ExtraHop

Ransomware | MITRE Techniques Demo Test Drive

ExtraHop

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.

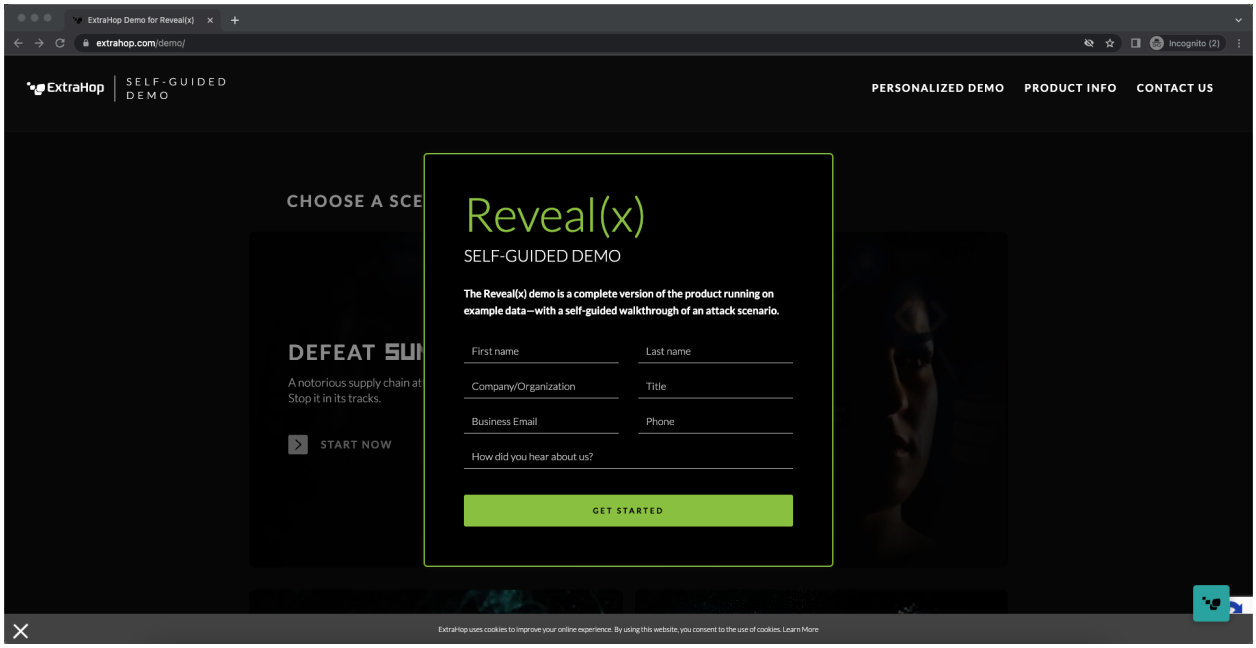
Indeed, modern ransomware attacks are so profitable that criminal groups like Black Basta, Lock Bit, Conti, and formerly REvil are continually developing new and innovative ways to systematically attack organizations while simultaneously increasing the difficulty of detection and prevention. These tactics 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.

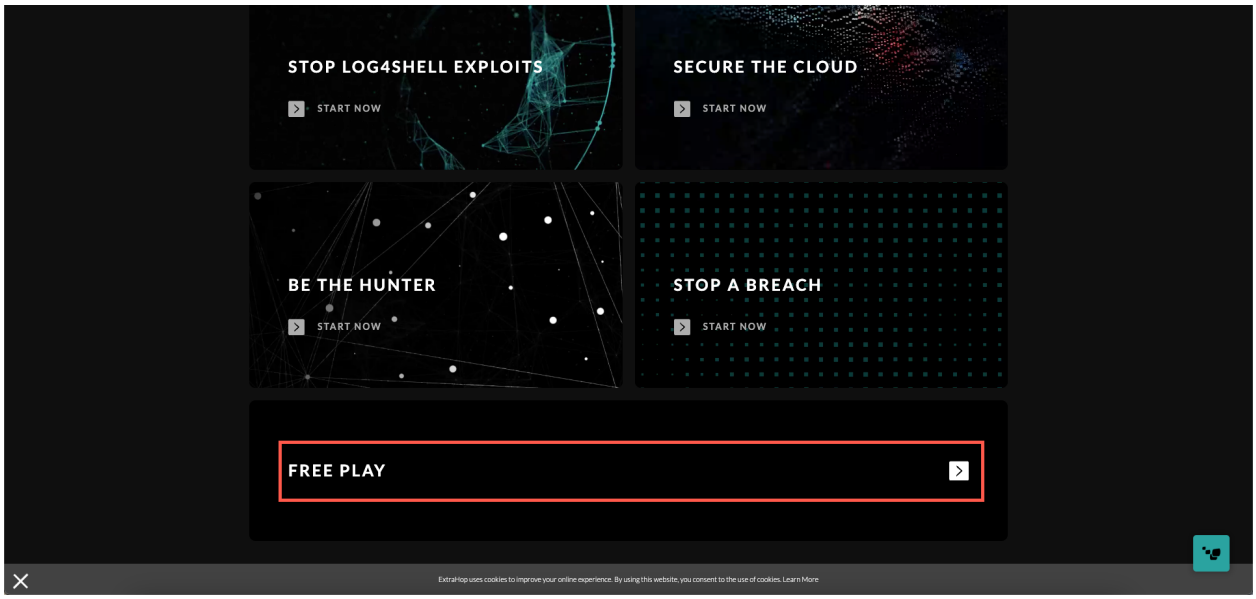
One prominent example is the speed with which the BlackByte ransomware gang began leveraging the Proxy-Logon and Proxy-Shell vulnerabilities as part of their standard attack playbook. The adaptability of these criminal groups and their ability to bypass traditional perimeter defenses serves to underscore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



