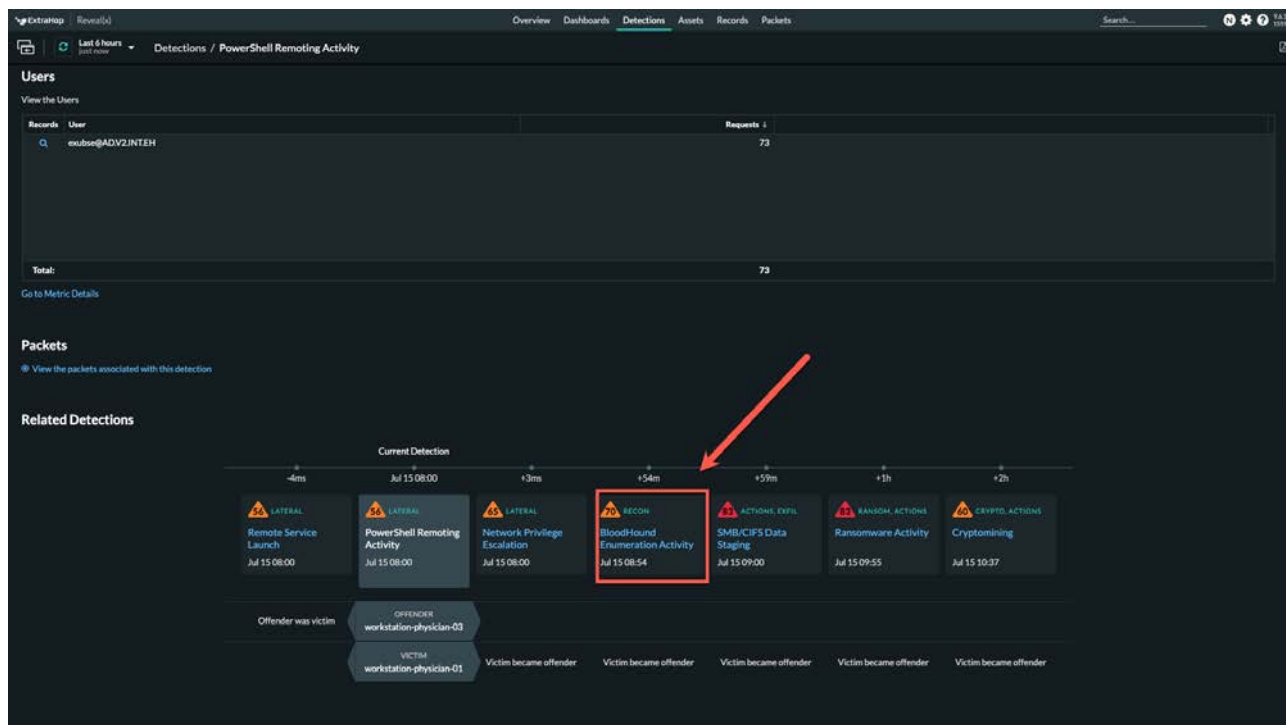
Commands
View the commands executed

Records	Command	New Service Created
1	%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "[*]([*])Size -eq 4(\$?)\$? - \$env:windir\system32\WindowsPowerShell\v...	1

Service Names
View the services created

Records	Service Name	New Service Created
1	SZQUCzX	1

Now, if we click back once to the original related detections, we can also see that the attacker has performed some Bloodhound Enumeration, click the highlighted Bloodhound threat as shown below.



Now, when looking at this Bloodhound activity, not only can we see that it was SharpHound as highlighted just above the record, but we can also see the actual metadata that was extracted from the packets during that conversation as highlighted in the record detail. This is incredible powerful in understanding what the attacker has done, as it shows the actual in query and can be shown to the investigators as they continue their work.

The screenshot displays the ExtraHop interface for a detection titled "BloodHound Enumeration Activity". The interface includes a navigation bar with "Overview", "Dashboards", "Detections", "Assets", "Records", and "Packets". The "Detections" tab is active, showing a list of detections. The selected detection is "BloodHound Enumeration Activity" (ID: 70), which occurred on Jul 15 08:23. The detection description states: "workstation-physician-03 sent an LDAP enumeration query that is associated with BloodHound, a reconnaissance tool for Microsoft Active Directory (AD) environments. BloodHound leverages data collectors to enumerate, or collect, AD information from devices such as domain controllers and identifies relationships between objects such as users, services, and devices." The "Data collector" is listed as "SharpHound". The "Offender" is "workstation-physician-03" (IP: 192.168.221.104) and the "Victim" is "domain-controller-01" (IP: 192.168.221.11). The "Records" section shows a single record with a search filter and search scope. A red arrow points to the "Records" section.

Now, let's back out to the original PowerShell Remoting Activity again. And scroll down, as it looks like they're doing some Data Staging. Click there as shown below.

The screenshot displays the ExtraHop interface for a detection titled "PowerShell Remoting Activity". The interface includes a navigation bar with "Overview", "Dashboards", "Detections", "Assets", "Records", and "Packets". The "Detections" tab is active, showing a list of detections. The selected detection is "PowerShell Remoting Activity" (ID: 70), which occurred on Jul 15 08:00. The "Users" section shows a table with one user: "esulson@ADV2.INTEH" with 73 requests. The "Packets" section shows a list of packets. The "Related Detections" section shows a timeline of events. A red arrow points to the "SMB/CIFS Data Staging" event (ID: 70) in the timeline.

