Digital Forensics and Cybercrime

Gianvito Caleca

2024

Contents

Part I

Cybercrime: threats, modus operandi, underground economy, financially-motivated malware

Chapter 1

Cybercrime: Threat Landscape

Working on security we work on **risk**, which is composed of different elements:

$$Risk = Asset \times Vulnerabilities \times Threats$$

The risk is the statistical and economical evaluation of the exposure to damage because of the presence of vulnerabilities and threats.
With no threats there are no risks, because it is the only thing that can nullify this equation. Assets and vulnerabilities are never absent.
With no *Threat model* we're completely misguided on the management of our system in terms of security.

1.1 Threat landscape

Threats can be roughly divided along three directions:

Internal vs External treaths an internal treath comes from the inside of the organization, it is part of the organization, while an external one don't.

Generic vs Targeted many security threats are generic:

- Generic threats: when you walk towards the underground, you're subjected to pickpocketers: they don't pick you because it's you, you're one of the others, it is a generic treath.
  Generic threats are not linked to us by definition, they are linked to us because we look alike somebody easy to be pickpocketed, not because we were the target.
- We can also consider also threats which are not so very generic: aggressions for sexual reasons are more targeted to one gender than one other, while still being generic.

- Targeted threats: specifically designed against us: criminals target **that specific company** *(e.g. the know how for racing cars, i want to steal from THAT company in particular).*

These directions also affect the kind of attacker: pickpocketers vs highly "professional" skilled stealer of information

Financially motivated vs Anything Else we divide:

- **financial attackers** *(which are the most of them)*,
- **other attackers** *(governments, secret services, hacktivists..)*.

Financially motivated attackers has 2 important positive characteristics:

- **easy to predict:** you look at valuable goods from companies and you can predict who the attackers can be *(e.g. ransomwares)*
- **they're relatively easy to handle:** just deny them the opportunity to take money, like making it too costly wrt what they want to earn.
  Notice that what is easy to understand is how to handle them, not to actually handle.

Non financially motivated ones are more difficult to handle:

- We cannot make them too costly or too risky *(e.g. Russians vs Ukraine's Donbass power plant: they have an entire state funding them, and they cannot be arrested for it)*, they have more money and they can take more risks
- If they're internal, they already know about the company and its security systems.
- The more motivated is the attack, the more determinated is the attacker

1.1.1 A gartner quadrant of threats

	Generic	Specific
Internal	**disgruntled**[1] employee	**socially-engineered or disonhest** employee *(financially motivated)*
External	Criminals, usually looking to make money *(financially motivated)*	A variety of advanced hackers *(mostly financially motivated)*

- **Generic internal threats:** a disgruntled employee who wants a raise, has something against his colleagues, was fired ...
  The treath doesn't need to be linked on what the organization does.
- **Specific internal attacks:** former employee stealing from old employer and bringing to the new one, it also exists a specific job which consists in being hired from companies just to steal from them.
  Or, employee can also be *social-engineered* into behaving like attackers.
- **Generic external attackers:** attackers which want to earn quick money, they aim to things which are common for all companies, like stealing money from bank accounts and so ....
  They are mostly motivated by financial reasons.
- **Specific external attackers:** industrial spies which aim for money, or governments or terrorists aiming for the destruction of a power plant near Donetsk.

The most important quadrant is than the one which comprends disonhest or social engineered people *(human factor)*: our instinct say us that we need to protect from the outside because we are clan-based animals, and we have our group of trustworthy animals *(our clan)* to which we are positively implicitly biased. **Think about the most famous security technologies:**

- Firewalls are meant to keep people out
- Antiviruses are meant for generic attacks, they use a generic list of malwares

Most of our security technologies protect against external attackers.

