



# SEC+

## Lesson 2: Comparing Threat Types

# Objectives

- Compare and contrast attributes and motivations of threat actor types
- Explain common threat vectors and attack surfaces

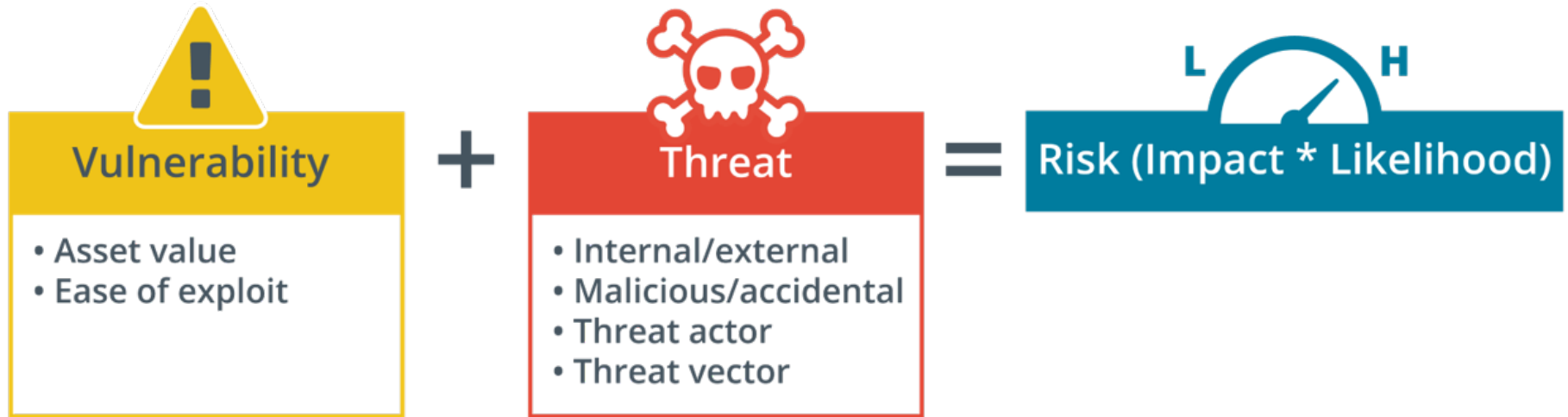
Lesson 2

# Topic 2A

## Threat Actors



# Vulnerability, Threat, and Risk



# Attributes of Threat Actors

- Known threats versus adversary behaviors
- Internal/external
  - Internal threats have authorized access already
  - Attribute of threat actor, not where attack takes place
- Level of sophistication/capability
  - Low capability actors rely on commodity tools
  - High capability actors can develop new attacks
  - Access to political or military assets
- Resources/funding

# Motivations of Threat Actors

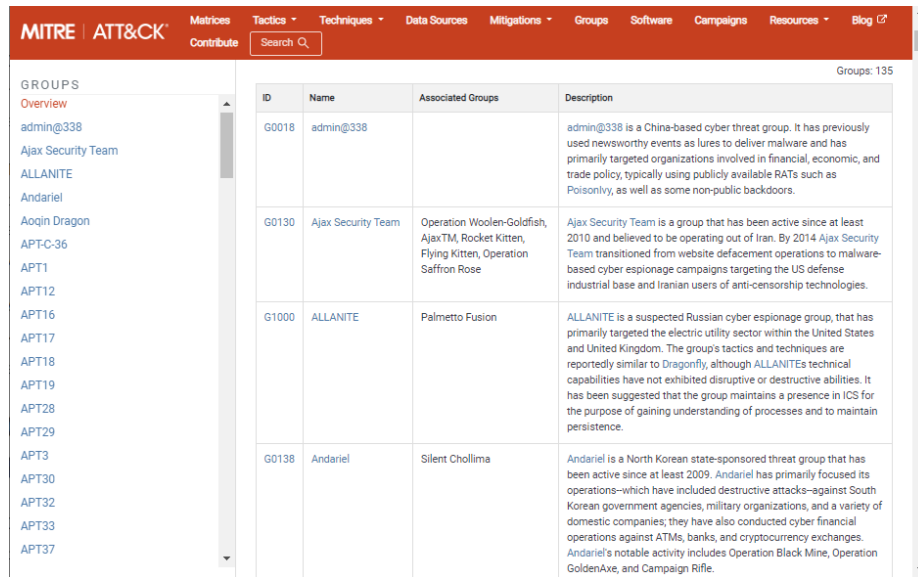
- Intent/motivation
  - Maliciously targeted versus opportunistic
  - Accidental/unintentional
- Strategies
  - Service disruption, data exfiltration, and disinformation
- Chaotic motivations
- Financial motivations
  - Blackmail, extortion, and fraud
- Political motivations
  - Whistleblowers, campaign groups, nation-state actors

# Hackers and Hacktivists

- The “Lone Hacker”
  - White hats versus black hats
  - Authorized versus non-authorized
- Unskilled attackers
  - “Script kiddies”
- Hacker teams and hacktivists