If you scroll down a bit, we have immediately visibility into the data that was staged and set for possible data exfil. It provides us direct evidence of every file and associated IP addresses used during this portion of the attack. This again was detected using our cloud scale ML as we can see that there is an unusual amount of data that's been moved.

Files
View the files that were potentially exfiltrated

Records	File	Goodput Bytes Read	Responses	Goodput Bytes Written	Access Time Mean (ms)
Q	accounts\2016_export.csv	10,492,322	1	—	74,024
Q	accounts\2010_export.csv	10,492,322	1	—	173,679
Q	accounts\2017_export.csv	10,492,322	1	—	128,142
Q	accounts\2012_export.csv	10,492,322	1	—	122,019
Q	accounts\2014_export.csv	10,492,322	1	—	134,513
Q	accounts\2015_export.csv	10,492,322	1	—	117,171
Q	accounts\2013_export.csv	10,492,322	1	—	66,457
Q	accounts\2011_export.csv	10,492,322	1	—	106,501
Q	accounts\assets\2010\apr_2010.xls	1,740,489	4	—	37,176
Q	accounts\assets\2013\sep_2013.xls	1,738,441	5	—	32,112
Q	accounts\assets\2015\dec_2015.xls	1,738,441	5	—	16,978
Q	accounts\assets\2016\new_2016.xls	1,736,393	5	—	32,934
Q	accounts\assets\2011\dec_2011.xls	1,736,393	5	—	30,316
Q	accounts\assets\2012\jan_2012.xls	1,734,345	5	—	25,907
Q	accounts\assets\2012\sep_2012.xls	1,734,345	5	—	10,308
Q	accounts\assets\2014\feb_2014.xls	1,728,301	5	—	25,799
Total:		1,004,364,129	1,470	0	

IPs
View the targeted servers

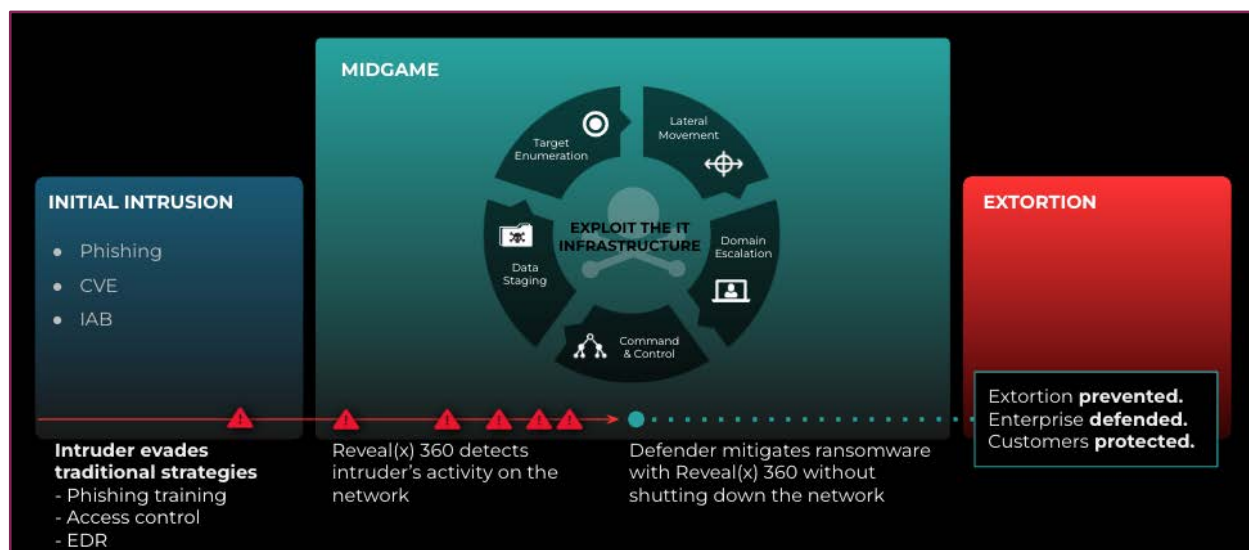
Records	IP	Host	CIFS Bytes In	CIFS Bytes Out	CIFS Packets In	CIFS Packets Out
Q	192.168.221.121	accounting-filer-server-01	1,211,517,809	154,506,340	164,557	57,606
Q	192.168.221.11	domain-controller-01	91,481	88,510	450	466
Q	192.168.221.301	workstation-it-admin-01	9,845	7,335	50	60

