Petya/NotPetya
Why It Is Nastier Than WannaCry and Why We Should Care

US National Security Agency (NSA) hacker tools dumped on the dark net, based on the EternalBlue exploit,[1] are continuing to evolve into attacks increasing in frequency and severity.

In April 2017, the hacker group known as Shadow Brokers released malicious code based on the NSA tools leaked on the dark net. The exploit used the Windows Samba SMBv1 vulnerability that WannaCry ransomware exploited in early 2017, infecting more than 300,000 systems worldwide in less than 72 hours. This malware infected any Windows operating system running an unpatched version of SMBv1 services. Telecommunications industries and the Industrial Internet of Things (IIoT) have been particularly vulnerable as often these disciplines use an older version of Windows to control their devices and networks. As was also seen in academic environments and hospitals, there are many older Windows operating systems connected to these networks, which are still not patched, still connected to their enterprise's network and still running this service.

F. Charlene Watson, CISM, CEH, ECSA, A+, Network+, Security+
Is a network architect with a concentration in cyber security. She has more than 30 years of combined experience in public safety and protection of people and information.

A major concern with the last round of ransomware attacks was the fact that the attackers are learning and evolving. In the case of WannaCry, the malware copies itself onto a remote machine under the path C:\Windows and uses rundll32.exe to start itself. The rundll32.exe program stands for "run DLL," meaning that it tells Windows to "run this DLL as an application (app)." It is a program code in the Windows operating system that is used to run other program codes in DLL files as if they were actually within or a part of that particular program.

While the rundll32.exe is a legitimate Microsoft program, black hat hackers name their processes the same file names as legitimate Windows programs to avoid detection (e.g., file.net). According to Palo Alto researchers, "This variant of Petya is spread *as* a DLL file," (emphasis added) rather than *using* one to copy itself, "which must be executed by another process before it takes action on the system. Once executed it overwrites the master boot record and creates a scheduled task to reboot the system. Once the system reboots," the malware encrypts "the New Technology File System (NTFS) master file table in the background" using the chkdisk command.[2] This is what is so devastating. Instead of encrypting files one at a time or a few at a time, it encrypts the entire master file table (MTF) and obliterates the master boot record (MBR), rendering it useless.[3]

What was different about this latest round of ransomware attacks is that even if a system was patched, it could still have possibly been compromised. One researcher confirmed, "Petya uses EternalBlue exploit, but also spreads in internal networks with WMIC and PSEXEC. That's why patched systems can get hit."[4]

The reason Petya/NotPetya spread so fast in the summer of 2017 is that it used two types of attack vectors, or a two-pronged attack: the network side and the client side. The client-side exploit is based upon the zero-day vulnerability in Microsoft Office and affects all versions of Microsoft Office, including Windows 10. According to Microsoft's security

updates released in April 2017, the "vulnerability exists in the way that Microsoft Office and WordPad parse specially crafted files. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change or delete data; or create new accounts with full user rights."[5] Baited Word documents were delivered to victims as attachments in emails. When users clicked on them, they were breached.

The network attack approach made use of the SMBv1 exploit, which allowed "remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server,"[6] which was the source of pain and suffering from the wildfire spread of the WannaCry attacks in early 2017. On the network side, it appeared that Petya/NotPetya used Active Directory's LSADump to get the administrative password and infect the entire network.[7] In a summary of an attack, one blogger relayed that even with the MS17-010 patch, an enterprise can be hit:

> *…the Trojan collects the locally stored Windows login credentials and misuses them with the PSEXEC tool. This is just a regular tool, usually used by system admins, to run other tools on remote machines they have regular access or logins to. This method works even if the system is fully patched as PSEXEC is not an exploit but a regular tool from Microsoft and SysInternals.*[8]

Another blog post noted that the machine attacked was a "Windows 10 Enterprise 64bit running McAfee AV + Encrypted HDD. Fully patched with June's updates and manually disabled/removed SMBv1."[9] And a third blogger noted that "even patched OS won't save you from infection as one infected machine quickly spreads the infection using other protocols like WinRM."[10]

An image of the spread of the malware can be seen in **figure 1**. It has been modified to take into account newer information that was discovered from many other sources since the attack occurred. Analysis is still ongoing by experts.[11]

As of this writing, the attack mostly appears to have been limited to affecting enterprises in Europe. However, it is beginning to creep into the United States. According to one security expert, the "global law firm DLA Piper has experienced issues with its system in the U.S. as a result of the outbreak."[12]

