9. Active Defense, Cyber Deception

Simona Buchovecká, Tomáš Čejka

Faculty of Information Technology, CTU in Prague

simona.buchovecka@fit.cvut.cz, tomas.cejka@fit.cvut.cz

November 9, 2020

Section 1

Theory & Terminology

What is Active Defense? Offensive Countermeasures.

- Employ offensive techniques, but with defensive posture
- Think poison (taken then consumed), not venom (injected)
- Lay traps inside your systems, but don't attack theirs
- **Does not replace the traditional layered security!**

Current Strategies are (sometimes) Not Working

- New attack vectors
- New attack methods
- More complex environment => more difficult detection
- No silver bullet

Cyber Deception

- Deliberate and calculated process of deceiving attackers to achieve more efficient defense
- Slow the attacker down, confuse the attacker
- Actively obfuscate your network to increase the amount of effort required to attack & noise created by attacker
- Time(Detection + Reaction) $<$ Time(Attack)

Legal Issues

- Annoyance and Attribution usually pose no risk
- Attack – ALWAYS consult with legal department
- Do not hide or obfuscate what you are doing
- Use warning banners & terms of use
  - Helps to define boundaries of the network

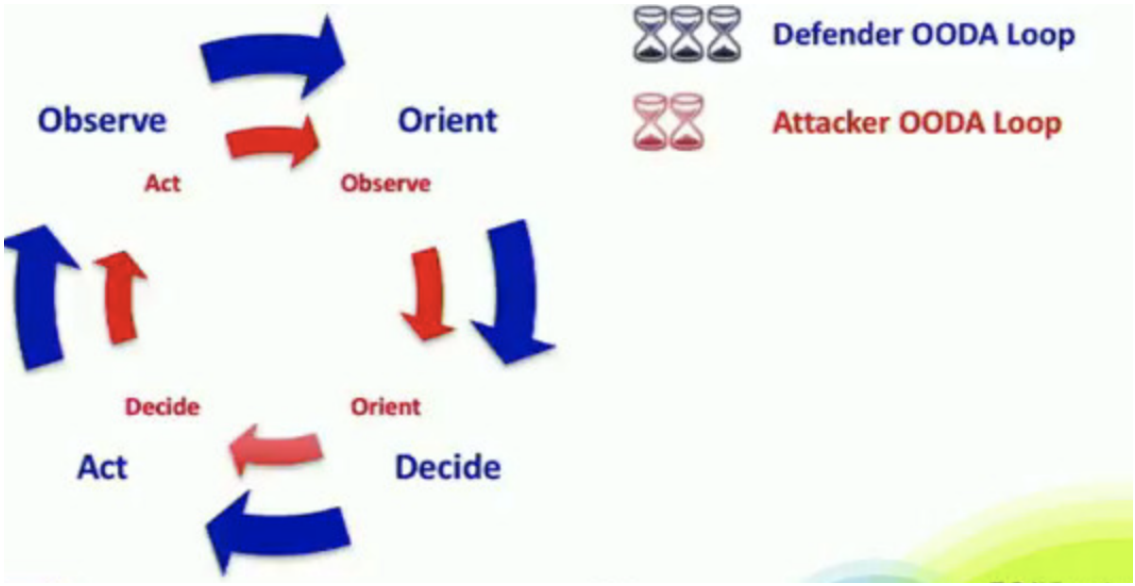
Phases

- **Annoyance** – waste attacker's time
- **Attribution** – know who is attacking you
- **Attack** – run active code on an attacker's system

Annoyance

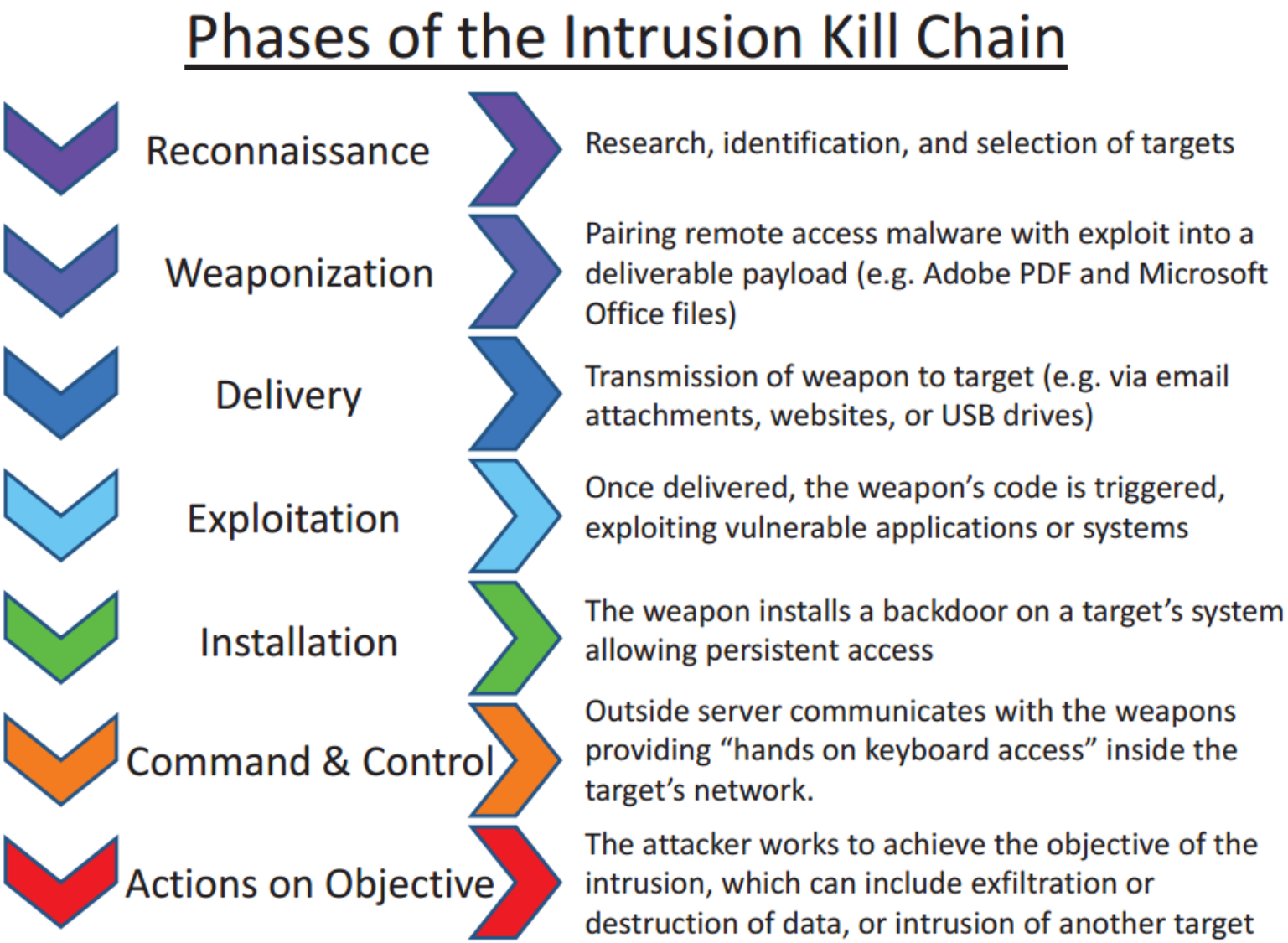
- Making the system/network more difficult to attack
  $\rightarrow$ the attacker has to take more actions
  $\rightarrow$ it is more likely to detect the attack

