Admiral Group

Computer Security Research Report 2018

Task - 1

Table of Contents

Contents

Admiral Group Company Security Research Report 2018 01

Table of Contents.....02

Student Declaration.....03

Company Overview.....04

Company Assets 04

Risk Insurance Company Face 05

Website Details of the current malware threats.....05

Most recent top threats 05

1. WannaCry.....06
2. Cerber 07
3. Kobter 08
4. Loyphish 10
5. Sirefef 11
6. Emotet 12
7. FBI Virus 13
8. SamSa Ransomware 14

Conclusion.....15

Recommendation.....15-16

Reference 17

Student Declaration

I can confirm the following details:

Student ID/Registration Number : R00144214

Name : Mohammed Alom

Module Name: Computer Security

Module Lecturer: Mr. Dylan Smith

I confirm that this is my own work.

Due Date: Friday 5th October 2018

Student Signature:

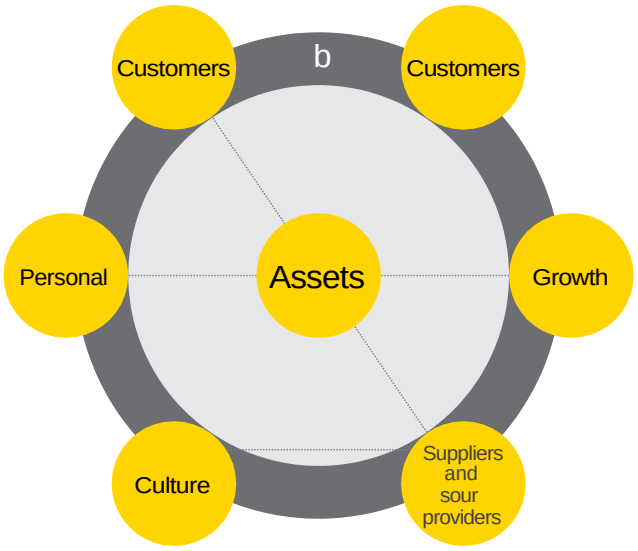
Signed: Mohammed Jahangir Alom

_____

Company Overview

Admiral Group is a public limited company and it is one of the largest insurance company in the UK and it has branch other European countries as well as US and Mexico. The company provides car, home, van and travel insurance. Recently company providing personal loan and car finance in the UK. The company providing service almost five million customers around the world. In terms of assets, the company has number crown jewels.

Company Assets



After studying and researching company website came up some of the assets that Admiral Group is dealing with would be -

- Policyholders
- Creditors
- Shareholders
- Shares Price
- Clients list
- Personal and Financial data and more

The company is very concern about their business security awareness due to recent online threat arise worldwide. The insurance sector has lagged far behind than other financial-sector industries in its adoption of cybersecurity technologies, perhaps because they have not (so far) been aggressively targeted by cyber thieves. As banks and other financial institutions were among the first under fire, they are now among the most secure.

Some of the risk they might face during their business dealing with customers and these primary cyber-risk to insurance companies today include –

Risks insurance companies face

- Cybersecurity/cybercrime (operational risk) ...
- Infrastructure vulnerabilities – unpatched software provide easy fodder for hackers
- Identify theft – can occur as a result of client account breach
- Automated threats – such as denial of service
- Pricing and product-line profit (insurance risk) ...
- IT / systems / technology gap (operational risk) ...
- Competition (strategic risk) ...
- Underwriting (insurance risk) ...
- Legislative & regulatory (operational risk) ...
- Investment market risk (investment risk)

Cyber-attacks these days are nothing new, but the latest round of attacks has highlighted the digital world. Hundreds of thousands of devices have been affected by the recent malware attacks. Many companies and digital users have neglected the aspect of cyber security for so long. Now, they're slowly realizing the importance of it.

Most recent top malware list

After investigating a few renowned and well-known websites such as

- McAfee
- Norton
- Trend Micro and
- Symantec
- Avast

to find out recent Malware facing the industry. After going through well revised all the content in all of the above-mentioned website came up recent top malware threats facing in the industry these days and that have attacked users in the recent times are –

1. WannaCry
2. Cerber
3. Kobter
4. Loyphish
5. Sirefef
6. Emotet
7. FBI Virus
8. SamSa – Ransomware

1.WannaCry

Image Source: Cisco Talos

Risk Analysis of the threat:

WannaCry has the ability to spread itself within corporate networks without user interaction, by exploiting known vulnerabilities in Microsoft Windows.

