Threat of new malware looms over cyberspace

A new threat looms large on the horizon of cyberspace. After Mirai and Reaper, cybersecurity agencies have detected a new malware called Saposhi, which is capable of taking over electronic devices and turning them into ‘bots’, which can then be used for any purpose, including a Distributed Denial of Service attack which, with enough firepower, can cripple entire industries.

Being monitored

A senior cyberpolice officer told *The Hindu* that Saposhi was detected around 15 days ago, and is currently being watched and studied.

“Saposhi is similar in its intensity to Reaper, which was taking over millions of devices at the rate of 10,000 devices per day. Various cybersecurity agencies are currently keeping tabs on it to get a better idea of what it is capable of,” he said.

In October last year, the Computer Emergency Response Team (CERT), a Central government body that deals with cyberattacks, had issued an alert about Reaper, a highly evolved malware capable of not only hacking devices like Wi-Fi routers and security cameras, but also hiding its own presence in the bot — a device taken over by a malware.

Sources said that while the CERT has not yet issued any alert regarding Saposhi, guidelines for protecting devices from Saposhi are likely to be issued in the days to come. “We need to first ensure that the information we have is indeed substantiated before raising alarm bells. Right now, what we know for sure is that Saposhi exists, and is highly capable. Factors like whether it is aimed at any particular kind of device, or has a specific purpose are still being verified,” another officer said.

Malwares like Saposhi, Reaper and Mirai are primarily aimed at DDoS attacks, in which the malware first creates a network of bots — called a botnet — and then uses the botnet to ping a single server at the same time. As the number of pings are far beyond the server’s capacity, the server crashes and denies service to its consumers. For example, if a large botnet attacks the server of a fleet cab provider, its server will crash, and scores of consumers will be unable to avail of its services, causing chaos in daily commuting as well as massive losses to the company.

In July 2016, small and medium internet service providers in Maharashtra fell prey to a DDoS attack, which caused disruption in the services of several Internet Service Providers (ISP) in the State.

Another malware, Mirai, using a botnet of 5 lakh devices, had caused the servers of Dyn, a leading domain name service provider, to crash, affecting services of popular websites like Twitter, Netflix and Reddit.

END