The Problem with Running Outdated Software

A New Net Technologies Whitepaper

Mark Kedgley

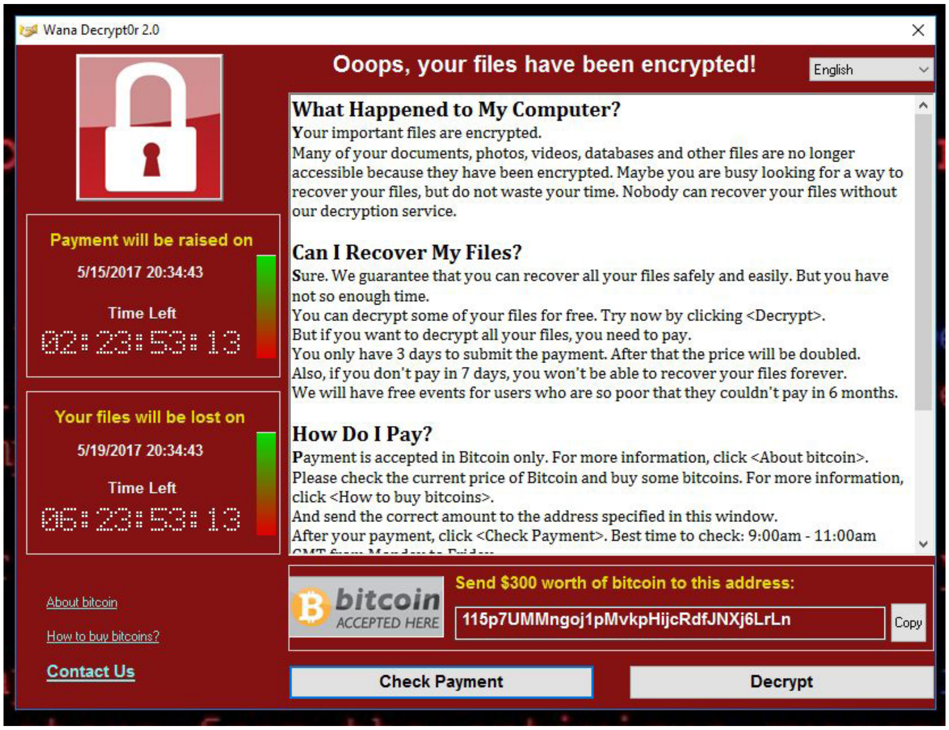
CTO - New Net Technologies

www.newnettechnologies.com

ABSTRACT

Given the latest WannaCryRansomware epidemic, which infected more than 230,000 users in over 150 countries, it's vitally important that organizations fully understand the risks associated with using out-of-date systems and software.

> *"In the corporate IT environment, the problem is substantially worse in that if your computer is not up to date with the latest security threat mitigations in place, then you're posing a risk to the entire network"*



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 20:34:43
Time Left
02:23:53:13

Your files will be lost on
5/19/2017 20:34:43
Time Left
06:23:53:13

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

WHY DO WE RESIST THE UPGRADE?

Change can sometimes be unnerving. It requires a bit of adjusting and is often times considered best avoided, especially when it comes to upgrading functioning production software. There is an understandable resistance to upgrading software where the version in use is familiar, well understood and from a functionality standpoint, isn't actually broken. Unfortunately, the same software is well known to hackers. They've had plenty of time to get well accustomed with software that's been around for years.

There are also associated costs to consider. Both the financial costs of course, but also resource costs and the potential changes required to the prevailing infrastructure.

At best this can lead to procrastination at worst complete avoidance.

So why bother with upgrades? Aside from any new and cool features that may be on offer, equally compelling is the need to resolve known vulnerabilities. Gartner estimate that over 99% of all published breaches in 2016 exploited known vulnerabilities!

Figure 2: Windows XP- one of the most notable obsolete software programs that has been cut off from support since April 2012

WATCH OUT - YOU MIGHT BE THE VULNERABILITY!

So the problem with running outdated software is not just the lack of new features or improved functionality provided but just as important it's the known and exploitable vulnerabilities.

In the corporate IT environment, the problem is substantially worse in that if your computer is not up to date with the latest security threat mitigations in place, then you are posing a risk to the entire network. This was the significant factor that made WannaCry such a devastatingly damaging cyberattack in that the Ransomware was designed to 'worm' around the network, infecting any other vulnerable systems. Individuals and their computers are the number one attack vector, usually via phishing emails with toxic links or malign attachments intended to exploit vulnerabilities.

2 MAJOR ISSUES WITH RUNNING OLDER SOFTWARE

According to guidance developed by the National Cyber Security Centre, obsolete software creates two major issues from a security perspective:

1. The software will no longer receive security updates from its developers, increasing the likelihood that exploitable vulnerabilities will become known by attackers

And

2. The latest security mitigations are not present in older software, increasing the impact of vulnerabilities, making exploitation more likely to succeed, and making detection of any exploit more difficult

Clearly, if these issues prevail, your organization becomes more likely to experience a high-impact security incident.

BOUND TO BE XPLOITED

Once software ceases to be maintained by its developer, there are limits on the mitigations that will be effective in defending against new cyber threats that will emerge. Over time, new vulnerabilities will be discovered that can be exploited by low-skilled hackers, leaving your organizations susceptible to attack, data loss, or even fiscal consequences.

One of the most notable obsolete software programs is the Windows XP operating system. NetMarketShare found that in 2015, just under 11% of desktop computers were still using Windows XP, which has been cut from support for over 3 years now.
After finally announcing it's simply not feasible to patch all of the security holes within the aging operating system, users were urged to upgrade before they lost support.

Many users believe that if they stay away from questionable websites and make sure not to open attachments from unknown senders then the risk posed by Windows XP can be minimalized. While that may have been true a decade ago, today's attackers are much smarter with their attack methods. Malware is often delivered through legitimate websites by attackers who upload malicious content through user-provided advertisements or can be shared via email as if they come from a known, trusted source.

THE PROBLEM WITH EXPLOITS

The problem with exploits are that they are either underpublicized or overly publicized. Some users are not aware of exploits being publicized, leaving them unable to protect themselves from attackers. On the other hand, some exploits are so hyped that hackers see a moment of opportunity and jump on those who are still vulnerable.

WHAT'S WORSE THAN UNPATCHED WORKSTATIONS? SERVERS!

Obsolete operating systems can serve as a conduit into a network, but businesses tend to not have a lot of important information stored locally. Servers, however, have been found to be a lot more attractive target for an attacker, because that's where all the really valuable data is generally found.

Servers hold a treasure trove of valuable information, including company documents, accounting and financial information, client information, and much more. More importantly, servers host the critical services that make the network run, including DNS, DHCP, remote access services, email, company website, databases, and in some cases, even users' desktops.

Vulnerable servers leave an organization susceptible to unauthorized access to its sensitive company data, adjusting or destruction of irreplaceable data, disruption of important network functions, and a complete shutdown of the network through DDoS attacks.

> "Vulnerable servers leave an organization susceptible to unauthorized access to its sensitive company data, adjusting or destruction of irreplaceble data, and a complete shutdown of the network"

WHERE DOES NNT STEP IN?

By providing the ability to understand and better control changes that occur within the IT environment, NNT maximizes preventative measures against known exploits, while providing a forensic-level early-warning detection of newly developed attack methods. If changes are allowed to occur without any means of detecting suspicious or potentially harmful changes, there will always be a risk that a breach or disruptive action will occur and worse, that it will go undetected.

HOW DOES IT WORK?

The starting point for Change Control is a secure environment, one which is configured to best protect against an attack. NNT enables organizations to establish a 'known, good, secure and compliant' state for every IT asset within the environment. We are one of an elite group of vulnerability management specialists actually certified by the Center for Internet Security (CIS).

Once we have confirmed that all systems are secure and fit for purpose, we track every change made to that state, however discreet or nuanced that change may be. With the help of intelligent threat control and change context, we are able to automatically approve changes as being safe or flag suspicious changes immediately for review.

HOW DOES IT WORK CONTINUED...

NNT utilizes unique Closed Loop Intelligent Change Control Technology along with Threat Intelligence Feeds that allow organizations to gain control of the changes that are happening and immediately highlight any that could represent a threat. No wonder NNT is rated #54 in the World's Hottest Security Companies by Cyber Security Ventures.