It is, Of course, the most-hyped cyber-attacks in the recent times. This is a ransomware attack module, where these malicious worms are deployed into the victims' devices through different types of doorways, mostly through phishing emails.

Type of threat:
WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017. After infecting a Windows computer, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them.

How it works:
It works through email. Once deployed, these worms encrypt the local files and allow the user to get back their data only after paying the demanded ransom.

How to remove WannaCry:
There are couple of steps need to do to overcome the WannaCry affected device. To remove this threat, download and run a scan with the Antivirus Software Bootable Recovery Tool. The files encrypted by WannaCry ransomware will remain encrypted. Anti-Virus products like (Norton) do not decrypt files that have been affected by these threats.

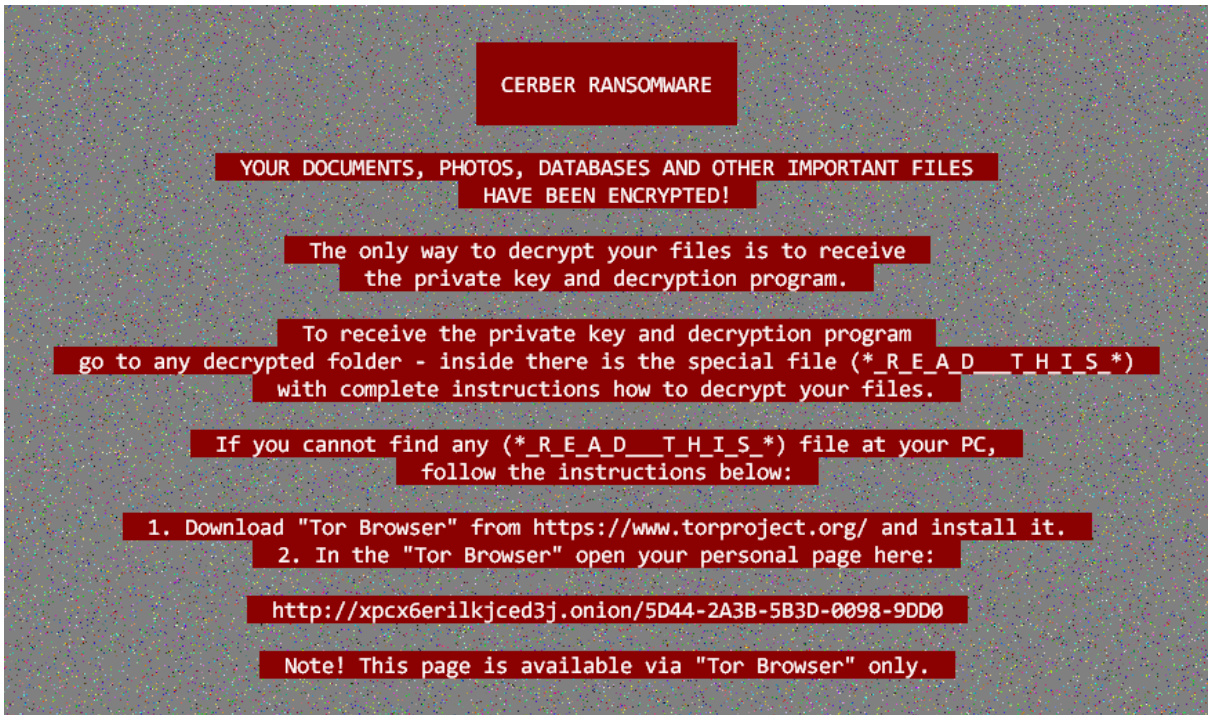
2. Cerber

Risk Analysis of the threat:

One of the most active kinds of ransomware out there, Cerber encrypts the files of infected users and demands money in exchange for giving access to their files back. It works even if you are not connected to the internet, so you can't stop it by unplugging your PC.

What is it:

Your first clue that your PC has been infected with Cerber will come after you log in, because your desktop wallpaper will have been changed to display a desktop note.



How does it work:

Typically, the victim receives an email with an infected Microsoft Office document attached. Once opened, the malware encrypts files with RC4 and RSA algorithms and renames them with a. cerber extension (if infected with one of the earlier variants of the malware) or a random file extension in the latest versions.