The Solution—Top Down/Bottom Up

Before discussing how to address this kind of attack, it is worthwhile to review:

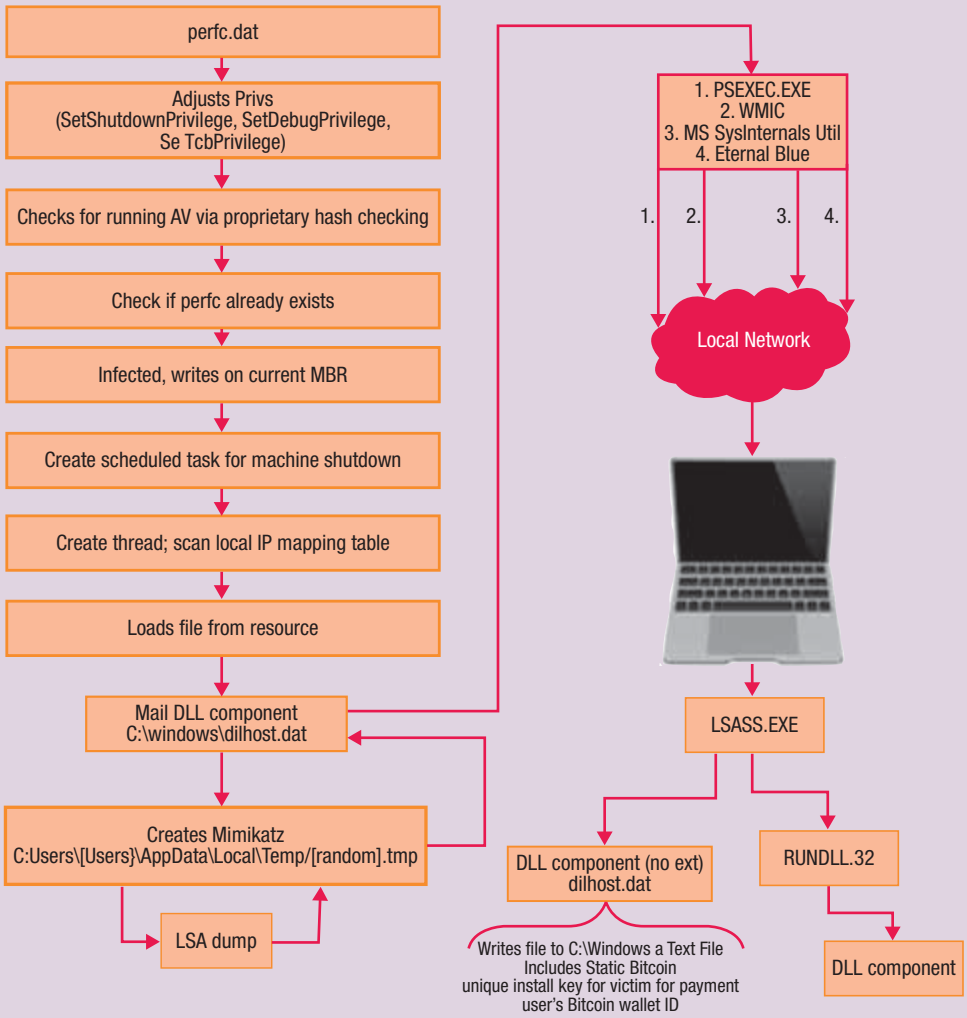
> *The top-down and bottom-up risk scenario development approaches are complementary and should be used simultaneously. In a top-down approach, one starts from the overall business objectives and performs an analysis of the most relevant and probable risk scenarios impacting the business objectives. In a bottom-up approach, a list of generic risk scenarios is used to define a set of more concrete and customized scenarios, applied to the individual enterprise's situation.*[13]

When evaluating and responding to these types of threats, which will now continuously be faced, it is important now more than ever to put this holistic concept into practice while learning to stay cyberresilient in the digital world. Taking this approach then, the following sections examine the practical application of these two important concepts.

Bottom Up

Patch, patch, patch. Also, with the LSADump issue, blocking all domain administrators from logging on to workstations might be prudent. However, this will not help if a compromise actually comes via the server. Also, running antimalware and antivirus software is a must. Too often, enterprises forget about these basic principles of protection.

