Enterprise Survival Guide for Ransomware Attacks

Shafqat Mehmoon

Enterprise Survival Guide for Ransomware Attacks

GIAC (GCIH) Gold Certification

Author: Shafqat Mehmood, shafqat.mehmood@me.com
Advisor: Adam Kliarsky
Accepted: April 30th, 2016

Abstract

Hardly a day passes by when we do not hear about a ransomware locking data and demanding the ransom. Ransomware is the most opportunistic type of malware, affecting from a single user to an entire organization. Internet Security Threat Report (2016) by Symantec indicates 35% growth in crypto-style ransomwares during the year 2015. Symantec has categorized ransomware as "An extremely profitable type of attack" (Symantec, 2016). This profitability is attracting more hackers into the business and allowing attackers to bring more human resource in the attack mechanism. To launch a ransom attack, attackers are directly contacting their victims notably via technical support scams. Symantec first reported this type of scam in 2010 and blocked 100 Million Tech-Support Scam in the year 2015 alone (Symantec, 2016).

The scope and sophistication of ransomware is evolving at very high rate and there is a need to develop a cyber security model against ransomware attacks. This document goes into the details of multiple stages of a ransomware attack and describes a multilayer offensive security approach to protect an organization from ransomware attacks.

1. Introduction

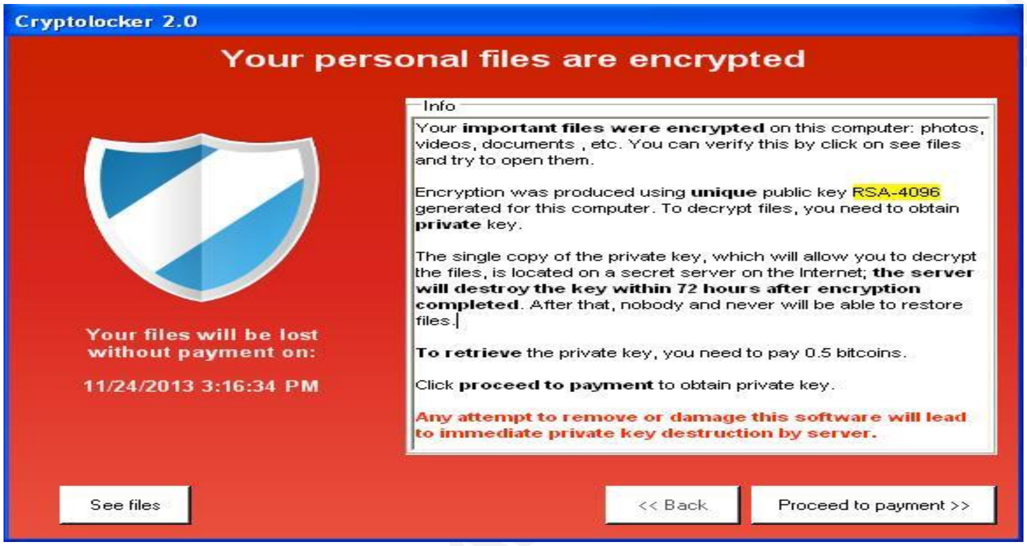
Ransomware or cryptolocker is a type of malware that can be covertly installed on a computer without knowledge or intention of the user. It can stay asleep or spread without user interaction until it receives a command from the hacker to encrypt files or completely lock the computer. The system is restored to normal (by the attacker) in lieu of financial benefit to the hackers.

Every cyber-attack is constructed using well-defined modular phases, and each phase should be accomplished sequentially. Rendering a cyber-attack entirely unsuccessful is all about blocking any one or more of these stages. Thus providing us not just one but multiple opportunities to detect and prevent a hacking attempt. In this paper, we understand how ransomware works and dissect its life cycle into multiple stages. Based the analysis of each phase, we build a multilayered security model around the IT infrastructure. The outermost protection layer targets the very first stage of the attack, and a successful attack has to breach all the detection/prevention controls at each layer. We accept the fact that hacking attacks such as ransomware are inevitable and prepare for the worse. We also discuss paying the ransom and explored the possibilities of recovering the data without pay the ransom.

2. Ransomware Attack

Ransomware could prevent the user from using their computer or accessing data. It holds the user’s computer and files for ransom. Ransomware is a piece of software very similar to malware. Malware is a program that installs itself on a computer and runs in the background, hiding its presence and stealing passwords, credit card, and other valuable information. Malware does all this without the user's knowledge. However, ransomware does not try to hide it. As soon as it has done its job, i.e. locked the computer or files, it notifies the user of its presence.

The victim gets a message (about encryption of data) on the screen similar to the one below:



Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Figure 1 - Cryptolocker Message Box

To add to the user's distress, typically a ticking countdown timer starts with a 72-hour deadline in which to pay the ransom or the decrypt key will be destroyed, thus removing any possibility of recovery.

Any attempt to interfere with the cryptolocker, such as stopping the cryptolocker service or entering a wrong payment info, usually results in the remaining time being halved. On the other hand, not paying the ransom within the due time can lead to the ransom amount being doubled with a new deadline.

Depending upon the particular version and type of the ransomware, there might be another pop-up screen showing the list of encrypted files. Users can verify that the files still exist, but the contents are merely unreadable garbage. Files are encrypted using asymmetric (RSA) encryption, where the key used for encryption cannot be used to decrypt the data. RSA algorithm uses two different keys, one (public) for encryption of data and one (private) for decryption. Once the data is encrypted, it is generally unrecoverable unless the user decides to pay the ransom (other recovery option discussed in next few sections). Paying the ransom does not guarantee recovery of data.

Among many other, the most common mode of ransom payment is Bitcoins. Bitcoin is a digital currency that has been designed with one aim in mind, namely, to do anonymous online transactions. From the transaction itself, it is impossible to trace the beneficiary. It is unfortunate that this revolutionary e-currency is almost exclusively being used to carry out crimes. In fact, many of its users come to know about it when they are asked to pay a ransom through Bitcoin.

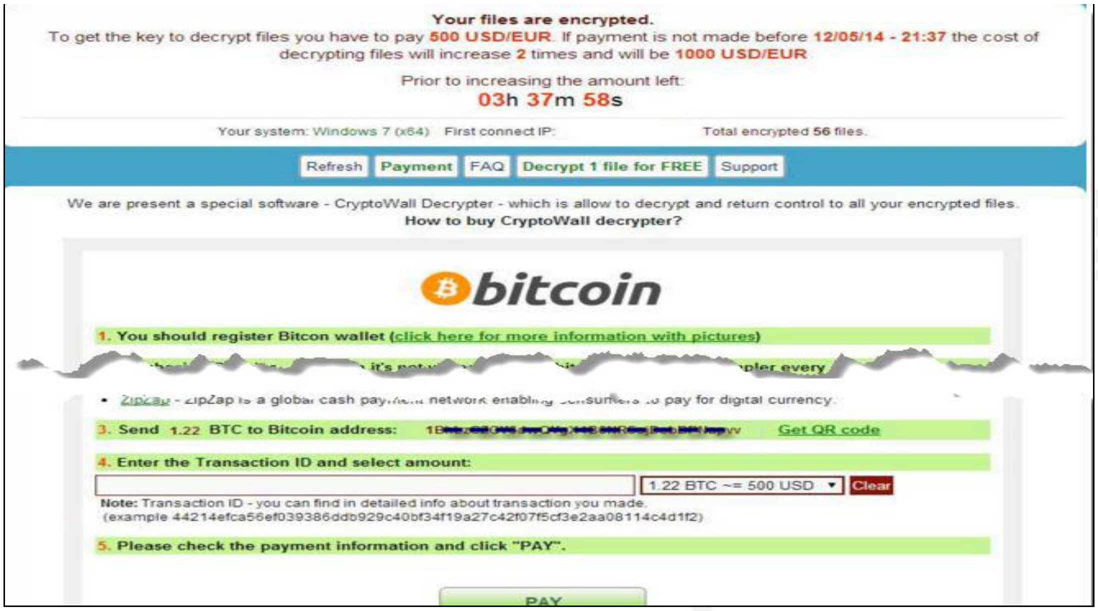
2.1. Ransom - The Dilemma

Once the data is encrypted, there are two options to recover the data. Either pay the ransom or recover the data without paying the ransom.

2.1.1. Paying the Ransom

Holding someone or something captive and demanding a ransom is a risky business. Getting money is hard but getting away with money is even harder. Typically, law enforcement marks the currency and tracks the spender when it comes to market. However, in today's digital world, demanding a ransom, for digital information being held hostage, has turned out to be the easiest way to extort money. In fact, this is the primary reason for the success of ransomware such as cryptolocker and cryptowall. Ransom payments have encouraged hackers and provided the necessary funding to develop more complex ransomware and launch them on a much wider scale. In 2012, Symantec estimated that 2.9% of victims paid the ransom. In 2014, the University of Kent did a survey and the results showed that a devastating 40% of victims paid the ransom. Learning from cyber criminals kidnappers in the real world have also started to demand ransoms in Bitcoins.

