ISSN No: - 2456 – 2165

Cryptolocking Technology

Poli Sivasankar Rao,
Department of Computer Science
shivamsccs@gmail.com

Malidevaraju Siva Sankar Raju,
Department of Computer Science
Sivasrav4@gmail.com

Abstract— **Attackers have developed a way to monetize files already on a victim's computer. They accomplish this through encrypting select files and then charging for access to the key. This type of malware has spawned a new classification, cryptoransomware, but is more commonly known by the name of most prevalent version, Crypto Locker, or its variants TeslaCrypt and CryptoWall. This article will discuss how it works, how it happens, and most importantly what enterprises can do to protect themselves above and beyond IDS/IPS and antivirus systems. Prescriptive guidance for ba-sic prevention, detection, mitigation, and recovery controls is offered.**

Keywords—Antivirus; Cryptoransomware; CryptoWal; TeslaCrypt; IDS/IPS; Malware;

I. CRYPTOLOCKER BASICS

The idea of a ransom attack against computer files is relatively new, but attackers are raking in millions doing just that. Rather than cracking the perimeter, taking over a system, or extracting and selling data, the data at rest is encrypted using public key infrastructure.

The files in each mapped, removable, and locally installed drive are enumerated and specific files are encrypted. The target is typically common document storage formats like Office, PDF, CSV, etc. The private key needed to decrypt the data is held by the attacker and must be purchased by the victim to regain access to the files. The victim is presented with a ransom note when logging on to the system and attempting to access files.

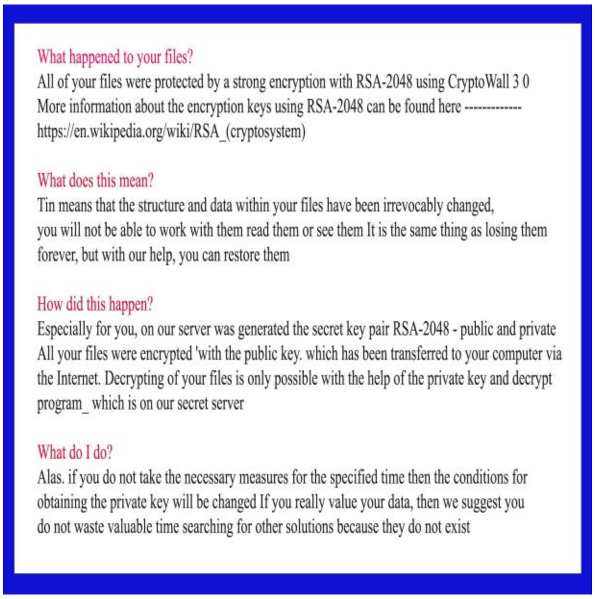
Attacks are usually three part. A compromised site or document includes an exploit kit like Nuclear or Angler, which directs the browser to download the malware from a shadowed domain. The malware executes and encrypts the files. As the files are encrypted, ransom notes are written in each Directory

Often, a randomly generated registry key is created and keeps a record of all encrypted files.

Once infected, a user has four options:

1. Pay the ransom
2. Restore from backup
3.Lose the files
4. Brute force the key

To brute force the key would require factoring 617-digit numbers, which would take about 6.4 quadrillion years on a standard desktop computer . This effectively takes brute forcing off the menu for most environments. The attack relies on public key cryptography, in which the private key needed to decrypt the data never actually exists on the victim's machine. The public key used to encrypt is all but worthless as it relates to decrypting the files.



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3 0
More information about the encryption keys using RSA-2048 can be found here ------------
https://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
Tin 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

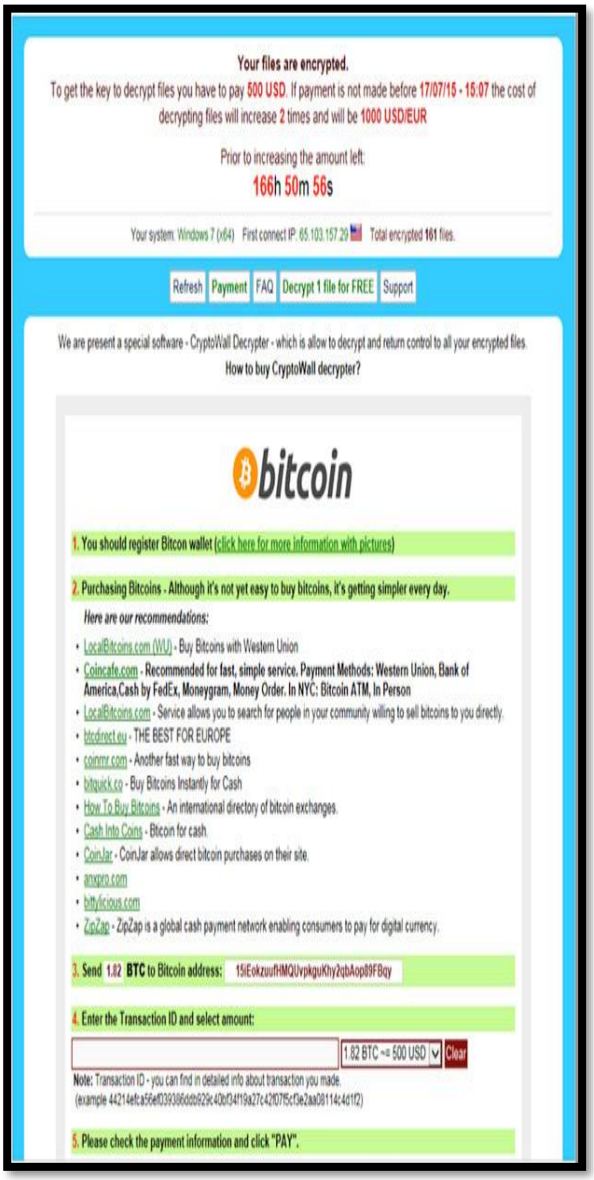
What do I do?
Alas. if you do not take the necessary measures for the specified time then the conditions for
obtaining the private key will be changed If you really value your data, then we suggest you
do not waste valuable time searching for other solutions because they do not exist

The cryptographic strength of the RSA algorithm is by design and is ordinarily used to secure web communications. For purpose of this article, brute forcing the key is not considered a legitimate recovery control.

If the victim decides to pay, the attacker typically requests payment using Bitcoin. At the time of this writing, the average ransom was between $500-750 USD. The value of the ransom will change depending on the number of encrypted files. If the victim fails to pay within the allotted time, the ransom will double or triple. Some versions offer to decrypt one file for free. Most variants offer free technical support if the victim is unable to decrypt after paying. Most variants do actually return the private key once the ransom is paid. Users can access the ransom page from the link in the ransomnote. see below screen shot.

If the victim can restore from backup, this is ideal. But for home users, this is not always the case. Many users choose to backup to removable media such as a USB hard drive. These, if left attached, will ordinarily also be encrypted with the infection. A USB drive attached to the computer but turned off or without power is likely safe, provided it is not powered over USB. Most users and enterprises will elect to lose the files that cannot be recovered from backup.

No matter what method is used post-infection—paying the ransom, restoring the files from backup, or deciding to lose the files—the operating system of the infected computer should always be re-installed in order to ensure a clean start.



Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 17/07/15 - 15:07 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:

166h 50m 56s

Your system: Windows 7 (x64) First connect IP: 65.103.157.29 Total encrypted 161 files.

