The Cybersecurity Iceberg

By ByteSeb

Disclaimer: "This video only has educational purposes. It contains flashing lights, loud noises and sensitive topics. Corrections and additions are always welcome."

Tier 1

Social Engineering[1]

This can be summarized in a sentence: It's easier to fool a person, than to fool a machine. Sounds sophisticated, but you've definitely seen these, in the form of Fake Download Buttons, completely real girls in your area, the millionth visitor, the whole "Enable notifications [or calendar] to continue" or phishing.

This last one is often seen as cloned websites, where a malicious actor will ask for your data, and you are likely to give it to them… I mean, a website it's very easy to clone. Just a couple of clicks, and you'll clone the entire layout of a legitimate page or email.

In some cases, they even add fake reviews and things like that. I've seen many older adults fall into this trap. I usually notice it's fake because the people they put there look like from a stock photo session, they have generic names, all the reviews are 5 stars, and never, ever commit any typos, or it's clearly a badly translated comment. That is not realistic.

To this, a countdown could be added to make the victim feel pressure in order to give in and fall into the scam...

And even the whole "Nigerian Prince"[2] thing could fall into this category, being predecessor of more complex scams, and speaking about that...

Social Media Scams

Social Media is great tool, when used correctly, which most people don't do. *I mean, after all, you're watching this video, right?*

So it's not surprising that due to the abstraction and scale that social media provides, it's becoming the best place to scam people.

For example, this is one that I personally have encountered. I've blocked around 10 numbers at this point, and 2 more while making this video, asking me via WhatsApp if I want to "earn money easily, by giving likes in YouTube", and I just replied: "I didn't know they spoke my language in Bangladesh".

1 *https://go.kaspersky.com/rs/802-IJN-240/images/NJ_Social_Engineering_KFP.pdf*
2 *https://www.dailystar.co.uk/news/world-news/nigerian-prince-scam-meme-arrested-17054041*

Seriously, that did actually happen. Be wary of any phone number from another country. Just anybody that you don't know and sent you a message. Some countries have worse regulations and they can get away with it easily. I'm pretty sure some of these are even bots, because they talk to me first, and reply extremely quickly and that is not something that happens to me.

Moving on to a weirdly nostalgic one, we have Facebook scams, in the form of chains. You have to remember one of these. Like, when your friend sent you a message that, between a lot of typos, told the story of a dead girl, and you had to share it because if you didn't, you died. I'm very likely dead multiple times by now because of all those ignored chains.

Quizzes were also very popular back then, and something I experienced years ago when a classmate sent me a quiz. You visit the link, and… It's a phishing site. Once they have your account, they keep sending these to your friends, and then, your friends will send them to their friends and so on.

Fortunately, even if I was naive, I made a typo, and the phishing site uploaded that one. I never got hacked, by pure accident. Now you know, if you see a phishing scam, put a random password. They'll always let you in or show a site error, they can't correct you because they don't actually know your password.

Ending this entry with YouTube scams. Very important to mention these.

Scams in comments, while not as bad as they used to be, they're still some out there, often bypassing the filter by stealing a real person's comment, adding a Telegram number with a girl, or just straight up impersonating creators. If you see one of these in my comments offering money… Don't trust them. I don't use Telegram, because who would I talk to? And I'm broke, so no…

There are some that have dissipated, but you never know. Those Sponsor Scams[3].

Someone sends a sponsor offer to the creator, attaching a very suspicious, definitely real .docx , pdf file or something similar, and when they open it… It was actually an executable, or lately, a Windows Screensaver .scr file. Most people don't use these anymore[4], but because they're pretty much executable programs, they can go under the radar easier, I mean, I bet you didn't know this extension.
Windows does not help you in this regard at all. File extensions are hidden by default, because they're just "too complex" for users to understand! And executable files are executable automatically, by just giving them the right extension.
Making it the right formula that allows them to steal the cookies of your browser session, bypassing the need to even have to steal a password, and 2FA in many cases. This is when the attacker steals the channel, changes the password and details about it, and they always post an Elon Musk crypto scam livestream, usually, even at midnight or whenever they think creators could be sleeping, to prevent them from noticing. This has happened to many big channels, even ones like Linus Tech Tips.

Now you know, that if you see a crypto scam on my channel, it's not me.

3 *https://blogs.opera.com/desktop/2022/02/warning-scammers-pretending-to-work-for-opera-gx-fake-manager-of-opera-software-partnership-proposal/*
4 https://julienvandorland.substack.com/p/the-scr-malware-hack-explained

By the way, there are websites like ScamAdviser or TrustPilot that compile multiple scams, and you can use them to check the legitimacy of a website.[5]

And you can always check where a picture is coming from with a reverse image search.

Hacking[6]

I know the term is very debatable. I've heard the original definition came from the word "hack", as in a person that knows how to find clever solutions to specific problems. But for the sake of convenience, we're going to just say "hacker" to refer to a malicious one, that can get into your system, sometimes also called a cracker.[7]

You've seen the classic "hacking" portrayal. A person that never commits mistakes and just types random buzzwords to a Terminal, saying "I'm In". While in reality, it's something way more boring, like a guy from Russia uploading a file, you download it, realizing it was not what you were looking for and delete it… Only to never know you got a trojan.

Mr Robot is one of those few ones that have a somewhat realistic representation, but for the rest, some subreddits exist to mock them, like r/masterhacker and r/itsaunixsystem.

Now, that's not saying that very smart attackers don't exist. There are a lot of hacking groups. Like the decentralized Anonymous, being the first thing that comes to your mind or lately, Lapsus has been very popular. Known for hacking Samsung, Microsoft, Uber and other companies. You probably have heard of the user teapot uber hacker, believed to have been associated with the group. He was the one that leaked GTA VI footage. He was 17… did it using a phone… And an Amazon Fire Stick...

But on the other side, there are technology prodigies that use their knowledge for other causes, aside from playing Doom on pregnancy tests[8] *(Text: I didn't even know they had screens. Maybe a Doom on Weird Devices Iceberg?)*. That's when the whole "hacking hats" thing comes up.[9]

Don't take it seriously, but in general, Black Hat hackers are the ones willing to do anything for money or personal benefits, white hats try to find vulnerabilities and report them to the owner, often claiming a monetary reward, or even being offered a job. But you also have the gray hats, who seem to follow their own moral code. They could make a vulnerability public, instead of privately reporting it, as a way of showing how dangerous it can be.

There's also the so called "Script Kiddies", that are often younger people that want to get into cybersecurity, which is not bad, but they tend to do it without learning the basics first, just buying malware, often being toxic, immature and creating problems they don't really know how to solve.

There are more, but honestly, I think they all could boil down to these. But if you think I missed something, let me know with a comment.

5 https://www.scamadviser.com/
6 *https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/*
7 *https://www.trustedreviews.com/explainer/what-is-a-hacker-3989651*
8 *https://www.popularmechanics.com/science/a33957256/this-programmer-figured-out-how-to-play-doom-on-a-pregnancy-test/*
9 *https://sectigostore.com/blog/different-types-of-hackers-hats-explained/*

Passwords

Yes, I know what you're thinking… Passwords, really? But just trust me, okay?
We know that a password is just a combination of characters to provide a way of verifying you're the person you say to be… In the best case scenario, you would have a long password, with uppercase, lowercase, numbers and special characters, unique for every single account you use, and you would remember to change them periodically, because it's useless to have a great password if you repeat it everywhere… But nobody does that, and you should look on HaveIBeenPwned[10] if it has already been leaked. You probably even use one of these common passwords[11], and if you do… Please, love yourself and change it.[12]

This is when it comes in handy to prefer using the term passphrase. Because believe it or not, you shouldn't underestimate the psychological power of changing a word. Like this xkcd comic[13] says:
(Shows comic)

Making your password something like Troubadour, and just replacing some of the letters with numbers is awful to remember and easy to crack, but a phrase like: correct horse battery staple is way harder to guess, but easy to remember. That's what you should do.

Remember that with every character you add to your password, the time needed to try to brute force it increases exponentially, and it's way better if you don't include anything related to you, for example, a date, something you like or dislike:
(Shows table)

Now, even with passphrases, you won't remember all of them, and you likely shouldn't. That's what password managers are for. They basically take care of handling your passwords. Storing them safely, creating them, typing them for you… Your browser or Big Tech account probably has one already, but honestly, I would only recommend Bitwarden, and it's not a sponsor. They are open source, have a great license, support basically all operating systems, all browsers, it's even on F-Droid and you can self host it. KeePass is also great, but not as convenient for most people because it's only local.

To this, you should consider enabling Two Factor Authentication, or 2FA. It's another security measure you have to validate in case that your email and password get leaked. You see this often in the form of SMS codes, which you shouldn't use, as they're unencrypted and somebody could intercept it and use it, or notifications, like the ones Android phones use, but I would also not recommend this, even if they're handy being just a button accepting the request, they're subject to what's called a Fatigue Attack. Basically, someone sending multiple requests hoping you misclick, get confused, or tired of so many notifications, and accept it to shut them up, giving that person access to your account.
Keep in mind I'm not a cybersecurity guru by any means. Always do your research, but I would only recommend you to use TOTP[14]. Which stands for Time-Based-One-Time-Password. It's just a unique, secure code that expires in some seconds, and you copy and paste. Works on multiple devices and offline.

10 *https://haveibeenpwned.com/*
11 *https://www.hivesystems.io/blog/are-your-passwords-in-the-green*
12 *https://en.wikipedia.org/wiki/List_of_the_most_common_passwords*
13 *https://xkcd.com/936*
14 *https://www.twilio.com/docs/glossary/totp*

It’s a universal standard, so you could use something like Google Authenticator, Aegis, for an open source Android alternative or Authenticator, for Linux. Some password managers also take care of this.

