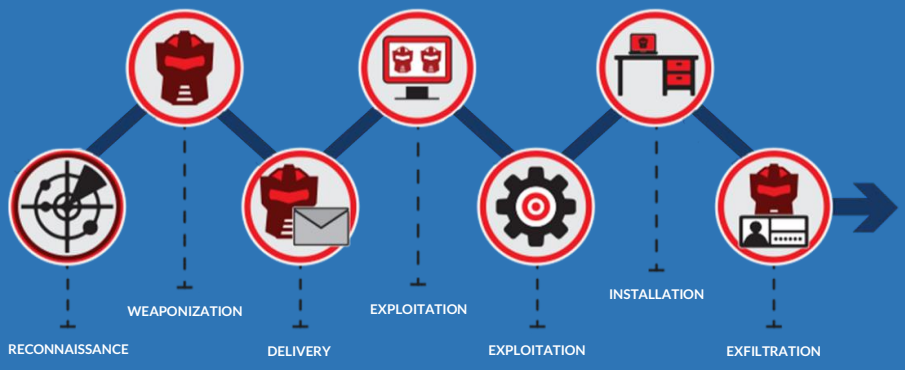
THE CYBER KILL CHAIN



For more intel, go to: http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

POISONTAP

Description: emulates Ethernet device over USB (or Thunderbolt). Highjacks all internet traffic from machine. Siphons and stores HTTP cookies and sessions from Alexa top 1,000 sites. Exposes internal router to attack, installs persistent web-based backdoor in HTTP cache. Does not require machine to be unlocked. Attack is persistent even after device is removed.

Kill-Chain Stage: Delivery & Exploitation

Mitigation Methodology:

- Disable Hardware (USB)
- Least Privilege Application Control
- Certificate Validation

More Intel:
Samy Kamkar - https://samy.pl/poisontap/

Inveigh, Responder & Seth

Description: Man-in-the-Middle attacks on multiple protocols allowing for password harvesting of multiple systems on the network.

Kill-Chain Stage: Reconnaissance, Exploitation
Mitigation Methodology: Network Intrusion Protection Systems, Firewalls, network segmentation

More Intel:

- Inveigh: https://github.com/Kevin-Robertson/Inveigh
- Responder: https://github.com/SpiderLabs/Responder
- SETH - https://github.com/SySS-Research/Seth

MouseJack

Description: Injecting keystrokes to a target computer via a vulnerable wireless mouse.

Kill-Chain Stage: Delivery, Exploitation, Installation
Mitigation Methodology:

- Firmware Update,
- Policy & Procedures
- Application Control

More Intel:
Bastille Research - https://www.mousejack.com/

Bash Bunny, USB Rubber Ducky, & Bad USB

Description: Keystroke injection tools.

Kill-Chain Stage: Delivery, Exploitation, Installation

Mitigation Methodology:

- Disable Hardware(USB)
- Least Privilege/Application Control
- Policy & Procedures

More Intel:

- HID Devices - https://en.wikipedia.org/wiki/Human_interface_device
- BashBunny - https://wiki.bashbunny.com/#!index.md
- USB Rubber Ducky - https://www.usbrubberducky.com
- Digispark Kickstarter ATTINY85 Arduino General Micro USB Development Board - https://www.kickstarter.com/projects/digistump/digispark-the-tiny-arduino-enabled-usb-dev-board

WiFi Pineapple

Description: Man-in-the-middle attack for wifi devices.

Kill-Chain Stage: Delivery & Exploitation

Mitigation Methodology:

- Disable WiFi when not in use
- Trusted Networks Only
- Virtual Private Networks
- Certificate Validation

More Intel:
Hak5 - https://www.wifipineapple.com/

USB Killer

Description: USB Device designed to instantly disable electronic devices.

Kill-Chain Stage: Exploitation

Mitigation Methodology:

- Hot Glue Gun

More Intel: USB Killer - https://usbkill.com/

Rainmaker
Andy@MeteorMusic.com
www.MeteorMusic.com
Twitter: R41nM4kr

CYBERARK

Andy Thompson, CISSP, SSCP, GPEN
Andy.Thompson@CyberArk.com
www.CyberArk.com
LinkedIn: andythompsoninfosec