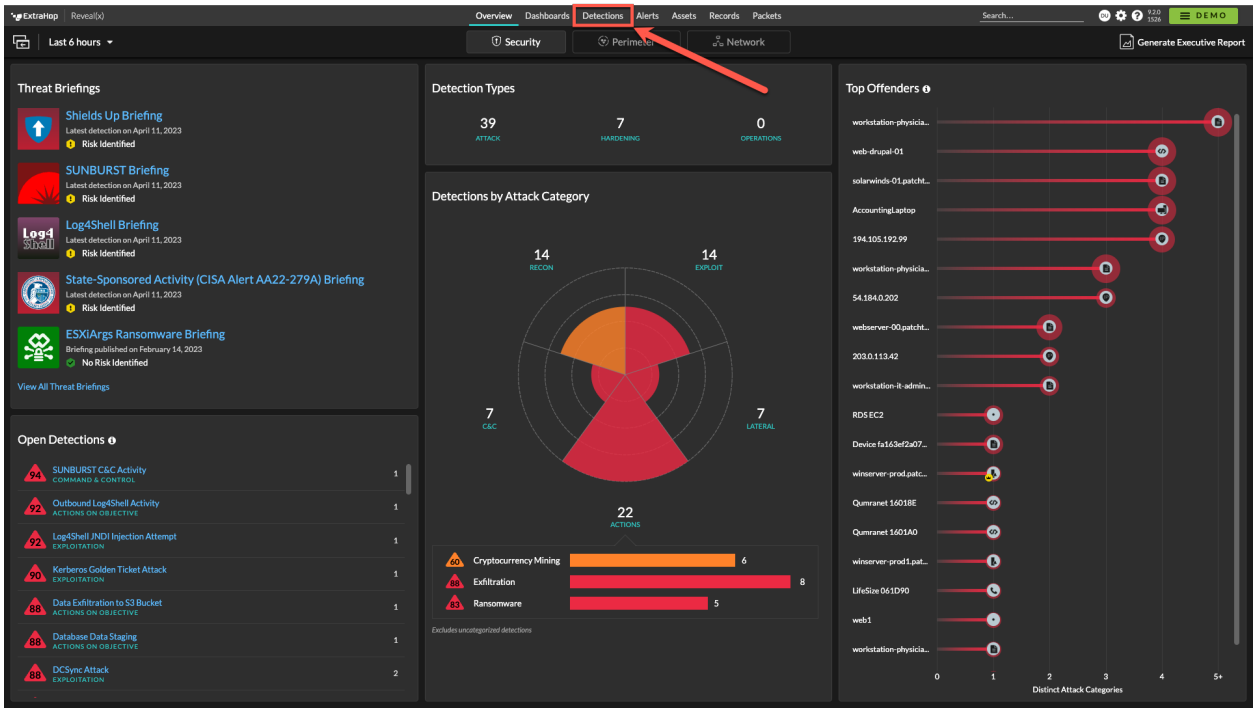
3. There are several guided scenarios listed that you could use at your leisure to walk through the platform capabilities. Please scroll down to the bottom of the page and click on ‘FREE PLAY’. This provides you with unscripted access and you will follow the steps below.



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.

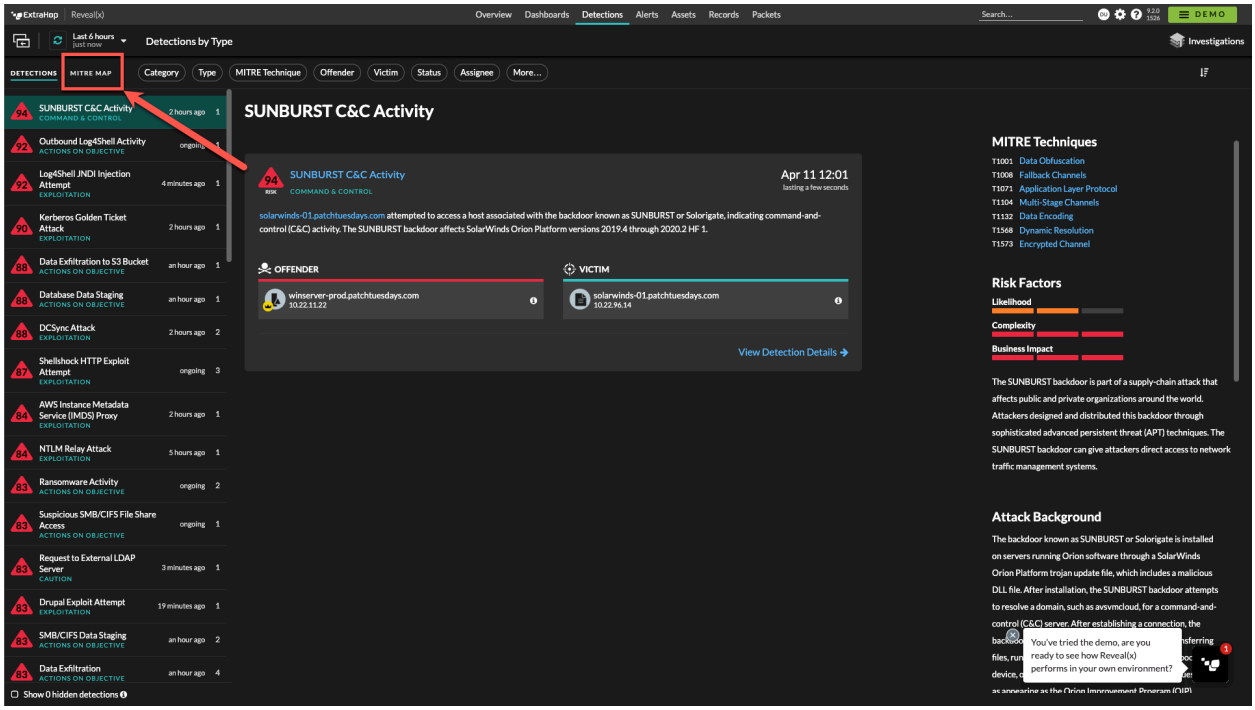
1. Click on the top-level Detections tab, as shown below to go to the detections page.



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.

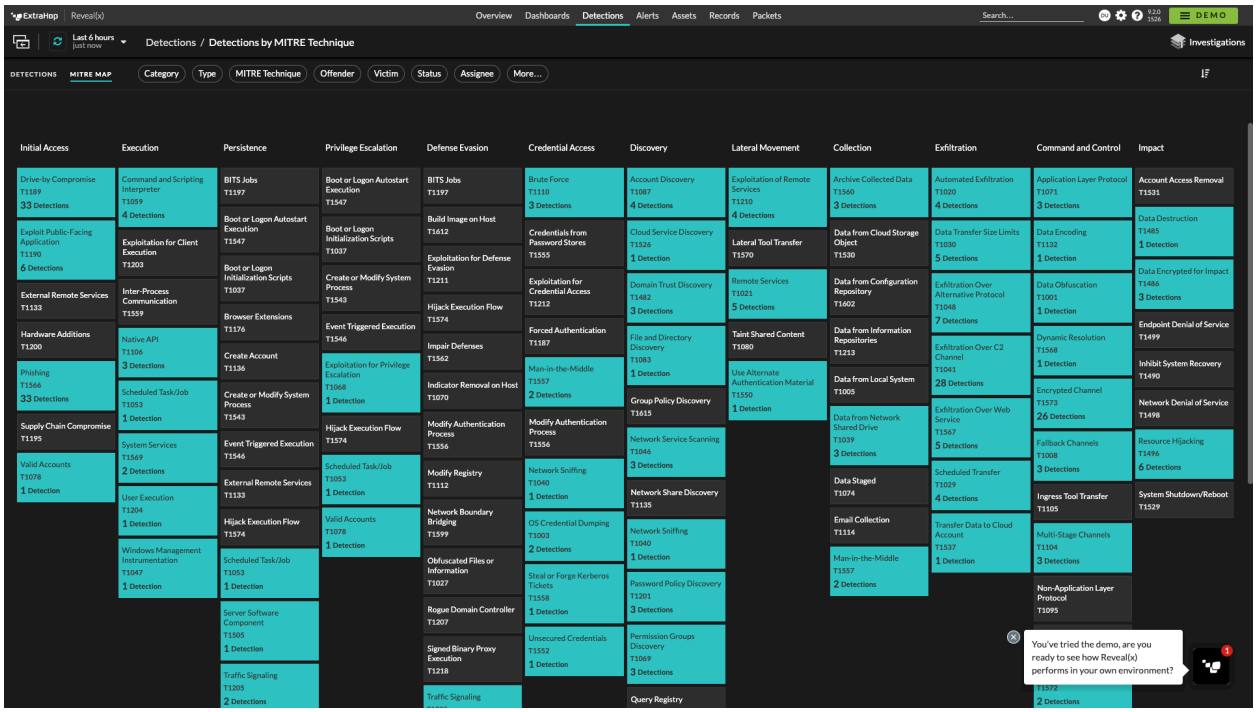
4. From here, click on the ‘MITRE MAP’, as noted below to go the mapping of the detections to the MITRE ATT&CK framework.



