SBS institute
700 S. Washington Ave. Ste. 200
Madison, SD 57042

WannaCry: Stop What You're Doing and Patch Your Computers!

Written by: Jon Waldman
Partner, EVP of IS Consulting - SBS CyberSecurity, LLC

WannaCry (also known as WannaCrypt, WanaCrypt0r, wCry, etc.) is the biggest malware event the Internet has ever seen, hands-down. And it was launched just last Friday! This version of ransomware is the prophetic fulfillment of all those fire-and-brimstone IT folks that have been saying there will be a global malware epidemic. WannaCry is being called a "weapon of mass destruction," and while that may be a bit extreme, all the "patch or perish" warnings being issued are 100% accurate.

What is WannaCry and how does it work?

The second version of WannaCry ransomware (the initial version first appeared in March of 2017) was released on Friday, May 12th. Before the end-of-business on that day, WannaCry was known to infect over 125,000 computers connected to the Internet. This particularly nasty strain of ransomware exploits a pair of zero-day vulnerabilities (ETERNALBLUE and DOUBLEPULSAR) that were first identified by the NSA and leaked by a hacking group known as "the Shadow Brokers." The vulnerabilities take advantage of SMB weaknesses (DOUBLEPULSAR) and also utilize worm-like properties (ETERNALBLUE), meaning the ransomware spreads itself automatically to any victim contacts it can find.

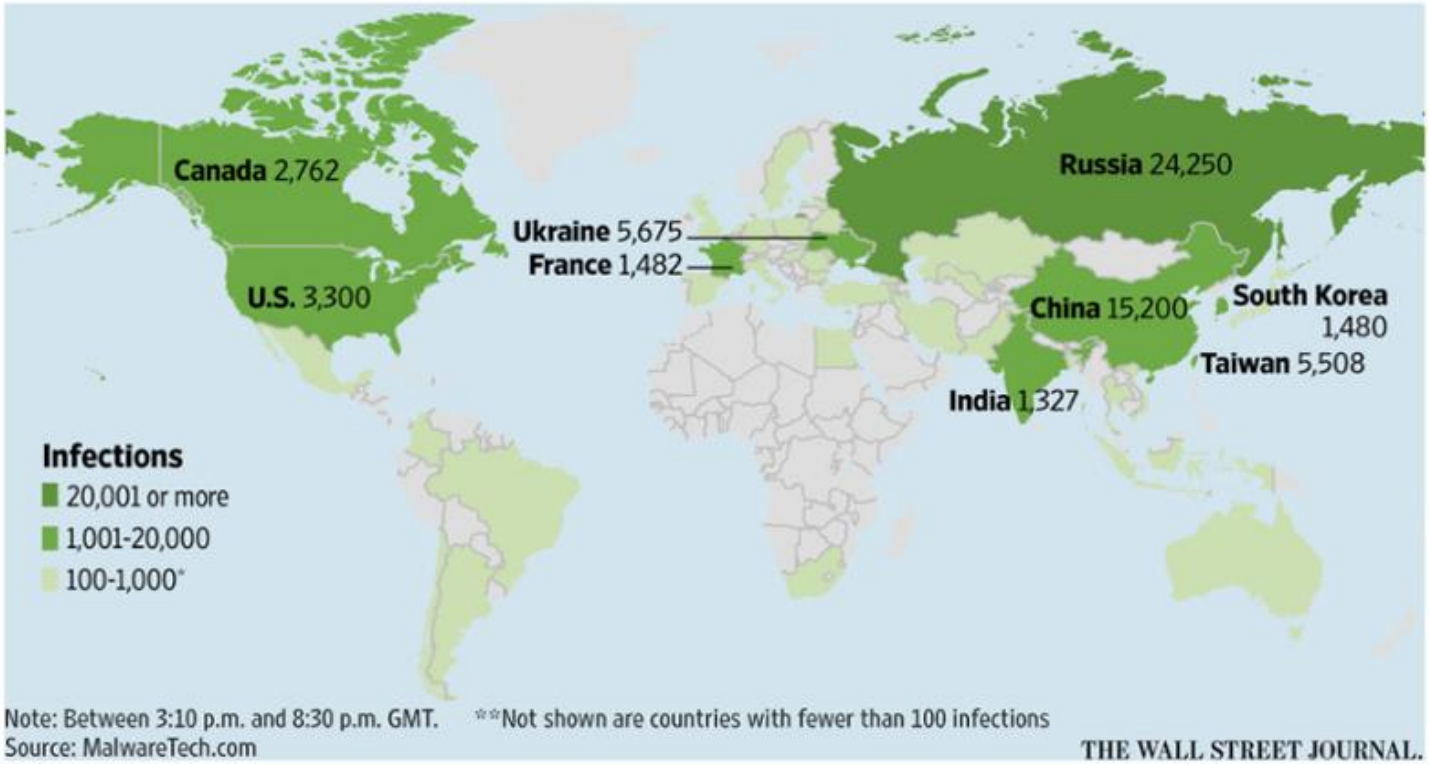
Pictured: Screenshot of WannaCry's Ransom Message

