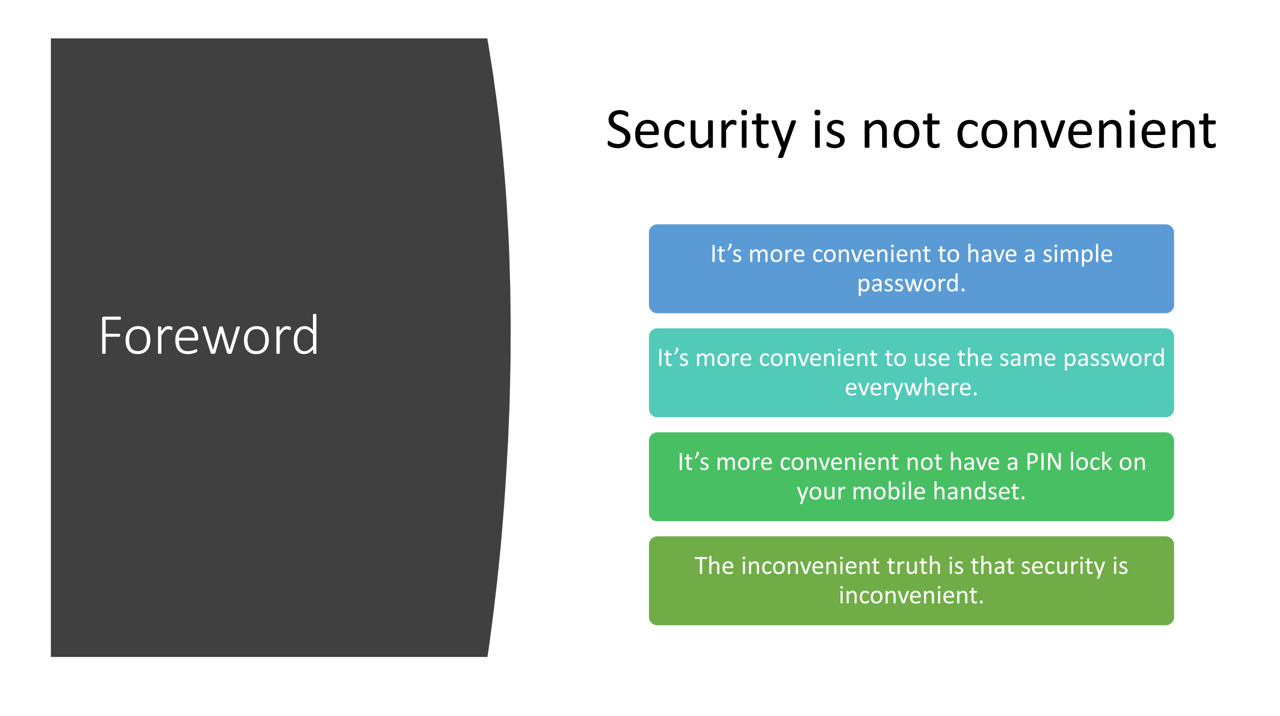
Cyber Security

My email password has been hacked again - that's the third time I've had to rename my cat.

