CIT CORK INSTITUTE OF TECHNOLOGY

INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Admiral Group

Computer Security Research Report 2018

Task – 1-2-3

# Table of Contents

Contents

# 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

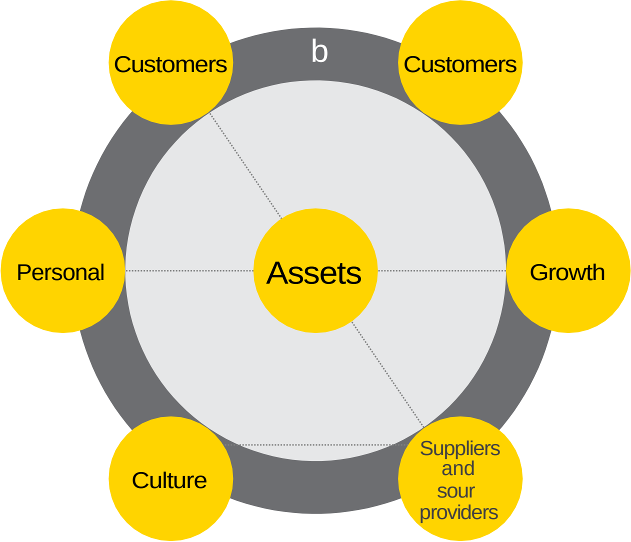
Student Signature:

Signed: Mohammed Jahangir Alom
____________________

## Company Overview

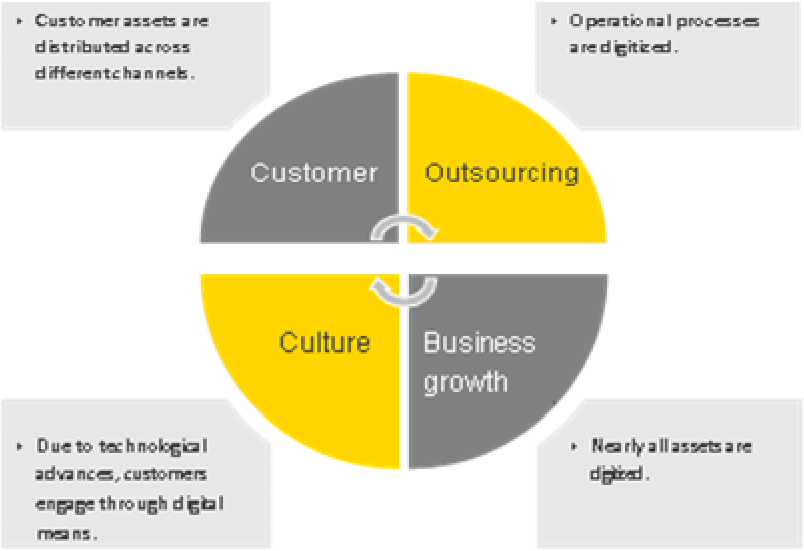
Admiral Group is a public limited company and it is one of the largest insurance company in the UK and it has branch other European countries as well as US and Mexico. The company provides car, home, van and travel insurance. Recently company providing personal loan and car finance in the UK. The company 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



- Customer assets are distributed across different channels.
- Operational processes are digitized.
- Due to technological advances, customers engage through digital means.
- Nearly all assets are digitized.

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**

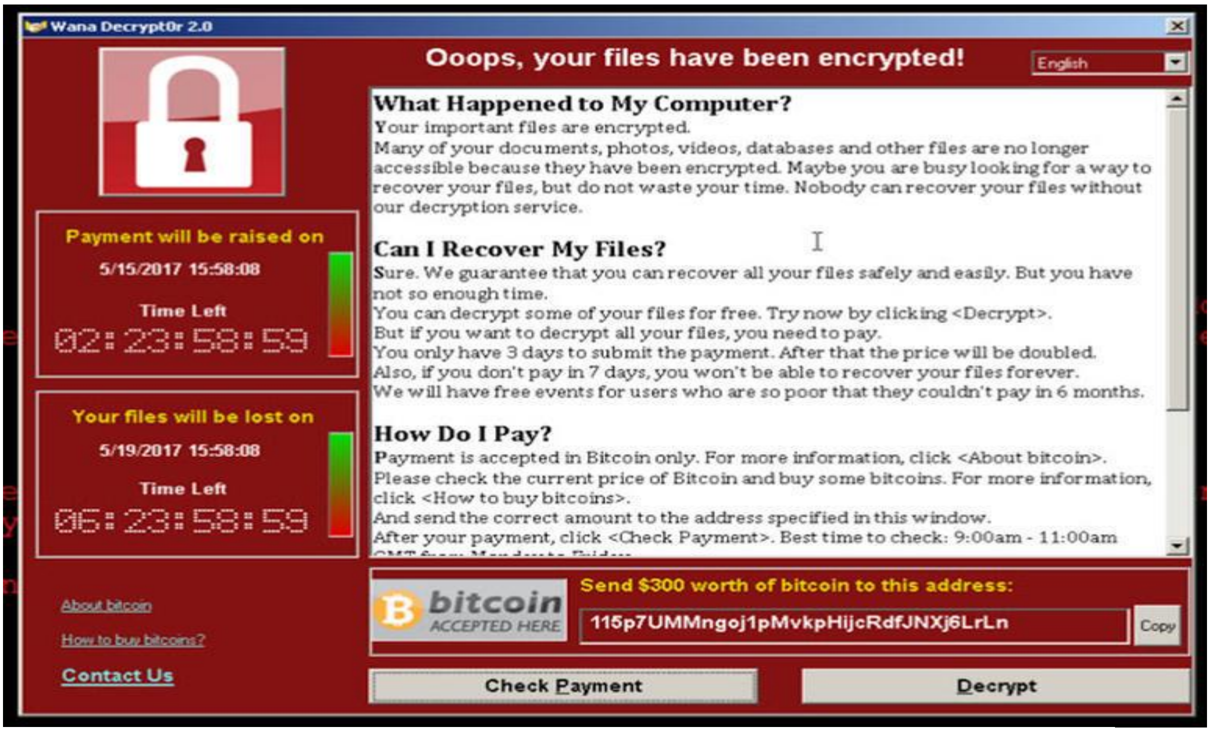
After investigating a few renowned and well-known websites such as

- 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



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

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.

