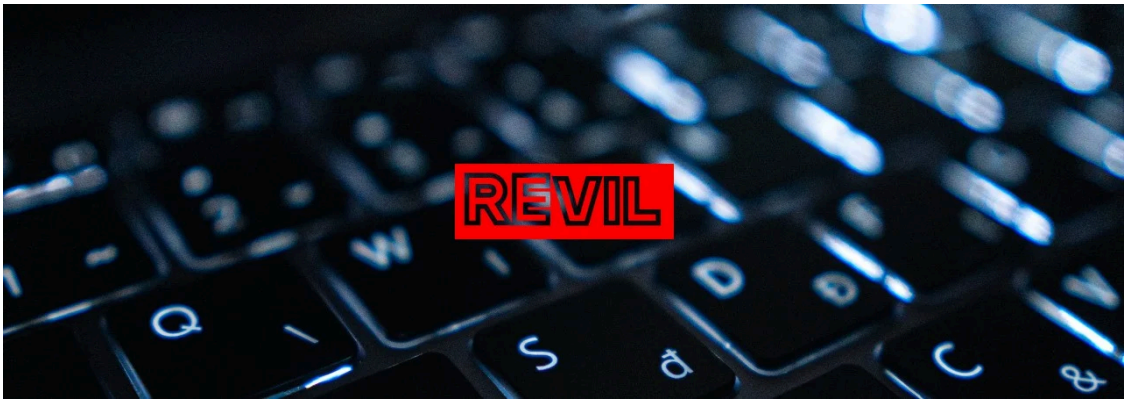
REvil ransomware scans victim's network for Point of Sale systems

By Sergiu Gatlan

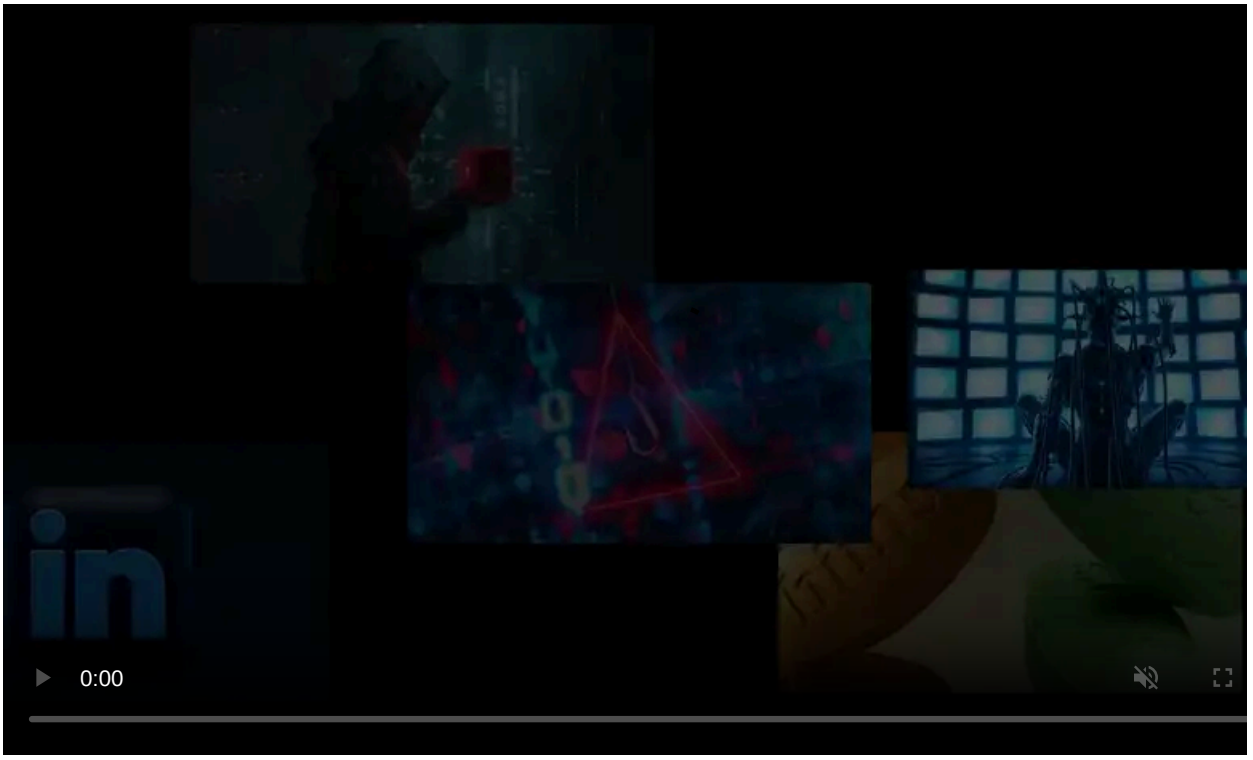
Published: 2020-06-23 · Archived: 2026-04-05 17:24:36 UTC

