Ransomware White Paper

Ransomware: How to Reduce Risk and Protect Your Business

By Ralph Lawhorn

The Ransomware virus has many variants, which utilize an array of methods to find a series of entry points to infect and encrypt a company's servers and data. Most infections occur as a result of unsuspecting employees opening infected emails which appear to be legitimate or by following an emailed link or visiting an infected website. Once the virus finds an entry point, it will begin to rapidly encrypt all the drives it can quickly access within the infected system. Clare Computer Solutions (CCS) has seen it encrypt single directories, while for other users it will encrypt the entire server, Operating System, and data. This virus can be stopped by utilizing high-quality antivirus software such as Symantec Endpoint Protection, which offers traditional file-based protection, alongside web browser and download protection.

All is not lost if your system has been compromised. The virus can be removed. However, we have found that there are two solutions that work best once a system has been compromised. The two options are to restore your system from the last good backup or simply attempt to pay the ransom.

There are no tools or Data Recovery Services that can decrypt your data; it is unrecoverable in this state. You will become aware that the infection has occurred when someone attempts to access a file that has been encrypted or it hits the Server Operating System.

The Ransom

The IT industry does not encourage the payment of the ransom as it is enabling the criminals to fund their development of the next generation of Ransomware, which in turn keeps the cycle

---

going as more users are infected on a global scale. But if you have no backup process for your data or you're unsure and cannot take a chance on an unchecked backup then you may have no choice but to pay the ransom.

In our experience with this virus, the ransom requested has been anywhere from $300-$1000 and must be paid in Bitcoin. By using this payment method, these criminals cover their tracks. But, paying the ransom has risks. We have heard of instances where a key was never sent or would not work, and the criminals would not reply to further emails. As a result the client was out the money and was down for several days before they could recover their systems.

Below we have outlined the steps we recommend (which we have employed ourselves with great results) to reduce your exposure to Ransomware and other viruses. If you take nothing else away from this article, please make sure that you have a solid backup solution in place and it is working.

Knowledge is Power:

Educate your staff. One of the most common causes of infection is an employee clicking on a link or opening a file sent from a legitimate source they might have corresponded with in the past. This email is a fake, or "spoofed" email that may not have been sent from the legitimate source. If you're questioning the legitimacy of an email, carefully inspect the email. If it's from a source that that you expect to receive emails from and they are sending you an unknown file, call them and inquire before opening. If it's a link then evaluate it before clicking on it. This can be done by hovering your cursor over it (DO NOT CLICK LINK). You will be able to see the URL provided. If the URL is from an unknown sources do not click this link. Proceed to move the infected email into the trash carefully, as you do not want to open or execute a link. Once moved to the trash, you will want to dispose of these garbage emails by empting your email trash can.

Employ Content Scanning / Filtering on Email Servers:

All incoming email must be scanned for viruses. This is the primary entry point for Ransomware. The next are websites that are infected. This is where a web content filter should be used. If the website is infected, the web filter will prevent its entry. There are appliance-based solutions and cloud-based solutions that are very cost effective and can be implemented to provide this service. At CCS, we use both cloud and appliance-based solutions. Our recommendations are based on several factors: such as number of users, and sites and

management needs. Some of the products we employ are Barracuda web filters and spam filter appliances alongside cloud hosted spam filtering for our clients that want to achieve email continuity.

Maintain Patch Levels for OS and Applications:

It is an industry best practice to keep the workstations, server operating systems and applications up to date and patched as this will help prevent infection to your network. If your systems are not being monitored or managed by your IT department or IT provider then you may wish to utilize Microsoft Window's "Automatic" updates. This should assist you in patching those applications that go unnoticed.

Block End Users from Executing Malware:

Newer Antivirus and Malware programs such as Symantec, Malwarebytes and Webroot have products that work well for this service. Unfortunately, these products can block legitimate software from executing but in most cases you can simply add an exclusion that will allow your software to run. You can configure and use "Group Policies" to implement software restriction policies to prevent the threat of Ransomware from running in the protected system areas.

Install and configure Host Intrusion Prevention:

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) solutions are very helpful but do require a certain amount of administration such as monitoring for alerts, notifications and events. For these solutions although they are effective, the man hours to maintain this system can be a deterrent for most small to medium sized businesses.

Limit User Access to Mapped Drives:

If users do not need access to drives or sharing privileges then remove them from the shared list. This can be controlled based on individual user rights and permissions. Group rights and login scripts will help to map drive access in your company.

Deploy and Maintain Backups:

The most important solution we constantly recommend to our clients is to constantly backup their system. We cannot stress this enough. The biggest takeaway from this article should be that the best protection is a solid backup scheme. We prefer image-based backups like Datto,

Storagecraft and Veeam. Configure these solutions to take multiple backups or snapshots throughout each day, providing a retention policy that goes back in time (One year retention policy is common; 2-3 years is becoming the industry norm). This type of retention policy will require a large amount of storage and the most cost effective approach in most cases is cloud based. There is a cost associated in storing these backups, images or snapshots regardless if they are stored local or offsite. If you were asked to put a value on your data for insurance purposes you will find that the yearly offsite fees for protecting your data is far less than data loss.

***This is not a complete list of all the methods or solutions that can be used; however these are the most common and cost effective methods of prevention. Remember, doing something is better than doing nothing at all. Again, if you take nothing else away from this article please make sure that you have a solid backup solution in place and it is working.*

About the author: Ralph Lawhorn is the President and Chief Operating Officer for Clare Computer Solutions.

For more information about Ransomware and how Clare Computer Solutions can protect your company, contact us or visit our website at www.clarecomputer.com to find out what CCS can do for you.