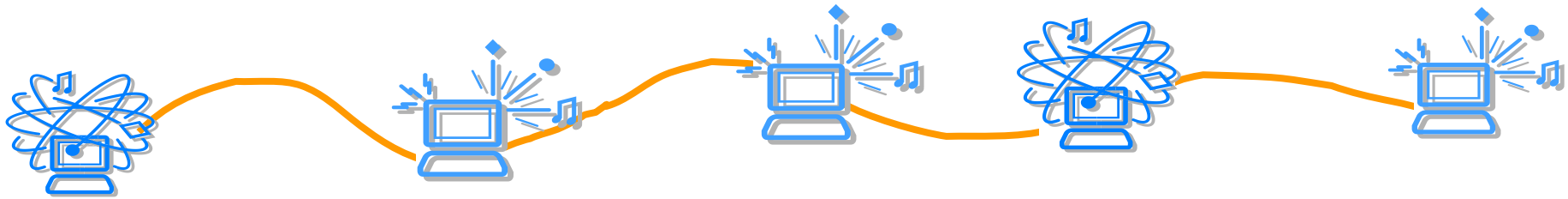
Segurança em Redes de Comunicação - SRC
Ciber-Kill Chain



Redes de Comunicação de Dados
Departamento de Engenharia da Electrónica e das Telecomunicações e de Computadores
Instituto Superior de Engenharia de Lisboa

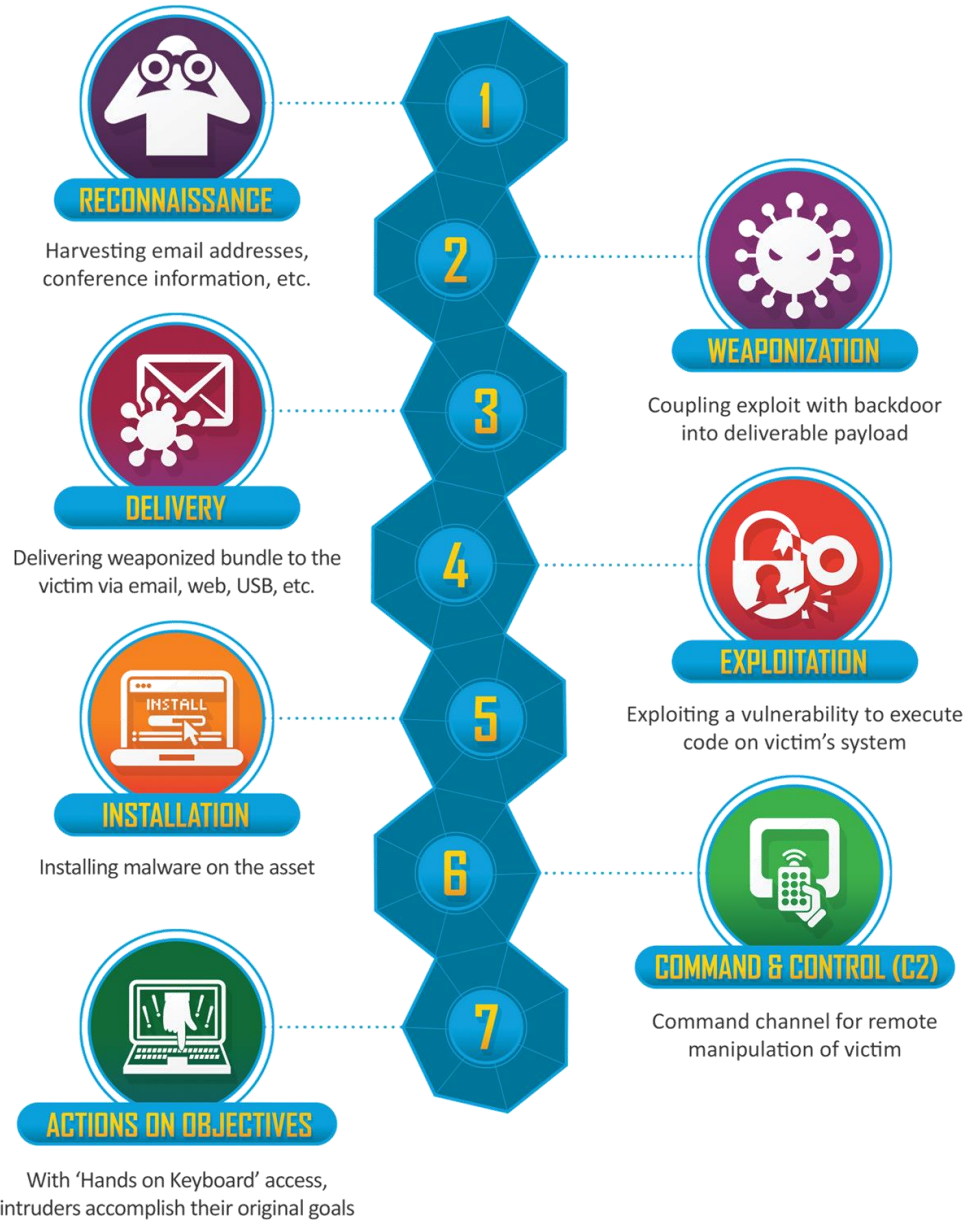
Overview (1/2)