A tough question for the victim is whether they should pay the money or not. Law enforcement agencies, as well as Symantec Corporation, advise against paying a ransom stating "criminals may not provide the key even after receiving the ransom." However, they do not provide an alternative solution. Of course, cybercriminals are also trying to win this battle of "trust and distrust". Recently, to lure the victim into paying the ransom, they have started a "try and verify" approach by adding a button "Decrypt 1 file for FREE” as shown the figure below.



Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **12/05/14 - 21:37** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:
03h **37**m **58**s

Your system: Windows 7 (x64) First connect IP: Total encrypted **56** 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)

it's not pler every

- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. **Send** 1.22 **BTC to Bitcoin address:** [redacted] Get QR code

4. **Enter the Transaction ID and select amount:**

1.22 BTC ~= 500 USD ▼ Clear

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

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

Figure 2 – Ransom Message

The ransom economy will not sustain if victims stop paying the ransom. Law enforcement agencies are trying to stop people from paying a ransom by raising awareness and caution while the criminals and crooks are trying to outwit them. This war is likely to continue and at the moment, the momentum seems to favor the criminals.

In November 2014, Dickson County Sheriff’s Office USA opted to pay a ransom of $572 to recover files. Later the Sheriff said, “I am thankful that is all they asked for.” In a similar case, the Durham, N.H. Police Department (USA) was infected in June 2015. They recovered the files from a backup, choosing not to pay the ransom. However, they paid $3000 to a contractor for a file clean up afterward.

2.1.2. Cracking the Private Key

Data Encrypted with the public key can only be recovered using the corresponding private key. Technically, it is impossible to decrypt a properly encrypted file without the private key. The bad guys are using the technology that has been developed over decades of research, and it constitutes the backbone of secure communication over the internet. Finding a private key using brute force (trying all possible combination of key phrase) presents a monumental computation problem, known as the “RSA Problem.” It has been almost 40 years since Rivest, Shamir and

Adleman first described the RSA algorithm for public-key cryptography. Since then, a combination of best minds and machines have failed to break the algorithm. In conclusion, we can say that it is not possible to decrypt the encrypted data without a private key.

3. Anatomy of Ransomware Attack

There are a number of ways an attacker can initiate an attack with the ultimate goal being to plant the malware/ransomware in the victim's machine.

The most common attack vector is a phishing email where the victim is tricked into clicking on a link in what appears to be a legitimate email message. Below diagram details 6 stages of ransomware attack. The last three steps use TOR (anonymous proxy) if it has not blocked by the organization.

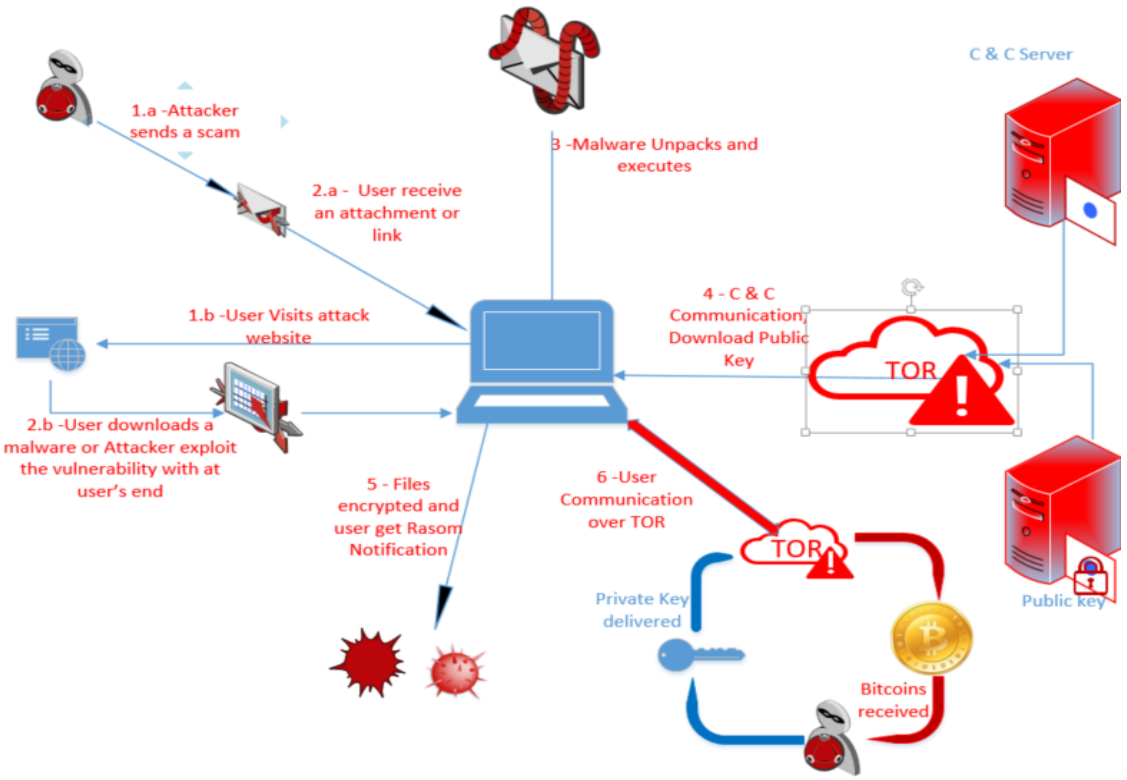

1.a -Attacker sends a scam
3 -Malware Unpacks and executes
C & C Server
2.a - User receive an attachment or link
1.b -User Visits attack website
4 - C & C Communication, Download Public Key
TOR
2.b -User downloads a malware or Attacker exploit the vulnerability with at user's end
5 - Files encrypted and user get Rasom Notification
6 -User Communication over TOR
TOR
Private Key delivered
Public key
Bitcoins received

Figure 3

3.1.1. Selection of a Victim

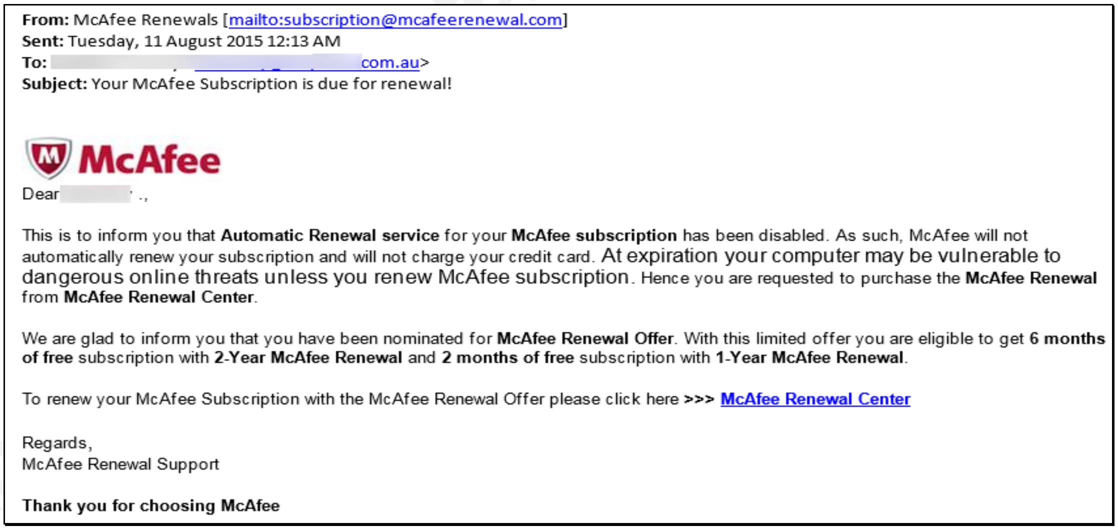
Attacker comes into contact with the victim by war driving or target attack technique.

War Driving

A ransom attack is launched on a massive scale to the entire target base, typically via a phishing email to a mailing list containing thousands of emails addresses or the victim visits the malicious or compromised website and download the infected executable or a vulnerability on their computer is exploited. Usually, an insecure organization with untrained users and unpatched client-side software can be a victim of war driving attack.

Targeted Attack

In targeted attacks, the attacker hand-picks a single or set of chosen targets. Recently, we encountered one such attack. When attackers realized (based on job advertisement) that McAfee products are being extensively used in the company, they sent a phishing email to get an employee into a chat session using a known Remote Support Access Provider.



From: McAfee Renewals [mailto:subscription@mcafeerenewal.com]
Sent: Tuesday, 11 August 2015 12:13 AM
To: [redacted]com.au>
Subject: Your McAfee Subscription is due for renewal!

McAfee

Dear [redacted].,

This is to inform you that **Automatic Renewal service** for your **McAfee subscription** has been disabled. As such, McAfee will not automatically renew your subscription and will not charge your credit card. At expiration your computer may be vulnerable to dangerous online threats unless you renew McAfee subscription. Hence you are requested to purchase the **McAfee Renewal** from **McAfee Renewal Center**.

We are glad to inform you that you have been nominated for **McAfee Renewal Offer**. With this limited offer you are eligible to get **6 months of free** subscription with **2-Year McAfee Renewal** and **2 months of free** subscription with **1-Year McAfee Renewal**.