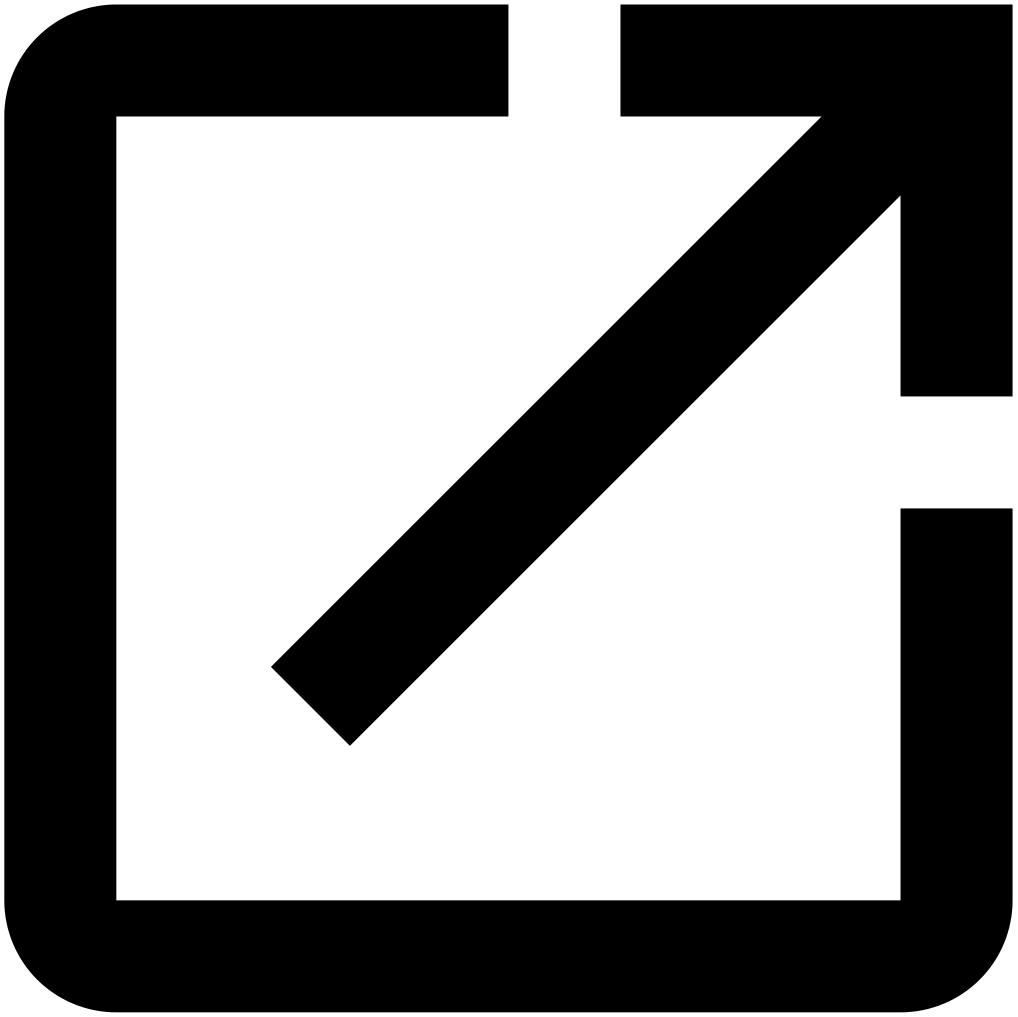


REvil ransomware operators have been observed while scanning one of their victim's network for Point of Sale (PoS) servers by researchers with Symantec's Threat Intelligence team.

REvil (also known as Sodinokibi) is a ransomware-as-a-service (RaaS) operation known for breaching corporate networks using exploits, exposed remote desktop services, spam, as well as hacked Managed Service Providers.

