Week 2 → 3.
Threat Analysis

Dr. M. Bilal Amin | bilalamin@utas.edu.au

UNIVERSITY of TASMANIA

Index

Threat Analysis

Threat analysis is an ongoing process adopted by an organisation for identifying, evaluating, and prioritising potential threats to its assets and infrastructure.

It involves analysing various factors such as vulnerabilities, attack vectors, potential impact, and likelihood of occurrence to determine the severity of a threat.

The goal of threat analysis is to understand the potential risks faced by an organization and take proactive measures to mitigate or manage them effectively.

Threat analysis helps in creating a threat model specific to an organisation, considering its unique infrastructure, cybersecurity posture, assets, and threat landscape.

Ref:

Attack Vectors

UNIVERSITY of TASMANIA

What is an Attack Vector?

Cyberattacks are launched through attack vectors, which allow unauthorized access to infrastructure entities (Computers, Workstations, Servers, networks etc.)

Through attack vectors, bad actors exploit system vulnerabilities to access sensitive data, personally identifiable information, and other valuables

Examples of attack vectors include malware, viruses, communication channels and social engineering

For a successful attack, bad actors apply a combination of attack vectors called an Attack Surface.

What is an Attack Vector? 16 Critical Examples in 2023

Ref:

What is an Attack Vector?

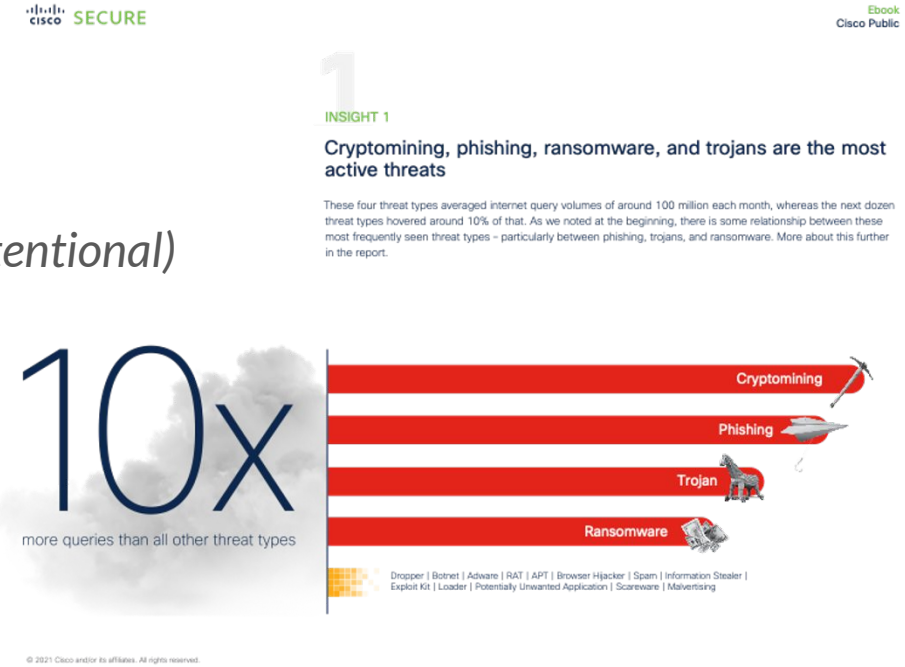
Attack vectors can be categorised into passive or active attacks

- *Passive attack vectors:*
  - *Exploits the target without affecting or utilising target's resources*
  - *Phishing, Social Engineering, Typosquatting etc.*
- *Active attack vectors:*
  - *Exploits the target by effective utilisation of the target's resources*
  - *Malware, viruses, trojans, Man-in-the-middle attacks, ransomware attacks etc.*

Ref:

Common types of attack vectors

- *Compromised/weak credentials*
- *Missing/weak encryption*
- *Malicious insiders*
- *Misconfiguration (intentional or unintentional)*
- *DDos*
- *SQL injections*
- *Trojans*
- *Man-in-the-middle attacks*
- *etc.*



Ref:

1. Malware

UNIVERSITY of TASMANIA

What is a Malware?

Malicious Software is an umbrella term for software entities that are harmful to a computer system.

"[malware] is a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network." Microsoft

Worm, virus, trojan, spyware, adware, rootkit, ransomware etc. all are synonymous; however, they have a different attack model.

Ref: Josh Fruhlingerm "Malware explained: How to prevent, detect and recover from it", 2019, https://www.csoonline.com/article/565999/what-is-malware-viruses-worms-trojans-and-beyond.html

History of Malware

Mathematician John von Neumann discussed the idea in his lecture series in the late 1940s and in his 1966 paper, "Theory of Self-Reproducing Automata." The paper speculated that "mechanical" organisms, like computer codes, could damage machines, copy themselves, and infect new hosts, just like biological viruses.

Ref: *Image source: https://en.wikipedia.org/wiki/John_von_Neumann*

History of Malware

Creeper Program

- *Proof-of-concept for self-reproducing automata*
- *Moves itself from one drive to another.*
- *No malicious intent, only displayed a simple message, ""I'M THE CREEPER. CATCH ME IF YOU CAN!"*

Animal

- *Buys time to infect during a game called "Animal" in which the program tries to guess the name of the animal*
- *A conjunction program called PREVADE copies the animal program in every directory possible occupying the space*

1971 — **1974** — **1975** — **1986**

The Rabbit "Wabbit" Virus

- *Copies itself reducing the overall performance of the system*
- *The speed of replication gave it the name "Rabbit" virus.*

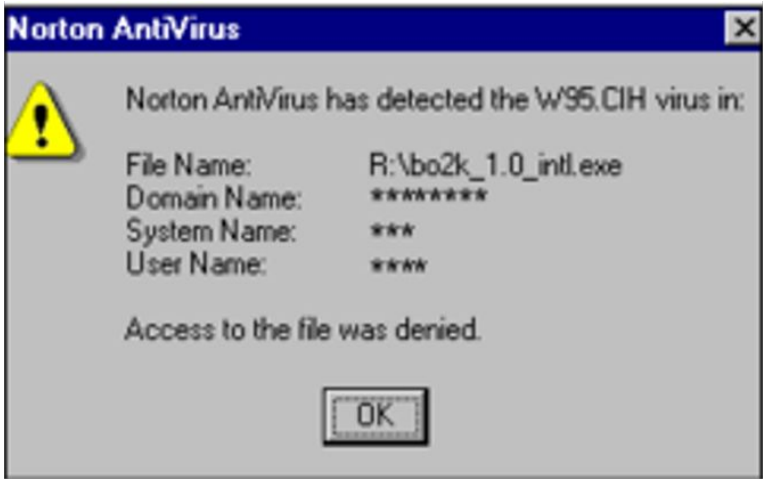
Brain

- *First boot-sector virus, Stealth-virus*
- *No malicious intent, two programmers from Lahore, Pakistan were trying to prevent their users to make illegal copies of their software*
- *First MATE attack*

Ref:

CIH/Chernobyl Virus (1998)

"CIH, also known as Chernobyl or Spacefiller, is a Microsoft Windows 9x computer virus that first emerged in 1998. Its payload is highly destructive to vulnerable systems, overwriting critical information on infected system drives and, in some cases, destroying the system BIOS."
"Chén Yínghào, a student at Tatung University in Taiwan, created the virus. It was believed to have infected sixty million computers internationally, resulting in an estimated US$1 billion in commercial damages"



Ref: https://en.wikipedia.org/wiki/CIH_(computer_virus)

The Love Letter Virus (2000)

Appeared on May 4, 2000, and was one of the most serious epidemics of this new era.
A simple email attachment with a file "LOVE-LETTER-FOR-YOU-TXT.vbs", with the subject line "I Love You"
The fact that the ILOVEYOU message often came from someone familiar made it more likely for new victims to open it, making it a proof of concept for how effective social engineering can be
When clicked, the worm replaced existing files with copies of itself, allowing it to spread to all the victims' contacts via email.