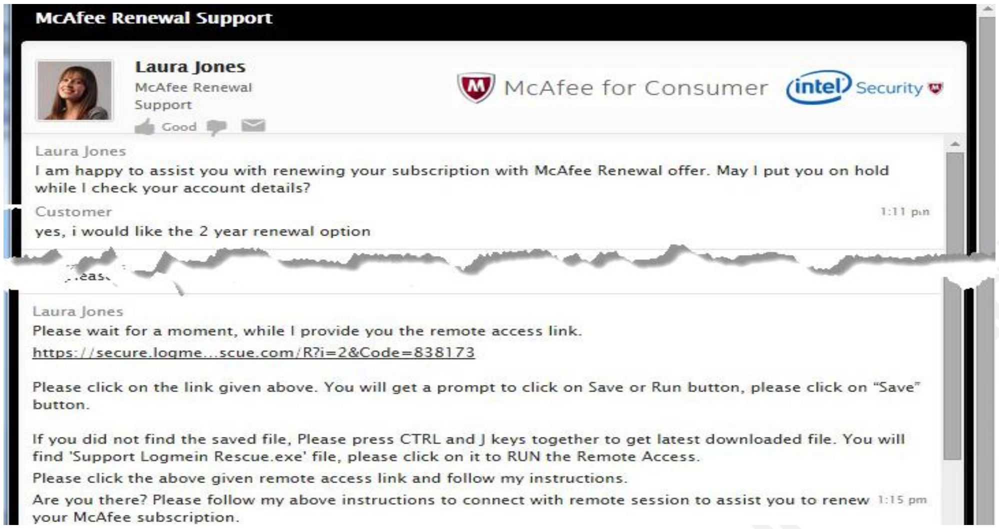
To renew your McAfee Subscription with the McAfee Renewal Offer please click here **>>>** **McAfee Renewal Center**

Regards,
McAfee Renewal Support

Thank you for choosing McAfee

Figure 4

Once the victim is drawn into the chat session, the hacker installs the malware/ransomware on the AV (Anti-Virus) server, thus neutralizing a critical defense. Then using McAfee ePO server as a staging machine, encrypt every accessible resource in the organization.



Laura Jones
McAfee Renewal Support

Laura Jones
I am happy to assist you with renewing your subscription with McAfee Renewal offer. May I put you on hold while I check your account details?

Customer 1:11 pm
yes, i would like the 2 year renewal option

...easi...

Laura Jones
Please wait for a moment, while I provide you the remote access link.
https://secure.logme...scue.com/R?i=2&Code=838173

Please click on the link given above. You will get a prompt to click on Save or Run button, please click on "Save" button.

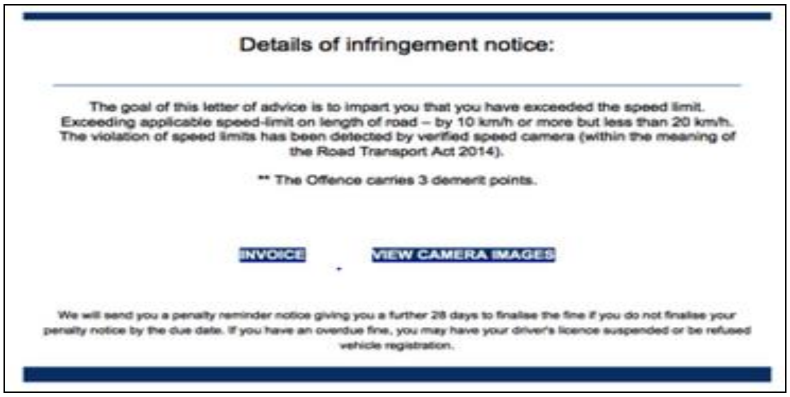
If you did not find the saved file, Please press CTRL and J keys together to get latest downloaded file. You will find 'Support Logmein Rescue.exe' file, please click on it to RUN the Remote Access.
Please click the above given remote access link and follow my instructions.
Are you there? Please follow my above instructions to connect with remote session to assist you to renew your McAfee subscription. 1:15 pm

Figure 5

We conducted around 14 different chat sessions over the duration of 48 hours and based on the vocabulary, sentence structure, and references to previous chat sessions; we concluded that at least 4 individual hackers were conducting the chat sessions. A clear evidence, either there is a group of hacker targeting the organization or they have outsourced the malware deployment to a call center. It appears that some ransom money is being invested back into the business. The sophistication and professionalism of targeted attack mean only highly resilient environment can survive these types of attacks.

3.1.2. Getting the Payload to the Victim's Computer

There are many ways to drop a generic ransomware, and a phishing email attack is the most popular. For example, in the traffic infringement notice in figure 6, both the INVOICE and VIEW CAMERA IMAGES links redirect you to the attacker's website.



Details of infringement notice:

The goal of this letter of advice is to impart you that you have exceeded the speed limit. Exceeding applicable speed-limit on length of road – by 10 km/h or more but less than 20 km/h. The violation of speed limits has been detected by verified speed camera (within the meaning of the Road Transport Act 2014).

** The Offence carries 3 demerit points.

INVOICE VIEW CAMERA IMAGES

We will send you a penalty reminder notice giving you a further 28 days to finalise the fine if you do not finalise your penalty notice by the due date. If you have an overdue fine, you may have your driver's licence suspended or be refused vehicle registration.

Figure 6 – Sample Phishing Email

Clicking on INVOICE or CAMERA IMAGE links leads to download and install of ransomware package.

3.1.3. Contact with Command and Control

The first step after installation of ransomware is to contact the command-and-control (C&C) server in order to get further instruction or encryption key. Most antivirus software block the malware by preventing its execution at first instance if it has a known detection signature. AV, IPS (Intrusion Prevent System) and Firewalls maintain a list of malicious Proxies and C&C IP addresses and thus detect the presence of malware when a malicious program attempts to communicate. This method is not a very efficient as it is not possible to build a comprehensive list of all malicious destinations. Additionally, C&C server may have already been taken down by law enforcement, and malware may be left as “Orphaned”. So, instead of using a static C&C server, hackers have started to use a Dynamic Domain Generation Algorithm technique. The latest variant of cryptolocker generates a list of 1200 domains and tries to connect them until a successful connection has been made. This process is repeated if the connected C&C has gone offline. This way a compromised computer can be under the control of numerous C&C Servers. This interconnected system of C&C Servers and compromised computers (bots) is referred to as a botnet. Hiding and protecting the C&C communication is fundamental to the existence of a botnet.

Recently, a US-based security company, Fire-eye, uncovered a Russian Cyber Threat Group, APT29, who used Twitter feeds as the communication protocol. The commands were embedded (not visible to naked eye) in standard images using steganography.

3.1.4. Download the Public Keys

An attacker may decide to use the infected system as a ransomware launching pad to spread the infection across the network. Once the attacker is satisfied with the number of infections in a particular organization, the public keys are delivered to all the bots.

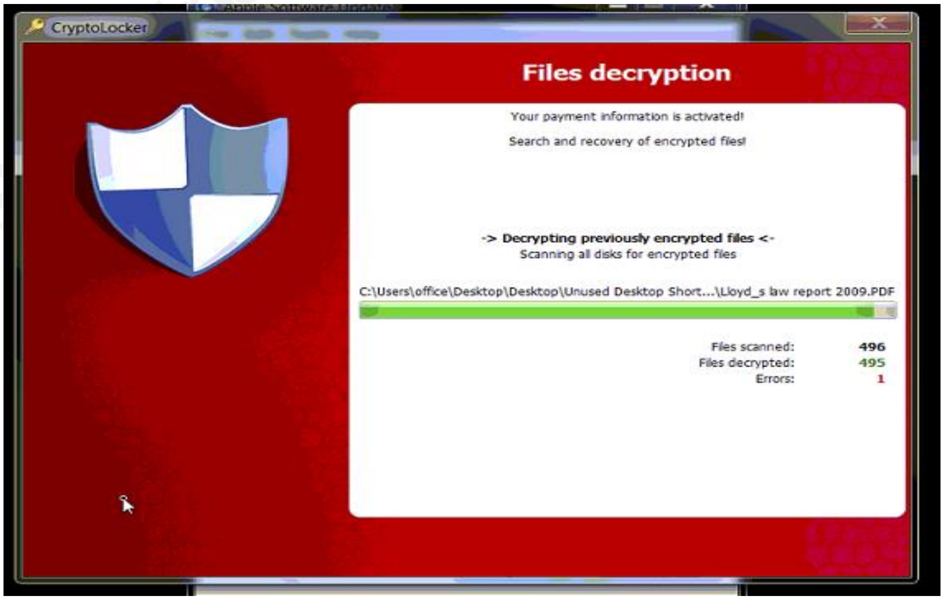
3.1.5. Encrypt the Files

The earlier versions of cryptolocker would just encrypt the files on the local computer. However, new variants try to encrypt the backup first. They specifically scan the local computer and remote file shares named in date format (keeping in mind 90% of backup folder/files names include date e.g. sql20150619.bak) and encrypt all the contents of these folders then it encrypts specific file types only. Encryption in-progress can be detected and interrupted by an incident response team, so it is critical for an attacker to prioritize the files to be encrypted, ensuring important files are encrypted first. Commonly, ransomwares start with files/folder with most recent access date.

