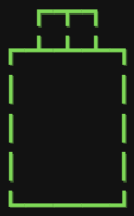
# Cyber Security 2025

Kunihito Takada

## bash-5.2$ *cat topics.txt*

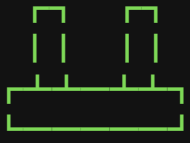
1. What even is “hacking”?
2. Cybersecurity statistics, facts, news
3. Abusing HIDs (Human Interface Devices)
4. MitM Attacks (Man in the Middle)
5. Password Management
6. Cyberattacks used in war
7. Recent news of hacking
8. Connection to other branches

## bash-5.2$ *cat details.txt*



**HIDa (Human Interface Device Abusing)**

Daily electronics such as keyboards, mouse, macros, are categorized as a HID. However, a harmless looking USB drive, could manipulate the connected device into thinking that it is a HID, taking over your controls on your device.



**MiTM (Man in The Middle)**

Communication in public Wi-Fi in your favorite café, local train station, or convenience stores, could be easily seen by third parties with free, lightweight, and banal pieces of software. However, there are always ways to prevent it.

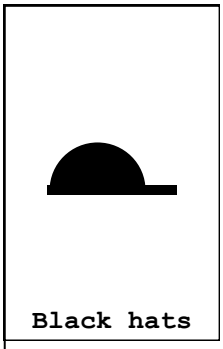
# Cybersecurity / What even is “hacking”?


You may heard the term “hacking” from movies, books, videos, news, and many media across the world in your life. Many may image a person sitting in front of a black screen, occupied, filled with green text, and insane speeds of typing. However, the process of cyberattacking, are not what the resembled image Hollywood gave you.

The term “hacking” originally meant “to do out something good” or to “outsmart” something. Some also say that the term originated from the word “hack” as in “hacking wood with an axe”. However, it is currently said that the nuance to “outsmart” is the correct origin of the term.

# Cybersecurity / Types of hackers

They are various types of hacking, and also various types of hackers as well. A couple of the 3 famous ones are the “White hats”, the “Black hats”, and the “Grey hats”.




**Black hats**

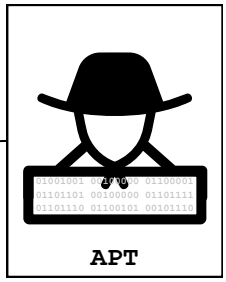
Black hats, also referred to as “crackers”, are the people who abuse an *unpatched vulnerability for their own benefits.


**Hacktivists**

People who hack for attention, popularity, ideologic reasons, etc.

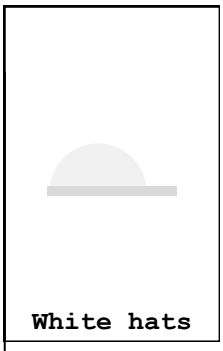

**Cyber criminals**

People who hack for money, resources, information, etc.



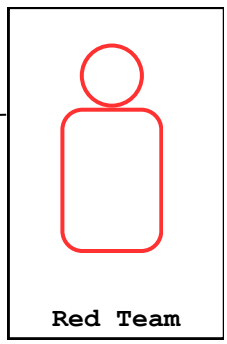

**APT (Advanced Persistent Threat)**

People who hack for an organization, nation, officials, etc., Targets organizations, such as companies and countries, rather than individuals.




**White Hats**

White hats are people who work for the targets, where they operate cybersecurity attacks for them. All cyberattacks that white-hat hackers conducts, must be with the concent.




**Red team**

A person conducts a series of tests, called penetration tests, to determine whether the system is vulnerable to any type of cyber attack in case of another incident that could occur.


Bug Bounty

## Bug bounty

Bug bounty programs conduct attacks for a set bounty, which is usually in the form of money, and find vulnerabilities before black-hat hackers conduct actual abuse. Bounties are usually opened by companies, asking the public to find new holes in their systems in exchange for money. Many companies open bounties since it is better to find the new bug and patch it before it is abused.

Grey hats

## Grey hats

Grey hat hackers are people who conduct cyberattacks without consent yet does not abuse it. Rather, they warn and tell the system about the new-found vulnerability.

Blue team

## Blue team

People who work with red team are called blue teams. A person from blue team, is rather not considered a “hacker”, but a cybersecurity specialist on the defensive. They operate in places that are called “SOC - System Operation Centers”, or “NOC - Network Operation Centers”. They monitor the system 24/7 with the help of automated software, and in a case of an incident, people from the “Incident response team” would conduct search of the vulnerability, and find for quick fixes, and patches available.

**Full credit to: (Johhny Harris)**

United States of America, uses sophisticated cyberattacks against Iranian uranium enricher facilities underground, disabling many of their equipment, and spreading their influence in other machines like a virus *(Johnny Harris)*.

The most frightening thing about cyber warfare is that it does not involve the loss of friendly personnel, and attacks can be anonymous, quiet, and, be that as it may, powerful.

Cyberattacks could be used without deploying personnel into warfare, and still be used in any period of time, either when in war, or not in war. Cyberwarfare is also cheap, and could target anything in a remote location, even involving civilians, like you.

