eSENTIRE

INCIDENT REPORT:

Proof of Concept Reveals PlugX Trojan Intrusion of 6+ Years

Attack Types:
PlugX Trojan

Industry:
Non-profit research organization

A cyberattack can compromise systems that drive an organization's operations and expose sensitive data. Financial institutions are obvious targets, but opportunistic cybercriminals will target organizations they suspect do not have banking-level security. In this case, a non-profit research organization was unaware a PlugX trojan had invaded its network and had been present for more than six years. Fortunately, eSentire's Security Operation Center (SOC), leveraging MDR for Network and MDR for Endpoint, quickly detected the threat actor's presence during a proof of concept exercise.

Patient Zero

eSentire was conducting a proof of concept (POC) with a potential customer. We installed an eSentire MDR for Network sensor, which immediately triggered an alert in our Security Operations Center (SOC) for a Command and Control check in for a PlugX trojan. Based on this, eSentire received permission from the customer to install an endpoint sensor on the machine that triggered the alert of a PlugX trojan, a remote access tool (RAT) that uses modular plugins. It is a common tool used by multiple threat groups because it is complex and often evades typical security measures.

Investigation revealed that legitimate antivirus (AV) software had been used to install the malicious trojan without being detected by the AV, through a technique called dll hijacking. The trojan had a lot of complexity and encryption, so that it did not appear malicious. It included a "do not execute until 2013" time code, revealing that the machine had been infected for several years. Decrypting this was no easy task.

The trojan initially loads a dll that is a simple launcher. It looks for an encrypted, hidden "stage-one" payload, which then launches a "stage-two" payload, also hidden, encrypted and compressed. When unpacked, it launches the final, malicious dll file containing the trojan. Investigation showed two functionalities for the final payload: periodic screenshots of the infected machine and a keystroke logger. There was no evidence of any screenshots to be found. But, we decrypted a 30mb file of keystroke data with timestamps going back to 2014.

Threat Quickly Eliminated

eSentire isolated the affected machine when we installed the endpoint sensor. It is unknown when the initial infection occurred because there was no sensor on the endpoint to collect telemetry. The malware had a network channel back to the attacker, but we had no way to prove what they saw. Luckily, what we were able to find in the 30mb file was not the company's critical data. The customer had an IT security company monitoring their network and they detected nothing for five-plus years. During the eSentire POC, eSentire detected, isolated, investigated and removed the longstanding threat in less than two weeks.

Summary of Events

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**.