3.1.6. Extortion of Money

The next step is to notify the victim about the damage and facilitate the trial recovery by providing the new cryptolocker software in case newly installed AV has deleted it. Common AV uninstall/exclusion steps are communicated along with payment instructions.

Once the ransom is paid and verified by the hackers manually (which may take a 2 to 48 hours), the private key may be delivered, and automatic decryption starts as shown in the Figure 7. No further support is provided if decryption fails on one or more files.



Files decryption

Your payment information is activated!

Search and recovery of encrypted files!

-> Decrypting previously encrypted files <-

Scanning all disks for encrypted files

C:\Users\office\Desktop\Desktop\Unused Desktop Short...\Lloyd_s law report 2009.PDF

```
Files scanned:     496
Files decrypted:   495
Errors:              1
```

Figure 7 – Cryptolocker Decryption Process

3.2. Getting the Data Back without paying ransom

In this section, we explore the different ways of recovering the encrypted data.

3.2.1. Recover the file from backup

The most efficient and effective way to get back the data is to restore data files from a backup. In most corporate environments files are backed up regularly so recovery should not be a problem. Normally a backup is made for shared and mapped drives. User desktop data is rarely saved.

Users should backup the files to a network drive or USB drive and disconnect it after the backup. Almost all ransomwares encrypt the network drives.

3.2.2. Use built-in file versioning services like Windows Volume Shadow Copy

Windows Volume Shadow Copy can be enabled on any drive. It keeps the version history of all the files on the drive and makes it possible to go back on the timeline. However, newer ransomwares try to delete all the shadow copies using a Windows command

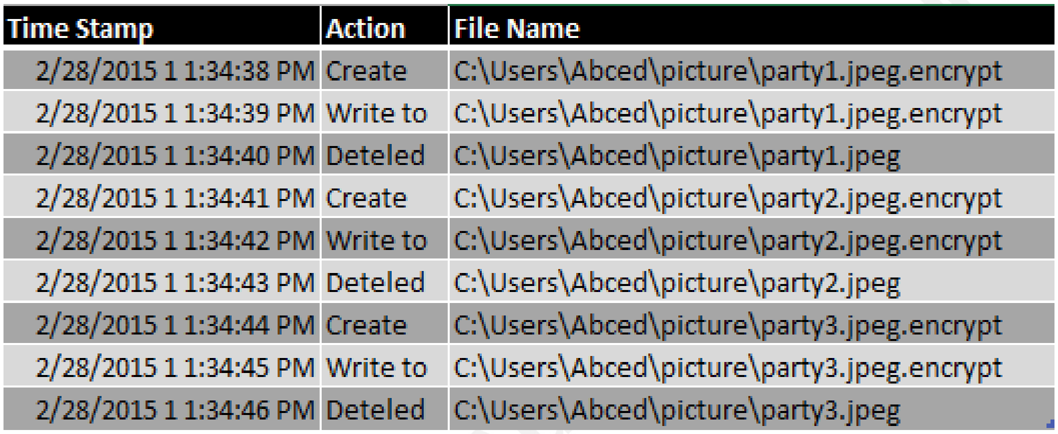
“C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet”

It is an interesting fact that the Volume Shadow Copy feature is also used by malware to store a malicious code and overwriting it with some innocent content to evade the anti-virus scanning even with an updated signature. This malicious code is later recovered and executed when needed.

3.2.3. Recover the most critical data using forensic techniques

When a file is opened for editing, almost all applications create a temporary copy of the original file. All the changes are made to the temporary file which overwrites the original file when saved. This is how Microsoft Office recovers files if the application closes abruptly. Once a user exits the application, the temporary file is deleted. On Windows, deleting a file means deleting the pointer to the file (not the contents) in NTFS/FAT/EFS file system. This space is then marked as free and available for overwriting. Using the advanced forensic techniques, it is possible to scavenge the free space on the disk for useful information. The longer the system is used after an attack, the greater the risk of original files being overwritten.

For example, during the encryption process, Cryptolocker 2.0 creates a new .encrypt file. It reads the contents of the original file and keeps it in memory, then encrypts the contents and writes the encrypted contents to the '.Encrypt' File – after which the original files are deleted.



Time Stamp	Action	File Name
2/28/2015 1 1:34:38 PM	Create	C:\Users\Abced\picture\party1.jpeg.encrypt
2/28/2015 1 1:34:39 PM	Write to	C:\Users\Abced\picture\party1.jpeg.encrypt
2/28/2015 1 1:34:40 PM	Deteled	C:\Users\Abced\picture\party1.jpeg
2/28/2015 1 1:34:41 PM	Create	C:\Users\Abced\picture\party2.jpeg.encrypt
2/28/2015 1 1:34:42 PM	Write to	C:\Users\Abced\picture\party2.jpeg.encrypt
2/28/2015 1 1:34:43 PM	Deteled	C:\Users\Abced\picture\party2.jpeg
2/28/2015 1 1:34:44 PM	Create	C:\Users\Abced\picture\party3.jpeg.encrypt
2/28/2015 1 1:34:45 PM	Write to	C:\Users\Abced\picture\party3.jpeg.encrypt
2/28/2015 1 1:34:46 PM	Deteled	C:\Users\Abced\picture\party3.jpeg

Figure 8 – File Activity

It is expected that the newer version of ransomware will use built-in Windows programs to permanently delete data. For example, in windows, a built-in tool designed to encrypt and decrypt data can also be employed to permanently delete the content using the command "**cipher /w c:\backup.txt".**

A similar command on Unix (depending upon the distribution) is "srm" or "rm -p" which can be used to delete a file to an unrecoverable state.

Securely deleting a file takes more time than creating it. Normally hackers study the target's usage pattern and perform an encryption/secure deletion process when the system is not in use.

3.2.4. Find flaws in the implementation of encryption

Most of the attacks against encryption are successful due to programming or architectural flaws in the encryption routine, such as using a repetitive, predictable seed, or misinformation about the strength of cryptographic routines etc.

A cryptolocker variant, Racketeer, which spread through a fake Energy Australia bill email, used a flawed process of generating an RSA key pair on a victim's machine, which was then cracked during analysis and the private key was recovered using brute-force technique.

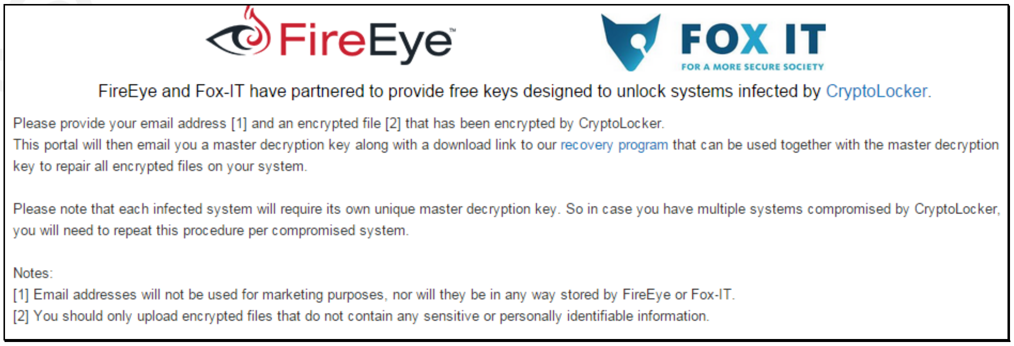
In another instance, security researcher Fakebit (fakebit.com) discovered a failed attempt at counterfeiting the well-engineered cryptolocker. This variant claimed to use 2048-bit RSA but instead used the Tiny Encryption Algorithm (TEA).

3.2.5. Law Enforcement tracks down criminals and seizes private keys.

Ransomware is a consistent threat, and governments and IT Vendors have to join forces to bring the criminals to justice.

One notable combined effort by the private and government sector is “Operation Tovar” against the botnet Gameover Zeus. Gameover Zeus was a peer to peer botnet network and it was widely used as a launching pad for cryptolocker attacks. In 2014, US Law Enforcement officials announced the success of Operation Tovar and intercepted the transfer of 500,000 private keys. The creator of Gameover Zeus botnet, nicknamed “lucky12345” was identified as a Russian man, Evgeniy Bogachev. In February 2015, the FBI announced a $3million reward for any information about his whereabouts.

Recently, FireEye and Fox-IT have set up a website[1] which offers a free decryption service to cryptolocker victims using a database of recovered private keys. Users can submit an encrypted file. All the private keys are tried against the file and if a match is found; it is emailed back to the user.



FireEye and Fox-IT have partnered to provide free keys designed to unlock systems infected by CryptoLocker.

Please provide your email address [1] and an encrypted file [2] that has been encrypted by CryptoLocker.
This portal will then email you a master decryption key along with a download link to our recovery program that can be used together with the master decryption key to repair all encrypted files on your system.

