Destructive Sodinokibi ransomware busting unsuspecting MSPs and SMBs

2019 revealed a new ransomware threat targeting businesses worldwide

Sodinokibi is a particularly nasty piece of ransomware that has been out on the prowl for managed service providers (MSPs) and their customers. According to ESET telemetry, this ransomware was first seen near the end of April 2019, with attacks soaring to a peak in June:

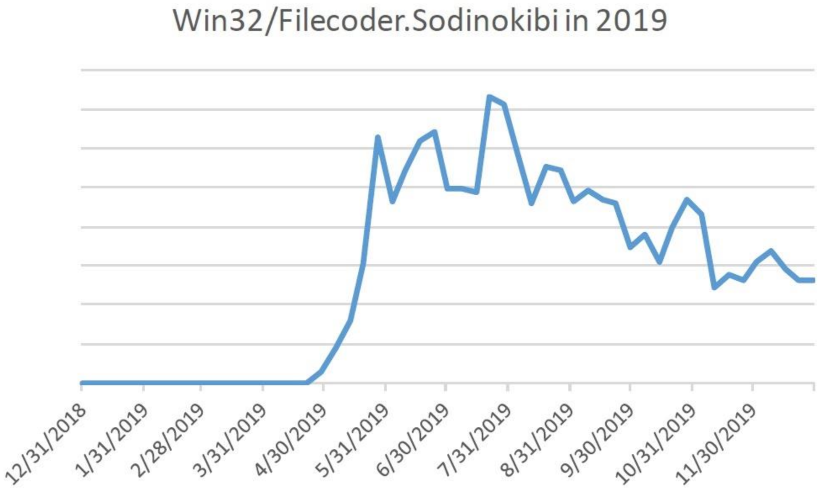

Figure 1: Sodinokibi detection trend

Throughout 2019, Sodinokibi mainly struck users in the United States, while covering a spectrum of targets from around the globe:

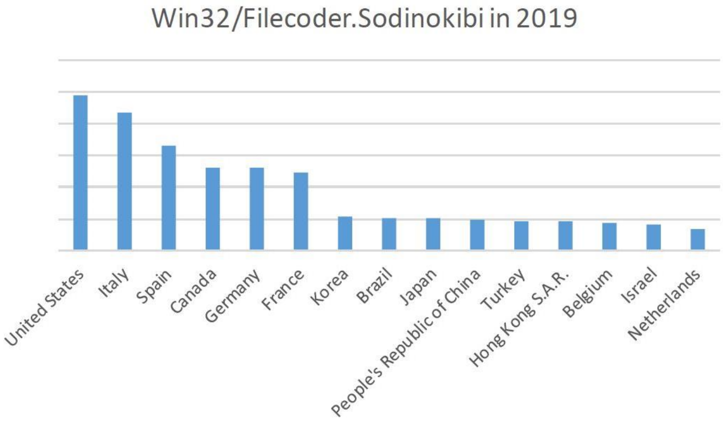

Figure 2: Sodinokibi detections per country

Many headlines in 2019 indicated the same – Sodinokibi ransomware breached the IT systems of a number of US-based MSPs, including LogicalNet, PerCSoft, The Digital Dental Record and TSM Consulting

Services in tandem with many of their customers. Threat actors often target MSPs in order to take advantage of their privileged access to customers' IT systems and spread malware in one fell swoop.

From what ESET researchers have observed, the threat actors behind Sodinokibi seem to prefer using automated tools like exploit kits or spam to distribute their ransomware, instead of more manual techniques like hijacking computers left exposed over remote desktop protocol (RDP).

Spam emails are a common vector for delivering malware to computers. Such emails can contain either a malicious link or an attachment that opens the way for malicious software such as ransomware and spyware to be run on affected computers.

Slightly more sophisticated, an exploit kit consists of an all-in-one malware package hosted on a compromised or malicious website that can scan the devices of website visitors for vulnerabilities. Exploit kits often look for weaknesses in software components such as Adobe Flash Player, Java Runtime Environment, JavaScript or Microsoft Silverlight in order to conduct an attack.

Decrypting Sodinokibi?

In the event of being held ransom by Sodinokibi, decryption is currently not possible without the private encryption keys. This is due to the strong grade of encryption algorithms implemented without any significant flaws by Sodinokibi for encrypting both the files and the encryption keys.

Sodinokibi uses the Salsa20/20 encryption algorithm to encrypt files and the Advanced Encryption Standard (AES) algorithm to produce unique encryption keys for each file. In consequence, having only one private key allows you to decrypt only one file encrypted by Sodinokibi. Furthermore, the private file encryption keys are themselves further encrypted by use of elliptic curve cryptography (ECC).

Prevention is the best option against Sodinokibi

Intelligence gathered by ESET telemetry shows that the devices most under attack by Sodinokibi often have misconfigured or outdated versions of security software.

For businesses, therefore, it is crucial to enforce security best practices throughout their entire IT infrastructure. Using a remote management dashboard, like ESET Security Management Center (ESMC) console, IT administrators can easily and quickly push out security software updates, monitor the execution of suspicious and/or forbidden processes and files, as well as turn up the dial for more vigorous detections via fine tuning of the machine learning, firewall, antispam, and Host-based Intrusion Prevention System (HIPS) modules present in ESET endpoint security products.

In the face of current targeting by Sodinokibi, MSPs and SMBs are behooved to take another look at their ransomware defenses and better understand the factors that lead to a compromise by ransomware. Businesses can follow the list of recommendations detailed here.