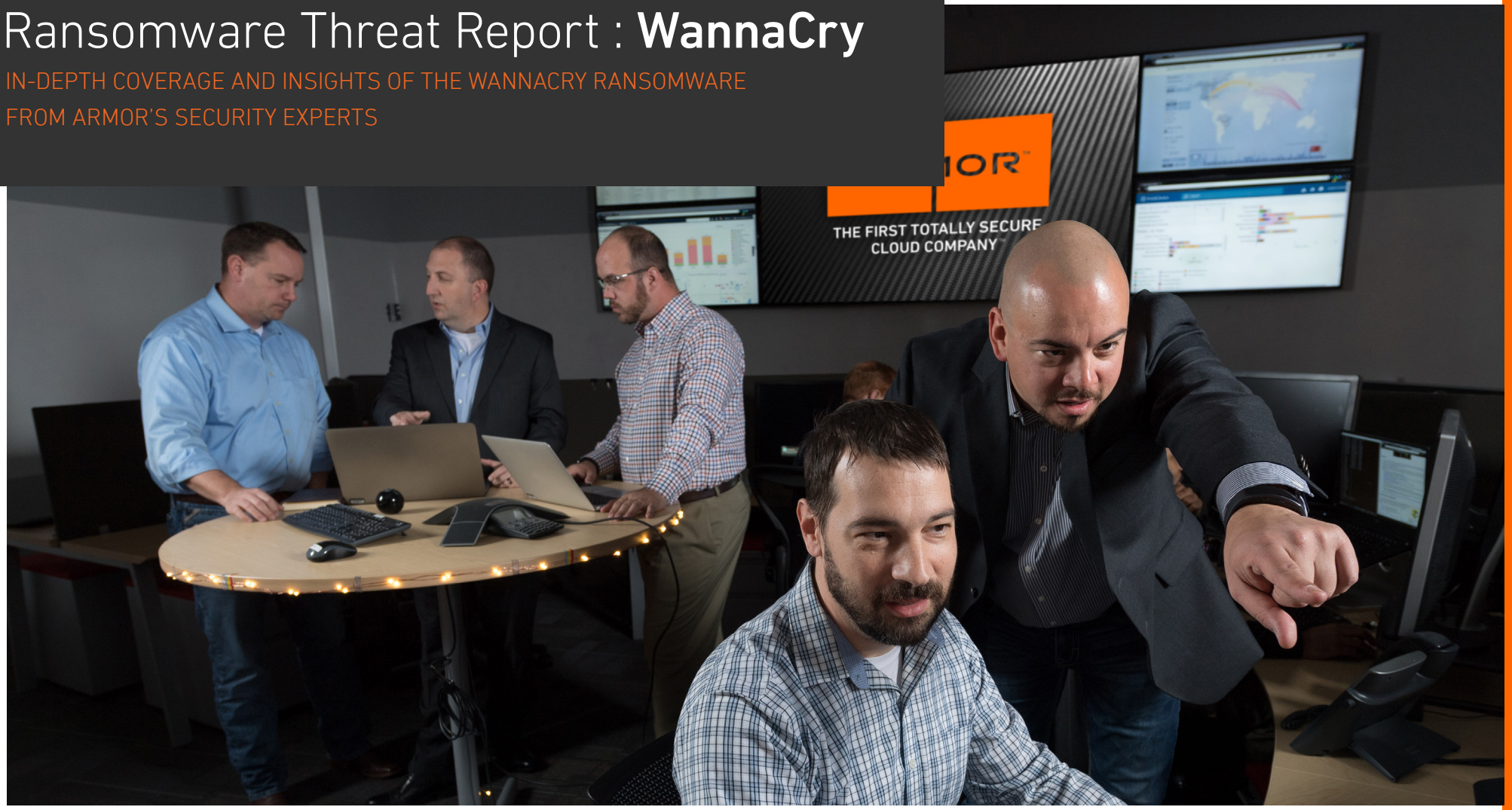
Ransomware Threat Report : **WannaCry**

IN-DEPTH COVERAGE AND INSIGHTS OF THE WANNACRY RANSOMWARE
FROM ARMOR'S SECURITY EXPERTS



Foreword from

Jeff Schilling CISM | Armor

Cyber insurance providers are always looking for that litmus test on how to judge if an organization seeking insurance is serious about their security program. I am going to say it bluntly — if an organization had significant business impact due to the WannaCry Ransomware operation, they were negligent in conducting security operations. This Microsoft flaw was big news back in March when the Shadow Brokers leaked the alleged stolen nation-state actor tools that took advantage of this flaw. This Microsoft flaw affected just about every operating system to include both user workstations and servers. Microsoft informed the world that this was a critical flaw and should be patched as soon as possible.

Fast forward three months later — we now have potentially more than 400,000 infected hosts in more than 124 countries.

What happened? Were people just not listening?

As I look at the media coverge, a lot of the dire predictions and headlines read something along the lines of: "The World has been Hacked." Let's step back from the hysteria and dissect what really happened late last week.

First, I was surprised that it took a threat actor more than three months to weaponize this flaw. Normally when zero day flaws are released in the wild, it only takes about 48 hours before we see threat actors using it to exploit systems. I was grateful that we had this extended amount of time to get our systems patched and also ensure we scanned our customer environments to see if they were vulnerable.

Why was this WannaCry campaign so successful?

Two root causes can be attributed to the success of this campaign. Both are a reflection of an organization's commitment to cyber security.

Many companies don't run a good patching program to ensure their systems are updated with the latest fixes for security flaws. It can take a company anywhere from 90-days to more than a year to

patch critical vulnerabilities like the one leveraged for WannaCry. When you look back at some of the biggest data breaches over the last five years, almost all of them involved vulnerabilities that were more than a year old when the company was breached.

