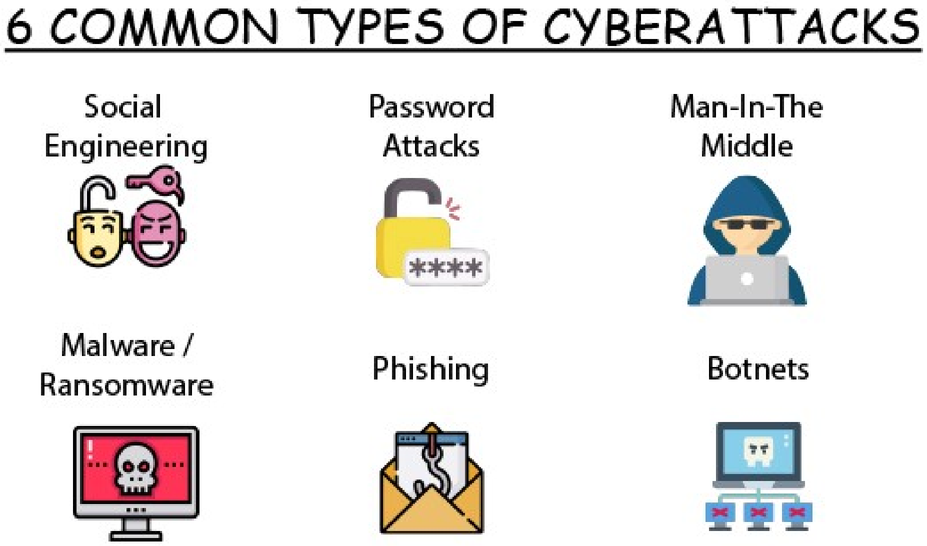
medium.com /@daviesombasa/types-of-cyber-attacks-ee040492fb48

