Learning from major cyber security incidents

About this free course

This free course is an adapted extract from the Open University course TM255 *Communication and information technologies* http://www.open.ac.uk/courses/modules/tm255..

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University –

https://www.open.edu/openlearn/science-maths-technology/learning-major-cyber-security-incidents/content-section-0

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Intellectual property

Contents

Introduction

Many computing devices can be connected to the internet almost anywhere and at any time. As a result protecting against attacks and preventing the leak of private and confidential information has become ever more important.

On top of this, the reasons behind attacks are becoming more diverse – ranging from financial gains and retaliations through to influencing political campaigns and disabling infrastructure. Anyone can be a victim of cyber-attacks.

In this course, you'll look at cyber security from the perspective of a computer user. Through a set of case studies you'll analyse various types of attack, look at what lessons can be learnt from major incidents and consider what security measures you should apply to protect yourself. To help you to follow the case studies, the same framework has been adopted to analyse and explain each attack. Each case study will answer the questions:

1. What was the attack?
2. How did it work?
3. Who were the attackers?
4. What lessons can be learnt?

This OpenLearn course is an adapted extract from the Open University course TM255 *Communication and information technologies*.

Learning Outcomes

After studying this course you should be able to:

- demonstrate an understanding of the key concepts, issues and technologies associated with cyber-attacks
- analyse cyber security incidents
- describe and discuss some of the technological, social, legal, ethical and personal issues that relate to cyber security incidents.

1 Cyber security basics

This course does not cover the basics of cyber security and online safety as these are covered in the badged OpenLearn course *Introduction to cyber security: stay safe online* (open the link in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on it).

If you haven't taken the abovementioned course or your memory needs to be refreshed, you are encouraged to visit the Glossary at the end of this course or the relevant section in the *Introduction to cyber security: stay safe online* course when you meet an unfamiliar term or concept related to cyber security.

Activities 1 to 4 should help you to assess your knowledge and to familiarise yourself with the basics of cyber security.

Activity 1

Allow about 10 minutes

In the context of computer security, briefly explain the meaning of the following terms:

- **vulnerability**
- **threat**
- **countermeasure**.

Answer

A *vulnerability* is a point at which there is potential for a security breach.

A *threat* is some danger that can exploit a vulnerability.

A *countermeasure* is an action you take to protect your information against threats and vulnerabilities.

Activity 2

Allow about 20 minutes

In the context of malware, briefly explain the meaning of the following terms:

- **virus**
- **worm**
- **Trojan**
- **ransomware**
- **spyware**
- **botnets**.

Answer

A *virus* inserts a copy of itself into applications or crucial parts of the operating system in order to infect other computing devices or storage media that interact with the infected computer.

A *worm* exploits the vulnerability of computing devices in a network and replicates itself by finding and infecting other vulnerable computing devices.

A *Trojan* is malware disguised as something useful and can be self-replicating.

Ransomware is malware that demands payment in order to refrain from doing some harmful action or to undo the effects of the harmful action.

Spyware records the activities of the user, such as the passwords they type into the computer, and transmits this information to the person who wrote the malware.

Botnets are created using malware that allows an attacker to control a group of computers and use them to gather personal information or launch attacks against others, such as for sending spam emails or flooding a website with so many requests for content that the server cannot cope (called a denial-of-service attack).

Activity 3

Allow about 20 minutes

a. In the context of encryption, briefly explain the meaning of the following terms:

- **plaintext**
- **ciphertext**
- **cipher**
- **encryption**
- **decryption**.

Answer

Plaintext is information that can be directly read by humans or a machine (this document is an example of plaintext). ‘Plaintext’ is a historic term predating computers, when encryption was only used for hardcopy text; nowadays it is associated with many formats including music, movies and computer programs.

Ciphertext is the encrypted data.

A *cipher* is the mathematics (or algorithm) responsible for turning plaintext into ciphertext and reverting ciphertext to plaintext (you might also see the word ‘code’ used – there is a technical difference between the two but it need not concern you now).

Encryption is the process of converting plaintext to ciphertext (occasionally you may see it called ‘encipherment’).

Decryption is the process of reverting ciphertext to plaintext (occasionally known as ‘decipherment’).

b. What is **asymmetric cryptography** and how does it differ from **symmetric cryptography**?

Answer

Asymmetric cryptography, also known as public key cryptography, sidesteps the key distribution problem because each user creates their own keys:

- the *private key*, which they keep safe and never distribute
- the *public key*, which can be sent to anyone with whom they want to exchange encrypted information.

Unlike with symmetric encryption, the two keys behave differently: the public key is the only key that can decrypt ciphertext encrypted using the corresponding private key, and the private key is the only key capable of decrypting files encrypted with the corresponding public key. Crucially, the value of one key cannot easily be determined from the other, so even if the public key falls into hostile hands, the value of the private key cannot be determined.

Activity 4

Allow about 20 minutes

In the context of network security:

- What is a **firewall** and how can it protect a network?
- What is an **intrusion detection system** and how does it work?

Answer

In a building, a *firewall* is a reinforced masonry wall that is designed to prevent a fire from spreading through the structure, allowing people time to escape. Similarly, in a computer network, a firewall is a barrier that blocks dangerous communications from spreading across a network, either from the outside world into a local network, or from one part of a local network to another.

An *intrusion detection system* (IDS) may be a dedicated device or software. It is typically classified as one of two types, depending on its responsibilities:

- a *network intrusion detection system* (NIDS), which is responsible for monitoring data passing over a network
- a *host intrusion detection system* (HIDS), which is responsible for monitoring data to and from a computer.

An IDS can support a network firewall. Ideally the firewall should be closed to all traffic apart from that which is known to be needed by the organisation (such as web traffic, email and FTP). An IDS can then be used to scan any traffic passing through the firewall for potential attacks using an NIDS, as well as being able to detect those coming from within – such as from a personal computer infected with malware – using an HIDS.

Intrusion detection may be considered passive; it identifies that an intrusion is taking place and informs an administrator, who must take appropriate action. However, it can also be reactive – as well as informing the administrator, the IDS can actively attempt to stop the intrusion, in most cases by blocking any further data packets sent by the source IP address. Such a system is also referred to as an intrusion prevention or protection system (IPS).

Now you have familiarised yourself with some of the key terms related to cyber security, you will next look at the first case study used in this course.

2 Case study 1: WannaCry

On 12 May 2017, a piece of malware spread rapidly and infected many computers across the globe. Many data files in infected computers were not openable. What was happening?

The next sections will answer the following questions:

1. What was the attack?
2. How did it work?
3. Who were the attackers?
4. What lessons can be learnt?

2.1 What was the attack?

Within a day, over 200 000 computers in 150 countries had been infected by **WannaCry**. Universities, government departments, hospitals, manufacturers, telecommunications companies and many other organisations were affected, including large, well-known companies and organisations such as FedEx, Hitachi, Honda, the National Health Service (England and Scotland), Nissan Motoring Manufacturing UK, O2 Germany, Renault and Telefonica. The malware was of a type known as ransomware, which locks the data files of an infected computer using encryption and demands a ransom payment for unlocking them.

In the UK, the worst-affected organisation was the National Health Service (NHS): around 50 health trusts in England and 13 in Scotland, including hospitals, GP surgeries and pharmacies, were affected (Evenstad, 2017). Problems with emails, clinical IT systems and patient IT systems caused a major disruption. This led to several problems including delays at hospitals, medical equipment malfunctioning, ambulances being diverted to neighbouring hospitals, and cancellation or postponement of non-urgent activities. It was believed that up to 70 000 devices, including computers and medical equipment, were affected (Ungoed-Thomas *et al.*, 2017).

Luckily, the spread of the malware was significantly slowed down by a security researcher, Marcus Hutchins, who accidentally discovered and activated the ‘kill switch’ of the malware the next day, on 13 May 2017. When inspecting the malware’s code, Hutchins noticed an unusually long internet domain name in the code. He checked and found out that the domain name was not registered, so he registered it. Unknown to him at the time, this effectively deactivated the malware from further spreading. Security experts later analysed the code of the malware and confirmed that the malware used the domain name as a kill switch, which can be used by its owner to stop the malware from spreading when things go wrong or out of control. However, the experts warned that variants of the malware that did not have a kill switch could exist or be further developed by attackers.