The Midgame

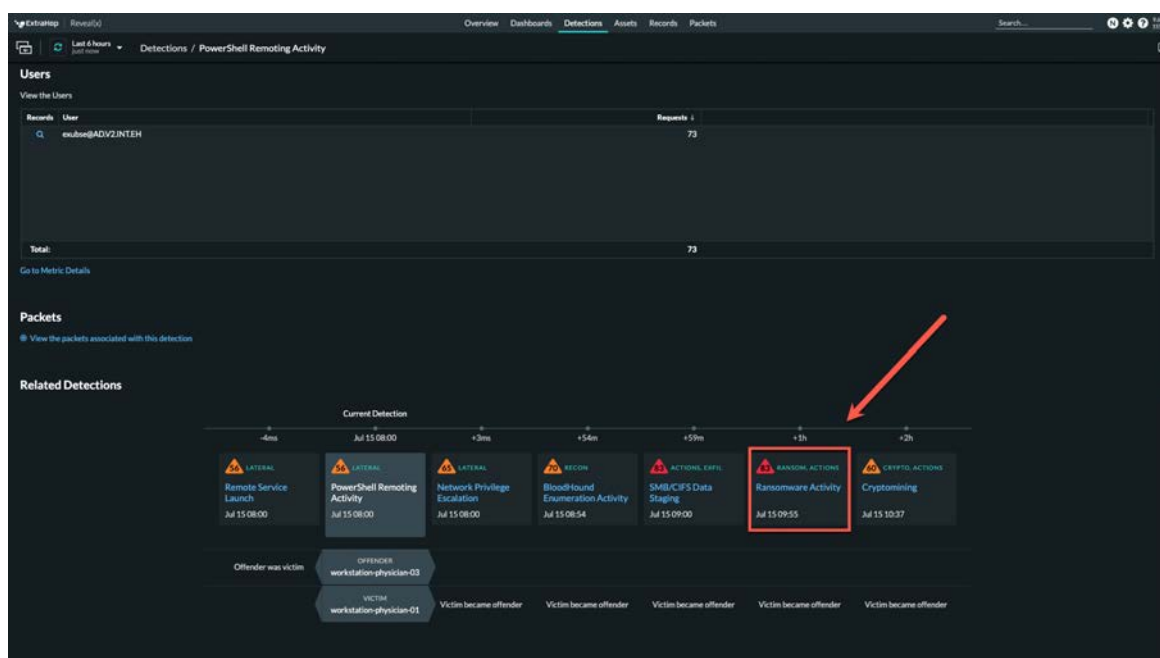
Preventing initial access may not be possible, but with [ExtraHop RevealX 360](#), defenders can detect and stop ransomware in the midgame before they achieve real damage. What we've seen so far has been that Ransomware midgame.

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 \(RDP\)](#), remote access, etc, 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.



Let's back up one more again and then click on the Ransomware Detection as shown below.



1. We can see the files that have been encrypted when accessed from the 'workstations-physician-01' PC to the 'accounting-filesserver-01'.
2. Note that we can see the bad actor has encrypted 2,000 total files.

3. For additional detail, click on 'Go to Metric Details as noted below'.

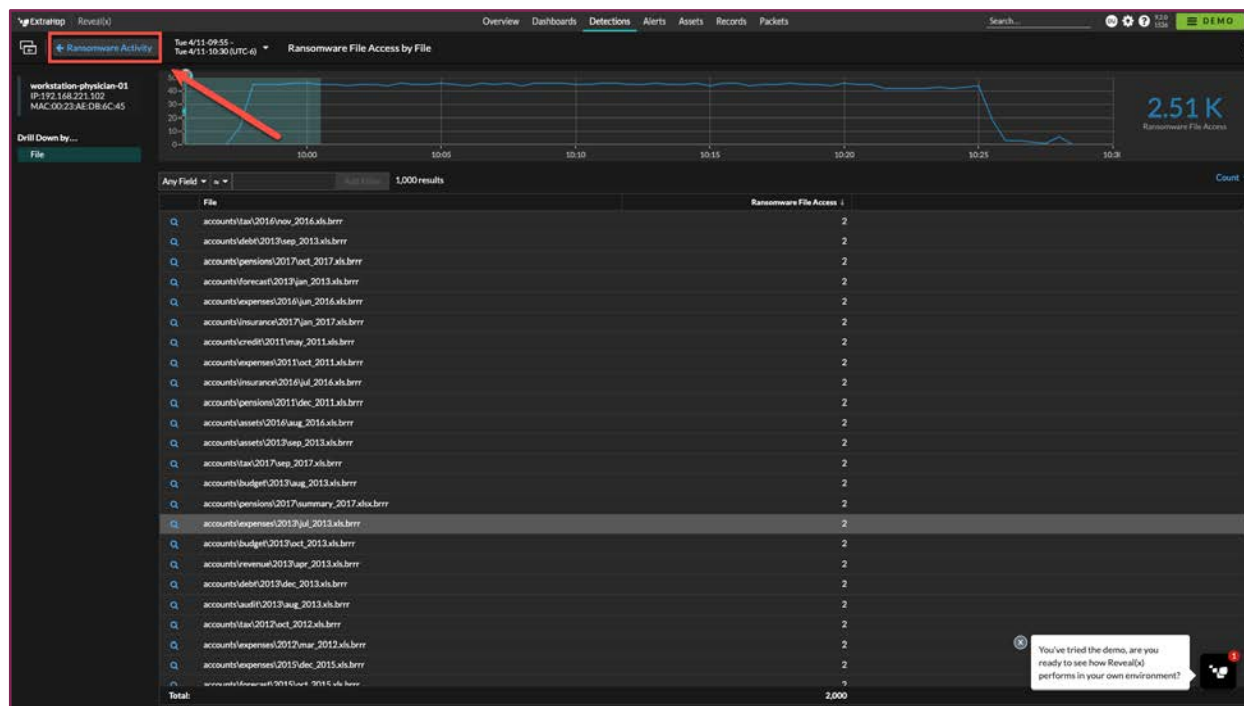
Files

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](#)

4. 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.
5. Once done, please click in the upper left-hand corner on 'Ransomware Activity' as noted below to return to the detection card.



