Antiterrorism

Awareness

U.S. ARMY

Army Strong[SM]

The Cyber Attack Cycle

Always Ready, Always Alert

Because someone is depending on you

Before proceeding to the Cyber Attack Cycle, it is useful to understand certain parameters relating to the cyber threat as defined by the U.S. Army Cyber Command

The Cyber Threat

Ends: Adversaries will use cyberspace to commit espionage, subversion (including insider threat), and sabotage.

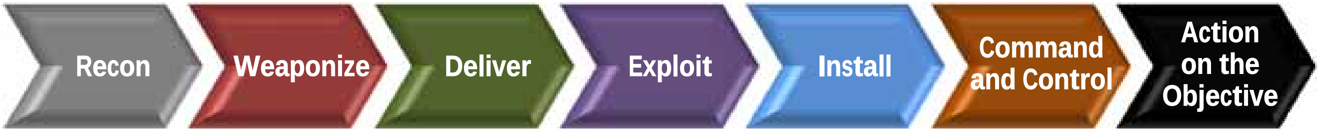
Ways: Adversaries gain intelligence and access via cyberspace in order to:

- Recruit insiders (subversion)
- Commit acts of sabotage (stop Army missions; crash networks, electric power, water facilities)
- Harm Army personnel, families, units, and operations
- Commit criminal actions against Army installations, facilities, units, personnel, and/or family members
- Enable conventional threat capabilities
- Identify U.S. vulnerabilities in weapons systems, facilities, and tactics, techniques, and procedures

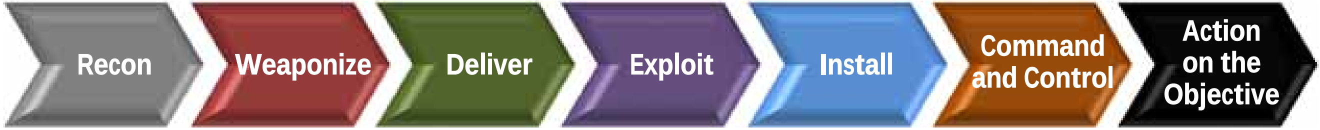
Means: To do this, adversaries tactics include:

- Exploiting people's trust through Phishing attacks
- Infiltrating Malware to perform unauthorized and often surreptitious actions on computers
- Exploiting Social Media through false personas
- Gathering open source information from online postings
- Using infected thumb drives, CDs, DVDs, or other computer memory products to transfer attack mechanisms
- Tampering with cell phones and laptops (both personal and official) especially while personnel are traveling overseas
- Exfiltrating information that enables sabotage and other harmful actions

The Cyber Attack Cycle depicted in the following pages educates you on how cyber adversaries operate in order for you to better defend our networks. The “Cyber Attack Cycle” outlines the sequential actions taken by adversaries in a cyber attack. Interrupting an adversary action anywhere along this cycle can serve to stop the attack.



Cyber Attack Cycle – Overview



Reconnaissance. Identification and selection of a target by harvesting email addresses or targeting social media users.

Weaponization. Coupling a remote access Trojan with a computer operating system or software application exploit into a deliverable payload. Increasingly, data files such as Microsoft Office documents or Adobe PDF files have been used as a weapon platform. spawning attacks on other computers.

Delivery. Implant of malware by remote or physical access to a targeted computer.

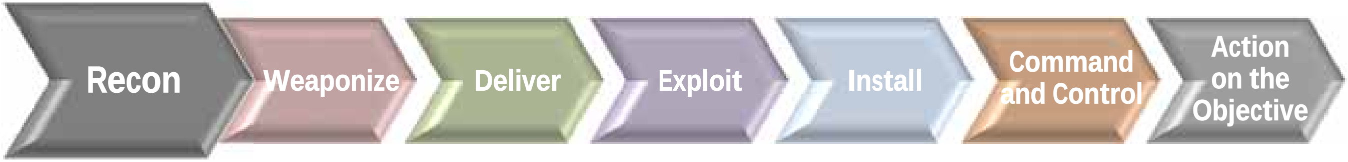
Exploitation. Triggering of the attacker's code. The payload exploits an application or operating system vulnerability. It can exploit the user by persuading him to open an executable attachment, or leverage a feature of the operating system that auto-executes code.

