Ransomware Response

First Response and Best Practices

Ransomware is one of the dominant threats currently facing healthcare IT departments. It is the modern digital equivalent of the age-old crime of kidnapping. As a member of the information services department, your first objectives when responding to a report of ransomware are to take the infected PC off the network as soon as possible and to prevent any further spread.

Ransomware Response

First Response and Best Practices

Ransomware is a form of malicious software that can spread through worms or viruses, called cryptoviruses. Its purpose is to encrypt an infected computer's files and then hold them for ransom, forcing the computer user to pay for a decryption key in order to unlock their data. There are a number of different names for ransomware such as WannaCry, CryptoLocker, Bad Rabbit, and more. The earliest forms of the cryptovirus would infect computers through email attachments or malicious downloads that when opened would rapidly spread throughout the computer. These early forms of ransomware would then encrypt files and demand a payment in order to decrypt, usually through easy to use pay cards or overseas money transfers. The earliest forms of ransomware were easy to stop and decrypt and often had the decryption key buried in the virus itself. Competent security professionals were able to decrypt the files quickly and with freely available online tools. Newer forms use more sophisticated techniques making it very difficult, if not impossible, to decrypt files without a decryption key and generally require payment to a bitcoin account- making it almost impossible to track the bad actors.

Attack Vectors

Ransomware spreads through a number of methods. The earliest forms spread through email attachments, zip files, office documents, macros, or executable files. Newer types of ransomware spread through a number of different routes. They can be spread through the normal methods just mentioned, but also through bad URL links, website advertising, website drive-by attacks, browser add-ons, and more. Several outbreaks have been attributed to phishing attacks, and there are methods for attacking through SMS and instant

Ransomware: An International Problem

We are aware that a number of NHS (National Health Service) organizations have reported they have suffered from a ransomware attack, this is not targeted at the NHS. It is an international attack. A number of countries and organizations have been affected.
– Theresa May

messaging. Originally, ransomware was a Windows problem, but it now exists on all major platforms including MacOS, iOS, Linux, and Android.

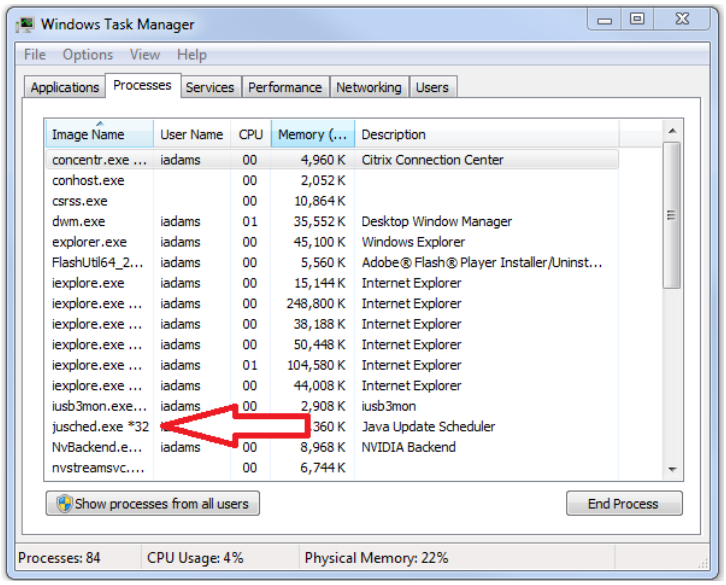
How to spot Ransomware

Most antivirus or antimalware programs will notify the user or system administrator if they detect or quarantine ransomware. It is quite common to notice a computer running sluggish when ransomware is running on a computer. Encrypting files is a slow, memory and CPU intensive task. Opening the task manager and noticing an unfamiliar program consuming a large portion of the CPU is a warning sign. Another common sign is receiving unexpected notifications that files are ready to be burned to a disk. Some (not all) forms of ransomware will target system `.ini` files. In the **`c:\Users\\AppData\Local\Microsoft\Windows\Burn\Temporary Burn Folder`** there is `a desktop.ini` file that is there all of the time. When the ransomware encrypts the file, and then deletes the original and leaves behind the encrypted replacement, Windows spots the new file and thinks you have new items to burn to a disk.

Other things to look for are unexpected files on the desktop with names like:

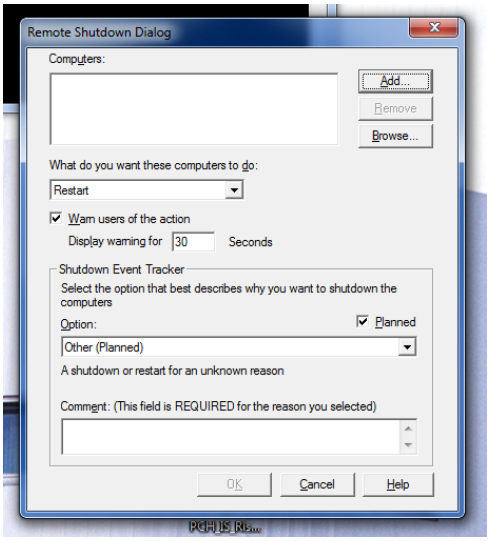
- `Restore_files_rvrk.html`
- `Recover_instruction`
- `Want your files back.`
- `Confirmation.key`
- `Cryptolocker`
- `Decrypt_instruct`
- `How_to_recover`
- `Readme_for_decrypt`

There are of course many, many more. Obviously if you suddenly cannot access files, if files you normally use are encrypted or missing, you should immediately assume an infection. One other important note is that most ransomware runs as a 32 bit application, meaning it will have a *32 next to the process name when viewing your running processes in Task Manager. Since most people are running x64 versions of Windows, noticing a 32 bit CPU intensive program running, that you do not recognize, can be a quick red flag and something to be on the lookout for.



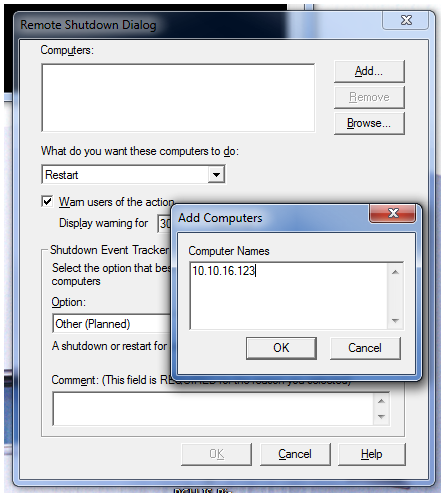
First Response

When making the initial response to a report of ransomware our first concern must be to stop it from spreading, both on the computer and across the network. If the responder is at the computer, and ransomware is confirmed, you will want to shut down as quickly as possible, pull the power cable and disconnect the network or force the computer to do a hard shut down. Taking the time to properly shut down the computer gives the cryptovirus additional moments to work or spread across the network. If you are uncertain about the presence of ransomware, immediately disconnect the network cable (or disable wireless) while checking the computer out.

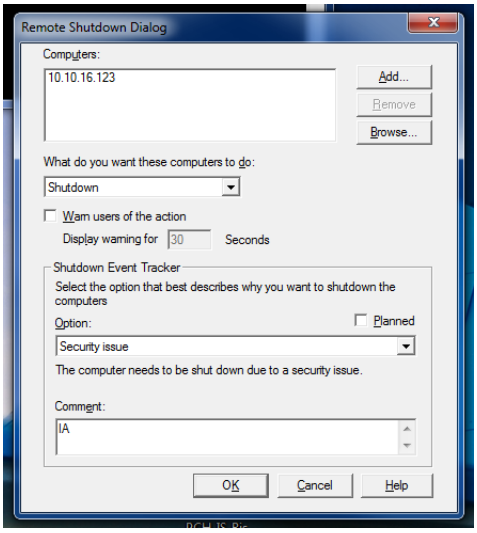


If you are not at the computer, it needs to be shut down remotely. You will need to open a command line with domain administrator privilege. This can be done under any logon by typing `cmd` into the start menu search bar, then right clicking on the `cmd.exe` program and choosing Run as administrator. At the command prompt type `shutdown -i` this will bring up the Remote Shutdown Dialog.

```
C:\Users\iadams>shutdown -i
```



Once the dialog box is open, click the Add button on the top right, enter the computer name or IP address of the computer and press OK.



Next, change the drop down menu to Shutdown, uncheck the box for *Warn users of the action*, uncheck the box next to *Planned,* Change the *Option* to *Security Issue*, then put initials in the *Comment* field and press OK. That should shut down the computer. It is important to then go and pull the computer so that users do not attempt to restart it.

You can practice this at any time on your computer so that you are comfortable pulling it up; simply put in a bogus IP address outside of the domain ranges so that you do not accidently shut off a computer, or choose a computer IP address that is safe to practice on so that you can observe the results.

Alternatively, and this is quicker, you can use the command line by typing `shutdown -s -f -m //name` where name is the computer name. The `-s` flag means a shutdown, the `-f` flag forces the command, and the `-m` means a remote machine followed by the machine name.

```
C:\Users\iadams>shutdown -f -s -m \\7010W23
```

Again, be sure to practice either method to be comfortable, accurate, and quick with them.

