

**7 Stages of Cyber Kill Chain  
Supplementary Reading**



# Overview

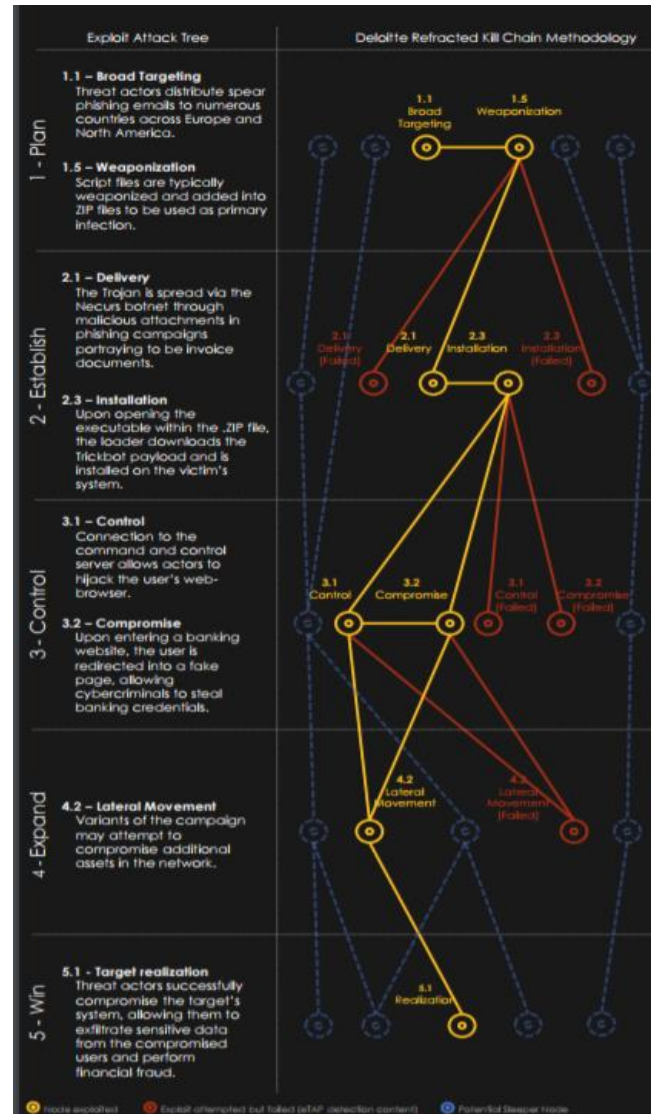
The “[cyber kill chain](#)” is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it.

Each stage demonstrates a specific goal along the attacker’s path.

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



<https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-thought-leadership-noexp.pdf>  
<https://www.alienvault.com/blogs/security-essentials/defend-like-an-attacker-applying-the-cyber-kill-chain>



**“It is vital that we have secure systems that we can trust, not just preventing credit card numbers from being stolen, but protecting ourselves from malicious attacks where there is hacking or Distributed Denial of Service attacks, you know what that is.**

Whether is it malware that infects our computers which steals sensitive information or possibly threatens critical infrastructure if it gets into the hospital IT systems, patients can die, if it gets into our power system, our power grid can be brought down, if it gets into our airport system, we can have a very serious problem.” says Mr. Lee Hsien Loong, the Prime Minister of Singapore.

# 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.

Types of reconnaissance attack:

- **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
- **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>



The screenshot shows the top portion of a BBC News article. The BBC logo is in the top left, followed by navigation links for News, Sport, Weather, Shop, Earth, and Travel. Below this is a red 'NEWS' banner with sub-links for Home, Video, World, Asia, UK, Business, Tech, Science, Magazine, and Entertainment. A secondary navigation bar includes Business, Market Data, Markets, Global Trade, Companies, Entrepreneurship, and Tech. The main article title is 'Social Media: A hunting ground for cybercriminals' by Andreas Illmer, a Technology of Business reporter, dated 26 July 2016. Social sharing icons for Facebook, Twitter, and Email are visible.



Do you ever hesitate to click on a post shared by a friend on Facebook? Not because it's a boring picture of their dinner, but because you're suspicious it might not actually have been posted by them?

