What malware to look for if you want to prevent a ransomware attack


intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike

Organizations are never going to stop ransomware attacks by looking for the ransomware.

When it comes to ransomware attacks, threat actors often spend time on an organization's networks for weeks (if not months) before the actual ransomware is launched. While these actors go to great lengths to mask their tracks, there are clues that can unearth the possibility of a ransomware attack before the actual ransomware shows up on an organization's system. In order to do this, however, organizations need to know what to look for before it's too late.

The following is a breakdown of what malware organizations should be on the lookout for in order to thwart a ransomware attack. While the presence of these particular kinds of malware does not automatically mean a ransomware attack is imminent, awareness of their utility will help security teams proactively protect their systems from the crippling, expensive impact of a ransomware incident.

Trojans

One of the most common malware families on the internet, trojans are often used by malicious actors as an initial way to gain access to an organization's network. Often delivered in some form of a phishing attack, trojans present attackers with the ability to siphon data from networks, leave a gateway for further malware delivery, or both.

Over the past decade, trojans were primarily used to siphon banking credentials, as attackers focused on obtaining access to financial accounts. With the rise in ransomware, threat actors have fine-tuned trojans to uncover credentials that can give them unfettered access to an organization's network.

A prime example of how trojans are used to set up ransomware attacks can be seen in the connection between Emotet and Conti. Intel 471 researchers recently discovered that Conti uses Emotet to gain a foothold in organizations' networks, then allows ransomware operators to pick targets from a pool of infected organizations. Conti has made Emotet a key part of their attack chain, specifically since Emotet was re-launched in November 2021.

Other trojans that have been used in recent ransomware attacks include QbotIcedID (aka BokBot), and ZLoader. Intel 471 researchers have noticed that the Conti group appears to have dropped BazarLoader in favor of a new malware called Bumblebee, which follows research from Google stating that Bumblebee has been used by an access broker with ties to Conti. Intel 471 researchers have observed Cobalt Strike, Metasploit, Sliver (an open-source backdoor programmed in Go), and IcedID as Bumblebee payloads.

Information Stealers

While information stealers are close in functionality to trojans, there can be slight differences between the two kinds of malware. Trojans will often steal information that is being entered into a machine (i.e. a keylogger), while information stealers are programmed to steal credentials and other information that is already stored on a machine.

Info stealers can collect all sorts of information, including browser cookies, autofill data, cryptocurrency wallets, File Transfer Protocol (FTP) clients and desktop applications. Threat actors use this information to search for high-level credentials that can allow them to move freely within an organization's network, find further high-value data they want to steal, and locations where they need to deploy ransomware in order to lock an organization's system.

Some ransomware crews have re-formulated info stealers that were used for a variety of crimes in the past, while others have created new ones specifically for their own use. Malware known as "StealBit" is used as an info stealer to support affiliates of LockBit ransomware. Rather than a conventional stealer designed for harvesting data from browsers, StealBit operates as a file grabber, allegedly cloning folders from corporate networks to the LockBit victim shaming blog in almost no time.

Other information stealers that have been used in ransomware attacks are KPOT, Mars, Raccoon, Redline and Vidar.

Penetration testing tools

There is a bevy of tools used by legitimate security professionals that have been co-opted into the attack chain of ransomware operators. While these tools are purchased and licensed by their developers, this software is often copied, cracked, or reversed engineered to serve ransomware gangs' nefarious purposes. These gangs often use these programs to further move throughout a network, and siphon administrative credentials that pave the way for ransomware attacks.

Cobalt Strike is one of these popular tools that has been embraced by ransomware gangs. These gangs and their affiliates use Cobalt Strike as a second-stage payload for many malware campaigns across many malware families. Intel 471 researchers have observed Cobalt Strike being delivered via Hanictor, SystemBC and Trickbot to further facilitate credential harvesting, lateral movement, and ransomware deployment. Additionally, the Conti ransomware group tried to buy a legitimate license for Cobalt Strike through a shell company made to look like a legitimate security enterprise.

Mimikatz, initially created by a security researcher to learn how Microsoft's authentication protocols were vulnerable to attacks, is a very popular tool amongst cybercriminals. Intel 471 researchers have observed several ransomware-as-a-service operations, including ALPHV, AvosLocker, and SunCrypt, use Mimikatz to harvest credentials from privileged network administrators.

Metasploit is similar to Mimikatz in that it's open source, but provides a wide array of add-ons that allow users to perform an extensive amount of tasks. Modules can be placed into Metasploit that allow for similar tasks like those in the malware listed above including keylogging, information stealing and the ability to drop further malware. Intel 471 researchers observed Conti and LockBit 2.0 recruiting developers that had experience deploying or working with Metasploit.

Not a panacea

To be clear: setting up a security strategy that only looks for these types of malware is not sustainable. Vulnerabilities still need to be patched, phishing emails will still be sent, and employees could still be targets of social engineering scams. However, being proactive about this specific malware may force attackers to move on from your organization and find a different target. Ignoring malware prior to a ransomware attack is a recipe for disaster.

May 12, 2022: *This blog has been edited to include that Google has made a connection between the Bumblebee loader and the Conti cybercriminal group.*