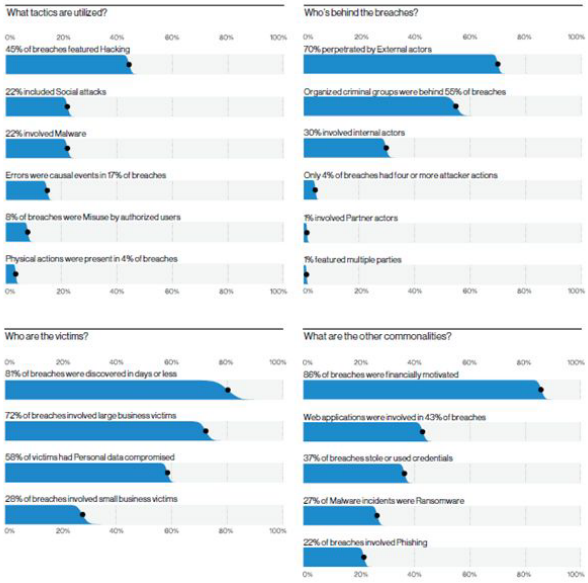
1.1.2 Examples of internal treaths

A bit more on:

- **Reckless or socially engineered employees:** in security we often have a wrong perception of the *human element*.
  When a company gets infected by a malware because a user clicked on a link or something similar, we blame the *stupid* user for it. But, actually it's not fault of the employee: it is fault of who had the responsibility to manage the fact that a threat was present and it had to be controlled.
  Since there will always be someone to click on links, our job is to make sure that they doing it doesn't cause damages to the organization.
  e.g. in aviation they study human factor to understand what to do to don't let people make mistakes: in airplanes cockpits there are different levers with different shapes, them are exactly shaped the same in different kinds of planes, it is a standard, and the reason is because people lost their lives because of similar levers.
  The solution wasn't to train pilots, but to make the threat difficult to happen.

- **Thirty-party users:** they're for example consultants that work in a company for a long time, where they actually do jobs very similar to the ones of the actual employees while not being true employees of the company.

1.1.3 Data breaches and targeted attacks



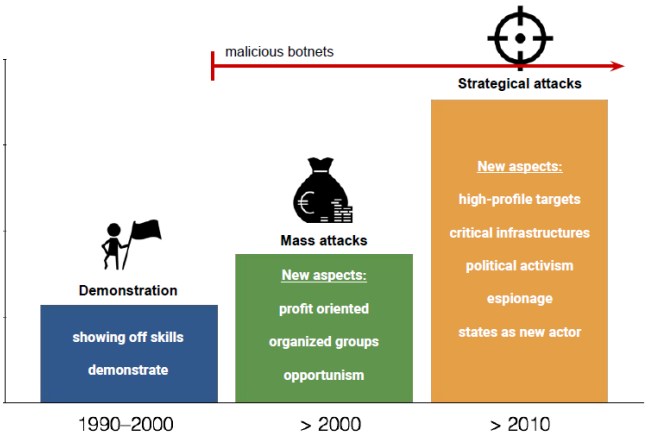
Verizon has a big sample of incidents made to their customers:

- The largest part of the attacks features hacking of some sort, the second larger chunk comprends social attacks.
- The 70% of breaches are perpetrated by external actors. This means that 30% of them starts from the inside, an incredibly high percentage.
  Consider that data are skewed[2], in the real world the internal attacks can be even more! *(remember the external threats reasoning, rationality (data) tells us that a lot of threats come from the inside, while our instinct guide us to be aware of the outside)*
- The 86% of them were financially motivated, 14% which are not, are a lot too!

These data are biased and are not representative of the true reality of threats, because simply they're not all collected. This collection can still help us to rationally think on how to manage the overall situation.
Keep in mind that some security incidents are specifically designed to be difficultly found, a lot of them has never been. This means that there is an entire set of breaches that no one ever investigated.
We measure attacks that we investigated/detected, and this is called the **observation bias**:
Other attacks by their nature be discovered, *(e.g. Dos, ransomware . . .)* that's the reason why they are so prevalent in our statistics: they are observed.