6. 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.

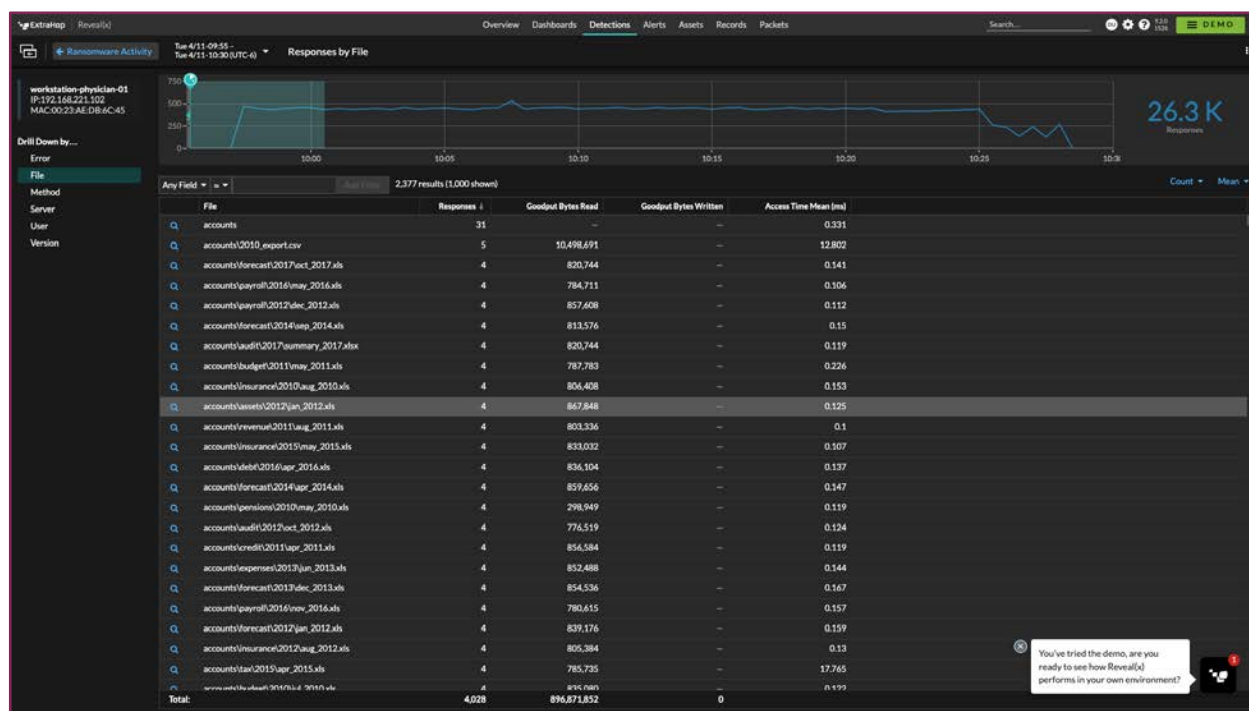
Files
View the files accessed

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

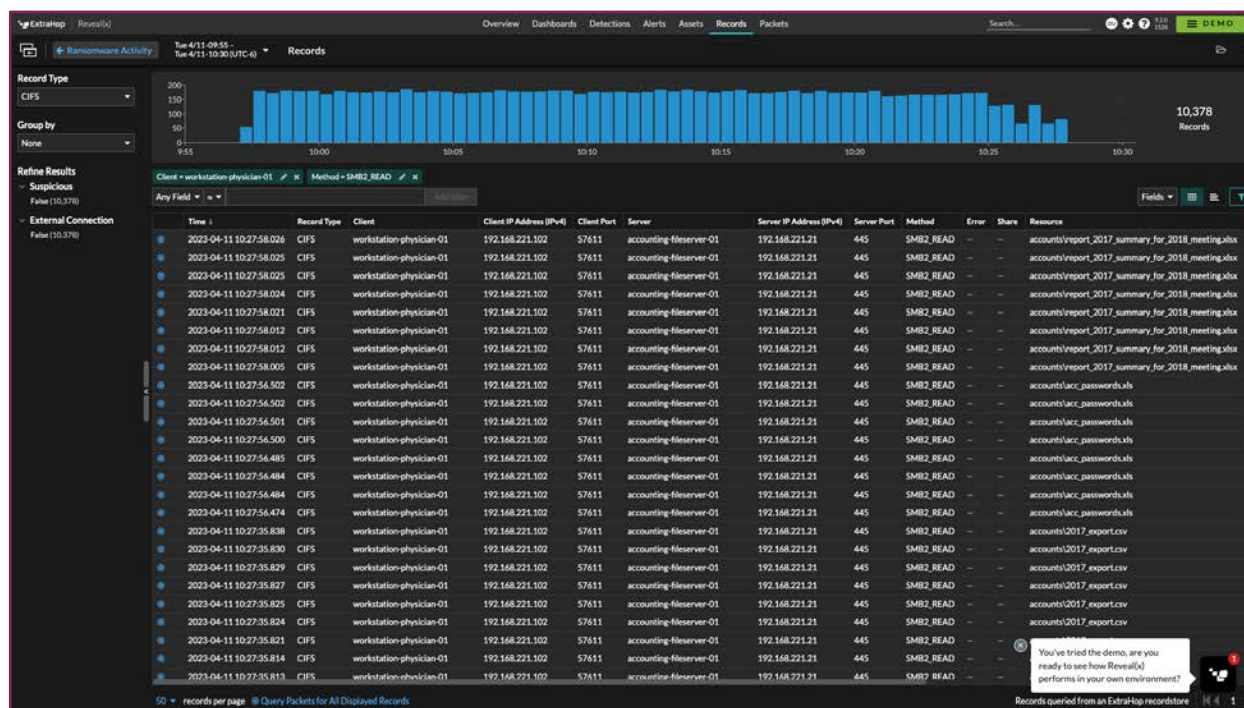
[Go to Metric Details](#)