1

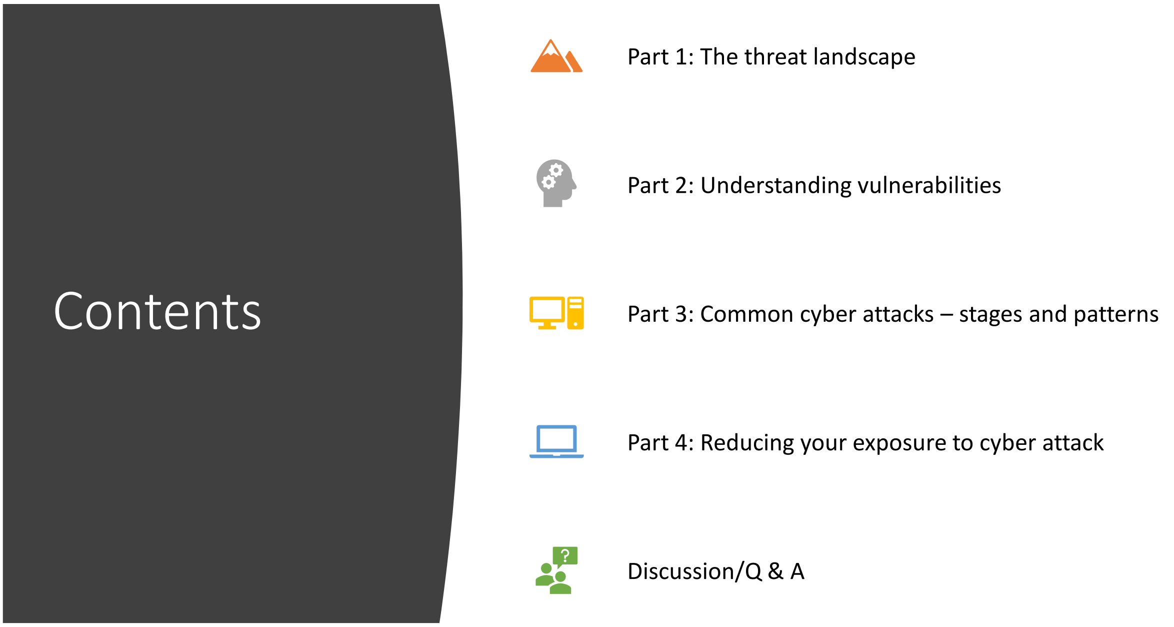


Foreword

Security is not convenient

- It's more convenient to have a simple password.
- It's more convenient to use the same password everywhere.
- It's more convenient not have a PIN lock on your mobile handset.
- The inconvenient truth is that security is inconvenient.

2



Contents

- Part 1: The threat landscape
- Part 2: Understanding vulnerabilities
- Part 3: Common cyber attacks – stages and patterns
- Part 4: Reducing your exposure to cyber attack
- Discussion/Q & A

3

Part 1: The threat landscape

4

Technical focus

Risk

In cyber security terms, risk is the potential for a **threat** to exploit a **vulnerability** that may result in some form of negative impact.

Threat

A person or thing that is likely to cause damage.

5

Who might be attacking you?

Cyber criminals interested in making money through fraud or from the sale of valuable information.

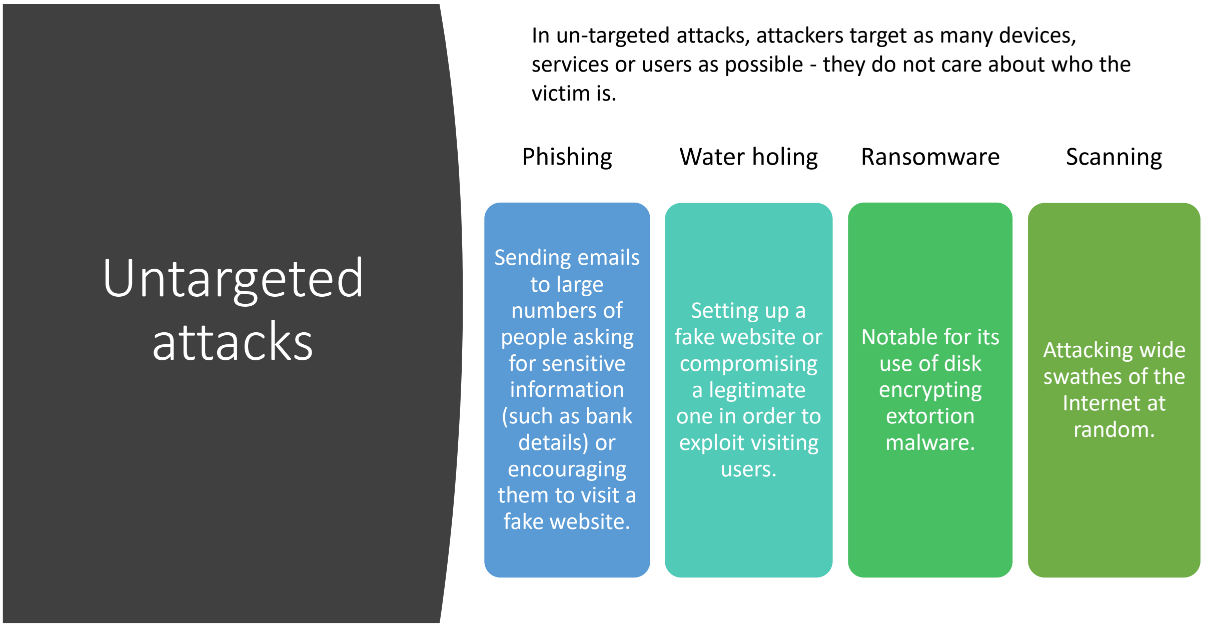
Industrial competitors and foreign intelligence services, wanting to gain an advantage for companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

