Malicious Software explores new Business Models – Politics

Posted on **July 19,2017** by **lynx**

Malicious software has become a major component of criminal business and geopolitics. In addition it is a convenient explanation for anything one does not want to investigate. Since code always come from somewhere you have to ask yourself many more questions when it comes to infected networks and compromised hosts. What is the agenda of the day? Journalist Erich Möchel has written an article about the arms race regarding malicious software. We have translated the original text from German to English. Expect the state of cyber in your network to rise in the course of the next years.

Arms race with Malicious Software enters a dangerous Phase

The enormous damage done by "Petya" and "WannaCry" can be traced back to a single, reworked tool from the leaked NSA pool of the "Shadow Brokers". Experts assume that this is only the beginning.

The latest outbreak of malicious software in the past week shows the dangerousness of the new phase the ”cyber" arms race has entered in the beginning of 2017. The core functions of "Petya" - like the ones of "WannaCry" that came before - stem from a large arsenal of high-quality malicious software, which had been developed for the NSA, but fell into the hands of an enemy intelligence service in 2016.

By now there is hardly any doubt that both campaigns were not carried out by criminals but state actors. In addition, the anti-virus industry assumes that these outbreaks were only the beginning and another arsenal could appear on the net. This arsenal of the CIA is already on Wikileaks, where since March new espionage programs are being presented every week.

The semi-leaked Arsenal of the CIA

Julian Assange's team keeps the programs to themselves, but alongside Wikileaks and the CIA itself, there is a third party,still unknown,who has this convolute of about a thousand espionage programs and digital burglary tools at its command. Whoever has exfiltrated this enormous data set from the intranet of the CIA, which is strictly separated from the Internet, and passed it on, has the same data set at his disposal, also containing all the malicious programs unpublished by Wikileaks.

This is a comprehensive wiki for the "cyber" warriors of the CIA, including manuals, tutorials, and related programs, which are clearly different from those of the NSA. All CIA programs are easy to apply and to use because they have not been written for programmers, but for taught "cyber lateral entrants". Furthermore, this entire set of malicious software was not written for the systematic complete tapping of data streams à la NSA, but for targeted ad-hoc espionage. For each eventuality, it provides one with simple but suitable auxiliary tools.

"Outlaw Country"

While the NSA prefers meaningless, randomly generated codes for their programs, the CIA's nomenclature is quite striking. The latest release of Wikileaks published on Friday is called "Outlaw Country" ("Land of the Lawless") and targets Linux servers and gateways. "OutlawCountry" causes infected computers to route traffic from a company or government network to the Internet via hidden servers of the CIA. Since at the internet

gateways and firewallls of large networks SSL / TLS encryption gets routinely broken up in order to enable anti-virus scans of incoming, encrypted data streams, the user's login data and passwords for any websites can also be tapped.

The case of "Petya" is an example of what can happen if such malicious programs fall into the hands of third parties who want to do something else than just spy. Apart from its name “Petya” has very little in common with an eponymous blackmail software, known since 2015. In the case of the new “Petya”, according to all the malware analysts, first-class "exploit" named EternalBlue, which had been used by the NSA for many years to exploit a serious windows vulnerability, has been combined with new features.

If Money Collection does not work

While EternalBlue was written for specific, "manual" espionage missions against certain networks, Pseudo-"Petya" caused "EternalBlue" to spread independently by the means of a so called "worm". In whichever internal network machines were identified, which windows systems were not up-to-date, they were captured by the NSA exploit. The camouflage as a blackmail software, however, did not last long after anti-virus experts had found out that the hard disks were not encrypted but formatted, that is, overwritten.

Furthermore, the only software module that did not work at all in this otherwise very efficient attack was the mechanism for collecting the ransom money. Prior to this, "WannaCry" had also proved to be ineffective precisely in that respect. Here too, the collection function was highly deficient. As is apparent from the blockchain data, these two spectacular malware fireworks have gained no more than $ 100,000 in bitcoins around the world. Since all transactions with these bitcoins are traceable, their conversion into real money will be difficult and, above all, diminished by high financial losses.

Control Computer as the real Target

The NSA's EternalBlue exploit was targeted only at computers with critical control and switching functions, which are usually connected to an internal network, but not to the Internet. This supposedly high security due to separation from the Internet has led to the fact that the security of such control PCs has generally been neglected so far. What happens when people try to save money through extending the maintenance cycles of their service contracts was demonstrated by the British health system, where controllers for medical devices were badly hit by "WannaCry".

As the "Postmortem" analyses show, the epicenter of pseudo-"Petya" was the Ukraine, the first series of infections mainly concerned computers and switchgear of power suppliers and telecoms there. Through its non-controllable worm function "Petya" afterwards quickly spread to other networks worldwide. The initiators hazarded the consequences of the resulting collateral damage and the "Shadow Brokers" had little scruples to simply publish high-quality digital intrusion tools on the net.

Forecast: Cloudy

In quite the same way - but probably even easier - many individual modules from the digital CIA burglar toolbox could be re-used for other purposes. When it comes to "security" by separating control computers from the Internet, the CIA arsenal also includes a module called "BrutalKangaroo". Its core function is to bounce over the so-called "air gap" into a physically separated "isle network", as is typical for systems like the ones used for power plant control.

Posted in:Discussion,Internet,Security | Tagged:Cyberwar,Infrastructure,Malware,SecInt,Security | With 0 comments