WannaCry, as with most ransomware, works by encrypting your files and demanding a ransom payment in exchange for the decryption key to your files. The ransom starts at $300 for the first 6 hours, granting the victim up to 3 days to pay the ransom before it doubles to $600. If you don't pay within a week, then the ransomware threatens to delete the files altogether. WannaCry even allows a victim to decrypt a few files to show you that you will, indeed, get your files back.

How is WannaCry delivered?

The initial distribution of WannaCry was spread through – you guessed it – phishing emails. WannaCry was disguised in a password-protected .zip file (the password is included in the email and "feels" like added security), which runs the ransomware upon execution of the .zip file.

Using the ETERNALBLUE zero-day exploit, the ransomware displays worm-like properties by scanning for open instances on port 445 to gain access to Server Message Block (SMB) protocol. It initiates an encryption routine to infect not only other hosts on the LAN but also hosts on the Internet. While ransomware and worms are not new news, the market has not seen a ransomware attack that combined those two components on this type of scale to date.



Pictured: Wall Street Journal/Malware Tech – WannaCry infections as of end-of-day on Friday

Who has WannaCry affected?

As of Monday, May 15th, WannaCry has affected over 200,000 "customers" (mostly businesses; not just hosts, but organizations or individuals) in over 150 countries, leaving many organizations unable to perform business operations. Organizations in Russia and China were among the most-severely-affected, but as of Friday, May 12th, over 3,300 US businesses were affected as well. Notable businesses affected include FedEx, Nissan, Renault, Deutsche Bahn, Russian Railways, MegaFon, Bank of China, Brazil's Social Security system, and many more.

Perhaps most concerning is the National Health Service system, the public health services provider of England, Scotland, Wales, and Northern Ireland, as upwards of forty (40) NHS healthcare institutions were affected by WannaCry. 90% of NHS institutions were primarily running Windows XP on workstations and servers, leading to surgical delays, transfers of patients, and even potentially worse outcomes.

The "Killswitch"

On Friday evening, a security researcher at MalwareTech discovered that WannaCry was attempting to avert discovery and capture. To prevent containment and capture of its code, the ransomware payload queried a certain domain name that was known to be unregistered. WannaCry was built to operate so that if a ping to this unregistered domain returned anything BUT a DNS error (signaling traffic manipulation), it would scuttle itself to avoid analysis. The security analyst that discovered this call-out in the ransomware code registered the unregistered domain to which WannaCry was calling, thus shutting down the attack inadvertently. The "killswitch" stopped the spread of the ransomware across the Internet, but shutting down the spread of the ransomware does not stop the infection if a local user opens the .zip file locally.

WannaCry Version 3

Just as soon as the WannaCry "killswitch" was discovered, a new variant appeared; this time without the killswitch. Security analysts have confirmed that the newest version of WannaCry, minus the killswitch, is propagating the Internet as you read this article. Interestingly enough, this latest version of WannaCry was not created by the same malware authors, but rather appears to be a copy-cat attack.

How to Defeat WannaCry

1. If you have not yet done so, be sure to install Microsoft's MS17-010 Security Update, which prevents WannaCry from affecting your Windows OS in the first place. Applicable to all currently-supported Microsoft Operating Systems, including Windows 10, Windows 8.1, Windows 7, Server 2008, Server 2012, etc.)
2. If you are running an older workstation or server past End-of-Life (Windows XP, Windows 8, and Server 2003), find the applicable Emergency Fix in the Microsoft Update Catalogue here: http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
3. If your organization utilizes Windows Defender, you can download updated threat definitions that allow you to detect WannaCry on a host here: https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt

4. If your files are already encrypted, a list of recovery and malware removal options can be found here: http://www.besttechtips.org/remove-wannacry-ransomware-decrypt-wncry-files/
5. If you attempted to restore from backup and failed (or you do not have backups in the first place), try a program like Shadow Explorer to see if the ransomware did not properly delete your Shadow Volume Copies. If a user did not click Yes at the UAC prompt, then there is a chance those are still available to start the recovery. Here is How to recover files and folders using Shadow Volume Copies.
6. As a last resort and all backups have failed, you could decide to pay and get the files decrypted. It appears to work.
7. Wipe any affected device and re-image from bare-metal (start from scratch).

