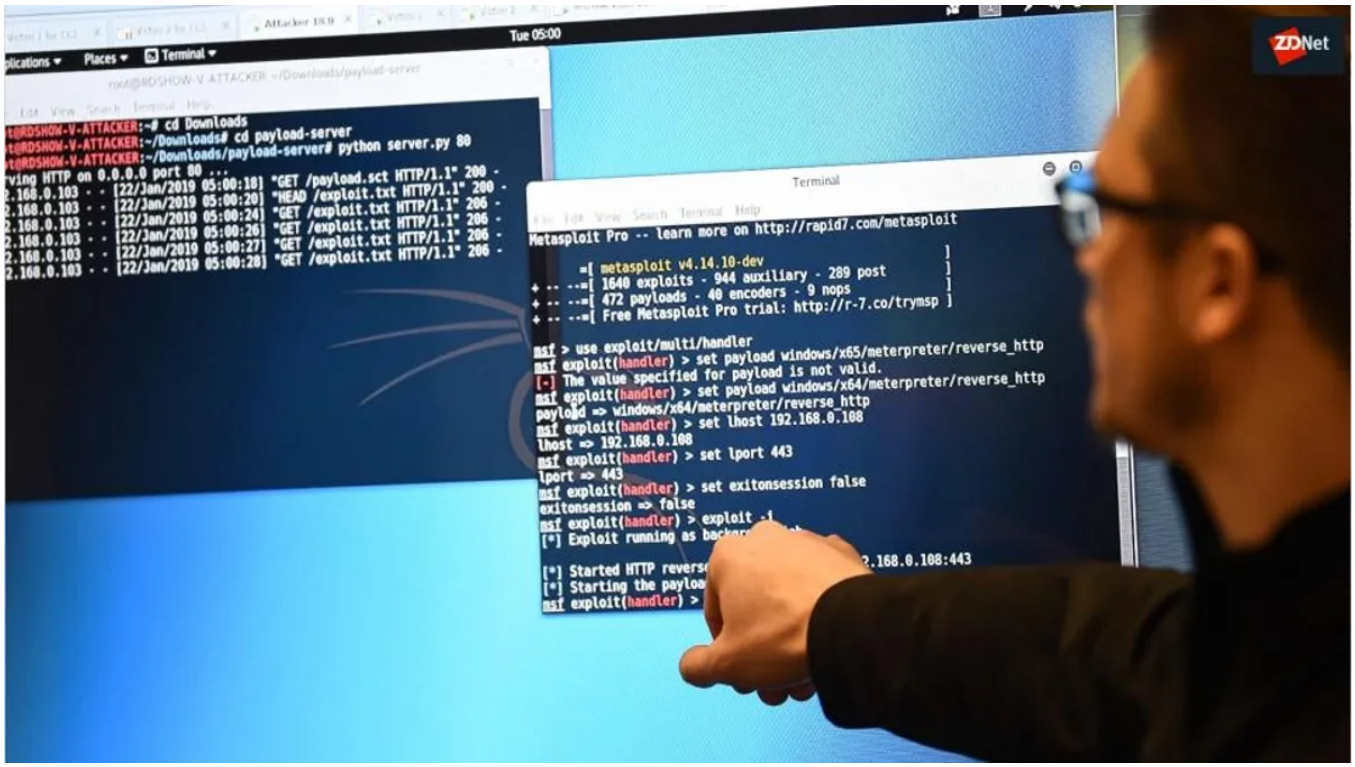
France warns of new ransomware gang targeting local governments

zdnet.com/article/france-warns-of-new-ransomware-gang-targeting-local-governments/



Home Innovation Security

CERT France says some local governments have been infected with a new version of the Pysa (Mespinoza) ransomware.

Written by Catalin Cimpanu, Contributor on March 18, 2020

-
-
-
-
-

Special feature

Special report: A winning strategy for cybersecurity (free PDF)

This ebook, based on the latest ZDNet/TechRepublic special feature, offers a detailed look at how to build risk management policies to protect your critical digital assets.

Read now

France's cyber-security agency issued an alert this week warning about a new ransomware gang that's been recently seen targeting the networks of local government authorities.

The alert, issued by France's CERT team, points to a rising number of attacks carried out with a new version of the Mespinoza ransomware strain, also known as the Pysa ransomware.

This ransomware strain was first spotted making victims last year, in October 2019. According to reports at the time, victims reported having data encrypted with the *.locked* extension added at the end of each ransomed file.

A new Mespinoza version was spotted two months later, in December 2019. This one used the *.pysa* file extension, which explains the second Pysa name under which this ransomware is sometimes referred to.

In previous cases of Mespinoza/Pysa infections, most of the victims were companies, suggesting that the group behind this new ransomware was specifically targeting large corporate networks in an attempt to maximize ransom demands and inherently its profits.

Now, CERT-FR says the Pysa gang has moved to target French organizations, with the agency receiving reports of multiple infections.

Unclear how the Pysa gang is infecting victims

CERT-FR said it is still investigating how the Pysa gang is gaining access to victim's networks. However, forensics clues left behind paint a picture of what could have happened on some of the infected/ransomed networks.

For example, CERT-FR said there was evidence suggesting that the Pysa gang launched brute-force attacks against management consoles and Active Directory accounts.

These brute-force attacks were followed by the exfiltration of a company's accounts & passwords database.

Victim organizations also reported seeing unauthorized RDP connections to their domain controllers, and the deployment of Batch and PowerShell scripts.

Furthermore, the Pysa gang also deployed a version of the PowerShell Empire penetration-testing tool, stopped various antivirus products, and even uninstalled Windows Defender in some instances.

CERT-FR says that in at least one case they analyzed, they also found a new version of the Pysa ransomware, which used the *.newversion* file extension instead of the older *.pysa*.

No encryption weaknesses

Investigators said they also analyzed the ransomware and its encryption algorithms, and they weren't able to find any implementation flaws that could permit victims to bypass the ransom payment and decrypt files for free.

According to CERT-FR, the Pysa ransomware code is "specific and very short" and "based on public Python libraries."

But attacks with Pysa aren't only limited to France. In an interview with *ZDNet* about this new ransomware gang, Emsisoft malware analyst and ID-Ransomware creator Michael Gillespie said the Pysa ransomware gang has also made victims outside France, across multiple continents, hitting both government and business-related networks.

The CERT-FR Mespinoza/Pysa alert is available here.

Latest big-game hunter

Mespinoza/Pysa is the latest ransomware gang that engages in a tactic called "big game hunting" or "human-operated ransomware" -- where ransomware gangs target high-profile targets, breach their networks, and then manually install ransomware on their networks.

This very focused targeting tactic is in stark contrast with the shotgun approach that has been used by ransomware gangs in the past, in the 2015 - early 2019 period, when they heavily relied on exploit kits and email spam to infect random victims.

Other ransomware gangs that engage in targeted "big-game hunting" include Ryuk, REvil (Sodinokibi), LockerGoga, RobbinHood, DoppelPaymer, Maze, and many more others.

Europol's top hacking ring takedowns