The second, and equally important, part of responding to a ransomware report is to check for additional outbreaks. Quickly look at other computers in the same department, particularly those computers that might have users who access the same share folders. Check the contents of share folders as well as the servers that the shares are built on. This process should be a team effort as multiple workstations and servers may need to be checked.

Finally, the user who was last on the infected computer should be asked about what they were doing when they suspected something was wrong. Do not accuse or place blame on the user, most modern strains of ransomware can be delivered through very innocuous means and the user may not know how it happened. However, the knowledge of how the computer was infected is important in determining the potential severity of the problem as well as helping to avoid future problems.

Remediation

Once a computer has been determined to have an infection, it must NOT be reconnected to any network when attempts to clean or save documents are made. For computers that are encrypted at the disk level (i.e. Bitlocker or TrueCrypt) booting the computer in safe mode, using the `msconfig` tool to control startup programs, and finally running multiple malware cleaning tools are the only way to insure it is safe to copy files off the computer. Finally, computers that we determined to have been infected with ransomware will not be returned until they have had the hard drives wiped (or replaced) and reimaged.

Prevention Strategies

Mitigating ransomware attacks and damage begins with backups. Backup everything. Then back it up again. Once the ransomware has infected a computer and encrypted a file the only way to recover the file is through a backup, or being a sucker and paying the ransom. However, we want to do everything we can to prevent the ransomware attack from occurring. This requires thinking about prevention at several different levels. First, the end user needs to be aware of potentially dangerous actions that they might engage in. This includes opening email attachments or downloading software, clicking on website pop-ups (particularly anything that is forcing a response and locking up the browser), or visiting unknown websites.

Next, computers should be restricted from running unknown code as much as possible. Workstations should have CryptoPrevent installed and the protection plan set to Maximum. Users should not be able to install and run software themselves on any computer; it must always require administrative rights.

No users should have administrative or Power User rights when logging onto a computer. While this is true for non-IS users, it holds especially true for IS employees as well. Domain, or PC Admin, accounts should never be used to logon to a workstation, especially one that might be infected. Day to day work on the floors does not necessitate using domain accounts to logon to a computer. While this sometimes makes work quicker or easier, it violates the principle of least privilege, and leaves your account open to abuse. Computers should only be logged onto with regular domain accounts or with the local workstation administrative account, and then elevated as necessary.

Finally, the single-most important part of any strategy to prevent and mitigate ransomware is to insure that all computers are up-to-date. A number of recent ransomware outbreaks, such as the WannaCry, were successful because they infected and spread on unpatched and out-of-date workstations and servers. Even when a cryptovirus successfully infects a single workstation, having other computers on the network updated will help to prevent the virus from spreading throughout the company. This is especially true of those viruses that spread through the early SMB 1.0 protocol.

Conclusion

The advent of new technologies, changes in configurations, advances in software and even daily maintenance, among other things, can create new and unknown security holes. It is our responsibility to insure that we are doing our jobs to properly secure and use our information systems. We need to be certain that we are staying up-to-date with current developments concerning ransomware and other threats. We should be taking the time to educate our end-users as the opportunity arises. Most importantly, we need to be proactive in our daily work: updating computers and computer software as needed, insuring that we are using best practices, and responding quickly to any potential issues.

Ian Adams | Security Analyst | Information Services
Parkview Community Hospital Medical Center

Appendix 1

Protecting Personal Devices

We want to be sure to extend the same level of care to our personal devices. Many of us work from home, not to mention the prevalence of BYOD. Allowing your personal devices to become infected introduces a new attack vector into business networks, something we have to avoid. The basics of protecting your personal devices at home, as well as mobile devices, are essentially the same as those within the business environment. Keep everything as up-to-date as possible, install updates as soon as they are available, be aware of what websites you browse to, what links you open, and what you download.

Unlike the hospital's computers however, there are a number of additional steps that you can take to protect your own personal devices. If you are running Windows, be sure to install the CryptoPrevent software from Foolish IT. Using browsers that enable you to block more advertising can be helpful to prevent malvertising, and be sure to trust your browser when it says a site contains malicious information and does not want to proceed. A major consideration is moving the DNS settings on all of your devices (including home routers) to OpenDNS (Cisco Umbrella) as this helps to eliminate any communication between malware and C&C servers on the internet; it also blocks access to most of the malicious URL's that are used to distribute ransomware and other malware. DNS layer security is generally considered the first line of defense against ransomware attacks in an enterprise environment, utilizing similar methods at home is a safe bet.

Be sure to back up your personal data and the data of any family members on a regular basis. If you do get infected, that is your only recourse to restoring information. After all, you don't want your kids using "I got ransomware" as an excuse to get out of doing homework.