esentire®

INCIDENT REPORT

An Adversary on the Network

A cyber-attack doesn't have to be sophisticated to be successful.

Today's attackers continue to utilize tools and methods designed to bypass traditional security controls. While technology is a necessary component to prevention, it must be combined with advanced analytics and skilled analysis by human hunters who look for common attack vectors and signals in the noise to detect and respond to threats in real-time.

For one of eSentire's clients, technology wasn't enough to stop a targeted threat actor from infiltrating its network. With the help of eSentire Managed Detection and Response™ and a team of dedicated security analysts and experts, one eSentire client narrowly avoided an adversary attack.

Here's the full report.

11:00 AM At approximately 11 AM, the eSentire Security Operations Center (SOC) was notified of unauthorized activity on the client's network. A brief investigation by SOC revealed at least one compromised workstation. Their analysis revealed that PsExec was used to deploy malware and credential stealing tools to the workstation. The host was isolated and the client was notified of the intrusion.

The incident was immediately escalated to Threat Intelligence (TI) analysts. Using esENDPOINT™, analysts traced the PsExec connection back to another compromised endpoint. This endpoint was being used a staging point to conduct reconnaissance and launch attacks inside the network. By collecting and analyzing artifacts, analysts were able to scope the breach through ad hoc hunting in esENDPOINT. Indicators were fed back into detection controls to ensure new infections were automatically flagged.

Working backwards from the point of detection, a follow-up investigation revealed that once inside, the adversary had leveraged privileged credentials to access critical systems such as domain controllers using Remote Desktop Protocol (RDP). The adversary dropped custom malware signed with a stolen certificate/signing key as they moved from system to system. Scouring the network for the workstation belonging to their target, the adversary deployed various tactics in their reconnaissance efforts, many of which were tracked by esENDPOINT. This allowed analysts to piece together the adversary's intentions. Once the target's workstation was located, the adversary used PsExec to deploy malware, and used PowerShell to load Mimikatz into memory to extract credentials. This activity was detected with a combination of detection methods, including advanced machine learning algorithms.

6:00 PM By 6 PM, 75% of compromised accounts and systems had been identified and contained. By 10 PM, nearly all compromised systems had been discovered.

12 HOURS Within the first 12 hours, TI flagged a potential modification in an OWA script using esENDPOINT. This information was relayed to the client who confirmed additional malicious code was added to the script to siphon off user credentials as they accessed their mailbox through OWA. Analysts then used esNETWORK™ to identify exfiltrated Outlook accounts by analyzing the relevant network traffic and provided a list of compromised accounts to the client.

24 HOURS Within 24 hours, based on analysis of the adversary's activity on the client's network, TI concluded that the adversary's primary objective was the Outlook and web browser credentials for a specific employee. TI correlated indicators relating to the adversary's capabilities and attack infrastructure against both proprietary and open data sources. They also scoured publicly available information on the client (including press releases, announcements and news articles) for possible attacker motivations. Their analysis prompted an immediate escalation with the client, who then took actions to restrict access to known entry points into their network.

Additional SOC and TI resources were delegated to ensure incident-related tasks were prioritized and reflective of the newly-assigned incident scope/ severity, and eSentire's incident response (IR) partner was also engaged. TI continued to cycle through identification and containment actions throughout the day. Analysis of attacker tools revealed several previously unknown persistence mechanisms. Using esENDPOINT, TI rapidly located residual infections.

72 HOURS Over the next three days, eSentire continued to coordinate with its IR partner to provide investigation updates and forensic materials. The SOC continued to oversee the incident response and analysts continued to handle ad-hoc requests from the client and IR partner. Using esLOG™, TI determined that the initial intrusion vector was through the VPN using stolen credentials, which may have been compromised in a prior phishing campaign. Multi-Factor Authentication (MFA) could have hindered or mitigated this intrusion vector as the adversary would have had to compromise the user's password as well as their second authentication mechanism. This information was communicated to the client and the IR partner.

In the following days, the IR partner continued its investigation with the support of the eSentire SOC and TI team who also worked with eSentire Advisory Services to further optimize the client's defenses (advising on multi-factor authentication) and move the client to recovery phase.

