



UNIVERSITY OF
PLYMOUTH

Cyber Threats & Adversarial Behaviours

Dr Hai-Van Dang

Centre for Security, Communications and Network Research

Module Overview

● Module Team:

- Dr Hai-Van Dang (Module Leader – Cyber security)
- Dr Lingfen Sun (Network)

● Communication:

- Contact hours: during lectures
- Surgery hours: TBC on DLE
- Microsoft Teams, email – for individual queries – 2 working days

Module Overview

● Assessment

- 30% - Set Exercise – Research-based task
- 70% - Report – Case Study Report

● Sessions

- Lecture – live and recorded, uploaded on DLE within 2 days
- Mentimeter, DLE used during lectures
- Practical – SMB101 (physical or VPN)

● Lecture slides: on DLE. The update version will be uploaded within 2 days after class

Module Overview

- Activities in class:

- Individual
- Group

- DLE overview

- Q&A: menti

Cyber Threats & Adversarial Behaviours - Your checklist

LO1: Can you name the motivations, attack vectors, threat consequences of the cyber threats? [1]

LO2: Can you research the trend of the cyber vulnerabilities? [6]

LO3: Can you know your rights by GDPR? [5]

LO4: Can you recognize the category of cyber crimes? [2]

LO5: Can you see how cyber kill chain is being used? [3,4]

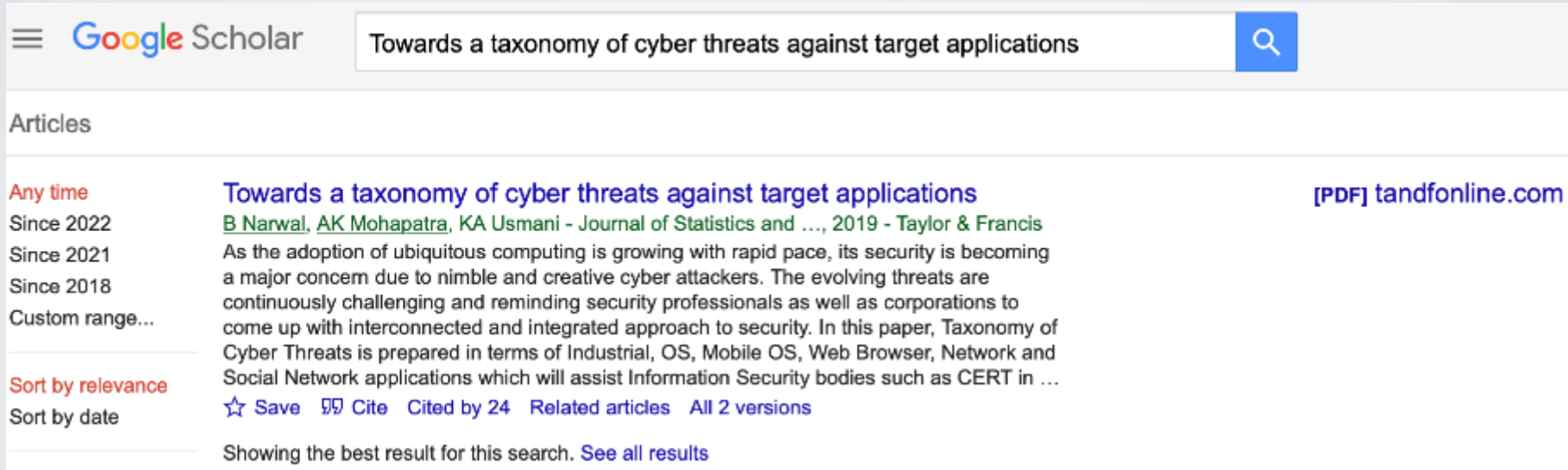
LO6: Can you recognize the different types of malware? [1]

Further reading

1. Narwal, Bhawna, Amar Kumar Mohapatra, and Kaleem Ahmed Usmani. "Towards a taxonomy of cyber threats against target applications." *Journal of Statistics and Management Systems* 22.2 (2019): 301-325.
2. McGuire, Mike, and Samantha Dowling. "Cyber crime: A review of the evidence." *Summary of key findings and implications. Home Office Research report* 75 (2013).
3. Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." *Leading Issues in Information Warfare & Security Research* 1.1 (2011): 80.
4. Martin, Lockheed. "Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform. Lockheed Martin Corporation (2015)." (2019).
5. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387
6. Cyber security breach surveys (DLE)

How to find the further reading material

● Google scholar



The screenshot shows the Google Scholar interface. At the top, the Google Scholar logo is on the left, and a search bar contains the text "Towards a taxonomy of cyber threats against target applications" with a search icon on the right. Below the search bar, the word "Articles" is displayed. On the left side, there are filters for "Any time" (with sub-options: "Since 2022", "Since 2021", "Since 2018", "Custom range...") and "Sort by relevance" (with sub-option: "Sort by date"). The main search result is for the article "Towards a taxonomy of cyber threats against target applications" by B Narwal, AK Mohapatra, and KA Usmani, published in the Journal of Statistics and ... in 2019 by Taylor & Francis. The abstract begins with "As the adoption of ubiquitous computing is growing with rapid pace, its security is becoming a major concern due to nimble and creative cyber attackers. The evolving threats are continuously challenging and reminding security professionals as well as corporations to come up with interconnected and integrated approach to security. In this paper, Taxonomy of Cyber Threats is prepared in terms of Industrial, OS, Mobile OS, Web Browser, Network and Social Network applications which will assist Information Security bodies such as CERT in ...". Below the abstract, there are links for "Save", "Cite", "Cited by 24", "Related articles", and "All 2 versions". On the right side of the result, there is a link "[PDF] tandfonline.com". At the bottom of the result, it says "Showing the best result for this search. See all results".

Google Scholar

Towards a taxonomy of cyber threats against target applications

Articles

Any time
Since 2022
Since 2021
Since 2018
Custom range...

Sort by relevance
Sort by date

Towards a taxonomy of cyber threats against target applications
B Narwal, AK Mohapatra, KA Usmani - Journal of Statistics and ..., 2019 - Taylor & Francis

As the adoption of ubiquitous computing is growing with rapid pace, its security is becoming a major concern due to nimble and creative cyber attackers. The evolving threats are continuously challenging and reminding security professionals as well as corporations to come up with interconnected and integrated approach to security. In this paper, Taxonomy of Cyber Threats is prepared in terms of Industrial, OS, Mobile OS, Web Browser, Network and Social Network applications which will assist Information Security bodies such as CERT in ...

☆ Save Cite Cited by 24 Related articles All 2 versions

Showing the best result for this search. See all results

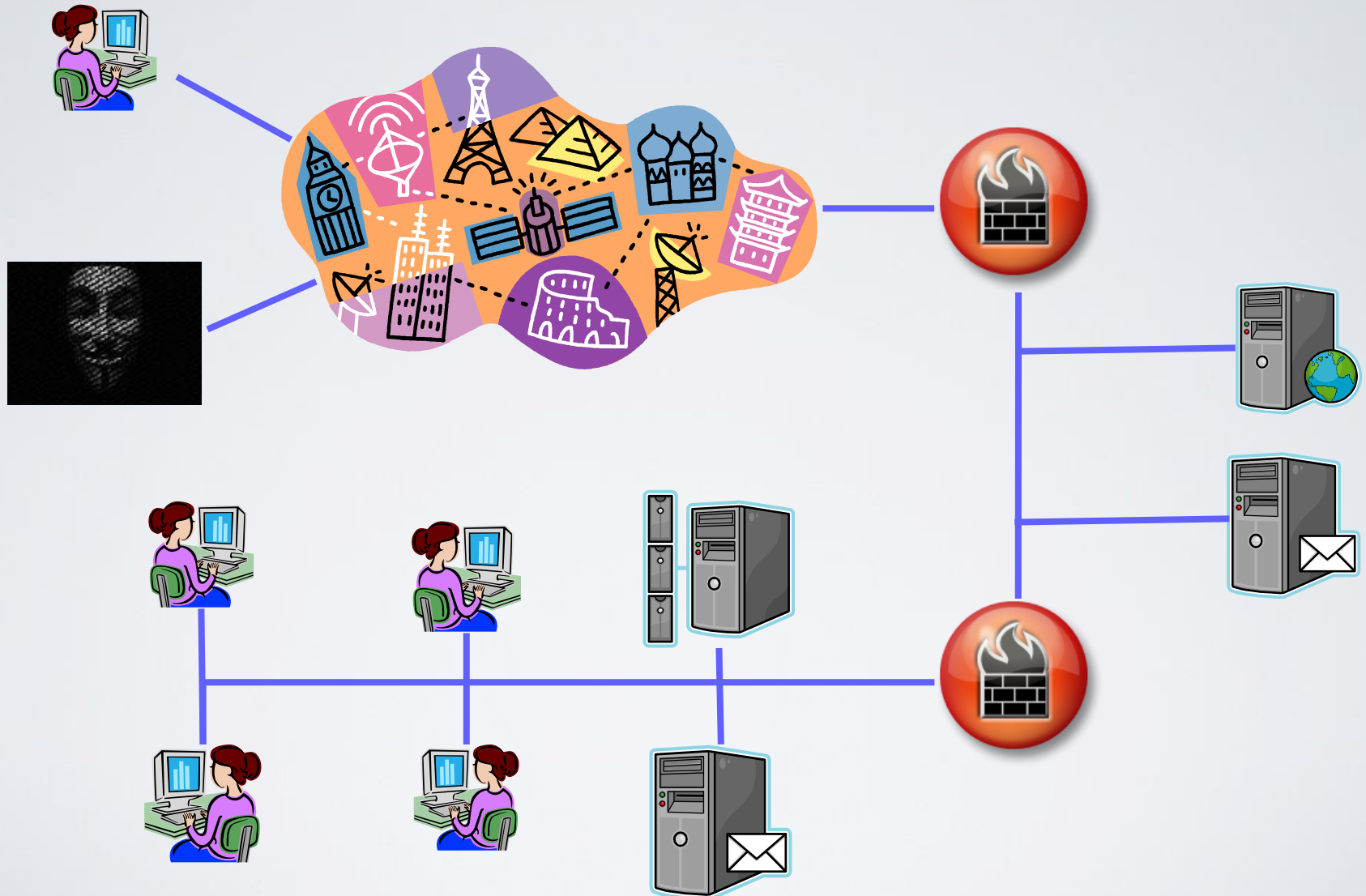
[PDF] tandfonline.com

● University library:

<http://primo.plymouth.ac.uk>

● Google

Cyber Security & Networks



Session Content

Introduction

Scale and Scope

Hackers

Malware

Conclusions

system and
Phishing

Spam

Denial of Service

Virus

Identity Theft

Ransomware

Tracking

Trojan Horses

Web defacement

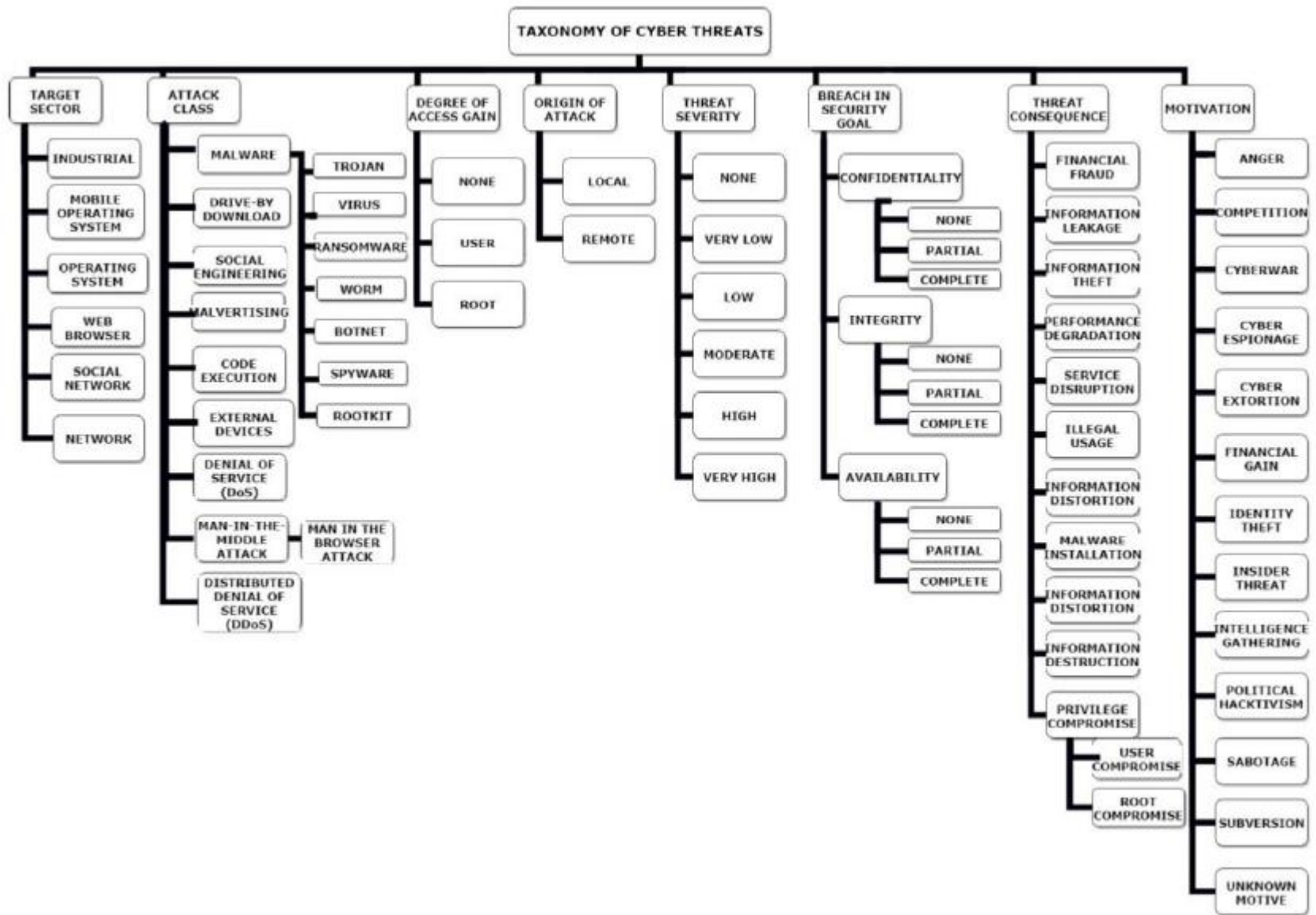
Norm

Spyware

Activities

Group: Introduce name to each other. Share the work: one as facilitator to ask and collect the answers, the others contribute (No worries if you do not know the answers).