7. 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



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



9. 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.

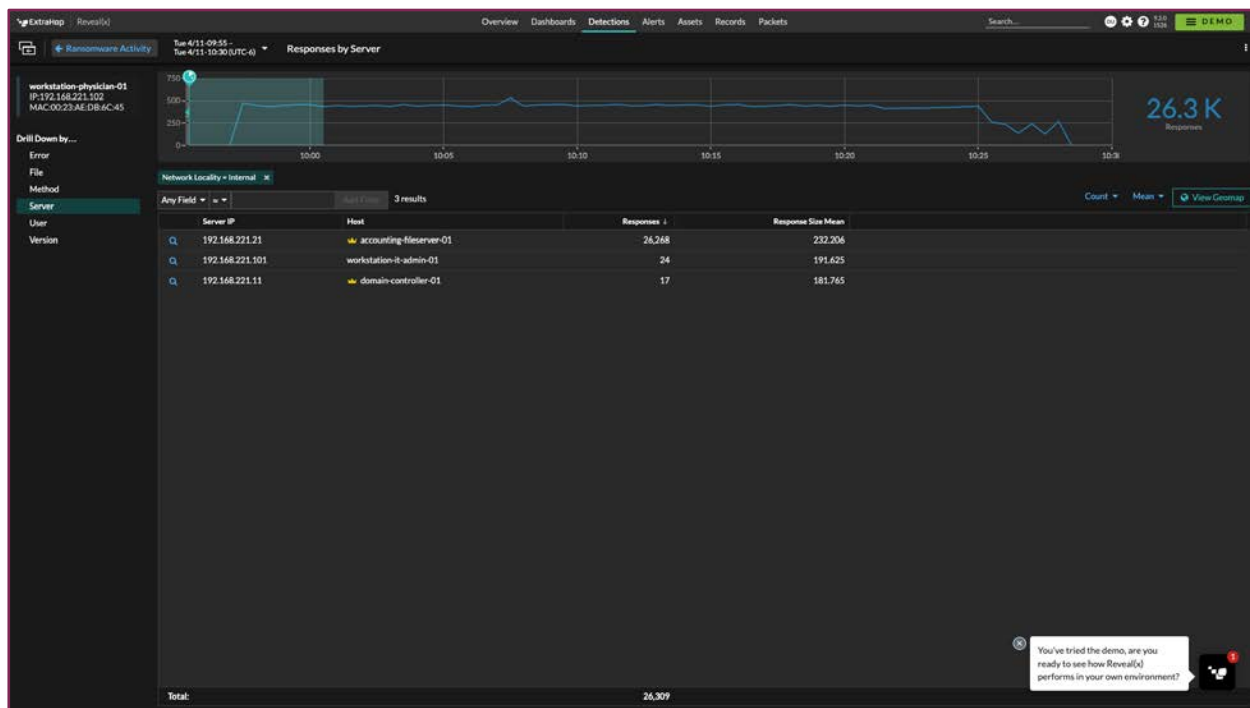
Servers

View the targeted servers

Server IP	Host	Responses	Response Size Mean
192.168.221.121	accounting-filer-server-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	