The "cyber kill chain" is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it. It was developed by Lockheed Martin and consists on 7 diferent stages to compromised a specific taerget.

Each stage demonstrates a specific goal along the attacker's path in order to obtain leverage to move to the next phase

Designing your monitoring and response plan around the cyber kill chain model is an effective method because it focuses on how actual attacks happen.

In cyber kill chain cyber security model, the attack is stimulated from a hacker's perspective against your organization's existing security defense mechanism that is in place. While simulating an attack and identifying the flaws isn't the only factor to determine, rather the impact and extent of the detected security vulnerability is to be known as well. Also, when a vulnerability is detected then it is implying that your organisation's data is compromised.



https://www.alienvault.com/blogs/security-essentials/defend-like-an- attacker-applying-the-cyber-kill-chain

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

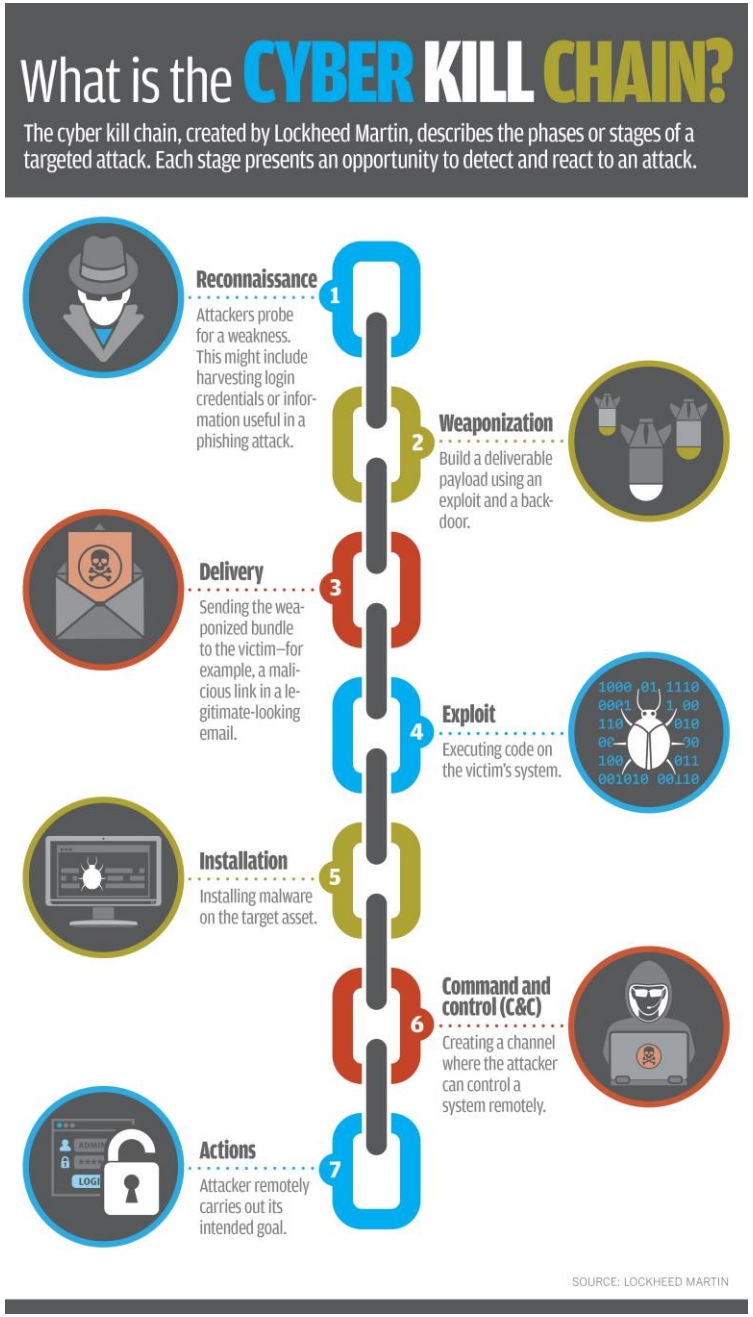
ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