TYPES OF CYBER ATTACKS

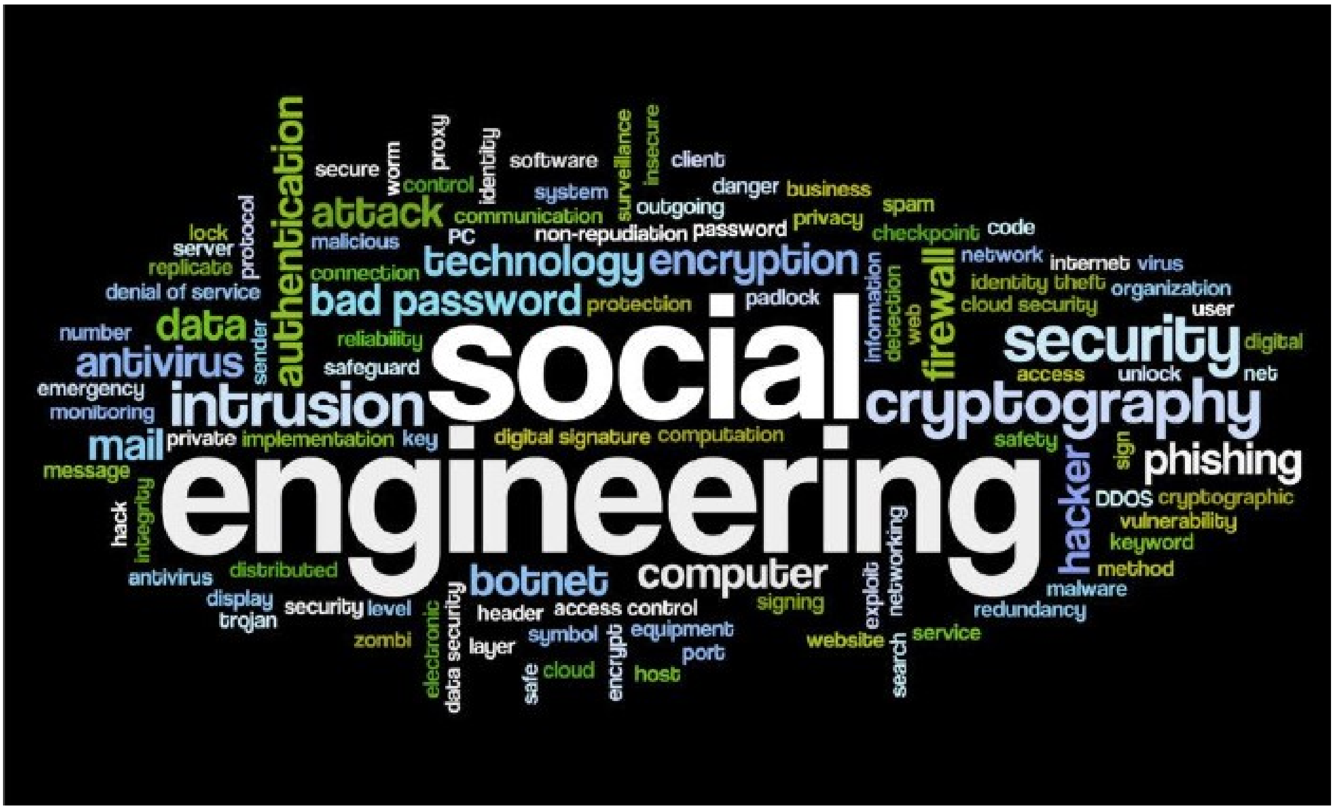
daviesombasa :: 14-3-2022

WHAT SHOULD YOU WATCH OUT FOR?

Data breaches can have a significant impact on a business or organization. It is important to be aware of what mechanisms adversaries can use to compromise you. Here are some of the top cyber attacks you should watch out for.



1. Social Engineering — obtaining information while impersonating someone else or an organizations. This is probably the easiest attack to execute since it relies on human behavior and tinkering with the human psychology.



It is categorized into three broad groups:

- **Using computers** — computers are used for execution

◇ Phishing — sending emails with malicious links aimed at either delivering malware or deceiving the target to reveal their private information.

◇ Pop-up attacks — pop up windows that appear while you are using the internet to try and trick you into giving away your personal information.

- **Using mobile devices** — mobile applications are used to carry out these attacks.

◇ Smishing — phishing carried out using SMS platform.

◇ Malicious applications — these may contain fake services or products keen on luring you to provide your personal information.

- **Using humans** — takes advantage of human interactions to obtain information.

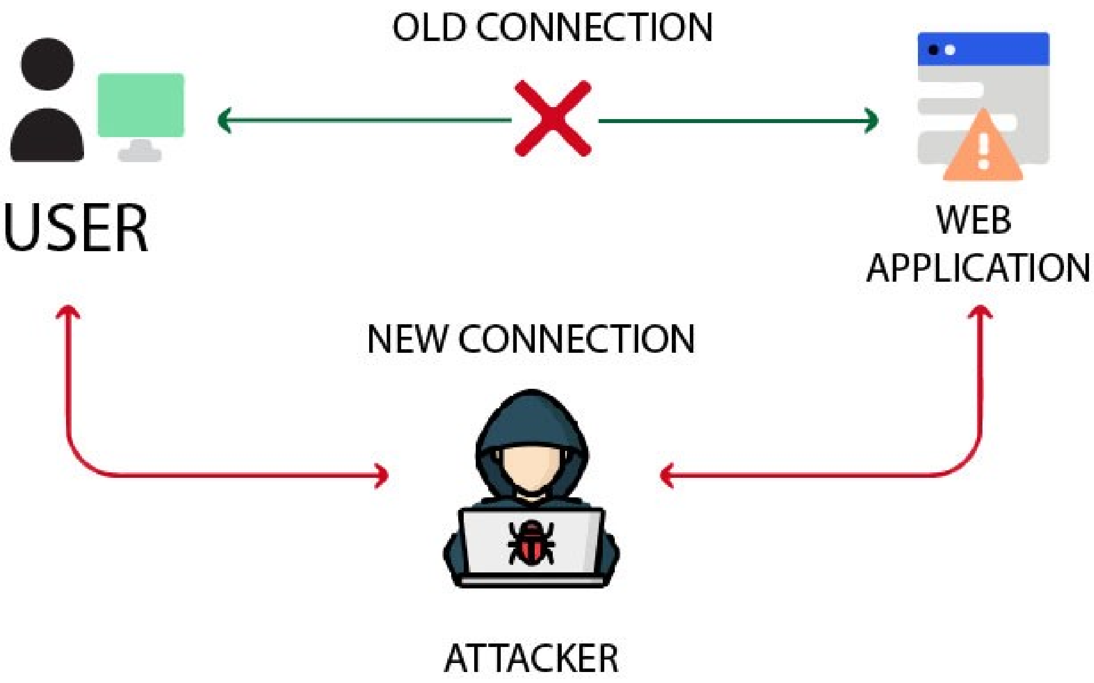
◇ Vishing — using voice to carry out phishing.

