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.

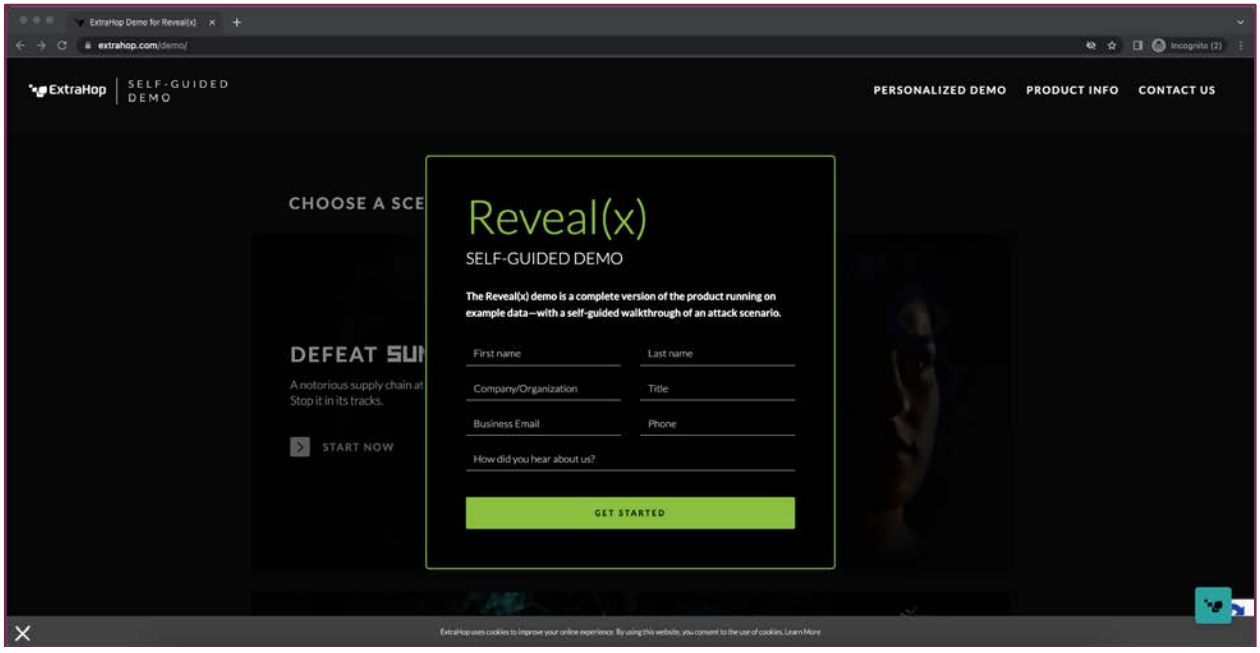
Unlike early ransomware attacks that focused on targets of opportunity, modern ransomware attacks leverage detailed playbooks that rapidly take advantage of new vulnerabilities to gain access to their victims' networks.

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.

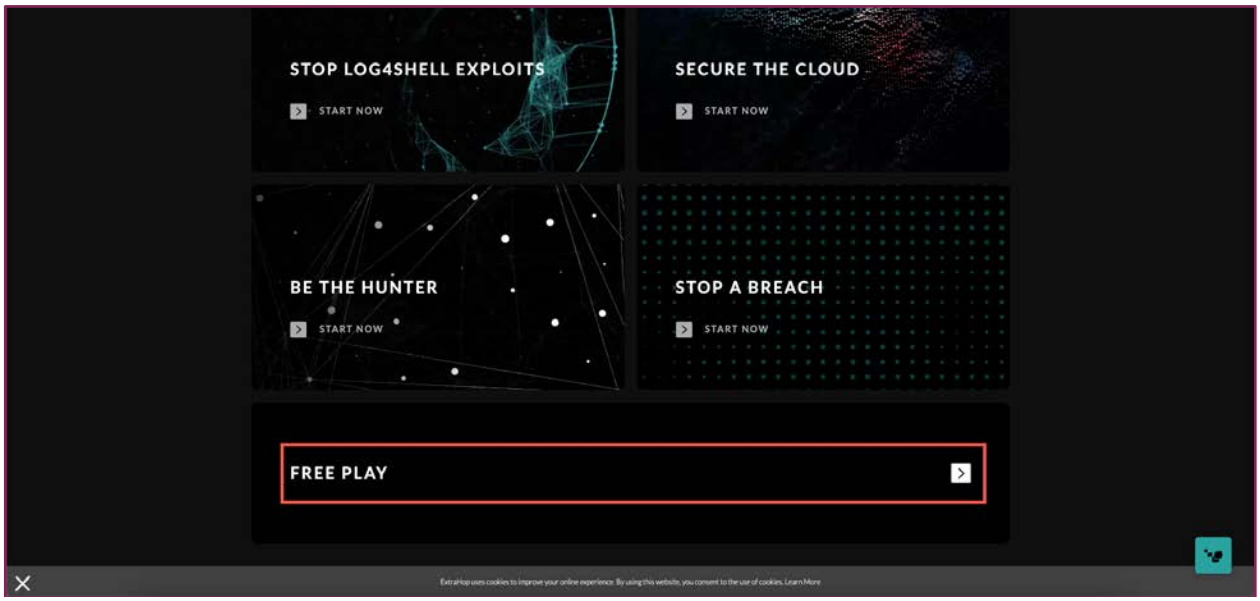
Lab Introduction

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'.



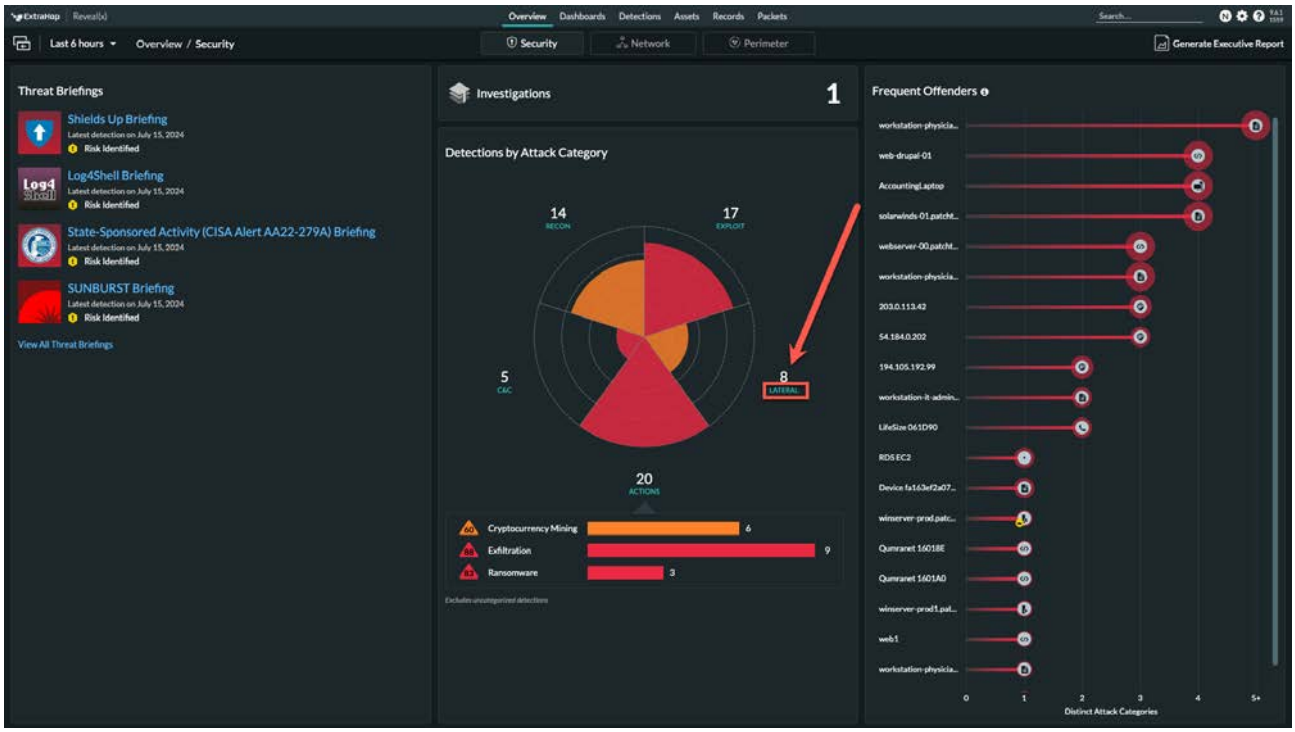
3. There are several guided scenarios listed that you could use at your leisure to walk through the platform capabilities. Please scroll down to the bottom of the page and click on 'FREE PLAY'. This provides you with unscripted access and you will follow the steps below.



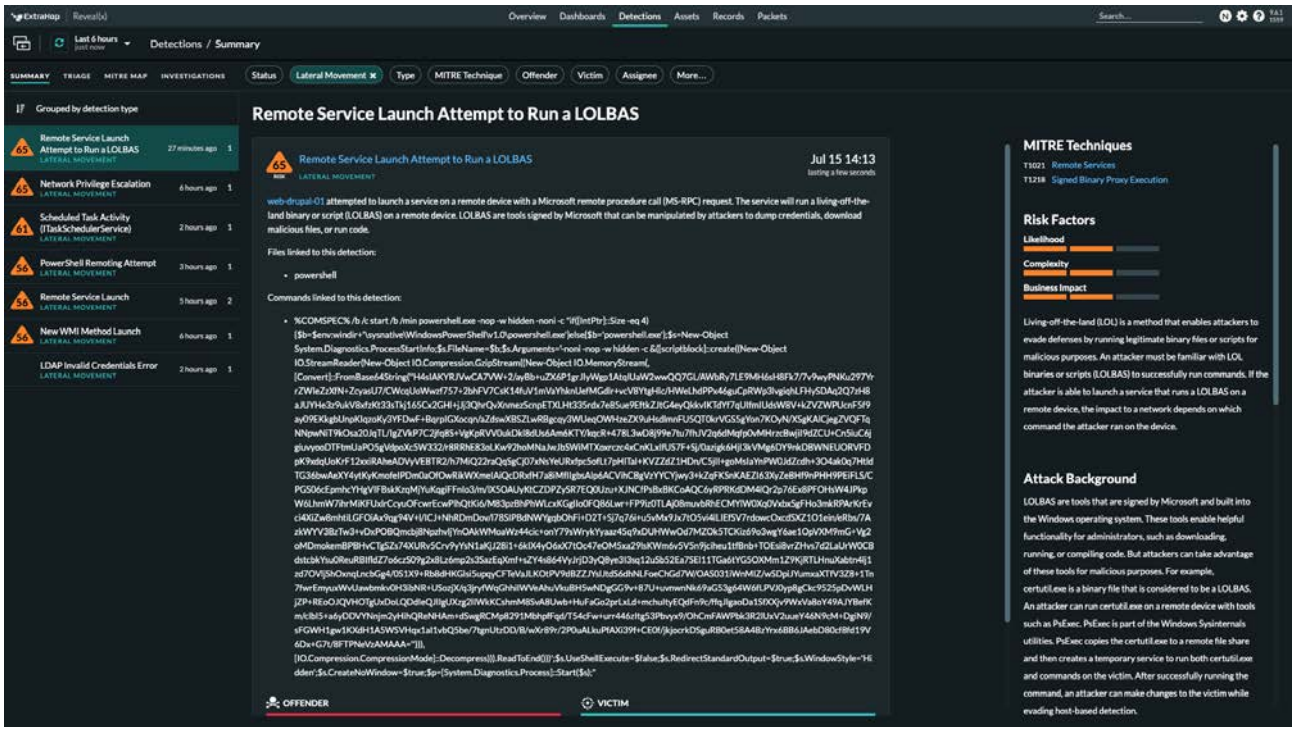
As you can see, once you're logged in, there are a number of different charts that highlight rich detail in the Overview pane. The separate panes located within here include:

- **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.