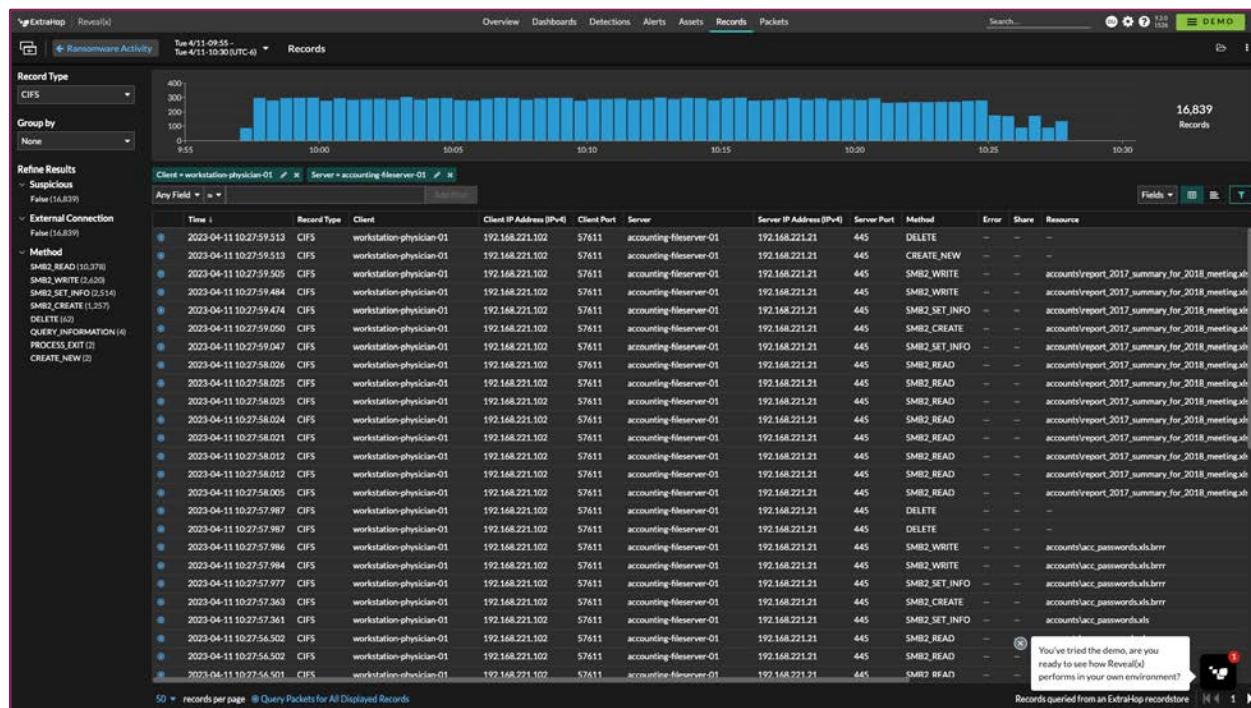
[Go to Metric Details](#)

10. Again, going to the 'Metrics Details' provides us additional detail on the Servers, as shown below.



11. Clicking on the magnifying glass for the 'accounting-filer-server-01' will now show us all metric details for that server, including all files, methods, timelines and resources accessed.

12. Note the Methods column and the different ones listed.



13. 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.

14. 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 Packet Query Results interface. The top navigation bar includes 'Overview', 'Dashboards', 'Detections', 'Alerts', 'Assets', 'Records', and 'Packets'. The 'Packets' tab is selected. The interface displays a search bar, filters, and a table of packet data. A red box highlights the 'Download PCAP' button in the top right corner. A red arrow points to the 'Download PCAP' button.

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

The screenshot shows the Wireshark packet capture interface. The packet list pane shows a list of packets. The packet details pane shows the details of a selected packet. The packet is a TCP Reset (RST) from 192.168.221.21 to 192.168.221.102. The details pane shows the packet structure, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and NetBIOS Session Service.

16. 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.

The screenshot displays the ExtraHop Reversal interface, specifically the 'Detections / Ransomware Activity' section. The interface is dark-themed with a sidebar on the left containing navigation icons. The main content area is titled 'MITRE Techniques' and shows 'T1486: Data Encrypted for Impact'. Below this, there are 'Risk Factors' with a 'Likelihood' bar chart and a 'Complexity' bar chart, both indicating a 'Medium' risk level. A paragraph explains that ransomware attacks are common due to their high return on investment and the ease of acquiring or creating malware. The 'Attack Background' section describes ransomware as malware that encrypts files, making them inaccessible until a ransom is paid. An illustration shows a red skull and crossbones icon connected to a blue circular icon with a dollar sign, which is then connected to a folder icon containing several files. The 'Mitigation Options' section lists several recommendations: maintaining off-site and up-to-date backup files, periodically restoring systems from backup files, disabling internal services exposed to the Internet, enforcing security zones, updating operating system software, and enforcing a strong password policy. The 'Reference' section includes a link to the MITRE ATT&CK technique T1486 and a link to a document titled 'How Ransomware Works and How to Prevent It'.

MITRE Techniques
T1486: Data Encrypted for Impact

Risk Factors
Likelihood
Complexity
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.

