Alessandra Trenchi

17 February 2023

LINKEDIN DEEPFAKES:

MOTIVATIONS + FORECASTS

A SCHOLARLY APPROACH

How to fight APT

AGENDA

Deepfakes?

Motivations

Possible solutions

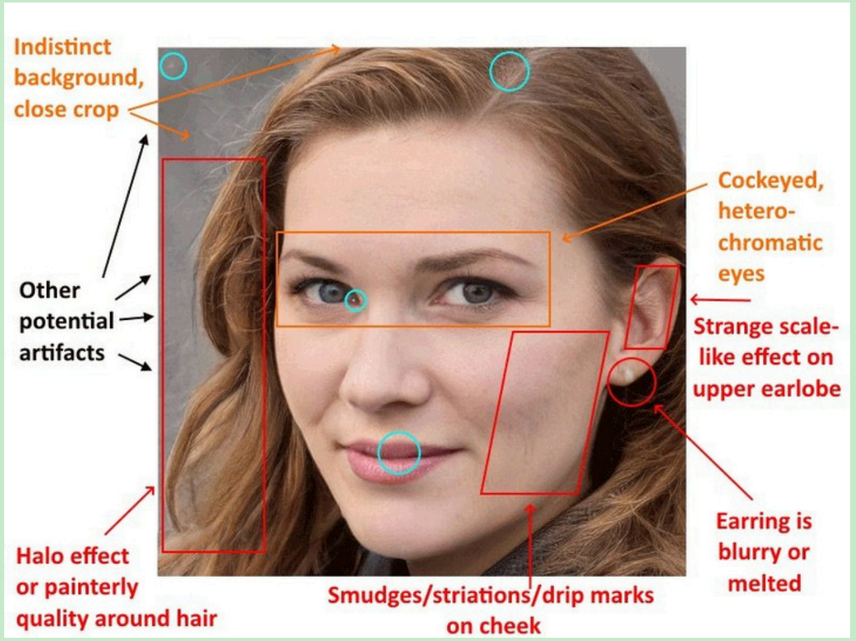
Linkedin reacts

Plan a Cyberdefense

Follow the directives!

DEEPFAKES?

- Synthetic computer-generated data: Ai-generated images + stolen text.
- **Who**? Gulf of profiles on high CEO roles (for trends and global events).
- **Target**? Us and Western government, high level companies and employees.
- Problem: Indistinguishable human faces.
- Problem: Linkedin declared they did not violate community guidelines.



Continuously improving through **GANs** technology

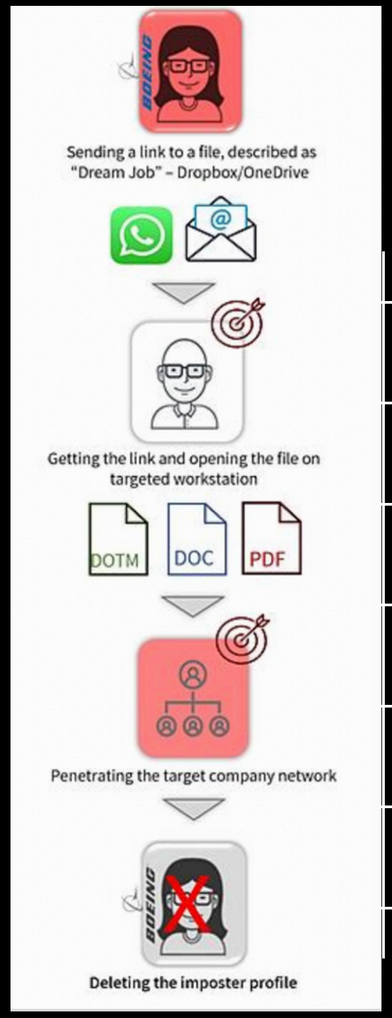
DEFINING THE ATTACK

- **Social engineering attack**-> tricking the attacker to reveal sensitive information or compromising the system.
- **Cyber geopolitical espionage** + **disruption**-> blockchain, cryptos: transaction surveillance, *theft* (private keys, identities), market and data *manipulation*.
- **DDoS** to *disrupt* the Blockchain network.
- Deepfakes as tools for **APT**.

ATTACK MOTIVATIONS:

- Botnets as a **scheme** to land jobs at cryptocurrency firms.
- Raise funds for North Korean leader.
- **Information warfare** and data mining to collate information about future cryptocurrency trends.
- **Launder cryptocurrencies** to evade Western sanctions.
- **Disinformation** and propaganda campaigns to spread *fake news*.

ATTACKERS



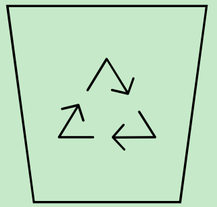
- North-coreans crypto-investors
- Identity thieves
- **LAZARUS Group** (potential nation-state actor)

POSSIBLE SOLUTIONS

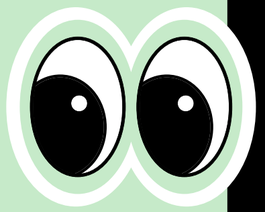
- Companies' spreadsheet **list** of employees-> Problem: often employees change and it would be a great amount of work for the companies.
- AI experts are pressing for regulation-> deepfakes **traceability** system, ML **trained models** to fight deepfakes.
- Blockchain verifications.
- E-mail verification -> Problem: e-mails do not confirm your identity.
- Providing an **ID** picture when registering the platform and giving verified users a verification mark.

PLAN A CYBERDEFENSE FOR APT

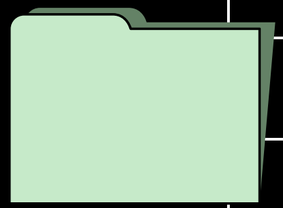
- **Goal:** identify and remediate any security weaknesses that could be exploited by an attacker -> ongoing process.
- Perform a **log analysisgfdgsdfg**.
- Develop a continuous threat modelling plan.
- Goal: fight deepfakes in a **scalable** way.
- Multifaceted approach based on collaboration.



LINKEDIN REACTS



Optimizations:



- *About this profile*: join date shown on profile.
- Added warnings on potentially risking messages.
- Microsoft **OAUTH 2.0** protecting users' sensible data.

LINKEDIN REPORTS

Trend of Linkedin Cyberdefense against deepfakes

FORECAST

The trend of cross-chain transfers is forecasted to grow to 10B$ by 2025.

This APT will evolve and adapt to Linkedin countermeasures.

DEEPFAKES RECOGNITION

The FBI warns on deepfakes stealing PII. Users must collaborate with authorities not to fall into **pig butchering**!

Good Practices:

- Check if there are any communication discrepancies.
- If the profile has a low number of connections.
- Do not open e-mails from unknown Linkedin users.
- Use Chrome Google Lens to crawl the web for the image source and check if the bios are AI generated texts.
- Do not give credit card numbers, share phone number or download documents from untrusted accounts!
- Always report accounts which seem fake.

FOLLOW THE DIRECTIVES!

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Treasury Department (Treasury) developed a **CSA** to highlight the cyber threat associated with cryptocurrency thefts and tactics->
Actions to take today to mitigate cyber threats to cryptocurrency.

- **Patch** all systems (in particular known exploited vulnerabilities).
- **Train** users to recognize and report fishing attempts.
- Use **multi-factor authentication**.

Users must collaborate and file reports to **IC3** when victims of cybercrime. Check the official website to get educated about the latest and most harmful cyber threats and scams.

SITOGRAPHY

https://www.sciencealert.com/people-who-dont-exist-look-more-real-than-actual-people-study-finds

https://krebsonsecurity.com/2022/10/glut-of-fake-linkedin-profiles-pits-hr-against-the-bots/

https://www.cnbc.com/2022/12/10/not-just-twitter-linkedin-has-fake-account-problem-its-trying-to-fix.html

https://resumeworded.com/linkedin-review/linkedin-summary-generator?generator=start&category=random

https://www.bitmat.it/blog/sicurezza/deepfake-come-riconoscerli-e-proteggersi/

https://www.bitmat.it/blog/internet/social-network/tra-fake-news-e-deepfake-il-2023-sara-lanno-del-grande-inganno/

https://www.bleepingcomputer.com/news/security/fbi-stolen-pii-and-deepfakes-used-to-apply-for-remote-tech-jobs/

https://techcrunch.com/

https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

https://www.cisa.gov/uscert/ncas/alerts/aa22-108a

https://www.ic3.gov/

https://www.linkedin.com/business/marketing/blog/agency/deep-fakes-and-digital-influencers-the-future-of-brand-marketing

https://screenrant.com/deep-fake-linkedin-profiles-sales-marketing-spot-how/

https://www.pnas.org/doi/10.1073/pnas.2120481119

https://krebsonsecurity.com/2022/09/fake-ciso-profiles-on-linkedin-target-fortune-500s/

https://www.bbc.com/news/world-asia-64494094

https://about.linkedin.com/transparency/community-report

https://www.thetimes.co.uk/article/latest-linkedin-contact-ai-generated-deepfake-social-media-h8wbghkvn