Technology of Business

Has the time now come

**"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."

# Weaponization



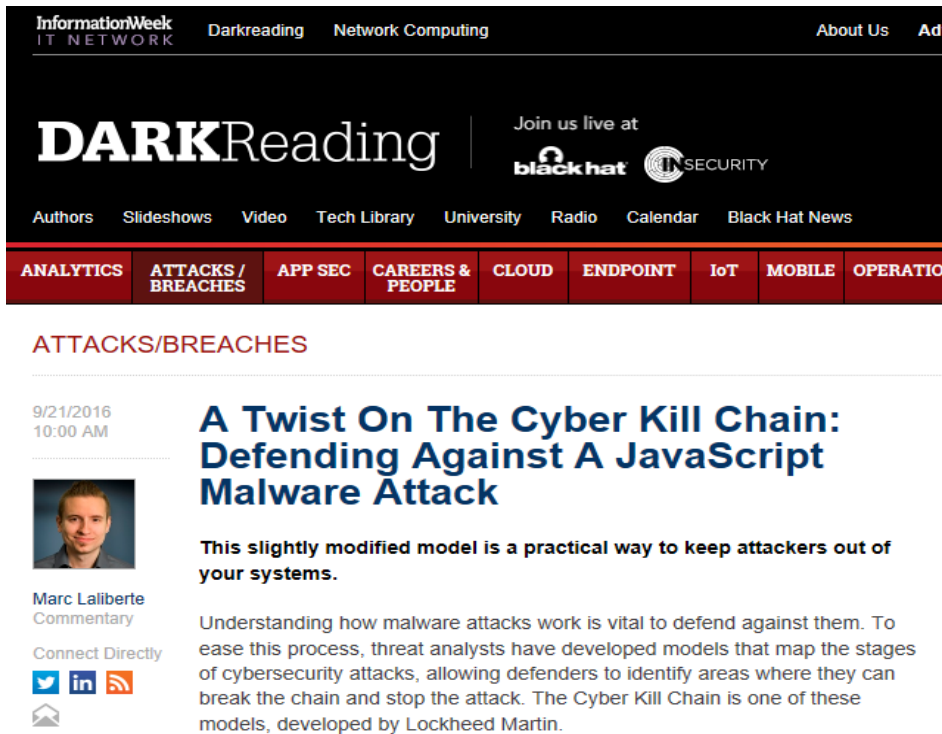
“Hackers used hundreds of thousands of internet-connected devices that had previously been infected with a malicious code – [known as a “botnet”](#) or, jokingly, a “zombie army” – to force an especially potent distributed denial of service (DDoS) attack.” The Guardian reports.

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/uscyperwar/cyber-weapons>





The screenshot shows the DarkReading website interface. At the top, there's a navigation bar with 'InformationWeek IT NETWORK', 'Darkreading', 'Network Computing', 'About Us', and 'Ad'. Below that, the 'DARKReading' logo is prominent, along with 'Join us live at blackhat INSECURITY'. A secondary navigation bar includes 'Authors', 'Slideshows', 'Video', 'Tech Library', 'University', 'Radio', 'Calendar', and 'Black Hat News'. A red navigation bar at the bottom lists categories: 'ANALYTICS', 'ATTACKS / BREACHES', 'APP SEC', 'CAREERS & PEOPLE', 'CLOUD', 'ENDPOINT', 'IoT', 'MOBILE', and 'OPERATIO'. The main content area features the article title 'A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack' dated 9/21/2016 at 10:00 AM. The author is Marc Laliberte, and the article is a commentary. A short summary states: 'This slightly modified model is a practical way to keep attackers out of your systems.' The main text begins with 'Understanding how malware attacks work is vital to defend against them. To ease this process, threat analysts have developed models that map the stages of cybersecurity attacks, allowing defenders to identify areas where they can break the chain and stop the attack. The Cyber Kill Chain is one of these models, developed by Lockheed Martin.'

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**

“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.**”

<https://www.alertlogic.com/blog/the-cyber-kill-chain-understanding-advanced-persistent-threats/>  
<http://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952>

# Exploitation

 tech

BUSINESS

CULTURE

GADGETS

FUTURE

STARTUPS

Hackers launched blistering ransomware attacks Tuesday against companies and agencies across the world, particularly targeting Ukrainian businesses.

**"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.

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

# 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.

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

# 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?

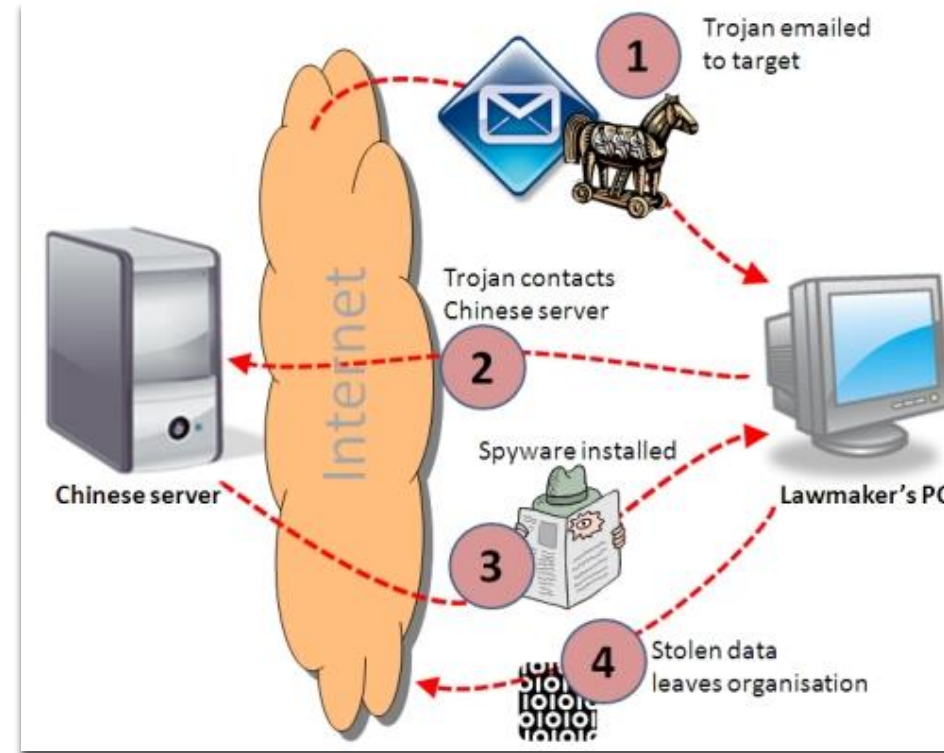
Command and control of a **compromised resource is usually accomplished via a beacon over an allowed path out of the network.**

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

<https://blogs.rsa.com/stalking-the-kill-chain-the-attackers-chain-2/>





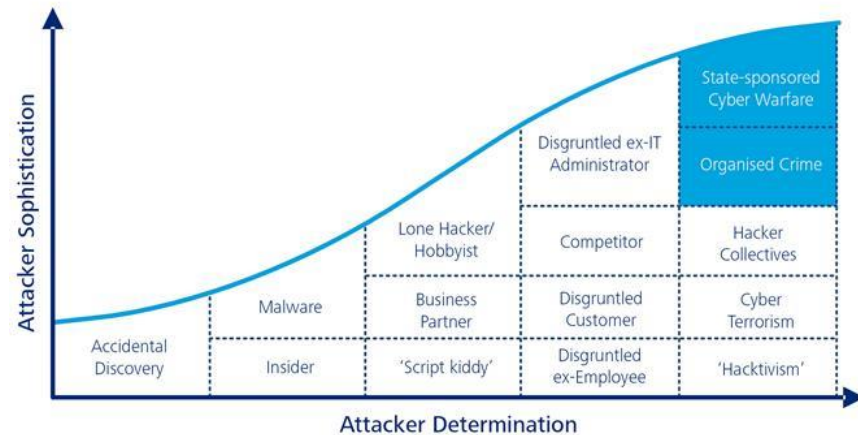
# Actions

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.



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



"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.

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

# Will Kill Chain Tactics work for your 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**.

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



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 244,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.