"É vital que tenhamos sistemas seguros nos quais possamos confiar, não apenas evitando que números de cartão de crédito sejam roubados, mas nos protegendo de ataques maliciosos onde há hackers ou ataques de negação de serviço distribuída, você sabe o que é.

Seja um malware que infecta nossos computadores que rouba informações confidenciais ou possivelmente ameaça a infraestrutura crítica se entrar nos sistemas de TI do hospital, os pacientes podem morrer, se entrar em nosso sistema de energia, nossa rede elétrica pode ser derrubada, se entrar nosso sistema aeroportuário, podemos ter um problema muito sério. " diz o senhor Lee Hsien Loong, o primeiro-ministro de Singapura.

Overview (2/2)

The "cyber kill chain" in. infographics



https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain
https://phoenixnap.com/blog/cyber-kill-chain

The Cyber Kill Chain model by Lockheed Martin describes how attackers use the cycle of compromise, persistence and ex filtration against an organization.

Defense strategies that focus exclusively on the perimeter and on prevention do not take into account the kill chain life cycle approach; this is a reason why attackers are continuing to be so successful.

Defending against persistent and advanced threats requires methods that detect and deny threats at each stage of the kill chain.

PHASE 1 - Reconnaissance

What are reconnaissance attacks?

A *reconnaissance attack,* as the name implies, is **the efforts of an threat actors to gain as much information about the network as possible before launching other more serious types of attacks**. Quite often, the reconnaissance attack is implemented by using readily available information.

What is the objective?

Reconnaissance Attacker will focus on "who", or the network: "Who" will **likely focus on privileged individuals (either for system access, or access to confidential data "Network" will focus on architecture and layout; tools, devices and protocols; and critical infrastructure.** It is like a robber understanding the behaviour of the victim and breaking into the victim's house.

Hackers initiate a **search through the Internet to find possible email ids, social media accounts, any high-level conference attendees list to get a plausible target.** It is easier to assume that such searches cannot be protected. The hackers **succeeded in getting information on their target via the Internet is mainly because of the poor security reasons**. The reconnaissance phase can be reduced when the attack surface is less. And **reducing your organization's risk to exposure can very well hinder hacker's advances**.

"**The problem with social media is that people have an inherent trust**," explains Mark James, security specialist with IT security firm ESET. "And that is what is being tapped into by those cybercriminals."

Types of reconnaissance attack:

1- Passive reconnaissance
Definition: A hacker looks for information not related to victim domain. He just knows the registered domain to the target system so he can use commands (eg. Telephone directory) to fish information about the target

2 - Active reconnaissance
Definition:A hacker uses system information to gain unauthorized access to protected digital or electronic materials, and may go around routers or even firewalls to get it.

http://itsecurity.telelink.com/reconnaissance/

https://www.techopedia.com/definition/3650/active-reconnaissance

PHASE 2 - Weaponization

"**Hackers used hundreds of thousands of internet-connected devices that had previously been infected with a malicious code – known as a "botnet"** or, jokingly, a "zombie army" – to force an especially potent distributed denial of service (DDoS) attack." The Guardian reports.

What are the more well-known cyber weapons?

- **Botnet**
  A network of computers forced to work together on the command of an unauthorized remote user. This network of robot computers is used to attack other systems.
- **DDOS**
  Distributed Denial of Service attacks is where a computer system or network is flooded with data traffic, so much that the system can't handle the volume of requests and the system or network shuts down.
- **Malware**
  Malicious software is injected into a system or network to do things the owner would not want done. Examples include: Logic bombs, worms, viruses, packet sniffers (eavesdropping on a network).

https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault
https://sites.google.com/site/uscyberwar/cyber-weapons

The attacker team found a weak point in the system and knows how to create an entry point. The criminal team now designs a virus or a worm to target the weakness.

If attackers found a zero-day exploit, they typically work fast before the victim discovers and fixes the vulnerability.

Once malware is ready, hackers typically place malicious software in ordinary documents such as a PDF or an Office file.

Defensive measures for the weaponization stage:

- Run security awareness training to help employees recognize weaponization tests.
- Analyze malware artifacts to check for suspicious timelines and similarities.
- Build detection tools for weaponizers (automated tools that couple malicious software with exploits).

PHASE 3 - Delivery

"In a drive-by download attack, your browser loads the attacker's infected ad. Network-based antivirus protection on your perimeter **can often block malicious JavaScript before it reaches the client**."

What is delivery?

Attacker sends malicious payload to the victim by means such as email, which is only one of the numerous intrusion methods the attacker can use. There are over 100 delivery methods possible.

Objective:

Attackers launch their intrusion (weapons developed in the previous step)

Two basic methods:

- Adversary-controlled delivery, which involves **direct hacking into an open port**
- Adversary-released delivery, which **conveys the malware to the target through phishing**

Criminals launch the attack into the target environment. The infection methods vary, but the most common techniques are:

- Phishing attacks.
- Infected USB devices.
- Exploiting a hardware or software flaw.
- Compromised user accounts.
- A drive-by download that installs malware alongside a regular program.
- Direct hacking through an open port or other external access point.

The goal of this step is to breach the system and silently establish a foothold. A popular tactic is to launch a simultaneous DDoS attack to distract the defenders and infect the network without alarming security controls.

Defensive measures for the delivery stage:

- Protect from phishing attacks.
- Use patch management tools.
- Flag and investigate changes to files and folders with file integrity monitoring (FIM).
- Monitor for strange user behavior such as odd login times or locations.
- Run penetration tests to identify risks and weak points proactively.

https://www.alertlogic.com/blog/the-cyber-kill-chain-understanding-advanced-persistent-threats-d88/

https://www.alertlogic.com/resources/videos/the-cyber-kill-chain-in-more-detail/

https://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952

PHASE 4 - Exploitation

"Ransomware **victims are always advised not to pay the ransom to get their files back because it encourages the attackers.** The best way to mitigate damage from ransomware is to update operating systems and backup data. " - CNN

Once attackers have identified a vulnerability in your system, they exploit the weakness and carry out their attack.

During the exploitation phase of the attack, the host machine is compromised by the attacker and the delivery mechanism typically will take one of two actions:

- Install malware (a dropper) allowing attacker command execution.
- Install malware (a downloader) and download additional malware from the Internet, allowing attacker command execution.

Once a foothold is established inside the network, the attacker will typically download additional tools, attempt privilege escalation, extract password hashes, etc.

After delivery to the user, computer or device, the malicious payload will compromise the asset, thereby gaining a foothold in the environment.

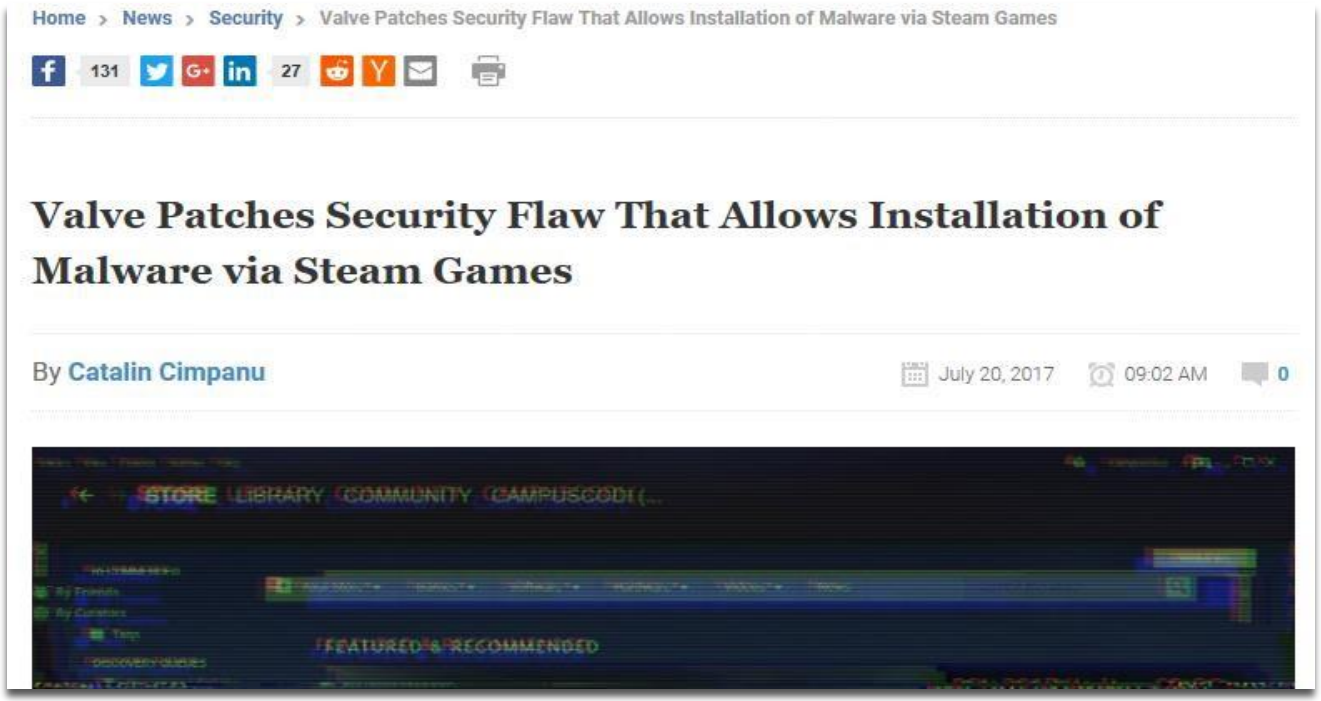
This is usually by exploiting a known vulnerability for which a patch has been made previously available.
While zero-day exploitation does occur, depending of the victim, in a majority of cases it is not necessary for adversaries to go to this expense.

http://money.cnn.com/2017/06/27/technology/hacking-petya-europe-ukraine-wpp-rosneft/index.html

When the security vulnerabilities are detected in your system, this phase is where the cyber-attack is performed. Hackers exploit the vulnerabilities and weak points in your organization's systems.

The aim of this phase is to gain unauthorised access and expose the security flaws to hackers' advantage.

PHASE 5 - Installation



"A vulnerability in Valve's Source SDK, a library used by game vendors to support custom mods and other features, **allows a malicious actor to execute code on a user's computer, and optionally install malware**, such as ransomware, cryptocurrency miners, banking trojans, and others."

What are the other possible malwares? Possible malwares include ransomware and remote-access Trojans and other unwanted applications.

Installation of either a web shell on a compromised web server or a backdoor implant on a compromised computer system enables adversaries to bypass security controls and maintain access in the victim's environment.

Once the exploitation of the system has been successful, the APT malware code will install itself onto the targeted information system. At this point, the APT malware will begin to download additional software if network access is available. This allows the delivery payload to remain small and undetectable.

The small size of the malware in this example would have limited functionality. Therefore, the APT will download additional components to have better control of the exploited information systems and to penetrate further into the target organization's network.

https://www.bleepingcomputer.com/news/security/valve-patches-security-flaw-that-allows-installation-of-malware-via-steam-games/

This often takes the form of something that communicates actively with external parties. The malware is usually stealthy in its operation, gaining persistence at the endpoints where it has able to access.

The adversary can then control this application without alerting the organization. Intruders move laterally to other systems and accounts on the network. The goal is to gain higher permissions and reach more data.

Standard techniques during this stage are:
- Exploiting password vulnerabilities.
- Brute force attacks.
- Credential extraction.
- Targeting further system vulnerabilities.

Defensive measures for the lateral movement stage:
- Implement Zero Trust security to limit the reach of compromised accounts and programs.
- Use network segmentation to isolate individual systems.
- Eliminate the use of shared accounts.
- Enforce password security best practices.
- Audit all suspicious activities of privileged users.

PHASE 6 - Command and Control

What is it?

Ransomware uses command and control connections to download encryption keys before hijacking your files.

For example, remote-access Trojans open a command and control connection to allow remote access to your system.

This **allows persistent connectivity for continued access to the environment** as well as a detective measure for defender activity.

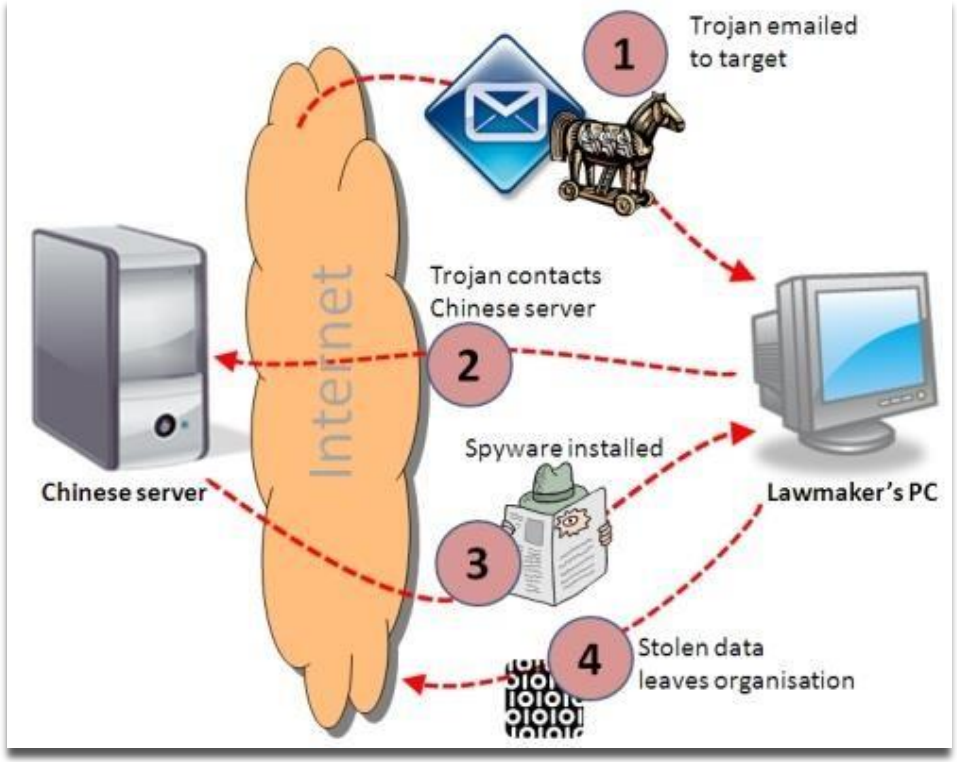
How is it done?