After getting access to a target's network, the operators spread laterally while also stealing data from servers and workstations, later encrypting all the machines on the network after gaining administrative access to a domain controller.


0:00



As part of the campaign observed by Symantec, the REvil affiliates used the off-the-shelf Cobalt Strike penetration testing toolkit to deploy REvil (aka Sodinokibi) ransomware payloads on their targets' networks.

Ransom doubled within three hours

In total, the researchers found Cobalt Strike on the networks of eight firms targeted in this campaign, with the attackers infecting and encrypting three companies from the services, food, and healthcare industry sectors with the REvil ransomware.

"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," Symantec explained.

Each of the victims was asked to pay $50,000 worth of Monero cryptocurrency or $100,000 if a three hours deadline expired.

The REvil actors did their best to evade detection after gaining access to their targets' networks by using infrastructure hosted on legitimate services such as Pastebin (payload storage) and Amazon CloudFront (command and control server).

They also disabled security software to prevent security teams from detecting their attacks and stole credentials later used to add rogue accounts as a simple way to gain persistence on the compromised machines.

Scans for PoS systems

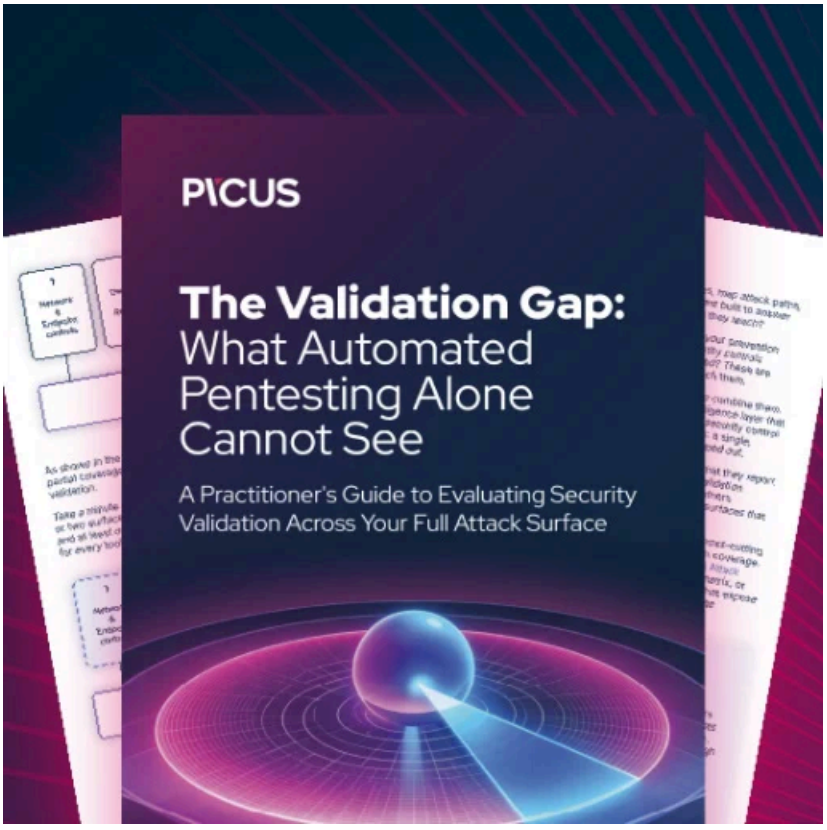
While the services and food companies were the perfect targets as they were large organizations capable of paying a large ransom to have their systems decrypted, the smaller healthcare org was a smaller outfit that couldn't pay the ransom.

In this case, probably prompted by the fact that there was a high possibility that the victim won't be able to pay for their "decryptor," the REvil operators also scanned the healthcare organization's network for PoS systems as part of a credit card data theft attempt or as an additional valuable target worth encrypting.

"While many of the elements of this attack are 'typical' tactics seen in previous attacks using Sodinokibi, the scanning of victim systems for PoS software is interesting, as this is not typically something you see happening alongside targeted ransomware attacks," Symantec concluded.

"It will be interesting to see if this was just opportunistic activity in this campaign, or if it is set to be a new tactic adopted by targeted ransomware gangs."

Earlier this month, REvil ransomware also launched an auction site for selling their victims' stolen data to the highest bidder.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/revil-ransomware-scans-victims-network-for-point-of-sale-systems/