[2] biased

1.2 Brief history of malicious software



Over the last few decades attacks and attackers changed:

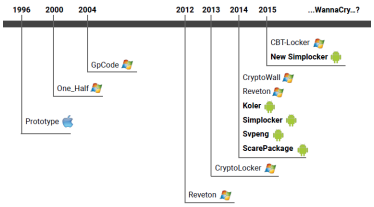
- **1990-2000:** most of the attacks were meant to show skills and explore
- **2000-2010:** with the birth of the Internet, massive, profit oriented attacks born. In this period were born also groups working as profitable enterprises of cybercrime.
- **2010-today:** attacks evolved: mass attacks kept happening, but now a lot of them are high profile financial attacks *(before: ransomwares, i ask small amount of money to single persons. now: ransomware attack specific companies to get a lot of money)*

Today financially motivated attackers are the "mass":
Direct monetization:

- Credit card/bank account frauds
- Ransomware attacks
- Fake antiviruses: they show you warnings that say your computer is infected, and to pay to activate the premium version to get rid of the malware. In reality they are just fake programs asking you to pay for a license.
- Premium calls: back in the days when you called to connect to the provider, someone managed to change the number to let you call a costly one.

1.3 Ransomwares and ransomware attacks

1.3.1 Brief history of ransomware



In 1996, a paper describing a crypto-malware that was exactly a ransomware was published about 15 years before CryptoLocker which was the first really successful one.
They just *"looked into the crystal ball"* of what in the future would be valuable: taking as hostage digital valuables could become a good way to steal money.
Then something happened:
the internet in 1996 was really different than the one of 2013, ransomwares needed a way for the user to pay a ransom in a way that was easy to perform. The preferred way to perform payments on internet is with credit cards, but this kind of payments have two important difects:

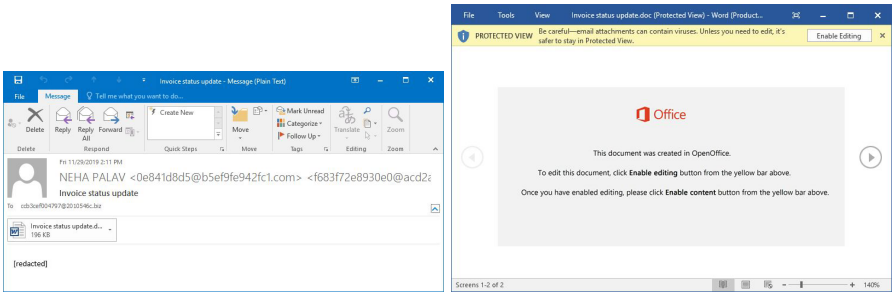
- they are trackable
- they are refundable when fraudolent

Then a new suitable way for payments was born: **cryptocurrencies**.
They perfectly fit this need: they are easily accessible, and payments are not reversible.

1.3.2 Ransomware screenshot and social meanings

Look at the structure of the timer: it is made to let you to percieve urgency. The stress of the urgency makes human take bad decisions, with the timer running you're more prone to pay because you feel that you have limited time. In social engineering attacks, urgency is always an important part. *(think about ultimatums in diplomacy, job offers with time limits, poltrone e sofà...)*

1.3.3 How to get infected



(a) (b)

Looking at the images we can see an interesting example:

- User receives an e-mail with a short text that contains some sensitive information and an attachment which is social engineered in a way that many people would click
- Microsoft Office shows a message to try to prevent code execution, but the user is prone to click "Enable" because the text contained in the document makes him think that's the right thing to do, even if a lot of grammar errors are present and the whole situation looks suspicious

One could have said that the user must had to be trained to not click, but the reality is that he is not understanding what's happening on his computer.
We can't train a generic user to not click: if your job is to open invoices received by e-mail, there is no way you can be trained.
Even if we train him to click only on what is coming from attendible e-mail addresses, if the *"attendible"* part was hijacked?
What we really should do is to figure out a way that when someone clicks enable, this won't cause any damage. Of course, to train the user to let this happen the less frequent possible is good, but not the main thing to do.

