ANATOMY OF AN ATTACK!

Are Your Crown Jewels Safe?

Dom Kapac, Security Evangelist

WHAT DO WE MEAN BY CROWN JEWELS?

- Crown jewels for most organizations are critical infrastructure and **data**
  - Data is a valuable asset to both individuals and organizations
  - Data is also valuable to hackers who want to get access to it

- You do not get to choose whether you are a target
  - You are targeted whether you have something of value; or
  - There is the perception that you do

WHAT DO WE MEAN BY CROWN JEWELS?

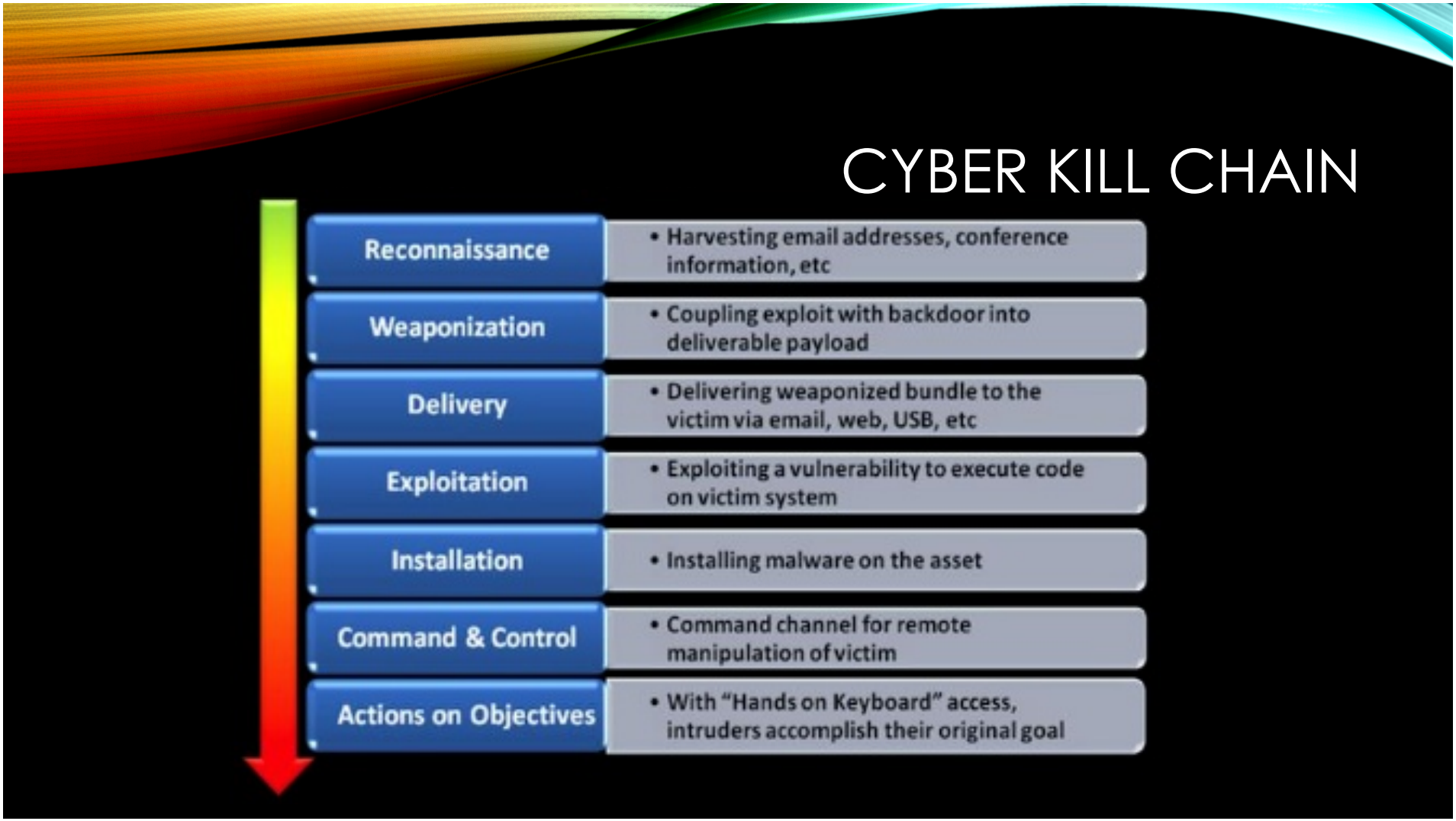
- How do hackers accomplish this goal?
  - Compromise of humans, servers, and other systems

- What are steps you can take to defend against the majority of intrusions?
  - Identify the crown jewels for your organization
  - Identify what security controls are presently in place
  - Determine whether this is consistent with your risk appetite

CYBER KILL CHAIN

1) Reconnaissance: gathering information about the target that will identify the attack vector and make the attack more likely to be successful
2) Weaponization: developing exploits with payloads such as malware and decoys
3) Delivery: phishing attacks, infected websites, USB drives, etc
4) Exploitation: activation of exploit code
5) Installation: delivering payloads, establish persistence and backdoors
6) Command and Control: internal network reconnaissance, understand network architecture, traffic flows
7) Actions on Target: expand compromise, maintain Persistence, ex-filtrate data

CYBER KILL CHAIN



HOW DO HACKERS ACHIEVE ACCESS?

- Exploiting vulnerabilities found within the code of applications and operating systems
- Client side or phishing attacks – often using social engineering tactics
- Malware and other payloads

WHAT IS A VULNERABILITY

- A vulnerability is a flaw or bug in code of applications or systems
  - some vulnerabilities are easier to exploit than others
- A vulnerability can also be a person who is unaware of security practices (social engineering – the human element)
- This presentation covers vulnerabilities in applications and systems
- How are vulnerabilities exploited? What tools are used?

WHAT IS AN EXPLOIT?

- Code that is used to exploit a vulnerability within a system in order to gain access
- When an exploit is successful, the attacker can drop payloads such as malware
- Exploits can be used to gain unauthorized access but also to cause a denial-of-service condition

WHAT IS A PAYLOAD?

- A payload is any code or tool that allows interactions with the system after a successful attack
- This is also referred to as a shell
- Tools to gain access to other systems within the network
- Tools to maintain access and extract data
- Malware

ANATOMY OF AN ATTACK!

- Vulnerability → Exploit → Payload

HOW TO DEFEND AGAINST THESE ATTACKS!

- No-one is immune
- Today's threats are more sophisticated and targeted than ever
- Doing the basics will prevent 80% of the problems
- You are likely to be judged more on how you respond to the problem than whether you had an incident

HOW TO DEFEND AGAINST THESE ATTACKS!

- Observe core security principles
  - strong authentication
  - least privilege
  - separation of duties
  - defense in depth
  - non-repudiation

- Implement non-technical security controls
  - information security policy, information classification
  - build a risk register and identify crown jewels
  - incident response plan
  - security education and awareness

HOW TO DEFEND AGAINST THESE ATTACKS!

- Deploy technical security controls
  - firewalls, VPN
  - intrusion prevention
  - web content filtering
  - email content filtering
  - anti-virus
  - hardened systems, disable unnecessary services
- Hygiene level controls such as the above are not enough
  - multi-factor authentication
  - restrict administrator privileges
  - encryption
  - patch operating systems and applications
  - application white-listing
  - vulnerability scanning

HOW TO DEFEND AGAINST THESE ATTACKS!

- Other necessary steps
  - change default passwords
  - do not use shared accounts
  - disable unnecessary services
  - enable logging, review logs
  - encrypt sensitive information
  - ensure vendors are adhering to security best practices

NOW FOR THE REAL FUN!

<LIVE DEMONSTRATION>