Ransomware Prevention Is Possible:
Fighting Today’s Extortive Threats
While advanced persistent threats and malware still plague some victims, it is ransomware that is still gaining real traction in today's cybersecurity landscape. The EternalBlue flaw that took over the news in May 2017 rose to popularity as a result of its inclusion in the data leaked by The Shadow Brokers. Utilized in multiple attacks alongside the also-released DoublePulsar exploit, including the installation of cryptocurrency miner Adylkuzz, the exploits are just the tip of the cyberwarfare tools The Shadow Brokers are claiming to have in their arsenal.

The latest EternalBlue and DoublePulsar based attacks, delivering the WannaCry Ransomware, have so far been hugely damaging to healthcare organizations while also impacting over 200,000 endpoints in 150 countries. WannaCry-WanaCryptor 2.0 was coupled with the EternalBlue exploit, allowing it to automatically propagate itself to vulnerable machines across the Internet. While not technically advanced, the use of EternalBlue and DoublePulsar created a ransomworm that spread much faster than any other previously reported ransomware outbreak.

**Anatomy of an Enterprise Attack**

This attack exploits a flaw in the Server Message Block (SMB) in Microsoft Windows, which can allow for remote code execution upon proper and successful exploitation. This flaw was patched in Microsoft's March 2017 update cycle (MS17-10).

However, many environments are still behind on patches for various reasons and may also be running legacy operating systems, such as XP, which are no longer updated/supported with security updates, leaving those systems exposed. Leveraging this exploit, the attackers can fully execute arbitrary code.

In the case of the WanaCrypt issue, we are dealing with a ransomware executable that includes additional worm functionality. It has the ability to scan and locate other machines and propagate itself to other adjacent and exposed hosts via the EternalBlue vulnerability.

Due to the nature of the flaw, machines propagated via the worm functionality do not require interaction from the user on the victimized host.

The worm/ransomware binary handles the remote execution. In most confirmable cases today, stage one is a malicious phishing email. This includes an attachment that the victim executes, which infects them, while simultaneously kick-starting stage two — the worm-type functionality and internal propagation/pivoting.

Ransomware has been around for well over a decade, but traditional antivirus solutions still require every single piece of malware to be discovered by its execution on an endpoint, meaning these solutions cannot stop ransomware until it infects that first victim. If your organization is the sacrificial lamb traditional antivirus providers need, you could be faced with an extremely costly ransom that may or may not yield the ability to decrypt your locked data. Depending on your organization's industry, this can affect every single one of your customers and every aspect of your business, and can even put critical infrastructure and human life in jeopardy.

All it takes is a couple clicks and the ransomware infects your entire network, encrypting every file, every drive, every server it can gain access to, and within minutes, your organization's most important data is encrypted. The only way to decrypt your data is to hope that once you pay the expensive ransom, the cybercriminal extortionist will be satisfied enough to send you the decryption code. Good luck with that!
Medical Industry Hit Hard, but Just One Example

There is certainly no shortage of threats to write about these days when it comes to ransomware and the recent surge of activity involving high profile attacks and victims. It is deeply concerning to hear about the high-profile medical entities that have been targeted lately. In this scenario, the price paid for the attack is not limited to the money paid as the ransom. A ransomware attack on a health center has proven to cause delays in patient care, which can also even lead to loss of human life.

In a highly publicized example of this type of attack, 40 hospitals that are part of the U.K.’s National Health Service (NHS), were hit simultaneously by the WannaCry Ransomware. Reports of canceled surgeries, medical appointments, and lab results on hold due to the ransomware flooded the news, and public outrage escalated the incident to worldwide news. The WannaCry infection highlighted the outdated and vulnerable infrastructure and security of the NHS. In the weeks after the attack, the hospital network was slow to recover and restore functions back to each of the 40 hospitals.

Petya Ransomware Returns as Goldeneye

A new variant of the notorious ransomware Petya is back again, and with yet another James Bond reference for a name: Goldeneye. Presumably from the same author of Petya and the Petya-Mischa combo, Janus Cybercrime Solution’s latest creation is another step in the evolution of their ransomware-as-a-service expansion.

Petya is a form of ransomware that overwrites the master boot record in order to block access to the user’s files and operating system. Safe Mode access is also disabled. Once Petya executes, the user’s machine will crash, restart, and show a skull-and-crossbones animation before displaying a ransom note asking for payment in bitcoins in order to decrypt the system.

Ransomware-as-a-service (Satan)

Ransomware is probably the most popular form of cyberextortion. It has been around for many years, but lately there has been a significant increase in the number of variations of ransomware. Due to its notoriety and potential for a high payout, ransomware is quickly evolving, and cybercriminals are developing new ways to distribute malware to make money.

In years past, expert malware authors would package up their know-how into costly exploit kits and sell them on the underground market. Cybercriminals would pay a hefty upfront cost before ever infecting a victim’s machine and realizing a profit.

One such ransomware-as-a-service is called Satan. Satan’s developers have posted the ransomware online and made it available for free. Any would-be cybercriminal with absolutely no programming skills can download and deploy Satan in just three easy steps, while also managing their ransomware campaigns in a central console hosted on the Satan developer page. Instructions on payload delivery, translation services, and customer support are even provided to would-be criminals. Then, when Satan is successful in an attack, the downloader pays the developer 30% and keeps 70% of the paid ransom.

What Should Security-Minded Enterprises Do?

These are examples from just one industry and three ransomware families, but they provide real-world examples of how enterprises can easily be infected, causing great harm to operations, brand reputation, customer relationships, and even the critical infrastructure that organizations all over the world rely upon. The true tragedy of the consequences of ransomware is that they are completely and totally avoidable with the right endpoint security product.

In the cases of the ransomware examples mentioned — WannaCry, Goldeneye, and Satan — Cylance’s award-winning artificial intelligence and machine learning based product, CylancePROTECT®, was successful in protecting against all the variants with its predictive mathematical models dating back to September 2015, long before the ransomware variants were even created. That’s the power of machine learning. Cylance’s math driven models take massive amounts of data about known malware and predict what future malware will look like in order to prevent it from getting into systems in the first place.

CylancePROTECT can stop ransomware before it ever executes, and Cylance’s Consulting Services team can remediate and repair the damage caused by ransomware attacks that have already occurred. To learn more, visit www.cylance.com/ransomware.
HOW RANSOMWARE WORKS

Entry Point -> Installation
Encryption -> Extortion

WHAT MAKES A COMPANY VULNERABLE

Lack of a Formal Backup Plan
No Cybersecurity Strategy in Place
Using Legacy Software and Outdated Hardware
Downloads from Email or Compromised Websites
Unpatched Operating Systems

RESPONSE AND RECOVERY

When you are the victim of an attack you should have someone to call for help. Our Incident Response team will work with you to contain the active threat and mitigate the risk.

Agentless Analysis for Linux, MAC, and Windows
Proprietary Machine Learning Technology
Analysis Tools Identify Scope of Incident Within Hours
Immediate Resolution for Quicker Incident Response