1. What can be motivation of the cyber attacks?
2. What can be threat consequences of the cyber attacks?
3. What can be the attack targets?



Source of image: [1]

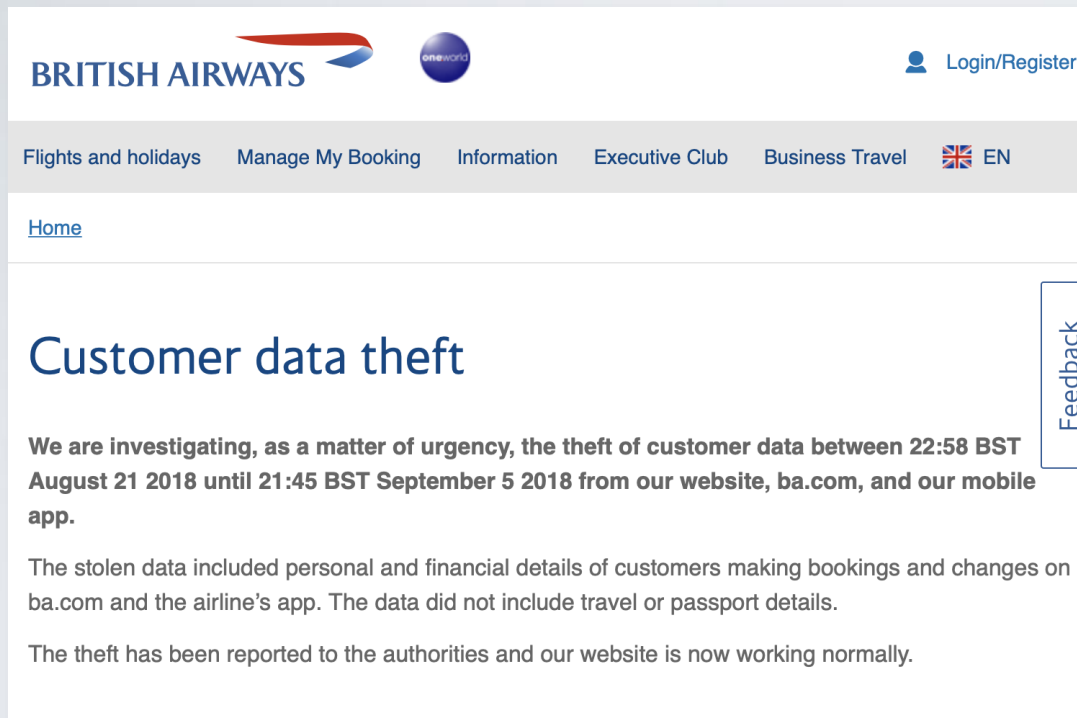
Example: Zeus

Group

- ⑩ Facilitator: share the work (Example: one finds answers for a,b,c, the other does d,e,f) and collect the answers.
- ⑩ Read [https://en.wikipedia.org/wiki/Zeus_\(malware\)](https://en.wikipedia.org/wiki/Zeus_(malware)) and identify the following information
 - a. Type of malware
 - b. Targeted system
 - c. Attack vector (attack class, i.e. a path or means of an attack)
 - d. Origin of attack (local or remote?)
 - e. Threat consequences
 - f. Motivation

Example Headlines

British Airways Hack



- BA experienced a "sophisticated, malicious criminal attack" on its website and app between 21 August and 5 September 2018
 - malicious code injection to the company's systems to achieve online card skimming
- Breach affected ~380,000 transactions, intercepting:
 - name, email address, credit card information (credit card number, expiration date and CVV/CVC)

<https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information>
(not accessible in Jan 2022)

Other source: <https://www.bbc.co.uk/news/business-48905907>,
<https://www.bbc.co.uk/news/technology-45446529>, last accessed Jan 2022

BA meets GDPR

- GDPR (General Data Protection Regulation) penalties can be up to 4% of annual global revenue

- BA's total revenue for 2017 was £12.23bn, so a potential maximum fine of £489m

- ICO (Information Commissioner's Office) fined BA £20 million (Oct 20)

The screenshot shows the ICO website with a red header containing the word 'NEWS'. Below the header is a navigation bar with links: Home, Your data matters, For organisations, Make a complaint, Action we've taken, and About the ICO. The main content area features a news article titled 'ICO fines British Airways £20m for data breach affecting more than 400,000 customers'. The article is dated 16 October 2020 and is categorized as 'News'. The text of the article states that the Information Commissioner's Office (ICO) has fined British Airways (BA) £20m for failing to protect the personal and financial details of more than 400,000 of its customers. It details an investigation into a data breach in 2018, where BA was fined for not having adequate security measures in place. The article also mentions that BA was the subject of a cyber attack during 2018, which it did not detect for more than two months. The ICO investigators found that BA ought to have identified weaknesses in its security and resolved them with security measures that were available at the time. Addressing these security issues would have prevented the 2018 cyber-attack being carried out in this way, investigators concluded. Information Commissioner Elizabeth Denham said: "People entrusted their personal details to BA and BA failed to take adequate measures to keep those details secure. Their failure to act was unacceptable and affected hundreds of thousands of people, which may have caused some anxiety and distress as a result. That's why we have issued BA with a £20m fine – our biggest to date." "When organisations take poor decisions around people's personal data, that can have a real impact on people's lives. The law now gives us the tools to encourage businesses to make better decisions about data, including investing in up to date security." Because the BA breach happened in June 2018, before the UK left the EU, the ICO investigated on behalf of all EU authorities as lead supervisory authority under the GDPR. The penalty and action have been approved by the other EU DPAs through the GDPR's co-decision process. In June 2019 the ICO issued BA with a notice of intent to fine. As part of the regulatory process the ICO considered both representations from BA and the economic impact of COVID-19 on their business before setting a final penalty.

Data protection

Contents

- [The Data Protection Act](#)
- [Find out what data an organisation has about you](#)
- Make a complaint

Make a complaint

If you think your data has been misused or that the organisation holding it has not kept it secure, you should contact them and tell them.

If you're unhappy with their response or if you need any advice you should contact the Information Commissioner's Office (ICO).

Your rights under GDPR

● menti

YOUR CUSTOMERS' RIGHTS UNDER GDPR



RIGHT TO BE INFORMED

Be transparent in how you collect and process personal information and the purposes that you intend to use it for. Inform your customer of their rights and how to carry them out.



RIGHT OF ACCESS

Your customer has the right to access their data. You need to enable this either through business process or technical means.



RIGHT TO RECTIFICATION

Your customer has the right to correct information that they believe is inaccurate.



RIGHT TO ERASURE

You must provide your customer with the right to be forgotten, provided that your legitimate interest to hold such information does not override theirs.



RIGHT TO RESTRICTION OF PROCESSING

Your customer has the right to request that you stop processing their data.



RIGHT TO DATA PORTABILITY

You need to enable the machine and human-readable export of your customers' personal information.



RIGHT TO OBJECT

Your customer has the right to object to you using their data.



RIGHTS REGARDING AUTOMATED DECISION MAKING

Your customer has the right not to be subject to a decision based solely on automated processing, including profiling.

Helping small businesses work towards Data Protection Compliance and deliver on their Web Application goals

www.ServeIT.com

Closer to home . . .



The screenshot shows the SC Magazine UK website. The header includes the SC Magazine logo, navigation links for SC US and SC UK, and a section for Vendor Webcasts. The main content area displays a news article titled "Derriford hospital hit by ransomware" by Roi Perez, dated September 05, 2016. The article text states that a Freedom of Information (FOI) request revealed that Plymouth's Derriford Hospital has suffered a ransomware attack. It also mentions that trust bosses say the attack was dealt with quickly and no patient data was released. A quote from a hospital spokesperson is provided, stating that the incident was an opportunistic 'phishing' form of general malware, not a targeted attack. The article concludes by noting that 47 percent of NHS Trusts in England have been hit by ransomware in the past year, according to data from FOI requests filed by security company NCC Group. A final line indicates that 60 Trusts responded, with 31 withholding information, many citing patient confidentiality.

SC Magazine UK > News > News Bytes > Derriford hospital hit by ransomware

Roi Perez, Community Manager
Follow @scmagperez

September 05, 2016

Derriford hospital hit by ransomware

Share this content: [f](#) [t](#) [in](#) [g+](#) [comment](#) [print](#)

A Freedom of Information (FOI) request filed by the Plymouth Herald has revealed that Plymouth's Derriford Hospital has suffered a ransomware attack.

According to the Plymouth Herald, trust bosses say the attack was dealt with quickly and no patient data was released.

A hospital spokesperson told the Plymouth Herald that, "The particular incident referred to was an opportunistic 'phishing' form of general malware, not a targeted attack on the trust and the trust was not directly approached for payment."

The news comes as 47 percent of NHS Trusts in England have been hit by ransomware in the past year, according to data from FOI requests which were filed by security company NCC Group.

60 Trusts responded with 31 of these withheld information with many citing patient confidentiality.

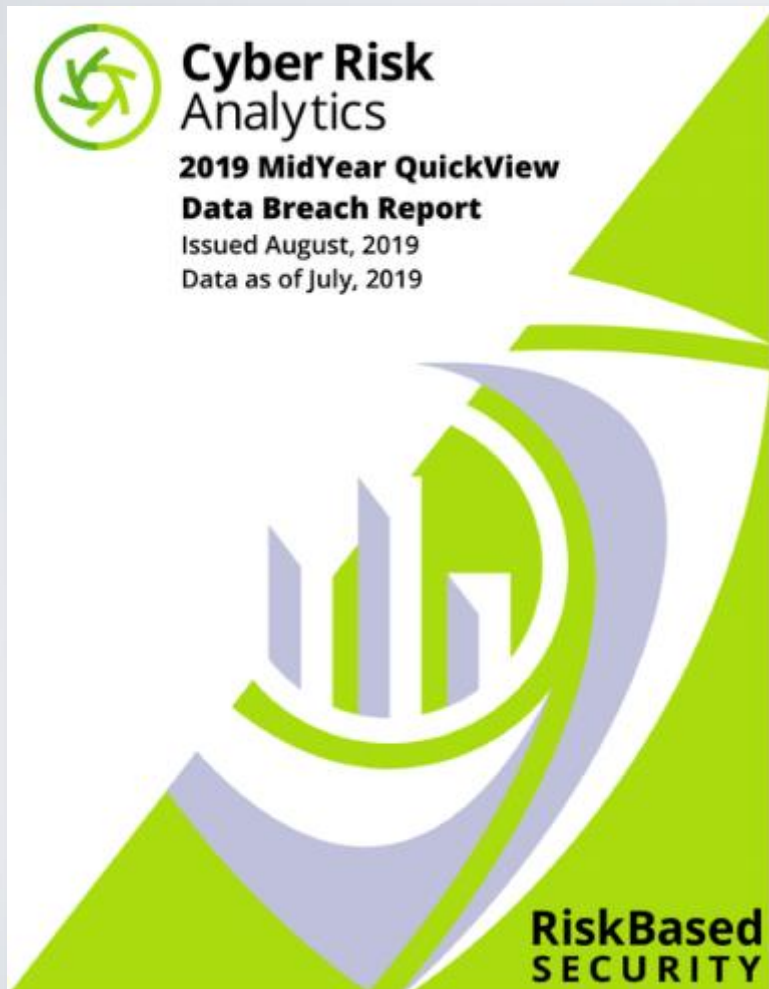
- 60 NHS Trusts in England responded to a freedom of information (FOI) request
 - 28 admitted being hit by ransomware
 - 31 did not confirm or deny

Criminals launch cyber attack at Plymouth school 'in return for ransom'

A UK criminal gang or individual deployed a virus attempting to disable data in return for a ransom, Hele's School Principal Justine Mason has revealed

Source: <https://www.plymouthherald.co.uk/news/plymouth-news/criminals-launch-cyber-attack-plymouth-3282812>

And for 2019 ...



- 3,813 breaches were reported by the end of June, exposing over 4.1 billion records
 - An increase of 54% in reported breaches and 52% in exposed records compared to mid-2018
 - Three breaches are within the top 10 largest breaches of all time
- Breach insights:
 - Web was the top breach type for *number of records exposed*, accounting for 79% of compromised records
 - Hacking was the top breach type for *number of incidents*, accounting for 82% of reported breaches
 - ~70% of breaches exposed email addresses and ~65% exposed passwords

And for 2020 ...