The idea is to make a password-less, likely even email-less future. With passkeys, you wouldn’t even have to make an email or password, because if you think about it, the only reason we use still use email is because all accounts require one. Like a workaround that needed to be fixed long ago and we forgot.

Quoting the passkey.org website, you authenticate by using something you know, like a PIN, something you have, like a physical security key or one of those security modules embedded on your phone or PC you never knew you had; and something you are, like a fingerprint or your face. All of this enables multi-factor authentication that is very secure and in practice, you don’t even need to think about it. You would probably not even need to care about it, just use your fingerprint and that’s it. Of course, it’s not perfect, as the implementation is early and varies, but with Apple, Google[15], Amazon and more big websites supporting it, I am hopeful that the adoption could be growing fast. Even though, we would have a period of transition where both would co-exist, but the objective is to replace passwords. This process could be less jarring thanks to password managers.

VPNs

For those who don’t know what an IP address is, it’s pretty simple. It’s like online shopping, you’ll never get your package if you don’t give an address, and you can’t send a package if you don’t have an address to send to. Your house has a single, unique in the world Public IP, at least, in the best case scenario.

A Virtual Private Network, or VPN takes care of disguising that Public IP to wherever one of their servers is located at, and that's when you have the side effect of being able to access content from other countries, and preventing tracking… To a degree. Because a VPN is useless if you log into the same accounts from your home IP, then the VPN’s IP, or post everything about yourself online… At least, when it comes to privacy. But, there are some legitimate uses for VPNs, like playing peer to peer games, without your approximate address being leaked, right, GTA Online?. Which, yes. Public IPs can give away your location, but it’s not directly, and because most IPs now group entire neighborhoods, it’s possibly not even a very accurate location. Just your city. I mean, still near enough for you to not want to reveal it, but even then, you could still be tracked by many other means.

IPs now grouping big areas instead of single houses has the side effect of not being able to expose your Minecraft, Nextcloud server or website to the internet. This is when you could use a VPN like Wireguard or Tailscale to disguise your IP as if you were at home all the time, accessing your stuff from anywhere, which could also have the side effect of protecting your traffic from Public WiFi networks.

But in summary, they’re not a silver bullet, they’ll never be one, as much as Youtubers with VPN sponsors would like to tell you, they don’t make you “untraceable”, and way less if it’s a sketchy, free VPN that in most cases sells your data and slows your network down… I could’ve just thrown

15 *https://blog.google/technology/safety-security/passkeys-default-google-accounts/*

in a VPN sponsor from offers I've gotten, but honestly, it just doesn't feel that right. If I get sponsored, it'll be something I could unironically see myself using, and one with great reputation.

Antiviruses[16]

An Antivirus is a type of virus… *(Beeping Interruption)*

Fine, seriously… It is a piece of software designed to protect you from malware, constantly scanning files in the background, preventing some executables from running, and blocking some network connections.

The reason why I made the "super funny joke" of why some consider antiviruses to be malware themselves is because they tend to slow computers down considerably, most retail PCs come with one preinstalled, and they're hard to remove for the average user. Depending on the product, pricing and point of view, they could fit into the category of Nagware[17] *(shows annoying popups with SFX)*, because it keeps begging for the user to pay the subscription; Spyware, because it keeps scanning user files, having some scandals because of this[18]; and just being Freemium[19], having trials, incomplete features and things like that.

Now, that is not saying they don't help at all… But depending on your use case, you probably don't need one. That is, if you're an experienced user that has no trouble distinguishing scams, does not download suspicious files and has good security measures. I mean, Windows already comes with Defender preinstalled, and despite the memes, it is actually one of the more decent ones out there. It does block some malware, and it does not yell at you, begging for a subscription. Probably, your grandma does need one, but just Defender, in my opinion.

This is where the theory comes, stating that some antivirus companies could be the ones to create malware themselves… And I can see the argument, but I doubt that's the case, because I don't think you need to make complex malware in order for people to get infected, and can still profit off of users by selling their info… Right Avast[20]?

There are some antiviruses that don't even pretend anymore, and are straight up scareware, like WinAntivirusPro[21]. Showing alerts to make the user think they have viruses or some made up things "too advanced for the free version", getting them to pay, without removing the true virus.

But there are 2 antiviruses I can see myself using. The first one is ClamAV[22]. Totally open source, also available for Unix systems.

And VirusTotal[23], not running in the background, it's just a website. You can drag and drop files you are suspicious of, or copy and paste links you think could have a scam or malware, and see the report without an account. Even though, keep in mind that many viruses come in unnecessarily

16 *https://www.malwarebytes.com/antivirus*
17 *https://www.sir-apfelot.de/en/what-is-nagware-48012/*
18 *https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation*
19 *https://en.wikipedia.org/wiki/Shareware*
20 *https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks*
21 *https://www.bleepingcomputer.com/virus-removal/winantiviruspro*
22 *https://www.clamav.net/*
23 *https://www.virustotal.com/gui/home/upload*

heavy sizes, without “real content”, for example, a Word file of 800MB, in order to reach the limit and avoid being scanned.

Oh, and also, whenever you buy a new pre-built laptop or PC, don’t even let it boot, just make a clean install of the OS of your choice. The retail versions of Windows usually come with a lot of bloatware preinstalled. The isos do too, but it’s way less.

Shoulder Surfing[24]

This is a technique used to obtain personal information by looking over the shoulder of someone directly to whatever they’re interacting with that has personal information. It’s pretty much like when you’re on the subway, and the guy behind you is really interested in knowing who cheated on your friend, but in this case, it’s worse, because the people that do it are also trying to guess and remember your sensitive information.

Many people still use patterns, yes. Even in 2024. The issue is that they only have so many combinations. You have 9 dots, basically, the only variable being the order, because you can’t repeat it. If 1 is included in a pattern, you can’t choose that number again. Leading to around three hundred, eighty nine thousand possible combinations, in the best case scenario. It’s a lot for a human, yes. But nothing a simple brute force attack couldn’t break.

PINs are slightly better, because they also introduce the factor of being able to repeat numbers, and a more unpredictable number of variables… But none of that matters if you’re using a common PIN, and most people do… So, if you’re using any of these or your birthday, change it.

People with experience would be able to guess your pattern pretty quickly because the numbers have a fixed position. In more recent Android updates, you can choose to hide your PIN, replacing the numbers revealed with random shapes, but it’s still not great. Some Android forks and skins let you scramble the position of the Pin Pad whenever you lock your phone, and it decreases the chances of a successful shoulder attack…

And while most people just fingerprint or face unlock their phones, when rebooting or whenever the biometrics fail, you’ll have no other choice but to use your PIN. So, it’s better to just choose a password. Even if it’s only numbers, the sole fact of making it a password increases the variables significantly, adding lowercase, uppercase, numbers and special characters, which by then, your phone is likely going to get locked, or you’ll notice. In the best case scenario you would use something like a passphrase, but most people won’t do that because it’ll get annoying.

You can always get one of those privacy screen protectors, but the availability depends on your model, and it could affect its color accuracy. That’s up to you.[25]

Kali Linux[26]

Operating Systems like Kali Linux are focused on Cybersecurity, and Penetration Testing, including a suite of multiple applications related to this field. In fact, there is even a mobile version of Kali, called Kali Nethunter, and Nethunter Pro.

24 https://www.beyondidentity.com/glossary/shoulder-surfing
25 *https://surfshark.com/blog/privacy-screen-protectors*
26 *https://www.kali.org/*

Nethunter is a fork of AOSP, with some interesting tools preinstalled. Nethunter Pro is not the same thing. It's a full Kali Linux build optimized for phones, apparently running Phosh as the DE. I would try any of these, but the amount of devices supported is very small, as expected with most alternative mobile OSes. I'm still waiting the day I can try a Linux phone.

However, it usually has some… bad reputation, not because it's not good, but because of the people that use it… Or more like: misuse it.
It's common to see some kids playing, pretending to be "hackers", because it's the cool thing, dude. But in reality, what it seems most of these kids go through, it's them managing to install the OS, which previously, you shouldn't do, as the root account was the only one there by default, most didn't know how to create a regular user account, and many people tend to troll them on the internet with dangerous commands, leading them to break their entire OS. And the worst thing is that most of the times, you don't even need to install Kali on bare metal, just use a VM or install these packages on any other Linux Distro, Kali just provides convenience most of the times.

Now, I don't think we should shame them. We should probably just head them in the right direction, teaching them how to protect themselves, instead of how to attack other people. I mean, after all, it's not legal.

Tier 2

Spyware[27]

This is a type of malware that collects personal information about you, it could be to sell you personalized ads, to steal your banking information, username or passwords. Some of these come in the form of Keyloggers, that as the name implies, keeps storing and sending your keystrokes to the attacker, knowing indirectly your accounts, passwords, messages you typed, applications you opened, it could be very sensitive information…

Signs of having spyware could be a device that is running slowly, when it previously didn't use to, having worse battery life and running out of space quicker than usual, as well as crashes.[28]

Examples of popular spyware are the following:

DarkHotel[29]: With the first reports believed to be from 2014, in South Korea, it infiltrated into the, often insecure, hotel WiFi networks, hoping to target company executives. They faked certificates, asking to download a fake software update, that once installed, steals information like passwords and other confidential data.

