CYLANCE™

WannaCry

Business Brief

Additional Help from Cylance®

Been Hit By WannaCry Ransomware?

If you've never dealt with ransomware before, it can be a long process. Let us help to simplify and streamline the process of remediating and restoring access to your data. Cylance has a full set of consulting services designed to contain an outbreak or provide incident response capabilities to minimize any impact of the WannaCry Ransomware.

Want To Be Sure You Haven't Been Breached?

Contact us to learn about how we provide peace of mind in the form of true threat prevention.

What Is WannaCry?

First detected on Friday, May 12, 2017, and still ongoing, the most recent worldwide threat dubbed WannaCry (aka WannaCrypt, WCry, WanaCrypt0r 2.0, or Wanna Decryptor) is an example of yet another ransomware variant. WannaCry Ransomware leverages a vulnerability within Windows operating systems and uses an exploit called EternalBlue to automatically target and propagate itself to vulnerable Microsoft Windows operating systems across the Internet. The EternalBlue exploit is reportedly just one of the tools believed to have originally belonged to the National Security Agency (NSA) that was stolen and dumped by the group who call themselves The Shadow Brokers.

Victims of WannaCry are impacted when they click on a phishing email that delivers a .zip file disguised as a fake invoice, job offer, security warning, undelivered email, etc. Once the infection takes place, it encrypts its victim's files using the AES cipher and demands a ransom that increases in value as time passes. In this case, WannaCry demanded payment ranging from $300 to $600 in bitcoins.

WannaCry is one of the largest reported attacks to ever impact businesses and governments around the world.

Who Was/Is Affected?

WannaCry infected thousands of endpoints, and some very high-profile targets were hit. Most notably and most reported, the U.K.'s National Health Service was torpedoed by the ransomware and forced to put life-saving surgeries on hold. Spanish telecom provider Telefonica sent employees home after the infection tore through its offices on Friday, May 12, 2017. Russia's Ministry of Internal Affairs reported more than 1,000 infections. Germany's rail system was also hit with WannaCry's ransom message appearing on train station pay terminals.



Figure 1 — Message that WannCry victim sees when data is encrypted.

This attack affected users running all versions of Windows, even older unsupported Windows XP. Although a patch to remove the underlying vulnerability for supported systems (for Vista and later systems) had been issued on March 14, 2017, delays in applying security updates and a lack of support by Microsoft of legacy versions of Windows left many users vulnerable. Due to the scale of the attack, to deal with the unsupported Windows systems, and to contain the spread of the ransomware, Microsoft has taken the unusual step of releasing updates for all older unsupported operating systems from Windows XP onwards.

The one stroke of good luck in this outbreak of WannaCry came from the actions of a UK-based researcher, going by the name MalwareTech, who shut the operation down by recognizing that one of the domains used by the attackers hadn't been registered. It turns out that if the domain was unregistered and inactive, the query would have no effect on the ransomware's spread. But once the ransomware checked the URL and found it inactive, it shut down the service. This kill switch functionality was likely put in place as an intentional kill switch, in case the creators ever wanted to rein in the monster they created.

So, MalwareTech registered the domain, took control of the site for $10.69 and started seeing connection from infected victims, and ultimately could track and slow down the ransomware's spread. However, WannaCry included features designed to detect security tools that would fake Internet access for quarantined PCs by using a single IP address to respond to any request the computer made, so it made protection very difficult with traditional signature-based AV.

Predictive Prevention Pays Off — How Cylance Can Help

The power of artificial intelligence and machine learning truly pays off in this case. CylancePROTECT® fully prevents all in-the-wild examples of the malware related to these specific attacks. WannaCry is prevented *before* it can execute, even when offline, requiring no cloud lookups, no custom or manual blacklist entries, and while using CylancePROTECT's default configuration.

In fact, customers who had deployed CylancePROTECT with AI models created all the way back in November 2015 are still protected from WannaCry. Even before the threat/exploit was known to exist, the AI security models were preventing it, illustrating the incredible capabilities of truly predictive, AI based endpoint security.

One of the very real, human benefits of deploying CylancePROTECT, is the peace of mind it provides to security operations teams. An example of this very real benefit can be seen in that our own Cylance Security Operations team did not lose their entire weekend to deal with this global threat. Knowing they were fully protected across the entire environment allowed them to monitor the situation without the need to go into full rapid response mode as many organizations were faced with because they relied on legacy, signature-based antivirus.

