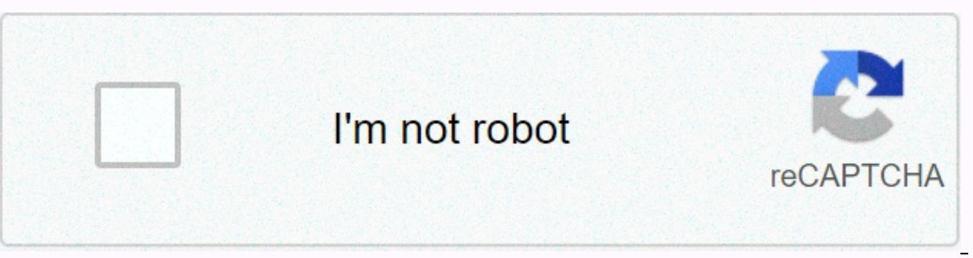
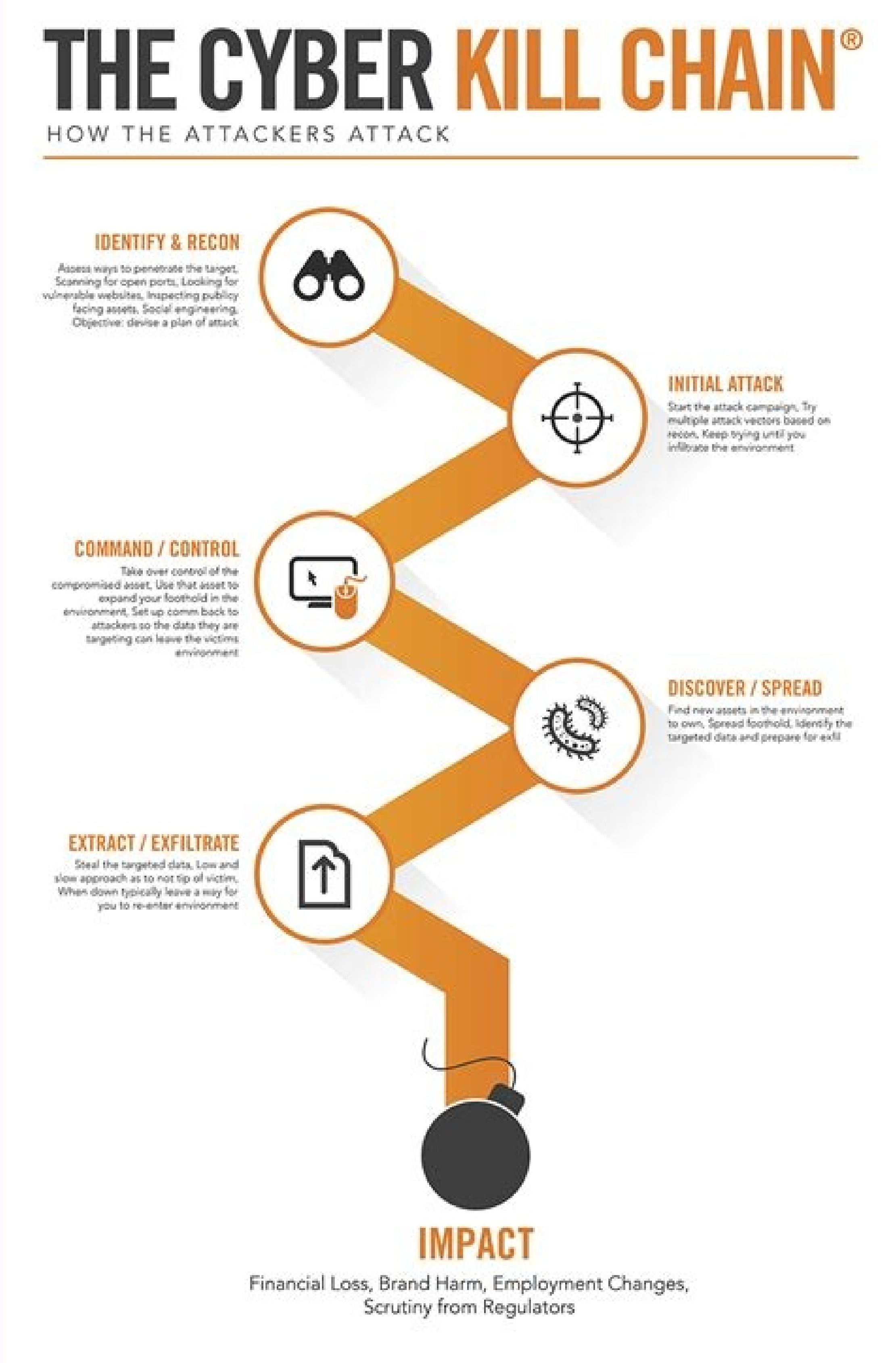


