bsi.

...making excellence a habit.™

Ransomware

Mitigating against this evolving threat

A Whitepaper

Executive summary

Ransomware is constantly evolving as malware writers identify more effective methods of infection and exploitation, in an attempt to create ever more effective malware that will ensure that payment is the victim's only option. This document provides a high level overview of ransomware and some guidelines on how to protect against the threat of this particular type of malware.

Ransomware is the term commonly used to describe a virus or malicious software that when executed will attempt to block access to a computer system or specific files that are likely to be of value to the victim. The ransomware then demands payment in return for providing the access to the system or documents, often demanding payment be made using bitcoin.

For an individual such an attack can be devastating as they may lose personal documents as well as photos of great sentimental value. However, such an attack on a business could have far more serious consequences apart from reputational damage, such as preventing the organization from conducting its normal day to day business. Hackers may also threaten to leak sensitive corporate files should the company refuse to pay the ransom.

Ransomware makers are constantly working to improve their malware as they attempt to stay one step ahead of security researchers and antivirus vendors. As a result, system administrators should expect to experience and have a plan to deal with such an event as part of their security policy.

How ransomware infects a system

With the improvements in software development practices and security awareness, modern Operating Systems (OS) are becoming increasingly robust, leading hackers to focus their efforts on weaker entry points for their attack. As a result, the end user has become the attack vector of choice for the majority of attacks.

Spam and phishing emails are commonly used to target unsuspecting end users in order to trick them into opening an attachment containing a malicious payload. The attachment is often an archive file (ZIP or RAR) containing code that will download or execute a payload upon opening. Macro enabled Microsoft Office documents are also commonly used to execute malicious payloads.

In addition, zero day vulnerabilities in applications such as Oracle, Java, Apple QuickTime, Adobe Reader, Adobe Flash, Microsoft Silverlight and web browsers have been targeted using infected websites and exploit kits such as Rig and Nuclear.

Once the attack is successful and the payload has executed, ransomware such as CryptoWall, TorrentLocker, TeslaCrypt and CTB-Locker encrypt specific files and documents. This is done using encryption that aligns to the Advanced Encryption Standard (AES). An AES encryption key is also encrypted using AES, therefore making it virtually impossible to decrypt the victims files. During the infection stage some ransomware variants, such as TorrentLocker, are known to take additional steps to ensure that the full impact of the attack is achieved, such as deleting the Volume Shadow Copy Service (VSS) items from the infected system to prevent backup copies of the encrypted files being restored.

At this point the ransomware will typically display a demand for payment in order to decrypt the files and in some instances may offer to decrypt two files for free to convince the victim to pay the ransom.

In a home user environment this attack may be limited to a single computer, however in a corporate environment where the user may have mapped network drives, the malware would have access to a far greater number of systems and documents that could be encrypted, thereby compounding the impact of the attack.

How to protect against ransomware

A Defence in Depth approach will help mitigate against malware and ransomware attacks and help reduce the impact should an attack be successful. The following actions should be implemented as a minimum to help mitigate against such attacks:

- **Regular offline backups**

Regular backups of all critical systems and files should be taken and stored offline, to prevent backup files from being encrypted or deleted by malware. These backups should be tested to ensure they will work in the case of restoration.

- **Ensure operating systems are regularly patched**

Operating systems and third party application software should be regularly patched to mitigate against known vulnerabilities.

- **Use up to date antivirus software**

Ensure that all systems have appropriately configured antivirus scanning policies and that the virus signature updates are applied regularly. The use of Host Intrusion Prevention Software (HIPS) should also be considered as an additional layer of defense on critical or exposed systems.

- **Where possible, use a content aware proxy to screen inbound and outbound traffic**

A content aware proxy server used to examine all inbound and outbound network traffic can control and block malware at the perimeter before it has a chance to execute. In addition, effective monitoring web traffic logs could assist in identifying suspicious network traffic. All outbound access should be blocked by default other than allowing web traffic through the web proxy.

- **Harden end user systems**

The end user systems are effectively the target of the attack and therefore applying appropriate hardening can prevent malware from executing:

  - Disable support for macros in all Microsoft Office documents, such as Word, Excel, and PowerPoint
  - Disable ActiveX content in Office applications.
  - Users should be assigned minimal permissions to conduct the work, in accordance with the principle of least privilege
  - Remove unnecessary software from systems to reduce the attack surface
  - Block the execution of binaries from the %APPDATA%, %OSDRIVE%\Users and %TEMP% paths using Software Restriction Policies (SRP). An example configuration for this can be found at the end of this document
  - Install and enable a pop-up blocker for web browsing
  - Disable JavaScript in web browsers where possible using a browser plugin such as "NoScript"
  - Use a modern sandboxed web browser such as Google Chrome
  - Block particular email attachments such as executables, batch files, JavaScript files

- **Educate system users**

Regular and engaging security awareness training should be a key mitigation against malware attacks, as without an end user opening malicious content, the attack cannot be successful.