Organizations are making the conscious decision to not make the investment to update unsupported software. According to most reports, a great majority of the WannaCry victims are using Windows XP, which has been an unsupported operating system for three plus years. This means Microsoft was not obligated to provide a security patch for these systems. After the outbreak hit late last week, Microsoft stepped up to provide a patch now for unsupported systems. Having unsupported software in your environment will make you non-compliant with many auditing standards, such as PCI and HIPAA, which is why many major US companies weren't affected by the outbreak.

Both root causes, poor patching programs and allowing unsupported software in corporate environments, are indicators of a poor cyber security program.

The sad state of cyber security readiness

In short, WannaCry demonstrates the vulnerability of systems and how in relative short order, this infrastructure can be compromised on an unprecedented global scale with the headlines to show for it. It also shows the critical importance of establishing a diligent patching program to thwart these attacks. The world knew something like WannaCry could be coming months ago and software companies addressed the issue with a viable patch. The onus was then on organizations to utilize the resources to keep their infrastructure safe. Which, unfortunately didn't happen in many cases.

So, for those looking for the litmus test of a cyber readiness of an organization, there's an ideal example with WannaCry, and it does make me "want to cry" at the sad state of our global cyber security readiness.

Jeff Schilling CISM | Armor

What is **WannaCry**?

WannaCry (also known as WCry or WannaCrypt) is a ransomware variant that targets Microsoft operating systems. It specifically exploits vulnerabilities in machines that are unpatched against the several tools released by the threat actor group known as the "Shadow Brokers."

As of the date of publication, the attack has affected more than 400,000 computers in nearly 150 countries, despite patches provided by Microsoft three months prior to WannaCry's release on May 12, 2017.

Despite the large number of affected systems, the ransomware has reportedly only earned $100,000[1] in paid ransom.

Notable victims of WannaCry include:

- **The UK's National Health Service (NHS)**
- **Spain's Telefonica**
- **FedEx**

Who is at risk?

While WannaCry targets all unpatched Microsoft computers, those hardest hit were organizations maintaining legacy operating systems (e.g. Windows XP and any previous Windows OS). Due to Microsoft ending support for these OSs, they are prime targets for threat actors. In addition to patching any currently supported OSs, we highly recommend transitioning business critical services away from legacy systems.

