Ransomware Prevention Is Possible:

Fighting Today's Bountiful Cornucopia of Extortive Threats

CYLANCE™

Australian cybersecurity headlines paint quite a frightening picture. Viruses are being called 'unbreakable' and Australia is being called the land of opportunity for attackers. Attack volumes are up over 100% each year and tens of millions of dollars are flowing to overseas bank accounts as ransomware victims try to buy their way out of security breaches.

While advanced persistent threats and malware still plague some victims, it is ransomware that is gaining real traction in today's cybersecurity landscape. A recent ransomware attack using the Locky virus specifically targeted Australia Post customers who received an email with an attachment that appeared to provide information about a package the customer was having delivered. The email expressed an issue with delivery and asked the customer to open a zip file containing a letter with more information about their expected package. The zip file was not a letter at all, but in fact, an executable file that quickly froze customers' computers, encrypted files, and then demanded a ransom be paid. The cybercriminals behind this scam went as far as to research public social media profiles to seek out email addresses for Australians whose profiles contained posts about recent online purchases.

ANATOMY OF AN ENTERPRISE ATTACK

While the Australia Post Locky attack turned consumers waiting for a package into victims, imagine if that consumer was a member of your business team and opened that zip file on their work computer while connected to your network. With the overwhelming success of ransomware attacks, attempts to gain access to enterprise data by cybercriminals are sharply increasing. What is most concerning about the rise in ransomware is the fact that traditional antivirus products are powerless to stop every single initial attack cybercriminals launch.

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 dollars and cents paid as the 'ransom'. A ransomware attack on a health center could 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, in February 2016, the Hollywood Presbyterian Medical Center, one of the U.S.'s most well known hospitals, which had been targeted by cybercriminals for some time, became infected with ransomware that shut down critical care systems for more than a week. Reports have indicated a possible $3.6 million ransom was paid and that select patients had to be transferred to other hospitals because connected medical devices had become inoperable and important medical records had become inaccessible.

Latest Variants in Ransomware PowerWare

One example of today's highly targeted ransomware is PowerWare, a unique type of ransomware that utilizes PowerShell code in malicious Microsoft Office documents to initiate the infection stage and encryption process. This means that no first-stage or stand-alone executable dropper will be present on the infected box. This is all done via PowerShell in VBA script within the weaponized Office documents. This technique itself is not new. PowerWare masquerades as an official-looking invoice document, but has the ability to exfiltrate data, drop Pony Loader, and initiate a Black Energy-style wiper.

The Petya Ransomware Project

Another example of ransomware is Petya. What makes Petya unique is the overwriting of the MBR as a mechanism to block access to the files and OS. Upon execution, the victim sees a quick crash, a reboot, a fake chkdsk screen, and finally a sinister and seizure-inducing skull and crossbones animation leading to the ransom instructions. Petya also inhibits the ability of the user to boot into Safe Mode. The emails sent to victims contain a link to a Dropbox folder rather than to a weaponized Office document. Instead, the Dropbox folder contains the first stage executable file.

Ransomware-as-a-service (Tox)

To make matters even worse, the proliferation of connected devices, the ease at which information can be exchanged on those devices, and the success of ransomware attacks, have led to what is known as ransomware-as-a-service. Cybercriminals are not only making money through attacks, but are now offering their services as programmers to would-be cybercriminals that are not as tech savvy, providing variants of their ransomware to others via online download for free or for a small fee. Then, when the ransomware succeeds in an attack, the original ransomware author is paid a commission.

One such ransomware-as-a-service is called Tox. Tox'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 Tox in just three easy steps. Then, when Tox is successful in an attack, the downloader pays the developer 20% and keeps 80% of the ransom.

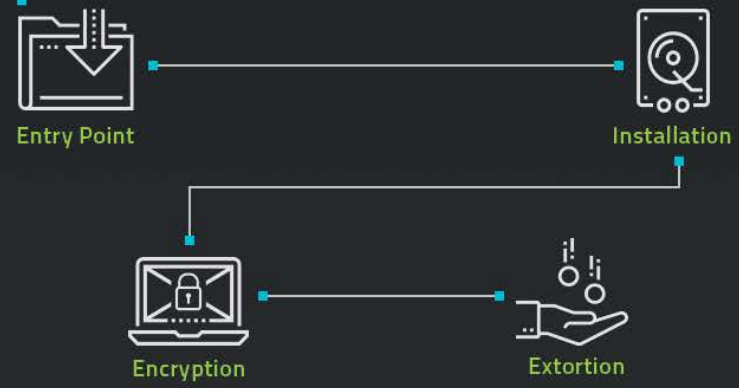
WHAT SHOULD SECURITY-MINDED ENTERPRISES DO?

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. A product based on artificial intelligence and machine learning that uses its knowledge of the characteristics of hundreds of millions of files to recognize when files are actually malicious ransomware can keep that ransomware from ever executing – keep it from ever delivering its devastating payload.

Cylance's award-winning artificial intelligence and machine learning based product, CylancePROTECT® can stop ransomware BEFORE it ever executes, and Cylance's Consulting 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



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 Techology

Analysis Tools Identify Scope of Incident Within Hours

Immediate Resolution for Quicker Incident Response

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

CYLANCE™

20170228-1404