Manufacturer Stops Zero-Day Ransomware Attack

ARIA ADR automatically contains in-progress attack while protecting against future polymorphic attacks and preventing critical data loss

SUMMARY – While under a ransomware cyberattack, a manufacturer deployed the ARIA Automated Detection and Response (ADR) solution as part of a managed service. Upon activation, ARIA ADR immediately protected all network devices from attack by dynamically writing policies at the firewall, the VPN, and the ARIA ADR inline device monitoring the network backbone. These automated, proactive measures stopped the in-progress attacks, prevented data loss, and denied further network entry.

SITUATION/CHALLENGES – This privately held Fortune 1000 manufacturer builds complex parts used in automobiles and works in conjunction with other affiliates and partners. These organizations have access via the manufacturer's VPN to pull and update MRP information, and other contractors use it to perform various tasks to managed systems. In light of this, one of the affiliates alerted the organization that they were the victim of a sophisticated ransomware attack. Another sign of the attack was that an employee's files stored on a SharePoint drive had disappeared.

Now on high alert, the executive team brought in a cyber forensic consultant to help find out what damage had occurred. They also contacted ARIA Cybersecurity and quickly deployed the ARIA ADR solution to determine if the attack was ongoing. Right away, ARIA ADR spotted unusual VPN activity and abnormal external communication on SAP servers and blocked both items. Unfortunately, the bad actors recognized the containment efforts and responded by triggering ransomware – active on remote laptops running the Sentinel1 EDR. Given that this ransomware, like most these days, was polymorphic meaning it changes with each deployment, an EDR is typically ineffective at finding the attack. Sentinel1 was no exception in this case, the bad actors were successful in encrypting the laptops. This attack illustrates a common methodology used by sophisticated attackers: Penetrate an organization and then laterally spread to as many devices as possible while looking for critical data of value that can be stolen, and then get paid on the way out by the victim by encrypting devices.

The attackers identified themselves as the DarkSide and demanded a $1M ransom. At the consultant's advice, the manufacturer elected not to pay the ransom. Reason being the customers affiliate, whom the DarkSide also attacked, paid the ransom, only to realize their data was posted on the Dark Web and their systems continued to come under attack.

Instead, the customer went through the highly disruptive process of taking their servers offline to reinstall the OS and applications using backup data. Upon server restart, it became immediately apparent, thanks to the presence of ARIA ADR, that the attackers had been inside the network for quite some time, and the backups were infected. At some point, the DarkSide hackers had planted polymorphic malware agents that "call out" to random command and control (CnC) sites hoping to allow reconnection by the intruders. The manufacturer's servers did exactly this upon restart, issuing attempted calls out through open ports on the firewall to never seen before DarkSide CnC sites. Unlike other tools, ARIA ADR can identify zero-day attacks by these abnormal communication attempts, and it immediately blocked the outbound threat traffic – via its inline appliance. ARIA ADR then via API updated the firewall policies to stop future communication from any device to and from these external sites. Thus, protecting the servers from intrusion and further attack until older back-ups could be retrieved and activated. ARIA's own EDR is now being rolled out to help prevent ransomware from executing on the laptops. ARIA EDR detects the intruders earlier and does more to contain the malware files before they execute.

ARIA ADR now protects this customer from the recurrence of this experience. It stops future intruders from getting very far if they do get in and can identify their initial attempts to get in - allowing actions to be taken to thwart them long before success.

PRODUCT/SERVICE – Seeking a solution that could quickly stem any further impact and fit into the existing infrastructure, the manufacturer deployed the ARIA ADR solution, along with the optional ADR inline appliance. Since they did not have the resources to support the round-the-clock surveillance required, they selected ARIA Cybersecurity and its MSSP partner CSPi, with a managed detection and response (MDR) service based upon the ARIA ADR solution. Leveraging the MDR service gave them access to CSPI's SOC, staffed with seasoned analysts and 24x365 support.

What makes the ARIA ADR ideal for cyber-attack protection is that it finds and automatically stops all types of attacks, even zero-day polymorphic malware and ransomware, in real-time. It does this first by monitoring of network data from across the organization. It then ingests log output from the Firewalls, DNS, DHCP servers, directories, and wireless controllers. It does the same for Cloud instances and web services like AWS, Azure, and GCP. The solution acts like a next-generation SIEM by also digesting log sources from all devices and applications while also ingesting the network traffic.

Unlike a SIEM, ARIA ADR feeds the ingested logs and network analytics into more than 70 behavioral-based threat models to find all forms of today's attacks. ARIA ADR follows the MITRE ATT&CK Framework using threat behaviors to identify, verify and isolate the attack. It goes further because it knows how these attack behaviors appear during their lifecycle – such as those used by nation-state back attackers that never follow the same pattern twice. It does this by using built-in AI and ML capabilities to identify attacks by tell-tale behaviors, spotlighting any suspicious activities. All of this work is fully automated reducing the work of a SOC by 95% and speeding up the ability to stop attacks from hours to seconds. Almost no attack can hide or be missed.

