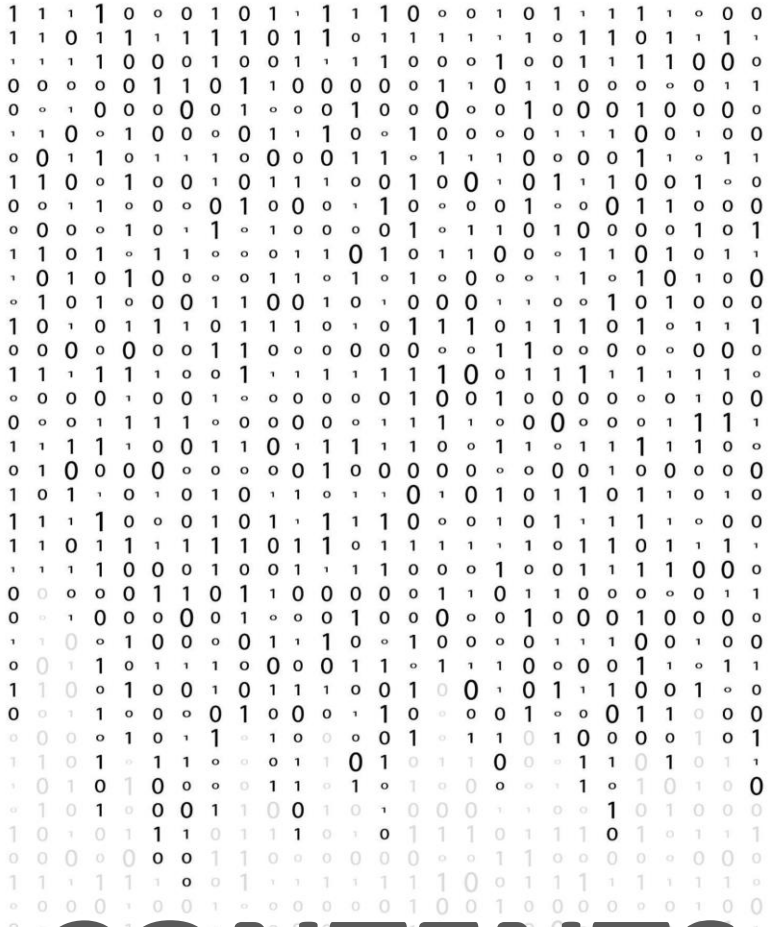
# INFORMATION SECURITY

## ATTACKERS AND TYPES OF ATTACK

PAULA QUEIROZ | JANUARY 2024



# CONTENTS

- Malicious Actors
- The Anatomy of a Hack
- Common Types of Attack
- Common Malware
- The Takeaway

PART 1

# Malicious Actors

# MALICIOUS ACTORS

## Types of hackers

The EC Council divides hackers in three main groups: black hats, white hats and grey hats, where each colour represents the type of relationship the individual (or group therefore) has with the system:

- Black hat hackers: unauthorised access
- White hat hackers: authorised access
- Grey hat hackers: sometimes white, other times black

This means that, although we “hackers” are commonly referred to as people who will gain unauthorised access to a system in order to exploit vulnerabilities, this isn’t necessarily always so, as follows.

# MALICIOUS ACTORS

## Black hat hackers

This is the type of hacker that generally comes to mind when we think of the word “hacking”. These are people who will identify systems vulnerabilities and gain unauthorised access to those systems in order to exploit them for malicious purposes - they are the “villains” of the hacking world.

Needless to say, there is a wide range of motivations for black hat hacking, and the type of damage caused can be as varied as the motivations. The end game might not be a financial gain (it might be, for instance, just causing disruption for the sake of it), but it is often so.

A “sub-group” of black hats is often referred to, in a derogatory fashion, as “script kiddies”. These will be individuals who, albeit the lack of significant technical skills, can be capable of launching attacks which might end up causing serious damage, simply by utilising tools already available and easily downloadable, which can even come with a GUI and instructions manual.

In any case, what must be retained concerning black hat hacking, are the simple facts that system access is unauthorised, and it has malicious intentions.

## White hat hackers

White hat hackers are the “good hackers”. These will normally be people with serious hacking skills who are hired by businesses to, through these use of these skills, identify vulnerabilities which, rather than being exploited, can be corrected as a means to prevent a malicious attack.

They will often be referred to as ethical hackers as, although they will attempt to identify security flaws often (but not always) using the same knowledge and tools as a black hat, they are authorised to do so, and their intention is to allow for the identification of vulnerabilities prior to their malicious exploitation, thus strengthening security by helping businesses spotting and closing closing any gaps.

Going back to the tools used, white hat hackers will tend to rely on industry-recognised tools built for the purpose of facilitating the identification of shortcomings in security. They also tend to be certified as ethical hackers (or equivalent) which gives businesses a degree of assurance that they are properly trained and follow industry-recognised methodologies.

## Grey hat hackers

The definition of this sub-group varies slightly: although some will basically mix the colours white and black, resulting in grey, when referring to individuals who do white hat hacking as a day-job, and black hat hacking outside business hours, others consider them to be neither one, nor the other.

