ENPM686-0201

Samridha Murali

03/07/2022

Current Event 3

For more than a decade, an elite hacker group (Equation) under the US National Security Agency has been attacking and infiltrating key sectors (Government departments, research institutions, communication companies, prestigious universities, aerospace, oil industry) in 45 countries including China, Russia, Japan, Germany, India. Equation has been creating a top-of-the-line backdoor Bvp47 (Telescreen) for over a decade which has been used to monitor countries. This can be traced back to as early as 2005 and continued to 2015 and later. On February 23, 2022 Chinese cybersecurity experts from Pangu Lab China publicly exposed the complete Chain of evidence about this attack. The malware could compromise a selected linux system and then install a back door on it. This backdoor is invisible to the admin and users will secretly communicate with the outside world. It used TCP SYN packets to set up covert communication channels. To invoke and analyse the code attacker's asymmetric private key was required (This hack is also called Bvp47, since 0x47 is the numerical value used in encryption algorithm). In 2017 Shadow Brokers leaked hacking tools stolen from Equation Group (widely believed to be associated with the US National Security Agency), it contained the private key to remotely trigger the telescreen.

Analysis reveals that Telescreen backdoors allow hackers to attack Linux, AIX, Solaris and Sun systems. The backdoor has been deployed in at least 64 targets in top universities, military related departments in, department of communication in China. The backdoor has compromised 287 hosts in 45 countries. This back door is extremely hidden and it's self-destructing. It is hard to trace them. The script tests its environment and deletes itself if it doesn't like its environment. Bvp47 is said to have been active for more than 10 years.

Good antivirus software will detect and eliminate Backdoors. Properly configured Firewall will essentially give back door protection. Installing patches and continuously updating to the latest version of Linux might help generally to eliminate backdoors (Bvp47 updated over the years). Bvp47 couldn't compromise windows systems luckly, but I don't think it's safe to move systems from linux to windows especially when they deal with top confidential data. When the threat is capable enough to persist in systems, from ubuntu v4.10 (2004 release) to ubuntu v16.04 (2015 version) without being noticed, it is something that everyone should be scared of irrespective of the antivirus software they run.

Integrity and availability of data in the compromised systems won't be affected, since backdoor will try to stay undetected. Inorder to protect confidentiality, one scheme i would propose is to store the encrypted data in computer and use a separate embedded system which is not connected to any network to decrypt and view data. Use physical key for encryption and decryption.

References :

1. Coa Siqi (2022, Feb 23), https://www.globaltimes.cn/page/202202/1252952.shtml
2. Thomas Claurn (2022, Feb 23), https://www.theregister.com/2022/02/23/chinese_nsa_linux/