◇ Tailgating — following someone through a restricted area and using their access to get in.

◇ Shoulder surfing — looking over someone as they key in their sensitive information such as passwords.

◇ Dumpster diving — perusing through dustbins, dumpsites near your target for information that may have been left there such receipts, invoices etc.

2. Man-in-the-middle Attack — this attack occurs when someone intercepts communication between the client and server or two people communicating.



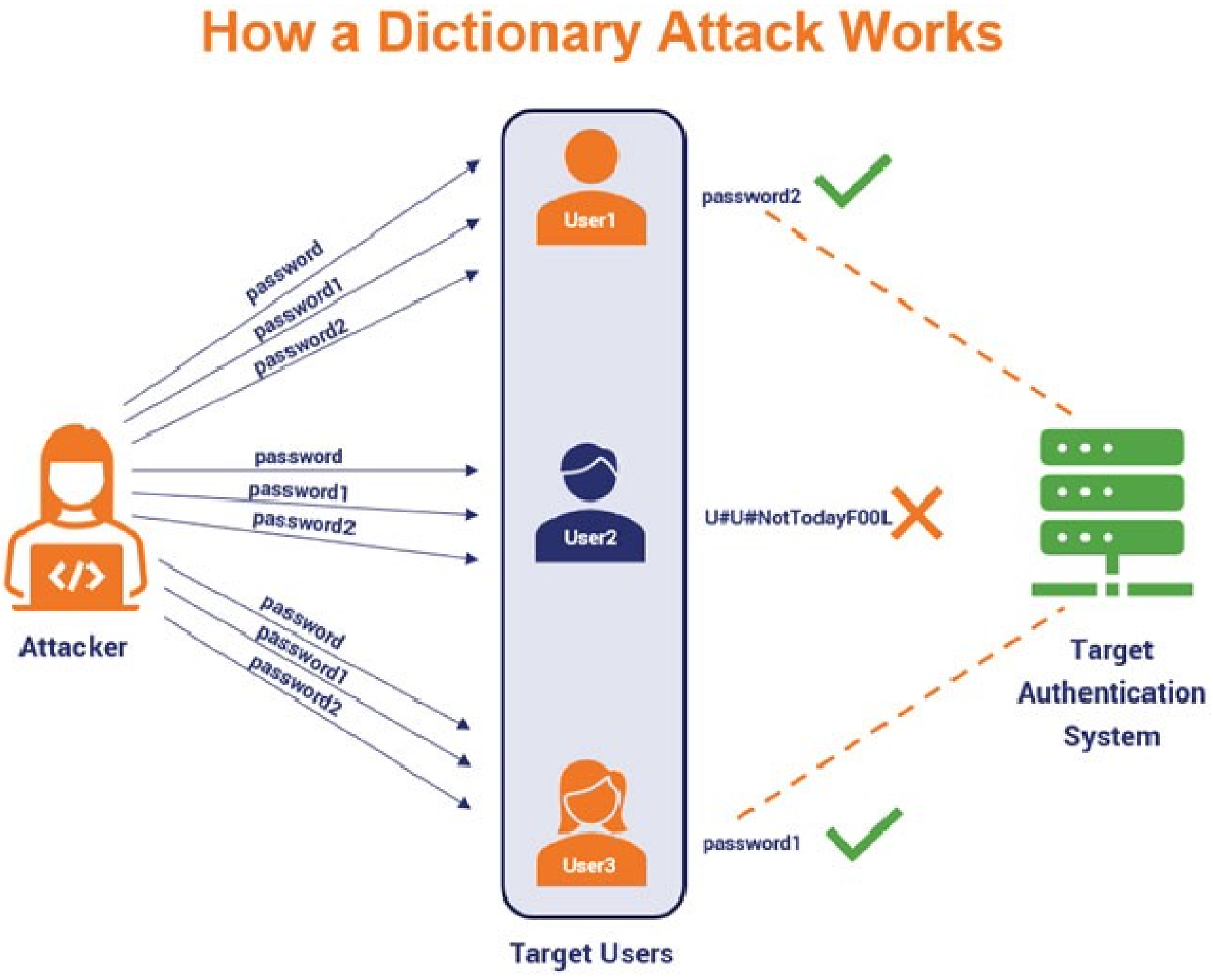
◇ **IP spoofing** — changing your source IP to imitate an IP which the target is aware of. This will trick your target into believing they are communicating with a legitimate IP address.
◇ **Session hijacking** — intercepting the secure communication between a user and a server and using obtained access control measures to access their information. TCP is a connection based communication used for reliable communication between two identities.
◇ **Replay** — data is intercepted and then re-transmitted to the user after performing some modifications of it.

