Ransomware: The Great White Shark of Malware & What You Need to do About it

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

Introduction

'STOP! Are you really sure you want to load this attachment? Are you certain that this link is safe?'

A prompt from your computer may be the difference between a disastrous Ransomware infection and a regular day at the office.

Right now, Ransomware is the Great White Shark of cyber attacks, the most feared malware of all, and both corporate and home users are running scared. And rightly so - Anyone who has had experience with Ransomware, will attest to the agony and disruption. But instead of worrying about an attack, what action can be taken to safely venture back into the water and not necessarily "with a bigger Boat"?

Who should be aware of the Ransomware threat?

Home User: The home-user community for ransomware has been highly active for a few years now but has escalated in recent months. Being given just hours to either pay the ransom or lose permanent access to everything on your personal computer is a stark choice (often enough to precipitate agreement to the extortion). What value would you put on all your personal documents, photos, music, etc?

Corporate User: The stakes are even higher for a corporation, where the absolute dependency on IT systems means ransomware could threaten the very life of the business itself.

In the case of the LA Presbyterian Hospital, this threat to life was more literal, in that patient systems were under threat from Ransomware - the hospital paid the equivalent of $17,000 dollars in BitCoin as the *"quickest and most efficient way to restore our systems and administrative functions"*; and just like that a dangerous precedent was set! More details later.

The terror of the deep - *The threat of Cyber Attack is a concern for all corporations and computer users, but nothing strikes more fear than RansomWare*

How does Ransomware typically attack systems?

Email – phishing, be it the mass, spear or now whale variety for corporate targets – is still the most common means of invoking a Ransomware attack. The home-user 'market' for the extortionists lends itself to mass-emailing, but this means that the malware can just as easily end up on Corporate Workstations. Significantly, now that there has been a very public precedent of a hospital paying a ransom, expect to see greater targeting of corporate targets.

The first thing we need to establish is the fact that Ransomware is no different than any other form of malware in terms of its delivery means – usually, but not exclusively, via email with either malware attachments or links to infected websites. The difference - and the scary part - is how it is used to extort money from victims.

Once the malware has been invited onto a user's computer it can then get to work, encrypting files before announcing its presence and declaring its ransom demand. The nature of its immediate demands and very tangible threat is precisely what makes it more feared than other malware. However, your line of defense and your approach to preventing Ransomware should be the same as it would be for any other Malware. Don't be thrown by the sensationalism surrounding Ransomware – Pragmatism should always prevail.

> *"This puts lives at risk, and it is sickening to see such an act"*
>
> *Phil Lieberman, Cybersecurity Expert*

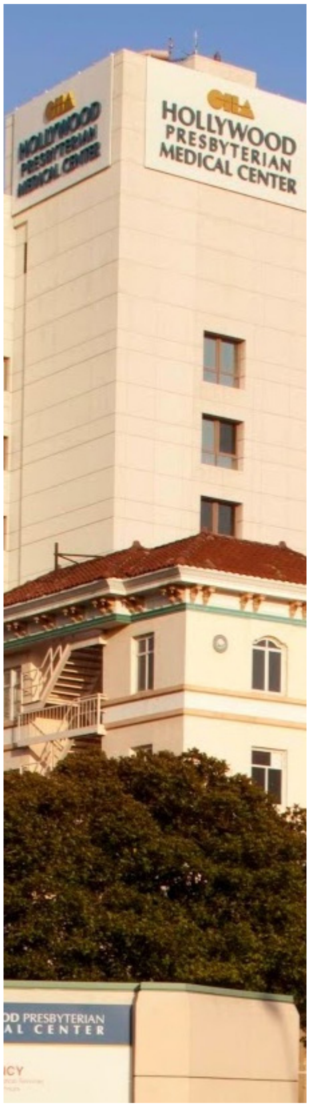

CHA
HOLLYWOOD PRESBYTERIAN MEDICAL CENTER
CHA
HOLLYWOOD PRESBYTERIAN MEDICAL CENTER
OD PRESBYTERIAN
AL CENTER

Figure 1: Dangerous Precedent? *The Hollywood Presbyterian Med Center paid a $17,000 ransom when hit with a Cyber Attack*

Corporate Ransomware Case Study

LA Presbyterian Med Center Case Study: The fact that this was a relatively quick and easy *'Hack for Cash'* is driving this predicted trend. The LA Presbyterian Medical Center attack speaks to both the targeting of Healthcare as well as the increase in Ransomware.

The assault on Hollywood Presbyterian occurred Feb. 5, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices, said Chief Executive Allen Stefanek.

The hacker demanded 40 bitcoin, the equivalent of about $17,000, he said.

