QUEZON CITY UNIVERSITY
COLLEGE OF COMPUTER STUDIES

WEEK 5-6

MALICIOUS ATTACKS, THREATS, AND VULNERABILITIES IMPACT AN IT INFRASTRUCTURE

IAS101 - INFORMATION ASSURANCE AND SECURITY 1
2ND SEMESTER

LEARNING OUTCOMES:

At the end of the session, the students should be able to:

- Describe how malicious attacks, threats and vulnerabilities impact an IT infrastructure
- Identify malicious code, common attacks and implement countermeasures
- Recognize social engineering and reduce risks associated with it
- Differentiate the classes of attacks

Malware (Malicious Software)

- Malware is defined as a specific set of codes or an application, specifically designed to harm and/or to gain access to a targeted computer, or spread across multiple computers; over the use of a network or a data storage device.

Image source: flickr.com, commons.wikimedia.org

Different Types of Malwares

Malware is malicious software consists of any harmful piece of program.

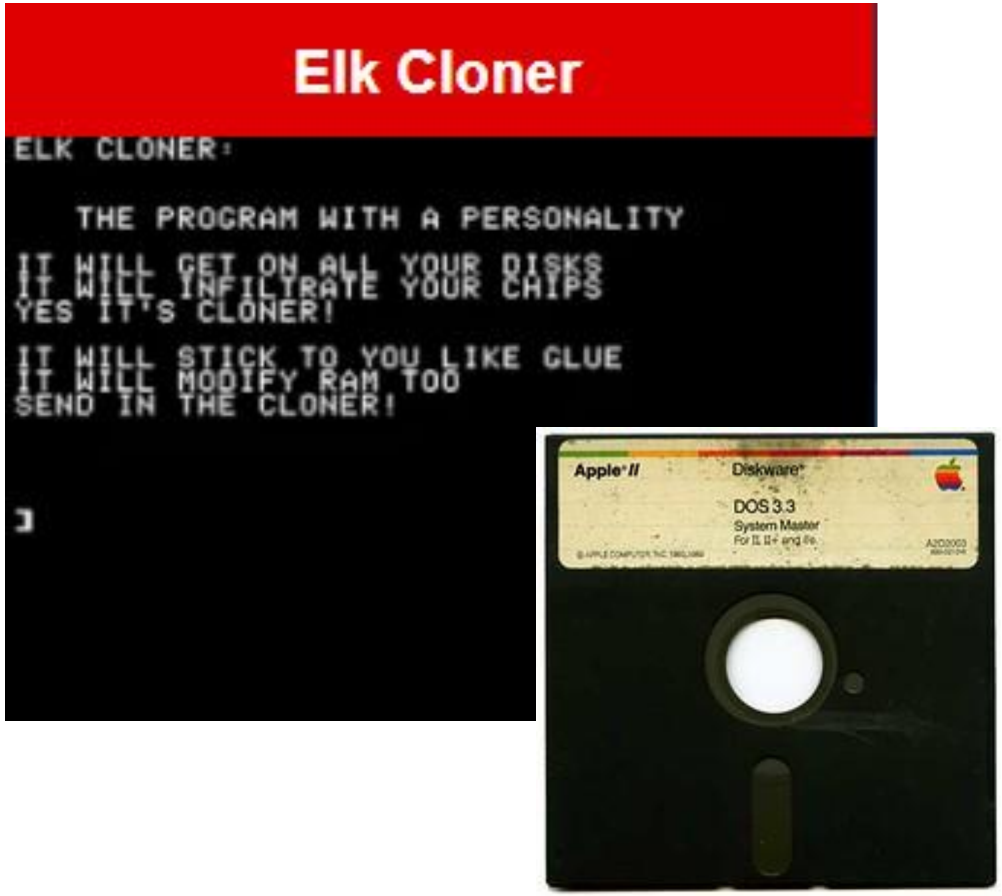
- Virus
- Worms
- Trojan Horse
- Spyware
- Bots and Botnets
- Ransomware
- Adware and Scams
- Spam and Phishing

Image source: ictworks.org

The First Malware of the World

The first malware was a virus that appeared in the realms of computer, and that virus is known as the **Elk Cloner.**

The “Elk Cloner” virus appeared on Apple Mac in 1982, and was created by Rich Skrenta from Pennsylvania, United States.



Elk Cloner

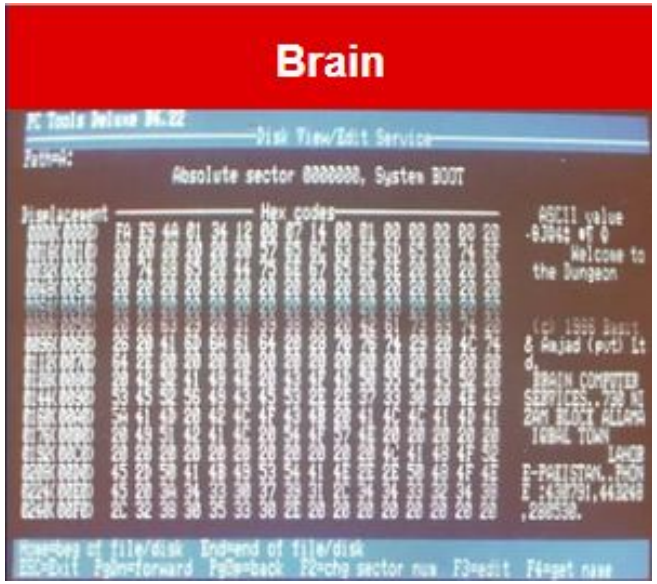
```
ELK CLONER:

   THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES IT'S CLONER!

IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM TOO
SEND IN THE CLONER!



]
```

Image source: https://malware.wikia.org/wiki/Elk_Cloner, flickr.com

First Most Damaging Virus

The **Brain Virus** was programmed by two brothers; Amid Farooq Alvi and Basit Farooq Alvi from Lahore, Pakistan in 1986.

It was the first full-stealth virus on MS-DOS. It infects 360KB-, 5.25-inch floppy disks.



