5-2022

Cyber Frameworks Small Business Application

Sergio Gonzales
California State University - San Bernardino

CYBER FRAMEWORKS

SMALL BUSINESS APPLICATION

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology:

Cybersecurity

---

by

Sergio Gonzales

May 2022

CYBER FRAMEWORKS

SMALL BUSINESS APPLICATION

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Sergio Gonzales

May 2022

Approved by:

Dr. William Butler, Committee Chair

Dr. Conrad Shayo, Committee Member

Dr. Jay Varzandeh, Chair, Information & Decision Sciences Dept.

ABSTRACT

This project is an analysis of two cyber-attack analysis frameworks and how they may relate to a small business environment. Small businesses suffer significantly from malware attacks like ransomware. This analysis looks at the Cyber Kill Chain framework and the MITRE ATT&CK framework by looking at how each compare when applied to a simple small network and a malware attack. Each framework broke down the cyber-attack differently and by looking at how the frameworks performed within the simplified network provided insights to when small businesses should focus on malware risk reduction. Each framework, despite having different methods of analysis, arrived at similar conclusions about the environment. The role that users play in the environment when it comes to malware prevention becomes evident. The frameworks show the importance of proper user training in malware prevention. In small businesses and other organizations with small budgets investing in user malware awareness may prove a better investment than complicated expensive to buy and expensive to maintain solutions.

ACKNOWLEDGEMENTS

I would like to thank my family and friends for all their support and encouragement. To all who said I couldn't I want to express my thanks for motivating me to show you I could.

I would also like to thank Professor William Butler and Professor Conrad Shayo for guiding me throughout this project.

DEDICATION

Plain and simple, this is dedicated to the wisest and most fearless person I have ever known, my father Sergio Gonzales Sr.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE:

INTRODUCTION

Project Motivation

Ransomware and Malware have continued to evolve since first appearing on computer systems. Today the headlines are regularly broadcasting the odd names of the latest ransomware attack. On May 7, 2021, the Darkside ransomware hit Colonial Pipeline, effectively shutting down the largest pipeline of refined oil products in the US (Neuman, 2021). Colonial Pipeline's data that Darkside had encrypted was held to a 75-bitcoin ransom, at the time valued at 5 million U.S. dollars. Ransomware attacks have become more prevalent and more sophisticated over time. The reason for this is because ransomware has become a very profitable industry for those who design malware/ransomware and for those who use it to extort money from victims.

The news media regularly posts about the latest data breaches and attacks on large enterprises and the government. The items that are not newsworthy are the effects of cyber-attacks, like ransomware, on small businesses. Small businesses bear a large part of the burden of a cyber-attack. The impact of an attack on a small business can be significant, potentially resulting in the business shutting down (Johnson, 2019). The US government is aware of this fact. During committee hearings for the *American Cybersecurity Literacy Act,* Senator Amy Klobuchar (D-MN) said "Ransomware attacks are on the rise, putting Americans' data and privacy at risk. Too often people do not

know about steps they can take to protect themselves online" (Klobuchar, 2021). The US government recognizes that there is a threat to small businesses and has passed legislation like Senate Bill S.2483 Improving Cybersecurity of Small Organizations Act of 2021.

The problem of numerous cyber-attacks has led to the creation of various framework designs to assist in the analysis and defense of attacks (Orchilles, 2022). Frameworks are created as a foundational structure on which to build on top for analysis and defense. The government response to this threat has been a series of documents and sites to assist individuals, groups, enterprises, and government entities. The National Institute of Standards and Technology (NIST) produced the Risk Manage Framework (RMF) SP 800-37 (NIST.Gov., 2018,). This framework is based on risk and designed to assist in selecting and implementing risk mitigating controls (Dempsey, 2014). The RMF from NIST is made up of seven steps. The steps are Prepare, Categorize, Select, Implement, Asses, Authorize and Monitor (NIST.GOV, 2018). Each step is designed to assist an organization with managing its cyber security risk management program.

Along with the Risk Management Framework from NIST, many others have been created. The Cyber Kill Chain is the most widely known, developed by defense contractor Lockheed Martin in 2011. The Cyber Kill Chain framework is also made up of seven steps. Unlike those from NIST, these steps are not risk-based but instead based on the components of a cyber-attack. A methodology based on the attack creates a framework that looks at both at offense and

defense. The premise is that understanding every move of the adversary will allow the defense the opportunity to stop the attack at one of the seven steps.

Another framework that has been developed, that is also based on the actions of the adversary is the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. The MITRE ATT&CK framework, unlike the others is made up of 14 tactics instead of seven and are used to create matrixes that assist in analysis. The tactics used by the ATT&CK framework are Resource Development, Initial Access, Execution, persistence, privilege escalation, defense evasion, Credential access, discovery, Lateral Movement, Collection, command and control (C2), exfiltration, and impact. With this many tactics, the matrices can be large and incredibly detailed (MITRE ATT&CK, 2021).

All the frameworks are designed to assist in the creation of a defense posture and when the defense fails. They assist in analyzing what went wrong and help to fill the gap that was exploited. Many private companies use one of these or a combination of frameworks for assistance in data defense.

Problem Statement

The US government has identified the threat of cyberattacks such as ransomware on small businesses (S.2483 - 117th Congress, 2022). Many of the small businesses defined by the U.S. Small business administration (SBA), small business size standards also have the budgets to have a framework to their

business. Within the SBA standards is the category of Microbusinesses. Microbusinesses are those employers with 1-9 employees, and in 2016 made up 74.8 percent of all private-sector employers (Headd, 2019). Many of the businesses this size are called Small Office, Home Office (SOHO) businesses. These microbusinesses have neither the budget nor expertise to apply one of these frameworks.

This project will answer the following questions:

- Which components of the Cyber Kill Chain and the ATT&CK frameworks are most relevant to the small office network?
- How can these components be implemented to small office (Microbusiness) networks?

This culminative experience project is organized as follows: chapter 2 will provide a review of the literature, chapter 3 will describe the methods used to answer the project questions, and chapter 4 will analyze the steps of the frameworks and determine the components that are most relevant to Microbusiness networks. Chapter 5 will provide the discussion, conclusions, and areas for further research.

CHAPTER TWO:

REVIEW OF LITERATURE

Cyber Kill Chains, What are They?

The kill chain was originally a military concept that was used to define the structure of an attack. The idea was that for an adversary to complete their main objective, they would have to complete a series of intermediary goals (Greenert & Welsh, 2013). It is the sum of these goals that creates the “kill chain” and each step links to the next step. To stop the adversary at any one of the steps breaks the chain. To break the chain the defenders must have a defense in place that mitigates a step in the kill chain. The steps to mount a defense are the inverse to steps for the kill chain to succeed.

The Cyber Kill Chain concept is essentially the same as the military version. You have an adversary with a goal which must be stop at one of the steps to prevent the adversary from reaching their goal. In 2011, military contractor Lockheed Martin developed their Cyber Kill Chain from a threat model they identified. Lockheed Martin identified a threat model from which it developed the Cyber Kill Chain. Lockheed Martin identified a threat model from which it developed the Cyber Kill Chain (*Hutchins E, et al., 2010)*.

There was a new threat landscape evolving and Lockheed Martin developed the model to address this new threat of the Advanced Persistent Threat (APT). The APT is an adversary with a high level of expertise and

substantial resources at their disposal. The APT can reach the objectives through many attack vectors and is not limited to a single methodology. The APT looks to establish footholds to exfiltrate information on a continuous basis (Hutchins et al., 2010). The cyber frameworks were created to mitigate the failures of previous conventional incidence response methods that were ill prepared to address the problem the APT posed. Conventional incidence response before the creation of frameworks had two flawed premises, item 1: response should happen after the point of compromise and item 2: the compromise was from a fixable flaw (Hutchins et al., 2010). The goal of the APT is to remain undetected for as long as possible, so in the case of item 1 responding after the compromise is a problem as the APT is completing their mission until discovered.

On December 20, 2020, the company FireEye announced that they had discovered an intrusion that used the popular commercial software Orion created by the company SolarWinds. FireEye named this backdoor malware “SUNBURST.” It was sophisticated software and a perfect example of an APT deployment. The threat actors designed their mission around SUNBURST knowing that it would not appear as an indicator of compromise (IOC) to traditional identification systems. This made scanners and other platforms that would normally look for IOC activity ineffective. FireEye announced their findings in December 2020 and the first evidence of confirmed sunburst activity occurred in March of 2020. The attackers that had compromised SolarWinds released their malicious code int the ORION software platform in February 2020. Once on the

system SUNBURST went to work unnoticed and undetected for 6 months by many if not most organizations until the FireEye announcement in December. This headline-making APT is an example of the real threat that ATPs' can have on an organization. According to the SEC filing from SolarWinds, 18,000 of its 300,000 customers had an installation of the products containing the SUNBURST vulnerability (cisecurity.org, 2021).

Multi-Layer Approach

The sophistication of the modern adversary has meant that defense must take on a multi-layer approach. The high-level view of architecture is not sufficient to identify, categorize, document, and mitigate gaps in architecture. NIST 800-53 under Systems and Services acquisition family (SA) is section SA-8. Section SA-8 Security and Privacy Engineering principles cover the principle of defense-in-depth (NIST, 2020). Defense-in-depth is not a one-to-one solution, it is instead a comprehensive methodology for protecting every identified asset. Infrastructures are made up of various layers. The layered approaches of NIST are risked based designs that look at the risk to an asset to determine how to apply a defensive control. The steps and flow of the risk management framework from NIST SP 800-37, Figure 1, are a complementary and iterative cycle allowing items to be revisited in any order.

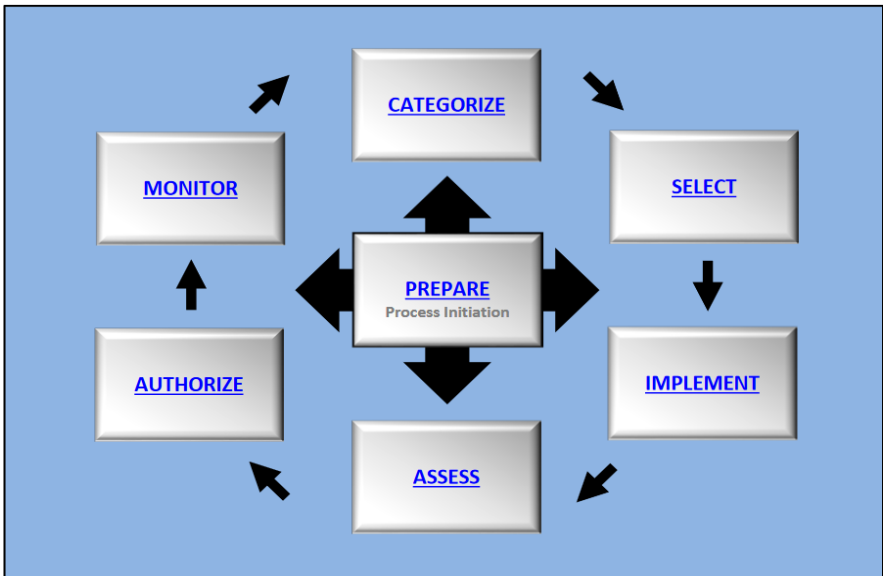


Figure 1. Risk Management Framework (Csrc.nist.org, sp. 800-37)

Cyber Kill Chain (CKC) Review

The Cyber Kill Chain (CKC) was developed by defense contractor Lockheed Martin in 2011. An intrusion-based model in which the adversary must breach the environment's perimeter, establish a foothold inside the environment, and move towards exploiting the "confidentiality, integrity and availability" (CIA) of the environment. From analysis of intrusions is how the CKC intrusion model was defined (Hutchins et al., 2010). As previously noted, the CKC is a seven-step process based on the intrusive actions of the adversary. The ideal scenario is to stop the adversary at one of the steps prior to the seventh. The adversary must move through each of the steps to accomplish their objective. This is key in deconstructing an attack when the attacker is successful. Being able to reverse engineer an attack after a breach creates a lesson learned opportunity for the

organization involved to resolve a vulnerability after being exploited. More importantly, the ability to reverse engineer an attack allows researchers to discover and analyze any new evolving techniques of the adversary. This is how IOCs are discovered and put into practice. By understanding the seven steps and how they flow together better defense practices can be created. Steps of the Cyber Kill Chain

The CKC is composed of seven steps to understand an attack and assist in preparing a defense. The links of the CKC, figure 2, are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and action on Objectives.

