Global Information Assurance Certification Paper

ATT&CKing Threat Management: A Structured Methodology for Cyber Threat Analysis

GIAC (GCFA) Gold Certification

ISSE 5501

Author: Andy Piazza, andy.c.piazza@gmail.com
Advisor: Tanya Baccam

Accepted: June 13, 2019

Abstract

Risk management is a principal focus for most information security programs. Executives rely on their IT security staff to provide timely and accurate information regarding the threats and vulnerabilities within the enterprise so that they can effectively manage the risks facing their organizations. Threat intelligence teams provide analysis that supports executive decision-makers at the strategic and operational levels. This analysis aids decision makers in their commission to balance risk management with resource management. By leveraging the MITRE Adversarial Tactics Techniques & Common Knowledge (ATT&CK) framework as a quantitative data model, analysts can bridge the gap between strategic, operational, and tactical intelligence while advising their leadership on how to prioritize computer network defense, incident response, and threat hunting efforts to maximize resources while addressing priority threats.

1. Introduction

Cyber threat intelligence is a daunting field and an intimidating topic for most organizations. Their analysts are overwhelmed with trying to keep up with the community as it shares new hunting techniques, GitHub projects, and conference presentations on the latest threats. They often find themselves unable to focus on developing basic, repeatable processes that provide long-term sustainability and value to the organization that they support. Organizations pump endless streams of raw data through internal sensors, open-source collection systems, and commercial threat feeds while expecting their analysts to tune the feeds, react to alerts, and stay abreast of the threat actors' intent and capabilities. This constant flow of data leads most analytical shops into what is commonly known as firefighting mode, which means that they react and respond to the latest flare-ups and rest between events when they can. These analysts often focus on one or two related reports at a time to collect indicators of compromise (IOCs), identify tactics, techniques, and procedures (TTPs), and run hunts in their environments. The artifacts that they previously collected become forgotten items in the form of incident tickets, share-drive folders, and threat intelligence platforms (TIPs).

Consistently stuck at the tactical level of analysis, these analysts cannot address the strategic and operational level requirements of managers and executives. The National Institute of Standards and Technology (NIST) highlights that the "senior management's commitment to information security initiatives is the single most critical element that impacts an information security program's success" (Bowen, Chew, & Hash, 2007). It is critical that threat analysis engages senior management and informs their decision-making processes at their level. IBM's Security Intelligence group defines strategic threat intelligence as "analysis and information that can help organizations understand the type of threat they are defending against; the motivation and capability of the threat actor; and the potential impacts thereof" (Gourley, 2018). Additionally, threat analysis can identify gaps in an organization's defense-in-depth coverage for those threat actors' capabilities. At the operational level, threat analysis can inform the organization's security awareness program to ensure that the training accurately describes the threat landscape. With operational intelligence, vulnerability management teams can prioritize patching to address actively exploited vulnerabilities. Intelligence analysts that are

hindered by tactical level analysis cannot abandon that work to execute the strategic and operational requirements of their organization. Effective intelligence programs require all three levels of analysis: tactical, operational, and strategic.

Intelligence managers must develop mature processes and analytical methodologies that bridge all three levels of analysis while providing analysts with repeatable and effective procedures to collect, catalog, assess, and act on the information that they process. This paper will demonstrate that the MITRE Adversarial Tactics Techniques & Common Knowledge (ATT&CK) framework can be leveraged as a quantitative data model to prioritize resource management and security engineering efforts, inform computer network defense and incident response procedures, and guide technical threat hunts while informing decision makers at all three levels of analysis.

2. Literature Review

While the Intelligence Community (IC) traces its roots back hundreds of years and has been a constant force since World War II, cyber threat intelligence (CTI) is a relatively new field that is still maturing through the work of analysts and organizations across both the public and private sectors. In intelligence analysis, practitioners rely on frameworks and data models to ensure consistency in their work and to reduce cognitive biases. This section discusses the existing cyber threat intelligence models and how organizations have leveraged them historically.

According to MITRE, ATT&CK is a "globally-accessible knowledge base of adversary tactics and techniques based on real-world observations" (MITRE, 2019). At the center of this system is the ATT&CK Matrix for Enterprise, which consists of Tactics as column headers and Techniques as values under those Tactics. Each Technique is a hyperlink to a Procedure page that provides a technical explanation of the specific Technique, the logs and data sources that are useful for analysis, and a list of actors that have previously used that Technique in an event. MITRE provides ATT&CK in the Structured Threat Information Expression (STIX) 2.0 JSON format via GitHub so that organizations can implement this data model in their STIX intelligence products and intelligence platforms (MITRE, 2019). Figure 1 below demonstrates how analysts can

navigate through the Enterprise Matrix to view the Tactics, Techniques, and Procedures (TTPs).

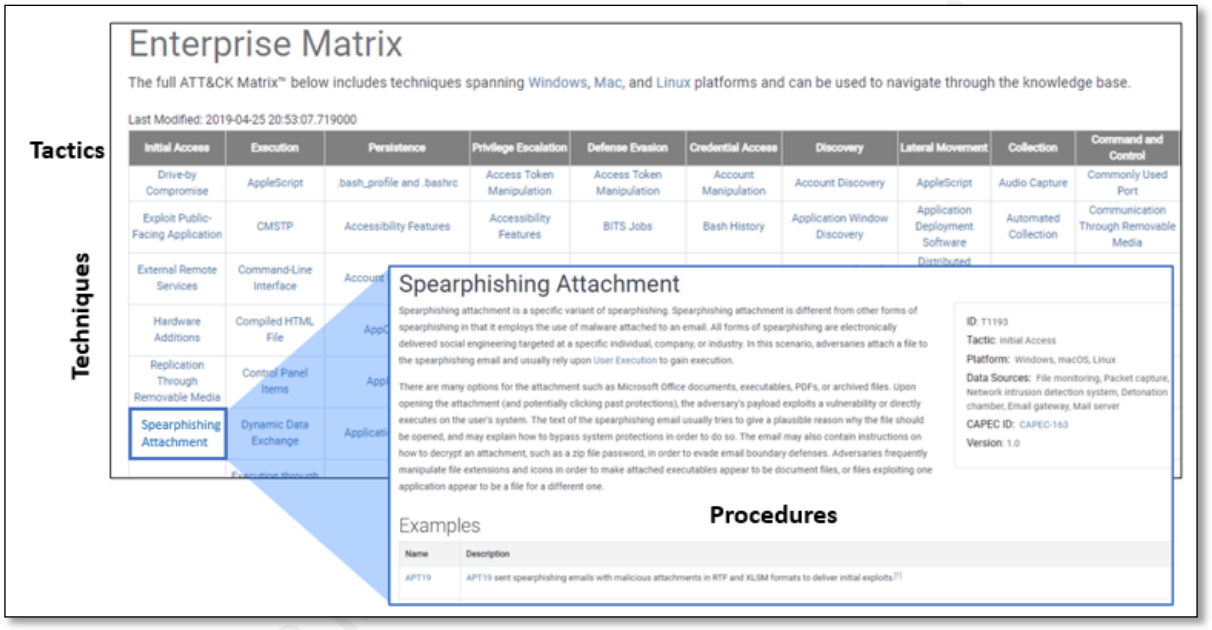


Figure 1: Enterprise Matrix with Tactics, Techniques, and Procedures

Before the release of the MITRE ATT&CK framework, threat analysts had two primary threat models for categorizing malicious activity: the Diamond Model for Intrusion Analysis (Caltagirone, Pendergast, & Betz, 2013) and the Lockheed Martin Cyber Kill Chain™ (Lockheed Martin, n.d.). These existing data models attempt to quantify and characterize cyber intrusions by grouping the activity in threat actor campaigns and intrusion events. These are sound intelligence models that organizations must not abandon while adopting the MITRE ATT&CK framework. In fact, research shows that these models integrate well with ATT&CK.

According to the debut white paper on the Diamond Model for Intrusion Analysis, it is "a formal method applying scientific principles to intrusion analysis - particularly those of measurement, testability, and repeatability - providing a comprehensive method of activity documentation, synthesis, and correlation" (Caltagirone, Pendergast, & Betz, 2013). At the time of its development, the authors of the model acknowledged that it is "cognitive and highly manual" (Caltagirone, Pendergast, & Betz, 2013). Their choice of words indicates the difficulty of adopting the Diamond Model for routine analysis, and research shows that the adoption of the Diamond Model by security vendors is relatively

limited. ThreatConnect states that their cyber threat intelligence platform is the only TIP built on the Diamond Model (ThreatConnect, n.d.). Rather than serving as the underlying data model for a security application, vendors traditionally only demonstrate how their tools map to the Diamond Model, which still requires manual processing by analysts to implement. Recorded Future's article "Applying Threat Intelligence to the Diamond Model for Intrusion Analysis" is a perfect example of a vendor demonstrating the alignment of their categories to the Diamond Model without fully adopting the data model within their platform (Carreon, 2018). For example, they translate that their tool's "Method" category directly correlates to the Diamond Model's Capabilities category rather than adopting the term Capabilities within their taxonomy.