Although this large-scale attack seemed to come and go quickly, it provided a stark warning of how vulnerable society is to cyber-attacks and how unprepared it is to deal with them. It was just pure luck that the saga ended so soon. The incident also raised a number of questions about data security. For example, how did the malware spread so rapidly? How did it work? Why did a large organisation such as the NHS fail to protect itself?

2.2 How did it work?

WannaCry belongs to a class of malware known as ‘worms’. As you saw in Activity 2, these are stand-alone, self-replicating programs that spread through network connections, accessing uninfected machines and then hijacking their resources to transmit yet more copies across the network.

Similar to a typical malware worm, WannaCry contains an infection module and a ‘payload’. The infection module is responsible for spreading the malware, while the payload module undertakes the actual attack. The payload module of WannaCry locks data files using encryption and handles the process for demanding a ransom. Once the malware is executed, both modules work at the same time.

However, compared to other worms, WannaCry spread much more quickly. How did it achieve this rapid spreading? The security experts who analysed the malware believed it employed a powerful hacking tool known as **EternalBlue**. This exploited a vulnerability in Microsoft Windows operating systems, allowing the malware to install and execute itself on a vulnerable computer without any action from the computer user.

The vulnerability exploited by EternalBlue existed in almost all versions of Windows operating systems including Windows XP, Windows Vista, Windows 7, Windows 8 and Windows 10, as well as some server and embedded versions. EternalBlue is believed to have been developed by the US National Security Agency (NSA) and then stolen by a hacking group known as the Shadow Brokers, who had been trying to sell it on the black market for a number of months before the WannaCry attack (Woollaston, 2017).

EternalBlue exploited a defect in Microsoft’s implementation of the **Server Message Block** (SMB) protocol, which allows applications on a computer to access files and services on other computers. This remote access to files and services usually happens within the same local area network (LAN), but it is possible for a computer outside the LAN to access files and services too if firewall settings allow it to do so (e.g. through the internet). However, allowing computers outside your LAN access will significantly increase the risk of attacks.

Once the WannaCry malware infects a computer, it will scan all computers within the same local network and some computers on the internet for the EternalBlue vulnerability. When vulnerable computers are found, it installs itself on these computers and executes the malware. Therefore each infected computer becomes an attacker and will keep looking for new victims. This is how the malware can spread so quickly. Figure 1 illustrates how WannaCry infects a computer.

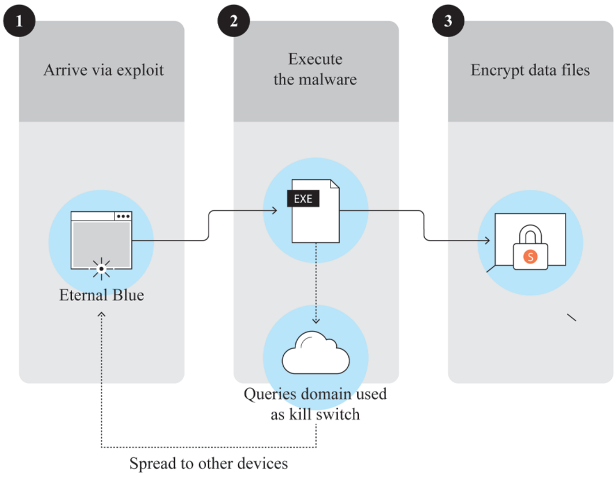
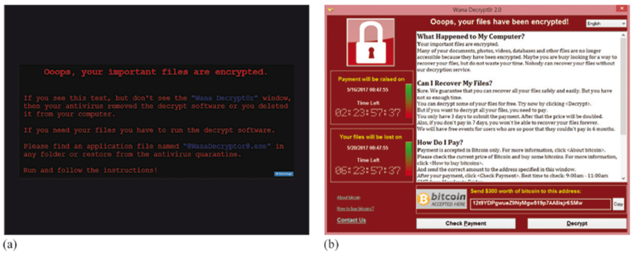


Figure 1 WannaCry’s infection process

Once installed, the payload module will look for a range of data files, including documents and images, on the infected computer and encrypt them using a complex combination of symmetric and asymmetric methods to ensure the files cannot be unencrypted easily. It then executes the ‘Wana Decrypt0r 2.0’ and displays a black Windows desktop background image with instructions in red text. Figure 2(a) shows the desktop background image, while Figure 2(b) shows the interface of the ‘Wana Decrypt0r 2.0’. This tells the victims that their data files have been encrypted and that they have to pay a ransom of $300 to a given address if they want to recover all their files. The ransom is to be paid in **bitcoin**, which is a digital currency but can be bought with real money at bitcoin exchanges. The interface also has three-day and seven-day countdown timers – these are used to create a sense of urgency, as the note in the interface states that the ransom will be doubled after three days and the data files will be deleted after seven days. To convince the victims that the ‘Wana Decrypt0r 2.0’ can recover their files, it offers a free demonstration of a few files being decrypted.


(a)

Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

(b)

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

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

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 2 (a) The desktop background image showing the instruction to open ‘Wana Decrypt0r’; (b) the interface of Wana Decrypt0r 2.0

When the attack broke out, security experts generally advised users not to pay the ransom, as it was not guaranteed that the files would be recovered after payment (Baraniuk, 2017). It might also encourage more attacks if attackers saw this as an easy way to make money.

2.3 Who were the attackers?

At the time of writing, nobody has claimed responsibility, nor has anyone been arrested for spreading the malware. One suspect is the Shadow Brokers group, as they were alleged to have stolen the hacking tool from the NSA. Moty Cristal, a professional negotiator, believed that the attackers did it not for money but to make a point, which was to show the group’s strength and remind large organisations to revise their cyber security strategies. He said:

> The failure of the perpetrators to auction it for big money, the leveraging of a long-known vulnerability, the low ransom demand in global parallel attacks (which decreases chances of being paid) and the fact that Russia has been dramatically hit, are all signs that the perpetrators could be American hackers frustrated by their failure to make big money. The attack has the signs of being the work of a group that preferred expressive impact over a modest amount of money.
>
> […] It was a global show of strength, an expressive one, that caused relatively low financial and operational damage, and ought to be used by UK government as a powerful reminder to revise its cyber security strategies.
>
> (Cristal, 2017)

However, according to a *Washington Post* article written by Ellen Nakashima in June 2017, the NSA believed that the hacking group Lazarus, linked to the North Korean government, was behind the WannaCry attack. The report stated that the Obama administration previously believed the Lazarus group was behind a series of cyber-robberies of banks in Asia as well as the 2014 hack of Sony Pictures Entertainment, which demanded that the company withdraw a film that ridiculed the North Korean leader, Kim Jong Un. Sanctions were imposed on North Korea by the US government after these attacks. The report further stated that the security researchers who analysed the code of WannaCry found similarities to the malware used by the Lazarus group, and that there was military intelligence indicating that North Korea was behind the attack.

In December 2017, the US government publicly announced that North Korea was the main culprit behind the WannaCry attack. This view was shared by the UK, Canada, New Zealand and Japan too, according to *CBS News* (2017). Nevertheless, North Korea always denied the allegation.

Without firm evidence and a proper court trial, it is hard to pinpoint who the culprit behind the WannaCry attack was. However, the Lazarus and Shadow Brokers groups appear to be the prime suspects.

2.4 What lessons can be learnt?

As the NHS was the organisation most affected by the WannaCry attack in the UK, the discussion here is focused on the experience of the NHS. Some of the lessons learnt might apply to other organisations too.

You might have expected a large and important organisation such as the NHS to have enough resources and support to protect itself against cyber-attacks. Furthermore, Microsoft announced the EternalBlue vulnerability and released a patch on 14 March 2017, which was almost two months before the attack. This should have given organisations enough time to patch the security hole and protect themselves against the WannaCry attack.

So why was the NHS still so badly affected by the WannaCry attack? What went wrong and what lessons can be learnt from this incident? According to Dan Taylor, Head of

Security, NHS Digital, the following were the main reasons that the NHS was so affected (Evenstad, 2017).