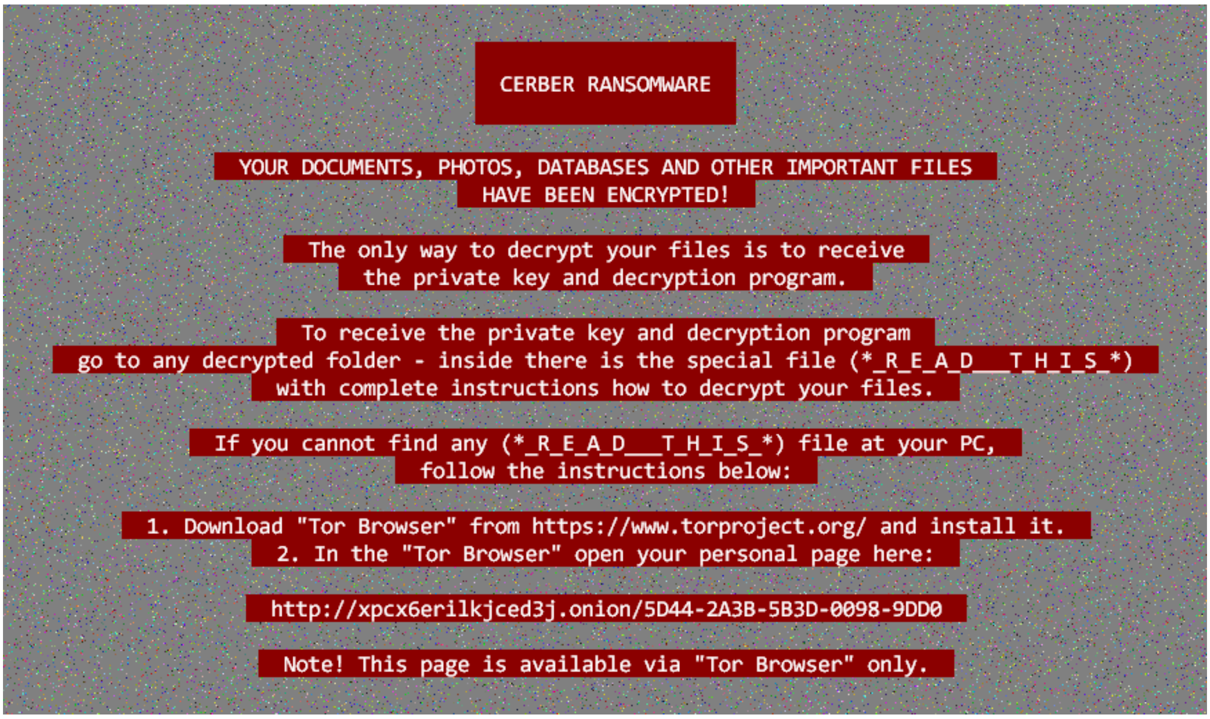
## 2. Cerber

### 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.



CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*_R_E_A_D___T_H_I_S_*)
with complete instructions how to decrypt your files.

If you cannot find any (*_R_E_A_D___T_H_I_S_*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://xpcx6eri1kjced3j.onion/5D44-2A3B-5B3D-0098-9DD0

Note! This page is available via "Tor Browser" only.

### 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

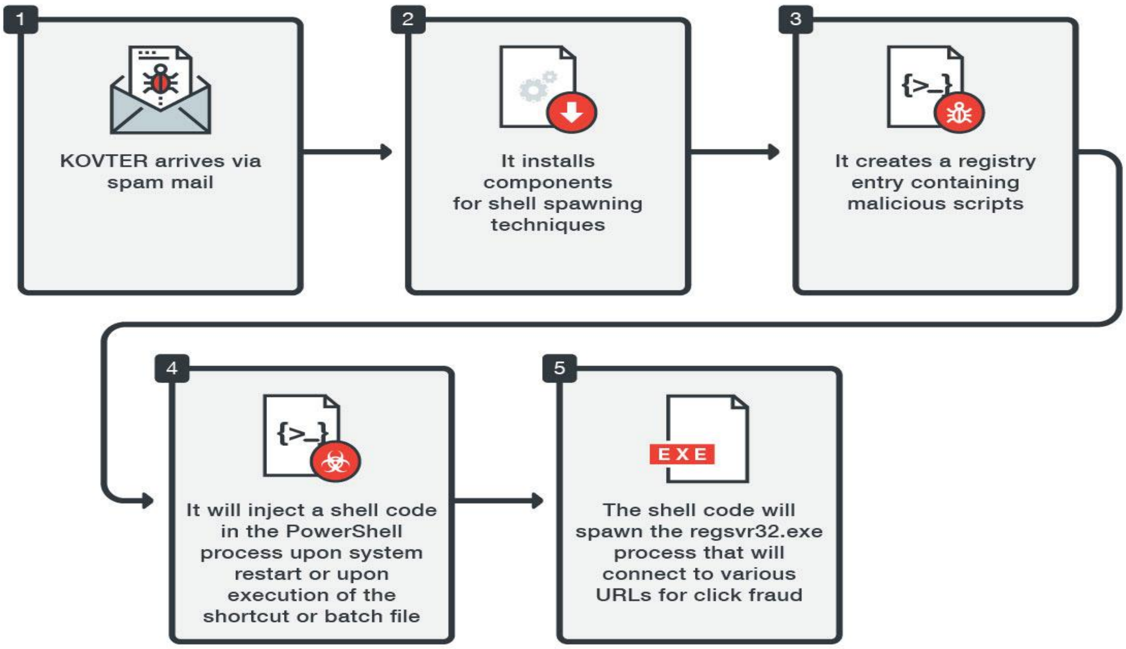
**Risk Analysis of the threat:**

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



1 KOVTER arrives via spam mail

2 It installs components for shell spawning techniques

3 It creates a registry entry containing malicious scripts

4 It will inject a shell code in the PowerShell process upon system restart or upon execution of the shortcut or batch file

5 The shell code will spawn the regsvr32.exe process that will connect to various URLs for click fraud

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

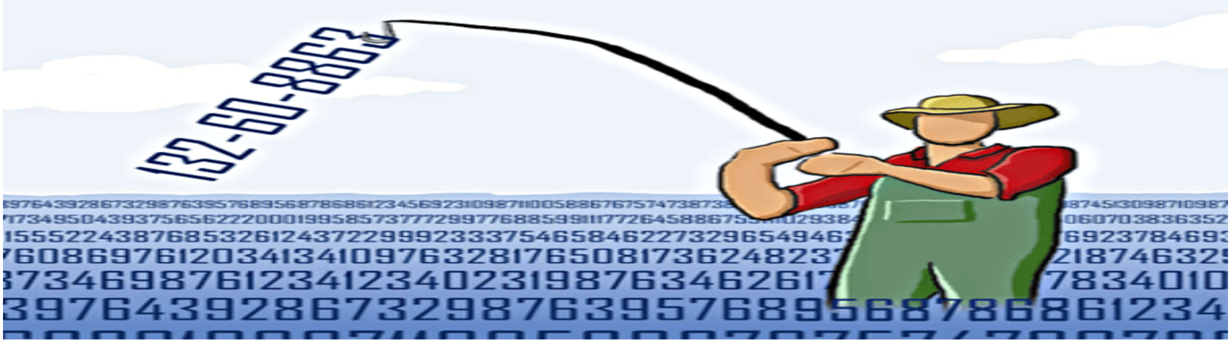


Image Source: techworld

**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:

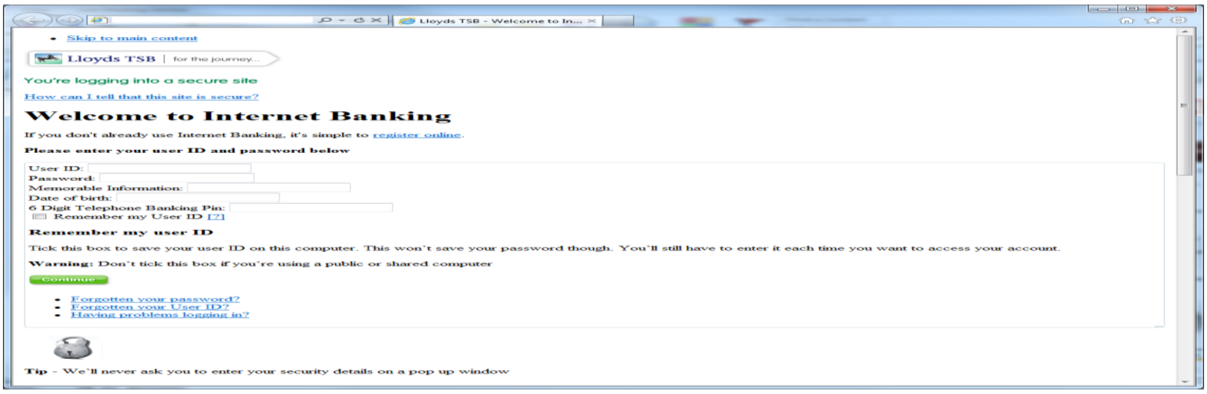
Phishing pages attempt to steal sensitive and confidential information from affected users to perpetrate fraud.