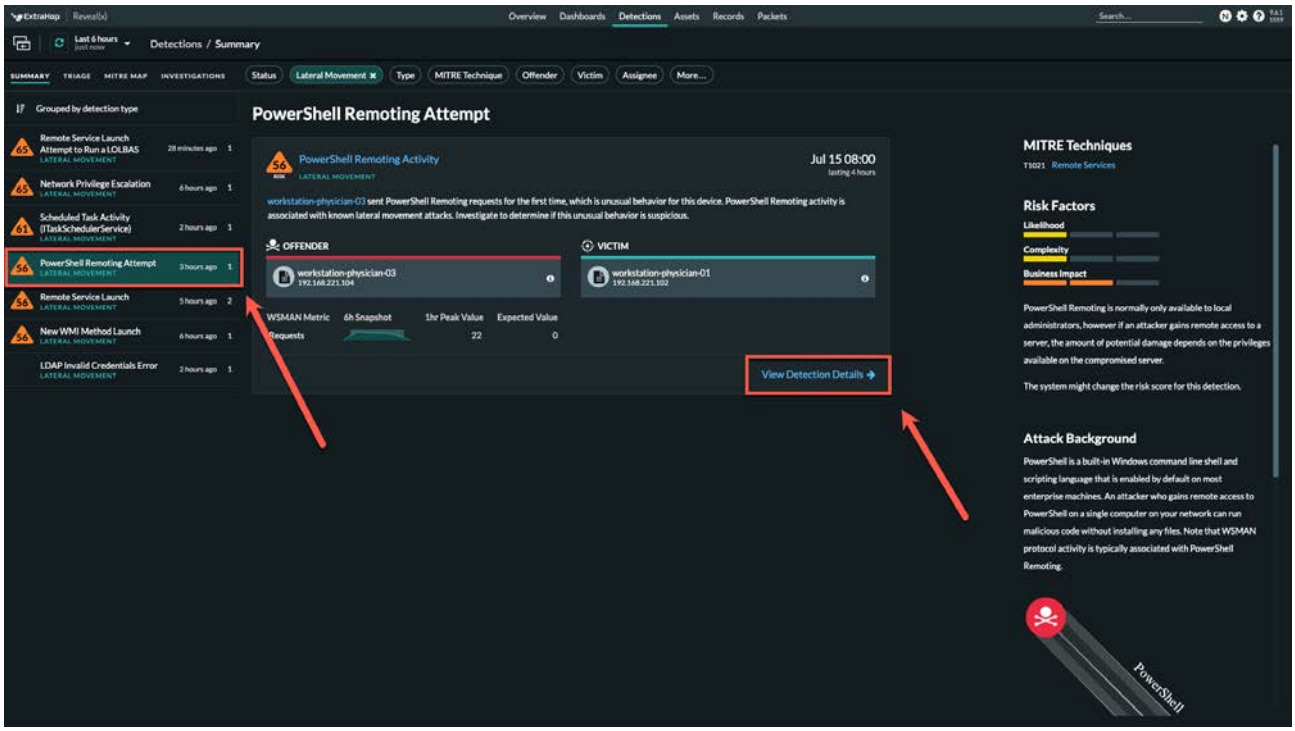
We will start from the overview screen of ExtraHop RevealX. When we're looking at the overview screen of ExtraHop RevealX) platform one of the things I would like to bring your attention to is the lateral movement. Click on Lateral Movement.



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.



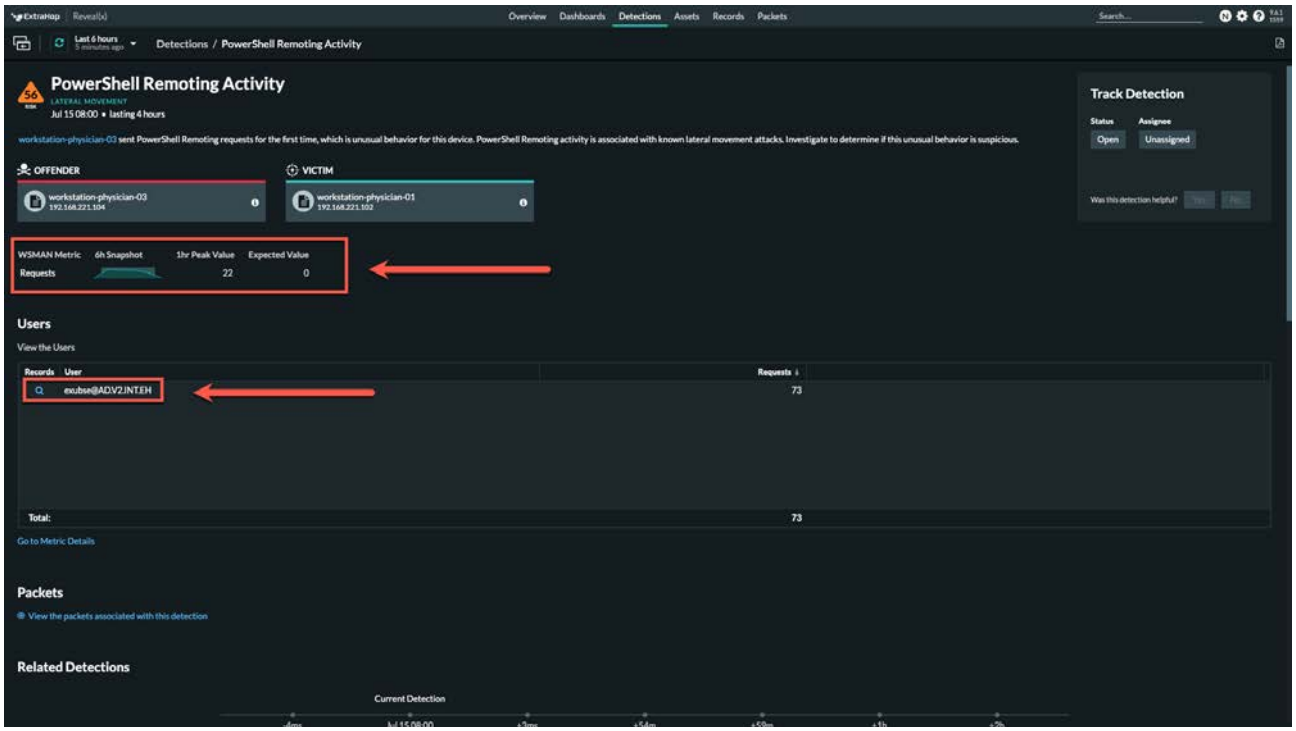
As you can see, there are six different lateral movement activities listed here. We're going to start on the PowerShell Remoting Attempt, as that's of interest here today. Go ahead click on that attempt on the left and then the View Detection Details as shown below. We're going to jump around a little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

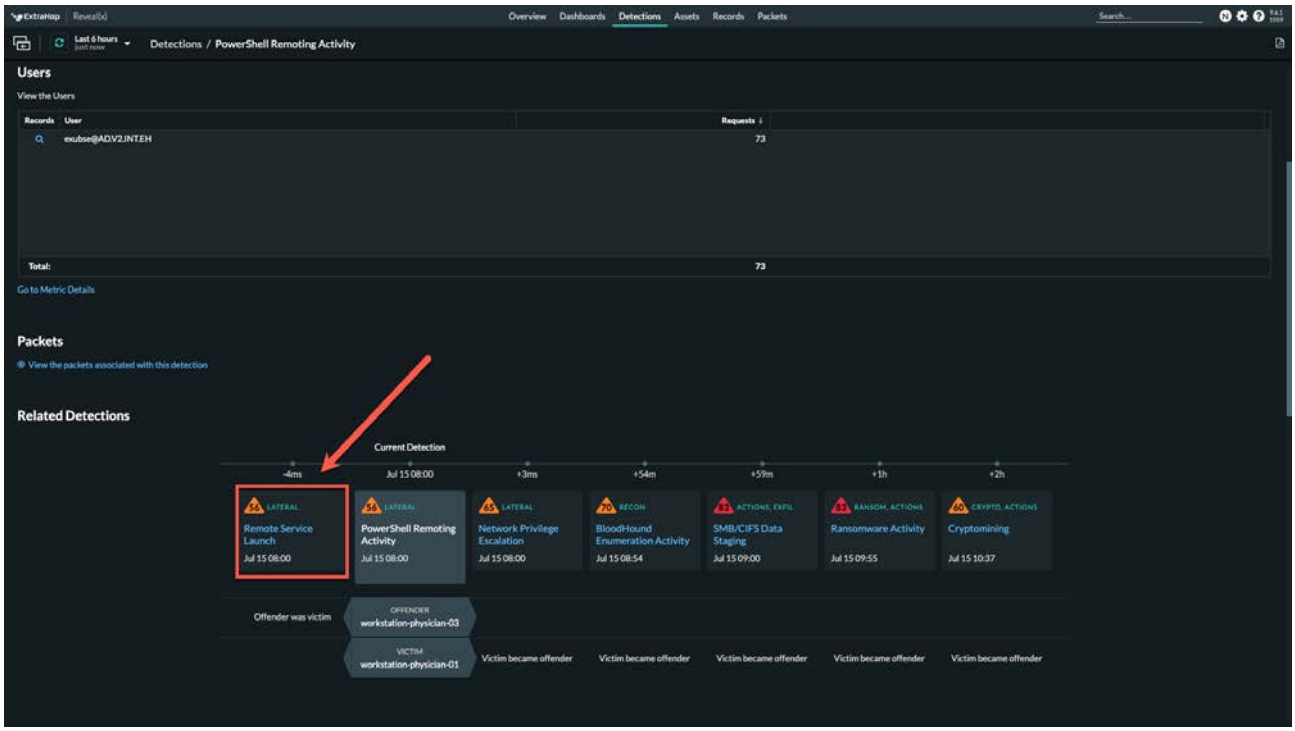
They have also never used WSMAN protocol to speak to each other, so this is interesting and warrants some additional investigation. Let's drill down a little.