A more recent example is Ghost RAT[30], with the last part standing for "Remote Administration Tool", that attacked in 2021 the Android gaming emulator NoxPlayer, for Windows and Mac, allowing them to access your device remotely, including the camera and microphone.

There are many examples more, like Microsoft Windows, but we still have more topics to cover...

27 https://www.malwarebytes.com/spyware
28 *https://us.norton.com/blog/malware/spyware*
29 https://naturenex.net/what-is-darkhotel-how-does-it-work-types-and-more/
30 *https://sectigostore.com/blog/spyware-examples-4-real-life-examples-that-shook-2021/*

Adware

To some, it could also be classified under Spyware, because Adware steals information, and also shows more advertisements based on that information. I had a relative that got one of these, and I can tell you that it is often even more aggressive than the average YouTube ads… And that's saying something.

The classic example of Adware is this…

Your 9 year old self goes and downloads CCleaner, that can allegedly turn your netbook into a beast because deleting garbage files is fixing core flaws this almost 40 year old operating system still has… But you didn't notice that the installer had a cleverly placed checkbox, enabled by default. When this is the twentieth installer you have to deal with, you leave everything by default, and spam "Next". Unknowingly agreeing to install this Ask Toolbar[31] thing, that hijacks your search engine, gives you awful search results, and shows a lot of sketchy ads… You try to remove it, but it's not that easy, being often protected by another add-on.

Surprisingly to many, Ask Search is legitimate, but it seems people could earn money by getting you to use it, and that's why it was bundled with this type of shareware.

And we can't forget about Bonzi Buddy[32], a program disguised as a virtual assistant in the form of a purple monkey that once installed, will ask for personal data, charge you for unlocking things like more songs (yes, because it sings) and will show a lot of ads, overwriting the browser's start page.

But most of the adware nowadays seems to have won, and changed focus to the mobile sector, where it is sadly, the standard to an extent. With apps that send you ads via notifications and banners. Some Android skins even have this type of adware as part of the Lock Screen[33].

Web Browser Malware

The Web Browser of your choice is probably the first thing you install on a clean system. (Yes, that's a dead meme, I don't care). And it's the place where you can get your news from, buy things from and interact with people online. Making it a key factor in your digital, and "real" life to an extent.

No wonder why some bad actors put their malware and scams in practice here. For example, with malicious browser extensions. Like Video Downloaders[34], VPNs, and knockoffs of legitimate extensions. You kind of see the pattern, right? Also with phone apps. You probably don't need these most of the times, as your browser might already have a feature like this, or you can use an open source extension. Remember that extensions can often access all of the content in a website, and this applies for all browsers. I'd say that the fewer extensions you use, the better.

Even without any extensions, you're vulnerable. Some websites can look legitimate, as we've discussed before, but some of them are really clever, using something called Typo Squatting. For

31 *https://malwaretips.com/blogs/remove-ask-toolbar-and-search/*
32 *https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Adware%3aWin32%2fBonziBUDDY*
33 *https://play.google.com/store/apps/details?id=com.miui.android.fashiongallery&hl=en&gl=US*
34 *https://www.tomsguide.com/news/28-bad-browser-extensions*

example, instead of typing google.com, with spell it with two g's, and don't visit it. Because this is not just an example. It installed adware disguised as a fake Antivirus called SpySheriff[35].
Some of these also add a Back Button Overload[36]. So no matter how many times you try to go back, you end up stuck in that page. To avoid this, I recommend opening links in a new tab with middle click, or holding down the back arrow button to see the history and be able to go multiple pages back.

But even if the URL seems like the real thing, it might not be that. For example, a domain like apple.com could look like this. Nothing wrong, right? Well, this "a" is not the one you know, it is a character that looks almost the same, from another language, effectively being to a computer, an entirely different thing. It's known as a Homograph Attack[37]. This, with the addition of a valid HTTPs certificate is able to fool a lot of people. That was the reason why the padlock icon was recently removed in Chromium. HTTPs is already the standard, and showing a green padlock could indirectly tell users that the site is "trustworthy", when in reality, it just represents the connection being encrypted. It can still be stolen, with a Man In The Middle Attack, but it would show a bunch of gibberish, and this security measure still does not mean that the site could be fake or that it hosts malware. Unfortunately, for some reason, Firefox still shows the padlock, and they still have that Homograph vulnerability.

And even if you download something from an official website, the file that you downloaded could have been replaced with a malicious version, that is what happened to CCleaner, unsurprisingly owned by Avast[38]. For more than a month, downloads of this program, from the official website were infected with malware aside from CCleaner, with users having no clue. This is when comparing hashes could be useful.

You'll see, a file has content, unique enough for this to generate a code based on mathematical operations, called a hash.

If two files have the same hash, even if they are literally called the same, made on the same second and the size is also the same, just a single character being different will be enough for the hash to change, and that's how you know if you're downloading what you thought. Linux Distros usually have the hash on their website, for you to compare it.

Software Cracks are often viruses

Yes, I'm sorry to inform you that your Photoshop crack, is very likely… Malware. Same for many other cracked or modded applications, like Whatsapp Gold. One that is known for promising a lot of features a billion dollar corporation's messaging app should've had since 10 years ago, like themes, support for larger files, downloading statuses, and things like that. Keep in mind that WhatsApp can always ban you, as it is a modded client, and most of the "advantages" have been finally introduced, with some minor exceptions.

Same goes for modded Windows versions, and I'm talking about those "Debloated iso's". They might not be malware directly, but because Windows is proprietary, the creators of these modifications don't really know what they are removing in the source code, and trying to study it is illegal, because copyright and so. But one of the things often removed from these "lighter" mods are Windows Defender and Updates. I know some of you hate them with a burning passion. And

35 *https://malware-history.fandom.com/wiki/SpySheriff*
36 *https://www.pcmag.com/news/chrome-browser-to-stop-websites-abusing-the-back-button*
37 *https://en.wikipedia.org/wiki/IDN_homograph_attack*
38 *https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/*

while you could manage to not get any infection without Defender, disabling Updates in general is a pretty bad idea, considering how targeted Windows is.

In case you're running Windows, avoid third parties, and just download them from the official website, or use a package manager, like WinGet[39].

Cryptojacking

You've definitely heard of cryptocurrencies. Summarized, one of the key points they have is that they're decentralized, and in order to verify a transaction, some computer around the world needs to solve a complex mathematical puzzle, requiring significant power consumption and resource usage, and the first one to solve it gets paid with that cryptocurrency. Depending on how much it is worth at that moment, it could be a lot of money. Cryptojacking is when you take advantage of this, and use computers from third parties, gathering the power of all of them and using it to mine cryptos. In some cases, you don't even have to download malware, as many websites used a now dead Javascript API with the name of Coinhive[40] that let them mine Monero. It was presented even as an alternative for Captcha, without bothering the user... you know, just draining their battery, to generate revenue for the website.

Troy Hunt, the same person behind Have I Been Pwned bought the domain, and it currently shows an explanation for the whole issue[41].

Worms

A computer worm is one of those programs capable of spreading through networks, file sharing, external drives and social media. Now, keep in mind that not all info is perfectly accurate, and most of these nowadays could fit into multiple categories.

It is believed that the Creeper worm was the first computer virus to ever exist[42]. Created by Bob Thomas, it just had the objective of knowing if the program could move between Tenex computers through the ARPANET, later modified by Ray Tomlinson to also self-replicate, showing one message "I'm the Creeper. Catch me if you can!". Ray also made the first antivirus, called Reaper, and as you can imply, it removed Creeper.

The first Internet Worm, however, seems to be the Morris Worm, created by then, 23 year old student Robert Tappan Morris[43] as a prank that spread through Unix systems used by Harvard, Stanford, Princeton, Berkeley and even NASA, a bug caused overload in the computers, rendering them useless, with damages of up to 10 million dollars, and being the first person convicted of accessing protected computers without authorization in the US. But he didn't go to jail, he had to pay a fine, be under probation and complete 400 hours of community service[44].

39 *https://learn.microsoft.com/en-us/windows/package-manager/winget/*
40 *https://web.archive.org/web/20180504143946/https://coinhive.com/*
41 *https://www.troyhunt.com/i-now-own-the-coinhive-domain-heres-how-im-fighting-cryptojacking-and-doing-good-things-with-content-security-policies/*
42 *https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds*
43 *https://securityintelligence.com/articles/how-morris-worm-changed-cybersecurity/*
44 *https://www.fbi.gov/history/famous-cases/morris-worm*

Finally, a more recent and popular example is ILOVEYOU, or the LoveLetter Worm.

What did you feel when I said that? Disgusted, right?

But let's say you're a person in the 2000's, and you get this email coming from your school or work crush. Just with a subject saying the most dubious phrase in history, the description reads "Kindly check the attached LOVELETTER coming from me."[45], and a LOVE-LETTER-FOR-YOU.TXT attachment. Now, that's when you'd feel intrigued instead, at least. Leading you to open the file and… It was a Visual Basic Script, but you didn't notice the last part. The worm corrupts your files and sends the same email to all your contacts. It was a really clever and successful demonstration of a worm and social engineering. You could say people were naive, and yes, but all of that was almost 24 years ago. And I'm sure that "You've Got Mail" movie didn't help. I haven't watched it, but it makes sense… You could think that people from these days could not fall into this specific worm, but the essence is the same. Seriously, Microsoft, how hard is an executable permission switch? Right, Tech is not there yet...

Malicious Macros

I told you about executables with hidden extensions, but there are some files that are actually what they claim to be, like a .docx Word file, and still contain malware. This is something that happens more often than what you'd think, and it can be pretty dangerous.

