Threatlandscape

Threat Actors

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

In this presentation we focus on threat actors.

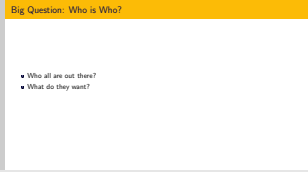
Its on the News

Its on the News

Cybersecurity is in the news. You hear about ransomware, advanced persistent threats, hacks, vulnerabilities, 0days and more... But what do these words mean? That is what we will learn about today. In this video we will focus on different threat actors.

Big Question: Who is Who?

- Who all are out there?
- What do they want?



In this video we will learn about different threat actors. Who is behind the cyber threats? What do they want?

Know Your Threat Actors

- Organized Crime
- Hacktivist
- Insiders
- State Actors

Know Your Threat Actors
- Organized Crime
- Hacktivist
- Insiders
- State Actors

In 2021 Organized crime made up over 80% of data breaches. The rest of the breaches were the work of unaffiliated hackers, insiders and state sponsored groups.

Source: Verizon DBIR 2021

Organized Crime

Organized Crime

No we don't mean mafia of course. Organized in the sense, they operate in an organized fashion. Have shifts, regular working hours, reporting structure. Cybercrime is a job.
Organized crime groups are motivated by financial gains.
The increasing access to financial resources allows them to purchase more sophisticated hacking tools on the dark net. There is also some transitivity between some nation state groups and organized crime groups. These factors lead to blurring of the lines when it comes to the sophistication of these groups.

Their most recent exploits have centered around ransomware.

Hacktivist

Hacktivist

Around 2010-2014 Hacktivism used to be a bigger problem. Non-affiliated, or loosely affiliated groups of hackers came together to further their political goals.
Since their goals are political their actions are a bit harder to predict than organized crime groups.
Although, Hacktivists hey day seems to have passed, there is still a steady stream of hacks originating from these groups. In 2021 Bellarusan hacktivists have hacked into the rail system of Bellarus, disrupting Russian weapons shipments to Ukraine border.

Insiders

Insiders

Insiders are people who already have some legitimate access. Insiders can inflict harm on information assets through either ignorance, or malice. In case of malice, the motivation is often financial, or revenge.

A secretary sending PII over e-mail is a data breach of the error variety.

A system admin deleting contents of a server is malicious action.

Even if you have no administrative control, you are at threat from insiders in your household.

That is why you use private browsing, and don't save passwords in your browser.

State Actors

Espionage

Sabotage

And in one case simple theft...

State Actors
Espionage
Sabotage
And in one case simple theft...

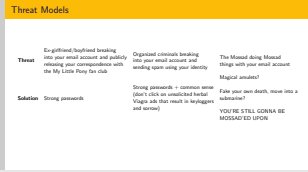
States employ well funded, well organized groups for strategic advantage. These groups often are the most sophisticated threats in the field. They have access to vast throves of vulnerabilities and exploits and they plan their intrusions with extreme care. Since they are motivated to see their actions through, they just persist in gaining access. Because of all these factors, they are often referred to as Advanced Persistent Threats.

Since their motivations are to gain strategic advantage for their states, they rarely are motivated by financial returns (North Korea is the sole exception). Mostly these groups are conducting espionage and sabotage actions.

Due to their competence and clandestine nature of their activities we know relatively little about their operations. What we glimpse is amazing to say the least. The most well known cases of State Actor actions were stuxnet, and notpetya.

Threat Models

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account Magical amulets?
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	Fake your own death, move into a submarine? YOU'RE STILL GONNA BE MOSSAD'ED UPON



Appropriate response is relative. Example here is from James Mickens. As he puts it so nicely: "If Mossad wants to do Mossady things to you, you will get Mossadded upon."