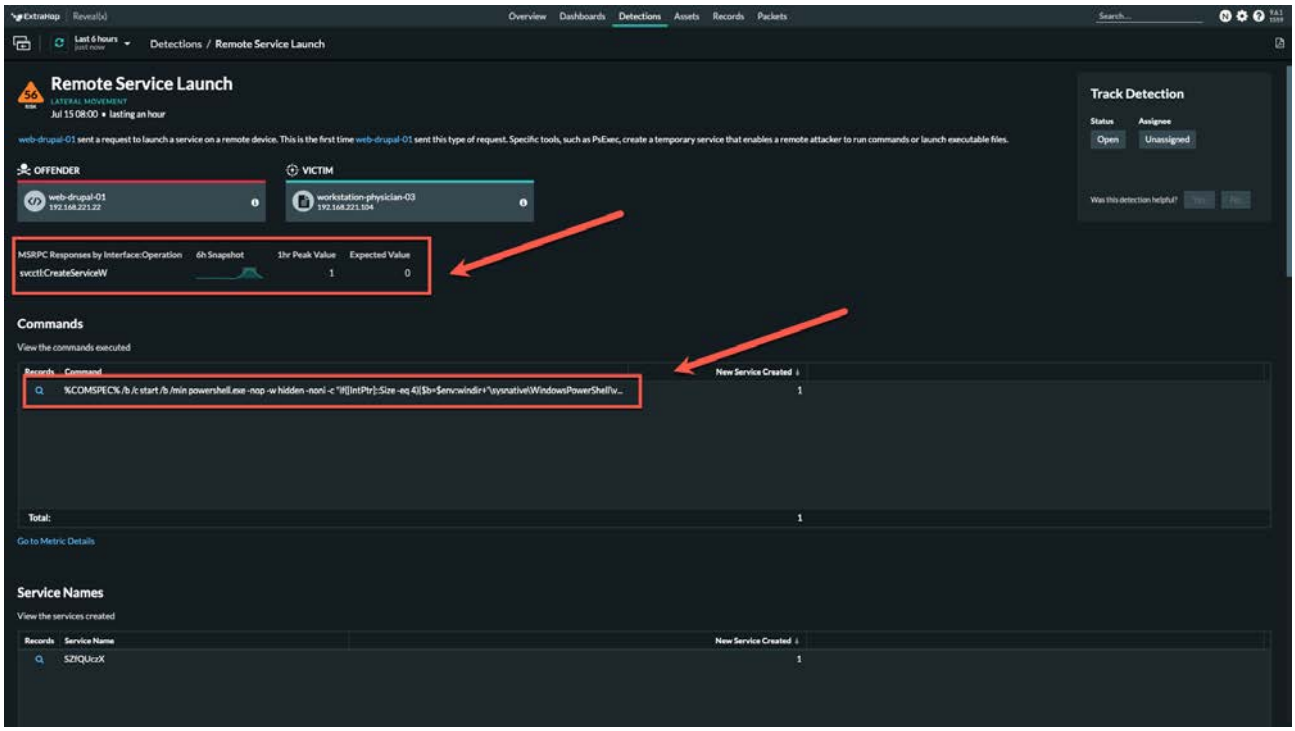
If we scroll down some, we can see related detection timeline and it starts to expand the story.

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.

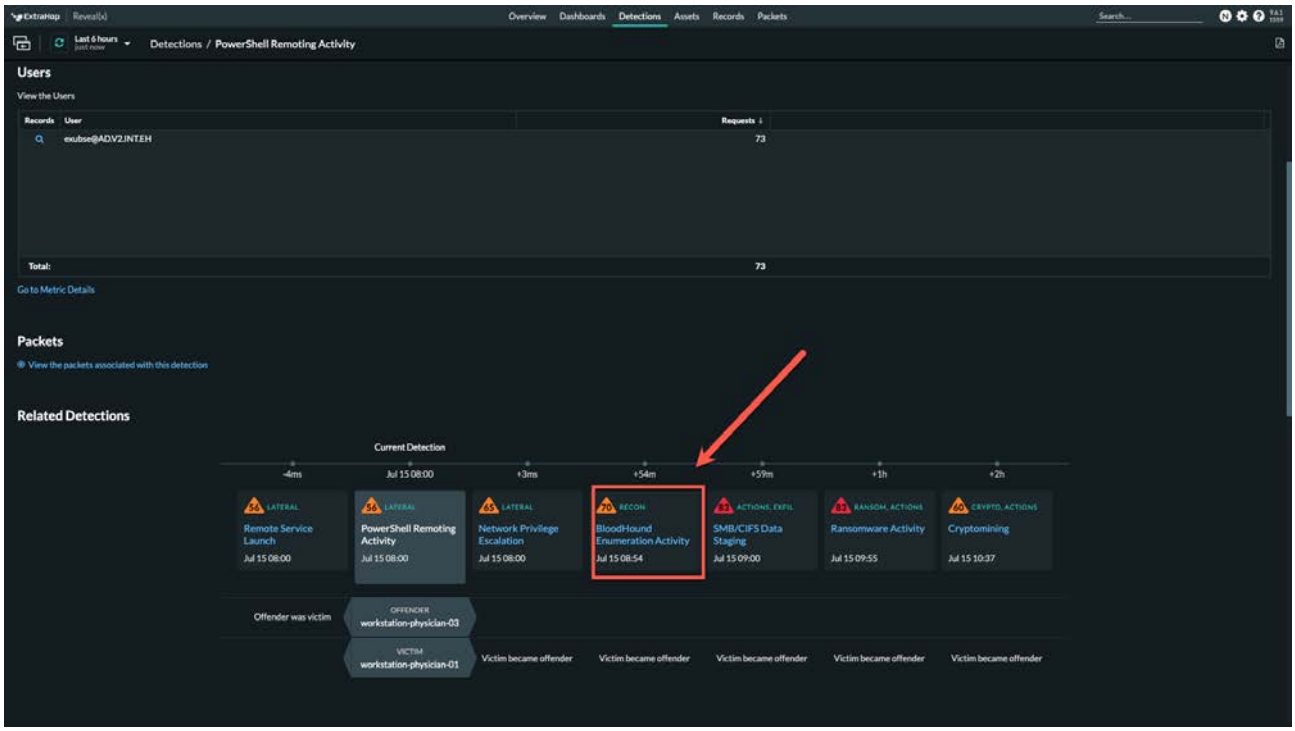
Click on the remote service launch icon highlighted below.



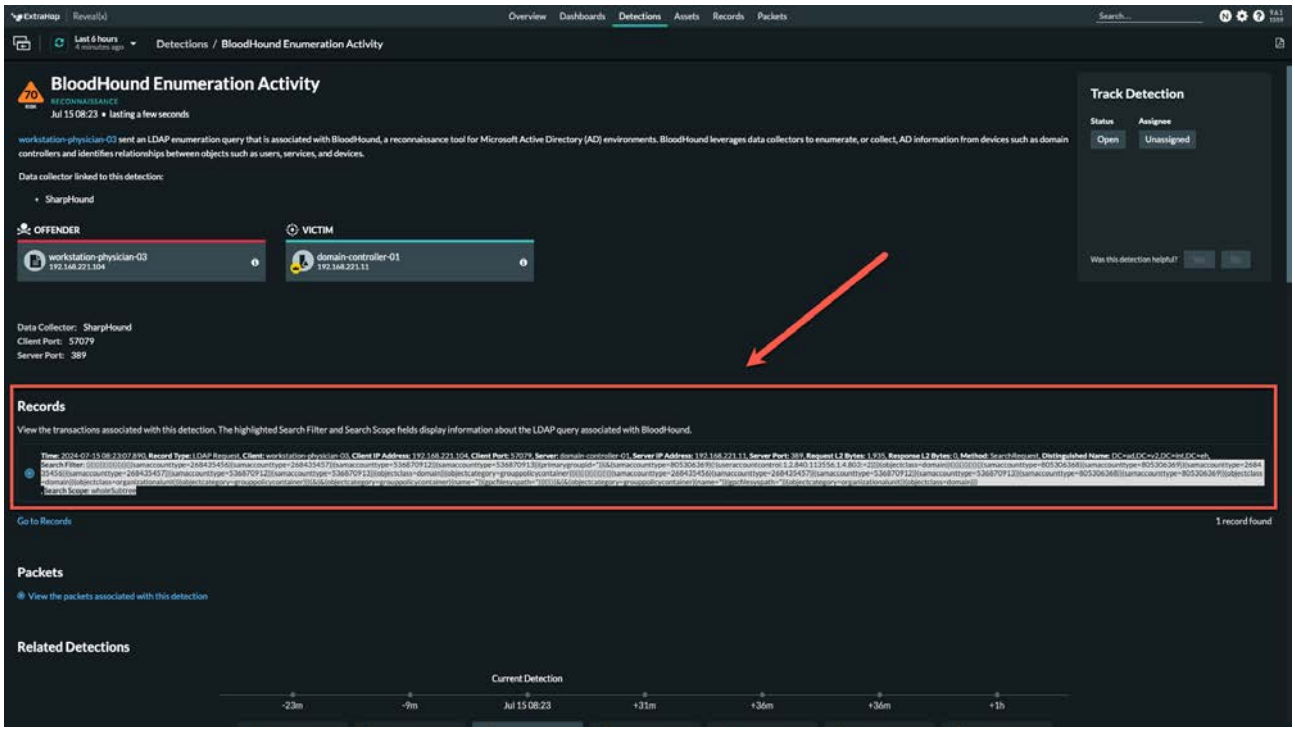
We can see below that this is also a ML attack. Now, it's important to note again, that the only reason we can see this is because we can perform Microsoft protocol decryption, including MSRPC in this case. We can even view the commands that were sent over the MSRPC protocol if you hover above the Command 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.