This second definition, which is the one used by the EC Council, will refer to grey hats as individuals who will, out of their own initiative (not hired or even authorised to do so), search for vulnerabilities which, rather than exploiting, they will inform businesses about.

When it comes to the sharing of this information, it can be done as “good samaritans” (not asking for anything in return), or basically as a means of extortion, when informing the target that a vulnerability exists, but requiring a fee in order to go any further, for instance providing information on how to fix it.

# MALICIOUS ACTORS


## Outsiders vs Insiders

Again, broadly speaking, when we refer to hackers, we tend to think about individuals on the outside trying to hack in. This is not always the case and it is a way of thinking that tends to lead into cultures of poor security within enterprises.

Now we'll be looking at:

**Outsider threats**, including
- Hacktivism
- State-sponsored hacking

**Insider threats**, including
- Wilful insider breaches
- Human error

# MALICIOUS ACTORS


## Outsiders threats

We generally have a good understanding of what threats coming from the outside look like, and we tend to have security controls following the concept of defense in depth in place to mitigate these. We'll look at different outsider attacks later on.

In broad terms, I would like to highlight or split outsider threats in terms of motivations, highlighting hacktivism and state-sponsored hacking as opposed to the stereotypical, ill-intentioned hacker that dominates our common understanding of what hacking looks like.

## Hacktivism

Hacktivists are individuals who resort of hacking as a means to fight for causes which they believe are worth fighting for.

Hacking in this case may come in the shape of gaining unauthorised access to data which can be used to expose situations which are believed to violate human rights, it can come with the goal of halting operations by entities which are claimed to do wrong to nature, etc - the common characteristic of all hacktivism is the fact that it consists of hacking in the context of activism (as the name indicates).

Whether or not we agree with these hacktivists, that's totally besides the point and, from an information security perspective, we do not make moral judgments of the validity of the motivations behind a hack - they are simply unauthorised individuals looking to exploit vulnerabilities in order to cause damage.

## State-sponsored hacking

State-sponsored hacking is a normal, daily job as seen from the perspective of the government which hires individuals to do precisely that - hacking. This obviously means that, in their country of origin/the country of which the government they are employed by, these people are working fully within the law.

The problem comes when the situation is seen from the other side, from the perspective of the target. To the target of any government-sponsored hacking, these individuals and the entities they represent are unauthorised outsiders using hacking skills to do something bad.

From attacks on electrical grids to meddling and steering the results of foreign elections, a number of high-profile state-sponsored hacks have been registered and widely discussed in recent years.

Hacking is, therefore, a powerful tool when it comes to rivalries between nations, with cyberwarfare being the extreme thereof, and a very real threat in today's world.

# MALICIOUS ACTORS

## Insider threats

Whilst many attacks may indeed come from the outside, insider threats are, according to some statistics, even more likely to cause serious damage than threats coming  the outside.Insider threats include but aren't limited to disgruntled or greedy employees who will exploit vulnerabilities willingly, they also include simple human error, as we can see if we google something like "worst security breaches on aws".

Insider threats come in two main shapes: wilful action and human error. In both cases, both security controls and good hiring, management and education practises are paramount, as discussed in a previous post.

## Wilful insider breaches

Sometimes people want to do damage (which can be done in many ways, from leaking data to destroying systems and crippling corporate operations) for many reasons of their own.

Unhappy employees may want to harm their employer, an employee whose employment is about to be terminated may want some sort of revenge, etc. Whatever the personal motivation, these individuals will use whatever level of access is granted to them within the corporate environment to cause troubles.

Needless to say, the higher the privilege set, the more and more insidious the damage caused.

## Human error

Humans make mistakes, there is no arguing against that. Any activity with involves human action comes with the inherent possibility of error, which is one of the reasons why we attempt to automate as much as possible.

Human error can come as a result of poor education or just a moment-in-time lapse of judgement, the stereotypical "pressing the wrong button by mistake", among others.

Enterprises must acknowledge that this is a threat inherent to the fact of working with humans - mitigation strategies (including training) and corrective/recovery measures may be put in place, but the danger itself cannot be eliminated: the security chain is only as strong as its weakest link, and the weakest link in infosec are always humans.

PART 2

# The Anatomy of a Hack

# THE ANATOMY OF A HACK


Any decent hack will normally follow a structure of five sequential steps:

**1. Reconnaissance**
**2. Scanning**
**3. Gaining access**
**4. Maintaining access**

and, finally,

**5. Clearing tracks.**

Good defense in depth will take into account every phase in lifecycle of a hack and attempt to halt it at every step so, in order to efficiently and robustly build this sort of defense, we need to understand the sequence we are implementing controls against.

# THE ANATOMY OF A HACK

## 1. Reconnaissance

Implicitly or explicitly, reconnaissance (also referred to as footprinting) is always the first step. At this stage, information about the target will be collected. This normally includes information about the network, host(s) and target-side individuals.

Reconnaissance can be done actively, through the use of dedicated tools, or passively by, for instance, exploring the contents of what your targets publish on social media, or it can be both.