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- btcdirect.eu - THE BEST FOR EUROPE
- coinrnr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bitcoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.82 BTC to Bitcoin address: 15iEokzuufHMQUvpkguKhy2qbAop89FBqy

4. Enter the Transaction ID and select amount:

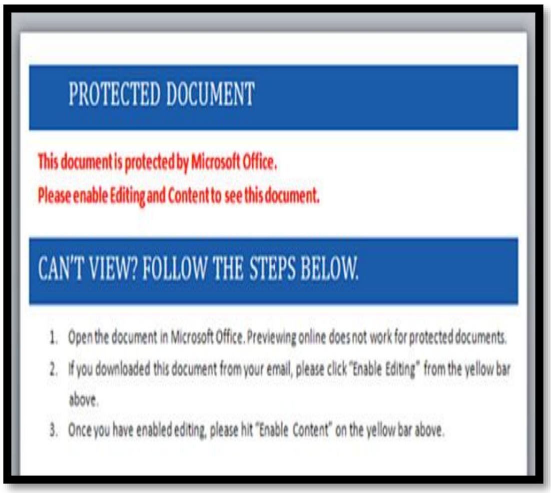
Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

What is especially impressive is not just that attackers would be so bold as to launch the attack, charge for the key, and provide technical support, but the relative ease with which these attacks succeed. This has become a true revenue stream, and the attackers are able to develop very sophisticated, clever ways to deliver their malware. The most common infection mechanisms are malicious Office documents and drive-by downloads.

III. EMAIL IS STILL A VECTOR

The malicious office documents typically are part of an email claiming to be a fax or an invoice. The user opens the document and the text of the document claims that the document is protected and cannot be viewed. However, the document comes to the rescue with instructions on how to enable the content: just follow the steps to enable macros -



PROTECTED DOCUMENT

This document is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.

Once the user follows the steps, the macro runs, the payload is delivered, and infection will commence. A variant of this is to include a zipped copy of the malicious script in hopes the user has a file association that will run the script when unzipped. Both versions rely heavily on script obfuscation techniques, so a manual or automated code review won't catch these. In some cases, the Office document is zipped; in some cases it is attached directly. Usually the filename includes .doc to mask the actual extension, .docm.

It's not just "bad" sites anymore

With the advent of content aggregating sites, users are increasingly able to visit a vast array of sites in relatively short order. Frequently, this includes personal blogs used to share ideas, most of which are built with standard templates and are not held to the same rigorous security standards that many corporate websites are held to. These sites have legitimate content and in and of themselves are not only harmless but often useful (see figure 4). Users aren't typically on guard with sites like these because they appear to be totally innocent. These, along with ads, are a typical source of drive-by downloads. Attackers need only infect a blog and wait for users to visit that page. Typically, the compromised site will include JavaScript that loads a malicious

Flash movie that runs in the background, takes advantage of an exploit within Flash, and downloads the malware.

In both cases, the actual malware is usually delivered from a randomly generated sub domain of a legitimate domain. Attackers will compromise the DNS account for a domain and register different sub domains, then use those for attack. Often, these sub domains are only used once. This has been dubbed "domain shadowing" by Nick Biasini.

IV. DEFENSE STRATEGIES

Preventing this type of infection is difficult. The attackers go to great length to hide the actual malware from analysis. The code is obfuscated. Shadowed domains are typically only used once for a given victim's public IP. The infection binary is removed when the encryption is complete. Most of the owners of sites actually delivering the malware have no idea that an infection has even occurred. Typical antivirus suites are ineffective until the machine is well beyond the event horizon.

Assuming an enterprise already has appropriate, updated email security and web browsing mechanisms in place, there are few additional protection steps that can be taken. Some firewall/IPS/IDS and web proxy solutions can be effective but leave an enterprise in the middle of the cat-and-mouse game of attacker-vs-vendor, waiting for updated signatures or definitions. Rather, it can be useful to employ a more active posture against this type of attack, of which there are four main protection mechanisms. To this end, I offer the following prescriptive guidance.

V. PREVENTIVE CONTROLS

1. First, if at all possible, disallow Flash for un trusted websites. This has some initial overhead while white listed websites are identified, but the ActiveX filtering feature in Internet Explorer has proven to be effective. Couple this with disabling Flash in Chrome and Firefox. Identify and implement a formal help-desk process to add sites to the white list. Ensure only knowledgeable personnel can approve adding to the white list.