The Lockheed Martin Cyber Kill Chain™ is arguably more popular than the Diamond Model as multiple information sharing programs and threat intelligence organizations use it in their products and threat feeds. For example, the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) uses the Cyber Kill Chain to categorize IOCs in their indicator packages, and they have used the model to catalog nation-state threat activity as well. Their pivotal report, "Enhanced Analysis of GRIZZLY STEPPE" (NCCIC, 2017), discusses the history of the Russian government's cyber activity through the lends of the Cyber Kill Chain.

As a third option for analysts to categorize threat intelligence, the United States Government (USG) developed the Cyber Threat Framework. According to the Director of National Intelligence (DNI) website, the Cyber Threat Framework "was developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries" (Office of the Director of National Intelligence, n.d.). However, neither private sector threat intelligence companies nor USG information-sharing organizations have adopted this framework in their unclassified intelligence products. The Cyber Threat Framework is better suited for strategic level reporting about cyber activity and does not provide any additional utility when compared to the Cyber Kill Chain and the Diamond Model. The model does very little to categorize technical indicators and malware capabilities.

While all three models are used to catalog threat actor activity from incidents and threat intelligence reporting, none of these models adequately inform decision-makers on where to invest in security controls, nor do they educate at the technical level where to prioritize threat hunt operations. Their ability to enlighten the decision-making process is limited to the operational level during an incident and does not inform incident responders on where else to look within a network for known TTPs and IOCs. For example, if a SOC analyst identifies packets as belonging to the Command and Control (C2) phase for a specific actor by using the Lockheed Martin Cyber Kill Chain™, the analyst can leverage that model to identify what historic IOCs to search for in previous stages of the kill-chain. This is beneficial because it can lead to the detection and mitigation of previously unidentified infections. This model falls short in that it does not provide a taxonomy for the TTPs used by the threat actor and it does not inform the responders which logs or systems they should look at for further evidence of activity.

The ATT&CK framework stands apart from previous threat models because it is a community-based project that consistently matures and evolves to meet the infosec community's needs. MITRE's open-source and cooperative approach works to ensure that the model has full buy-in from the community that uses it every day. To ensure that the framework remains a collaborative effort, MITRE hosts an annual conference specifically for practitioners of ATT&CK, known as ATT&CKcon (MITRE, 2018). Continuously developing the framework is a team effort that has led to the April 2019 release of a new tactic and hundreds of updates to techniques, actor pages, and minor editorial modifications (MITRE, 2019). This combination of effectiveness and public support ensures that the model continues to grow.

Additionally, ATT&CK is powerful at all threat levels of intelligence analysis and reporting, which has led to broad adoption of the model by analysts and vendors alike. Currently, the best example of using ATT&CK at the three levels of analysis is Palo Alto Networks' Unit 42 creation of their open-source project called the Adversary Playbook (Unit 42, 2019). Unit 42 states that "through observation and data sharing, defenders can create a custom version of the Adversary's playbook, and then use that playbook to better defend their network with defensive playbooks" (Unit 42, 2019). When a researcher initially navigates to an actor profile in the Unit 42 Playbook Viewer, they see a strategic

view of actors' historical campaigns along with an initial description of the actor's intent and capability. Clicking on a specific campaign provides an understanding of the actor's activity against a target or set of victims. This campaign view maps the ATT&CK techniques to the Cyber Kill Chain, providing a step-by-step understanding of the attack's progression. Viewing an individual technique presents the researcher with a technical-level view of the IOCs observed with that technique, as well as the appropriate hyperlinks back to the technique page on the MITRE site, as seen in Figure 2.

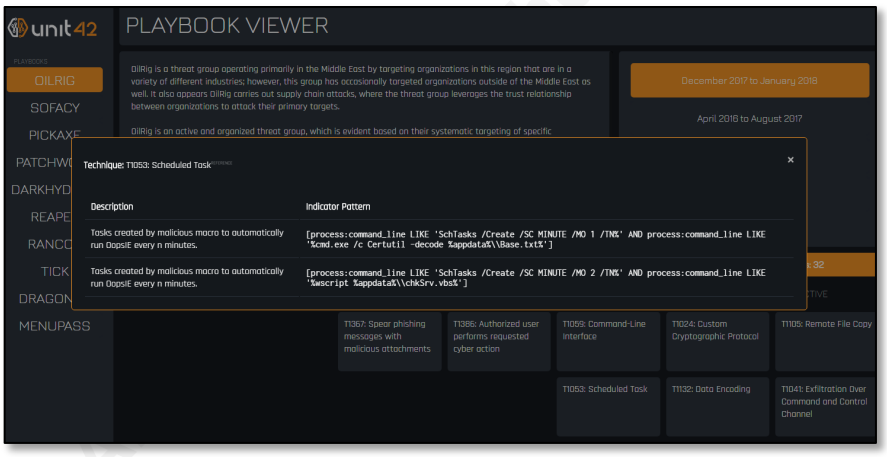


Figure 2: Unit 42's Playbook Viewer (Unit 42 2019)

When previous models were released, such as the Diamond Model and Cyber Kill Chain, some security vendors adopted these models and used them in their platforms and marketing material. These models were primarily implemented in platforms to categorize the data stored in these systems, such as the previously mentioned example of the Diamond Model being used in the ThreatConnect TIP. In the case of the MITRE ATT&CK framework, vendors use it to assess the defense capabilities that their security solutions provide to their end customers.

Additionally, MITRE conducts ATT&CK evaluations against vendors that are willing to undergo third-party testing. These evaluations use the framework to assess the abilities of security products and services to detect known adversary behavior (MITRE, 2018). For security vendors, the results of these tests serve as bragging rights in marketing material, such as Carbon Black's statement that they "demonstrated strong results that set us apart from the rest of the security products tested" (Carbon Black, 2019). For defenders, these appraisals provide a strategic view of their network's

defensive posture in the form of technique coverage maps. These coverage maps are a critical component in calculating an enterprise's defense-in-depth capability. By combining each vendor coverage map into the ATT&CK Navigator, which is a free tool that MITRE hosts for people to create custom ATT&CK maps, organizations can get a comprehensive view into their defensive capabilities.

Research shows that the ATT&CK framework is potent at all three levels of intelligence analysis. It is generally well received by the infosec community and is actively embraced by security vendors as a tool to evaluate their products and as a data model within their tools to categorize threat activity. However, research into the usage of the ATT&CK framework against large data sets remains underrepresented within contemporary research. The next sections of this research will address this shortcoming and demonstrate how the model can go beyond merely informing all three levels of analysis to a state of prioritizing decision-making at those levels.

3. Research Methodology

This research leveraged the MITRE ATT&CK framework as a quantitative analysis methodology by focusing on four phases of analysis: Collect, Catalog, Assess, Act (CCAA) – a data processing model that was formerly presented by the author at a conference in 2017 (Piazza, 2017). This methodology converts data and information into intelligence. To conduct this research, reports were collected from multiple sources, cataloged using ATT&CK, and then the dataset was analyzed to identify trends in the techniques used by threat actors. The Act phase identifies how enterprises can leverage these findings to improve their network visibility and inform the decision-making processes within an organization.

In the Collect phase, reports were gathered from twenty-two distinct sources to replicate the vast amount of data that the average threat intelligence analyst has access to using free resources. This data included reporting at various levels of maturity- from thorough Advanced Persistent Threat (APT) campaign reports to short blogs by infosec researchers. This broad collection effort not only mimics the real collection efforts of an average threat analyst, but also it ensures that the results are statistically meaningful.

The scope of the Collect phase was limited to reports that specifically discussed threat activity that was directly observed by infosec analysts. The key scoping requirement concerning report collection was to gather original analysis and exclude "analysis of analysis," such as infosec blog's discussing other security researchers' findings. While this scope includes vendor reporting, it excludes academic papers that focus on potential techniques, secondary analysis of another team's findings that do not provide additional technical information, and any report that does not include multiple tactics or techniques.

These reports were then Cataloged using the MITRE ATT&CK framework's tactics and techniques, which are identified on the ATT&CK Matrix for Enterprise website (MITRE, 2019). Using an Airtable relational database, the researcher developed a table with each of the eleven tactics as separate columns with their corresponding techniques in multiselect fields. An Airtable database was chosen to replicate a threat intelligence platform's (TIP) ability to categorize threat reporting using ATT&CK without having to procure or develop a system for this research. Additionally, Airtable enabled the researcher to remain technology agnostic, which leaves room for TIP vendors and in-house solutions to match this capability in their tools. The Airtable data structure included the following fields:

Field Name	Field Type	Description
Report Date	Date	Date the report was published
Report Title	Short Text	Title of the report
Report Author	Description	Author's name
Report URL	Short Text	Source URL
APT Name	Short Text	Name of actor, if any
Initial Access	Combo box | multi-select	Selectable list of techniques
Execution	Combo box | multi-select	Selectable list of techniques
Persistence	Combo box | multi-select	Selectable list of techniques
Privilege Escalation	Combo box | multi-select	Selectable list of techniques
Defense Evasion	Combo box | multi-select	Selectable list of techniques
Credential Access	Combo box | multi-select	Selectable list of techniques
Discovery	Combo box | multi-select	Selectable list of techniques
Lateral Movement	Combo box | multi-select	Selectable list of techniques
Collection	Combo box | multi-select	Selectable list of techniques
Exfiltration	Combo box | multi-select	Selectable list of techniques
Command and Control	Combo box | multi-select	Selectable list of techniques

Table 1: Database field structure

Creating the table structure is tedious work in a traditional database or spreadsheet since each combo box has anywhere from nine options to over 67 unique values. Thankfully, MITRE provides a downloadable Excel file with the ATT&CK framework mapped by tactic and technique. This prevents analysts from having to manually copy and paste these values into a database structure or spreadsheet. Figure 3 below demonstrates the download button on the Navigator's page. The second image is the downloaded spreadsheet (Figure 4).