**Why Hacking is the Future of War**

Johnny Harris

Independent journalist making videos that help you better understand the world

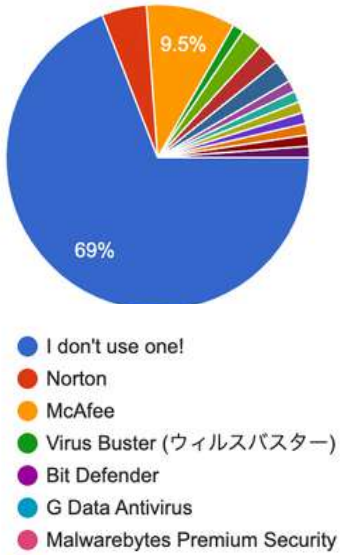
**https://www.youtube.com/watch?v=15MaSayc28c**

The video of the following is an incredible resource for learning why hacking is the future of warfare. The video was created by independent journalist, Johnny Harris. Watching this video would provide you with further information about cyberwarfare. This page uses this video as its resource.

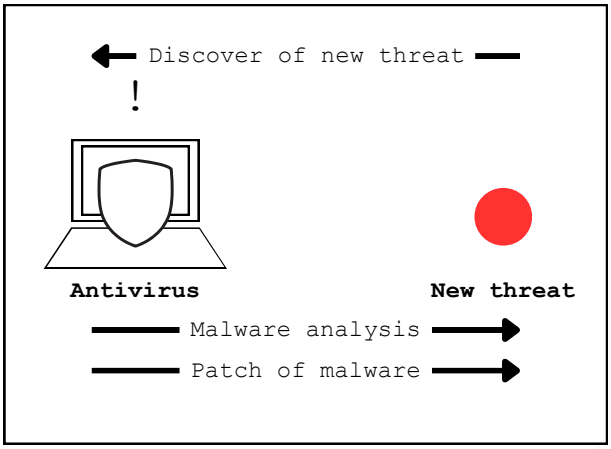
# Malware / Antivirus. Why does it matter?

**Malware Infection Screen (Virus)**

Cybercriminals discovers sophisticated methods and vulnerabilities in systems daily, and keep evolving. However, anti-virus software engineers also keep patching the evolved vulnerabilities in systems. These just may appear a cat and mouse game, yet it protects you from many types and vectors of attacks. Regardless the attack is from compromised downloads, mails, zero-day attacks, etc., anti-virus software would update its software everyday, and protects your device to its max extent.




Research conducted against 84 YIS students and teachers, shows **69%** (58 people) does not use an anti virus, and the others (**31%**) use an anti virus. Most of the YIS community are potentially vulnerable to malwares.



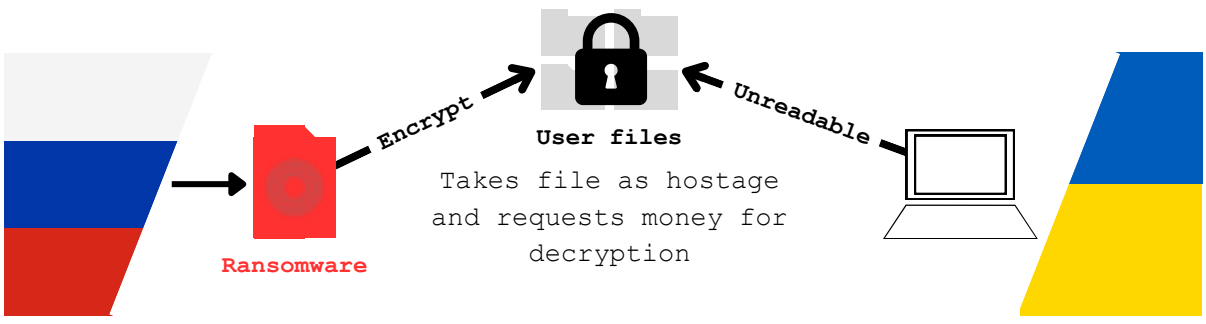

Antivirus is also the antibody of your computer. Antivirus evolves every day, establishing many of its defense systems against newly discovered attacks, updating its defense.


(BBC)

In 2017 Ukraine, red text covered all over Ukrainian computers. They were infected by Russia's newest malware, outputting the following text, to their prey:

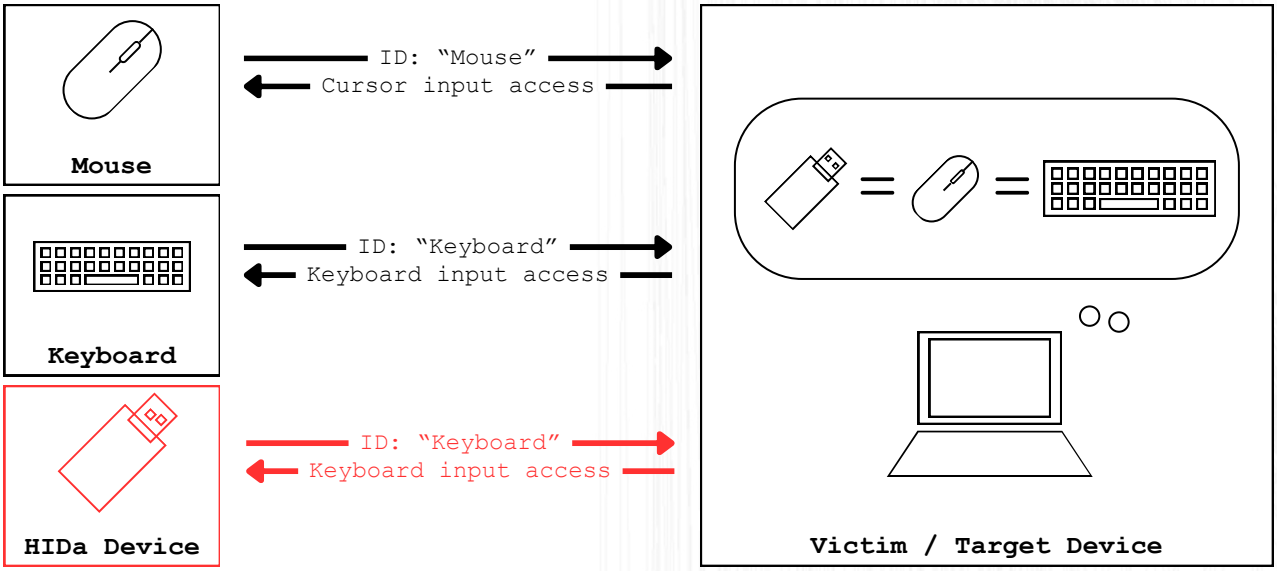
**Ooops, your important files are encrypted.**
**If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.**
**We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.**
**Please follow the instructions:**
**1. Send $380 worth of Bitcoin to following address:**
1Mz7153HMuXXTuR2R1t78mGSdzaAtNbBWX
**2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:**
**If you already purchased your key, please enter it below.**