Brain

```
PC Tools Deluxe R4.22
                    Disk View/Edit Service
Path=A:
            Absolute sector 0000000, System BOOT
Displacement   ---------- Hex codes ----------      ASCII value
[illegible]                                          .0J04; of 0
                                                        Welcome to
                                                      the Dungeon

                                                      (c) 1986 Basit
                                                      & Amjad (pvt) Lt
                                                      d.
                                                       BRAIN COMPUTER
                                                      SERVICES..730 N
                                                      ZAM BLOCK ALLAMA
                                                       IQBAL TOWN
                                                                 LAHOR
                                                      E-PAKISTAN..PHON
                                                      E :430791,443248
                                                      ,280530.
Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Image source: https://malware.wikia.org/wiki/Elk_Cloner, welivesecurity.com

Brief History of Malwares

- 1990 focused targeting on Colleges and Universities
- Mid 20th century started targeting businesses
- After the year 2000 target was the Internet
  - To attack or takedown websites
    - Destroying the online presence and credibility
    - Financial Theft

Image source: https://malware.wikia.org/wiki/Elk_Cloner, welivesecurity.com

Cyber Security and Cyber Crime Statistics

“ In 2019, 93.6% of malware detected was only seen on a single PC. This is the highest yearly rate we’ve ever seen, although the number has been above 90% since 2014.”

– 2020 Webroot Threat Report

Cyber Security and Cyber Crime Statistics

- Malicious hackers are bow attacking computers and networks at a rate of **one attack every 39 seconds** (University of Maryland)
- 81% of surveyed organizations were affected by a successful cyber attack in 2019 (CyberEdge Group 2020 Cyberthreat Defense Report)

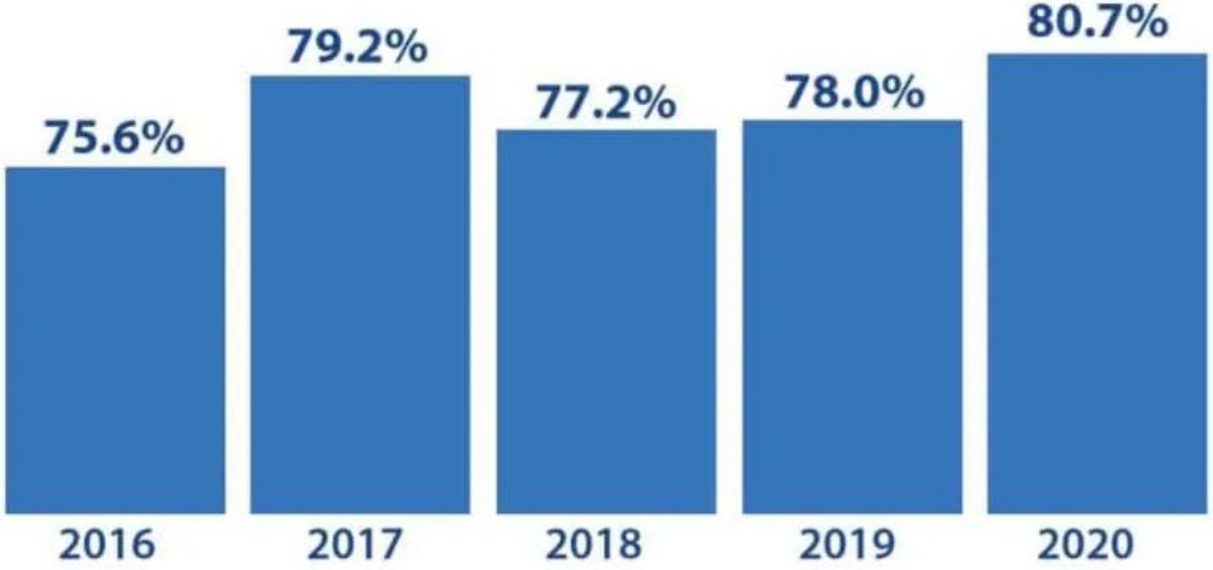