1.3.4 Encryption mechanism: how do ransomware work

Once the malware starts on target computer, it generates a random symmetric key, usually one per file, and it encrypts each file with this symmetric key.
The symmetric key itself it's encrypted with a public key, of a key pair generated on the server of the group that runs the malware. The private key is on the server. You need to pay the ransom.
Most of this is automated, when you're requested to pay a ransom, when cryptocurrencies are trasnferred to the addres, it releases the key associated to that address. Different keys to allow the attackers to decrypt only a part of the samples to demonstrate that they can do it.

crypto miner is another example of direct monetization.

1.4 Indirect monetization

examples: abuse of computing resources information gathering (stealing of account infos to sell them) making the machines part of a botnet to rent the botnet

1.4.1 Botnets

slide 17 Controller of the botnet rent out it to perform tasks, most typical example is Dos thousand of machines.. Another use is spamming, generating phishing campains, mine cryptos, parallel decryption earn money out of the rent

1.4.2 Rise of the bots

slide 18 back in the days botnets were used to control IRC channels to manage the chat. Then instead of using the compromised machines to control the IRC, then used the chat to control the bots. the significant challenge in this type of crime is that each bot per se is not dangerous for the machine itself, but other machines. The cost of cleaning up your machine falls on you There is a small cost that needs to be payed from each member of the community in order to don't let nobody in the group to get big damage (same thing as vaccination) As long as enough people protect their computers, the fact that your computer has a botnet is not a big problem to you. If lot of people let their computers be part of the botnet, big damage for the internet, big damage for everyone. Until that moment, selfishly not caring about it is not so a big trouble.

1.4.3 Geolocalization of botnets CC

chart. every quarter you can have a new updated chart. It tells us about command and controls of botnets that we know, they are so larger enough. Observation bias. Also all statistics on crime, cybercrime .. suffer of the same type of bias which is called the heatmap effect. biased on the density of the population and how much data we collected from there not lot of data on China example: black hole.. less technological advanced or shitty governments are so.. you always have USA on top: more penetration in internet where this think is tracked altre cose.. Also countries like netherlands: significant increase tells us that something is on, it could be some netherland organization decided to participate in this data feed putting a lot of data could also be that maybe some kind of attack used bots in netherlands. Singapore is ahead of China? Heatmap effect in the opposite, they're mostly behind the great firewall, most of the things cannot be tracked. There are footprints of Russians and Chinese hacking groups Russian hacks russian computers also Chinese conservative.

1.4.4 Type of malware families

most of them botnets of some sort, can do all of the things but they're used to do only one of them There are malwares classified as credential stealers: stealing credentials banking trojans: credential stealers specifically trained to perform stealing of bank account infos. Gozi most common banking trojan Zeus was the most important one.

Remote Access Tools: basic botnet oriented malware, allow control of a computer in order to perform whatever.

Loaders: specifically designed to allow a botmaster to load a program of whatever sort on a computer. Maybe a client ask you to install a certain malware on a lot of computers, and you can do.

We talk about families because there are groups that develop (only) the source code of them, and who performs the attacks buys the code and personalizes it for the specific attack. Three business: how to develop them, how to configure them, how to use them

There is a market for services related to malwares and cyber attacks (cybercrime as a service, underground market...) structured around the needs of cyber criminals. This market is fueled by the money that these schemes make. Some of these money pays for the tools used to make that money. SLIDE someone stole money from 104000 taxpayers. What is the value of someone personal datas that you exchange with agenzia delle entrate? You can sell identities on the black market. Worth because them can be used for fraud, open bank accounts used for money laudery. The more they're useful, the more they are worth. Worth 50 dollars for you that sell it, who pays is going to use them for fraud which is worth more. Market fueled from an enormous amount of money that people stole. SLIDE 23

another way in which malwares are installed drive by download, exploit breaks your browser and executes code on your machine. This requires your browser to be vulnerable and for you to visit the website which uses it. people compromises or run websites like porn, streaming, cracks of programs. you're not scared of the strange url if you are in need to see streaming, download crack, in contrast with amazon if you buy shoes. you can also place the "trap" in a legitimate website.