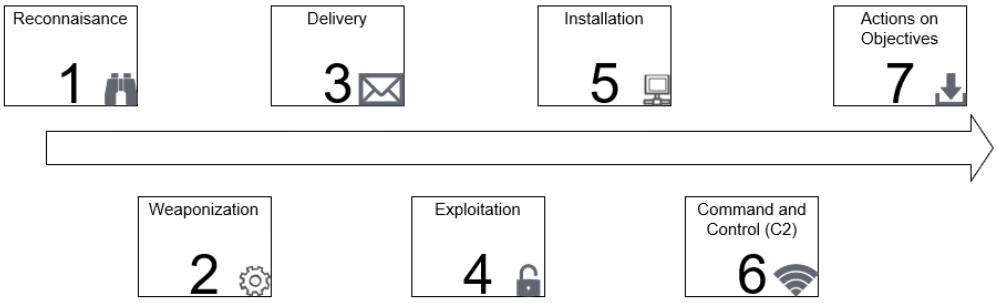


Figure 2 Cyber Kill Chain Steps

Step 1: Reconnaissance Here the adversary conducts research to identify potential targets. Targets are often found through Open-source intelligence (OSINT). Another method for finding a target is using Botnets to scan perimeters for vulnerabilities. This is the mission planning phase of the operation.

Step 2: Weaponization The weaponization phase is where the information gathered during phase one is used to create a method for delivering the payload. This could be inserting the payload into a file that can be emailed. Creating websites that can install malicious code via the browser of file download. The main goal here is to create malware that takes advantage of an exploit and turns that into a deliverable payload.

Step 3: Delivery This is the phase that is the official start of the adversary's operational contact with the target. It is here that the payload is launched at the target. This could be a website exploit, a phishing email to a malicious site, and email with a malicious document, etc. The Lockheed Martin Incident Response Team (LC-CIRT) found that the three most common vector for delivery of the payload were email attachments, websites, and USB media (Hutchins et al., 2010). Understanding the delivery vectors allows an organization to identify the delivery vectors of the highest risk to the organization. This knowledge is from understanding the operation of this phase. Knowing and understanding these vectors gives the defender the first opportunity to mitigate an attack this step. An example of a mitigation could be scanning emails for malicious data before they are allowed to enter the user's mailbox for viewing.

Step 4: Exploitation It is in the exploitation phase that the payload is delivered within the environment. The malicious payload is now within the organization. The payload will exploit the target either by taking advantage of a vulnerability in an application or the operating system. Sometimes, adversaries

can take advantage of users by exploiting user behavior, such as getting a user to open an email. This is the phase where the defender gets the second opportunity to act in defense of the organization. The intruder is now inside the environment. Here is where defense begins to make a difference. If an email with a malicious attachment now sits on an internal mail server this could be that any scanners failed to identify, alert, log, quarantine/sanitize the malicious payload. An effective tactic at this phase can be as simple as the training of users to be aware of and be able to identify malicious emails. This type of training can stop an adversary at this step.

Step 5: Installation In the installation phase the adversary seeks to establish persistence. The goal of the attack at this stage is to establish itself as an APT. This is performed through the installation of an application, usually some type of backdoor that allows access to the system even after the original exploited vulnerability is resolved. Through this backdoor application, the adversary can achieve and maintain persistence. This is the third opportunity for the defender to stop the attack. Having tools in place that can possibly detect, alert, log or act on anomalous behaviors is a start to stopping the adversary at this step.

Step 6: Command and Control (C2) This is when the malware or application establishes communication to outside the organization to the C2 network. Once communication to the C2 network is created, the adversary has now established a presence within the target environment. The defender must

now discover the communication to the C2 network by identifying the outbound communications. Blocking communication to the C2 will break the chain at this step. This will involve detection of the traffic but often the APT will hide the communication within common protocols to try and obfuscate detection.

Step 7. Action on objectives. This is the final step. The adversary now has established access to the environment and can begin moving toward accomplishing their objective. The objective can be anything from collecting data, exfiltration, destroying infrastructure from the inside, lateral movement through the environment, and overwriting or corrupting data. With established persistence, the APT is free to explore the environment looking for the adversary's objective requirements. At this stage, the defender must react as fast as possible to any signs of intrusion. Time is critical for defenders once the APT is inside the network and actively working towards completing the objective. The adversary will continue establishing a greater foothold in the environment until the defender detects, identifies, and stops the attack.

The CKC has also served as a valuable diagnostic and analysis tool by dividing the attack into smaller segments that can be looked at individually in greater detail. When multiple attacks are executed that follow a similar methodology during the kill chain analysis patterns begin to emerge. Identifying the patterns allows for a greater understanding of the attack. T These identified patterns give the defender mitigating controls at the steps where the emergent

patterns point to an exploitable weakness or where a control can be used to break the chain.

MITRE ATT&CK Review

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a framework designed to around the behavior of the cyber adversary. Like CKC it has various steps called tactics of the attack lifecycle and the targeted platform. MITRE ATT&CK evolved out of a MITRE project to document adversarial tactics, techniques, and procedures (TTPs) against Microsoft Windows systems. Developed in 2013 the first ATT&CK framework was designed around the Windows enterprise environment. Continued research by MITRE expanded the framework to 96 techniques within 9 tactics. The project has continued to evolve and expand. In 2017 MITRE ATT&CK included Windows, MAC, Linux and Mobile, added Cloud in 2019 and Integrated Control Systems (ICS) in 2020 (Strom et al., 2018).

ATT&CK has demonstrated that it is applicable in various use cases. Like the CKC, it can be applied to adversary emulation and defense gap analysis. One use case is in the development of behavioral analytics. Analytics that look at behaviors are useful in detection of malicious activities within an environment without the need of prior knowledge of the exploitation method. As shown in the CKC model identifying patterns is also a major feature of the ATT&CK model. In today's large organization a key operational feature is the Security Operation

Center (SOC); it is at this centralized location where large enterprises aggregate all their monitoring and alerting. The ATT&CK framework is useful to the SOC to measure how effective a SOC is at detecting, analyzing, and reporting malicious activities

The ATT&CK Matrix

The MITRE ATT&CK framework is a matrix made up of tactics known to be used by adversaries to reach an objective. The list of tactics is equivalent to the 7 phases of the CKC. The ATT&CK framework has taken the tactics and associated them into a series of techniques. The matrix is formed when the tactics are associated with specific techniques. For example, the reconnaissance tactic contains the active scanning technique. With each tactic there are several techniques, for example, reconnaissance contains 10 techniques. The adversary must move through each of the 14 tactics to reach the objective, in the exact same way that in the CKC the adversary must move through the 7 phases. MITRE has created matrices for several architectures under three main categories enterprise, cloud, mobile and ICS.

The Tactics of the ATT&CK Matrix

The ATT&CK matrix for enterprises contains 14 tactics. Within each tactic there are a series of techniques. Each technique has one or more sub-techniques defined. The most significant feature of the matrix is that each technique describes in detail what the adversary is trying to accomplish with that technique. This is important for conducting an analysis of a successful attack by an

adversary. The fourteen tactics of the ATT&CK matrix for enterprises are Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact (see APPENDIX A).

Tactic 1 Reconnaissance. The adversary gathers information to plan an operation. This could be done through active scanning, or gathering identity information like email addresses, credentials, and employee names.

Tactic 2 Resource Development. In this objective the adversary may need to acquire resources. An example technique inside this object is Acquire Infrastructure and this contains the sub-technique: domains. The adversary may acquire domains for phishing email campaigns or C2 network operations.

Tactic 3 Initial Access. The adversary is actively trying to gain access to the network. A commonly used technique listed in this objective is phishing and includes three sub-techniques with one being the spear phishing attachment. In this type of phishing email a malicious attachment is included in the email to attempt to gain access to the organization's network. Tactic three, like the third step in the CKC is the first point where the defender has an opportunity to place a defensive control to stop the progression of the attack.

Tactic 4 Execution. This objective consists of techniques that will run adversary-controlled code on the local system when executed. There are twelve techniques in this tactic, many of which have sub-techniques to further provide

details as to how this objective may be accomplished. This is another tactic where the defense can place controls to mitigate exploitation.

Tactic 5 Persistence. At this stage in the ATT&CK matrix the adversary is inside the environment and needs to establish a persistent foothold. This tactic has nineteen techniques, many with sub-techniques. The techniques used for this tactic will maintain the adversary's access regardless of system interruptions that would usually cut access.

Tactic 6 Privilege Escalation. The techniques within this tactic are about the adversary gaining a higher level of privilege so that they can continue moving forward towards mission completion. This step may involve the adversary going from standard user permissions to root level or administrator level. These techniques often overlap with those from the persistence tactic.

Tactic 7 Defense Evasion. In defense evasion the adversary is trying to actively avoid being detected. This tactic contains techniques and sub-techniques that are used to stop security software or use trusted processes to hide malware applications. Defense evasion has the largest number of techniques with twenty-nine in total.

Tactic 8 Credential Access. This is one of the most important tactics to the success of the adversary. Capturing allows the APT to expand its presence by being able to use valid credentials to access systems. In environments that impose a single sign-on (SSO) system, one compromised account will give the

adversary unrestricted access to all the authorized resources of the compromised account.

Tactic 9 Discovery. This is a crucial part of the attack the adversary is at a point trying to learn as much as possible about the environment. Stopping the adversary at this part of the operation will limit how the adversary will act to reach the next phase and may not be able to continue forward.

Tactic 10 Lateral Movement. Here, the adversary moves throughout the environment, often using valid credentials to move throughout multiple systems. Lateral movement can be propagated through tainted share techniques, by placing malicious software in shared locations where other users can trigger the software. This places the adversary at the persistence phase of the newly compromised machine. A mitigation for this would be execution prevention by blocking the execution of malicious software.

Tactic 11 Collection. The now identified materials of value are collected. With the data collected the usual next step is to steal the data via the exfiltration. The APT will often try to maintain access to the compromised system for as long as possible. This will involve an intermediary step twelve before exfiltration of data or in conjunction with removing the data.

Tactic 12 Command and Control. This C2 tactic, if successful allows the adversary to communicate with the system(s) in the environment under the adversary's control. To avoid detection, the attacker must hide the communication channel by appearing normal expected network communication.

A common mitigation is the use of network intrusion prevention systems that try to identify the C2 specific traffic.

Tactic 13 Exfiltration. This tactic consists of the adversarial techniques used to remove the high value target data away from the organization and into the adversary's possession. That data maybe exfiltrated via the C2 channels or some other channel. This step is extremely critical for the organization as data is actively being exfiltrated out of the environment. The amount of data to leak out of an environment is directly related to the amount of time it takes for the defender to detect and close this phase of the attack. This tactic is difficult to mitigate with preventive controls because the communication is based on taking advantage of already exploited system features. The best option for mitigation will be the detection of exfiltration techniques, such as the detection of unusual network traffic.

Tactic 14 Impact. This tactic is the most detrimental to the organization. The goal of this tactic is to destroy systems and data. The most technique seen from this tactic is the Data Encrypted for Impact technique. This impact tactic technique is more commonly known as the ransomware attack.

The MITRE ATT&CK framework is designed to be very flexible and detailed in the way it approaches an intrusion-based attack. The layout of the matrix creates a flow path as the adversary moves along the objectives executing Adversarial Tactics and Techniques (ATT); this road map can easily be followed. Following the attack trail assists in the design and implementation of mitigating

controls. These trails created from the analysis of multiple organizations hit by a similar attack have allowed the MITRE ATT&CK framework to create groups of related intrusion activities. These groupings are the designations for clusters of similar activities that may also overlap with other groupings. The groups can then be correlated to actual threat actor groups or communities.

CHAPTER THREE:

METHODOLOGY

Analysis Process

Kill chain frameworks have proven to be an effective tool for analyzing cyber-attacks from both offensive and defensive viewpoints. Defense against the adversary can be a challenge for large companies and possibly harder for small companies. To the attacker both are important targets. The frameworks have proven effective for large organizations. The focus of this project is not to evaluate, claim or determine efficacy. The purpose is to look at the frameworks from the defensive posture of a small office network environment.

Procedure.

The process for comparing the two frameworks will be done by taking an adversarial approach at the defender network. By following the adversaries' attack step-by-step the goal is to associate the steps of the attack with a step in a framework. The identified steps of the framework will be correlated against points on a network diagram. If the points on the network can be identified, what are the recommended mitigating controls from the framework, and is that control in or available? This will result is data that can be analyzed to compare the frameworks.

The Frameworks. The two frameworks will be compared separately. The seven steps of the CKC framework will be applied to the network and aligned to the adversary’s attack process. Then the 14 steps of the ATT&CK framework will

be applied. They will both go up against the same adversary and the same network.

The Target: Small Business Network. The network is a basic small business network. This is a low-budget network and is limited in its allocated resources. Sophisticated mitigating controls are non-existent due to the low budget requirement of the small business. The network will be defined simply as desktops running windows 10. In 2020 windows 10 made up 72.2 percent of windows, including machines, desktop, and laptop (Keizer, 2020). Windows 10 includes the Windows Defender Antivirus, a local software firewall product for free. In any environment where cost is a factor “free” holds a significant stake and because Windows Defender is free many competitors offer a free version of their software. This is updated along with the operating system on “Patch Tuesday,” Microsoft’s now well-known second Tuesday of every month patch release cycle. (Security Update Guide FAQs, 2022). Lastly this simple network will have the internet access firewall that is supplied to anyone who signs up for a basic internet plan from their local Internet Service Provider (ISP). By default, all these ISP supplied devices block inbound internet traffic and allow outbound internet traffic. These devices function like the ones that an ISP would supply to home users when a person requests internet for their home. This level of simplicity and lack of sophistication provides the most basic test bed to compare frameworks.

The Adversary: Bazar Malware. The adversary will be the Bazar malware which had two common forms: the BazarLoader malware or BazarCall malware (Duncan, 2021). This adversary has several features that made it a good candidate for the project. One feature is that it is a good candidate for spam email delivery. Investigations showed that several methods were used to email it out as spam emails. The emails used combined various social engineering techniques to get the payload on to the system. The first example campaign was BazarLoader it targeted large enterprises using business-focused emails. The emails appeared to be invoices or inquiries that contained a malicious attachment or link to a malicious site. The emails were made to appear personal to try and get the employee to open the malicious attachment (Brandt, 2021). Another BAZAR malware campaign was BazarCall. This campaign combined two social engineering techniques. The first part was a spam email with no personal information, links, nor attachments; rather the email stated that a free trial subscription was expiring and about to auto renew for an expensive fee. To stop the auto-renew from happening the victim is directed to call customer service at some phone number to cancel the auto-renew. Any person calling the number would talk to someone who would direct the victim to a very professional looking website with the unsubscribe details and the unsubscribe button. Clicking the button delivers the malicious payload infecting the local machine with BazarLoader (Duncan, 2021).

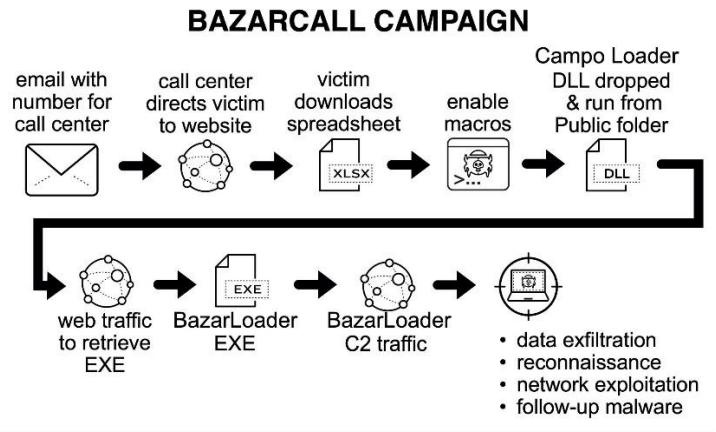


Figure 3 BazarCall Chain of Events (Duncan 2021)

The Evaluation Process.

Step 1. Align Framework to Malware. This process involves taking the Bazar processes and corelate them with the steps of a framework. The Bazar process contains nine events. The malware processes may fall under a single framework step, multiple steps, or none of the steps. After the malware and the framework have been aligned, proceed to the next step.

Step 2. Align Malware to the Network. Involves taking the Bazar malware processes and corelating it to the target network. The results of this analysis will be identical for both tests because the network and the malware are not changing. This step only needs to be performed once for the Bazar malware.

Step 3. Create Final Overlay. This step involves combining the first two steps into a final diagram that demonstrates how all the pieces interact for the given framework. This test will be used to look at how well the frameworks mesh

with a small network. This step should provide enough detail for the data needed to look at our problem statement.

CHAPTER FOUR:

FRAMEWORK ANALYSIS

This chapter will follow the process for the analysis procedure. The process will be applied to each framework. The adversary and the network will remain constant. The adversary will be the well-known and studied Bazar malware.

Cyber Kill Chain Analysis

The Lockheed Martin Cyber Kill Chain (CKC) is a seven-step process based on the intrusive actions of the adversary. The steps of the CKC are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Action on Objectives.

Step 1. Align to CKC Framework to Malware

The first step of the CKC is reconnaissance and is considered a pre-attack step. The adversary is not interacting with the target but during this phase is researching potential targets or developing a strategy to reach out to targets, like with the use a spam phishing email campaign. Targets rarely detect this phase of the CKC even if the target is well funded. In the case of small businesses with small budgets and low technical knowledge they do not usually have the resources to conduct this phase.

The weaponization phase is the second stage in the CKC and a pre-attack phase. This is the step when the Bazar malware is developed. The weaponization as seen with Bazar is learned after the discovery of Bazar. There was no evidence of the development life cycle prior to the malware first detection.

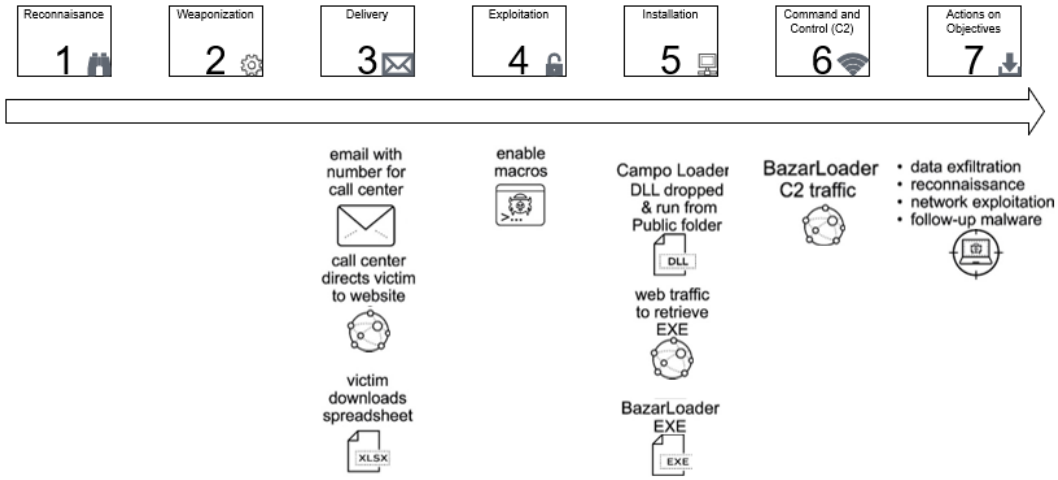


Figure 4 CKC With Bazar, Based on Duncan,2021

Step three “Delivery” is the first point of contact between the CKC and Bazar malware. Delivery contains all actions required to get the weapon onto the target systems (Hahn et. al., 2015). During the summer of 2021, the samples of the Bazar there were being spread via three campaigns. All three campaigns used email in some form to get the attention of the target (Duncan, 2021). In the two most common campaigns, the adversary would either email the target an email with a malicious attachment or an email with the contact information for a

call center. The call center would direct the target to a web site where the target would download the weaponized spreadsheet document (Duncan, 2021).

Table 1. Two Common Delivery Methods

Option A	Option B
Send email with malicious attachment	Send email with call center request
Attachment is malicious spreadsheet	Call center redirects victims
	Victim downloads malicious spreadsheet

The Exploitation phase is the key phase for how the CKC, Bazar malware, the adversary and target line up. At this point the payload is on the target system ready for deployment. The document contains an action or set of actions known as macros that want to run on the target system. Macros are disabled by default and the user interaction is required to allow the macros to run. The confidence to allow the macro to run has been instilled in the target user via social engineering measures in the delivery phase.