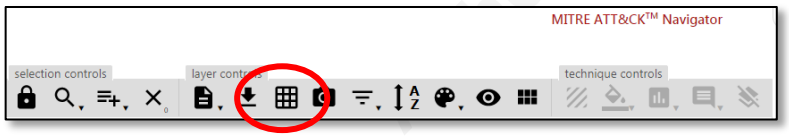
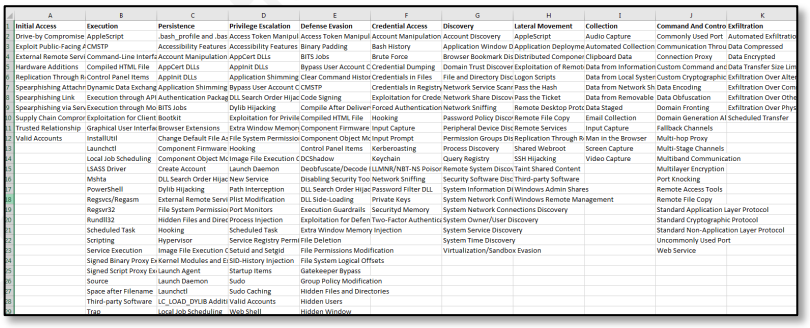


Figure 3: ATT&CK Navigator Download to Excel Button



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Contro	Exfiltration
Drive-by Compromise	AppleScript	.bash_profile and .bas	Access Token Manipul	Access Token Manipul	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltratio
Exploit Public-Facing A	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window D	Application Deployme	Automated Collection	Communication Throu	Data Compressed
External Remote Servi	Command-Line Interfa	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Dis	Distributed Componer	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account C	Credential Dumping	Domain Trust Discover	Exploitation of Remot	Data from Information	Custom Command and	Data Transfer Size Lim
Replication Through R	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command Histor	Credentials in Files	File and Directory Disc	Logon Scripts	Data from Local Systen	Custom Cryptographic	Exfiltration Over Alter
Spearphishing Attachr	Dynamic Data Exchang	Application Shimming	Bypass User Account C	CMSTP	Credentials in Registry	Network Service Scanr	Pass the Hash	Data from Network Sh	Data Encoding	Exfiltration Over Com
Spearphishing Link	Execution through API	Authentication Packag	DLL Search Order Hijac	Code Signing	Exploitation for Crede	Network Share Discov	Pass the Ticket	Data from Removable	Data Obfuscation	Exfiltration Over Othe
Spearphishing via Serv	Execution through Mo	BITS Jobs	Dylib Hijacking	Compile After Deliver	Forced Authentication	Network Sniffing	Remote Desktop Protc	Data Staged	Domain Fronting	Exfiltration Over Phys
Supply Chain Compror	Exploitation for Client	Bootkit	Exploitation for Privile	Compiled HTML File	Hooking	Password Policy Discor	Remote File Copy	Email Collection	Domain Generation Al	Scheduled Transfer
Trusted Relationship	Graphical User Interfa	Browser Extensions	Extra Window Memor	Component Firmware	Input Capture	Peripheral Device Disc	Remote Services	Input Capture	Fallback Channels	
Valid Accounts	InstallUtil	Change Default File As	File System Permissio	Component Object Mc	Input Prompt	Permission Groups Dis	Replication Through R	Man in the Browser	Multi-hop Proxy	
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels	
	Local Job Scheduling	Component Object Mc	Image File Execution C	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication	
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode	LLMNR/NBT-NS Poisor	Remote System Discov	Taint Shared Content		Multilayer Encryption	
	Mshta	DLL Search Order Hijac	New Service	Disabling Security Too	Network Sniffing	Security Software Disc	Third-party Software		Port Knocking	
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijac	Password Filter DLL	System Information Di	Windows Admin Shares		Remote Access Tools	
	Regsvcs/Regasm	External Remote Servi	Plist Modification	DLL Side-Loading	Private Keys	System Network Confi	Windows Remote Management		Remote File Copy	
	Regsvr32	File System Permissio	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol	
	Rundll32	Hidden Files and Direc	Process Injection	Exploitation for Defen	Two-Factor Authentica	System Owner/User Discovery			Standard Cryptographic Protocol	
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol	
	Scripting	Hypervisor	Service Registry Permi	File Deletion		System Time Discovery			Uncommonly Used Port	
	Service Execution	Image File Execution C	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service	
	Signed Binary Proxy Ex	Kernel Modules and Ex	SID-History Injection	File System Logical Offsets						
	Signed Script Proxy Ex	Launch Agent	Startup Items	Gatekeeper Bypass						
	Source	Launch Daemon	Sudo	Group Policy Modification						
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories						
	Third-party Software	LC_LOAD_DYLIB Additi	Valid Accounts	Hidden Users						
	Trap	Local Job Scheduling	Web Shell	Hidden Window						

Figure 4: Navigator's Downloaded Excel File

Airtable's ability to create drop-down values from imported data is also critical to easily implanting this data model. Users simply create a new base using their "Add a base" function, select "Import a Spreadsheet" and then paste the Navigator's export into the "Or paste table data here" field that is in the screenshot on the left. The screenshot on the right in Figure 5 demonstrates how Airtable interpreted the data during import.

Andy Piazza, andy.c.piazza@gmail.com

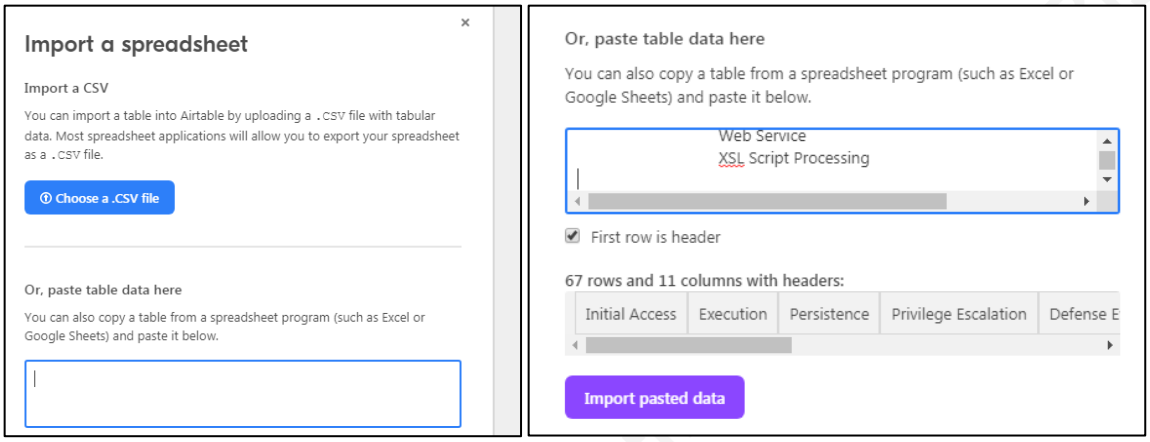


Figure 5: Import a Spreadsheet view without (Left) and with data (Right)

After importing the data, the researcher changed each field type to "Multiple Select," and Airtable converted the existing values into multiple choice options, as seen in Figure 6. This process was repeated across all of the tactic columns. Once complete, all of the existing rows of data can be deleted to clear the database, and report cataloging can begin. The technique options are available for selection, as seen in Figure 7.

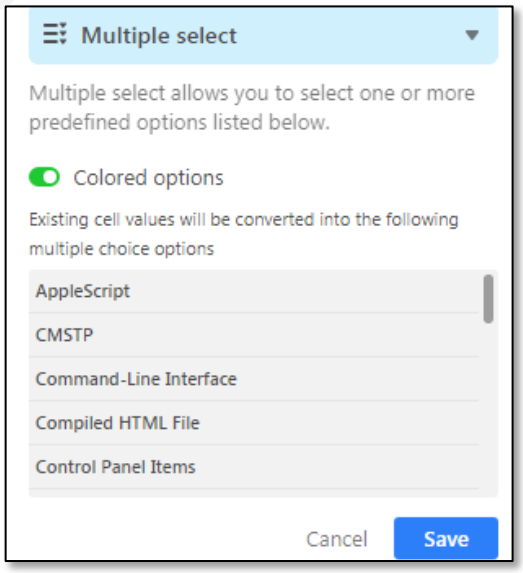


Figure 6: Changing Field Properties to Multiple Select

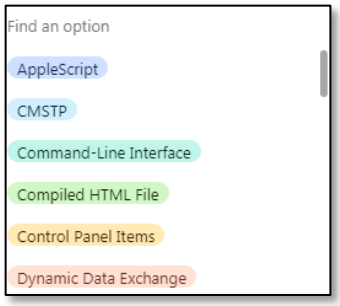


Figure 7: Multiple Select Example

Figure 8 below presents the analyst's view when creating a report in Airtable's single-record view with the system's spreadsheet view in the background. The form view also includes tracked changes in the Activity pane in the right-hand column. This activity tracking includes which changes were made along with the user that made the changes. This is beneficial to ensure appropriate change management within teams.

