Many faces of cybercrime, by Michał Najborowski, 15.11.21

People argue that in their everyday computer use they don't really need any antivirus or malware protection. As shown in the recent statistics, nearly 50% of Americans don't use antivirus software. One of the most popular tip to stay safe online is reasonable browsing. That indeed could be true… 15 years ago, when there weren't so many online applications gathering personal data and explicit downloads of unknown data was likely the only reason of getting infected. But nowadays over 350 000 new pieces of malware are detected every day and by far at least 20 different types of cybercrime were categorized, so there is a chance one could become a victim without even noticing! Taking above under consideration, currently there is a disturbingly high number of types of cybercrime techniques, each equally dangerous, if performed by an experienced cybercriminal, and that number is vastly growing. Law forces and governments should invest more resources into online safety PR campaigns to raise awareness about how many threats are lurking in the World Wide Web.

To begin with, what is cybercrime in the first place? It is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. So it means that if the computer contains some valuable data like personal information or medical record, the computer itself would probably be the target of the attacker. But in most cases the computer stands as a gateway to the real target, as cybercriminals tend to take control over some random machine and perform the hack from there, covering their tracks in case law forces find out source of the attack.

The number of cybercrime types may not seem significant, but it's enough for a hacker to pick one that catches off guard an average internet user, not to mention there are subcategories for each of the main type. A blessing in disguise, modern operating systems come with the built-in antivirus software that is fairly capable of detecting most popular malware. That's where social engineering attacks take their lead. For instance - phishing attacks. This type of cybercrime focuses on pretending to be trusted organization and luring victim into opening malicious link. One of the most popular technique of distraction is to send emails almost indistinguishable from the official ones, containing elements like logo, font or footnotes, all used by the proper institution. The content often says that the account password has been recently changed and if that action was not performed by the account owner, the password should be immediately changed again through the link given in the email. The link then redirects to a website once more containing the same original design and the very much alike URL, different only by one letter that's hard to spot. The person is then asked to put the old and the new password, actually giving their current login details to the attacker. That's why it is crucial to use additional protection like two-factor authentication, especially the type that bases on randomly generated codes every 20 seconds.

However not all of the cybercrime-like types are officially illegal. One of them is known as PUPs - Potentially Unwanted Programs. They're often installed along with the software that the person actually intended to install, which is most likely due to the fact that the software is free of charge. During installation there are additional steps encouraging user to try other programs offered by some unknown, third-party organizations. Usually the only way to prevent installing this kind of software is to uncheck a very small checkbox or click on a grayed out button, very unlikely to be the first choice compared to a colorful and visible „next" button. The result can be as slightly

frustrating as swapping the default browser or search engine with other, less effective one; or ending up with some unwanted software that can stay unnoticed, gathering personal data that can leak later, due to most likely low security standards popular among small, meaningless companies. What's worse such companies tend to sell such data, which of course is the moment when the whole thing becomes actually illegal.

Not only hackers take crucial part in stealing personal information or other sensitive data, but users, who share nearly all of their details across all the internat. All thanks to social media. Apps like Facebook or Instragram actually gather much more information about the user than it looks like. For example under disguise of asking for a privilege to access phone contacts to find out which one them already has an account, the social media app gains access to SMS messages. It's because of the character of the phone native contact app, which typically features phone calls, contact book, recent calls and SMS chats, all in that single app. Furthermore users often send private photos between each other, which even after deletion stay on the server forever. Social media never forgets. With just a little privilege, social media apps can even constantly gather user's location or name of other apps installed on the phone and exact time of their usage. Combine it with the phishing attack described before and it ends up with a material perfect for all sorts of cyberstalking and cyberbullying.

This is just a small deep-dive into what can be achieved with only a few of existing types of cybercrime. Imagine what could be done with a single computer using all of the techniques gathered together. There is a lot of cybercrime types and knowing that the number is rising, the internet won't become a safer place by itself. Let's keep the personal data outside of the social media as much as possible, double check sources of all messages and use additional protection to keep the virtual environment safe.

Bibliography:

- Types of Cybercrime - https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/
- Antivirus and Cybersecurity Statistics, Trends & Facts 2021 - https://www.safetydetectives.com/blog/antivirus-statistics/
- Cyberattacks and Seniors – How to Protect Vulnerable Users Online - https://home.sophos.com/en-us/security-news/2020/senior-citizen-cyber-attack
- Nearly 50% of Americans don't use antivirus software and other startling facts - https://community.spiceworks.com/topic/2140300-nearly-50-of-americans-don-t-use-antivirus-software-and-other-startling-facts
- 2021 Cyber Security Statistics - The Ultimate List Of Stats, Data & Trends - https://purplesec.us/resources/cyber-security-statistics/
- Top 12 Cybercrime Facts and Statistics - https://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/
- Co wie o mnie Facebook? - https://noizz.pl/big-stories/dzien-bezpiecznego-internetu-co-wie-o-tobie-facebook-sciagnij-dane-i-sprawdz/rgh8kw4