Bellevue Bank and Trust

Bellevue Bank and Trust Cyber Fusion Team

MITRE ATT&CK Threat Assessment

Table of Contents

1 Document Information and History

1.1 Version History

Version	Change Date	Changes and Description	Editor	Approval Date	Approver
1.0	7/8/2022	Initial Template Creation	Steven Maestas	7/8/2022	SMM
2.0	1/29/2023	Completed assignment	Lathan Birmingham		

1.2 Distribution

This threat assessment is intended to be stored by the BB&T lead security administrator. This report can be utilized by BB&T both cybersecurity red and blue teams to improve the overall security posture. This threat assessment is confidental information owned by BB&T.

2 Introduction

This is the Bellevue Bank and Trust (BB&T) annual MITRE ATT&CK threat assessment.

2.1 Purpose

The purpose of this comprehensive threat assemsent is to determine BB&T’s ability to detect and respond accordingly to attacks targeting the organization. Threat assessments are apart of an overall process referred to as ‘risk management’. The ultimate purpose of risk mangement is to measure uncertain risks.

2.2 Definitions

MITRE ATT&CK “MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community [1].”

Threat Assessment “Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat [2].”

Threat Actor **“**An individual or a group posing a threat [3].”

TTPs Tactics, techniques, and procedures (TTP) – “The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique [4]”

EDR **“**Endpoint detection and response (EDR) solutions detect threats across your environment, investigating the entire lifecycle of the threat, and providing insights into what happened, how it got in, where it has been, what it's doing now, and what to do about it. By containing the threat at the endpoint, EDR helps eliminate the threat before it can spread [5].”

SOD **“**Separation of duties “refers to the principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time). An example of dynamic separation of duty is the two-person rule. The first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first [6].”

SIEM “Security Information and Event Management tool – “Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface [7].”

SOAR “Security orchestration, automation and response (SOAR) technology helps coordinate, execute and automate tasks between various people and tools all within a single platform. This allows organizations to not only quickly respond to cybersecurity attacks but also observe, understand and prevent future incidents, thus improving their overall security posture. A comprehensive SOAR product, as defined by Gartner, is designed to operate under three primary software capabilities: threat and vulnerability management, security incident response, and security operations automation. Threat and vulnerability management (orchestration) covers technologies that help amend cyberthreats, while security operations automation (automation) relates to the technologies that enable automation and orchestration within operations [8].”

3 Threat Assessment

3.1 Threat Actors

Below is a table of MITRE known threat actors. Each description is taken directly from the Mitre ATT&CK website to properly portray each group. The groups highligted in purple are the ones that should be on the radar of BB&T.

Threat Actor	Description	Tools Used
APT38	APT38 is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.[1] Active since at least 2014, APT38 has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of Bangladesh heist, during which APT38 stole $81 million, as well as attacks against Bancomext (2018) and Banco de Chile (2018); some of their attacks have been destructive	DarkComet, ECCENTRICBANDWAGON, HOPLIGHT, KillDisk, Mimikatz, Net
Evilnum	Evilnum is a financially motivated threat group that has been active since at least 2018.	EVILNUM, LaZagne, More_eggs
FIN10	FIN10 is a financially motivated threat group that has targeted organizations in North America since at least 2013 through 2016. The group uses stolen data exfiltrated from victims to extort organizations.	Empire
Earth Lusca	Earth Lusca is a suspected China-based cyber espionage group that has been active since at least April 2019. Earth Lusca has targeted organizations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam,	certutil, Cobalt Strike, Mimikatz, NBTscan, Nltest, PowerSploit, ShadowPad, TaskList, Winnti for Linux

Threat Actor	Description	Tools Used
	the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some Earth Lusca operations may be financially motivated.	
FIN8	FIN8 is a financially motivated threat group known to launch tailored spearphishing campaigns targeting the retail, restaurant, and hospitality industries.	dsquery, Impacket, Net, Nltest, PUNCHBUGGY, PUNCHTRACK
Ember Bear	Ember Bear is a suspected Russian state-sponsored cyber espionage group that has been active since at least March 2021. Ember Bear has primarily focused their operations against Ukraine and Georgia, but has also targeted Western European and North American foreign ministries, pharmaceutical companies, and financial sector organizations. Security researchers assess Ember Bear likely conducted the WhisperGate destructive wiper attacks against Ukraine in early 2022.	OutSteel, Saint Bot, WhisperGate
Tonto Team	Tonto Team is a suspected Chinese state-sponsored cyber espionage threat group that has primarily targeted South Korea, Japan, Taiwan, and the United States since at least 2009; by 2020 they expanded operations to include other Asian as well as Eastern European countries. Tonto Team has targeted government, military, energy, mining, financial, education, healthcare,	Bisonal, gsecdump, LaZagne, Mimikatz, NBTscan, ShadowPad

Threat Actor	Description	Tools Used
	and technology organizations, including through the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017).	
Andariel	Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focused its operations--which have included destructive attacks--against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. Andariel's notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle.	gh0st RAT, Rifdoor
Cobalt Group	Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions since at least 2016. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims. Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak	Cobalt Strike – Mimikatz, More_eggs, PsExec, Sdelete, SpicyOmelette
Dark Vishnya	DarkVishnya is a financially motivated threat actor targeting financial institutions	PsExec, Winexe

Threat Actor	Description	Tools Used
	in Eastern Europe. In 2017-2018 the group attacked at least 8 banks in this region.	
GCMAN	GCMAN is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services.	
Indrik Spider	Indrik Spider is a Russia-based cybercriminal group that has been active since at least 2014. Indrik Spider initially started with the Dridex banking Trojan, and then by 2017 they began running ransomware operations using BitPaymer, WastedLocker, and Hades ransomware.	BitPaymer, Cobalt Strike, Donut, Dridex, Empire, Mimikatz, PsExec, WastedLocker
RTM	RTM is a cybercriminal group that has been active since at least 2015 and is primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name (RTM).	RTM
Silence	Silence is a financially motivated threat actor targeting financial institutions in different countries. The group was first seen in June 2016. Their main targets reside in Russia, Ukraine, Belarus, Azerbaijan, Poland and Kazakhstan. They compromised various banking systems, including the Russian Central Bank's Automated Workstation Client, ATMs, and card processing.	Empire, Sdelete, Winexe

3.2 Tools

These are the top 10 tools used by the groups listed above, starting with the most common. All descriptions of the tools come straight from the MITRE ATT&CK software webpage [9].

Mimikatz “Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks [9].”

PsExec “PsExec is a free Microsoft tool that can be used to execute a program on another computer. It is used by IT administrators and attackers [9].”

Empire “Empire is an open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure PowerShell for Windows and Python for Linux/macOS. Empire was one of five tools singled out by a joint report on public hacking tools being widely used by adversaries [9].”

Cobalt Strike “Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system [9].”

Net “The Net utility is a component of the Windows operating system. It is used in command-line operations for control of users, groups, services, and network connections. [1] Net has a great deal of functionality, [2] much of which is useful for an adversary, such as gathering system and network information for Discovery, moving laterally through SMB/Windows Admin Shares using net use commands, and interacting with services. The net1.exe utility is executed for certain functionality when net.exe is run and can be used directly in commands such as `net1 user` [9].”

Nltest “Nltest is a Windows command-line utility used to list domain controllers and enumerate domain trusts [9].”

LaZagne “LaZagne is a post-exploitation, open-source tool used to recover stored passwords on a system. It has modules for Windows, Linux, and OSX, but is mainly focused on Windows systems. LaZagne is publicly available on GitHub [9].”

Sdelete “SDelete is an application that securely deletes data in a way that makes it unrecoverable. It is part of the Microsoft Sysinternals suite of tools [9].”

ShadowPad “ShadowPad is a modular backdoor that was first identified in a supply chain compromise of the NetSarang software in mid-July 2017. The malware was originally thought to be exclusively used by APT41, but has since been observed to be used by various Chinese threat activity groups [9].”

Winexe “Winexe is a lightweight, open-source tool similar to PsExec designed to allow system administrators to execute commands on remote servers. Winexe is unique in that it is a GNU/Linux based client [9].”