At the end of this phase, you will come out with a bit of a “map” of your target you will have a broad but solid idea of what your target looks like and what it’s made of.

## 2. Scanning

As the name indicates, this phases consists of launching one or (normally) more scans that allow for the identification of precisely pinpointed weaknesses in your target.

Common scans will include vulnerability scanning, port scanning and network mapping, and software is readily available to perform these, either legally or not.

Whilst scanning for open ports, running services, active vulnerabilities, etc will allow for pinpointing what exactly can be attacked, network making provides a clear route to follow when doing so, by providing the typology of the target environment from a networking perspective.

# THE ANATOMY OF A HACK

## 3. Gaining access

Again, this phase is self-explanatory. This is when the hacker establishes access to the target system.

This phase will normally (but not strictly necessarily) including a privilege escalation step, where the individual gains privileged (administrator) access to the system.

Whilst admin access will certainly come in handy (for the obvious reasons), extremely high privileges are not necessary in order to inflict damage - think of classified data: we don't need the ability to alter it, access and leakage can be devastating enough on their own.

This is one of the reasons why we segregate access to different systems and don't repeat admin passwords across multiple hosts: once the hacker has escalated privileges within "A", we don't want those privileges to extend to "B" and, if an admin password is decrypted, we don't want them to be able to use precisely the same at every hop along their way.

## 4. Maintaining access

If we go back to the the different types of hackers, the difference between this phase and the previous becomes clear enough: following the CEH definition of a grey hat hacker, this individual will probably not be interested in staying connected to the target - the fact that they have managed to establish this connection may be enough to demonstrate that a vulnerability exists and proceed to target extortion.

On the other hand, the hacker may not be done and, for many different reasons, they may want to maintain access so they can go further in their attack.

This phase of a hack represents the entire window during which the hacker does (or tries to do) whatever they set out to do, and this can be many things.

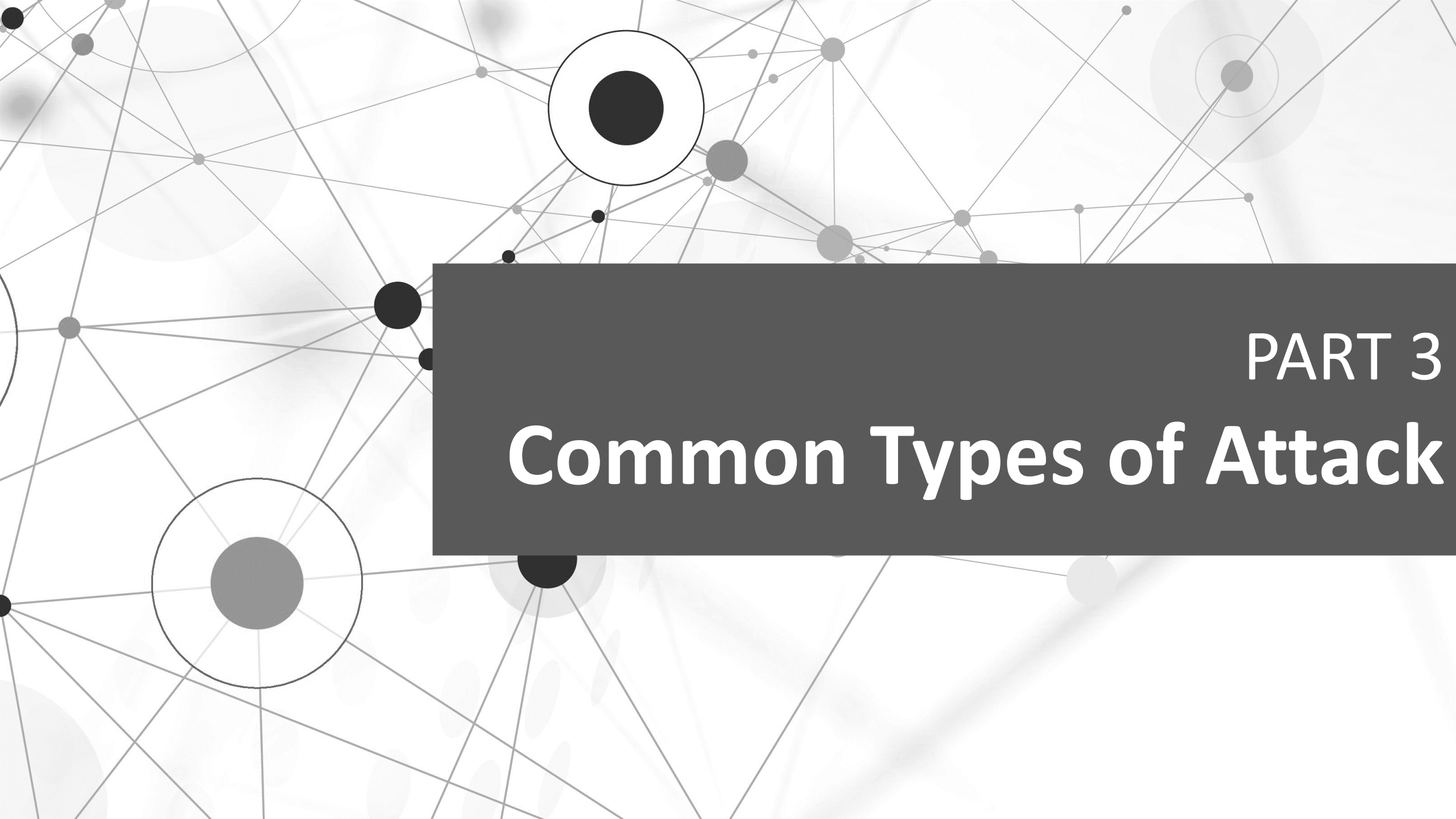
This is the stage at which privilege escalation becomes truly handy as the higher the level of access, the more the hacker will be able to do.