OODA Loop

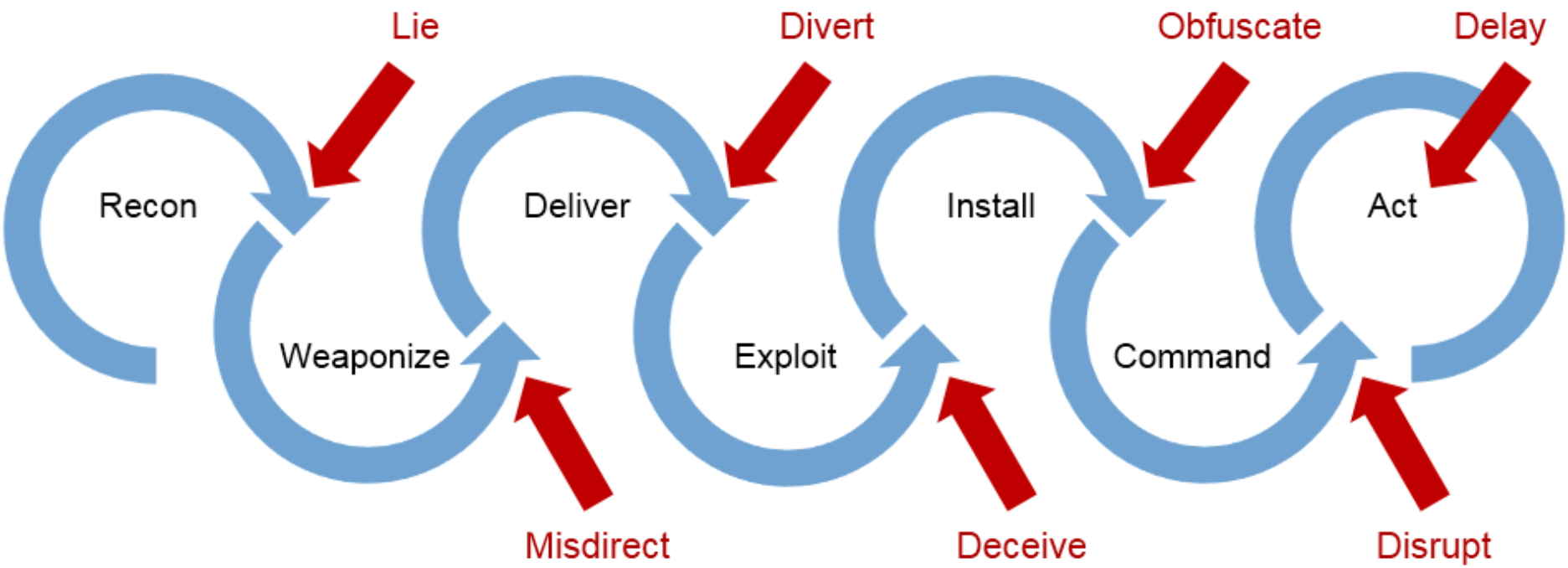


- Observe
- Orient
- Decide
- Act
- Set up tricks and traps, than watch very closely
- Whoever's OODA loop is faster, wins
- **Goal**: Disrupt attacker's OODA loop

Kill Chain


Phases of the Intrusion Kill Chain
Reconnaissance
Research, identification, and selection of targets
Weaponization
Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery
Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation
The weapon installs a backdoor on a target's system allowing persistent access
Command & Control
Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective
The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Disrupting the Kill Chain



Obfuscate the Environment

- Change web server identification
- Change TCP/IP protocol stack of your OS
- Filter out the User-agent strings that attackers/testers use

Spider/Crawler Traps

- Create random links and serve them for crawlers
- Be Careful – don't do it on externally facing webserver, crawled by Google – setup robots.txt (attackers may be interested into it)
- Possibly even setting up a DoS on the automated scanner
- Infinitely recursive directories

Honeypots

General Information

- Object intended to be interacted with by an attacker
- Research vs. Production honeypots
- Helps you to learn about attacker

Principle

- No production system should interact with honeypot
- Any interaction with honeypot is considered malicious and should be responded to immediately
- May be interconnected into honeynet

Honeytables

- Table within database populated with bogus data

Honeyports

- Used to dynamically blacklist attacking systems
- Dynamic blacklisting can be source of potential issues (spoofing originating system may cause blacklisting of legitimate system)
  - Potential solution: trigger blacklisting script only when full established connection is made

HoneyDNS

- Jon Oberheide, Manish Karir, Z. Morley Mao: **Characterizing dark DNS behavior**

Client-side Honeypot

- Automate analysis without endangering your system
- Automatically downloads and analyzes requested webpage/file

Entrapment vs. Enticement

- Entrapment – we persuade the attacker to commit a crime that he would otherwise not commit
- Enticement – the attacker would have committed (or was intended to commit) a crime anyway – Honeypots
- Entrapment is always illegal!

Whitelisting/System Integrity Checks

- Monitor filesystem - look for indicators of change

Attribution

- Identify who is attacking, even if using proxies/tor ...
- Track your intellectual property
- Google, shodan.io, censys.io, ...
- DNS tools (dig)
- Port scans, vulnerability discovery (nmap, wpscan, ...)
- Credential harvesting
- Location – geotagged media

Dealing with Proxies/TOR

- Some of the attacker's application are configured to communicate via proxy, some of them may be not
- Goal: invoke application that might not go through the proxy and have the attacker connected to you
  $\rightarrow$ you will get real IP address
- Application that may be used: Office, Flash, Java, ...
- Web bugs – insert arbitrary code into the file (works even if macros are disabled in Office documents) – HTML code is inserted into the document, and Word will call back

Attack

- **Once again you want to make sure that any of the techniques covered here are discussed with legal and approved by management**
- Client-side attacks predominantly
- We want attacker to come to us (preferably after reviewing the warning banner)
- Even though attacker is violating law, he still has rights that you cannot violate!

Client-side Attacks

- Java Script (e.g., BeEF framework)
- Java applets (e.g., SET)
- Macros in documents

Section 2

Practical Section

Firewalls

- Stateless
- Statefull
- Port-knocking
- Application Layer Firewall

Blacklisting

- Whitelist / greylist / blacklist
- Fail2ban

DDoS Defense / Mitigation

- Load balancing, DNS Fluxing
- Cloud services / hosting
- CloudFlare, Google Shield
- Rate-limiting
- Remotely Triggered Blackholing (RTBH)
  - Blackhole routing
  - DNS sinkhole

DDoS Mitigation

- Scrubbing center (appliance)
  - Corsa, A10, CESNET
- Service
  - RadWare, Akamai, CloudFlare, ...
  - `http://www.toptenreviews.com/business/internet/best-ddos-protection-services/`
- FENIX
  - Trusted secured community in the Czech peering center, can be isolated

References

- John Strand: Offensive Countermeasures, The art of active defense
- Gartner study: Emerging Technology Analysis: Deception Techniques and Technologies Create Security Technology Business Opportunities
- Jon Oberheide, Manish Karir, Z. Morley Mao: Characterizing dark DNS behavior

Questions?