In reality you'll endup in a series of redirect chain In that redirection chain you endup in the exploitation pack for your browser: there is people selling this service kit to try 10-12 exploits tipo abbonamento 10.000€ mese

SLIDE 24 Advertisement of someone selling,

SLIDE 25(?) Dashboard of black hole: exploitation as a service black hole ended in 2013 because the guy was arrested.

These people just buy exploits, because they just can earn 10s millions per month and pay exploit hackers to develop them.

SLIDE 25: these ecosystems can exists because some of the activites done are not illegal. Developing exploits per se is not illegal, selling one is not illegal, the usage of them may be or may be not illegal. Even the services related to the configuration of malware are not, execution and operation may be. If you're

sufficiently shielded and you run in countries that cannot persecute you, we can know even name and surname but people cannot be arrested.

packers develop things used in malwares, lot of other affiliates: quality assurants change them to not be detected from antiviruses bulletproof hosting: hosts that kind of close an eye, for instance russian business network hosted whatever. borderline organization with lot of regular customers, and some bad ones

botnets are both enabler or attacks + the part of money laundering SLIDE 26 someone looking to buy vulnerabilites. SLIDE 29 monetization takes a lot of forms: people buying and selling cc numbers for 30$ of sure and safe money instead of laundering. an example is buying apple computers or expensive things. They sell a volume of these for little sure and easy money.

To make the card i bought for 30 in something more valuable travel industry: ethnic travel agencies are those that work with immigrants lot of planes to fill-up partially tourists and business people part of them sold in blocks to people who travel back to their home countries for a low price. legal business.

This creates possibility for a fraud: these people are used to buy in cash the tickets for a much lower price than you can find online. if you buy tickets with a stolen credit card from a regular travel agent and resell them for cash in a poor neighbor as a ethnical travel agent you make less money, if person find out you have sold the ticket for a lower secure money. if buyer is very unlucky gets to the airport and gets arrested.

If you detach others from the picture (online), it's easier to commit crimes: example steal a car vs steal a movie. lot of cyber criminal would not do the same thing in the real world different PERCEPTION. This makes crime happen more often online, lot of crime enablers ethical people understand consequences of your actions.

Telephone of Khashoggi was infected with spywares. Who sold the eploits for this phone to let the spyware installed would never had killed Jamal The exploit maybe or not may not be used in that way. this permits more people in participate

SLIDE 31 MONEY MULES AND MONEY LAUNDERY most cybercrime end up with a digital form of money. Your problem is to bring this in a form which is not linked to the crime. On a certain level this may sound easy, in general it is not because most of the transfers leave a trace. The real moment in which a criminal brakses the chain of traceability is the moment when cash turn physical cash or goods and go back digital again.

Some of the schemes are traditional: pay invoice to a company somewhere in the world, runs some processes, pays other companies...

Particular cyber crime one: use of money mules: they're traditionally accomplished, they know what they're doing, they have not so much to luse they open bank accounts, receive the money and hand cash to somebody

some of them open account with different identity, and to catch them you need to do while they whitdraw. More difficult.

Nigerian prince: ask you money in order to get more money, cost 500 dollars to get 1 billion until you realize that you have been scammed they keep asking

you money.

A variant is connected to the money mule. you actually get the promised money, i give you money, withdraw them and send them phisically with money transfer to someone keep 30% Or send the money in an envelope to a postal box in kazakhstan

Money arrive in your bank account from bank accounts of compromised people. At a certain point they arrest you. Good lawyer: you've been cheated. Ridai il 30 che ti sei tenuto e ripaga il 70 Bad lawyer: you get persecuted.