3. Phishing — use of email to obtain information or launch an attack on an organization.

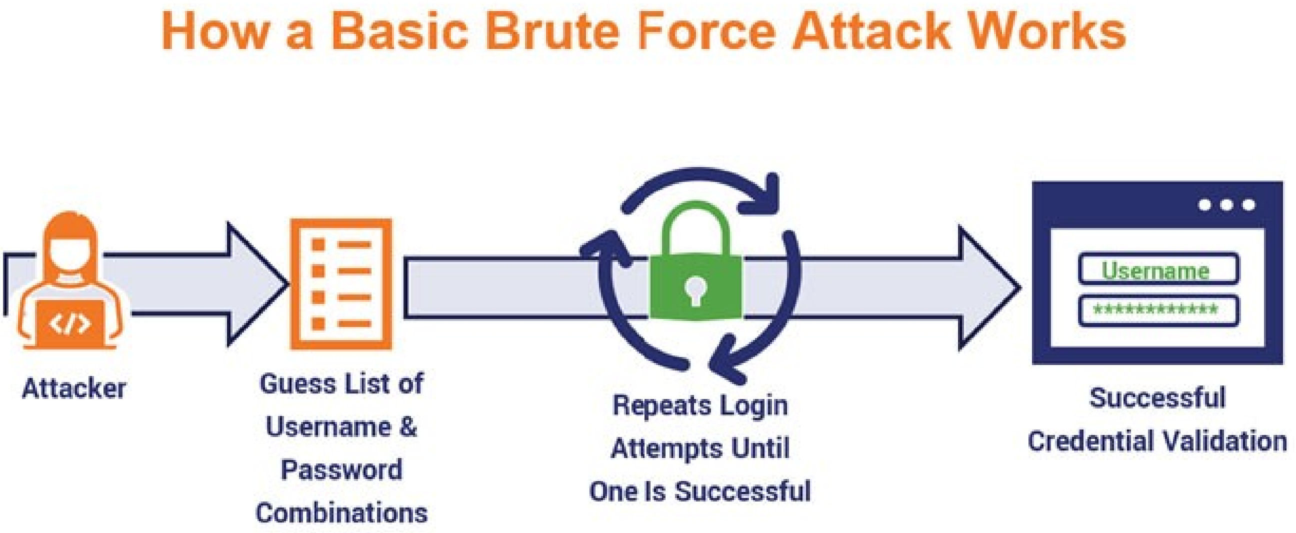
◇ **Spear phishing** — targeting a certain demographic of people e.g people working in one organization.
◇ **Whale Phishing** — targets the senior personnel at a company such as Chief Executive Officer (CEO), Chief Technical Officer (CTO), Chief Financial Officer (CFO), Managing Director (MD).