Installation. Creation of access point on a victimized computer that allows the attacker unauthorized entry and exit on a victimized computer and network.

Command and Control. The installation of malware on targeted computers that allows the attacker to communicate instructions to the previously installed payload malware providing the attacker with the means to conduct a cyber attack.

Actions on objectives. The final stage required for a successful attack. The most common objective is data exfiltration or stealing information from the affected computer. Attackers might also want to change or erase files on the affected computer, and move laterally throughout affected computers IT environment spawning attacks on other computers.

Cyber Attack Cycle – Recon

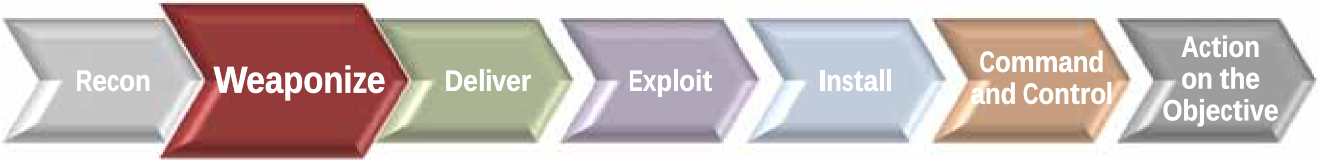


Reconnaissance. Identification and selection of a target by harvesting email addresses or targeting social media users.

Examples of Reconnaissance:

- Unsolicited email messages (SPAM) from unknown persons or organizations
- Attempts to “friend” you or “add” you to business contacts on social media sites by persons you do not know
- Network intrusions and data exfiltration

Cyber Attack Cycle – Weaponize

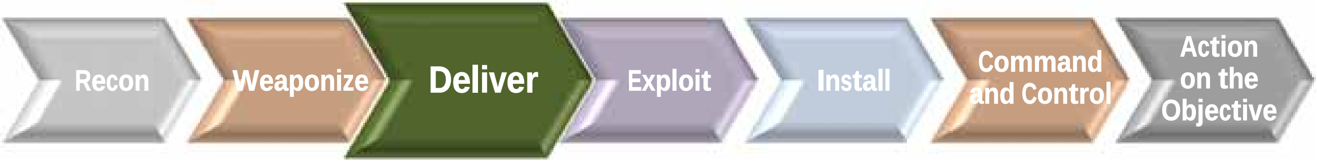


Weaponization. Coupling a remote access Trojan with a computer operating system or software application exploit into a deliverable payload. Increasingly, data files such as Microsoft Office documents or Adobe PDF files have been used as a weapon platform. spawning attacks on other computers.

Examples of Weaponization:

- Leveraging a known or unknown vulnerability on a computers operating system or software application that will allow an attacker to modify the intended operation or functions of one or more computers on a network
- Email attachments from known or unknown entities containing malware or viruses
- Unknown applications, processes, or scripts running that may or may not be detected by the computer's antivirus software

Cyber Attack Cycle – Deliver



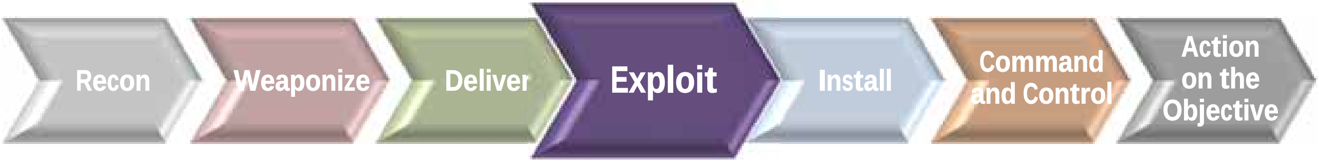
Delivery. Implant of malware by remote or physical access to a targeted computer.