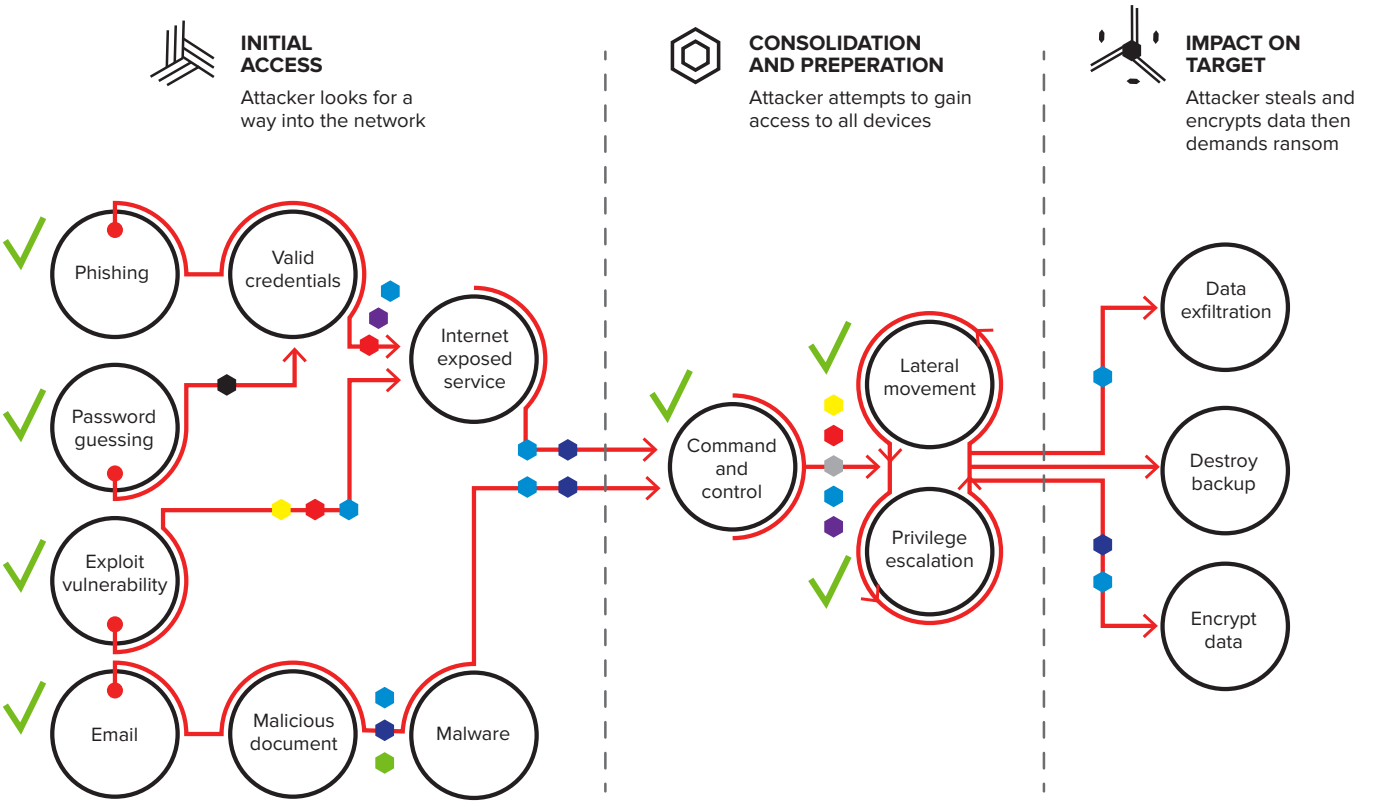
Taking action to stop attacks is critical. For business applications that can't afford processing delays, the inline appliance enables ARIA ADR to look at all the "backbone" network packets – to find and then stop attack conversations while maintaining wire-rate – at speed from 1Gb to 100G. Its fail-to-wire capabilities allow it to be deployed as a bump-in-the-wire. ARIA ADR can also write polices to the firewalls and take out compromised credentials at the directories. If an EDR agent is deployed it can quarantine then remove malware files, as well as allow ADR to take the device offline. Thereby providing a means to stop attacks on any surface.

For critical resources, the remediation actions can be configured to kick in and shut down the attack immediately upon detection – milliseconds matter with such fast-moving attacks.

COMPETITION – The installed Fortinet Firewall and Sentinel1 EDRs proved ineffective at detecting the sophisticated attacker's entry and lateral spread onto protected devices. During the quick evaluation, the manufacturer considered DarkTrace as well as ARIA ADR. DarkTrace was only able to provide a partial solution and deemed too complex to be successfully operated by the existing IT staff. In particular it lacked proper remediation and full detection capabilities to stop the novel, elusive attacks notorious from nation-state backed attackers.

ARIA ADR finds all of these MITRE Framework attack vectors by monitoring behaviors properly as shown in the figure below. The AI automation stops any attack, reacting in milliseconds faster than any human can.

Whereas Sentinel1 missed them all, while Darktrace only claimed to detect half of these:



CONCLUSION / RESULTS – The manufacturer saw immediate results with the ARIA ADR solution. Upon deployment, the DarkSide attackers were denied device access, network entry and were unable to steal data. In subsequent months DarkSide attempted a variety of attacks, and ARIA ADR detected and stopped them, demonstrating the installed preventative measures continued to work.

The manufacturer also experiences brute force attack attempts against VPN and Outlook365 credentials, and ARIA ADR monitors these attacks to detect and stop any successful access attempt. If there is penetration, the ARIA ADR solution will recognize the behaviors and disable those credentials immediately at the directory level. Between the MDR service and the benefits of ARIA ADR, the manufacturer is assured that no matter how attacks morph and change, they will be stopped.

Contact Us to Schedule a Technical Demonstration or Arrange an Evaluation ✉ ARIAsales@ariacybersecurity.com

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110

Follow Us: Linkedin • Facebook • Twitter • Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS