COMPUTER FORENSICS AND CYBER CRIME ANALYSIS

Thats a lot of words in the title

Fabio Lorenzato

Contents

Part I

Legal part

Chapter 1

Introduction

Back in the days, it was really easy to analyze the communication between two people, because the technology was easier and know, meaning that the technology is *between us*. Nowadays the technology is more *about us*, for example we use AI for facial recognition. Another example are the social network algorithms that track our activity online. This means that we use the technology to be ”analyzed” instead of using it only to communicate. Most likely, the technology will be *in us*, which not only means robotics, but also be more integrated with human beings.

In those scenarios, computer forensics became more complex, having to take in account no only the quality of data(ie: a voice call), but also the quantity, which makes mistakes more likely to happen in some instances. Another aspect of computer forensics will be to discern what is human from what is a machine(ie: deep fakes, generative ai), and in particular where the liability lies. Furthermore, it is necessary to handle the legal aspect of different countries, which is quite difficult because of natural language limitations. An ideal solution would be to translate laws in code, which is basically impossible, so we can approximate this solution with **legal design** This has still to deal with two issues, which are information overloading(too much information), and the fact that laws are written by lawyers for lawyers, which makes them difficult to understand.

Another aspect to consider is the GDPR, and the still to come AI act, for example the article 22 prevents automatic systems to make decisions having legal weight without the control of a human. An example of this is the Lex Machina framework, which was able to predict the decisions of the judges via ML methodologies, which was banned because it could influence the decisions of people and judges. After all, false positives in digital forensics **can change people lives**.

Chapter 2

Foundations of digital forensics

First of all, lets define what can be considered digital evidence. There are many definition but the one that is most commonly used,and the preferred one at the exam, is:

> **Digital evidence** is *any* information of evidential value whether memorized or sent in a **digital format**.

Digital evidence has some defining characteristics: it is invisible to the untrained eye (it usually not simple to find), it may need to be interpreted by a specialist, it may be altered or destroyed trough normal use and it can be copied without limits (you must always work on a copy to avoid tampering evidence).

Digital evidence, to be admissible in court, must have some properties:

- **Authenticity**: avoid any digital evidence **tampering**. Only certified formats should be used.
- **Reliable and believable**: the evidence must be redly **understandable** to the judge. Sometimes a report is not available to explain the evidence, so it must be self-explanatory.
- **Proportional**: **respect** fundamental **rights** of parties affected by the measure
- **Admissible**: **compliant with law** and best practices(admissible in court). One thing is to have evidence, the other is to have it admissible in court, and that's not always the case.

There are three main kinds of digital evidence:

- **Created by man**: any piece of digital data that is the result of a step or action taken by a human person. Of those, there are two types:
  - **Human to human**, such as an email
  - **Human to machine**, such as a file saved on a disk
- **Created independently by the computer**: any piece of digital data that is the result of the processing of data carried out by a software in accordance with a specific algorithm and without human intervention (e.g. telephone records or Internet Service Provider logs)

- **Created by both man and the computer**: an electronic spreadsheet where data is entered by the human, while the computer works out the result.

Lets now define what digital forensics is:

> **Digital forensics** is the process of getting hold of evidence without modifying the IT system in which the evidence is found, ensure that the evidence acquired in another medium is identical to the original and analyze the evidence without modifying it.

The "Big Five" of digital forensics

There are some principle that are to be followed during digital forensics:

- **Data Integrity**: No action taken should change electronic devices or media, which may subsequently be relied upon in court.
- **Chain of Custody**: An audit trail of all actions taken when handling electronic evidence should be created and preserved.
- **Specialist Support** If investigations involving search and seizure of electronic evidence it may be necessary to consult external specialists.
- **Appropriate Training**: First responders must be appropriately trained to be able to search for and seize electronic evidence if no experts are available at the scene.
- **Legality**: The person and agency in charge of the case are responsible for ensuring that the law and the above listed principles are adhered to.

2.1 Digital Investigation Procedure

Digital investigation is carried out in many steps.

