The Cyber Kill Chain
Employing Offensive Response Actions

Abstract

Working in Cyberspace Operations from multiple aspects has led me to question the multiple methods and frameworks used to defend enterprises. This has also led to an effort of integrating military operational frameworks where focuses remain on small, yet focused, synchronized integrated teams. This is unfortunately a new concept for cyberspace teams. It has led to some heated discussions among my colleagues because we all know all frameworks are wrong, but some are useful and further every analytical operator has internal prejudices. I seek to present F3EAD as a framework for DCO-RA & possible Offensive Cyber Operations.

Debate continues to evolve on adversary capabilities, advanced persistent threats, and current offensive and defensive capabilities worldwide to respond. Further there exists debates on the proper employment of frameworks. It is understood by veterans in the Information Security community that the continued nuanced development of defense in depth measures and frameworks for the most part is not a new concept. A critical missing link has been operative & actionable intelligence provided by operational analysts. This omitted capability is one that has continued to evolve from ancient methods of warfare.

F3EAD as the Cyber Kill Chain is most effective as an Offensive Response Action Framework through its fusion of intelligence with operations. F3EAD accomplishes all phases at a rapid pace based on its ability to combine conventional intelligence cycles, with doctrinal integration, as well as rapid inclusion of globally present TTP. The connected nature of Cyber Operations provides enhanced visibility to real time assessment worldwide. Developed as a methodology against kinetic targets, its proven employment against insurgencies presented its flexibility against non-lethal methods, time sensitivity, and High Payoff Targets. This framework and whitepaper seeks to provide F3EAD as the answer to developing Defensive Cyber Operations Response Actions (DCO-RA) and possible Offensive methods for consideration. Combined, these response and offensive postures can help project power by application of force in and through cyberspace.

The Intrusion Kill Chain

The introduction of the Intrusion Kill Chain by Lockheed Martin, represented an intelligence-driven DEFENSE process to allow information security professionals to proactively re-mediate and mitigate advanced threats in the future. The process, defensive in nature aligns to the requirements of F3EAD and provides proven reversal gapped filled capability.

The phases of the Intrusion Kill Chain are

- Reconnaissance
- Weaponization
- Delivery

- Exploitation
- Installation
- C2
- Action

Application of F3EAD
Cyber Threats and Attack methods both defensive and offensive are not linear. Operations can only be successful through their persistence. In the application of the find-fix-finish-exploit-analyze-disseminate (F3EAD) targeting cycle, a "pattern of life" is presented based on persistence and repetitiveness. (George Crawford, 2011). It is this pattern of life that provides indicators and true value against an operation and target analysis. Further, offensively understanding the process enables an organization to build capability for course of action development based on long term understanding of an adversary's capability. Metaphorically, this is understanding climate with flexibility to adapt to the weather.

Different engagements are taken throughout the F3EAD cycle and distinct differences and overlaps of other thoughts on the cyber kill chain are interwoven during intrusions and attacks.

Find

Within the F3EAD Cyber Kill Chain, Find is the first step. It encompasses reconnaissance activity based on a measured initial focus. Specifically, find activity in the kill chain occurs by Actors at all levels both in intelligence collection, and operational employment. This is the point where selection of High Valued Targets and Centers of Gravity (COG) occurs. Target selection in the past has often been delegated from a centralized decision process. The security breach by (DEADEYE JACKAL AKA Syrian Electronic Army (SEA)) (Merrit, 2014) actors against Forbes Inc. was a designated operation from the organizations leadership with a deliberate attempt at impacting data confidentiality. However, recent attack trends indicate multiple strains of C2 direction have been employed. In other recent efforts, discombobulated organizations and sects such as Anonymous obtained direction and target selection criteria regionally.

After direction is offered the actors employ intelligence capabilities both active and passive to exploit information with a focus on Facility, Individuals, Virtual, Equipment and Organizations (FIVE-O) targets for the selected operation.

