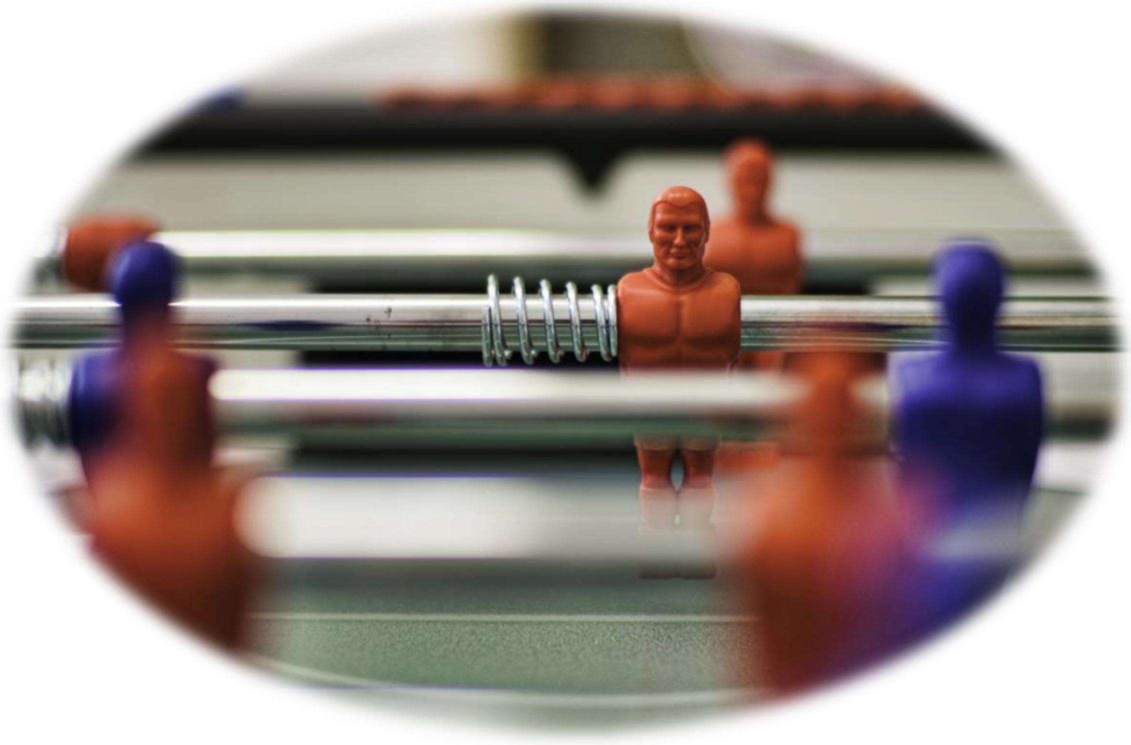


MITRE | ATT&CK™

IMPLEMENTING AN ADVERSARY-FOCUSED FRAMEWORK

Josh Hakala | University of California, Berkeley
W220 Managing Cyber Risk | April 2019

Introduction

Globally, businesses are faced with an ever-increasing sophistication of cyber threat actors and attacks. Conventional network and host-based security controls such as firewalls, intrusion prevention systems, web proxies, antivirus, and other hardware and software often lack the capabilities to detect and prevent advanced attacker tactics and techniques. By following guidance from governments, organizations, and cybersecurity industry best practices, many organizations have implemented key elements to reducing, mitigating, or solving a multitude of cybersecurity risks, but not all. These security elements include, but are not limited to, best practices for hardening systems and networks, as well as incorporating in-depth governance, risk, and compliance frameworks for managing cyber risk within enterprise environments.

Businesses have many options and mandates for cybersecurity risk and control frameworks and standards, including Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and others. These frameworks provide mostly clear guidance on safeguarding enterprise environments, health records, card data, and more. Standards, tools, and frameworks are tremendously important and are often mandated for specific industries for good reasons, but most share at least one key limitation: they often do not include modeling adversary objectives and techniques used in attacks. Creating an intelligence framework built on identifying how adversaries achieve their objectives enables defenders to build new detection and prevention capabilities against those techniques. And choosing to model a framework after Advanced Persistent Threat (APT) actors enables defenders to build in protections against some of the most sophisticated techniques, which often trickle down to commodity malware and attacks. Coupling traditional security controls and frameworks with a systematic knowledge base of known adversary techniques and behaviors is critical to thwarting future attacks based on similar attacker methodology.

Advanced Persistent Threat Modeling

Models that attempt to solve cybersecurity problems from an adversary-focused perspective do exist and have been used by blue teams for at least several years. In 2011, Eric Hutchins, Michael Cloppert, and Rohan Amin of Lockheed Martin proposed a new model called the Cyber Kill Chain® (See Appendix A). The authors based the model on their analyses of numerous APT campaigns and intrusions. This model defines APT activities as a series of 7 distinct phases: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives (See Figure 1). These phases outline attacker campaigns from the start, where the threat actor researches the target to find potential weaknesses and attack vectors; to the finish, where an attacker has completed objectives such as espionage, data destruction, financial gain, etc.