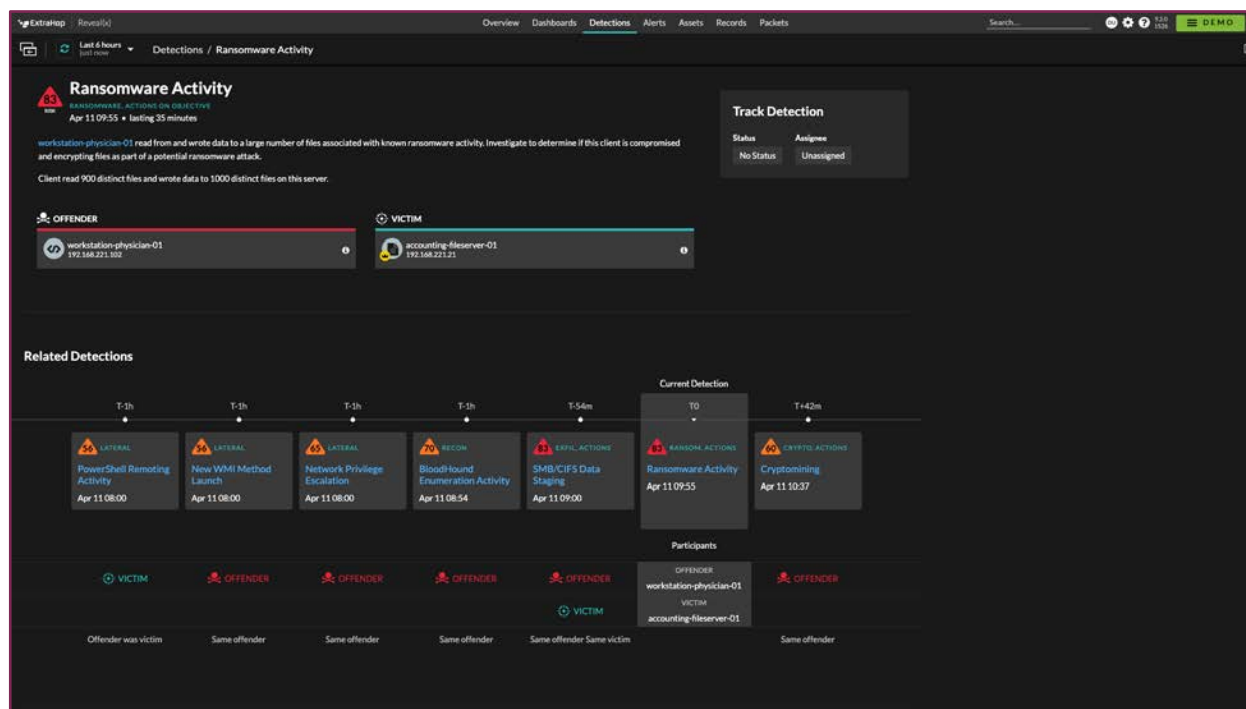
Attack Background
Ransomware is a type of malware that encrypts files on a victim machine, which makes those files inaccessible until the victim pays a ransom for the decryption key. Ransomware attacks can originate from phishing emails, exploited network services, or large-scale attack campaigns. After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

Mitigation Options

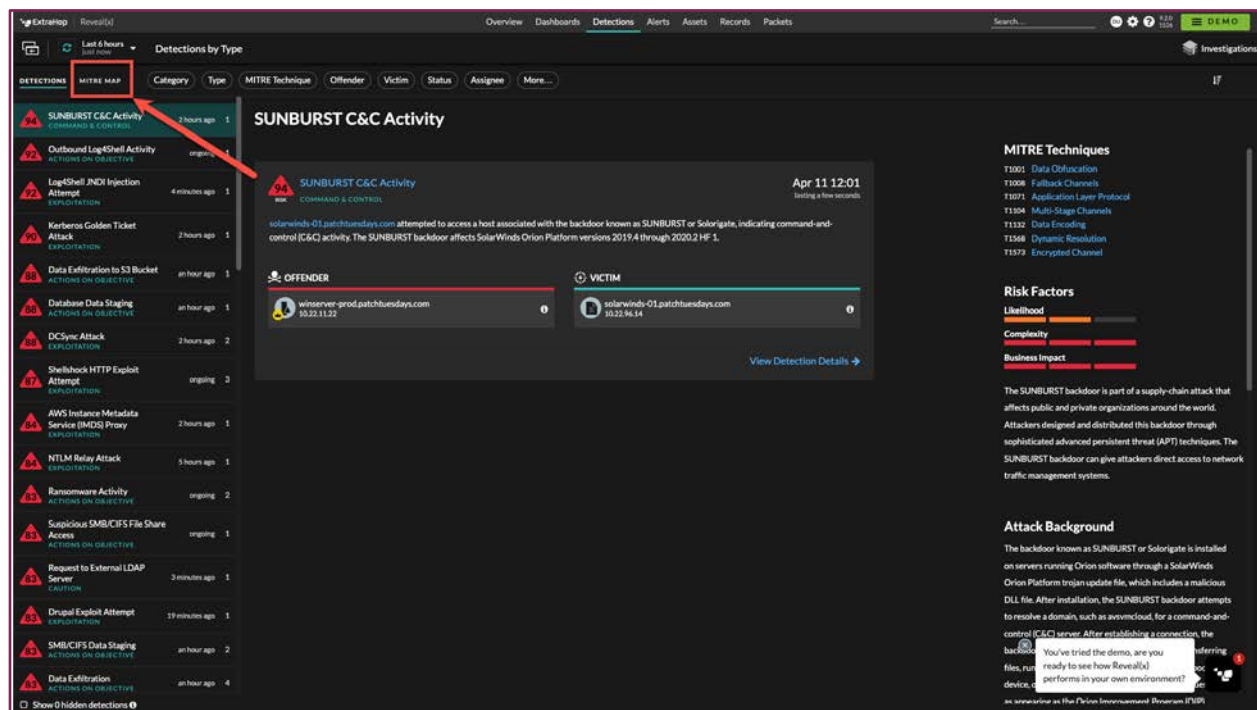
- Maintain off-site and up-to-date backup files that can restore critical systems
- Periodically restore systems from backup files to make sure they are working
- Disable internal services that are exposed to the Internet, especially services that run over file sharing or remote access protocols
- Enforce 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

17. 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.