If you don't know what a Macro is, in this case, it is a program you can make yourself, to help you automate actions in the Microsoft Office Suite. You can write them in Visual Basic, and they are not necessarily malicious, but I guess most people don't know about them, not having proper protection until recently, and that's why they are a great method of infection.

An example of this is the malware Emotet[46], a trojan that spread in 2020 via emails, containing a Word document as an attachment. Once opened, Word will use read-only mode, that disables macros and editing. The document contains a fake popup of sorts, trying to get the user to enable the previously mentioned features, and if the user does so, it runs the macro, that installs the TrickBot trojan, capable of stealing passwords, cookies, sending spam, and it spreads through your network.

If you look closely at the popup, you'll notice pretty obvious grammatical mistakes, like "the file was created on IOS device". Microsoft and Apple would never spell it with an uppercase "I", and also "Click Enable Edition", sounds weird. I know it's a little ironic coming from me… but come on. I'm not the one making malware with typos!. Also, the Office logo is misaligned by 2 pixels vertically, and a real window would not have asymmetrical padding, being closer to the upper left corner. Yes, I literally measured it. *No, I haven't gone out in a week, how do you know?*

Even though, there is an updated template, looking more like this, nicknamed "Red Dawn", it fixes most of the grammatical mistakes, but not the padding mistakes.

45 *https://www.kaspersky.com/blog/cybersecurity-history-iloveyou/45001/*
46 *https://www.bleepingcomputer.com/news/security/emotet-spam-trojan-surges-back-to-life-after-5-months-of-silence/*

Correct me if I'm wrong, but even if Microsoft has patched some macros in 2022[47], seems to be only for Office 2013 and newer. There is probably no need for a macro to be bundled with an online Word file, so I would not trust them.

Also, LibreOffice and probably some other alternatives do support macros, so some malware made for MS Office could work to a degree in other operating systems. But there's also this malicious LibreOffice Draw file, by the name of badbunny.odg. It runs a macro compatible with macOS and Linux that displaying: "Hey, (Username) you like my BadBunny?", with an image below of a man dressed as a rabbit doing… predictably, rabbit things... involving a woman. It seems to be more of a shock prank or proof-of-concept that could've been way worse, but don't look it up, please[48].

Ransomware

As the name implies, when it infects your computer, it behaves like a ransom, encrypting the whole operating system, and any other plugged external drives too, asking for money, in order to give you a password to decrypt your files, and recover them. There is no way around it in most cases. It doesn't matter if you successfully remove the malware itself, because your data will still be inaccessible if there is no decryption tool. Booting up another live OS to bypass it or taking the drive out still does not help, because even if you copy the files, they'll be unreadable. You could pay to get the key… But even then… They still could just refuse to give it to you. After all, you don't even know who they are, because the payment is via some cryptocurrency, and due to its nature is very hard to track down.

The most popular example is the one you're seeing right now, called WannaCry[49], it exploited a vulnerability in Windows, because of course it's Windows, called EternalBlue, allegedly made by the NSA. Now, Microsoft did release a patch one month before the widespread attack, but most people don't want to upgrade. I understand Windows Update tends to suck, but losing everything also sucks. They demanded 300 dollars worth of bitcoin, increasing it later to 600 dollars. You only had 3 days to pay the ransom, or your files would be shredded. And it was even worse, because the malware had a flaw where even if you paid, there was no way for them to know what computer paid and which one didn't, causing around 4 billion dollars in damages and losses…

WannaCry does not work as of now[50]. It had a very likely, accidental killswitch that nobody knows precisely what it was for, but could reinforce the theory that it was unfinished. It checked if a really long, bogus and hardcoded domain existed. Because nobody had it, the malware would continue… But, an ex-black hat hacker by the name of Marcus Hutchins[51], while reverse engineering the ransomware, noticed this weird behavior, buying the domain for $10, this activated the hardcoded killswitch and stopped copies of the malware from executing, likely saving millions of computers in the process, even though, he was arrested and sentenced later to one year of supervised release, as he helped to make the banking malware Kronos years before. Tells you that you probably shouldn't see people in black and white…

47 *https://www.bleepingcomputer.com/news/microsoft/microsoft-plans-to-kill-malware-delivery-via-office-macros/*
48 Hey, script reader… What did I tell you? Fine: https://www.zdnet.com/article/openoffice-macro-worm-exposes-bad-bunny/
49 *https://www.kaspersky.com/resource-center/threats/ransomware-wannacry*
50 *https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/*
51 *https://en.wikipedia.org/wiki/Marcus_Hutchins*

Now, while those original WannaCry copies don't work anymore, thanks to the domain killswitch. This one, in an updated version without that flaw and other ransomware attacks are still very present, some not only encrypt the data, but leak it.

The best way to protect yourself against something like this is prevention. Make regular backups to an external drive and unplug it, avoid downloading suspicious files, always have your OS to the latest version.

Tier 3

Threat Model[52]

As much as we hate to admit it, we're never going to be perfectly private and secure, and the more you seem to improve these aspects, you stand out more, and the less convenient it will very likely be for you. So, a threat model helps you to decide who it even is that you're trying to hide your information and secure your data from. There is not a universal method, but by starting to brainstorm with questions like: What are my priorities: Is it a government? Individual bad actors? Companies?

For example: If you're trying to hide from Google, you could drop Android entirely, Chromium and YouTube, and the many hundreds of things they own, even indirectly, with things like Captchas, Sign In with Google, Firebase, that probably applications you didn't even know used and so on… But even when doing this, you could be subject to an attack, and running Tor everyday when they still know your real name and address is not going to help. It's all about balancing priorities and sacrifices.

You could do small steps, like checking this PrivacyTest.org[53] chart, comparing all browsers and switching to a better one, using temporary email, downloading your Google Takeout data, disabling whatever you don't need and deleting unnecessary accounts.

I would recommend you channels like Techlore[54], Eric Murphy[55] and The Linux Experiment[56]. But remember, there is only so much information I can give you in this video, again, don't blindly trust what I or someone else says. The cybersecurity community… or just tech community is very prone to gatekeeping and things like that.

And I know there's always going to be that guy that says "But I have nothing to hide". In that case: Could you give me your phone unlocked for a second?

Gaming Hacks

One of the biggest attacks was the 2011 Playstation Network breach. Starting when Sony removed OtherOS, a feature letting you install Linux on PS2's and 3's, and it was totally official[57]. Even the

52 *https://www.techlore.tech/resources*
53 https://privacytests.org/
54 https://www.youtube.com/watch?v=DHZRhboZhfI&t=8s
55 https://www.youtube.com/watch?v=H414XdcbC4Q.
56 https://www.youtube.com/@TheLinuxEXP/videos
57 *https://web.archive.org/web/20080202170343/http://ps2dev.org/*

US Air Force used this feature to create a supercomputer[58]. The removal bothered many modders. One of them was George Hotz, that you might know as that 17 year old to be the first person to hack an iPhone into accepting other carriers[59]. In 2010, he managed to hack a PlayStation 3 by getting access to the encryption keys that could allow users to flash anything they wanted to the console[60], like Homebrew. It's a modification that can make consoles do things they were not intended for, like backing up saves, installing emulators and sideloading games. And the latter is the one Sony had issue with, filing a restriction order against Geohot *(his nickname)*, who had added protections in order to stop people from using the jailbreak to run external games[61]. Sony eventually dropped the case, but they had already crossed the line, as Anonymous were angry[62] and launched a DDOS attack to the PlayStation Network, forcing Sony to shut it down for 23 days until they stopped, followed by another hacking group with the name of LulzSec, leaking the banking and personal information of around 77 million PlayStation users[63].

To this day, people still mod around their PlayStations and install Linux on them[64], because it's just a game you can't win, it's a matter of time. But people also use some of these security flaws in games to cheat, like in GTA Online. This game still uses P2P connections, making it very insecure. A modder can always get your IP easily, find out your country and spawn enough items for the game or your computer to crash[65]. But It's understandable, because Rockstar barely earns money from it, right?

Some gamers are also being subject of scams, where they ask for personal information, or to download malware in order to get money in Fortnite, Roblox or whatever game is trending[66].

But even worse, in some cases, the own anti-cheat systems can be malware. Like in 2013, when an Anti-cheat made by the Esports Entertainment Association was used by one of the developers to mine crypto on the test user's computers[67].

What happens to deleted files?

We know that moving a file to the trash can does not delete it. It's more of a prevention measure in case you removed something you did not intend to, being able to restore it if you do in inside of the usually, 30 days window.

But even if you delete files from the trash can… These could still be there, in some way.

When you do it, the operating system marks that part in the disk as something that can be replaed by other content. It depends a lot, but chances are that that specific thing you deleted never gets overwritten by another file, so the data remains there. It could be partially or completely available still. That's when programs like Recuva can still recover your files.

58 *https://phys.org/news/2010-12-air-playstation-3s-supercomputer.html*
59 *https://www.imore.com/original-iphone-hacked*
60 *https://www.edn.com/the-sony-playstation-3-hack-deciphered-what-consumer-electronics-designers-can-learn-from-the-failure-to-protect-a-billion-dollar-product-ecosystem/*
61 *https://www.cnet.com/home/smart-home/geohot-speaks-out-on-ps3-jailbreak-legal-battle/*
62 *https://www.eurogamer.net/anonymous-hackers-declare-war-on-sony*
63 *https://www.cbsnews.com/news/lulzsec-explains-why-its-gone-on-hack-rampage/*
64 *https://www.youtube.com/watch?v=bRKiiv9ATfI*
65 *https://kotaku.com/meet-the-people-who-helped-turn-gta-online-into-a-cheat-1795296864*
66 *https://www.theguardian.com/money/2021/oct/17/from-fortnite-to-fifa-online-video-game-players-warned-of-rise-i*
67 *https://www.keengamer.com/articles/features/opinion-pieces/kernel-level-anti-cheat-and-7-games-or-programs-that-use-it/*

If you don't want this to happen, you can use something like File Shredder[68] or BleachBit[69]. This is an open source, Linux and Windows system cleaner. It can help you to "shred" your files, which means directly overwriting that part of the disk, making it very unlikely to be recovered… Even then, most file managers in most operating systems offer image, audio and video thumbnails by default, to avoid recreating them, that could be unnecessarily demanding according to the amount of files you have, they usually just store a low res copy of that picture inside of another system directory. In Linux, it's under the dot cache folder, so you could take a look there every once in a while...

Also, assume that everything you upload to the internet is always going to remain there. If you have this mindset, it's less likely you will upload something that you later regret.

Trojans

Getting their name as a reference to the Trojan horse story, this is a type of malicious program that disguises itself as a legitimate one, or just a system file, to avoid detection[70].

While running in the background, they can download files from the internet, steal accounts, contacts and download other malware. Some phone Trojans can send text messages, that are often charged to the user.

ANIMAL is considered the first computer Trojan[71], released back in 1975, it was just a game that asked 20 questions to guess the animal you're thinking of. It spread across the network, without doing anything harmful, really. It was back when most of the malware was a joke or to show off the skills of the developer.

One of the most popular examples is the Memz Trojan[72]. Getting its name from Memes and created by the user Leurak, it is not necessarily made with bad intentions, but more as a proof of concept for a video. Still, it can be pretty dangerous, so… If you plan on running it, do it from a VM, and be careful. I limited the colors here, because there are a lot of flashing lights.

It starts by asking for confirmation twice *(Shows dialogs)*, and once accepted, runs the notepad, with the following message. From there, it can browse on the internet things like:

> *How to remove a virus*
>
> *Bonzi buddy download free*
>
> *facebook hacking tool free download no virus working 2016*

And more...

68 *https://flathub.org/apps/com.github.ADBeveridge.Raider*
69 *https://www.bleachbit.org/*
70 *https://us.norton.com/blog/malware/what-is-a-trojan*
71 *https://www.malwarebytes.com/trojan*
72 *https://malware-history.fandom.com/wiki/MEMZ*

After some time, Memz will move the cursor, show popups and random icons, making a "tunnel effect" and more visual annoyances[73] that make the PC practically unusable. If you try to kill Memz with the Task Manager, showing multiple random messages, like "Somebody once told me… The Memz are gonna roll me", before showing a Blue Screen Of Death.

Once the computer reboots, instead of the classic Windows Start Screen, You'll see the text "Your computer has been trashed by the MEMZ Trojan. Now enjoy the Nyan Cat…".

There is allegedly a harmless version of the trojan, but I'm not confirming that one.

Botnet

This is a group of computers that were infected without the user's knowledge, pretend to work normally, but once they are activated, they work together to perform attacks, like Denial Of Service, capable of taking a website down due to request saturation, even if just temporarily. They are also able to click on a lot of ads to gain profit fraudulently, solve Captchas, and send spam.

Because most of these PCs and even phones are legitimate ones, and they're from all around the world, it's not that easy to block them. I mean, in some cases, we're talking about millions. More recent types of botnets are decentralized, and can include IOT devices, like thermostats, cameras and light bulbs[74]. These, usually run a type of Linux or BSD, because they don't need direct human intervention to work, being controlled through a remote app, have great support for low cost architectures, they're flexible, lightweight and free[75]. But the systems IOT devices run tend to be unmaintained. I mean, after all, how's the user going to notice? This was the case of the Mirai botnet, infecting devices via Telnet[76], with common passwords. If you don't know, this command is the predecessor of SSH, and it's very insecure. This botnet was originally just going to attack rival Minecraft servers with DDOS attacks, yes… But on October 21st, 2016, the botnet attacked Dyn[77], a domain provider for giants like AirBnB, Amazon, Github, Netflix, Paypal, Reddit and more, leaving users without access to these services.

The source code was released, leading to the creating of more botnets. Some are rented by script kiddies to perform attacks, and this seems to be the future: Malware As A Service.

Some people theorize most computers could be part of a botnet. If you see some weird behavior like sudden overheating, more resource usage than expected and slow networks, you could check the traffic and see what's really going on.

If you're using IOT devices, please don't. At best, they're a privacy nightmare and buggy, at worst, they could literally leave your door open. If you need to use it, at least change the default password, block external Telnet, SSH and HTTP(S) ports; and self host it with Home Assistant[78] or something. The more I get into Tech, the more hesitant I am to jump into the next tech buzzword bandwagon.

73 *https://dzogame.vn/gaming-gear/malware-bien-may-tinh-cua-ban-thanh-mot-dia-nguc-so-kinh-hoang-nhu-the-nao-13337-58.html#gsc.tab=0*
74 *https://telnyx.com/resources/iot-devices*
75 *https://en.wikipedia.org/wiki/ARC_(processor)*
76 *https://www.makeuseof.com/why-you-should-not-use-telnet/*
77 *https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/*
78 *https://www.home-assistant.io/integrations/*

Tier 4

Forkbombs

Getting their name due to creating infinite sub-processes and put into a diagram, could look like the shape of a Fork, these are attacks that take up all the user's resources.

I'm giving you an example, but never run it. Again, because of YouTube I have to specify that everything in this video is presented with benign, educational purposes.

The commands you're seeing right now are classic examples of Fork Bombs[79] [80]. In summary, they call themselves, and create a background sub-process that will create another one and so on, until the computer's RAM is full, forcing your computer to freeze and reboot. In these cases, they don't do a lot of damage, because just the memory was overloaded, and in most cases, you can easily kill the root process to stop it, depending on how much RAM and Swap you have, and how quick you are. Or prevent it to an extent by limiting resources to other users with the command ulimit, or globally in the /etc/security/limits.conf file, even though, in some systemd OSes, you could already have a process limit.

Fork bombs don't necessarily have to be a command in an OS, they could be a bug, or more graphical, draining the resources quicker, usually by spawning windows. This is the case of youareanidiot[81], a website that still exists, at least, a recreation. It shows these smiley faces, and if you click on any of them, or press Ctrl, Alt, Delete, or F4, the page will override these keys, and replacing the action to spawn even more windows instead. Before you go and try it, because I know some of you will, this is cross-platform, as it is a very small Javascript program, and depending on your browser, it could block the Pop-ups or not. Also, I found this in the source code, being able to add itself to Internet Explorer as a bookmark. It also shows a lot of flashing lights and loud noises, with the most annoying song you'll hear in your life. Some variations install malware, are more aggressive with the amount of spawned Windows, contain shocking pictures and more. Kill it with a Task Manager, but not from the shortcut, or force stop it from the App List.

Fork Bombs are one of those malicious pieces of software that can affect the host system, even in a virtualized environment[82]. Because the computer sees the VM as a normal process, it can still overload the host system if you don't apply the proper resource limits.

Another more dangerous variation of this are zip bombs[83]. These look like zip files and apply to any system, but once extracted, your OS will become extremely saturated, as it turns out that small kilobyte sized file contained Petabytes, being around millions of GB. It's a titanic amount of information even a high end PC could not process that well. But in reality, most of these only have blank files, copied and recursively compressed. Some of them don't even need to use recursion to work, and could include other malware. Just by themselves, the zip bombs will not only make your PC very slow and consume your RAM, leading to crashes, but they could also fill up your entire disk in a short amount of time and overheat your system. Be very careful with the files you

79 *https://itsfoss.com/fork-bomb/*
80 *https://www.youtube.com/watch?v=LtGpKve-LDw*
81 *https://github.com/Mist0090/youareanidiot.cc/blob/main/scripts/you.js*
82 *https://security.stackexchange.com/a/9017*
83 *https://www.microsoft.com/en-us/windows/learning-center/what-is-a-zip-bomb*

download from the internet. These zips shouldn't require an executable or write permission, because they're technically just being read. Zip bombs are really easy to make, and could be automated. Only accept from trusted sources, and if you're suspicious, you could inspect it with VirusTotal.

Rootkit[84]

Named after the words "root", the superuser's name in most Unix-like systems and "kit", as in a collection of software, I think you can already guess what they're capable of. Even though, don't be confused by the name, they could attack any system, regardless of Unix-like or not. Once they have access to elevated permissions, they're able to get access to all information in the PC, changing passwords, stealing data and downloading other malware, of course.

There are some that go too deep, called bootkit, and even manage to go before the operating system, replacing your bootloader with a modified one, like BlackLotus[85], that basically managed to fool Windows and Secure Boot, flashing itself as part of the UEFI. I'm not going to pretend to understand how they did this, but it is a reminder of being really careful when downloading any type of updates.

For this entry, it's important to mention DRM implementations that could be considered a rootkit. If you don't know what that is, it stands for Digital Restrictions… I mean, Digital "Rights" Management, just not *your rights*. For example, have you ever wanted to take a screenshot in Netflix? Not necessarily with bad intentions, but it could be that something funny happened in your favorite show, and you took a screenshot to send it to your friend… But when you look at it… It's black, when the show clearly was just fine. Well, that, and many other artificial limitations are DRM, and is often one level above the user, mainly in phones and browsers. With the objective of unsuccessfully stopping users from distributing unauthorized copies, even if they bought them and it wasn't a subscription.

