Violent Attack Vectors in Web3: A Detailed Review

#Abstract

Operational security professionals work to figure out where their information can be breached. Looking at operations from a malicious third-party's perspective allows us to spot vulnerabilities we may have otherwise missed so that we can implement proper countermeasures.

The most important thing to understand here is the path of the cyber attack – its vector. Let's take a closer look.

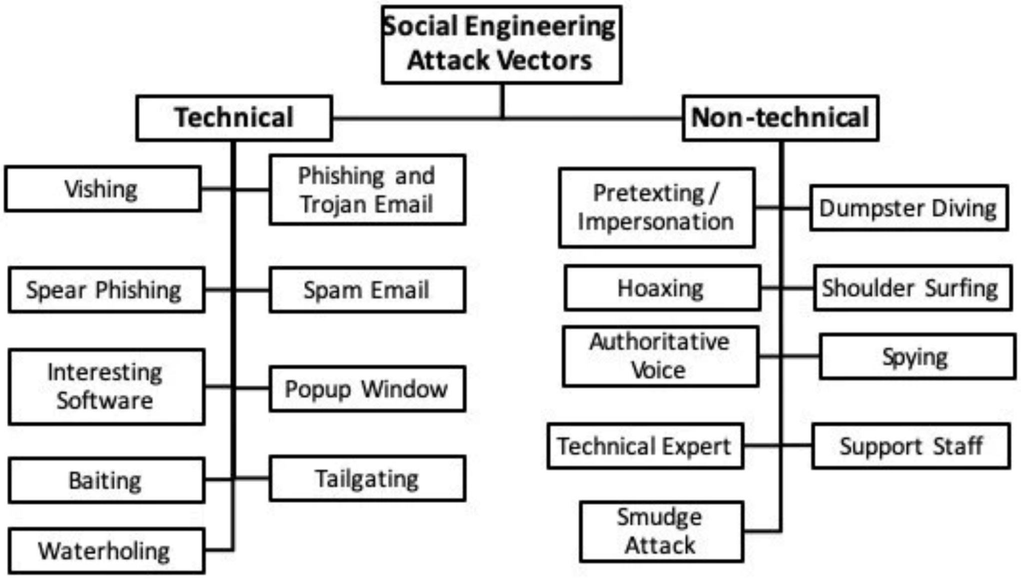
#Example No. 1 - RAT & Social Engineering

Let's take a hypothetical situation in which your computer gets infected with a Remote Access Trojan (RAT) virus. One of two things may happen. If the attack was carried out by a rookie hacker (i.e a lamer) then he likely orchestrated a wide massive attack without a target in mind. He can steal some information on you like your browser cookies and then sell it.

- **Social Engineering. Example (1).**

The second option is that this was a direct attack. The hackers made a phishing page on your router, through which you could enter your password (poisoning the DNS server). To prevent this type of attack, you ideally need to separate your machines and networks. You should also check certificates.

Here is an example of a very dangerous cyber attack on your crypto wallet:



- **Your computer gets infected by malware with a crypto clipper.**
- **Let us say you want to send money from your crypto account to your friend.**
- **When you attempt to copy and paste your friend's crypto, ETH, or BTC address, the clipper will substitute your friend's address with a generated one that looks a lot like your friend's (starts and ends with the same characters).**
- **Thus, instead of sending crypto to your friend's account you actually direct the money directly into the hacker's account.**

Consider checking the entire address of your addressee's wallet before you click Send.

- **Read carefully: graph.org/Social-Engineering-Your-Way-Into-The-Network-09-13**

Sophisticated crypto criminals will throw at you a mix of attack vectors. It could be a Social Engineering vector, plus phishing and classic malware. They might even attempt a physical attack!

#Example No. 2 - The Troll and the Knight

Let us take Jane who is a diligent employee at her company. Information about Jane is publicly available on her social networks. Some sensitive information about her might have even been revealed in some leaks, such as the 2014 Yahoo Mail user account information breach. Generally, she is no different from you or us. So far, so good.

- **github.com/frostbits-security/MITM-cheatsheet**

But then, a troll shows up and starts stalking her around social networks, writing hurtful comments, for example. He expands his cyberbullying to others in Jane's company, bringing distress to his victims.

Even at this stage, the attack has done enough damage to cripple the culture of openness inside the company. Employees may stop sharing personal information or speaking candidly about problems for fear of ridicule or retaliation.

Jane continues to suffer the troll's attacks in silence. If Jane blocks the troll's account, he will make another. If he knows her address, multiple pizza deliveries may suddenly arrive at her door. It is no life.

At this point in our story, in comes John. He is a stranger but, he too has a public account and has suffered from the actions of this same troll as evident from attacks on his page. He makes Jane a proposition for cooperation on how to stop the attacks. He says he knows a way to silence the troll.

Sure he knows the way. The Knight to the Rescue and the Evil Troll are one and the same person. The troll's trick was to establish an emotionally supportive bond with someone who was experiencing pain.

John created a condition where Jane is now more likely to follow John's seemingly innocent suggestion. She may click on a URL link or open a file sent to her. She might even come out and meet John.

This story may end badly for Jane. A potential scam by John should have been stopped at the beginning – at the stage when the target got recruited.

Are there any good guidelines to follow so that we do not end up in Jane's position?