- The NHS had a complicated organisational structure that allocated the responsibilities of policy making, service commissioning and data and information organisation to three different bodies, namely the Department of Health, NHS England and NHS Digital respectively. Although NHS Digital acted as the central data and information organisation, each NHS trust or GP surgery looked after its own data security. NHS Digital did not have direct control over the maintenance of computing assets in local hospitals and GP surgeries.
- The NHS's main order of business is health and care. Technology and data security are not its main concerns, despite the fact that it has an obligation to protect the data it holds. With the NHS under severe financial constraints, keeping computing equipment up-to-date was not its priority. Although the patch for the EternalBlue vulnerability had been available for two months, most NHS trusts had not applied it to their computing equipment.
- To make matters worse, the NHS trusts had many different systems, including some old legacy systems. Applying patches to all these systems – especially the legacy systems – without affecting the critical clinical systems was not simple. Improperly applying a patch to a clinical system could render it unusable. These systems are critical for the NHS to operate its business. If the choice was between clinical risk and security risk, many NHS trusts would bear the security risk.
- Finally, communication was a problem too. The language and terminology used by NHS Digital were not always understandable by the health professionals. The responses to queries were not very timely either.

Since the WannaCry attack, the NHS has identified areas for improvement, which include the need for clearer communications and accountability for cyber security in every NHS organisation at senior leadership and board level. Local organisations must ensure effective management of their technology infrastructure, systems and services (Smart, 2018).

Although these points are explicitly about the NHS's failure to prepare itself for the WannaCry attack, similar reasons may also lie behind the failures of many other large organisations who fail to protect themselves.

Before moving on to the next case study, complete the three activities on WannaCry below.

Activity 5

Allow about 15 minutes

Based on how WannaCry spreads, why is it described as a worm rather than a virus or Trojan? Explain your answer.

Answer

WannaCry is classified as a worm because it exploits the vulnerability of computing devices in a network and replicates itself by finding and infecting other vulnerable computing devices.

It is not a virus because it doesn't insert a copy of itself into applications or crucial parts of the operating system in order to infect other computing devices or storage media that interact with the infected computer.

It is also not a Trojan because it is not disguised as something useful.

More coverage of malware can be found in the 'Malware' section of the *Introduction to cyber security* course on OpenLearn (open the link in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on it).

Activity 6

Allow about 15 minutes

Judging by how WannaCry works and spreads, explain what two main security measures the NHS trusts could have taken that would have prevented WannaCry from attacking their computing devices.

Answer

If their Windows-based computing devices had been patched with Microsoft's update for the EternalBlue vulnerability in time, it would have prevented their computing devices from being infected.

Furthermore, any computing devices that do not need to use the Server Message Block (SMB) service should have their SMB protocol disabled through a proper firewall setting to prevent unnecessary exposure.

Activity 7

Allow about 20 minutes

The spread of WannaCry was significantly slowed down after its kill switch was found and activated. However, security experts – including Sean Dillon, a senior security analyst at RiskSense – expected that new malware based on WannaCry would surface in the future and that this malware would not have a kill switch (Mimoso, 2017).

Complete a quick web search to find out the latest development. You can use a search term such as 'WannaCry variants' for your search.

Feedback

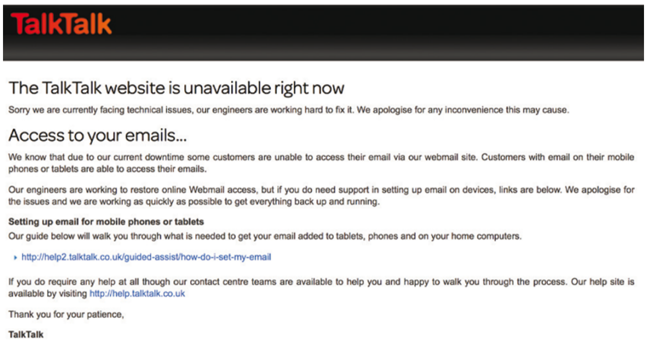
Within a few days of the WannaCry attack, a number of variants were detected. Most of them were created by editing a small part of the original malware's code. For example, one variant used a different domain name as its kill switch, while another removed the kill switch altogether. Some copycat attackers simply replaced the bitcoin addresses in the code with their own, so payments would be directed to them (Mimoso, 2017).

In October 2017, the computer network of Pinehurst-based FirstHealth of the Carolinas in the USA was reported to be infected by a variant of the malware. The organisation took the system offline for a day in attempting to remove the malware (Davis, 2017).

Following the attention given to the malware in May 2017, more computers and devices were subsequently patched. Variants of WannaCry, which also exploit the EternalBlue vulnerability, do not appear to be as infectious as the original malware. However, the situation may have changed by the time you are doing this activity.

3 Case study 2: the TalkTalk hack

At around midday on 21 October 2015, the website of TalkTalk – a large telecommunications company and internet service provider – suddenly became unavailable. A holding page, as shown in Figure 3, stated that TalkTalk was having some technical issues and that engineers were working to fix them.



The TalkTalk website is unavailable right now

Sorry we are currently facing technical issues, our engineers are working hard to fix it. We apologise for any inconvenience this may cause.

Access to your emails...

We know that due to our current downtime some customers are unable to access their email via our webmail site. Customers with email on their mobile phones or tablets are able to access their emails.

Our engineers are working to restore online Webmail access, but if you do need support in setting up email on devices, links are below. We apologise for the issues and we are working as quickly as possible to get everything back up and running.

Setting up email for mobile phones or tablets
Our guide below will walk you through what is needed to get your email added to tablets, phones and on your home computers.

- http://help2.talktalk.co.uk/guided-assist/how-do-i-set-my-email

If you do require any help at all though our contact centre teams are available to help you and happy to walk you through the process. Our help site is available by visiting http://help.talktalk.co.uk

Thank you for your patience,

TalkTalk

Figure 3 A holding page stating that TalkTalk's website is unavailable

So what had really happened?

3.1 What was the attack?

TalkTalk had discovered that their website was being attacked, which forced them to bring down the website to prevent further attacks and to investigate the scope of the damage. It turned out that there were ways to gain unauthorised access to the underlying database that was associated with the website. The database contained personal information such as the names, addresses, phone numbers, email addresses, dates of birth and financial information of TalkTalk's customers. The company initially feared that personal information belonging to all four million of their customers had been stolen, but later found that the scale of data lost was much smaller. TalkTalk issued a statement in November of the same year confirming the following lost data (BBC News, 2015):

- 156 959 customers had personal details accessed.
- From those customers, 15 656 bank account numbers and sort codes were stolen.
- 28 000 stolen credit and debit card numbers were 'obscured' (some digits of the card number were hidden) and 'cannot be used for financial transactions'.

Nevertheless, for these 156 959 customers, it could have been be the start of a nightmare. They were vulnerable to identity crimes and scams. In fact, a number of customers claimed that they received scam phone calls a few days before TalkTalk disclosed the attack (Bain, 2015). For those who were in a long contract with TalkTalk, this was especially frustrating because TalkTalk did not allow customers to terminate the contract early unless they paid an early termination fee or proved they had suffered financial loss as a result of a scam directly related to this data breach. No doubt this policy angered customers and dented their trust in the company further (Millman, 2017).

In TalkTalk's quarterly report release in February 2016, the financial loss resulting from the attack was estimated to be £60 million, which included costs related to responding to the incident, extra loads put on the call centres, and repairing vulnerable systems. In three months, TalkTalk also lost 95 000 customers, who left because of the attack (Burgess, 2016).

In addition, the Information Commissioner's Office (ICO), which is the UK's independent authority for upholding information rights in the public interest, fined TalkTalk £400 000 for 'security failings that allowed a cyber attacker to access customer data with ease' (ICO, 2016). The ICO's investigation concluded that the attack could have been prevented if TalkTalk had taken basic security measures to protect their systems. The fine was the largest the ICO had ever issued at that time.