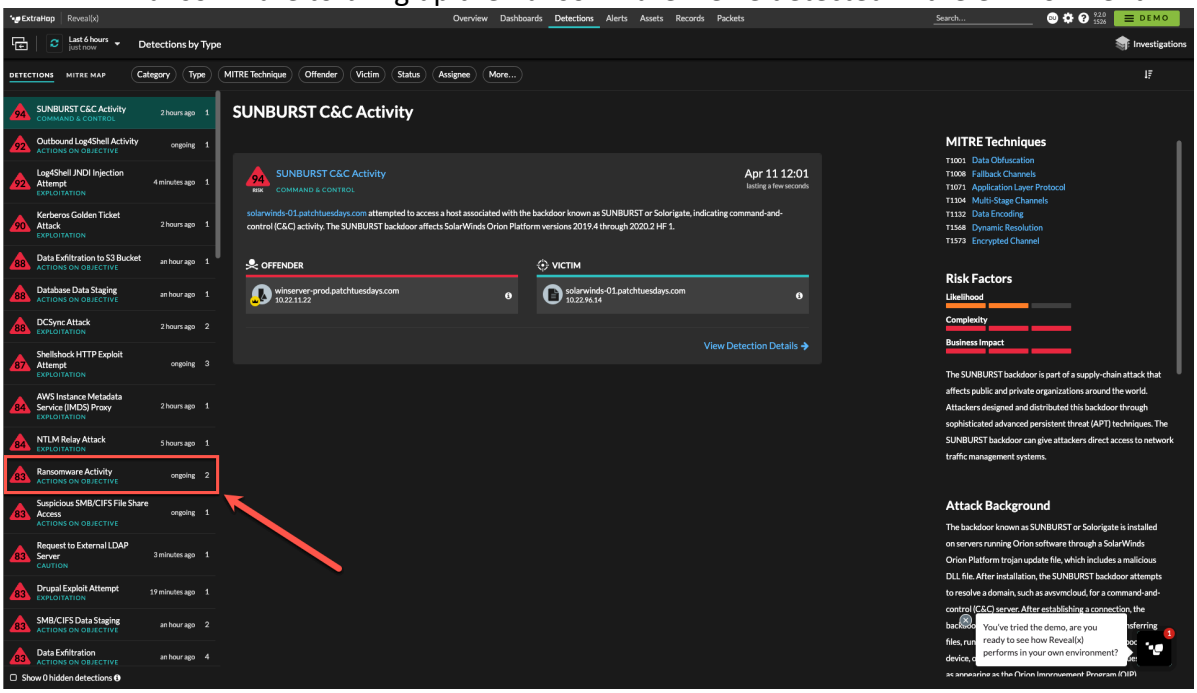
5. From here, you can see the MITRE ATT&CK matrix and the mapping of the detections from the previous page. These are also all clickable to get the MITRE subcategory ID and associated detections found by the platform.

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.

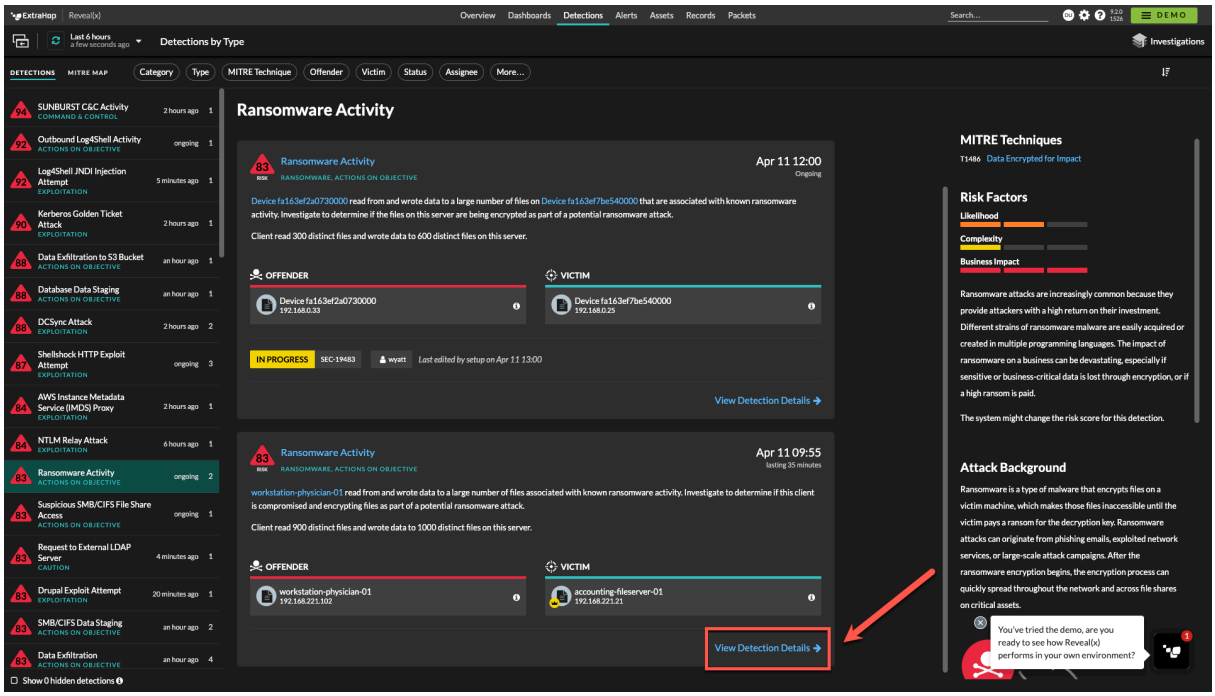
7. Click on the Detections tab, listed next to the MITRE MAP in the upper left corner to return to the Detections tab.



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.



