Malware Smominru

Malware Smominru, whose incidence was first reported in 2017, continues to infect computers in a big way.

- It is affecting nearly 4,700 computers every day, with over 90,000 computers affected globally in August 2019.
- The botnet **relies on more than 20 dedicated servers, mostly located in the US,** though some are hosted in Malaysia and Bulgaria.
- In its post-infection phase, it **steals victim credentials, installs a Trojan module** and a **cryptominer** and propagates inside the network.
- The malware seems to have the ability to come back to hit the old victims if they fail to tackle the problem completely. About one-fourth of the affected machines were infected again after Smominru was removed from them.
- The victims range from universities to healthcare providers suggesting that hackers are not too particular about their targets.
    - However, about 85% of infections have occurred on Windows 7 and Windows Server 2008 systems.
    - The objective seems to silently use infected computers for mining cryptocurrency at the victim's expense.
- China, Taiwan, Russia, Brazil and the US have seen the most attacks.

Note

- **Malware:** Short for malicious software, it refers to any kind of software that is designed to cause damage to a single computer, server, or computer network. Ransomware, Spy ware, Worms, viruses, and Trojans are all varieties of malware.
- **Botnet:** The word Botnet is formed from the words **'robot' and 'network'.** It is a **network of infected computers that can be controlled remotely,** forcing them to send spam, spread viruses, or stage Distributed Denial of Service (DDoS) attacks without the consent of the computer's' owners.

Source: HBL