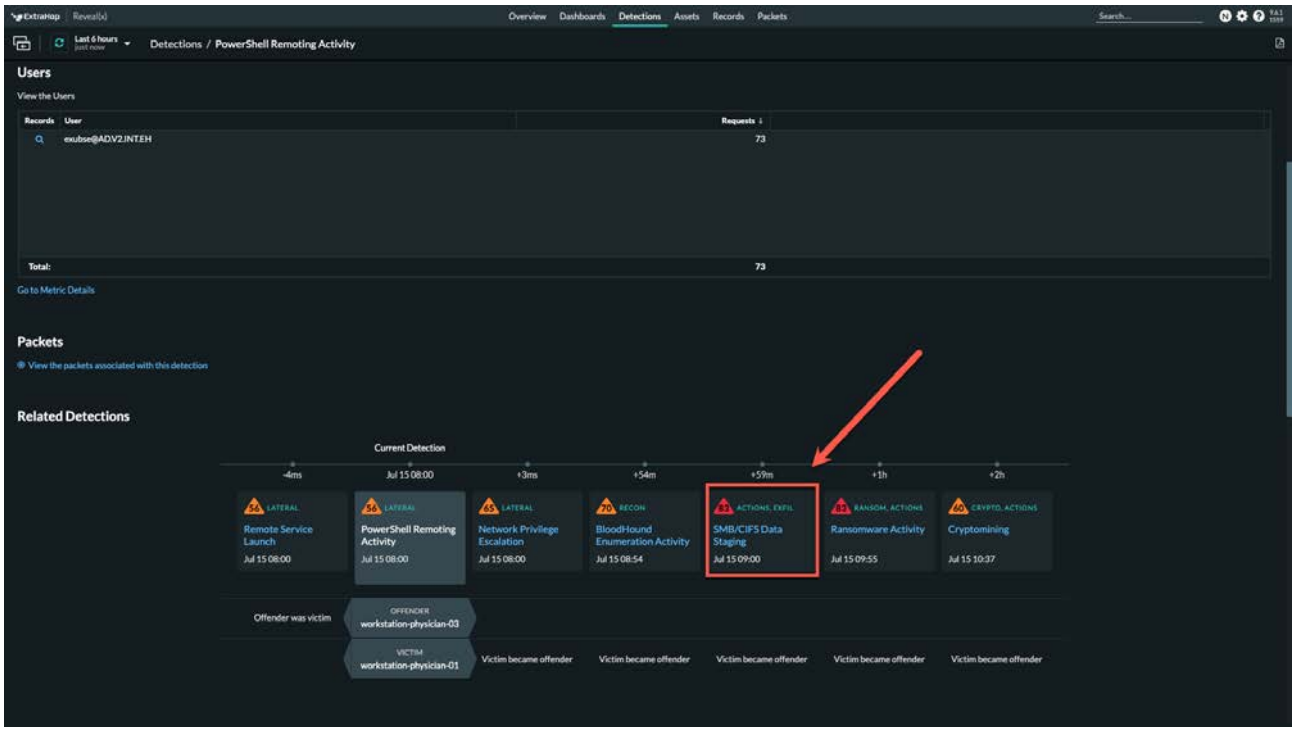
Now, if we click back once to the original related detections, we can also see that the attacker has performed some Bloodhound Enumeration, click the highlighted Bloodhound threat as shown below.



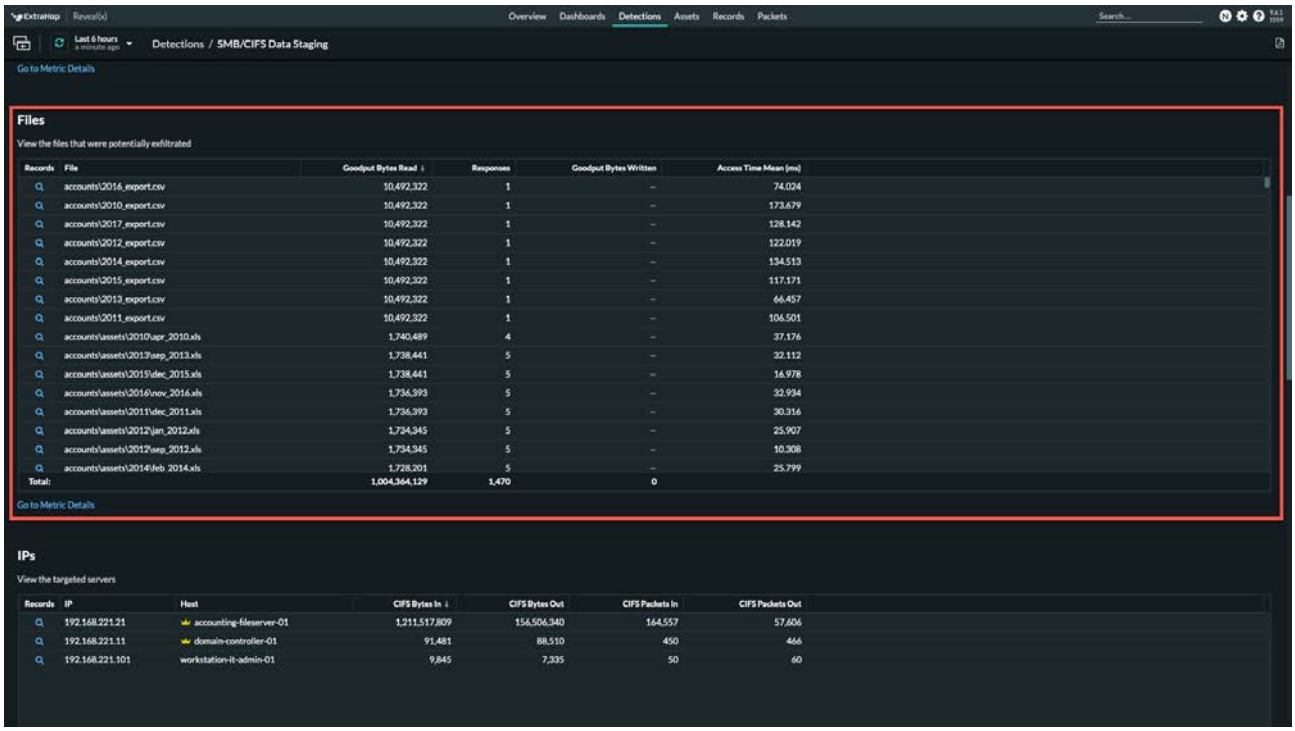
Now, when looking at this Bloodhound activity, not only can we see that it was SharpHound as highlighted just above the record, but we can also see the actual metadata that was extracted from the packets during that conversation as highlighted in the record detail. This is incredible powerful in understanding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



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.



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.

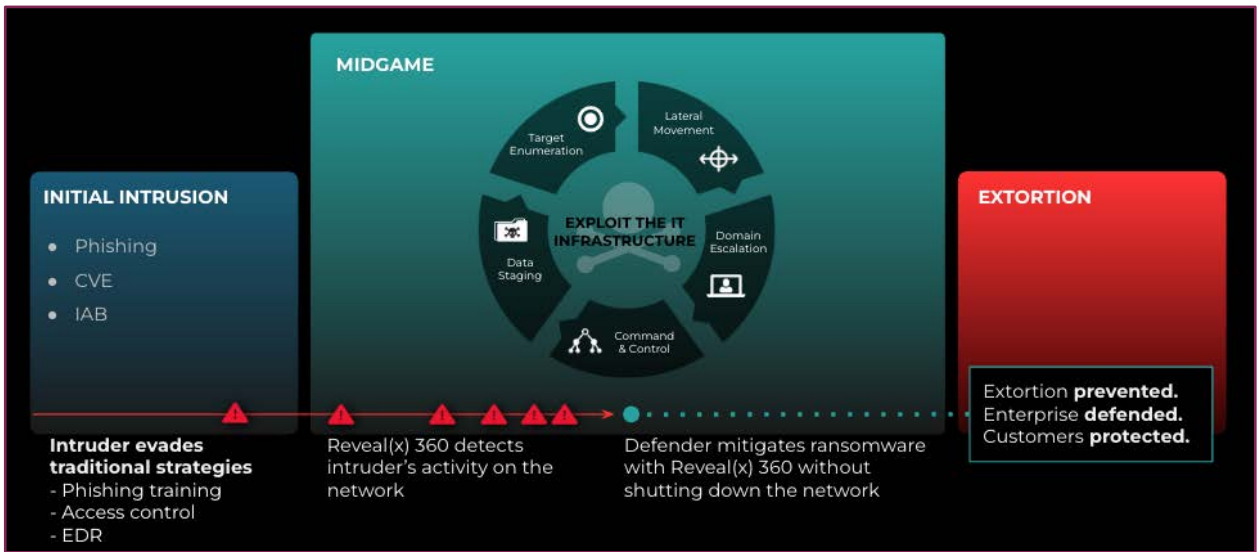


The Midgame

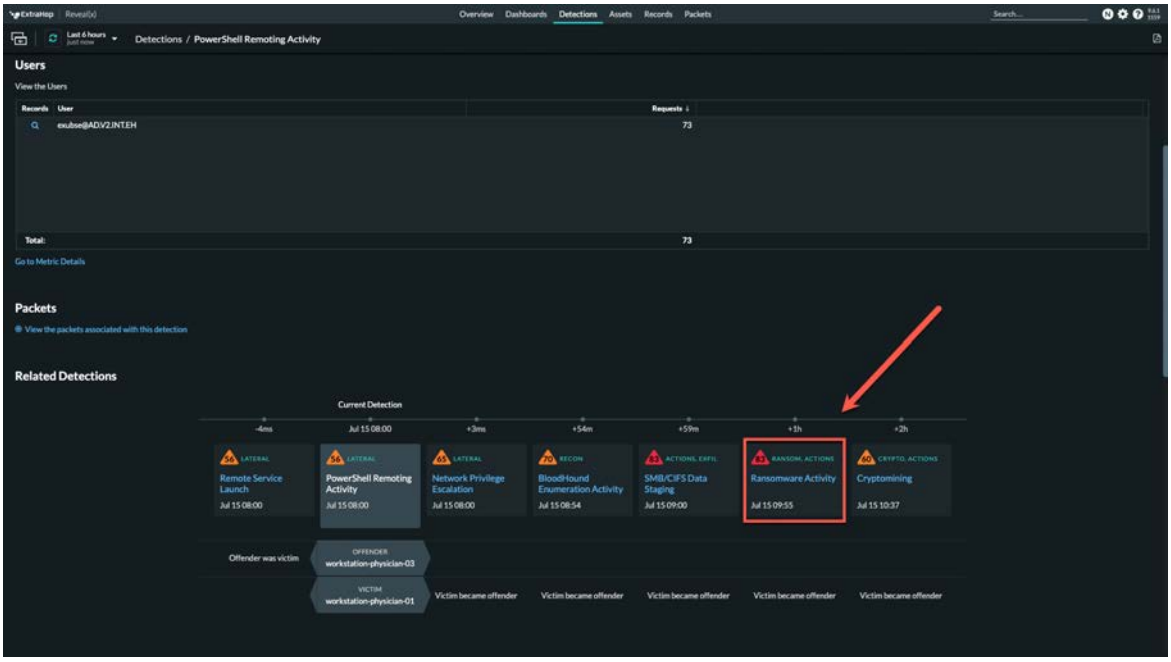
Preventing initial access may not be possible, but with ExtraHop RevealX 360, defenders can detect and stop ransomware in the midgame before they achieve real damage. What we've seen so far has been that Ransomware midgame.