How to remove:

Antivirus technology detects and removes Cerber ransomware, as well as other kinds of malware. If your PC is infected with Cerber ransomware, antivirus will detect it, quarantine it and destroy it.
Unfortunately, there is no Cerber decryptor that works to recover files that have already been encrypted. This is why prevention is essential.

3. Kovter

Image source: Trend Micro

Risk Analysis of the threat:

The Kovter infection is a trojan that performs click-fraud while running on a computer. This infection is typically installed via exploit kits found on hacked web sites or trojan downloaders like Nemucod.

When Kovter is installed, the actual infection is stored in the Windows registry rather than as a file on a hard drive. This method of storing the malware files in the registry rather than the hard drive makes it more difficult for antivirus programs to properly detect it.

Type of threat: Kovter dected by trend Micro and It is a trojan type of threat. It is looking for right opportunities usually when the user downloaded illegal files.

How it works: Kovter working flow and how its work

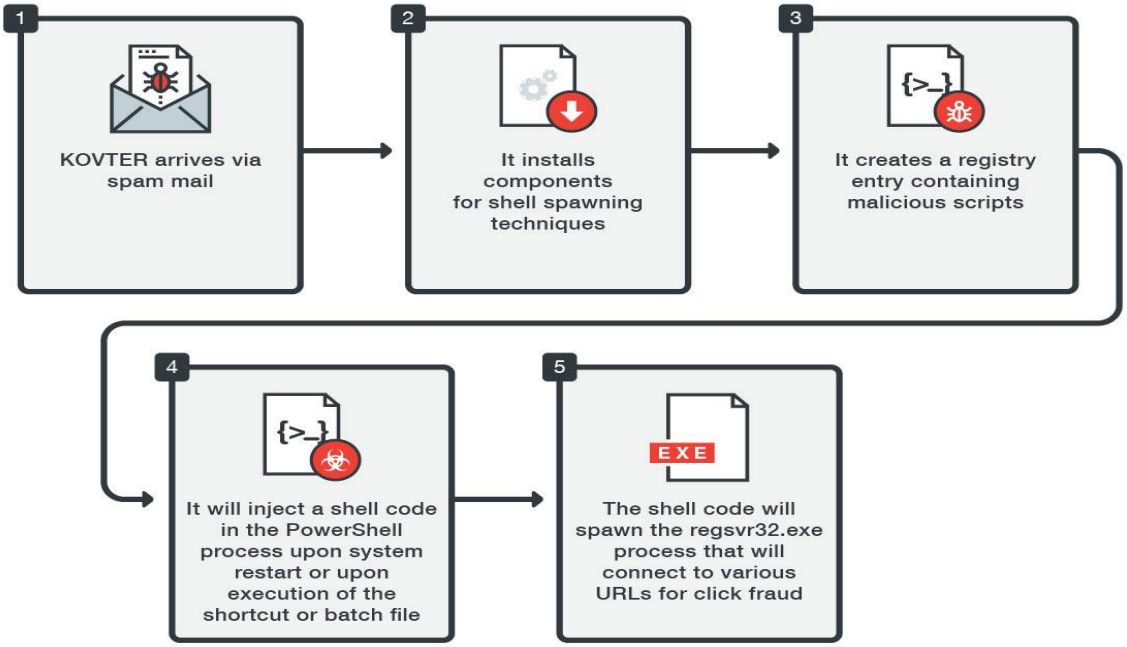


Image: KOVTER infection flow

How to remove:

- Always update the anti-virus software installed in your computer and conduct regular full scanning at least once a week;
- Enable pop-up blocker;
- Install a powerful ad-blocker for Chrome, Mozilla and Internet Explorer;
- Do not open e-mail attachments or hyperlinks you receive from an unknown sender or they could contain malware;
- Clean your Windows Registry; and
- Be cautious about unsolicited attachments.

