CASE STUDY

22 Minutes: Compromise to Containment

eSentire Dispatches Sophisticated Attacker Before Business Disruption

Attack Types:

Malware, Powershell

Industry:

Finance – Asset Management

Whether for monetary gain or to disrupt business operations, cybercriminals have made financial organizations a top target. A cyberattack can compromise systems that drive operations and expose their clients' personal financial data. This can result in millions of dollars in fines and lost revenue, as well as an incalculable amount of damage to a financial firm's reputation.

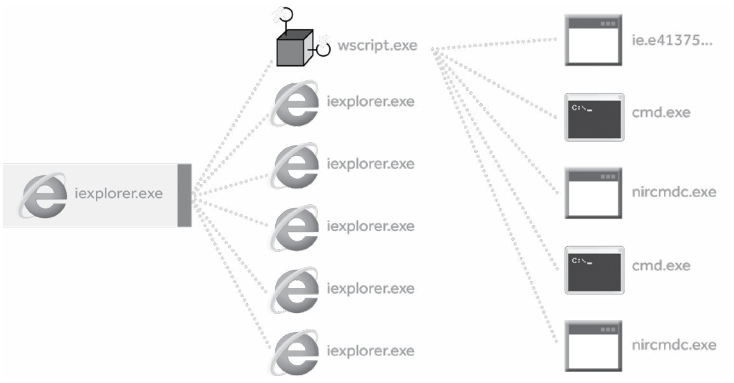
While most financial organizations recognize this and have strong preventative security controls in place, clever social engineering and one wrong click by an employee can open the door to a company's network. For one eSentire financial client, this is exactly what happened. Fortunately, eSentire's Security Operation Center (SOC) leveraging eSentire MDR for Endpoint and eSentire MDR for Network proprietary machine learning capabilities detected the threat actor presence almost immediately and mitigated the threat in 22 minutes.

> The incident occurred as a result of social engineering and where an employee unknowingly downloaded a malicious file which spread laterally across our environment. eSentire was able to quickly identify the threat through a combination of their machine learning platform and security analysts, who worked with us to quarantine and isolate. Given our business, the potential for financial and reputational impact was significant and this helps easily justify our investment in eSentire's solution to our Board.
>
> - Head of IT Infrastructure,
> UK-headquartered investment management company

Patient Zero

At the onset of the incident, the eSentire SOC received an alert from eSentire MDR for Endpoint that a JavaScript file was being downloaded to a computer on our financial client's network. The SOC team began investigating and, with the help of machine learning and eSentire MDR for Network, they were able to follow the threat actor's activity and quickly contain the threat.

Further investigation showed that, on the client side, Patient Zero had unknowingly downloaded and launched a malicious JavaScript file via Internet Explorer. Our SOC team observed that the network traffic captured at the time of compromise indicated that a potentially malicious web redirect via a website related to the SocGholish cybercrime campaign may have instigated the infection.



Once the malicious JavaScript file executed, it downloaded two other tools, one of which took two screenshots of the infected machine's desktop. The SOC team saw in the network traffic that the screen shots were sent back to the attacker. This is a common "staging" tactic used by attackers to see if their payload is being opened in a sandbox. First the malicious script is executed, followed by the staging tactic test to see whether the environment is a sandbox so they do not expose their malware. Then, if safe, the attacker's next step is to execute the malware.

The second tool downloaded by the initial JavaScript script was a remote control launcher. It was saved to the disk, renamed and then executed. This process triggered a malware alert from the SOC to the client. Once executed, it launched the built-in Windows Remote Access Tool which was recorded establishing a connection to an external channel, which is the likely command-and-control channel that was used for the malicious activity that immediately followed.

Just a few seconds after the remote control session was created via the Remote Assistance tool, some persistent malware was installed on the victim host. From there, lateral movement began.

Lateral movement

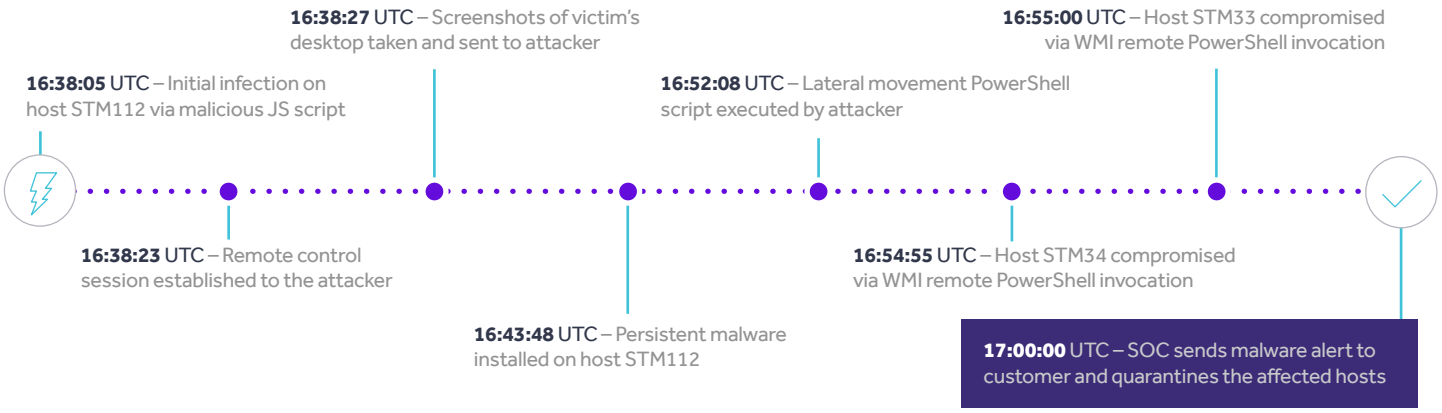
The lateral movement phase began approximately 10 minutes after persistence was established on Patient Zero. An encoded PowerShell command was executed that downloaded an RC4-encrypted second-stage PowerShell script and launched it. As soon as the attacker used a PowerShell command, eSentire's proprietary BlueSteel machine learning tool picked up on the suspicious activity and another alert was generated.

The command was executed under Patient Zero's normal user account, without local admin privileges. After downloading and decrypting the second-stage PowerShell script, the attacker performed a scan of the local network for the purpose of infecting additional machines on the network. Two additional hosts on the local were subsequently compromised by remotely executing a similar PowerShell command.

Threat quickly eliminated

The attacker's total dwell time on the network was approximately 22 minutes, with lateral movement beyond Patient Zero occurring 10 minutes after initial compromise. Utilizing a combination of eSentire MDR for Endpoint which detected the malicious JavaScript file, machine learning from BlueSteel that detected the malicious PowerShell command, and eSentire MDR for Network which alerted on the suspicious web redirect, the attacker had no chance to reach their objective. eSentire was able to isolate the three compromised hosts and terminate the attackers command and control channel to the network.

22 Minute Timeline



If you're experiencing a security incident or breach contact us **1-866-579-2200**

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.