May 15, 2017

CUSTOMER UPDATE: Cyren Internet Security Detects, Blocks WannaCry Ransomware Worm Attack

Cyren also discovers file sharing services delivering WannaCry 2.0 ransomware

MCLEAN, Va., May 15, 2017 /PRNewswire/ -- Cyren (NASDAQ: CYRN), a leading internet Security as a Service provider, has issued a Customer Update for all of the company's customers and partners regarding the recent massive ransomware outbreak known as WannaCry (aka WannaCryptor, Wcrypt, and WannaCrypt). Cyren's cloud security products fully protect customers and partners from all known variants of the WannaCry ransomware delivered over email or the web.

1. Cyren customers are protected from all WannaCry variants and were protected from the initial malware outbreak by Cyren's SaaS email security gateway, web security gateway, and cloud sandboxing services.
2. Cyren Threat Intelligence Services partners are protected from all WannaCry variants and were protected from the initial malware outbreak by our OEM threat intelligence services for anti-spam, anti-malware, anti-phishing, IP reputation, and URL filtering.
3. Cyren's cloud-based platform identified and protected customers from the first early stages of the WannaCry attack. This included detection of the initial vulnerability exploit payload and classification of all related evidence of the attack in email and web, including "kill switch" IP addresses and command & control (C&C) server callbacks.
4. Cyren's cloud has identified over 300 variants of the WannaCry attack to date. Cyren's cloud automatically classifies any related indicators of the attack, and protects customers from compromised URLs that are used as droppers.
5. Cyren's cloud continues to identify infected URLs as well as malicious IP addresses and the C&C server with which the WannaCry attack communicates.
6. Cyren has identified that WannaCry is still being delivered through several file sharing services over HTTPS.
7. More details can be viewed on the Cyren blog at: https://blog.cyren.com/articles/wannacrypt-ransomware-spreads-via-nsa-exploit.html

How WannaCry Works
On Friday, May 12, a massive ransomware attack called "WannaCry" hit a broad set of organizations in Europe, including the UK National Health Service (NHS) and Spanish telecom firm Telefonica. Cyren's blog article (https://blog.cyren.com/articles/wannacrypt-ransomware-spreads-via-nsa-exploit.html) provides further detail about the attack and how it works. One of the important things to note is how the attack spreads. Traditionally, ransomware is delivered via email, but this attack appears to have added Worm capabilities to the ransomware, giving it the ability to self-propagate once inside an organisation by spreading from machine to machine using unpatched vulnerabilities in the Windows operating system. Note that, while the initial attack was stopped by a security researcher who was able to shut down a "kill switch" in the malware, new strains of the ransomware are emerging that have removed this functionality. Organizations need to take steps to make sure they protect themselves against both the initial exploit and lateral propation. See Cyren's guidance on this below.

How Customers Can Protect Themselves

- Patch Windows machines
  - Ensure that the MS17-010 security update is installed on all Windows machines within an organization. (Security Update for Microsoft Windows SMB Server (4013389).
  - This applies to older systems as well, for which Microsoft has discontinued support. For this specific attack, Microsoft has issued a patch for Windows XP, 8, and Server 2003.
  - See also: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- Disable SMBv1
  - In line with Microsoft's guidance from 2016, see: https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/, and disable SMBv1 on all Windows systems: https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
- Consider firewalling off access to all file servers
  - In January 2017, U.S. CERT recommended the following step in the wake of the release of the Eternal Blue exploit stolen from the U.S. National Security Agency by the Shadow Brokers hacking group: https://www.theregister.co.uk/2017/01/18/uscert_warns_admins_to_kill_smb_after_shadow_brokers_dump/
- Gateway email and web security
  - Ensure that all email and web security solutions are up to date and can block malicious emails and malware Command & Control server communications.

- Beware of emails containing suspicious attachments
  - Be suspicious of emails from unknown senders containing Office documents, PDFs and JavaScripts, or any other suspicious attachments.
  - Consider using a sandboxing service to identify evasive malware and zero-day threats.

About Cyren
Cyren (NASDAQ and TASE: CYRN) protects more than 600 million users against cyber attacks and data breaches through its cloud-based web security, email security, DNS security and cloud sandboxing solutions. Relied upon by many of the world's largest technology companies such as Dell, Google, McAfee and Microsoft, Cyren offers enterprise-focused security-as-a-service solutions as well as embedded solutions for software and security providers. Cyren's global cloud security platform processes more than 17 billion daily transactions and uses innovative zero-day protection technology to proactively block over 130 million threats each day. Learn more at www.cyren.com.

Blog: blog.cyren.com
Facebook: www.facebook.com/CyrenWeb
LinkedIn: www.linkedin.com/company/cyren
Twitter: www.twitter.com/CyrenInc or twitter.com/cyren_ir

Media Contact:
Matthew Zintel
Zintel Public Relations
281.444.1590
matthew.zintel@zintelpr.com

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/customer-update-cyren-internet-security-detects-blocks-wannacry-ransomware-worm-attack-300457332.html

SOURCE Cyren