Please note that each infected system will require its own unique master decryption key. So in case you have multiple systems compromised by CryptoLocker, you will need to repeat this procedure per compromised system.

Notes:
[1] Email addresses will not be used for marketing purposes, nor will they be in any way stored by FireEye or Fox-IT.
[2] You should only upload encrypted files that do not contain any sensitive or personally identifiable information.

Figure 9 – Website offered by FireEye and Fox-IT

[1] https://www.decryptcryptolocker.com/

3.3. Prevention

Chinese General, Sun Tzu said, “War is half won if you know your enemy. Additionally, if you know yourself, you may retreat, but you will never be defeated.” It is also true in the fight against ransomware. We are aware of the adversary, but we are not entirely aware of all the possible ways in which our defenses may be breached. The following are ways to overcome the most common weaknesses and enhance our defenses against cryptolocker.

3.3.1. User training

The majority of ransom-lockers spread through phishing and scam emails. So it is worth keeping an eye on the current scam and spam trends. One good source is the Australian government initiative scamwatch. Security professionals and system administrators should follow the latest trends and educate users.

In the corporate security, users are the weakest link and appropriate training plays an important factor in preventing security breaches and if a breach occurs, helps in containing the threat. For example, a trained user can only prevent an attack discussed in section 3.1.1.

3.3.2. Efficient Patch Management

According to HP’s annual Cyber Risk Report, 44% of attacks during the last year were due to unpatched code that was two to four years old. Two most common causes of delay in patch deployment are instability and downtime. A new patch may destabilize the system and a system with a high availability requirement waits until the industry has tested it. Many times we have seen a patch being released hurriedly to fix a vulnerability. These untested patches fix security vulnerabilities but occasionally cause operational issues. On a few occasions, we installed patches that were released to fix the issues caused by an earlier patch.

3.3.3. Effective and Mandated IT Security Team

IT Security is an ever-evolving field and requires continuous training and research. However, we still see IT professionals performance being measured with traditional measurement tools focusing on utilization and billability. It is critical for a security specialist to keep up with training, conferences, and learn about new vulnerabilities in order to stay up-to-date with the latest threats.

When a security team realizes a potential risk, a difficult step is convincing business management to put in the necessary time and effort to deploy the essential preventive controls. Traditional ways of measuring ROI (Return On Investment) are ineffective due to business not fully realizing the risk until it is too late. In 2014, Sony Entertainment spent tens of millions of dollars after security breaches cost the company about $1.25 billion.

3.3.4. Backup

The most effective defense against ransomware is the backup of data files. A corporate user’s data, stored on a network drive, is backed up on a regular basis. However, it is not standard practice to backup a user's desktop. Information system administrators need to expand the scope of backups with storage and bandwidth upgrades. With the possibility of backups being encrypted by ransomware, we need to keep multiple copies of data (backup of backups), over a longer period.

3.3.5. Restrict Write Permission

Access should be granted on a need to know basis. Restrictive ACLs significantly reduce the ransomware damage. The best way to save data is to write backup to a Drop Folder and only allow full control to a specific high-security user. To create a Drop Folder, grant the Write permission to Everyone and grant the Read/List/Delete permission to the manager who can recover files from the folder. A Drop Folder can be created on Windows server using the following steps:

1. Click **Start**, point to **Programs**, point to **Accessories**, click **Windows Explorer**, and then locate the folder for which you want to set permissions. In this example, use the folder called Drop and the user named Manager1.
2. Right-click the **Drop** folder, click **Properties**, and then click the **Security** tab.
3. Click the **Everyone** group. If the Everyone group is not listed, you can add the group by clicking **Add**.

4. Click **Allow** for the **Write** permission, and then click to clear the check boxes for the remaining permissions.
5. Click **Deny** for **Read & Execute**. This will also explicitly deny permissions for the List Folder Contents and Read permissions.
6. Keep the Everyone group and remove all other listed groups and users. To do this, click a group or user, and then click **Remove**.
7. Click **Add**, and then add the appropriate user. In this example, add Manager1. Click **OK**.
8. In **Permissions**, click the **Manager1** user, click to clear the **Full Control** check box, and then click **Allow** for the **Modify** permission.

3.3.6. Restrict the use of Elevated Privileges

When a corporate user is attacked, only data files that are accessible to that user are encrypted. In many cases, administrators use elevated privileges for normal operations such as browsing the internet and checking email. Any wrong click may download ransomware, running with same elevated privileges and may result in the entire organization's data (including backups) being encrypted.

3.4. Multilayer Protection using Software Tools

This section describes a multilayer layer protection approach to protect against rasonwares attack using software security tools. We have used McAfee tools as a model. However, similar or better software are also offered by other vendors. These protection measures are not foolproof but significantly reduce the risk of a ransomware the attack.

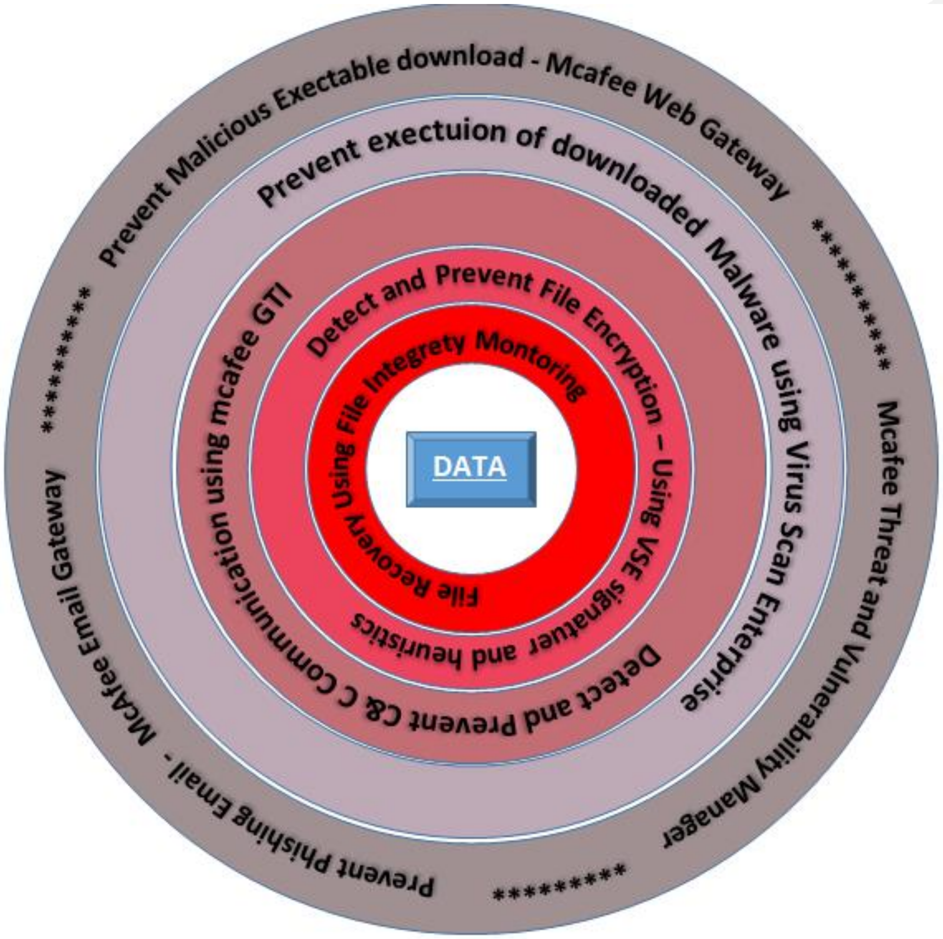

Prevent Malicious Exectable download - Mcafee Web Gateway
****
Mcafee Threat and Vulnerability Manager
****
Prevent Phishing Email - Mcafee Email Gateway
****
Prevent exectuion of downloaded Malware using Virus Scan Enterprise
Detect and Prevent C& C Communication using mcafee GTI
Detect and Prevent File Encryption – Using VSE signater and heuristics
File Recovery Using File Integrety Montoring
DATA

Figure 10 – Multilayer Protection

3.4.1. Prevent the initial contact

Two of the most common ways to attack a user is through email or a web browser. In the first instance, a user receives an email with an invitation to either open an attachment or click on a link in the email.

McAfee Email Gateway uses a propriety spam-scoring algorithm, which monitors all incoming email traffic and filters out emails with potentially unsafe attachments, links, etc. Generally, in a large enterprise, on average 85% of email traffic is spam and catching this 85% is crucial for the safety of the entire company. Careful training and configuring an email gateway appliance can result in 99.9% of spam messages being blocked.