Examples of Delivery:

Transmission of the payload to the target. The three most-prevalent delivery vectors for weaponized payloads:

- Email messages with attachments containing malware
- Websites containing malware that attack from a remote location
- USB and other removable media containing malware

Cyber Attack Cycle – Exploit

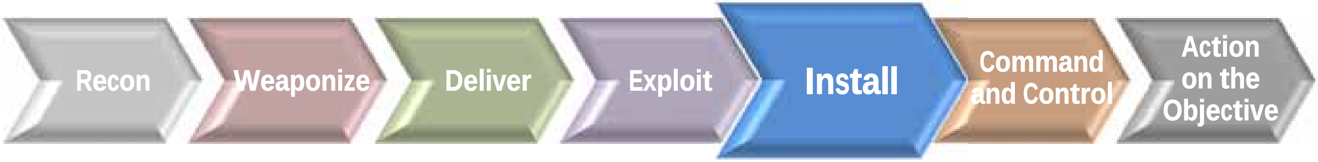


Exploitation. Triggering of the attacker's code. The payload exploits an application or operating system vulnerability. It can exploit the user by persuading him to open an executable attachment, or leverage a feature of the operating system that auto-executes code.

Examples of Exploitation:

- The attacker's malware seeks and locates a known or previously unknown software application or operating system vulnerability on a targeted network
- An attacker persuades a user to open a malware executable attachment
- The interception of computer wireless transmissions to monitor, modify, interrupt, or deny normal system or user operations or functions

Cyber Attack Cycle – Install

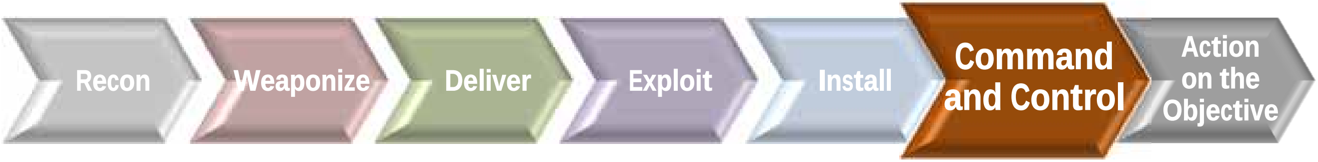


Installation. Creation of access point on a victimized computer that allows the attacker unauthorized entry and exit on a victimized computer and network.

Examples of Installation:

- Installing a remote access Trojan or backdoor on the victimized system and network, allowing the attackers to affect all users of the system
- The physical emplacement of internal or external hardware devices that allow an attacker unauthorized access to a computer system or network
- An attacker leverages a feature of a computer operating system that auto-executes malicious functions

Cyber Attack Cycle – Command and Control

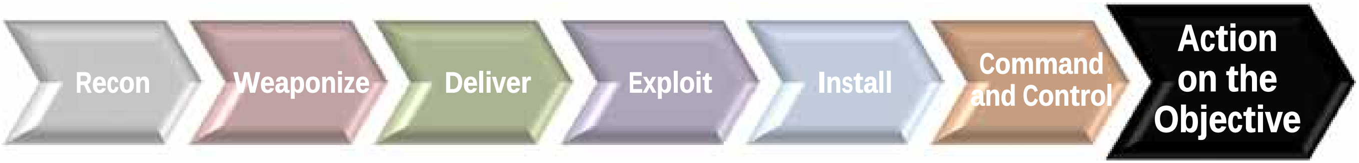


Command and Control. The installation of malware on targeted computers that allows the attacker to communicate instructions to the previously installed payload malware providing the attacker with the means to conduct a cyber attack.

Examples of Command and Control:

- An outbound beacon from the infected computer to the attacker, which is sort of a “phone home” function, that initiates a command and control dialogue between the attacker and the targeted computer
- A connection that provides an attacker with “hands-on-the-keyboard” access to a targeted computer
- The initiation of applications on a targeted computer that are not a normal user command or operating systems function

Cyber Attack Cycle – Action on the Objective



Actions on objectives. The final stage required for a successful attack. The most common objective is data exfiltration or stealing information from the affected computer. An attacker's goal may also be to change or erase files on the affected computer while simultaneously moving throughout the affected network spawning attacks on other computers.

Examples of Actions on the objective:

- Data exfiltration—copying and removing files from computers or servers
- Data corruption—altering or erasing data from computers or servers
- Attacks to destroy—launching harmful applications or queries
- Redirecting browser queries

This product was developed in collaboration with the U.S. Army Cyber Command

PROVOST MARSHAL GENERAL
U.S. ARMY

Headquarters, Department of the Army
Office of the Provost Marshal General
(DAPM-MPO-AT)
2800 Army Pentagon - Washington, DC 20310-2800