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.



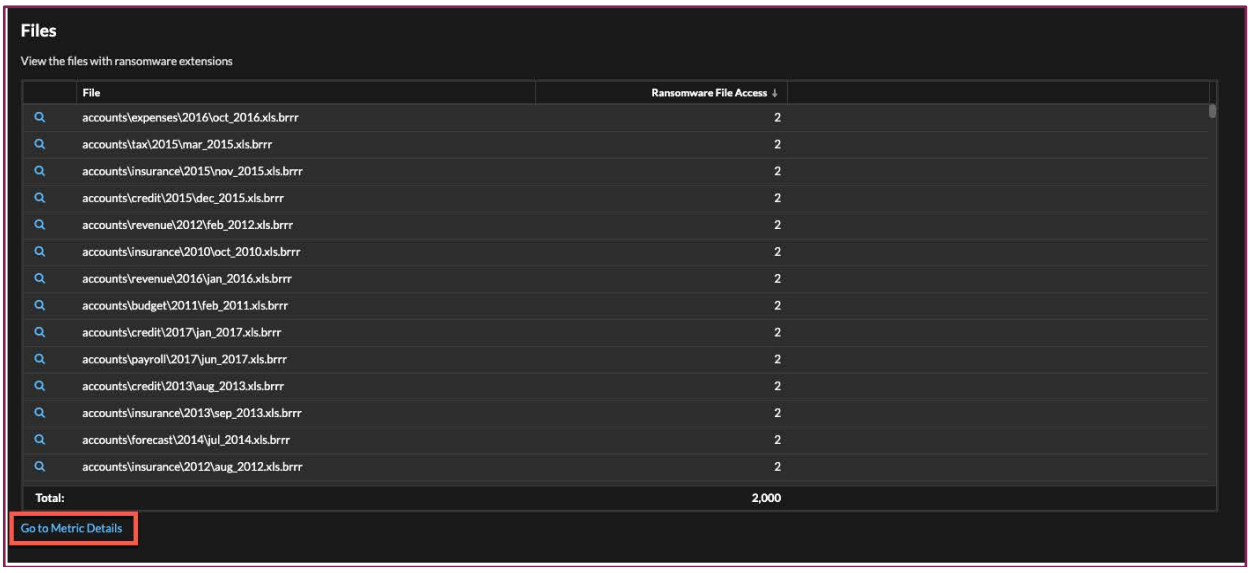
Let's back up one more again and then click on the Ransomware Detection as shown below.



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

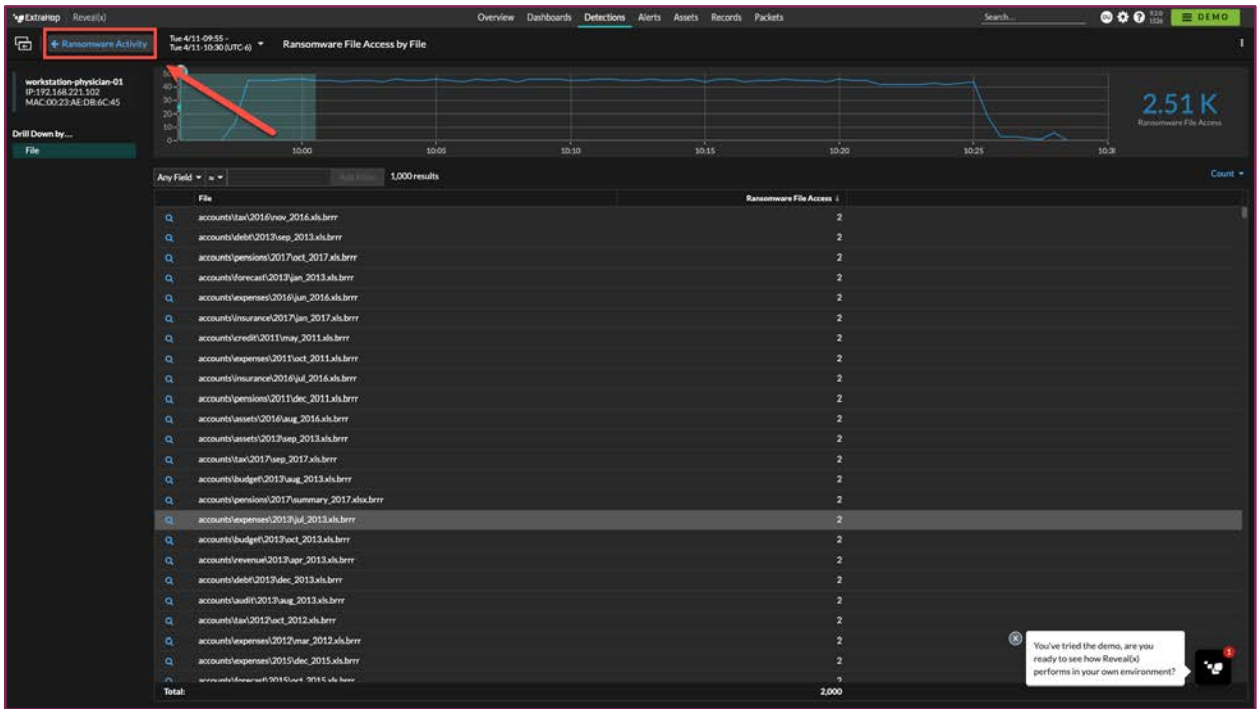
2. Note that we can see the bad actor has encrypted 2,000 total files.

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

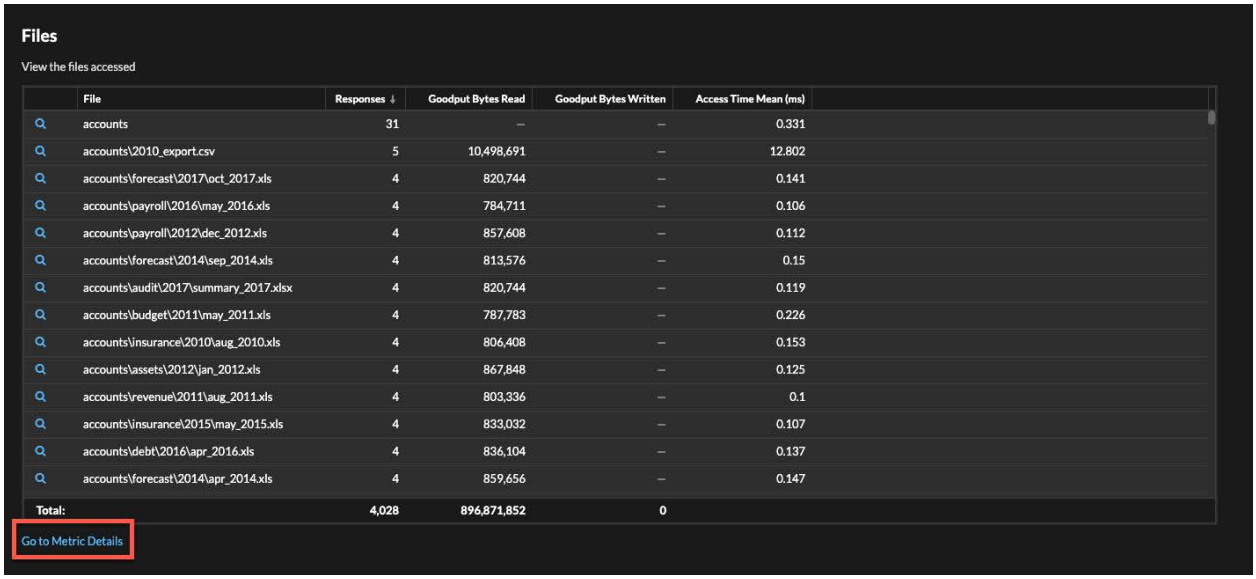


4. From here we can drill down and visualize the timeframe, and encrypted files. Click on the magnifying glass for additional detail for methods, time, and our record detail for each.