The phased attack model outlined by Lockheed Martin was partly influenced by military related kill chain methodology used by the United States Department of Defense, which includes the stages “fix, track, target, engage, and assess” (Lockheed Martin 2011). Another precursor to the Cyber Kill Chain was in Mandiant’s Exploitation Life Cycle model, released in 2010, which also contains similarity’s to Lockheed’s model, but is a more narrowly-focused 7-step model: reconnaissance, initial intrusion, establish a backdoor, obtain user credentials, install various utilities, privilege escalation/lateral movement/data exfiltration, and maintain persistence (See Appendix B). This model often represents a typical attack life cycle, but was too specific, thus why Lockheed Martin’s Cyber Kill Chain model gained so much popularity within the cybersecurity community in the proceeding years. The Cyber Kill Chain is a more robust and universal model that articulates a broader set of sequential activities that are performed by adversaries.

Additionally, one of the most respected cybersecurity training organizations, SANS, has recently created a course that closely aligns to the Cyber Kill Chain model, titled “Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses.” The curriculum dissects the kill chain phases by mapping a handful specific activities an attacker can use in each phase and practical defense mechanisms to detect and prevent them. Applying this methodology to an enterprise can be an effective strategy and baseline for analysis of threats, however the generalness of each kill chain phase leaves it the blue team to figure out the actual techniques used by adversaries. This lack of detailed techniques used is the reason why companies and security vendors are shifting their cyber threat actor modeling to the MITRE ATT&CK™ framework.

MITRE ATT&CK™

In 2015, MITRE publicly released the first iteration of ATT&CK, short for Adversarial Tactics, Techniques, and Common Knowledge. This is a framework that was created to describe the specific techniques used by attackers to accomplish objectives at various stages of their attack. Instead of a set of linear phases, MITRE has organized this data into a matrix of 11 high-level objectives, called tactics, and each of those tactics contains any number of techniques in which an adversary can achieve it. See Appendix C for example matrix. The 11 tactics map similarly to steps 3 through 7 of the Cyber Kill Chain. The first two steps in the Cyber Kill Chain, Reconnaissance and Weaponization are not normally detectable by a target because those objectives generally occur outside the target’s environment and visibility. MITRE has created a separate matrix called PRE-ATT&CK of 15 tactics that are associated with the first 2 steps in the Cyber Kill Chain but are not covered in this paper.

Each of the 11 tactics contain numerous techniques that have been observed to be used by various adversaries. When drilling into a specific technique of the ATT&CK matrix through a web browser or an API call, the user is presented with a description of the technique’s purpose, associated attack tools (sometimes native OS capabilities / applications), attacker groups known to have used the technique, and detection and mitigation steps that can be taken. These detection and mitigation steps are not for something as trivial as detecting a file name or hash, but instead something like a Windows Event ID or PowerShell command with specific strings or parameters that are known to be associated with malicious activity. This makes it possible to create a generic enough alert that can detect a new malware sample with relatively high fidelity.

Pyramid of Pain

In 2013 Dave Bianco, a Security Architect who worked at sqrrl at the time, created the *Pyramid of Pain* to visualize Indicators of Compromise (IoCs). See Figure 1. In this pyramid model, Bianco describes the varying levels of difficulty detecting IoCs, from the more trivial ones at the bottom—file hashes, IP addresses, domain names, to the most challenging ones at the top— Network/Host Arifacts, Tools and TTPs (Tactics, Techniques, and Procedures). It is easy to develop detection around hash values, IPs, and domains, but it is also easy for an attacker to modify a file hash, change IPs or domains of their attack infrastructure; this requires little money and time from the adversary. This becomes a simple cat and mouse game between defenders and attackers, but it buys the bad guys more time every time they change those IoCs.

Conversely, it is more difficult for the targeted business to create detection and prevention capabilities further up the pyramid but when they achieve that level of detection maturity, it forces an attacker to change their tooling and develop new tactics and techniques. This becomes a more costly and time-consuming endeavor for the adversary; essentially defenders are inflicting more and more pain on the adversary the further up the pyramid we go. And thus it is possible the attacker may to move on to a softer target as they cannot or will not spend the time to retool or develop new tactics.