◇ **Pharming** — achieved by redirecting users to fake, illegitimate or incorrect website the users did not intend to access.

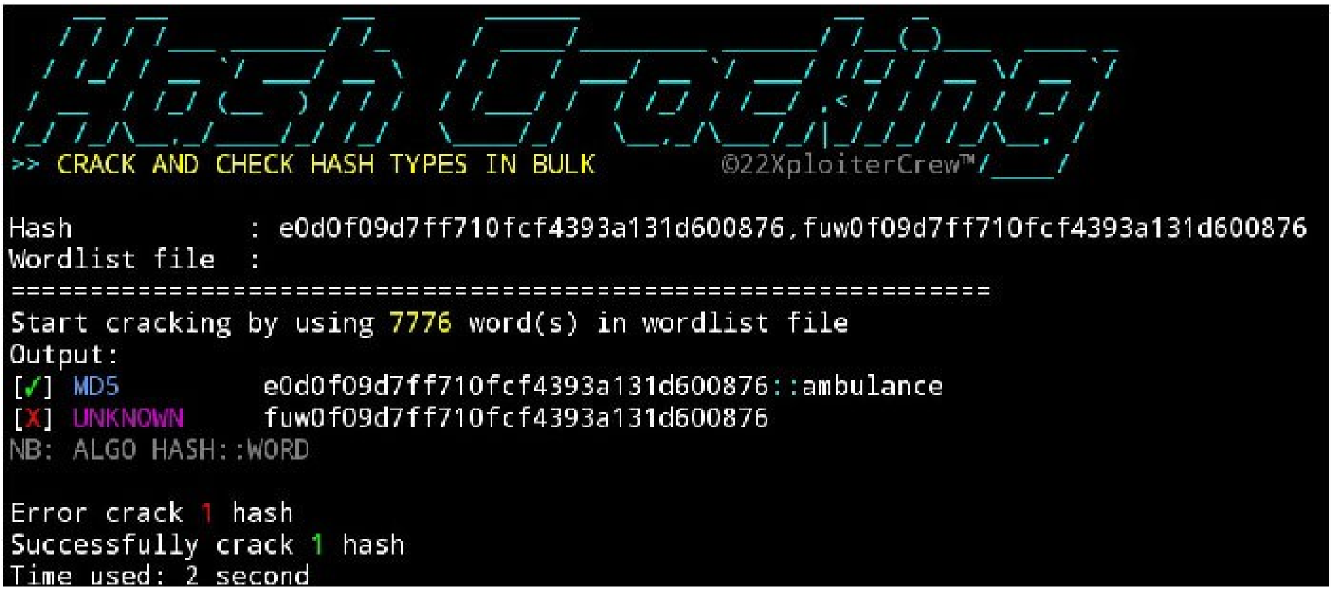
4. Password Attack — the process of obtaining a users password.
◇ **Dictionary Attack** — emanates from the ‘dictionary’ which contains possible combination of characters in which one of them could be the user’s password.



◇ **Brute Forcing** — trying every possible combination of characters to try and predict the password. This can crack any password. The only challenge is the time it will take obtain it and any password protection procedures that may have been put in place such as limiting login attempts.


How a Basic Brute Force Attack Works
Attacker
Guess List of Username & Password Combinations
Repeats Login Attempts Until One Is Successful
Username
****
Successful Credential Validation

◇ **Hash cracking** — passwords are usually stored in hash values to prevent someone from easily reading them. Hash cracking tries to predict what password could have been used to generate the password hash obtained.



```
>> CRACK AND CHECK HASH TYPES IN BULK          ©22XploiterCrew™/____/

Hash             : e0d0f09d7ff710fcf4393a131d600876,fuw0f09d7ff710fcf4393a131d600876
Wordlist file    :
=============================================================
Start cracking by using 7776 word(s) in wordlist file
Output:
[✓] MD5          e0d0f09d7ff710fcf4393a131d600876::ambulance
[X] UNKNOWN      fuw0f09d7ff710fcf4393a131d600876
NB: ALGO HASH::WORD

Error crack 1 hash
Successfully crack 1 hash
Time used: 2 second
```

Image Source :

5. Botnet / Distributed Denial of Service Attacks — this is a combination of multiple devices that can be used to launch an attack on a single system. Attacks could be a simple ping request or an HTTP request for a webpage.

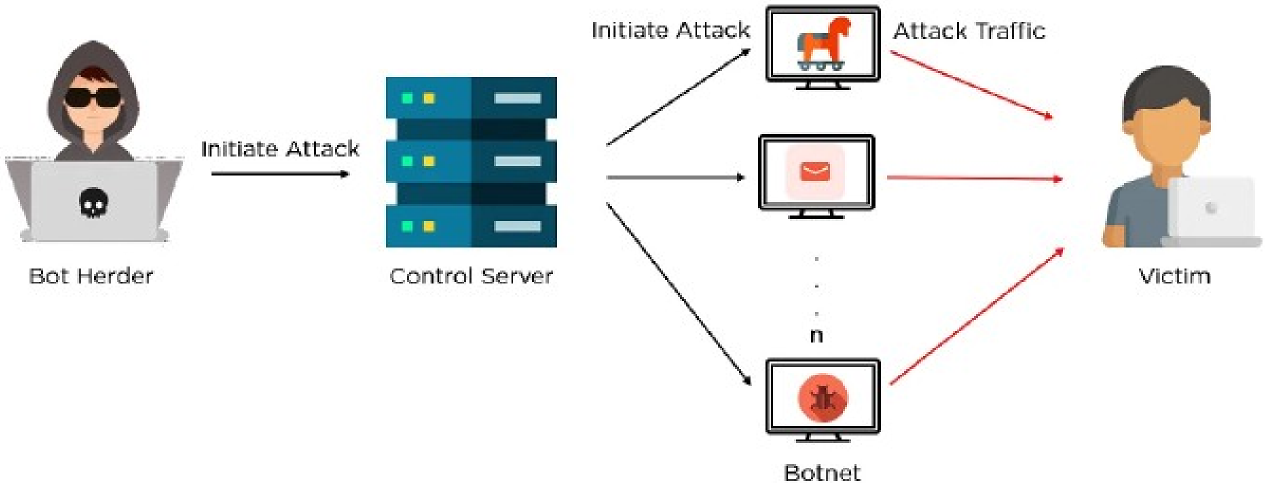


Image Source :

6. Malware / Ransomware Attack — a cyber attack where the adversary delivers software that encrypts your information and will only offer you access to the information after you have paid a ransom. The malware could be in form of a virus, worm, Trojan etc.