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



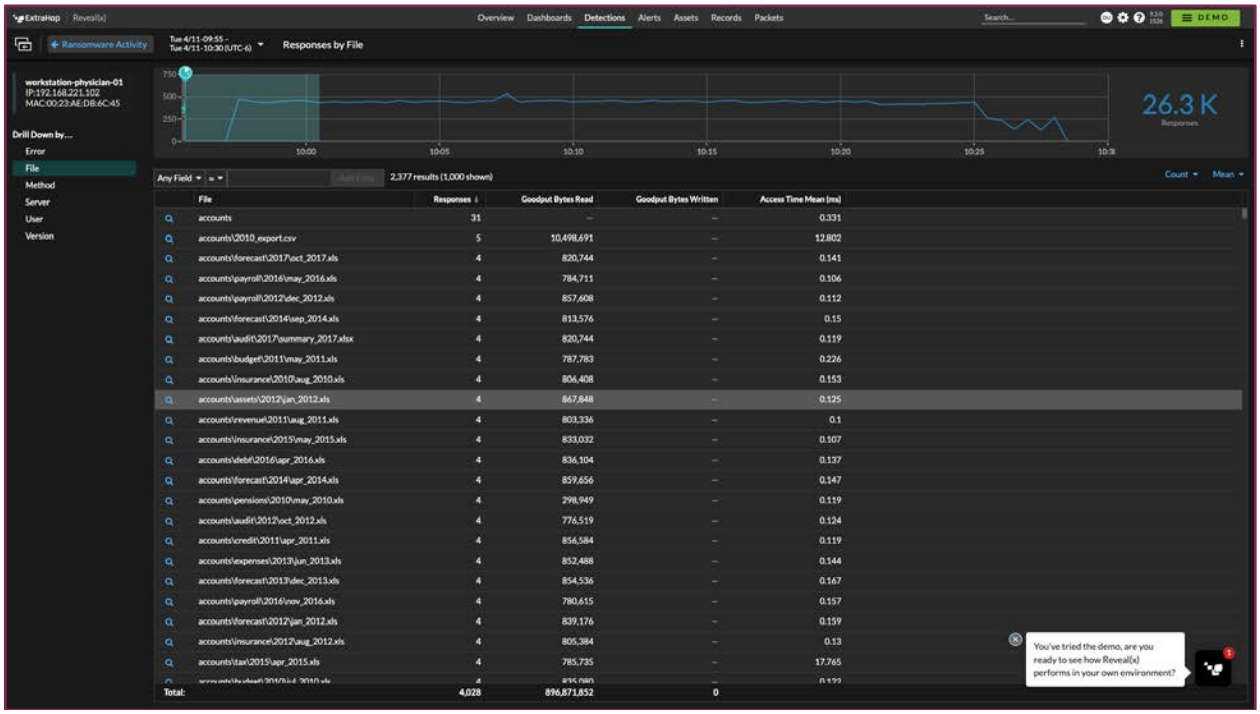
6. As you continue to scroll, you can see files accessed, but not encrypted. This may be important to understand the data accessed when evaluating other post breach items, such as Impact to the Brand, PII, Intellectual Property, etc.



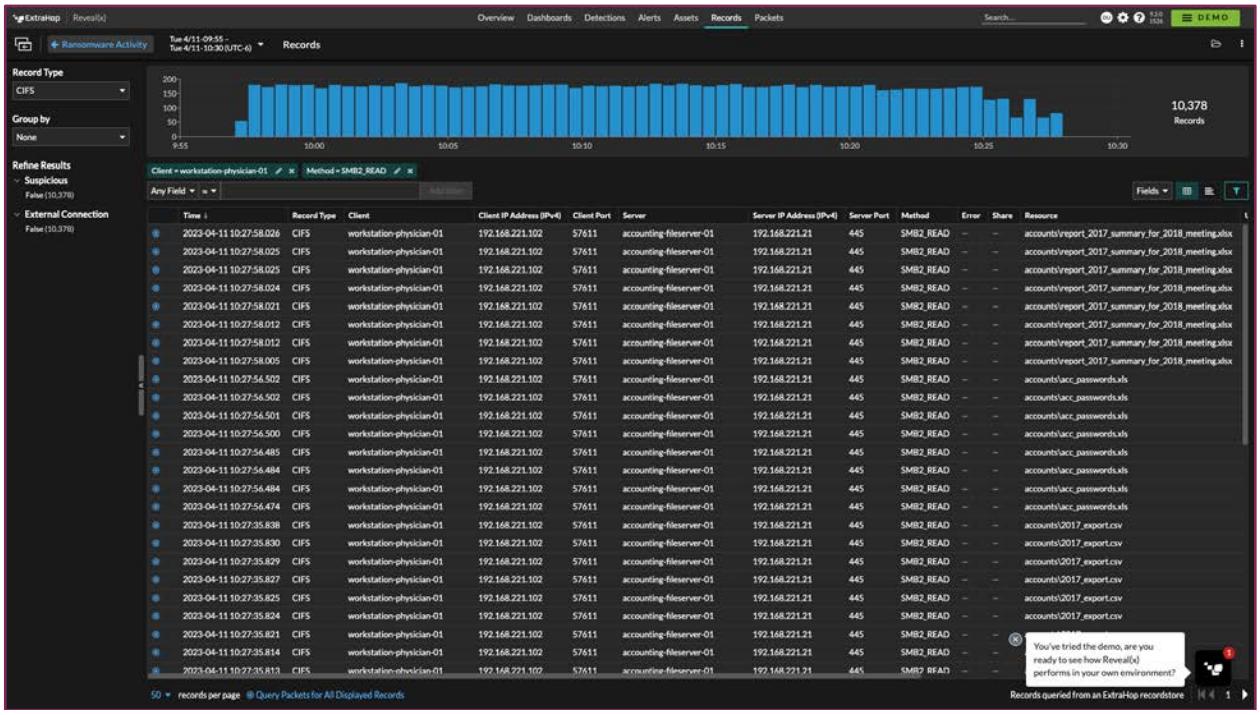
File	Responses	Goodput Bytes Read	Goodput Bytes Written	Access Time Mean (ms)
accounts	31	–	–	0.331
accounts\2010_export.csv	5	10,498,691	–	12.802
accounts\forecast\2017\oct_2017.xls	4	820,744	–	0.141
accounts\payroll\2016\may_2016.xls	4	784,711	–	0.106
accounts\payroll\2012\dec_2012.xls	4	857,608	–	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**	

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:

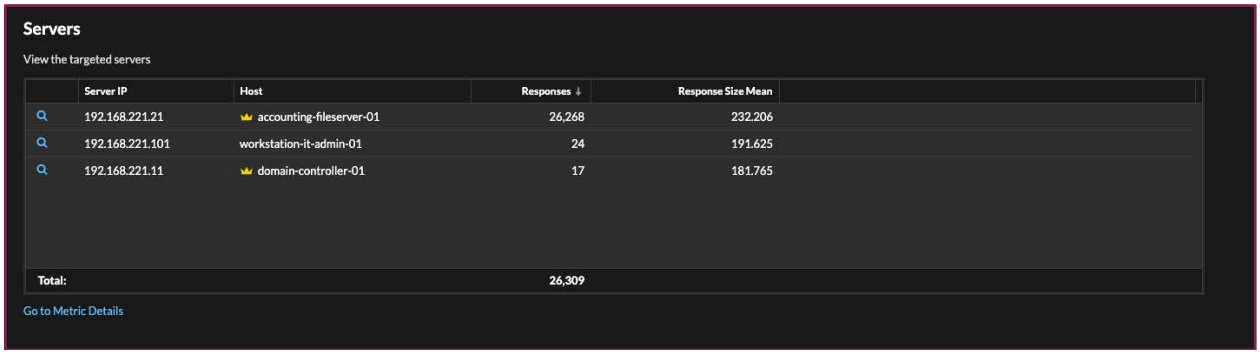
    a. Error
    b. File
    c. Method
    d. Server
    e. User
    f. Version



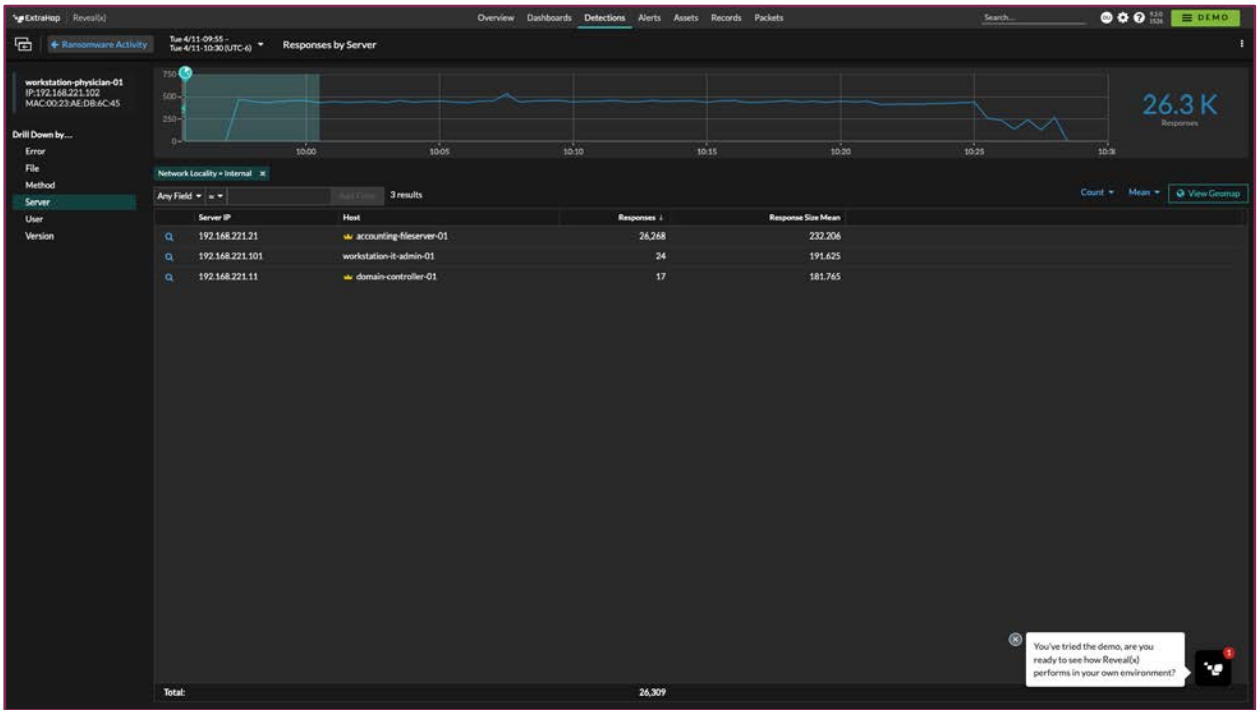
8. Additional drill down detail and associated metrics can be seen in the screen show below.



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.

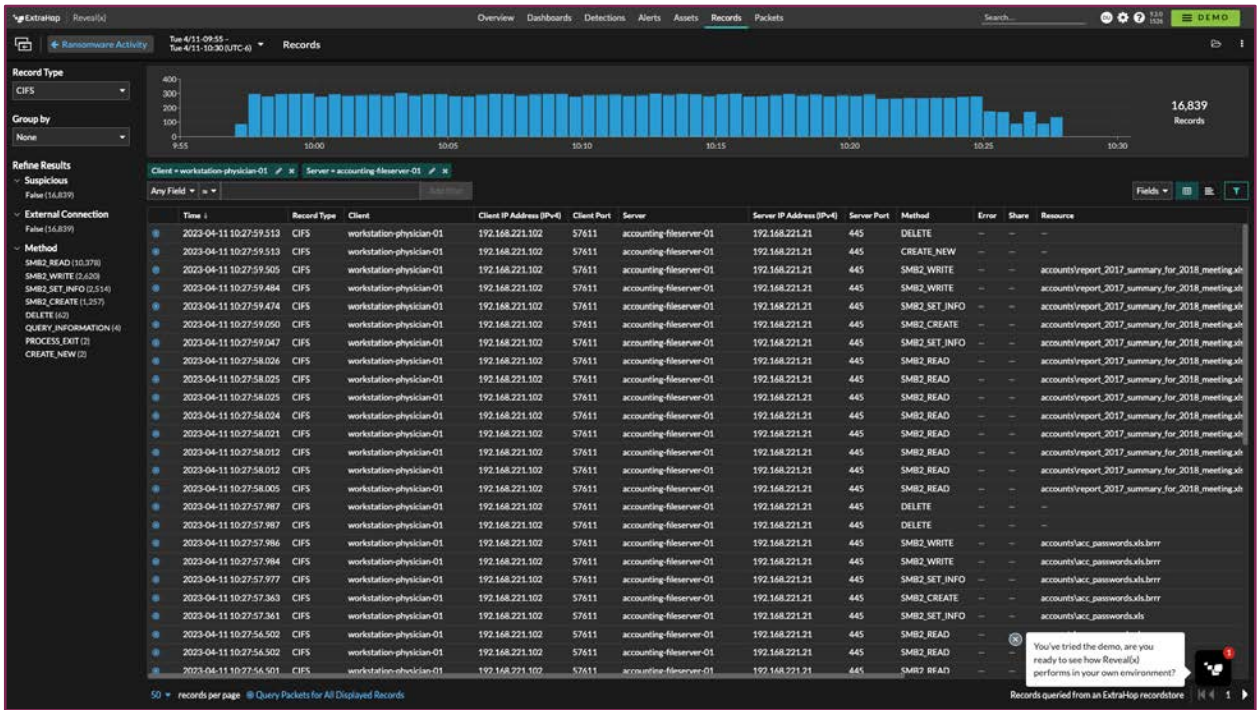


10. Again, going to the 'Metrics Details' provides us additional detail on the Servers, as shown below.



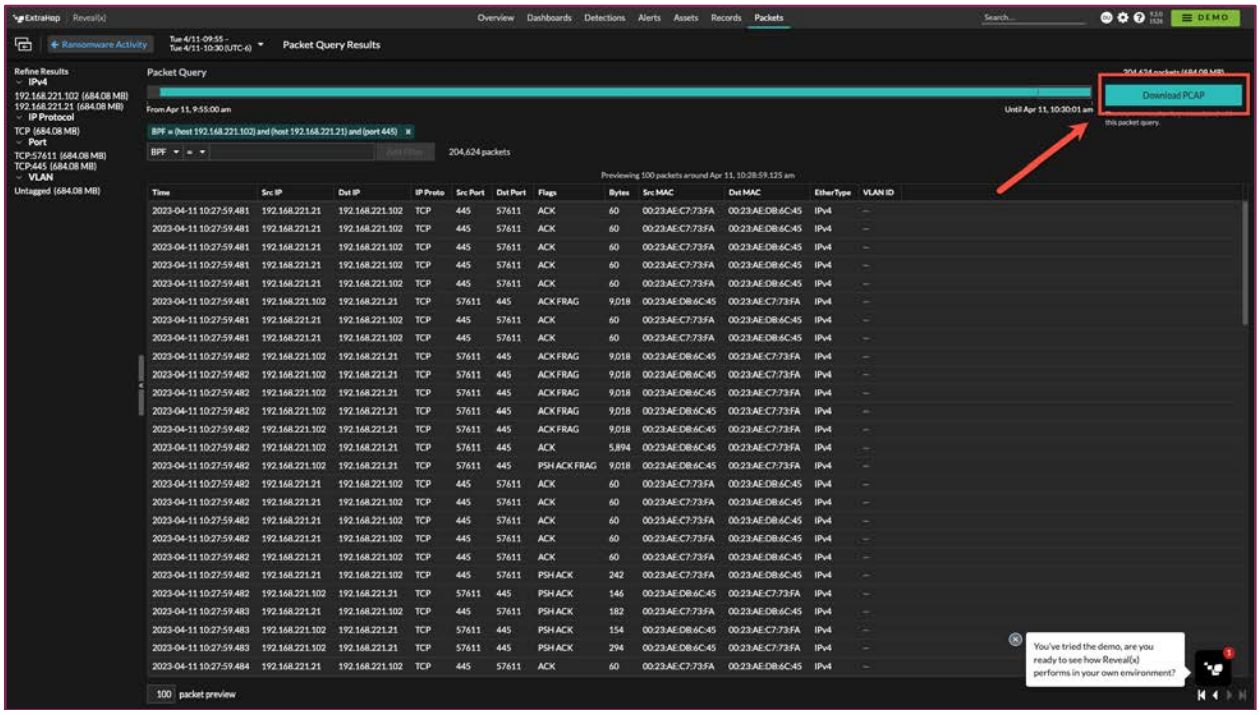
11. Clicking on the magnifying glass for the 'accounting-fileserver-01' will now show us all metric details for that server, including all files, methods, timelines and resources accessed.

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

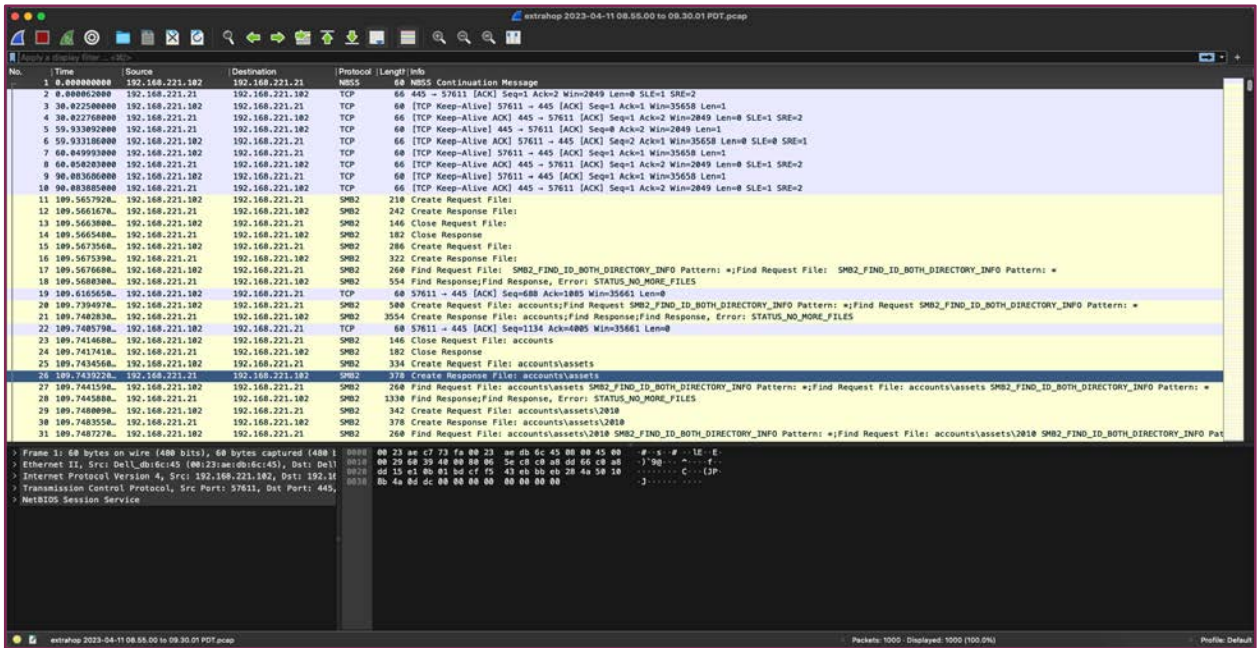


13. Clicking on the bullseye on the left of each record will take us to the packet capture that the platform stored during the breach. See below for details.

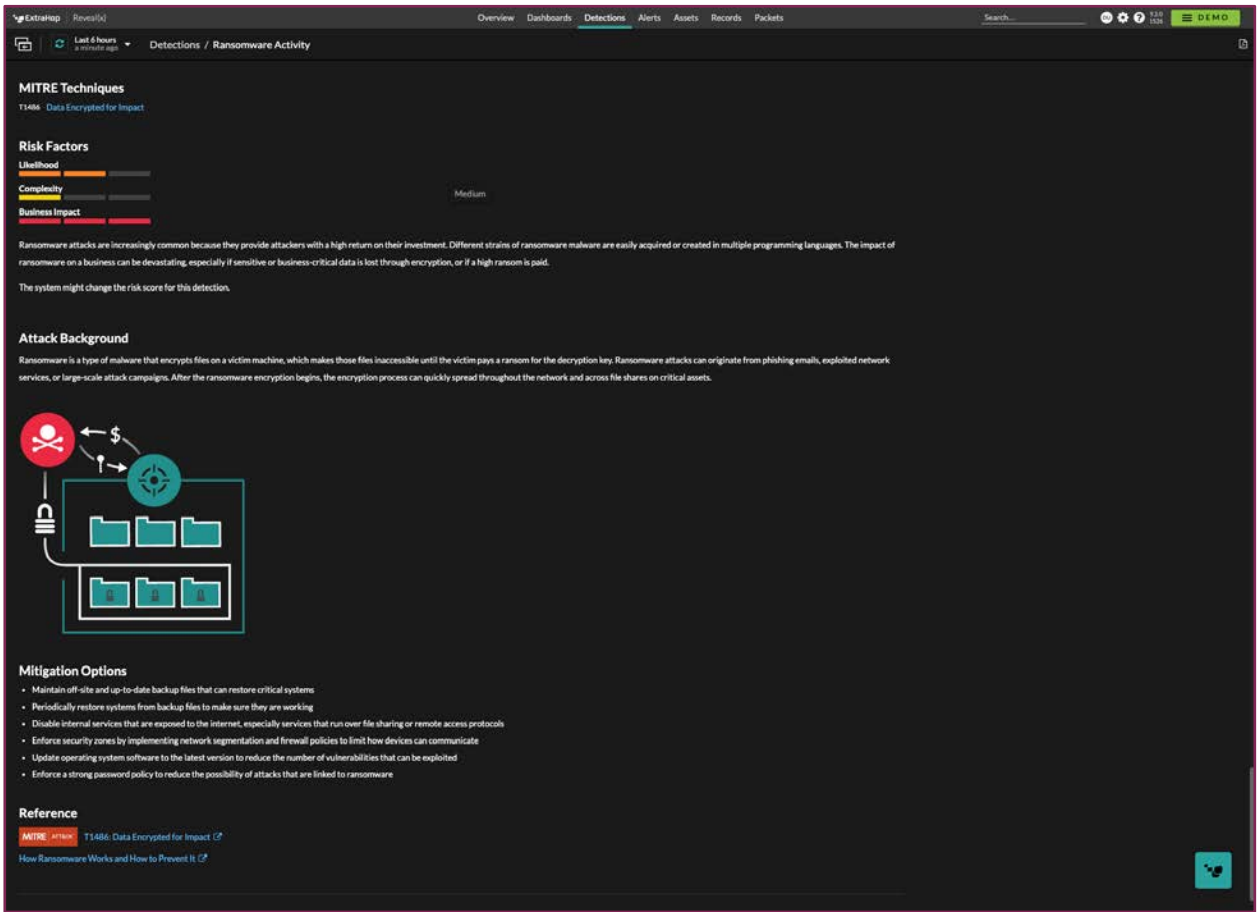
14. Here you can see the full transaction of each record as noted in the previous screen. We've also included the ability to download the PCAP for this specific record.