**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.



- Skip to main content

Lloyds TSB | for the journey...

You're logging into a secure site

How can I tell that this site is secure?

Welcome to Internet Banking

If you don't already use Internet Banking, it's simple to register online.

Please enter your user ID and password below

User ID:
Password:
Memorable Information:
Date of birth:
6 Digit Telephone Banking Pin:
□ Remember my User ID [?]

Remember my user ID

Tick this box to save your user ID on this computer. This won't save your password though. You'll still have to enter it each time you want to access your account.

Warning: Don't tick this box if you're using a public or shared computer

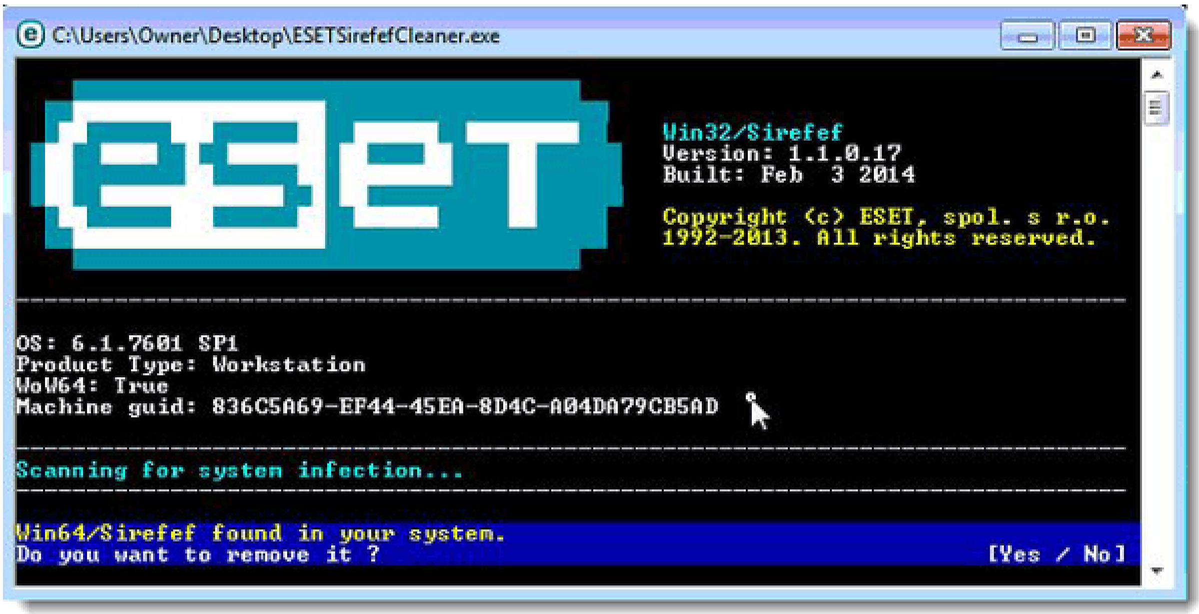
Continue

- Forgotten your password?
- Forgotten your User ID?
- Having problems logging in?

Tip - We'll never ask you to enter your security details on a pop up window

**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



```
Win32/Sirefef
Version: 1.1.0.17
Built: Feb  3 2014

Copyright (c) ESET, spol. s r.o.
1992-2013. All rights reserved.

--------------------------------------------------------------------------------
OS: 6.1.7601 SP1
Product Type: Workstation
WoW64: True
Machine guid: 836C5A69-EF44-45EA-8D4C-A04DA79CB5AD
--------------------------------------------------------------------------------
Scanning for system infection...
--------------------------------------------------------------------------------
Win64/Sirefef found in your system.
Do you want to remove it ?                                          [Yes / No]
```

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.

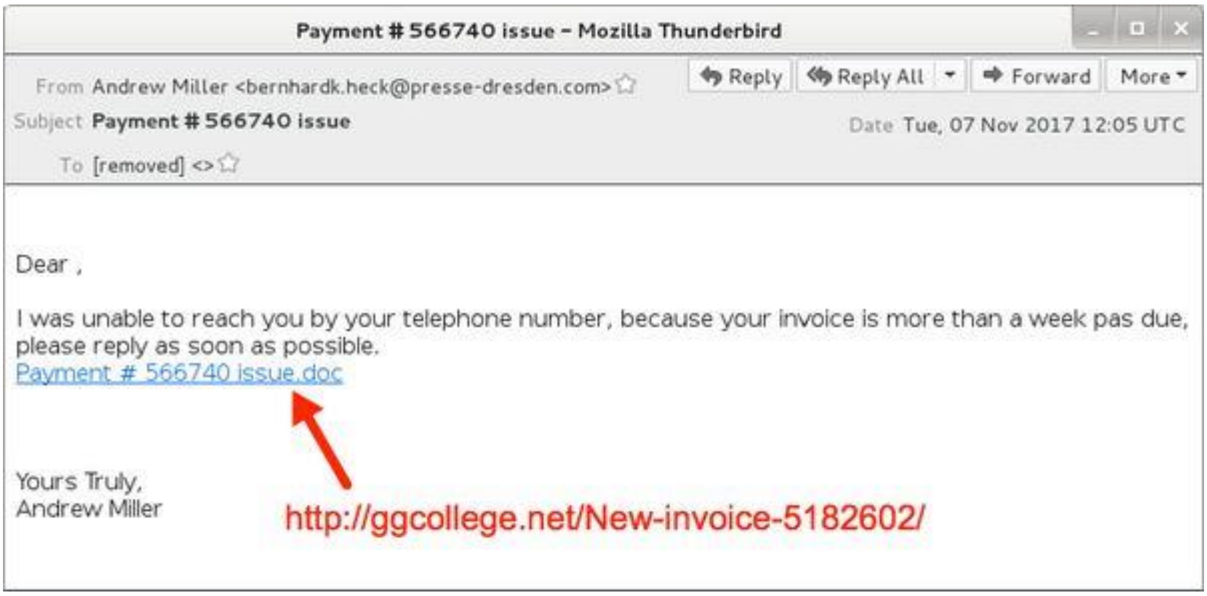
**How does it work:**

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



From Andrew Miller <bernhardk.heck@presse-dresden.com>
Subject Payment # 566740 issue
To [removed] <>
Date Tue, 07 Nov 2017 12:05 UTC

Dear ,

I was unable to reach you by your telephone number, because your invoice is more than a week pas due, please reply as soon as possible.
Payment # 566740 issue.doc

