Here's how the ransomware attack was stopped – and why it could soon start again

18 May 2017, by Adrian Winckles

Credit: Shutterstock

The ransomware cyber attack that has so far affected around 300,000 computers in 150 countries could have been much worse. In fact, it still could be. The spread of the malicious software (malware), nicknamed WannaCry or WannaCrypt, has been halted several times by researchers who have identified flaws in the program known as kill switches. But cybercriminals are already fighting back by altering the code, leading to a game of cat and mouse as researchers then have to hunt for a new kill switch.

Ransomware is a type of malware that blocks access to a computer until money is paid to release it. It is normally spread as an attachment on an email but WannaCry is different because it can spread through a local network on its own.

It looks for other computers running a file and printer sharing protocol called Server Message Block (SMB), which is found in older operating systems such as Windows XP that no longer receive routine security updates. It then uses a flaw in SMB to spread to other computers without their users having to download the file. This explains why more computers have been affected than is typical with this kind of malware.

The Achilles heel of malware is the need to call home to its operator. For ransomware, there has to be a mechanism for the program's operator to collect the ransom money and unlock the data. These communications can provide a way for law enforcement to track down the cybercriminals, so they often build into their malware something called a kill switch.

Generally, a kill switch is a mechanism for turning off a device or a piece of software remotely – and abruptly – in an emergency, such as when it has been stolen or accessed without authorisation. In malware, a kill switch is a way for the operator to terminate their connection to the software to prevent authorities from discovering their identity.

One kill switch method is to redirect the malware's communications to a "sinkhole" server, which can render it ineffective. Investigators can study the malware and look for such a kill switch or a way to take over the software.

A sophisticated piece of malware will often run its control communication across multiple unregistered internet domains. By periodically changing the domain it uses, the software can thwart attempts to understand or neutralise it. This means investigators need to constantly adapt and register any new domains the malware may try to use to make the sinkhole effective.

Accidental death

In the case of WannaCry, a researcher using the pseudonym MalwareTech ended up accidentally activating the kill switch when he tried to create a sinkhole in order to study the software. WannaCry included code that looked to check if a specified domain had been registered. If it received a response from the domain, it shut down. If not, it continued to work. So when MalwareTech registered the domain, it effectively activated the kill switch.

This kill switch was probably inserted to prevent investigators studying the software in a closed virtual environment called a "sandbox". These typically respond to all communication attempts by the malware with signals from registered domains. So when WannaCry received a response from the domain, it was tricked into thinking it was in a sandbox and shut down to protect itself.

The problem is that modifying WannaCry's code so it looks for a different unregistered domain will allow new versions of the software to continue running. In fact, one new variant of the malware has already been stopped after researchers registered the new domain, activating the related kill switch.

An interesting paradox is that WannaCry was developed using a surveillance tool called EternalBlue created by the US National Security Agency (NSA) and leaked by a group of hackers known by the pseudonym Shadow Brokers. They are now claiming to have further harmful source code for WannaCry and are threatening to release it into the wild for anyone to modify freely. Based on the history of previous similar malware, copycats are extremely likely. With major modifications to the source code, the recent updates made to anti-malware software will become futile as the the cycle begins again.

Researchers are even questioning why WannaCry's kill switch existed at all given that it was so easy to discover and execute. The danger is that WannaCry was just a test to illicit the response of defenders so deadlier variants can be unleashed later.

This article was originally published on The

Provided by The Conversation

APA citation: Here's how the ransomware attack was stopped – and why it could soon start again (2017, May 18) retrieved 21 October 2021 from https://techxplore.com/news/2017-05-ransomware_1.html