Figure 1—Two-Pronged Attack



Another overlooked option, according to one blogger: "…also worth reconsidering having a single antivirus (AV) solution on both PCs and servers."[14] Additionally, users should be instructed that if their machine reboots and they see the chkdisk message stating that it is "Repairing the file system on C:," they should power off immediately, disconnect from the network, and use a LiveCD or an external machine/connection to recover any files that may still be accessible if it was caught in time.[15] And for the good of the entire digital ecosystem, stop running SMBv1.

Top Down

As society moves into this new age of digital counterinsurgency, C-suites, senior leadership and all the major stakeholders who possess the power of the checkbook need to take a seat at the table and educate themselves on a top-down/bottom-up governance approach to due diligence in terms of an enterprisewide cyber security/risk management framework. This will take time and resources—both people and infrastructure. Using the US National Institute of Standards and Technology (NIST)

Cybersecurity Framework (CSF) as a reference, one of the very first tasks is asset management. "When it comes to tackling the security of connected devices, administrators in and outside the security suite need to think (fast) about asset management. You can't protect what you don't know. Version management layers on top of this, allowing systems administrators to understand what they have and what needs attention."[16] Software that is used for searching, monitoring and analyzing big data that is machine-generated, along with asset management software, to determine what is connected to the network at all times is no longer a nice thing to have. It is imperative. And C-suites, senior leadership and all major stakeholders are going to have to come to the table to begin supporting these basic, digital cyberresiliency measures.

It can be overwhelming to keep enterprise networks up 24/7 while keeping them safe from attackers at the same time. Adding to these growing threats is the approaching 31 December deadline for NIST SP 800-171 compliance by most US government contractors and private companies affected by the US Defense Federal Acquisition Regulation Supplement ruling in October of 2016.[17] This has created the perfect storm for cyberfatigue, i.e., the "sense of resignation, loss of control, fatalism, risk minimization, and decision avoidance," in dealing with cyber security decisions.[18] It becomes so easy then to give up and quit. With this, combined with the latest leaks of gizmo codes and gadgets via cybercriminals, it is no wonder many security engineers, professionals and C-suite executives feel discouraged and pessimistic. Yet there is hope.

Implementation of the NIST CSF using COBIT® 5 is a great place to start. Using ISACA's Auditing Toolkit Cybersecurity: Based on the NIST Cybersecurity Framework,[19, 20] one can see where initiating just five security controls can have a significant impact:

1. Application white listing
2. Using standard, secure systems configurations
3. Patching application software for zero-day exploits
4. Patching system software for zero-day exploits
5. Reducing admin privileges

Take a look at number two, using standard, secure, systems' configurations. Per ISACA's Auditing toolkit:[21]

1. Determine if the organization has created or adopted baseline configurations (e.g., Center for Internet Security [CIS] benchmarks, Security Technical Implementation Guides [STIG]) for systems (e.g., servers, desktops, routers).
2. Sample systems against the organization's baseline configurations to ensure standards are followed and enforced.

> **"It was a nasty little piece of malware that was brilliantly designed to inflict the greatest possible damage in the shortest amount of time."**

Many of the machines/systems that were compromised in this attack were running varieties of the Windows operating system. There was everything from Windows XP to Windows 10 and Server 2003 to 2016, many of which were connected on a flat network. It was a nasty little piece of malware that was brilliantly designed to inflict the greatest possible damage in the shortest amount of time, taking advantage of the fact that if there is only one single machine on the victim's network that is not managed/configured properly and is the weak link in the chain of connected devices, it will use that one single device to spread itself to all other devices.

The Future—Why This Matters

The final point at issue is that, while hitting enterprise operations is destructive enough to the

global digital economy, the fact that this is hitting several power grid networking infrastructures in Ukraine is the most disturbing. "The attack has even affected operations at the Chernobyl nuclear power plant, which has switched to manual radiation monitoring as a result of the attack. Infections have also been reported in more isolated devices like point-of-sale terminals and ATMs."[22]

These issues, combined with the attack being on the heels of the release of information regarding the CrashOverride malware, which was specifically engineered to attack supervisory control and data acquisition (SCADA) systems, make this issue particularly alarming.[23] With all of these serious cyberthreats and concerns beginning to aggregate, and a global economy's and society's dependency on all things digital, if this does not scare executive and government leaders into becoming more educated regarding all things cyber, then unless there is human life lost, and those ignoring these issues suffer financial pain because of the loss of life, not much will change. And this then, is the reason why it is important to care about this latest round of malware attacks.