Yours Truly,
Andrew Miller

http://ggcollege.net/New-invoice-5182602/

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

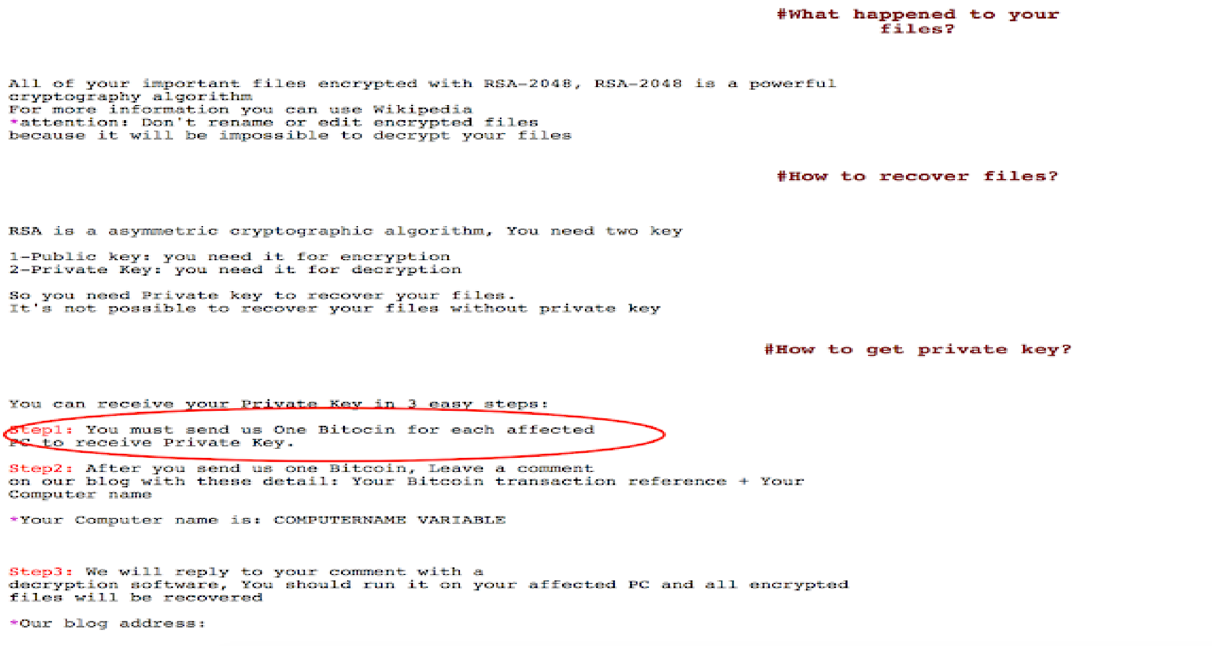
### Risk Analysis of the threat:

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.

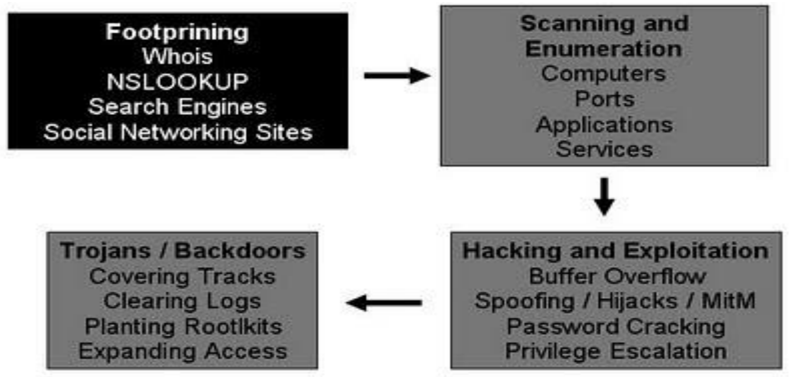
By now, you may have gotten a deep insight into some of the highly dangerous malware threats that have attacked and affected thousands of devices in the recent times. If you want to safeguard yourself from such attacks, you must tighten up your security defences by using a good anti-virus program that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

## Task 2:

In this article I am going to write about the footprinting and the method used by hacker due to weakness of the company. How company can stay vigilant and can protect its resources by resolving those weakness. In the later part of the article I will discuss about the social engineering process and how company is going to affected by social engineering. Also recommendation for the company both physical and digital authentication should take care for its business.

**Definition of the Footprinting:**

For the hacker footprinting is an information gathering process to penetrate company resources through weak link. Through this process, different tools and techniques are used to collect as much as information against the target and its assets. This is a pre-attack stage and target can never trace back.
Today's a hacker uses several freely available resources to gather maximum information for the target company. In this process no, direct contact is made with the target. Footprinting plays a crucial role in determining the success in later steps/hacking attempts.



*This is the basic block diagram which shows the steps that are include in the penetration testing methodology*

There are other several tools and techniques used in Information Gathering. Also, there is no predefined steps of instructions in Footprinting to be performed.

**Here is the list of the method and techniques used to gather information:**

- Websites Footprinting
- Whois Database Lookup
- Search Engines Hacking
- Similar Domain Search
- Negative Website Search
- Social & Business Networking Websites
- Classified/Job Websites
- Internet History – Achieve Pages
- DNS Footprinting – MX Entry
- Traceroute
- DNS queries
- Network enumeration
- Network queries
- Operating system identification
- Organizatioanl queries
- Ping sweeps
- Point of contact queries
- Port scanning
- Register queries (WHOIS queries)
- SNMP queries
- World Wide Web sidering

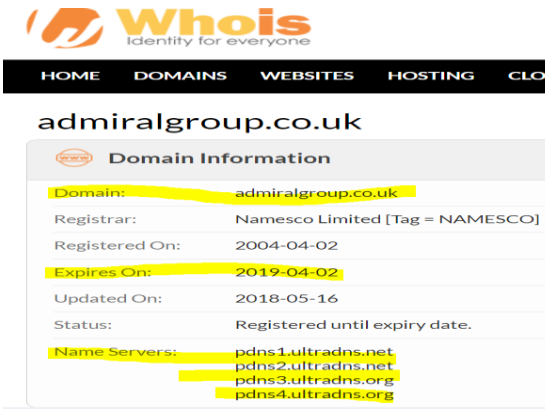
**Here I will give little description some of the method and technique**

**Websites Footprinting** – through this technique Hacker can get valuable information once they visit target website and can collect great amount of information, such as their emails addresses, partners, client's list, physical addresses of their offices and HR openings etc.
For further analysis hacker can put invalid email address. Errors can appear if you put invalid data in search boxes or contact forms. Errors can reveal details about website content management system software, its version, scripting and type of server used– Linux or Windows etc.