This was the case of the Sony BMG Rootkit[86]. In 2005, they would use the Autorun feature enabled by default in Windows, that lets you choose the behavior of external drives. In this case, it would install the XCP rootkit on your PC the moment you inserted the CD. As an attempt to stop users from ripping it. There was no notification about this, and the user could not remove it, consuming a lot of resources in the background. But the geniuses at Sony made an accidental vulnerability by hiding all the files starting with the "sys" prefix, leading to Trojans like Breplibot to take advantage of this, and disguise themselves more successfully. The worst part is that even if you tried to remove the rootkit, it could potentially be illegal, as you would be bypassing DRM. Another Dystopian thing to worry about. And I'm pretty sure that didn't stop users from ripping their CDs. I mean, it was the 2000's and we're going full circle here.

Niche Malware

As of now, you've seen mostly Windows malware. I've already mentioned Android malware in a previous Iceberg, but we haven't seen a lot of more niche examples.

84 *https://us.norton.com/blog/malware/rootkit*
85 *https://securityaffairs.com/148482/malware/source-code-blacklotus-uefi-bootkit-leaked.html*
86 *https://www.makeuseof.com/tag/drm-threat-computer-security/*

Apple's software is often regarded as the pinnacle of user interface, experience and security, but that does not mean it's invulnerable, nothing is, nothing will be. Elk Cloner was the first virus for the Apple II computer, but it was harmless, made as a hidden prank that got triggered when you played a game fifty times[87].

What could be considered the first harmful example, was the worm Leap[88] for the formerly called OS X. After receiving a compressed tar file from iChat, that contained a program disguised as leaked pictures of the next OS X update. This worm will open a Terminal that asks for your password in order to be run, and if given, it will use Spotlight to find your 4 most recently used apps, owned by you and not the system, changing their permissions, and adding an extended attribute. Basically, just metadata, like the one you could find in mp3's, but for all files[89]. In this case, it is a property with the name of "Oompa", and "Loompa" as value. That's how it knows what apps are affected, and where the alternative name for this worm comes from. You probably wouldn't ever see this, correct me if I'm wrong, but I think the Finder and most Linux file managers don't show them, so you'd have to use the Terminal. A persistent copy of Leap will be saved to /tmp, and sent to all your Bonjour iChat contacts[90].

As for Linux, the first virus was Staog, written in Assembly, by a group known as VLAD, residing in memory and infecting any executable, exploiting multiple vulnerabilities to become root.

Even if really rare, there have been some more desktop focused Linux malware, like "EvilGnome[91], discovered in July 2019 and getting its name from the attempt to disguise itself as a GNOME Extension. But turns out it is a self-extractable file[92], storing its contents to the cache dotfolder / gnome-software / gnome-shell-extensions, adding a cronjob, that will run every minute, with the rest of the files being keyloggers, an audio recorder and screenshot taker. Pretty intrusive, and yeah, thinking about it, also a real Shell extension could do similar things, as they have access to more low-level things like window management, clipboard content and core aspects of the UI. So, be careful with whatever it is you download, even if it is a GNOME or Plasma add-on. Read the reviews, check the permissions, the source code and if you're running GNOME, install only via the Extensions Manager.

There is another very interesting type of proof-of-concept Linux malware I found by Mazin Ahmed[93], where an attacker could replace a genuine desktop file with another modified copy. In case you don't know what they are, they define entries in the App List of a Linux Desktop. You would open the application, but instead of that application, it would look like it, because you can change the icon, but running a command or other thing instead. The limitation this has is that they need to have executable permissions, and whatever they do is limited to them. Also, as far as I know, this could also happen with the equivalent of a desktop file in Windows. But it's definitely something to keep in mind.

87 *https://www.thepcinsider.com/history-of-computer-virus/*
88 *https://www.cnet.com/tech/computing/oompa-loompa-trojan-osxoomp-a-3-clamxav-virus-definitions-updated-when-the-trojan-will-ask-for-an-administrator-password/*
89 *https://wiki.archlinux.org/title/Extended_attributes*
90 *https://www.macworld.com/article/178874/leapafollow.html*
91 *https://intezer.com/blog/research/evilgnome-rare-malware-spying-on-linux-desktop-users/*
92 *https://github.com/megastep/makeself*
93 *https://mazinahmed.net/blog/using-ubuntu-desktop-as-malware-vector/*

Finally, as a quick mention, most routers run some type of Linux or BSD, and they can also be infected with malware[94], becoming part of a botnet, like the previously mentioned Mirai. It is not common, but it can be dangerous, as with the router, you have indirect network access, to all the wired and wireless devices in a house or business, and it can slow the internet down, download weird files, show more ads, do suspicious redirections and more. Please, change the password, because it also gives access to the Web UI, and set up a guest network, you could even use a QR to connect visitors, more secure and convenient for both.

And while, Unix-like systems are usually more secure than Windows[95] [96]. *I'm making another unnecessarily long video about this*, but summarized, it's not only because of the smaller marketshare, but because they are just inherently more secure with things like default permissions, ownership, and application permissions in macOS, and Flatpak in Desktop Linux… Still update your systems, don't blindly run programs and all of that, because some hackers have started to keep these systems in mind too[97].

Hardware Vulnerabilities

Hardware vulnerabilities are usually worse, because they cannot be fixed, or at least, not completely with a software update.

You've probably heard about Spectre and Meltdown[98]. They exploited a behavior in CPUs called Speculative Execution, that is when the processor tries to guess what it needs to do first, if it's doing the right thing, you could save some processing power, and if it's wrong, it does the other thing instead. But, because this works to a kernel-level, somebody with bad intentions could make the CPU run code it shouldn't, and get very sensitive information like passwords. The worst part is that basically most processors from the past 20 years are affected by this, including Intel, AMD, Apple and ARM. Fortunately, some patches have been made, but require separating the kernel and user processes more, meaning that in most cases, there's going to be a significant performance decrease, and it is a partial fix.

Speaking more about firmware. In 2018, a copy of a legitimate ASUS UEFI Update was modified and uploaded[99], even managing to sign it with the official keys from Asus, and keeping the same size, so checking hashes would be irrelevant, because they would've been different either way. This attack, called ShadowHammer, is believed to have affected around a million computers, but interestingly enough, they were targeting specifically 600 computers with hardcoded MAC Addresses. Until Kaspersky found it in 2019. If you have an ASUS Motherboard, you can check if you're one of those targets in the website I'll leave below[100], you likely want to clear CMOS and update the UEFI, but do it whenever you're sure that your power source and network are stable, because a wrong update, depending on the motherboard, could be irreversible, and brick it, making your computer unusable. Don't ask how I know.

Finally, both Intel and AMD contain microcontrollers within their processors, the Management Engine and Platform Security Processor, respectively. Both have been criticized for running a mini,

94 *https://us.norton.com/blog/privacy/how-to-tell-if-someone-hacked-your-router*
95 *https://www.progress.com/blogs/unix-has-always-been-more-secure-than-windows*
96 *https://security.stackexchange.com/questions/96004/are-there-technical-differences-which-make-linux-less-vulnerable-to-virus-than-w?rq=1*
97 *https://www.intego.com/mac-security-blog/10-years-of-mac-malware-how-os-x-threats-have-evolved/*
98 *https://www.cloudflare.com/learning/security/threats/meltdown-spectre/*
99 *https://www.theregister.com/2019/03/25/asus_software_update_utility_backdoor/*
100 *https://shadowhammer.kaspersky.com/*

proprietary operating system that handles very sensitive data[101]. Leading to some people calling this "Spyware at the Hardware Level". Regardless of the veracity of this claim, it is true that it runs at a deeper level than the OS and UEFI. Both of these companies, are usually very good when it comes to open sourcing their drivers and technologies, so it is a little weird that they decided to not open source this. I can see why it could be "security by obscurity", but that didn't prevent them from having many security vulnerabilities that could be used to install rootkits, steal encryption keys and run external code.
You can disable them in some cases[102], but for most CPUs made in the past decade, if even possible, it's very hard, and could have some security implications, unfortunately...

Quantum Computers could break encryption

Encryption is not perfect. It can be cracked eventually, but it relies on how long it would take for it to be solved. In most cases, with a good algorithm and passphrase, we're talking about centuries, millennia or literal millions of years, and by then, you've likely already changed the password, and we're all going to be dead, too.

However, there is a type of supercomputers that have taken relevancy in the past years: Quantum computers. Like the name suggests, they work in a similar way to the concept of Quantum Mechanics, that I'm clearly not an expert at, but the people that are at MIT explained in this article how they could, theoretically break 2048 bit RSA encryption in 8 hours[103], ridiculously short for something this complex.

This opens a very frightening scenario where governments and corporations that have Quantum Computers at their disposal take this as an advantage to decrypt sensitive data. And I'm not just referring to your messages and personal info, but to military and medical information of other countries.

Now, you probably shouldn't worry as of now. As the same article mentions that in order to do something like this, we'd need a 20 million qubits Quantum Computer, and the most powerful one we have is of 70 qubits[104].

Still, some organizations like Google have already started to promote the use of Post-Quantum Encryption[105].