The malware used in this attack, is called a ransomware. It would take over all the users files and encrypts them all so that the user cannot recover them for its hostage. The ransomware requests money for decryption, and in most cases, it takes NFT (bitcoin, etherum, etc.) for its form of payment, due to its untraceability *(Johnny Harris)*.

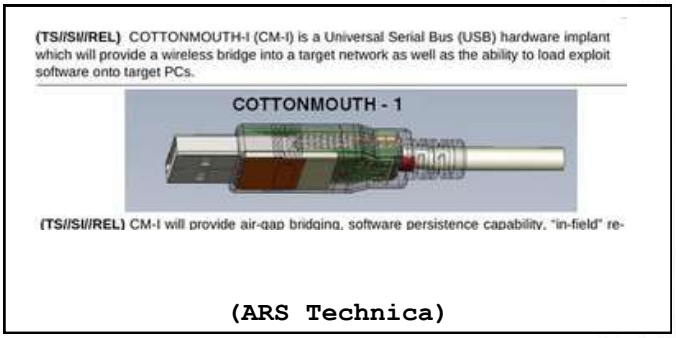


# HID Attacks / What is it?

HID stands for "Human Interface Devices". Daily electronics such as keyboards, mouse, that you use are categorized in HIDs, and used to identify the type of the connected USB device *(Lenovo)*.




Abusing this HID feature, USB devices programmed to emit HID signals to the computer could gain input access to the computer, could operate malicious macro actions into the device, such as installing malware, turning off antivirus, etc. *(Sweeney)*
HIDa (Human Interface Device abusing) devices could be hidden around in daily products as well. Charger cables, USB hard drives, cheap electronic products, etc. These HIDa devices are also referred to rubbery duckies.

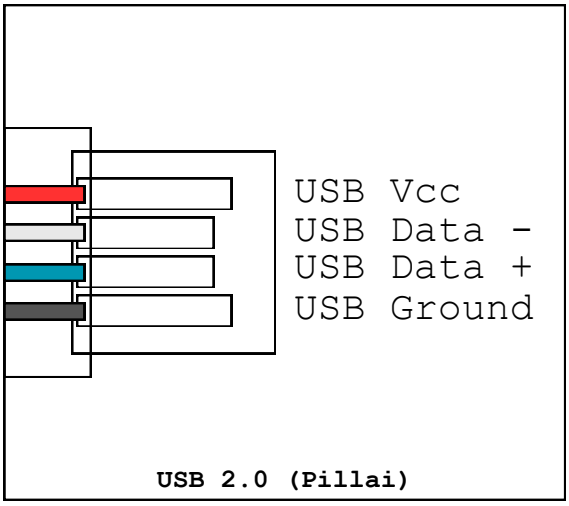



**(ARS Technica)**

Cottonmouth-1 was created by the US-NSA, and a HID device was implemented inside a casual USB-3.0 cable (ARS Technica).

# HID Attacks / How do I avoid it?

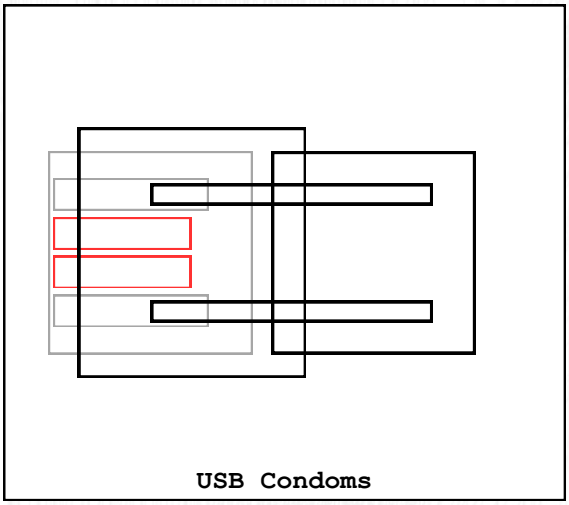
"USB Condoms" are one of the solutions to prevent HID attacks. Charging your computer via USB condoms, only allow ports that are required to send electricity to pass, and other unnecessary data ports would be physically blocked. Now, to understand how a USB condom work, is to understand how a USB port work.



USB 2.0 (Pillai)

For instance, USB 2.0 is a simple universal design for a USB port. This model communicates with the computer with the USB Data - and USB Data +, with electrical signals which has a similar concept with Morse code *(Pillai)*.

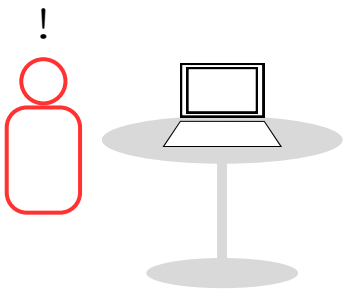
As seen in the diagram, the condom only allows electrical units to pass through, and connect to your device. This could be used when charging, preventing potential threats of HIDa in charging cables in public places *(Hudson)*.


USB Condoms

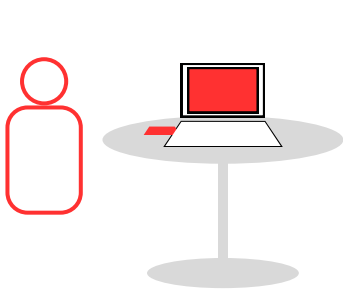
# HID Attacks / The "Shock and awe" tactic


**MacOS accessory authentication**

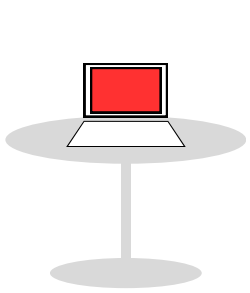
However, modern software and operating systems has many built-in prevention systems. MacOS, requires the user to authenticate an accessory to connect to its device, yet useless to the "shock and awe" tactic.



**Step 1: Find an opened device**

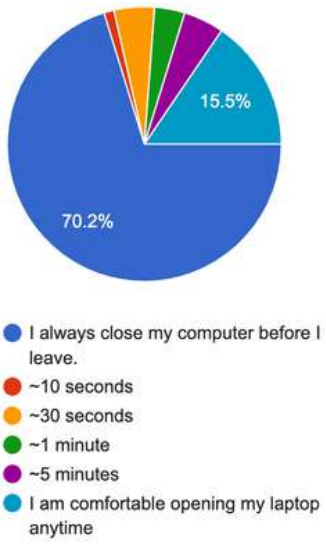


**Step 2: Plug in HIDa device and wait...**



**Step 3: Plug out HIDa device, and leave**

The shock and awe tactic, is used when the attacker has physical access over the device. The attacker would plug in the HIDa accessory into the opened device, and leave the place, inputting malicious operations.




Research was conducted against 84 people in the YIS community, asking:

***"How comfortable are you with opening your laptop when you're away?"***

**15.5%** (13 people) answered that they were comfortable opening their computer anytime to the public, being vulnerable to this tactic.

# HID Attacks / Connection to social problems

HID attacks recently had been a social problem globally. Hiding HIDa devices into charging outputs are often referred to “juice jacking”, and could be majorly seen in airports, hotels, malls, event venues, just to name a few *(Gregory)*. Notably, many of the HID attacks are easy to create, and also could be easily purchaced online.

**USB Rubberducky from hak5**

For instance, these HIDa device kits, are easily purchasable from internet shopping, and with highly advanced user-friendly firmware for the attackers device.

When creating HID devices, free licensed software, and cheap development tools, just like the Raspberry Pi Pico, Zero models. The attacks could be easily made by following tutorials online, websites, etc.

**Raspberry Pi Pico**

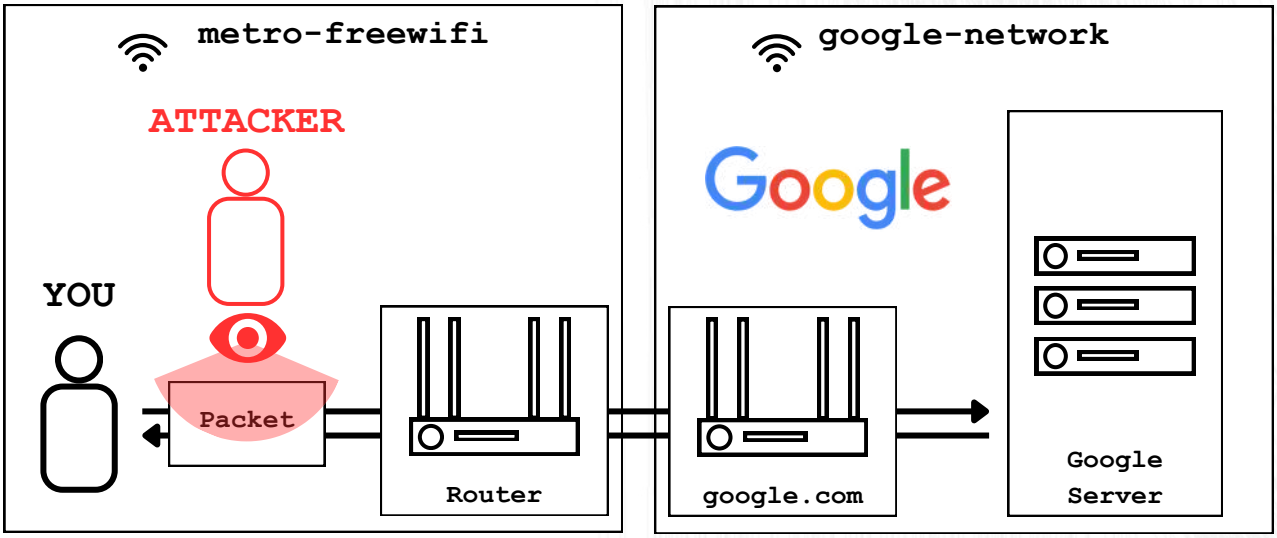
**Criminals**

Many black hat cyber criminals adopt these types of attacks, due to its cheapness, easiness, and high returns.

