Key Learnings from “Big Game” Ransomware Campaigns



A mid-year crypto crime update released in July by Chainalysis found that cryptocurrency related crime was trending downward. The exception was ransomware, which the company predicted was on pace for its second-biggest year with the resurgence of “big game” hunting. Now, with ransomware attacks against major casino operations dominating the headlines, and these same hackers also hitting large companies in sectors including in manufacturing, retail, and technology, the report seems eerily prescient.

The approaches for addressing ransomware attacks are very specific to each organization and unique to the circumstance. Victims have handled the attacks differently – from paying the ransom to fighting it. There’s a lot that goes into these decisions which happen behind closed doors.

However, as other organizations who fall into the “big game” category redouble their efforts around ransomware risk mitigation, there’s a lot of readily accessible data about

these campaigns that can help. There are also key steps every organization should take to leverage threat and event data across the lifecycle of a cyber incident. Here are three to consider:

1. Understand the threat. If your board, leadership team, and strategic customers and partners haven't asked what you're doing to address the current surge in ransomware, they will. You need to be able to answer questions about these attacks, if they pertain to the organization, and what you are doing to mitigate risk. This requires understanding data about the ransomware campaign, including the adversary utilizing it, their motivations, and the industries they have been known to actively target. There's no shortage of external data sources to tap into, including commercial, open source, government, industry, existing security vendors – as well as frameworks like MITRE ATT&CK. Not to mention RSS feeds, research blogs, news websites, and GitHub repositories.

You also need an internal understanding of your organization's vulnerabilities and the capabilities you have in place to defend against it. Not only will this help you communicate with key stakeholders, but also allow you to operationalize the data in preparation for an attack. A platform that aggregates and normalizes all this data and enables you to prioritize it using parameters you set based on your risk profile, security infrastructure, and operational environment will help you confidently address questions about the risk and your ability to mitigate.

2. Identify the internal presence of the threat. If you think a ransomware campaign is already in progress, the groundwork you did to understand the threat may help you get ahead of the attack before data is exfiltrated and systems are locked up. By looking at the intersection of the ransomware campaign and your infrastructure, you can focus your efforts on the most applicable adversaries to your business and the tactics they use. For example, there may be artifacts from the adversary

already in your environment, such as a particular IP address, to look for. By correlating that external data with threat and event data from your SIEM or endpoint detection and response (EDR) solution you can quickly zero in on anomalous activity that may indicate the presence of an adversary so you can act with precision and speed.

3. Harden the infrastructure and communicate. Unfortunately, we all know that sophisticated threat actors continually shift tactics and use multiple attack vectors to infiltrate organizations. Once inside, they are also adept at remaining below the radar and establishing persistence, which makes it difficult to detect early and understand the scope of the attack. We have seen this play out in the latest round of ransomware attacks.

Advertisement. Scroll to continue reading.
At later stages in the attack, threat intelligence can help you improve incident response and mitigate risk. Once you do see an indicator of compromise, to learn more about what is going on and the scope of the attack you can pivot to additional external threat intelligence and dig deeper for greater contextual awareness and understanding. For instance, other artifacts associated with this specific ransomware campaign that you can look for in your other tools and other tactics used that you need to be aware of. As you observe what is happening across your environment, correlating internal and external data to get a complete picture of what is going on, you can quickly determine activity that is part of the ransomware campaign and how that campaign is unfolding. With a platform that is integrated with multiple systems across your security infrastructure you can engage your incident response team to mitigate risk and remediate and you can proactively harden your preventative infrastructure.

Coming full circle, you can also communicate with all your key stakeholders to explain what happened, how you addressed it, and give them confidence that the organization is protected

against similar attacks in the future. Undoubtedly there’s more to the story of these ransomware attacks that may never be made public. But there’s also a lot of incredibly valuable data that is available for security practitioners. The keys to successfully utilizing this data to mitigate risk is to focus on a smaller subset of data that is relevant to your organization, dig deeper into that data as soon as you suspect an attack is in progress and operationalize that data so you can take the right actions faster.

https://www.securityweek.com/key-learnings-from-big-game-ransomware-campaigns/