WikiLeaks revealed malware of CIA hacks and spies on Linux computers

WikiLeaks has just published the Vault 7 document that provides detailed information about a supposedly CIA project that allows remote hacking and spying on Linux-based computers.

Called OutlawCountry, this project allows CIA hackers to redirect outbound network traffic on the target machine to the computer system controlled by CIA to retrieve I / O data.

This OutlawCountry tool includes a kernel module that the CIA hacker downloads through the shell to the target system and creates a Netfilter table hidden with a vague name on the user's Linux machine.

'This new table allows creating certain rules, using the iptables command. These rules will hijack the rules currently in use and the administrator will only see them when they know the table name. When removing the kernel module, the table will also be deleted '.

Many CIA tools help hack Linux computers

Although the installation and method of OutlawCountry are not described in detail, it seems that CIA hackers rely only on exploiting holes and the back door to bring the kernel module into the Linux machine.

However, there are some limitations when using this tool because the kernel module only works with the corresponding kernel kernels.

'OutlawCountry 1.0 includes a kernel module for CentOS / RHEL 6.x 64-bit, this module only works with predefined kernels. In addition, OutlawCountry 1.0 only supports hidden DNAT rules into PREROUTING, 'WikiLeaks said.

CIA Vault 7 leak earlier

Last week, WikiLeaks also launched a top secret CIA malware that tracked the location of PCs and laptops running Windows operating systems. With the name ELSA, this malware takes the ID of a nearby public wifi hotspot and merges it with the global data of the public wifi location.

Since March, 14 cases have been revealed by Vault 7, including:

1. **Brutal Kangaroo** - the CIA suite for Windows machines towards closed networks or air-gap computers in organizations and businesses without direct access.
2. **Cherry Blossom** - the CIA framework, usually implanted based on firmware for remote control, is used to monitor the Internet activity of the target machine by exploiting errors on Wifi devices.
3. **Pandemic** - the CIA project allows spy organizations to turn Windows file servers into hidden attack machines, which can silently infect other machines on the target network.
4. **Athena** - spyware is designed to completely control remote Windows machines, works with all Windows versions, from Windows XP to Windows 10.
5. **Archimedes** - an intermediate attack tool thought to be created by a spy organization, targeting computers inside the LAN.
6. **Scribbles** - software designed to embed web beacons into confidential documents, allowing CIA hackers to monitor internally.
7. **Grasshopper** - framework allows CIA to create arbitrary malware to break into Windows system and overcome anti-virus tool.
8. **Marble** - the source of the tool makes it difficult to find anti-forensic computers, mostly code sneaky or packaged to hide the true source of malware.
9. **Dark Matter** - exploit vulnerability designed and used to target iPhone and Mac.
10. **Weeping Angel** - a spy tool used by the CIA to invade smart TVs, turning them into hidden microphones.
11. **Year Zero** - a tool to hack popular software and hardware.