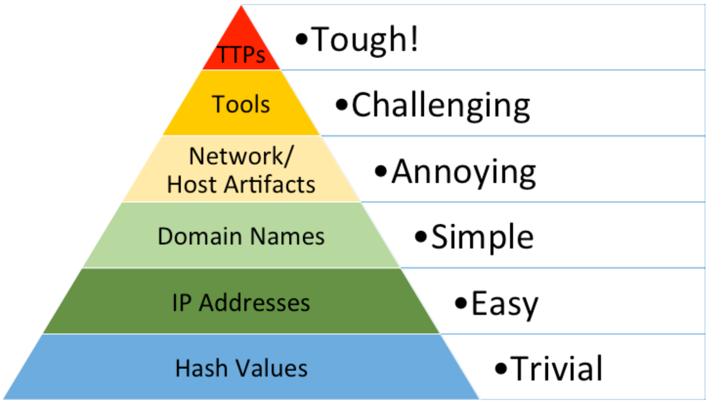


Figure 1: Dave Bianco’s Pyramid of Pain

The ATT&CK Advantage

The ATT&CK methodology exemplifies a key desired detection and prevention capability outlined by Bianco’s taxonomy: it disrupts attacker operations from the top portions of the Pyramid of Pain creating more pain for the attacker. ATT&CK provides to defenders the descriptions not of the traditional ephemeral IoCs, but instead a knowledge base of known adversary TTPs, tools they use, and relevant host and network artifacts.

ATT&CK is not specifically defining how to defend against these various threats, as that is part of a related but separate MITRE project named CAR (Cyber Analytics Repository). CAR provides an analysis of the individual techniques and describes in pseudocode how defenders can detect associated activity. The CAR project has been around for a while now, but its priority has diminished the last few years, until recently, where MITRE has redesigned the CAR website to make it easier to contribute to and they encouraged security professionals to do so. Effectively, blue teams need to be able to translate the ATT&CK techniques into queries for detections within their SIEM (Security Information and Event Management) or other systems and can use CAR as a source of analysis of what information is needed to detect and hunt for the threats.

ATT&CK Challenges

While ATT&CK and CAR are extremely useful, there is a challenge defenders experience when attempting to convert this information into meaningful detections within their enterprise. Most platforms do not have a direct way to translate ATT&CK and CAR terminology into SIEM search parameters or detection signatures. However, we can look to other areas of cybersecurity monitoring that have standardized detection capabilities. It is possible to create detections for malicious files and network traffic in the form of YARA rules and Snort signatures, respectively. Snort is an open source intrusion detection system currently developed by Cisco. Snort signatures can be universally used in other network intrusion detection and prevention systems and are a means detect many types of attacks and exploit techniques.

YARA, created by Victor Alvarez at Virustotal, is open source and the industry standard for malware classification, and used by malware researchers and threat research organizations around the world. YARA is a string pattern matching system that quickly classifies and detects malware samples through static analysis and does not require running the sample inside of a sandbox. So, in cybersecurity we possess standardized means to detect malicious files and network traffic, but we currently lack an industry standard for writing detection signatures of malicious activity identifiable in log files.

In 2017, security researcher Florian Roth proposed a solution to this problem with Sigma, an open source “Generic Signature Format for SIEM Systems.” Roth aptly states, “Sigma is for log files what Snort is for network traffic and YARA is for files.” The idea behind Sigma is that researchers could use standard terminology for detections that could be converted into various SIEM ingestible searches. Sigma consists of the Sigma format for writing the standardized signatures, and the Sigma converter (Sigmac), a command line utility which maps the Sigma signatures to SIEM specific terminology. As of this writing, Sigmac supports 12 different platforms, including Splunk, Arcsight, QRadar, and Kibana. It remains to be seen if Sigma becomes the next industry standard like YARA and Snort, but it is a promising initiative that attempts to solve a big problem. Sigma also supports tagging events with keyworks, and naturally most if not all the

Sigma rules that have been written to date include the ATT&CK tactic and specific technique ID. Integrating MITRE ATT&CK and Sigma enables defenders to translate nearly all ATT&CK techniques into their SIEM with relative ease, vastly improving detection, and providing meaningful alerts than can be referenced to exact attacker techniques for additional context.

ATT&CK Evaluations

MITRE has a strong record of building out reputable and widely-used security tools for defenders and making them open source; ATT&CK is no exception. This framework has effectively become the industry standard because it articulates the techniques in a manner that are useful for blue teams, red teams, and even cybersecurity vendors. Additionally, many cybersecurity vendors are incorporating the ATT&CK terminology within their own platforms to align to the most well-formulated and complete threat intelligence framework.

To put Endpoint, Detection, and Response (EDR) platforms to the test, last year MITRE invited vendors to participate in an APT simulation event; MITRE attempted to execute a series of ATT&CK techniques against each vendor's EDR platform. All vendors who elected to compete were presented with the same "malware" generated by MITRE directly mapped to ATT&CK and designed to simulate the known behaviors of a Chinese threat actor known as APT3. The primary purposes for MITRE's ATT&CK Evaluations were to provide transparency around the detection capabilities of EDR platforms and challenge vendors to improve their products. ATT&CK Evaluations is the first real industry standard that tests a vendor's ability to detect threat actor tactics and techniques. After the exercise, some vendors created posts or conducted seminars on how they fared the best, but anyone can validate those claims.

Officially there was no scoring, and all test results can be viewed on MITRE's website or through a JSON dump. The purpose of not scoring vendors was to demonstrate the true objectiveness of the exercise, and to encourage researchers and organizations to review the findings. This helps defenders look beyond each vendor's marketing jargon and bold claims of completely stopping breaches, and instead demonstrates a real-world analysis of the platforms with real adversary methods. Within the evaluation's dataset, for each vendor there are descriptions and detection notes of each attack technique attempted, as well as screenshots of what any detection or telemetry data within the platform looked like. The screenshots are particularly helpful because sometimes they showed that although a vendor might have had telemetry data on a technique, it could have just been buried in a giant text blob that had to be extracted via a manual search query and was not an automated alert; whereas other vendors might have had precise detection for that particular attack technique. That is why it is important for companies looking for an EDR solution to really dig into through the results.

A couple more notes about the evaluations. First, the tests conducted were based on detecting techniques, not preventing them. This is significant because it is hypothetically possible when looking at an entire chain of attack techniques, one vendor could be good at preventing early kill chain techniques but might have some prevention gaps later in the kill chain. In contrast, it is possible another vendor fails to detect earlier kill chain techniques, but perhaps avoids any real damage on endpoints because they have more prevention capability later in the kill chain. It is important to evaluate what gaps exist in your existing or potential EDR platforms and to understand where other security controls and tools (host, network, or cloud based) within the security stack might fill any of those gaps to mitigate the risk.

Second, an area of concern MITRE did acknowledge was that the ATT&CK evaluations in their current iteration do not account for false positive detections. Essentially, vendors were provided a Windows system and MITRE allowed them to configure their application how they saw fit. It is possible some of the vendor detection configurations were dialed up in the test and those settings may not realistically work in an enterprise environment because they could result in many false positive detections. Sometimes the more aggressive detection settings within EDR tools are very noisy in their detections, resulting in a more than acceptable false positive rate. It is possible some of the results are slightly exaggerated due to the tested configurations, but overall should be a good representation of the products' capabilities.

Another advantage of ATT&CK is it's possible to arrange the matrix techniques by threat actor, which can be helpful for businesses that want to conduct internal exercises focused on emulating specific adversaries. This provides red teams clear steps they can use to mimic in their plans. In addition to providing the ATT&CK techniques on their website and via API, MITRE has also released CALDERA, an "automated adversary emulation system" that can be used for red/purple team simulations, EDR tool evaluations, internal training, and defensive gap analyses. CALDERA also allows teams to perform similar tests to the ATT&CK Evaluations within their own corporate environment against a vendor who did not participate in the evaluations.

An excellent alternative to CALDERA is Red Canary's Atomic Red Team library. Red Canary has majority of the MITRE ATT&CK framework implemented as a collection of small, portable detection tests; these are generally a one-line commands to emulate an adversary technique. Red and blue teams can use these for the same reasons identified above, but the advantage of Atomic Red Team is these attacks are leveraging the exact technique execution steps outlined in the framework, whereas CALDERA is calling them through an agent installed on the machine, which may possibly taint detection measures from EDR tools because the agent initiates the "malicious" activity.

Budget Defense and ATT&CK

MITRE Enterprise ATT&CK is free and open source project. Any organization can build detections by mapping the tactics to specific endpoint event logs or network activity, for free. Florian Roth's Sigma is a free and open source generic log signature writing format. Sigma can complement the ATT&CK framework by easily translating ATT&CK terminology to actual SIEM event detections and alerts. Add in advanced logging capabilities inside Windows using PowerShell and Sysmon logs, it is possible to create granular, actionable detections for a large portion of the ATT&CK matrix, especially the most commonly used techniques. Additionally, there are multiple open source efforts on GitHub that have already mapped the majority of the ATT&CK matrix to specific Windows Sysmon events via a custom Sysmon configuration file. When these customized Sysmon events are triggered, within the log event data they include the exact MITRE tactic and technique used. Combining ATT&CK methodology with Sigma, PowerShell and Sysmon allows defenders to create dashboards and alerts that reflect the ATT&CK techniques with much less effort. Properly implemented and it is possible to achieve near parity in detection capability to some of the most expensive and advanced SIEM and EDR platforms without purchasing a new product.

From a red team perspective, organizations can take advantage of CALDERA and Atomic Red Team. Again, both are free and open source, mapped to ATT&CK, and can supplement or replace other red team tools. Also, these platforms can be used for training, detection correlation and validation, and EDR solutions testing. The cost of entry for real adversaries is continually going down, as tools like exploit kits and other malware are being rapidly developed and sold in cheap subscription or a la carte cost models. Also, many white hat security researchers create excellent exploitation tools for assessing security to promote change within the industry. While these tools are exceptionally useful for defenders, they are being used by adversaries too. All the low cost or free options available to malicious actors has only exacerbated the security crisis. However, although ATT&CK was developed by assessing highly sophisticated threat actors, the advantage of implementing ATT&CK is these techniques are found in commodity malware too. It should not be necessary for companies to pay for absurdly expensive tools that when there are free alternatives that are robust and well-maintained. Companies need to embrace and contribute to these open source solutions as that will drive the industry into a safer direction, where everyone is sharing threat details and collaborating on real solutions to the problems.