Cyber Key Terrain

Most recently within the U.S. Department of Defense community there have been efforts to define Cyber Key Terrain. Although not exclusive, it can be conveyed that this terrain consists of critical components to an area of operations. (Joint Publication 3-12 Cyberspace Operations) mashed C-KT is: Those critical Information Systems within the information environment that enable the joint force commander's (JFC's) objectives to retain freedom of maneuver in cyberspace, enable other operational activities, and can deny freedom of action to adversaries. C-KT can consist of interdependent networks, critical infrastructures as well as the nodes on those networks, and the system data that support them. The C-KT provides the US military, its allies, and partner nations capability to gain and maintain a strategic, continuing advantage in the

operational environment (OE), and can be leveraged to ensure the nation's economic and physical security. (Commercial Example: Hospital, C-KT for different operations areas ACCOUNTING, and critical billing systems, ER/OR, and associated IT systems)

Fix

Fix is all the activities of the reconnaissance and intelligence collection against the selected target. At this point during F3EAD, the level of target intimacy is high enough to fix a target and employ execution measures. Mature operations will have vetted the intelligence gain loss or addressed how target attack could impact desired outcomes and even further the extent of possible collateral damage. Rapid vetting of the target selection increases the ability for progression to the finish phase. Fortunately breached computer systems like any crime scene, contain a trail of clues. When it comes to advanced cyber-attacks, attackers may provide actor attribution within malware code, phishing emails, command-and-control (C2) servers used, and even operational behavior (FireEye, 2013). In this phase the C2 communication often presents staging sites and bread crumbs. This phase requires a centralized intelligence, surveillance and reconnaissance (ISR) capability to ensure true effectiveness. The hyperfocus on the target at this stage escalates the targeting process to the time sensitive decisive next stage in the F3EAD.

Reconnaissance

Cyberspace is not contained virtually, as it is consists of servers, cables, computers, satellites, and networked systems. Unfortunately, the tendency to use the terms cyberspace and Internet interchangeably is pervasive even though the Internet, is only a piece of the common. (Cavelty)

The depth of network obscurity and attribution requires the first phase in attempting a cyber-attack to be reconnaissance.

The goal of recon is to identify weak points of the target or asset in order to exploit the vulnerability. In depth reconnaissance requires generous resource allocation to find weaknesses in an assets capabilities. Further within the confines reconnaissance activity both passive and active reconnaissance techniques exist. These activities align with the F3EAD phases for developing a probable target to confirming a target for attack. This is specifically the Find & Fix stages. Passive reconnaissance is the effort to gather information without alerting the asset. Passive recon is the preferred method as it makes the least amount of "noise" and minimizes the chance the target or sensors collecting intrusion data will be alerted and repair or increase the security posture. Footprinting as part of passive recon includes scrubbing the internet for information against the target. The development of metadata and information tagging has ensured there is more than enough tagged data to be discovered via search engines, company registries, or even social media sites. Active recon makes more noise in the context of security sensor alert visibility. This activity can include efforts to map the network, ping devices and also attempts to determine port availability.

Throughout the find and fix phases of F3EAD and within the reconnaissance umbrella efforts occur to decrease the chances indicator overlook. Find/Fix is the use of intelligence feeds for information collection and further focusing collection activity to locate, identify and determine

availability of a target. This moves a target in a time sensitive capacity from probable to confirmed, such as is finding an IP space and then understanding the systems, ports, OS and synchronizing most likely known vulnerabilities. Multiple defensive efforts can be derived from intelligence gained throughout these phases.

Finish

Finish, the 3rd phase in F3EAD is important as it is the first decisive coordinated Tactics Techniques and Procedures (TTP) employment in an operation. Finishing is the completion of a mission set rather than finishing "destroying" an adversary. The finishing as conveyed in small operations is revealed in the analysis of Izz-ad-Din Al –Qassam Cyber Fighter attacks on multiple Financial Institutions between 2012 and 2013 (Holden, 2013). The actors displayed use of this methodology based on long term efforts and distinct engagements. As seen during the campaign, the efforts were staggered over a distinct duration an entailed multiple re-attacks. This phase combines toolsets, intelligence, capabilities and a user “grey matter” as a complete weapon system for target engagement. Battle Damage Assessment (BDA) begins in this phase and is carried out forward to determine to internal and external impacts of action offensive/response action employment. BDA is continuous and and assists in course of action development.

Within the *Finish Phase* of F3EAD, Weaponization, Delivery, Exploitation (Small- “e”), Installation, C2, and Action activities also occur.

Weaponization

Weaponization is defined by the coupling of know vulnerabilities with a known weapon platform. Simplicity examples of this capability exists in the use of “Penetration Testing” tools such as Metasploit and Backtrack and Remote Access Tools. However, there are state-sponsored, state-sanctioned, and state-directed actors who have allocated millions of dollar in the development of Cyber Attack weaponization capabilities to include Russia, Iran, and China. (Office, 2013) These actors continue to leverage the fact that critical infrastructures present a dangerous combination of known and unknown vulnerabilities in the cyber domain, strong and rapidly expanding adversary capabilities, and limited threat and vulnerability awareness. Becoming more network-dependent and improved inter-connectivity has drastically increased the threat of unauthorized entities from taking control of, or damaging our infrastructure. Additionally, simple weaponization can include the actions & groundwork of drafting an email, its content and preparation, and utilizing a client to send to an unsuspecting user. An example resulting from this methodology can be seen (DEADEYE JACKAL actors AKA SEA) (Merrit, 2014) was considered a feeble attempt at “hacking” through use of Social Engineering to compromise the Associated Presses Twitter account and posting a false report. The perceived unskilled hackers tied the Twitter event with ongoing events worldwide to complete an influence operation that for a small duration impacted the U.S. economy. The subsequent impression was a Dow Jones drop of over 150 points and a loss of millions in shareholder equity.

Delivery

Transmission of the weapon to the targeted infrastructure and environment to include remote networks, and/or hosts enables close hold capability. The most prevalent infection and injection vectors which continue to result in breaches is displayed below. (BITS, 2011)

- **Installed/Injected by Remote Attacker** – Vulnerabilities that allow remote command execution via exposed software (e.g. SQLi)
- **Email** – Embedded URLs, or malicious attachments
- **Web/Internet Auto Infection** – Drive-By downloads, iFrame exploits
- **Web/Internet User-Initiated** – User downloads (e.g. Bootleg & Unauthorized software)
- **Portable Media & Devices** – USB devices, mobile devices – "BYOD"

Although the methods are the primary delivery mechanisms each can enable additional delivery instruments to include secondary malware install from enabled malware, network propagation, and code injection through C2 to enable exploitation. The existence of a shared threat space is a knowledge base that needs to be leveraged (Sergio Caltagirone)

(e)xploitation

Exploitation occurs after the payload from the weapon system is delivered to the target. Exploitation targets application, system, and users as a vulnerability for the purpose of code execution and to gain initial toehold and insider insight. The presentation of the (e)(small e) is derived from large Exploitation which for long term purposes provide more benefit through converting vast amount of information collected into a form usable by analysts. Intelligence accomplished this through a variety of methods including decryption, language translations, and data reduction and capture to be exploited for use in the analysis process.

Installation

Installation is described as the actions taken after a system is initially compromised. This is the activity of installing a remote capability through a Trojan or backdoor on the victim system enabling the adversary to maintain persistence inside the environment.

Installation as a phase is understated in the design of the Cyber Kill Chain. The lack of acknowledgement is based on the unfortunate truth that most protection measures in every enterprise are employed at this level. Strategically, defensive approaches to the (e)xploit and Installations phases have been addressed in NISTs Cybersecurity Framework. The categories address detection through anomalies & events, Continuous Security Monitoring, and Detection Processes (NIST, 2014). Security teams, employ methods through Host Based Security Systems, Antivirus tools, data at rest software, etc.in a defense in depth effort and last resort to detect and mitigate intrusions. In a F3EAD comparison at this point it is too late. There may be no requirement for additional C2; the adversary is in.

Command and Control (C2)

C2 is the establishment of a channel for communicating orders to and from a sites of compromise and the tasking authority. Typically this method is performed through encrypted means and often

disguised as normal traffic. Compromised systems displaying actor persistence require this C2 to allow manual or automated direction from the actor. The same channels are often used for encapsulating and extracting information.

C2 in F3EAD is the continuous ability to hold the target at risk. The beginning of leveraging Exploitation and Analysis. It is a requirement for sustaining long term capabilities. Further, creating the ability to open and close C2 channels diminishes a target organization from preventing event expansion and mitigating its effects for recovery (NIST, 2014).

Actions on Objectives (A&O)

The Kill Chain for many CERTS, SOCs and CND teams completes the "Intrusion" and chain at this phase. The A&O insists during this phase intruders take actions to achieve original objectives. The most common progressive objective is data exfiltration. Data exfiltration involves collecting, encrypting and extracting information from the target environment. Further, the A&O describes that alternatively, intruders may only desire access to the initial target host for use as a hop point for additional compromise inside the network.

F3EAD presents that Actions & Objectives are capabilities leveraged over multiple phases rather than the end of the intrusion. As stated previously the Kill Chain cannot be linear and although CKC is not, defenders are offered an out and finalization with only mitigation of threat. F3EAD differs from other frameworks based on emphasis of the exploit and analyze steps as the main effort. Recognition is placed on efforts feeding the intelligence operations cycle in which intelligence leads to operations that yield more intelligence leading to more operations. (Department of the Army, 2010).

Exploit

When the COG is Held at risk, it must be exploited immediately. Exploitation is a methodical, detailed collection process to gather potential intelligence. Kinetic exploitation effectiveness relies on prior planning to include SOP, search plans, prepared site exploitation kits, and tactical questioning plans. The non-kinetic to which we work in cyber, often has deficiencies as cyberspace is more dynamic. Although this is not an excuse, it is a challenge faced by analysts both offensive and defensive.

Critical to exploitation is leveraging enablers in support of the objective. Based on the intelligence and information "interrogation" gathering in this phase it is most crucial to both Defensive and Offensive operations as it guides response actions. Trends and analysis is crucial to supporting the exploit phase as information exploited during current operations along with previous discovered TTP, and artifacts provide clues analysts need to evaluate aspects of FIVE-O including capabilities, and intentions. It drives home the awareness of the enemy as a system of systems. Analyst must leverage contextual indicators along with information gleaned from current operations to both operate more strategically, respond tactically, and report holistically.

Additionally, at this point within F3EAD there may be substantial information to support a cyber attack. A Cyber Attack is *cyberspace actions that create various direct denial effects in*

cyberspace and manipulation that leads to a denial that is hidden or that manifests in the physical domains. (JP 3-12). For clarity these are actions to Deny, Degrade, Disrupt, Destroy, and/or Manipulate. Although we have seen many examples of these "actions" in the last 24 months, the community at large is hesitant to call the incidents "Cyber Attacks", because of the lack of supporting direct intent & MAC address level attribution.

Analyze

Analysis, truly the crux of the problem we face both in offense and defense for three specific reasons. Analysis is a long term process and most often organizations with bottom lines do not support long term hyper-focus on areas of operations that do not appear to have a strong ROI. This is the case as the dynamics of both cyber targets and adversaries both hacktivist and state sponsored do reveal TTPs but only if you follow the crumbs. Database the discovered information, and use resources from those who have already established artifacts. The second need during analysis is addressing root cause analysis with two overlays of the 5W's and a TTP breakdown. (EXAMPLE)

- Tactic: Ex-filtration of Company Intellectual Property
- Techniques: Targeted Waterholes, Spearphishing, Malware Installation
- Procedures: Open Source Reconnaissance to harvest email address bank, network mapping, "current organizational focus" discovery efforts.

The TTP breakdown is required during analysis to determine what mitigation and what possible response actions can be employed. It has to be done anything else is only bandage application.

The third piece of development required to support a mindset shift from traditional Cyber Kill Chain assessment is the analysts ability coordinate findings. It is not simply dissemination, but rather vetting the analyzed information. This can be done through working groups and will allow peers across the community of trust to inject their perspectives. Keeping in mind this is a time consuming process, the effort needs to be managed with vision.

Disseminate

Conveying vision vertically and laterally is challenge but remains for leadership the indicator that things are getting done. This allows the team to convey that there is an alignment of what leadership believes is the cyber key terrain and what the analysts and technical SMEs know are the - critical infrastructure elements and how they integrate. Additionally, INFORMATION dissemination helps build the craft because the audience for your threats broadens and both TTP and postures and tuned enabling rapid response against future events. Information sharing is a great thing and unfortunately, in the realm of cybersecurity there is a justified level of trust that doesn't exist. This is where open platforms for cyber threat intelligence can and should be leveraged.

Conclusion

There is no perfect way to address both defensively or offensively the APT (almost went through an entire posting without saying APT). However, my background with the military and work with the commercial sector has helped me realize that we are missing the critical synchronized & fused teamwork that occurs in the Special Operations Community. There are so many unknowns in the realm of cyberspace that the linkage can only be compared to that of guerrilla tactics and art rather than Checking Off Boxes - what traditional Information Security was all about. You can't audit cybersecurity, it is an ongoing day in and day out focus which requires Finding, Fixing, Finishing, Exploiting Analyzing and Disseminating the "Intelligence/Targeting/Information" both internally and externally to leverage capabilities to support current and future DCO-RA & Offensive operations.

Joey Hernandez: Is former Cyber Operations Tactician for the DOD, former professor with the Alamo Community Colleges in San Antonio, and consultant to DHS.