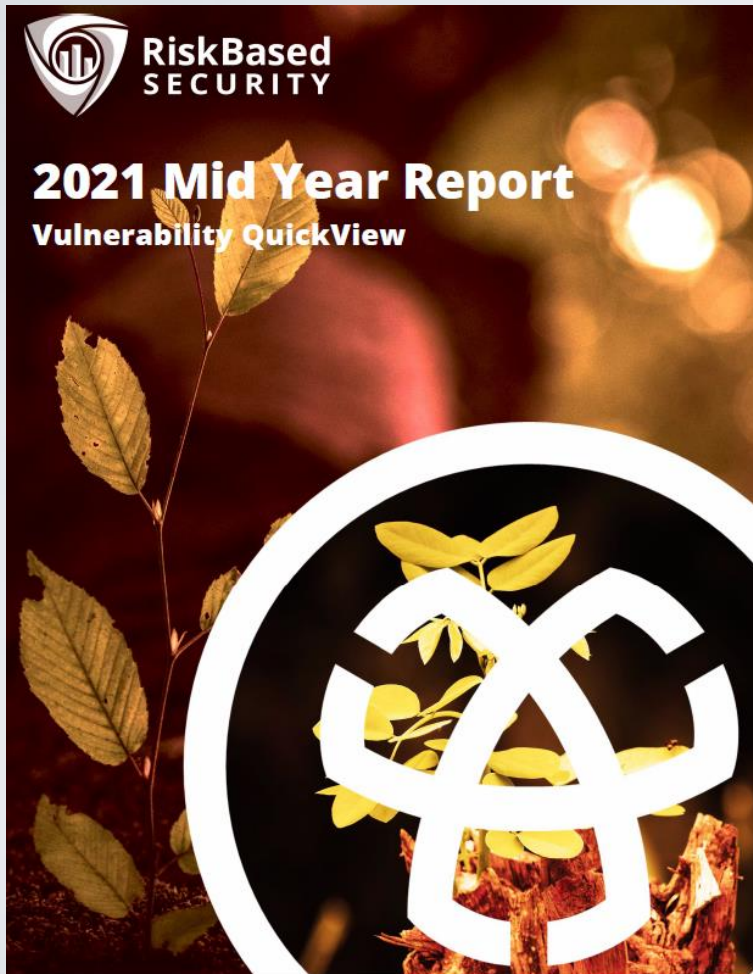


2020 Mid Year Report Data Breach QuickView



- 2,037 publicly reported breaches by the end of June, exposing over 27 billion records
 - A decrease of 52% in reported breaches compared to a 54% increase in exposed records compared to mid-2019
 - 27 billion in 6 months is more than the total of 2019 by more than 12 billion
 - Two of the largest breaches ever reported
- Breach insights:
 - Payment card details exposed surpassed 90 million records
 - Healthcare sector nearly matched the information sector – accounting for 14.3% of the reported breaches

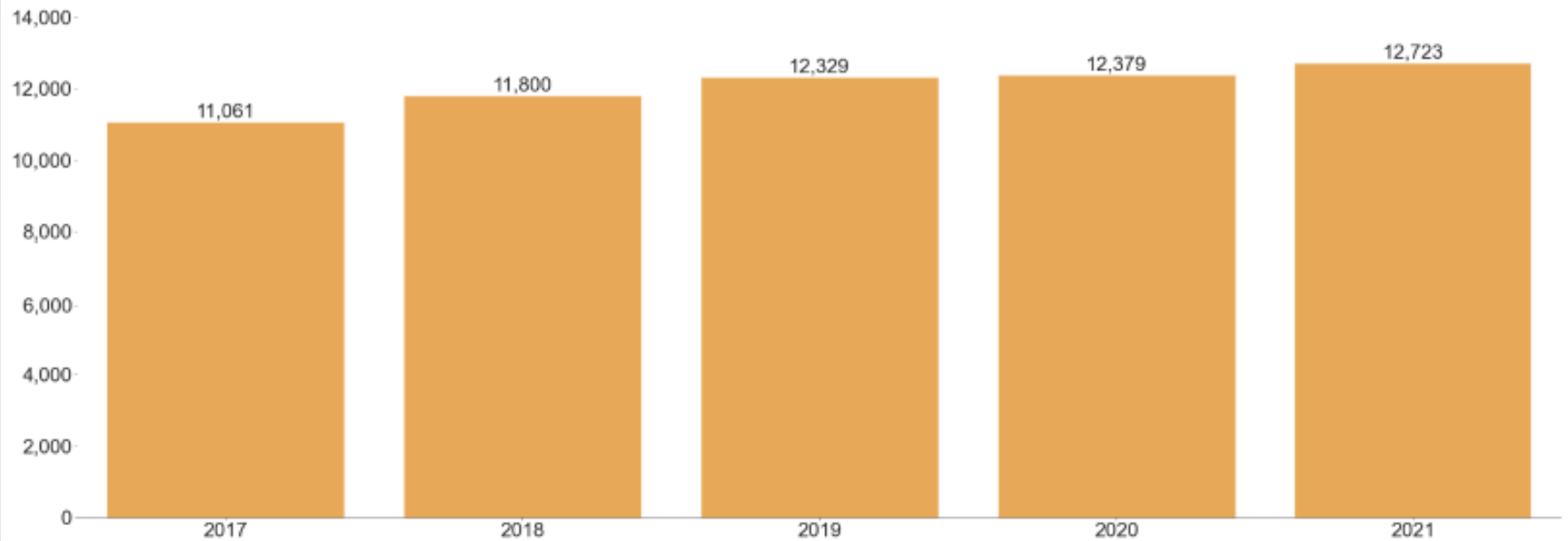
And for 2021 ...



- 12,723 vulnerabilities that were disclosed during the first half of 2021.
 - 2.8%, compared to the same period in 2020, despite ongoing business disruptions.
 - an average of 80 new vulnerabilities per day
 - 849 vulnerabilities that are remotely exploitable but do not have a mitigating solution.
- Insights: see the next slides







Vulnerabilities increase

Figure 1: Number of vulnerabilities disclosed by Q2, in the last five years



Top ten products by vulnerabilities disclosures in Q2 2021

Table 1: Top ten products by vulnerability disclosures in Q2 2021, as compared to 2020.

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
Debian Linux	1 	2	628	609
Fedora	2	N/A	584	N/A
openSUSE Leap	3 	1	526	692
Ubuntu	4	4	443	521
Windows 10	5	5	274	478
SuSE Linux Enterprise Server (SLES)	6 	10	260	394
Windows Server (Semi-Annual Channel)	7 	8	259	427
Windows Server 2019	8 	7	248	436
Google Pixel / Nexus Devices	9	9	242	414
SuSE Linux Enterprise Server for SAP	10 	15	233	360

Top ten vendors by vulnerabilities disclosure in Q2 2021

Table 2: Top ten vendors by vulnerability disclosures in Q2 2021, as compared to 2020

Name	Rank 2021	Rank 2020	Count 2021	Count 2020
Software in the Public Interest, Inc.	1 	8	628	610
Microsoft Corporation	2 	3	627	789
SUSE	3 	4	590	782
Fedora Project	4	N/A	584	N/A
IBM Corporation	5 	6	547	708
Oracle Corporation	6 	1	521	915
Google	7 	5	503	753
Cisco Systems	8 	10	463	384
Canonical Ltd.	9	9	444	522
Red Hat	10 	2	439	843

Scope and Scale

Name a few cyber crimes

- Menti

Categories of Computer Crime and Abuse

Audit Inspectorate (1981)

- Fraud



- Theft



- Survey repeated every 3-4 years
- Last one was 2004/5

Categories of Computer Crime and Abuse

Audit Commission (2005)

- Fraud
- Hacking
- Invasion of Privacy
- Sabotage



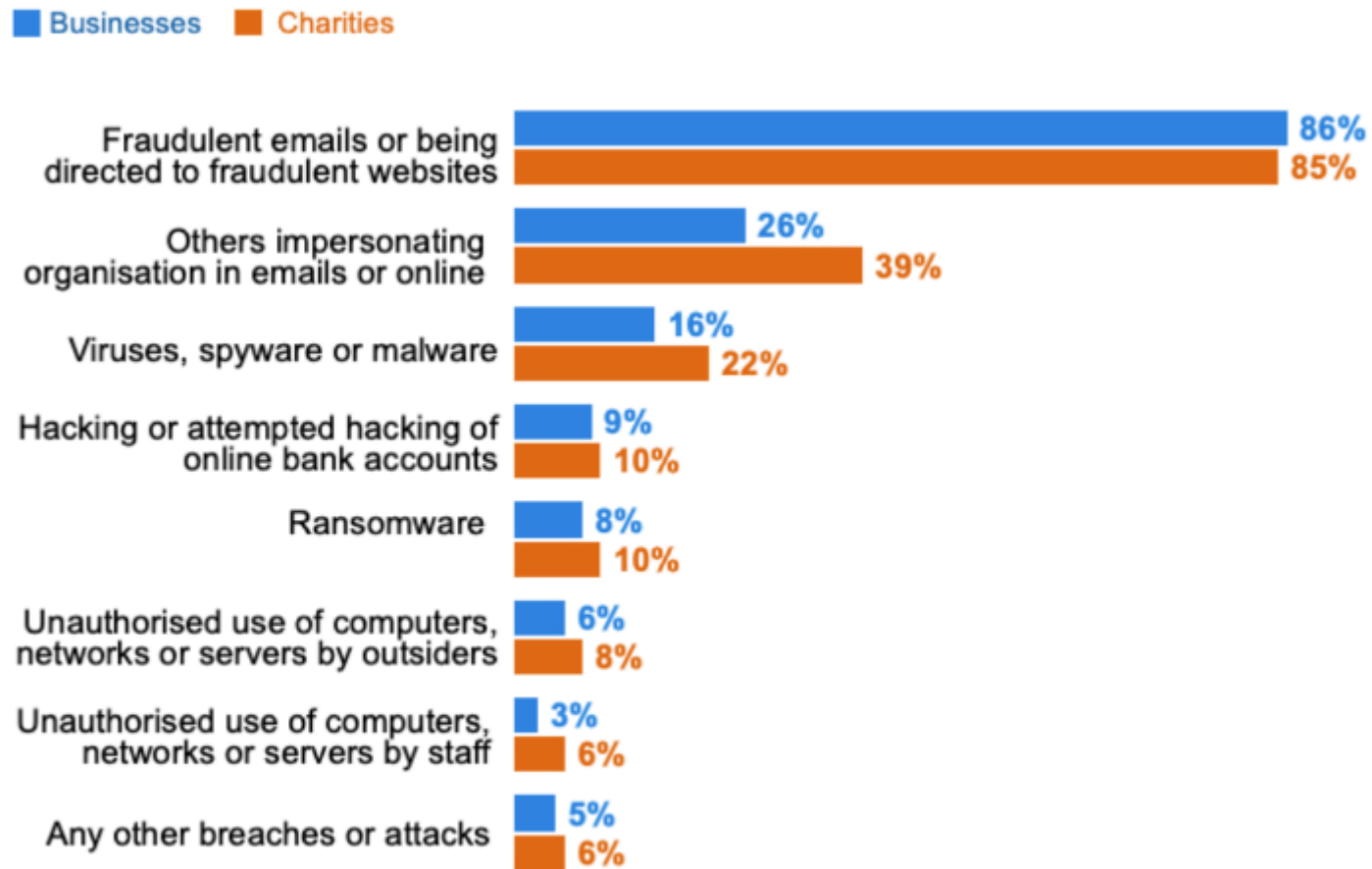
- Theft
- Use of unlicensed software
- Private work
- Virus / Denial of Service
- Accessing pornographic / inappropriate material

And since 2005...?

DLE quiz – cybercrime – 8 mins

- Mobile device malware
- Cryptojacking
- Ransomware
- Advanced Persistent Threats
- Mass exposures / data leaks
- Social network misuse
- IoT threats
- Spear phishing
- Business Email Compromise

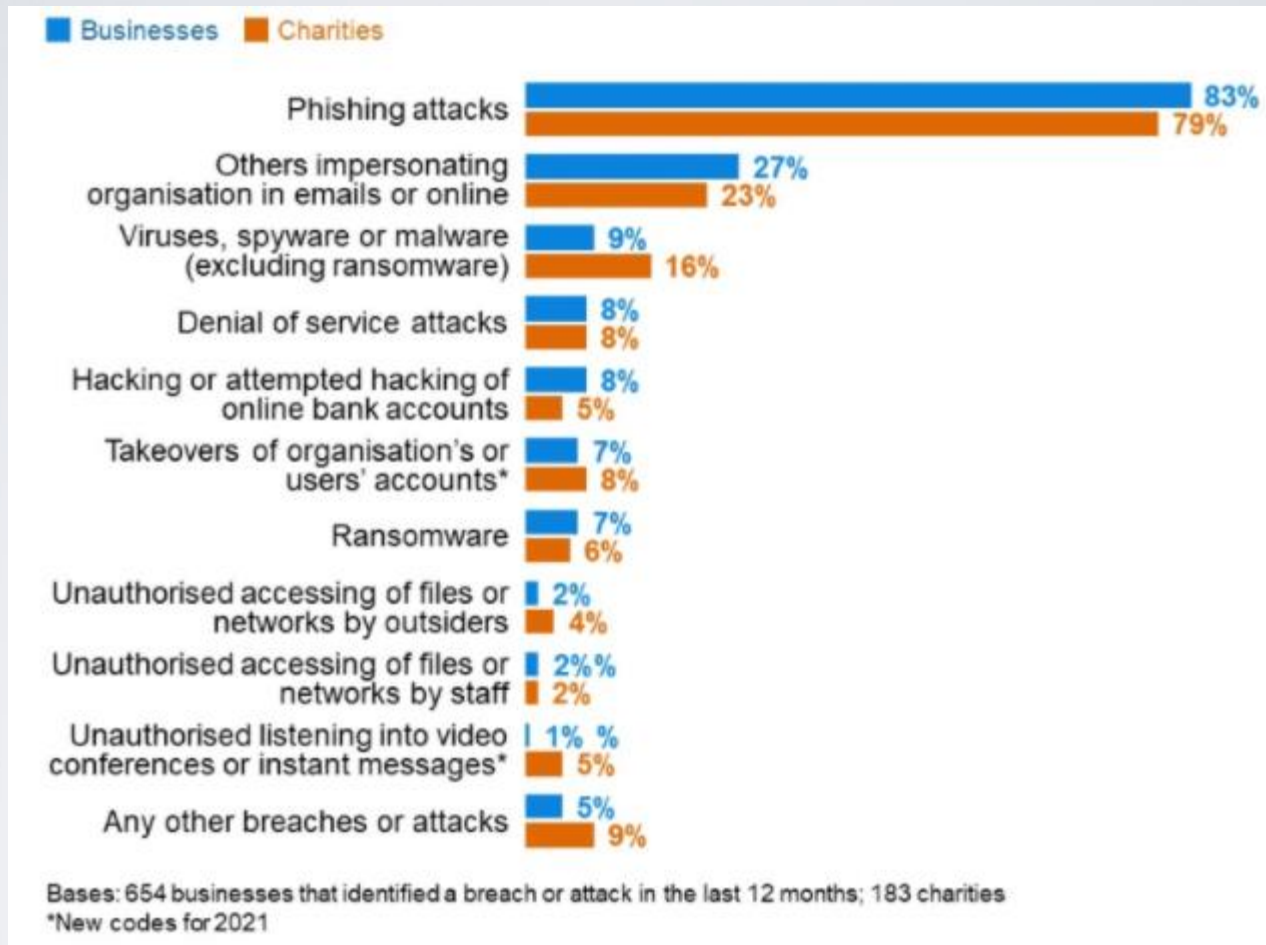
Current status



Bases: 748 businesses that identified a breach or attack in the last 12 months; 134 charities

(Cyber Security Breaches
Survey 2020)

Current status



(Cyber Security Breaches
Survey 2021)

Increasing cyber threats

“... I think that the fact I am here is also the bad news, because it indicates the level of cyber threats, it just proves that now we’re living in a different world ... These threats they don’t stay the same level, there is evolution ... Now we’re living in the era of cyber wars, cyber weapons, cyber sabotage ...”