1. Click on the MITRE MAP, as noted below to go to the mapping of the detections to the MITRE ATT&CK framework.



2. 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.
3. 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.
4. Click on the Detections tab, listed next to the MITRE MAP in the upper left corner to return to the Detections tab.
5. You can now see all the methods that ExtraHop has detected and have also mapped out against the MITRE ATT&CK framework.

ExtraHop Reveal360

Overview Dashboards **Detections** Alerts Assets Records Packets

Search... 1/10 12/18 DEMO

Investigations

DETECTIONS MITRE MAP Category Type MITRE Technique Offender Victim Status Assignee More...

17

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise T1187 33 Detections	Command and Scripting Interpretation T1059 4 Detections	BITS Jobs T1197	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Brute Force T1130 3 Detections	Account Discovery T1087 4 Detections	Exploitation of Remote Services T1130 4 Detections	Archive Collected Data T1060 3 Detections	Automated Exfiltration T1071 3 Detections	Application Layer Protocol T1131	Account Access Removal T1131
Exploit Public-Facing Application T1190 5 Detections	Exploitation for Client Execution T1303	Boot or Logon Autostart Execution T1547	Boot or Logon Initialization Scripts T1087	Build Image on Host T1612	Credentials from Password Stores T1333	Cloud Service Discovery T1334 1 Detection	Lateral Tool Transfer T1376	Data from Cloud Storage Object T1330	Data Transfer Size Limits T1030 5 Detections	Data Encoding T1122 1 Detection	Data Destruction T1045 1 Detection
External Remote Services T1133	User Process Communication T1059	Boot or Logon Initialization Scripts T1037	Create or Modify System Process T1543	Exploitation for Defense Evasion T1211	Exploitation for Credential Access T1212	Domain Trust Discovery T1483 5 Detections	Remote Services T1021 5 Detections	Data from Configuration Repository T1602	Exfiltration Over Alternative Protocol T1048 7 Detections	Data Obfuscation T1001 1 Detection	Data Encrypted for Impact T1486 3 Detections
Hardware Additions T1130	Native API T1096 3 Detections	Browser Extensions T1176	Event Triggered Execution T1346	Hijack Execution Flow T1154	Forceful Authentication T1187	File and Directory Discovery T1089	Taint Shared Content T1089	Data from Information Repositories T1113	Exfiltration Over C2 Channel T1041 1 Detection	Endpoint Denial of Service T1479	Endpoint Denial of Service T1479
Phishing T1166 33 Detections	Scheduled Task/Job T1053 1 Detection	Create Account T1134	Exploitation for Privilege Escalation T1068	Indicator Removal on Host T1070	Man-in-the-Middle T1051 2 Detections	Group Policy Discovery T1135	User Alternate Authentication Material T1100 1 Detection	Data from Local System T1005	Exfiltration Over Web Service T1047 26 Detections	Denial of Service T1158 1 Detection	Inhibit System Recovery T1490
Supply Chain Compromise T1195	System Services T1549 2 Detections	Event Triggered Execution T1546	Hijack Execution Flow T1374	Modify Authentication Process T1556	Modify Authentication Process T1336	Network Service Scanning T1046 3 Detections	Network Share Discovery T1135	Data from Network Shared Drive T1029 3 Detections	Exfiltration Over Web Service T1047 5 Detections	Encrypted Channel T1173 26 Detections	Network Denial of Service T1478
Valid Accounts T1078 1 Detection	User Execution T1124 1 Detection	External Remote Services T1133	Scheduled Task/Job T1053 1 Detection	Modify Registry T1112	Network Sniffing T1040 1 Detection	Network Service Discovery T1135	Network Sniffing T1040 1 Detection	Data Staged T1074 4 Detections	Scheduled Transfer T1029 4 Detections	Full-Tier Channels T1008 3 Detections	Resource Hijacking T1476 6 Detections
	Windows Management Instrumentation T1047 1 Detection	Hijack Execution Flow T1574	Valid Accounts T1078 1 Detection	Network Boundary Bridging T1599	OS Credential Dumping T1005 2 Detections	Network Sniffing T1040 1 Detection	Network Sniffing T1040 1 Detection	Email Collection T1114	Transfer Data to Cloud Account T1087 1 Detection	Ingress Tool Transfer T1103	System Shutdown/Reboot T1129
	Scheduled Task/Job T1053 1 Detection		Obfuscated Files or Information T1027	Regain Domain Controller T1207	Host or Range Enumeration Tools T1356 1 Detection	Unusual Credentials T1032 1 Detection	Permission Groups Discovery T1069 3 Detections	Man-in-the-Middle T1057 2 Detections	Transfer Data to Cloud Account T1087 1 Detection	Multi-Stage Channels T1104 3 Detections	Non-Application Layer Protocol T1095
	Server Software Component T1005 1 Detection		Server Software Component T1005 1 Detection	Signed Binary Proxy Execution T1218		Query Registry					
	Traffic Signaling T1205 2 Detections			Traffic Signaling							

You've tried the demo, are you ready to see how Reveal360 performs in your own environment?

800-879-8079