Activity 8

Allow about 15 minutes

To placate their affected customers, TalkTalk offered them free credit monitoring for a year. Credit monitoring is a process of continuously monitoring one's credit history in order to detect suspicious activity. By following the link below or finding your own resources, identify how a credit report can indicate the key warning signs of identify fraud.

How to spot the warning signs of identity fraud (Experian, 2018)

(Open the link in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on it).

Feedback

The following are some key points identified from the web page:

1. When a credit application is set up, lenders will usually 'search' for your credit rating. By checking the search history on your credit report, you may notice unusual activities.
2. The credit report will show your address. If it has been altered by a fraudster, you should notice this.
3. The credit report also lists any loans and credit card accounts you applied for. If there are any listed that you didn't apply for, it is a sign that you are a victim of identity theft.

3.2 How did it work?

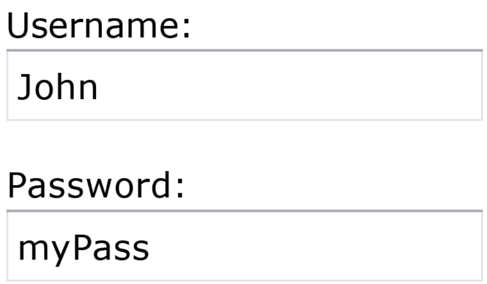
Judging by the large fine and the harsh comment from the ICO, you may have guessed that the TalkTalk attack was a relatively simple one. It was a type of attack known as a **Structured Query Language injection** (SQLi) – which, at the time of writing, has been well known and understood within the security field for over a decade.

The Structured Query Language (SQL) is a programming language that is used for managing **relational databases** and their data. As the contents of most modern commercial websites are database-driven, many web pages are dynamically created based on templates, user inputs, the data in the database and other information. This method enables web pages to be more easily personalised. However, if the designer of the template – which is usually a **script** or program that can access the databases – does not consider SQLi prevention, an attacker can append SQL codes to their input fields in the web page to manipulate data in the database, even if they are not authorised to do so.

To give you an insight into how the SQLi attack works, Box 1 gives a simplified example.

Box 1 How the SQLi attack works

Suppose there is a landing web page that asks you to enter your username and password, as shown in Figure 4.



Username: John

Password: myPass

Figure 4 A landing web page asking for username and password

This web page is controlled by a script, which will create a personalised web page if the user logs in successfully. The script takes the entered username and password from the input fields of the web page and uses them to construct a SQL query statement. For this example, the query statement is to ask the database to return the user's stored information, including the password, so that it can compare it with the entered password. As 'John' and 'myPass' were entered, as shown in Figure 4, the script will create a query statement like the one below:

```
SELECT * FROM Users WHERE Name = "John" AND Password = "myPass"
```

Don't worry if you don't understand what the above SQL query statement means, as this will be explained now. The first part:

```
SELECT * FROM Users
```

asks the database to select all the fields (as the `*` symbol means all the fields) in the data table named `Users`. Table 1 shows the contents of the `Users` data table.

Table 1 An example table from a relational database, showing records of all the users

ID	Name	Address	Email	Phone	Password
1	Faisal	10 ABC Street, Some Town	faisal@abc.com	01234 567890	hisPass
2	John	20 ABC Street, Some Town	john@abc.com	01234 123456	myPass
3	Mei-ling	30 ABC Street, Some Town	meiling@abc.com	01234 098765	herPass
…	…	…	…	…	…
156959	Bert	1 DEF Drive, Another Town	Bert99@abc.com	01567 987654	BertHasAtleastTriedtoUseAsecurePassword^3

The second part:

```
WHERE Name = "John" AND Password = "myPass"
```

is a condition statement, which determines which row(s) in the data table are affected. In this example in Table 1, it is the second row as the contents in the `Name` and `Password` field match with those in the condition statement. In other words, the SQL statement asks the database to return all the data of the user whose name is ‘John’ and password is ‘myPass’.The following row of data will hence be returned:

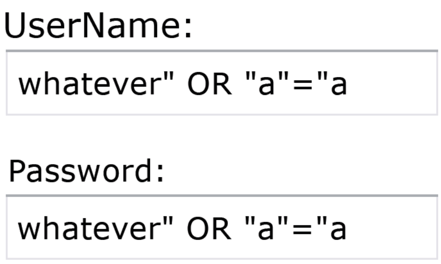
ID	Name	Address	Email	Phone	Password
2	John	20 ABC Street, Some Town	john@abc.com	01234 123456	myPass

Now, if the attacker can find a way to make the database bypass the checking of the username and password, it can potentially obtain all the information in the database. One way to achieve this is to construct the SQL statement as follows:

```
SELECT * FROM Users WHERE TRUE
```

As the condition statement is now always `TRUE` regardless of what the entered username and password are, the database will return everything in the `Users` table.

An attacker cannot change the SQL query statement directly as they have no control of the script. Nevertheless, they may be able to influence what the constructed SQL query statement will be by carefully crafting and appending SQL codes to the ‘Username’ and ‘Password’ fields in the landing web page. Figure 5 shows an example.



UserName:

whatever" OR "a"="a

Password:

whatever" OR "a"="a

Figure 5 Example SQLi code

These inputs look quite odd – for instance, they are missing the beginning and ending quotation marks. However, they are specially crafted such that when the script combines the entered username and password to construct the SQL query statement, it will become:

```
SELECT * FROM Users WHERE Name = "whatever" OR "a"="a" AND Password =
"whatever" OR "a"="a"
```

The condition statement now contains two `OR` clauses and one `AND` clause. The `OR` operator will output `TRUE` if either of the conditions on the left and right sides of the `OR` operator is `TRUE`. As `"a"="a"` (two identical letters) will always be evaluated as `TRUE`, the query statement is in effect equivalent to:

```
SELECT * FROM Users WHERE TRUE AND TRUE
```

The AND operator will output TRUE if both of the conditions on the left and right sides of the AND operator are TRUE. This means the query statement is equivalent to:

```
SELECT * FROM Users WHERE TRUE
```

This query statement will make the database bypass the checking of the username and password and show all the information in the Users data table.

The TalkTalk attackers used a similar SQLi principle to steal TalkTalk's customer information. SQLi can also be used to add or delete data or even to delete the whole database. The web page designer must therefore ensure that any user inputs obtained through fields in a web page are free of SQL codes. There are a number of ways of doing this validation, but they will not be described here as they are out of the scope of this course.

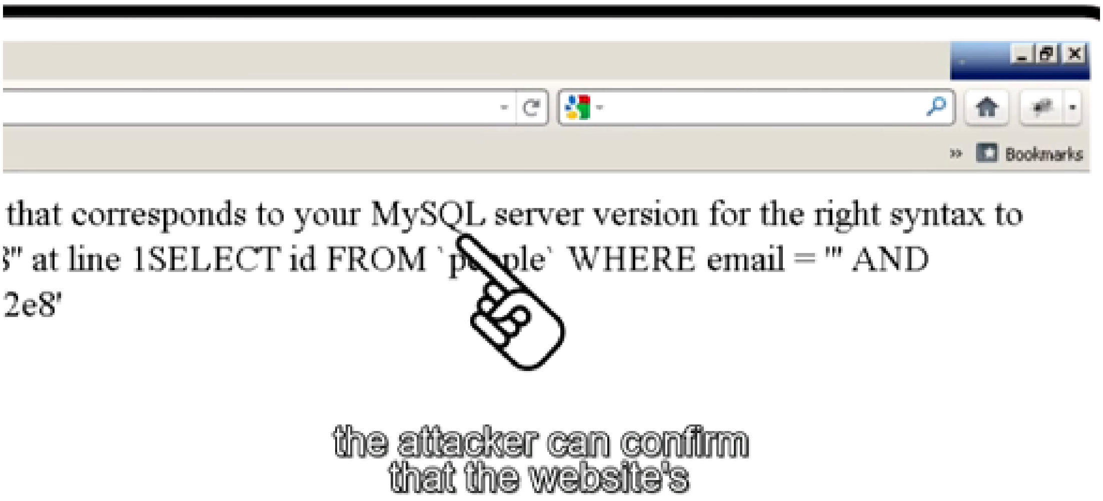
Activity 9

Allow about 5 minutes

To reinforce your understanding of the SQLi attack watch Video 1, which explains the attack using an animation.