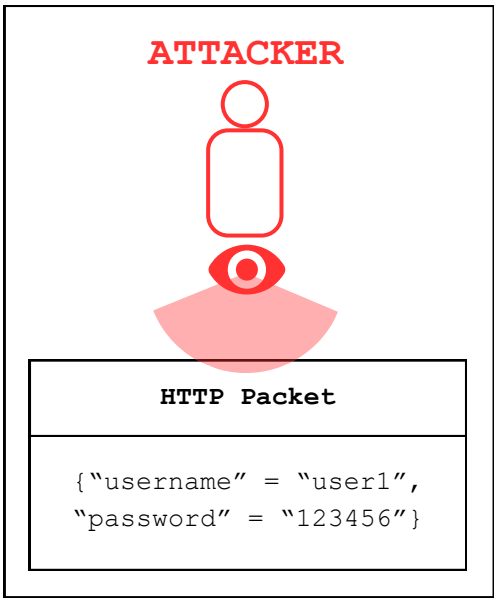
As explained in the **“HID Attacks / How do I prevent it?”** section, using USB condoms, or using chargers and cables from the original brand are the easiest ways of preventing these types of attacks. Additionally, cheap electronics are also a major hiding-place for the HIDa devices, indicating that cheap products has a high risk to yourself.

# MiTM Attacks / How does it work?

What is going on every time you open **google.com?**




When accessing any web server *(e.g, google.com)*, your device sends a packet to the server, and starts its communication. All packets sent/received from any server, is observable to every user that is in the same Wi-Fi network *(Lindemulder and Kosinski)*.




Every valuable information, such as your username and password that were sent to a server, could be stolen in the process. Today, the MiTM attack could be done with free and accessible software such as Wireshark, Ettercap, etc.

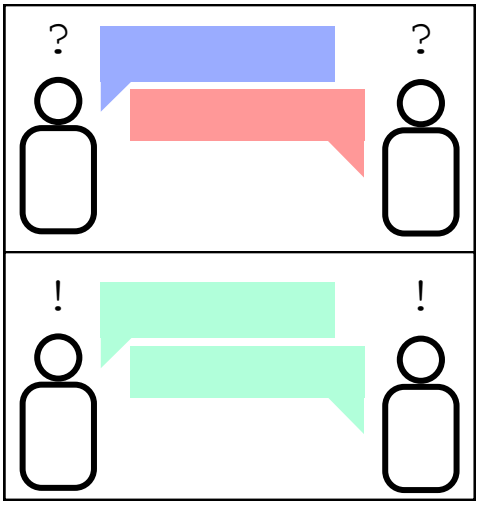
Observing packets in the same wifi network, is called a MiTM (Man in The Middle) attack, and is **19%** of the successful types of cyberattacks done in 2024 *(Blanton, Sean)*.

# MiTM Attacks / What is the difference of HTTP and HTTPs?

**http**://abcdef.gh
**https**://abcdef.gh

When net surfing, you probably recognized the "http" and "https" on the link. But really, what is the difference in the two?

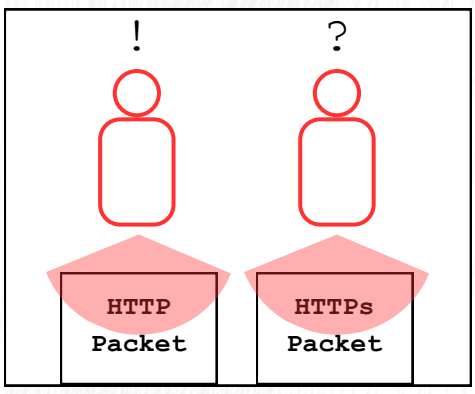
The http or https stands for "Hyper Text Transfer Protocol". Whenever you load a website, it renders based on a programming language called HTML, which stands for "Hyper Text Markup Language". And in order to receive the HTML of the website, you and the web server communicates with a packet.




However, every computer needs a mutal language to increase readability, and decreased errors. That is where "packet protocols" take in place. HTTP and HTTPs are one of the types of the packet protocols, to transfer hypertext across the internet *(Cloudflare)*.

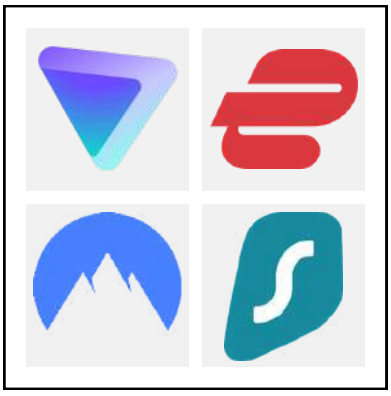
HTTP and HTTPs is distinguishable by if the packet encrypts itself, or not. The "s" in HTTPs stands for "secure". The encryption process includes many complex series of calculations to protect your privacy *(Cloudflare)*.

When using the HTTPs protocol to communicate on the web, it prevents people in the same Wi-Fi network from seeing the contents of the packet, protecting your privacy.

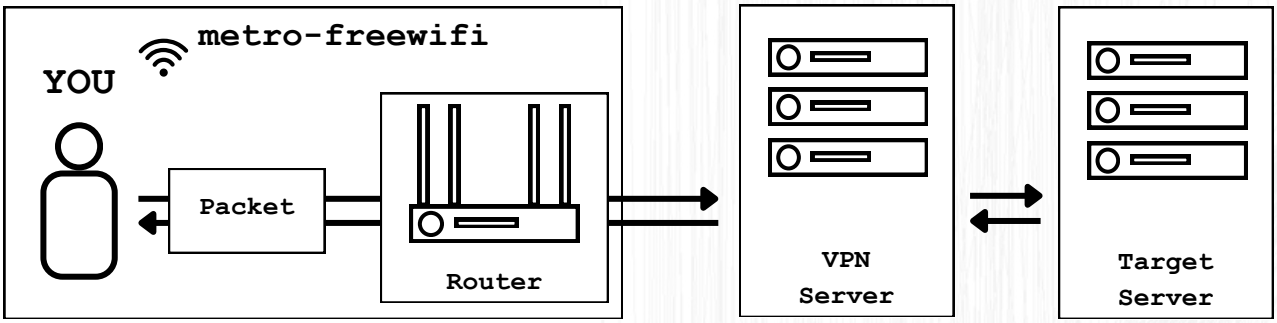


# MiTM Attacks / How do I avoid it? VPN is the answer!

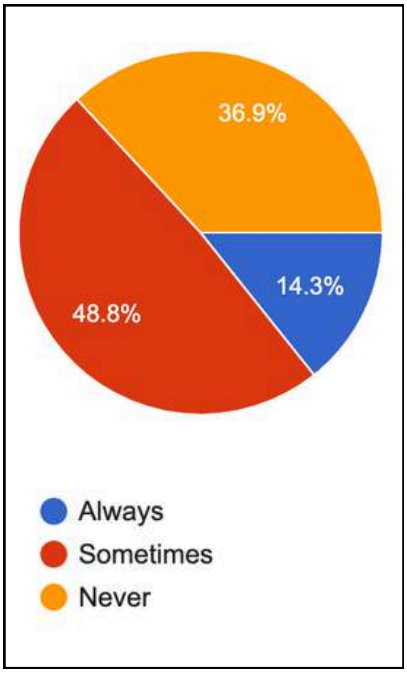
As explained earlier, encrypting packets prevents attackers and people from reading the contents of your sent or received packets. Using a VPN not just does not encrypt your packets, but additionally provide with other benefits such as avoiding region blocking, low data profile, safer internet browsing, etc. *(Vigderman and Turner)*



Proton, Surf shark, Nord, Express, and others offer free VPN services with data caps, slower speeds, and limited server locations to balance the need for a secure internet connection with advertising or premium features.




A VPN (Virtual Private Network) is a system which routes your packets through the VPN server, and sends it to the target server. This manipulates the target server into thinking that you are sending packets from the VPN server, establishing a safer internet connection. In result, the IP address that you truly use, would be hidden and be replaced with the VPN server's IP address *(Vigderman and Turner)*.




Research was conducted against 84 participants in YIS, were asked:

***"Do you use a VPN in a public / free Wi-Fi? (cafe wifi, train wifi, etc.)"***

**36.9%** answered that they never use VPNs, and **48.8%** answered that they sometimes use VPNs.
In result, **85.7%** are potentially vulnerable to the MiTM attack.

## MiTM Attacks / Connections with geopolitics in China

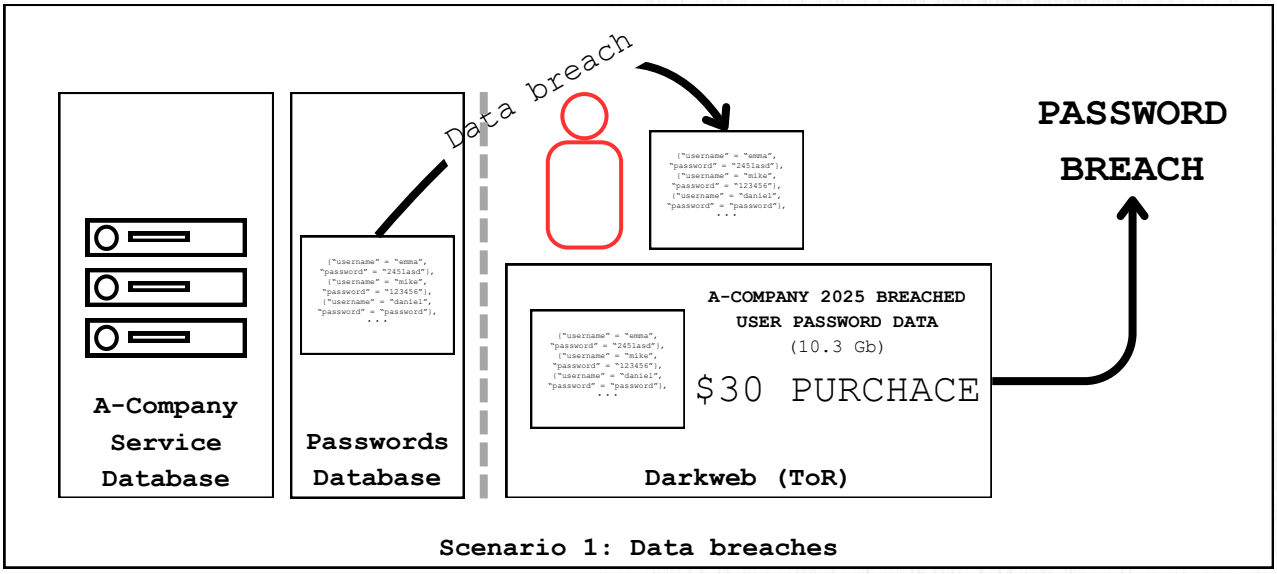
Chinese APT (Advanced Persistent Threat) group, LuoYu, has been operating a new type of attack, which is far different compared to the conventional MiTM, which is referred to as MotS (Man on the Side) attacks, using it against to Chinese indivisuals *(Blackberry)*.


