Source : www.thehindu.com Date : 2020-02-13

HOW COMMON RANSOMWARE VARIANTS ATTACK VICTIMS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

The research highlights how ransomware tries to slip unnoticed past security controls by abusing trusted and legitimate processes | Photo Credit: REUTERS

There are three main modes of distribution for the major ransomware families that are poised to increase their attacks this year, security researchers warned on the occasion of Safer Internet Day on Tuesday.

One of the ways ransomware spreads is by replicating itself rapidly to other computers for maximum impact, researchers from cybersecurity firm Sophos said in a report 'How Ransomware Attacks', a playbook for defenders that explains how ransomware variants attack and impact victims.

Ransomware that spread by replicating itself is called a 'cryptoworm'. The WannaCry attack that caused damage worldwide in 2017 is an example of this kind of ransomware.

These malware also spread as ransomware-as-a-service (RaaS), which are sold on the dark web as a distribution kit (for example, Sodinokibi).

The third most common way of their spread is as automated active adversary attack, where attackers manually deploy the ransomware following an automated scan of networks for systems with weak protection.

This automated, active attack style was the most common approach seen among the top families listed in the report, which includes detailed analysis of 11 of the most prevalent and persistent ransomware families, including Ryuk, BitPaymer and MegaCortex.

The research highlights how ransomware tries to slip unnoticed past security controls by abusing trusted and legitimate processes, and then harnesses internal systems to encrypt the maximum number of files and disable back-up and recovery processes before an IT security team catches up.

"The creators of ransomware have a pretty good grasp of how security software works and adapt their attacks accordingly. Everything is designed to avoid detection while the malware encrypts as many documents as possible as quickly as possible and makes it hard, if not impossible, to recover the data," said Mark Loman, Director of Engineering for Threat Mitigation Technology at Sophos, and the author of the report.

"In some cases, the main body of the attack takes place at night when the IT team is at home asleep. By the time the victim spots what's going on, it is too late. It is vital to have robust security controls, monitoring and response in place covering all endpoints, networks and systems, and to install software updates whenever they are issued," Loman said.

To protect against ransomware, check that you have a full inventory of all devices connected to your network and that any security software you use on them is up to date, the researchers recommended.

Always install the latest security updates, as soon as practicable, on all the devices on your network.

You should also keep regular back-ups of your most important and current data on an offline storage device as this is the best way to avoid having to pay a ransom when affected by ransomware, the researchers said.

Administrators should enable multi-factor authentication on all management systems that support it, to prevent attackers disabling security products during an attack, they added.

END