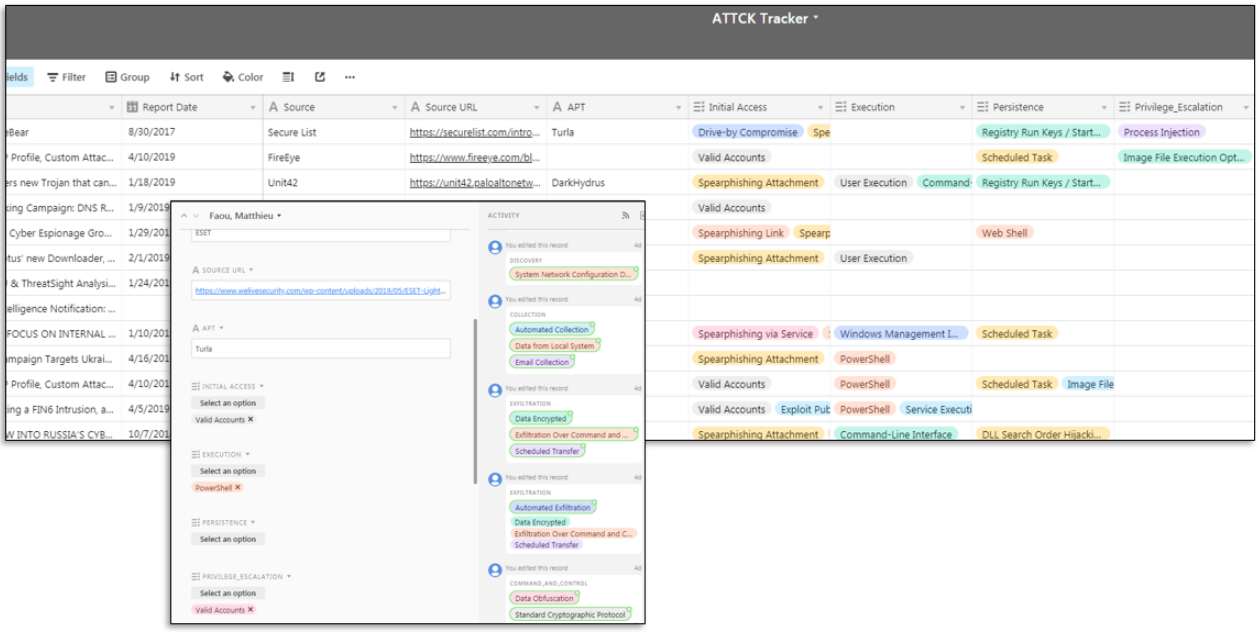


Figure 8: Airtable Form and Table views

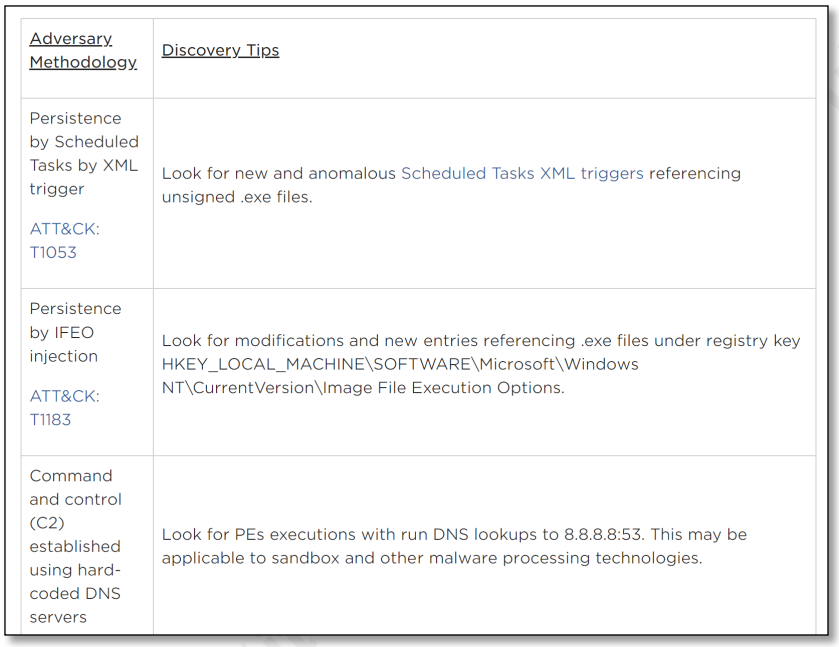
Once threat reporting was cataloged using this table structure, spreadsheet software was leveraged to develop statistics and visualizations during the Assess phase. For example, Excel's countif formulas were used to count how many times each technique was cataloged in the system, and that data was sorted to display the Top 10 most used techniques observed in threat reporting. Cataloging and analysis are critical elements in developing threat actor playbooks and their corresponding heat maps, which

were inspired by Roberto Rodriguez's work to visualize an organization's ability to hunt each ATT&CK technique (Rodriguez, 2017). These heat maps provide a visual representation that informs prioritization efforts for detection, monitoring, and threat hunting efforts during the Act phase. This visualization empowers SOC managers and security leaders to drive discussions within the Security Operations Center (SOC) for closer monitoring of specific malicious techniques.

4. Analytical Findings

After processing 50 reports, the dataset consists of 122 unique Techniques with 613 total categorizations. This sampling entails the activity from 41 threat actors with incidents going back to 2012. This research led to several interesting findings and some critical lessons-learned with the potential to shape future analytical methodology developments. This section demonstrates the value in expanding upon this analytical methodology and how this type of report cataloging provides critical insight at the strategic, operational, and tactical levels of intelligence analysis and decision-making.

Analysis began with an assumption that working through threat reports to catalog them accurately for each Tactic and Technique was going to be a significant challenge. After all, the ATT&CK framework includes several hundred techniques with varying levels of technical details available for each. Instead, this research identified that a few threat researchers are already categorizing their threat reports using this model. They often included ATT&CK tables that were already mapped to IOCs and provided specific hunting suggestions, such as search strings and file paths to research, which can be seen in Figure 9. These mapping tables are immediately actionable by threat analysts and are the equivalent of an "Executive Summary for Threat Analysts." They provide a quick overview of the intrusion, the IOCs of interest, and how other analysts may detect this activity in their environments. In highly dynamic environments, such as a SOC, the immediacy of this threat data in a table is instantly applicable to threat analysis procedures.



Adversary Methodology	Discovery Tips
Persistence by Scheduled Tasks by XML trigger ATT&CK: T1053	Look for new and anomalous Scheduled Tasks XML triggers referencing unsigned .exe files.
Persistence by IFEO injection ATT&CK: T1183	Look for modifications and new entries referencing .exe files under registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.
Command and control (C2) established using hard-coded DNS servers	Look for PEs executions with run DNS lookups to 8.8.8.8:53. This may be applicable to sandbox and other malware processing technologies.

Figure 9: FireEye used ATT&CK in their Triton blog (Miller, Brubaker, Zafra, & Caban, 2019)

The system's usability and applicability extend beyond reports that were categorized during production by the original analysts. Indeed, the model lends itself to seamless processing of threat reports that were previously uncategorized. The example in Figure 10 below demonstrates how intrusion reports are translated using the MITRE ATT&CK techniques within the Airtable ATT&CK Tracker. From the NCCIC report on the left, it is apparent that this attacker conducted system information discovery, system network configuration discovery, and many other system enumeration techniques that belong in the MITRE Tactic "Discovery." While they practice using this cataloging system, analysts develop intimacy with the ATT&CK Enterprise Matrix and increase their speed in processing threat reports. This intimacy with the system not only improves their threat analysis skills, but also it advances their threat hunting skills as they develop a

deeper understanding of how other threat researchers have identified these techniques in various network environments.

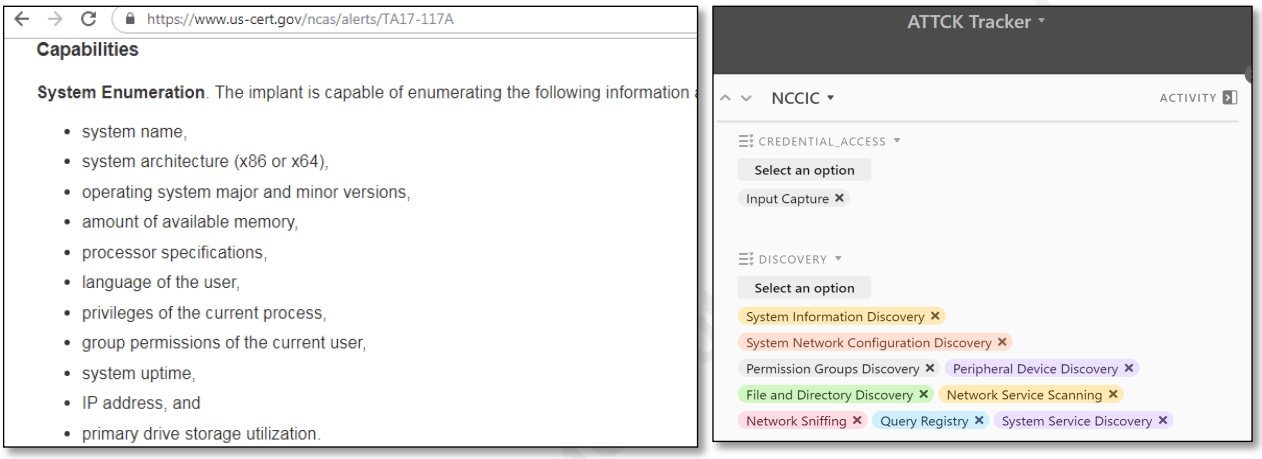


Figure 10: ATT&CK Extraction from TA17-117A into the ATT&CK Tracker (NCCIC, 2017)

In addition to the ad-hoc hunting that typically occurs while processing threat reports into a TIP, organizations conduct threat hunts in their environments to identify previously undetected malicious activity. Carbon Black defines threat hunting as "an advanced security function that combines a proactive methodology, innovative technology, highly skilled people, and in-depth threat intelligence to find and stop the malicious, often hard-to-detect activities executed by stealth attackers that automated defenses may miss before they can execute on their objective" (Carbon Black, n.d.). This research provides a structured methodology to identify specific Techniques for prioritized and in-depth threat hunts, as Carbon Black recommends.

This research led to the development of a Top Ten Reported Techniques list that provides operational level insights into these hunting prioritizations. In Table 2 below, MITRE Technique T1060, "Registry Run Keys/ Startup Folder," is the most observed technique from the sampled reporting. MITRE's T1060 webpage lists the default registry keys created by default in Windows and provides multiple examples of threat actors that have leveraged these keys to establish persistence on a host (MITRE, n.d.). Implementing a threat hunt for enterprise-wide collection and analysis of registry artifacts is a logical next-step for organizations conducting this type of analysis. Another method to identify hunt prioritization includes tracking "first observed" techniques, as these may

be emerging threats that are not detectable by current IDS/IPS capabilities. First-observed mapping requires further research and analysis that is beyond the scope of this project.

Rank	Technique	Count
1	Registry Run Keys / Startup Folder	23
2	Standard Application Layer Protocol	22
3	Spearphishing Attachment	21
4	PowerShell	20
5	Commonly Used Port	19
6	Obfuscated Files or Information	19
7	Command-Line Interface	18
8	System Information Discovery	17
9	File and Directory Discovery	15
10	Remote File Copy	14
11	Scripting	14

Table 2: Top "Ten" Reported Techniques

As part of this research, a notional defense-in-depth (DID) map is presented to demonstrate the strategic value of threat actor capability maps when applied to an enterprise. The fictitious company Notional Inc. developed a hypothetical enterprise defense-in-depth map, with a leading Endpoint Detection and Response (EDR) solution, an Intrusion Detection System (IDS), and an email security appliance. Collectively, this notional security stack provides monitoring coverage for the techniques highlighted in green. Yellow denotes where the existing tools provide enough visibility for threat hunting, but where the organization's visibility is limited. For example, Notional Inc.'s IDS can monitor and alert on HTTP traffic, but it is blind to TLS traffic in this notional environment, so the C2 Tactics are labeled yellow.

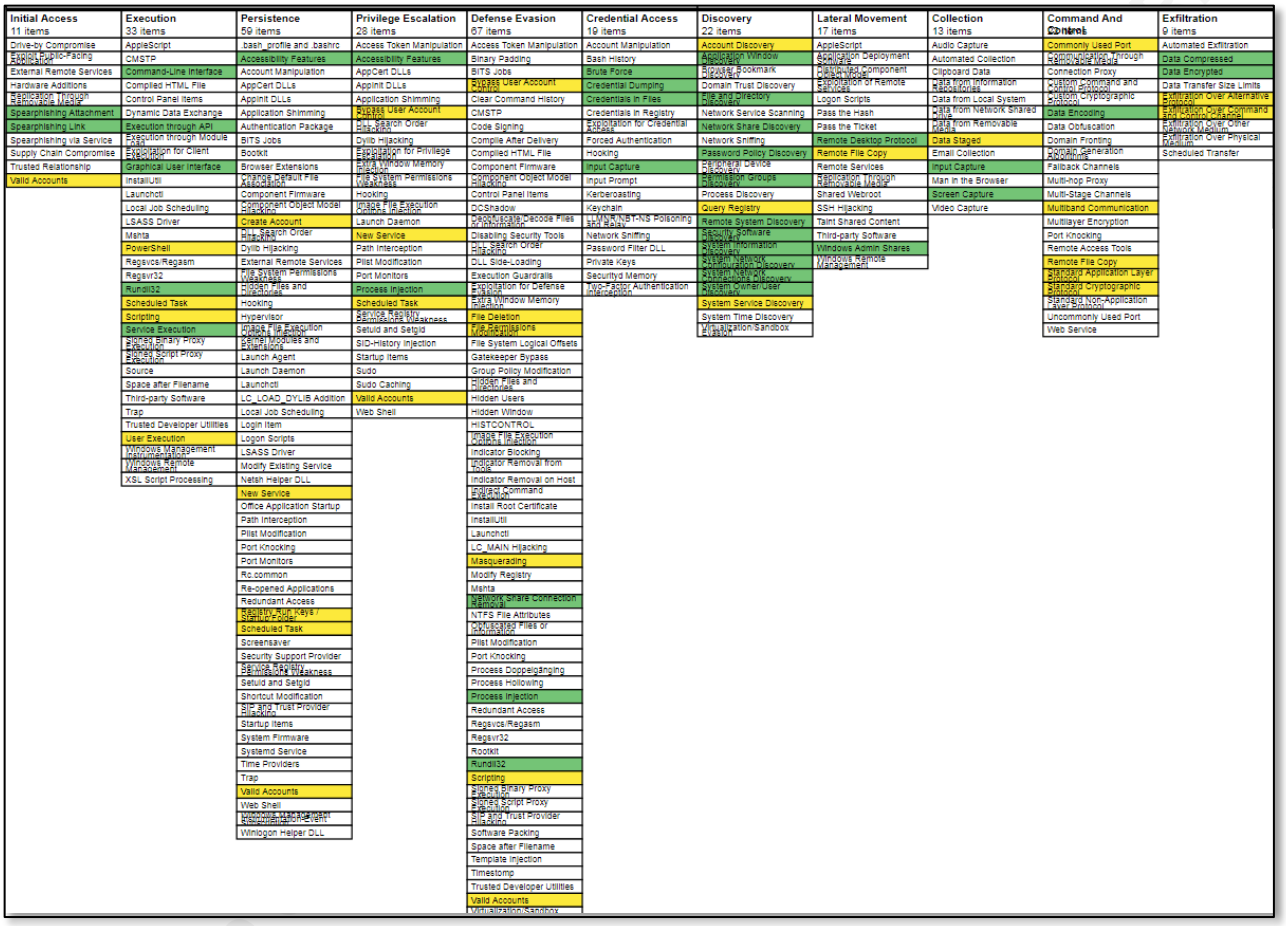


Figure 11: Notional Inc.'s Defense-in-Depth Enterprise Security Map

Using the data from this research, Notional Inc. created an actor capability map in the ATT&CK Navigator. Techniques that appeared in twenty or more documents are highlighted grey while those identified within ten to twenty reports are purple. This heat

Andy Piazza, andy.c.piazza@gmail.com

map enables organizational leaders to visualize the most active threat actor techniques and to make educated decisions for prioritization of projects and resources.

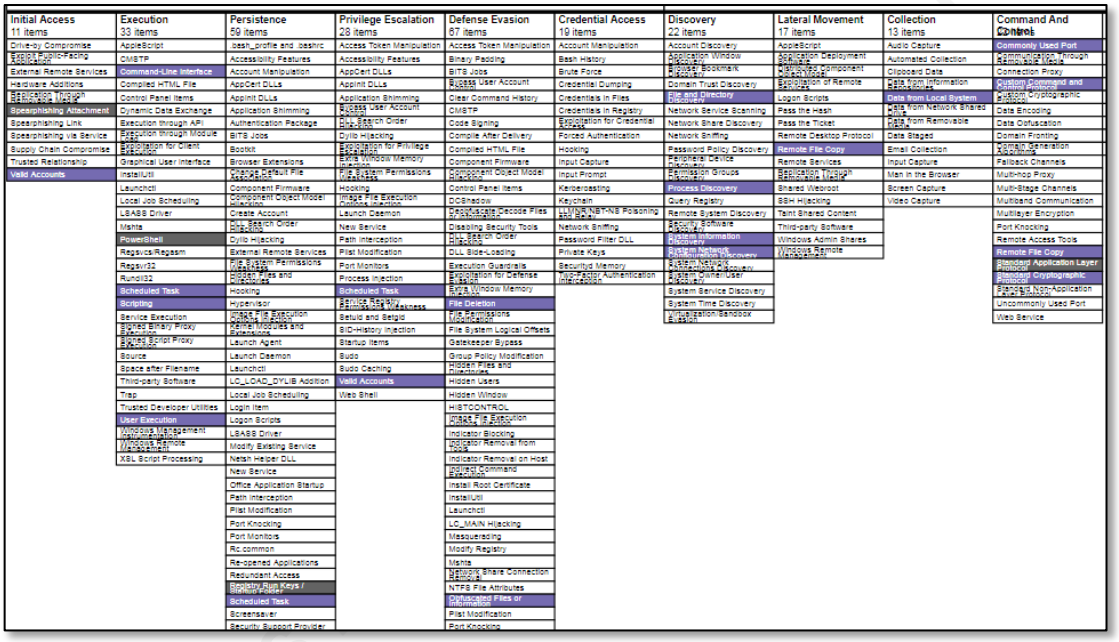


Figure 12: Threat Activity Heat Map

At the same time, the threat activity heat map provides a visual representation of the malicious techniques that require prioritized defense-in-depth considerations within the security stack and prioritized response from a SOC analyst perspective. Organizations reveal the strategic value of this analysis by overlaying this heat map on top of the defense-in-depth map. This overlay procedure with this researcher's heat map and the notional enterprise map identifies that the techniques "Registry Run Keys / Startup Folder" (T1060) and "Standard Application Layer Protocol" (T1071) are highly used by threat actors but are difficult to monitor with the currently deployed toolsets. In fact, the Notional Inc. enterprise map provides zero coverage for technique "Obfuscated Files or Information" (T1027) and research shows that it is the sixth most popular technique with over 19 reports referencing its usage. "Process Discovery" (T1057) and "Custom Command and Control Protocol" (T1094) are two additional methods that are actively used by threat actors but are not covered by the Notional Inc.'s security stack.

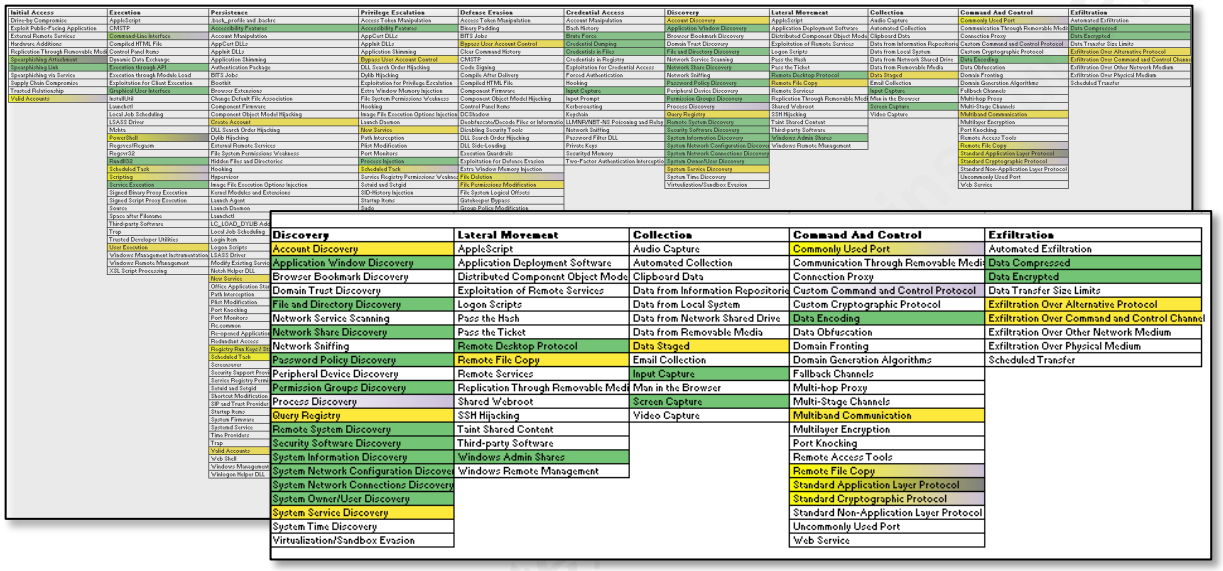


Figure 13: Activity Heat Map Overlaid onto Notional Inc.'s Defense-in-Depth Map (zoomed section for clarity)

This simple visual is a byproduct of routine threat management processes (e.g., intelligence analysts processing reports into a TIP), and yet it has significant implications for how strategic decision-making is accomplished for resource management. From this overlay product, the Notional Inc. management team identified multiple strategic, operational, and tactical level efforts to increase their ability to detect and defend against malicious activity in their environment. At the strategic level, this overlay initiated research by the Notional Inc.'s security engineering team to identify security capabilities that provide visibility into the techniques "Custom Command and Control Protocol" (T1094), "Obfuscated Files or Information" (T1027), and "Process Discovery" (T1057). At the operational level, SOC managers have instructed their detection and monitoring teams to prioritize response to EDR alerts concerning techniques "Valid Accounts" (T1078), "Scripting" (T1064), and "Registry Run Keys / Startup Folder" (T1060). At the tactical level, the hunt team prioritized threat hunts into "Registry Run Keys / Startup Folder" (T1060) and "PowerShell" (T1086).

5. Pushing the Research Further

Implementing MITRE ATT&CK as a structured methodology for collecting and categorizing threat reporting within modern TIPs and analyst platforms extends the

Andy Piazza, andy.c.piazza@gmail.com

applicability of those systems beyond basic threat indicator management. This research identifies various ways that organizations benefit from implementing MITRE ATT&CK within their toolsets, threat management workflows, and decision-making processes. Moving forward with this method, additional research is required to identify the best data structure for incorporating this model into a TIP.

MITRE's own Andy Applebaum blogged about his team's exploration into data visualization concepts for the ATT&CK framework and how that team developed an ATT&CK Roadmap (Applebaum, 2019). Their concepts include an actor heat map that compares APT28 capabilities against APT29, a capability gap matrix, and an adversary emulation diagram for red teams to use when planning operations. All three of these proof-of-concept diagrams are worth exploring. Specifically, threat analyst teams would benefit greatly from the actor heat map capability as a built-in function within their TIP, since the development of these heat maps is quite manual and cumbersome.

One challenge that this project identified is that it is time-consuming to search across the various tactic columns to find the appropriate ATT&CK technique. It may work better to have the full list of values in a single column to search and select from rather than stacking them under separate tactics. An unwarranted amount of time was lost during research while searching for the appropriate column for each technique. Future researchers should test multiple data structures for ease-of-use prior to implementation into daily processes.

Additionally, the value of this data increases with the size of the dataset. Therefore, further cataloging of threat reports will provide significant insight into the evolution of threat actor TTPs over time. For example, analysts with a large dataset of hundreds of incidents could develop actor timelines that visually depict when a specific threat actor was observed using a new technique. Figure 14 below is an example of how analysts can visualize an actor's capabilities over time. It is worth stressing that this is only a proof-of-concept timeline and that additional research into Turla's historical activity is required to accurately develop this model.

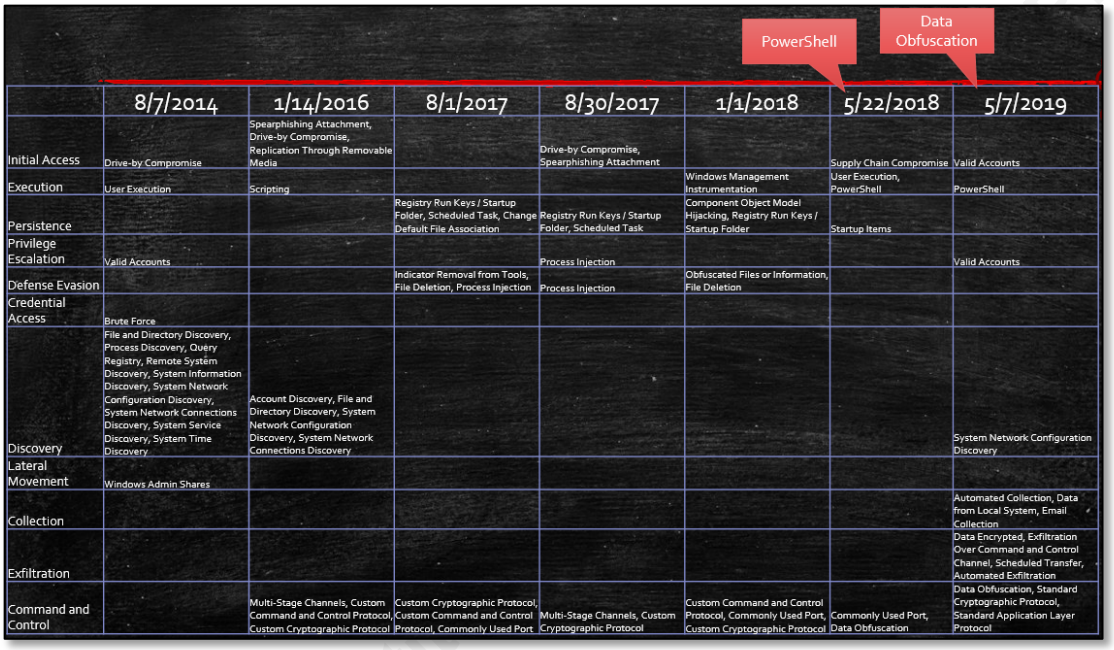
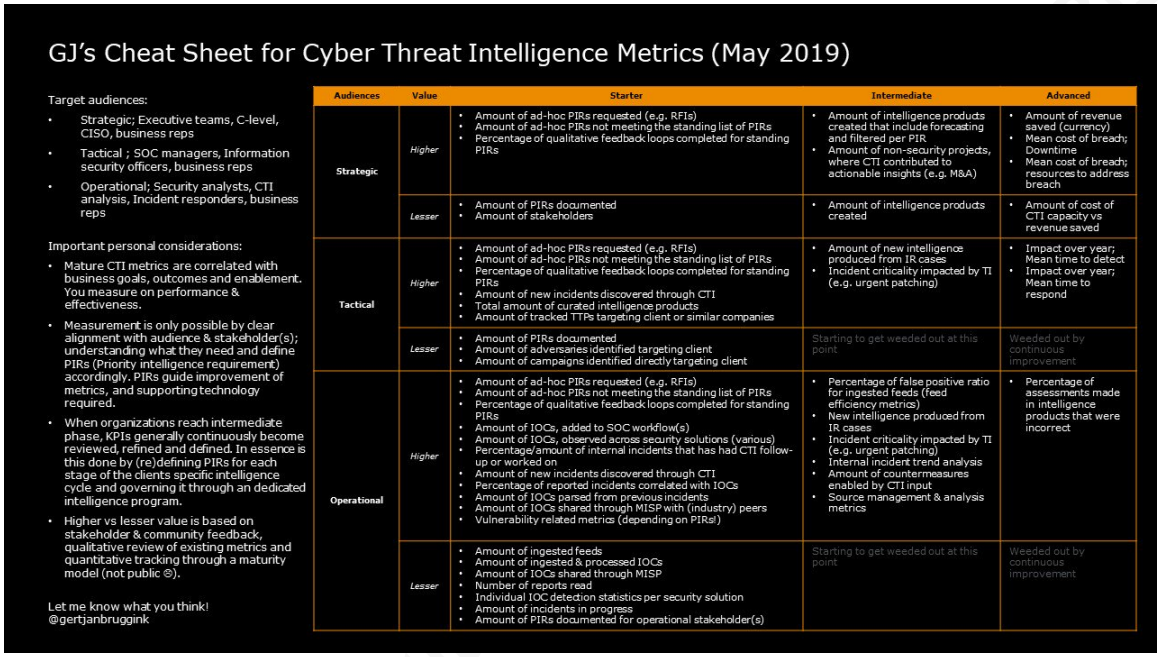