**Luoyu Logo**

According to TeamT5, LuoYu has a solid goal, which is to target its attacks to Chinese dissidents, not just in Chinese mainland, but Chinese people in Europe, US, and in Russia *(Blackberry)*.

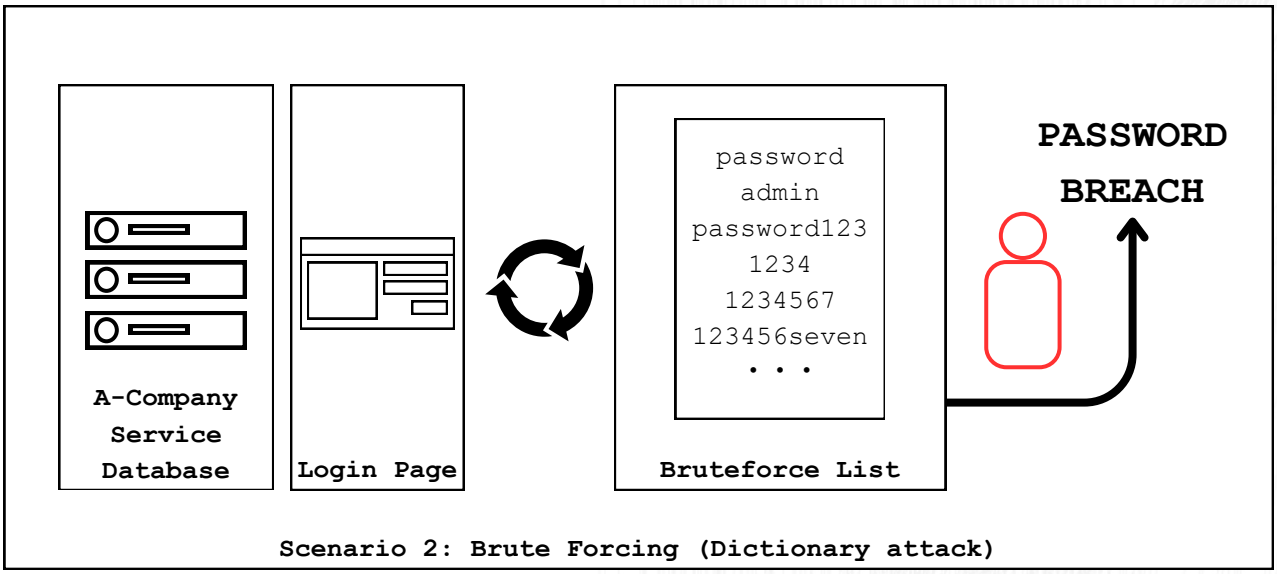
# **Passwords** / Are you really safe?

Hackers usually steal your passwords in two main ways: by exploiting data breaches or using brute force attacks like dictionary attacks.




**Scenario 1: Data breaches**

When a service experience a data breach, passwords and usernames breach to unauthorized people. Frequently, this compromised data is traded on the dark web, where malicious entities purchases, and abuses it for their own benefits.




**Scenario 2: Brute Forcing (Dictionary attack)**

On the other hand, dictionary attacks involve hackers guessing your password by trying out frequently used passwords. This method is a form of brute-forcing, where they systematically attempt to crack your password until they get it right.

## **Passwords** / How do I protect?

Installing reliable password managers, not using the same password across multiple platforms, making your password complex, checking if your password is breached frequently, turning two-factor authentication, are many of the valid methods to protect your password. Notably, checking if your password is leaked on the darkweb, is one of the most effective ways to counter the **"Scenario 1 - Data breaches"**. You can check using free open services, such as "haveibeenpwned.com"

**Check if your password is breached:**
*https://haveibeenpwned.com*

**555 million** password breaches which were public on the darkweb had been recorded since 2017, and the numbers would keep growing on and on (Chang). Many are caused by either setting an easy password just like "12345", "password", and data breaches.

# Citations / Works cited

**Works Cited**


Blackberry. "中国系 APT が自動アップデート機能を悪用して WinDealer マルウェアを配信しています。その手口を詳細解説" ["A Chinese APT is exploiting the automatic update feature to distribute WinDealer malware. Detailed explanation of its modus operandi"]. Blackberry, 5 Aug. 2022, blogs.blackberry.com/ja/jp/2022/08/threat-thursday-china-based-apt-plays-auto-updater-card-to-deliver-windealer-malware. Accessed 24 Jan. 2025.

Blanton, Sean. "90+ 2024 Cybersecurity Statistics and Trends." Jumpcloud, 31 Oct. 2024, jumpcloud.com/blog/cyber-attack-statistics-trends. Accessed 22 Jan. 2025.