Eugene Kaspersky

Plymouth University Graduation Speech

September 2012



Categorising Cybercrime

● Cyber-dependent crimes

- offences that can only be committed by using a computer, computer networks, or other form of ICT (Information and Communication Technology)
- include the spread of viruses and other malicious software, hacking, and DDoS attacks,
- primarily acts directed against computers or network resources, but there may be secondary outcomes (e.g. fraud)

● Cyber-enabled crimes

- traditional crimes that are increased in scale or reach by use of computers, networks or other ICT
 - **fraud** (including mass-marketing frauds, 'phishing' e-mails and other scams; online banking and e-commerce frauds);
 - **theft** (including theft of personal information and identification-related data); and
 - **sexual offending against children** (e.g. grooming, possession/creation/distribution of sexual imagery)

Lack of standardisation

Cyber-dependent Crime Categories

Information Security Breaches Survey 2014

- Actual penetration into the organisation's network
- Denial of Service attack
- Attack on Internet or telecommunications traffic

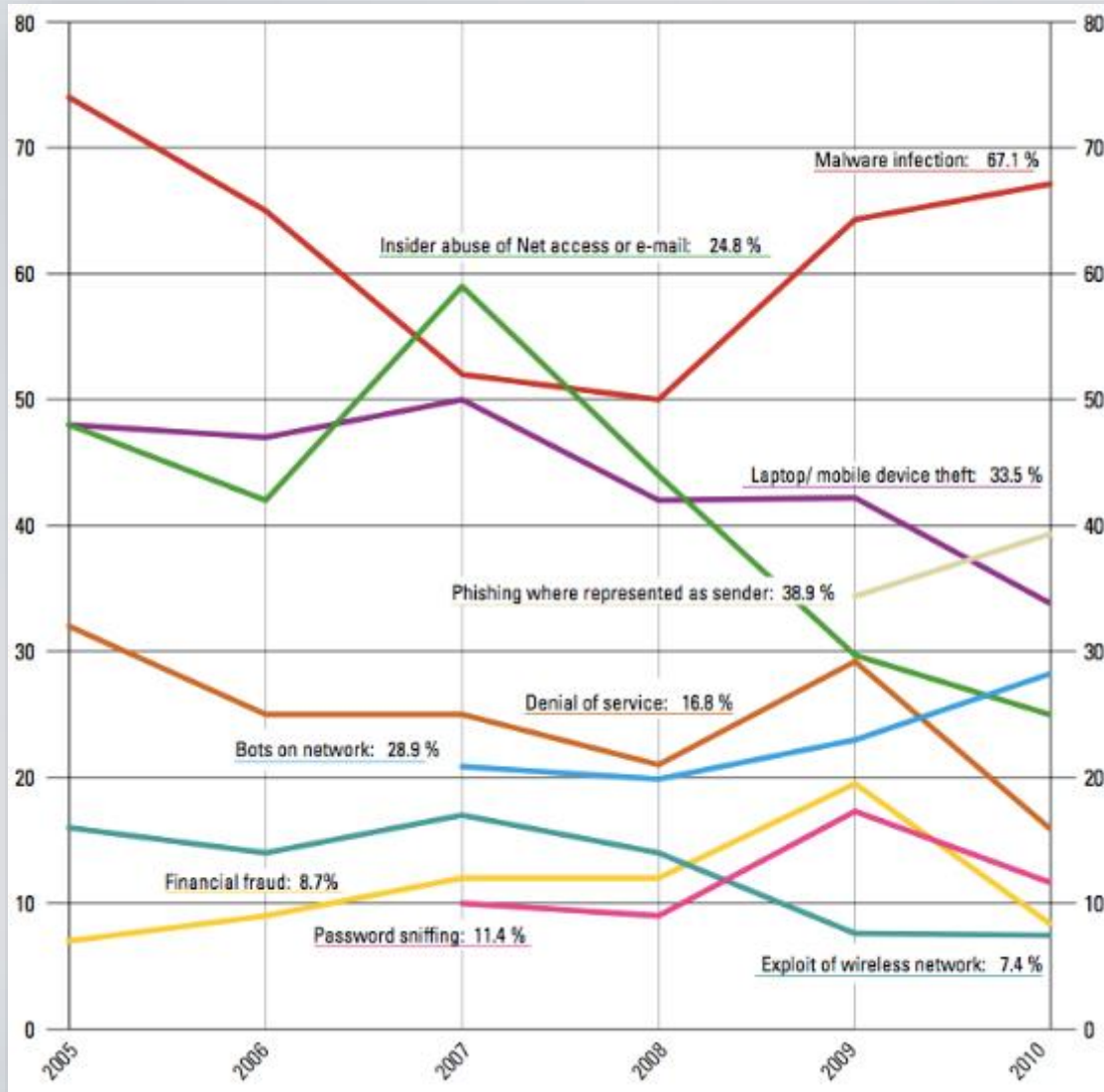
CSI 2010/11 Computer Crime and Security Survey

- Malware infection
- Bots / zombies within the organization
- Password sniffing
- Denial of Service
- Web site defacement
- Other exploit of public-facing Web site
- Exploit of wireless network
- Exploit of DNS server
- Exploit of client Web browser
- Exploit of user's social network profile
- Instant messaging abuse
- Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)
- Unauthorized access or privilege escalation by insider
- System penetration by outsider

Ernst & Young Global Information Security Survey 2014

- Cyber attacks to disrupt or deface the organization
- Cyber attacks to steal financial information (credit card numbers, bank information, etc.)
- Cyber attacks to steal intellectual property or data
- Internal attacks (e.g., by disgruntled employees)
- Malware (e.g., viruses, worms and Trojan horses)
- Zero-day attacks

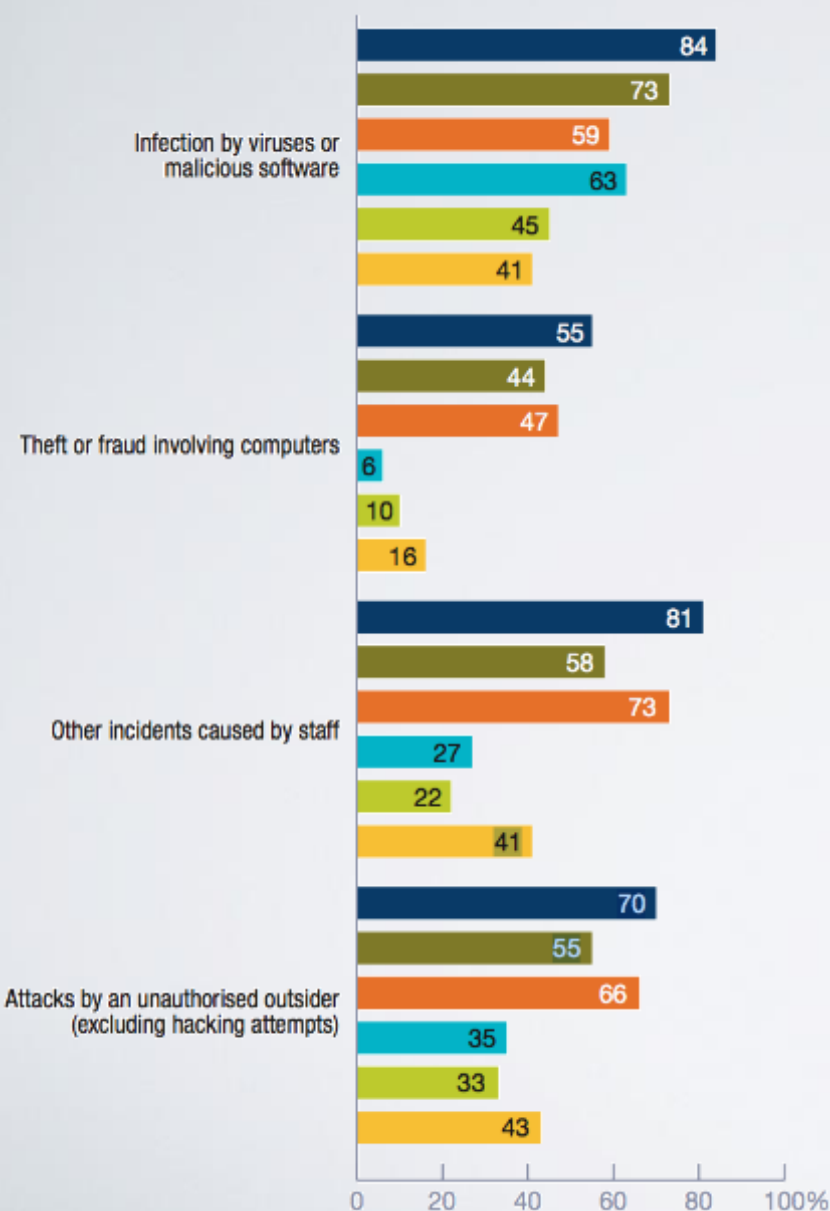
Trends for key incident types



● Responses of 148 US corporations, government agencies, financial, educational and medical institutions

(CSI Survey, 2010)

Causes and perpetrators of incidents



ISBS 2015 - large organisations



ISBS 2015 - small businesses

ISBS 2014 - large organisations



ISBS 2014 - small businesses

ISBS 2013 - large organisations



ISBS 2013 - small businesses

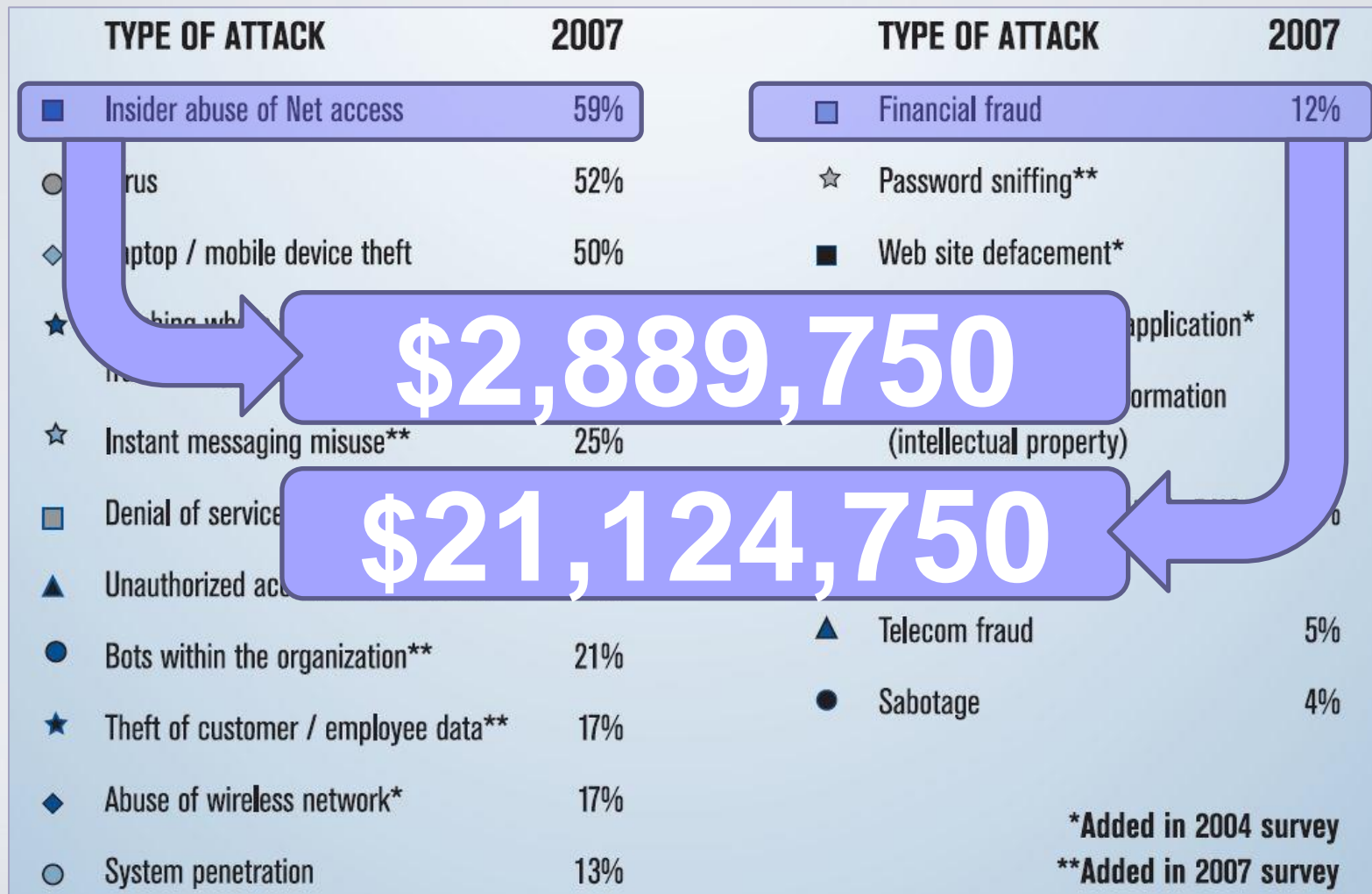
	Large organisations	Small businesses
Infection by viruses or other malicious software	3 (5)	2 (3)
Theft or fraud involving computers	2 (3)	2 (1)
Other incidents caused by staff	6 (6)	2 (3)
Attacks by an unauthorised outsider (excluding hacking attempts)	6 (11)	3 (5)
Any security incidents	14 (16)	4 (6)