Considera RICETTAZIONE: apple computer sold at 40% in meno....

points, virtual currency of games has been used for this...

If you are a cyber criminal with crypto you need an exchange which is not any exchange but a stronzo one.

Chapter 2

Cryptocurrencies: abuses and forensics

we talk about them in the way they are used in cybercrime.

Bitcoin is the attempt to create electronic cash. cash has a lot of properties that you would replicate, in the digital world usually you don't have these properties.

electronic distributed ledger (node of where all the transaction happened) no central authority need to solve a problem which is very hard problem of byzanine consensus blockchain enables the creation of distributed ledger. used to run bitcoin, but you can use any other ledger to run blockchain

SLIDE 4 in the bitcoin world every user uses a wallet (the way they were designed originally) in btc the concept of cryptographic pair of keys can hold a certain amount of btc by using the keys you can use/send those money what uses them is called wallet.

SLIDE 5 bitcoin address is alphanumeric string which identifies a point where you can send bitcoin and where them can start from. In order to know how much btc are in that key you need to go to the origin of all the transactions and track the flow of them to understand how much of them are there now.

Not really efficient but can run without central authority The only reason for using a blockchain is if it is really so important to get a way out of a central authority it is the less efficient thing ever but it has a way out of central authority. for any other reason it doesnt' make sense.

WE WANT TO DO TRANSACTION ON A LEDGER WITH NO AUTHORITY, WHE USE THIS SHITTY TECHNOLOGY SLIDE 6 as soon the transaction is on the immutable ledger the money are on the other address. How do we ensure that this is the only transaction done with that bitcoin we need to have a consolidated immutable ledger with a central authority this would be easy. how do we agree on a ledger which cannot be back modified?

slide 7 certain btc associated with your public key joe signs a transaction which moves them to alices' wallet.

I need to have an history that cannot be modified Joe could unsign the key. How do we do?

Transactions are put in a block, block linked in a so-called block chain (linked list) we want this list to be immutable

Mining: Solves 2 problems: ensuring that the list cannot change generate bitcoin

we seal the block and get a little btc in reward, and when we seal the block we tell everyone were we want to send the reward

mining is a very computational demanding activity hash function collect transaction, put them in the block, put there a destination for a reward brute-force the block in a way that the hash of the block has a certain number of zeros to start with. This is difficult, the more zeros at the beginning, the more difficult for a miner to find the right combination. Miners are using computational power to trying to find the right solution, once they find it they publish the solution. At this point the other miners, look at the transaction that are not in a block yet, try to put them in the next block and try again. The more computational power you put, the faster you will get to the solution.

The difficulty increases more and more, the reward got smaller and smaller but btc value gets larger and larger.

block = set of transactions + reward location which a sha256 with a certain number of zeros.

After I found a solution, the new block must be linked to this one ... mancaun pezzo 13.56 sul next hash

Sooner or later two entities get a solution at the same time or more or less. What happens? For some people chain ends with block a and some with block b, do i append to a or to b? what happens is a fork slide 13,14 ... alternative ending of the chain some nodes see the 1st, some the 2nd. you start from there and search the next one. you can see now two different blockchains. sooner or later someone finds a solution who mines on the green blockchain fount the purple solution the rule now is that the true blockchain is the longest one. purple block is one ahead, i'm no more in the true one. it doesn't make more sense to try again the red one. give up and go to the shortest.

This is done because in order to revert a payment you'd need to go back on your block, go ahead mining until your blockchain is now the longest one means that you compete with all the others.

Blockchain solves the problem of central authority by making people to do useless thing

Part II

Fraud detection and analysis

Part III

Digital Forensics principles

Part IV

Acquisition, analysis, evaluation and presentation of evidence

Part V

Ethics elements

Part VI

Optional: casi studio specifici