Borys, Christian. "The Day a Mysterious Cyber-attack Crippled Ukraine." BBC, 4 July 2017, www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine. Accessed 24 Jan. 2025.

Chang, Jenny. "55 Important Password Statistics You Should Know: 2024 Breaches & Reuse Data." Finances Online, 6 Jan. 2025, financesonline.com/password-statistics/. Accessed 24 Jan. 2025.

Cloudflare. "What is HTTP?" Cloudflare, www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/. Accessed 24 Jan. 2025.

---. "What is TLS (Transport Layer Security)?" Cloudflare, www.cloudflare.com/learning/ssl/transport-layer-security-tls/. Accessed 24 Jan. 2025.

Cyber Security Awareness. "How Safe is Free/public WiFi?" Cyber Security Awareness, 29 May 2024, cybersecurityawareness.co.uk/resources/blog/how-safe-is-free-wifi/. Accessed 23 Jan. 2025.

Gallagher, Sean. "Playing NSA, hardware hackers build USB cable that can attack." ARS Technica, 21 Jan. 2015, arstechnica.com/information-technology/2015/01/playing-nsa-hardware-hackers-build-usb-cable-that-can-attack/. Accessed 23 Jan. 2025.

Gregory, Jennifer. "Juice jacking: Is it a real issue or media hype?" Security Intelligence, 25 Aug. 2023, securityintelligence.com/articles/juice-jacking-is-it-real-or-media-hype/. Accessed 24 Jan. 2025.

Hudson, Skye. "USB Condoms Protect Your Data While You Charge." Make Use Of, 13 Sept. 2013, www.makeuseof.com/tag/usb-condoms-protect-your-data-while-you-charge/. Accessed 24 Jan. 2025.

Lakshmanan, Ravie. "Crypto Scam App Disguised as WalletConnect Steals $70K in Five-Month Campaign." The Hacker News, edited by Mohit Kumar et al., Y Combinator, 28 Sept. 2024, thehackernews.com/2024/09/crypto-scam-app-disguised-as.html. Accessed 28 Sept. 2024.

Lenovo. "What is a Human Interface Device." Lenovo, www.lenovo.com/us/en/glossary/hid/. Accessed 23 Jan. 2025.

Lindemulder, Gregg, and Matthew Kosinski. "What is a man-in-the-middle (MITM) attack?" IBM, 11 June 2024, www.ibm.com/think/topics/man-in-the-middle. Accessed 23 Jan. 2025.

McLean, Mike. "Cyberattack statistics 2024." Embroker, 10 Oct. 2024, www.embroker.com/blog/cyber-attack-statistics/. Accessed 23 Jan. 2025.

Pillai, Vysakh P. "USB-2.0." Embeddedinn, 23 Jan. 2013, embeddedinn.com/articles/tutorial/usb-2-0/. Accessed 23 Jan. 2025.

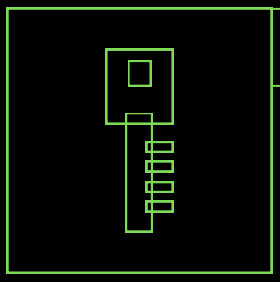
Sweeney, Aaron. "Have you used a USB port to charge your phone in public? You could be at risk of 'Juice Jacking.'" NTI Now, 27 Sept. 2023, ntinow.edu/juice-jacking-cybersecurity/. Accessed 23 Jan. 2025.

Vigderman, Aliza, and Gabe Turner. "Is a VPN Encrypted?" Security, 25 June 2024, www.security.org/vpn/encryption/. Accessed 23 Jan. 2025.

"Why Hacking is the Future of War." YouTube, uploaded by Johnny Harris, 14 Feb. 2024, www.youtube.com/watch?v=15MaSayc28c. Accessed 25 Sept. 2024.

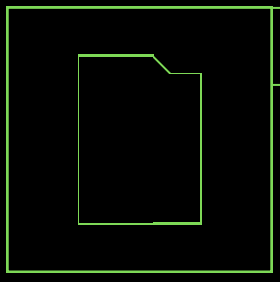
# Cybersecurity 2025

Thank you for reading! This magazine was created under the philosophy of educating many people to counter against the cyberattacks, evolving in proportion of the new modern digital society. I hope that many of the readers were either interested, or educated and benefit in any way through this magazine.



## Passwords Brute forces (dictionary attack)

Daily electronics such as keyboards, mouse, macros, are categorized as a HID. However, a harmless looking USB drive, could manipulate the connected device into thinking that it is a HID, taking over your controls on your device.



## Malware Malicous software

Malware would take over your device, and operate various malicious commands. Some may encrypt all of your files, and lock your computer, demanding a ransom, some may steal many of your personal information and abuse it.

## Cyberwarfare APT (Advanced persistent threats)

The most frightening thing about cyber warfare is that it does not involve the loss of friendly personnel, and attacks can be cheap, anonymous, quiet, and, be that as it may, powerful.

Contact if there are any further questions or possible misinformation.


**NAME:** Kunihito Takada
**MAIL:** 27takadak@yis.ac.jp
**PHONE:** (+81) 080-7897-7419
**GPG KEY:** F9872A0174EF923F52F0FB15AC8EC60AF0BF8032


//open terminal on your device, and type in
`curl parrot.live`
//press **Enter (Return)**, and press **control+c** to quit.

This magazine is also available online!

https://github.com/Kunihito-Takada/cybersecurity-2025/blob/main/magazine.pdf