ATT&CK Horizon

MITRE’s relentless pursuit to push the industry to a safer state has resulted in many great tools, including others not discussed in detail in this paper. Alongside continual development on Pre-ATT&CK and Enterprise ATT&CK, MITRE is also developing a Mobile matrix used for describing adversarial tactics and techniques for mobile devices. There are not as many mobile phone security initiatives and tools compared to traditional enterprise systems, and thus focus around mobile phone security is more limited. Because the shift to move many systems and services to the cloud also often accompanies a mobile application version, the Mobile ATT&CK matrix will become a pivotal knowledge base of mobile threats and a very welcomed contribution.

In 2018 MITRE held its first convention, called ATT&CKcon, to promote the framework within the cybersecurity industry. The event was held on the MITRE campus in Mclean, VA, where they held a modest conference of 20 presentations, but they included notable companies like GE, Verizon, CrowdStrike, Microsoft, and Palo Alto. They will have another conference in October 2019 to continue their pursuit of making cyber threat intelligence and adversary detection available to the masses.

The first round of the ATT&CK evaluations had several participant vendors in the APT3 simulation but proved to be well received by security researchers, and even the vendors. Researchers found value in the objective testing methodology and transparent results, and security vendors were generally able to prove their platforms capabilities. This first round essentially became a proof of concept to testing the detection techniques and behaviors of adversaries in commercial EDR platforms. MITRE has created rolling admissions so other vendors could enroll in the first round's test exercise, but they also plan to conduct other APT simulations.

In February 2019, MITRE announced that the next set of adversary emulation techniques will follow APT29, attributed as a Russian state-sponsored actor linked to their Federal Security Service (FSB) and Foreign Intelligence Service (SVR). This actor was selected because of the vast number of organizations and sectors targeted. For this second go-round, while there is a significant amount of open source intelligence on APT29, MITRE is seeking additional contributions from the community as to make the simulation as accurate as possible. One advantage of sourcing the security community is it will result in a larger set of techniques to be tested against EDR platforms. Because they will have a larger attacker data set MITRE will be able to test more techniques used by that threat actor. This will put even more pressure on security vendors for the second set of evaluations.

REFERENCES

https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

https://www.recordedfuture.com/analytical-threat-intelligence-frameworks/

http://rvasec.com/slides/2014/Bianco_Pyramid%20of%20Pain.pdf

https://www.slideshare.net/FireEyeInc/mtrends-2010-the-advanced-persistent-threat

https://www.sans.org/course/defeating-advanced-adversaries-kill-chain-defenses

https://attackevals.mitre.org/

https://medium.com/mitre-attack/cyber-analytics-repository-migrated-to-github-4641d7f748f2

https://atomicredteam.io/

https://github.com/olafhartong/sysmon-modular

https://github.com/Neo23x0/sigma

https://www.slideshare.net/secret/gvgxeXoKblXRcA

https://www.snort.org/faq/what-is-a-signature

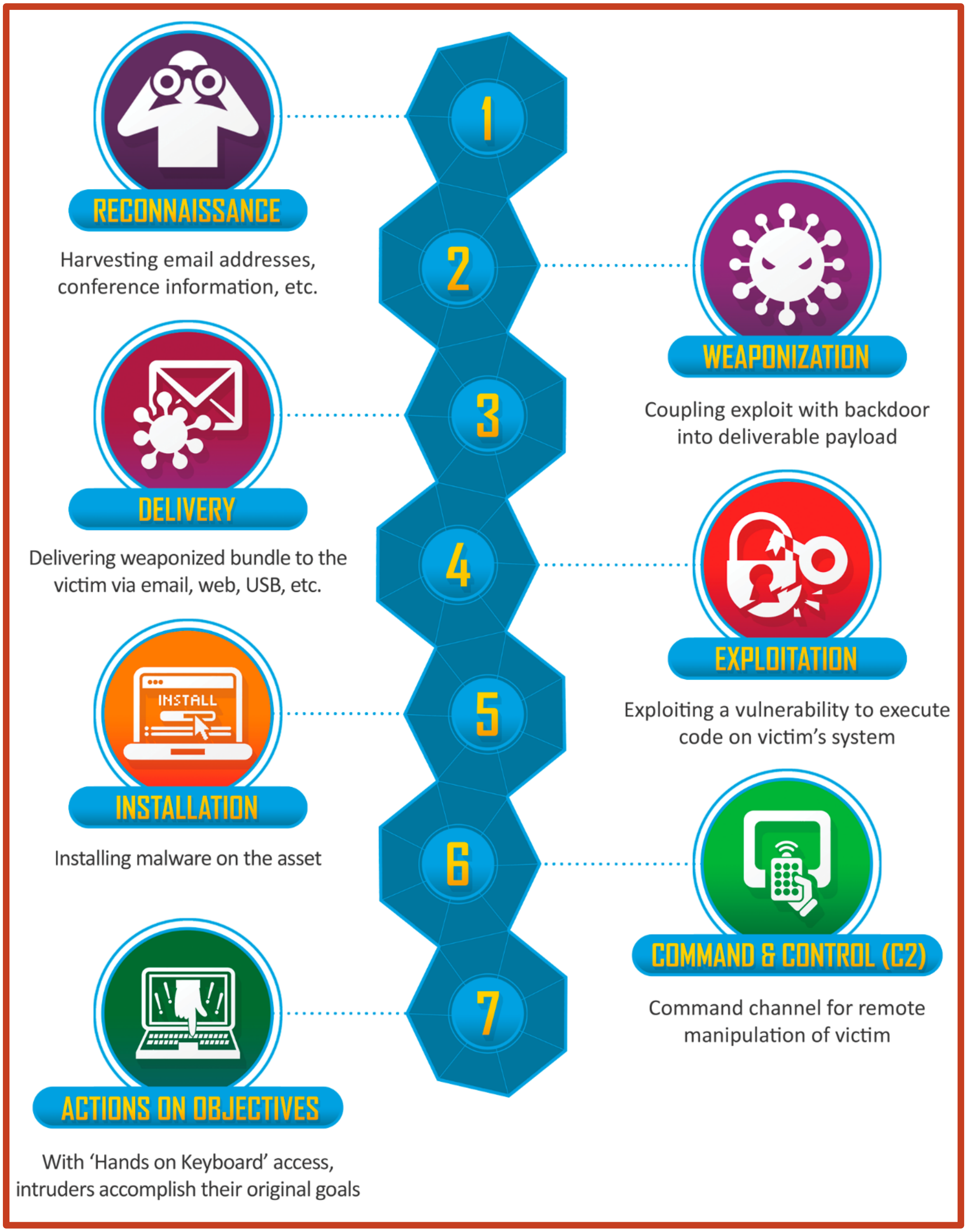
https://medium.com/mitre-attack/open-invitation-to-share-cyber-threat-intelligence-on-apt29-for-adversary-emulation-plan-831c8c929f31

https://www.slideshare.net/KatieNickels/first-cti-symposium-turning-intelligence-into-action-with-mitre-attck

https://github.com/olafhartong/sysmon-modular

APPENDIX A:

Lockheed Martin Cyber Kill Chain



RECONNAISSANCE

Harvesting email addresses, conference information, etc.

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

INSTALLATION

Installing malware on the asset

COMMAND & CONTROL (C2)

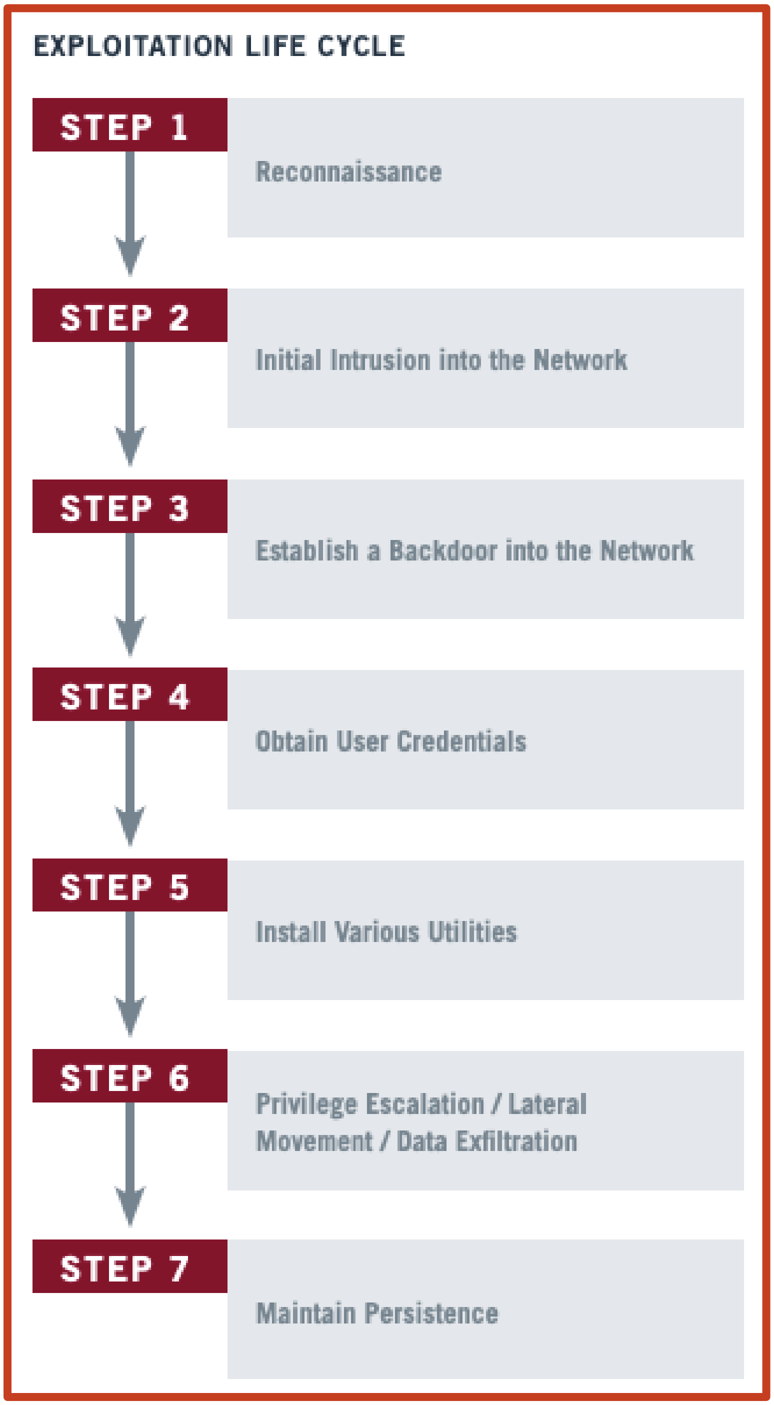
Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