3.4.2. Prevent Download

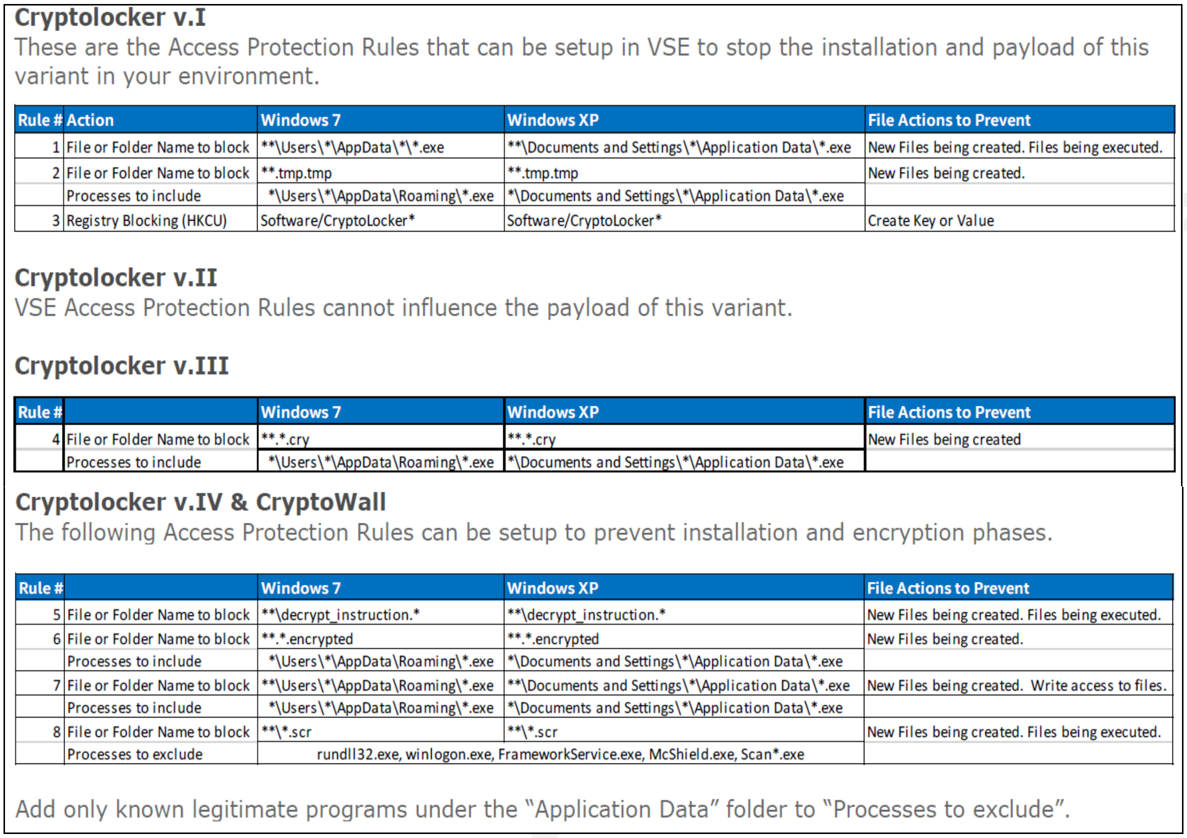
Carefully crafted phishing emails can beat the best spam filters in the world and breach through an email gateway. Once a malicious has arrived in user's inbox, McAfee Click Protect provides a highly effective protection layer to cautious users by showing unmasked URL, risk rating and a preview of the target page. Again, users can be deceived. This is when the next layer of protection kicks in. The McAfee Web Gateway using Global Threat Intelligence (GTI) and Threat Intelligence Exchange (TIE) can block malicious payloads and safeguard the user from known threats.

Another important defense inline is the McAfee Next-Gen Firewall (NGFW), which can scan each file being downloaded. McAfee Global Threat Intelligence can provide the file reputation information. Many threats do not reveal themselves until they are executed. NGFW intercepts executables and uploads them to ATD (Advance Threat Detection Cloud). The ATD system executes files in a sandboxing environment, analyzing each line of code and sending back a file reputation score. It also protects against an Advance Evasion Technique (AET) where an attacker splits up a malicious payload into smaller pieces, disguising them, and sending them across multiple protocols.

3.4.3. Prevent the Execution Malware

Malware download on the system indicates that perimeter defenses, mentioned above, have been breached. McAfee Virus Scan Enterprise (VSE) can stop the execution of malicious code using features such as On Access Scanner, Download Execution Prevention and Anomaly Detection.

After analyzing various ransomware, McAfee suggests protection configurations using McAfee Virus Scan as shown in figure 12.



Cryptolocker v.I

These are the Access Protection Rules that can be setup in VSE to stop the installation and payload of this variant in your environment.

Rule #	Action	Windows 7	Windows XP	File Actions to Prevent
1	File or Folder Name to block	**\Users*\AppData**.exe	**\Documents and Settings*\Application Data*.exe	New Files being created. Files being executed.
2	File or Folder Name to block	**.tmp.tmp	**.tmp.tmp	New Files being created.
	Processes to include	*\Users*\AppData\Roaming\*.exe	*\Documents and Settings*\Application Data*.exe	
3	Registry Blocking (HKCU)	Software/CryptoLocker*	Software/CryptoLocker*	Create Key or Value

Cryptolocker v.II

VSE Access Protection Rules cannot influence the payload of this variant.

Cryptolocker v.III

Rule #		Windows 7	Windows XP	File Actions to Prevent
4	File or Folder Name to block	**.*.cry	**.*.cry	New Files being created
	Processes to include	*\Users*\AppData\Roaming\*.exe	*\Documents and Settings*\Application Data*.exe	

Cryptolocker v.IV & CryptoWall

The following Access Protection Rules can be setup to prevent installation and encryption phases.

Rule #		Windows 7	Windows XP	File Actions to Prevent
5	File or Folder Name to block	**\decrypt_instruction.*	**\decrypt_instruction.*	New Files being created. Files being executed.
6	File or Folder Name to block	**.*.encrypted	**.*.encrypted	New Files being created.
	Processes to include	*\Users*\AppData\Roaming\*.exe	*\Documents and Settings*\Application Data*.exe	
7	File or Folder Name to block	**\Users*\AppData\Roaming\*.exe	**\Documents and Settings*\Application Data*.exe	New Files being created. Write access to files.
	Processes to include	*\Users*\AppData\Roaming\*.exe	*\Documents and Settings*\Application Data*.exe	
8	File or Folder Name to block	***.scr	***.scr	New Files being created. Files being executed.
	Processes to exclude	rundll32.exe, winlogon.exe, FrameworkService.exe, McShield.exe, Scan*.exe		

Add only known legitimate programs under the "Application Data" folder to "Processes to exclude".

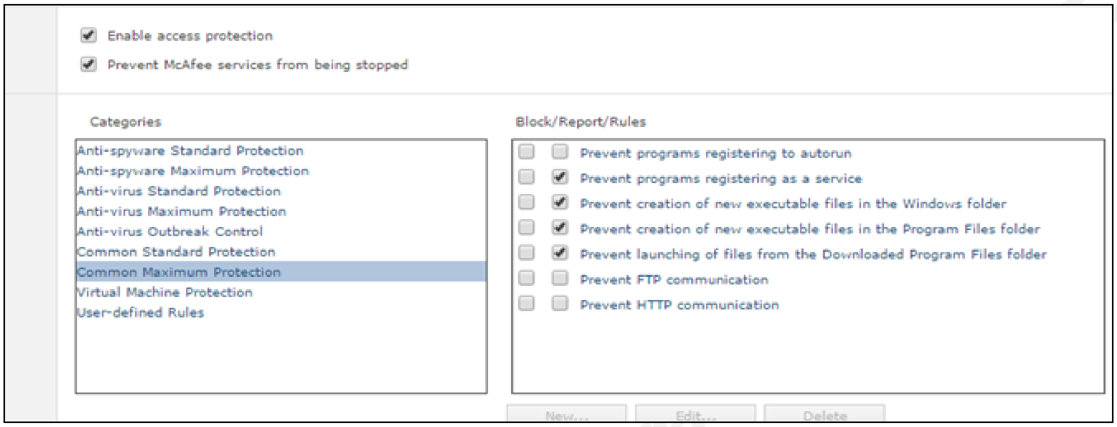
Figure 11 - McAfee Virus Scan Settings

Collectively, VSE, Host Intrusion Prevention System (HIPS) and Application Control (provides complete protection from unwanted applications) have proven to be one of the most effective defenses against malware and ransomware.

Application whitelisting can provide reliable protection against ransomware. The first step in application whitelisting is to mark and allow the execution of all the trusted applications. This process is called baselining. This white list can be shared across multiple hosts, and anything above the baseline is blocked by default and can be allowed manually on a case by case basis.

It is recommended that a rule be created to prevent a non-trusted process calling a trusted process or dll. The administrator must also create rules to prevent specific executables from hooking on to other executables.

During many security audits, the most common finding is the default protection setting which is report only. In the below figure, block column is unchecked while only logging is enabled for few entries.



☑ Enable access protection

☑ Prevent McAfee services from being stopped

Categories

- Anti-spyware Standard Protection
- Anti-spyware Maximum Protection
- Anti-virus Standard Protection
- Anti-virus Maximum Protection
- Anti-virus Outbreak Control
- Common Standard Protection
- Common Maximum Protection
- Virtual Machine Protection
- User-defined Rules

Block/Report/Rules

□	□	Prevent programs registering to autorun
□	☑	Prevent programs registering as a service
□	☑	Prevent creation of new executable files in the Windows folder
□	☑	Prevent creation of new executable files in the Program Files folder
□	☑	Prevent launching of files from the Downloaded Program Files folder
□	□	Prevent FTP communication
□	□	Prevent HTTP communication

Figure 12 – Common Settings

It is advisable to change these settings and enable Block to prevent the execution of malware at the initial stage. Changing these setting from Report to block should be done carefully and gradually, starting with a group of less critical users.