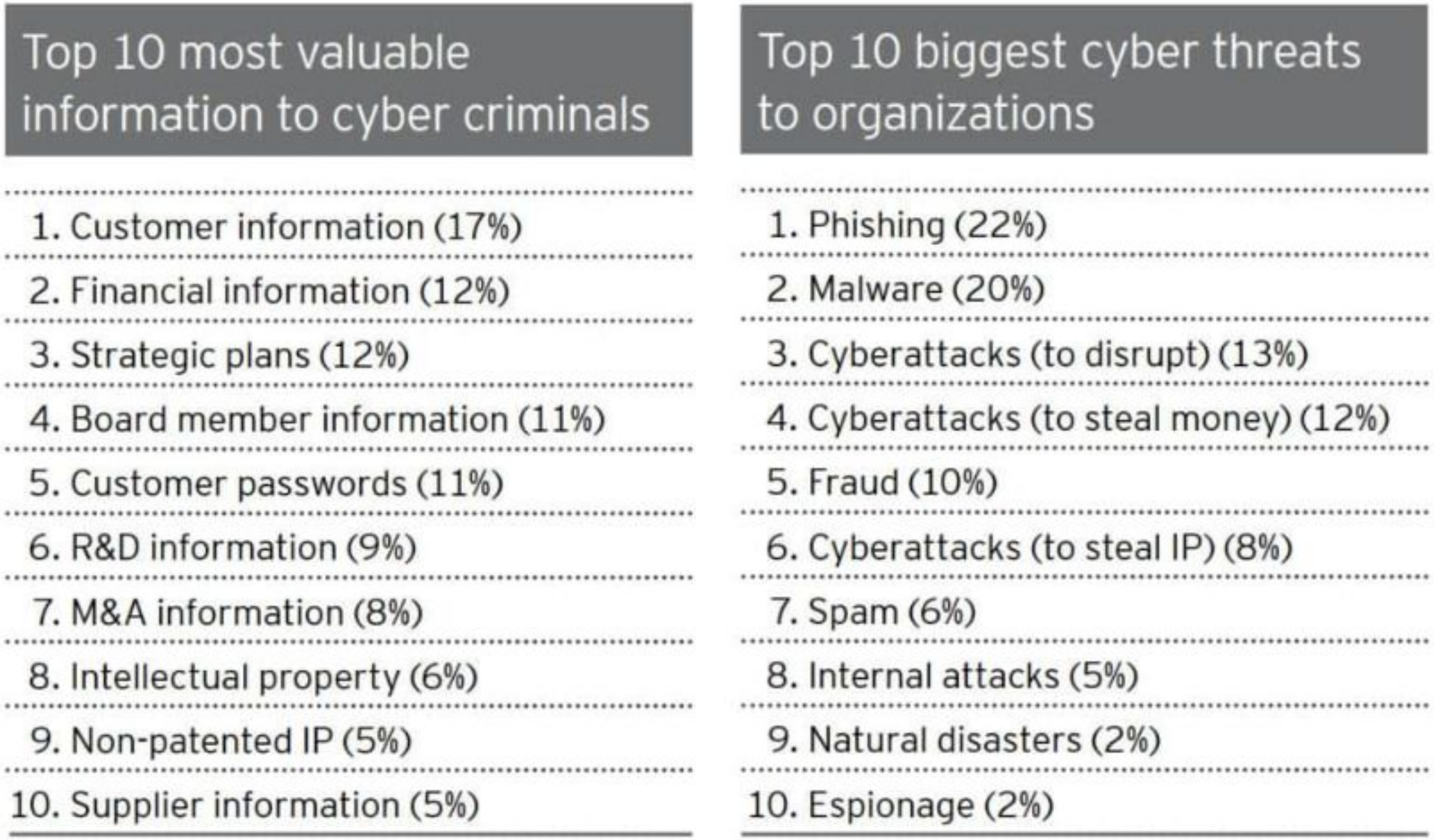


Figure: Percentage compromised by at least one successful attack, by year.

Cyber Security and Cyber Crime Statistics



Top 10 most valuable information to cyber criminals

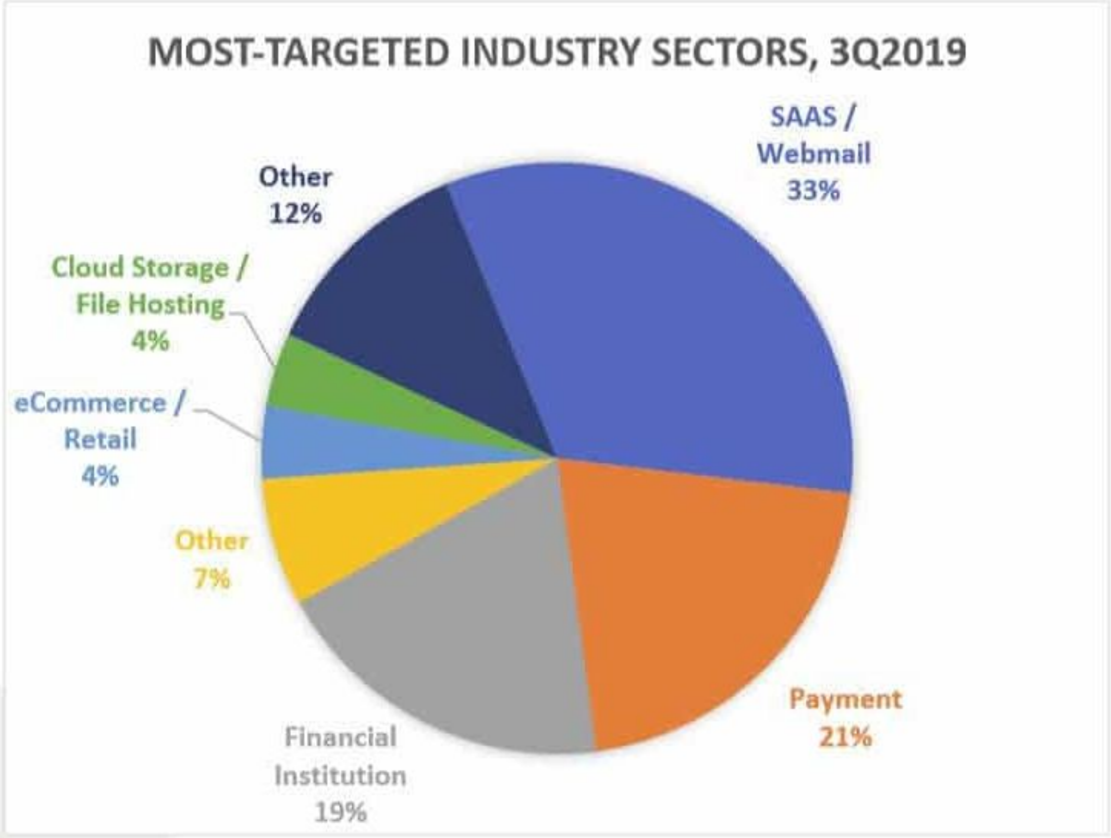
1. Customer information (17%)
2. Financial information (12%)
3. Strategic plans (12%)
4. Board member information (11%)
5. Customer passwords (11%)
6. R&D information (9%)
7. M&A information (8%)
8. Intellectual property (6%)
9. Non-patented IP (5%)
10. Supplier information (5%)

Top 10 biggest cyber threats to organizations

1. Phishing (22%)
2. Malware (20%)
3. Cyberattacks (to disrupt) (13%)
4. Cyberattacks (to steal money) (12%)
5. Fraud (10%)
6. Cyberattacks (to steal IP) (8%)
7. Spam (6%)
8. Internal attacks (5%)
9. Natural disasters (2%)
10. Espionage (2%)

Source: EY – Global Information Security Survey 2018 - 2019

Cyber Security and Cyber Crime Statistics



Source: APWG's Phishing Activity Trends Report for Q3 2019

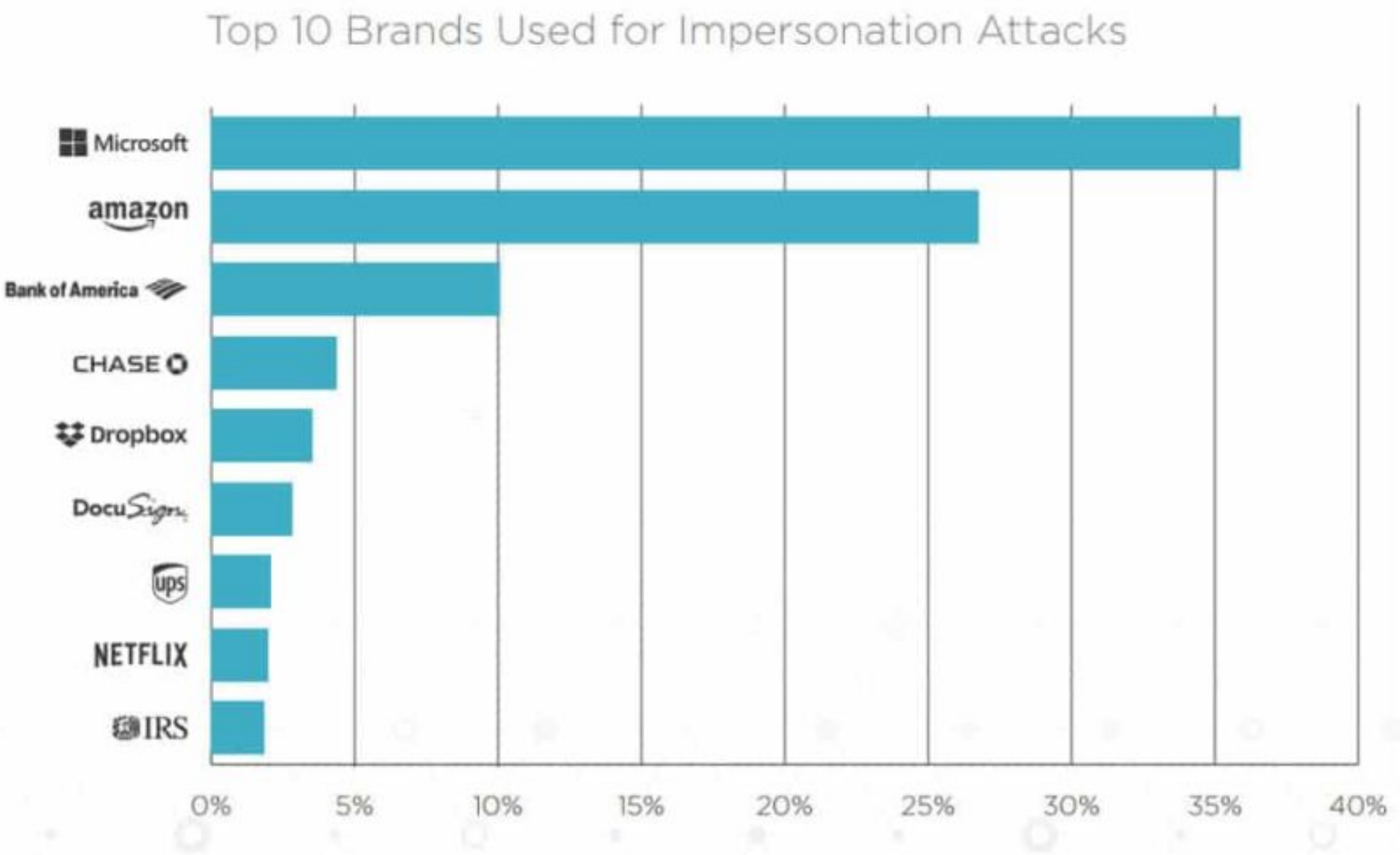
Cyber Security and Cyber Crime Statistics