Median number of breaches
(2014 figures in brackets)

(BIS ISBS, 2015)

Incidence versus Cost

CSI Computer Crime Survey (2007)



Points to note

- Figures only relate to *reported* incidents
 - It is often conjectured that the true level of computer crime remains much higher than reported
 - organisations do not wish to risk undesirable consequences such as bad publicity, legal liability, or loss of custom
- Financial loss is just one impact that may result from cybercrime
 - other impacts may be disruption to services, loss of data or damage to reputation etc
 - more difficult to quantify and may actually be more significant in many contexts

Hackers

Hackers



- Common use refers to individuals attempting and/or gaining unauthorised access to IT systems
- Distinction sometimes drawn between Hackers (explorers) and Crackers (malicious)
- Explorers or intruders?
 - “We’ re not doing any harm”

Example – The Morris Worm

- Robert Tappan Morris, a 23-year-old doctoral student from Cornell
- November 1988
- no dangerous payload
- tried and convicted of violating the 1986 Computer Fraud and Abuse Act

Source : **Computer security basics**, Rick. Lehtinen

Defining Hackers

Common Dictionary Definitions

“Someone who hacks into other people’s computer systems”

Cambridge British English Dictionary, 2013

“a person who secretly gets access to a computer system in order to get information, cause damage, etc. : a person who hacks into a computer system”

Merriam-Webster Online Dictionary, 2013

“Computer Slang:

- a. a computer enthusiast.
- b. a microcomputer user who attempts to gain unauthorized access to proprietary computer systems.”

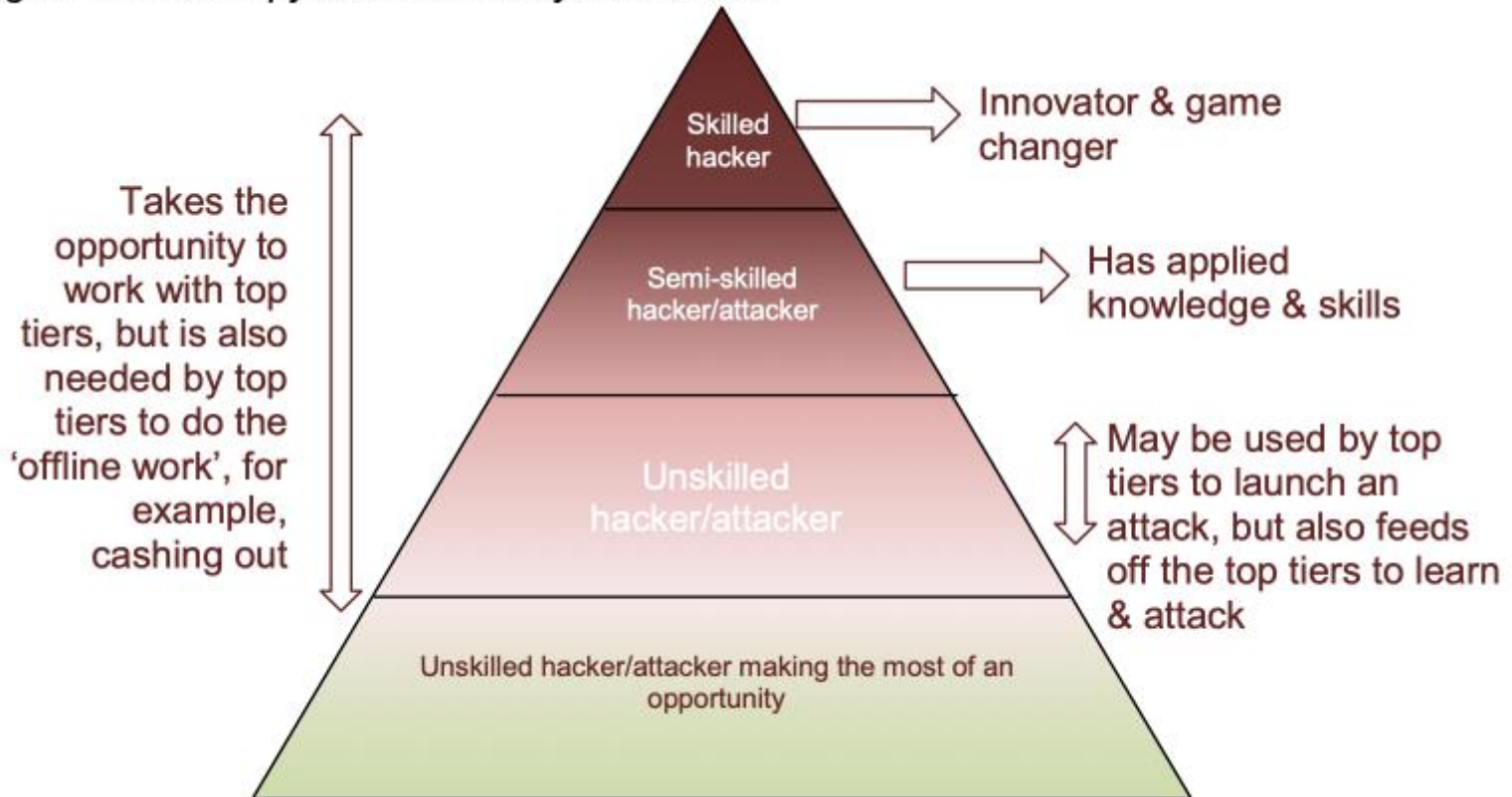
Dictionary.com, 2013

Classifying Hackers

- Calling someone a 'hacker' is like calling someone who breaks the law a 'criminal'
 - It provides a top-level label, but gives you no idea of what they have actually done
- Classifying hackers is easier said than done:
 - Some say it is simply Hacker vs Cracker
 - Others use the names Black Hat, White Hat and Grey Hat
- Many other sub-groups can be identified
 - Hacktivists, Script Kiddies, Warez D00dz etc.
 - BUT there is no definitive overall list

Categories by skill levels

Figure 1.7: Skills pyramid for the cyber attacker



Source: Holt (2013)

Why do people hack?



- Egotism
- Espionage
- Ideology
- Intellectual challenge
- Mischief / Fun
- Money
- Revenge

Classify the attackers

Group

Identify the following information about John Draper, Kevin Poulsen, Kevin Mitnick, Gary McKinnon

- Skill level (according to the pyramid)
- Motivation
- Type of hacker
- What did they do?
- What were they charged?

Notable Hackers

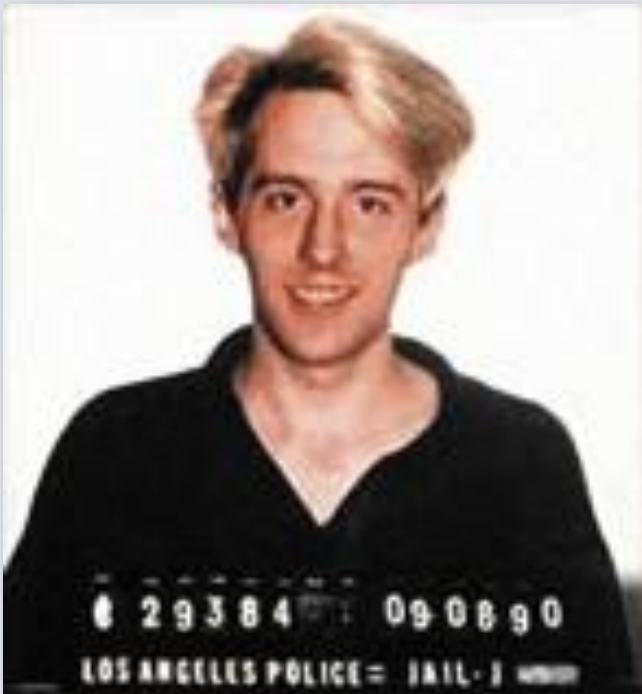
John Draper



- Better known as Cap'n Crunch aka John Draper
- Early 1970s phone phreaker
 - Blue Boxes, toy whistles, an Esquire article and prison!
- Later wrote EasyWriter wordprocessor for the Apple II and later the IBM PC

Notable Hackers

Kevin Poulsen



- Active in the 1980s/early 90s under the handle of 'Dark Dante'
 - Hacked into radio shows to win prizes (e.g. a Hawaiian holiday and a \$50,000 Porsche!)
- Suspected of espionage (charges dropped)
- Jailed for 51 months and fined \$56,000
- Subsequently a senior editor at Wired.com

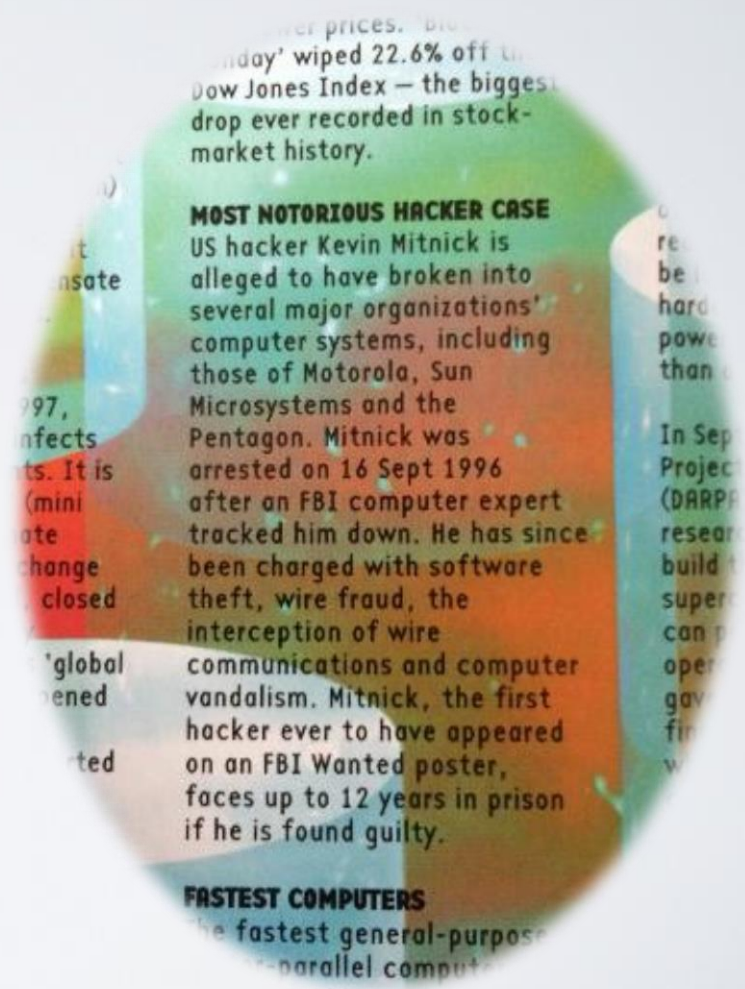
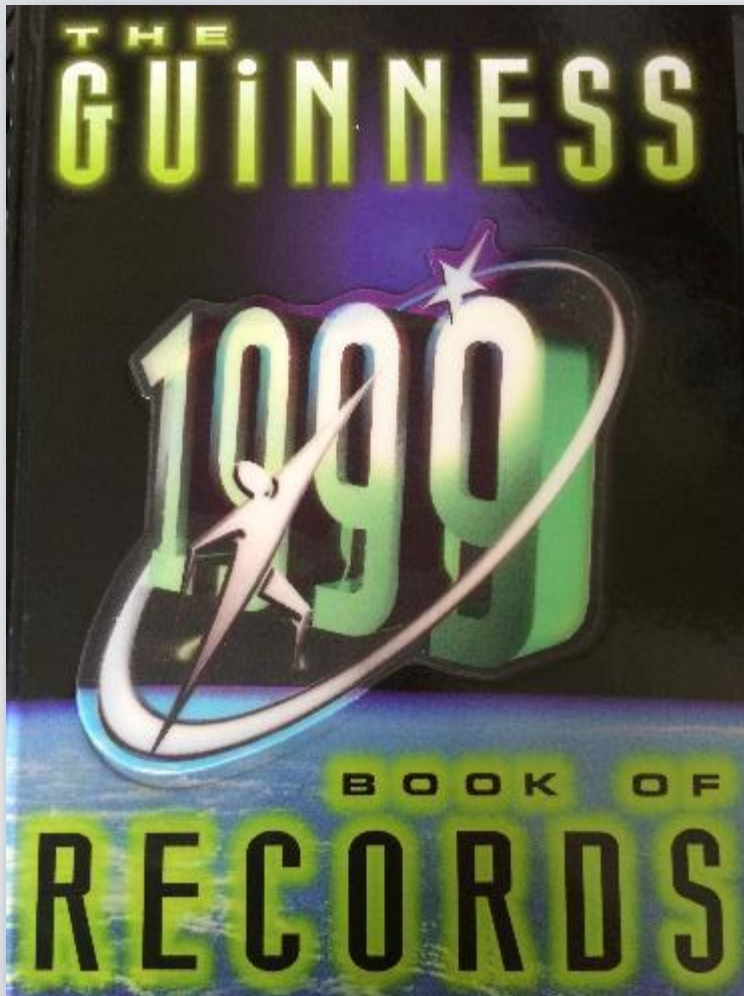
Notable Hackers

Kevin Mitnick

- Probably the best known example
- “America's Most Wanted Computer Outlaw”
- The subject of 4 books and one Hollywood film
- Entry in *1999 Guinness Book of World Records*: ‘Most Notorious Hacker Case’



Mitnick the 'Record Breaker' ...

