WannaCry threat update

On Friday, 12 May 2017, organisations across the world were hit by a massive ransomware attack, named WannaCry, which exploited a (now patched) Microsoft Windows vulnerability revealed in the Shadowbrokers dump on 14 March 2017. Kaspersky Lab researchers have continued to track the evolution of the threat over the weekend.

Evolution of the ransomware

The total number of variants in circulation on Monday, 15 May 2017 is still unclear – but over the weekend two notable variants emerged.

Kaspersky Lab does not believe any of these variants were created by the original authors - most likely they were patched by others keen to exploit the attack for their own ends.

Fast-moving cyber attacks wreak havoc worldwide
15 May 2017

The first one started spreading on Sunday morning, at around 2am UTC/GMT and was patched to connect to a different domain. Kaspersky Lab has so far noted three victims for this variant, located in Russia and Brazil.

The second variation that appeared during the weekend appears to have been patched to remove the kill switch. This variant does not appear to be spreading, possibly due to the fact it has a bug.

Number of infections to date

Further analysis of network logs suggests the WannaCry ransomware may have started to spread on Thursday, 11 May 2017. Kaspersky Lab states that is difficult to estimate the total number of infections. Its own telemetry indicates that over 45,000 users have been attacked, but this represents a fraction of the total numbers of attacks (reflecting Kaspersky Lab's customer share.)

A more accurate picture of the world situation can be drawn from the sinkhole for the kill switch hardcoded in most versions of WannaCry: Currently the Malwaretech sinkhole, which is collecting redirections from the 'kill switch' code, has registered about 200,000 hits.

This number does not include infections inside corporate networks where a proxy server is required for connecting to the internet, meaning that the real number of victims might easily be larger.

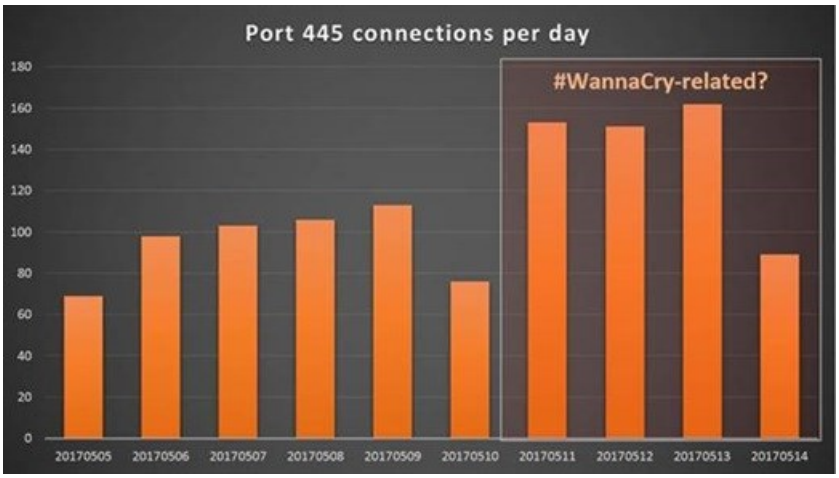
The number of WannaCry attack attempts detected by Kaspersky Lab on Monday, 15 May 2017 has declined six-fold compared to the same time on Friday, 12 May 2017. This suggests the infection may be coming under control.

Advice to reduce the risk of infection

- Install the official patch from Microsoft that closes the vulnerability used in the attack (there are also patches available for Windows XP, Windows 8, and Windows Server 2003).
- Ensure that security solutions are switched on all nodes of the network.
- For those who do not use Kaspersky Lab solutions, the company suggests installing the free Kaspersky Anti-Ransomware Tool for business (KART).
- If Kaspersky Lab's solution is used, ensure that it includes the System Watcher, a behavioural proactive detection component, and that it is switched on.
- Run the Critical Area Scan task in Kaspersky Lab's solution to detect possible infection as soon as possible (otherwise it will be detected automatically, if not switched off, within 24 hours).
- Reboot the system after detecting MEM: Trojan.Win64.EquationDrug.gen.
- Use Customer-Specific Threat Intelligence Reporting services to be informed about possible attacks.
- WannaCry is also targeting embedded systems. Kaspersky Lab recommends ensuring that dedicated security solutions for embedded systems are installed, and that they have both anti-malware protection and Default Deny functionality enabled.

Technical data

More detailed descriptions of the WannaCry attack method, and Indicators of Compromise can be found on Securelist.



The two new variants of the WannaCry ransomware are as follows:
Variant 1: md5: d5dcd28612f4d6ffca0cfeaefd606bcf
Connected to: ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
Variant 2: md5: d724d8cc6420f06e8a48752f0da11c66