2.1.1 Identify the Suspect

The first phase is also the most difficult one, because there are many tools to be anonymous in the internet. The general approach to this phase is the following:

1. An investigator receives a **complaint** by a victim of **cybercrime** or detect an illegal content on line. (OSINT can be used to detect illegal content)
2. The investigator uses the Court System to compel the ISP to **reveal** a **physical location** that corresponds likely to the source of Network (**IP Address**)
3. Under a **warrant** (depending from the Jurisdiction) the location is searched and any computer or other device is seized

But why the ISP has to cooperate and give away the IP address? In the EU it is because **Data Retention Directive** 2006/24/EC, that requires that all the data of the communication must be stored for a certain amount of time, from 6 to 24 months. This directive was unconstitutional in many countries,

> **Data retention** (or data preservation) generally refers to the **storage** of call detail records (CDRs) of telephony and internet traffic and transaction data (IPDRs) by governments and commercial organizations

In any case data retention is usually a problem because there's no a homogeneous law for data retention, mainly for privacy reasons.

Even if there's no data retention law, the request of user data disclosure have been a lot in the past years have steadily increased, because the processes have been automated, as you can also see from figure 2.1.

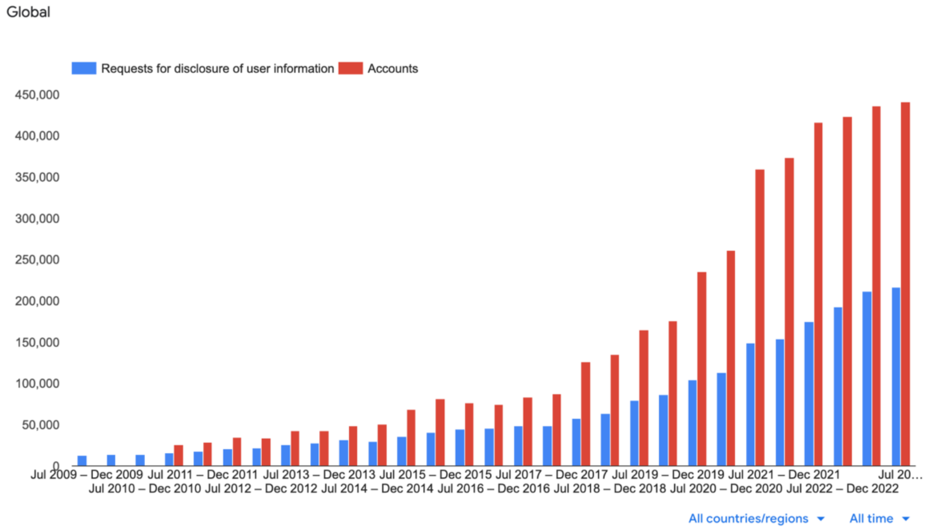

Figure 2.1: Requests for user data disclosure during the years

Another instrument that could be used to identify the suspect is the **facial recognition**, that can be used only for terrorism situations, but not in a systematic way.

2.1.2 Detecting and Seizing Digital Evidence

Anyone wanting to seize and validate digital/electronic evidences (content of an e-mail or an entire hard-disk) has to respect two fundamental **rules**: Bit-Stream Copy and Hash Function.

Bit-Stream Copy

> A **bit-stream copy** can **clone** the **entire drive**.

It is a particular form of duplication in which the content of the physical unit is read sequentially loading the minimum quantity of data that can from time to time be directed, then recording it in the same sequence on a standard binary file, generating a physical image of the original medium.

Hash Functions

During the forensic analysis of modifiable media, the Hash guarantees the intangible nature of the data that it contains.

> The Hash is a **one-way function**, by means of which a document of random length is converted into a limited and fixed length string.

This string represents a sort of 'digital fingerprint' of the non- encrypted text, and is called the Hash Value or the Message Digest. If the document is modified, even to the slightest extent, then the fingerprint changes as well. In other words, by calculating and recording the fingerprint, and then recalculating it, it can be shown beyond all doubt whether the contents of the file, or the medium, have been altered, even accidentally.

In any case we have two main problems while acquiring data: encryption and jurisdiction. After all, the ISP, TELECO or even a bank does have to cooperate and give out the data. Another big issue it the cloud computing aspect, because the location of data is another big problem, because it can be either:

- **at rest**: does not reside on the device.
- **in transit**: cannot be easily analysed because of encryption.
- **in execution**: will be present only in the cloud instance

Validation of digital evidence is a very important step, because it is the only way to prove that the evidence is authentic. This is especially important for proof found on the internet. There are some tools that can be used to validate digital evidence, such as Web Forensics. Another issue that has to be accouted for is the **chain of custody**, that is the process of maintaining and documenting the location and handling of evidence. After all, the bit is eternal, but the storage medium is not.

2.1.3 Validating Digital Evidence

2.1.4 Chain of Custody

2.1.5 Analysis of Digital Evidence

2.1.6 Presentation in Court

Chapter 3

Cybercrime Convention

Because this part it *really boring* we will start with an example.

3.1 E-commerce on the Dark Web

The Dark Web provides a **platform** for buyers and sellers to engage in e-commerce transactions, often involving **illicit goods and services**, like guns, fake documents etc.. This anonymous marketplace operates with the same principles as traditional e-commerce, but with heightened security and privacy measures to conceal identities.
Vendors on the Dark Web offer a wide range of products, from drugs and weapons to stolen data and hacking services. Buyers can browse listings, read reviews, and complete purchases using cryptocurrencies, all while maintaining a high degree of anonymity.

3.1.1 Silk Road

Silk Road, often referred to as the "eBay of drugs," was an **online marketplace**that facilitated the sale of a wide range of illegal substances, including narcotics and controlled substances. At its peak in 2013, Silk Road had a reported annual revenue of $89.7 million.

- **Combining Tor, PGP, and Bitcoin**: Ross Ulbricht leveraged the anonymity of Tor, the encryption of PGP, and the decentralized nature of Bitcoin to create the Silk Road marketplace.
- **Bitcoin-only Payments**: Silk Road required all transactions to be conducted using Bitcoin, providing an added layer of anonymity and making it harder to trace purchases.
- **User-friendly Interface**: Silk Road featured a well-designed interface that allowed users to easily navigate the site and leave feedback on their transactions.
- **Intermediary Role**: Silk Road acted as an intermediary between buyers and sellers, handling the payment process and logistics of shipping items purchased on the marketplace. This is one of the main sources of success of the platform.

At its peak, Silk Road had over 950,000 registered accounts, 1.2 million transactions, and nearly $79 million in commissions. Ulbricht was arrested in 2013 due to some critical mistakes, like using its personal email to advertise the website and having counterfeit documents delivered to his home address when he found out that he was on investigation.
Ulbricht faced 7 key charges, including drug trafficking, money laundering, and computer hacking, which were consolidated into 3 main counts against him and the trial ended in just 13 days with a life sentence plus 180$ million in damages.
What we can learn about this? First, the anonymity is really an issue with ongoing investigations, but everyone can make mistakes, which means that eventually, the law will catch up with you. Second, everyone can create this kind of platform, which implies that is necessary to solve the issue. For this purpose, cooperation is most fundamental, and the Budapest Convention is the first step in this direction, by creating standards and protocols for international cooperation in this field.

3.2 Budapest Convention

The Budapest Convention on Cybercrime is an international **treaty** that aims to address the challenges posed by cybercrime and promote cooperation among countries in combating these offenses. It has three main purposes:

- Harmonizing national laws on cybercrime
- Improving investigative techniques
- Increasing international cooperation

In involves **68 countries**, including the United States, Canada, and many European nations.

> Keep in mind that the council of Europe and the European union are two different entities. The first one is able to invite entities that are outside of the latter one.

Some countries opposed to the convention like India, which has since reconsidered, and Russia, which rejects it due to concerns about sovereignty and refuses to cooperate too.
Other states has signed but no ratified (Ireland and South Africa), which means that they are not bound by the convention(in this case is just a principle declaration, without legal value).

> The **difference** between signing and ratifying a treaty is that **signing** a treaty is a **preliminary step** that indicates a country's **intention to be bound** by the treaty, while **ratifying** a treaty is the **formal act** of **accepting** the treaty and agreeing to be bound by its terms. A country can sign a treaty without ratifying it, but it cannot ratify a treaty without signing it first.

The convention aims to help in the **fight against crimes** that can only be committed through the **use of technology**, where the devices are both the tool for committing the crime and the target of the crime, and crimes where technology has been used to enhance another crime, such as fraud. It **provides guidelines** for any country **developing domestic laws on cybercrime**and serves as a basis for international cooperation between parties to the convention but was later expanded to cover other areas of crime, such as hate crimes.

3.2.1 Original key provisions

The original convention was adopted in 2004 and covers:

- the **criminalisation** of **conduct**, ranging from illegal access, data and systems interference to computer-related fraud and dissemination of child abuse material;
- **procedural powers** to **investigate cybercrime** and secure electronic evidence in relation to any crime;
- **efficient international cooperation** between parties.

Parties are members of the Cybercrime Convention Committee and:

- **share information** and **experience**;
- **assess implementation** of the convention;
- **interpret** the convention through **guidance notes**.

Of the 27 Member States, 26 have ratified the convention. Ireland has signed but not yet ratified it.

3.2.2 Additional Protocol 1(2006)

This protocol extends the scope of the convention to cover xenophobic and racist propaganda disseminated through computer systems, providing more protection for victims.
It furthermore:

- reinforces the legal framework through a set of guidelines for criminalising xenophobia and racist propaganda in cyberspace;
- enhances the ways and means for international cooperation in the investigation and prosecution of racist and xenophobic crimes online.

3.2.3 Additional Protocol 2(2024)

This protocol aims to further enhance international cooperation.
It addresses the particular challenge of **electronic evidence** relating to cybercrime and other offences being held by service providers in foreign jurisdictions, but with law enforcement powers limited to national boundaries.
Its main features are:

- a new **legal basis** permitting a **direct request to registrars** in other jurisdictions to obtain domain name registration information;
- a new **legal base** permitting **direct orders to service providers** in **other jurisdictions** to obtain subscriber information;

- **enhanced** means for **obtaining subscriber information** and **traffic data** through government-to-government cooperation;
- expedited **cooperation** in **emergency situations** including the use of joint investigation teams and joint investigations.

3.2.4 New Global Cybercrime Treaty

The Budapest Convention has been a model for other countries and regions in developing their own cybercrime laws and treaties.
The **United Nations** has also been working on a new global cybercrime treaty, which would build on the Budapest Convention and expand its scope to cover new forms of cybercrime and emerging technologies.
We will see it later on.

3.3 Harmonization of national laws and international cooperation

3.3.1 International Cooperation Provisions

This provision s based on a very simple principle.

> Parties are to cooperate "to the **widest extent possible**" in investigating electronic evidence.

This is necessary because mutual assistance is often slow and can even take months to complete(3 up to 6). The Mutual assistance agreement(thanks to the Cybercrime convention) allows for expedited requests using "expedited means of communication", which means that, to an expedited request, one must provide adequate levels of security and authentication(eg. encrypted communication).
Furthermore, parties may share information without a formal request if it would assist in investigations or help the receiving party with any related offences.

3.3.2 Mutual Assistance Provisions

Procedural Powers for Assistance grant the ability to expedite the preservation of stored computer data, as well as the disclosure of traffic data. In addition, they allow for the real-time collection of traffic data and the interception of content data. Assistance in these matters is provided in accordance with domestic laws and applicable treaties, subject to any reservations.
Article 23, which outlines the General Cooperation Principle, emphasizes that mutual assistance should be offered to the widest extent possible. This applies specifically to cyber-related offenses and the collection of electronic evidence for any criminal offense.
However, there are restrictions to this cooperation. These limitations may arise in cases related to extradition, mutual assistance in the real-time collection of traffic data, and the interception of content data.

3.3.3 24/7 Network for Immediate Assistance

Each party is required to designate a contact point that is available 24/7. The primary purpose of this contact point is to provide immediate assistance in cybercrime investigations, legal proceedings, or the collection of electronic evidence. This system is modeled after the G8 network of contact points.

The goal of this provision is to expedite the processing of urgent mutual assistance requests by overcoming delays associated with traditional bureaucratic channels.

Part II

Technical part

Chapter 4

Introduction to digital forensics

First of all, we need to understand some basic concepts.
Forensics analysis is the process of investigating and analyzing information to gather evidence to solve legal problems. In order to do that, the collections, presevation and analysis or presentation of digital evidence is required to support the investigation. **Computer forensics** does just that.
Forensic science is not a new field, it has been around since the ancient times. The first recorded use of forensic science was around 1900 BC in Babylon, where fingerprints were used to identify the author of a clay tablet. Digital forensics is a relatively new field, it started in the 1980s with the advent of personal computers, for example the first convicted person for digital crimes was Robert Tappan Morris, who created the Morris Worm in 1988, and found out by analyzing computer logs and network activity.

> **Computer Forensics** is the **discipline** that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

In general, when carrying out a forensic investigation, the following questions are important to keep in mind to fully understand the crime scene:

- **What** happened? What is the timeline of events?
- **Who** was involved?
- **When** did it happen?
- **Where** did it happen?
- **How** did it happen?
- **Why** did it happen?
- **How** did the incident occur?

All this questions allow to **support legal proceedings**, the mitigation of damages and mature future prevention strategies.

4.1 Computer forensics goals

The main goals of computer forensics are:

1. **retrieve** the **input** data(ie: what has been typed)
2. **determine** the **actions** performed by the user (ie: what programs have been run)
3. **analyze** the **used files** (ie: what files have been modified)
4. **identify** the **damage** done to the system (ie: what files have been deleted)

> In essence, the goal of computer forensics is to **gain conprehansion** of **what happened**, at least technically speaking.

4.2 CF terminology & relevant concepts

Before going any further, we need to understand some basic concepts and terminology used in the field of computer forensics.

For a definition of **digital evidence**, we can refer to definition 2. In general, we can expect to deal with different types of digital evidence, because they can use different level of **abstraction**. Most of the time that are fragile, because they can be easily modified or destroyed, which is undesirable during forensics investigations. Its also difficult to correlate connection between data and real events, and to prove that correlation in court.

Another important concept is the **chain of custody**.

> The **chain of custody** is the **documented** and **unbroken process** of handling evidence, from the moment it is collected to the moment it is presented in court.

This is important because it ensures that the evidence is not tampered with, or even accessible by unauthorized personnel, and its most important to ensure that the evidence is admissible in court. For those reasons it requires knowledge about logging procedures, secure storage and legal protocols, because many security measures are required to ensure the integrity and confidentiality of the evidence.

> **Data Acquisition** is the process of **collecting evidence** from devices without altering or damaging the original data.

This is one of the most subtle one, because it requires a deep knowledge of how memory works, because it may be required to do disk imaging when the data is at rest or even live data acquisition when the data is in use. In any case, understanding of whats going on in memory is required to avoid data corruption and tampering.

> **Write Blockers** are hardware devices, or software tools, used to prevent any data from being written to a storage device during analysis, preserving the original data content.

Hardware write blockers are the most secure, because we don't have to trust that the software is behaving correctly, but are also more expensive. In any case, they are fundamental for legally defensible acquisitions.

> **Forensic Image** is a **bit-by-bit copy** of digital media, including deleted files and data in slack space, which is an exact replica of the original device.

This is a strict requirement for digital forensics, because it allows to preserve the original data, for example if the data is not exactly copied the same way, the result of an hash function will be different.

4.3 Forensics scenarios

When doing a forensic investigation, there can be different scenarios that can be encountered. Some common scenarios are:

- internet abuse from employee
- computer-aided frauds
- data unauthorized manipulation, like data theft or disclosure
- computer/network damage assessment
- . . . and any time digital evidences may be involved in an incident

4.4 Investigation phases

The investigation process can be divided into several phases, at least from a technical point of view. Those depends on the standards that are followed in a given country where the investigation is taking place(fore example in America the NIST standards are followed).

4.4.1 Identification

Its the first step of the investigation, an it take place when the crime scene has been accessed. The goal is to identify which are the potential sources of relevant that, which will be used as digital evidence if relevant.
Most of the time we have an overwhelming amount of data, but most of it is not relevant to the investigation. Reducing the amount of data is also a goal of this phase. On the other hand, it is also possible to miss some important data, so it is important to be careful.
It is important to recognize (all relevant) data sources before any acquisition begins, like:

- hard drives (HDD/SSD)
- memory (RAM)
- mobile devices (smartphones, tablets)
- cloud storage

- network traffic
- removable media (USB drives, DVDs)
- ...

The steps to follow in this phase are:

- if possible, acquire data before reaching the crime scene(pre-analysis), instructing the staff to identify possible sources of evidence
- perform an **initial survey** of the scene (physical or network environment)
- **identify key devices** and data locations (local storage, remote servers, cloud services)
- **check** for **connected devices**, including peripherals like printers, removable media, or network-attached devices
- **map** all potential **data sources** using network topology

Pay much attention to the ephemeral storage of data, with reference to the order of volatility. The order of volatility is a concept that refers to the order in which data should be collected, based on how long it will be available.

4.4.2 Collection

After the identification phase, one must physically or remotely taking possession of the evidence (e.g. a computer) and its connection (e.g. Network or physical, like USB disk). The timing is most crucial in this phase, while also maintaining the integrity of the evidence, to minimize the risk of evidence tampering or data loss.
The steps to follow in this phase are:

- isolate devices to prevent them from being tampered with remotely (e.g., disconnect them from the network)
- use devices to block external communication for mobile or wireless devices (e.g. faraday bags)
- use network isolation tools for virtual and cloud environments to prevent remote access (e.g security groups, virtual private cloud, firewall rule)

Its important to ensure the integrity of the evidence while maintaining the system running, because shutting it down can cause the loss of volatile data(e.g. RAM).

4.4.3 Acquisition

It refers to the process of electronically retrieving data by running various CF tools and software suite. Its a separate phase from the collection phase.

> It’s the process of creating a forensic copy (bit-by-bit image) of the original data to ensure that the acquired data is a faithful replica of the source while also maintaining data integrity

The acquisition method can be divided into two categories:

- **Static acquisition**: the data is acquired while the system is turned off, and the data is at rest.
- **Live acquisition**: the data is acquired while the system is running, and the data is in use.

Depending on the method used, the acquisition can be done in different ways and using different tools.

Static acquisition

Static acquisition can be carried out as follows:

- shut them down carefully to avoid losing data (e.g. for encrypted devices, consider methods for capturing data without triggering loss of access, for example before the decryption key is wiped from RAM)
- attach the device to a forensic workstation using a write blocker
- use forensic imaging tools to create a complete image of the storage device
- generate a hash value (e.g., SHA-256) of the original media before and after acquisition to verify integrity
- store the image on a secure forensic storage device

Be careful that the data is properly hashed and verified after the acquisition.

Live acquisition

Live acquisition can be carried out as follows:

- choose a method that minimizes system interference while capturing volatile data. This requires some knowledge of the system(FS, applications running, etc)
- dump RAM (memory acquisition) and capture data from running processes or network connections.
- perform network traffic capture
- document all acquisition actions and steps to ensure chain of custody and admissibility
- hash the volatile data wherever possible to maintain data integrity

Integrity

It ensure that the acquired data is an exact replica of the original and has not been altered. To do so, some steps are required:

- choose a method that minimizes system interference while generating a hash (MD5, SHA-256) of the acquired image or data dump
- compare the hash value to the original data hash (for static data) to verify its integrity

- document the hashing process, including the algorithms used and the results, in the chain of custody documentation

> Any discrepancies in hash values would require re-acquisition and could damage the credibility of the evidence

4.4.4 Evaluation

Now that all the data has been collected, it is time to evaluate it. In this phase the data is analyzed to substantiate claims and to determine how they could be used against the suspect.

4.4.5 Presentation

At last, the evidence is presented in a clear and understandable way to the court, in a manner which is suitable for lawyers, non-technical staff and the law.

Chapter 5

Non-trusted environment issues

Sometimes technical level, at low level is necessary, as well as the effect that our actions can have on the system(eg: misbehaving).
As such, the environment should not be trusted at all.

5.1 Compromise causes

Now we will see some of the most common causes of compromise.

5.1.1 Node infection

Some of the most common causes of node infection are:

- legitimate software containing malicious code (trojan horses), social engineering, physical access, bug/configuration error exploitation (OS syscall, device driver, application, firmware and BIOS, browser ...)
- backdoors creation, data stealing, hidden (or not so much) processes disruption, . . .
- persistent unauthorized access to a system (as root - i.e. rootkits)
- spyware (sensitive information collection)
- Ransomware (encryption of sensitive data)

Nowadays, the most common cause of node infection, is social engineering, which use the psychological weakness as an attack vector.

5.1.2 Network infection

- nodes capable to read and write data while in transit, actors capable to ”poison” routing mechanisms
- access and modification of network data flow, redirection versus illegitimate destination
- Sniffers and (growing) family of Man-in the-*

5.1.3 Supply chain attacks

A reliable environment is a must, but sometimes the attack can come directly from the supply chain. Whatever tool or service is used, it can be compromised.

- Compromise of service, hardware, or software of a third-party vendor or partner used (and trusted) by the target organization.
- Gain access to the target organization, inject unauthorized behavior.
- Infrastructure for update management.
  - e.g., SolarWind Orion Attack:
    - Malicious code into software updates of Orion network monitoring platform.
    - Distributed to over 18,000 customers, including government agencies and large corporations.
- Libraries and dependencies.
- Hardware during manufacturing.
- IT infrastructure management service.
- ...

5.1.4 Manipulation from the system owner

If technical-savy, the system owner can manipulate the system to compromise it in many ways, such as installing modified applications, different drivers or even alter system calls.

5.1.5 Men-at-work

Man-in-the-middle (MitM) An attacker intercepts and alters communication between two unsuspecting parties. This includes:

- *HTTP session hijacking:* Intercepting session cookies to impersonate a user.
- *ARP table poisoning:* Manipulating ARP tables to redirect network traffic.

Man-in-the-browser Browser infections that modify web pages or transactions. A well-known example is the *Zeus* banking trojan, which alters online transactions to steal funds or data.

Man-in-the-cloud Attackers steal credentials or tokens to access cloud environments. For example:

- Intercepting *Google Drive OAuth tokens* to access and manipulate files stored in Google's cloud.

Man-in-the-mobile (MitMo) Mobile infections intercept communication, such as two-factor authentication (2FA) codes. An example is *ZitMo*, which intercepts SMS messages and forwards them to a command-and-control (C&C) server.

Man-in-the-disk Exploiting vulnerabilities in handling external storage, allowing modification of temporary files stored on external devices, leading to potential data manipulation or theft.

Man-in-the-memory (MitMem) Intercepting or modifying data while it's stored in RAM. This often involves fileless malware, which does not leave traditional traces on disk, making it harder to detect.

Man-on-the-side Attackers observe and inject communication without necessarily modifying it. For example, *China's great cannon* can observe and manipulate traffic on a wide scale.

Man-at-the-end Endpoint communication compromise using techniques like keyloggers to capture sensitive information such as passwords or financial data.

5.2 Advanced Persistence Threats (APT)

Advanced persistent threats (APT) are undetected cyberattacks designed to steal sensitive data, conduct cyber espionage or sabotage critical systems over a long period of time.

These threats utilize **advanced techniques** such as customized malware(unrecognizable by anti viruses), exploiting zero-day vulnerabilities, and employing evasion strategies to avoid detection. APTs are often directed at specific high-value targets, requiring substantial resources, expertise, and careful preparation to execute effectively.

The "**persistent**" aspect of APTs highlights their long-term nature. Once a system is compromised, the attackers **maintain access** for an extended period, sometimes escalating their level of control or spreading the infection further. During this phase, operations are kept low-profile, often employing stealth techniques like using minimal bandwidth and mimicking legitimate traffic to avoid raising suspicion.

Finally, the "**threat**" component refers to the fact that APTs are usually carried out by **highly skilled individuals** or groups with strategic goals in mind, such as espionage or intelligence gathering for foreign governments. These attackers aim to achieve long-term objectives while staying undetected for as long as possible.

5.2.1 APT attack process

The Advanced Persistent Threat (APT) attack process can be broken down into several key stages.