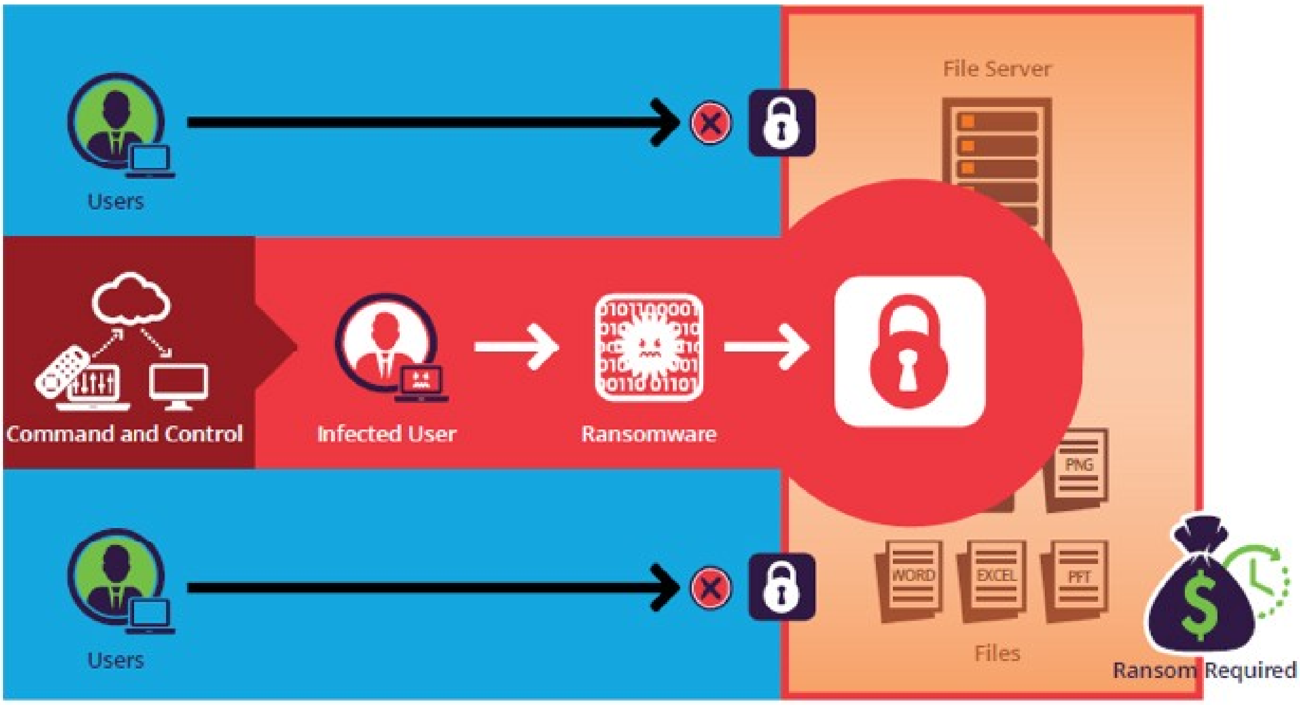
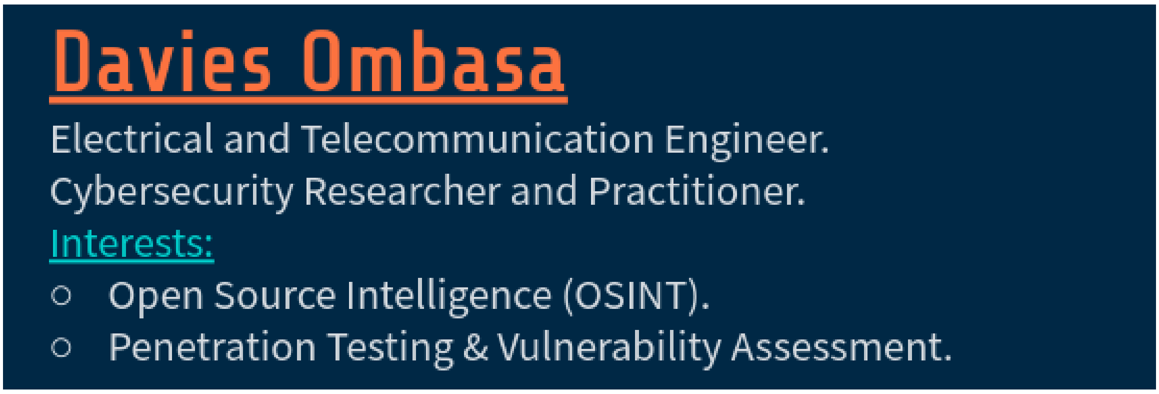


Image Source :

About the writer:



Davies Ombasa

Electrical and Telecommunication Engineer.
Cybersecurity Researcher and Practitioner.

Interests:

- Open Source Intelligence (OSINT).
- Penetration Testing & Vulnerability Assessment.