Therefore, by empowering end users to be able to recognize the threat, they will be less susceptible to falling victim to the attack. In addition, training users on how to respond in the event of a successful attack can limit the overall damage. Users should be made aware of the risks associated with phishing emails, spam and opening malicious attachments.

What to do if infected

In the event that you or your organization have the misfortune of being the victim of a ransomware attack, it's recommended that the ransom demand be ignored. Paying the ransom does not guarantee the recovery of the affected files and will only encourage ransomware creators to further develop their capabilities. In addition, by paying a ransom it may make you or your organization a target for further attacks, as the hackers know there is a good chance that further payments will most likely be made in future.

The following actions should be considered when dealing with an infection:

- Isolate the infected machine from the network to prevent the spread of infection
- Conduct an analysis of the system infection to identify the attack vector and where possible, make changes to prevent future exploitation of the identified attack vector
- Remove the malware from the infected system using antivirus and/or if possible format the system and apply a clean operating system image
- Restore files and documents from most recent backup prior to infection
- Report the attack to law enforcement

Configuring Microsoft Software Restriction Policies (SRP)

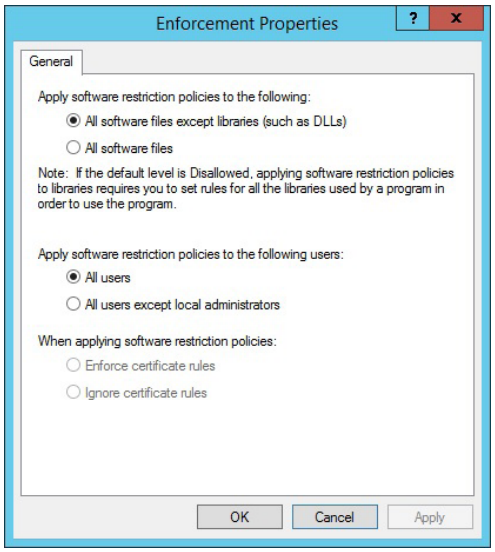
The Microsoft SRP feature provides administrators with a mechanism for controlling the ability for software to execute on a system. The policy can be applied to domain systems using Group Policy or on individual systems using the Local Security Policy.

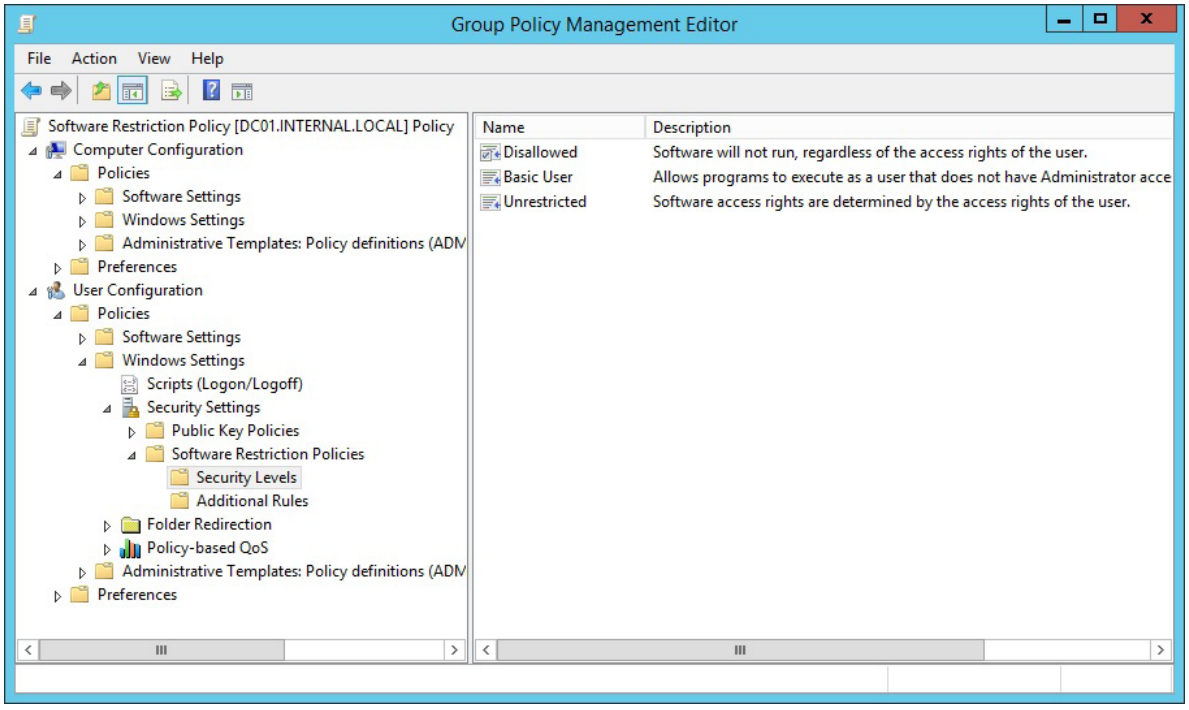
By blocking the execution of binaries from the %APPDATA%, %OSDRIVE%\Users and %TEMP% paths, and only allowing applications to execute from the Windows and Program Files directory, the ability for malicious attachments or downloads to execute is greatly reduced.

