Wannacry, Code Red, and „Cyber“ Warfare

Posted on **May 14,2017** by **lynx**

Society and businesses increasingly rely on networked infrastructure. This is not news. Worms that used networks to spread to new hosts in order to infect them is also not news. Code Red did this back in 2001. There is a new worm going around. Its name is Wannacry, and it is allegedly based on published attack code developed by the NSA. The malicious software is delivered by email. After successful installation it infects the host and propagates to other systems by using probes to port 139/TCP, 445/TCP and 3389/TCP. It belongs to the class of ransomware, encrypting files and demanding ransom. Thousands of infected systems are still active. The attack is still ongoing. If you are in doubt if you have compromised systems within your network, we recommend taking a look at how to spot the malware.

The new ingredients of this worm are known vulnerabilities and network capabilities to spread near infected computers. This means that nearby hosts will be infected even if they did not receive the initial email with the malicious document. The patch for the exploited vulnerability is out since 14 March 2017. The code seems to be based on tools published by the Shadow Brokers in August 2016. Since the code has already been changed and uses different payloads, the threat will persist for a while. It's easy to blame the lack of upgrades, but upgrading can be quite difficult. Containing networked systems, filtering local network traffic (especially taking care of management access protocols), and keeping an eye out for an increase in scans works regardless of the weaknesses exploited.

The deeper problem has to do with how we handle vulnerabilities in software. Bugs need to the disclosed as early as possible. Developers and vendors do need a chance to fix their code. This is especially true for vulnerabilities (where the bug has been applied) and exploits (where the vulnerability has been refined to production status). There is also a connection to malicious software used in law enforcement, military operations, and intelligence organisations. Breaking into networks or computer systems works well if you possess knowledge about exploits no one else has. Wannacry is a good example of how this secret code endangers critical infrastructure. There have been reports that hospitals in the UK were hit by the worm. Back in 2012 fx talked about this very scenario in the keynote presentation (titled We Came In Peace – They Don’t: Hackers vs. CyberWar). The existence of 0-days put everyone at risk. This is why biological warfare does not work – and we are dealing with a virus in the wild attacking networked systems as of now.

At DeepINTEL we will discuss strategic aspects of information security. This includes how to handle threats like Wannacry and how to counter these threats.

Posted in:High Entropy,Security | Tagged:Cyberwar,Espionage,Infrastructure,Malware,Mindset | With 0 comments