**Whois Database Lookup**
Whois lookup is an important step in information gathering process. Whois lookup against any website can reveal information about servers on which website is hosted & its location. Whois lookup also displays name, address and contact numbers of technical staff, domain owner and domain registrar. Here some WHOIS Lookup Websites listed below:

- www.whois.com
- www.whois.domaintools.com
- www.whois.net
- www.whois.com/whois/

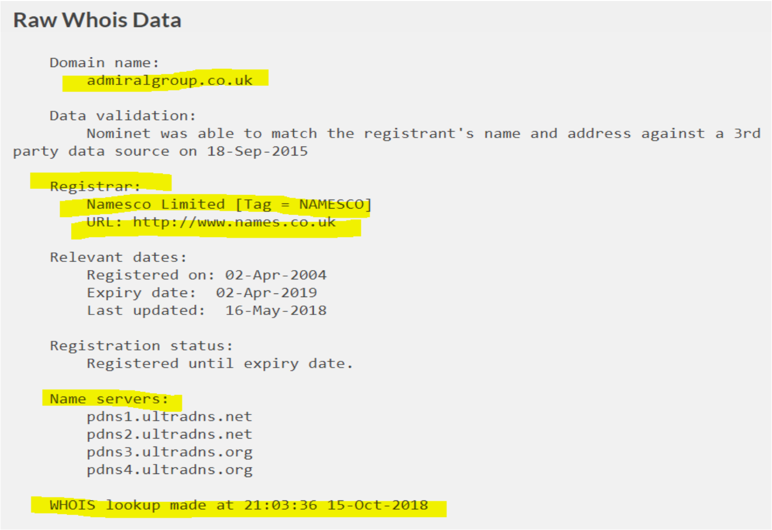
**Some very valuable information gathers through by whois website for Admiralgroup**



admiralgroup.co.uk

Domain Information

| | |
|---|---|
| Domain: | admiralgroup.co.uk |
| Registrar: | Namesco Limited [Tag = NAMESCO] |
| Registered On: | 2004-04-02 |
| Expires On: | 2019-04-02 |
| Updated On: | 2018-05-16 |
| Status: | Registered until expiry date. |
| Name Servers: | pdns1.ultradns.net<br>pdns2.ultradns.net<br>pdns3.ultradns.org<br>pdns4.ultradns.org |



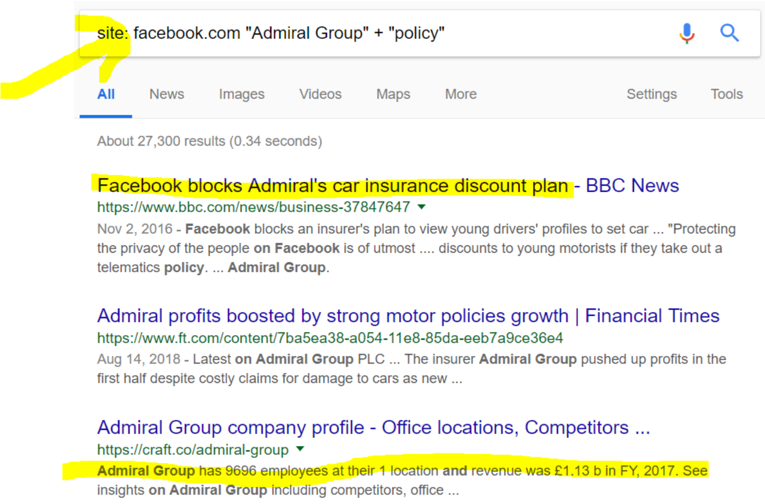
Raw Whois Data

```
    Domain name:
        admiralgroup.co.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd
party data source on 18-Sep-2015

    Registrar:
        Namesco Limited [Tag = NAMESCO]
        URL: http://www.names.co.uk

    Relevant dates:
        Registered on: 02-Apr-2004
        Expiry date:  02-Apr-2019
        Last updated:  16-May-2018

    Registration status:
        Registered until expiry date.

    Name servers:
        pdns1.ultradns.net
        pdns2.ultradns.net
        pdns3.ultradns.org
        pdns4.ultradns.org

    WHOIS lookup made at 21:03:36 15-Oct-2018
```

**Search Engines Hacking**
Hacker will get valuable information through search engine like Google, Yahoo, Bing etc. Google Advance search | Google Hacking can help a hacker to locate detailed information like company policies, employee's details & online hidden pages etc.

This information gathers for research purpose through whois.com

## Following is an example of Google search engien Hacking:



site: facebook.com "Admiral Group" + "policy"

About 27,300 results (0.34 seconds)

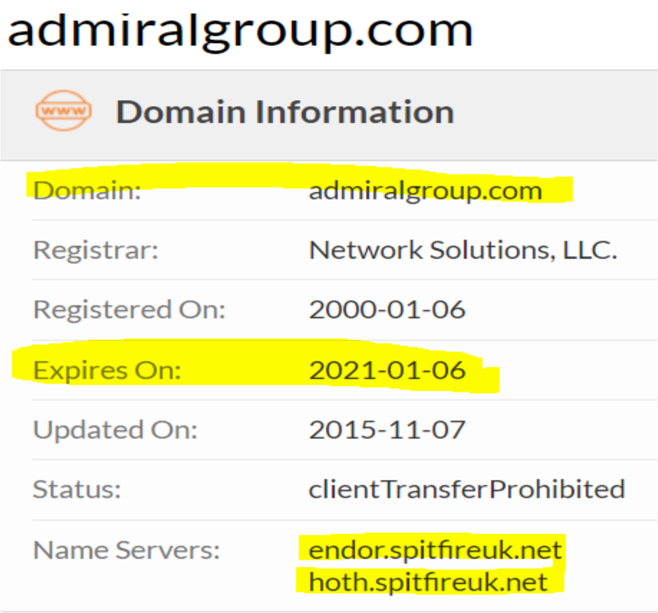
Facebook blocks Admiral's car insurance discount plan - BBC News
https://www.bbc.com/news/business-37847647
Nov 2, 2016 - **Facebook** blocks an insurer's plan to view young drivers' profiles to set car ... "Protecting the privacy of the people **on Facebook** is of utmost .... discounts to young motorists if they take out a telematics **policy**. ... **Admiral Group**.

Admiral profits boosted by strong motor policies growth | Financial Times
https://www.ft.com/content/7ba5ea38-a054-11e8-85da-eeb7a9ce36e4
Aug 14, 2018 - Latest **on Admiral Group** PLC ... The insurer **Admiral Group** pushed up profits in the first half despite costly claims for damage to cars as new ...

Admiral Group company profile - Office locations, Competitors ...
https://craft.co/admiral-group
**Admiral Group** has 9696 employees at their 1 location **and** revenue was £1.13 b in FY, 2017. See insights **on Admiral Group** including competitors, office ...

***Google Search Command:***
site:facebook.com "Admiral Group" + "policy"
The above Google search query target facebook.com for all the persons having name *Admiral Group* and talking about the Company.

### Similar Domain Search



admiralgroup.com

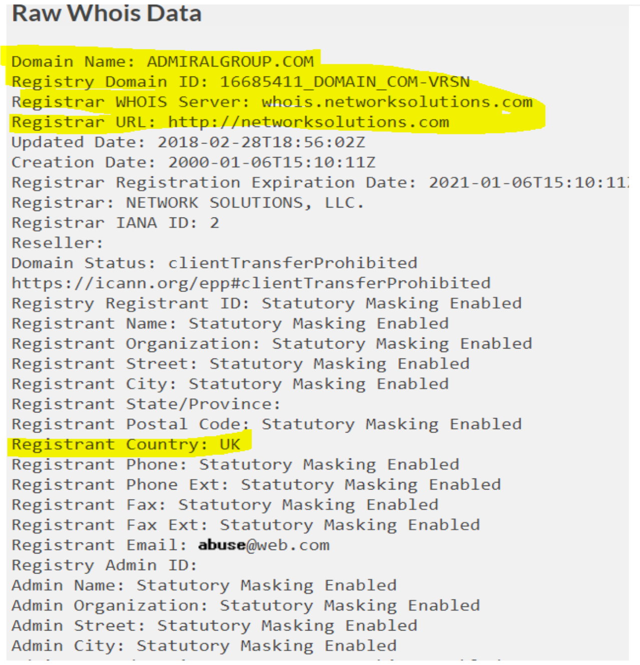
Domain Information

| | |
|---|---|
| Domain: | admiralgroup.com |
| Registrar: | Network Solutions, LLC. |
| Registered On: | 2000-01-06 |
| Expires On: | 2021-01-06 |
| Updated On: | 2015-11-07 |
| Status: | clientTransferProhibited |
| Name Servers: | endor.spitfireuk.net<br>hoth.spitfireuk.net |

If example.com is your target's website domain then you can look at example.in, example.net, example.org for a worldwide variety sources. Further, looking for in.example.com, uk.example.com (country basis) or en.example.com (language basis) can reveal more useful information.