What is **Ransomware**?

As one of the most prolific forms of malware today, ransomware wreaks havoc by encrypting its victim's data and holding it hostage for a fee (typically paid in bitcoin). While its delivery methods are nothing new - a malicious file or phishing email - its profitability is what truly sets it apart from other malware variants. More than $200 million was paid out in Q1 2016 alone. In 2015, ransomware was responsible for more than $1 billion in losses.

How to deal with ransomware

The best defense to ransomware is being proactive. Every team should have clear plans around system snapshots and data backup. It is equally as important to have a regular scanning and patching routine. When it comes to activities after you've been breached; restoring from a readily available backup is the best way to counter this threat.

However, without one, your options are limited: Hope there's a unlocker tool available for your ransomware, or pay the ransom – something that Armor and the FBI actively discourage

6 Steps for Dealing with Ransomware

1. **Back up your data.** This is the most important and effective way to minimize the risk of ransomware. Backups should be done at regular intervals and stored offline and offsite, if possible, to prevent the infection from spreading. Backups should be retained for more than 45 days, and backup restoration procedures should be frequently tested. While this won't prevent an infection, it will allow you to recover quickly.

2. **Update OS and software.** Keeping your software and operating systems up to date can minimize exploitable vulnerabilities. Eliminating easy access for threat actors.

3. **Use your antivirus**. Use an updated modern antivirus solution such as Trend, Kaspersky, Avira, Avast or Bitdefender. Many of these offer more than just antivirus, so find a solution that works for your environment.

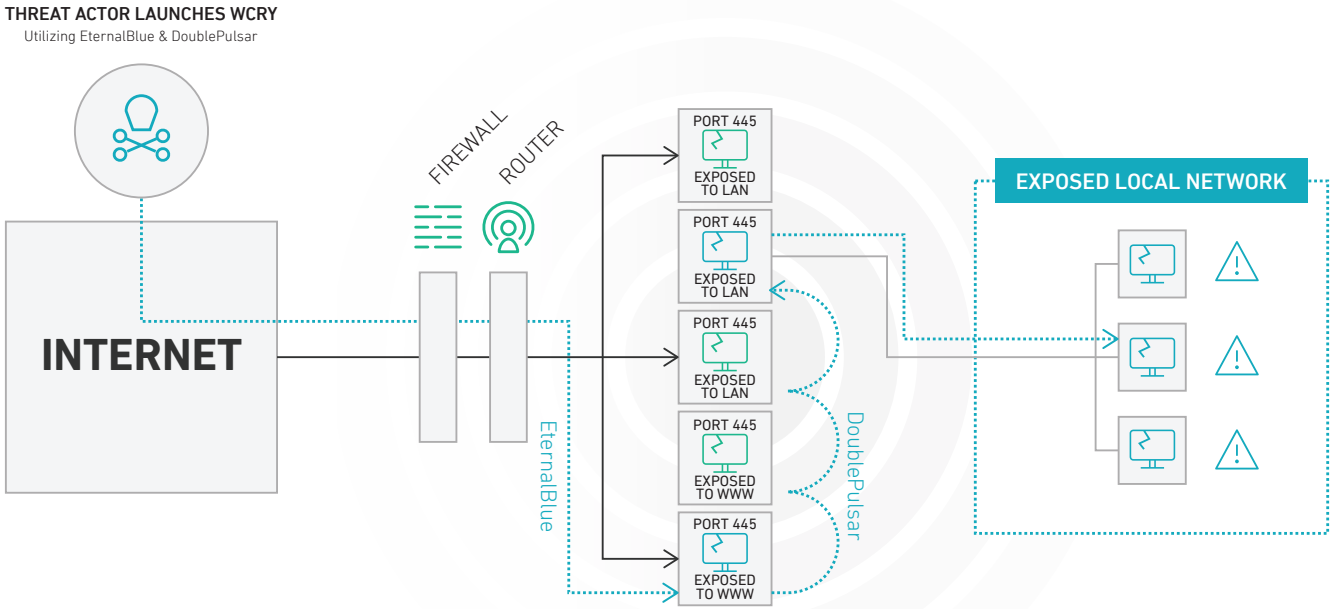
4. **Guard against phishing.** Cyber criminals love to send out tainted attachments in emails that look legitimate. Make sure your antispam settings are adjusted to catch as many fake emails as possible. Also, don't skimp on user awareness training. You can never be too cautious when it comes to spotting suspicious attachments or links from unknown senders.

5. **Assess.** Try to determine the name of the ransomware as there are freely available tools to decrypt some of the older versions. nomoreransom.org is a great resource for unlocking tools and information about ransomware.

6. **Notify.** Ransomware attacks should be reported to your local law enforcement. Unfortunately, less than 25% of ransomware attacks are reported. By reporting this crime, you help with the apprehension of the cybercriminals and, hopefully, prevent others from being affected. Please refer to the Report a Crime page from No More Ransom to determine the appropriate law enforcement agency

How WannaCry spreads

WannaCry propagates by scanning for new hosts through **TCP port 445,** which handles Server Message Block (SMB) network communications (i.e. file sharing). Once it's found a vulnerable system, it can utilize two of the Shadow Brokers' leaked tools, **ETERNALBLUE** and **DoublePulsar** to access and encrypt its victim's data.



Once infected, the computer displays a pop up window with instructions for paying the ransom, an initial fee of $300, and two countdown clocks:

- **A three-day deadline** before the ransom increases to $600
- **A seven-day deadline** until your data is deleted and unrecoverable

Interestingly enough, none of those who have paid the ransom have had their data unlocked.

Which is why, with all ransomware, paying the ransom is not always the best option – and there is never a guarantee that your data will be returned. Patching your OS and restoring from a backup is the best way to thwart ransomware. However, if no backup is available, payment may be your only option, unless you can tolerate potentially losing the data forever.

This is a decision that only your organization can make and is one that can't be made lightly. Simply paying the ransom with consideration of the risks only further incentivizes threat actors to pursue ransomware attacks.

How do you defend against WannaCry?

The good news of this is that these vulnerabilities are not zero-day exploits. Patches for these vulnerabilities were released prior to Shadow Brokers releasing these tools and are available to apply to any potentially affected system.

To protect your systems, we suggest you take the following steps:

- **Block ports** 139 and 445 TCP from public access ASAP.
- **All Windows-based systems need to be patched**. Reference Microsoft bulletin MS17-010 for critical vulnerabilities and updates: https://technet.microsoft.com/library/security/MS17-010
- **Disable SMBv1 is not required**, reference this article to disable it: 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
- **Isolate all legacy systems**, e.g., Windows Server 2003, Windows XP, Vista.

Additional guidance for Microsoft Azure customers

Microsoft recommends some additional steps for Azure customers when preventing WannaCry, as outlined on the Microsoft Azure blog[2].

- **Patch your Microsoft system**. Azure customers should immediately install MS17-010 to resolve this vulnerability, which exploits Service Message Block (SMB) vulnerability (CVE-2017-0145).
- **Review SMB endpoints**. Assess all Azure subscriptions that have SMB endpoints exposed to the internet, commonly associated with ports TCP 139, TCP 445, UDP 137, UDP 138. Microsoft recommends against opening any ports to the internet that are not essential to your operations.
- **Utilize Windows Update** to keep your machines up-to-date with the latest security updates.
- **Use Network Security Groups** (NSGs) to restrict network access.
- Confirm that **malware protection is deployed and updated**.
- Configure backups with **multifactor authentication**.

How Armor Responded to WannaCry

Armor had previously identified the root vulnerability that enabled WannCry's spread. Through active managed protection, we worked to ensure proper patching and configuration changes were enacted. As a result, **none of our customers have been affected with the ransomware to date**. In the event a customer was compromised, Armor's included **14-day environment snapshot** would have allowed for recovery through a rollback.

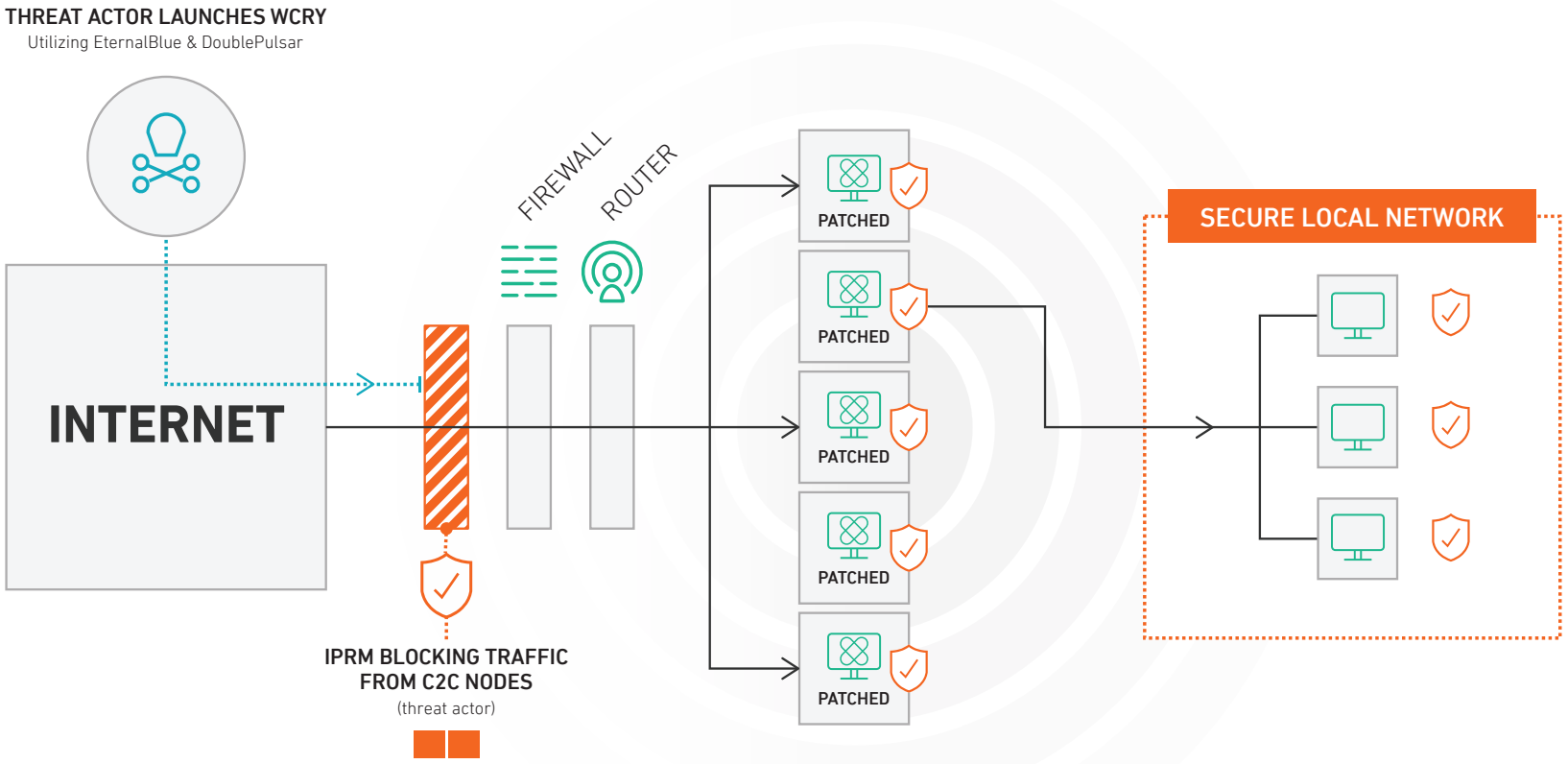
The timeline below outlines our responses to the Shadow Brokers' leak, the emergence of WannaCry and what's next.

- Provided patches for our customers, or awareness that they needed to patch for vulnerabilities
- Scanned our customer environments for potential vulnerabilities
- Provided malware protection to block the ransomware from being successful
- Developed customer signatures for intrusion detection based off on threat research

- Ensured that command and control nodes were blocked by Armor security stack

How Armor Protected against the spread of WannaCry

With all vulnerable systems previously patched, our security stack easily blocked WannaCry's intrusion methods. Additionally, our **IP Reputation Management blocked traffic from C2C nodes** distributing WannaCry for an added layer of protection against the ransomware.



Patch Management Checklist

Our biggest piece of advice for safeguarding yourself from all cyber threats, not just ransomware: **Don't suck at patching!**

Use the printable checklist below to ensure your organization follows patch management best practices, based on the National Institute of Standards and Technology (NIST) framework[2].

- ☐ **Inventory -** Assess your organization's IT resources and create an inventory of hardware, operating systems and software.
- ☐ **Monitor -** Continuously monitor security sources (see subscription sidebar) for vulnerability announcements, patch and non-patch updates as well as emerging threats corresponding to the inventoried software.
- ☐ **Prioritize -** Prior to acquiring, test and deploying new patches, determine the order of priority of patchable systems based the severity of identified vulnerabilities and performance impact.
- ☐ **Test -** All patches should be tested with standardized configurations similar to production environments. Monitor performance during testing to ensure the patch does not negatively affect the environment.
- ☐ **Deploy -** If the patch does not negatively affect your environment, install it across all identified and prioritized systems.
- ☐ **Distribute -** Notify all local administrators about vulnerabilities and remediations that correspond to software packages.
- ☐ **Automate -** Patches should be deployed automatically to IT devices using enterprise patch management tools. This allows an administrator to update hundreds or even thousands of systems from a single console – simplifying deployment in the presences of homogeneous computing platforms, with standardized desktop systems and similarly configured servers. Multiplatform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations may also be integrated.
- ☐ **Configure -** Utilizing automatic application update features in many newer applications can minimize the work required to identify, distribute and install patches. If this interferes with the organization's configuration management process, a locally distributed automated update process is recommended.
- ☐ **Verify -** Confirm that that the patches have been deployed and all targeted vulnerabilities remediated.
- ☐ **Train -** Administrators should be trained regarding how to apply vulnerability remediations.

Patch Subscription Services

The following resources can help ensure that each part of your network has the most up-to-date patches.:

- **United States Computer Emergency Readiness Team**
- **Microsoft Technet**
- **Red Hat Security Updates**
- **Oracle Critical Patch Updates, Security Alerts and Third-Party Bulletin**

The Importance of Patching

It's no stretch to say that WannaCry's impact would have been significantly less if more organizations maintained an effective patch management program.

Microsoft provided a patch for the vulnerabilities exploited by the ransomware months before its emergence. Had the impacted organizations performed routine vulnerability scans and assessed the threat of the Shadow Brokers' leak, they likely would not have been infected – limiting the profitability and spread of WannaCry.

Next Steps in the Fight Against WannaCry

We are actively monitoring the progress of WannaCry – and recommend you do so as well. At the time of publication, there were 452 variants of the ransomware reported. Systems with up-to-date patches and secured with the steps outlined in the prevention section of this white paper, should be protected against infection.

However, with the situation rapidly evolving, staying ahead of the threat is a necessity. The following resources are your best means of observing WannaCry's progress and ensuring that your critical systems are secure.

Information from Microsoft:

- *Information and patches*
- *How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server*

Overview of WannaCry:

- *Introduction to WannaCry*
- *Technical details*
- *Breakdown of tools in the Shadow Brokers' leak*

Sources:

[1] Inside the digital heist that terrorized the world-and only made $100k Keith Collins - https://qz.com/985093/inside-the-digital-heist-that-terrorized-the-world-and-made-less-than-100k/

[2] WannaCrypt attacks: guidance for Azure customers https://azure.microsoft.com/en-us/blog/wannacrypt-attacks-guidance-for-azure-customers/

[3] Creating a Patch and Vulnerability Management Program. Peter Mell, Tiffany Bergeron and David Henning. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf