An NCC Group Publication

Understanding Ransomware: Impact, Evolution and Defensive Strategies

Prepared by:

NCC Group Cyber Defence Operations

- Emily Mitchell
- Will Alexander
- Nikos Laleas
- Jacqueline Gough
- David Cannings

Contents

1 Introduction

In recent months there has been an increase in the number of ransomware trojans, such as CryptoLocker, that encrypt the files on a computer or the network it is part of, and demands payment for their recovery. While these can be frustrating for a home user, their impact on a company can be highly damaging, with potentially many years of work lost across a large number of users.

Although ransomware trojans have existed for many years, the success of the latest variants is largely due to well-implemented public-key cryptography and the inability of users to recover their files without paying the ransom. This use of public-key cryptography is very different from older threats that implemented flawed encryption techniques (allowing file recovery) or were easily disabled by a skilled IT administrator.

Computers are usually initially infected through a malicious email or compromised website. Ransomware trojans sometimes pretend to be from a reputable organisation to extort money from their victims, examples have included law enforcement[1] and the UK postal service[2].

In this whitepaper we discuss the potential impact of ransomware trojans, the technology behind a number of recent threats and most importantly how enterprises can begin to protect themselves from losing business critical data.

2 Business Impact

2.1 Annoyance or Business Risk?

For individual employees there is the risk of losing valuable data that has not been backed up. This impact can be frustrating and may have an immediate impact on a team or business unit. However, the risk to an organisation can be wider than just one employee.

Some ransomware will encrypt files on any drive, including network shares. These are commonly mapped to all users in large corporate environments and where there is weak access control there is the potential of losing large amounts of data from multiple areas of a business. Therefore the impact to a company might be a number of days restoring from backups and rebuilding computers, or it could be the permanent loss of critical data.

Infections which initially come from email can be spread internally within an organisation as employees forward documents or access shared mailboxes.

Modern ransomware trojans will not alert the user until they have finished encrypting files, thus making it much harder to turn off a computer to preserve files. Some will also impose time restrictions on payment, further pressuring victims.

2.2 Case Study

NCC Group recently assisted a client in which an employee lost two years of work from their Microsoft Windows laptop due to CryptoWall, despite the laptop having up-to-date antivirus on the day of infection. The laptop was infected while at home through a drive-by download served by a malicious advertising server. File encryption started a few minutes later and continued the next day when the laptop was connected to the internal corporate network.

During our incident response, we discovered that over 28,000 files had been encrypted, including those on a corporate shared drive belonging to other users. On the first day of the engagement the detection rate of this variant by anti-virus products was less than three out of 54 products, as reported by VirusTotal.

[1] http://www.dotfab.com/resources/urausy-ransomware-hits-the-world-again/
[2] http://www.actionfraud.police.uk/beware-of-royal-mail-scam-emails-that-contain-cryptolocker-feb14

The antivirus product used by our client did not detect this trojan until NCC Group forensic experts identified the file on the infected laptop and worked with the vendor to supply a sample thus allowing signature development.

2.3 Data Recovery Likelihood

Recovering data encrypted by modern ransomware trojans is often impossible, even with the assistance of forensic experts. Some recent ransomware trojans have included flaws which allowed recovery of the encryption key, however, new variants are quickly released to fix these problems.

We therefore recommend that proactive measures are taken to reduce the likelihood of ransomware successfully encrypting data and to limit the impact of this type of incident. Advice suitable for a corporate environment is given later in this whitepaper.

2.4 Paying to Recover Data

Paying the ransom to recover data funds further criminal activity and provides a viable market for criminals to operate within. Payment may also leave victims open to future extortion and does not guarantee that data will be recovered. NCC Group therefore recommends that companies should not pay any ransom.

Advice from Microsoft states: "*We recommend that you do not pay the ransom.There is no guarantee that paying the ransom will return your PC to a usable state.*"[3]

The UK's National Crime Agency says: "*The NCA would never endorse the payment of a ransom to criminals and there is no guarantee that they would honour the payments in any event.*"[4]

3 Evolution of Ransomware

3.1 Historic Examples of Ransomware

Ransomware trojans appeared as early as 1989 with the "PC Cyborg trojan"[5], which encrypted filenames and demanded payment of $189 to the author. However, many early ransomware trojans would simply limit access to a computer, displaying a message to the user demanding payment.

Over time these ransomware trojans increased in sophistication. In 2005 the GPCode (or PGPCoder[6]) trojan was identified, which encrypted common document and archive files before demanding payment. Although early versions used weak cryptography a variant in 2006 used a 660 bit RSA key, which was eventually cracked by an antivirus company[7]. Later variants used stronger keys and overwrote files, the first steps toward modern encrypting ransomware.

Over time, other types of ransomware emerged, including fake antivirus programs. These display warnings or alerts which look alarming and are often difficult for the average user to remove, prompting many to pay the ransomware authors.

A typical warning from this type of ransomware is shown below. This image is set as the desktop wallpaper and includes the threat that information stored in the internet history could "break your life".

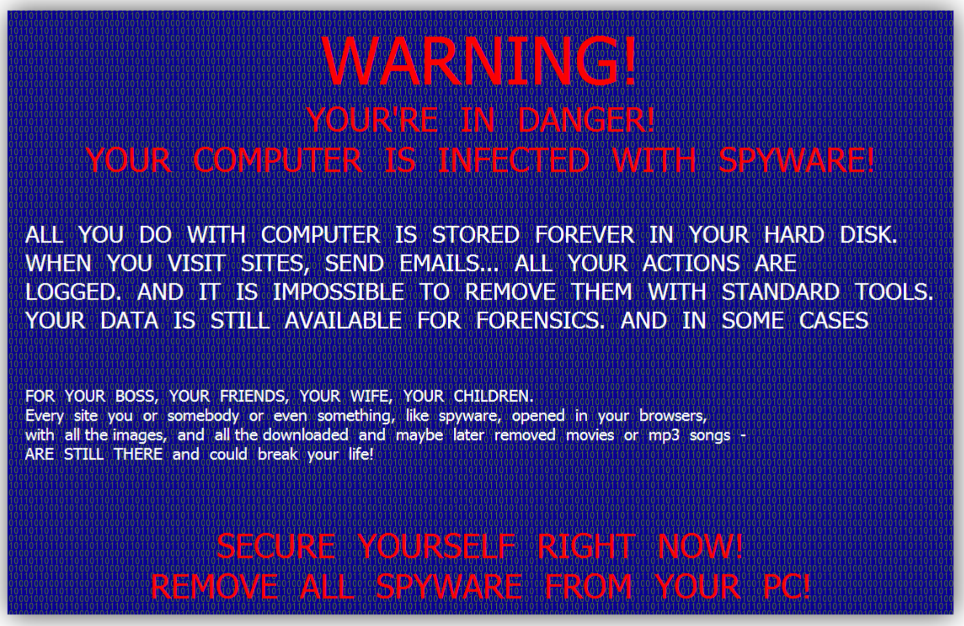
[3] http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

[4] http://www.nationalcrimeagency.gov.uk/news/256-alert-mass-spamming-event-targeting-uk-computer-users

[5] http://en.wikipedia.org/wiki/AIDS_(trojan_horse)

[6] http://en.wikipedia.org/wiki/PGPCoder

[7] http://www.securelist.com/en/analysis/189678219/Blackmailer_the_story_of_Gpcode



WARNING!

YOUR'RE IN DANGER!

YOUR COMPUTER IS INFECTED WITH SPYWARE!

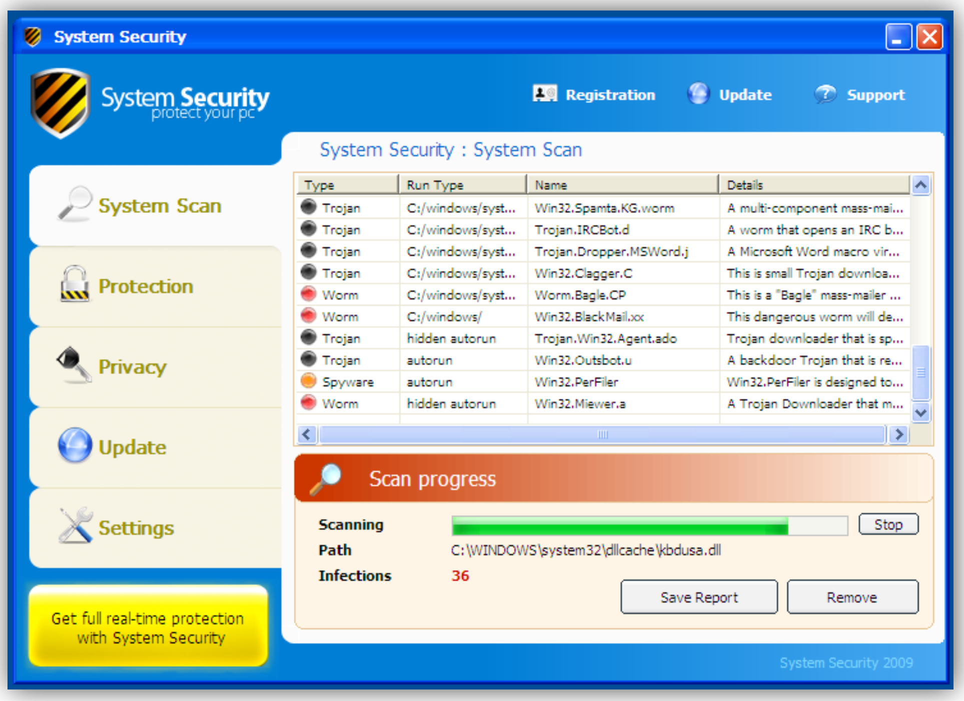
ALL YOU DO WITH COMPUTER IS STORED FOREVER IN YOUR HARD DISK.
WHEN YOU VISIT SITES, SEND EMAILS... ALL YOUR ACTIONS ARE
LOGGED. AND IT IS IMPOSSIBLE TO REMOVE THEM WITH STANDARD TOOLS.
YOUR DATA IS STILL AVAILABLE FOR FORENSICS. AND IN SOME CASES

FOR YOUR BOSS, YOUR FRIENDS, YOUR WIFE, YOUR CHILDREN.
Every site you or somebody or even something, like spyware, opened in your browsers,
with all the images, and all the downloaded and maybe later removed movies or mp3 songs -
ARE STILL THERE and could break your life!

SECURE YOURSELF RIGHT NOW!
REMOVE ALL SPYWARE FROM YOUR PC!

Image 1 - Desktop wallpaper set by a typical fake anti-virus

This fake antivirus program goes on to display the following fictitious list of infections, which prompts the user for registration and payment.



System Security : System Scan

Type	Run Type	Name	Details
● Trojan	C:/windows/syst...	Win32.Spamta.KG.worm	A multi-component mass-mai...
● Trojan	C:/windows/syst...	Trojan.IRCBot.d	A worm that opens an IRC b...
● Trojan	C:/windows/syst...	Trojan.Dropper.MSWord.j	A Microsoft Word macro vir...
● Trojan	C:/windows/syst...	Win32.Clagger.C	This is small Trojan downloa...
● Worm	C:/windows/syst...	Worm.Bagle.CP	This is a "Bagle" mass-mailer ...
● Worm	C:/windows/	Win32.BlackMail.xx	This dangerous worm will de...
● Trojan	hidden autorun	Trojan.Win32.Agent.ado	Trojan downloader that is sp...
● Trojan	autorun	Win32.Outsbot.u	A backdoor Trojan that is re...
● Spyware	autorun	Win32.PerFiler	Win32.PerFiler is designed to...
● Worm	hidden autorun	Win32.Miewer.a	A Trojan Downloader that m...

Scanning
Path C:\WINDOWS\system32\dllcache\kbdusa.dll
Infections 36

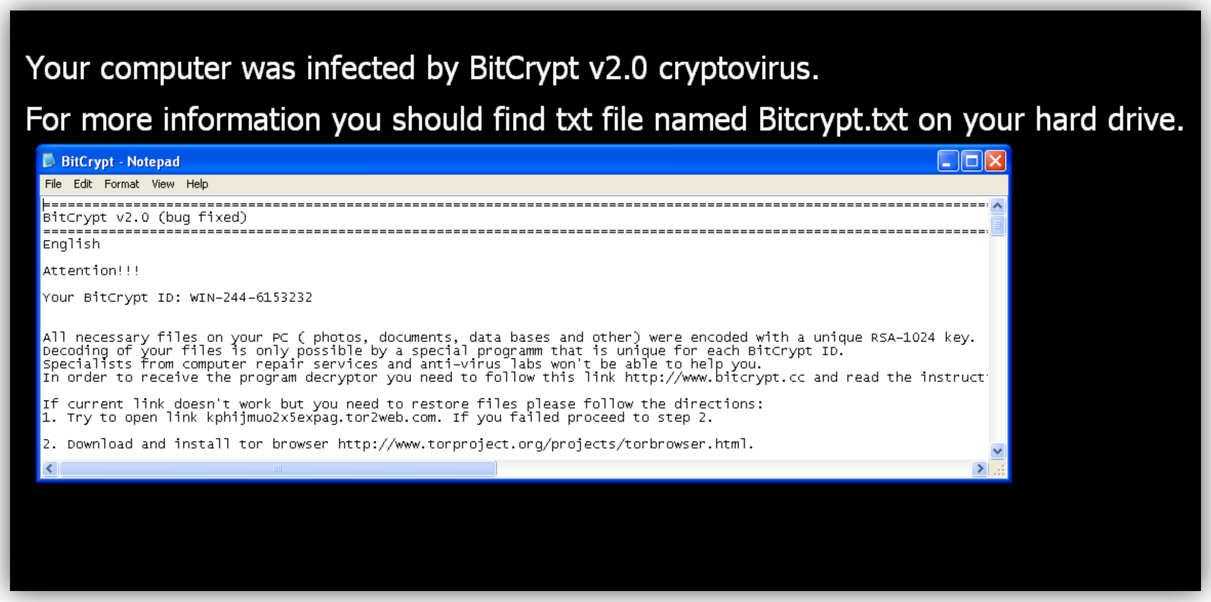
Image 2 - False threats shown to a user by fake anti-virus

3.2 Modern Encrypting Ransomware – Microsoft Windows

Modern ransomware trojans typically implement strong, asymmetric encryption. The most robust implementations do not generate encryption keys on the infected machine and therefore data cannot be retrieved even if encryption is interrupted early.

CryptoLocker is perhaps the most famous modern ransomware trojan and was first seen in September 2013. However, a large number of clones have since been identified, all hoping to make a profit from encrypting files and charging for their return. Particularly successful imitations include CryptoDefense[8] and BitCrypt (Cribit).

Despite the successful use of encryption, some modern ransomware trojans present a very basic message to the user and arguably look less believable than fake antivirus programs. The warning displayed to a BitCrypt victim is shown below.



Your computer was infected by BitCrypt v2.0 cryptovirus.

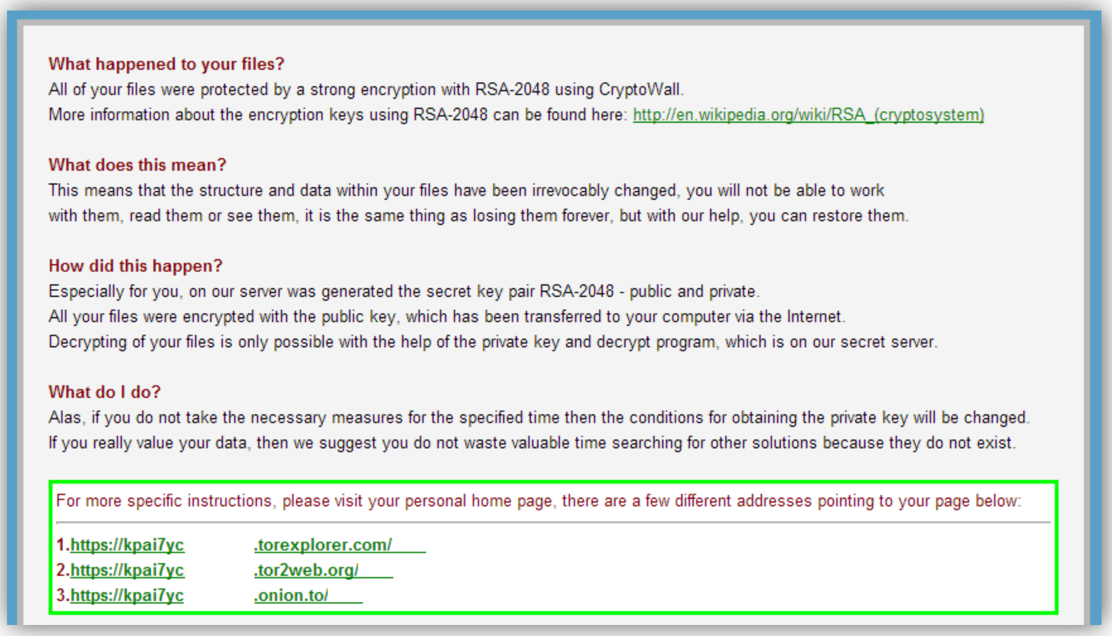
For more information you should find txt file named Bitcrypt.txt on your hard drive.

```
====================================================================================================
BitCrypt v2.0 (bug fixed)
====================================================================================================
English

Attention!!!

Your BitCrypt ID: WIN-244-6153232


All necessary files on your PC ( photos, documents, data bases and other) were encoded with a unique RSA-1024 key.
Decoding of your files is only possible by a special programm that is unique for each BitCrypt ID.
Specialists from computer repair services and anti-virus labs won't be able to help you.
In order to receive the program decryptor you need to follow this link http://www.bitcrypt.cc and read the instruct

If current link doesn't work but you need to restore files please follow the directions:
1. Try to open link kphijmuo2x5expag.tor2web.com. If you failed proceed to step 2.

2. Download and install tor browser http://www.torproject.org/projects/torbrowser.html.
```

Image 3 - The message displayed by BitCrypt upon infection

Many ransomware infections come from “drive-by downloads” on compromised websites, for example CryptoLocker was frequently delivered using the GameOver/Zeus exploit kit. However, other infection mechanisms have also been used, including emails with a malicious attachment or link. Encrypting ransomware frequently demands payment in alternate currency such as Bitcoin or Litecoin.

[8] http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.https://kpai7yc .torexplorer.com/
2.https://kpai7yc .tor2web.org/
3.https://kpai7yc .onion.to/

Image 4 - Instructions for file recovery as shown by CryptoWall

Files selected for encryption differ between variants but encrypting ransomware will typically target files on all accessible drives including fixed (local) drives, removable media and network shares.

Further technical information on the evolution of ransomware can be found in the Sophos paper "Ransomware: Next-generation Fake Antivirus"[9].

3.3 Modern Encrypting Ransomware – Smartphones and Tablets

After the relative success of PC-based trojans there have been a number of instances of ransomware for smartphones or tablet devices. For example in May the Reveton ransomware was observed on the Android platform[10].

It is possible that the overall effect on these platforms will be lower; current trojans require users to have a jailbroken device or to manually install software. In addition many mobile platforms implement technical controls such as application sandboxing which can improve resilience against unauthorised modification of data. It should be noted that mobile devices will often still have the concept of shared data which is accessibly by applications. This data typically includes photographs and downloaded content. As a result the impact while potentially less can be still somewhat disruptive.

Where devices are issued to staff the policy should lock down changes to configuration and ensure that users are unable to modify their device in a manner that could affect corporate data or that corporate data is sufficiently segregated from user installed apps.

3.4 Modern Encrypting Ransomware – Apple Mac OS X

To date while we have seen low grade non-encrypting ransomware samples target Mac OS X users[11] no publically documented samples of encrypting ransomware have been seen. This lack of

[9] http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/ransomware-next-generation-fake-antivirus.aspx
[10] http://labs.bitdefender.com/2014/05/reveton-icepol-ransomware-moves-to-android/
[11] http://blog.malwarebytes.org/fraud-scam/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-

samples however, should not be interpreted as the platform being immune to such threats. When Windows targets begin to yield less for the criminals in terms of payments it is only reasonable to predict that criminals will look to alternate platforms and thus consider Mac OS X as a viable platform to target.

4 Defensive Strategies

This section presents a number of suggestions for mitigating modern ransomware trojans. Please contact NCC Group if you require advice specific to your organisation or to understand how to deploy these technical mitigations in your corporate environment.

It is important to note that antivirus is only part of a viable defensive strategy against ransomware due to the large number of new variants each day. We recommend a mixture of user education, policy & procedure and technical mitigations to reduce the risk of ransomware trojans and mitigate the impact if an infection occurs.

4.1 Best Practice Advice

Best practice advice should be followed at all times, including (but not limited to) the following:

- Regular backups should be taken of all critical data and where possible be stored off-line or in a manner which will ensure integrity
- Antivirus should be installed and regularly updated on all machines
- Patches for operating systems and software (especially web browsers, office suites and common document readers) should be installed as soon as they are available
- Corporate laptops should use a VPN connection (with two-factor authentication where appropriate)
- Restrictive access control should be employed to ensure users can only access the data for their function
- Regular, on-going security testing should be conducted

4.2 Policy & Procedures and User Education

Every company, regardless of size, should have a business continuity, disaster recovery plan and incident management policy along with a set of supporting procedures. These policies and procedures should consider the impact to routine business if computer systems were unavailable or data was lost. Individuals should be appointed and given the authority to make decisions during an incident, including the ability to call in external help where required.

Users should be regularly reminded of the acceptable use policy for corporate assets, including whilst machines are operated at remote locations or from home. Advice should be provided to users about the risks from browsing inappropriate websites, installing unauthorised software or opening malicious emails.

4.3 Technical Mitigations

In order to limit damage to data stored on network shares it is advisable to map these as local drives only when absolutely required. User or group-based file permissions should be implemented to protect data from being deleted or modified by users who do not have a valid business reason to make changes.

Some resilience may be gained from running a different antivirus product on servers than the one used on laptops or workstations. However, it is more important to ensure that any antivirus or security products are regularly updated and online features (cloud-based protection) are enabled

users/

where appropriate.

In some corporate environments it may be possible to apply a whitelisted approach to external internet access. Access can be enabled only for sites directly relevant to the business, reducing the risk of drive-by downloads from unauthorised websites or personal webmail.

A powerful technical mitigation is the use of Software Restriction Policies (SRP) on Microsoft Windows platforms. On some locked-down workstations, these can be used to whitelist specific applications[12]. However, in many corporate networks it is more realistic to restrict execution from a small number of common directories, as described in the following section.

For mobile devices where the ability exists via Mobile Device Management to limit which applications can be installed either device wide or within a dual-persona corporate container it is recommended that this functionality be leveraged.

For organizations using Mac OS X in order to be able to block certain applications or untrusted binaries a third party aftermarket solution will be required.

4.3.1 Software Restriction Policies on Microsoft Windows

In most cases ransomware is delivered directly from an exploit kit in a web browser or as an email attachment. Therefore it is essential to restrict access to file system locations that programs are likely to be executed from. These locations are usually temporary directories, used by software such as Internet Explorer, WinZip, WinRAR or 7-Zip.

Software Restriction Policies (SRP) are a feature introduced in Windows XP and Server 2003, which allow users and domain administrators to control the ability of programs to execute. This is achieved within the context of whitelisted and blacklisted paths, file names, network zones and executables identified by their hash or their publisher certificate.

There are usually three directories where files are temporarily stored upon extraction or when clicking “Run” instead of “Save” when downloading an executable with Internet Explorer:

- %AppData%
- %LocalAppData% (Windows > 6.0)
- %UserProfile%\Local Settings (Windows XP)

Applying a restriction policy to the above folders will also affect their sub-folders, thus it is crucial that administrators whitelist any executables that already exist in the directory tree as long as they are sure that they are not malicious. In the table below are listed directories that are likely to be used by software to extract in and run their content from.

Table 1 - Important paths to apply restrictions

Name	Path	Comments
Application Data	%AppData%	
Local Settings	%LocalAppData%	Windows > 6.0
Local Settings	%UserProfile%\Local Settings\	Windows XP
Outlook 2010 Attachments	%HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security\OutlookSecureTempFolder%	Path derived from registry key
Outlook 2010 Attachments	%HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\14.0\Outlook\Security\OutlookSecureTempFolder%	Path derived from registry key

[12] http://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf

Name	Path	Comments
Outlook 2007 Attachments	%HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Outlook\Security\OutlookSecureTempFolder%	Path derived from registry key
Outlook 2007 Attachments	%HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security\OutlookSecureTempFolder%	Path derived from registry key
Outlook 2003 Attachments	%HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security\OutlookSecureTempFolder%	Path derived from registry key
Outlook 2003 Attachments	%HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\Security\OutlookSecureTempFolder%	Path derived from registry key

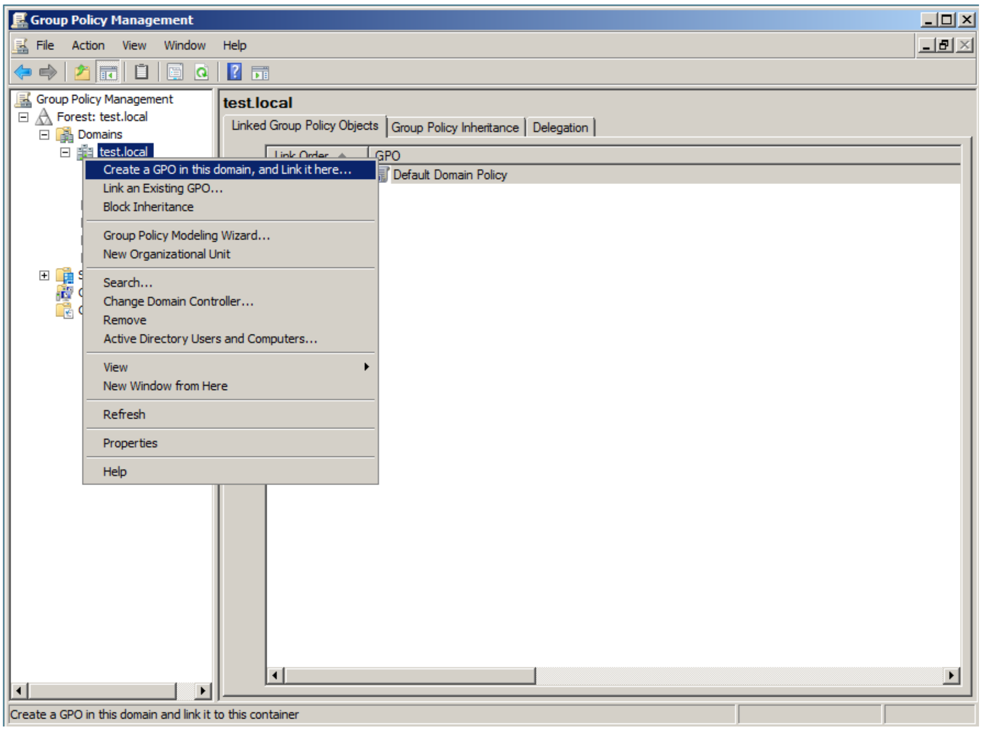
There also some application specific folders that may need to be whitelisted or considered separately from wider SRP implementation.

Table 2 - Optional paths

Name	Path	Comments
Internet Explorer Temporary Internet Files	`%LocalAppData%\Microsoft\Windows\Temporary Internet Files`	
Windows Built-in Zip	`%LocalAppData%\Temp\*.zip\`	Windows > 6.0
Windows Built-in Zip	`%UserProfile%\Local Settings\Temp\*.zip\`	Windows XP
WinRAR	`%LocalAppData%\Temp\Rar*\`	Windows > 6.0
WinRAR	`%UserProfile%\Local Settings\Temp\Rar*\`	Windows XP
WinZip	`%LocalAppData%\Temp\wz*\`	Windows > 6.0
WinZip	`%UserProfile%\Local Settings\Temp\wz*\`	Windows XP
7-Zip	`%LocalAppData%\Temp\7z*\`	Windows > 6.0
7-Zip	`%UserProfile%\Local Settings\Temp\7z*\`	Windows XP

NCC Group has prepared a step-by-step guide on how to create and apply the Software Restriction Policies.

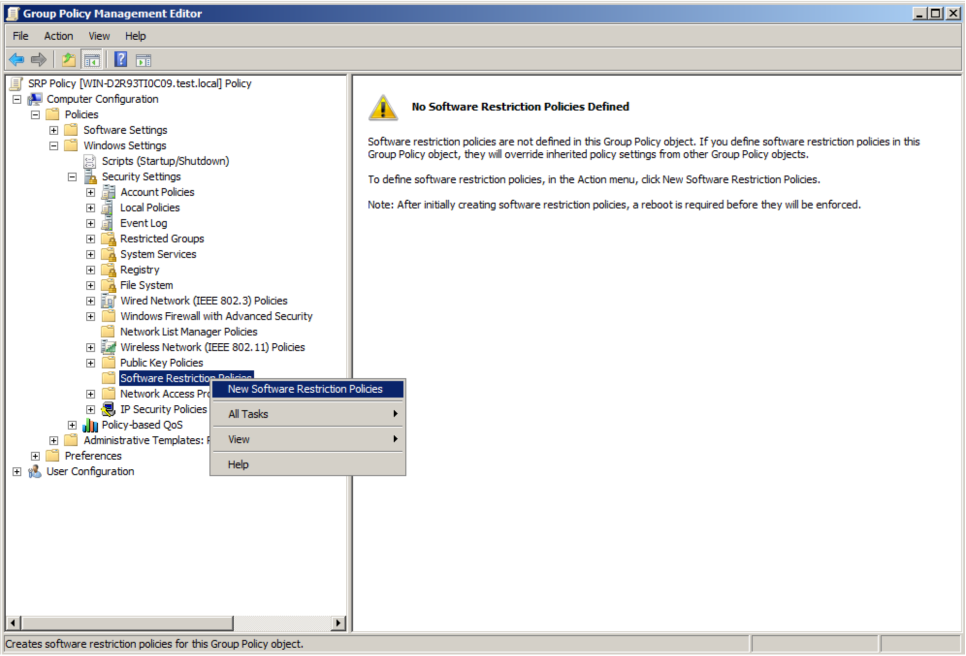
1. On the Domain Controller, load the Group Domain Management console (e.g. run the command “gpmc.msc”).
2. In the correct domain, right click and choose “Create a GPO in this domain” as shown in the screenshot below. Alternatively, you can choose to edit the Default Domain Policy but this is **not** recommended.



Create a GPO in this domain and link it to this container

Image 5 - Creating a new Group Policy object

3. Type a new name for the policy and click “OK”.
4. Right click on the new policy and choose “Edit”. This will bring up the Group Policy Management Editor which will allow configuring the SRP.
5. Go to “*Computer configuration -> Windows Settings -> Security Settings -> Software Restriction Policies*”. If no SRP have been defined before, right click and choose “New Software Restriction Policies as shown in the screenshot below.


Group Policy Management Editor
File Action View Help
SRP Policy [WIN-D2R93TI0C09.test.local] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Pro
IP Security Policies
Policy-based QoS
Administrative Templates:
Preferences
User Configuration
New Software Restriction Policies
All Tasks
View
Help

No Software Restriction Policies Defined

Software restriction policies are not defined in this Group Policy object. If you define software restriction policies in this Group Policy object, they will override inherited policy settings from other Group Policy objects.

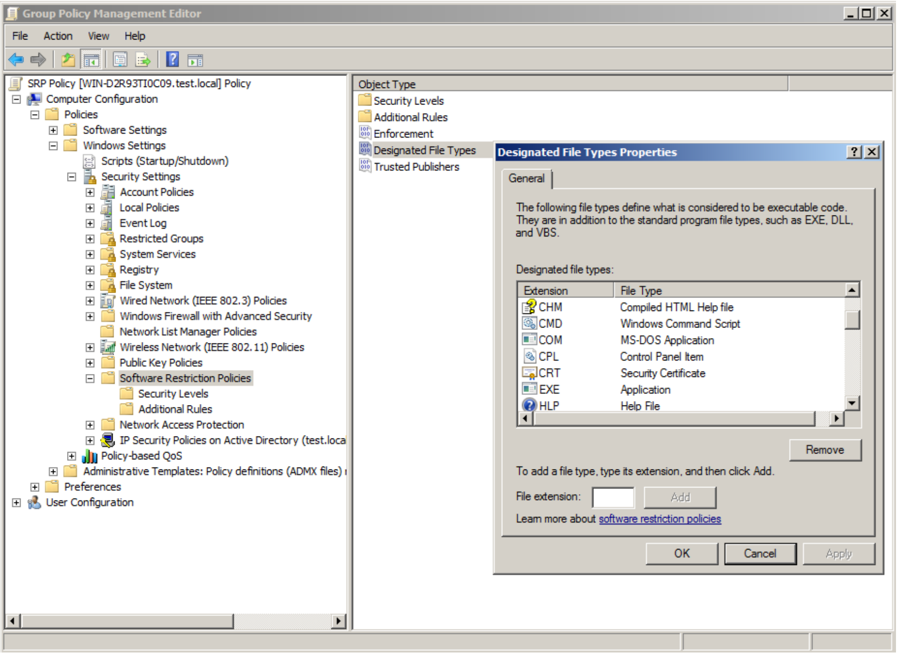
To define software restriction policies, in the Action menu, click New Software Restriction Policies.

Note: After initially creating software restriction policies, a reboot is required before they will be enforced.

Creates software restriction policies for this Group Policy object.

Image 6 - New Software Restriction Policies

6. Defined in the “Designated Files Types” window are all the file extensions which are considered executables. The list can be modified by adding new or removing existing extensions. Because many programs have shortcuts in one of the `%AppData%` sub-folders (such as pinned programs on the Quick Launch bar) they might stop working despite the fact that the actual executable is located in a non-blacklisted path. This is due to the fact that the shortcut extension, `.lnk`, is included in the “Designated File Types” list. In this case, the extension can either be removed from the list or the desired shortcuts can be added to a separate whitelist.


Group Policy Management Editor
File
Action
View
Help
SRP Policy [WIN-D2R93TI0C09.test.local] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access Protection
IP Security Policies on Active Directory (test.loca
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) i
Preferences
User Configuration
Object Type
Security Levels
Additional Rules
Enforcement
Designated File Types
Trusted Publishers

Designated File Types Properties

General

The following file types define what is considered to be executable code. They are in addition to the standard program file types, such as EXE, DLL, and VBS.

Designated file types:

Extension	File Type
CHM	Compiled HTML Help file
CMD	Windows Command Script
COM	MS-DOS Application
CPL	Control Panel Item
CRT	Security Certificate
EXE	Application
HLP	Help File

Remove

To add a file type, type its extension, and then click Add.

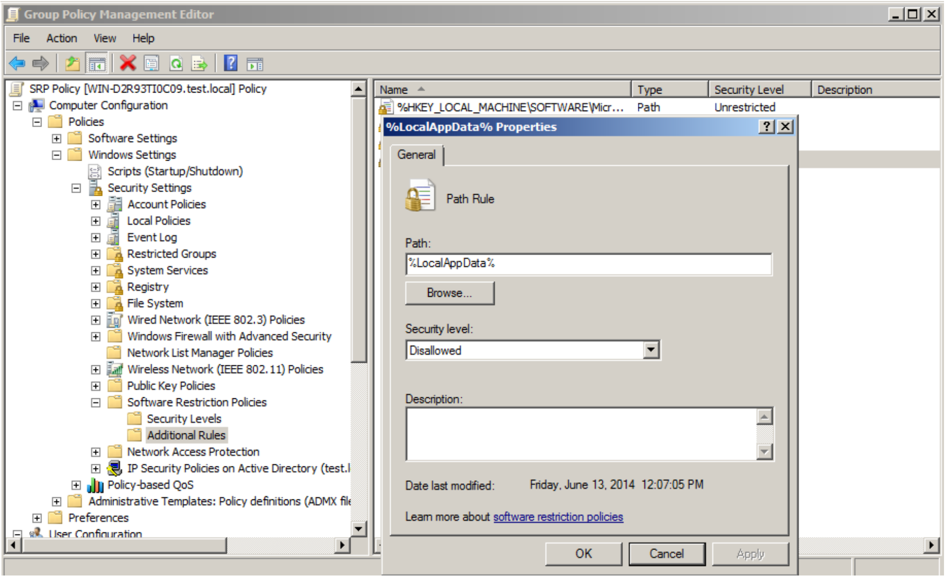
File extension: Add

Learn more about software restriction policies

OK Cancel Apply

Image 7 – Viewing designated file types

7. Under “Additional Rules” we can create new rules by right clicking and selecting “New Path Rule” as can be seen below.


Group Policy Management Editor
File
Action
View
Help
SRP Policy [WIN-D2R93TI0C09.test.local] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access Protection
IP Security Policies on Active Directory (test.l
Policy-based QoS
Administrative Templates: Policy definitions (ADMX fil
Preferences
User Configuration

Name	Type	Security Level	Description
%HKEY_LOCAL_MACHINE\SOFTWARE\Micr…	Path	Unrestricted	

%LocalAppData% Properties

General

Path Rule

Path: %LocalAppData%

Browse...

Security level: Disallowed

Description:

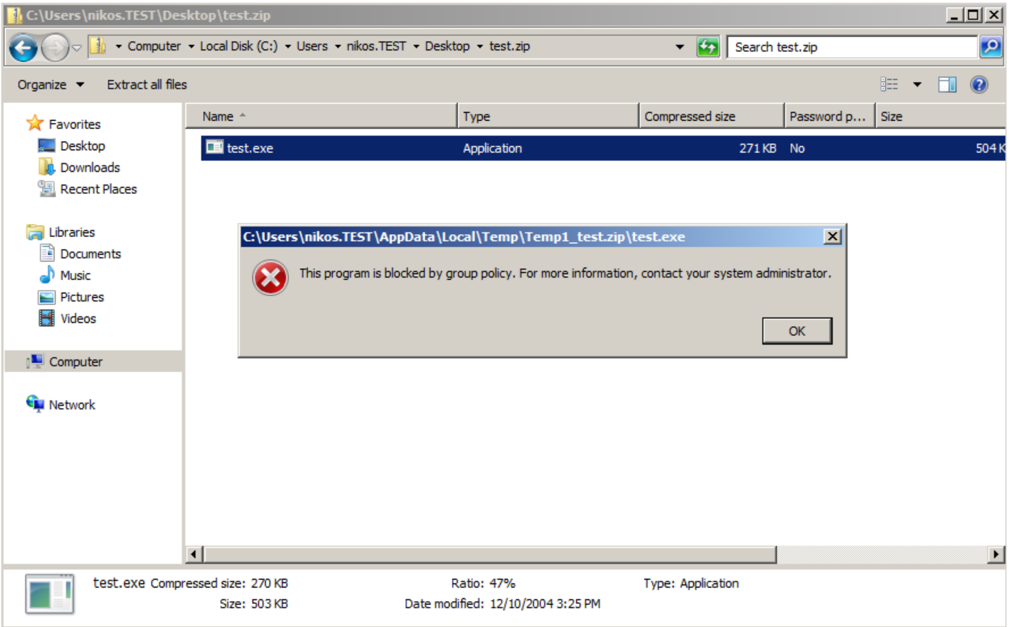
Date last modified: Friday, June 13, 2014 12:07:05 PM

Learn more about software restriction policies

OK Cancel Apply

Image 8 - Adding a new path rule

The policy will be applied when a domain user logs in. In a realistic scenario that a user receives an email containing a ZIP attachment with malware in it, the user will see the following message:



C:\Users\nikos.TEST\Desktop\test.zip

Name	Type	Compressed size	Password p...	Size
test.exe	Application	271 KB	No	504 K

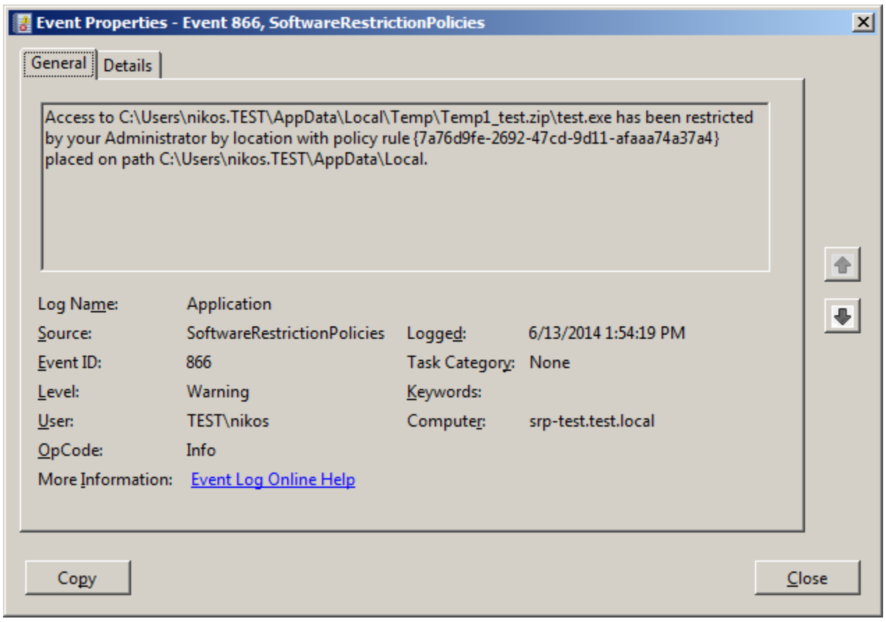
C:\Users\nikos.TEST\AppData\Local\Temp\Temp1_test.zip\test.exe

This program is blocked by group policy. For more information, contact your system administrator.

test.exe Compressed size: 270 KB Size: 503 KB Ratio: 47% Date modified: 12/10/2004 3:25 PM Type: Application

Image 9 - The error message displayed to a user when a program is blocked

Even though the zip file was saved on the user's desktop, the malware was temporarily extracted in `%LocalAppData%` where a Software Restriction Policy was in place, hence protecting the user from accidental infection. The incident will be logged by the Event Viewer as a warning as show in the screenshot below.



Event Properties - Event 866, SoftwareRestrictionPolicies

Access to C:\Users\nikos.TEST\AppData\Local\Temp\Temp1_test.zip\test.exe has been restricted by your Administrator by location with policy rule {7a76d9fe-2692-47cd-9d11-afaaa74a37a4} placed on path C:\Users\nikos.TEST\AppData\Local.

Log Name: Application
Source: SoftwareRestrictionPolicies
Logged: 6/13/2014 1:54:19 PM
Event ID: 866
Task Category: None
Level: Warning
Keywords:
User: TEST\nikos
Computer: srp-test.test.local
OpCode: Info
More Information: Event Log Online Help

Image 10 - The incident as shown in Windows Event Viewer

This configuration whilst not a panacea can mitigate in a manageable fashion the common infection vectors used by encrypting ransomware on Microsoft Windows today.

5 Conclusions

Due to the financial success of recent ransomware trojans it is likely that new variants will continue to emerge. Successfully defending against modern encrypting ransomware will require a blended approach of user education, technical mitigations and preparation for if an incident occurs.

Implementing technical controls can take time and require careful testing; however these are likely to assist with the overall defence against both ransomware and other threats. Compared to the potential cost of losing corporate data this investment is likely to prove worthwhile.

NCC Group can offer proactive advice, security assurance and incident response services. If you are an existing customer please contact your account manager for tailored advice and consultancy.

6 References & Further Reading

- Wikipedia: Ransomware - http://en.wikipedia.org/wiki/Ransomware_(malware)
- US-CERT: Alert (TA13-309A) CryptoLocker Ransomware Infections - http://www.us-cert.gov/ncas/alerts/TA13-309A
- Federal Trade Commission: FTC, FBI Warn Consumers About ‘Cryptolocker,’ A New Breed of Computer Malware - http://www.ftc.gov/news-events/press-releases/2014/02/ftc-fbi-warn-consumers-about-cryptolocker-new-breed-computer
- Sophos: CryptoLocker urgent alert - here's how YOU can help! - http://nakedsecurity.sophos.com/2013/11/16/cryptolocker-urgent-alert-heres-how-you-can-help/