## 5. Clearing tracks

Straight off the top of our heads, two main reasons why a hacker will want to clear their tracks will pop up: the hacker obviously doesn't want to be caught and, in many cases, the hacker won't want the target to realise they have been hacked.

Concerning the latter, this will largely depend on the goal of the hack itself as, very often, the longer the hack goes unnoticed, the more damage it will have inflicted when it's finally identified.

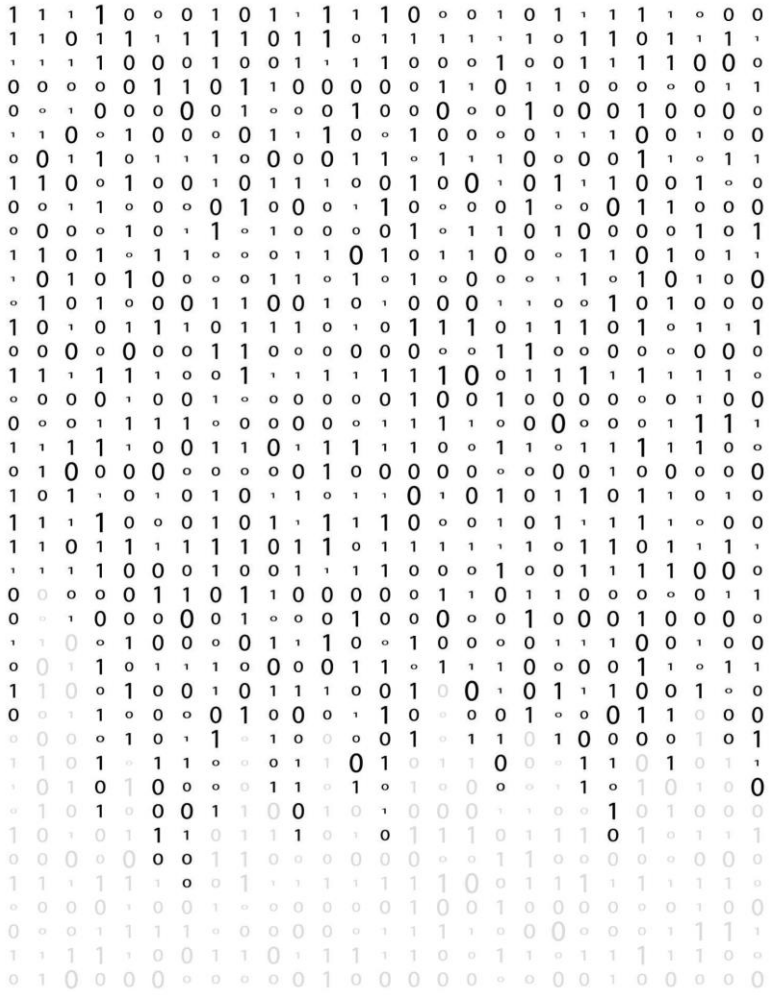
**When, in an earlier document, we spoke about the CIA triad and the value of unaltered logs, here they are of the utmost importance as modification, corruption and deletion thereof will most certainly be in a decent hacker's plan, which is why having safe, unalterable copies of such logs is so very important.**



PART 3

# Common Types of Attack

# COMMON TYPES OF ATTACK



The following is obviously not a comprehensive view of all there is and all we are potentially exposed to in terms of attacks.

**However, by listing some of the most common types of attacks and providing a high-level description of each, my goal is just to provide an idea of what we are most likely to be targeted by, and what our security controls must, at its most basic, be absolutely prepared to handle.**

I dare saying that, an enterprise which is not prepared to react to at least these, is an enterprise which is not prepared in terms of information security at all.

# COMMON TYPES OF ATTACK

## DoS and DDoS

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are attacks which, rather self-explanatorily, aim at service disruption - services are denied to their consumers.

These can technically be a great number of things (for instance TCP SYN flood attacks, teardrop attacks, smurf attacks, ping-of-death attacks, botnets, etc) all of which have the above in common. The way they normally work is by stretching a system's resources beyond its capacity, causing it to either malfunction or, depending on the specific system and configuration, shut service down.

The difference between the two is the number of hosts used to attack the target, where, if the attack is distributed (DDoS), a number of different hosts (the more hosts, the more stress will be put on the target) are used simultaneously during the same attack.