Figure 14: EXAMPLE- Turla Timeline

Timeline concepts are extendable to include demonstrating how long it takes for a newly discovered advanced technique to be employed by a threat actor that is assessed to be low-to-moderately skilled. That specific visualization is useful as it establishes an adoption lifecycle. Additional data points for that timeline may include when an open-source or commercial exploit kit incorporates new capabilities rendering them more accessible to low skilled actors.

Additional development is required surrounding CTI metrics and key performance indicators (KPI) with regards to the MITRE ATT&CK framework. One suggestion includes tracking changes made to the defense-in-depth coverage within the enterprise based on threat intelligence analysis and hunting results. Gert-Jan Bruggink provided useful insight into developing metrics and KPIs in his "GJ's Cheat Sheet for Cyber Threat Intelligence Metrics" (Bruggink, 2019). Tracking changes to the environment based on this structured methodology aligns with his consideration for classifying a metric as higher value or lower value based on "qualitative review of existing metrics and quantitative tracking through a maturity model" (Bruggink, 2019).

Andy Piazza, andy.c.piazza@gmail.com



GJ's Cheat Sheet for Cyber Threat Intelligence Metrics (May 2019)

Target audiences:

- Strategic; Executive teams, C-level, CISO, business reps
- Tactical ; SOC managers, Information security officers, business reps
- Operational; Security analysts, CTI analysis, Incident responders, business reps

Important personal considerations:

- Mature CTI metrics are correlated with business goals, outcomes and enablement. You measure on performance & effectiveness.
- Measurement is only possible by clear alignment with audience & stakeholder(s); understanding what they need and define PIRs (Priority intelligence requirement) accordingly. PIRs guide improvement of metrics, and supporting technology required.
- When organizations reach intermediate phase, KPIs generally continuously become reviewed, refined and defined. In essence is this done by (re)defining PIRs for each stage of the clients specific intelligence cycle and governing it through an dedicated intelligence program.
- Higher vs lesser value is based on stakeholder & community feedback, qualitative review of existing metrics and quantitative tracking through a maturity model (not public ®).

Let me know what you think!
@gertjanbruggink

Audiences	Value	Starter	Intermediate	Advanced
Strategic	Higher	• Amount of ad-hoc PIRs requested (e.g. RFIs) • Amount of ad-hoc PIRs not meeting the standing list of PIRs • Percentage of qualitative feedback loops completed for standing PIRs	• Amount of intelligence products created that include forecasting and filtered per PIR • Amount of non-security projects, where CTI contnbuted to actionable insights (e.g. M&A)	• Amount of revenue saved (currency) • Mean cost of breach; Downtime • Mean cost of breach; resources to address breach
	Lesser	• Amount of PIRs documented • Amount of stakeholders	• Amount of intelligence products created	• Amount of cost of CTI capacity vs revenue saved
Tactical	Higher	• Amount of ad-hoc PIRs requested (e.g. RFIs) • Amount of ad-hoc PIRs not meeting the standing list of PIRs • Percentage of qualitative feedback loops completed for standing PIRs • Amount of new incidents discovered through CTI • Total amount of curated intelligence products • Amount of tracked TTPs targeting client or similar companies	• Amount of new intelligence produced from IR cases • Incident criticality impacted by TI (e.g. urgent patching)	• Impact over year; Mean time to detect • Impact over year; Mean time to respond
	Lesser	• Amount of PIRs documented • Amount of adversaries identified targeting client • Amount of campaigns identified directly targeting client	Starting to get weeded out at this point	Weeded out by continuous improvement
Operational	Higher	• Amount of ad-hoc PIRs requested (e.g. RFIs) • Amount of ad-hoc PIRs not meeting the standing list of PIRs • Percentage of qualitative feedback loops completed for standing PIRs • Amount of IOCs, added to SOC workflow(s) • Amount of IOCs, observed across security solutions (various) • Percentage/amount of internal incidents that has had CTI follow-up or worked on • Amount of new incidents discovered through CTI • Percentage of reported incidents correlated with IOCs • Amount of IOCs parsed from previous incidents • Amount of IOCs shared through MISP with (industry) peers • Vulnerability related metrics (depending on PIRs!)	• Percentage of false positive ratio for ingested feeds (feed efficiency metrics) • New intelligence produced from IR cases • Incident criticality impacted by TI (e.g. urgent patching) • Internal incident trend analysis • Amount of countermeasures enabled by CTI input • Source management & analysis metrics	• Percentage of assessments made in intelligence products that were incorrect
	Lesser	• Amount of ingested feeds • Amount of ingested & processed IOCs • Amount of IOCs shared through MISP • Number of reports read • Individual IOC detection statistics per security solution • Amount of incidents in progress • Amount of PIRs documented for operational stakeholder(s)	Starting to get weeded out at this point	Weeded out by continuous improvement

Figure 15: "GJ's Cheat Sheet for Cyber Threat Intelligence Metrics (May 2019)" (Bruggink, 2019)

The last area identified for further research and development is the ATT&CK Matrix itself. The MITRE team is doing an outstanding job coordinating inputs from the community to add new capabilities, descriptions, and actor correlations. However, it is time for this information security community to contribute additional details to the technique pages on how to explicitly detect, hunt, and mitigate these malicious capabilities. Care must be taken to explain how to assess large datasets and how to remove false positives. Current threat hunting blogs and conferences serve as amazing resources for new threat hunters, but they are spread to the far corners of the internet. Having direct links from the ATT&CK technique pages to specific training will go a long way to increase the adoption of the framework.

6. Conclusion

Information security and cyber threat intelligence are highly demanding career fields with new technologies, capabilities, and malicious actors emerging into the market at a regular pace. Structured analytical methodologies, data models, and intelligence frameworks are critical components of effective intelligence programs. These program elements ensure that threat analysis focuses on providing timely, accurate, and contextual

products at the strategic, operational, and tactical levels of the decision-making hierarchy. This paper demonstrated the effectiveness of the MITRE ATT&CK framework at each of those levels.

Leveraging a structured analytical method to collect and catalog threat intelligence reports and cyber incidents within an analyst platform extends the utility of that data beyond the value of individual events. Essentially, the ATT&CK techniques become a metadata layer that turns a collection of reporting into a dataset that can be analyzed and acted upon independently of the contents of the reports themselves. This data modeling provides analysts with the ability to conduct trends analysis based on specific threat actors and emerging capabilities. It elevates their daily workstreams beyond the monotonous routine of endlessly reviewing threat feeds and pumping IOCs into the environment.

This research project adds to a remarkable canon of existing ATT&CK projects while remaining fresh and unique in perspective. The information security community will continue to push this framework forward and explore new use-cases for this model. Implementing this model into additional analyst platforms, security tools, and business processes will enable intelligence-based decision making at all levels of organizations that adopt this structured methodology. This project demonstrated how the MITRE Adversarial Tactics Techniques & Common Knowledge (ATT&CK) framework functions as a quantitative data model to prioritize resource management and security engineering efforts, inform computer network defense and incident response procedures, and guide technical threat hunts while informing decision makers at all three levels of analysis.