# Nation-state Actors and Advanced Persistent Threats

- Attached to military/secret services
- High level of capability
- Advanced Persistent Threat (APT)
- Espionage and strategic advantage
- Deniability
- False flag operations



The screenshot shows the MITRE ATT&CK Groups page. The left sidebar lists various groups, and the main content area displays a table with the following data:

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as Poisonivy, as well as some non-public backdoors.
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G1000	ALLANITE	Palmetto Fusion	ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom. The group's tactics and techniques are reportedly similar to Dragonfly, although ALLANITE's technical capabilities have not exhibited disruptive or destructive abilities. It has been suggested that the group maintains a presence in ICS for the purpose of gaining understanding of processes and to maintain persistence.
G0138	Andariel	Silent Chollima	Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focused its operations—which have included destructive attacks—against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. Andariel's notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle.

*Screenshot © 2023 The MITRE Corporation.  
This work is reproduced and distributed with  
the permission of The MITRE Corporation.*

# Organized Crime and Competitors

- Organized crime
  - Operate across legal jurisdictions
  - Motivated by criminal profit
  - Can be very well resourced and funded
- Competitors
  - Cyber espionage and disinformation
  - Combine with insider threat

# Internal Threat Actors

- Malicious internal threat
  - Has or has had authorized access
  - Employees, contractors, partners
  - Sabotage, financial gain, business advantage
- Unintentional insider threat
  - Weak policies and procedures
  - Weak adherence to policies and procedures
  - Lack of training/security awareness
  - Shadow IT

# Threat Actors

- Vulnerability, threat, and risk
- Attributes of threat actors
  - Internal/external, level of sophistication/capability, resources/funding
- Motivations of threat actors
  - Service disruption, data exfiltration, disinformation
  - Chaotic, financial, political
- Hackers and hacktivists
- Nation-state actors and advanced persistent threats
- Organized crime and competitors
- Internal threat actors

Lesson 2

# Topic 2B

## Attack Surface



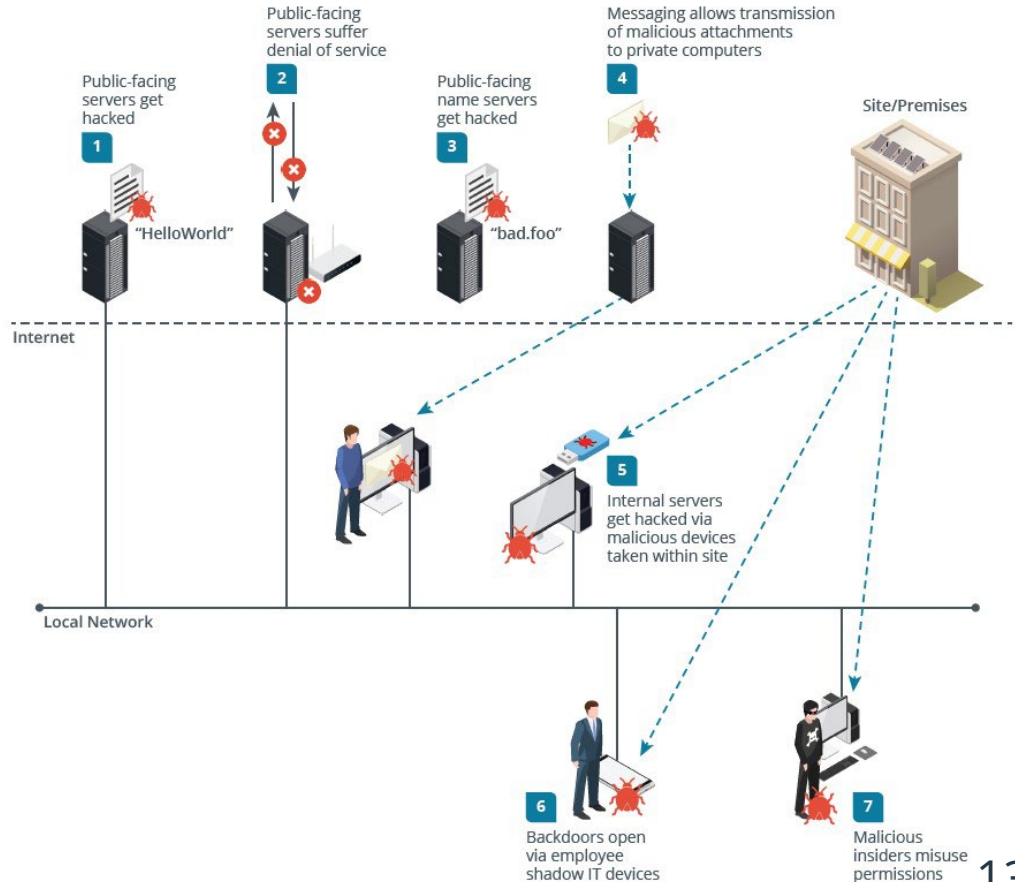
# Attack Surface and Vectors

- Attack surface

- Points where an attacker can discover/exploit vulnerabilities
- Physical, network, application, and human surfaces
- Whole organization or single system/app scope

- Threat vectors

- High capability actors can expand attack surface by developing novel vectors



# Vulnerable Software Vectors

- Vulnerable software
  - Faults in code or design
  - Delays and difficulties in patching
- Unsupported systems and applications
- Client-based vs. agentless
  - Characteristic of automated vulnerability scanners

# Network Vectors

- Remote versus local exploit techniques
- Unsecure networks
  - Lack of confidentiality, integrity, availability
- Specific vectors
  - Direct access and wired (physical ports)
  - Remote, wireless, cloud, and Bluetooth
  - Default credentials
  - Open service port (TCP and UDP ports)

# Lure-based Vectors

- Bait that will tempt the target into opening it
- Removable device
  - Drop attack
- Executable file
  - Trojan Horse malware
- Document files
  - Macro and scripting technologies
- Image files
  - Viewer/browser vulnerabilities

# Message-based Vectors

- Email
- Short Message Service (SMS)
- Instant messaging (IM)
- Web and social media
- Voice calls

# Supply Chain Attack Surface

- End-to-end process of designing, manufacturing, and distributing goods and services to a customer
- Procurement management
- Suppliers, vendors, and business partners
- Whole supply chain can be highly complex
  - Deny threat actors opportunity, time, and resources
- Managed service providers (MSPs)

# Attack Surface

- Attack surface and vectors
- Vulnerable software
- Network vectors
  - Remote versus local
  - Direct access, wired, remote/wireless, cloud, Bluetooth, default credentials, open ports
- Lure-based vectors
  - Devices, programs, documents, images
- Message-based vectors
  - Email, SMS, IM, web/social media
- Supply chain attack surface
  - Design, manufacture, distribution

## Lab Activity

- Assisted Lab: Finding Open Service Ports

Lesson 2

# Topic 2C

## Social Engineering



# Human Vectors

- “Hacking the human”
- Purposes of social engineering
  - Reconnaissance and eliciting information
  - Intrusion and gaining unauthorized access
- Many possible scenarios
  - Persuade a user to run a malicious file
  - Contact a help desk and solicit information
  - Gain access to premises and install a monitoring device

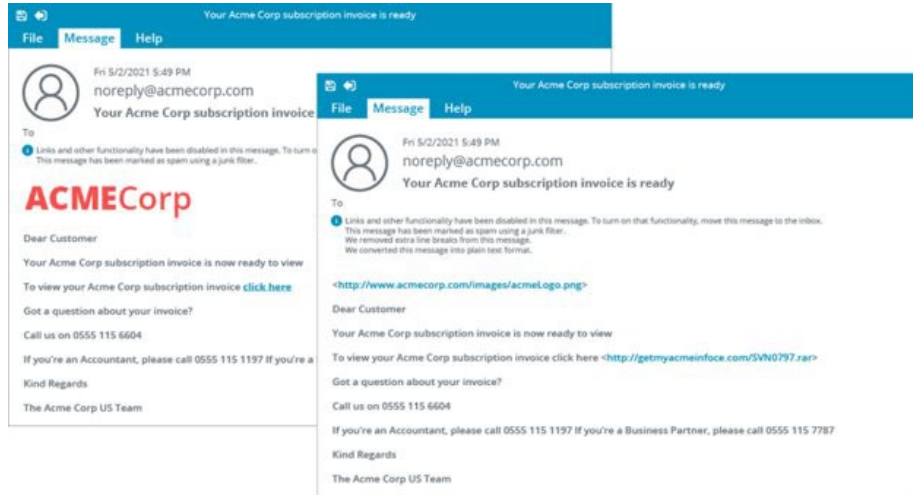
# Impersonation and Pretexting

- Impersonation means pretending to be someone else
  - Persuasiveness/consensus/liking approach
  - Coercion/threat/urgency approach
- Pretexting
  - Exploit situations where identity-proofing is difficult
  - Using a scenario with convincing additional detail
  - Obtain or spoof data that supports the identity claim



# Phishing and Pharming

- Phishing
  - Trick target into using a malicious resource
  - Spoof legitimate communications and sites
- Vishing
  - Using a voice channel
- SMiShing
  - Using text messaging
- Passive techniques have less risk of detection
- Pharming
  - Redirection by DNS spoofing



# Typosquatting

- Make phishing messages more convincing
- Email spoofing techniques
  - From field confusion
- Typosquatting
  - Cousin domains that look like a trusted domain

# Business Email Compromise

- Target phishing/vishing/SMiShing to a specific individual
  - Pose as colleague, business partner, or vendor
  - Spear phishing, whaling, CEO fraud, angler phishing, ...
- Brand impersonation and disinformation
  - Make convincing fake phishing messages, business correspondence, and pharming websites
  - Disinformation versus misinformation
- Watering hole attack
  - Compromise a third-party site that the threat actor knows is used by the target

# Social Engineering

- Social engineering
- Human vectors
- Impersonation and pretexting
- Phishing and pharming
- Typosquatting
- Business email compromise

## Lab Activity

- Assisted Lab: Using SET to Perform Social Engineering

CompTIA Security+ Exam SY0-701

# Lesson 2



## Summary