Petya Variant Cripples European Businesses

As malware becomes more sophisticated, cyber security teams must remain vigilant. Spohn Security Solutions offers advice on detecting and avoiding attacks.

(Austin, TX) July XX, 2017 – In the wake of May's WannaCry attack, which affected more than 230,000 computers in over 150 countries, a fast moving malware outbreak was reported June 27 in targets in Spain, France, Ukraine, Russia, and other countries.[1,2] The attack infected large banks, law firms, shipping companies and even the Chrenobyl nuclear facility in the Ukraine.[3] As with WannaCry, hackers employed a malicious software using the EternalBlue vulnerability in older Microsoft Windows systems to rapidly spread across an organization.[1,2] The new malware is thought to be a variant of Petya, a wiper malware designed to destroy systems and data with no hope of recovery.[4]

"This new malware dubbed Petya, or NotPetya as it seems to be a completely new form of malware, is far more destructive than WannaCry," says Timothy Crosby, Senior Security Consultant for Spohn Security Solutions. "The motivation behind WannaCry seems to have been merely financial, while the Petya variant aimed to create widespread system destruction where data was not as easily recovered." In addition, the Petya variant corrupts the MBR and MFT making complete system restoration incredibly difficult, if not impossible, for those infected.[3]

Using EternalBlue, both WannaCry and the Petya variant exploit a vulnerability in the SMB data-transfer protocol used to share files and printers across local networks.[1,2,3,4] WannaCry, a traditional malware, resides on a computer or device in the form of files, either embedded in or masquerading as non-malicious files.[5] After the WannaCry attack, Microsoft released a patch for the SMB vulnerability.[3] However, the Petya variant goes a step further by employing two additional ways of spreading rapidly within an organization, by targeting a network's administrator tools.[6] So, if the SMB route failed, the Petya variant is able to harvest credentials from the infected system and, using PsExec and WMIC administrative tools, gain access to other systems on the network.[4]

Malware, such as the malicious software used in the Petya variant attacks, is growing increasingly sophisticated employing techniques that are not easily remediated. Fileless malware, for instance, resides in areas not normally scanned, such as the random access memory or even the operating system kernel itself.[5] Because it does not rely on files to run, propagate and accomplish its purpose, fileless malware is virtually impossible to detect using standard cyber security protocols.[5]

"To remediate in a NonPetya-like situation, a cyber security team must be vigilant about the activity on the network," advises Crosby. "Security teams should monitor for aberrant and unexpected behavior like administrator credentials being captured." To prevent permanent damage to data and network systems, businesses should employ a host of protection programs that notify personnel when there is a threat.[7] These programs can mitigate risk by

halting the spread of ransomware throughout the entire network and alerting IT when malware is attempting to encrypt files.[7]

Crosby adds that most attacks can easily be prevented by following a few simple rules. First, download the latest version of Windows and turn on automatic updates. Ensure that antivirus software is up to date and fully patched. Remind employees to not open files sent from unknown sources. And, lastly, back-up computers regularly keeping backup files off-site.

About Spohn Consulting:

Spohn Consulting, Inc., an Austin, Texas-based privately held company established in 1998 by Darren L. Spohn, is an authority in navigating fortune 500 companies and medium-to-small businesses through security business challenges of the 21st Century. Spohn Consulting works with organizations to assess their information security posture (the security status of an enterprise's networks, information, and systems based on Identification and Authorization resources, e.g., people, hardware, software, policies, and capabilities in place to manage the defense of the enterprise and to react as the situation changes), offer customized instructor-led training, and sell telecom services. Utilizing varied scopes of engagement, they deliver recommendations which can be measured against best practice or compliance standards. For more information on cyber security visit https://spohnsolutions.com/.

1. Solon, Olivia, and Alex Hern. "'Petya' Ransomware Attack: What Is It and How Can It Be Stopped?" *The Guardian*. Guardian News and Media, 28 June 2017. Web. 13 July 2017.

2. Brandom, Russell. "A New Ransomware Attack Is Hitting Airlines, Banks and Utilities across Europe." *The Verge*. The Verge, 27 June 2017. Web. 13 July 2017.

3. Sjouwerman, Stu. " Looks Like A New Worldwide Ransomware Outbreak." *KnowBe4*. N.p., 27 June 2017. Web. 13 July 2017.

4. Quora. "How Similar Are WannaCry And Petya Ransomware?" *Forbes*. Forbes Magazine, 05 July 2017. Web. 13 July 2017.

5. BioCatch. "Fileless Malware: What It Is and How To Protect Against It." *BioCatch*. N.p., 27 Feb. 2017. Web. 13 July 2017.

6. Henley, Jon, and Olivia Solon. "'Petya' Ransomware Attack Strikes Companies across Europe and US." *The Guardian*. Guardian News and Media, 27 June 2017. Web. 13 July 2017.

7. Purdue, Madeline. "How to Protect Your Windows Computer from the Petya Ransomware Attack." USA Today. Gannett Satellite Information Network, 27 June 2017. Web. 13 July 2017.

###

Media Inquiries:
Karla Jo Helms
JoTo PR

888-202-4614
www.jotopr.com