Smominru Malware

May 21, 2020

Why in news?

- This malware is another growing concern

What are its whereabouts?

- This affects about 4,700 computers every day and in August 2019 this affected over 90,000 computers worldwide.
- The botnet depends on over 20 servers, mostly in the U.S. but some are based in Malaysia and Bulgaria.
- In its post-infection phase, a Trojan module and a cryptominer are being stolen, and propagated within the network.
- The ransom ware seems to be capable of returning to the old victims if they do not thoroughly address the issue. After Smominru was removed, approximately one-fourth of the affected machines were again infected.
- The victims range from academics to medical professionals which indicate the hackers do not rely too much on their targets.
- On Windows 7 and Windows Server 2008 systems, approximately 85 percent of infections occurred.
- The target appears secretly to use infected computers at victim’s expense for crypto currency mining.
- The most threats have happened in Beijing, Taiwan, Russia, Brazil and the USA.
- It has different kinds of worms, viruses and the short-form of malicious software designed to affect any type of computer through a software.