Video content is not available in this format.

Video 1 Animated explanation of the SQLi attack



```
that corresponds to your MySQL server version for the right syntax to
$'' at line 1SELECT id FROM `people` WHERE email = ''' AND
2e8'
```

the attacker can confirm that the website's

3.3 Who were the attackers?

Two days after TalkTalk discovered the attack, its then chief executive, Dido Harding, said during a media interview that the company had suffered a 'significant and sustained' cyber-attack and received a ransom demand from someone purporting to be the hacker. The cybercrime unit of the Metropolitan Police had started investigating the attack, but very little information about the attack was available. However, a former detective from the cybercrime unit, Adrian Culley, suspected that the attack was the work of Islamist militants, as a group claiming responsibility for the attack had stated that it was done in the name of Allah. The group also posted sample customer data, claimed to be obtained from the attack, on the website Pastebin, which is often used by hackers for publishing stolen information (Khomami, 2015).

However, three days later, a 15-year-old boy was arrested in Northern Ireland on suspicion of being related to this attack. On 29 October 2015, a 16-year-old boy was arrested in Feltham, west London. Two days later, a 20-year-old man was arrested in Staffordshire. A further two male teenagers were arrested in Wales and Norwich within the next few weeks. They were all arrested on suspicion of offences under the *Computer Misuse Act 1990*. It became apparent that the attack had been undertaken by a group of British youngsters.

According to a report from *Channel 4 News* (White, 2015), a hacker who claimed to have been involved with the TalkTalk attack said the event happened days before TalkTalk discovered the attack. The hacker was in a Skype group call with friends when one member shared a security flaw he had discovered in TalkTalk's website via a Google search. Such a basic flaw discovery technique should not have worked on a big company like TalkTalk, so they were laughing about TalkTalk's unbelievably bad security. The hacker further said that multiple people had used the security flaw to extract data from TalkTalk's customer database: 'it got passed around … at least 25 people had access to it'. He claimed he only did it for fun and to impress his mates. He further claimed that he warned TalkTalk about the security flaw by posting a tweet an hour before the attack that highlighted the flaw and tagged TalkTalk's Twitter account, but TalkTalk were not interested.

However, not all the attackers did it for fun. The then 20-year-old man arrested in Staffordshire in 2015, Matthew Hanley, and his friend Connor Allsopp, aged 18 at the time and arrested in 2017, were trying to sell the data that Hanley had stolen from TalkTalk's website and the website's security flaw for profit. The pair pleaded guilty to charges relating to the TalkTalk attack.

At the time of writing, six people have been arrested in relation to the TalkTalk attack and five of them have been charged:

- Aaron Sterritt (aged 15 at the time of the attack, so his name was not revealed until 2018) was charged under the *Computer Misuse Act* and admitted to unauthorised access to computer material. He was ordered to complete 50 hours of community service, apologise to TalkTalk in writing and complete at least one cyber-crime education session (News Letter 2018).
- A 17 year old, who could not be named because of his age, was arrested in Norwich in November 2015. He was charged under the *Computer Misuse Act* and admitted to seven offences at Norwich Youth Court in November 2016. The prosecution produced evidence that in addition to performing the initial breach of the TalkTalk site, the teenager had shared information about the site's weaknesses on the internet. He was given a 12-month rehabilitation order.
- Daniel Kelley, aged 19 from Wales, was charged with eighteen offences including money laundering and blackmail against the then-CEO of TalkTalk as well as offences under the *Computer Misuse Act*. Kelley pleaded guilty to eleven charges, including that of blackmail.

- Matthew Hanley and Connor Allsopp were jointly charged with eleven offences at a trial at the Old Bailey in London. They were alleged to have attacked not only TalkTalk but also computers belonging to NASA, the National Climatic Data Center, Spotify, Telstra and the RAC. Hanley was charged under the *Computer Misuse Act* with committing fraud against TalkTalk customers. Allsopp was charged with two offences of supplying articles. In April 2017, the two were tried at the Old Bailey in London. Allsopp pleaded guilty to all offences. Hanley admitted to the charge of attacking TalkTalk, but not to the other attacks.

Activity 10

Allow about 10 minutes

You may not have met the *Computer Misuse Act 1990*. Use the link below or another resource to find out and list the computer misuse offences covered by the *Computer Misuse Act 1990*, including the latest amendments.

You should open the link in a new tab or window by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.

Computer Misuse Act 1990 (Great Britain. *Computer Misuse Act 1990*)

Answer

At the time of writing, the Act covers five offences, as listed below. However, new offence(s) or other amendment(s) may have been introduced by the time you attempted this activity.

- 1. Unauthorised access to computer material.
- 2. Unauthorised access with intent to commit or facilitate commission of further offences.
- 3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
- 3ZA. Unauthorised acts causing, or creating risk of, serious damage.
- 3A. Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA.

3.4 What lessons can be learnt?

The attack originated from a group of teenagers showing off their hacking skills and having a laugh, but the consequences of the attack to TalkTalk and its customers were huge. TalkTalk not only suffered a big financial loss but also damaged its brand, and left its customers facing the possibility of identity theft crimes and scams for years to come.

Based on an analysis carried out by Colin Tankard, managing director of a data security company, here is a summary of what went wrong and how the attack could have been prevented (Tankard, 2015):

- The three web pages that were vulnerable to SQLi were inherited from Tiscali when TalkTalk took over its UK business in 2009 (ICO, 2016). According to the ICO's investigation, TalkTalk did not undertake proper security testing or secure the problem web pages before allowing them to access their databases. This obviously was a big mistake.

- According to the ICO’s investigation, there was a security bug in the database management software in use at that time which allowed attackers to bypass access restrictions. The patch for that bug had been available for over three and a half years before the attack. However, TalkTalk did not apply the patch in time. Tankard (2015) believes that this indicates poor patch management practice. Systems must be kept up to date with security patches in a timely manner. Outdated systems that cannot be patched should be isolated from the main network.
- According to Tankard (2015), TalkTalk may not have proactively monitored network activities, such as server logs, to detect unusual behaviour at the time of the attack. According to the report from *Channel 4 News* (White, 2015), the attack happened continuously for days before TalkTalk discovered it. The ICO also reported two previous SQLi attacks in the same year. This should have given TalkTalk enough warning to undertake proper proactive action. Tankard (2015) believes it is possible that TalkTalk’s technical team were aware of the alerts but chose to ignore them. Therefore, management should have had a mechanism to receive these alerts as well.
- Given that TalkTalk had suffered two previous attacks within a year, they still did not appear to have a good strategy to manage such an event and their response to the attack was slow (Tankard, 2015). They didn’t report the incident to the ICO until a full day after they discovered the attack. They also failed to inform their customers straight away so that their customers could be more vigilant to scams. During the first press interview, TalkTalk’s CEO, Dido Harding, did not know whether the data was encrypted and was unable to give any details of the attack. This made customers frustrated. According to Tankard (2015), TalkTalk should have prepared a robust disaster recovery plan. They also had not significantly strengthened their defences after the previous attacks, which was another big mistake.
- Although investment in a proactive threat detection system is costly, the damage of a breach can be much more expensive. It is better to prevent an attack from happening than to have to deal with the consequences of it.
- Finally, the TalkTalk attack demonstrates how vulnerable business networks can be. Businesses must start to check their networks and isolate any parts not strictly necessary for providing services to their customers. In case one area is compromised, the isolated parts are still protected. They should also incorporate in their network some 'honeypots', which are fake servers that lure attackers to them in order to monitor and analyse their activities. This would allow the businesses to determine a strategy to stop the attack and to report the suspicious activities to the police.

4 Case study 3: the Mirai botnet

The **Mirai** botnet can launch highly sophisticated **distributed denial-of-service** (DDoS) attacks, which can overwhelm and cripple almost any website. In this section, you'll look at how the Mirai malware infects Internet of Things (IoT) devices and harnesses their computer power to launch DDoS attacks.