4. PWS:HTML/Loyphish.G

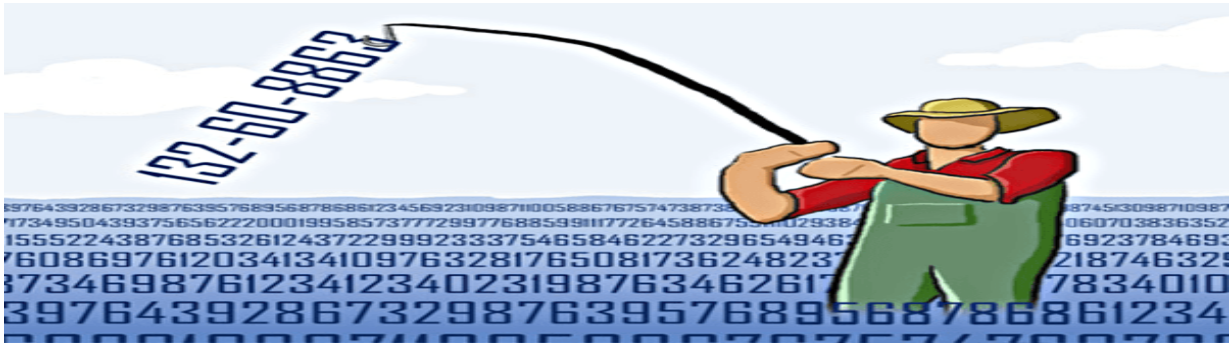


Image Source: techworld

Risk Analysis of the threat:

The following may indicate the presence of this malware:

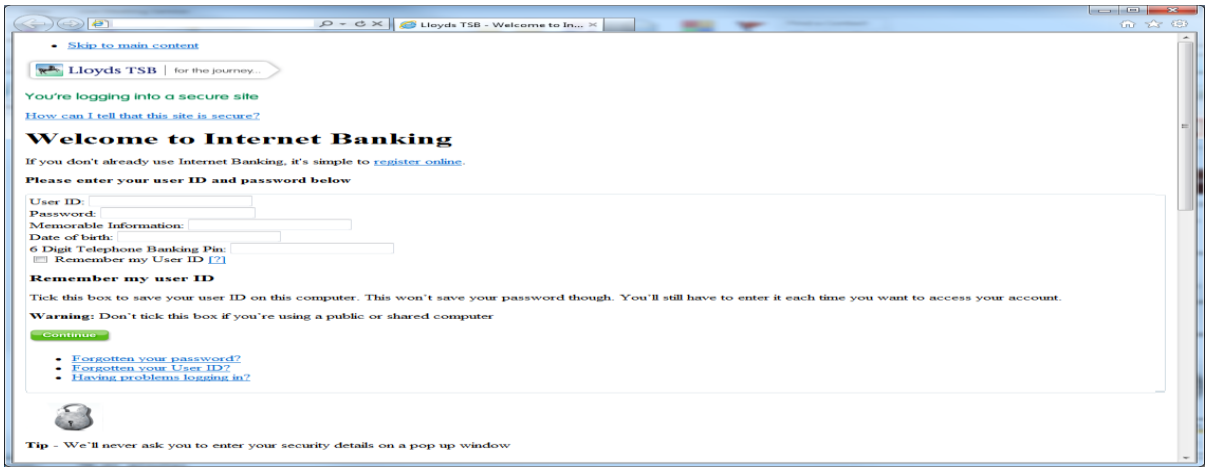
- An email inviting or requesting you to fill in your online banking details
- The display of the following pages, or ones similar, that ask you to fill out your online banking details:

Phishing pages attempt to steal sensitive and confidential information from affected users to perpetrate fraud.

What is it and how it works:

PWS:HTML/Loyphish.G is a password-stealing malicious webpage, known as a phishing page, that disguises itself as a legitimate online banking webpage. It is a member of the PWS:HTML/Phish family.
The webpage attempts to steal your online login information by tricking you into filling out your details in a form on a fake page, and then sending that information to a remote attacker.

These webpages are highly sophisticated in design, which makes you believe that you're interacting with the original website of your bank. These pages are cleverly built with all the original images, logos, and text. These attacks are targeted against pretty much everyone.



How to remove it - To detect and remove this threat and other malicious software that may be installed on your computer, run a full-system scan with an appropriate, up-to-date, security solution.