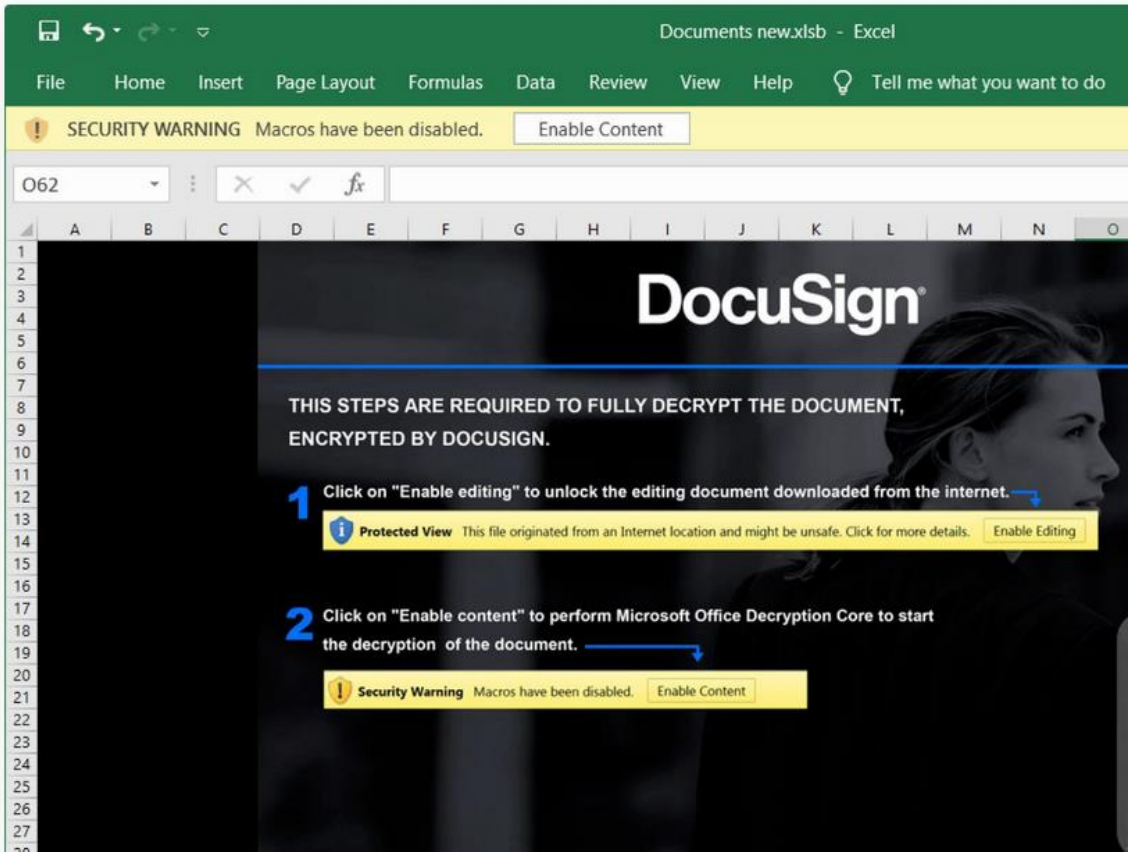


Figure 5 Screenshot of the Malicious Excel Spreadsheet (duncan,2021)

Phase five the installation of the BazarLoader executable. For this phase to be completed there are 2 steps that need to be accomplished with the macros being enabled in the previous phase. The first part is the macro needs to be able to exit the system. If the macro can exit the network to the adversary's remote systems, then it retrieves the BazarLoader executable and installs it on the local system. The level of control that the adversary can exert over the system is based on the level of exploitation the attack was able to perform. This step is

where the adversary establishes persistence by modifying the system to maintain remote access to the system.

Phase six of the CKC framework is when command and control (C2) is established. The adversary can now remotely access the system through the C2 channel. This two-way communication channel lets the adversary manipulate the target system. With remote access established, the adversary can move to the next step.

The last phase in the CKC is the action on objectives. The adversary can now proceed to completing their mission objectives. This can be collecting data, exfiltration of data, and further reconnaissance of the target environment looking for ways to expand the scope of the mission. The defender must detect this phase and stop the adversary as soon as possible because the adversary is now actively acting within the environment.

Step 2. Align Malware to Target

The Bazar malware primary focus is to exploit the user to get the malicious software on the target system. Once the malware is on the target system it proceeds to exposit the local host to gain access to the rest of the network. As a result, the adversary remains a persistent threat until it is discovered and cleansed from the system.

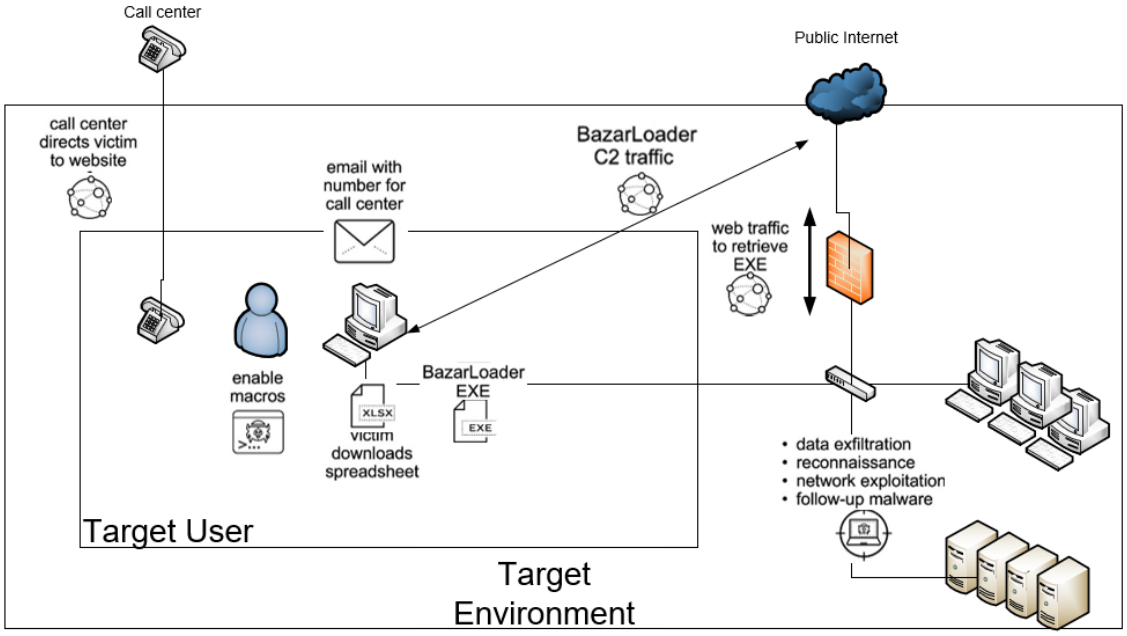


Figure 6 Bazar Within the Network

Step 3. Combine Cyber Kill Chain with Bazar Within the Target Network

In combining the CKC and the Bazar malware with the network the goal is to look for patterns. First there is no need to add steps one and two from the CKC as they are pre-attack steps and not with the scope of the network's capability. This determination was made because many small businesses lack the resources to investigate steps one and two from the CKC. This overlay seen in figure 7 shows an emerging pattern. The benefit of frameworks like the CKC is in the assistance with finding patterns that may help with defense in a cyber-attack.

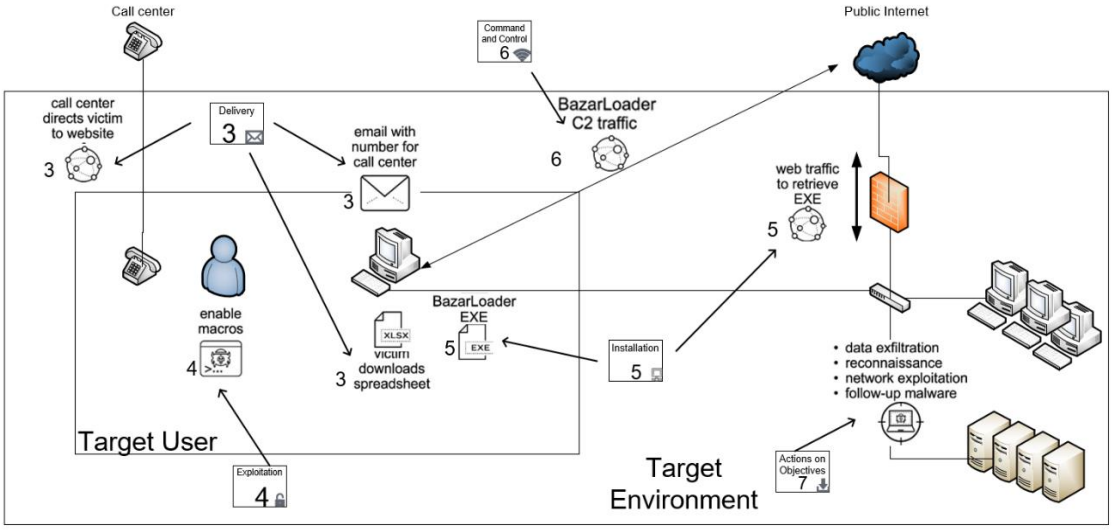


Figure 7 CKC With Bazar in Network

The ATT&CK Framework Analysis

The MITRE ATT&CK Framework is a series of tactics and techniques. There are 14 tactics in the enterprise matrix. The fourteen are Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. The ATT&CK matrix has more items than the CKC framework. The ATT&CK framework will be more detailed in how it breaks the adversary's steps. There is a need for shorthand to denote techniques with sub-techniques with the added detail. When a sub-technique is used the main technique will first define it with the sub-technique as follows [technique: sub-technique] (MITRE ATT&CK 2021). after being defined will be referred by the sub-technique.

Step 1. Align to ATT&CK Framework to Malware

In the ATT&CK framework the first two steps are not in scope. Just like in the CKC, the pre-attack parts of the framework cannot be measured when correlating the malware process to the framework. The Initial access tactic is the first point of contact. There is one technique with one sub-technique in the initial access tactic, [Phishing: Spear phishing Link]. The primary technique is Phishing. This identifies the email sent to the user to start the process. The one sub-technique is spear phishing since the email was designed to convince the target to not ignore the email and follow any required process defined in the email.

This tactic has 12 techniques and Bazar uses five of the twelve. Two main techniques are 1) Native API and 2) Windows management instrumentation. There are four sub-techniques, Native API is the technique that involves the Bazar malware using a windows native application programming interface (API) as part of its processes. The second listed main technique is Windows management instrumentation Bazar uses this call to query the OS about the installed antivirus engine. The sub-techniques are [Command and Scripting Interpreter: PowerShell], [Command and Scripting Interpreter: Windows Command Shell], [Scheduled Task/Job: Scheduled Task], and [User Execution: Malicious Link]. The adversary uses Windows Command Shell to execute cmd.exe to perform reconnaissance (MITRE ATT&CK 2021). The Malicious Link is the key part to compromising the user.

Persistence is what makes the APT extremely harmful to the organization. In this tactic the adversary deploys one primary technique and four sub-techniques. The techniques used are BITS jobs, [Boot or Login AutoStart Execution: Registry Run Keys / Startup Folder], [Boot or Login AutoStart Execution: Shortcut Modification], and [Boot or Login AutoStart Execution: Winlogon Helper DLL].

Privilege escalation is one of the most important components of the adversary's plan of attack. There are six sub-techniques used to complete this goal there are [Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder], [Boot or Logon AutoStart Execution: Shortcut Modification], [Boot or Logon AutoStart Execution: Winlogon Helper DLL], [Process Injection: Process Doppel ganging], [Process Injection: Process Hollowing], and [Scheduled Task/Job: Scheduled Task].

The next tactic is defense evasion, and it is here that we encounter the first repeat technique, BITS jobs. The other main techniques are De-obfuscate/Decode Files or Information and Process Injection. The sub-techniques are [Impair Defenses: Disable or Modify Tools], [Indicator Removal on Host: File Deletion], [Masquerading: Double File Extension], [Masquerading: Masquerade Task or Service], [Masquerading: Match Legitimate Name or Location], [Subvert Trust Controls: Code Signing], and [Virtualization/Sandbox Evasion: Time Based Evasion].