Activity 11

Allow about 15 minutes

a. You may not have met denial-of-service attacks. If not, you should visit Section 3.4 of OpenLearn's *Network security* course and read the explanation about DoS attacks. Then visit How to Survive a Botnet Attack (also on OpenLearn) and watch the animated tutorial about botnets.

You should open the links in new tabs or windows by holding down Ctrl (or Cmd on a Mac) when you click on the link. Return here when you have finished.

Briefly explain what denial-of-service attacks and botnets are.

Answer

Denial-of-service attacks prevent the normal use or management of communication services, and may take the form of either a targeted attack on a particular service or a broad, incapacitating attack. For example, a network may be flooded with messages that cause a degradation of service or possibly a complete collapse if a server shuts down under abnormal loading. Another example is rapid and repeated requests to a web server, which bar legitimate access to others. Denial-of-service attacks are frequently reported for internet-connected services.

(OpenLearn, no date)

The term *botnet* or 'zombie army' is used to refer to a number of computer networks that have become infected as a result of malicious third-party software sneaking onto a user's computer and then linking it to others to send spam to, or steal data from.

(OpenLearn, 2011)

b. Now watch Video 2 which briefly explains what the Mirai botnet is. As you watch note down how the botnet attacks a website.

Video content is not available in this format.

Video 2 The Mirai botnet

Provide your answer...

4.1 What was the attack?

On 21 October 2016, a major network outage occurred that rendered many well-known websites – including Twitter, Netflix, Spotify, Reddit, PayPal and eBay – inaccessible for hours. The outage was caused by an attack on an important protocol underpinning the infrastructure of the internet called the **Domain Name System** (DNS). This translates the alphabetic internet domain and host names, such as the website addresses entered into web browsers, into numeric IP addresses. Without this translation, the website names will not be converted to computer-readable numeric IP addresses and hence the web browser will not be able to connect to the website you want to go to. Only a small number of companies in the world are hosting this crucial 'web directory' and Dyn is one of them. Dyn provides DNS services to around 30 international corporations, including those listed above.

On the day in question, Dyn was targeted by a series of highly sophisticated DDoS attacks. It started at about 12 p.m. BST and the company managed to fix the problem after two hours. However, another attack happened at 4 p.m. and it took the company another three hours to resume the main service.

The magnitude, duration and complexity of this DDoS attack were much higher than those of ordinary DDoS attacks, and this led security experts to suspect that this was a state-sponsored attack. Internationally renowned security expert Bruce Schneier said 'it feels like a large nation state. China and Russia would be my first guesses' (Griffin and Walker, 2016). Another security expert, Lawrence Orans, a research vice president at Gartner specialising in web security and DDoS attacks, agreed and said 'An attack of this magnitude can't be executed by a kid in his bedroom […] It's more sophisticated than that. A nation state would be a prime suspect' (Griffin and Walker, 2016).

Despite the security experts' suggestions that this might be a state-sponsored attack, it wasn't actually the first attack of this kind. Very similar attacks happened in September 2016 and included extraordinary high-traffic attacks to the blog of the security journalist Brian Krebs (620 Gbit/s) and French cloud company OVH (1 Tbit/s). To bring down an ordinary website, a traffic volume of 20–40 Gbit/s is usually enough so the traffic for these two attacks was many times higher than needed. Who was behind these attacks? Would kids really be unable to launch this kind of attack in their bedroom? If not, was a nation state the culprit, as Schneier and Orans suggested?

All these DDoS attacks were launched using an unusually large botnet composed of computing devices from all over the world. Unlike conventional botnets, this botnet was made up of online consumer devices such as IP cameras, network-enabled media players and home routers. As many of these devices had weak security protection and many of their users didn't change the default settings (including factory default usernames and passwords), they could be hacked fairly easily. A piece of malware known as Mirai (which means 'future' in Japanese) is able to exploit the security weakness of these devices and 'harvest' them to form a large and diverse botnet. Mirai randomly scans the internet for vulnerable devices; once one is found, it will attempt to gain access and take control over of it. The device's owner will not usually notice the hijack as the device will still be functioning, though perhaps a little slower than usual.

4.2 How did it work?

Many consumer connected devices (sometimes known as IoT device) are built on an off-the-shelf embedded open source Linux platform, such as the Busybox. These devices are designed to be low cost and plug-and-play (easy to use).

To compete for the market, manufacturers often focus their designs on functionality and ease of use rather than security. To allow the convenience of remote controlling these devices, a standard server is often embedded and turned on by default so that users can control these devices anywhere once they are powered on and connected to the internet. The two commonly used servers are based on **Teletype Network** (Telnet) and **Secure Shell** (SSH), which are network protocols for providing a remote terminal to control a computer system. From this terminal, a user can completely take control of the computer, including the ability to download, install and execute software. SSH is more secure than Telnet as it uses encryption to protect the transmission of the data. However, as many of these IoT devices use default factory usernames and passwords, which can be found by a web search, even SSH's encryption cannot protect against unauthorised access.

The Mirai malware exploits this remote control feature and uses it to take control of the connected devices. The botnet owner starts by installing the Mirai botnet software on a master computer, which will have overall control of the botnet. The software will continuously scan the internet using random IP addresses on ports 22 and 23, which are the default network ports for the SSH and Telnet servers respectively.

Once a victim is identified, Mirai will try and log in to their SSH/Telnet server using a list of known default usernames and passwords for commonly used consumer connected devices. After logging in to the device, the malware will record the device's IP address, remote server type, username and password on its master computer for future reference. It will then download a copy of the Mirai malware and execute it on the victim's computing system, which then becomes a part of the botnet and also scans the internet to find more victims. To ensure it has exclusive control of the device and to prevent other botnet malware from exploiting it, the malware will also close the ports for the SSH and Telnet servers and open secret ports for exclusive remote control of the device.

As these computing devices are usually running on fixed firmware, the malware cannot be installed on the device's operating system. This means the malware will be erased if the device is rebooted. However, the malware keeps a record of its connection information at the master computer, so if a device is rebooted the master computer can attempt to reconnect to it quickly using the recorded connection information.

As mentioned before, a traffic volume of 20–40 Gbit/s is usually sufficient to bring down an ordinary website. In the Dyn attack, the Mirai botnet was thought to have control over 450 000 devices, each of which could generate 1–30 Mbit/s of traffic. This enabled the botnet owner to attack a website with hundreds of gigabits per second of traffic, which is enough to bring down even a well-protected company such as Dyn (Xander, 2016).

Another strength of the Mirai botnet is that it consists of devices randomly distributed all over the world. This randomness makes it very difficult to defend against a DDoS attack: because there is no apparent pattern to the traffic, it is hard to filter out the unauthorised traffic from the legitimate traffic.

Activity 12

Allow about 15 minutes

Based on what you have learnt about the Mirai malware, what are the basic measures you should put in place to secure your connected devices?

Answer

To prevent your connected devices from being used as part of a botnet, you should at least do the following:

- Change the device's default login name and password to something you can remember but would be hard for someone else to guess.
- If you are not intending to remotely access these devices using Telnet and SSH, ensure your firewall blocks all incoming connections to ports 22 and 23.

The following two points were not covered in the study material fully, so you are not expected to have picked them up. However, they are also basic measures to prevent IoT devices from being attacked:

- Check and update the firmware of your connected devices regularly.
- If your internet connection has become slower than usual, disconnect all the connected devices to see if the connection speed improves. If it does, there may be a problem with one of the connected devices.

4.3 Who were the attackers?

At the time of writing, it is still not known for sure who the attackers behind the Dyn attack are. As botnets are available for hire, people without good computer knowledge can also launch attacks, so this attack did not have to be a state-sponsored one. One of the powerful botnets on hire at that time was vDOS; this was investigated and reported in depth by the freelance security journalist Brian Krebs, which subsequently led to it being shut down by the police (Krebs, 2016). It was believed that the extremely high-traffic (620 Gbit/s) DDoS attack on Krebs's blog (*Krebs on Security*) in September 2016 was an act of retaliation against Krebs.