2. Second, filter inbound email for attached ZIP and Microsoft Office documents. Consider blocking macro-enabled Office documents altogether. Often, the majorities of inbound emails that match this filter are malicious and never need to reach a user's inbox. Additionally, continue the message and inform the user that the attachment was filtered; identify and implement a formal help-desk process whereby users can request the attachment after it has been screened. An enterprise may consider white listing for this as well.

3. Third, disable macros within the Office suite. It may be appropriate to enable with notification or disable altogether. The former will give the user the ability to override and execute the macro, while the latter requires administrator intervention. Both can be installed using Group Policy.

4. Fourth, and most difficult to implement, is application white listing. There are several commercial products that can help with this. These can be restricted to only allow certain binaries to execute. This has the highest level of overhead to implement and should be a last line of defense.

VI. DETECTIVE CONTROLS

Detecting the incident based on a user noticing is not reliable and spends precious time.

The ransom note doesn't open automatically for the user until the encryption process is complete. Depending on the speed of the infected machine and the resources to which it has access, the actual encryption process can take days. Worse yet, the encryption happen in the background and the user might leave for vacation. Frequently, IT isn't notified until the user calls because his computer isn't working properly. Such an infection can avoid detection longer than some backups are held. Effective detection mechanisms can help stop an attack earlier. There are two primary detective mechanisms.

The first mechanism is an enterprise data management solution. Most CryptoLocker variants will leave small traces behind in each directory where encryption has taken place, usually a variant of files name "HELP_DECRYPT." Enterprise data management solutions can monitor for the creation of these files and even take an action such as disabling the user's Active Directory account if these files are detected.

These systems can also detect substantial data access patterns, consistent with CryptoLocker enumerating directories looking for files to encrypt. Lastly, they can assist with post-infection investigations, including identifying the time and date of the infection and which files were encrypted.

VII. RECOVERY CONTROLS

Lastly, frequent and reliable backups are key. Once the attack is successful, this is the most reliable recovery mechanism. Ensure that a recovery point objective has been considered for network files and shares. A careful review may show that this area has been overlooked and is actually mission critical. Consider both the files that could be lost as well as the loss of availability of the share, drive, or server. Once the critical file resources are identified, implement appropriate backup mechanisms. Ensure restore mechanisms are tested and staff responsible for restoring data are properly trained.

VIII. CONCLUSION

Persistent attackers have created a lucrative and effective threat. The right combination of prevention, detection, mitigation, and recovery strategies can help ensure that a would-be disaster is instead an annoyance. Hopefully, enterprises armed with an understanding of CryptoLocker fundamentals and practical security measures will be better poised to defend against it.

References

1. Nick Biasini, Angler Lurking in the Domain Shadows, Iron Geek – http://www.irongeek.com/i.php?page=videos/bsideslasvegas2015/cg04-angler-lurking-in-the-domain-shadows-nick-biasini.
2. sIBM, IBM X-Force Threat Intelligence Quarterly, 1Q 015, IBM – http://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03073usen/WGL03073USEN.PDF.
3. Villeneuve, Nart, TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware, FireEye –https://www.fireeye.com/blog/threat research/2015/05/teslacrypt_followin.html.
4. Naraine, Ryan (6 June 2008). "Blackmail ransomware returns with 1024-bit encryption key". ZDnet. Retrieved 25 October 2013.
5. Lemos, Robert (13 June 2008). "Ransomware resisting crypto cracking efforts". SecurityFocus. Retrieved 25 October 2013.
6. "Results of online survey by Interdisciplinary Research Centre in Cyber Security at the University of Kent in

Canterbury" *(PDF). kent.ac.uk. University of Kent in Canterbury. Retrieved 25 March 2014.*

7. "Australia specifically targeted by Cryptolocker: Symantec". ARNnet. 3 October 2014. Retrieved 15 October 2014.
8. "CryptoDefense ransomware leaves decryption key accessible". Computerworld. IDG. Retrieved 7 April 2014.