Same company may have different works at different countries and may be presenting different information in different languages.

**Try:** touch.facebook.com, mbasic.facebook.com, facebook.com.



```
Raw Whois Data

Domain Name: ADMIRALGROUP.COM
Registry Domain ID: 16685411_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-02-28T18:56:02Z
Creation Date: 2000-01-06T15:10:11Z
Registrar Registration Expiration Date: 2021-01-06T15:10:11
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Statutory Masking Enabled
Registrant Name: Statutory Masking Enabled
Registrant Organization: Statutory Masking Enabled
Registrant Street: Statutory Masking Enabled
Registrant City: Statutory Masking Enabled
Registrant State/Province:
Registrant Postal Code: Statutory Masking Enabled
Registrant Country: UK
Registrant Phone: Statutory Masking Enabled
Registrant Phone Ext: Statutory Masking Enabled
Registrant Fax: Statutory Masking Enabled
Registrant Fax Ext: Statutory Masking Enabled
Registrant Email: abuse@web.com
Registry Admin ID:
Admin Name: Statutory Masking Enabled
Admin Organization: Statutory Masking Enabled
Admin Street: Statutory Masking Enabled
Admin City: Statutory Masking Enabled
```

## Social & Business Networking Websites

If you want more detailed information about a company or person then you must take a look at some social-professional sites. Websites like Linkedin.com and Google+ can reveal great deal of business information such as professional connections and clients list.

Facebook website might have some fake profiles and unofficial groups of a company. But professional social networking website like Linkedin.com usually have trusted and frequently updated information about individual/company or clients.

## Internet History – Archive Pages

Hacker will get the information through passive reconnaissance that includes looking for information that was deleted from the website. ***Archive.org*** is a website established in 1996 which manages to achieve webpages of almost all websites.

Information or pages deleted from a website might have information about ex-employees. These ex-employees can be called and can disclose some information about the company, their environment and work strategy.

## DNS Footprinting – MX Entry

DNS (Domain Name System) records look can reveal information about MX entry which indicates where and which email application services are being used. This information can be used later to exploit mail services and email accounts.

DNS Lookup Websites

- www.dnswatch.info
- www.who.is/dns
- www.dnsstuff.com

## Traceroute

Tracert is a command that can used in both linux and windows which is used to trace path between a user and target system's machine. Some websites also facilitate tracert and trace-routing.

**Weakness which could be exploited in the company through footprint:**

Hacker can target on Admiral Group by number of ways. As Admiral Group is heavily relied on all sort of technology which makes company more vulnerable as well as easy target for the hacker to get valuable information.

I have attached above few screenshots which I gathered during the research purpose base on Admiral Group and I found quite easily company IT related information.

Every company has a unique footprint and Admiral Group is not such different in any case. When employees interact online, there is also a unique, digital footprint of information left behind. This individualized identity is online. Even when an employee leaves, their digital footprints (i.e., identity) never disappear completely.

As Admiral Group is an International recognized company they are dealing with everyday lots dealing with online such as chat, email, video conference etc.

Hacker are increasingly targeting different weakness on employees. They are sending official-looking e-mails to target organisations, and vendors to try to trick employees into giving up passwords or other credentials. Armed with employee passwords, criminals can access mines of sensitive information and use it to steal identities and commit fraud.

Hacker can easily target with phishing email and which is one of the main cause for big data thefts in recent years. including the 2013 breach at the big-box retailer Target Corp., which affected nearly 1 million consumers in Massachusetts alone. One of the biggest bank heists in the world — the theft of $1 billion from dozens of banks around the world, starting in 2013 — began with phishing e-mails, according to Kaspersky Lab, a Russian computer security company with offices in Woburn that reported on the bank breach earlier this year.

**Solutions to resolving company weaknesses:**

- Protecting company employees Digital Footprints
- One way to reduce such risk is by using a trusted malware scanner. Most malware (including keyloggers) will be detectable by any up-to-date security software.
- using two-step verification.
- Using a solid password manager. Password manager tools will automatically input your passwords for you so there are typically no keystrokes available for a keylogger to record.

**Hacker will achieve its goal through social networking and other uses of the internet. Level of threats are facing company:**

Social media is "the internet and mobile technology-based channels of communication in which people share content with each other example is Facebook, Twitter. Social media can have tremendous benefits but also can have serious security risks for organizations. Two of the greatest risks to organizations are malware and inadvertent disclosure of sensitive information (Waxer, 2011).

Seventy-two percent of companies believe employees' use of social media poses a threat to their organizations (Schroeder, 2010).

Others point to the threats of social media such as malware, illegal activities, and damage to company reputation. Additionally, there are risks to corporate data security (Fraser and Dutta, 2009). These concerns have led many companies to ban social media sites outright. Credit Suisse, Dresdner Kleinwort, British Gas, and Lloyds TSB use security systems to block access to social media sites. Citigroup, Goldman Sachs, JPMorgan and UBS restrict access to Facebook.

**Types of threats:**

The report described the types of threats that social media technologies could pose in a business environment. Some threats identified in the report were

- **Insufficient Authentication Controls**

In many social media applications, sensitive information is spread among many various locations. This makes it more likely that an inexperienced user will introduce a weakness that will adversely affect the entire system.

- **Cross Site Scripting (XSS)**

Cross site scripting is a type of attack in which the victim's web browser is induced to execute malicious code. Depending on the type of attack, the malicious code may steal the victim's personal information as well company valuable data which consider is company assets.

- **Phishing**

Many people view social media sites on cell phones or other mobile devices. This makes it harder to distinguish real and fake web sites.

- **Information Integrity**

Data integrity is one of the foundations of information security. Malware introduced on a platform or network can modify user information and databases. Users who do not diligently update their antivirus software can make their systems vulnerable.

# Task 3:

**Social Engineering:**

Social engineering is the art of manipulating people behaviour as well as their mindset, so they give confidential information to others.

**Social Engineering Attack an Example: Email from a friend**

If a criminal manages to hack or socially engineer one person's email password they have access to that person's contact list–and because most people use one password everywhere, they probably have access to that person's social networking contacts as well.

Once the criminal has that email account under their control, they send emails to all the person's contacts or leave messages on all their friend's social pages, and possibly on the pages of the person's friend's friends.