For older Windows XP systems, CylancePROTECT provides complete support and protection from WannaCry to ensure legacy systems, as well as all new versions, are secure.

#WannaCry Timeline

What Happens When the Hash Changes?
Or, the Hack Method Changes?

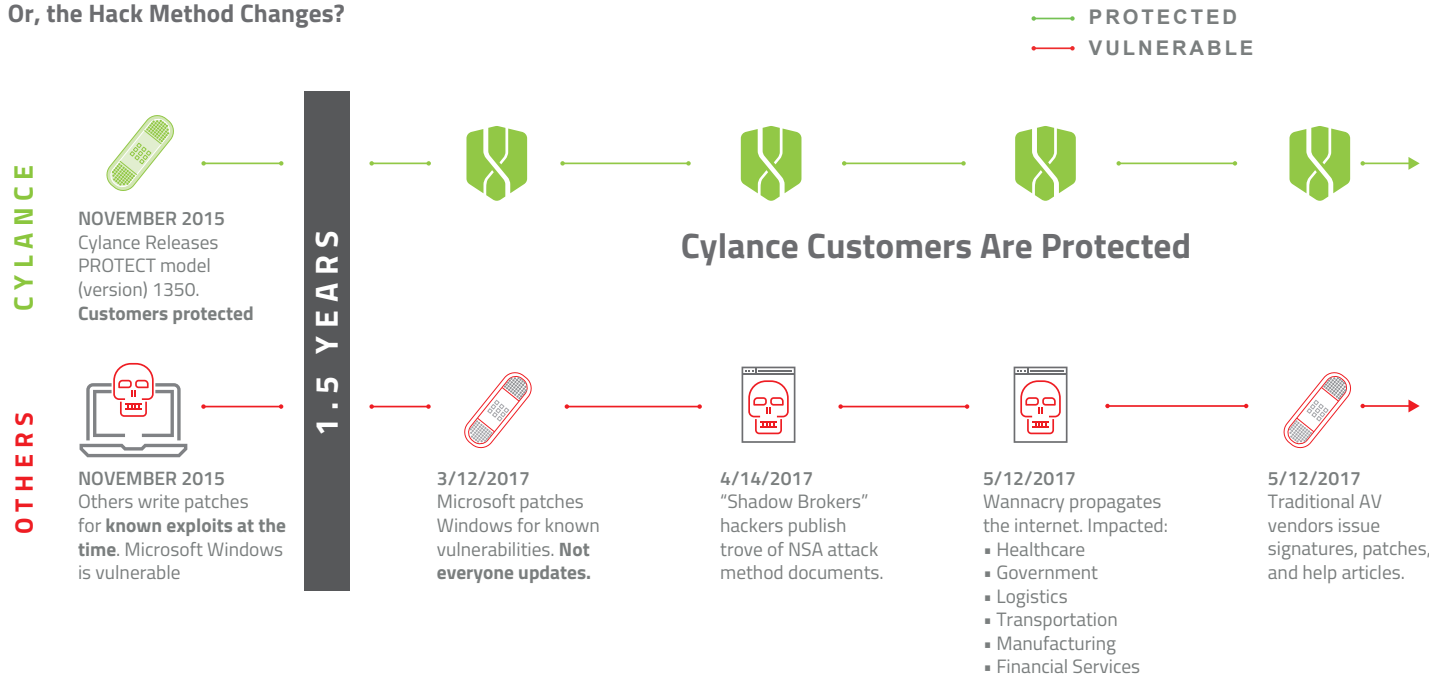


Figure 2 — Timeline of the WannaCry attack and how CylancePROTECT used 18-month old AI models to prevent it.

About Cylance

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist.

By coupling sophisticated machine learning and artificial intelligence with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

In addition to employing strong and effective endpoint controls (i.e. CylancePROTECT), users are also encouraged to:

- Keep software up-to-date, including operating systems
- Avoid dangerous web locations
- Educate users to detect potential cyberattacks delivered via phishing emails, infected banners, spam emails, social engineering attempts, etc.
- Ensure they have CylancePROTECT auto-quarantine, script control, and memory protection enabled and fully configured

CylancePROTECT is 100% predictive and prevents cyberattacks from being successful by providing a proactive security posture with extremely high efficacy that traditional AV solutions can't provide. It leverages the power of artificial intelligence, algorithmic science, and machine learning to provide seamless and silent pre-execution attack prevention with zero reliance on signatures or cloud lookups.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612



©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170515-1120