Fileless Malware[106]

This is an increasingly popular type of malware. Until now, all of them had as a common pattern the presence of malicious files, but this time, you don't even need any external executable to damage a system, because it exploits core system components to be the ones to cause damage, often running malicious code stored in memory. This is actually how most malware began, before

101 *https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/intel-me-sps-and-txe-patched-after-discovery-of-vulnerabilities*
102 *https://hackaday.com/2020/06/16/disable-intels-backdoor-on-modern-hardware/*
103 *https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/*
104 *https://www.technologyreview.com/2019/05/09/135440/the-new-benchmark-quantum-computers-must-beat-to-achieve-quantum-supremacy/*
105 *https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world*
106 *https://www.fortinet.com/resources/cyberglossary/fileless-malware#:~:text=Fileless%20malware%20is%20malicious%20code,downloaded%20to%20your%20hard%20drive.*

hard drives. And, while that means rebooting the computer is going to get rid of it, even if you do it within a couple of minutes, it could've done a lot of things by then, like spreading through your network or downloading another type of malware. Making it very hard to notice and find the perpetrators because any evidence is going to be permanently wipe
One of the first instances of this could've been The Code Red Worm[107], as it didn't download any type of file, just took advantage of a vulnerability in the Microsoft Internet Protocol Server, exploiting a Buffer Overflow, basically, storing a value longer than what that variable could hold, so it is replaced by whatever the attacker wants[108]. Because all of these variables are saved in RAM, no files were needed, being able to hack any infected web servers, displaying the message you're seeing right now. And later, launching a DDOS attack to the White House's website. And that was in 2001… Imagine what they could pull off today...

Physical Security

Standing for "Quick Response", QR Codes are here to stay[109]. And even though, they're pretty comfortable and not inherently bad, only being able to store around 4000 text characters, they can be used for malicious purposes. A new type of attack has risen ever since the pandemic, being pretty easy to do[110]. An attacker places a QR Code in public, often covering up a legitimate code, and once scanned, it can forward that device to a phishing website, or initiate an automatic download. Remember that it is text, but you'd be amazed at how much information you can store just with raw text: Phone numbers, WiFi networks that could be insecure, links, even code, I guess. But I don't think that last one is necessary for most attacks to be successful.

USBs are also one handy little thing we all use. And it has become popular to leave them in public places, like parking lots, known as a Drop Attack. Curious people will plug them to see what they have… And you very likely won't like it. Some disguise themselves as a USB Keyboard, requiring no additional drivers in almost all operating systems, being able to do something like opening a Terminal and running some commands by itself, the possibilities are limitless and in a matter of seconds. Devices like the Rubber Ducky can do things like these, but you don't necessarily need that in some cases. Like I mentioned before, somebody could put an Autorun script that executes malicious code, and deletes itself in a matter of seconds, and you would never know.

Even if no malware is present, there could be instances of pendrives having illegal material, that could be very disturbing and get you in a lot of trouble.

A similar case could happen with public USB outlets[111]. Even if not widespread, it's technically possible for a USB charging station to propagate malware to your phone if you connect it, as some implementations of USB can provide power and data transfer[112]. To prevent it, try to avoid USB ports, and just go for power outlets, that are limited to charging, being often faster. If there is no choice and you have to use a public USB charger, never select data transfer, just charge only, and turn Developer Options off.

107 *https://www.wired.com/2001/07/code-red-is-this-the-apocalypse/*
108 *https://www.comparitech.com/blog/information-security/buffer-overflow-attacks-vulnerabilities/*
109 *https://www.businessinsider.com/guides/tech/what-is-a-qr-code?r=MX&IR=T*
110 *https://www.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan*
111 *https://www.fcc.gov/juice-jacking-tips-to-avoid-it*
112 *https://www.snopes.com/fact-check/serious-threat-of-juice-jacking/*

Some other dangerous devices to look out for are USB Killers. And as the name implies, these are able to generate an electrical charge that fries your battery, and could potentially explode.

Remember to also have more traditional means of physical security, in the case of information and valuable possessions, a physical vault is going to be useful, and a paper shredder can help you to get rid of important documents. Covering your webcam with a piece of tape can be better than no cover at all, some of them including a privacy shutter nowadays, but if possible, try to get a device that not only covers the camera, but blocks the hardware connection directly.

A Faraday bag[113] could be helpful to block absolutely all wireless connections, like Wi-Fi, Bluetooth, NFC and cellular.

Also, look for hidden cameras in hotels. Yes, it's more usual than you think. Some can't even be seen easily by the human eye, so use your phone[114].

I know it could sound like paranoid-levels of security, but people in certain countries might need this and it's always good to know prevention measures.

Tier 5

Deep Web

The mystified Deep Web[115] is essentially what Search Engines don't index. For example. If you look up in Google or other Search Engine: "gmail", you'll find a lot of search results, between them, the official website as the first result, that is what search engines index, often called the "Clear Net"

In this example, the Deep Web would be your specific email inbox. As you cannot find that one by searching on the internet[116]. Same goes for banking information, private videos on YouTube and you get the idea… It's not necessarily something bad.

When most people say "Deep Web", they're usually referring to the Dark Web. Which is a type of Deep Web you usually can only access them with a link of .onion domain, accessible by the Tor Web Browser. Standing for "The Onion Router", this is an open source fork of Firefox, created by the US Government, and this is no conspiracy, it's literally what happened.

Every computer connects to the Tor Network, working as nodes and volunteers. Your traffic goes through many of these nodes, always encrypted and decentralized, making it very hard to track. Perfect for some more illicit type of businesses and actions, even though, it does have its legitimate uses, like circumventing censorship. Even Facebook has its extremely ironic .onion counterpart.

It has increased in popularity in the past few years, mainly by YouTubers that make fake videos about ordering "really creepy things" from the Dark Web.

But there is some reality to this. It is true that some things like substances have been traded here, creating multi-million dollar websites like the defunct Silk Road. Which his creator got caught

113 *https://www.howtogeek.com/791386/what-is-a-faraday-bag-and-should-you-use-one/*
114 *https://edition.cnn.com/travel/article/hidden-spy-cam-airbnb-scli-intl/index.html*
115 *https://www.cloudwards.net/the-deep-web/*
116 *https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web*

when suspicions were confirmed, as he used the same username when he promoted his Dark Web business in the early days, and when he asked for programming help in a forum, giving his full name and email[117].

Seems like the bad reputation also comes from other websites, that host content including conspiracy theories, alleged leaked documents, being the ones from WikiLeaks at least partially confirmed, instructions for dangerous things, often fake hitman scams, and content involving vulnerable people… I apologize for the censoring, but I'm trying to stay within the guidelines, because this is likely going to get demonetized, but at least, I don't want the video to be taken down. I hope you can understand…

The whole myth blurred the lines and I guess some of it began as a meme, becoming later a creepypasta. It introduces the more fictional concept of the "Mariana's Web"[118] in reference to the Mariana Trench, the deepest point on Earth, and things like that. It supposedly gets harder to access it the lower you go, with some exaggerations saying that at the lower levels you would need to genius in quantum mechanics and things like that, being able to find sensitive government information, Tesla's inventions, the Location of the Atlantis, Alien footage and more.

There is also the rumor of so called "Red Rooms", a website where you see a person… Have the worst time of their life… via streaming. Donators could participate in this by giving instructions… Of course, this is very likely fake, as the Tor Network is known for being really slow. It's like if you used multiple VPNs, and it just wouldn't work.

But honestly… I would worry way more about the Clear Net than the Dark Web. I bet it's not that different. There is only so much moderation a person and AI can do. So be careful out there.

Ashley Madison Data Breach

Created in 2008, this is a dating website… With the infamous slogan of "Life is short. Have an affair". You know where this is going...

The users of this platform faced their worst nightmare when in 2015, the information of around 30 million users was leaked in the form of multiple data dumps[119], containing names, passwords, addresses, phone numbers and banking information. It is not clear how many of these are actually real, as the dating site does not ask for email confirmation, being prone to a lot of bots, that the leaked confirmed… With 90-95% of real, active accounts being men[120].

The company also lied about their policy of deleting your account if you paid. The information was still stored there.

The consequences were pretty bad, because aside of the obvious, many people were shamed, and least, one passing has been confirmed explicitly related to this incident[121].

117 *https://en.wikipedia.org/wiki/Ross_Ulbricht#cite_note-Popper-29*
118 *https://www.techtricksworld.com/mariana-web/*
119 *https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked*
120 *https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/*
121 *https://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/index.html*

This, and other data breaches like the 2014 iCloud Breach[122] remind us the importance of cybersecurity, and that we shouldn't rely this much on third parties. After all, Cybercrimes seem to be the future of illegal activities…

It's worth thinking it twice, you probably *do* have something to hide...

Horror Malware

I had a hard time looking up more "real" pieces of Horror Malware. Some of them fall under the Lost Media and Creepypasta territory, but I'm only giving you things that seem to have some truth to them.

The most obvious real examples are the family of horror malware. Including the Annabelle, Jigsaw[123] and RedEye ransomware. It seems like around 2017, it became very popular to use horror or controversial figures, like that German person or Anonymous, that I doubt would do something like this to a random person, but it's to add a more psychological effect that could potentially increase the chances a successful attack. Probably the source code got out or was offered as a Ransomware service, because they look practically the same, just switching the background. Some variations are more aggressive, and can even start deleting files as time goes on. In the case of RedEye, seems like it doesn't encrypt the files, just overwrites all files with 0's, acting as some sort of wiper, with almost unrecoverable data, likely regardless of payment[124].

Another quick mention goes to Windows XP Horror Edition[125]. I won't go into detail, as I've talked about it in the OS Icebergs, but it's a program disguised as a Windows Update that will turn your system into this, and will eventually brick it after a lot of jumpscares overriding the Master Boot Record. Clean versions exist, but I would not try it either way.

