COMP6224 2019-20
Foundations of Cyber Security

Cyber Actors

Week 1 – Wednesday 4th October 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Cyber Security Research Group

blog | twitter

Learning Outcomes

At the end of this lecture you should be able to

- LO1 Describe main cyber threat actors
- LO2 Compare their attack motivations and methodologies

Outline

- Cyber Actors
  - Cybercriminals
  - Nation States
  - Hacktivists
  - Insiders
  - Script Kiddies
- Attack Instigator vs Perpetrator

Cybercriminals

- Interested in illegal profit
- Typical attacks
  - Money theft
  - Personal document ransom
  - Data breaches
  - Distributed Denial of Service (DDoS)
- Attack vectors
  - Malware
  - Social Engineering/Email
  - Botnet

- ➢ **Cybercriminals**
- Nation States
- Hacktivists
- Insiders
- Script Kiddies

Nation States

- Interested in
  - High quality intelligence
  - Sabotage activities/critical infrastructures
  - Subversion, e.g. political election
- Typical attacks
  - Influence campaigns
  - Data breaches
  - DDoS
  - Advanced Persistence Threats (APT)
- Attack vectors
  - Same as Cybercriminals, but more advanced
  - Social media

- Cybercriminals
- ➢ **Nation States**
- Hacktivists
- Insiders
- Script Kiddies

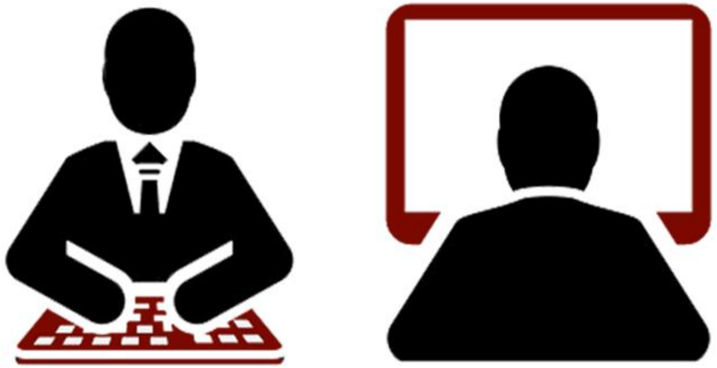
Hacktivists

- Motivated by political, religious, social ideologies
- Typical attacks
  - Web defacements
  - Leakage of confidential/compromising information
  - Data breaches
  - DDoS
- Attack vectors
  - Malware
  - Social Engineering/Email
  - Botnet

- Cybercriminals
- Nation States
- ➢ **Hacktivists**
- Insiders
- Script Kiddies

Insider Threats

- Legitimate access to valuable resources
- Intentional attacks, e.g. by disgruntled employees
  - Publish information on the web
  - Install a logic bomb
  - Steal and sell information
- Unintentional attacks
  - Accidentally delete/post classified files
  - Visit malicious websites, which leads to infecting the enterprise network



- Cybercriminals
- Nation States
- Hacktivists
- ➢ **Insiders**
- Script Kiddies

Script Kiddies/Noobs

- Less skilled hackers, motivated by
  - Desire to join real hacker groups
  - The challenge itself
  - Curiosity
- Just use tools found on the Internet
  - No strategy
  - No clear methodology
  - Despite this, they can succeed!!!

- Cybercriminals
- Nation States
- Hacktivists
- Insiders
- ➢ **Script Kiddies**

Attack Instigator/Perpetrator

- When analysing cyber attacks, we should also distinguish between
  - Attack instigator
  - Attack perpetrator

- Examples
  - An insider can be bribed by a cyber criminal group or nation state
  - A cyber criminal group can be hired by a nation state or another organisation

Who is behind cyber attacks?

- **Group activity (5 minutes)**: for each of the following scenarios, discuss in groups what type of cyber-attack instigator/perpetrator can be responsible
    1. The internal database of a high school has been hacked and stored marks have been tampered with
    2. Edward Snowden collected and disclosed classified documents on US National Security Agency (NSA) global surveillance programs
    3. A company has been targeted by a cyber attack which led to the theft of company's industrial secrets

- **Open discussion (5 minutes)**

- Cybercriminals
- Nation States
- Hacktivists
- Insiders
- Script Kiddies

Who is behind cyber attacks?

- Possible answers
  1. The internal database of a high school has been hacked and stored marks have been changed
     - Script kiddie as both instigator and perpetrator
     - Someone interested in changing marks as instigator, who paid someone else (cyber criminal, in this case) to do it, i.e. to be the perpetrator
  2. Edward Snowden collected and disclosed classified documents on US National Security Agency (NSA) global surveillance programs
     - Hacktivist and insider, he operator as instigator and perpetrator
  3. A company has been targeted by a cyber attack which led to the theft of its industrial secrets
     - It depends on what happen to those secrets
     - If disclosed publicly, hacktivists might be the instigators and perpetrators
     - Otherwise, if they are sent on the black market, cyber criminals might be the instigators and perpetrators
     - Otherwise, if those secrets are valuable for some government
       - Nation states might be the instigators and perpetrators
       - Nation states might be the instigators, cyber criminals the perpetrators

Recap

	Why do they launch attacks?	What kind of attacks do they launch?	What means do they use to attack?
Cybercriminals			
Nation States			
Hacktivists			
Insider Threats			
Script Kiddies			

Key point: they are not mutually exclusive, more types of attacker can be involved in the same cyber attack

References

- Andress, J. and Winterfeld, S., 2014. Cyber warfare: techniques, tactics and tools for security practitioners. Second Edition. Elsevier.
  - ○ Chapter 2: Cyber Threatscape
  - ○ Section "ATTACKERS (MAJOR CATEGORIES OF THREATS)" (pp 27-30)