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



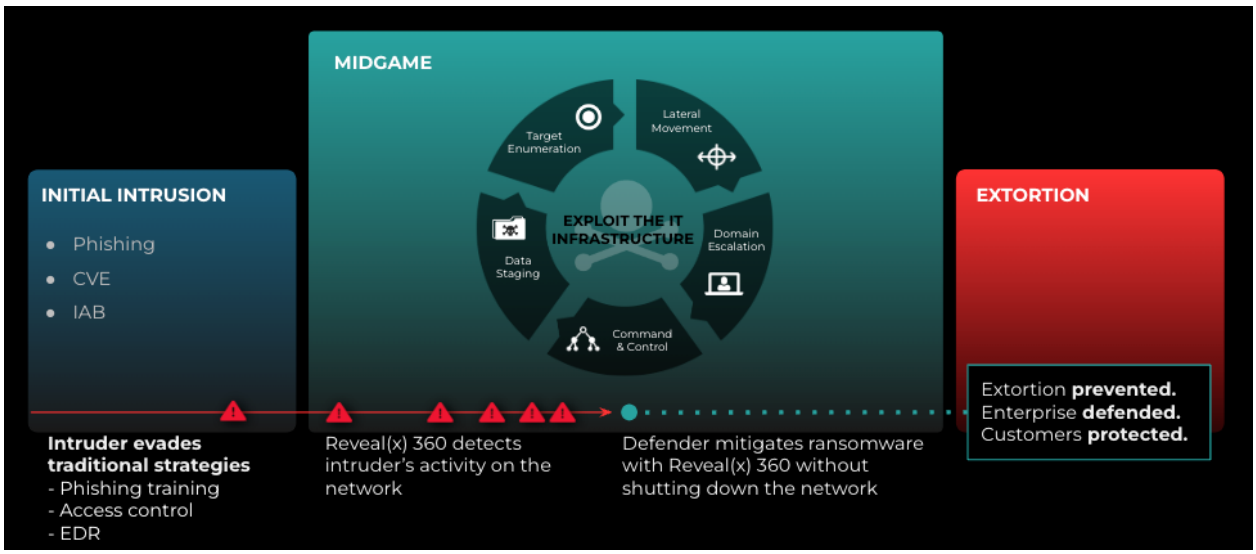
ExtraHop

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.

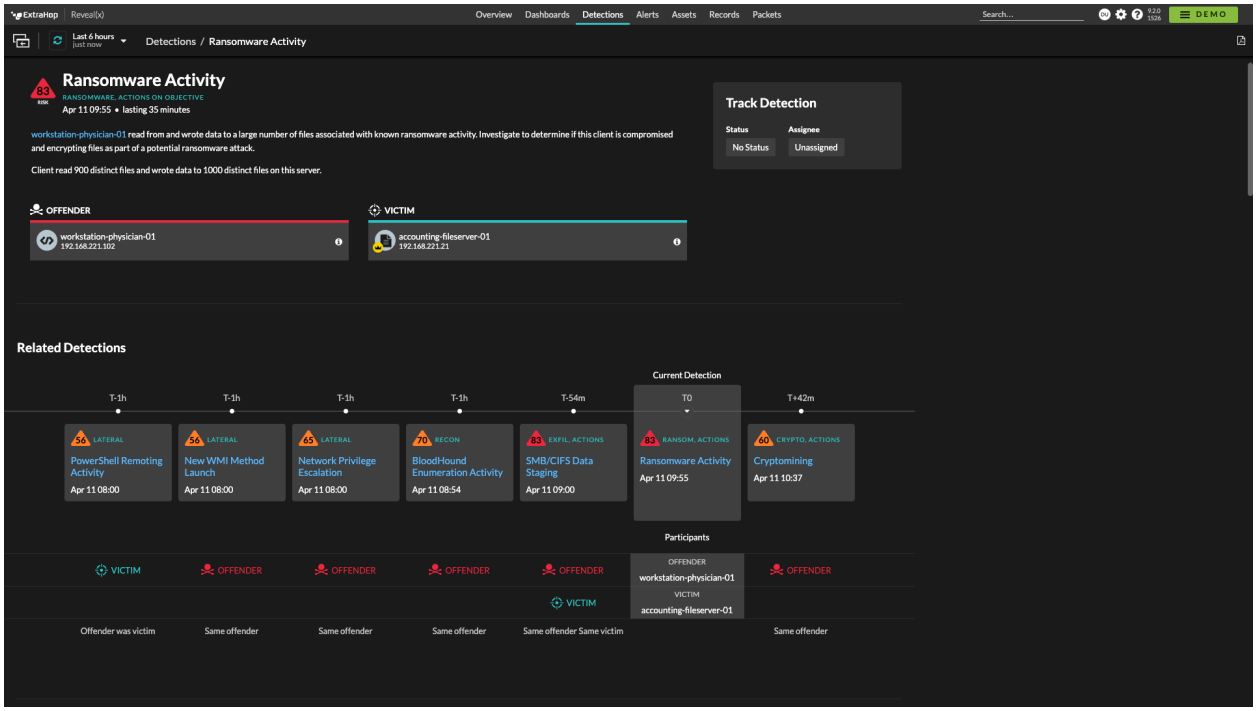
Using machine learning, you can detect behaviors that signal a ransomware attack in progress, with alerts that flag attackers as they enumerate targets, escalate domain privileges, and send C2 over noisy channels like DNS. It also spots data staging before encryption starts, allowing your business to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

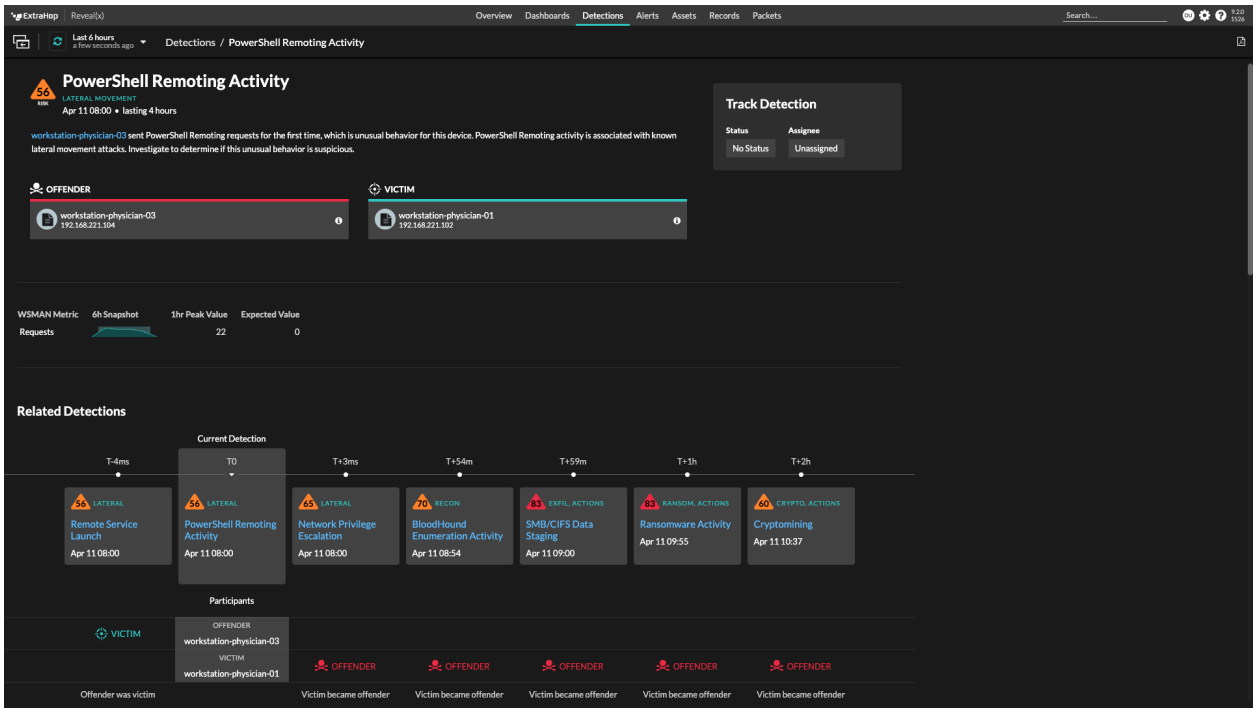
2. From here, we can see the offender and victim in this specific detection. It lists the related detections both prior and post ransomware encryption, even with the bad actor having installed Cryptomining software transferred over the Stratum protocol and connecting to the mining pool at pool.tupportxmr.com.



