How and Why Hackers Operate

Infocom Security

Dinos Pastos / @dinopio / d@cy.net

First thing is first... Admit it.

Hands up if **YOU** or **YOUR COMPANY** has ever been compromised in the past.

Not admitting it always makes things worse in the long run.

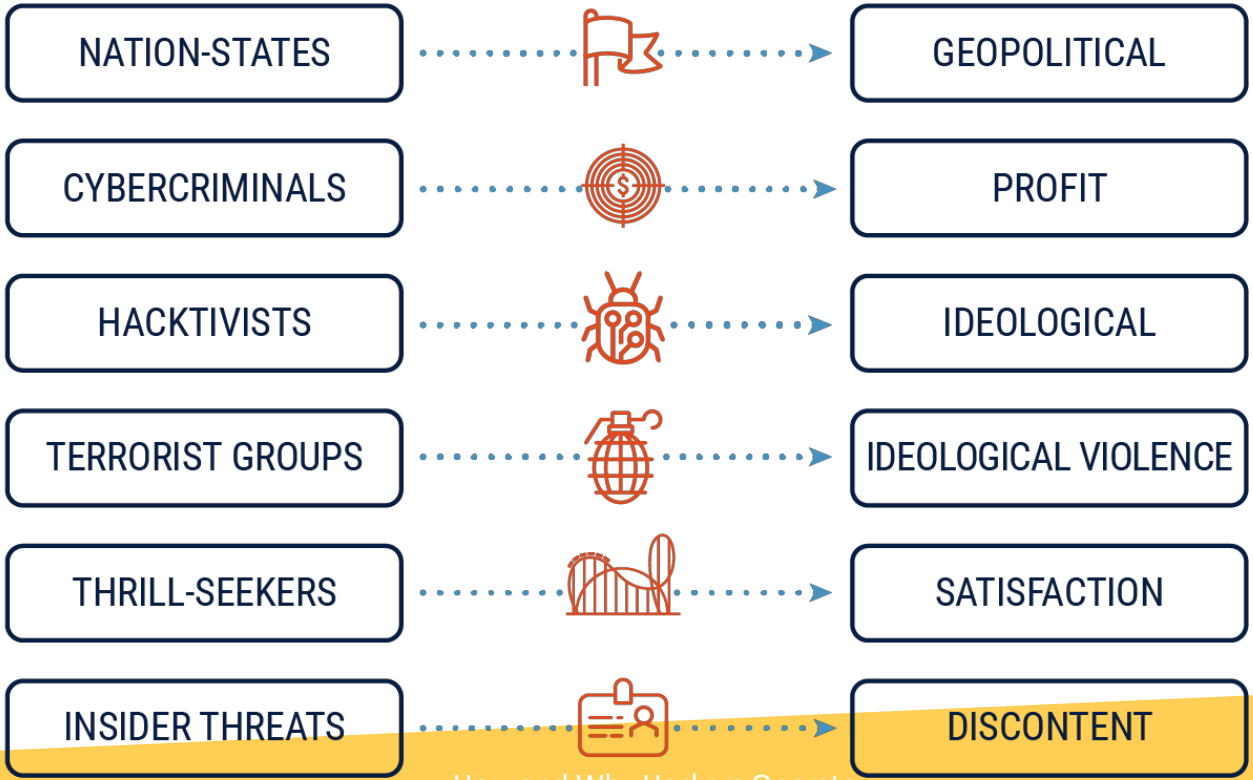
Who are the hackers?
Why do they do it?
How do they do it?

WHO

CYBER THREAT ACTOR

WHY

MOTIVATION



How do Hackers Succeed

Hackers employ a multitude of attacking methods, depending on their target(s). Hackers succeed to compromise security **mostly** due to the following:

- Use of Leaked data/credentials compromised from 3rd parties.
- Social Engineering - The human factor is easier to manipulate.
- Exploitable Software & Hardware deployments.
- Pre-installed Backdoor Access - Compromised Chain of Supply.
- Bad Security Policy, insufficient staff training & ignorance.

Leaked Data?

There are **over 7.8 Billion user records** floating around on the internet.
During the past 5 years, there have been leaks from organizations like:

- Dropbox
- LinkedIn
- Yahoo
- Adobe
- ISP’s, Hosting providers, Cloud providers.
- Governments, Political Parties, Population lists, Voter lists.
- Social Networks
- Various online services (free or paid)

Cyprus and Leaked Data

There are 35000+ Cypriot Email accounts ending with **.cy** with passwords.
That does not include companies or individuals who use **.com** or other TLDs.

Lists include Cypriot Government .gov.cy Email accounts too!

Lets see some!

Social Engineering

because there is no patch to human stupidity

From **phishing emails** to **spoofed phone calls**, hackers have found that the easiest way get what they want is to just ask for it. Targeting high profile personnel is very effective as usually the Chiefs of companies (**CEO, CFO, COO, CHRO**) are not security literate.

Business Email Compromise (BEC) and Email Account Compromise (EAC) scam losses worldwide increased by 136% from December 2016 to May 2018, in the same period **overall BEC/EAC losses result in $12 billion**.

Exploitable Software & Hardware

Software Deployments

Software is buggy and when online we are at risk if not maintained, monitored, updated constantly.

Hardware

Any device connected to your network is a point of entry!

PC, Fax, Copiers, Cameras, IoTs, etc.

Mobile Devices

Don’t trust all vendors equally. Some really don’t care about security or updates.

Both hardware and software

Backdoor Access / Supply Chain

Pre-installed malware:
A batch of many Android devices shipped with malware last year. Sending sensitive data back to unknown actors. This attack is getting very popular.

Shipment interception:
A threat actor can manipulate devices as they're in transit between the manufacturer and the customer, similar to how the *NSA had reportedly intercepted networking equipment* and implanted backdoor surveillance tools before delivery to international customers. Routers, Switches, Laptops, Smartphones, Crypto wallets can be easily compromised with this attack method.

Hardware implants:
As seen in the case of the *Bloomberg Report about SuperMicro Chinese Motherboard implants*

Security is not a product but a process!

- Do not expect your staff to be security conscious without **security awareness and training**.
- A **security policy** needs to be embraced by everyone in an organization with the correct **roles and procedures**.
- **Reward** when applied, **Punish** when ignored.

How and Why Hackers Operate

Thank you :D

Dinos Pastos / @dinopio / d@cy.net