The first stage is **initial intrusion**, where attackers gain access to the target system through a weak point. This can involve exploiting zero-day vulnerabilities or using spear phishing techniques to infiltrate the system.

Once inside, the attackers move on to **foothold establishment**, setting up persistent access through the installation of backdoors or stealth malware, ensuring they can return to the compromised system at will.

Following this, attackers escalate their control over the system through **privilege escalation**. By stealing credentials or exploiting vulnerabilities, they elevate their permissions, allowing them to have greater control and access to sensitive parts of the network.

In the **lateral movement** stage, attackers expand their presence within the target organization, spreading their infection and stealing additional credentials or exploiting further vulnerabilities to infiltrate other systems.

Finally, the attackers reach **goal achievement**, where they accomplish their objectives, which typically involve data exfiltration or sabotage of critical systems. At this point, they extract valuable information or disrupt operations as planned.

5.2.2 APTxx

The term **APTxx** is used to refer to organized hacker groups, often linked to nation-states. One notable example is **APT28**, also known as *Fancy Bear*, a group widely believed to be sponsored by the Russian government.

APT28 has been active since at least the mid-2000s, with operations dating back to 2008. The group is known to operate according to Russian business hours, and its actions frequently align with Russian government strategic interests, particularly in regions like the Caucasus. Their targets have included critical sectors such as aerospace, defense, energy, government, media, and even dissident groups. The group is primarily involved in activities related to espionage, political influence, and cyberwarfare.

One of their most infamous operations was the **2016 Democratic National Committee (DNC) Hack**, in which APT28 breached the DNC during the U.S. presidential election. The attack led to the leakage of sensitive information, which was used to influence the election's outcome.

Another major event linked to Russian actors was the **NotPetya attack** in 2017. Although disguised as a ransomware attack, it was designed to target Ukrainian institutions specifically. However, the malware spread globally, causing billions of dollars in damages and severely disrupting operations worldwide.

APT28 typical behavior

APT28 exhibits a range of sophisticated techniques in its cyber operations, targeting various devices, including desktops, laptops, and mobile devices. One of their primary methods involves employing (spear-)phishing messages that direct potential victims to realistic websites designed for credential harvesting. To enhance the effectiveness of these phishing campaigns, APT28 often registers domains that closely resemble those of legitimate organizations. For instance, they might use a deceptive domain such as *qov.hu.com* to mimic the official site of the Hungarian government, *gov.hu*.

In addition to domain spoofing, APT28 utilizes URL-shortening services to obscure malicious links. They deliver malware through highly realistic and targeted emails, often containing "weaponized" attachments in the form of .docx or .pdf files. These attachments exploit vulnerabilities in the recipient's software, allowing for further infiltration.

Once access is achieved, APT28 actively seeks to harvest credentials using techniques such as keyloggers and central memory dumping. The group adopts various evasion techniques, including malware code obfuscation, the use of signatures from compromised certificates, timestomping (modifying timestamps), and encrypted communication to avoid detection.

APT28 also engages in “lateral movement” within the compromised organization by exploiting the harvested credentials. They utilize Remote Desktop Protocols, Windows Management Instrumentation Command-line (WMIC), and PsExec to execute commands on remote Windows systems. For remote Linux systems, they employ SSH for secure connections. Furthermore, they perform privilege escalation by exploiting both the harvested credentials and existing vulnerabilities within the target systems.

A significant aspect of APT28’s operations involves data exfiltration, which they conduct through custom Command-and-Control (C2) communication methods, such as **Zebra C2**. This communication can be optionally compressed for large data transfers and is typically routed through encrypted protocols, including HTTPs, FTPs, or even custom protocols to ensure stealth.

While APT28 primarily adopts espionage techniques, they have also been involved in destructive attacks characterized as wiper actions. Notable examples include the use of **KillDisk**, designed to destroy the master boot record, as well as various disk-wiping tools, particularly targeting the energy sector.

In addition, the group frequently implants custom malware, such as **X-Agent**. This multi-functional malware implant is capable of various malicious activities, including data exfiltration and keystroke logging. Notably, X-Agent is designed to operate across multiple platforms, including Windows, Linux, Android, and iOS, thereby maximizing its potential impact on diverse target environments.