> **"A coffee pot connected wirelessly to an enterprise network can be the vector of infection for systems that are not cared for or properly patched."**

Many of a nation's industrial control systems will far outlive the operating systems that control their human machine interfaces. This means that a coffee pot connected wirelessly to an enterprise network can be the vector of infection for systems that are not cared for or properly patched. Hopefully, to quote a recent blog post, "Maybe now we will get some real traction in the security space and be able to protect ourselves better in the future."[24]

Endnotes

1 Microsoft Corporation, Security Update for Microsoft Windows SMB Server (4013389), Microsoft Security Bulletin MS17-010—Critical, 14 March 2017, *https://technet.microsoft.com/en-us/library/security/ms17-010.aspx*

2 Howard, R.; "Threat Brief: Petya Ransomware," 27 June 2017, Palo Alto Networks blog post, *https://researchcenter.paloaltonetworks.com/2017/06/unit42-threat-brief-petya-ransomware*

3 Khandelwal, S.; "Petya Ransomware Spreading Rapidly Worldwide, Just Like WannaCry," *The Hacker News*, 27 June 2017, *http://thehackernews.com/2017/06/petya-ransomware-attack.html*

4 Hypponenm, M.; "@mikko," Twitter, 27 June 2017, *https://twitter.com/mikko/status/879742221326721028*

5 Microsoft Corporation, Microsoft Security Update Guide, 11 March 2017, *https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199*

6 *Op cit*, Microsoft Corporation, Security Update for Microsoft Windows SMB Server (4013389)

7 Group-IB, 27 June 2017, *https://twitter.com/GroupIB_GIB/status/879772068300165120*

8 Avira, "Petya Strikes Back," 28 June 2017, *https://blog.avira.com/petya-strikes-back/*

9 Jeff; "View of Someone Who Was Impacted by Petya," Traffic-Analysis, Analyzing Traffic, *https://www.traffic-analysis.co.uk/2017/06/view-of-someone-who-was-impacted-by-petya/*

10 Bojko, M.; "Petya(notPetya) Ransomware Attack and How to (Auickly) Vaccinate Lots of Machines," 1 July 2017, *https://marcinbojko.wordpress.com/2017/07/01/petyanotpetya-ransomware-attack-and-how-to-quickly-vaccinate-lots-of-machines/*

11 McAfee Enterprise, "New Variant of Petya Ransomware Spreading Like Wildfire." 27 June 2017, *https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire*

12 Krebs, B.; "'Petya' Ransomware Outbreak Goes Global," Krebs on Security blog post, 27 June 2017, *https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/#more-39734*
13 ISACA®, *CRISC Review, Questions & Explanations Manual, 4th Edition*, 2015, USA, p. 41
14 Collin, S.; "Petya.A Infection—Summary of Events," 28 June 2017, *http://webcache.googleusercontent.com/search?q=cache:mZ_PKcMM1cEJ:colsec.blogspot.com/2017/06/petyaa-infection-summary-of-events.l%3Fview%3Dflipcard+&cd=1&hl=en&ct=clnk&gl=us*
15 *Op cit*, Khandelwal
16 Bone, J.; "Ransomware Attacks Accentuate Need for Asset Management," *ISACA Now* blog post, 28 June 2017, *www.isaca.org/KnowledgeCenter/Blog/Lists/Posts/Post.aspx?ID=821*
17 US Defense Acquisition Regulations System, Department of Defense, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)*, 21 October 2016, *https://www.federalregister.gov/documents/2016/10/21/2016-25315/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for*
18 Stanton, B.; M. F. Theofanos; S. Spickard Prettyman; S. Furman; "Security Fatigue," *IT Professional*, vol. 18, iss. 5, September-October 2016, p. 26–32
19 ISACA, *Cybersecurity: Based on the NIST Cybersecurity Framework*, January 2017, *https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx*
20 ISACA, *Implementing the NIST Cybersecurity Framework*, August 2014, *https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx*
21 *Op cit,* ISACA 2017
22 Brandom, R.; "A New Ransomware Attack Is Infecting Airlines, Banks, and Utilities Across Europe," *The Verge*, 27 June 2017, *www.theverge.com/2017/6/27/15879480/petrwrap-virus-ukraine-ransomware-attack-europe-wannacry*
23 Dragos Incorporated, *Crashoverride: Analysis of the Threat to Electric Grid Operations*, industry report, 12 June 2017, *https://dragos.com/blog/crashoverride/CrashOverride-01.pdf*
24 *Op cit*, Collin