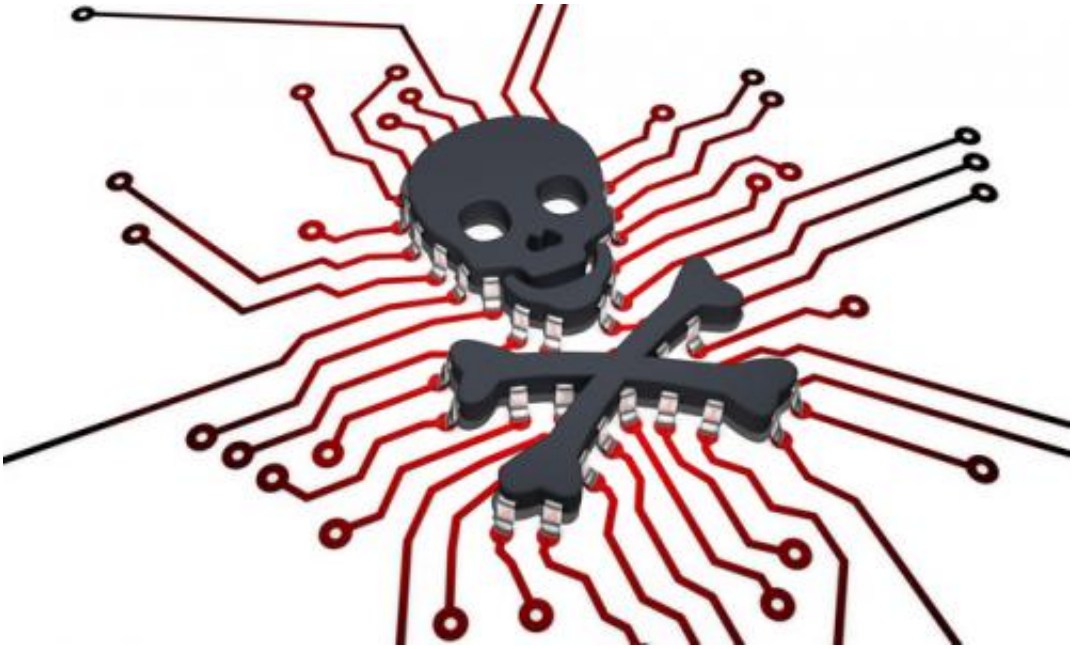
Introducing one of the most sophisticated espionage bugs ever discovered

November 25 2014, by Andrew Smith



Worry only if you have something to hide. Credit: Finchen

The computer-security firm Symantec says it may have found some of the most sophisticated malicious software ever made. The cyber-espionage bug, called Regin, has been making attacks for many years without being caught.

Most malware – which you are tricked into loading when you access free software, illegal film downloads or pornography sites – wants to spread as widely as possible. It aims to gather data that can be used for

malicious purposes, such as holding your device ransom. That is why it spreads indiscriminately. The six-year-old Regin malware is different. It is unlikely to accidentally infect your system, unless the attacker wants that to happen.

The Swiss army knife of malware

Regin makes use of multiple stages to complete its attack. Once the victim is duped into loading the trojan application, by sending you an email with an infected attachment, it will download encrypted components needed for the attack. This allows the trojan to be easily adapt remotely, which makes it difficult for any anti-malware software to keep up.

Regin is more cunning still. As each component is downloaded, decrypted and activated, it then downloads another component. Each potentially different and very difficult to detect. Eventually it installs a kernel, the core application that runs the malware. It then loads its own "user framework" a collection of applications and system calls that talk to the kernel. All this enables Regin to access data on the attacked computer and spy as it is directed to.

Regins seems to be the Swiss army knife of malware, adapting to the user and the intended attack, adding different tools and resources in a stealthy stepwise manner. One victim gets one unique set of tools, and another victim gets a completely different set.

The tools Regin deploys include key loggers (recording which buttons on the keyboard are pressed), mouse-click monitors, network-traffic monitoring, screen capturing software and tools that log messenger chats.

This multi-staged attack has the hallmarks of a complex capable agency. The suspicion is that a western intelligence agency is behind Regin. The

release pattern suggests that the period between 2008 and 2011 was used for field trials. Since then attacks have been highly targeted. Russia and Saudi Arabia top the list among of those attacked so far.

Should I panic?

The variant discovered by Symantec will have already been included in their database. Anti-malware companies compete for customers, but they do share intelligence ensuring that no single provider is vulnerable. This means that, if you are using an anti-malware application and have enabled it to download all current malware definitions, you will be already protected or should receive protection in less than 48 hours.

But they have only been able to detect and respond to one variant. There are others and there will be more. Anti-malware companies play a cat and mouse game with cyber-criminals and malware creators. This situation is no different. The interesting part is that the attacks do not seem to be random. Like Stuxnet, which was used to attack Iran's nuclear facilities, and Stuxnet-like malware, Duqu, Regin's attacks have been highly targeted.

This is why I do not think that you will be affected (unless you have good reasons to be concerned). But I do strongly advise everybody to ensure that their anti-malware applications are kept up to date.

Source: The Conversation

espionage-bugs.html