5. Sirefef

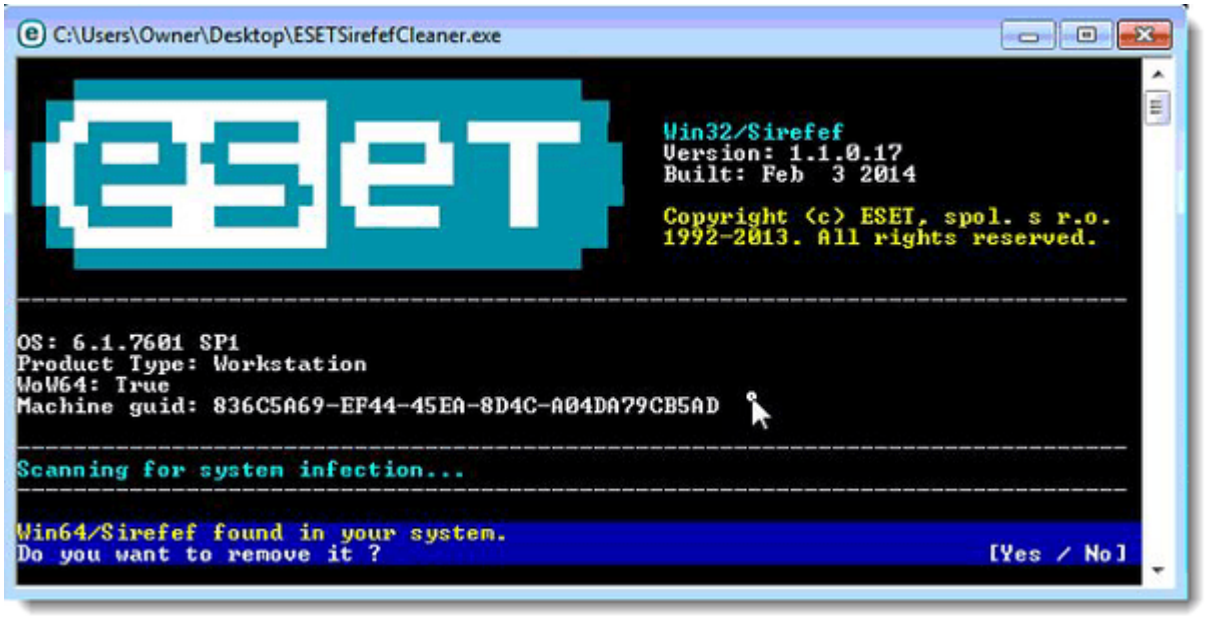


Image Source: vir.us

Risk Analysis of the threat:
The **Sirefef trojan** is a dangerous threat that has been circulating for several years.
This is one of the most advanced malware threats out there. Many devices have been affected by this in the recent times. Also known as ZeroAccess, Sirefef also transmits your confidential information to remote servers. Additionally, it can also disable your Windows Firewall and Windows Defender as well.

What is it: It's a Trojan type of virus.

How does it work:

This malicious threat operates in complete stealth mode, leaving little to no trace of its existence in your device. This file usually gets into your device when you're downloading pirated files, software, and similar others. So, if you're downloading cracked software or keygens, you could be making your computer vulnerable.

To remove Sirefef Trojan virus, follow these steps:

Step 1: Use ESETSirfefCleaner tool to remove Sirefef Trojan
Step 2: Use RKill to stop the Sirefef Trojan malicious processes
Step 3: Scan your computer with Malwarebytes Anti-Malware to remove Sirefef Trojan
Step 4: Double-check for malicious programs with HitmanPro
(OPTIONAL) STEP 5: Use Zemana AntiMalware Portable to remove Sirefef Trojan