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.

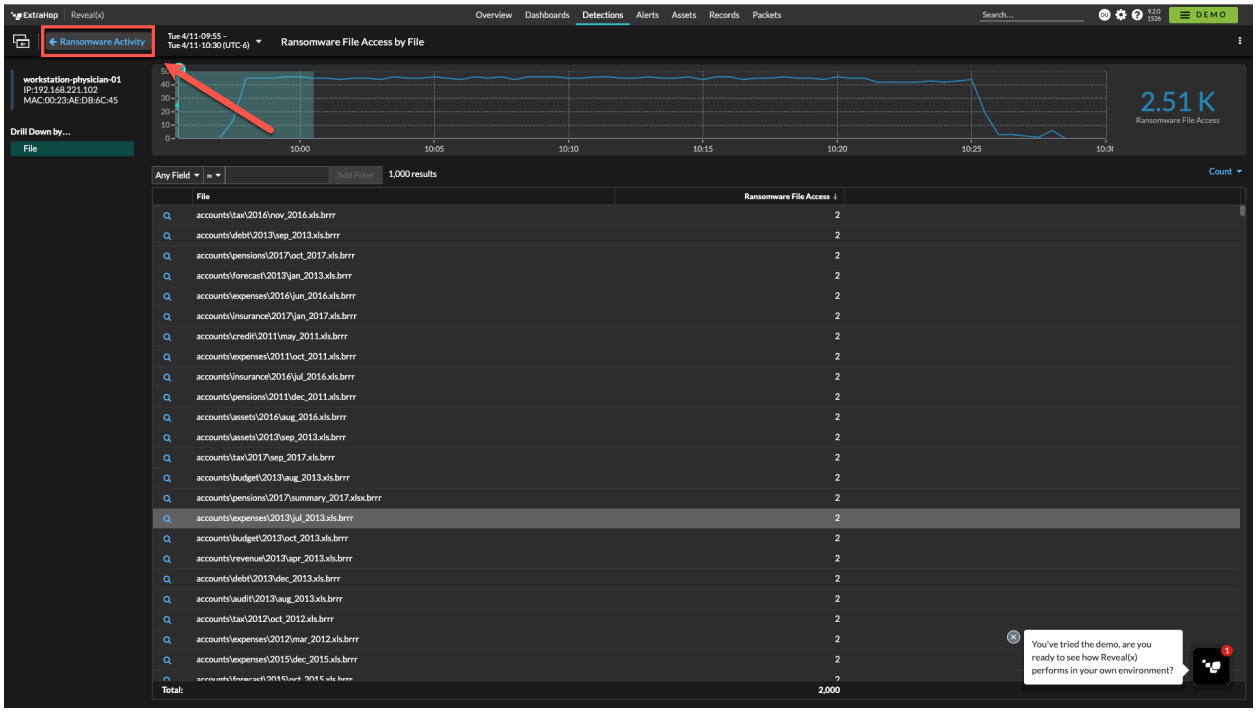
7. We can see the files that have been encrypted when accessed from the ‘workstations-physician-01’ PC to the ‘accounting-fileserver-01’.

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

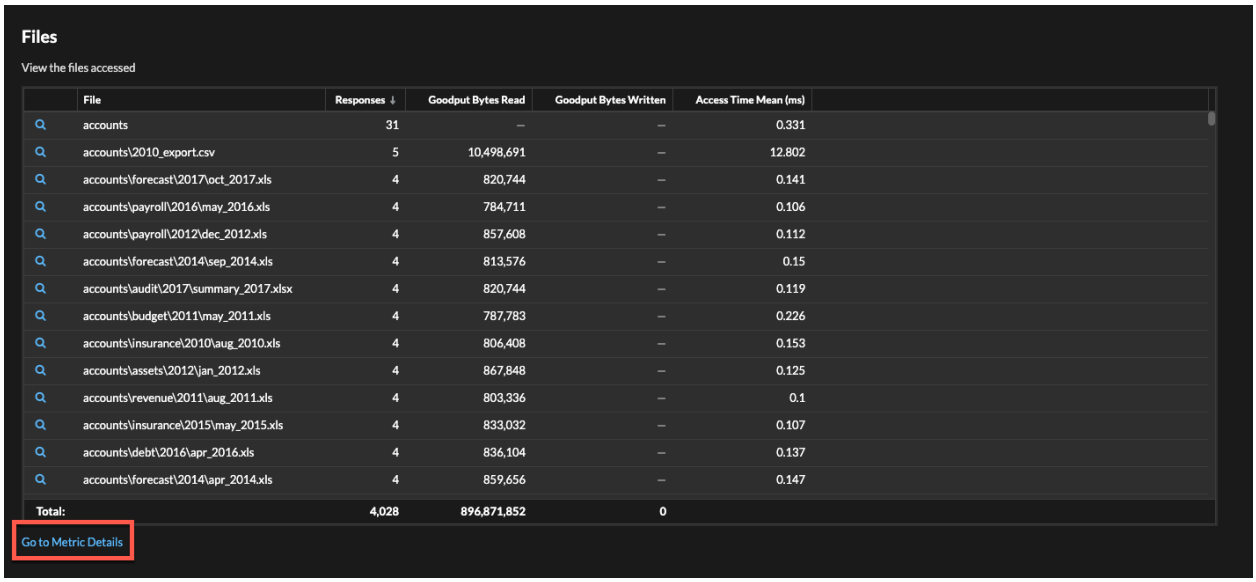
9. For additional detail, click on ‘Go to Metric Details as noted below’.

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.