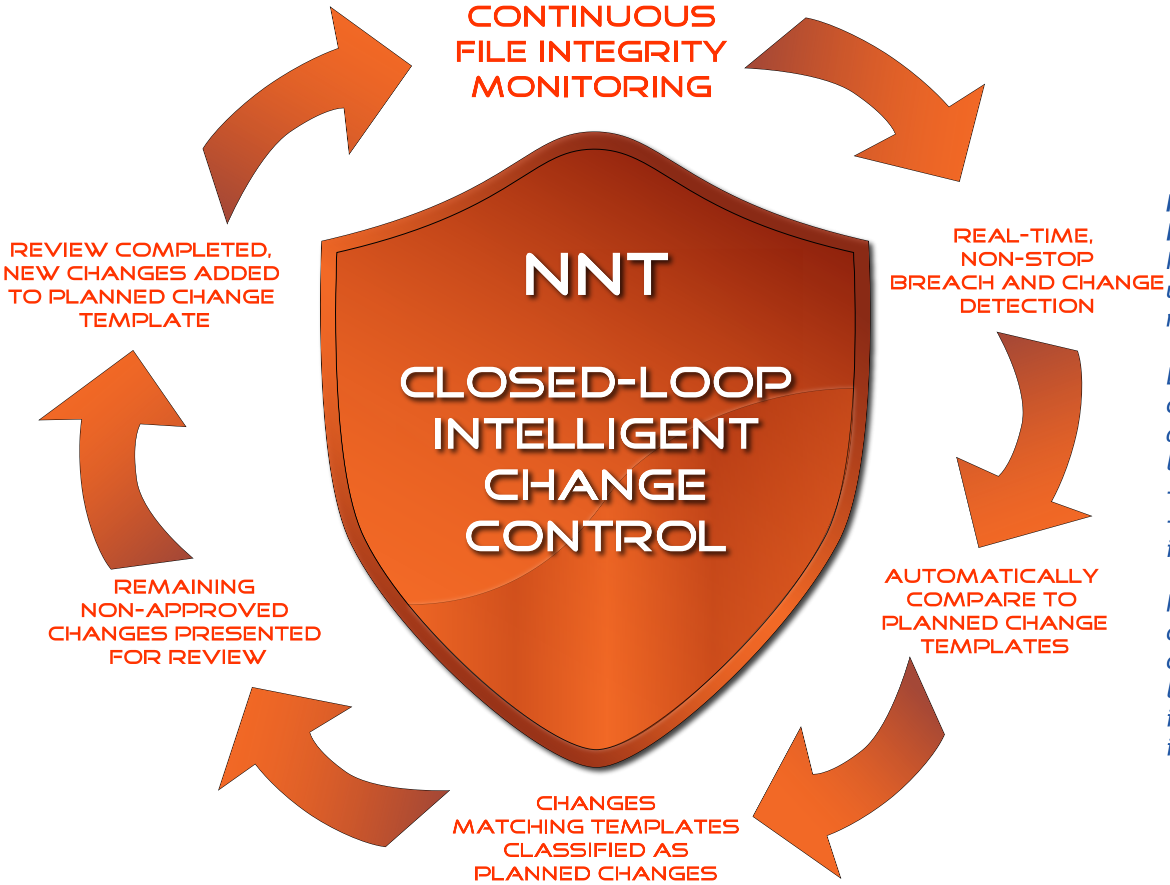


***Figure 3: Closed-Loop Intelligent Change Control** gives Information Security Teams an unfair advantage over hackers, malware and inside-man threats.*

By automatically assessing changes, all expected/pre-approved changes can be isolated leaving just unplanned changes - which may be breach activity - exposed, to then be properly investigated.

In addition, all unplanned changes found to be legitimate can optionally be added to the list of pre-approved changes, improving the systems' intelligence further

WHAT DOES NNT SPECIFICALLY PROVIDE?

Within the NNT solutions we provide:

- System Configuration, Vulnerability Hardening & Compliance Management
- Real-time, Intelligent & Context-based File Integrity Monitoring
- Automated File Approvals using the world's largest whitelist
- Change Policy Control
- Configuration Drift Management
- Security Information and Event Log Management

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