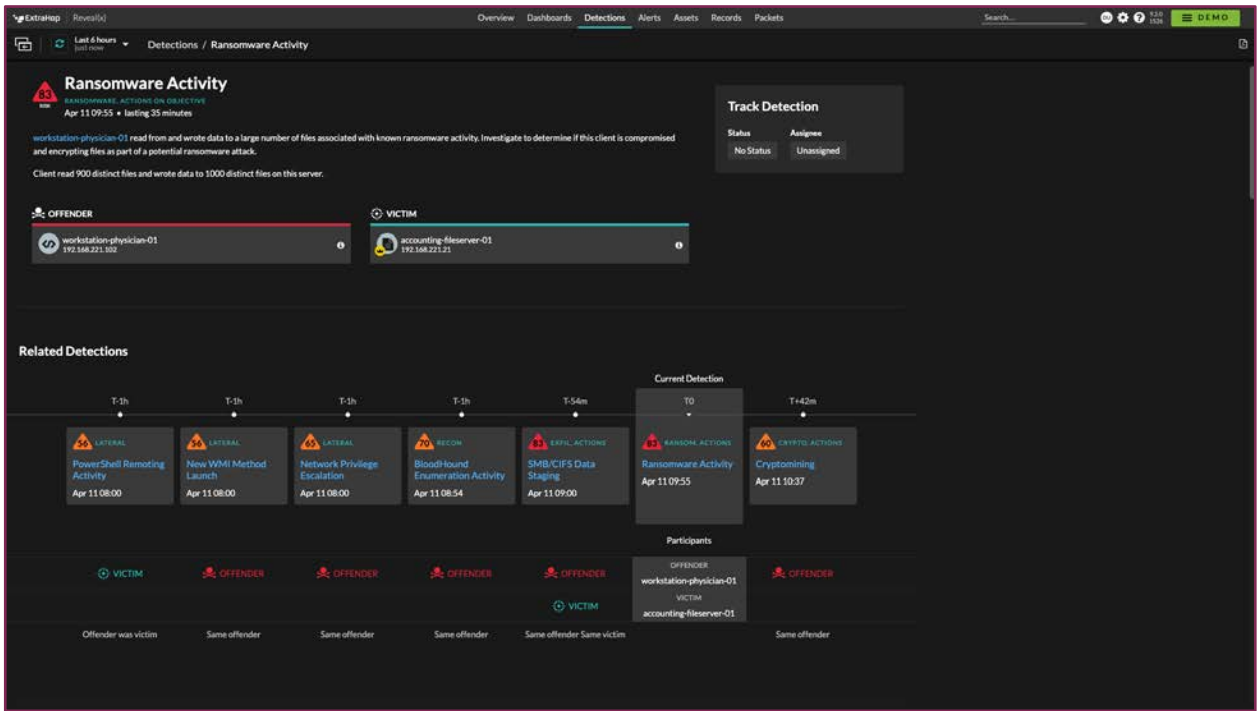
15. Opening the downloaded PCAP in wireshark now shows us the full packet detail.



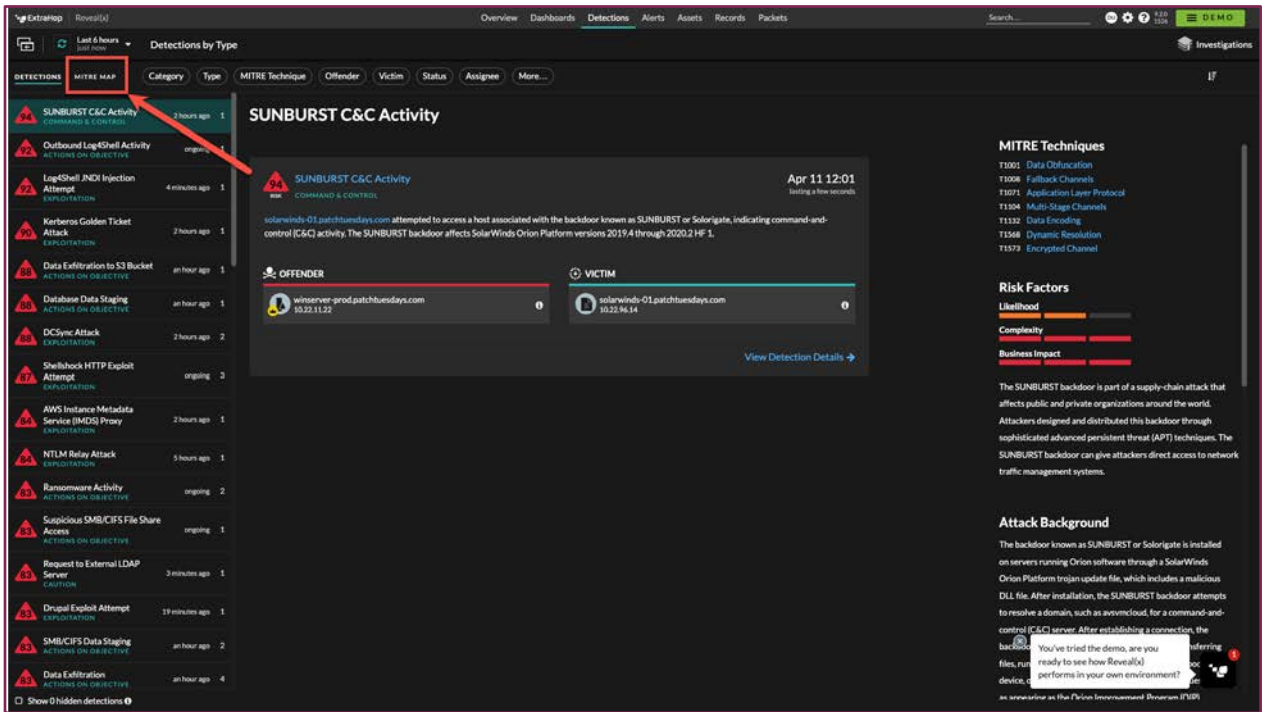
16. Again, click on the upper left corner on ‘Ransomware Activity’ and scroll down and you’ll see the MITRE ATT&CK Techniques used, background and additional mitigation options listed to recover from the breach.



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.

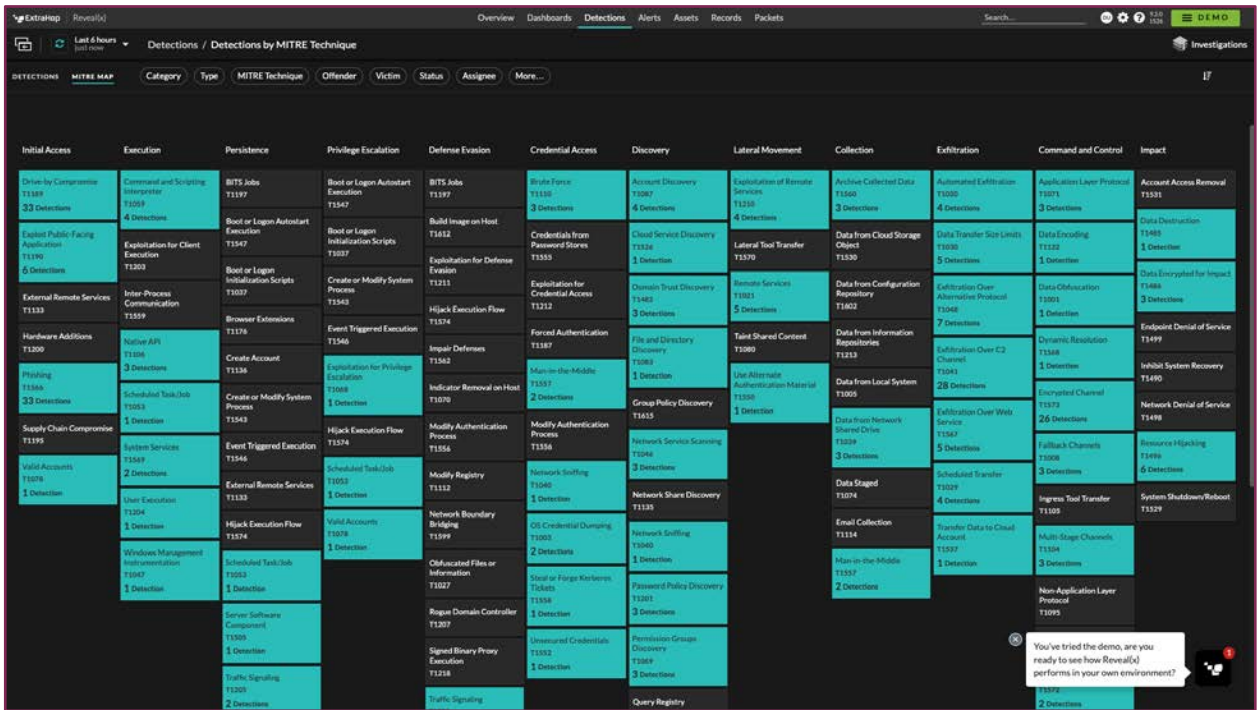


2. From here, you can see the MITRE ATT&CK matrix and the mapping of the detections from the previous page. These are also all clickable to get the MITRE subcategory ID and associated detections found by the platform.

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.


Overview
Dashboards
Detections
Alerts
Assets
Records
Packets
DEMO
Detections / Detections by MITRE Technique
Investigations
Category
Type
MITRE Technique
Offender
Victim
Status
Assignee
More...
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact
You've tried the demo, are you ready to see how Reveal(x) performs in your own environment?