Command and control of a **compromised resource is usually accomplished via a beacon over an allowed path out of the network.**

Beacons take many forms, but in most cases they tend to be:

- HTTP or HTTPS-based
- Made to look like benign traffic via falsified HTTP headers

In cases that use encrypted communication, beacons tend to use self-signed certificates or use custom encryption over an allowed path



In this phase, adversaries have control of assets within the target organization through methods of control (often remote), such as DNS, Internet Control Message Protocol (ICMP), websites and social networks. This channel is how the adversary tells the controlled "asset" what to do next and what information to gather.

The methods used to gather data under command include screen captures, key stroke monitoring, password cracking, network monitoring for credentials, gathering of sensitive content and documents. Often a staging host is identified to which all internal data is copied, then compressed and/or encrypted and made ready for exfiltration.

https://www.beyondtrust.com/resources/glossary/cyber-attack-chain

Command and control is the sixth phase of the cyber kill chain.

Command and control, also known as C2, is when the attacker has put in place their management and communication APT code onto to the target network. T

his software allows the attacker to fully manage the APT code in the environment and allows the attacker to move deeper into the network, exfiltrate data and conduct destruction or denial of service operations.

This implies that once a system is compromised and/or infected, the system has to call home to a Command and Control (C&C) system for the cyber attacker to gain control. This is why 'hunting' has become so popular. They're looking for abnormal outbound activities like this.

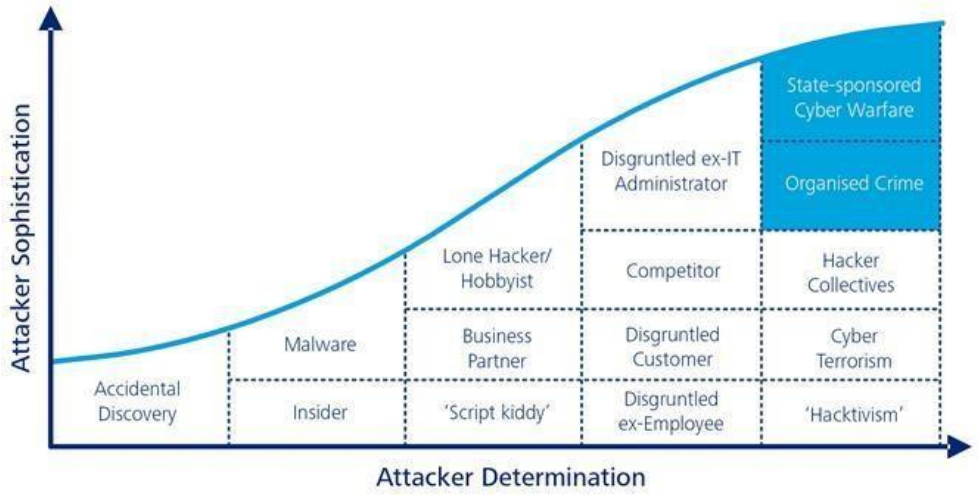
PHASE 7 – Actions on Objectives

What does "Action" mean in cyber terms?

Action refers to the how the attacker accomplish his final goal.

The attacker's final goal could be anything from extracting a ransom from you in exchange for decrypting your files to exfiltrating customer information out of the network. In the latter example, data-loss prevention solutions can stop exfiltration before the data leaves your network. In other attacks, endpoint agent software can identify activity that deviates from established baselines and notify IT that something is amiss.

This is the elaborate active attack process that can take months, and thousands of small steps, in order to achieve.




ABC NEWS

Just In | Australia | World | Business | Sport | Science | Arts | Analysis | Fact Che

Print | Email | Facebook | Twitter | More

Ransomware cyberattack hits Australia as EU warns victims worldwide may grow

Updated 15 May 2017, 6:56am

More Australians could find they have become victims of a massive global cyber attack when they turn on their computers this morning, the Federal Government is warning.

The attack, which locks computers and holds users' files for ransom, hit 200,000 victims in 150 countries over the weekend.

"What we are seeing is the exact same features that have occurred overseas: a **freezing of their IT systems and a ransomware note."** said Dan Tehan

Mr Tehan said the attacks were on small- to medium-sized private sector businesses and that government departments had been told to ensure they were protected.

The actions and objectives of the APT are dependent on its specific mission. The APT could be focused on data exfiltration, denial of service or destruction.

In the case of data exfiltration, the APT may be interested in organizational proprietary data such as engineering designs or employee and customer Personally Identifiable Information (PII). In the case of a denial of service, like the Ukrainian power outage of December 2015,the APT may disable a key component of the organization's infrastructure to temporarily disrupt services.

Finally, in the case of destruction, an APT like the Stuxnet worm may seek to operate industrial control systems outside of their manufacturer specifications, resulting in catastrophic failure.

http://www.abc.net.au/news/2017-05- 14/ransomware-cyberattack-threat-lingers-as-people-return-to-work/8525554

http://www.darkreading.com/attacks-breaches/a-twist-on-the- cyber-kill-chain-defending-against-a-javascript-malware- attack/a/d-id/1326952

This final phase covers how the adversary exfiltrates data and/ or damages IT assets while concurrently dwell time in an organization. Then measures are taken to identify more targets, expand their footprint within an organization and -most critical of all-exfiltrate data.

The CKC is then repeated. In fact, a critical point with the CKC is that it is circular, and not linear. Once an adversary enters in the network, he starts again with the CKC in the network, with doing more reconnaissance and making lateral movement inside of your network.

In addition, it is necessary to keep in mind that while the methodology is the same, adversaries will use different methods for steps of the internal kill chain once inside, versus being outside the environment.

In fact, once the attacker is inside the network, it becomes an insider, a user with privileges and persistence, and this prevents the organization's security teams from suspecting the attack and realizing that it is already in the advanced stages of the extended model of the Cyber-Kill Chain

Will Kill Chain Tactics work for your Organization?

It is recommended that an organization implement a **defense-in-depth strategy** that will serve to protect the organization's people, process, and technology in a holistic and layered fashion. Some defense-in-depth areas include:

- Implementation of an enterprise-wide information security program with the leadership backing and authority
- Effective user training and awareness related to email-borne threats (phishing)
- Strong cyber hygiene practices throughout the organization.

If you don't already have security and visibility built into your corporate environment, this may seem like an impossible hill to climb. But **implementing a Cyber Kill Chain doesn't have to be done overnight**. Take smaller measures, completing stages as you are able. **Do a check of your web presence to see what information it could give an attacker**. Have **each of your sites do an inventory of all computers so you can update them** all. **Implement layered security to decrease the possibility that threats will slip through unnoticed. Create a policy for dealing with malware events. Educate your staff about what to do with unexpected, suspicious emails.**

While not a security tool or mechanism, a kill chain helps select the right strategies and technologies to stop attacks at different stages. Use a kill chain as a base for an effective security strategy and continue to grow your company without worrying about costly setbacks.

http://resources.infosecinstitute.com/cyber-kill-chain-is-a-great-idea-but-is-it-something-your-company-can-implement/#gref

ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

The Cyber Kill Chain model demonstrates a hack – to gain unauthorised access to data or assets inside your organization's security perimeter. The attacker performs reconnaissance, the intrusion of the security perimeter, exploitation of your security vulnerabilities, gaining and escalating privileges, lateral movement to gain access to more sensitive data, attempts to obfuscate their activity, and finally, exfiltrate data from the organization.

The only way to protect what you've worked hard to build is to be vigilant when it comes to cybersecurity. If you'd like to know more about how your business can benefit from managed services, just give us a call, we are here to help.

cyber kill chain is used to demonstrate each and every stage of a successful cyberattack. It is an end-to-end procedure to demonstrate a hacker's footprint.