6



Untargeted attacks

In un-targeted attacks, attackers target as many devices, services or users as possible - they do not care about who the victim is.

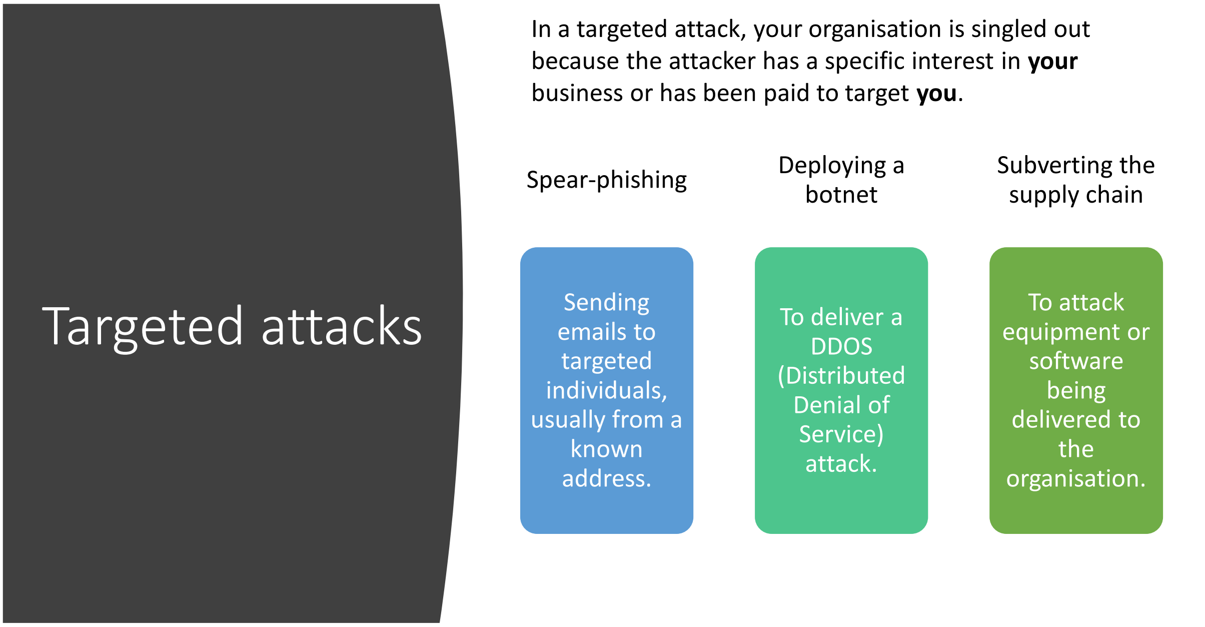
Phishing
Sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Water holing
Setting up a fake website or compromising a legitimate one in order to exploit visiting users.