APPENDIX B:

Mandiant Exploitation Life Cycle



EXPLOITATION LIFE CYCLE

STEP 1 Reconnaissance

STEP 2 Initial Intrusion into the Network

STEP 3 Establish a Backdoor into the Network

STEP 4 Obtain User Credentials

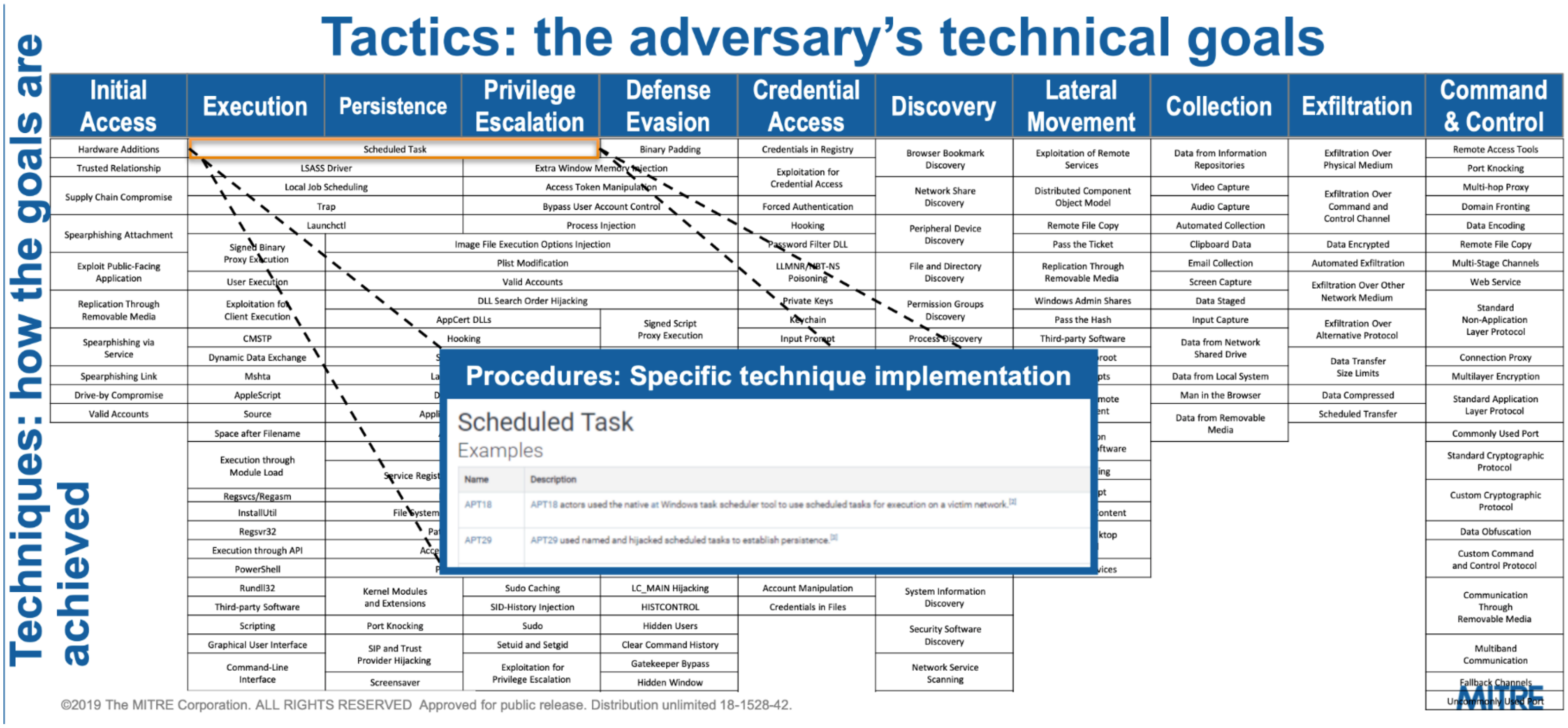
STEP 5 Install Various Utilities

STEP 6 Privilege Escalation / Lateral Movement / Data Exfiltration

STEP 7 Maintain Persistence

APPENDIX C:

Example ATT&CK Matrix



Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access
- Hardware Additions
- Trusted Relationship
- Supply Chain Compromise
- Spearphishing Attachment
- Exploit Public-Facing Application
- Replication Through Removable Media
- Spearphishing via Service
- Spearphishing Link
- Drive-by Compromise
- Valid Accounts

Execution
- Scheduled Task
- LSASS Driver
- Local Job Scheduling
- Trap
- Launchctl
- Signed Binary Proxy Execution
- User Execution
- Exploitation for Client Execution
- CMSTP
- Dynamic Data Exchange
- Mshta
- AppleScript
- Source
- Space after Filename
- Execution through Module Load
- Regsvcs/Regasm
- InstallUtil
- Regsvr32
- Execution through API
- PowerShell
- Rundll32
- Third-party Software
- Scripting
- Graphical User Interface
- Command-Line Interface

Persistence
- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- DLL Search Order Hijacking
- AppCert DLLs
- Hooking
- S
- La
- D
- Appli
- Service Regist
- File System
- Pa
- Acce
- P
- Kernel Modules and Extensions
- Port Knocking
- SIP and Trust Provider Hijacking
- Screensaver

Privilege Escalation
- Extra Window Memory Injection
- Access Token Manipulation
- Bypass User Account Control
- Process Injection
- Sudo Caching
- SID-History Injection
- Sudo
- Setuid and Setgid
- Exploitation for Privilege Escalation

Defense Evasion
- Binary Padding
- Signed Script Proxy Execution
- LC_MAIN Hijacking
- HISTCONTROL
- Hidden Users
- Clear Command History
- Gatekeeper Bypass
- Hidden Window

Credential Access
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Password Filter DLL
- LLMNR/NBT-NS Poisoning
- Private Keys
- Keychain
- Input Prompt
- Account Manipulation
- Credentials in Files

Discovery
- Browser Bookmark Discovery
- Network Share Discovery
- Peripheral Device Discovery
- File and Directory Discovery
- Permission Groups Discovery
- Process Discovery
- System Information Discovery
- Security Software Discovery
- Network Service Scanning

Lateral Movement
- Exploitation of Remote Services
- Distributed Component Object Model
- Remote File Copy
- Pass the Ticket
- Replication Through Removable Media
- Windows Admin Shares
- Pass the Hash
- Third-party Software
- root
- pts
- mote ent
- on oftware
- ing
- pt
- ontent
- ktop
- vices

Collection
- Data from Information Repositories
- Video Capture
- Audio Capture
- Automated Collection
- Clipboard Data
- Email Collection
- Screen Capture
- Data Staged
- Input Capture
- Data from Network Shared Drive
- Data from Local System
- Man in the Browser
- Data from Removable Media

Exfiltration
- Exfiltration Over Physical Medium
- Exfiltration Over Command and Control Channel
- Data Encrypted
- Automated Exfiltration
- Exfiltration Over Other Network Medium
- Exfiltration Over Alternative Protocol
- Data Transfer Size Limits
- Data Compressed
- Scheduled Transfer

Command & Control
- Remote Access Tools
- Port Knocking
- Multi-hop Proxy
- Domain Fronting
- Data Encoding
- Remote File Copy
- Multi-Stage Channels
- Web Service
- Standard Non-Application Layer Protocol
- Connection Proxy
- Multilayer Encryption
- Standard Application Layer Protocol
- Commonly Used Port
- Standard Cryptographic Protocol
- Custom Cryptographic Protocol
- Data Obfuscation
- Custom Command and Control Protocol
- Communication Through Removable Media
- Multiband Communication
- Fallback Channels
- Uncommonly Used Port

Procedures: Specific technique implementation

Scheduled Task

Examples

Name	Description
APT18	APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network.[2]
APT29	APT29 used named and hijacked scheduled tasks to establish persistence.[3]

SOURCE:

https://www.slideshare.net/KatieNickels/first-cti-symposium-turning-intelligence-into-action-with-mitre-attck