Ref:

The Code Red Virus (2001)

The worm did not infect files on the system and existed only in the memory

This fast-replicating worm exploited a flaw in Microsoft Internet Information Server and manipulates communication protocols to spread globally in hours

First Zero–day attack

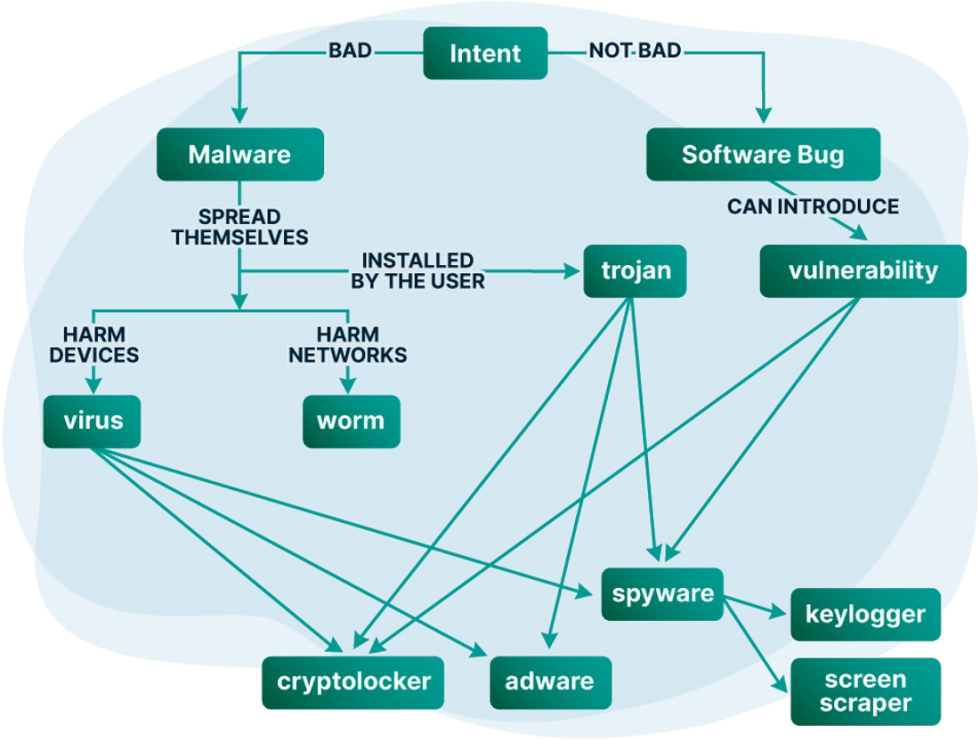
Ref:

Types of Malware

1. *Virus → Spreads with a trigger, mostly a user action*
2. *Worm → Spread automatically with events*
3. *Trojan → Hides itself as or within a legitimate software*
4. *Rootkit → Hides deep within its target usually close to boot sector*
5. *Exploit kit → Goes after known vulnerabilities*
6. *Adware → Feeds Ads*
7. *Spyware → Monitors users activity, may send the activity data to third-party*

Ref:

Types of Malware



Ref: *Image source: https://www.expressvpn.com/blog/what-is-malware/*

Types of Viruses

1. Boot sector viruses
2. Resident viruses
3. Direct action viruses
4. Polymorphic viruses
5. Multipartite viruses
6. Macro viruses

Ref:

How are viruses removed?

Typical anti-virus software uses methods such as signature-based detection to identify viruses in a system

The virus signature file repository gets updated regularly for effective and up-to-date detection

However, the anti-virus software are easy to cheat by developing metamorphic or polymorphic viruses which quickly change their signature over time

Ref:

2. Social engineering

UNIVERSITY of TASMANIA

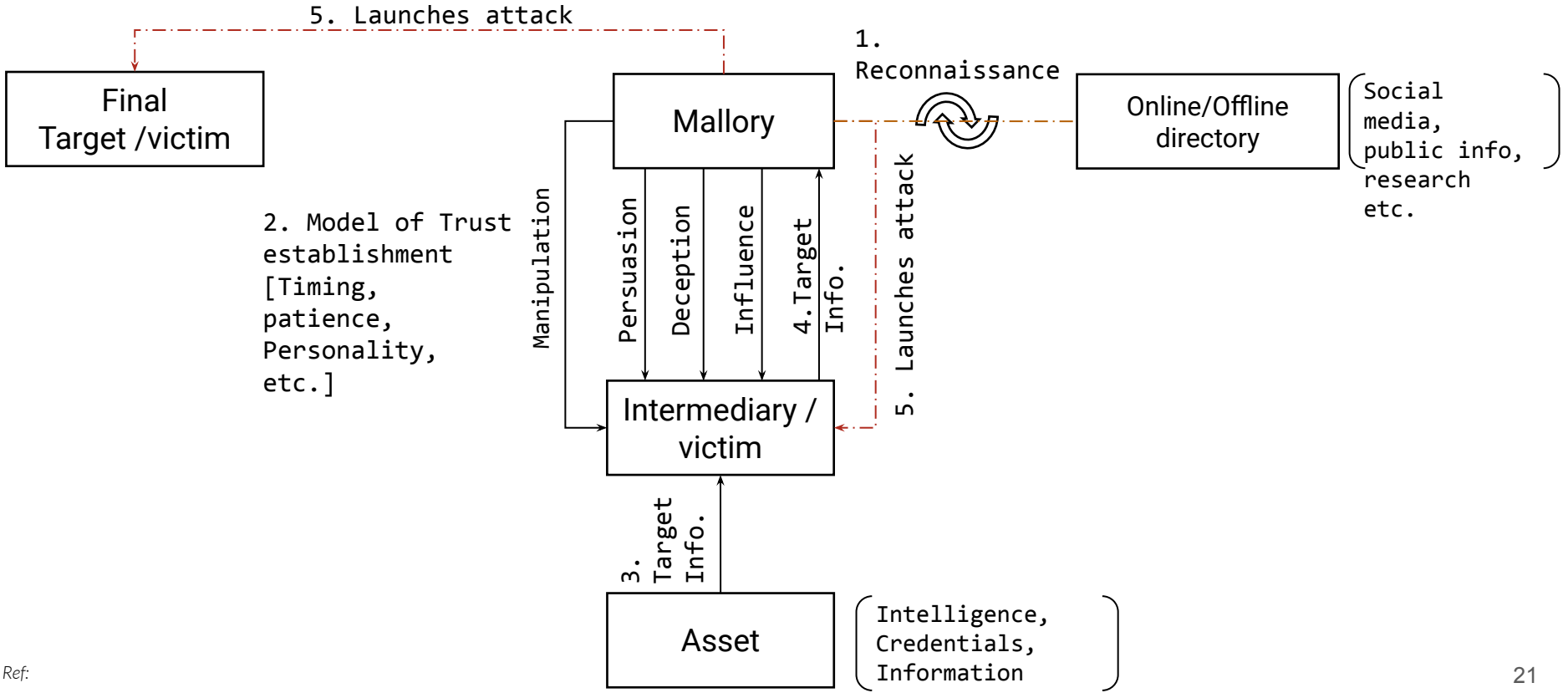
What is social engineering

The term "social engineering" describes a wide range of malicious activities accomplished through human interactions.
Users are tricked into making security mistakes or giving away sensitive information by psychological manipulation.
It preys on users' lack of knowledge/awareness, insecurities and stressful situations.
For example, U.S Presidential election 2016

- *Emails and data from the Democratic Party were leaked due to spear phishing attacks*
- *Members of the Democrat party were invited to change their passwords through a fake Gmail email created by hackers.*
- *The hackers then accessed hundreds of Clinton campaign emails containing sensitive information.*

Ref:

