

Mitigating Potential Data Breach through Lateral Movement Hunting



Snapshot

Client Industry: ATM Service Provider

Country: India

Challenge: Detecting a Trojan intrusion that could potentially result in exfiltration of data

Solution: Proactive monitoring using SISA EOT and other advanced tools

Benefits: Threat mitigation and improved security posture

Threat of Sensitive Data Loss

With greater technology adoption and the emergence of cutting-edge technologies, we've also seen a transformation of the cyber threat landscape. Hackers are becoming more sophisticated than ever - finding new techniques to intrude into information systems and steal sensitive data. With the rise of cybercrimes, businesses run a greater risk of being attacked, leading to huge reputational and monetary losses.

One popular type of attack that businesses are exposed to is Malvertising - the process of incorporating a malicious script in the form of a file/software into someone's information systems to extract sensitive data without their permission.

One of SISA's client faced a similar situation where their security systems were intruded by a backdoor Trojan, a type of Malvertising. A Trojan generally operates by attaching itself to a file while the user opens a suspicious attachment or inserts a pen drive with malicious files. It then takes control over the system, by infecting other files, one by one. In the case of SISA's client, the Trojan started exporting data out from the company's environment.

As the name suggests, a Trojan seems harmless at first sight even though it can be potentially dangerous. Antiviruses often fail to detect malicious scripts within Trojans. This requires advanced threat detection tools and solutions.

In this case, the intrusion was detected by SISA's EOT tool, which was monitoring hundreds of systems within the client's premises as part of its mandate. The EOT tool detected that an IP address, which was reputed as a botnet, was communicating with a private IP of the company's internal networks. Investigations revealed that the Trojan entered the system via malicious traffic (from an autorun.inf file) and created three files (movies.exe, videos.exe and SVC hosts.exe) in the system, without the admin's knowledge.

Rigorous Investigation

Post some thorough investigations, SISA's experts discovered that the infected private IP had started communicating and transferring data to another system within the environment. The data exfiltration was happening from this system and its antivirus had failed to detect it.

Below are some of the details that the SISA's threat hunting team detected:

Ingress Point

The hacker used an IP, which is reputed as a botnet to

communicate with the private IP. This was enabled by malicious traffic that entered the system.

Lateral Movement

The intruder did not use the system that he used to intrude for exfiltration of data. Instead, he made the private IP communicate with another system (by lateral movement), inside the network to bring the data out.

Egress Point

After communicating with the infected internal IP, the other private IP mentioned above was found to be exfiltration the data out from the client's premises.

After identifying the threat and its lateral movement, SISA gave the client an immediate high alert notification, sharing the list of IPs that were communicating with the botnet and detailing how the threat engrossed their environment. In addition, SISA provided the client with a mitigation report to get rid of the adversary. SISA also helped the client achieve this by isolating the infected systems and completely clearing the malicious scripts that persistently regenerated even after deleting.

This was absolutely a potential data breach; but SISA's threat hunting team's expertise in proactive detection and response helped the client come out of danger before it lost any sensitive data.

Timely Detection and Improved Security Posture

Threat hunting is a complex as well as a challenging procedure, where expertise and usage of the right tools play a critical role. SISA's threat hunting team consists of dedicated security analysts that perform log monitoring and threat hunting around the clock, with advanced threat detection tools.

SISA's robust threat hunting team has evolved based on expertise gained through years of investigating breaches. The team has immense expertise in proactively hunting and responding to breaches 24x7.

This approach paid off in the case of the client, since timely threat detection and early mitigation helped save the entity from a potential breach.

By engaging SISA, the client organisation was able to benefit from the most advanced threat detection tools and practices, thereby improving its security posture considerably.

Reach us at sales@sisainfosec.com