Andy Piazza, andy.c.piazza@gmail.com

References

Airtable. (2019). *Airtable*. Retrieved from Airtable: https://airtable.com/

Applebaum, A. (2019, March 4). *Visualizing ATT&CK*. Retrieved from Medium: https://medium.com/mitre-attack/visualizing-attack-f5e1766b42a6

Bowen, P., Chew, E., & Hash, J. (2007). *Information Security Guide for Government Executives.* Gaithersburg: National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/nistir/7359/final/documents/CSD_ExecGuide-booklet.pdf

Bruggink, G.-J. B. (2019, May 9). *GJ's Cheat Sheet for Cyber Threat Intelligence Metrics*. Retrieved from Twitter: https://twitter.com/gertjanbruggink/status/1126434409383714816

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The Diamond Model of Intrusion Analysis.* Hanover: Center for Cyber Intelligence Analysis and Threat Research.

Carbon Black. (2019). *Carbon Black Outperforms All Other EDR Solutions in MITRE ATT&CK™ Evaluation*. Retrieved from Carbon Black: https://www.carbonblack.com/why-cb/certifications-public-testing/mitre-attack-matrix/

Carbon Black. (n.d.). *What is Cyber Threat Hunting*. Retrieved from Carbon Black: https://www.carbonblack.com/resources/definitions/what-is-cyber-threat-hunting/

Carreon, C. (2018, July 25). *Applying Threat Intelligence to the Diamond Model for Intrusion Analysis*. Retrieved from Recorded Future: https://www.recordedfuture.com/diamond-model-intrusion-analysis/

Gourley, B. (2018, March 19). *Security Intelligence at the Strategic, Operational and Tactical Levels*. Retrieved from SecurityIntelligence:

https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/

Lockheed Martin. (n.d.). *The Cyber Kill Chain*. Retrieved from Lockheed Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Miller, S., Brubaker, N., Zafra, D. K., & Caban, D. (2019, April 10). *TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping*. Retrieved from FireEye: https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

MITRE. (2018). *ATT&CK Evaluations*. Retrieved from ATT&CK Evaluations: https://attackevals.mitre.org/

MITRE. (2018). *MITRE ATT&CK Navigator*. Retrieved from GitHub : https://mitre.github.io/attack-navigator/enterprise/

MITRE. (2018). *MITRE ATT&CKcon*. Retrieved from MITRE: https://www.mitre.org/news/corporate-events/mitre-attckcon

MITRE. (2019, May). *CTI/Enterprise-Attack*. Retrieved from GitHub: https://github.com/mitre/cti/tree/master/enterprise-attack

MITRE. (2019). *MITRE ATT&CK*. Retrieved from MITRE: https://attack.mitre.org/

MITRE. (2019, April). *Updates - April 2019*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/resources/updates/

MITRE. (n.d.). *T1060: Registry Run Keys / Startup Folder*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1060/

NCCIC. (2017). *AR-17-20045: Enhanced Analysis of GRIZZLY STEPPE.* Washington DC: DHS.

NCCIC. (2017, April 27). *TA17-117A: Intrusions Affecting Multiple Victims Across Multiple Sectors*. Retrieved from US-CERT: https://www.us-cert.gov/ncas/alerts/TA17-117A

Office of the Director of National Intelligence. (n.d.). *Cyber Threat Framework*. Retrieved from Office of the Director of National Intelligence: https://www.dni.gov/index.php/cyber-threat-framework

Andy Piazza, andy.c.piazza@gmail.com

Piazza, A. (2017, October 6). *SlideShare*. Retrieved from Putting the Human Back in the Loop for Analysis: https://www.slideshare.net/AndyPiazza/putting-the-human-back-in-the-loop-for-analysis

Rodriguez, R. (2017, July 17). *How Hot is Your Hunt Team*. Retrieved from Cyber Wardog Lab: https://cyberwardog.blogspot.com/2017/07/how-hot-is-your-hunt-team.html

ThreatConnect. (n.d.). *Andrew Pendergast: Vice President of Product*. Retrieved from ThreatConnect: https://threatconnect.com/team/andrew-pendergast/

ThreatConnect. (n.d.). *The Diamond Model for Intrusion Analysis*. Retrieved from ThreatConnect: https://threatconnect.com/resource/the-diamond-model-for-intrusion-analysis/

Tilbury, C. (2019, May 7). *Finding Registry Malware Persistence with RECmd*. Retrieved from SANS Digital Forensics and Incident Response Blog: https://digital-forensics.sans.org/blog/2019/05/07/malware-persistence-recmd

Unit 42. (2019, February 20). *PAN-unit 42 Playbook Viewer*. Retrieved from GitHub: https://github.com/pan-unit42/playbook_viewer

Zimmerman, E. (2019). *RECmd*. Retrieved from GitHub: https://github.com/EricZimmerman/RECmd

Figures

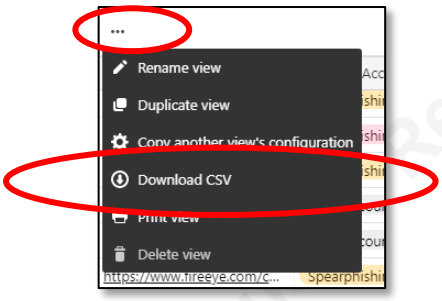
Andy Piazza, andy.c.piazza@gmail.com

Tables

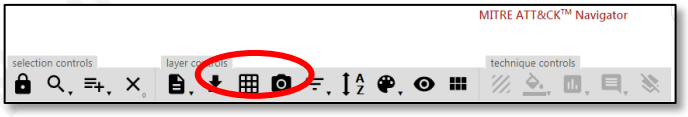
Andy Piazza, andy.c.piazza@gmail.com

Appendix
Calculating Technique Prevalence

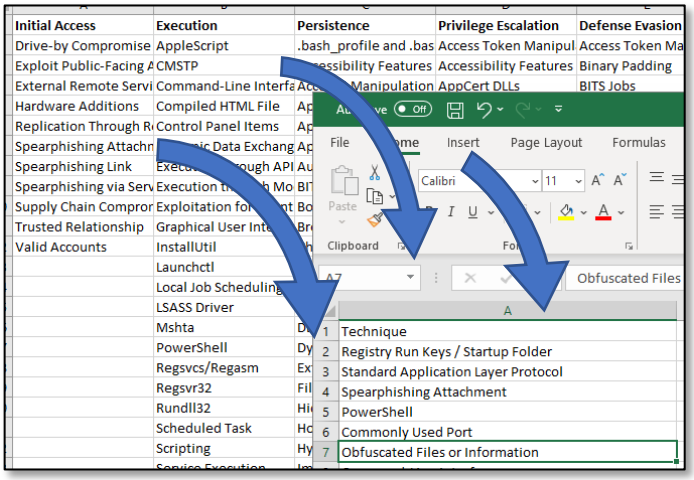
1. Export the cataloged data from Airtable.



2. Open in Microsoft Excel and save a working copy as an .XLSX extension, since .CSV does not support formatting and calculations.
3. Create a new blank worksheet in this file titled "Technique Count."
4. In a separate window, download the ATT&CK Navigator table to CSV.



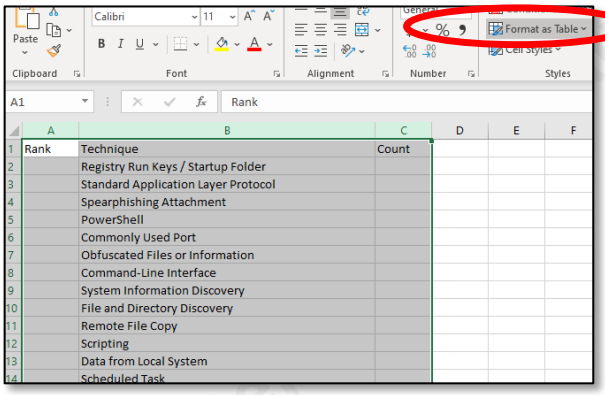
5. Manually copy and paste each column of techniques from the Navigator data and paste them in a single column within the new "Technique Count" worksheet that was created in step 3, above.



6. Close the ATT&CK Navigator CSV.
7. In the "Technique Count" spreadsheet, insert a new column to the left of the Techniques column and name it "Rank."

Andy Piazza, andy.c.piazza@gmail.com

8. Insert a column to the right of the Techniques column and name it "Count."
9. Select all three columns and all rows of data and click Format as Table.
    a. Note: do not select the entire worksheet.



10. In cell C2, which should be the first blank cell under "Count" column header, insert the formula:

```
=COUNTIF('Reports-Grid view'!G:Q,"*"& B2 &"*")
```

    a. "Reports-Grid view" is the name of the worksheet where the exported Airtable data resides.
    b. This formula tells Excel to count every time the technique listed in the Technique column (B2) of this worksheet is found in the data on the reports table's columns G through Q (Reports-Grid view'!G:Q).
    c. Since the data is formatted as a table, Excel will auto-extend the formula for the rest of the calculations.
11. Sort column C to show the highest count on top.
12. Enter a 1-10 ranking in the "Rank" column to generate the Top Ten Techniques list.

	A	B	C
1	Ra	Technique	Count
2	1	Registry Run Keys / Startup Folder	23
3	2	Standard Application Layer Protocol	22
4	3	Spearphishing Attachment	21
5	4	PowerShell	20
6	5	Commonly Used Port	19
7	6	Obfuscated Files or Information	19
8	7	Command-Line Interface	18
9	8	System Information Discovery	17
10	9	File and Directory Discovery	15
11	10	Remote File Copy	14
12	11	Scripting	14