Ransomware
Notable for its use of disk encrypting extortion malware.

Scanning
Attacking wide swathes of the Internet at random.

7



Targeted attacks

In a targeted attack, your organisation is singled out because the attacker has a specific interest in **your** business or has been paid to target **you**.

Spear-phishing
Sending emails to targeted individuals, usually from a known address.

Deploying a botnet
To deliver a DDOS (Distributed Denial of Service) attack.

Subverting the supply chain
To attack equipment or software being delivered to the organisation.

8

Insider threat

Although we have discussed threats from the Internet, insiders (anyone who has legitimate access to your systems as an employee or a contractor) should also be considered as part of a holistic security regime.

- An insider could simply use their normal access to compromise your information.
- Without appropriate training, insiders can also accidentally compromise a system or the information it holds.
- In the worst-case scenario, an insider could be working for an adversary.

9

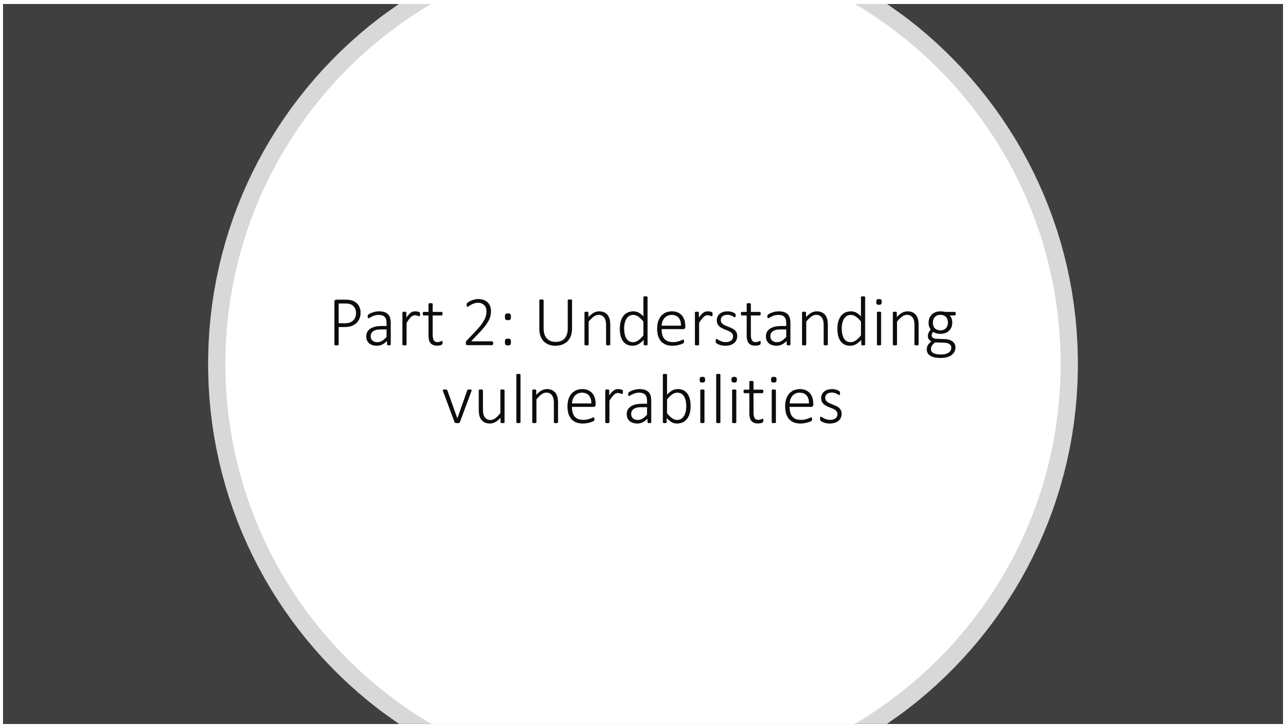
Every organisation is a potential victim

It is often difficult to provide an accurate assessment of the threats that specific organisations face.

Every organisation is a potential victim. All organisations have something of value that is worth something to others.

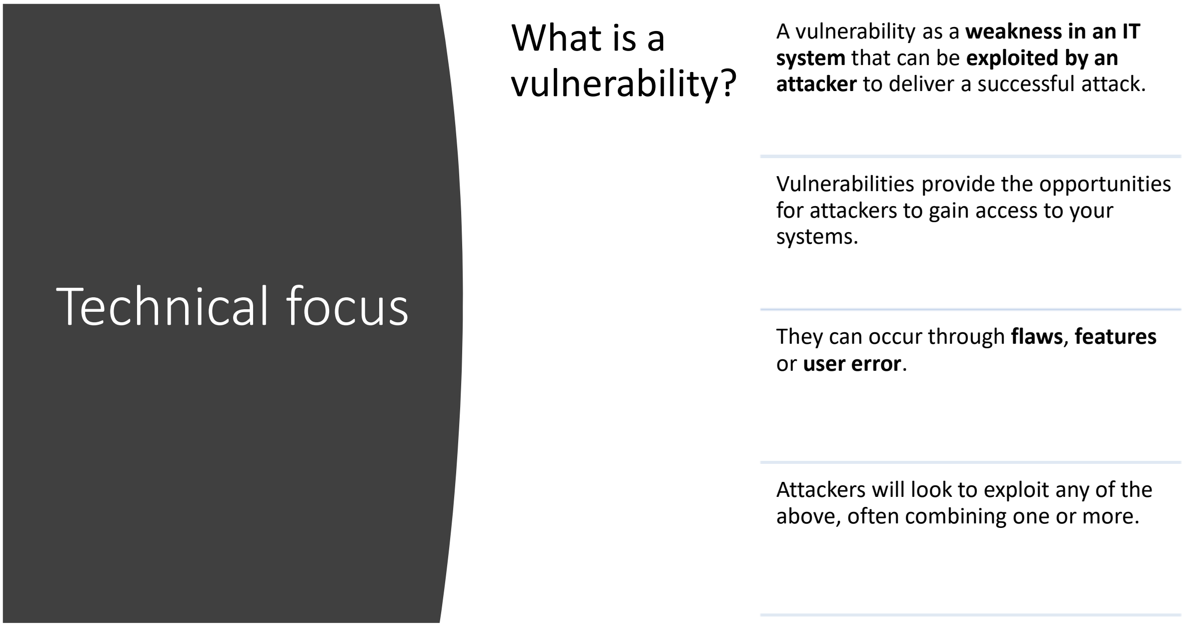
As part of risk management processes, assess whether you are likely to be the victim of a targeted or un-targeted attack.

10



Part 2: Understanding vulnerabilities

11



Technical focus

What is a vulnerability?

A vulnerability as a **weakness in an IT system** that can be **exploited by an attacker** to deliver a successful attack.

Vulnerabilities provide the opportunities for attackers to gain access to your systems.

They can occur through **flaws**, **features** or **user error**.

Attackers will look to exploit any of the above, often combining one or more.

12

Understanding vulnerabilities

Flaws

A flaw is **unintended functionality**.

A flaw may either be a result of poor design or mistakes made during implementation.

Flaws may go undetected for a significant period.

Most common attacks we see today exploit these types of vulnerabilities.

13

Understanding vulnerabilities

Features

A feature is **intended functionality** which can be misused by an attacker to breach a system.

Features may improve the user’s experience, help diagnose problems or improve management, but they can also be exploited by an attacker.

When Microsoft introduced macros into their Office suite in the late 1990s, macros soon became the vulnerability of choice. Macros are still regularly exploited today.

JavaScript, widely used in dynamic web content, continues to be used by attackers. This includes diverting the user’s browser to a malicious website and silently downloading malware and hiding malicious code.

14

Understanding vulnerabilities

User Error

Users can make mistakes, such as choosing a common or easily guessed password, or leave their laptop or mobile phone unattended.

Even the most cyber aware users can be fooled into giving away their password, installing malware, or divulging information that may be useful to an attacker.

A computer or system that has been carefully designed and implemented can minimise the vulnerabilities of exposure to the Internet.

Unfortunately, such efforts can be easily undone (for example) by an inexperienced system administrator who enables vulnerable features, fails to fix a known flaw, or leaves default passwords unchanged.

15

Part 3: Common cyber attacks – stages and patterns

16

Stages of an attack

An attack often consists of repeated stages. The attacker is effectively probing your defences for weaknesses that, if exploitable, will take them closer to their goal.

Survey
Investigating and analysing available information about the target in order to identify potential vulnerabilities.

Delivery
Getting to the point in a system where a vulnerability can be exploited.

Breach
Exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access.

Affect
Carrying out activities within a system that achieve the attacker's goal.

17

Stages and patterns

Survey

Attackers will use any means available to find technical, procedural or physical vulnerabilities which they can attempt to exploit.

Attackers will use open source information such as LinkedIn and Facebook, domain name management/search services, and social media.

User error can also reveal information that can be used in attacks – something as simple as not removing document authors can reveal a lot about who works within an organisation.

Attackers will also use social engineering (often via social media) to exploit user naivety and goodwill to gain further, less openly available information.

18

Stages and patterns

Delivery

During the delivery stage, the attacker will look to get into a position where they can exploit a vulnerability that they have identified, or they think could potentially exist.

Examples include:

Attempting to access an organisation’s online services.

Sending an email containing a link to a malicious website or an attachment which contains malicious code.

Giving an infected USB stick away at a trade show.

Creating a false website in the hope that a user will visit.

19

Stages and patterns

Breach

The harm to your business will depend on the nature of the vulnerability and the exploitation method used.

The attacker may be able to:

Make changes that affect the system’s operation.

Gain access to online accounts.

Achieve full control of a user’s computer, tablet or smartphone. Having done this, the attacker could pretend to be the victim and use their legitimate access rights to gain access to other systems and information.

20

Stages and patterns

Affect

Depending on their motivation, the attacker may seek to explore your systems, expand their access and establish a persistent presence. Possible results include:

Retrieving information they would otherwise not be able to access, such as intellectual property or commercially sensitive information.

Making changes for their own benefit, such as creating payments into a bank account they control.

Disrupting normal business operation, such as overloading the organisation's internet connection so they cannot communicate externally or deleting the whole operating system from users' computers.

After achieving the objective, the more capable attacker will exit, carefully removing any evidence of their presence.

21

Part 4: Reducing your exposure to cyber attack

22

Reducing your exposure using essential security controls

Boundary firewalls and gateways

Establish network perimeter defences, particularly web proxy, web filtering, content checking, and firewall policies.

Malware protection

Establish and maintain malware defences to detect and respond to known attack code.

Patch management

Patch known vulnerabilities with the latest version of the software, to prevent attacks which exploit software flaws.

Whitelisting and execution control

Prevent unknown software from being able to run or install itself, including Autorun on USB and CD drives.

23

Reducing your exposure using essential security controls

Secure configuration

Restrict the functionality of every device, operating system and application to the minimum needed for business to function.

Password policy

Ensure that an appropriate password policy is in place and followed.

User access control

Include limiting normal users' execution permissions and enforcing the principle of least privilege.

Security monitoring

To identify any unexpected or suspicious activity.

24

Reducing your exposure using essential security controls

User training education and awareness

Staff should understand their role in keeping your organisation secure and report any unusual activity.

Security incident management

Put plans in place to deal with an attack as an effective response will reduce the impact on your business.

Get cyber security certified

Review the available standards relating to cyber security and complete the process to get certified.

Consider cyber liability insurance

Cyber liability insurance will cover your business if the worst does happen. Policies will cover direct losses such as the cost of repairing, replacing or restoring systems, data or websites following an attack.

25

Cyber security standards

Cyber Essentials & Cyber Essentials Plus

The UK Government and industry have worked together to produce a scheme designed to help UK organisations improve their defences and demonstrate publicly their commitment to cyber security.

As a set of baseline technical controls, the Cyber Essentials scheme has a very wide audience. Organisations large and small, public, private and charitable can all benefit from the provisions set out in the scheme.

The process of certification has been designed to be light weight and easily manageable while at the same time providing a respected standard in cyber security.

26

Cyber security standards

IASME Governance Standard

The IASME Governance standard, based on international best practice, is risk-based and includes aspects such as physical security, staff awareness, and data backup.

The IASME standard was recently recognised as the best cyber security standard for small companies by the UK Government.

The IASME governance self assessment includes the Cyber Essentials assessment within it as well as an assessment against the requirements of the GDPR.

The audited IASME certification is seen as a realistic alternative to ISO27001 by an increasing number of companies.

27

Cyber security standards

ISO/IEC 27001

The ISO/IEC 27000 family of standards helps organisations keep information assets secure.

ISO/IEC 27001 will help your organisation manage security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard providing requirements for an information security management system (ISMS).

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

28

The ‘dark web’

What is the dark web?

The internet is made up of three different layers: the surface web, the deep web and the dark web.

The dark web is a network of **untraceable** online activity and websites on the internet.

Where did it come from?

The dark web was created by the US government.

US military researchers developed the technology, known as Tor (The Onion Router) in the mid-1990s.

Tor now hosts roughly 30,000 hidden sites.

Who uses the dark web, and why?

The dark web is used by all sorts of people for all sorts of reasons - but it's not surprising that it's used for illegal activity.

Tor has effectively become a black market for goods such as drugs, **personal details** and even guns.

29

The ‘dark web’

What personal details may be available?

Email addresses, usernames, passwords and other personally identifiable information (PII).

The data comes from web site compromises where PII has been stolen.

Breaches of note include:

2018: Marriott – 500 million compromised accounts.

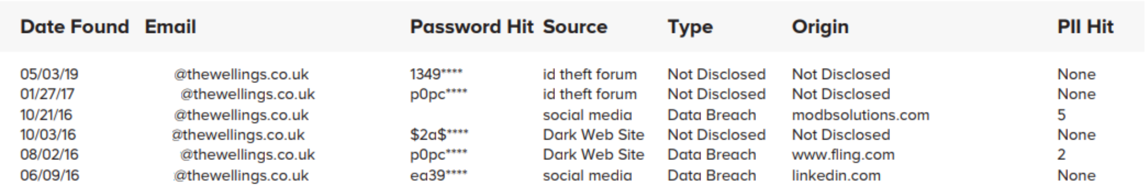
2017: Equifax – 143 million compromised accounts.

2016: Adult Friend Finder – 412.2 million compromised accounts.

2014: Yahoo – 3 billion compromised accounts - real names, email addresses, passwords, dates of birth and telephone numbers.

Services are available to track company’s compromised credentials and alert when new breaches have been discovered.

30



Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
05/03/19	@thewellings.co.uk	1349****	id theft forum	Not Disclosed	Not Disclosed	None
01/27/17	@thewellings.co.uk	p0pc****	id theft forum	Not Disclosed	Not Disclosed	None
10/21/16	@thewellings.co.uk		social media	Data Breach	modbsolutions.com	5
10/03/16	@thewellings.co.uk	$2a$****	Dark Web Site	Not Disclosed	Not Disclosed	None
08/02/16	@thewellings.co.uk	p0pc****	Dark Web Site	Data Breach	www.fling.com	2
06/09/16	@thewellings.co.uk	ea39****	social media	Data Breach	linkedin.com	None

31

Wrap up

32

Discussion/Q & A

33