Ransomware now combined with data leakage

Threat Memo - TM 20-005 - Date: 15/01/2020 - Version: 1.0

TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime	Ransomware, Data leakage	World	Any	A1

Key Points

- Ransomware extortion cases have started to include (and realise) data leakage threats.
- In a number of cases in December 2019 and January 2020 operators of ransomware released victims' internal data.
- The tactic represents an upscaling of ransomware operations in spite of the technical and logistical requirements.

Summary

Cybercriminals operating ransomware campaigns appear to have adopted a new method to push their victims into paying the demanded amount. They combine the locking up of files with exfiltration and public exposure of the victim organisation data. This is a way to publicise the data breach and push the victim to pay, out of fear of internal files leaking to the world.

Some recent events illustrating this method have been:

- In December 2019 the US cable manufacturer Southwire sued the (unknown) operator of the *Maze* ransomware for allegedly stealing 120GB of data and encrypting 878 devices of the company. Following the rejection of the ransom blackmail the attackers released some of this date on a website they had set up for this purpose.
- According to public sources on January 10, 2020, the operators of the *Sodinokibi* ransomware (also known as *REvil*) published stolen data claimed to be from the HR company Artech Information Systems after ransom was not payed. Links to the about 337MB of victim files where published on a Russian hacker forum. As part of their extortion tactic, the attackers threatened further data exposures if the ransom was not payed.
- On January 13, 2020, the operators of the *Nemty* ransomware went so far as to publicise their plans to create a blog to be used as a repository of data stolen from ransomware victims.
- News reports on December 21, 2019, indicated that the *Zeppelin* ransomware was used in concert with the tool *ConnectWise* that operated an agent and allowed the remote management of the victim system. The *ScreenConnect* client was discovered in the case of a breach of a real estate company and is apparently used to allow attackers to inspect and collect data of interest.

Comments

Threatening to leak sensitive data is an extra lever to force victims into paying ransom. Additionally, publication of internal data also exposes the victim organisations to legal action for customer/personnel data mishandling.

Deploying toolset with extra features to collect and exfiltrate files is a step up in post-intrusion operations for attackers. Furthermore, setting up an infrastructure to disseminate captured files, with all the subsequent operational security for the attacker, represent an additional investment of time and resources.

As a positive consequence however, data exfiltration activities may provide another detection opportunity for the victim, especially utilising tools like Data Leakage Prevention systems (DLPs).

Finally, any victim of the new extortion technique should consider that the attacker may not have actually accessed and exfiltrated all the organisation's documents but just about enough to make a convincing threat.

Some other novel features demonstrated by ransomware lately have been:

- The use of the "wake-on-LAN" BIOS functionality by the *Ryuk* ransomware to activate devices switched off, in order to attack and encrypt them.
- According to security researchers in December 2019, some ransomware is also attacking Network Attached Storage (NAS) devices in home and enterprise environments.

These developments underline a sustained effort by cybercriminal ransomware operators to find new ways to extort victims.