Detect the Presence of WannaCry and SMBv1 Servers on Your Network

This section is taken directly from the KnowBe4 blog cited below but contains valuable resources. Warning: this section is technical.

One of the easiest ways to monitor what is happening on your network is to set up a SPAN\Mirror port or use a network TAP. This will give you access to flows and packet payloads so you can see who is connecting to what and if there is anything suspicious moving around. Check out this blog post if you use Cisco switches, it explains how you can monitor multiple network segments without the need to remember what is connected to what switch port. If you don't use Cisco switches, there is an excellent resource on the Wireshark wiki site which looks at how to setup monitoring on other switches.

Four things to monitor in order to detect WannaCry:

1. Check for SMBv1 use
2. Check for an increase in the rate of file renames on your network
3. Check for any instances of the file @Please_Read_Me@.txt on your file shares
4. Check for any instances of files with these extensions
    a. .wnry
    b. .wcry
    c. .wncry
    d. .wncryt

There is one caveat though, this infection moves out like lightning from patient zero, and all vulnerable machines are locked in less than two minutes, so monitoring alone would not be enough to stop this monster. Here is a video showing a machine on the left infected with MS17-010 worm, spreading WCry ransomware to the machine on the right in real time.

How Can You Stop Attacks Like These in the Future?

Ransomware attacks like WannaCry are not going to become less frequent. This new global ransomware outbreak is going to spawn more copy-cats and inspire others to get more creative with their malware. We haven't seen "the big one" yet, but this is close.

Here are a few things you can to do put your organization in the best position to defend against or respond to major attacks like WannaCry:

1. **Ensure you have a consistent, repeatable Patch Management program.** Failing to patch your workstations, servers, and devices in today's world is akin to signing your business' death warrant. Patch your devices religiously.
2. **Employ the highest quality Data Backup Program you can implement technically or financially.** Backups today are CHEAP, especially compared to the cost of being unable to recover. If you can, backup to multiple locations (having both an online and offline copy is recommended), and test your backups regularly.
3. **Deploy new-school security awareness training** using a product like KnowBe4, which includes simulated social engineering tests via multiple channels, not just email.
4. **Check your firewall configuration and monitor all outbound traffic** to make sure no criminal network traffic is leaving your network. If you do not know how to monitor your internal or outbound traffic, consider investing in a Security Information and Event Management system (managed or local).
5. **Disable and/or block SMBv1 on all machines immediately**. See this guide from Microsoft on how to disable SMBv1, and/or block SMBv1 ports on network devices, including UDP ports 137, 138 and TCP ports 139, 445.
6. If your organization does not implement a Secure Email Gateway (SEG), **consider adding SEG as an additional security layer**. Make sure your SEG is able to perform URL filtering and that it's tuned correctly to your organization.
7. **Review your Vendor Management Program.** If you utilize third parties to manage your network, host confidential customer information, or provide critical, hosted applications in the cloud, check with your vendor to discuss how WannaCry may affect their organization or the availability of your information or systems.
8. **Update your Incident Response Plan.** Make sure your Incident Response Plan has procedures for protecting, detecting, and responding to ransomware attacks. Test your IRP frequently using real-world scenarios and update your plan with new discoveries or gaps identified in testing.

How SBS Can Help

If you are looking for some additional information around cybersecurity risk management, implementing cybersecurity controls, and Information Security Programs, SBS Information Security Consultants and IT Auditors have worked with over 1500 organizations across the United States to mitigate the risk of cyber attacks. If you are not sure what to do to prevent cyber attacks or to recover from one, SBS will work with you to make the best preventative or recovery decisions possible for your organization.

Three (3) ways you can test your organization right now for cyber threats include testing your People, your Processes, and your Technology. SBS CyberSecurity is one of the largest resellers of the KnowBe4 phishing email assessment software, which helps train users on how to identify and mitigate phishing email attacks, as well as to assess that training in a low-risk, real-world phishing scenario. Learn more here: https://sbscyber.com/products/sbsknowbe4/

You can also test your network for known vulnerabilities, making sure that all patches have been implemented on your network, with a Network Security Assessment. Learn more about your options here: https://sbscyber.com/auditing/networksecuritytesting/.

Finally, you can test your processes (policy, procedure, and governance) with an External IT Audit. Learn more here: https://sbscyber.com/auditing/itaudit/

For additional information security updates or assistance with anything information security related, please visit us at www.sbscyber.com and let us know how we can help!

Sources

- https://blog.knowbe4.com/ransomware-attack-uses-nsa-0-day-exploits-to-go-on-worldwide-rampage
- https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- https://www.engadget.com/2017/04/14/shadow-brokers-dump-windows-zero-day/
- https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html
- https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
- http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/
- http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html