Malware: InvisiMole---Someone is watching you

Dilpreet Singh Bajwa

POST 7: 12-7-18/Malware: InvisiMole---Someone is watching you

Suppose you have open your laptop and place it on your bed or table in your bedroom and roaming all over in your bedroom and talking to someone over phone and all your activities/conversation were monitored and recorded by someone without your knowledge through webcam and microphone of your own compromised laptop. May be some of yours special or personal moments also get recorded and can be misused. It may also happens that the laptop is present at the meeting room of your organization where all important plans are discussed and through this infected laptop all your conversation, plans can be stolen. The condition is more worrisome if the infected laptop is of more important person like defense minister, Defense secretary or any important person of an army or security agency of a nation than what can be compromised or at stake, you can't even imagine.

All this and much more capability is present in a malware detected recently named as: "InvisiMole". It's a spyware. It was discovered by security researchers from ESET and it was active since 2013. It has very advance capabilities and there is a possibility that it can be created by some well organized group of attackers or by some nation against a nation. This result is deduced from the fact that despite its extensive capability, the malware has been active on only dozens of targeted computers in Russia and Ukraine.

InvisiMole is designed for stealth and theft. No information yet available about its origin, its creator or for what type of target it followed because most of the clues has been stripped including compilation dates which replaced with zeros, so that no information can be gained about its timeline and lifespan. To hide itself from the eyes of administrators and analysts, the malware encrypts its strings, internal files, configuration data and network communication. The malware has very advance capability and constitute two modules named RC2FM and RC2CL, both have their own set of commands and spying feature but the modules also help each other to perform the operations. Both of the modules are feature-rich backdoors, which together have the ability to collect as much as information possible about the victim.

First Module- RC2FM: This is invisiMole's main module. It is smaller than other module and less advance than the second module. It supports only 15 commands. This module is used to perform operations like to alter settings of system, steal and search data. It also has the capability to turn on the webcam and microphone of the system and take screenshots, record audio and send it over the network to its command and control server. Other important feature this module performs is that it manages proxy settings to send data in case the local network setting obstructing the module to contact its command and control server.

Second Module- RC2CL: This module is more capable than the first one and has almost all the capabilities which you can expect from an advance malware. It supports over 80 commands. Its capability includes registry key manipulation, manipulating and getting list of local software, running remote shell commands, controlling drivers, collecting network information, disabling firewall and other security features. Like first module it can also control webcam, microphone of the system and also manage proxy settings. In addition, it also has anti-forensic features like deleting its traces so that forensics tools not be able to detect it.

InvisiMole is fully-equipped spyware having rich capabilities and intentionally was used against a very small number of high-value targets which makes possible for it to conceal itself for almost five years.

Sources:

https://www.bleepingcomputer.com/news/security/invisimole-is-a-complex-spyware-that-can-take-pictures-and-record-audio/

https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/invisimole-spyware/amp/