Sodinokibi: Ransomware Attackers also Scanning for PoS Software, Leveraging Cobalt Strike

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

Threat Hunter TeamSymantec

Researchers at Symantec, a division of Broadcom (NASDAQ: AVGO), have spotted a Sodinokibi targeted ransomware campaign in which the attackers are also scanning the networks of some victims for credit card or point of sale (PoS) software.

It is not clear if the attackers are targeting this software for encryption or because they want to scrape this information as a way to make even more money from this attack.

The attackers are using the Cobalt Strike commodity malware to deliver the Sodinokibi targeted ransomware to victims. Eight organizations had the Cobalt Strike commodity malware on their systems, with three of the victims subsequently infected with the Sodinokibi ransomware. The victims infected with Sodinokibi were in the services, food, and healthcare

sectors. The companies targeted in this campaign were primarily large, even multinational, companies, which were likely targeted because the attackers believed they would be willing to pay a large ransom to recover access to their systems.

The attackers are aiming to make a lot of money - for victims infected with Sodinokibi the ransom requested is $50,000 in the Monero cryptocurrency if paid within the first three hours, and $100,000 after that.

Tactics, tools, and procedures

The attackers leverage legitimate tools in these attacks, and at one point we observed a legitimate remote admin client tool by NetSupport Ltd being used to install components during these attacks. In April, Symantec threat researchers found evidence of Sodinokibi attackers using similar tactics, when they spotted them using a copy of the AnyDesk remote access tool to deliver malware and other tools in at least two attacks.

The attackers in this campaign also use ‘legitimate’ infrastructure to store their payload and for their command and control (C&C) server. The attackers are using code-hosting service Pastebin to host their payload (the Cobalt Strike malware and Sodinokibi) and are using Amazon’s CloudFront service for their C&C infrastructure, to communicate with victim machines.

Pastebin and CloudFront are both legitimate services but have been observed being exploited by bad actors for similar malicious activity in the past. The advantage for malicious actors of using legitimate services to host payloads and for their C&C infrastructure is that traffic to and from a legitimate service is more likely to blend in with an organization’s legitimate traffic, and so is less likely to be flagged as suspicious and blocked.

Cobalt Strike is an off-the-shelf tool that can be used to load shellcode onto victim machines; it has legitimate uses as a penetration testing tool but is frequently exploited by malicious actors. The tactics used in this series of attacks are similar to tactics seen used in other targeted ransomware attacks before. Microsoft released research in April into attacks by six ransomware gangs, including Sodinokibi, and said that many of the groups employ similar tactics. The vector for most attacks observed by Microsoft was either the exploitation of vulnerable network devices or brute-force attacks on Remote Desktop Protocol (RDP) servers, and initial intrusion was followed by the use of living-off-the-land and commodity tools to perform credential theft and lateral movement before deploying the ransomware payload on multiple computers. So the tactics employed in this attack campaign are tactics commonly used by targeted ransomware gangs.

Once on a network, the attackers take various steps to reduce the chance they will be detected and to increase the chances of their attack working. The attackers attempt to disable any security software on the machine so their activity can’t be detected. They also enable remote desktop connections so they can use them to launch malicious commands.

The attackers also appear to be interested in stealing credentials on victim machines, and are observed adding user accounts, presumably in an attempt to maintain persistence on victim machines and also in a further attempt to keep a low profile on victim networks.

We see the attackers using encoded PowerShell commands in some of these attacks. PowerShell is a Windows command line tool that has many legitimate purposes but is also frequently abused for nefarious purposes by malicious actors using living-off-the-land tactics.

We see the Sodinokibi ransomware deployed on three of the victims that were infected with Cobalt Strike.

Sodinokibi

Sodinokibi is a targeted ransomware - we saw targeted ransomware attacks increase by 62 percent in 2019, and targeted ransomware is one of the biggest threats on the cyber security landscape currently.

Sodinokibi (aka REvil) first appeared in April 2019, but the actors behind it are widely believed to be the same actors who operated the GandCrab ransomware. GandCrab was a highly active targeted ransomware that first appeared in 2018. However, in June 2019 its operators announced that they were 'retiring', claiming that they had made more than $2 billion from the ransomware. However, it's widely thought that they simply turned their focus to the Sodinokibi ransomware instead.

Sodinokibi was originally believed to be operated by one group but it is now thought to operate as a ransomware-as-a-service (RaaS), where one group maintains the code and rents it out to other groups, known as affiliates, who carry out attacks and spread the ransomware. Any profits made are then split between the affiliates and the original gang.

Since it appeared on the scene, Sodinokibi has been one of the most prolific targeted ransomware strains and has been seen in numerous high-profile incidents. Actors using Sodinokibi were apparently responsible for the hack of foreign exchange service Travelex on New Year's Eve. The attack left the company offline for almost a month and caused huge disruption to its business, according to public reports. The attackers were said to have demanded a ransom of $6 million in that incident, with Travelex reportedly eventually paying $2.3 million to regain access to its systems. In January, it was reported that Sodinokibi's average ransom demand was $260,000, so this was a huge ransom.

Sodinokibi hit several other high-profile companies in the last year and, similar to the Maze ransomware group, announced in December 2019 that it would release data stolen from victims if its ransom demands weren't met. Since that announcement, the gang has been observed offering the data of victims for sale on hacking forums, and at the beginning of June an auction site was launched where the group said it will sell off stolen data to the highest bidder.

Victims

The three victims that were infected with Sodinokibi in this campaign were in the services, food, and healthcare sectors. The food and the services companies that were infected were both large, multi-site organizations that were likely capable of paying a large ransom - the type of company that would typically be targeted with Sodinokibi. However, the healthcare organization appears to have been a smaller operation. Interestingly, this victim's systems were also scanned by the attackers for PoS software. It may be that the attackers realized this business might not be in a position to pay the large ransoms usually demanded in a Sodinokibi attack, and so scanned for PoS software to determine if they could profit from the compromise in another way, or they may have been scanning for this kind of software simply to encrypt it too.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.