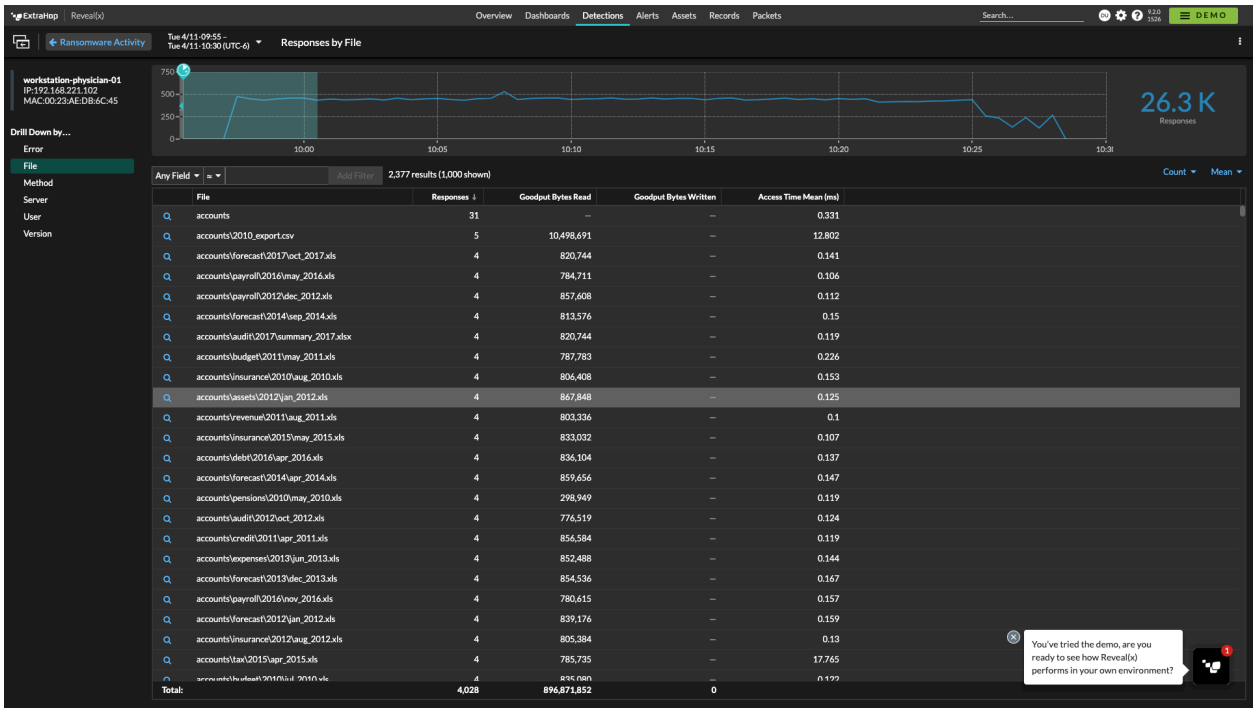


12. As you continue to scroll, you can see files accessed, but not encrypted. This may be important to understand the data accessed when evaluating other post breach items, such as Impact to the Brand, PII, Intellectual Property, etc.

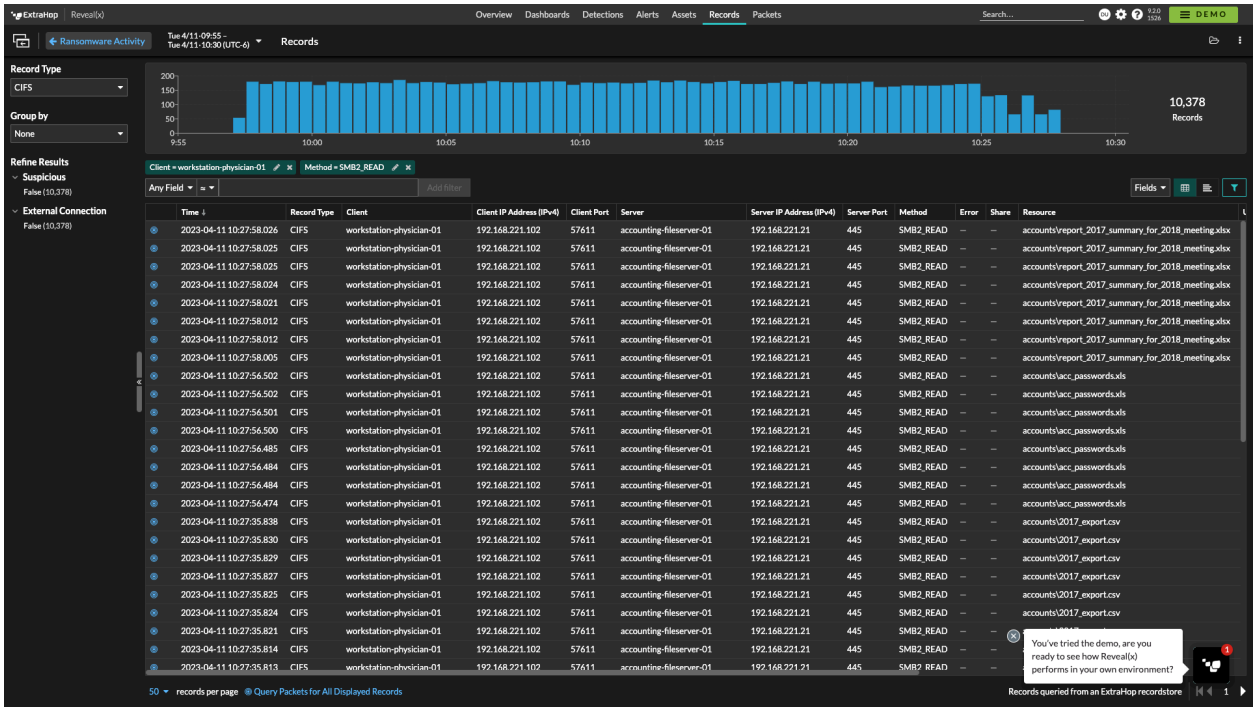


13. Again, you now see that while over 4,000 files were accessed, just 2,000 were encrypted with the ransomware. As you click on the 'Metric Details' again, you can now drill down on the left-hand pane by:

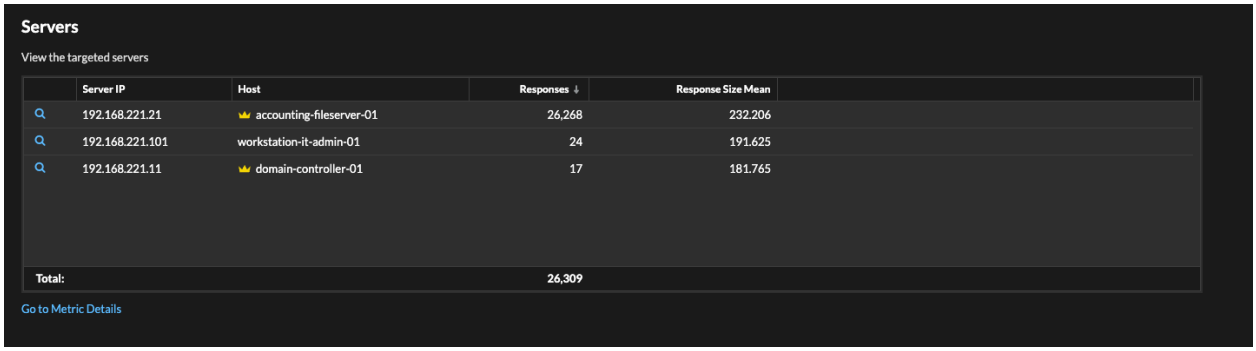
    a. Error
    b. File
    c. Method
    d. Server
    e. User
    f. Version