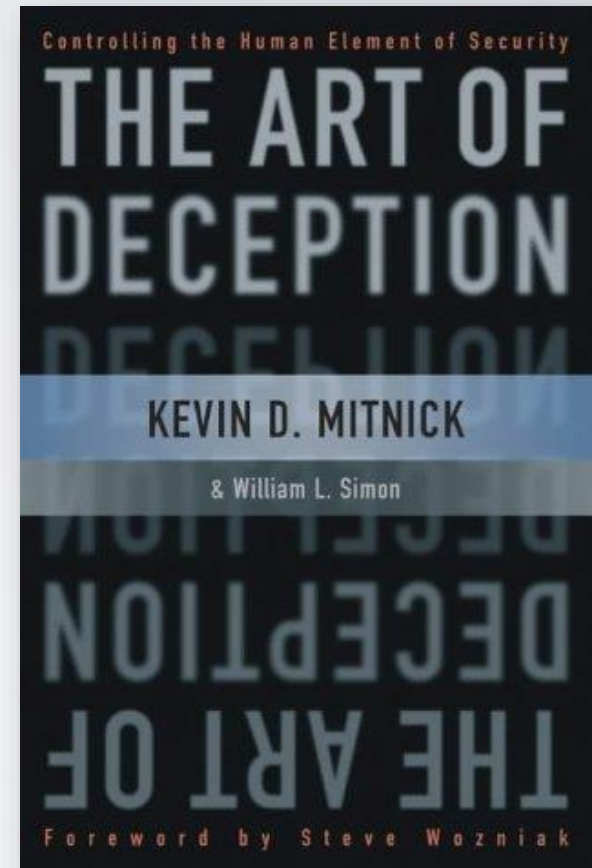


The Mitnick Timeline

- **1981** –Physical break-in at Pacific Bell's COSMOS phone centre.
- **1983** – Use of computer at University of Southern California to gain illegal access to the ARPANET.
- **1984** – Arrest warrant issued for running unauthorised TRW credit reference checks.
- **1987** – Convicted of stealing software from Santa Cruz Operation.
- **1989** – Repeated unauthorised entries into systems at DEC's Palo Alto research lab in 1987/88. Sentenced to one year in prison

The Mitnick Timeline

- **1992** - Violated probation and went underground. Accused of stealing software from Motorola, Nokia and Sun, among others.
- **1994** –Stole software, email and other files from a system belonging to Tsutomu Shimomura.
- **1995** – Arrested in North Carolina, after over 2 years on the run.
- Left prison in **January 2000** and published 'The Art of Deception' in **October 2002**.



Kevin Mitnick

Pre- and post-prison quotes

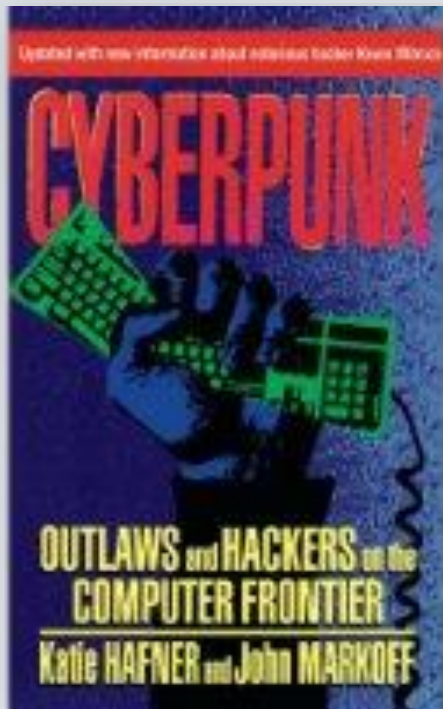


- *“I saw myself as an electronic joy rider . . . I was like James Bond behind the computer. I was just having a blast . . . I was an accomplished trespasser. I don’t consider myself a thief”.*

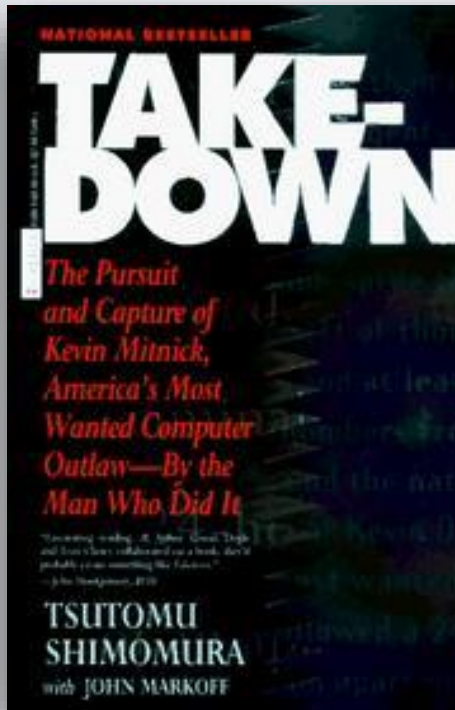


- *“I do want to make a public apology . . . My past actions have invaded their privacy by getting into machines and getting into their code, and I do regret doing that stuff because it’s wrong to do”.*

The Mitnick Story



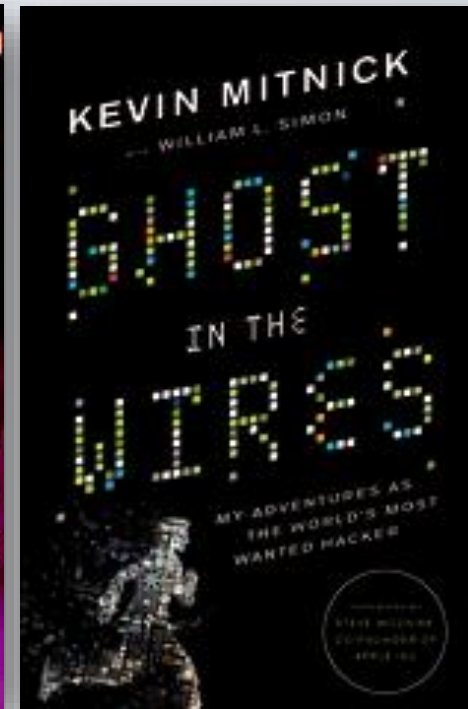
1991



1995



1996



2011

Notable Hackers

Gary McKinnon



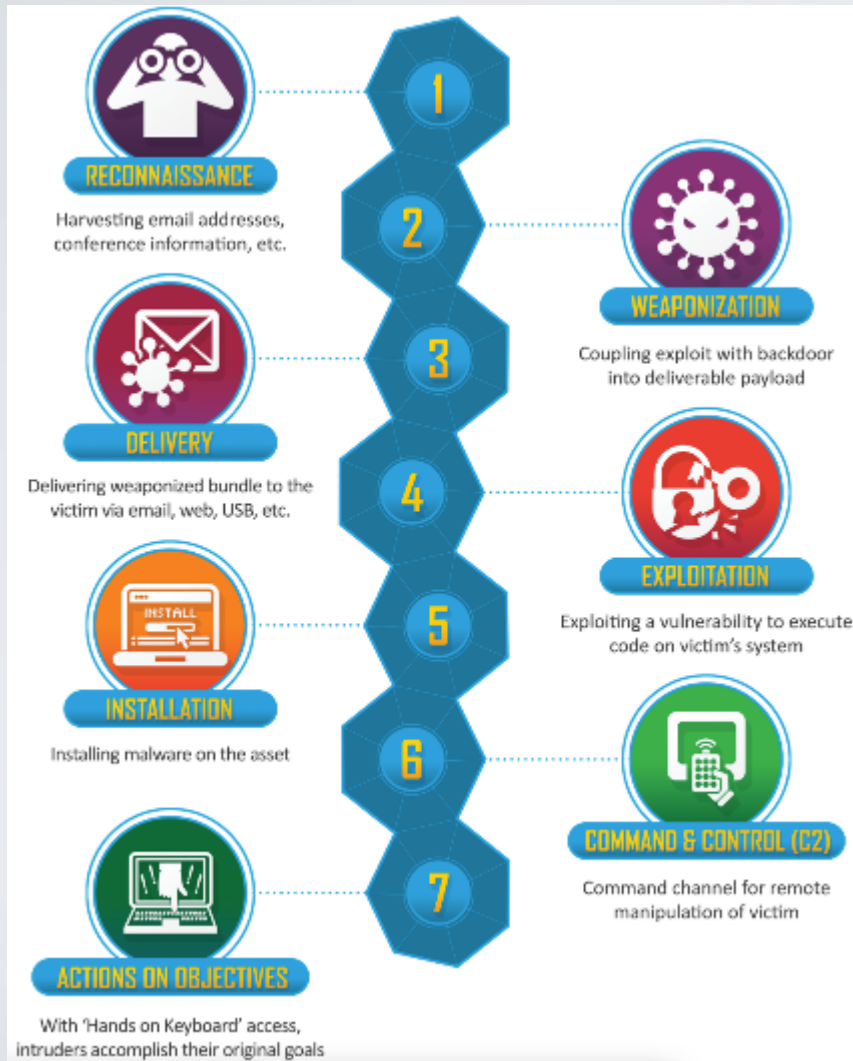
- Unemployed UK sysadmin
- Indicted by US grand jury in 2002, for hacking into over 90 systems between Feb 2001 and March 2002:
 - US Army, US Air Force, US Navy, Department of Defense, and NASA
 - Estimated damage in the region of \$900,000
- Used automated vulnerability scanning to identify unpatched Windows NT flaws

The McKinnon case

An example target

- Earle Naval Weapons Station
 - responsible for replenishing munitions supplies to the US Atlantic fleet
- Attacked three times between April and September 2001
- final attack (on 23/9/2001 ... 2 weeks after 9/11)
 - shut down the entire network of 300 machines after deletion of key system files
 - system outage for a week, and unable to send/receive external email for a further 3 weeks
- October 2012 - Home Secretary blocks extradition

Cyber Kill Chain



- Developed to aid security professionals in identifying the steps adversaries will follow
- Based upon techniques/concepts of military kill chains

Apply cyber kill chain (1)

● Menti

● You are working in the security team in company A. Your team receives two alerts:

- a) an event produced from a Network Intrusion Detection System (NIDS)
- b) an event from a Host Intrusion Prevention System (HIPS)

Which would you prioritize to deal first and why?

Apply cyber kill chain (2)

(Menti)The below graph showing each stage of the process on one axis and the countermeasure along the other can then identify the tool in place to perform the mitigation at that stage in the box where each intersects. An empty box indicates gaps where investments can be made to further enhance the organization's protections.

Which would you prioritize to invest and why?