The most dangerous part to the environment is credential access. Access to credentials gives the adversary a lot of power over the system allowing the adversary to gain access across the environment with the user's credentials. Now in the credential access tactic the are no techniques executed by the Bazar malware.

One of the tactics with the greatest number of techniques executed is the discovery tactic. With ten techniques and five sub-techniques the list is Domain Trust Discovery, File and Directory Discovery, Network Share Discovery, Process Discovery, Query Registry, Remote System Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Information Discovery, System Time Discovery, [Account Discovery: Local Account], [Account Discovery: Domain Account], [Software Discovery: Security Software Discovery], [System Location Discovery: System Language Discovery], and [Virtualization/Sandbox Evasion: Time Based Evasion].

Often, malware will not contain a tactic and completely bypass a tactic because a previously exploited step allowed the next step to be skipped. The tactic lateral movement is completely bypassed because Bazar is primarily a downloader and backdoor malware.

Bazar now begins to collect data from the system, this step is the collection tactic, and the executed technique is Data from Local system. Bazar can search the local file system for data. The problem is that now Bazar is looking for places to hide files that will be downloaded when C2 is established.

This next step is the Command and Control (C2) tactic. Four out of the 16 listed by ATT&CK are used and four sub-techniques. The main techniques are Fallback Channels, Ingress Tool Transfer, Multi-Stage Channels, and Web Service. The four sub-techniques are [Application Layer Protocol: Web Protocols], [Dynamic Resolution: Domain Generation Algorithms], [Encrypted Channel: Symmetric Cryptography], and [Encrypted Channel: Asymmetric Cryptography].

With C2 established the adversary is free to complete the last two tactics, exfiltration of data and impact. The C2 communication channel is crucial for the adversary to continue forward and critical for the defender to detect and stop. The tactic for data is competed with technique Exfiltration Over C2 Channel. This is no need for additional software because Bazar executed [Command and Scripting Interpreter: PowerShell] during the execution tactic. PowerShell provides the adversary with secure copy (SCP) allowing the data to be exfiltrated using the native built-in application. The last stage is the Impact tactic and like with CKC, the adversary must be detected and stop as quickly as possible. The complete up to date descriptions of the tactics and techniques can be referenced at https://attack.mitre.org/techniques.

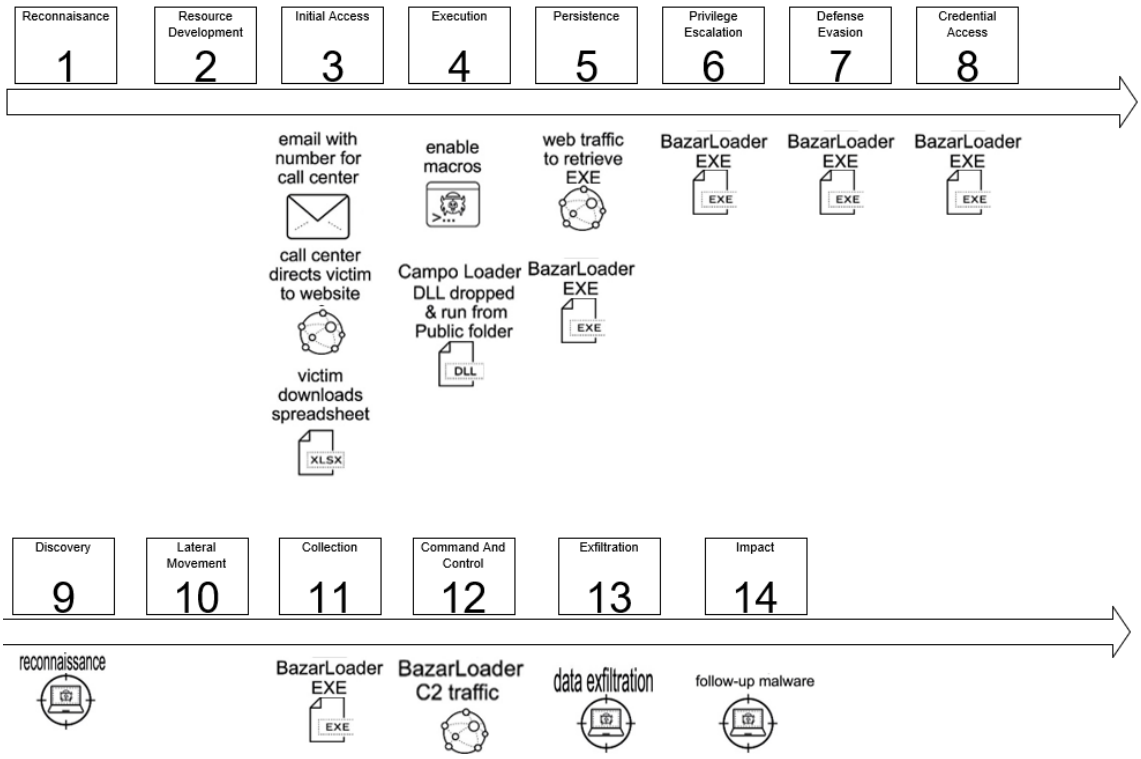


Figure 8 ATT&CK With Bazar, Based on Duncan, 2021

Step 2. Align to Malware to Target

This Step is the exact same as described in the step two CKC analysis. Please refer to that section for details on the Bazar malware to network comparison. The figure shown here is from the CKC step analysis. During the ATT&CK analysis, there is no change in how the Bazar malware moves through the network during the ATT&CK analysis.

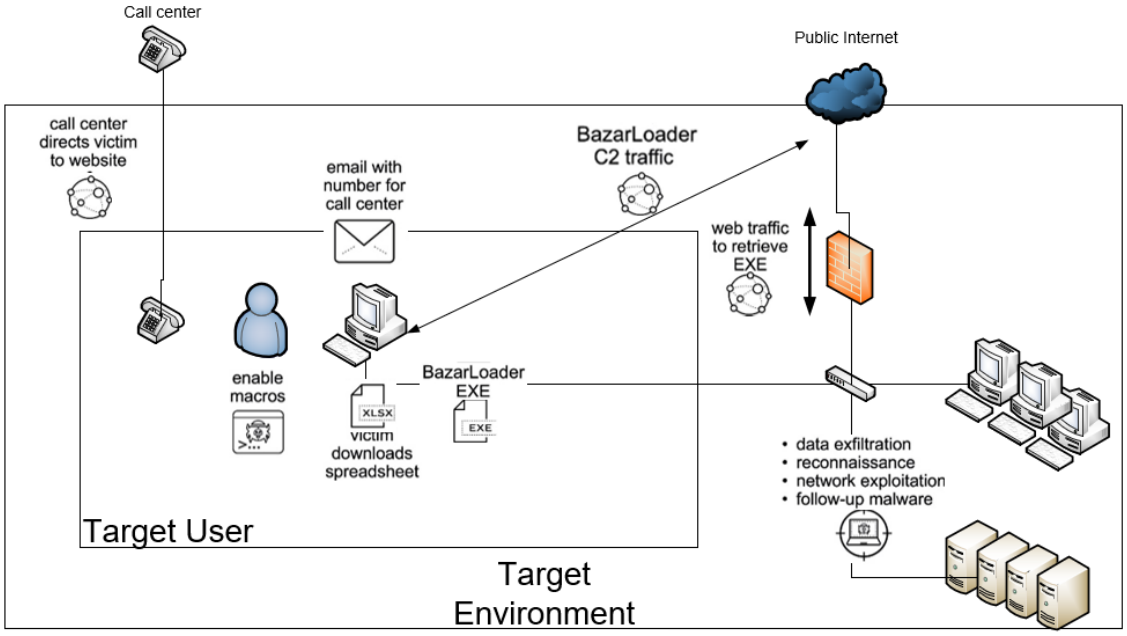


Figure 9 Bazar Within Network, Based on Duncan,2021

Step 3. Combine ATT&CK Framework With Bazar Within the Target Network

Starting with step one of the analysis the level of detail that is produced by MITRE ATT&CK framework is evident. In this part of the analysis the diagram produced also displays a fair amount of detail. Like in the CKC analysis step three of the CKC, the pre-attack steps will not be listed for being out of scope. The first contact tactic is tactic three, Initial Access. Patterns begin to emerge as the Bazar malware flows through the network. The patterns that emerge are the factors that assist in malware analysis and defense.

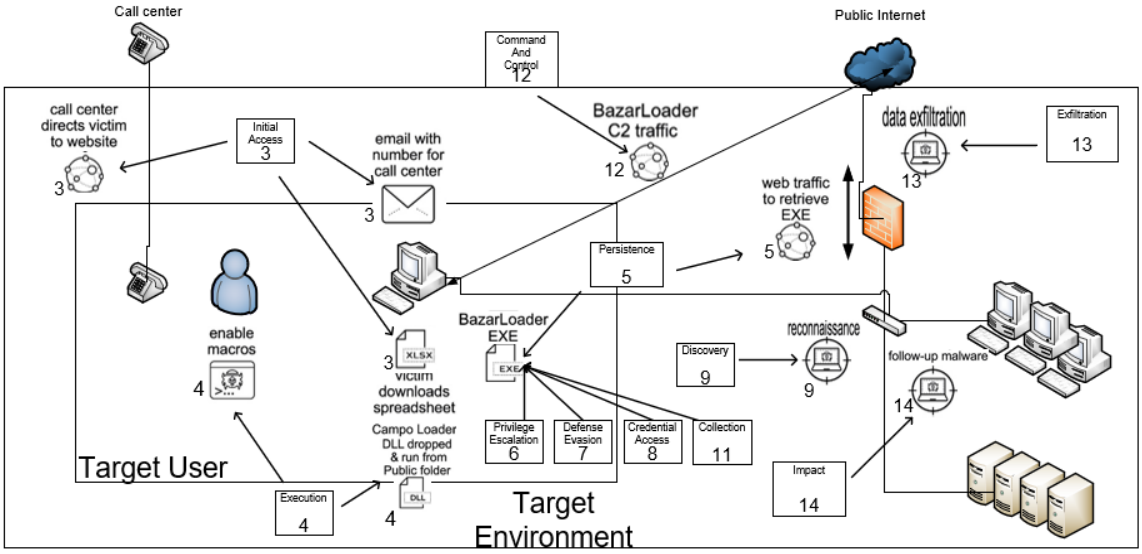


Figure 10 ATT&CK Applied to Malware Network

Observations

The two frameworks have been applied to the malware network. The two frameworks provided a substantial amount of information. The CKC proved informative with just 7 steps. The ATT&CK framework provided a great level of detail about how the malware acted within the network. The benefit of the results that each framework can provide to the small business may give the business assistance in lowering the risk of compromise from malware/ransomware attack and other threats that can be analyzed with these types of frameworks. While a single product that covers many of the vectors observed might be outside of the budget of some businesses, especially microbusinesses. The information provided by a framework still has value.

CKC Analysis Results

As part of the overall mission the primary object of the adversary is to enter the network. Once inside the adversary can focus on whatever the final goal of the mission may be. The observation is that steps three through five are key for the adversary to enter the environment. Those steps are delivery, exploitation, and installation. From the known behavior of the Bazar malware and how it aligns with the seven steps of the CKC, a risk to the environment is highlighted, see Figure 11.

