ars TECHNICA

Scam of The Week: A New Ransomware Outbreak Similar to WCry is Shutting Down Computers Worldwide

Article retrieved from: arstechnica.com
Article written by: Dan Goodin 6/27/17

A new ransomware attack similar to last month's self-replicating WCry outbreak is sweeping the world with at least 80 large companies infected, reportedly including drug maker Merck, international shipping company Maersk, law firm DLA Piper, UK advertising firm WPP, and snack food maker Mondelez International.

PetyaWrap, as the ransomware is called, uses the same potent National Security Agency exploit that allowed WCry to paralyze hospitals, shipping companies, and train stations in a matter of hours on May 12. EternalBlue, as the exploit was code-named by its NSA developers, was published in April by a still-unknown group calling itself the Shadow Brokers. The leak gave people with only moderate technical skills a powerful vehicle for delivering virtually any kind of digital warhead. Microsoft patched the underlying vulnerability in Windows 7 and 8.1 in March, and in a rare move the company issued fixes for unsupported Windows versions 24 hours after the WCry outbreak. That meant infections were only possible on machines that were running outdated versions of the OS.

PetyaWrap, according to researchers at antivirus provider F-Secure, uses a modified version of EternalBlue. There are also reports that it makes use of booby-trapped Microsoft Excel documents attached to phishing e-mails. The precise relationship between the malicious attachments and the EternalBlue exploit isn't yet clear. One possibility is that the e-mails are used to infect one or more computers in an organization, and the ransomware then uses the NSA exploit to spread to other machines on the same network.

Ransomware and credential stealer together

According to researchers at Recorded Future, Tuesday's attacks appear to deliver two payloads. One is the new version of the Petya ransomware package. Tuesday's version, which some researchers have started calling PetyaWrap, holds data hostage until users pay $300 in Bitcoins. The other payload is an information stealer that extracts usernames and passwords from victim computers and sends the data to a server controlled by the attackers. That would mean that while an infected computer has been rendered inoperable by the ransomware, the attackers would already have access to potentially high-value credentials that were stored on the machine.

Researchers with AV provider Eset said in a blog post that unlike many ransomware packages, PetyaWrap doesn't encrypt individual files. Instead the encryption is aimed at a computer's entire file system. The ransomware targets the computer's master boot record, which is a crucial piece of data that allows a computer to locate its operating system and other key components.

Tuesday's attack spread widely almost immediately. It initially took hold in Ukraine, but soon it reportedly spread to Spain, France, Russia, and the United States. WPP, the British ad company, said on Twitter that some of its IT systems were hit by a cyber-attack. Its website remained unreachable as this post was going live. Meanwhile, Reuters reported that Ukrainian state power distributor Ukrenergo said its IT system were also hit by a cyber-attack but that the disruption had no impact on power supplies or broader operations.

Others hit, according to Bloomberg, included Ukrainian delivery network Nova Poshta, which halted service to clients after its network was infected. Bloomberg also said Ukraine's Central Bank warned on its website that several banks had been targeted by hackers. Security company Group-IB said at least 80 companies have been infected so far.

The rapid spread mimics the WCry outbreak, which within about 12 hours infected more than 727,000 computers in 90 countries. WCry was designed to be a worm, meaning once it infected a computer it could spread to other connected computers without requiring any user interaction. It's not yet clear if the PetyaWrap has the same self-replicating ability. The number of organizations that have been disrupted would suggest that it does.

If you are a client of ours and ever notice anything unusual with your PC, immediately unplug the PC from the network, power it down and give us a call (614) 827-9400. We will inspect the machine for any signs of malicious activity.

GroupEleven