NetWire

February 16, 2021

In news: NetWire was in news with respect Elgar Parishad case accused Rona Wilson(installation of the NetWire remote access Trojan ("RAT") on Wilson's computer)

About the NetWire

- It is a remote access Trojan focused on password stealing and keylogging, as well as including remote control capabilities.
- It has been used by malicious groups since 2012 and distributed through various social engineering campaigns (malspam)
- This multi-platform malware has since undergone several upgrades and was identified in different types of attacks that range from Nigerian scammers to advanced persistent threat (APT) attacks.
- As per the experts, NetWire RAT has been observed during 2020 as one of the most active botnets.
- The threat spreads essentially through COVID-19 themed attacks
- This malware was one of the malware families most exploited in COVID-19 phishing campaigns between February and April 2020.

How does it work?

- Nowadays, NetWire is often launched via social engineering campaigns or as a later payload of another malware chain.
- Criminals send emails with malicious files attached to a wide number of users and expect at least someone to open the infected file.
- Once a victim clicks on it, the malware file is downloaded onto the victim's computer.
- The shared files often used by crooks are PDF, Word and

IMG files

- As a result, after clicking on the shared URL, the next stage is downloaded onto the victim’s computer
- After being executed on the victim’s side, several anti-analysis techniques to protect it from being analyzed are executed.
- It dynamically extracts the malicious code into the memory and executes it in order to bypass Antivirus detection.

Malware families most actively exploited COVID-19 phishing campaigns are:

AngentTesta, Netwire, LokiBot, HawkEye, Aurora, Hakbit, Form Book

What is Phishing?

It is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.