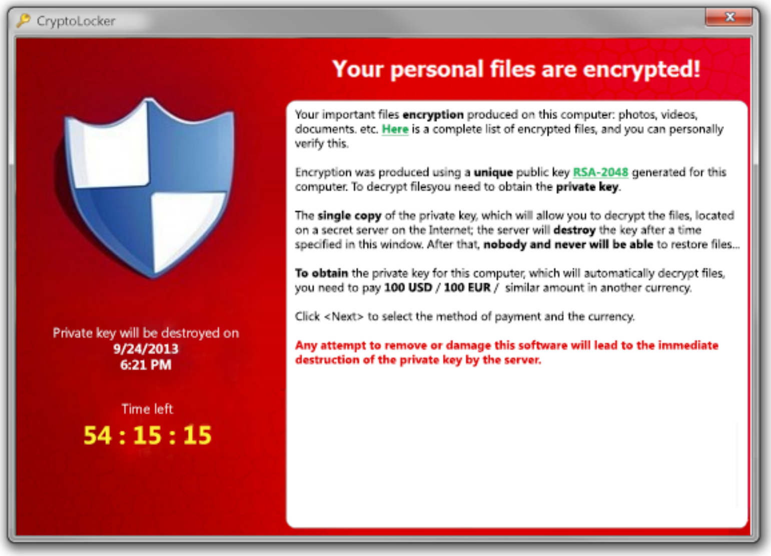
"The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Stefanek said. *"In the best interest of restoring normal operations, we did this."*

The hospital said it alerted authorities and was able to regain control of all its computer systems by Monday, with the assistance of technology experts.
Phil Lieberman, a cybersecurity expert, said that, while ransomware attacks are common, targeting a medical institution is not.

"I have never heard of this kind of attack trying to shut down a hospital. This puts lives at risk, and it is sickening to see such an act," he said. *"Health management systems are beginning to tighten their security."*

http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

CryptoLocker - Best avoided!



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Figure 2: You don't want to see this *Classic Ransomware operation - after the malware is in place, a unique encryption key is generated for each computer infected and is used to encrypt data on the machine. If the ransom is not paid within the allotted time the files are lost forever.*

Make sure backups are up to date and isolated from the computer, otherwise they may be encrypted too.

So - What should you be doing right now to prevent Ransomware?

Over and above standard firewalling and anti-virus protection, there are additional defenses that should be in place to defend against phishing, given that this is the primary delivery mechanism used. Unfortunately, phishing is, by design, notoriously tough to prevent, due to its cunning and devious methods. The malware is invited in by the recipient, typically either by opening an attachment or by activating/downloading a link, thereby largely subverting Corporate IT Security.

> *“...phishing is, by design, notoriously tough to prevent, due to its cunning and devious methods...”*

The best approach is to therefore harden the user workstation environment, to prevent malware activity where possible and to at least place more obstacles in the way when not. As with any hardening program, a balance must be found between strong security and operational ease of use.

The majority of exploitable vulnerabilities can be mitigated within the Workstation Operating System, and further protection can be provided using manufacturer extensions such as Microsoft’s EMET (Enhanced Mitigation Experience Toolkit) and Windows Defender or 3rd Party AV.

Secure the Desktop and the User

But when it comes to users’ emails and their content, accurately protecting against the bad while allowing the good is beyond any technological solution. While blocking all email attachments and links would improve security, there aren’t many users that would sign up for this. A more graded approach to protecting the user is needed.

Figure 3: Secure the Desktop Users and their desktop applications - specifically email clients and browser - are the conduit for Ransomware so leveraging all available safety and security settings available is essential

And in fact this solution already exists for most browsers and the Microsoft Office Applications. Controlled by Group Policy, the desktop applications otherwise used to welcome in Ransomware can be fine-tuned to mitigate exploitable vulnerabilities while requiring elevated approval for other functions – this may slow the user down for certain tasks, but that additional pause for thought while the system prompts for approval elevation will ensure security hygiene is observed.