As Krebs' investigation continued, the author of the Mirai malware released the source code to a hackers' forum using the nickname Anna Senpai. It was believed this was an act to distract police investigators rather than the malware authors being 'generous'. Nevertheless, Krebs eventually identified the authors of the malware based on analysis of the data from DDoS mitigation services, studying the discussions in the hackers' forums and interviewing people in January 2017. The real identities of Mirai's authors are 21-year-old Paras Jha from New Jersey and 20-year-old Josiah White from Pennsylvania, USA. The pair were co-founders of Protraf Solutions LLC, which is ironically a company that specialises in mitigating large-scale DDoS attacks! The pair were subsequently charged and pleaded guilty to creating the Mirai malware (though there was no convincing evidence to prove that they carried out the Dyn attack).

Paras Jha was a computer science student at Rutgers University, New Jersey, at that time. He also admitted attacking the university a number of times between 2015 and 2016, causing the university to spend hundreds of thousands of US dollars to improve security. He was also suspected to be responsible for the attack on the French cloud company OVH in September 2016, aiming to disrupt the services of gaming servers hosted by OVH in order to gain advantage for the gaming server he supported.

Apart from using the botnet to attack servers, Jha, White and a third person called Dalton Norman also admitted to conducting a click fraud, which is a form of online advertising fraud that fools the advertiser into believing their hosting advertisement receives a much higher click rate than it actually does. As a result of the click fraud they received about 200 bitcoins, which were worth over $180 000 in January 2017 (Krebs, 2017).

4.4 What lessons can be learnt?

The Mirai malware can form a highly sophisticated botnet by exploiting the security weakness of many ill-designed IoT devices. One lesson which must be learnt is to ensure unsecured computing devices aren't connected to the internet. A connected unsecured computing device will not only harm the security of your own network but can also be used to attack others.

A UK government advisor on internet safety, John Carr, suggested a licensing system for IoT devices, saying he 'would support the establishment of a new licensing regime to ban unsecure appliances from being hooked up to the web' (Loeb, 2017). According to an Institution of Engineering and Technology article, 'the UK government's new National Cyber Security Centre already assesses certain types of devices, such as smart energy meters, to ensure they are safe from hackers' (Loeb, 2017). This indicates that the government had already become aware of the need to prevent unsecured computing devices from connecting to the internet.

Another lesson to learn is to properly protect your own network by, for example, checking that a firewall has been correctly installed and set up, being vigilant of cyber-attacks and keeping software up to date.

5 Attacking infrastructure

In 2010, a malware known as **Stuxnet** was discovered. The malware was specifically designed to target **programmable logic controllers** (PLCs), which are widely used to control industrial motors. It was believed that the malware was designed by the US and Israeli security agencies to sabotage Iran's uranium enrichment plant, in an effort to stop or delay its nuclear programme.

If malware can target and sabotage an industrial plant, it is possible that other malware could disrupt critical infrastructures such as electricity, gas and water supply systems and communication systems. At the time of writing, no malware has yet caused large-scale infrastructure failure. However, there have been signs to suggest that attempts have been made.

In the following activity, you'll do a web search to find out whether there is any malware that can attack critical infrastructures or how close it has come to being capable of doing so.

Activity 13

Allow about 60 minutes

Carry out a web search to look for at least two reports about a theoretical or actual infrastructure attack from the past three years. Summarise the main points of the reports you found.

Feedback

At the time of writing, some small-scale critical infrastructure cyber-attacks have happened. The most well-known one was the attack on the Ukrainian power network that left hundreds of thousands of people in the west of the country without power for hours. Full details of this and other attacks on critical infrastructure can be found using the link below:

- Top 5 critical infrastructure cyber attacks (Ball, 2017)

As for the UK, the two news reports below relate to critical infrastructure cyber-attacks:

- Russia preparing to mount cyber-attack on Britain's "critical infrastructure", GCHQ and FBI warn (Swinford, 2018)
- Major cyber-attack on UK a matter of "when, not if" – security chief (MacAskill, 2018)

Conclusion

In this course, you have looked at the analysis of a number of major cyber security incidents: what the attacks were, how each attack worked, who the attackers were and what lessons could be learnt.

One common factor in all these incidents is human error. Often the attacks could have been prevented if proper security measures were taken.

You've learnt that networked devices that have not been properly secured will affect not only the security of their users but also the security of others, as the hacked devices can be used to mount wider attacks. The availability of hacking tools also enables people with little computing knowledge to launch sophisticated attacks.

The final activity, which asked you to investigate more recent potential or actual attacks on critical infrastructure, should have alerted you to the very real need for continued diligence in cyber security.

This OpenLearn course is an adapted extract from the Open University course TM255 *Communication and information technologies*.

Glossary

Asymmetric cryptography

Also known as public key cryptography. A method that sidesteps the key distribution problem, as each user creates their own keys:
• the private key, which they keep safe and never distribute
• the public key, which can be sent to anyone with whom they want to exchange encrypted information.

Bitcoin

A digital currency that is mainly used online. However, it can be bought or sold with real money at bitcoin exchanges.

Botnet

A network created by malware that allows an attacker to control a group of computers and use them to gather personal information or launch attacks against others, such as sending spam emails or flooding a website with so many requests for content that the server cannot cope.

Cipher

A mathematical algorithm that turns plaintext into ciphertext and reverts ciphertext to plaintext.

Ciphertext

Information that is encrypted such that it cannot be directly read by humans or a machine.

Countermeasure

An action you take to protect your information against threats and vulnerabilities.

Decryption

The process of reverting ciphertext to plaintext.

Distributed denial of service (DDoS)

A type of attack that floods computer servers with a massive amount of traffic coming from many different computers or computing devices. A DDoS attack can render a server unable to provide services to their legitimate users.

Domain Name System

The system that translates alphabetic internet domain and host names, such as the website addresses you enter into web browsers, into numeric IP addresses. Without this translation, the website names would not be converted to computer-readable numeric IP addresses and hence the web browser would not be able to connect to the website you want to go to.

Encryption

The process of converting plaintext to ciphertext.

EternalBlue

A hacking tool that exploits a defect in Microsoft’s implementation of the Server Message Block protocol, discovered in March 2017.

Firewall

In a computer network, a firewall is a barrier that blocks dangerous communications from spreading across a network, either from the outside world into a local network, or from one part of a local network to another.

Intrusion detection system

An intrusion detection system is used to monitor data passing over a network or a computer in order to detect intrusion.

Key

In the context of cryptography, a secret that is used to encrypt or decrypt messages.

Mirai

Malware that attacks and takes over unsecured consumer devices and uses them to launch distributed denial-of-service attacks on websites.

Plaintext

Information that can be directly read by humans or a machine.

Programmable logic controllers

Very commonly used programmable controllers, which are often used to control industrial motors.

Ransomware

Malware that demands payment in order to refrain from doing some harmful action or to undo the effects of the harmful action.

Relational database

A very commonly used database type. This type of database organises data in tables and links the tables using indexes.

Script

A small piece of computer program that aims to automate a process.

Secure Shell

A network protocol for providing a remote terminal. SSH is more secure than Telnet because it uses encryption to protect the transmission of the data.

Server Message Block

A protocol that allows applications on a computer to access files and services on other computers in a network.

Structured Query Language injection

A hacking technique for gaining unauthorised access to databases through ill-designed web pages.

Stuxnet

Malware specifically designed to target programmable logic controllers. It was believed that the malware was designed by the US and Israeli security agencies to sabotage Iran's uranium enrichment plant, in an effort to stop or delay its nuclear programme.

Spyware

Malware that records the activities of the user, such as the passwords they type into the computer, and transmits this information to the person who wrote the malware.

Symmetric cryptography

A cryptography method in which both the encryption and decryption processes take place based on a common key. As a result, it is important to keep the key secret.

Teletype Network

A network protocol for providing a remote terminal to control a computer system.

Threat

Some danger that can exploit a vulnerability.

Trojan

A Trojan is malware disguised as something useful and can be self-replicating.

Virus

A virus inserts a copy of itself into applications or crucial parts of the operating system in order to infect other computing devices or storage media that interact with the infected computer.

Vulnerability

A point at which there is potential for a security breach.

