Worldwide ransomware attack linked to hacked NSA cyberwarfare arsenal

Kevin Reed
13 May 2017

A massive global cyberattack—likely caused by the spread of malware developed by the US National Security Agency as part of its cyberwarfare arsenal—hit computers around the world on Friday and rendered them inoperable. The malicious ransomware attacked computers in 99 countries and locked down their files while demanding that system administrators pay a fee of between $300 and $600 within six hours in exchange for regained access.

The malware, known as "WannaCry" or "WanaCrypt," rapidly infected computers of organizations internationally such as the National Health Service in the UK, the Spanish telecom firm Telefonica and the US-based delivery service FedEx. Some news outlets reported that the bulk of the cyberattack on Friday took place in Russia, Ukraine and Taiwan. It was also reported that the malware disrupted the functioning of banks, transportation systems and other mission-critical operations around the world.

According to cybersecurity experts, the malware is targeting computers running Microsoft Windows. When downloading or clicking on an infected file or application, the malware exploits a security flaw in the operating system and proceeds to encrypt the files of the target system and then demands a payment in bitcoin (electronic currency) by a specified date in exchange for restoring access.

The ransomware is also a "worm," which means that it is engineered for self-replication as far and wide as possible and aimed at being transferred to all computers connected with the host system.

Although Microsoft released a patch to fix the OS security vulnerability in March 2017, many users had not updated their systems in time and remained vulnerable to the ransomware. Meanwhile, those users that paid the demanded ransom are reporting that—rather than having file access restored—the malware demands a greater sum of money and threatens to delete all files on the system.

The outbreak of the viral ransomware is connected to the public release in April by the hacking group calling itself Shadow Brokers of a trove of NSA and CIA cyberwarfare documents and computer code. The group published what it described as documents stolen from an NSA server housing the complete arsenal of US cyberwarfare weapons that had been left poorly protected.

In March, the anti-secrecy website WikiLeaks released documents related to the malware theft in an effort to alert the cybersecurity community and the public that the software was being circulated in the black market and posed a significant threat. WikiLeak's Julian Assange called the theft of the cyberwarfare arsenal by hackers, "a historic act of devastating incompetence" by the US intelligence establishment.

Additionally, Assange and WikiLeaks exposed the fact that the US government was well aware that their inventory of malware, spyware, netbots, viruses and "Trojan horses"—the product of decades of CIA and NSA cyberwarfare preparations—had been stolen and did nothing to work with the computer industry or to notify the public about the theft of these items from their servers.

At that time, the corporate media around the globe also refused to warn about the dangers posed by the circulation of the malware code among hacker groups and others on the periphery of the US military-intelligence community. Rather than demand emergency action to protect the public from what is now unfolding, the subservient media continued its

vilification of WikiLeaks and asserted false claims that the exposure of the criminal activity of the US government threatened national security and endangered the lives of security personnel.