aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

ACCELERATE RANSOMWARE DETECTION AND RESPONSE

With Aruba IntroSpect

WHAT ARE THE CHANCES?

While no organization expects it, every organization can be a victim of ransomware and the results can be catastrophic. Attacks are on the rise and from a big picture perspective, Cybersecurity Ventures predicts global ransomware damage costs to be $20 billion by 2021 which equates to ransomware attacking a business every 11 seconds.[1]

Today, cyber criminals are increasingly incentivized due to the size of ransomware payments and even if they don't get a direct payment, they are emboldened that at some level their attack was successful by news of the massive remediation costs of those that don't pay a ransom. Whether or not a ransom payment is made, losses can be widespread which could include impact on revenue, other finances, data, operations, reputation, trust and the organization's entire ecosystem.

PREVENTING THREATS AT THE PERIMETER

Perimeter-based security defenses like firewalls and anti-virus solutions that keep bad things out are no longer sufficient. Advanced threats such as polymorphic trojan dropping malware and rapid acting ransomware that bypass the perimeter can bring an entire network and organization to a standstill simply beginning with just one errant click by a single user.

Prevention remains the first line of defense. There are the tried and true cyber security hygiene best practices such as training employees, keeping endpoint software updated, and religiously backing up data. Becoming a harder target for ransomware attacks can also be done by implementing safeguards at the network level using dynamic segmentation and applying a zero trust or least privilege philosophy with strong access controls.

Yet, prevention is not enough as some ransomware attempts are successful and invade the infrastructure. In the July 2019 Ponemon and IBM Cost of a Data Breach report, the average time to identify and contain a breach was 279 days and the longer the lifecycle of the breach, the more expensive it was.[2] When this happens, the critical determining factor is the ability to rapidly detect a threat and respond as early as possible – before any real damage is done.

WHAT IS RANSOMWARE?

Ransomware is a type of malware threat actors use to infect computers and encrypt computer files until a ransom is paid… After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible computers. If the threat actor's ransom demands are not met (i.e., if the victim does not pay the ransom), the files or encrypted data will usually remain encrypted and unavailable to the victim. Even after a ransom has been paid to unlock encrypted files, threat actors will sometimes demand additional payments, delete a victim's data, refuse to decrypt the data, or decline to provide a working decryption key to restore the victim's access.[3] *Department of Homeland Security.*

ADDRESSING THREATS ON THE INSIDE

Aruba IntroSpect is a threat detection and response platform specifically designed to defend against stealthy threats inside the network using continuous monitoring and integrated AI-based network, behavioral and threat analytics.

Specifically for ransomware, the Aruba Threat Labs team researched over 85 ransomware families and their variants to understand their behavior. Supervised machine learning models were then built to detect ransomware-type encryption activities with greater accuracy to speed detection, investigation and response.

VISIBILITY AND DETECTION

Malware moves through an attack sequence and performs certain activities on a device and over the network to carry out its nefarious goals. Malware can be detected at any point in the attack kill chain of infection, command and control, lateral spread and execution – yet to limit damage, it's important to detect the presence of malware early.

Here are a few examples of how IntroSpect speeds the detection of ransomware.

- **Behavioral analytics.** Continuous monitoring and analysis provides visibility into what is happening on the network and alerts on suspicious activity indicating a threat. For example, when a host is accessing an abnormal number of unique internal IP addresses, this can indicate an attacker is moving laterally to reach high value data or servers.
- **Network analytics.** When a host begins beaconing out to a known or rare C2 domain at regular intervals in a low and slow type attack, IntroSpect detects and alerts on this type of activity in real time.
- **Threat analytics.** If a host accesses a Server Message Block (SMB) network share then begins a large number of read – write – rename – delete actions indicative of bulk encryption, IntroSpect delivers high priority alerts that this is an active ransomware attack that needs immediate attention.

INVESTIGATION AND RESPONSE

Once malware is detected, security teams must be able to quickly prioritize, investigate and respond. IntroSpect leverages AI-based analytics to deliver high fidelity, actionable alerts. Incidents are prioritized through a single risk score that represents overall risk. Security analysts have access to robust forensics and a threat hunting platform to accelerate decision making and actions.

Incident response is initiated through analysts, playbooks, SIEMs, and syslog alerts to various network and security solutions. Additionally, Aruba ClearPass Policy Manager allows IT and security teams to automatically quarantine, re-authenticate or blacklist users and devices in real time based upon policies.

POST-INCIDENT INVESTIGATION

Best practices include a post incident investigation to ensure the threat is eradicated and to understand the root cause of the incident to bolster future defenses. Yet many skip this step and get back to business as usual. It's important to consider the following:

- At times, a ransomware attack is a diversion to hide something bigger.
- Knowing the techniques, tactics and procedures of how the attack happened in the first place will help to prevent future attacks.
- Understanding if there was a breach or unauthorized access to data or systems that needs to be addressed.
- Determining if the attack is thoroughly cleaned up and there's no lingering infiltration, malware or access.

IntroSpect makes this post incident investigation easier through the forensics and threat hunting features built into the platform. Security teams gain granular contextual data, intelligence and insights all the way down to the packet level.

FINAL CONSIDERATIONS

As the overall cyber threat landscape gets increasingly dangerous, it's important to keep threats out using perimeter security and to defend from the inside to stop threats that at times evade those perimeter solutions.

Aruba IntroSpect is an award-winning platform that delivers comprehensive visibility across IT, network and security infrastructures to close security gaps. The advanced threat detection is driven by AI-powered security analytics to detect malicious, negligent or compromised users, IoT and systems. And security teams are more efficient and effective with high fidelity threat prioritization and accelerated incident investigation and response.

What does your organization have to lose?

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2] https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[3] https://www.us-cert.gov/ncas/tips/ST19-001

aruba
a Hewlett Packard Enterprise company

SO_RansomwarewithArubaIntroSpect_SK_081419 a00081683enw