The eSentire Solution

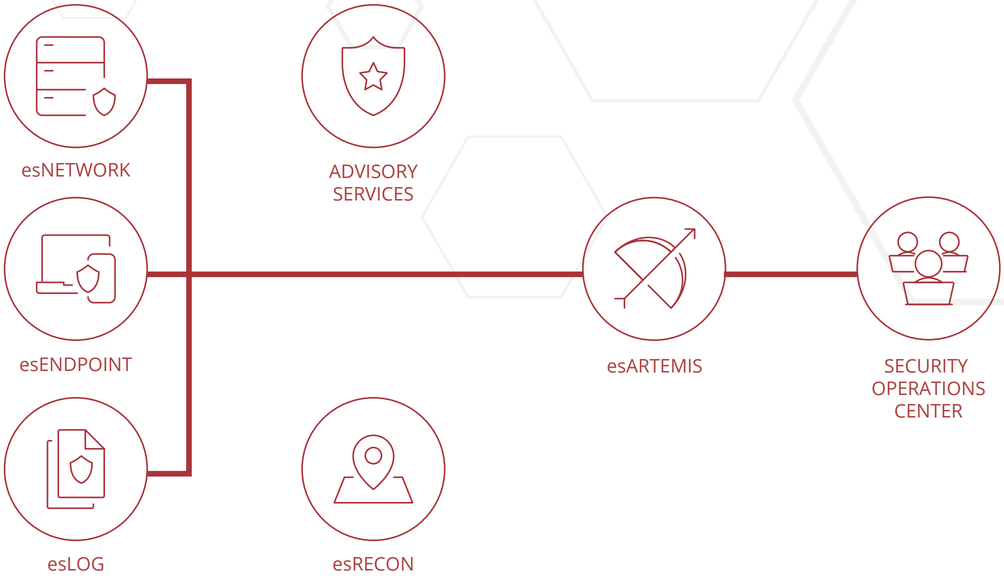
With the help of eSentire Managed Detection Response (MDR), this client was very well-positioned to detect and respond to this highly focused, and new attack on their business.

The client had esENDPOINT deployed not just to user endpoints, but also to their servers and domain controllers. This helped assess quickly the impact and seriousness of the incident. Without esENDPOINT, SOC and TI analysts would not have been able to react as quickly as they did. The adversary moved quickly to gain access to the network in less than a day, and being able to identify and contain the threat was largely due to endpoint visibility.

The client also had esNETWORK and esLOG deployed, which allowed SOC and TI analysts to correlate network activity, VPN authentication logs and endpoint activity with each other. In a breach affecting many machines and user accounts, this was an invaluable source of information.

A Better Approach to Cybersecurity

eSentire Managed Detection and Response (MDR) keeps organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Our 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events.



esENDPOINT

- Allows analysts to conduct scope analysis in minutes
- Enables SOC to monitor for new IOCs via watchlists
- Enhances visibility into adversary's actions

esNETWORK

- Alerts on network reconnaissance
- Identifies extraction compromised information
- Blocks malicious Command & Control (C2) communication

esLOG

- Helps identify unauthorized VPN logins
- Searches logs from multiple sites in one place
- Used to store and preserve vital evidence

eSentire Threat Intelligence

- Improves speed of investigations by tracking adversarial tradecraft
- Reduces the chance of a successful breach by proactively preventing future intrusions
- Accelerates collaboration and knowledge extraction among subject matter experts

4 Key Takeaways

Prevention is futile unless paired with detection and response

Adversaries are well funded and determined, and prevention is powerless against new and highly-focused attacks. Denying or limiting adversary success is within your control. This can be achieved through having proper prevention hygiene backed up with a forensics-rich detection and response capability. The ability to rapidly respond to threats detected throughout the attack lifecycle is critical to preventing attacks from being business impacting.

Complete visibility is key

Traditional log management and signature-based approaches would never have succeeded in detecting, much less responding to this attack. This attack utilized stolen credentials and circumvented most of the standard technical controls in place, except for eSentire MDR. Full forensics was critical – across esENDPOINT, esNETWORK, and esLOG.

White-glove service from start to finish

Analysts remained on high alert, even a week later, providing investigative support throughout the detailed analysis and clean-up efforts. eSentire quickly deployed an IR partner and set up appropriate and dedicated communication channels to support every effort of the customer – with no additional cost to the client.

Advanced tradecraft

Best-in-class tools like esENDPOINT provided the visibility needed to navigate the breach. But eSentire goes beyond these tools – to employ advanced techniques that make them even more effective. Without these capabilities and constant tuning, out-of-the-box technology would not have detected this.

Are you at risk?

Contact us to learn about how eSentire Managed Detection and Response™ can help protect your organization from cyber threats.

About eSentire

eSentire® is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business disrupting events. For more information, visit www.eSentire.com and follow @eSentire.

esentire®