1. **The piece of advice "don't let strong emotions influence your actions" applies well for investing in stocks or when choosing a life partner. It can be your first rule in the digital world playground.**
2. **If you get scammed, do not lose heart. One thing victims often tell us after being defrauded is "I can't believe I was so stupid." Scams happen to the best among us. Evolutionary psychology tells us that we have been wired by evolution to trust**

other humans for the purpose of our survival. This is why any exploitation of this strong evolutionary adaptation is particularly painful to us.

3. If you are in a managerial role, make sure your employees aren't sick, tired, or go hungry at work. When employees are physically or emotionally weakened, they become vulnerable to psychological influence.
4. If you work a lot with files, particularly PDFs, you can use these protective measures.
5. While you may be wary of third parties trying to steal your information, you should also watch out for insider threats, such as negligent employees and disgruntled workers.
6. We recommend that you follow these 25 rules to safeguard yourself from nefarious Internet scammers.

The exploitation of love or anger happens less often because the scammer would need to maintain a psychological connection with the victim, requiring skill, time, and familiarity with the target. In our situation, the scammer exploited the victims' fear. What is more, in order for this attack to succeed the victim had to be rushed.

A skillful social engineer will not give the victim much time to think, and will always press for urgency. This is the first thing to pay attention to – If you are rushed to give out sensitive information (or any information at all, for that matter), it is a good time to pause.

The second point to note is that when you find yourself in a similar situation, do not try to solve the problem by yourself. Ask a friend, a frequent contributor to your favorite Discord server, or a moderator of any well-known DAO. Good people want to help. Get a second opinion.

Sometimes scammers just want to get dirt on the victim or de-anonymize the target. Often, however, sophisticated cyber exploits can come coupled with either a malware injection or a phishing attack, or some other surprise.

#Example No. 3 - An IoT hack "on steroids"

It is no secret that hackers can find out which keys you press. To do this, a hacker needs to install a key-logger (See 1 & 2) on the victim's computer. However, it is already possible to simply find out what a person is typing just by the sound from the microphone or, let's say, an IoT device speaker.

But how does it work exactly? Let's get to the bottom of it!

Each key on the keyboard has a unique sound. The distance between the keys, the microphone, and the rate at which they are pressed are different for each symbol. In short, a spectrogram analysis is able to distinguish the keys from each other and determine which buttons correspond to a particular sound.

The algorithm would analyze the parameters of each sound if a hacker gained access to a microphone or speakers. To protect against audio key-loggers, try using Unclack on MacOS and Hushboard for Linux. They will mute the microphone when you are typing.

- keytap.ggerganov.com
- keytap2.ggerganov.com
- keytap3.ggerganov.com

The described attack can be used in a combination with the IoT hack in which hackers may use speakers, and therefore a microphone, in order to recognize your seed phrase and steal your crypto assets. This is not a Joke!

- If you are an IoT device owner, then carefully read!

Banks have long been concerned with creating a system of acoustic protection not only in meeting rooms and office management but also in the security departments. Banks can use deep underground laboratories and huge Faraday cages for this purpose.

In essence, a cold wallet is just a pseudo-AirGap system (100% AirGap is impossible to achieve on Earth by definition) and it can be cracked.

#Example No. 4 - IOS +MacOS Attack Vectors

In my favorite chat room recently I was asked, in light of recent events, would it be safer to use MacOS & IOS for work? Is it true that they have better security? I don't have a definite answer here - both yes and no.

First of all, There is a lot of malware for macOS/IOS, the thing is that exploits 0days/1 day for MacOS/IOS costs slightly more than Windows/Android.

There is no difference, just a difference in the price of preparation and in the price of different exploits (including file gluing exploits or delivery exploits - they always cost more), I suggest you go to Zerodium and see the prices.

In general, the toolkit is more or less the same so don't assume that macOS is more secure. Again, it is based on FreeBSD. In other words, know who is working against you and what they are capable of.

In other words, the chances of getting into a massive attack are less, but the chances of being hacked by someone who is not sorry to spend 5-10 thousand dollars to prepare for your hack are equal on all devices and almost all operating systems.

Hackers also care about economics, profit, and cost. If they are confident they can take the risk. Keep that in mind.

- **Carefully read: officercia.mirror.xyz/0uiAGM50rkQSvHbptcrVkCkyxsnewpAFIdu3oyga42Y**

Use Qubes OS, Whonix, Tails, or Graphene OS (which is way better than closed and thus unable to estimate risks IOS. Jailbreaking a device makes everything even worse) but some of them require a lot of preparation work and do not have out of the box security! But. Any secure OS can't help you if you don't care about simple security rules - keep that in mind.

#Conclusion

I am not asking you to comply with all of this, but you must remember the main rule in this particular case:

- **Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.**

If we finally want to give people the opportunity to be their own bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money.

Yes, it seems like it is a veritable minefield over there. Keep the faith. Learn the latest attack techniques, white hat cheat sheets, and defenses. Only knowledge can defeat criminals*'* knowledge. In this intellectual boxing match the most prepared wins, and we want that to be you!

Also published here.

- ***Authors: Officer_CIA, Nazar Taras***

Support is very important to me, with it I can spend less time at work and do what I love - educating DeFi & Crypto users!

- **Check out my GitHub**
- **Track all my activities**

- **All my Socials**
- **Join my TG channel**

If you want to support my work, you can send me a donation to the address:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

#Thank you! ❤️