EXTORTION TECHNIQUES ARE ON RISE AGAIN

The effected information resource

- This has been increasing and has been causing more and more problems in the modern age where people make money via social media. Many companies has reported about this and listed such ways of ¨e-theft¨.

- Purchasing credentials and session tokens from criminal underground forums
- Paying employees at targeted organizations (or suppliers/business partners) for access to credentials and MFA approval
- People accepting link that was sent via message and thinking the website they are going is something legit.
- Simply hack their way into anothers account and demand randsom for it.

The modus operandi

- It was reported that the ¨Extortion people¨ generally work in teams, because they will need larger amount of people usually to pull these off. There are two general ways of doing this:

1. Attack first, ask randsom secound.
2. Or extortion first and believe that the attack is coming.

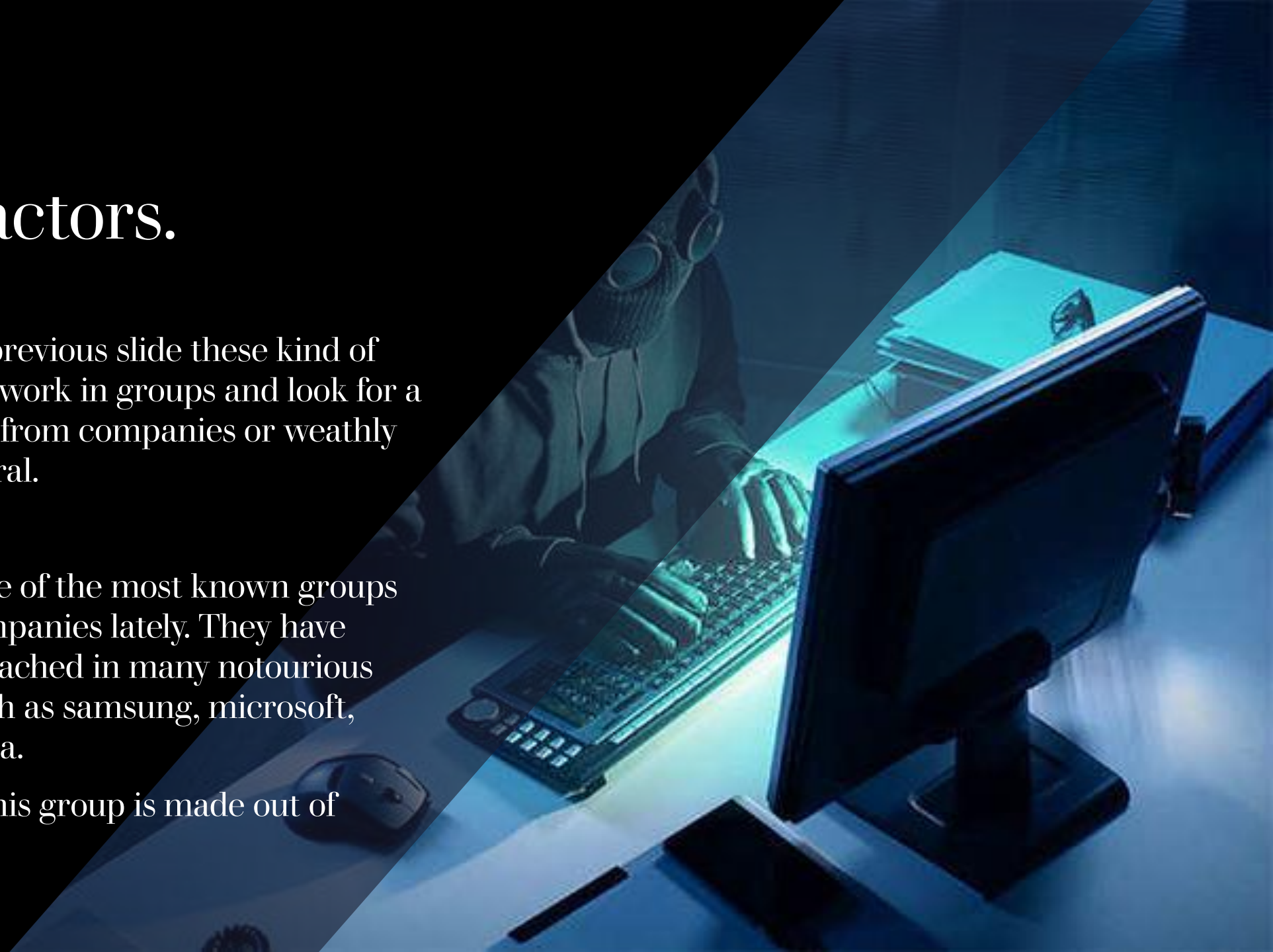
In either way it is scary for the company or for the private people because there is no way of knowing that in which part of the system/platform are they attacking.

This can also be done with ¨phishing¨ messages or emails. They are quite effective.

Threat actors.

- As said in the previous slide these kind of people usually work in groups and look for a large randsom from companies or weathly people in general.

- LAPSUS$ is one of the most known groups that target companies lately. They have succesfully breached in many notourious companies such as samsung, microsoft, unisoft and okta.
- It is said that this group is made out of teenagers.



Protection measures

Investing in your identity theft protection. This can save yoy personally hundreds of euros if it helps you detect messages or email you are receiving. One wrong click could be it.

Keep you information confidental. This means don´t give it out to websites you are not sure about and ask from the company if the message you received is possably from someone else.

Be quick to be in contact with the police. They have their own professionals who handle these sorts of things and can help you if someone is asking for randsoms.

Share you experiences. People make mistakes but stupid people don´t learn from them.

Sources:

- file:///C:/Users/santt/Downloads/ENISA%20Threat%20Landscape%202022.pdf
- https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
- https://techxmedia.com/lapsus-a-teen-extortion-group-exposes-cyber-gaps-in-mature-organizations/