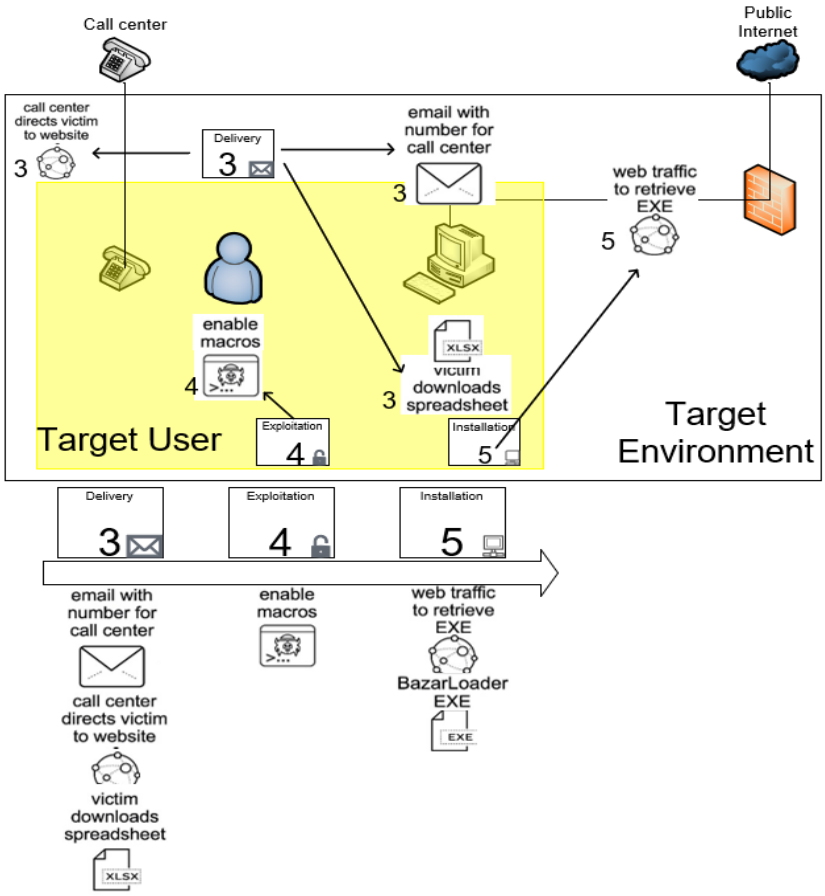


Figure 11 CKC Observed Steps 3-5

In the analysis the first point of contact is step three delivery. Each phase has a recommended course of action. The actions are Detect, Deny, Disrupt, Degrade, Deceive, and Destroy. The recommended actions for the delivery phase from the CKC are listed on table two below. The Course of Action Matrix provides four mitigating control recommendations. Two low-budget solutions and two potentially costly solutions. The recommendations per phase are listed under the action.

Table 2. Course of Action Matrix for CKC (Hutchins E. et al, 2010)

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance						
Weaponization						
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	Chroot jail	AV			
C2						
Action on Objectives						

Figure eleven has the user's scope isolated within a shaded area. The Bazar malware campaign exerted influenced over three items in the shaded area. The first was that Bazar was able to arrive on the user's PC via an email that by-passed standard email filtration. Filtration services are offered to some extent by all email service providers from Gmail to outlook365 often for free or as part of the subscription service. Small businesses take advantage of the lower cost and low maintenance requirements these services offer. Adversaries that send out malicious emails are particularly good at creating email campaigns that can often get passed filtering. For this reason, email filtering was not one of the four recommendations.

The four actions highlighted under delivery are Detect, Deny, Disrupt, and Degrade. The recommended mitigations for Deny was Proxy filter and the recommendation for Degrade was queuing. Both options for the small budget small business are cost prohibited. These solutions incur some cost and require some level of technical knowledge, often requiring the small businesses to hire some type of professional services to deploy the solution and maintain it. The two actions that are most favorable to the target small business are Detect and Disrupt. The recommendation for detecting is vigilant user and for disrupting the recommendation is inline antivirus (Hutchins E. et al, 2010).

The importance of the vigilant user to the defense of the network becomes evident in figure eleven. The framework accurately shows how important the user is in the Bazar campaign. The user has three opportunities to stop Bazar. The value of understanding how to identify potentially malicious emails is visible. The next two key items are first, the user needs to reach out to the call center and second the user at the instruction of the call center, downloads a malicious file. Users in this situation would benefit from knowing how to identify the email senders. The CKC step four is exploitation and the mitigations for Detect, Deny, and Disrupt are Host Intrusion Detection system (HIDS), Patch and Data Execution Prevention (DEP) (Hutchins et al, 2010). At this phase for the small business, only one recommendation has a cost and significant technical requirement, and that action is HIDS. For a HIDS solution the business may also need assistance deploying the solution and maintaining it. The other two are

Patching and DEP. These are easily accessible mitigations. Microsoft provides free security patches for their operating systems until they reach end of life.

Malicious code being executed via macros is such a big problem that beginning April 2022 Microsoft will start blocking macros by default (Brown & Eickmeyer, 2022). The last section of the CKC is step five installation and the mitigations are Detect, Deny, and Disrupt are Host Intrusion Detection system (HIDS), Chroot jail and Anti-Virus (AV) (Hutchins et al, 2010). Already discussed are the problems with HIDS. The Deny action is Chroot jail, a feature not available on the windows operating systems and the Disrupt option is AV that is freely available with the windows operating system or available from third parties for relatively low cost.

ATT&CK Analysis Results

The fourteen tactics of the ATT&CK matrix for enterprises are Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. It was determined that only twelve of the 14 techniques apply to the simple small business network. The techniques of the ATT&CK framework when applied to the network produce a pattern near identical to the results of the CKC analysis. The very robust ATT&CK framework is reduced to three of the twelve tactics in a small simple network. This is because this environment is the basic minimum that a small business would need to accomplish its business mission. The ATT&CK

framework has proven itself to be a great tool for analysis of every detail of an adversary's attack methodology. The features that make the ATT&CK framework great for larger enterprises, malware researchers, and security product research/development are lost on small businesses. The three tactics that emerge as having the greatest impact and that provide the potential for the best and lowest cost mitigation are Initial Access, Execution, and Persistence, see Figure 12.

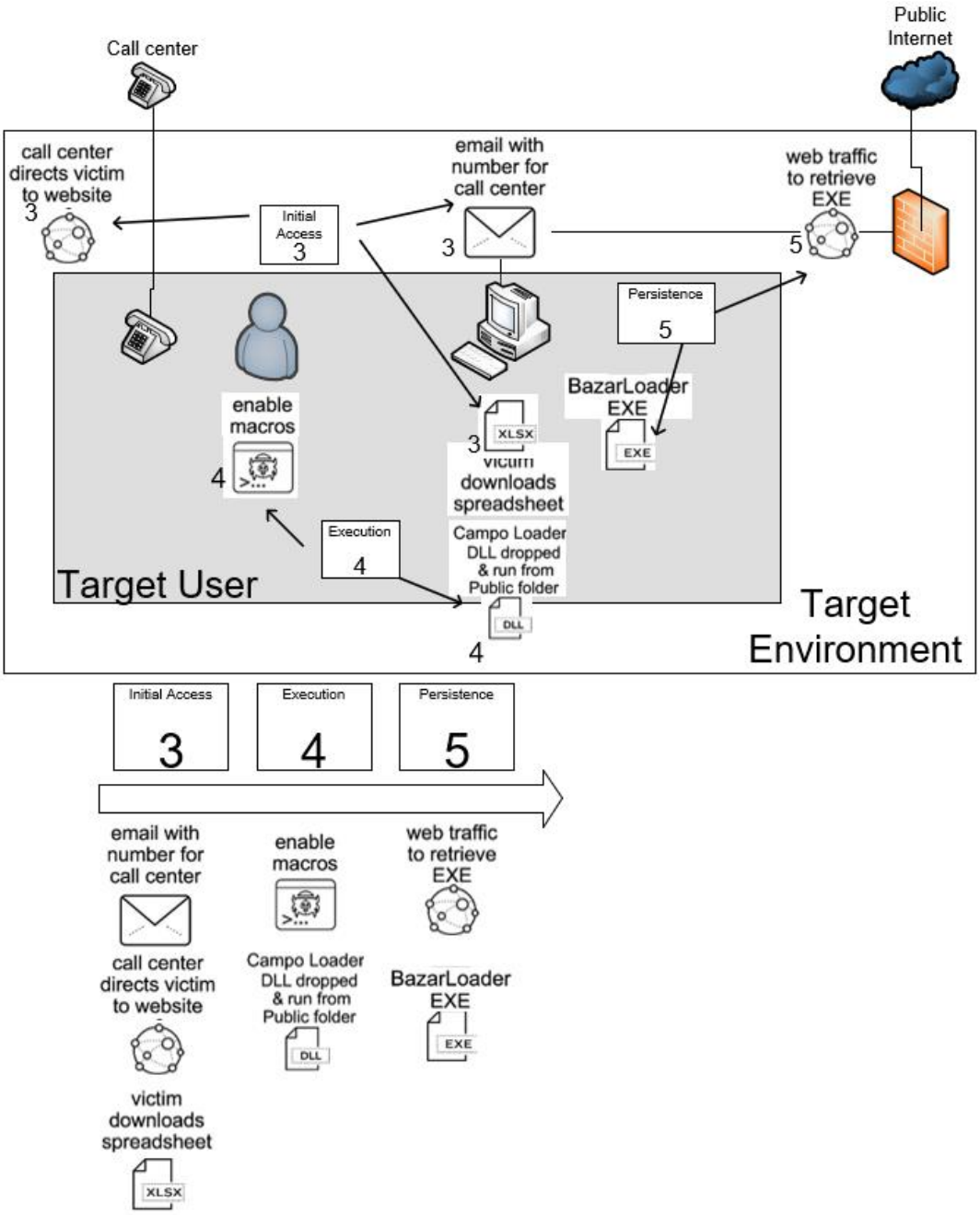


Figure 12 ATT&CK Observations Step 3-5

There are more techniques within the three tactics of the ATT&CK Framework than there were from the seven steps of the CKC. The ones specific to the Bazar malware are listed in Table3. The MITRE ATT&CK framework provides a series of recommended mitigations for each technique. The ATT&CK framework also lists if there is no recommended mitigation or easily implemented control.

Table 3. ATT&CK Tactics and Techniques Steps 3-5 (attack.mitre.org, 2022)

Tactic: Initial access	Tactic: Execution	Tactic: Persistence
Phishing: Spear phishing Link	Native API	BITS Jobs
	Command and Scripting Interpreter	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
	Command and Scripting Interpreter: PowerShell	Boot or Logon AutoStart Execution: Winlogon Helper DLL
	User Execution: Malicious Link	Boot or Logon AutoStart Execution: Shortcut Modification
	Windows Management Instrumentation	Scheduled Task/Job

	Scheduled Task/Job	

The mitigations for the techniques from steps three through five listed in table three vary in ease and complexity. Referring to figure 12, the shaded area highlights the user's realm of influence over the environment. The first tactic is Initial Access, and the technique is Phishing: Spear phishing Link. The ATT&CK framework recommended mitigations for Bazar are Restrict Web-Based Content, Software Configuration, and User Training restricting web-based content can be challenging of a small business with limited technical resources to implement as a technical solution. Often a small business would have to use an outsourced resource for a technical solution. For all businesses big or small but especially small ones with small budgets. The best option for a control would be an acceptable use policy for the organization. There are freely available guides from many sources, such as the document for NIST 800-53. NIST 800-53 section 3.1 Access controls provide much of the information needed for an organization to create an acceptable use policy (NIST, 2020). The second mitigating control is software configuration. It does require some technical knowledge for an organization that self-host email but for those organization using a service like Office 365 from Microsoft or Gsuite from google both vendors have guides available to assist users (Davis et al., 2022). The third mitigation for Phishing:

Spear phishing Link is User Training. The ATT&CK framework like the CKC has identified the risk posed by the user.