		Detect	Deny	Disrupt	Degrade	Deceive
1	Reconnaissance	Web analytics	Firewall ACL			
2	Weaponization	NIDS	NIPS			
3	Delivery	Vigilant User	Proxy filter	Inline AV	(a)	
4	Exploitation	HIDS	Vendor Patch	EMET, DEP		
5	Installation	HIDS		AV		
6	Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect
7	Actions on Objectives	(b)			Quality of Service throttle	Honeypot

Malware

Malware

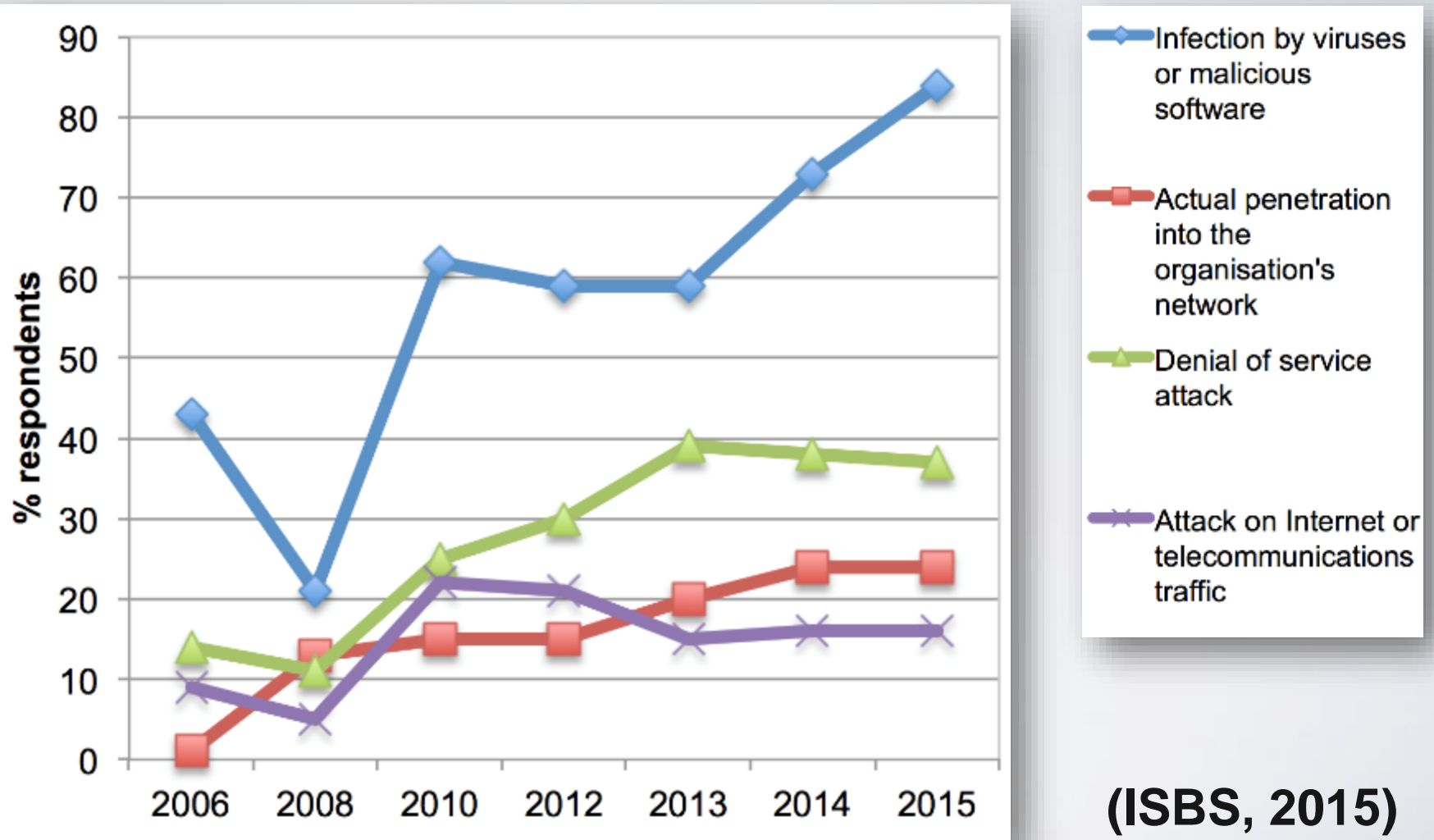
- A long-standing problem, growing in scale, sophistication and routes
- Kaspersky Lab reported identifying 360,000 new malicious files per day in 2020
 - an increase of 125,000 per day compared to 2012

(Source: Kaspersky Lab, Dec 2014)

 - in 2008, we talked of 8,000 new strains per month
- Commonly reaches, and targets, end-users



Historically a top threat



Types of Malware



- **Virus**

A *non-autonomous* program that replicates and spreads itself by infecting systems, programs or files.

- **Worm**

Code that is able to replicate and spread *autonomously* through systems and networks.

- **Trojan horse**

A program containing unexpected hidden functionality, potentially operating alongside expected behaviour

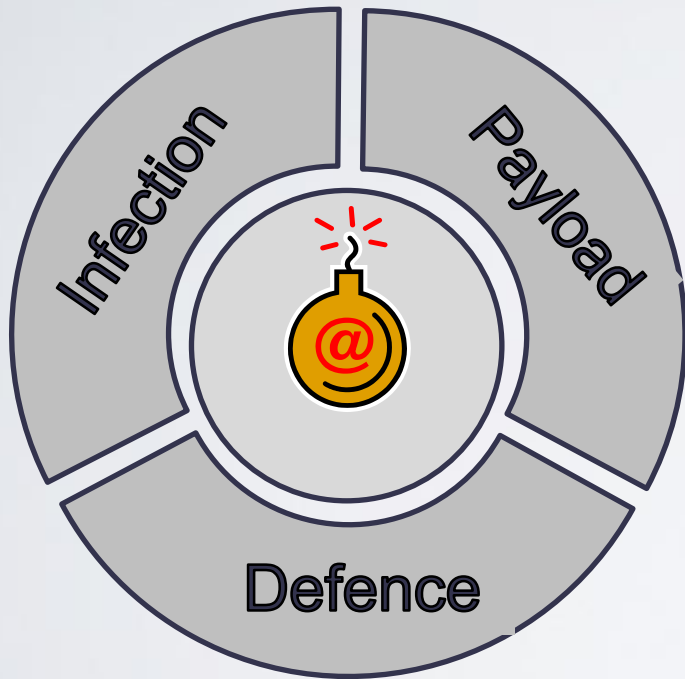
- **Spyware**

Parasitic software that invades users' privacy by gathering information

Characteristics

Virus	Worm
A virus infects a system by inserting itself into a file or executable program	A worm infects a system by exploiting a vulnerability
It might delete or alter files or change the location of files in the system	Typically, does not modify any stored programs, it exploits the CPU and memory
It alters a computer system without knowledge or consent of a user	It consumes network bandwidth, system memory – possibly consequence of DoS
A virus cannot spread to other computers without manual intervention	A work can replicate itself and spread across a network
A virus spreads at a uniform rate as programmed	A worm spreads more rapidly than a virus
Viruses are difficult to remove from infected machines	Compared with a virus, a worm can be removed easily

Dimensions of malware behaviour



● Infection

- reflects how and where users are likely to come into contact with malware

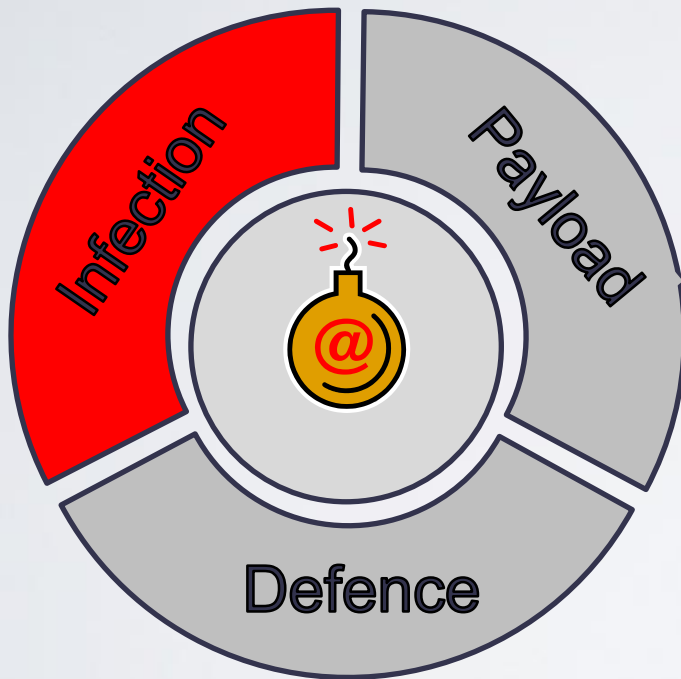
● Payload

- Determines what the malware will actually *do* and represents the most variable (least predictable) aspect of behaviour

● Defence

- The ability of the malware to ability to safeguard itself against detection and removal

Infection vectors



- Email attachments
- Instant messaging
- Peer-to-peer file sharing
- Exploitation of unpatched vulnerabilities
- Compromised websites (drive-by downloads)
- Removable media

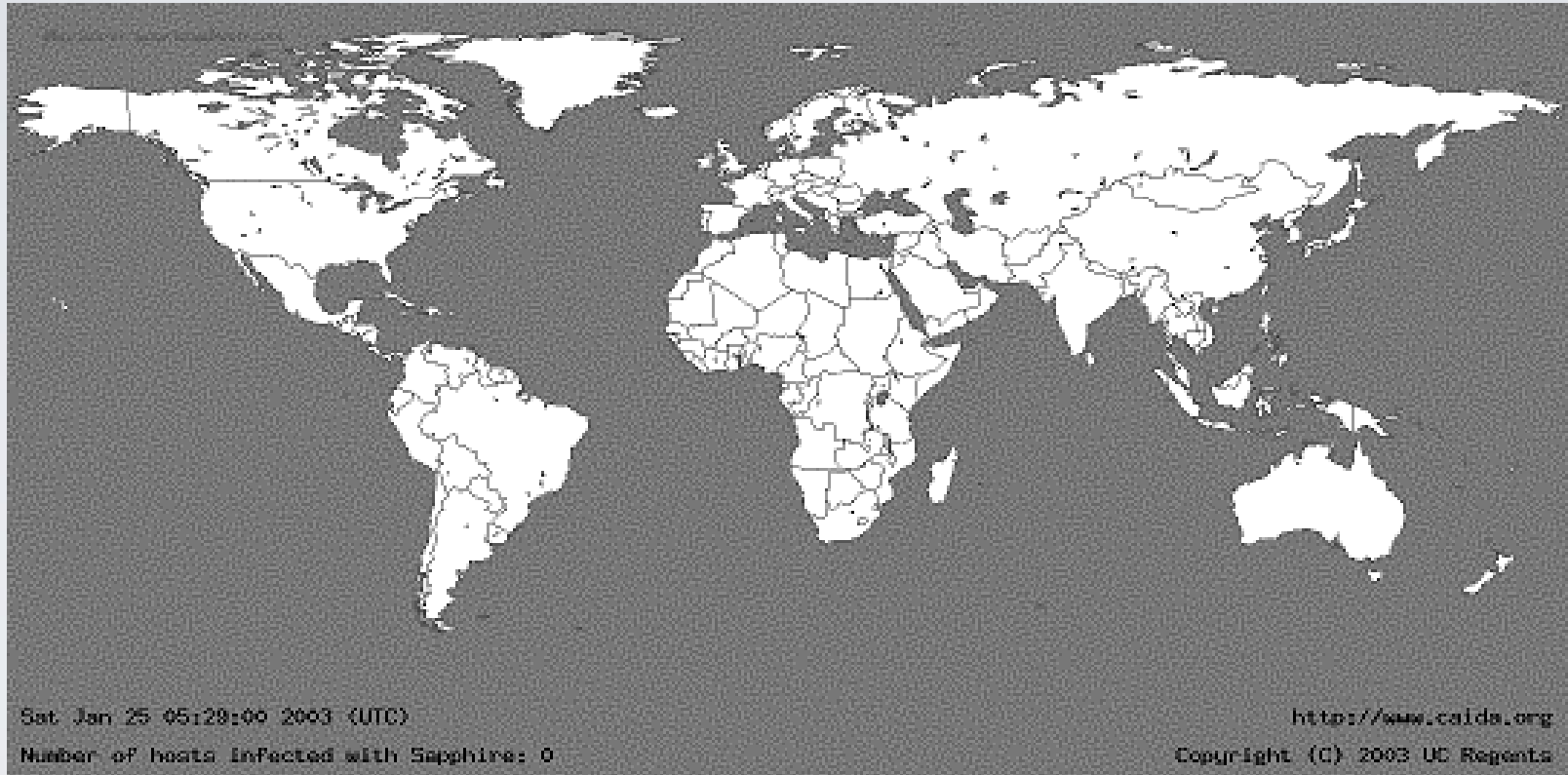
Malware	Year	Injection Technique	Propagation Techniques
StormWorm	2007–2008	Email attachments/ File execution	File dropper Overwrite/deletion P2P C2 structure and Fast Flux communication chaining
AutoIT	2008	File execution	Copies generated onto removable drives by overwriting the autorun.inf
Downadup	2009	File execution	File transfer, file sharing, copying itself across network shares or shares with weak passwords
Bacterialoh	2009	File execution (P2P network-based)	Disguised as a crack utility that a user downloads and executes locally
Koobface	2009	Client-side exploit	Spread through social networking sites with a loaded URL linked to the malware through sites such as Facebook, MySpace, Friendster, and LiveJournal

Less reliance upon users

- Early 1990s** Relied upon people to exchange disks between systems, to spread boot sector and file viruses
- Mid 1990s** A move towards macro viruses, which enabled the malware to be embedded in files that users were more likely to exchange with each other
- Late 1990s** The appearance of automated mass mailing functionality, removing the reliance upon users to manually send infected files
- Early 2000s** Avoiding the need to dupe the user into opening an infected email attachment, by exploiting vulnerabilities that enable infection without user intervention

Slammer worm (2003)