“ During July 2018 through October 2018, Agari data indicates ***62% of all identity-deception based attacks leveraged display name deception*** *aimed at impersonating a trusted individual or brand – typically an outside vendor, supplier or partner”*

– Q4 2018: Email Fraud and Identify Deception Trends by Agari

Cyber Security and Cyber Crime Statistics

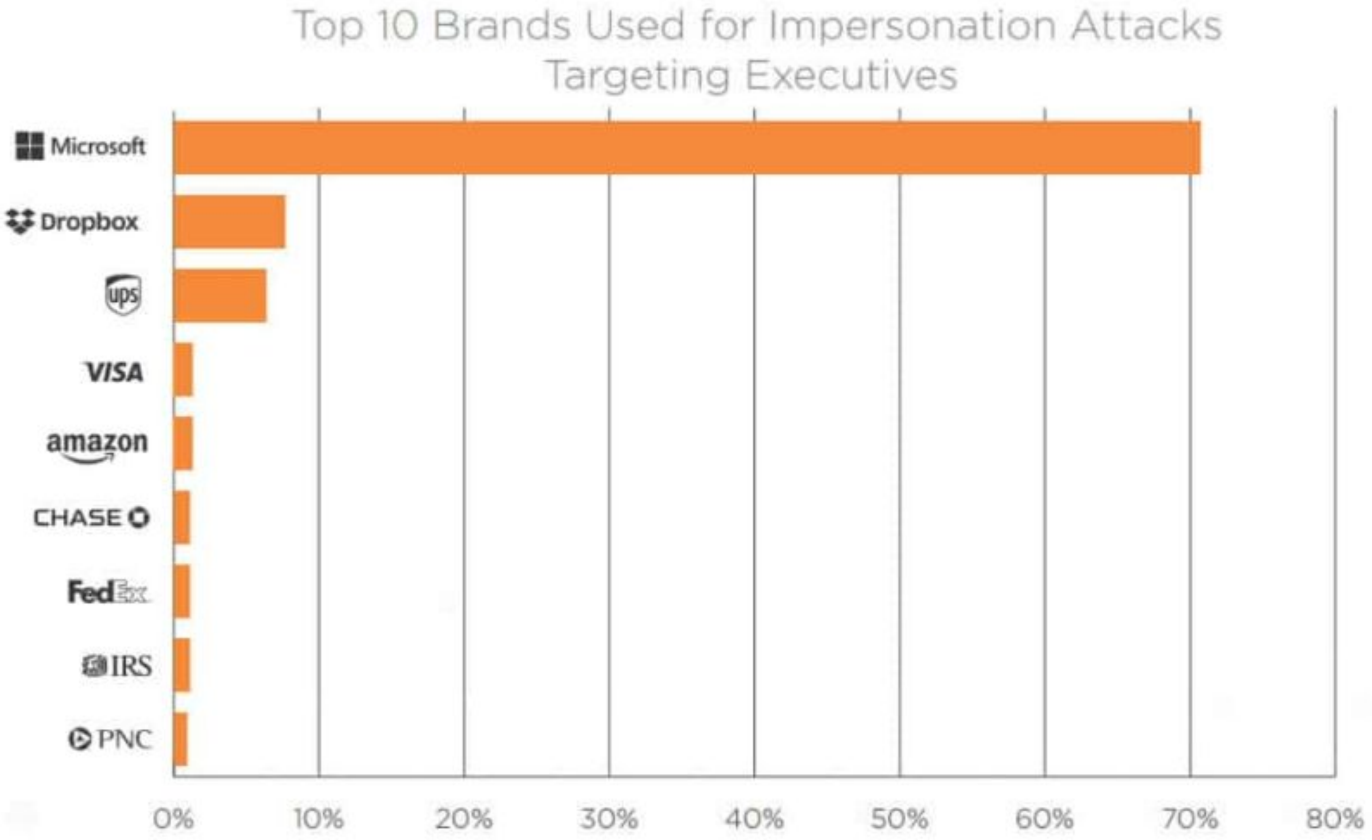
- The most frequently impersonated brands are Microsoft (35.87% of the time) and Amazon (26.79% of the time). (Q4 2018: Email Fraud and Identity Deception Trends by Agari)



Source: Q4 2018: Email Fraud and Identity Deception Trend by Agari

Cyber Security and Cyber Crime Statistics

- When it comes to fooling executives, scammers, spammers, and other bad actors leverage the trust people have in Microsoft and Dropbox.



Source: Q4 2018: Email Fraud and Identity Deception Trend by Agari

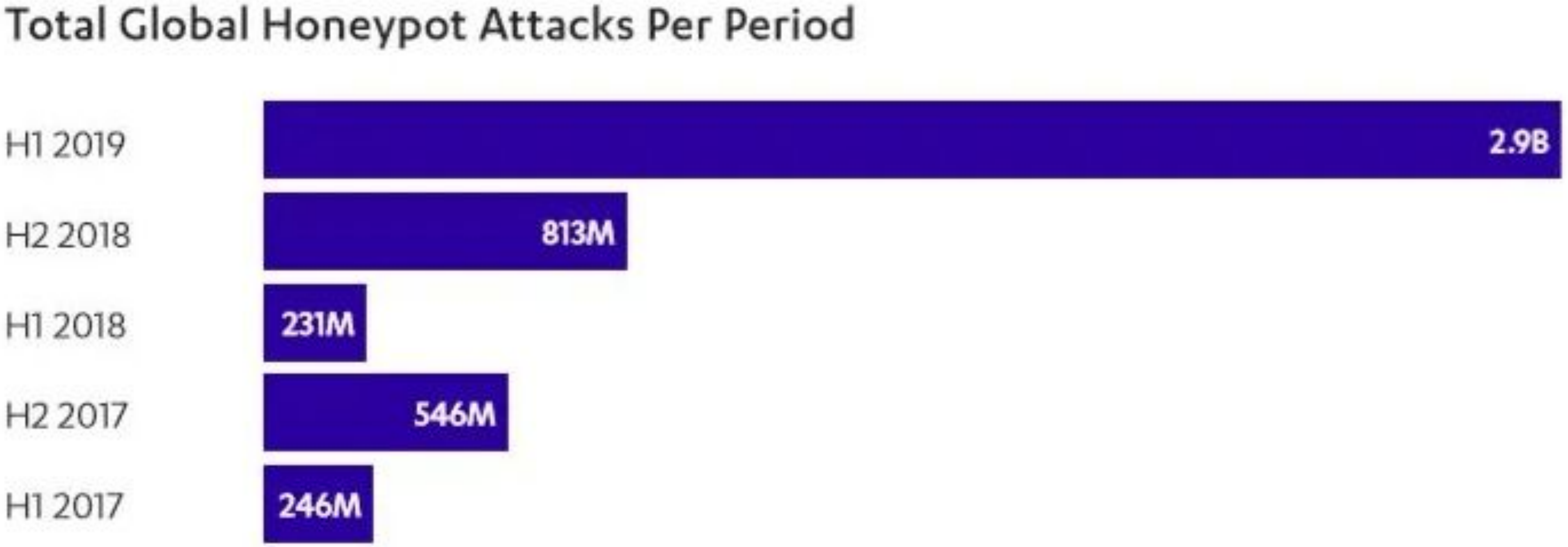
Cyber Security and Cyber Crime Statistics

“The number of Internet connected devices is expected to increase from 31 billion in 2020 to ***35 billion in 2021 and 75 billion in 2025****”*

– Security Today’s The IoT Rundown for 2020

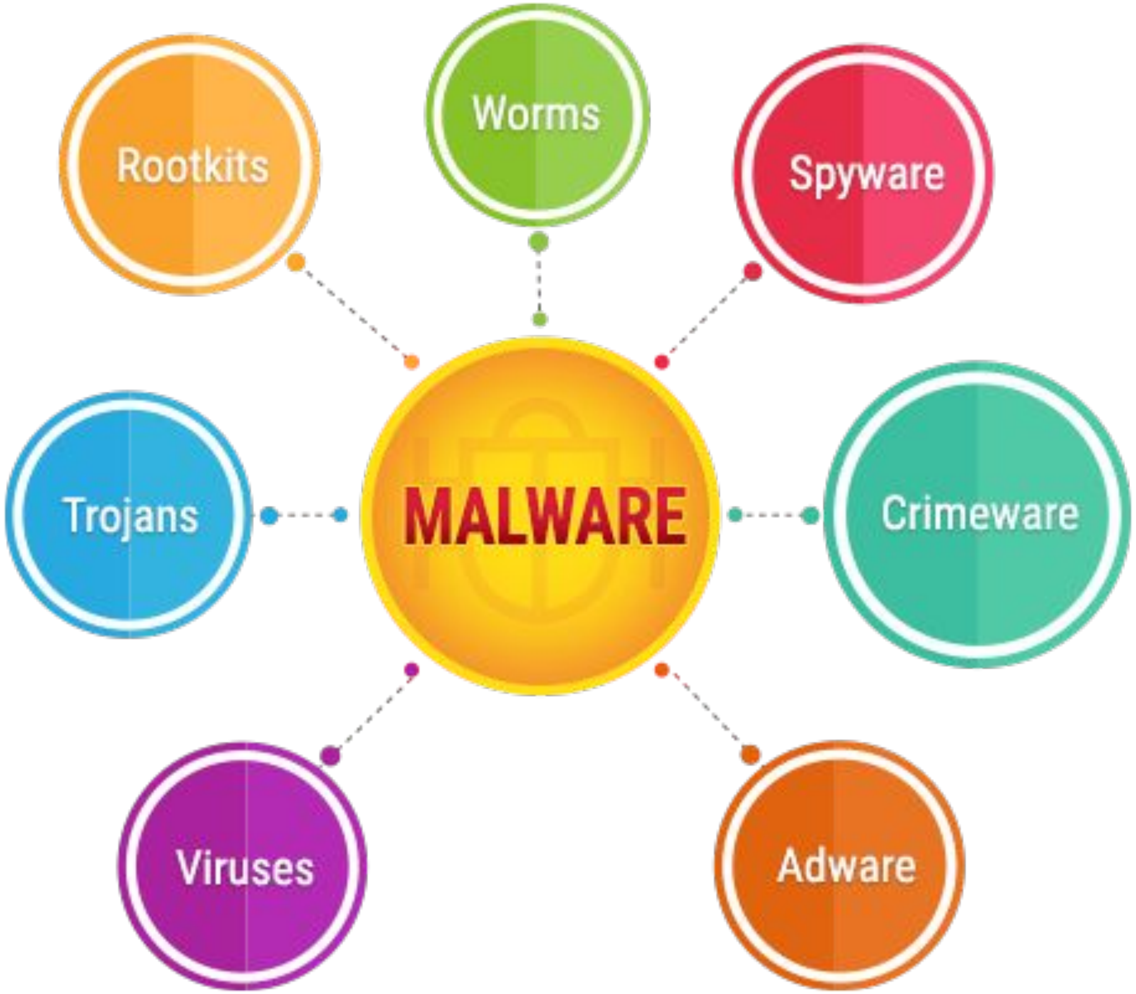
- In the first half in 2019, the number of cyberattacks on IoT devices increased by 300%. (F-Secure Attack Landscape H1 2019)
- This represented 2.9 billion events and was the first time numbers have surpassed a billion. (F-Secure Attack Landscape H1 2019)

Cyber Security and Cyber Crime Statistics



Source: F-Secure Landscape Report H1 2019

Types of Malware



Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content
  - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
  - Executes secretly when the host program is run
- Specific to operating system and hardware
  - Takes advantage of their details and weaknesses

Virus Components

Infection Mechanism

- Means by which a virus spreads or propagates
- Also referred to as the infection vector

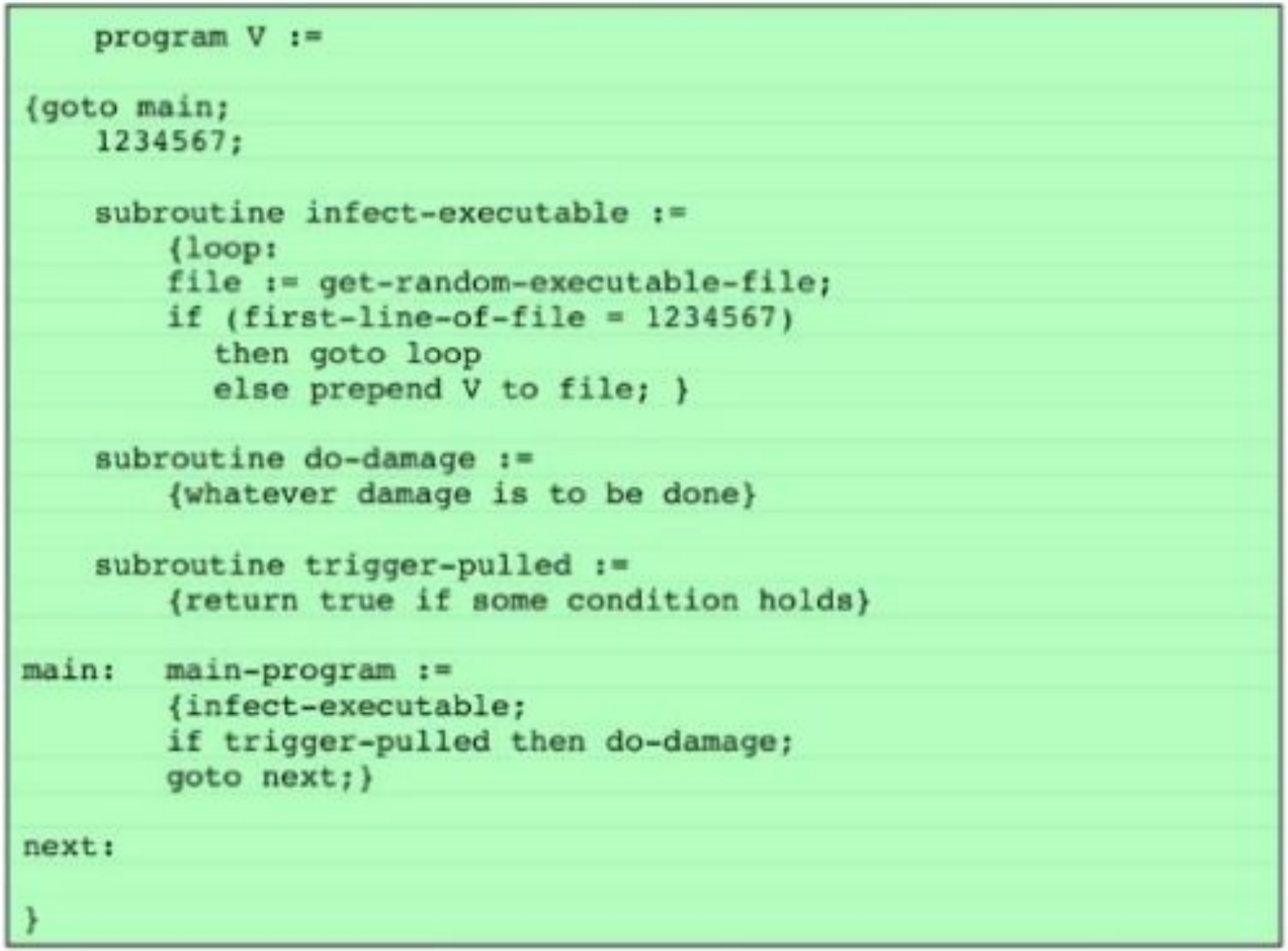
Trigger

- Event or condition that determines when the payload is activated or deactivated
- Sometimes known as a *logic bomb*

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity

Virus Structure



```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

Source: ITSY3104 – Computer Security A – Lecture 5 – Malicious Software

Virus Classifications

- Boot sector infector
  - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- File infector
  - Infects files that the operating system or shell considers to be executable
- Macro virus
  - Infects files with macro or scripting code that is interpreted by an application
- Multipartite virus
  - Infects files in multiple ways

Virus Countermeasures

- Prevention – ideal solution but difficult

- Best approach is to be able to do the following:
  1. **Detection** – determine & locate virus
  2. **Identification** – identify the specific virus that infected
  3. **Removal** – remove all traces of the virus from the infected program

- If detect but can’t identify or remove, must be discard and replace infected program

Digital Immune System

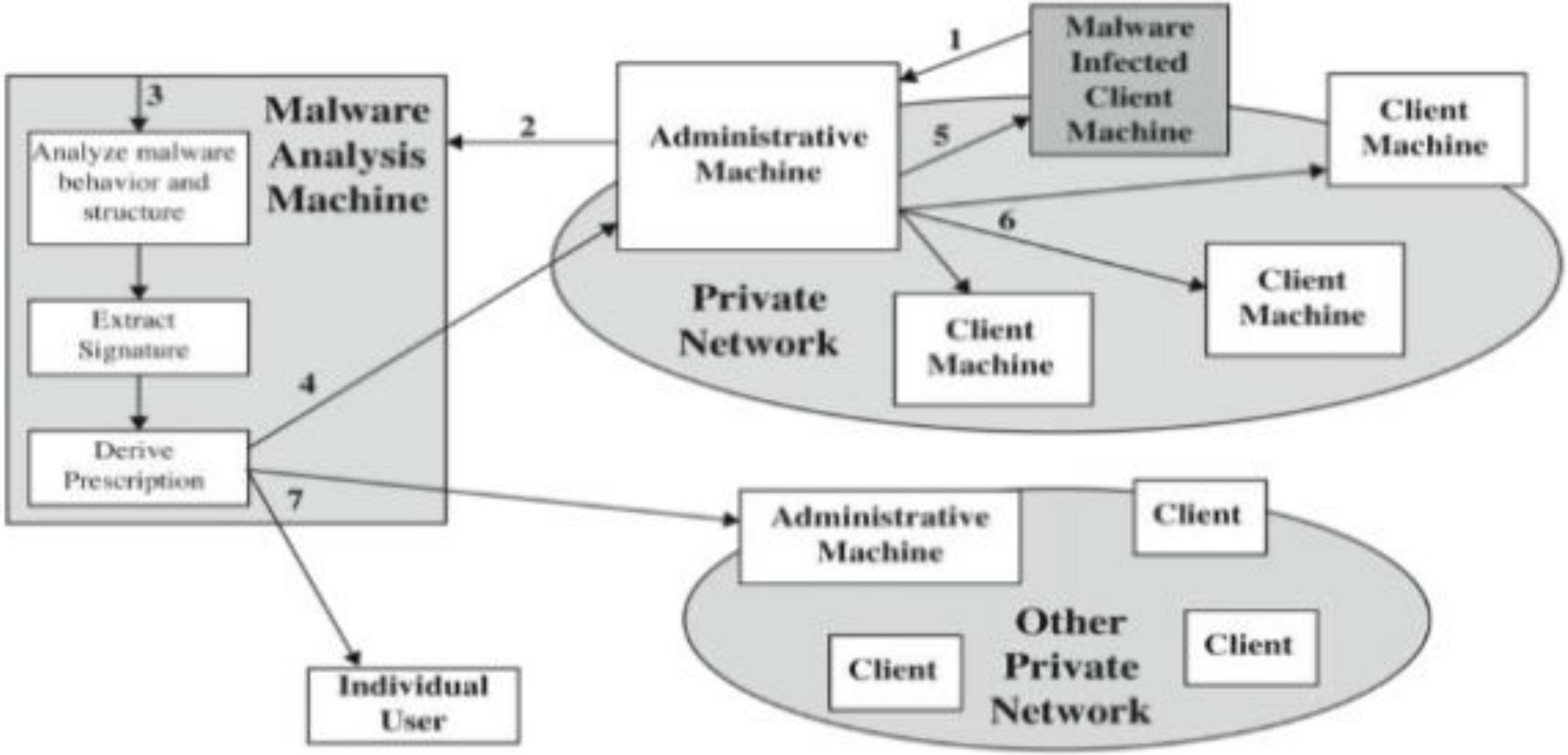


Figure: Digital Immune System

Source: ITSY3104 – Computer Security A – Lecture 5 – Malicious Software

Digital Immune System

- The **Digital Immune System** is a comprehensive approach to virus protection developed by and subsequently refined by Symantec.

- The motivation for this development has been the rising threat of Internet-based virus propagation, and the need to acquire a global view of the situation.

Worms

- Programs that actively seeks out more machines to infect
  - Each infected machine servers as an automated launching pad for attacks on other machines

- Worms are spread via software vulnerabilities or phishing attacks. Once a worm has installed itself into your computer's memory, it starts to infect the whole machine and in some cases, the whole network.

Worms

- Depending on the type of worm and your security measures, they can do serious damage.
    - Modify and delete files
    - Inject malicious software onto computers
    - Replicate themselves over and over to deplete system resources
    - Steal your data
    - Install a convenient backdoor for hackers
- They can infect large numbers of computers fast, consuming bandwidth and overloading your web server.

Bots and Botnets

- A bot is a computer that’s been infected with malware so it can be controlled remotely by a hacker
- The bot (aka a *zombie computer*), can then be used to launch more attacks or to become part of a collection of bots (aka a **botnet**)
- Botnets are popular with hacker show-offs (the more bots you collect, the mightier the hacker you are) and cyber criminals spreading ransomware.
- Botnets can include millions of devices as they spread undetected.

Bots and Botnets

- Botnets help hackers with all manner of malicious activities, including:
  - DDoS
  - Keylogging, screenshots and webcam access
  - Spreading other types of malware
  - Sending spam and phishing messages

Trojan Horses

- A trojan horse is malicious program that disguises itself as a legitimate file, because it looks trustworthy.
- Trojan themselves are a doorway. Unlike a worm, they need a host to work. Once you’ve got the Trojan on your device, hackers can use it to:
  - Delete, modify and capture data
  - Harvest your device as part of a botnet
  - Spy on your device
  - Gain access to your network

Ransomware

- Ransomware denies or restricts access to your own files. Then it demands payment (usually with cryptocurrencies) in return for letting you back in

- **WannaCry** is a malware which affected MS operating systems that did not have the latest patch installed for a known vulnerability.

Ransomware

- To reduce the risks of ransomware attacks:
  - Always keep your Operating System up to date
  - Keep your Anti-Virus software up to date
  - Back-up your most important files
  - Don’t open attachments from unknown sources (WannaCry was spread via a .js attachment)

Adware & Scams

- Adware is one of the better known types of malware. It serves pop-ups and display ads that often have no relevance to the victim.

- Some users will put up with certain types of adware in return for free software (games for example).

Adware & Scams

- Always remember that not all adware are equal:
  - At best, it’s annoying and slows down your machine
  - At worst, the ads link to sites where malicious downloads await unsuspecting users.

- Adware can also deliver Spyware and is often easily hacked, making devices that have it installed a soft target for hackers, phishers and scammers

Spyware

- Spyware secretly records your online activity, harvesting your data and collecting personal information such as usernames, passwords and surfing habits.

- Spyware is a common threat, usually distributed as a freeware or shareware has an appealing function on the front end with a covert mission running in the background that you might never notice.

Spyware

- It’s often used to carry out identity theft and credit card fraud.
- Once on a victim’s computer, spyware relays the data to advertisers or cybercriminals.
- Some spyware installs additional malware that make changes to your settings.

Spam and Phishing

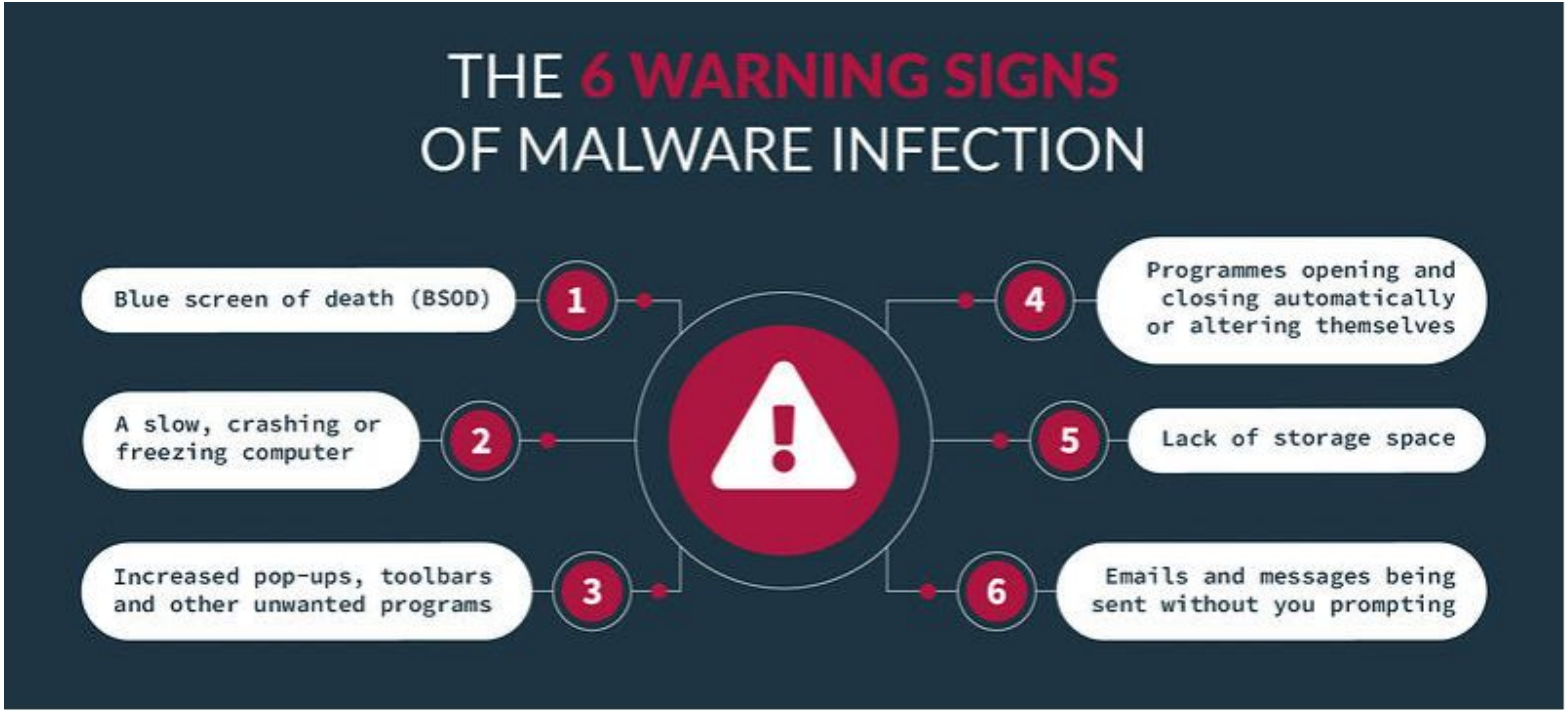
- Phishing is a type of social engineering attack, rather than a type of malware. It is a common method of cyber attack.
- Phishing is successful since the emails sent, text messages and web links created look like they’re from trusted sources.
- They’re sent by criminals to fraudulently acquire personal and financial information.

Spam and Phishing

- Some are highly sophisticated and can fool even your most savvy users, especially in cases where a known contact’s email account has been compromised and it appears you’re getting an instruction from your boss or IT colleagues.

- Others are less sophisticated and simply spam as many emails as they can with a message about checking your bank account details

Warning Signs of Malware Infections



THE 6 WARNING SIGNS OF MALWARE INFECTION

1 Blue screen of death (BSOD)

2 A slow, crashing or freezing computer

3 Increased pop-ups, toolbars and other unwanted programs

4 Programmes opening and closing automatically or altering themselves

5 Lack of storage space

6 Emails and messages being sent without you prompting

Source: https://www.comtact.co.uk/blog/what-are-the-different-types-of-malware

Warning Signs of Malware

- If you noticed any of the following, you may have malware on your device:
  1. A slow, crashing or freezing computer
  2. Blue screen of death (BSOD)
  3. Programmes opening and closing automatically or altering themselves
  4. Lack of storage space
  5. Increased pop-ups, toolbars and other unwanted programs
  6. Emails and messages being sent without you prompting them

Summary

- A malware is a set of malicious codes created to harm and get access to a targeted computer.
- The Elk Cloner was the first known computer virus in the history.
- Brain Virus was the first most damaging virus in the history attacking MS-DOS computers infecting floppy disks
- According to Global Information Security Survey 2018 - 2019, Customer information is the most valuable information for cyber criminals, and Phishing is the number one biggest cyber threats to organizations
- A virus is a piece of software that infects programs and executes secretly when the host program is run
- A worm is infecting machine servers to make it as an automated launching pad for attacks on other machines.

Summary

- A bot also known as zombie computer that is used to launch mre attacks or to become part of a collection of bot (a.k.a. a botnet)
- A trojan horse disguises as a legitimate file and serves as a doorway to host a computer or network illegitimately.
- A ransomware restricts the victim to access their own files then ask money in order to return the access to the owner using cryptocurrencies.
- An Adware serves as an pop ups and display ads to help hackers, phishers, and scammers get on you and your devices.
- A spyware is a freeware or shareware the tracks and records your online activity, harvesting your data, and collecting your personal information.

Summary

- Phishing is successful since the emails sent, text messages and web links created look like they’re from trusted sources.
- You will know that your computer has a malware if your device is: (1) slow, crashing or freezing, (2) experiencing BSOD, (3) Programmes are automatically opening, closing, and altering themselves, (4) lack of storage space, (5) increased pop ups, toolbars and other unwanted programs, (6) email and messages are being sent without you prompting them.

- Prevention is key to avoiding malware infections in the future.
- Practice safe browsing habits
- keep your software updated
- Use reputable antivirus software
- Regularly back up your important files to minimize the risk of malware infections.

END OF PRESENTATION.
THANK YOU!