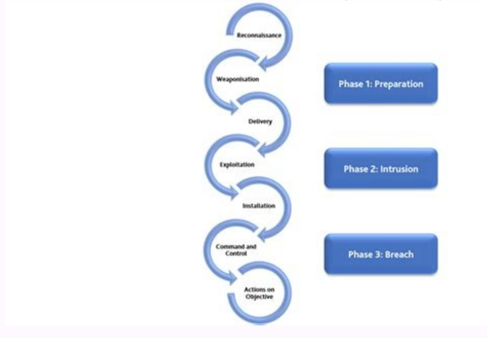
□ I'm not robot

# Lockheed martin kill chain pdf

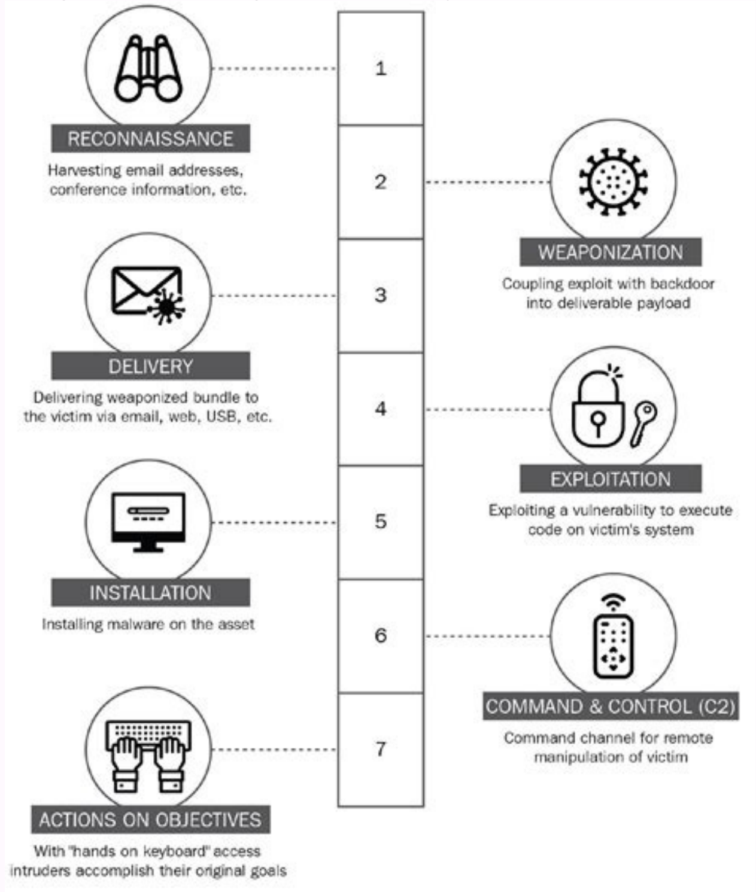
The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data.
The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).


THE CYBER KILL CHAIN®
HOW THE ATTACKERS ATTACK
IDENTIFY & RECON
Assess ways to penetrate the target, Scanning for open ports, Looking for vulnerable websites, Inspecting publicy facing assets, Social engineering, Objective: devise a plan of attack
INITIAL ATTACK
Start the attack campaign, Try multiple attack vectors based on recon, Keep trying until you infiltrate the environment
COMMAND / CONTROL
Take over control of the compromised asset, Use that asset to expand your foothold in the environment, Set up comm back to attackers so the data they are targeting can leave the victims environment
DISCOVER / SPREAD
Find new assets in the environment to own, Spread foothold, Identify the targeted data and prepare for exfil
EXTRACT / EXFILTRATE
Steal the targeted data, Low and slow approach as to not tip of victim, When down typically leave a way for you to re-enter environment
IMPACT
Financial Loss, Brand Harm, Employment Changes, Scrutiny from Regulators

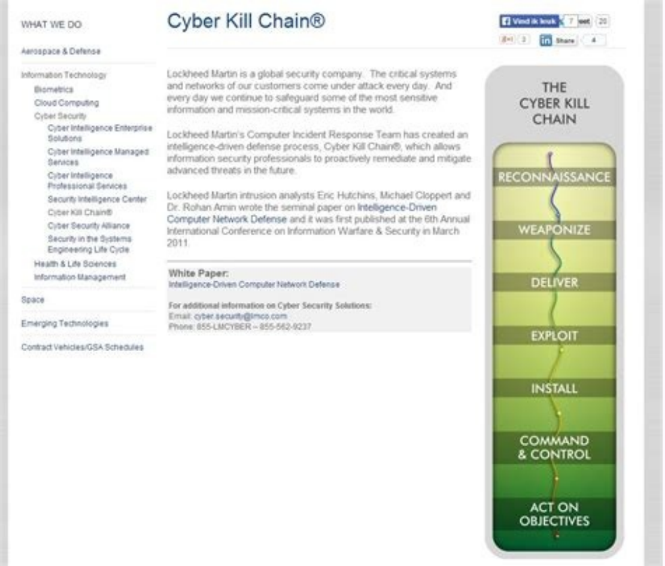
Lockheed Martin derived the kill chain framework from a military model – originally established to identify, prepare to attack, engage, and destroy the target. Since its inception, the kill chain has evolved to better anticipate and recognize insider threats, social engineering, advanced ransomware, and innovative attacks. Let's discuss each step in the kill chain in detail. Campaign Design We have made a lot of assumptions about the security posture of Evil Corp to better describe things.



The attack campaign must be designed carefully and in a stepwise manner so that finer details can be taken into account. In this article, I will be using the popular Lockheed Martin Cyber Kill Chain (CKC) methodology to craft my attack process against Evil Corp. The general workflow is depicted in the figure given below.
Reconnaissance This is the initial and the most important step that must be performed patiently for better output. regrouping worksheets year 3 Here, we will collect the information about the target as much as possible using Open Source Intelligence (OSINT) that includes company presence in social media, target mailing lists, and identifying open ports using active recon tools like Nmap or masscan. The more you can collect with reconnaissance, the higher will be the chance of successful penetration into the target environment. Using tools like Shodan and theHarvester, we can easily collect emails of the employees and analyze the naming scheme. If the naming scheme is known e.g jsmith@evilvcorp.com for John Smith.
We can easily extend the mailing lists using this scheme and the company employees list which will be later used in the Delivery stage for phishing. We can also try password spraying to the collected email lists using the data breaches credentials and see if we can get a hit. Due to the password reuse behaviors of people, this is likely to have a successful result. Weaponization This is the stage of crafting the malicious payloads that will actually execute inside the target workstations and everything must be done in a stealthy manner so that we don't get caught. We need to disguise our malware in benign-looking payloads like PDFs, Word documents, or ZIP files. In the case of our malware, it will be using the EternalBlue exploit at its core. I am pretty confident that this exploit will work because it uses SMB (samba in case of Linux) protocol to spread across the network and is pretty quiet. Since over 600 workstations of Evil Corp are directly connected with switches only, there must be a system in place for files and printer sharing that will definitely use this popular SMB protocol (port 139 and 445). Moreover, 10% of the system runs on Windows XP (windows support already ended) and most of them are still running Windows 7 that haven't got security updates due to firewall issues, we have a good chance that our payload will work. We will wrap this payload inside the SFX file with the .exe extension which is a self-extracting archive. So once the victim downloads the attachment in the email, the archive will automatically be extracted and the payload will be injected into the victim workstations. Delivery No matter how state-of-the-art the malware is if there is not any way to deliver the payload to the target. We will be using spear-phishing as our delivery mechanism since we have already harvested enough employee emails from the reconnaissance stage. Targeting a single victim won't work in our case since there is diversified use of operating systems and we won't know who is running the machine that is vulnerable to EternalBlue.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With "hands on keyboard" access intruders accomplish their original goals

The malicious email is depicted below. We will disguise ourselves as the IT team and send phishing emails concerning the company's security. gifuwolegokipifobokaf.pdf
We will make the victims believe that there have been malware infections inside the organization and they need to work together to make Evil Corp secure. The company's logo is also included to make them feel at home. And the red banner is sure to catch the attention of the victims. The loyal employee will surely feel his/her responsibility to protect the organization from any dangers by downloading the patch. The SFX will automatically extract itself and inject the EternalBlue into the system making our delivery stage successful. Exploitation After successful delivery, malware needs to find a way to launch itself on the victim machine. It will look for the vulnerability in the SMB protocol (139 and 445 ports) to exploit the system. corinna kopf only.fans leak The infected host will spread out the malware into the whole network using this protocol since every host will be listening to file shares and printing information all the time. If found, then comes the installation stage where the malware will seek higher privileges in order to maintain persistence.



Cyber Kill Chain®

Lockheed Martin is a global security company. The critical systems and networks of our customers come under attack every day. And every day we continue to safeguard some of the most sensitive information and mission-critical systems in the world.

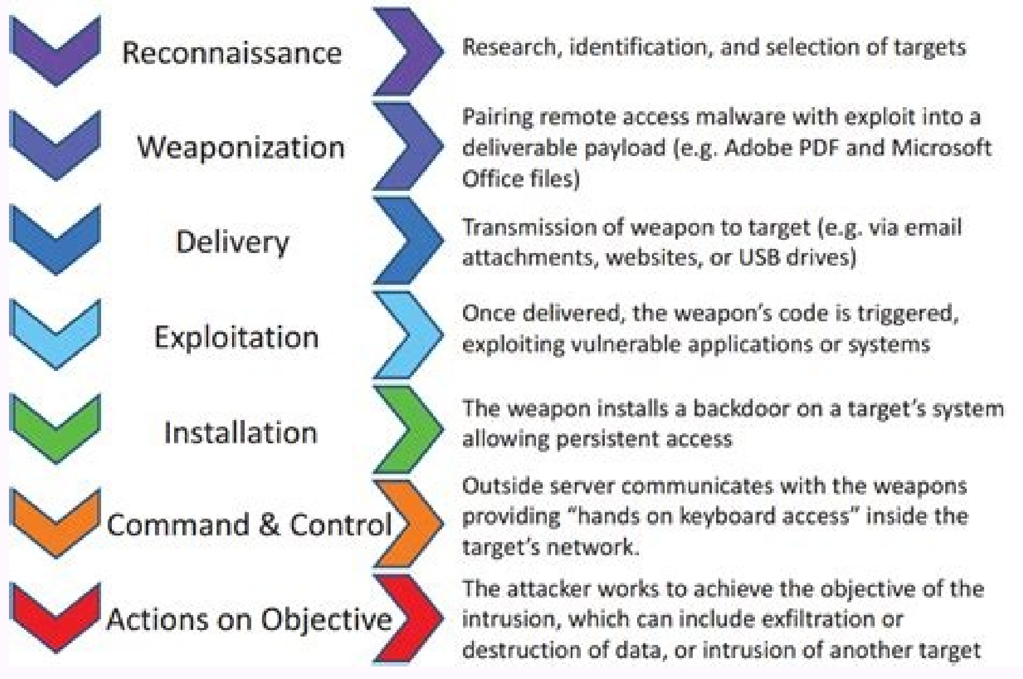
Lockheed Martin's Computer Incident Response Team has created an intelligence-driven defense process, Cyber Kill Chain®, which allows information security professionals to proactively remediate and mitigate advanced threats in the future.

Lockheed Martin intrusion analysts Eric Hutchins, Michael Cloppert and Dr. Rohan Amin wrote the seminal paper on Intelligence-Driven Computer Network Defense and it was first published at the 6th Annual International Conference on Information Warfare & Security in March 2011.

White Paper:
Intelligence-Driven Computer Network Defense

For additional information on Cyber Security Solutions:
Email: cyber.security@lmco.com
Phone: 855-LMCYBER – 855-562-9237

If the vulnerability is not found in that host, the malware will remain in the dormant stage listening to the further commands from the Command and Control System. hemnes daybed instruction manual
Installation Once the penetration to the network is successful, things won't stop here. We must seek for ways to stabilize our malware and maintain a thorough persistence on the system so that the malware will survive even after reboot. We will transplant our malware inside the stable background service processes so that connection to C2 will remain at any conditions. Also, local enumeration will be done inside the Windows system to find any possible privilege escalations (lateral or vertical). Along with the exploitation, the malware will give back a meterpreter session (reverse shell) to us for further commanding. This gives us as an attacker the ability to control the whole flow from a centralized system. Command and Control For effective communication with the malware and exfiltrating the confidential data out of the target, we need a centralized commanding server. Since our payload will give back us a reverse shell, there won't be a problem creating a connection. But generally using a hardcoded IP address for the C2 server is bad practice since it could be easily blacklisted if suspected. In this case, our malware will use Domain Generation Algorithm (DGA) which will generate random domain names that are associated with a live C2 server. So that the domain blacklisting approach won't work since the IT team won't know what to block in advance. Action on objectives This is the strategic part of the campaign and all the previous steps were executed with the motivation of reaching this stage. The main objective for this attack is to exfiltrate the business data and the employee's credentials so that we can create a huge business impact on Evil Corp potentially taking down the whole company. ilber ortayl? turklerin tarihi pdf oku Founder of cybersecnerds.com. baringo_county_bursary_form.pdf
Electronics Engineer by profession, Security Engineer by passion. I am a Linux Enthusiast and highly interested in the offensive side of the CyberSec industry. You will find me reading InfoSec blogs most of the time. Military concept for attack sequence This article is about the military and information security concept. For 2019 film, see Kill Chain (film). For the television episode, see NCIS (season 11) § ep246. The term kill chain is a military concept which identifies the structure of an attack. It consists of: identification of target[citation needed] dispatching of forces to target[citation needed] initiation of attack on target[citation needed] destruction of target[citation needed][1] Conversely, the idea of "breaking" an opponent's kill chain is a method of defense or preemptive action.[2] Military F2T2EA One military kill chain model is the "F2T2EA", which includes the following phases: Find: Identify a target.


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

Find a target within surveillance or reconnaissance data or via intelligence means. Fix: Fix the target's location. Obtain specific coordinates for the target either from existing data or by collecting additional data. Track: Monitor the target's movement. Keep track of the target until either a decision is made not to engage the target or the target is successfully engaged. Target: Select an appropriate weapon or asset to use on the target to create desired effects. Apply command and control capabilities to assess the value of the target and the availability of appropriate weapons to engage it. Engage: Apply the weapon to the target. Assess: Evaluate effects of the attack, including any intelligence gathered at the location.

This is an integrated, end-to-end process described as a "chain" because an interruption at any stage can interrupt the entire process.[3][4] Previous terminology The "Four Fs" is a military term used in the United States military, especially during World War II.[citation needed] Designed to be easy to remember, the "Four Fs" are as follows: Find the enemy – Locate the enemy. Fix the enemy – Pin them down with suppressing fire. Fight the enemy – Engage the enemy in combat or flank the enemy – Send soldiers to the enemy's sides or rear.

Finish the enemy – Eliminate all enemy combatants.[citation needed] Proposed terminology The "Five Fs" is a military term described by Maj. Mike "Pako" Benitez, an F-15E Strike Eagle Weapons Systems Officer who served in the United States Air Force and the United States Marine Corps. Designed to update the Kill Chain to reflect updated, autonomous and semi-autonomous weapon systems, the "Five Fs" are described in "It's About Time: The Pressing Need to Evolve the Kill Chain"[5] as follows: Find encapsulates the unity of effort of Joint Intelligence Preparation of the Operating Environment, matching collection assets to commander's intent and targeted areas of interest. This inevitably leads to detections, which may be further classified as an emerging target if it meets the intent. Fix is doctrinally described as "identifying an emerging target as worthy of engagement and determines its position and other data with sufficient fidelity to permit engagement." Fire involves committing forces or resources (i.e., releasing a munition, payload, or expendable) Finish involves employment with strike approval authorities (i.e., striking a target/firing directed energy/destructive electronic attack). This is similar to a ground element executing maneuvers to contact but then adhering to prescribed rules of engagement once arriving at the point of friction. Feedback closes the operational OODA Loop with an evaluative step, in some circumstances referred to as "Bomb Damage Assessment".

North Korean nuclear capability A new American military contingency plan called "Kill Chain" is reportedly the first step in a new strategy to use satellite imagery to identify North Korean launch sites, nuclear facilities and manufacturing capability and destroy them pre-emptively if a conflict seems imminent.

The plan was mentioned in a joint statement by the United States and South Korea.[6][7] Cyber Intrusion kill chain for information security[8] Attack phases and countermeasures More recently, Lockheed Martin adapted this concept to information security, using it as a method for modeling intrusions on a computer network.[9] The cyber kill chain model has seen some adoption in the information security community.[10] However, acceptance is not universal, with critics pointing to what they believe are fundamental flaws in the model.[11] Computer scientists at Lockheed-Martin corporation described a new "intrusion kill chain" framework or model to defend computer networks in 2011.[3] They wrote that attacks may occur in phases and can be disrupted through controls established at each phase. Since then, the "cyber kill chain" has been adopted by data security organizations to define phases of cyberattacks.[12] A cyber kill chain reveals the phases of a cyberattack: from early reconnaissance to the goal of data exfiltration.[13] The kill chain can also be used as a management tool to help continuously improve network defense.

According to Lockheed Martin, threats must progress through several phases in the model, including: Reconnaissance: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network. Weaponization: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities. Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives) Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability. until dawn character traits template Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder. Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network. Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom. Defensive courses of action can be taken against these phases:[14] Detect: Determine whether an intruder is present. Deny: Prevent information disclosure and unauthorized access. Disrupt: Stop or change outbound traffic (to attacker). hydrology by sk garg pdf

Degrade: Counter-attack command and control. Deceive: Interfere with command and control. Contain: Network segmentation changes A U.S. Senate investigation of the 2013 Target Corporation data breach included analysis based on the Lockheed-Martin kill chain framework.

It identified several stages where controls did not prevent or detect progression of the attack.[8] Alternatives Different organizations have constructed their own kill chains to try to model different threats. FireEye proposes a linear model similar to Lockheed-Martin's. In FireEye's kill chain the persistence of threats is emphasized. This model stresses that a threat does not end after one cycle.[15] Reconnaissance Initial intrusion into the network Establish a backdoor into the network. Obtain user credentials.

Install various utilities. Privilege escalation/ lateral movement/ data exfiltration Maintain persistence. Critiques Among the critiques of Lockheed Martin's cyber kill chain model as threat assessment and prevention tool is that the first phases happen outside the defended network, making it difficult to identify or defend against actions in these phases.[16] Similarly, this methodology is said to reinforce traditional perimeter-based and malware-prevention based defensive strategies.[17] Others have noted that the traditional cyber kill chain isn't suitable to model the insider threat.[18] This is particularly troublesome given the likelihood of successful attacks that breach the internal network perimeter, which is why organizations "need to develop a strategy for dealing with attackers inside the firewall. They need to think of every attacker as [a] potential insider".[19] Unified kill chain The unified kill chain consists of 18 unique attack phases that can occur in advanced cyber attacks. The Unified Kill Chain was developed in 2017 by Paul Pols in collaboration with Fox-IT and Leiden University to overcome common critiques against the traditional cyber kill chain, by uniting and extending Lockheed Martin's kill chain and MITRE's ATT&CK framework. act 1 scene 2 julius caesar answers

The unified version of the kill chain is an ordered arrangement of 18 unique attack phases that may occur in end-to-end cyberattack, which covers activities that occur outside and within the defended network. As such, the unified kill chain improves over the scope limitations of the traditional kill chain and the time-agnostic nature of tactics in MITRE's ATT&CK. The unified model can be used to analyze, compare, and defend against end-to-end cyber attacks by advanced persistent threats (APTs).[20] A subsequent whitepaper on the unified kill chain was published in 2021.[21] References ^ "Kill Chain Approach". Chief of Naval Operations. April 23, 2013. Archived from the original on June 13, 2013. ^ Jonathan Greenert; Mark Welsh (May 17, 2013). "Breaking the Kill Chain". Foreign Policy. Retrieved June 30, 2016. ^ a b Lockheed-Martin Corporation-Hutchins, Cloppert, and Amin-Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains-2011 ^ John A. 7-17 sounds animals make worksheet Tirpak (July 1, 2000).

"Find, Fix, Track, Target, Engage, Assess". Air Force Magazine. ^ Benitez, Mike (May 17, 2017). "It's About Time: The Pressing Need to Evolve the Kill Chain". tecumseh ohh60 shaft size War on the Rocks. ps4 cannot find update file

Retrieved April 28, 2020. ^ Sanger, David E. (July 6, 2017).

"Tiny Satellites From Silicon Valley May Help Track North Korea Missiles". The New York Times. Retrieved July 7, 2017. ^ "06/30/17 - Joint Statement between the United States and the Republic of Korea | U.S. Embassy & Consulate in Korea". U.S. Embassy & Consulate in Korea. 2017-06-30. Retrieved 2017-07-07. ^ a b "U.S. Senate-Committee on Commerce, Science, and Transportation-A "Kill Chain" Analysis of the 2013 Target Data Breach-March 26, 2014" (PDF). 11054477294.pdf Archived from the original (PDF) on October 6, 2016. calculus early transcendentals 9th edition pdf ^ Higgins, Kelly Jackson (January 12, 2013). "How Lockheed Martin's 'Kill Chain' Stopped SecurID Attack". DARKReading. Retrieved June 30, 2016. ^ Mason, Sean (December 2, 2014). "Leveraging The Kill Chain For Awesome". DARKReading. Retrieved June 30, 2016. ^ Myers, Lysa (October 4, 2013). "The practicality of the Cyber Kill Chain approach to security". CSO Online. Retrieved June 30, 2016. ^ Greene, Tim (5 August 2016). "Why the 'cyber kill chain' needs an upgrade". Retrieved 2016-08-19. errorless biology book pdf free download

^ "The Cyber Kill Chain or: how I learned to stop worrying and love data breaches". 2016-06-20. Retrieved 2016-08-19. ^ John Franco.

"Cyber Defense Overview: Attack Patterns" (PDF). Archived (PDF) from the original on 2018-09-10. Retrieved 2017-05-15. ^ Kim, Hyeob; Kwon, HyukJun; Kim, Kyung Kyu (February 2019). "Modified cyber kill chain model for multimedia service environments". Multimedia Tools and Applications. 78 (3): 3153–3170. doi:10.1007/s11042-018-5897-5. ISSN 1380-7501. 53077588858.pdf ^ Laliberte, Marc (September 21, 2016). "A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack".

DARKReading. ^ Engel, Giora (November 18, 2014). "Deconstructing The Cyber Kill Chain". DARKReading. Retrieved June 30, 2016. ^ Reidy, Patrick. "Combating the Insider Threat at the FBI" (PDF). BlackHat USA 2013. ^ Devost, Matt (February 19, 2015). "Every Cyber Attacker is an Insider". OODA Loop. ^ Pols, Paul (December 7, 2017). "The Unified Kill Chain" (PDF). Cyber Security Academy. ^ Pols, Paul (May 17, 2021). "The Unified Kill Chain". worcester 24i junior timer manual UnifiedKillChain.com. Retrieved from "