Petya ransomware attack shuts down computers in 65 countries

Kevin Reed
29 June 2017

In the second massive cyberattack in 44 days, both originating from malicious software developed by the US National Security Agency, personal computers in at least 65 countries were shut down Tuesday by an epidemic of ransomware known as Petya.

The attack had its greatest impact and first manifestation in Ukraine, where an estimated 12,500 computer systems were infected. Initial reports of the malware came when Ukrainian computer users attempted to update their copies of the tax and accounting software MeDoc. From there, the ransomware spread quickly all over the world, with major outages reported in Belgium, Brazil, Germany, Russia and the United States.

Among the corporations hit by the attack were the American pharmaceutical giant Merck, the British advertising agency WPP, the French multinational Saint-Gobain, the Russian steel and mining company Evraz and the Australian factory of the chocolate company Cadbury. In Ukraine, government ministries, ATMs and transit and airports systems were paralyzed and workers at the Chernobyl nuclear disaster site were forced to monitor radiation levels manually because their computers became inoperable.

In the US, Heritage Valley Health Systems, a Pennsylvania health care provider, was forced to cancel operations at its hospitals in Beaver and Sewickley due to the computer outage caused by Petya. According to some security experts, the latest ransomware attack represents a more sophisticated and lethal application of the malware than previously encountered.

The Petya ransomware causes computers to stop functioning and brings up a red screen with white letters that says the hard disks on the system have been encrypted with “military grade encryption.” The files on the system will be restored, the message explains, only in exchange for a payment of $300 in bitcoin electronic currency to a specified email address. It is not clear if making the ransom payment leads to the restoration of file access.

Once cybersecurity experts identified the email account, it was shut down.

The virus attacks Windows-based computers by taking advantage of the EternalBlue vulnerability. EternalBlue is known as an “exploit” or “bug” in the Windows operating system that can be used to cause unexpected behavior. Although Microsoft had released security updates to address the EternalBlue issue when they became aware of the problem last March, the latest attack is a “new variant” of Petya that can circumvent previous software patches.

Once a single system has been infected, the ransomware has the ability to move from computer to computer on a network without users doing anything. The Petya virus also has the ability to utilize unprotected machines to access networking features and infect machines that have been previously protected. Because of these innovations, some security experts are referring to the new ransomware as GoldenEye.

It is well known that the EternalBlue exploit was developed by the NSA as part of its arsenal of cyberwarfare weaponry for use against the rivals of US imperialism. Due to a combination of recklessness and stupidity, however, the NSA’s arsenal servers were hacked earlier this year and the tools were stolen by as-of-yet unidentified hackers.

In April, an Internet group known as Shadow Brokers published information about the NSA arsenal, including details about exploits that take advantage of vulnerabilities in enterprise firewalls, anti-virus products and Microsoft software.

The Petya attack comes less than two months after the outbreak in early May of the WannaCry ransomware, which spread around the world in a similar manner. In that instance, the malware shut down hundreds of thousands of computers in more than 150 countries.

So far, the NSA has not acknowledged any responsibility for the malware code that has now disrupted the economy in countless countries and endangered the lives of millions of people on two separate occasions. Computer security experts are coming forward in increasing numbers to demand that the NSA work with specialists to help defend computer systems from the destructive mayhem that the agency has unleashed upon society.

Although no one has taken responsibility for the latest epidemic, the location and timing of the Petya attack—centered in Ukraine and launched one day before a holiday marking the break of Ukraine from the USSR—points to possible political motivations. Some media outlets, as well as the Ukrainian government, have begun making well-worn and unsubstantiated allegations about “Russian hacking.”