The following configuration should tested as a starting point in using SRP to lockdown applications on systems.

1. Create an SRP and set the enforcement option to apply to "All software files except libraries (such as DLLs)" and "All users".

2. Configure the Default Security Level to "Disallowed". This will prevent all applications from executing, regardless of the access rights of the user.

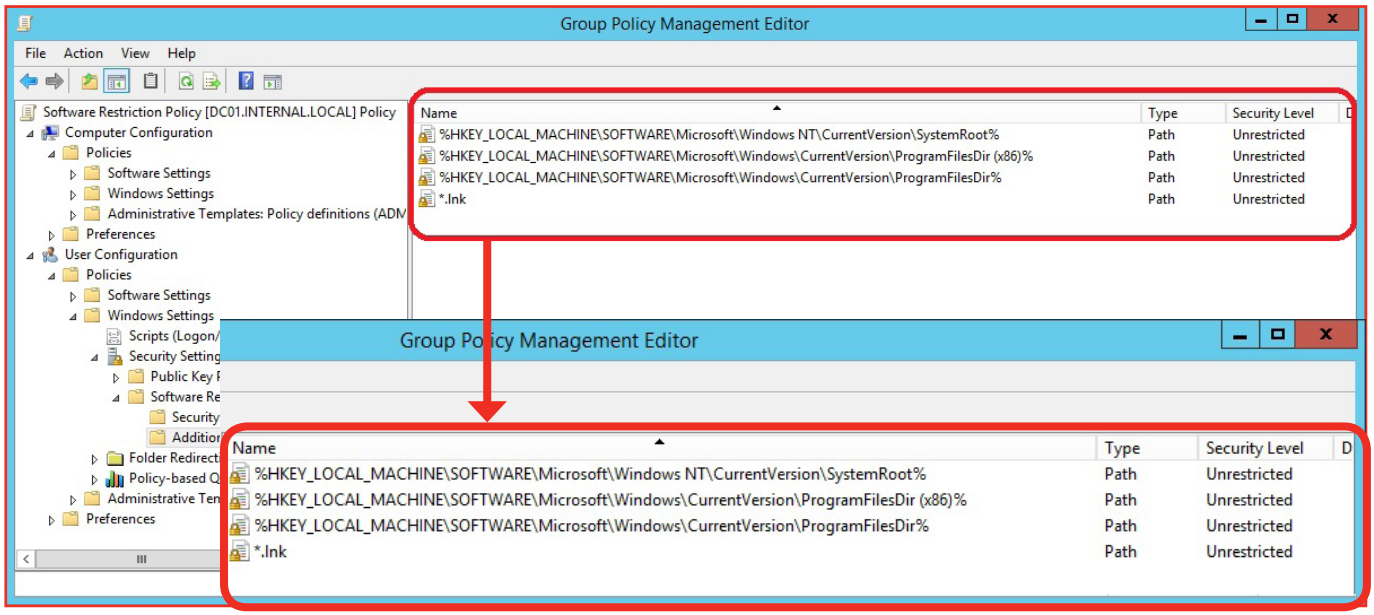




3. Configure "Additional Rules" for the following permitted paths:

- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%
- *.lnk

These rules define the exceptions to the "block all" configuration created in steps 1 and 2, and permit the execution of files used by the Windows OS and installed applications.



4. Test the configuration on a non-production environment prior to implementation to ensure that the changes do not affect critical applications

Software Restriction Policies can be further customized to meet more specific requirements such as using hash or certificate rules to restrict or allow applications regardless of their location. Further information on configuring SRP can be found in the Microsoft document located in the references section.

Conclusion

We offer a range of services and solutions to help clients protect and avoid cyber threats such as ransomware and malware attacks. Our consultants work with you to enable you to better respond to security incidents and help you build a more resilient IT infrastructure and protect your critical data.

For more information visit **bsigroup.com** or email: *cyber@bsigroup.com*

References

NoScript Firefox extension
https://noscript.net/

TechNet - Using Software Restriction Policies to Protect Against Unauthorized Software
https://technet.microsoft.com/en-gb/library/bb457006.aspx

Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience help you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that effect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services.

Security awareness

Phishing and user awareness training, SaaS solutions, social engineering and simulation testing

Data management and privacy

GDPR services, information lifecycle management and eDiscovery and forensics

Compliance and testing

PCI DSS services, cyber lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

CYBER ESSENTIALS

CREST STAR

UKAS TESTING 8237

Find out more

Call UK: +44 345 222 1711
Call IE: +353 1 210 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

bsi.