This one also appears to have been real. Agor.io[126] was an intentional Typosquatting website, as back in that time, the real game Agar.io was becoming very popular among people of all ages. However, Agor.io presented a screamer of Jeff The Killer that couldn't be closed, with an excessive amount of flashing lights, and a loud metallic sound, that you could think as an obvious troll and attempt to trigger seizures in photosensitive people, and according to this Reddit post[127], it was successful at hurting someone. Regardless of whether the post is saying the truth or not, other users' testimonies and info I found could confirm the existence of this website. As many other Flash Malware or Scam websites. It's likely lost, due to the shutdown of the website in 2015, and the death of Adobe Flash, on December 31st, 2020[128].

Finally, Garry's Mod is a 2006 sandbox game, and as the name suggests, mods play a big part in this, adding more items and features. The G-Man Virus is believed to have been a 2009 mod from Garrysmod.org, that showed a jumpscare of the G-Man character from the Half-Life Series. It could also open shock websites, remap keybindings and more. We only have recreations, but in this

122 *https://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9?r=MX&IR=T*
123 *https://www.theregister.com/2016/04/20/jigsaw_ransomware/*
124 *https://www.securityweek.com/redeye-ransomware-destroys-files-rewrites-mbr/*
125 *https://screamer.wiki/Windows_XP_Horror_Edition*
126 *https://screamer.wiki/Agor.io*
127 *https://www.reddit.com/r/Agario/comments/36w5w8/filling_a_lawsuit_against_the_owner_of_agorio/*
128 *https://www.howtogeek.com/700229/adobe-flash-is-deadheres-what-that-means/*

video by the user kitty0706[129], we see what could be a real footage of the lost G-Man Virus, aligning perfectly with the dates and recreations[130] in testimonies found in forums. There have been other real Gmod confirmed malware[131] [132]. So, I think it's likely for this to have existed. Let me know your opinion below.

Finally, let's talk about Sad Satan[133]. This is a real horror game, allegedly from the Dark Web. It doesn't matter where it truly came from, because the content is very disturbing either way. Containing extremely graphic content, that is very likely straight up illegal. There are "clean" versions, but these can even contain a lot of malware that according to some, is able to get out of virtual machines, and the so called "clean version" seems to be pretty much lost. Do not download this, it's not worth the risk at all[134]...

Snowden Leaks

In 2013, journalists at The Guardian gathered in a hotel room in Hong Kong to meet the now ex-NSA contractor Edward Snowden. They didn't know it at first, but with the release of the first article, claiming the US Government collected every day, millions of information from the Telecom Provider Verizon[135] [136], starting a series of revelations considered to be one of the biggest ones in the US History.

Confirming one of those things we all know and don't like to remember and that we very likely shouldn't have normalized. We're being spied on. Even if you're not a potential threat, and it doesn't matter if you're not American.

Other reports state that the agency intercepts fibre optic cables, communications from other regions, like China, the EU and Latin America and by 2014, they stored around 200 million SMS messages[137].

This is only a fraction of the alleged thousand of documents Snowden had[138]. But he still had to trade his job at the NSA in Hawaii for exile in Russia, to evade the potential 30 years of prison he could face returning to the US[139].

I recommend you to watch most of his interviews. He says some interesting things and gives some great Cybersecurity advice.

Thinking about all the Surveillance that could have been happening over these 10 years, I think being slightly paranoid is probably not very exaggerated…

129 *https://www.youtube.com/watch?v=gTihL6kH9iA*
130 *https://youtu.be/6sybLo8HzV4?feature=shared&t=705*
131 *https://knowyourmeme.com/memes/events/glue-library-goatse-screamer-incident-garrys-mod*
132 *https://www.pcgamer.com/garrys-mod-cough-virus-is-cured-but-it-could-have-been-worse/*
133 *https://kotaku.com/a-horror-game-hidden-in-the-darkest-corners-of-the-inte-1714980337*
134 *https://tvtropes.org/pmwiki/pmwiki.php/VideoGame/SadSatan*
135 *https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order*
136 *https://www.theguardian.com/us-news/2015/may/07/nsa-phone-records-program-illegal-court*
137 *https://www.bbc.com/news/world-us-canada-23123964*
138 *https://www.pbs.org/wgbh/frontline/article/how-edward-snowden-leaked-thousands-of-nsa-documents/*
139 *https://www.theguardian.com/us-news/2023/jun/07/edward-snowden-10-years-surveillance-revelations*

John McAfee's Final Years

John McAfee is known for creating the antivirus named after him. Ever since 2012, his public life has been surrounded in controversy and legal issues[140], because his neighbor was found without signs of life and with a bullet wound, causing McAfee to run away to Guatemala, stating that he "maybe said 15 words to him the 5 years he lived there", but also, that he thought his neighbor probably poisoned his dogs. When police found him, he was allowed to go back to Miami. He wanted to run for president in 2016, starting to promote Cryptocurrencies and according to The Verge, charging $105,000 per tweet to promote coin offerings. In late 2020, he was arrested in Spain, accused of tax evasion and money laundering, facing up to 30 years in prison, but shortly after… He was found in his cell. He had taken his own life[141]...

Killer Malware

WannaCry was infecting an enormous amount of computers, and it was only a matter of time until they got to… Hospitals[142]. One of the last places were you'd want ransomware that prevents your machines from saving the lives of other people. But it happened, and according to this report by the UK's National Audit Office, just by having 34 locked computers, around 19,000 appointments were canceled, and many patients had to travel further, including the accident and emergency departments, and in these situations, you don't want to take any chances because one literal second could be the difference between life and death...

Aaron Swartz[143]

He was a genius. At 13, he made the Info Network, a sort of predecessor to Wikipedia. At 14, he co-founded RSS. At 19, he was one of the co-founders of Reddit[144]. He was also very involved in preventing the "Stop Online Piracy Act", that could've made it easier for the US government to shut down any website accused of copyright. He also contributed to Creative Commons, Markdown and the Tor Network.

In 2011, he entered to the MIT's Building 16, connecting a refurbished Acer laptop to one of the servers in a restricted utility closet and began copying millions of academic journals, costing usually thousand of dollars in yearly subscriptions. It was all revealed later due to the security cameras, and was found, when he was riding his bike, intercepted by the police and the Secret Service, with the possibility of being in federal prison for up to 35 years.

The trials lasted almost two years, but finally, in early 2013, he was given a sentence, and after losing a great part of his money on the trial, as well as being devastated by the result, and the fact that he was planning to marry his girlfriend before this, ended up costing his life[145].

140 *https://www.bbc.com/news/technology-57591682*
141 *https://edition.cnn.com/2021/06/23/tech/john-mcafee-death/index.html*
142 *https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf*
143 *https://www.theguardian.com/technology/2013/jun/02/aaron-swartz-hacker-genius-martyr-girlfriend-interview*
144 *https://malicious.life/episode/episode-164/#:~:text=United%20States%20vs.,Aaron's%20girlfriend%20at%20the%20time.*
145 *https://www.npr.org/sections/thetwo-way/2013/01/12/169235633/aaron-swartz-reddit-cofounder-and-online-activist-dead-at-26*

After his death, Anonymous hacked two MIT websites, replacing them with tributes to Aaron, leading to many other attacks, and other hackers releasing scientific articles too as a tribute[146].

I don't want to end this entry too dark, so I'm going to share with you this Aaron Swartz quote, because I think it summarizes the purpose of this video perfectly:

> *"Be curious. Read Widely. Try new things. What people call intelligence just boils down to curiosity"*

Cyberwarfare

What is so bad to be deserving of this last place?

I've been making Iceberg videos for around 2 years now. And I don't think there is anything so realistic and so dreadful before. Because this could affect all of us…

I'm speaking about Cyberwarfare, a concept that is not even far fetched, and just a reality that we have barely managed to dodge.

Stanislav Petrov was a soldier in the Soviet Union, back in the Cold War. One of the nuclear attack warning systems raised the alarm. He only had 10 minutes to take one of the hardest decisions in all human history[147]. It was either send an attack, that would very likely mean a global conflict of nuclear proportions, or ignore it, and face the risk of being erased forever…

Trusting his gut, he chose the latter, ignoring the alarm, that turns out had a false positive, avoiding one of the biggest, and probably last conflict the human race could've suffered.

But this has not ended, it's an ongoing trend. Just think about all that's possible with the latest technology. I wouldn't be surprised if in the coming decades we start to see more psychological malware. Imagine a country launching a stealthy piece of malware against another one, that starts to manipulate the behavior and thoughts of the citizens. What if it starts to make random searches, or delete files that you were sure existed, but can't remember? They wouldn't know why they do what they're doing, what they like, what they buy, what they believe...

If we start to see implants in the brains of people… What could stop a bad program from introducing Nocebo effects? To distract them more, make them more aggressive or depressed? Or… Just directly damaging their brains by overheating?

Sounds exaggerated, but what is true is that we've already seen malware that attacks public infrastructure, and in the worst case scenario… Nuclear Plants. Like Stuxnet[148], a worm that is believed to have gotten to an Iran Nuclear Plant via a USB, manipulating the speed of the machinery enough for it to damage them to an extent. It was fortunately not as bad.

But, what if… As you're watching this video, many more malware that we'll never know about is being developed and attacks, in the moment you least expect it, without giving you a second to realize what's happening…?

146 *https://web.archive.org/web/20140114180753/http://beta.slashdot.org/submission/3245329/*
147 *https://www.rbth.com/blogs/2013/09/12/the_man_who_stopped_world_war_iii_and_sacrificed_his_career_29317*
148 *https://www.malwarebytes.com/stuxnet*

(Nuclear explosion footage)

(Iceberg Theme Plays)

(Shows sources)