DDoS is normally achieved through the use of hosts which have been compromised by malicious software, which renders them controllable by the attacker - if this is the case, we are often talking about a botnet attack.

DoS and DDoS attacks might be a part of more complex attacks. Grinding a certain service to a halt (for instance, security equipment which goes down) can be the first step before gaining control of another system which the former is supposed to protect, as we'll see next.

## TCP SYN flood attacks

Here, the buffer space during a Transmission Control Protocol (TCP) session initialization handshake is exploited.

The target system's small in-process queue is flooded with connection requests, which go unanswered by the attacker's system.

The target will time-out as its connection queue fills up whilst waiting for these replies, and it will either malfunction or crash.

To protect ourselves against TCP SYN flood attacks, we place hosts behind firewalls configured to stop inbound SYN packets. Additionally, we may also increase the size of connection queues and decrease the timeout on open connections.

# COMMON TYPES OF ATTACK

## Teardrop attacks

Teardrop attacks will cause an overlapping of length and fragmentation offset fields in sequential IP packets.

Given the nature of TCP/IP, the target will attempt to reconstruct these packets but will not be able to do so.

Whilst attempting to make sense of the information it is receiving, the target will become unstable and end up crashing.

SMBv2 and ports 139 and 445 will normally be disabled as a protective measure against such attacks, and security patches also tend to be available for the same purpose.

## Smurf attacks

These attacks rely on IP spoofing and ICMP which will attempt to increase traffic in the target network to a degree which it cannot handle.

ICMP echo requests launched from a spoofed host are launched against target broadcast IP addresses.

The ICMP echo requests are repeatedly sent to all IP addresses within the network range where the spoofed host sits, and all replies are sent back to the host the request originated from.

This results in huge amounts of network traffic which may result in serious network congestion.

We protect ourselves against these attacks by disabling IP-directed broadcasts at a router level and/or by configuring devices so as to not answer ICMP requests from broadcast addresses.

## Ping of Death

Here we exploit the maximum IP packet size (65,535 bytes) by sending the target fragments of a packet which, when assembled, weight more than this maximum.

When the host tries to assemble the oversized packet, it will become sluggish and/or unstable with, for instance, buffer overflows.

As a means to protect ourselves against this, we will place hosts behind firewalls which calculate the sizes of the packet once assembled. If, when the fragments are put together, the packet size exceeds the maximum value, the firewall will drop them before they reach the target.

# COMMON TYPES OF ATTACK

## Botnets

Botnets are C&C (command & control) networks made of huge collections of hosts which will normally have been infected by malicious software, rendering them controllable by a hacker.

These hosts are called bots or zombies, and they will normally be geographically dispersed, making them harder to spot as the traffic looks more “genuine” than if it all came from the same location.

The likelihood of being victims to such an attack is decreased by RFC3704 filtering (for denial of traffic from spoofed addresses and verification of its correct source) and “black hole filtering” (where, once a DDoS attack is spotted, a BGP host will send out routing updates to ISPs which start routing all traffic directed at the target to a null0 interface).

## Man-in-the-Middle attacks

Man-in-the-Middle (MitM) attacks consist of an intruder who places themselves in the middle of client-server communications.

There are many types of MitM attacks, and we’ll look at some of those next.

## Session hijacking

An attacker hijacks a session between a client and a server using a machine which will use the client’s IP address.

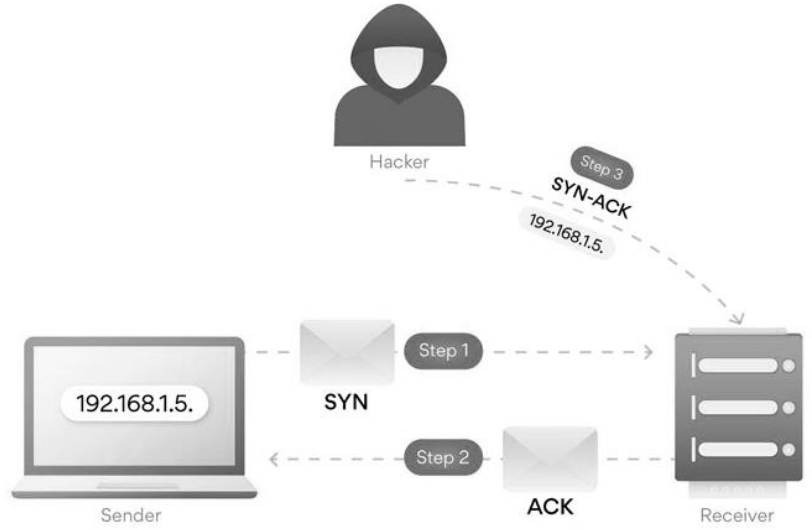
The attacker may first connect to the client, gaining control of it and terminating its session with the server whilst “stealing” its IP address and spoofing its sequence numbers.

The server will keep communicating with that IP address thinking that it’s still communicating with the client.

## IP Spoofing

In this attack, the attacker will target a victim using a packet which will look like it’s been originated by a known/trusted host’s IP address.

Since the target thinks the packet source is a trusted one, it will process it, regardless of its actual contents.



# COMMON TYPES OF ATTACK

## Phishing, Spear Phishing and Whaling

Phishing (and spear phishing, and whaling) is a bit like fishing with a “f”, except that it’s done by email but, in conceptual terms, it works mostly the same way: the bait is released and the attacker waits to see who bites it.

There is a heavy social engineering component to successful phishing, as there is an obvious need to make the bait as appealing as possible to its audience. Phishing emails can be about winning prizes, participating in social action, etc.

A decent phishing email will have to look credible, normally emulating the layout of emails from known credible sources (spoofing), and the action it requires the target to perform (for instance, clicking something to install a piece of malicious software, or being redirected to a malicious website, ie through website cloning) needs to appear to the target as something they think is needed/worth doing.

The difference between the three, phishing, spear phishing and whaling lies mainly on the target.

# COMMON TYPES OF ATTACK

## Phishing

In “simple” phishing, the audience will be rather large and largely indiscriminate. There is no targeting of a single individual, so there will be no personalisation of contents. The larger the target audience, the greater the chances that someone will take the bait. In a way, it’s a bit like launching a fishing net off a ship and waiting to see what the day’s catch will be.

## Spear phishing

Spear phishing, on the other hand, is targeted at a specific audience, normally senior corporate staff, so there is a considerable degree of target research required. Messages will look personal and appealing to the individual (hence the need for research - to make something appealing to the individual, we need to know what is it that appeals to them).

When it comes to spear phishing (and whaling), spoofing becomes very important, as the more legitimate the sender looks, the more likely the target is to perform the action required (for instance, someone pretending to be a senior manager in the business you work for, needs to appear to be sending the email from an account that matches the business domain).

The same goes for phishing that requires targets to navigate to malicious websites: the target is unlikely to share (for instance) banking information on a website which doesn’t look like their bank’s legitimate one, so cloning is paramount.

## Whaling

Whaling is a very specific type of phishing where the attacker will try to impersonate someone very high up on the corporate hierarchy in order to gain the perceived authority to tell staff (normally management-level staff) to do something (again, installing malicious software, navigating to malicious websites, etc).

The fact that this type of phishing is not only targeted (like spear phishing) but also includes this additional layer of deception (impersonation of someone of authority) makes it potentially more destructive but also theoretically harder to execute, and increasingly so as corporations will currently tend to train staff on how to spot potential phishing attacks.

When it comes to phishing (like much in terms of information security in general), education is the best layer of defense, so infosec training campaigns should always be invested in by enterprises who wish to harden what is normally the most vulnerable layer in their security strategy: people.

# COMMON TYPES OF ATTACK

## Drive-by attacks

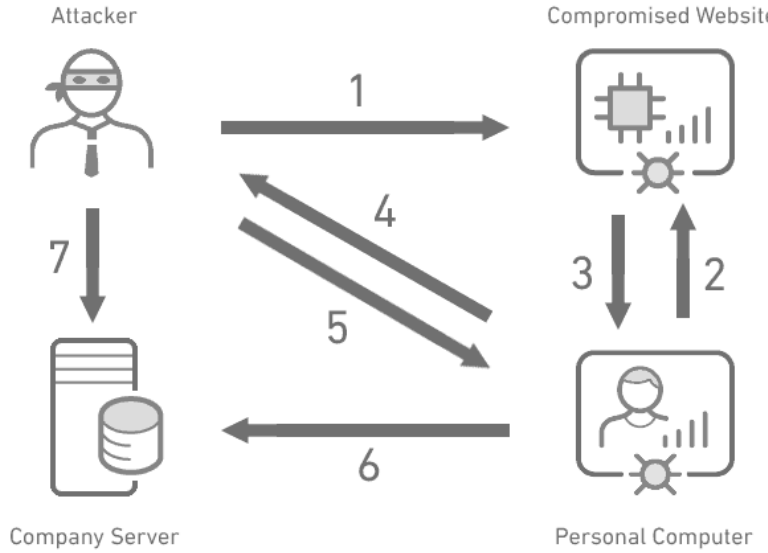
Drive by come attacks come as an efficient alternative to cross-site scripting (which is a bit hard to execute as most webapp hosting server will be hardened with anti-malware solutions) by making use of mostly common HTML vulnerabilities, through injection.

Drive-by attacks basically consist of malicious code injection on a vulnerable website. Once the malicious code is in place, these attacks are very efficient as a means of, for instance, spreading malware, as they not require users to click any button or perform any action other than navigating to the infected website.

In today's world, drive-by attacks are considered to be technically challenging to execute (we will normally have tools in place to check code security, for instance and, theoretically at least, developers are increasingly well trained in the matters of secure development).

From a business (site owner) perspective, hiring the right people to do development, with the right skill-set encompassing security, and the use of code verification tools for security purposes is extremely important.

### Example of a drive-by attack sequence




1. **Injection**: the attacker embeds or injects a malicious element into a compromised web page.
2. **Vulnerability exploits**: the user views the page, triggering the malicious element. The element exploits a vulnerability in a part of the software stack on the user's computer.
3. **Injection**: the attacker embeds or injects a malicious element into a compromised web page.
4. **Vulnerability exploits**: the user views the page, triggering the malicious element. The element exploits a vulnerability in a part of the software stack on the user's computer.
5. **Download**: the element downloads malicious files silently to the user's device. In this example, the payload is a Trojan horse. Attackers may use other payloads.
6. **Execution**: the Trojan horse (in this example) executes, opening a shell the attacker can use to gain control over the device.
7. **Remote control**: the attacker gains remote control. This enables them to extract valuable data from the user's device.
8. **Lateral movement**: the attacker can now use credentials obtained from the user's device to connect to another, more valuable system, such as a company's website or network.

# COMMON TYPES OF ATTACK

## Password attacks

We're probably all pretty familiar with password attacks, from simple "password guessing" to standard dictionary-based brute-forcing to rainbow tables, we are presumably all, at the very least, more or less familiar with the concept of a "password attack".

Password attacks are as common as common gets in terms of infosec so enterprises (and users at home) must always go for strong passwords and (in the corporate context) implement password policies including minimum number of characters, complexity, forbidden words, password age, account lockouts, etc.

## Eavesdropping attacks

Eavesdropping attacks consist of interception of network traffic in order to obtain valuable information in transit. It can be done either passively or actively.

Whilst passive eavesdropping is done by simply sniffing network traffic, active eavesdropping (tampering, probing or scanning) involves disguising as a "benign" node and sending out queries.

Encryption is considered to be the best protection against eavesdropping.

## Birthday attacks

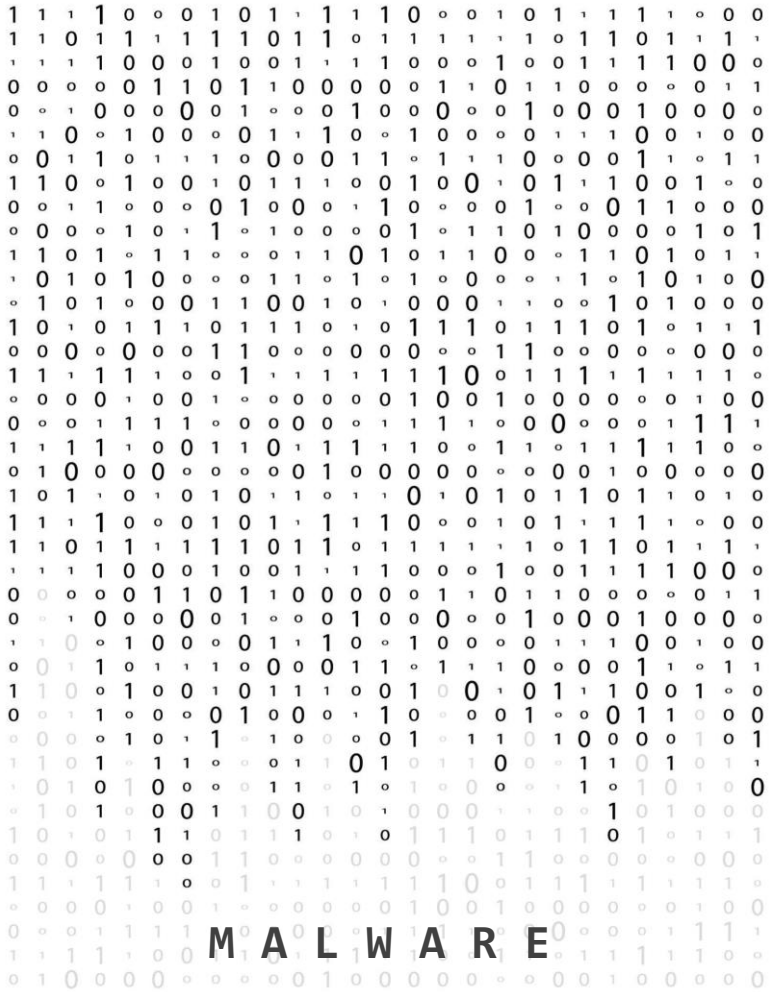
These are attacks targeting the hashing algorithms used to verify data integrity. When data (ie a message) is processed through a hash function, a unique message digest (MD) is generated.

The birthday attack involves a malicious message with an MD engineered to be the same as that of the legitimate one. If this is achieved, then the legitimate message can be replaced with the malicious one and the receiver won't be able to tell the difference as the MD is the same.

PART 4

# Common Malware

# COMMON TYPES OF MALWARE




**In terms of cyber security threats, malware is an universe in its own right so, albeit there being far more types of malware than those described here, we'll just look at a few for illustrative purposes.**

# COMMON TYPES OF MALWARE

## Ransomware

- Ransomware has the purpose of denying a victim access to their own data, with the threat of either destruction or disclosure unless a ransom is paid - hence the name.
- Most modern ransomware attacks rely on cryptoviral extortion, which is when the victim's data is encrypted, and the victim will only be given the decryption key if the ransom is paid.
- Ransomware is one of the reasons why businesses who store large amounts of data invest in airgapping technologies and perform WORM backups.

## Spyware

- Spyware can take many shapes and have many specific purposes, but it always basically consists of a piece of software normally installed in a victim's system to collect information about users, configurations, behaviours, etc. without the victim's knowledge.
- Depending on the specific piece of spyware, it can also silently install other malicious programs.
- One of the most common ways to get spyware installed on a victim's machine is by associating it to a piece of freeware the victim wilfully installs without knowing that the spyware is included in the package.

## File infectors

- These viruses are usually attached to existing executable code (ie .exe files), but some file infectors might create virus files with the same name instead.
- In either case, the virus code is executed when the file is opened.

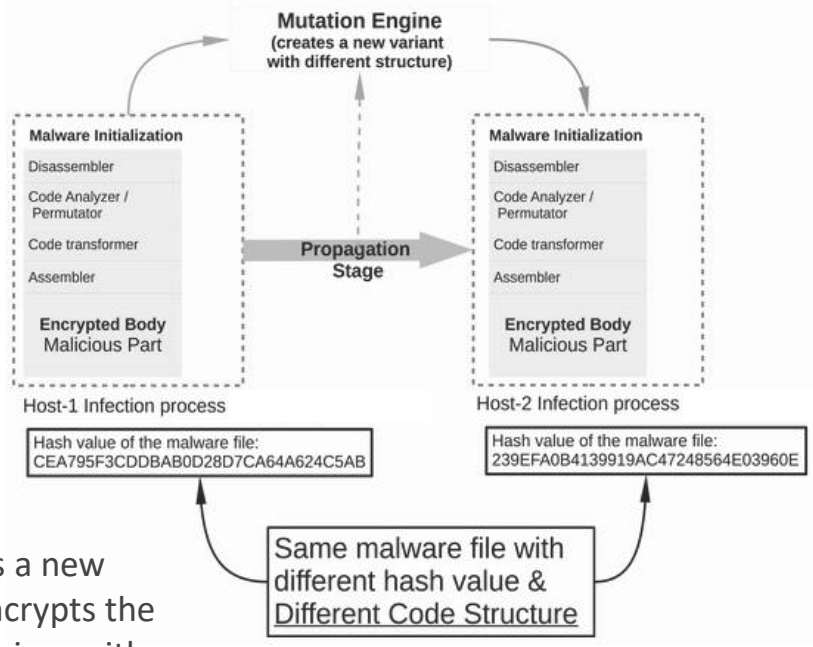
## Boot-record infectors

- System or boot-record viruses attach themselves to the master boot record on hard disk drives.
- When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.

# COMMON TYPES OF MALWARE

## Polymorphic viruses

- Polymorphic viruses always come with a mutation engine and hide themselves through cycles of encryption and decryption.
- The encrypted virus and the mutation engine are initially decrypted by a decryption program. The virus proceeds to infect an area of code.




- The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine.
- The encrypted package of mutation engine and virus is attached to new code, and the process repeats.
- Polymorphic viruses are hard to detect but have a high level of entropy, which enables a number of commercial antivirus/anti malware solutions to detect them.

## Logic bombs

- A logic bomb is a piece of malicious software attached to an application, which is triggered by a specific event, such as a logical condition or a specific schedule.

## Trojans

- Trojans are pieces of malicious software that hide in legitimate programs. Unlike viruses, Trojans do not self-replicate.
- Trojans can launch attacks on their hosting system and/or establish backdoors to be exploited by attackers.

## Worms

- Unlike viruses, worms don’t get attached to host files, instead, they are self-contained, independent pieces of software that propagate across systems and networks.
- The most popular way of spreading worms is via email and worm activity can, amongst others, result in systems’ DoS across the network.

PART 5

# The Takeaway

# THE TAKEAWAY

**Whether perpetrated/allowed to happen by ousiders or insiders, whatever their motivations may be – if there is a motivation at all as, as we've discussed, numerous security incidents are caused by honest mistakes – enterprises of all sorts and sizes are intrinsically exposed to a large number of security risks which will only keep increasing with the complexity steadily, continuously added to our systems and processes.**

What there is to be done about it is not an "off the shelf", "one size fits all" solution, it is rather a blend of controls ranging from pure technology to human factors, including, but not exclusive to:

- ✓ Good hiring and termination practices.
- ✓ Continuous training and sensibilization, including non-IT staff.
- ✓ Related to the above, stopping "black box-style" infosec, making security everyone's business.
- ✓ Adhering to recognised security best-practices.
- ✓ Following proven frameworks adapted to the business nature and needs, including a robust RFM implementation.
- ✓ Keeping track of the technological estate, knowing what we have and how we protect it.
- ✓ Keeping track of the threat landscape outside the enterprise, and adapting to it.
- ✓ Adding technical controls to human factors to create robust defense in depth, not forgetting complexity vs manageability.
- ✓ Dedicating serious time and resources (human and financial) to information security is always crucial.

# THE TAKEAWAY

**I hope this helps!**