6.Emotet

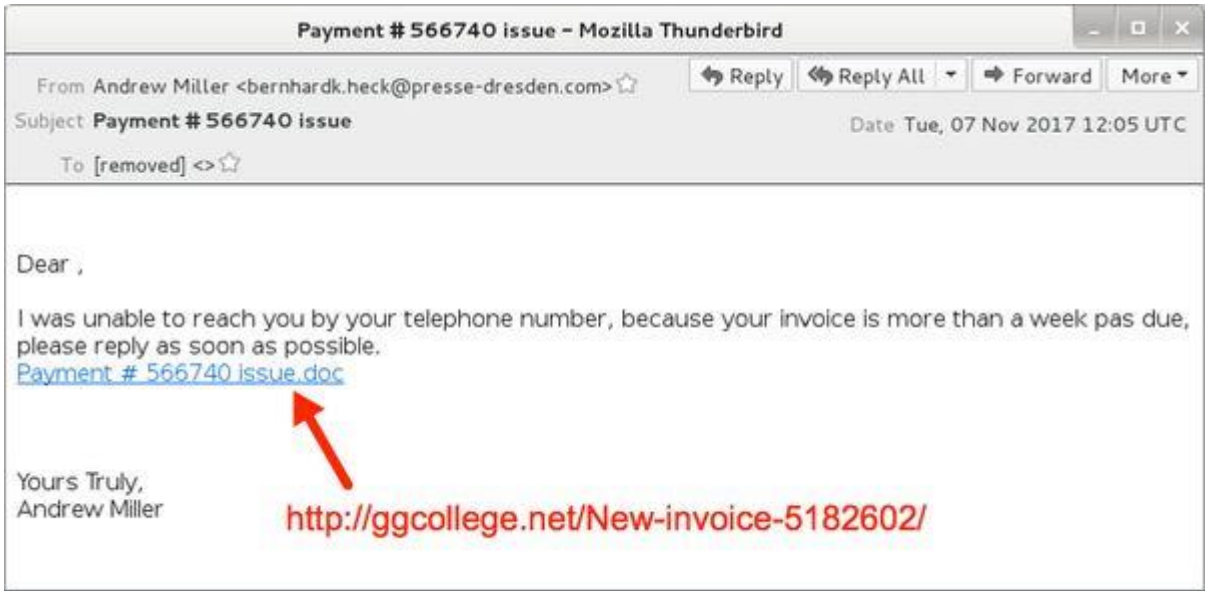


Image Source: eset

Risk Analysis of the threat:

Emotet is high-risk malware designed to record personal data and proliferate other viruses. Research shows that Emotet infiltrates systems without users' consent. After successful infiltration, this malware modifies system settings and uses the infiltrated computer to proliferate itself further.

What is it:
It is a modular trojan that download or drops banking Torjans.

How it works –
Initial infection occurs via malspam emails that contain malicious download links, a PDF with embedded links, or a macro-enabled Word is a modular banking Trojan which uses keystroke logging to compromise victim credentials when the user visits a banking website.

How to remove it –

Manual threat removal might be a lengthy and complicated process that requires advanced computer skills. Spyhunter is a professional automatic malware removal tool that is recommended to get rid of Emotet trojan.

7. FBI Virus

Risk Analysis of the threat:

This kind of virus in the company staffs can easily be affected while they were using online every day due to nature of the work involve constantly for insurance company staffs.

What is it:

It is a highly dangerous malware, FBI virus which is alternatively known as FBI Moneypack Scam, is a very cleverly designed malicious file.

How does its work:

When attacked by this threat, your computer will display an alert which states that your computer has been locked down due to violations of copyrights. This alert tries to deceive you that you've been blocked due to any type of illegal access or downloads of files such as music, software, movies, and many others. In order to get your computer unblocked, you would have to pay two hundred dollars. Many commoners have fallen victim to this scam, making it one of the hazardous attacks in the recent past.

How to remove this threat:

Option 1: Remove FBI MoneyPak lock screen virus with System Restore
Step 1: Restore Windows to a previous state using System Restore. ...
Step 2: Remove FBI MoneyPak malicious files with Malwarebytes Anti-Malware Free. ...
Step 3: Double-check for the FBI MoneyPak virus with HitmanPro.

If you're still among such people who don't take the digital security seriously, you should definitely know about the latest attacks that have targeted loads of devices all around the world.

8.SamSa - Ransomware

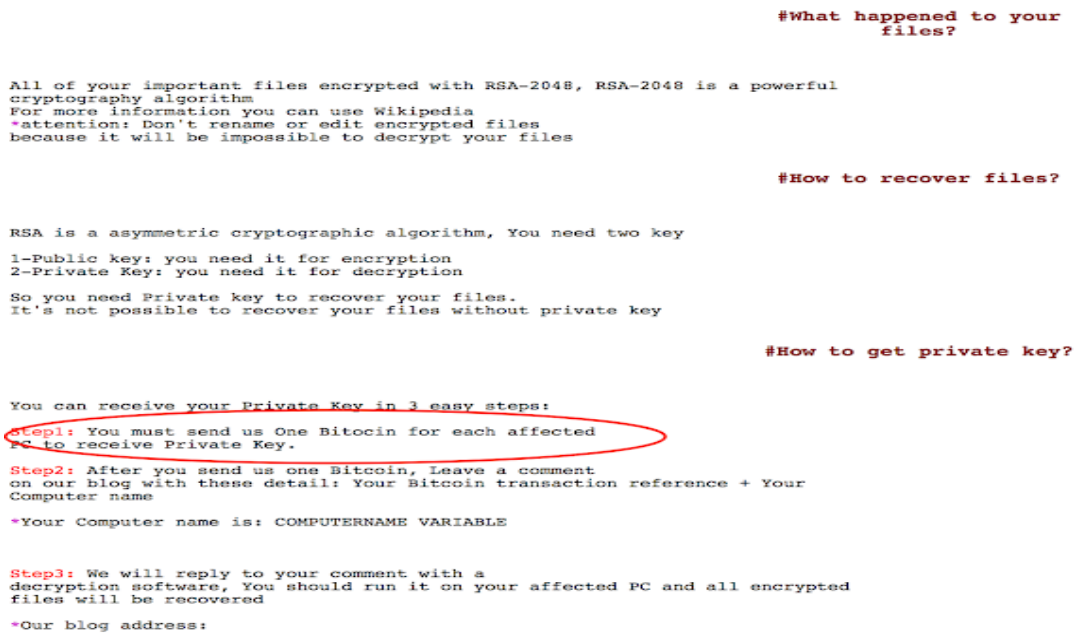
Risk Analysis of the threat:

The ransomware targets a range of sectors including healthcare, industrial control, and government. The malicious software seeks out insecure RDP connections as well as vulnerable JBoss systems to carry out its infections.

How does it work:

Upon compromising the system, the sample will launch a samsam.exe process which begins the process of encrypting files on the system.

SamSam encrypts various file types with Rijndael and then encrypts that key with RSA-2048 bit encryption. This makes the files unrecoverable unless the author made a mistake in the implementation of the encryption algorithms.



#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files
because it will be impossible to decrypt your files

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us One Bitocin for each affected PC to receive Private Key.

Step2: After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

*Your Computer name is: COMPUTERNAME VARIABLE

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our blog address:

Recommendation

Company can follow below recommendation and encourages all users and administrators to adhere to the following basic security "best practices": **to stay safe in the business as well as to keep safe and secure their customer valuable information.**

- Never open email attachments or links that seem irrelevant and came from suspicious email address. Delete these emails immediately. Download your programs from official sources only. The same applies to updating software.
- It is very important to keep installed applications up-to-date.
- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available.
- Enforce a password policy all level in the company. Complex passwords make it difficult to crack password files on compromised computers.
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task.
- Disable AutoPlay to prevent the automatic launching of executable files on network.
- Turn off file sharing if not needed.
- Disable anonymous access to shared folders
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further.
- Train employees not to open attachments unless they are expecting them.
- Do not execute software that is downloaded from the Internet unless it has been scanned for viruses.
- If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request.
- Do not accept applications that are unsigned or sent from unknown sources.

Conclusion

The main reasons for computer infections are poor knowledge and careless behaviour. The key to safety is caution. Therefore, pay close attention when browsing the Internet and downloading/installing/updating software.

By now, you may have gotten a deep insight into some of the highly dangerous malware threats that have attacked and affected thousands of devices in the recent times. If you want to safeguard yourself from such attacks, you must tighten up your security defences by using a good anti-virus program that offers an effective combat system against malware threats.

Reference:

http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1242281415644/Asset_Structures_for_Insurers.pdf

https://en.wikipedia.org/wiki/Admiral_Group

https://www.cisecurity.org/blog/top-10-malware-january-2018/

https://www.colocationamerica.com/blog/latest-malware-threats

https://blog.talosintelligence.com/2016/03/samsam-ransomware.html

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kovter-an-evolving-malware-gone-fileless

https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=PWS:HTML/Loyphish.G

https://docs.microsoft.com/en-gb/windows/security/threat-protection/intelligence/understanding-malware

https://pnpacg.ph/main/2-uncategorised/259-acg-cyber-security-bulletin-no-128-understanding-the-risk-of-kovter-trojan

https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

https://malwaretips.com/blogs/remove-sirefef-trojan/

https://www.pcrisk.com/removal-guides/12862-emotet-virus

http://virus.wikia.com/wiki/Suspicious.Emit

https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html

https://www.websecurity.symantec.com/security-topics/malware-scanning

https://businessworld-usa.com/cyber-security-risks-facing-insurance-companies-2017/

https://www.avast.com/c-cerber

https://www.ey.com/Publication/vwLUAssets/ey-cyber-strategy-for-insurers/$FILE/ey-cyber-strategy-for-insurers.pdf