Evolving Trickbot Adds Detection Evasion and Screen-Locking Features

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/evolving-trickbot-adds-detection-evasion-and-screen-locking-features

The malware known as Trickbot started off as a banking trojan that used phishing techniques – primarily malicious spam – to trick users into visiting copycat websites to steal their credentials. Its authors continue to develop the already-troublesome malware by adding features designed to make it more difficult to counter.

Security researchers discovered a new module called spreader_x86.dll that contains two files, SsExecutor_x86.exe and screenLocker_x86.dll that form part of Trickbot’s new arsenal. The first file, SsExecutor_x86.exe increases the malware’s evasion capabilities by attempting to add a link to the trojan's startup path by taking over registry use profiles to maintain persistence. ScreenLocker_x86.dll, on the other hand, gives Trickbot behavior that is similar to ransomware, as it attempts to lock victims' machines.

The module's locking mechanism deploys after the main infection chain runs, which could indicate that it is being used to attack unpatched corporate networks. The new functions could have been added to expand the monetization schemes – corporate networks will often have built-in security that prevents employees from visiting malicious URLs to minimize the impact of these kinds of attacks. On the other hand, ransomware-style attacks could act as a backup strategy, as well as a proven source of revenue for the attackers.

Cybersecurity is like a cat and mouse game between security providers and malware authors. While security vendors constantly update and refine their software with new technology and features, the same can be said about malware. Thus, while traditional security methods have become effective at preventing threats from affecting an organization, there are methods of maximizing security with a proactive incident response strategy. This is especially true for targeted attacks such as the recent Chessmaster campaign, which use a wide array of sophisticated tools and tactics, or with evolving malware such as Trickbot, which can be challenging to mitigate for traditional security methods alone, especially if they add evasion tools that allow them to slip through perimeter based security.

Cryptocurrency miners are examples of elusive malware that are on the rise in 2018. Many of these kinds of malware work in the background, without showing obvious signs that they are already using resources for mining – something that can be problematic for certain traditional security solutions. Employees that use personal laptops or works remotely compounds this issue, as perimeter-based security is even more limited in this scenario. With a proactive incident response strategy, the organization's security personnel can collect and analyze endpoint data, as well as provide intelligence on how to detect similar future attacks.

A successful attack can be devastating to both a company’s finances and reputation, especially when it comes to threats that directly affect customers and shareholders. Once an attack has done its damage to an organization, remediation can often take a large amount of time and resources. This is why it's important to address threats before they can do their damage. Given the sophisticated nature of many modern-day attacks, this often means that traditional security solutions have to be supplemented with a human element – often involving IT personnel and system administrators working with security tools to monitor the network, detect and respond to any threats on the network.

Other proactive incident response strategies that organizations can implement:

- Keeping comprehensive logs of what happens within the network, which will allow IT personnel to track any suspicious activity such as C&C server communication and traffic from malicious URLs
- Once an activity or data is deemed as suspicious, it should automatically be investigated to determine if it is malicious
- Sifting through logs and data can be a challenge, but standardized alerts will help with streamlining the monitoring process

Actively monitoring the network for any potential threats, as well as quickly responding to these threats as they appear, can provide the organization’s security team the threat intelligence that they will need to identify malicious activities that may not be visible to traditional security solutions.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below.   2. Press Ctrl+A to select all.   3. Press Ctrl+C to copy.   4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Managed Detection and Response