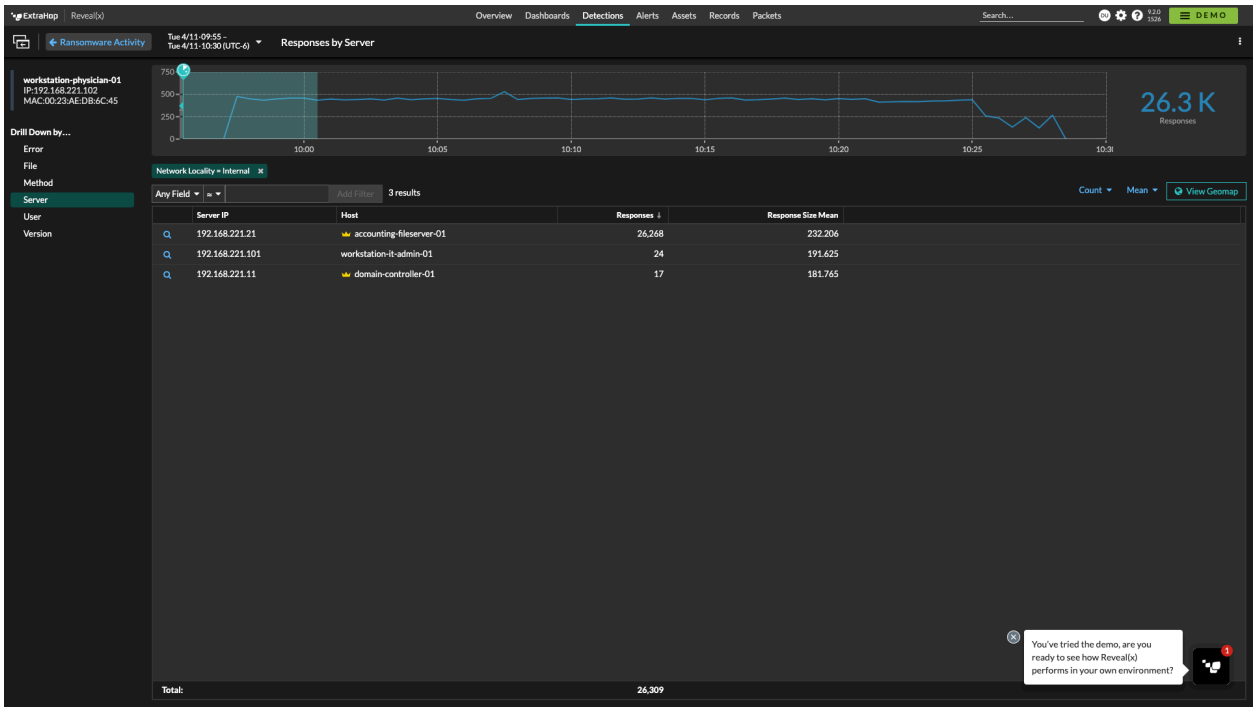
14. Additional drill down detail and associated metrics can be seen in the screen show below.



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.

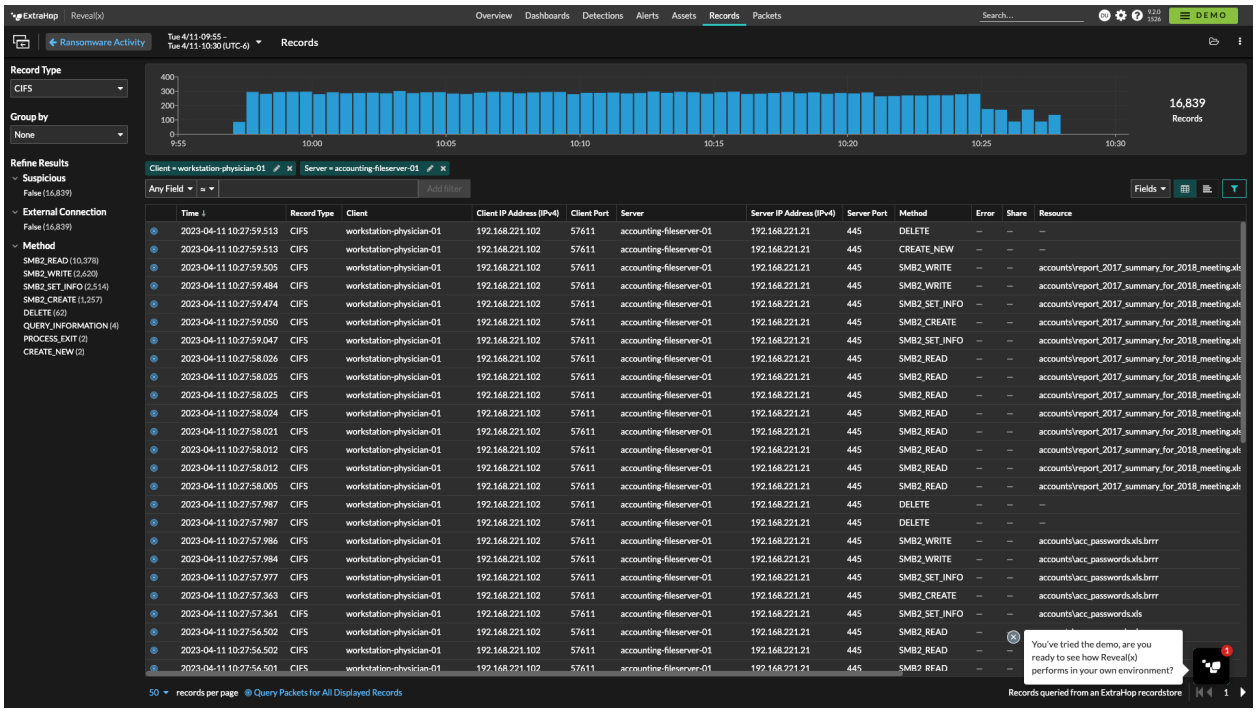


16. Again, going to the ‘Metrics Details’ provides us additional detail on the Servers, as shown below.



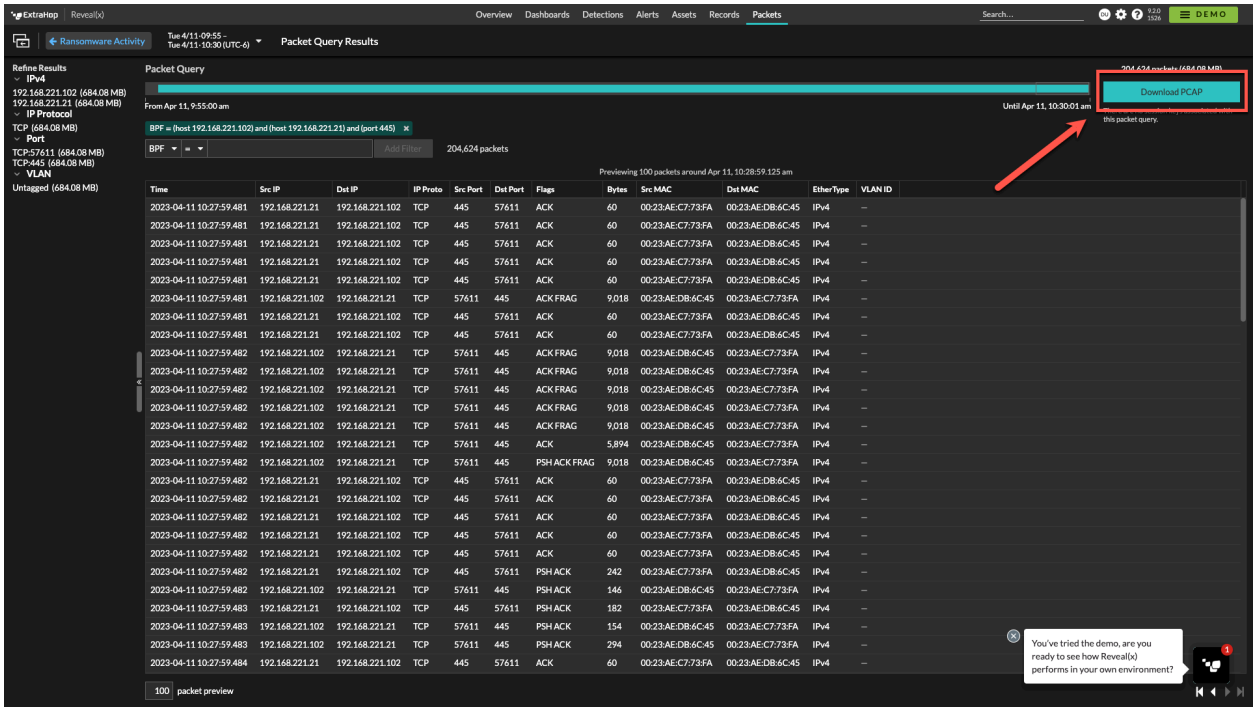
17. Clicking on the magnifying glass for the ‘accounting-fileserver-01’ will now show us all metric detail for that server, including all files, methods, timelines and resources accessed.