Execution is the second tactic and the ATT&CK framework has assigned six techniques to the Bazar malware. Some of the mitigations repeat within techniques. These repeating controls would be good candidates to implement because they cover more than one technique. Focusing on the overlapping mitigations will reduce the amount of risk for several techniques while reducing the amount of effort and time a risk mitigation project may take. The complete graph of all grouped techniques to mitigations can be seen in APPENDIX C. The graphed results of the techniques to mitigations exhibit how the ATT&CK matrix mitigations can be used to find the ones that cover the most techniques. This is extremely helpful to a budget conscience small business or organization.

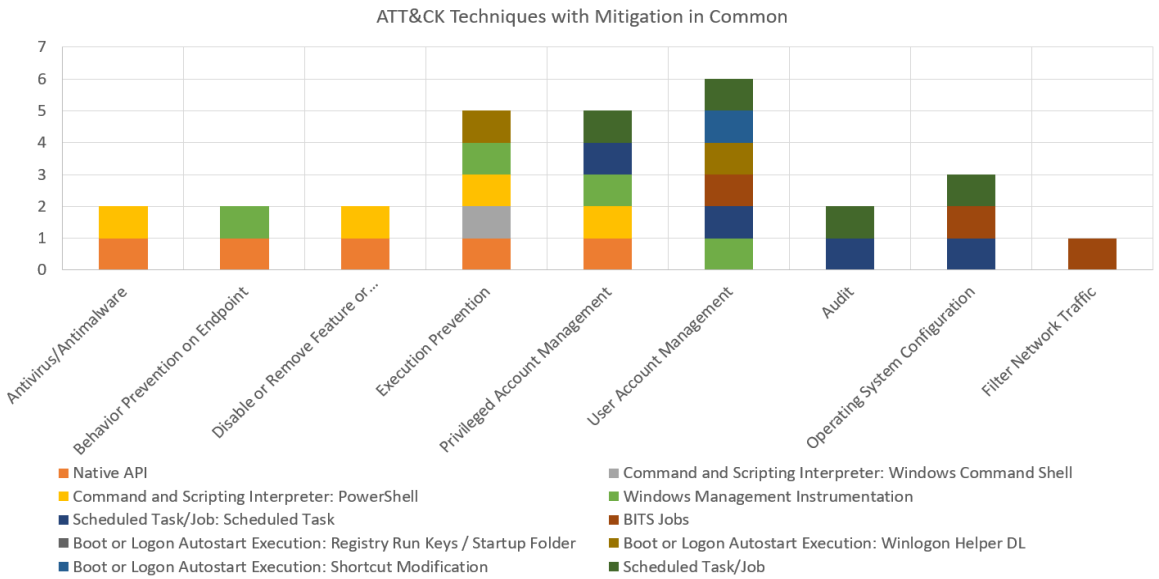


Figure 13 Overlapping Controls

To best mitigate against the Bazar malware based on the ATT&CK Framework, the best mitigations to deploy would be execution prevention, privilege account management, and user account management, see Figure 13. The implementation of these three mitigations will also mitigate parts of the following techniques: Native API, Command and Scripting Interpreter: PowerShell, BITS Jobs, Windows Management Instrumentation, and Scheduled Task/Job: Scheduled Task. The three mitigations from Figure 13 are user-related and implementing them along with the user training mitigation mitigates both the initial access and execution tactics. This will improve any organization's security posture.

The MITRE ATT&CK Framework provides a significant amount of information about this small network. The ATT&CK Framework was not limited by the lack of data about the network but instead demonstrated that knowledge about the behavior of the attack is enough to give a small network the information needed to prepare a potential defense against an adversary. Like in the CKC, the MITRE ATT&CK framework discovered mitigations that can be applied to any network, especially small networks with limited resources.

CHAPTER FIVE:

SUMMARY AND CONCLUSION

Summary of Analysis

The analysis of Lockheed Martin's Cyber Kill Chain framework and the ATT&CK Framework from MITRE produced similar results when applied to a small simple network and a known malware. The network and malware were a constant part of the analysis when each framework was applied. Each framework had a different approach for the malware. The results were similar because of the two constants. This allowed a back-to-back comparison that highlighted the differences between the two. Similarities should be the focus of risk mitigation for any budget conscience small business. The key similarity between the two frameworks is the user. The user is known to be a major risk factor in the prevention of any malware campaign the uses phishing techniques, malicious files, malicious downloads, and malicious websites. Any of these malicious techniques are a major threat to a business when put in front of an untrained user. Both frameworks excelled at aligning with both the network and the malware. The frameworks demonstrated that even small unsophisticated networks benefit because both showed that the biggest risk to the network is the user. The common mitigating controls to protect the network revolve around the user since they assist in deploying the malware inside the network.

Which Components are Relevant to Small Office Networks?

The best components from both frameworks that are most relevant to the small business network from the analysis are steps three, four and five. These three steps provide the most impact on any organization. The three steps from the CKC are Delivery, Exploitation, and Installation. The mitigations from the steps are Vigilant user, Proxy filter, In-line AV, HIDS, Patch, and DEP. Steps three, four and five of the ATT&CK framework are Initial Access, Execution, and Persistence for the associated mitigations refer to APPENDIX A.

Can These Components be Applied to Small Office Networks?

The analysis demonstrated that in the three elements that both frameworks have in common, it is training users to be more vigilant and aware of potentially malicious email, files and website has a major impact on prevention. The user training will benefit all organizations but in small and micro businesses that do not have large budgets for sophisticated hardware and software or for dedicated technical staff, user training offers the greatest benefit. The second control from the three components that benefit the organization and is also associated with user behavior is the hardening of users' devices. The ATT&CK framework points this out because of the level detail it produces for steps three through five.

Conclusion

This project setup an analysis of two kill chain frameworks and reviewed how they applied to a known malware and applied that information to a simple

small network. Then looked at what the information gathered could be applied lied to a business that has a small size and budget. While no recommendation is a guarantee of attack prevention. What was learned is that some mitigations can improve an organization's security posture while not requiring complicated technical solutions or incurring large financial costs. In conclusion, a well-informed user has proven to be a particularly good defense.

Future Work

The aspect of cyber defense with methods that are affordable and available to small businesses, microbusinesses and the small office home office is a subject that has been neglected. This opens the landscape for future work to look at more variables and solutions to the problem that malware and ransomware pose to these small budget entities. There is much more work to assist these entities in improving their cyber defense postures.

APPENDIX A:

ATT&CK FRAMEWORK BAZAR STEPS 3-5 MITIGATION MATRIX

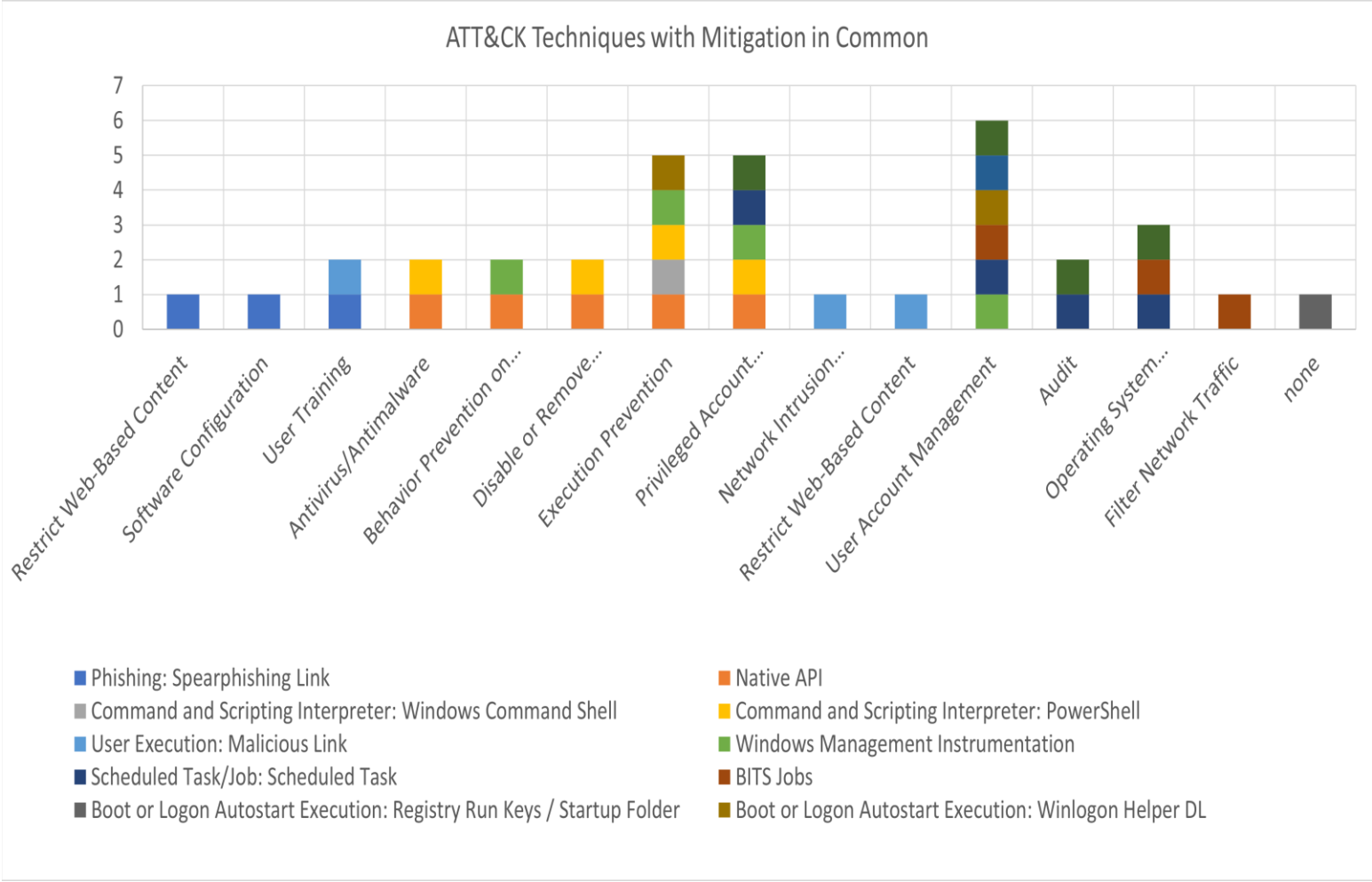
Technique	Tactic	Mitigation	Description	Reference
Phishing: Spearphishing Link	Initial access	Restrict Web-Based Content	Determine if certain websites that can be used for spear phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.	https://attack.mitre.org/techniques/T1566/002/
		Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain	
		User Training	Users can be trained to identify social engineering techniques and spear phishing emails with malicious links.	
Native API	Execution	Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.	https://attack.mitre.org/techniques/T1059/
		Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual Basic and JavaScript scripts from executing potentially malicious downloaded content	
		Disable or Remove Feature or Program	Disable or remove any unnecessary or unused shells or interpreters.	
		Execution Prevention	Use application control where appropriate.	
		Privileged Account Management	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.	
Command and Scripting Interpreter: Windows Command Shell	Execution	Execution Prevention	Use application control where appropriate.	https://attack.mitre.org/techniques/T1059/003/
Command and Scripting Interpreter: PowerShell	Execution	Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.	https://attack.mitre.org/techniques/T1059/001/
		Disable or Remove Feature or Program	It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions.	
		Execution Prevention	Use application control where appropriate.	
		Privileged Account Management	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing	