Attack model



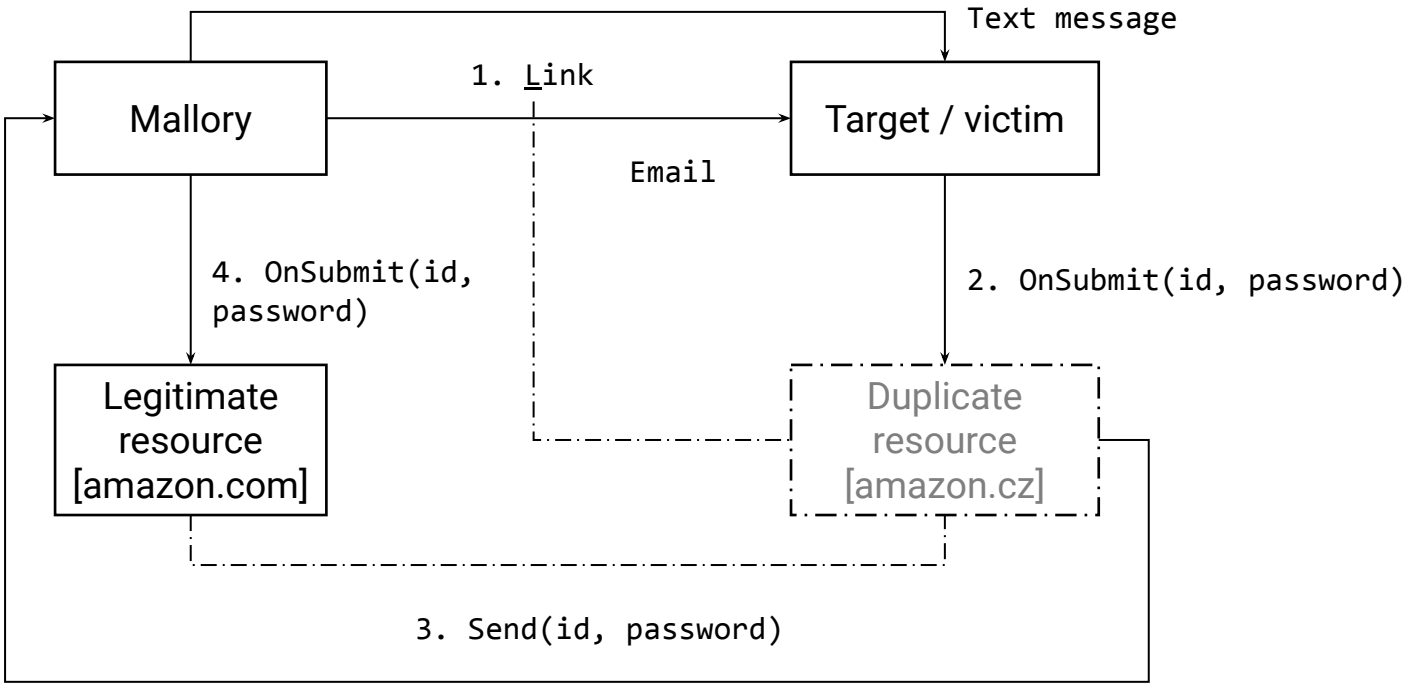
Ref:

Phishing attacks

- *One of the most successfully applied social engineering technique is a phishing attack*
- *“Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.”*
- *“The information is then used to access important accounts and can result in identity theft and financial loss.”*

Ref: *https://www.phishing.org/what-is-phishing*

Attack model



Ref:

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Types/techniques

- *Spear phishing*
  - *Unlike conventional phishing attacks "spray and pray", spear phishing is a targeted attack in which victims or intermediaries are identified with a comprehensive reconnaissance.*
  - *Less generic more personalized*
- *Spam*
- *Man-in-the-middle-attacks*
- *Session hijacking*
- *etc..*

Ref:

3. Denial-of-Service

UNIVERSITY of TASMANIA

What is a DoS attack?

DoS attack is meant to deprive the legitimate user by shutting down / making the target service inaccessible.

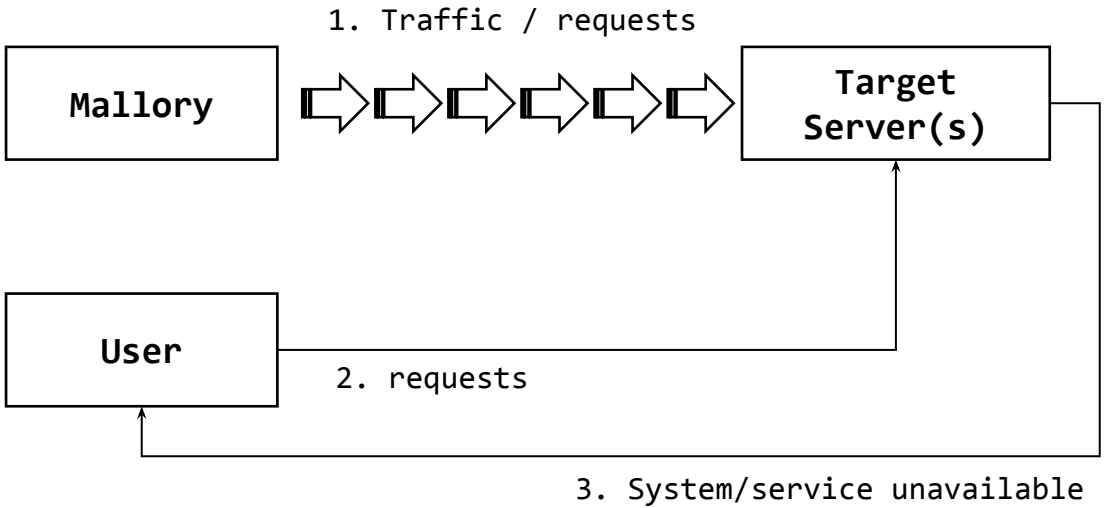
DoS attacks can be aggressive (flood of traffic) and/or trigger-oriented (malware).

In DoS attacks, high-profile organizations, such as banks, media companies, and commerce companies, are often targeted.

It is rare that DoS attacks result in significant data loss or theft, but they can cost the victim a great deal of money and time.

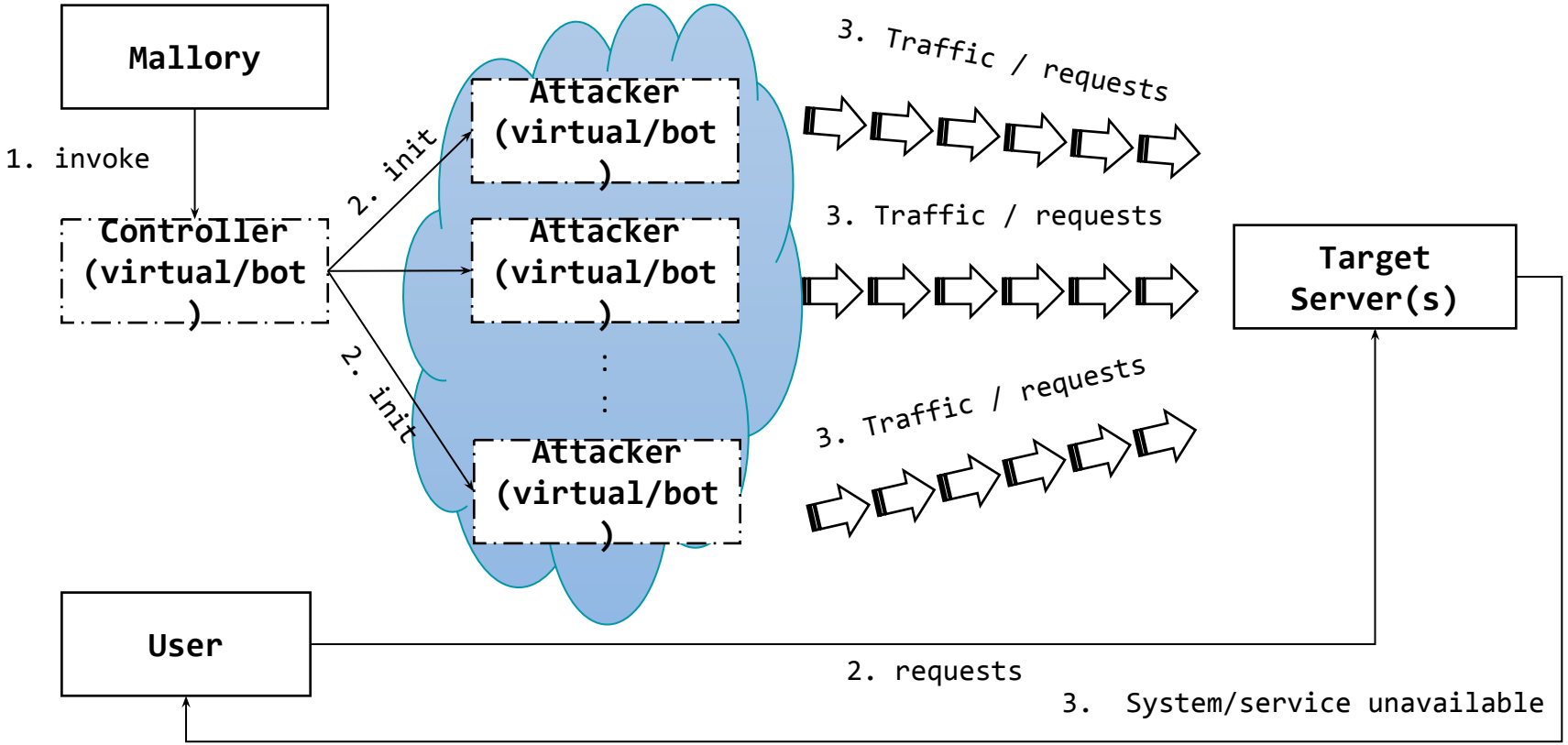
Ref:

Attack model



Ref:

Attack model



Ref:

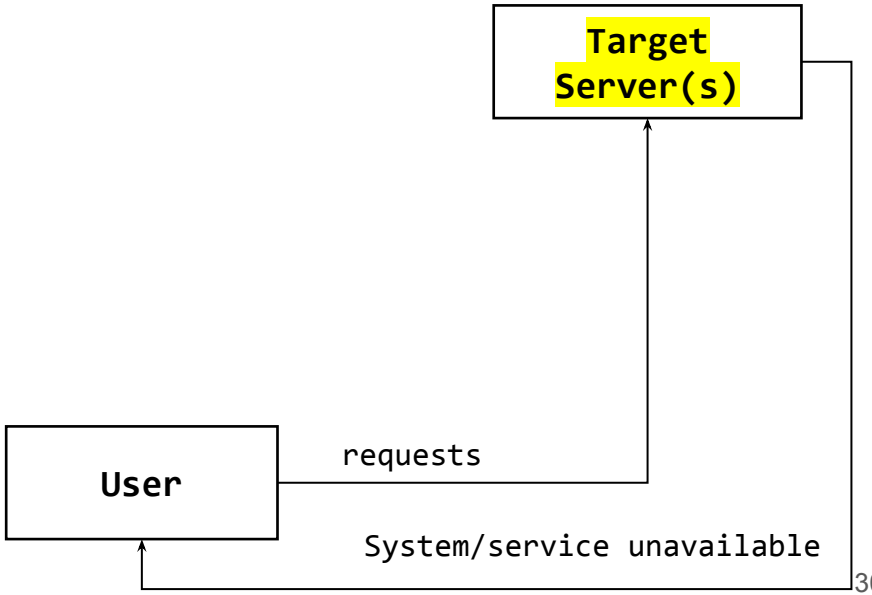
Attack model - Target layers

Application layer attacks

- Web-applications
  API
  Webservices
  Cloud services
- Difficult to distinguish legitimate from malicious request

Network layer attacks

- SYN floods: Exploits the TCP handshake process. Hacker sends a pile of requests from fake IPs and never completes a handshake
- Spoofing/Smurf DDoS: Infinite loop of ICMO ping messages that crashes the system



Ref:

DoS Prevention

Its difficult to prevent a DoS; especially a DDoS attack; however, there are several measures that can be implemented to minimise the risk and mitigate the impact.

1. *Elastic control over Network Bandwidth*
    a. *This includes continuous monitoring of the network and allocation of bandwidth based on usage.*
    b. *Load balancing of traffic between different servers, preventing a single point of failure*
    c. *Implement traffic filtering and scrubbing services that can analyse the incoming traffic and remove and suspicious/malicious request.*
2. *DDoS Protection Services*
    a. *This include cohesive implementation of hardware and software infrastructure.*
    b. *Configure routers and firewalls for SYN flood protection*
    c. *Keep the software systems updated including firewalls, web servers, operating systems, anomaly detection systems.*
3. *Incident Response planning*
    a. *Implement and maintain an incident response plan which outlines the steps and responsibilities for all stakeholders to take in case of an incident*
4. *Education of stakeholders*
    a. *Implement education programs for all stakeholders*

Ref:

4. Ransomware

UNIVERSITY of TASMANIA

What is a ransomware attack?

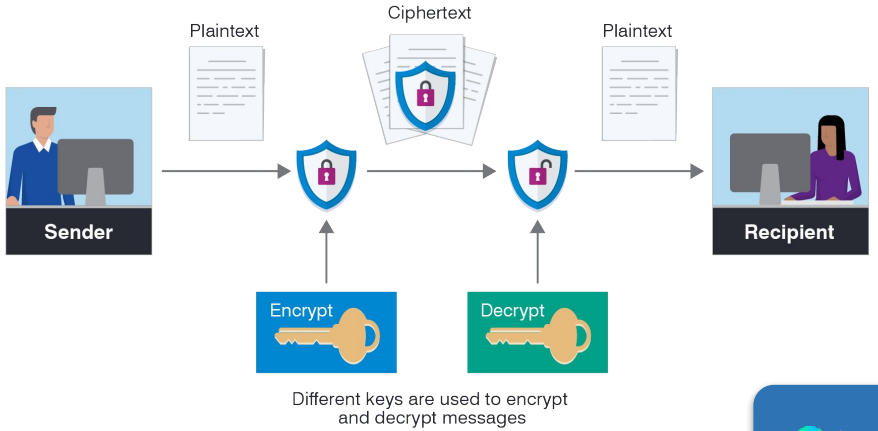
Ransomware attacks are malware attacks where bad actors encrypt a victim's data and demand ransom for the decryption key.
Ransomware attacks can be delivered through various means, including phishing emails, malvertising, and exploit kits.
The attack starts with the victim unknowingly downloading or opening the malicious file or link, allowing the ransomware to infiltrate their system.
Once inside, the ransomware encrypts files and prevents access until the ransom is paid, usually in cryptocurrencies for anonymity. The ransom amount can range from a few hundred dollars to thousands, payable to attacker in Bitcoin.
These attacks can target individuals, businesses, or even government institutions to exploit the value of the encrypted data.
Ransomware attacks can result in significant financial and reputational damage.

Why Are Ransomware Attacks Emerging?

Ref:

What is encryption?

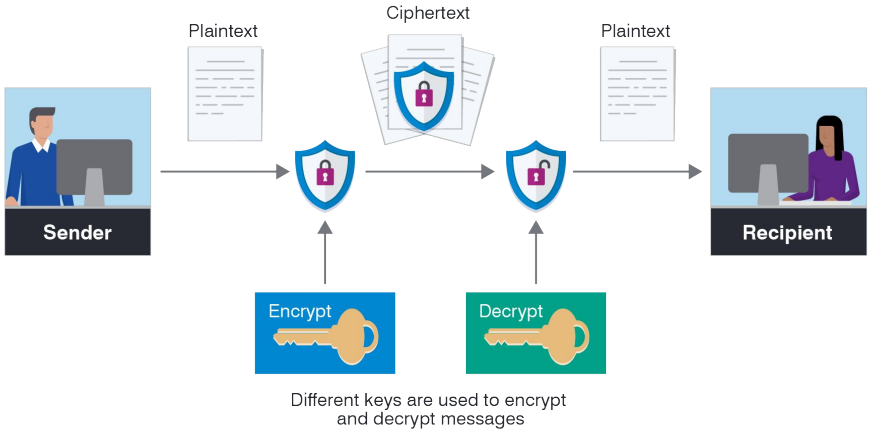
Encryption is the conversion of data into a form, called ciphertext, which cannot be easily understood by unauthorized people; thus securing the content.
For this conversion, encryption applies algorithms/key for transformation from data to ciphertext.



Ref: *Image source: https://www.proofpoint.com/au/threat-reference/encryption*

What is encryption?

Encryption is the conversion of data into a form, called ciphertext, which cannot be easily understood by unauthorized people; thus securing the content.
For this conversion, encryption applies algorithms and a key for transformation from data to ciphertext.




```
If Encrypt.key.isSame(Decrypt.key)
      Encryption == “Symmetrical key”
Else
      Encryption == “Asymmetrical/Public key”
```

Ref: Image source: https://www.proofpoint.com/au/threat-reference/encryption

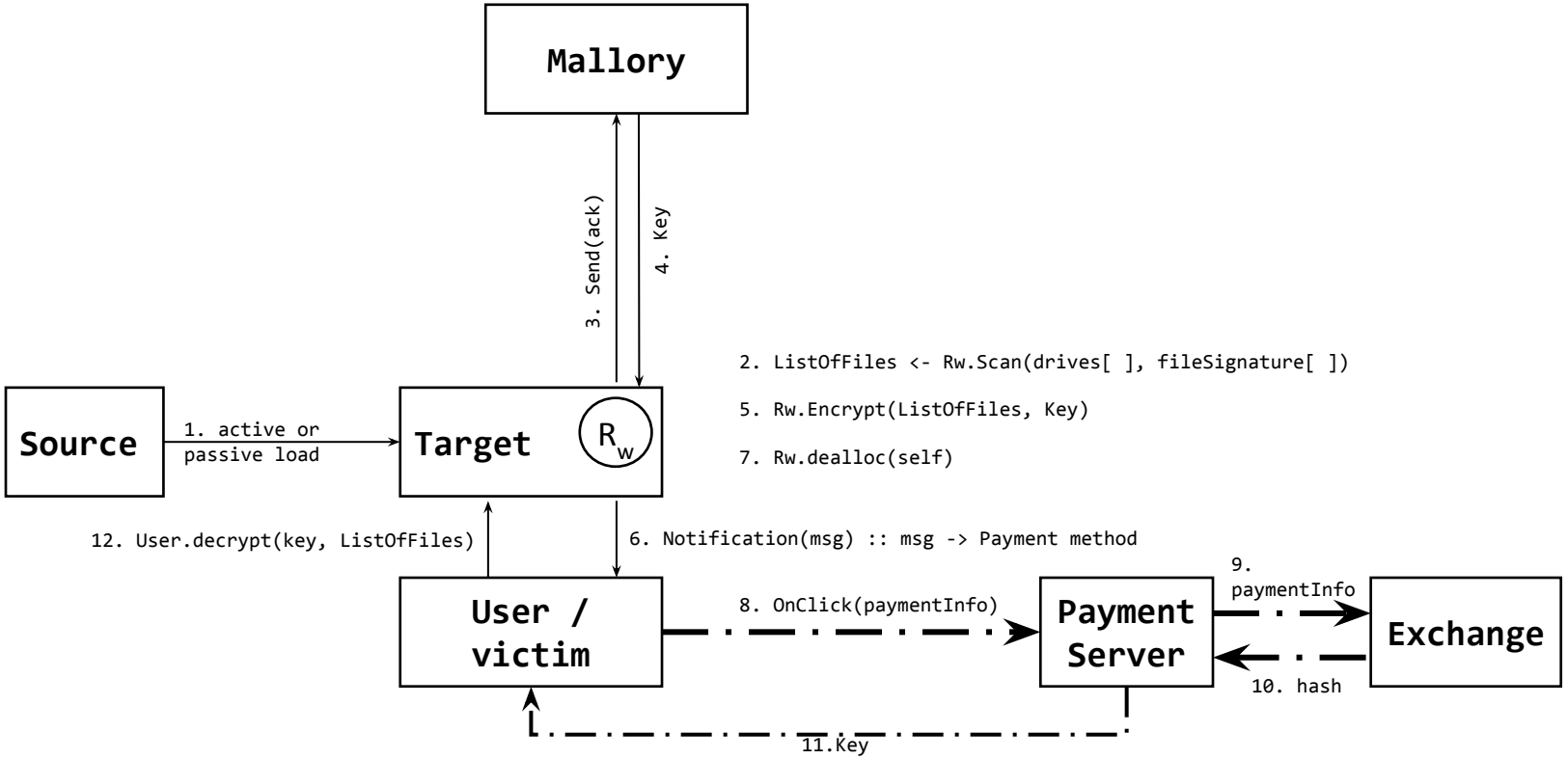
Strength of encryption?

Strength of a encryption scheme is called "Key space" also called "Key length"

- *An encryption scheme with a 128-bit key would have roughly 340,282,366,920, 938,000,000,000,000,000,000,000,000 possible key combinations*
- *A single processor, assuming a power of 500,000 passwords per second would break that key in about 21,580,566,141,612,000,000, 000,000,000 years*
- *Pretty Good Privacy (PGP) can radically drop this power to only a few hundred per seconds*

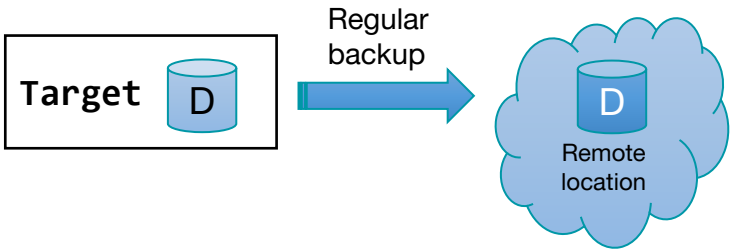
Ref:

Attack model

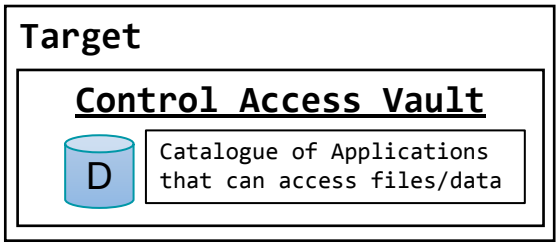


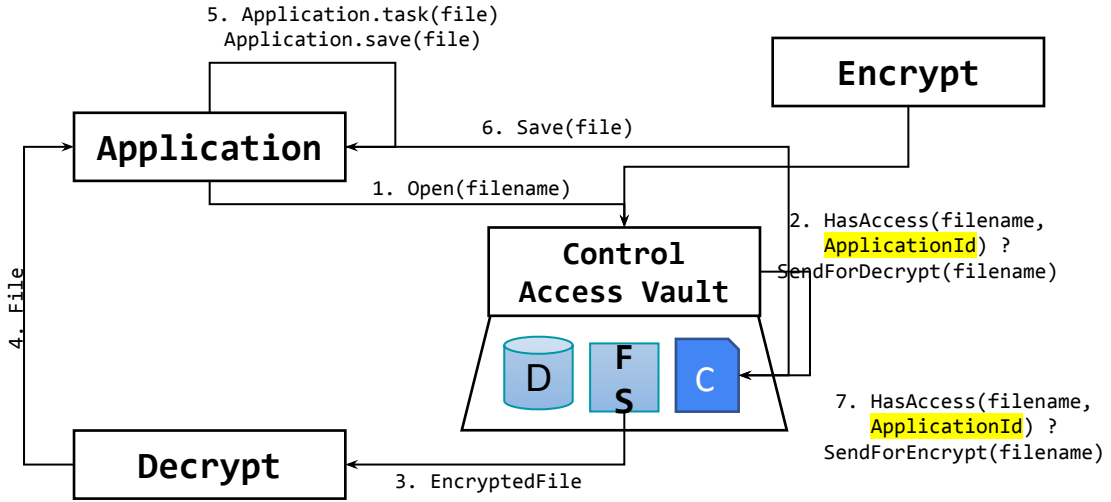
Ref:

Preventive measures



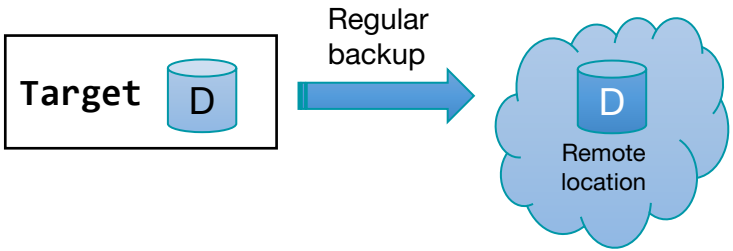
- *After restore to default, download the latest backup*
- *Data between the incident and the last backup will be lost*



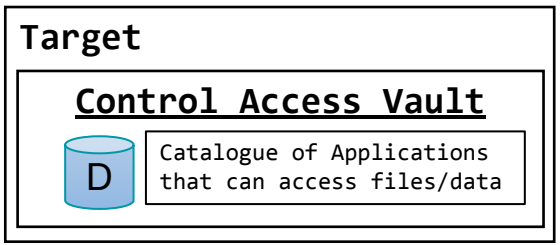


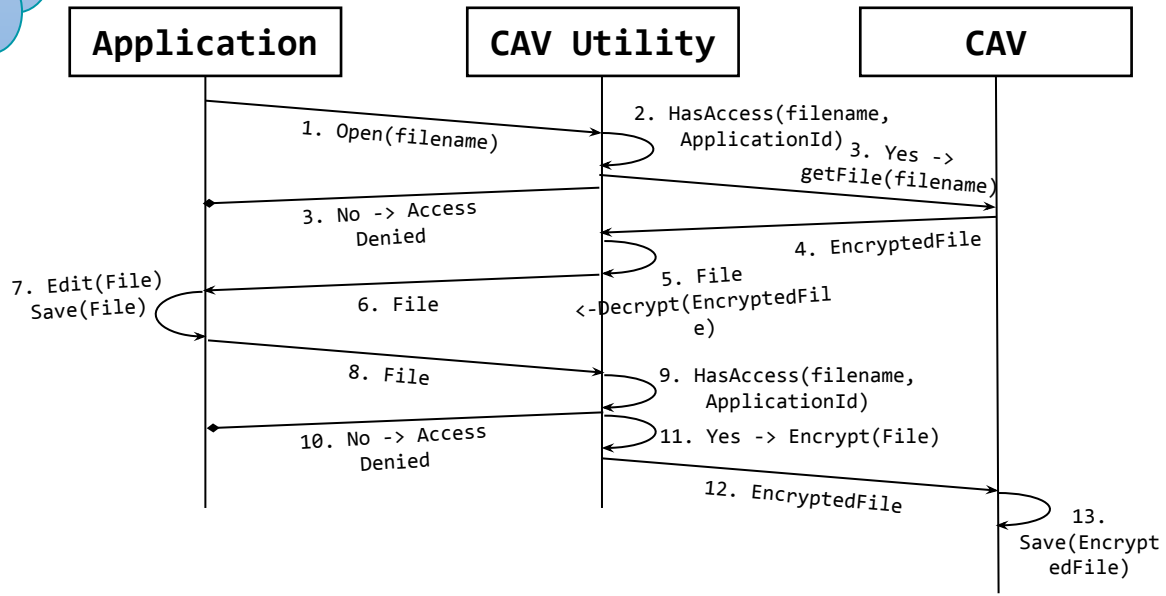
Ref:

Preventive measures



- *After restore to default, download the latest backup*
- *Data between the incident and the last backup will be lost*





Ref:

5. Crypto-mining / Crypto-jacking

UNIVERSITY of TASMANIA

What is a crypto mining?

In Cryptomining/jacking, attackers use malware to exploit another computing resource to mine cryptocurrency without their permission or knowledge of the owner.

- *Cryptocurrencies operate on a distributed data structure called "Blockchain". A block in a chain consists upon a collection of transactions.*
- *To create a block, a complex mathematical process needs to execute for block validation.*
- *Cryptocurrencies offer rewards for this validation process.*
- *This process demands a significant amount of electricity for computation, e.g., Bitcoin network of today uses over 112.19TWh of energy/year (https://digiconomist.net/bitcoin-energy-consumption)*

Attackers may use several delivery mechanism including social engineering to install malware that covertly mines cryptocurrency in the background.

Cryptojacking causes the target device or computer to slow down significantly, consume excessive amounts of power, and potentially damage the hardware.

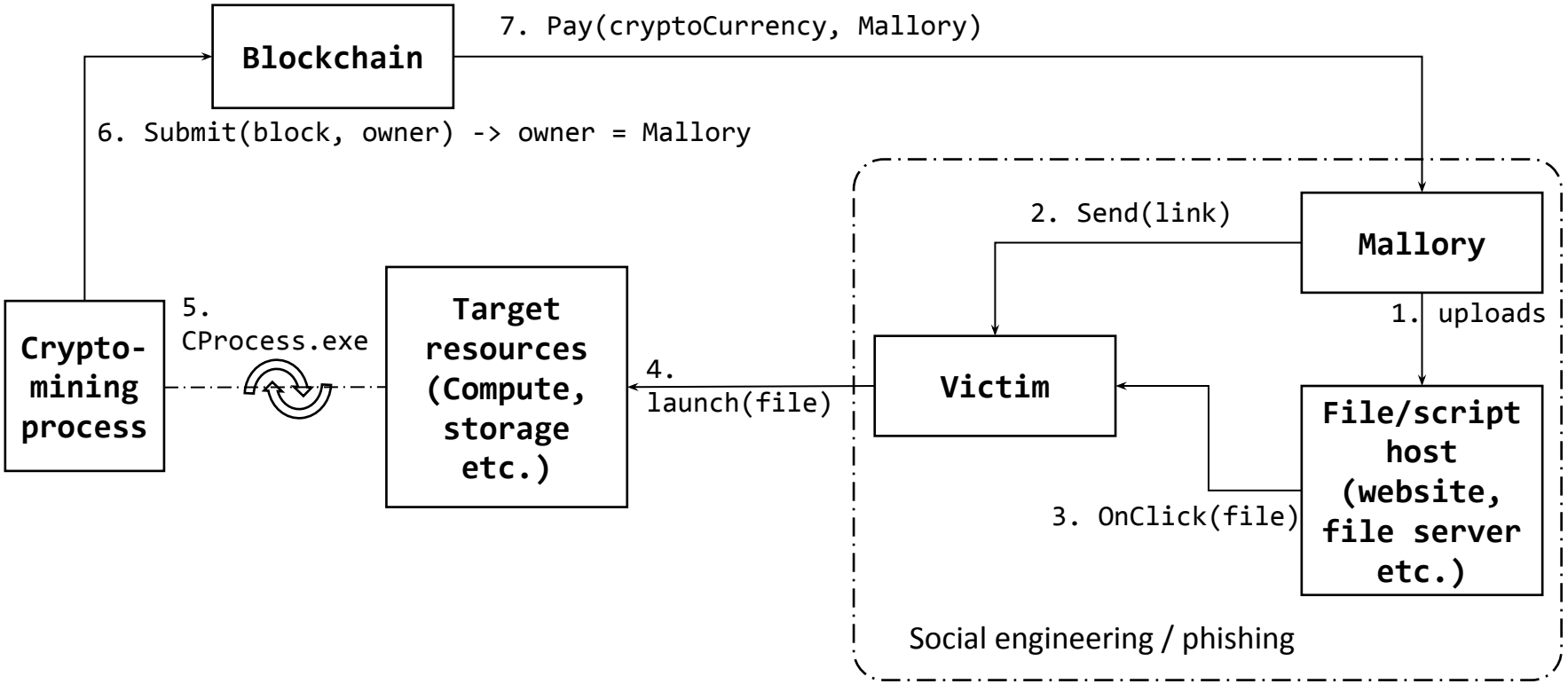
Some research data indicates that average smartphone batteries expand to a point of device deformity by using it for 48 hrs. for mining.

(https://www.zdnet.com/article/this-crypto-mining-android-malware-is-so-demanding-it-burst-a-smartphone/)

Why Are Ransomware Attacks Emerging?

Ref:

What is a crypto mining?



Ref:

How to detect?

1. *Slow performance: Cryptojacking can consume a considerable amount of computational power, causing the device to lag or freeze frequently.*
2. *Overheating: Cryptojacking consume more CPU/GPU power, thus generating excessive heat. A high CPU/GPU usage indicator in the system utilities such as task manager can identify such situation.*
3. *Increased electricity consumption: Cryptojacking consumes a significant amount of electricity as it puts the device's resources to work; however, this can only be noticeable if a cluster of devices are infected.*
4. *Battery drain: Due to compute intensive tasks, overheating, the battery drain from a portable infected device is significantly higher than average use.*
5. *Suspicious processes: Cryptojacking software may hide under obscure process names to avoid detection. A profile of running processes in task manager can identify the obscure one.*
6. *Browser extensions: Similar to infected processes, malicious browser extensions can have the similar impact.*
7. *Antivirus and network monitoring tools of today have the capabilities to detect malware and obscure processes exhausting computing and network resource.*

Ref:

How to prevent?

1. *Keep your preventive measures such as mentoring tools up-to-date*
2. *Use ad-blockers and script-blockers*
3. *Do regular scanning of the computational resources*
4. *Educate the stakeholders*

Ref:

Anatomy of a Cyberattack

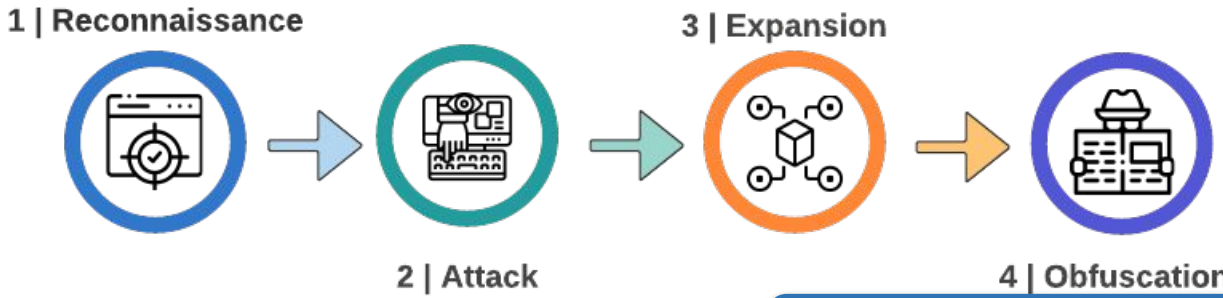
UNIVERSITY of TASMANIA

Anatomy of a cyberattack

Anatomy of a cyberattack is an informal study of threat analysis in which a cyber incident is studied by elaborating its events into a step of processes.

Varied definitions with elaboration of steps exists in the cybersecurity space; however, the overall scope is defined in four primary steps

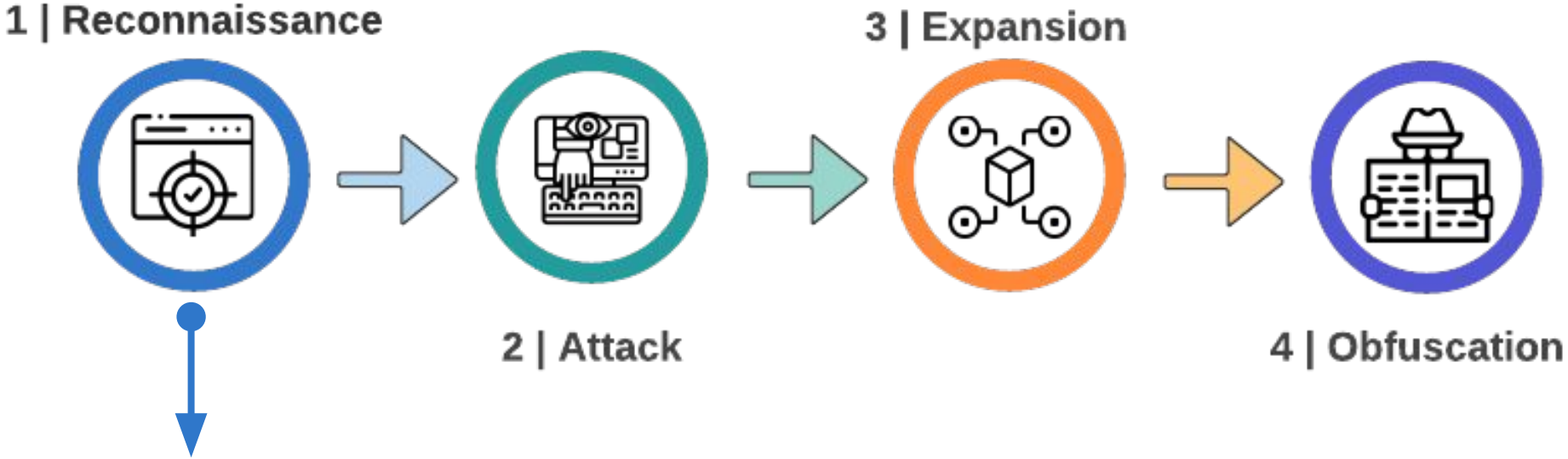
1. *Reconnaissance*
2. *Attack*
3. *Expansion*
4. *Obfuscation*



The Anatomy of a Cyber Attack (2022)

Ref:

1. Reconnaissance



The Network Attackers want to know the trust relationships in the network, and then how to exploit them- Who can make changes (system administrators) to critical business applications

Attackers look for vulnerabilities and potential entry points, such as the contact details of employees collected from company websites, LinkedIn or social media.

Ref:

1. Reconnaissance

It is the initial stage of a cyberattack where attacker studies the targets for potential weaknesses, impact value and entry points.

Scope of information gathering in this stage is:

1. *Hardware infrastructure – this includes network topology, IP and subnets, routers, firewalls and other network devices*
2. *Software infrastructure - this includes Operating systems and their versions, system- and application software running on the machines, Open ports, endpoints and services being hosted*
3. *Identity information - this includes usernames, emails, passwords, authentication protocols etc.*
4. *Cybersecurity posture - this includes a formal description of the level of defenses and preventive measures in place.*
5. *Potential vulnerabilities - this includes a subset of Hardware, Software, and Identity information that can be a potential point of strike. Known vulnerabilities in the system that can be exploited when required*
6. *Social engineering opportunities - this includes information about individual with a certain set of weaknesses such as, lack of awareness or education*

Based on this information attacker (in parallel) executes the weaponising stage where necessary tools and malwares are developed or acquired to create the payload for the attack.

Ref:

Types of Reconnaissance

1. *Active*

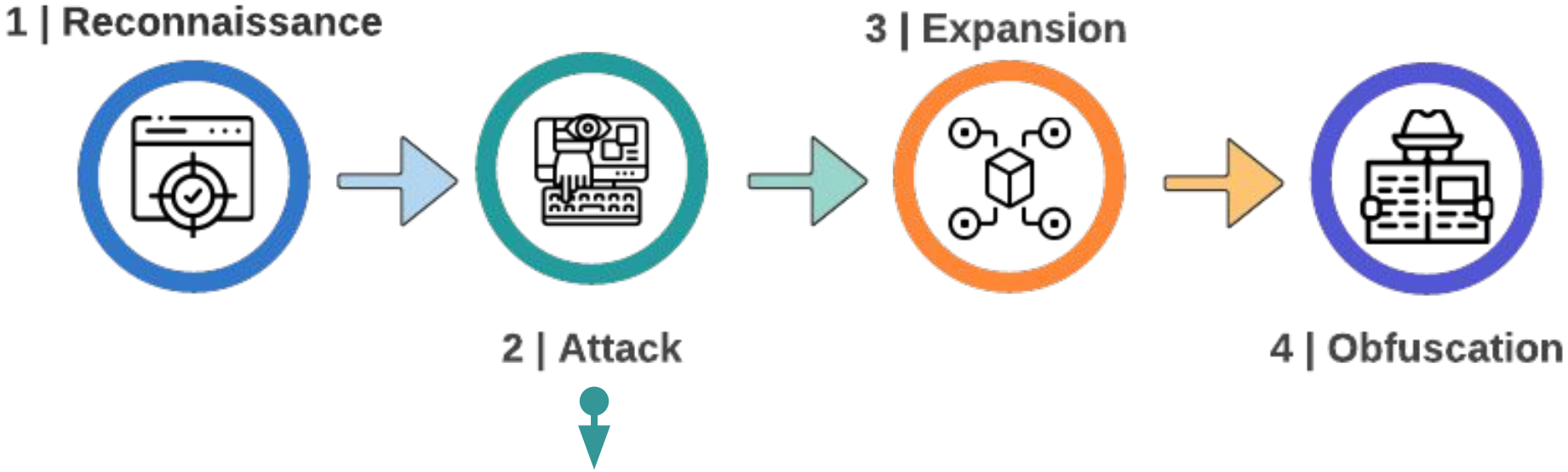
This involves direct interaction with the target system or infrastructure. Attackers use techniques such as network or port scanning, vulnerability scanning. This also includes social engineering attacks such as spear phishing attacks to extract sensitive information

2. *Passive*

This involves information gathering without any interaction with the target system or infrastructure. Publicly available resources such as search engines, social media, public records and listings are used to gather information. Attacker may also use tools such as WHOIS and DNS lookups for further details.

Ref:

2. Attack



This stage starts when the attacker push the 'go' button and launch the attack.
It may involve taking data out of your system, also known as 'exfiltration', or it may be the activation of ransomware.

Ref:

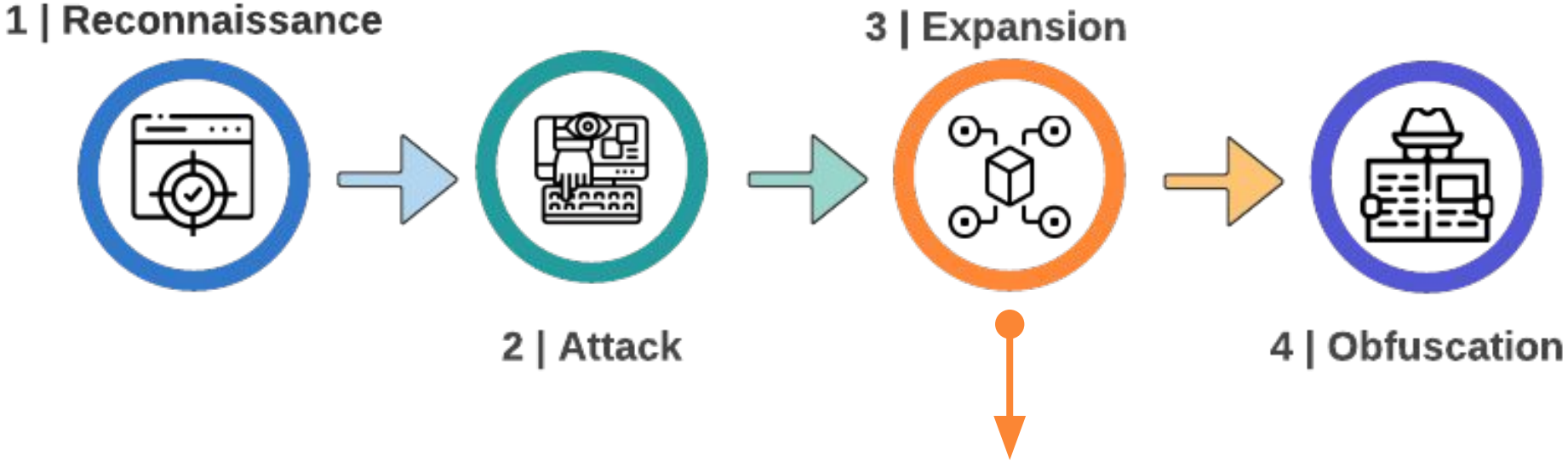
2. Attack

The go-ahead stage of the cyberattack where the payload is delivered to the target system or infrastructure via predetermined protocol. This protocol can be sending payload through channels such as emails, compromised endpoints, websites, infected portable devices.

As a next step in the stage, the payload is executed in the target environment, taking advantage of the vulnerabilities identified in the system.

Ref:

3. Expansion



Attacker intrudes all systems on the network using malicious programs.
Malicious programs enable attacker to hide in multiple systems in the organisations and regain access to the network even after being detected.

Ref:

3. Expansion

During expansion, the attackers expand their foothold on the targeted system and infrastructure by installing malicious tools such as backdoor remote access tools.

Upon successful installation and achieving the scope of expansion, the attackers establish a command and control chanel with the infrastructure, allowing system manipulations to achieve their goals.

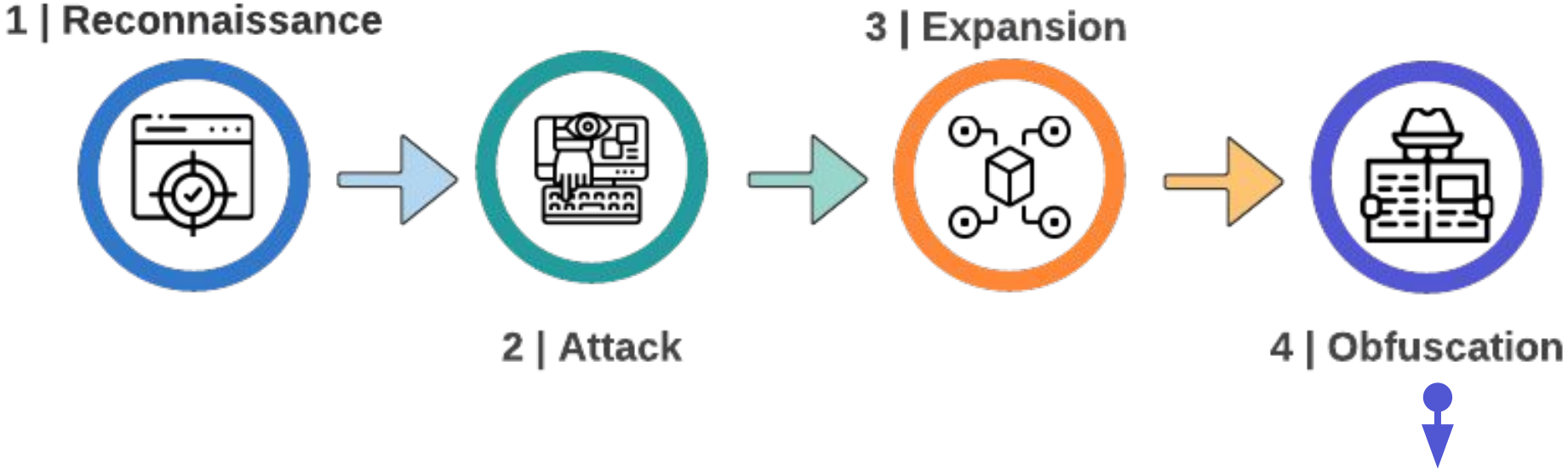
This step follows with a further penetration into the target system and infrastructure, by moving across the system, installing support channels, and overall escalating privileges to gain border access.

During the 2. Attack and 3. Expansion, attackers exfiltrate the asset (data) containing information such as personal data, financial information, business secrets, intellectual property etc.

An ongoing cyber attack usually gets noticed during the expansion stage

Ref:

4. Obfuscation



The main purpose of obfuscation is confusing and disorienting the incident response team.
For successful obfuscation, attackers use various tools and techniques such as spoofing, log cleaning, zombied accounts, and Trojan commands.

Ref:

4. Obfuscation

Obfuscation stage is where attackers gain as much time as possible to complete their task and cover their tracks.

During this stage attackers leave invalid bread crumbs to confuse incident response team while altering evidence such as deleting logs, altering timestamps, and creating decoy network traffic.

Ref: