CORE SECURITY

Executive Report

Stopping an Infection from Becoming a Breach

Today's advanced threats are persistent, trying various different evasion techniques to remain hidden. Core Security Network Insight provides enterprises with the ability to

- Rapidly discover these active threats and pivot on the findings to remove the adversary's control over the infected devices
- Prioritize the remediation of the infected endpoints that pose the highest risk to the business

This report will illustrate how Core Security Network Insight rapidly discovered LazyAlienBikers (a threat previously unclassified by the security community, now known to be associated with the MEvade malware) for Fortune 500 companies.

Advanced Threats

At the time of the discovery, LazyAlienBikers (Unclassified) had no widespread recognition within the security industry, despite being present in several Core Security Network Insight customers. In most cases and deployments, newly discovered LazyAlienBikers infections were fairly dormant and had no data exfiltration with minimal C&C activity. However, in some Fortune 500 company deployments, the threat exhibited evasive behavior in order to exfiltrate megabytes of information from multiple endpoints.

LazyAlienBikers' data exfiltration techniques successfully

- Used SSH over HTTP ports in order to bypass firewall blocking of non-HTTP traffic
- Tunneled through Web Security Gateways on port 443
- Used a custom compile of the PuTTY client to provide encryption and look more legitimate to the naked eye
- Exfiltrated megabytes a day from selected endpoints while other infections remained dormant

Morphing Malware

Evidence further indicates that the infected systems first attempted other failed direct exfiltration paths before moving to the successful evasion techniques of SSH over HTTP. Immediately upon discovery of the malicious activity by Core Security Network Insight, incident response teams examined the infected endpoints. Investigations revealed that while SSH was used, there was no legitimate SSH client installed on any of the infected systems. Despite host-based analysis tools struggling to pinpoint the hidden malware, the security teams found the intuitive collection of overwhelming case evidence provided by Core Security Network Insight enabled simple and quick validation of the infections.

Targeted Remediation

Security teams, relying on the case evidence demonstrated by the Core Security Network Insight console, were able to rapidly respond to the incidents. Following best practice, Core Security customers performed the following actions

- Removed the endpoints indicated by Core Security Network Insight with a high Risk Score
- Added the malicious destination addresses of the observed communications to their inline prevention solutions
- Firewall Block List
- Web Gateway's Custom Block Category List
- DNS Blackhole Servers
- Established a response plan for dealing with any future detections of the threat

These actions resulted in a dramatic drop of successful communications from infected endpoints, protecting the organizations while they were able to successfully eradicate the threat completely from their network.

While numerous endpoints at multiple companies were infected with LazyAlienBikers; Core Security Network Insight's rapid discovery of the infections and security and risk teams' best practice incident response efforts quickly minimized business risk of the infections.

Conclusion

Core Security Network Insight provides organizations with automated discovery of hidden threats, enabling security teams to:

- Perform quick validation with full case evidence collected by Core Security Network Insight
- Prioritize remediation efforts to the highest risk devices through Core Security's Risk Score
- Block active infections while working through the incident response workflow
- Adapt their security posture to prevent adversaries from successful attacks in the future

ABOUT CORE SECURITY

Core Security provides market-leading, threat-aware, identity, access and vulnerability management solutions that provide actionable intelligence and context needed to manage security risks across the enterprise. Solutions include multi-factor authentication, provisioning, Identity Governance and Administration (IGA), Identity and Access Intelligence (IAI), and Vulnerability Management (VM). The combination of these solutions provides context and shared intelligence through analytics, giving customers a more comprehensive view of their security posture so they can make better security remediation decisions and maintain compliance.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

CORE SECURITY