- **Contain a link** that you just have to check out–and because the link comes from a friend and you're curious, you'll trust the link and click–and be infected with malware so the criminal can take over your machine and collect your contacts info and deceive them just like you were deceived
- **Contain a download** of pictures, music, movie, document, etc., that has malicious software embedded. If you download–which you are likely to do since you think it is from your friend–you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know. And on, and on.

People who take the bait may be infected with malicious software that can generate any number of new exploits against themselves and their contacts.

**How to protect:**

While phishing attacks are rampant, short-lived, and need only a few users to take the bait for a successful campaign, there are methods for protecting yourself. Most don't require much more than simply paying attention to the details in front of you. Keep the following in mind to avoid being phished yourself.

**Tips to Remember:**

- Slow down. Hackers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- Research the facts**.** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research.
- Beware of any download. If you don't know the sender personally and expect a file from them, do not download it will be a mistake.
- Foreign offers are fake. If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

**Ways to Protect Yourself:**

- Delete any request for financial information or passwords.
- Reject requests for help or offers of help.
- Set your spam filters to high
- Secure your computing devices. Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn’t automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks.

**What is physical security:**

Physical security is very important, but it is usually overlooked by most organizations. It is necessary if you do not want anyone to snatch away your information or destroy it, in case of natural calamity. The reason could be anything, the attacker doing it for personal gain, financial gain, for seeking revenge or you were the vulnerable target available. If this security is not maintained properly, all the safety measures will be useless once the attacker gets through by gaining physical access. Though physical security is proving to be challenging than previous decades as there are more sensitive devices available (like USB drives, laptops, smartphones, tablets, etc.) that enables the stealing of data easy and smooth.

As mentioned before there are fewer measures used for physical security and no one pays heed to it as attention is mostly on technology-oriented security. This slip-up gives the attacker a chance to exploit data or open ports. They scheme plans of penetrating the network through unauthorized means. Though there are internal threats too, for example, employees that have access to all the areas of the company can steal the assets with ease.

**List of things that help to maintain a good and strong physical security.**

- Intrusion detector
- CCTV, smart cards
- Fire extinguisher
- Guards
- Suppression systems
- Intrusion alarm
- Motion detectors
- Physical access
- Chain link fence
- RFID tags
- Barbed wire and much more.

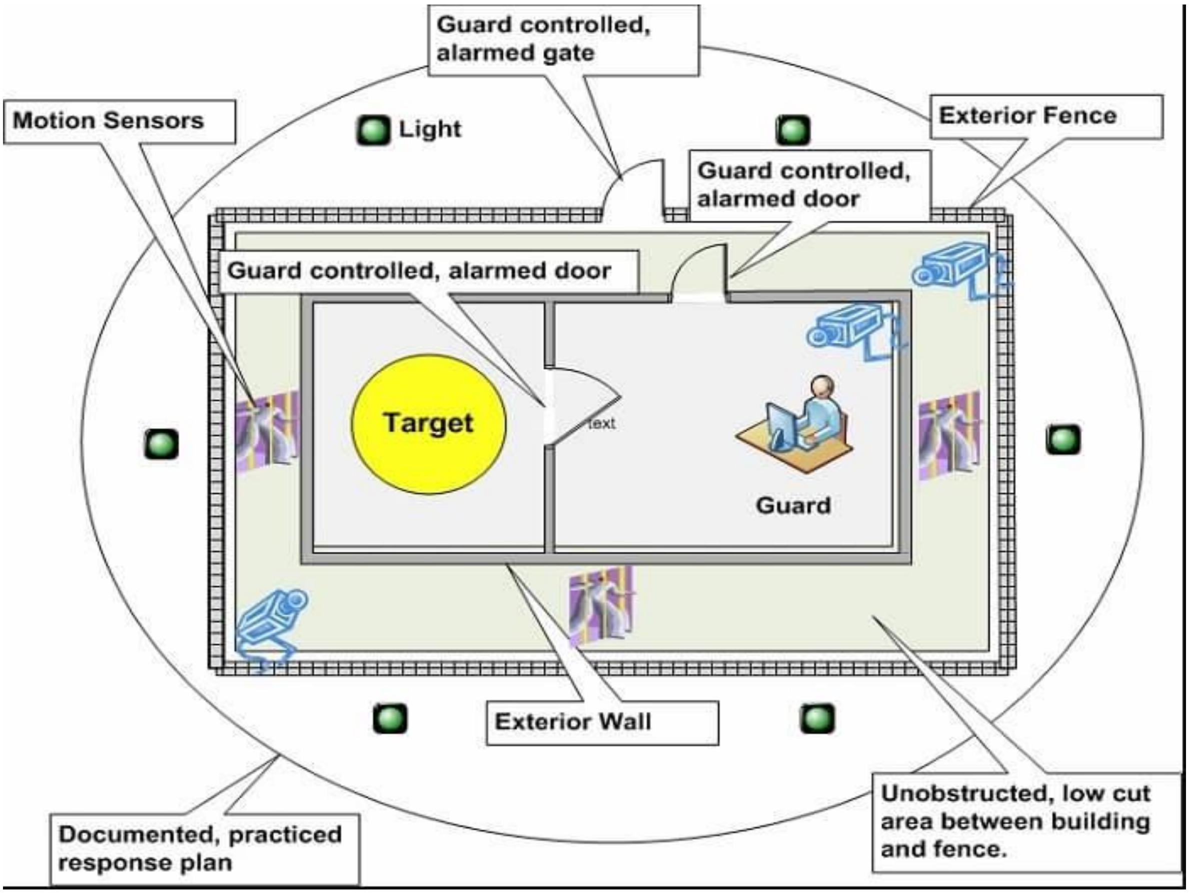
**Why physical security is important in organizations:**

Business continuity is of extreme importance for organizations to survive in today’s competitive market and a potential loss event can affect it negatively. These events need to be addressed and mitigated. Security of sensitive information is also a crucial aspect for organizations as it any leakage of information can impact the business, for example: a new product design or next product launching plans.

We'll take a look at some of the most essential security measures we should implement now, if you haven't already done so.

Company can take number of steps to protect physical access to the company assets and company should use both technology and security personnel to achieve its goals.

Company need to protect its assets from intruders, internal threats, cyber attacks, accidents and natural disasters, which in turn requires a mix of technology and in-person monitoring that requires placement of security staff.


Guard controlled, alarmed gate
Motion Sensors
Light
Exterior Fence
Guard controlled, alarmed door
Guard controlled, alarmed door
Target
text
Guard
Exterior Wall
Documented, practiced response plan
Unobstructed, low cut area between building and fence.

*An example of physical security detecting target in real time. Source: TechRepublic*

**Good Practices for Successful Physical Security:**

- First line of defence is fenced walls or razor wires.
- Protective barriers for stop forced entry of persons or vehicles.
- Locks method to enable only individuals with a key or access control card to open or lock a door or gate. Locks may be connected to a more comprehensive security monitoring system.
- Surveillance cameras and sensors that track movements and changes in environment. lighting to ensure all monitored areas are visible at any given moment.
- Security guards should cover all entry points as well as indoor.
- Only authorized personnel get into a restricted area.

**Good practices to protect digital security:**

**1. Frequent engage and train employees.**

Employee will be weak link in a company security if they are not trained about security issues. And overall IT system security is only as strong as its weakest link! Every user must know which data is considered sensitive and be familiar with the company's security policy and related guidelines.

