WannaCry: Are you safe?

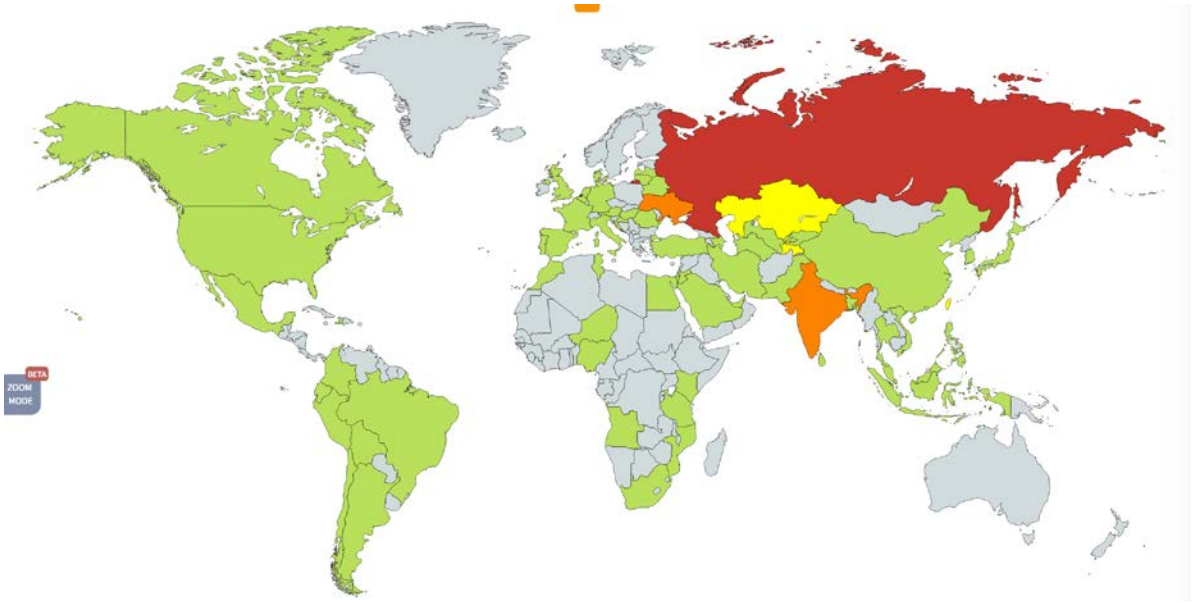
May 13, 2017

A few days ago, an outbreak of the Trojan encryptor WannaCry started. It appears that the epidemic is global. We call it an epidemic since the extent of it is quite huge. We counted over 45,000 cases of the attack in just one day. In reality, the number is definitely *much* higher.

What happened?

Several large organizations simultaneously reported an infection. Among the organizations were several British hospitals that had to suspend their operations. According to the data released by third parties, WannaCry has infected more than 100,000 computers. Essentially, this is why it has drawn so much attention.

The largest number of attacks occurred in Russia, but Ukraine, India, and Taiwan have suffered damage from WannaCry as well. All in all, we have discovered WannaCry in 74 countries. This was only on the first day of the attack.



What is WannaCry?

Generally, WannaCry comes in two parts. First of all, it's an exploit which purposes are infection and propagation. And the second part is an encryptor that is downloaded to the computer after it has been infected.
This is the main difference between WannaCry and the majority of other encryptors. In order to infect a computer with a common encryptor, a user has to make a mistake, for example, by clicking a suspicious link, allowing Word to run a malicious macro, or downloading a suspicious attachment from an email message. A system can be infected with WannaCry without doing anything.

WannaCry: Exploit and Propagation

The creators of WannaCry have taken advantage of the Windows exploit known as "EternalBlue", which exploits a vulnerability that Microsoft patched in security update MS17-010, dated March 14 of the current year. By using the exploit, the malefactors could gain remote access to computers and install the encryptor.
If you have the update installed, and this vulnerability no longer exists, then any attempts to hack the computer remotely will be futile. However, researchers from Kaspersky Lab's GReAT (Global Research & Analysis Team) would like to specifically point out that patching the vulnerability will not deter the encryptor from operating in any manner. Therefore, if you launch it somehow (see above for *making a mistake*), then the patch will not do you any good.
After hacking a computer successfully, WannaCry attempts to spread itself over the local network onto other computers, in a manner of a computer worm. The encryptor scans other

computers for the same vulnerability that can be exploited with the help of EternalBlue, and when WannaCry finds vulnerable machine, it attacks and encrypts files on it.

It turns out that by infecting one computer, WannaCry may infect an entire local area network and encrypt all of the computers on the network. This is why large companies suffered the most from the WannaCry attack — the more computers there are on the network, the larger the damage.

WannaCry: Encryptor

As an encryptor, WannaCry (sometimes called WCrypt or WannaCry Decryptor, even though, logically, it is an *encryptor*, not a *decryptor*) does the same as other encryptors; it encrypts files on a computer and demands a ransom for decrypting them. It most closely resembles a variation of the infamous CryptXXX Trojan.
WannaCry encrypts files of different types (the full list is located here), which, of course, include office documents, pictures, videos, archives, and other file formats that may potentially contain critical user data. The extensions of the encrypted files are renamed to .WCRY (thus, the name of the encryptor), and the files become completely inaccessible. After this, the Trojan changes the desktop wallpaper to a picture that contains information about the infection and actions that the user supposedly has to perform in order to recover the files. WannaCry spreads notifications as text files with the same information across folders on the computer in order to ensure that the user definitely receives the message.

As usual, everything comes down to transferring a certain amount in the bitcoin equivalent to the wallet of the evildoers. After that they will (probably) decrypt all of the files. Initially, cybercriminals demanded $300 but then decided to raise the stakes: the latest WannaCry versions feature a ransom amount of $600.

Malefactors also intimidate the user by stating that the ransom amount will be increased in 3 days and, moreover, that it will be impossible to decrypt the files in 7 days. We do not recommend paying the ransom to the evildoers, as nobody can guarantee that they will decrypt your files after receiving the ransom. As a matter of fact, researchers have shown that other cyber extortioners sometimes simply delete user data, which means that no physical possibility to decipher the files remains, even though malefactors would still demand the ransom as if nothing has happened.

How domain registration suspended infection and why the epidemic is probably not over yet

Interestingly enough, a researcher going by name Malwaretech managed to suspend infection by registering a domain with a long and absolutely nonsensical name online. It turned out that some versions of WannaCry addressed that very domain and if they did not receive a positive reply, then they would install the encryptor and start their dirty deed. If there was a reply (i.e., the domain had been registered), then the malware would stop all of its activities.

After finding the reference to this domain in the Trojan code, the researcher registered the domain, thus suspending the attack. For the remainder of the day, the domain was addressed several tens of thousands times, which means that several tens of thousands of computers had been saved from becoming infected.

There is a theory that this functionality was built into WannaCry like a “circuit breaker” in case something goes wrong. Another theory that is adhered to by the researcher himself is that this is a way to complicate the analysis of the malware’s behavior. In testing environments used in research, oftentimes it is purposely made that the positive reply comes from *any* domain, and, in this case, the Trojan would do nothing in the testing environment. Regretfully, for new versions of the Trojan, it is enough for evildoers to change the domain name indicated as the “circuit breaker” to resume infection. Therefore, it is very likely that the first day of the WannaCry outbreak will not be the last.

How to defend against WannaCry

Unfortunately, there is currently nothing that can be done to decrypt files that have been encrypted by WannaCry (however our researchers are on it). This means that the only method to fight against infection is to not get infected in the first place.

Here are several pieces of advice on how to prevent infection and minimize damage.

- If you already have Kaspersky Lab security solution installed on your system, then we recommend doing the following: manually run a scan for critical areas, and if the solution detects a malware like MEM:Trojan.Win64.EquationDrug.gen (this is how our anti-virus solutions detect WannaCry), then you should reboot your system.
- If you’re our customer, keep the System Watcher on, it’s essential to fight new varieties of the malware that might emerge.
- Install software updates. This case earnestly calls for installing the system security update MS17-010 for all Windows users, especially when Microsoft even released it for

systems that are not officially supported anymore, such as Windows XP or Windows 2003. **Seriously, install it right now**. Now is exactly the time when it's really important.

- Create file backup copies on a regular basis and store the copies on storage devices that are not constantly connected to the computer. If there is a recent backup copy, then encryptor infection is not a catastrophe but a loss of several hours spent on system re-installation. If you do not feel like creating backups by yourself, then you can take advantage of a backup feature built into Kaspersky Total Security that can automate the process.

- Use a reliable anti-virus. Kaspersky Internet Security can detect WannaCry both locally and during attempts to spread it over a network. Moreover, System Watcher, a built-in module, has a feature of rolling back any unwanted changes, which means that it will prevent file encryption even for those malware versions that are not yet in anti-virus databases.