For example, MS Outlook security policy options are available to control:

- How administrator settings and user settings interact in Outlook 2013
- Outlook COM add-ins
- ActiveX and custom forms security
- Programmatic Access settings
- Settings for Attachments, Cryptography, Digital signatures, Junk email, Information Rights Management and Protected view

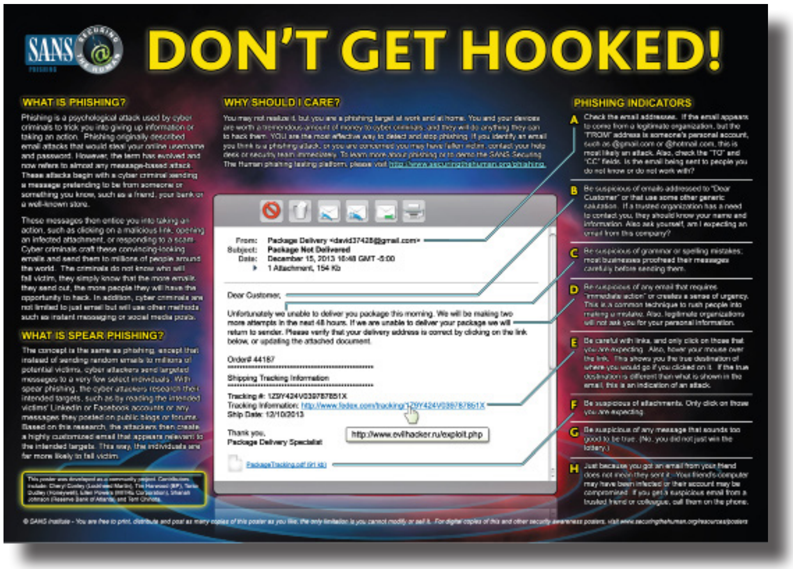
Similarly, fine grain security settings are available for Excel, Word, PowerPoint and Office, all serving to mitigate vulnerabilities within the application that could be exploited by an attacker, overall bolstering Ransomware defenses.

Likewise for contemporary browsers like Chrome, Firefox and Internet Explorer, anti-phishing controls should be enabled alongside other built-in security measures that are often disabled by default.

HOW DOES IT WORK CONTINUED...

Key Questions Regarding Desktop Application Hardening

- Which settings need to be set and which are optional?
- What are the implications in terms of user experience and application function if security settings are enabled?
- How do you actually apply the necessary secure configuration, and how do you do it in bulk for your entire IT estate?



DON'T GET HOOKED!

WHAT IS PHISHING?

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods such as instant messaging or social media posts.

WHAT IS SPEAR PHISHING?

The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tanya Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta), and Terri Chinolla.

WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human phishing testing platform, please visit http://www.securingthehuman.org/phishing.

From: Package Delivery <david37428@gmail.com>
Subject: Package Not Delivered
Date: December 15, 2013 10:48 GMT -5:00
1 Attachment, 154 Kb

Dear Customer,

Unfortunately we unable to deliver you package this morning. We will be making two more attempts in the next 48 hours. If we are unable to deliver your package we will return to sender. Please verify that your delivery address is correct by clicking on the link below, or updating the attached document.

Order# 44187
****
Shipping Tracking Information
****
Tracking #: 1Z9Y424V0397B7B51X
Tracking Information: http://www.fedex.com/tracking/1Z9Y424V0397B7B51X
Ship Date: 12/10/2013

http://www.evilhacker.ru/exploit.php

Thank you,
Package Delivery Specialist

PackageTracking.pdf (91 kb)

PHISHING INDICATORS

A Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?

B Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?

C Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.

D Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.

E Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different than what is shown in the email, this is an indication of an attack.

F Be suspicious of attachments. Only click on those you are expecting.

G Be suspicious of any message that sounds too good to be true. (No, you did not just win the lottery.)

H Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.

© SANS Institute - You are free to print, distribute and post as many copies of this poster as you like; the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

Figure 4: Securing the Human: *Among others, the SANS Institute offer posters and desktop-wallpaper to remind and reinforce good cyber security hygiene among users.*

Educating users in respect of cyber security will improve the employees', and in turn the organization's, ability to remain secure across all fronts, not least where Ransomware attacks are concerned

Help is at Hand: The NNT Ransomware Mitigation Kit

NNT, in conjunction with The Center for Internet Security (CIS), provide a comprehensive suite of system hardening templates based on absolute best practices.

These can be leveraged to ensure all of your systems (workstations included) retain the most appropriate checks designed to harden your environment and protect from Ransomware.

NNT's is an accredited CIS member and as such we are able to automate and control the provision of all relevant hardening standards including your Microsoft Applications. Within minutes, a full vulnerability assessment can be performed against your user workstation platforms and the applications being used. Full remediation guidance is provided to make corrective action a straightforward task.

NNT can also provide a Ransomware Mitigation Kit, comprising the necessary automated vulnerability checks and also the Group Policy/Puppet templates to automatically fix any weaknesses identified.

Best of all, these layers of defense against RansomWare are also backed up with the fastest-available, real time system integrity and change control detection technology to further ensure that, if the unthinkable happens and you do fall victim to an attack, any suspicious changes or activity is immediately brought to your attention before major damage can be perpetrated.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative. W: www.newnettechnologies.com E: info@nntws.com