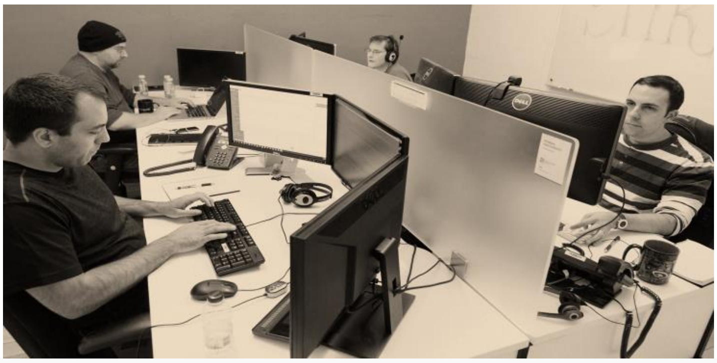
**2. All time secure work stations.**

Companies should be established strong policy on which software can and can't be installed on work stations. Furthermore, work stations must always be up-to-date and equipped with at least antivirus and antispam software, and a local firewall that is correctly set up.

**3. Priorities sensitive data.**

Company must manage their sensitive information, i.e. any data whose loss or theft could be damaging or even disastrous. Companies must know at all times where the data resides and on which physical equipment it is located, in order to define specific security measures.

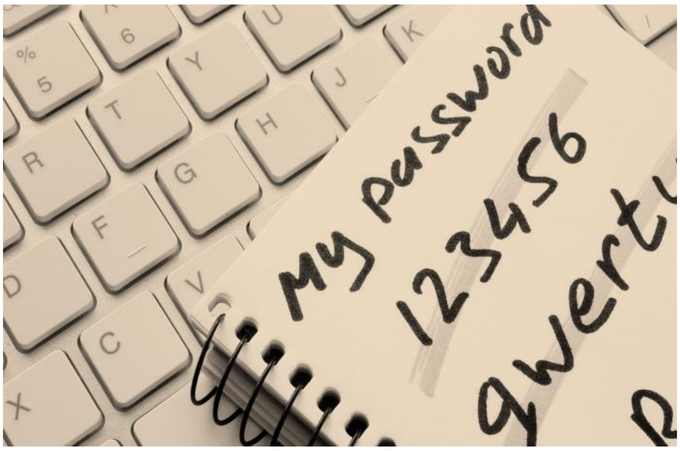
### 4. Make sure proper management of user accounts.



Company always need to ensure flawless management of user accounts, removing them as soon as employees leave the company and regularly reviewing accounts in order to ensure the appropriate level of rights

### 5. Provide proper guidelines for password creation.

Employees must receive detailed guidelines on how to create good passwords. The guidelines must strictly forbid the writing down of passwords on any physical media (notepads, whiteboards, etc.) or non-encrypted digital media (“passwords.txt”, email, etc.).



### 6. Place proper authentication procedures.

For stronger security accounts, use a two-step verification process. This involves authenticating a user with a password, plus another identifier such as a physical item in the user’s possession (a FIDO U2F USB key, an OpenPGP card, an RFID chip, a token, a single-use code sent via SMS, etc.), biometric data (fingerprints, voice recognition, iris scanning, etc.), or even a geographic location (the connecting device must be within a certain physical location).

## 7. Limit the devices authorized to connect to the company network.

Devices belonging to visitors or to employees are a vulnerability over which the company has no control. To facilities these needs, company better off creating a specific Wi-Fi network entirely separate from the rest of the company infrastructure. At the same time, company should control the use of external USB keys on company systems.

## 8. Encrypt all sorts of data transmitting over the Internet.

Any non-encrypted data circulating on the Internet is vulnerable: such as emails. All these communications must go through secure protocols (HTTPS, IMAPS, SMTPS, POP3S, SFTP, etc.) Remember that email always travels on networks in an unencrypted manner. Assume that any information sent by email can be intercepted and read by anyone, unless the contents are encrypted using OpenPGP, PGP, GPG or another encryption method.

## 9. Partition the network.

Company should isolate machines that offer services visible on the Internet (for example, Web hosting) from the rest of your company network

## Conclusion:

Physical security is usually overlooked when it comes to security. Most companies tend to take care of technical and administrative aspects of security. All the firewalls, intrusion detector system, cryptography, and other security measures would be useless if someone were able to break in and steal the assets or important data.

Physical Security is a continuous effort and at no point of time it can be considered as perfect. There may always be chances of unseen and unpredictable events, even those which have never occurred in the history. A balance approach is required to ascertain that physical security can play its part when needed.

Bottom line is, there is no one perfect way to reduce your cybersecurity risk; organizations need a multi-pronged approach.

**Reference:**

[1] FootPrinting-First Step Of Ethical Hacking https://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

[2] Securing Your Company's Digital Footprint - https://www.ivanti.com/blog/securing-companys-digital-footprint

[3] Reducing the Risks of Social Media to Your Organization https://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749

[4] What is Social Engineering? Example & Prevention Tips https://www.webroot.com/ie/en/resources/tips-articles/what-is-social-engineering

[5] The Best Practice in Physical Security https://www.getkisi.com/blog/physical-security-examples

[6] The Importance of Physical Security in the Workplace https://resources.infosecinstitute.com/importance-physical-security-workplace/#gref

[7] Tips to improve your facility's physical security https://www.isgtech.com/tips-to-improve-your-facilitys-physical-security/

[8] For hackers, people are an IT system's weak link https://www.bostonglobe.com/business/2015/05/13/hackers-target-system-vulnerabilty-people/itLk7GJ9gKsl85puKxFNbO/story.html

[9] website: https://who.is/tools/

[10] Assest Structures for Insurers http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1242281415644/Asset_Structures_for_Insurers.pdf

[11] Admiral Group https://en.wikipedia.org/wiki/Admiral_Group

[12] Top 10 Malware 2018 https://www.cisecurity.org/blog/top-10-malware-january-2018/

[13] The Latest Malware Threat that affected user worldwide https://www.colocationamerica.com/blog/latest-malware-threats

[14] SamSam: The Doctor Will See You, After He Pays The Ransom https://blog.talosintelligence.com/2016/03/samsam-ransomware.html

[15] Kovter: An Evolving Malware Gone Fileless https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kovter-an-evolving-malware-gone-fileless

[16] WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack? https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/

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

[18] Understanding malware & other threats https://docs.microsoft.com/en-gb/windows/security/threat-protection/intelligence/understanding-malware

[19] Anti Cybercrime group https://pnpacg.ph/main/2-uncategorised/259-acg-cyber-security-bulletin-no-128-understanding-the-risk-of-kovter-trojan

[20] What you need to know about the WannaCry Ransomware https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

[21] How to completely remove SIrefef Trojan (Virus Removal Guide) https://malwaretips.com/blogs/remove-sirefef-trojan/

[22] Emotet virus removal guide https://www.pcrisk.com/removal-guides/12862-emotet-virus

[23] Supicious.Emit http://virus.wikia.com/wiki/Suspicious.Emit

[24] McAfee Labs Threats Reports https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html

[25] Malware Scanning https://www.websecurity.symantec.com/security-topics/malware-scanning

[26] Cyber Security Risks Facing insurance companies https://businessworld-usa.com/cyber-security-risks-facing-insurance-companies-2017/

[27] Cerber ransomware https://www.avast.com/c-cerber

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