			the PowerShell execution policy, depending on environment configuration.	
User Execution: Malicious Link	Execution	Network Intrusion Prevention	If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity.	https://attack.mitre.org/techniques/T1204/001/
		Restrict Web-Based Content	if a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious files.	
		User Training	Use user training as a way to bring awareness to common phishing and spear phishing techniques and how to raise suspicion for potentially malicious events	
Windows Management Instrumentation	Execution	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by WMI commands from running. Note: many legitimate tools and applications utilize WMI for command execution.	https://attack.mitre.org/techniques/T1047/
		Execution Prevention	Use application control configured to block execution of wmic.exe if it is not required for a given system or network to prevent potential misuse by adversaries. For example, in Windows 10 and Windows Server 2016 and above, Windows Defender Application Control (WDAC) policy rules may be applied to block the wmic.exe application and to prevent abuse.	
		Privileged Account Management	Prevent credential overlap across systems of administrator and privileged accounts.	
		User Account Management	By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect or disallow all users to connect remotely to WMI.	
Scheduled Task/Job: Scheduled Task	Execution	Audit	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges.	https://attack.mitre.org/techniques/T1053/005/
		Operating System Configuration	Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM.	
		Privileged Account Management	Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process.	

		User Account Management	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote system	
BITS Jobs	Persistence	Filter Network Traffic	Modify network and/or host firewall rules, as well as other network controls, to only allow legitimate BITS traffic.	https://attack.mitre.org/techniques/T1197/
		Operating System Configuration	Consider reducing the default BITS job lifetime in Group Policy or Registry	
		User Account Management	Consider limiting access to the BITS interface to specific users or groups.	
Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder	Persistence	none	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	https://attack.mitre.org/techniques/T1547/001/
Boot or Logon AutoStart Execution: Winlogon Helper DLL	Persistence	Execution Prevention	Identify and block potentially malicious software that may be executed through the Winlogon helper process by using application control tools like App Locker that are capable of auditing and/or blocking unknown DLLs.	https://attack.mitre.org/techniques/T1547/004/
		User Account Management	Limit the privileges of user accounts so that only authorized administrators can perform Winlogon helper changes.	
Boot or Logon AutoStart Execution: Shortcut Modification	Persistence	User Account Management	Limit permissions for who can create symbolic links in Windows to appropriate groups such as Administrators	https://attack.mitre.org/techniques/T1547/009/
Scheduled Task/Job	Persistence	Audit	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges.	https://attack.mitre.org/techniques/T1053/005/
		Operating System Configuration	Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM.	
		Privileged Account Management	Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process.	
		User Account Management	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.	

APPENDIX B:

ATT&CK TECHNIQUES WITH MITIGATION IN COMMON


ATT&CK Techniques with Mitigation in Common
7
6
5
4
3
2
1
0
Restrict Web-Based Content
Software Configuration
User Training
Antivirus/Antimalware
Behavior Prevention on...
Disable or Remove...
Execution Prevention
Privileged Account...
Network Intrusion...
Restrict Web-Based Content
User Account Management
Audit
Operating System...
Filter Network Traffic
none
Phishing: Spearphishing Link
Native API
Command and Scripting Interpreter: Windows Command Shell
Command and Scripting Interpreter: PowerShell
User Execution: Malicious Link
Windows Management Instrumentation
Scheduled Task/Job: Scheduled Task
BITS Jobs
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Boot or Logon Autostart Execution: Winlogon Helper DL

REFERENCES

Alert (AA20-352A). CISA. (n.d.). Retrieved February 8, 2022, from http://www.cisa.gov/uscert/ncas/alerts/aa20-352a

Berrueta, E., Morato, D., Magana, E., & Izal, M. (2019, October). A survey on detection techniques for cryptographic ransomware. Retrieved February 19, 2022, from https://ieeexplore.ieee.org/document/8861029

Brandt, A. (2021, April). Bazarloader deploys a pair of novel spam vectors. Sophos News. Retrieved February 30, 2022, from https://news.sophos.com/en-us/2021/04/15/bazarloader/

Brown, D., & Eickmeyer, A. K. (2022, February). Macros from the internet are blocked by default in office - deploy office. Macros from the internet are blocked by default in Office - Deploy Office | Microsoft Docs. Retrieved February 30, 2022, from https://docs.microsoft.com/en-us/DeployOffice/security/internet-macros-blocked

CISA. (n.d.). Cyber Resource Hub. Retrieved February 26, 2022, from https://www.cisa.gov/cyber-resource-hub

Cisa.gov. (2022, February). Cyber assessment fact sheet - cisa.gov. Retrieved February 27, 2022, from https://www.cisa.gov/sites/default/files/publications/VM_Assessments_Fact_Sheet_PCA_508C.pdf

Cisecurity.org. (2021, March). The SolarWinds Cyber-Attack: What You Need to Know. Retrieved February 2022, from https://www.cisecurity.org/solarwinds

Cyber kill chain®. Lockheed Martin. (2020, January 15). Retrieved February 26, 2022, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Davis, C., Cole, L. H., & Modery, A. R. (2022, March). Configure anti-phishing policies in Microsoft Defender for Office 365 - office 365. Office 365 | Microsoft Docs. Retrieved March 30, 2022, from https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-mdo-anti-phishing-policies

Dempsey, K. (2014, February). NIST Computer Security Division csrc.nist.gov Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02192014.pdf . Retrieved February 15, 2022, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Department of Homeland Security. (2016, September). Recommended practice: Improving industrial control ... - cisa. Retrieved February 27, 2022, from https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Duncan, B. (2021, May). Bazarcall method: Call Centers Help spread bazarloader malware. Unit42. Retrieved February 18, 2022, from https://unit42.paloaltonetworks.com/bazarloader-malware/

Duncan, B. (2021, October). Case study: From bazarloader to network reconnaissance. Unit42. Retrieved February 18, 2022, from https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/

G, E. (2021, July 13). 31% of US companies close down after falling victim to ransomware - atlas VPN. atlasVPN. Retrieved February 18, 2022, from https://atlasvpn.com/blog/31-of-us-companies-close-down-after-falling-victim-to-ransomware

Greenert, A. J., & Welsh, G. M. (2013, May 17). Breaking the kill chain. Foreign Policy. Retrieved March 20, 2022, from https://foreignpolicy.com/2013/05/17/breaking-the-kill-chain/

Hahn, A., Thomas, R. K., Lozano, I., & Cardenas, A. (2015, August 29). A multi-layered and kill-chain based security analysis framework for cyber-physical systems. International Journal of Critical Infrastructure Protection. Retrieved February 30, 2022, from https://www.sciencedirect.com/science/article/pii/S187454821500061X

Headd, B. (2019, September 26). The role of microbusiness employers in the economy. SBA's Office of Advocacy. Retrieved February 19, 2022, from https://advocacy.sba.gov/2017/08/01/the-role-of-microbusiness-employers-in-the-economy/

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2010). Intelligence-driven computer ... - Lockheed Martin Space. Retrieved February 18, 2022, from https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Johnson, R. (2019, October 16). 60 percent of small companies close within 6 months of being hacked. Cybercrime Magazine. Retrieved February 8,

2022, from https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Joint Task Force. (2020, December 10). Security and privacy controls for information systems and organizations. Computer Security Resource Center. Retrieved February 15, 2022, from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Joint Task Force. (2018, December 20). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. Computer Security Resource Center. Retrieved February 26, 2022, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Keizer, G. (2020, November 4). Windows by the numbers: Windows 10 rolls on past 70%. Computerworld. Retrieved February 18, 2022, from https://www.computerworld.com/article/3199373/windows-by-the-numbers-windows-10-rolls-on-past-70.html

Klobuchar, A. (2021, November 30). Klobuchar, Thune announce commerce committee passage of bipartisan legislation to reduce cybersecurity risks. U.S. Senator Amy Klobuchar. Retrieved February 8, 2022, from https://www.klobuchar.senate.gov/public/index.cfm/2021/11/klobuchar-thune-announce-commerce-committee-passage-of-bipartisan-legislation-to-reduce-cybersecurity-risks

Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017, April). paybreak: Defense Against Cryptographic ransomware. Retrieved February 18, 2022, from https://www.researchgate.net/publication/315862748_PayBreak_Defense_Against_Cryptographic_Ransomware

LOCKHEED MARTIN. (2015). A white paper presented by: Lockheed Martin Corporation. Retrieved February 15, 2022, from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

MITRE Corporation. (2021). Mitre ATT&CK®. Retrieved February 18, 2022, from https://attack.mitre.org/

MITRE ATT&CK® Navigator. (2022, January). Bazar S0534. Retrieved March 30, 2022, from https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0534%2FS0534-enterprise-layer.json

MITRE. (2020, November). Bazar Version (S0534). MITRE ATT&CK. Retrieved March 30, 2022, from https://attack.mitre.org/software/S0534/.

Neuman, S. (2021, May 11). What we know about the ransomware attack on a critical U.S. pipeline. NPR. Retrieved February 26, 2022, from https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline

Nicole.keller@nist.gov. (2022, March 1). Ransomware. NIST. Retrieved February 8, 2022, from https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

Nist.gov. (2022, March 29). Ransomware. NIST. Retrieved February 8, 2022, from https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

Orchilles, J. (2022, April 11). Cyber Kill Chain, MITRE ATT&CK, and Purple Team. SANS Institute. Retrieved April 17, 2022, from https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/

Ransomware 101. CISA. (n.d.). Retrieved February 20, 2022, from https://www.cisa.gov/stopransomware/ransomware-101

Richardson, R., & North, M. M. (2017, January 1). Ransomware: Evolution, mitigation and prevention. Faculty Publications. 4276. Retrieved February 30, 2022, from https://digitalcommons.kennesaw.edu/facpubs/4276

S.2483 - improving cybersecurity of small organizations ... (n.d.). Retrieved March 21, 2022, from https://www.congress.gov/bill/117th-congress/senate-bill/2483

Security Update Guide Faqs. Microsoft. (2022, January). Retrieved February 18, 2022, from https://www.microsoft.com/en-us/msrc/faqs-security-update-guide

The solarwinds cyber-attack: What you need to know. CIS. (2021, November 9). Retrieved February 8, 2022, from https://www.cisecurity.org/solarwinds

Stop ransomware. CISA. (n.d.). Retrieved February 26, 2022, from https://www.cisa.gov/stopransomware

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018, March). Attack design and philosophy march 2020 - Mitre ATT&CK®. Retrieved February 30, 2022, from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf