In May 2017, thousands of people first heard about ransomware when they were denied admission to hospitals. The reason for this was the outbreak of the ransomware program WannaCry, which paralyzed work and forced several hospitals to return to pen and paper.

The ransomwares were born due to two innovations of last 10 years: encryption and bitcoin. Before these innovations this kind of attacks was not popular, because of ease of bank transfer tracking, cash payment was difficult, and if any variant got successful, people would trade tips on how to defeat it rather than pay the bill.

Once group of hackers ShadowBrokers who stole the tools of another group, Equation (there are fairly reasonable suspicions that Equation is related to American intelligence - NSA). At first, the hackers tried to sell the stolen goods, and then, when no one bought anything, they simply posted all the exploits in the public domain. Which, of course, was used by attackers of various sorts.

This is how WannaCry was born - a worm consisting of rather poor encryption code and a powerful exploit called EternalBlue, which used a zero-day vulnerability in various Windows versions to spread. When they say "a zero-day vulnerability," they mean that no one was aware of this vulnerability before. Including the developer company, which for this reason did not fix anything: in order to release a patch, you must at least know what to patch.

Many experts agree that the WannaCry worm escaped when its creator was unable to keep it in the test environment, and as a result, an unfinished ransomware worm burst onto the Internet, knocking on remote computers indiscriminately, penetrating them through a vulnerability in Windows and encrypting the entire contents of the drives. And then it spread further and further, to the next computers. It looked like a domino effect - not just one domino at a time, but in all directions at once.

At the same time, ordinary ransomware always offer an option: pay the attacker - and he will send you a decryption code so that you can return the data. WannaCry also offered such an option ... only it was impossible to decrypt the files. Either it was a bug in the code - another argument in favor of the escaped worm theory, or WannaCry was immediately planned as a destructive weapon for all civilizations connected to the Internet.

The epidemic was stopped in an amazing way. Young researcher Marcus Hutchins, known under the nickname Malwaretechblog, like many other researchers around the world, rushed to analyze WannaCry - to understand how to defend against it, how it spreads, whether files can be decrypted, and so on. And he discovered that before encrypting the drive, the malware for some reason sends an appeal to a non-existent domain on the Internet. "What happens if I register this domain?" Thought Hutchins. And registered. And I found out that after that the malware no longer does anything: that is, it does not stop spreading, but it no longer encrypts disks.

So Hutchins stopped the epidemic and briefly became a global hero. And a little later he was arrested by the FBI for the fact that at a very young age he managed to write the code for banking Trojans himself, and later switched to the bright side - but that's another story.

Since then, however, WannaCry has been improved: the access to the domain has been removed, other bugs have been fixed - and the worm is still terrorizing the planet. But Microsoft released the patch pretty quickly, so most computers are now immune to WannaCry.

Refs

1. <https://3dnews.ru/1009634/10-samih-vpechatlyayushchih-kiberatak-v-istorii>
2. <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware>
3. <https://www.theguardian.com/technology/2017/may/15/accidental-hero-who-halted-cyber-attack-is-22-year-old-english-blogger>
4. <https://en.wikipedia.org/wiki/The_Shadow_Brokers>