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

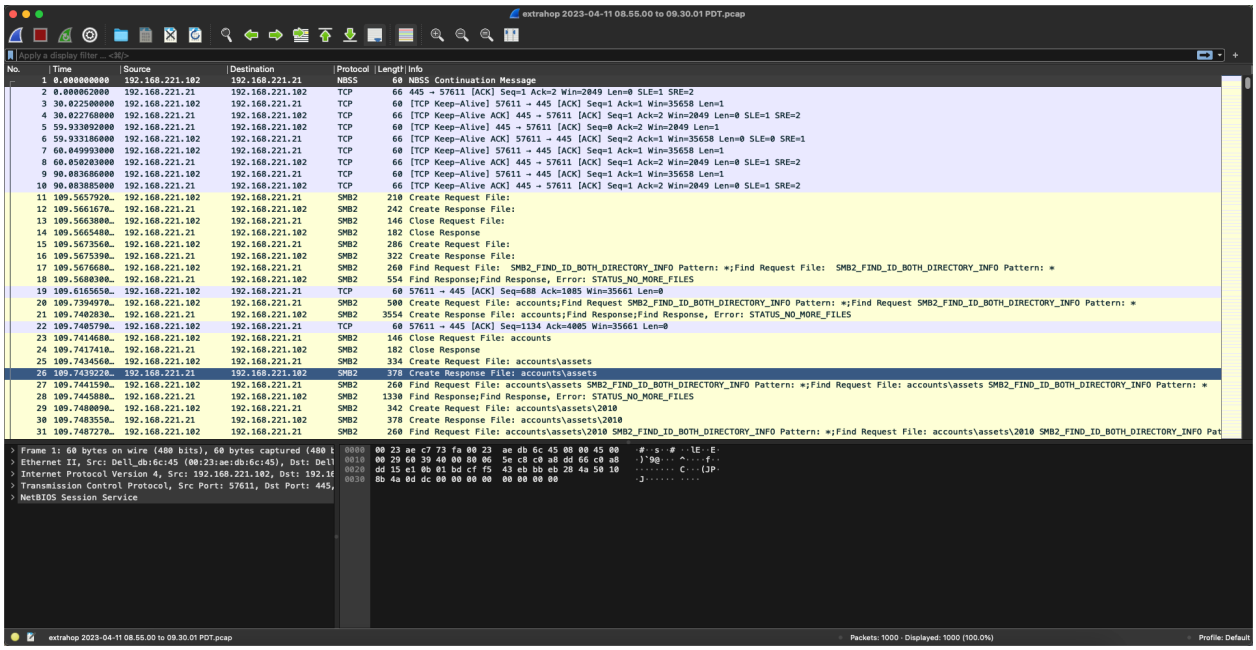


19. Clicking on the bullseye on the left of each record will take us to the packet capture that the platform stored during the breach. See below for details.

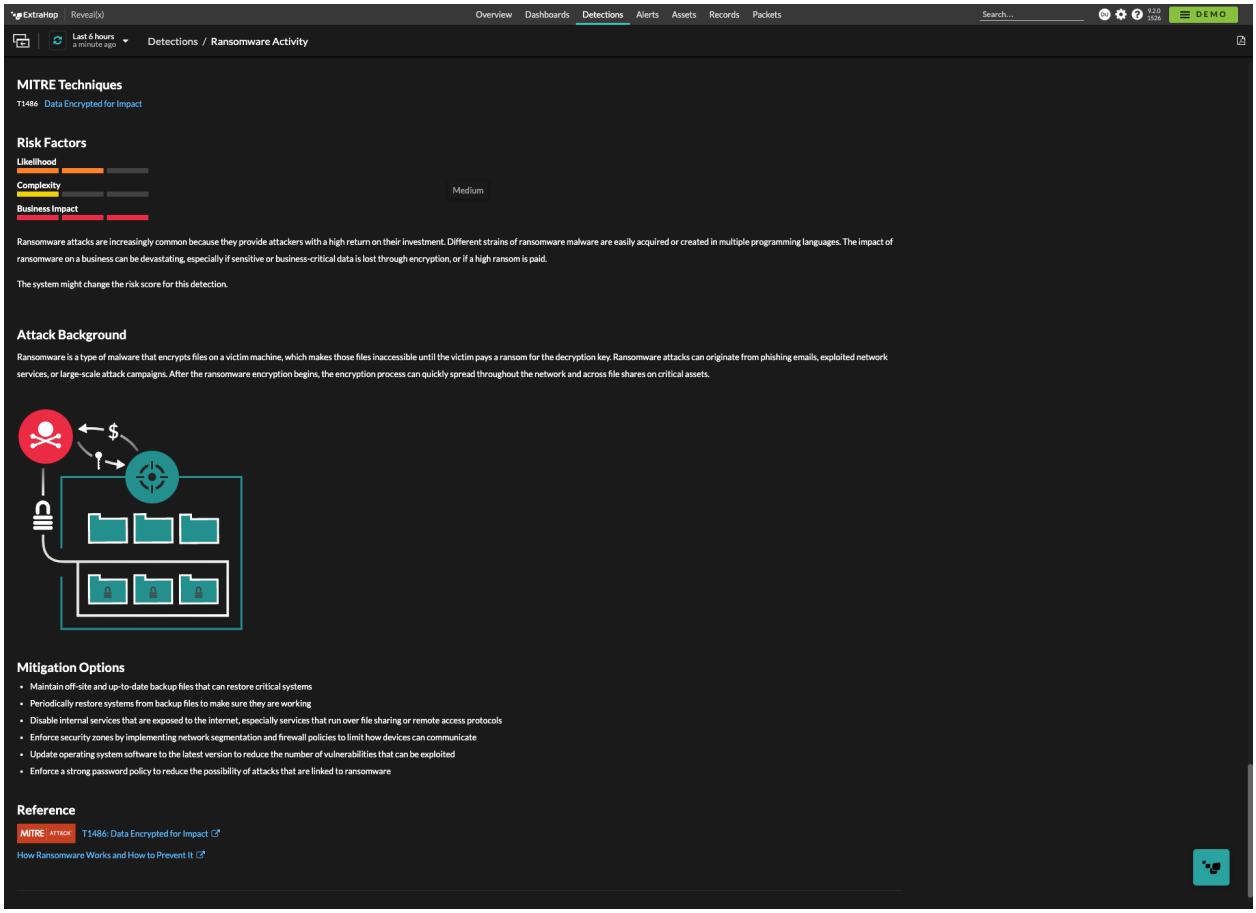
20. Here you can see the full transaction of each record as noted in the previous screen. We've also included the ability to download the PCAP for this specific record.



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.



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.