WannaCry

Fast-spreading malware that surfaced in May 2017. When it infects a computer, it 'locks' the data files (rendering them unusable) and demands a ransom.

Worm

A worm exploits the vulnerability of computing devices in a network and replicates itself by finding and infecting other vulnerable computing devices.

References

Bain, I. (2015) 'TalkTalk cyber-attack: customer got scam call nearly a day before', *The Guardian*, 23 October. Available at: www.theguardian.com/business/2015/oct/23/talktalk-cyber-attack-customers-scam-calls-day-before-announcement (Accessed: 19 October 2018).

Ball, T. (2017) 'Top 5 critical infrastructure cyber attacks', *Computer Business Review*, 18 July. Available at: www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/(Accessed: 19 October 2018).

Baraniuk, C. (2017) 'Should you pay the WannaCry ransom?', *BBC News*, 15 May. Available at: www.bbc.co.uk/news/technology-39920269 (Accessed: 19 October 2018).

BBC News (2015) 'TalkTalk hack "affected 157,000 customers"', *BBC News*, 6 November. Available at: www.bbc.co.uk/news/business-34743185 (Accessed: 19 October 2018).

Burgess, M. (2016) ‘TalkTalk hack toll: 100k customers and £60m’, *WIRED*, 2 February. Available at: www.wired.co.uk/article/talktalk-hack-customers-lost (Accessed: 19 October 2018).

CBS News (2017) ‘White House says WannaCry attack was carried out by North Korea’, *CBS News*, 19 December. Available at: www.cbsnews.com/news/white-house-says-wannacry-attack-was-carried-out-by-north-korea/ (Accessed: 19 October 2018).

Cristal, M. (2017) ‘NHS hack wasn't about making money. It was about disgruntled hackers making a point’, *WIRED*, 15 May. Available at: www.wired.co.uk/article/motivation-nhs-hack (Accessed: 19 October 2018).

Davis, J. (2017) ‘New WannaCry variant takes down North Carolina provider’, *Healthcare IT News*, 24 October. Available at: www.healthcareitnews.com/news/new-wannacry-variant-takes-down-north-carolina-provider (Accessed: 19 October 2018).

Evenstad, L. (2017) ‘CW500: How the NHS WannaCry cyber attack unfolded’, *Computer Weekly*, 17 October. Available at: www.computerweekly.com/news/450428252/CW500-How-the-NHS-WannaCry-cyber-attack-unfolded (Accessed: 19 October 2018).

Experian (2018) *How to spot the warning signs of identity fraud*. Available at: www.experian.co.uk/consumer/warning-signs-of-id-fraud.html (Accessed: 19 October 2018).

Great Britain. *Computer Misuse Act 1990: Elizabeth II. Chapter 18* (1990) London, The Stationery Office.

Griffin, A. and Walker, T. (2016) ‘Internet outage takes down Twitter, Netflix, PayPal and many of the web’s most visited websites’, *Independent*, 21 October. Available at: www.independent.co.uk/life-style/gadgets-and-tech/news/netflix-twitter-internet-down-not-working-broken-paypal-ebay-facebook-instagram-a7374506.html (Accessed: 19 October 2018).

ICO (2016) ‘TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack’, *ICO News*, 5 October. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/ (Accessed: 19 October 2018).

Khomami, N. (2015) ‘TalkTalk hacking crisis deepens as more details emerge’, *The Guardian*, 23 October. Available at: www.theguardian.com/business/2015/oct/23/talktalk-hacking-crisis-deepens-as-more-details-emerge (Accessed: 19 October 2018).

Krebs, B. (2016) ‘Alleged vDOS Proprietors Arrested in Israel’, *Krebs on Security*, 10 September [Blog]. Available at: https://krebsonsecurity.com/2016/09/alleged-vdos-proprietors-arrested-in-israel/ (Accessed: 19 October 2018).

Krebs, B. (2017) ‘Mirai IoT Botnet Co-Authors Plead Guilty’, *Krebs on Security*, 13 December [Blog]. Available at: https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/ (Accessed: 19 October 2018).

Loeb, J. (2017) ‘Number plate system proposed for IoT devices to boost security’, *Engineering and Technology*, 18 October. Available at: https://eandt.theiet.org/content/articles/2017/10/number-plate-system-for-iot-devices-proposed-by-government-advisor-to-boost-security (Accessed: 19 October 2018).

MacAskill, E. (2018) ‘Major cyber-attack on UK a matter of “when, not if” – security chief’, *The Guardian*, 23 January. Available at: www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin (Accessed: 19 October 2018).

Millman, R. (2017) ‘TalkTalk hack: Two men plead guilty to TalkTalk hack’, *IT Pro*, 27 April. Available at: www.itpro.co.uk/security/24136/talktalk-hack-two-men-plead-guilty-to-talk-talk-hack (Accessed: 19 October 2018).

Mimoso, M. (2017) ‘WannaCry Variants Pick Up Where Original Left Off’, *Threatpost*, 15 May. Available at: https://threatpost.com/wannacry-variants-pick-up-where-original-left-off/125681/ (Accessed: 19 October 2018).

Nakashima, E. (2017) ‘The NSA has linked the WannaCry computer worm to North Korea’, *The Washington Post*, 14 June. Available at: www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html (Accessed: 19 October 2018).

News Letter (2018) ‘Identity of NI TalkTalk hacker revealed’, *News Letter*, 14 March. Available at: www.newsletter.co.uk/news/crime/identity-of-ni-talktalk-hacker-revealed-1-8415382 (Accessed: 19 October 2018).

OpenLearn (no date) ‘3.4 Active attacks’ *Network security*. Available at: https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-0 (Accessed: 23 December 2019).

OpenLearn (2011) *How to survive a botnet attack*. Available at https://www.open.edu/openlearn/science-maths-technology/computing-ict/how-survive-botnet-attack (Accessed 23 December 2019).

Smart, W. (2018) *Lessons learned review of the WannaCry Ransomware Cyber Attack*, London, Department of Health and Social Care, UK Government. Available at@ www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (Accessed: 19 October 2018).

Swinford, S. (2018) ‘Russia preparing to mount cyber-attack on Britain’s “critical infrastructure”, GCHQ and FBI warn’, *The Telegraph*, 16 April. Available at: www.telegraph.co.uk/politics/2018/04/16/russia-preparing-mount-cyber-attack-britains-critical-infrastructure/ (Accessed: 19 October 2018).

Tankard, C. (2015) ‘What can we learn from the TalkTalk hack?’, *ITProPortal*, 3 December. Available at: www.itproportal.com/2015/12/03/what-can-we-learn-from-the-talktalk-hack/ (Accessed: 19 October 2018).

Ungoed-Thomas, J., Henry, R. and Gadher, D. (2017) ‘Cyber-attack guides promoted on YouTube’, *The Times*, 14 May. Available at: www.thetimes.co.uk/article/cyber-attack-guides-promoted-on-youtube-972s0hh2c (Accessed: 19 October 2018).

White, G. (2015) ‘TalkTalk hack – new details emerge’, *Channel 4 News*, 5 November. Available at: www.channel4.com/news/talktalk-hack-insiders-reveal-how-it-was-pulled-off (Accessed: 19 October 2018).

Woollaston, V. (2017) ‘WannaCry ransomware: what is it and how to protect yourself’, *WIRED*, 22 May. Available at: www.wired.co.uk/article/wannacry-ransomware-virus-patch (Accessed: 19 October 2018).

Xander (2016) ‘DDoS on Dyn – The Complete Story’, *ServerComparator*, 21 November [Blog]. Available at: https://web.archive.org/web/20161121175123/https://servercomparator.com/vpn/blog/dyn-mirai-ddos-complete-story (Accessed: 19 October 2018).

Acknowledgements

This free course was written by Patrick Wong. It was first published in February 2020.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this free course:

Images

Course image: © metamorworks / www.shutterstock.com

Video/Audio

Video 1: © Reprint Courtesy of International Business Machines Corporation © International Business Machines Corporation.

Video 2: © Courtesy Symantec Corporation

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Don't miss out

If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University – www.open.edu/openlearn/free-courses.