3.4.4. Detect and Block C&C communication

McAfee is continuously detecting and protecting its customers from a vast variety of threats. When a new malware appears in the wild, it is picked up, and all of its functions and Command & Control are dissected and analyzed. An attack signature is developed and passed to Virus Scan Engines around the world in the form of daily updates. Additionally, the following information is then passed to various layers of protection using the McAfee Global Threat Intelligence (GTI) feed which includes the following data.

- McAfee GTI file reputation
- McAfee GTI web reputation
- McAfee GTI web categorization
- McAfee GTI message reputation
- McAfee GTI network connection reputation

3.4.5. Detect and Prevent File Encryption

Most malware makes calls to Windows encryption related DLLs. It is possible to detect and block the calls by untrusted applications using McAfee VSE (Virus Scan Enterprise) and HIPS (Host Intrusion Prevention System) technologies.

3.4.6. McAfee File Integrity Monitoring

McAfee file and application monitoring can be used to detect malicious changes to system files and the registry. File Integrity Monitoring can be used to detect a mass file create/modify and file rename activity and raise an alarm. The content monitoring feature keeps tracks of changes to the file content and can help recover critical files.

3.4.7. McAfee DLP

DLP (Data Loss Prevention) agent is essentially a legitimate rootkit with built-in anti-jamming and tamper protection features. It intercepts every call to the file system and certain processes in memory. The purpose is to monitor and log every attempt to touch the organizational data. Effective security policies with proper alert setting can easily detect cryptolocker. For example, a system admin can develop an alert mechanism by creating a new file with a unique random string “sfjskldfjsdlkf” in it. This file is excluded from backups and will not normally be accessed by a user or a process. However, it will be included in ransomware’s bulk encryption activity, firing the critical preconfigure alarm/actions via ePO or SEIM.

In terms of incidents response, DLP logs are an import forensic artifact with two import features.

Non-Repudiation: Traceback the activity in detail to culprit process, application and user that cannot be denied.

Logs are Forensically Sound: Proper time stamping, hashing and an established chain of custody that can be used in court as evidence.

3.4.8. McAfee Asset and Vulnerability Manager.

A chain is as strong as its weakest link and finding this link before it can fail is critical to the integrity of the entire system. The McAfee Asset and Vulnerability Manager is designed to find the most vulnerable spots. It continuously scouts the entire information infrastructure, and as soon as a new system, phone, computer, or printer etc.

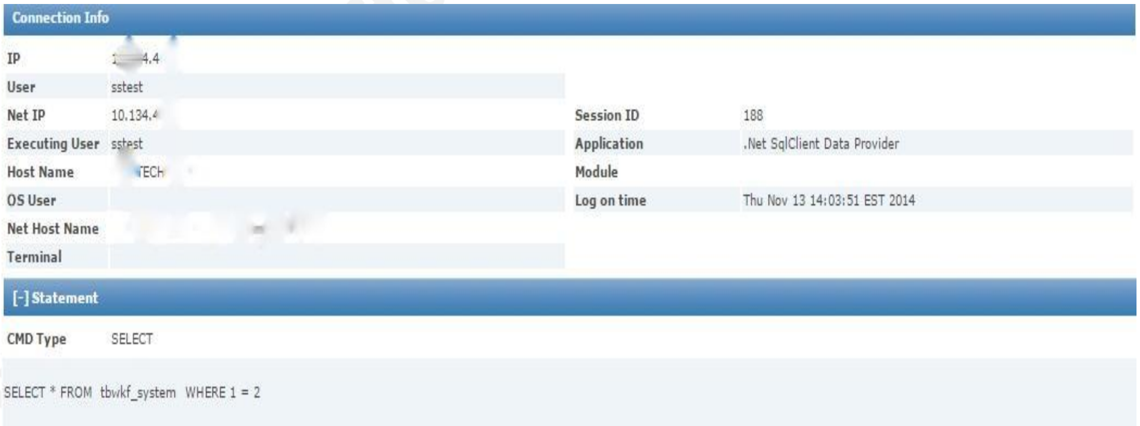
appears on the network, it runs a predefined scan on it and raises an alarm if the system is hackable. Every insecure system is a potential entry point into the entire IT infrastructure. McAfee Asset and Vulnerability Manager also assigns a risk score to every asset and communicate it to SIEM for incident prioritization.

3.4.9. Database Security

Almost all critical data is stored in databases and these databases are buried deep in layers of security. A hacker's ultimate dream and the worst nightmare for an organization is the compromise of this database. How vital is database security? The Ashley Madison data breach in July 2015 proved that database hacks can cause company shutdown, divorces, and suicides.

McAfee Database Security Product sits in front of the database and scans all the traffic and database commands and protects against obfuscate SQL statements. It can protect an unpatched database against a known vulnerability, a feature known as virtual patching.

As an example, the SQL statement below is used by attackers to verify authentication but does not pull the data to avoid detection.



Connection Info

IP	[redacted]4.4		
User	sstest		
Net IP	10.134.[redacted]	Session ID	188
Executing User	sstest	Application	.Net SqlClient Data Provider
Host Name	[redacted]TECH	Module	
OS User		Log on time	Thu Nov 13 14:03:51 EST 2014
Net Host Name	[redacted]		
Terminal			

[-] Statement

CMD Type	SELECT

```
SELECT * FROM  tbvkf_system  WHERE 1 = 2
```

Figure 13 – Attacker SQL Statement

3.4.10. Coordinated Defense Using SIEM

An army without a commander is like sheep without a shepherd. A commander has complete situational awareness. As shown in the following diagram below, McAfee

SIEM (Security Information and Event Management) acts as a commander in IT Security Infrastructure, making decisions based on the log information collected from all IT resources. Information gathering and log collection is the lifeline of cyber security intelligence in an organization. Analyzing the huge stream of logs coming in at 10s of thousands of events per second is a challenge, industry is trying to cope with. SIEM solutions collect information, correlate the data and present it to security analysts for further analysis and action.

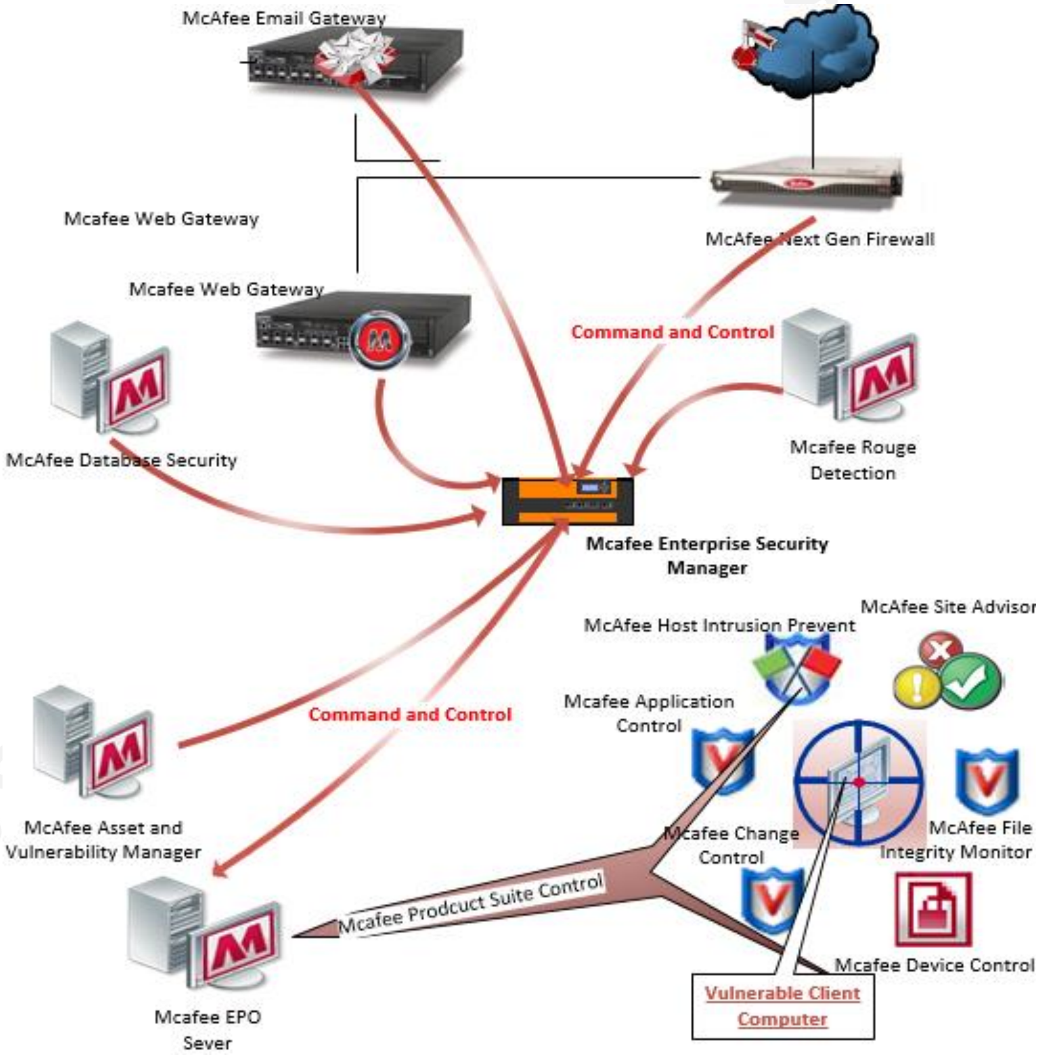


Figure 14 – Example Using McAfee

Currently, there is a significant delay between a breach taking place, detection and the first response. The human factor can result in a significant delay in reaction time against a threat.

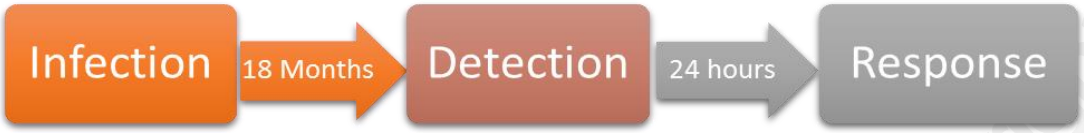


Figure 15 – Infection, Detection, Response

My first lesson as a Cyber Security Practitioner was “Stay calm; you cannot act faster than the GHz processor”. However, the next generation SIEMs can be configured with the automated response for known attacks, which allows us to deliver the first response at GHz. McAfee ESM leverages McAfee Advanced Threat Defence (ATD: advanced sandboxing), Data Exchange Layer (DXL: A virtual communication fabric among devices) and Threat Intelligence Exchange (TIE: Threat information sharing protocol across the network). Depending upon the threat and circumstance, SIEM can pass commands to the strategically positioned network/host-protection elements in the network and isolate any threat as soon as it has surfaced.

3.5. Conclusion: Ransomware+ and Beyond

The advancement in ransomwares is going at a very high pace. With no apparent hurdle, it can become a crisis in few years. Ransomware can hit mobile devices and Internet of Things (IoT). The day is not far when ransom will become a major threat to Privacy and Personally Identifiable Information (PII) data. Criminals will not only encrypt the data but they will also exfiltrate a copy of data from our computers, mobile devices and (possibly) cloud storage. This data will be used to blackmail the users and collect ransom in periodic installments.

Intelligent cars, automated homes, and personal wearables record every aspect of our life. Most of the users do not know that their hi-tech life is being recorded with accurate timestamps including all the secrets that we would protect at any cost. We need to understand the value of our personal data, realize the risk associated with it and actively devise ways to manage, track, monitor and secure personal data interactions and transactions.

References

[Screenshot]. Retrieved from https://thecomputerperson.wordpress.com/2014/03/08/cryptolocker-cc-weirdness/

Advanced Evasion Techniques and Anti-Evasion Technologies | McAfee Next Generation Firewall Technology. (n.d.). Retrieved from http://www.mcafee.com/au/products/network-security/next-generation-firewall-technologies/anti-evasion.aspx

Analysis of CryptoLocker Racketeer spread through fake Energy Australia email bills - Vínsula, Inc. (n.d.). Retrieved from http://vinsula.com/2014/06/10/analysis-of-cryptolocker-racketeer/

Bitdefender Offers CryptoWall Vaccine | Bitdefender Labs. (n.d.). Retrieved from http://labs.bitdefender.com/projects/cryptowall-vaccine-2/bitdefender-offers-cryptowall-vaccine/

Cazalla. (2015, January). Kidnappers Demand Ransom Be Paid With Bitcoin | Qntra.net. Retrieved from http://qntra.net/2015/01/kidnappers-demand-ransom-be-paid-with-bitcoin/

Chris Gadd. (2014, November). Dickson Sheriff’s Office pays ransom to cyber criminals. Retrieved from http://www.tennessean.com/story/news/local/dickson/2014/11/11/dickson-sheriffs-office-pays-ransom-cyber-criminals/18868325/

FBI — EVGENIY MIKHAILOVICH BOGACHEV. (n.d.). Retrieved from http://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

FireEye - Fox IT Scanner. (n.d.). Retrieved from https://decryptcryptolocker.com/

Gameover ZeuS - Wikipedia, the free encyclopedia. (n.d.). Retrieved April 10, 2015, from http://en.wikipedia.org/wiki/Gameover_ZeuS

How To Set Up a File System for Secure Access in Windows 2000. (n.d.). Retrieved from http://support.microsoft.com/en-us/kb/kbview/300691

New ransomware threat for Australia: SSO Alert Priority High | Stay Smart Online. (2014, September). Retrieved from https://www.staysmartonline.gov.au/alert_service/message?id=1132172&name=New+ransomware+threat+for+Australia%3A+SSO+Alert+Priority+High+#.VQT0YYGUczE

Operation Tovar - Wikipedia, the free encyclopedia. (n.d.). Retrieved April 10, 2015, from http://en.wikipedia.org/wiki/Operation_Tovar

Protecting against Cryptolocker & CryptoWall. (n.d.). Retrieved from https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25203/en_US/Cryptolocker_Update_RevD.pdf

R.L. Rivest, A. Shamir, and L. Adleman. (n.d.). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (Doctoral dissertation). Retrieved from http://people.csail.mit.edu/rivest/Rsapaper.pdf

Ransomware Do's and Dont's: Protecting Critical Data. (2015, February). Retrieved from http://www.symantec.com/connect/blogs/ransomware-dos-and-donts-protecting-critical-data

RSA problem - Wikipedia, the free encyclopedia. (n.d.). Retrieved April 10, 2015, from http://en.wikipedia.org/wiki/RSA_problem

SANS Digital Forensics and Incident Response Blog | TorrentLocker Unlocked | SANS Institute. (2014, October). Retrieved from http://digital-forensics.sans.org/blog/2014/09/09/torrentlocker-unlocked

HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group

. Retrieved from https://www2.fireeye.com/APT29_HAMMERTOSS2.html

SCAMwatch radar. (n.d.). Retrieved from http://www.scamwatch.gov.au/content/index.phtml/tag/SCAMwatchRadar/

ISTR: Internet Security Threat Report (2016, April). Retrieved from

. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Cyber-Erpresser infizieren Computer und verschlüsseln die Daten mittels. Retrieved from

. http://www.datenretter-koeln.de/blog/cyber-erpresser-infizieren-computer-und-verschluesseln-die-daten-mittels-ransomware/

Last Updated: April 15th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Bucharest May 2019	Bucharest, RO	May 06, 2019 - May 11, 2019	Live Event
SANS Security West 2019	San Diego, CAUS	May 09, 2019 - May 16, 2019	Live Event
SANS Perth 2019	Perth, AU	May 13, 2019 - May 18, 2019	Live Event
SANS Stockholm May 2019	Stockholm, SE	May 13, 2019 - May 18, 2019	Live Event
SANS Dublin May 2019	Dublin, IE	May 13, 2019 - May 18, 2019	Live Event
SANS Milan May 2019	Milan, IT	May 13, 2019 - May 18, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VAUS	May 19, 2019 - May 24, 2019	Live Event
SANS New Orleans 2019	New Orleans, LAUS	May 19, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, NL	May 20, 2019 - May 25, 2019	Live Event
SANS MGT516 Beta Two 2019	San Francisco, CAUS	May 20, 2019 - May 24, 2019	Live Event
SANS Autumn Sydney 2019	Sydney, AU	May 20, 2019 - May 25, 2019	Live Event
SANS Hong Kong 2019	Hong Kong, HK	May 20, 2019 - May 25, 2019	Live Event
SANS Krakow May 2019	Krakow, PL	May 27, 2019 - Jun 01, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
SANS London June 2019	London, GB	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS Zurich June 2019	Zurich, CH	Jun 03, 2019 - Jun 08, 2019	Live Event
Enterprise Defense Summit & Training 2019	Redondo Beach, CAUS	Jun 03, 2019 - Jun 10, 2019	Live Event
SANS Kansas City 2019	Kansas City, MOUS	Jun 10, 2019 - Jun 15, 2019	Live Event
SANS SEC440 Oslo June 2019	Oslo, NO	Jun 11, 2019 - Jun 12, 2019	Live Event
SANSFIRE 2019	Washington, DCUS	Jun 15, 2019 - Jun 22, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LAUS	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Cyber Defence Canberra 2019	Canberra, AU	Jun 24, 2019 - Jul 13, 2019	Live Event
SANS ICS Europe 2019	Munich, DE	Jun 24, 2019 - Jun 29, 2019	Live Event
SANS Paris July 2019	Paris, FR	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Cyber Defence Japan 2019	Tokyo, JP	Jul 01, 2019 - Jul 13, 2019	Live Event
SANS Munich July 2019	Munich, DE	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	OnlineES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced