THREAT INSIGHT

ActZero

Emerging Threats

Managing risk in the face of the unknown

Businesses, are under constant pressure to manage risk against cybersecurity threats. Many of these threats pose a low to moderate risk to the business. Some are high-risk or even critical threats. The most dangerous of threats, and one that has been seen increasingly in the first half of 2021, is the 'Emerging Threat'. A prime example of an emerging threat is the recent Kaseya attack — a supply chain ransomware attack by leveraging a vulnerability in Kaseya's VSA software against multiple managed service providers (MSP), and their customers. And there are many more, like the HAFNIUM Exchange attack, and SolarWinds.

Check out this article on more emerging threats to watch out for in 2021.

Characteristics of an Emerging Threat

While there is no specific checklist for classifying an emerging threat, these do generally share one or more of the following criteria:

- Widespread news coverage of the vulnerability or exploit. However, not all emerging threats are news headlines. Often accompanied by urgent warnings from the operating system, hardware, or software vendor.
- Novel critical risk vulnerability - Indicators of Attack (IOAs), Indicators of Compromise (IOC), or patches may not yet be known or available
- Vulnerability is currently being exploited, or there exist clear, publicized steps for doing so
- Older vulnerabilities are being targeted by new ransomware

> "SMBs don't have it easy today. On top of the challenges created by the pandemic, the high profile cyberattacks on airlines, Colonial Pipeline and even NATO show that every organization is vulnerable,"
>
> Trevor Gruenewald
> CEO of ECI Software Solutions.

Declaring the 'Emerging Threat'

ActZero has a dedicated process for handling emerging threats. We first stand up a 'Tiger Team'. This team is made up of representatives from many departments across the company including, but not limited to the Security Operations Centre, Data Science and Security Engineering, Product Management, Customer Experience and Marketing. Each team member plays a critical role in ensuring that we investigate, contain, manage and communicate all information as quickly and with the greatest amount of transparency to not only internal stakeholders, but to our customers and partners.

Tackling Emerging Threats

When an emerging threat is declared, our Tiger Team begins a series of actions in response:

Communications

News of an emerging threat comes in many forms. Sometimes its widespread news coverage of a vulnerability or exploit, or maybe it's discovered in cybersecurity channels. Either way, it's critical that businesses be informed as quickly as possible. At ActZero, the moment we become aware of a threat through our sources (darkweb monitoring, threat intelligence, general monitoring, etc.), we quickly pass on this information to our customer with information regarding our own findings, and recommendations from the affected vendor. Communications continue if and when further updates occur. Targeted communications will occur to affected/at risk customers in the event of positive detections.

Threat Hunting

Upon discovery, our Tiger Team immediately initiates targeted threat hunts to identify the breadth of the threat, risks to our customers, and active indicators of compromise and/or attack. This will enumerate all IOAs and IOCs published, and check for any sign of attack activity in their environment. These scans stay running until the threat has subsided.

If or when attack evidence is found, customers are notified with details of associated attack, the attack evidence, and action plan. This may include immediate action by ActZero, combined with immediate or secondary remediation guidance to the customer.

The Efficacy Review

Next, we evaluate our protection and detection technologies, determining what, if any need to be modified to more proactively handle similar threats in the future. This is a critical stage in advancement of any MDR. Constant tuning of your detections and machine learning models is needed to keep up with, or stay ahead of cybersecurity risk.

Establishing Protection

It is never possible to say that any set of vendors will defend against the next incarnation of these well-funded threats. To claim so is disingenuous. However, a vendor should be able to detect and stop most of the attack techniques - which we were able to do with both HAFNIUM and SolarGate

At ActZero, we're constantly improving our capabilities to help detect, stop, and communicate emerging risks quicker each time — helping us Cover More Ground in protecting our customers.