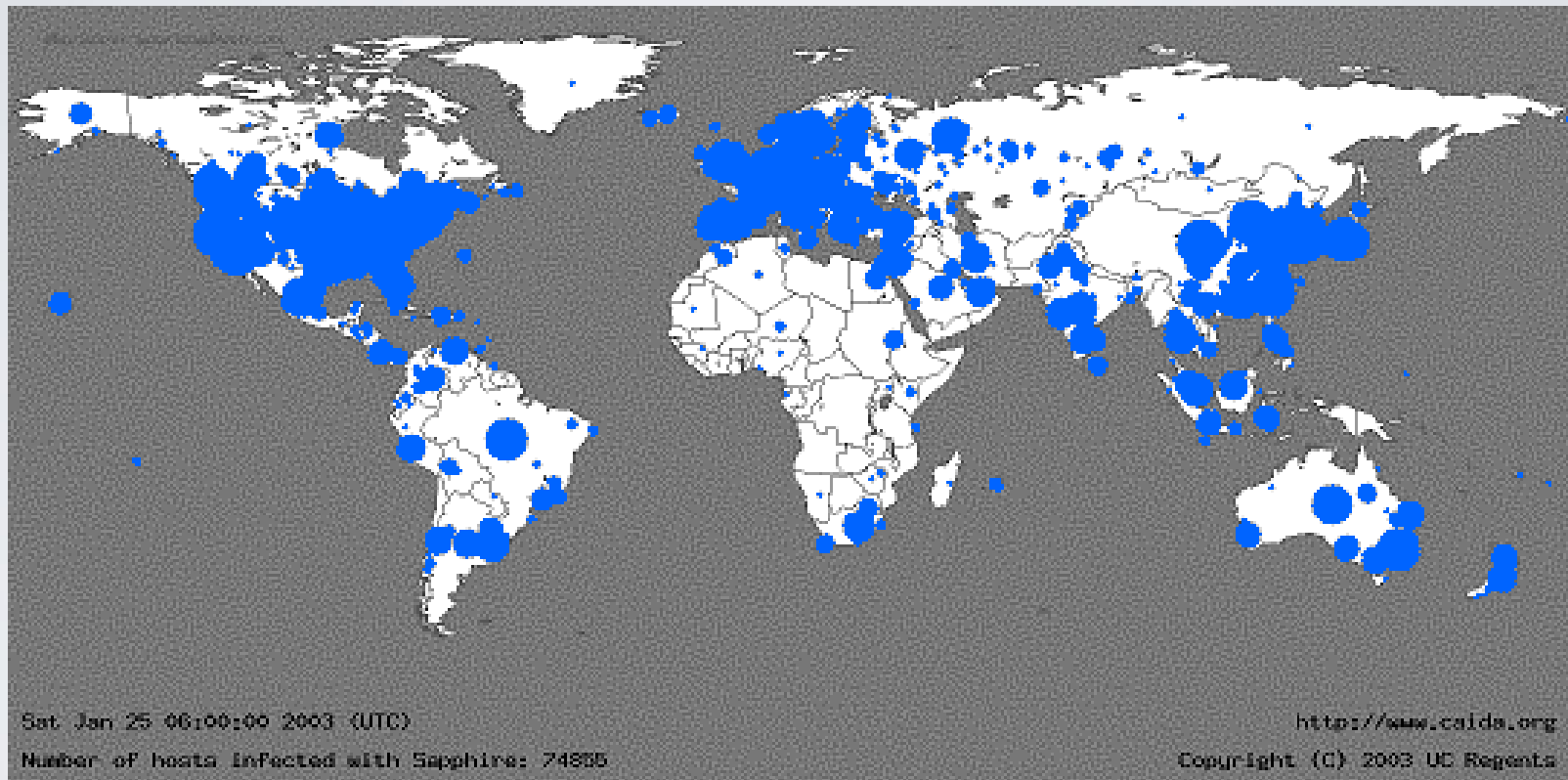
Before release ...



25 Jan 2003 - 05:29:00 / 0 victims

Slammer infections

... 31 Minutes Later



25 Jan 2003 - 06:00:00 / 74,855 victims

14 years later . . .



SC Media UK 
@SCmagazineUK

SQL sequel: Sequel Slammer worm
resurfaces after more than a decade



SQL Sequel: Sequel Slammer worm resurfaces
after more than a decade
scmagazineuk.com

08/02/2017, 17:01

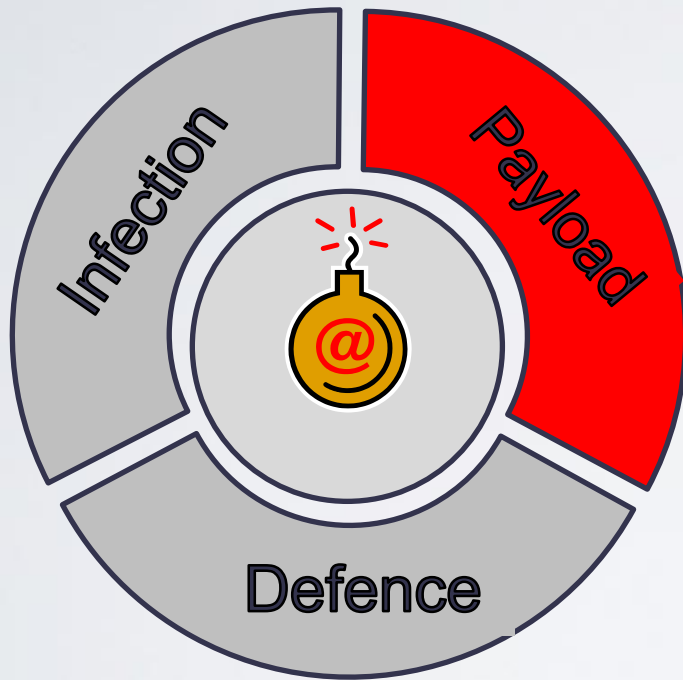
"One theory to why it's attempting to make a comeback is that cybercriminals are seeking easy ways to cause DoS and slow down the entire Internet, just like with the recent Mirai botnet ... And reusing old malware is the easiest way"

Maya Horowitz

Group manager, Threat
Intelligence at Check Point

Source: www.scmagazineuk.com/sql-sequel-sequel-slammer-worm-resurfaces-after-more-than-a-decade/article/636251/

Payload actions



- Damaging systems
 - Damaging and deleting files
 - Corrupting the BIOS
- Stealing information
 - Copying files
 - Keylogging
- Hijacking systems
 - Opening backdoors
 - Remote control (Botnets)

Back in the old days ...

- Many early viruses were more of a nuisance than actually harmful

```
CLINT    WAU      32300 07.05.93    20.25
WHIP     WAU      6806 23.04.92     2.01
POP      WAU      4486 05.11.91     4.50
SYSINI   WRI     58496 01.10.92     7.11
PRINTERS WRI     37760 01.10.92     7.11
WININI   WRI     23168 01.10.92     7.11
NETWORKS WRI     22528 01.10.92     7.11
EXCEL    XLB       267 26.08.93    16.15
F-EXCEL  ~EX     32352 03.12.93    17.31
F-COREL  ~EX     32736 01.10.92     7.11
F-WORD   ~EX     32736 01.10.92     7.11
F-AMIPRO ~EX     32352 03.12.93    17.31
F-WP     ~EX     32352 03.12.93    17.31
GDW      SCR    489888 08.06.93    13.20
GDWREAD  TXT      4667 17.08.93    14.19
F-PROT   BAK       454 11.01.94    13.28
MOSAIC   <DIR>      20.01.94    19.22
MOSAIC   BAK     10691 11.11.93    15.32
MOSAIC   INI     10683 20.01.94    19.50
APPLICA0 GRP      4693 23.01.94    15.33
```



The Ambulance virus (1990)

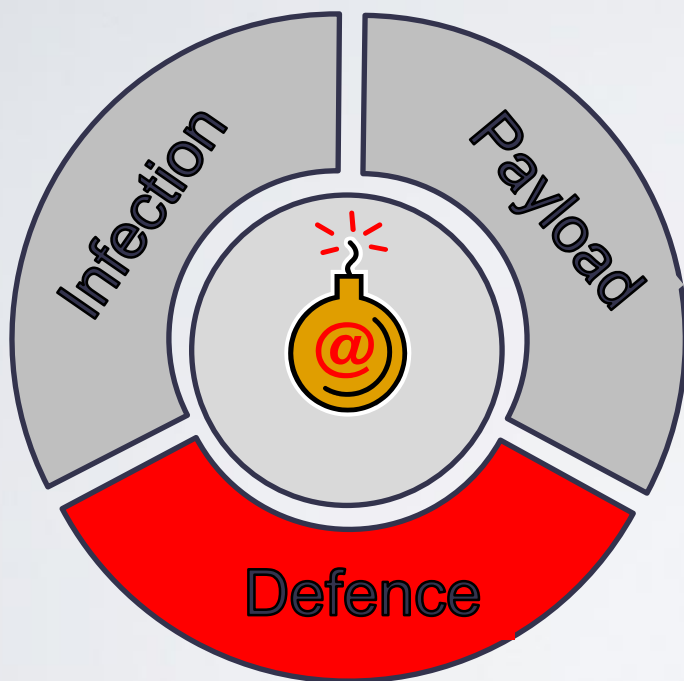
More recently . . .

● WannaCry (May 2017)

- Also known as WannaCrypt or WanaCrypt0r
- An example of Crypto Ransomware
- Infection of 200,000 computers across 150 countries
- Notable victim was the UK National Health Service, due to continued use of unsupported (and hence unpatched) Windows XP

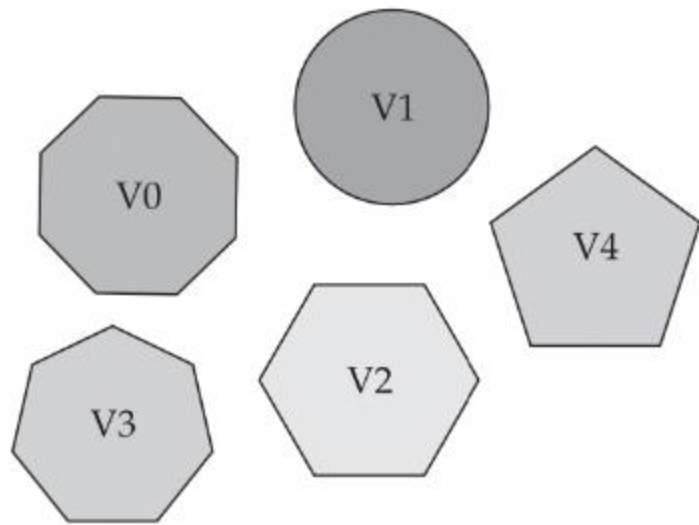


Defences

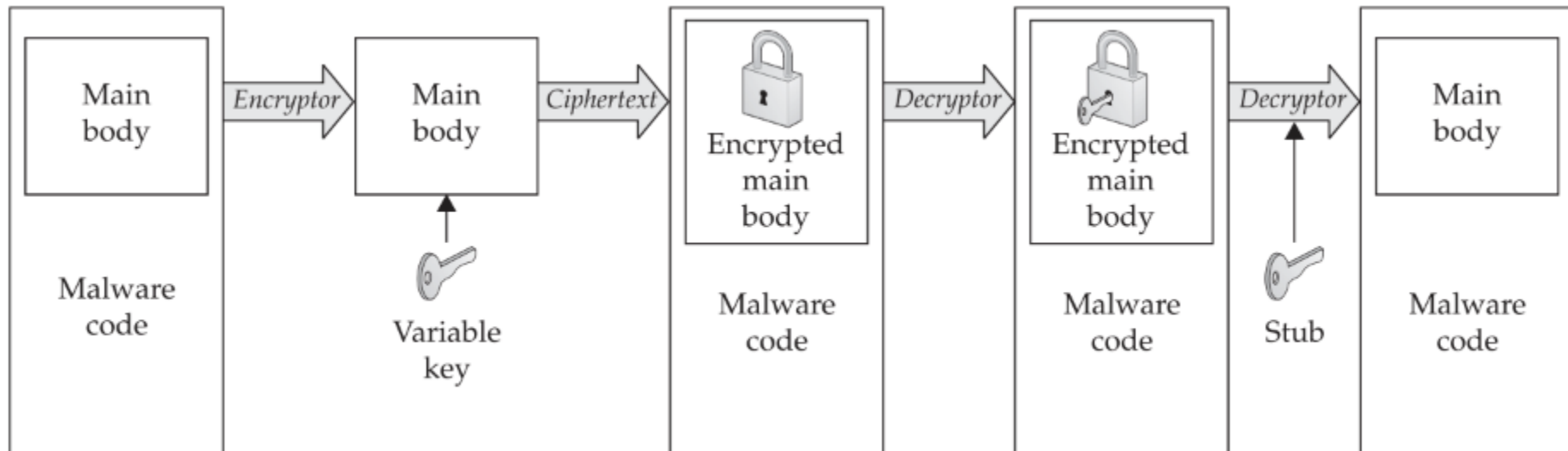


- Passive techniques (hiding)
 - Stealth techniques
 - Polymorphism and metamorphism
- Active techniques (attacking)
 - Changing system configuration so that security software no longer runs at start up
 - Blocking access to over antivirus (AV) vendors' sites to prevent updates
 - Terminating processes relating to AV and firewall processes

metamorphism



polymorphism



Evolving self-defence

- Brain virus (1986)

- intercepted any attempts to read the infected boot sector
- if anyone tried to inspect the disk, they would be presented with a copy of the original, uninfected boot sector

- Gaobot worm (2005)

- blocked access to 35 security-related sites and had a list of over 420 different processes that it tried to terminate

Evolving self-defence

- Shifu Trojan (2015)

- A banking Trojan, which affected Japanese banks and financial institutions in Aug/Sept 2015
- Based upon techniques reused from a variety of previously detected malware (e.g. Zeus, Conficker)
- Notably *included its own anti-malware module* to ward off other banking Trojans and ensure that it retains control of the compromised systems

<http://news.softpedia.com/news/shifu-banking-trojan-comes-with-its-own-antivirus-to-keep-other-malware-at-bay-490580.shtml>

Malware on the move

- Malware now commonly targets smartphones and tablets as well as desktops and laptops
- Android has proven to be a very popular malware platform due to:
 - large user base
 - unrestricted deployment of apps



Conclusions

- The range and number of cybercrime incidents is increasing
- IT is increasingly be the native environment for crime
 - New threats are likely to emerge in the future, alongside new end-user Internet services
- Malware continues to be the major category of incident for most users
 - The threat has continually evolved to target new services
 - Has spawned and sustained a whole subset of the industry
- No single solution
 - appropriate technologies **and** suitable awareness initiatives are required

Activities

1. GDPR, Cyber Threats & Adversarial Behaviours quizzes on DLE
2. Summarise the cyber threat trend in year 2022 from a report of a popular organisation (cyber security breaches survey of UK government, Risk based security, SANS,...)
3. Identify the infection, payload, defence of Wannacry
4. Find an example of the usage of Cyber Kill Chain



UNIVERSITY OF
PLYMOUTH

Dr Hai-Van Dang

hai-van.dang@plymouth.ac.uk

**Centre for Security, Communications
& Network Research**

www.plymouth.ac.uk/cscan