NBTscan NBTscan is an open-source tool that has been used by state groups to conduct internal reconnaissance within a compromised network [9].”

More_eggs “More_eggs is a JScript backdoor used by Cobalt Group and FIN6. Its name was given based on the variable "More_eggs" being present in its code. There are at least two different versions of the backdoor being used, version 2.0 and version 4.4 [9].”

4 Top MITRE ATT&CK

As defined by the NIST, an SLA, or service level agreement, "represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination [9]." The purpose of an SLA is to have written agreements for standards and services, this ensures that all parties are on the same page. SLAs can include penalties for failed obligations by a party. Setting distinct and measurable guidelines is essential, as it reduces the likelihood of disappointing a party and provides alternatives if agreements are not met.

4.1 Ransomware

These are the MITRE Top 10 Techniques used in ransomware. All definitons are taken directly from the MITRE ATT&CK Techiques webpage [10].

T1486: Data Encrypted for Impact

"Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted [10]."

T1490: Inhibit System Recovery

"Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. This may deny access to available backups and recovery options [10]."

T1027: Obfuscated Files or Information

"Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses [10]."

T1047: Windows Management Instrumentation

"Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by Remote Services such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM). Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS [10].”

T1036: Masquerading

“Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names [10].”

T1059: Command and Scripting Interpreter

“Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell [10].”

T1562: Impair Defenses

“Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators [10].”

T1112: Modify Registry

“Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution [10].”

T1204: User Execution

“An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing [10].”

T1055: Process Injection

“Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process [10].”

4.2 Organizational TTPs

These are the MITRE Top 10 techniques deemed most likely to affect BB&T. This list was generated via the MITRE top 10 calculator. All definitons are taken directly from the MITRE ATT&CK Techiques webpage [10].

T1059.001 - Command and Scripting Interpreter: PowerShell

“Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems) [10].”

T1059.002 - Command and Scripting Interpreter: AppleScript

“Adversaries may abuse AppleScript for execution. AppleScript is a macOS scripting language designed to control applications and parts of the OS via inter-application messages called AppleEvents. These AppleEvent messages can be sent independently or easily scripted with AppleScript. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely [10].”

T1059.003 - Command and Scripting Interpreter: Windows Command Shell

“Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as SSH [10].”

T1059.004 - Command and Scripting Interpreter: Unix Shell

“Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux and macOS systems, though many variations of the Unix shell exist (e.g. sh, bash, zsh, etc.) depending on the specific OS or distribution. Unix shells can control every aspect of a system, with certain commands requiring elevated privileges [10].”

T1059.005 - Command and Scripting Interpreter: Visual Basic

“Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as Component Object Model and the Native API through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core [10].”

T1059.006 - Command and Scripting Interpreter: Python

“Adversaries may abuse Python commands and scripts for execution. Python is a very popular scripting/programming language, with capabilities to perform many functions. Python can be executed interactively from the command-line (via the `python.exe` interpreter) or via scripts (.py) that can be written and distributed to different systems. Python code can also be compiled into binary executables [10].”

T1059.007 - Command and Scripting Interpreter: JavaScript

“Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser [10].”

T1059.008 - Command and Scripting Interpreter: Network Device CLI

“Adversaries may abuse scripting or built-in command line interpreters (CLI) on network devices to execute malicious command and payloads. The CLI is the primary means through which users and administrators interact with the device in order to view system information, modify device operations, or perform diagnostic and administrative functions. CLIs typically contain various permission levels required for different commands [10].”

5 MITRE Sightings Report

The MITRE Sightings Report provides a picture of common adversary behaviors including:

- which techniques adversaries use
- how their use changes over time, and
- how adversaries use techniques together

"The Center for Threat-Informed Defense (Center), in collaboration with AttackIQ Inc., Fortinet's FortiGuard Labs, The Global Cyber Alliance, Verizon Business Solutions, and two other Center Participants, set out to answer these questions in the Sightings Ecosystem project. The Center recruited various security and service providers through existing connections, a blog post announcing the project, and the 2021 Black Hat cybersecurity event. Over several months, data contributors voluntarily shared over 6,000,000 Sightings of MITRE ATT&CK® techniques observed on their platforms. (A special thank you to ConnectWise Cyber Research Unit, LLC, FirstEnergy Corp, Red Canary, and our other data contributors. This effort would not have been possible without them.) This information created a picture of common adversary behavior including which techniques adversaries use, how their use changes over time, and how adversaries sequence techniques. Defenders can use this information to create a threatinformed defense against what they are most likely to see, not just the latest cyber threat headlines [13]."

5.1 Most Observed Techniques

Taken from the MITRE Sightings Report, these are the 15 most observed techniques. All definitons are taken directly from the MITRE ATT&CK Techiques webpage [10].

Scheduled Task/Job [T1053]

"Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to System Binary Proxy Execution, adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process [10]."

1. Command and Scripting Interpreter [T1059]

“Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution [10].”

2. Hijack Execution Flow [T1574]

“Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads [10].”

3. Proxy [T1090]

“Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. [1] Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic [10].”

4. Non-Application Layer Protocol

“Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

ICMP communication between hosts is one example. Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts. However, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications [10].”

5. Masquerading [T1036]

“Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of Masquerading [10].”

6. Signed Binary/Proxy Execution [T1218]

“Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system. Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as split to proxy execution of malicious commands [10].”

7. Create or Modify System Process [T1543]

“Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services. On macOS, launchd processes known as Launch Daemon and Launch Agent are run to finish system initialization and load user specific parameters.

Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect.

Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges [10]."

8. Process Injection [T1055]

"Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel [10]."

9. Impair Defenses [T1562]

"Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components [10]."

10. Windows Management Instrumentation [T1047]

"Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by Remote Services such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM).[1] Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement [10]."

11. Obfuscated Files or Information [T1027]

"Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and Deobfuscate/Decode Files or Information for User Execution. The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. Adversaries may also use compressed or archived scripts, such as JavaScript.

Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.

Adversaries may also obfuscate commands executed from payloads or directly via a Command and Scripting Interpreter. Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature-based detections and application control mechanisms [10]."

12. Modify Registry [T1112]

"Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.

Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility Reg may be used for local or remote Registry modification. Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API.

Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via Reg or other utilities using the Win32 API. Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence.

The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. Often Valid Accounts are required, along with access to the remote system's SMB/Windows Admin Shares for RPC communication [10]."

13. Remote Services [T1021]

"Adversaries may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).

Legitimate applications (such as Software Deployment Tools and other administrative programs) may utilize Remote Services to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including VNC to send the screen and control buffers and SSH for secure file transfer. Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data [10]."

14. Ingress Tool Transfer [T1105]

"Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command-and-control channel or through alternate protocols such as ftp. Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. Lateral Tool Transfer).

Files can also be transferred using various Web Services as well as native or otherwise present tools on the victim system.

On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, and PowerShell commands such as `IEX(New-Object Net.WebClient).downloadString()`

and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget` [10]."

6 DeTT&CT

MITRE' DeTT&CT project and web editor allows you to determine which techniques you can detect by selecting the different types of log sources available. A quote from the creators of DETT&CT - "By creating DeTT&CT we aim to assist blue teams using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviours. All of which can help, in different ways, to get more resilient against attacks targeting your organisation [11]."

6.1 DeTT&CT Process and Results

First, I entered basic information into the DeTT&CT web editor, including the platforms BB&T uses. I then added the data of what our log files collect. For example, this is what I entered for the Active directory Credential Request:

- Device Completeness: 5
- Timeliness: 5
- Retention: 3
- Data Field Completeness: 5
- Consistency: 5

After entering data for all logs, I downloaded and saved the YAML file. From here, the YAML file should be processed and uploaded to the MITRE ATT&CK Navigator by copying the .yaml file to a container or having DeTT&CT installed and running the command:

```
python dettect.py ds -fd input/dettect.yaml -l
```

7 Mitigations

To add the mitigations layer to the MITRE ATT&CK Navigator, we selected the below mitigations, colored them yellow, and assigned each a score of 10.

7.1 Mitigation Results

We mitigated the following techniques, with a score of 10 for each. All descriptions are taken from the MITRE ATT&CK Mitigations webpage [12].

Account Use Policies

"Configure features related to account use like login attempt lockouts, specific login times, etc. [12]."

Active Directory Configuration

"Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc. [12]."

Antivirus/Antimalware

"Use signatures or heuristics to detect malicious software [12]."

Audit

"Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses [12]."

Behavior Prevention on Endpoint

"Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior [12]."

Data Backup

"Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise [12]."

Data Loss Prevention

"Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII), and restrict exfiltration of sensitive data [12]."

Exploit Protection

“Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring [12].”

Filter Network Traffic

“Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic [12].”

Limit Access to Resource Over Network

“Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc [12].”

Limit Hardware Installation

“Block users or groups from installing or using unapproved hardware on systems, including USB devices [12].”

Limit Software Installation

“Block users or groups from installing unapproved software [12].”

Multi-Factor Authentication

“Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator [12].”

Network Intrusion Prevention

“Use intrusion detection signatures to block traffic at network boundaries [12].”

Operating System Configuration

“Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques [12].”

Password Policies

“Set and enforce secure password policies for accounts [12].”

Privileged Account Management

“Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root [12].”

Restrict Web-Based Content

“Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc [12].”

Software Configuration

“Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates [12].”

SSL/TLS Inspection

“Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity [12].”

Update Software

“Perform regular software updates to mitigate exploitation risk [12].”

User Account Control

“Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access [12].”

User Account Management

“Manage the creation, modification, use, and permissions associated to user accounts [12].”

User Training

“Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction [12].”

Vulnerability Scanning

“Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them [12].”

8 Gap Analysis

Gap analysis is a computed layer that shows where are detections and mitigations are weak against the threat that BB&T faces. The Gap Analysis was created from the 5 previous layers using the domain as ATT&CK v11 & the score expression as (a+b+c)-(d+e). I changed the palette to the 'green to red' and changed the low value to 0. This generated a layer with green, white, yellow, orange, red and light green items. These colors represent techniques where BB&T may not have the best visibility or mitigations if an attacker chooses to use that specific technique.

8.1 Gap Analysis Results

Techniques marked as white do not have either threats nor controls addressed. Other colors are those that have some gap as identified previously.

White

- Search Open Websites/Domains
- Stage Capabilities
- External Remote Services
- Replication Through Removable Media
- Trusted Relationship
- Serverless Execution
- Account Manipulation
- BITS Jobs
- Event Triggered Execution
- External Remote Services
- Modify Authentication Process
- Server Software Component
- Traffic Signaling
- Escape to Host
- Event Triggered Execution
- BITS Jobs
- File and Directory Permissions Modification
- Indicator Removal
- Modify Authentication Process
- Traffic Signaling
- Adversary-in-the-Middle
- Modify Authentication Process
- Steal or Forge Authentication Certificates
- Cloud Service Discovery
- Password Policy Discovery

- Replication Through Removable Media
- Adversary-in-the-Middle
- Data from Cloud Storage
- Data from Network Shared Drive
- Traffic Signaling
- Exfiltration Over Web Service
- Transfer Data to Cloud Account
- Firmware Corruption

Light Green

- Network Service Discovery

Yellow

- Valid Accounts
- Command and Scripting Interpreter
- Scheduled Task/Job
- Scheduled Task/Job
- Valid Accounts
- Exploitation for Privilege Escalation
- Scheduled Task/Job
- Valid Accounts
- Masquerading
- Steal Web Session Cookie
- Domain Trust Discovery
- File and Directory Discovery
- Remote System Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Service Discovery
- Data from Local System
- Ingress Tool Transfer
- Proxy
- Data Encrypted for Impact
- System Shutdown/Reboot

Red

- Windows Management Instrumentation
- Process Injection

- Impair Defenses

The technqiues listed under yellow and red should be top priority for BB&T.

9 References

[1] "Mitre ATT&CK®," *MITRE ATT&CK®*. [Online]. Available: https://attack.mitre.org/. [Accessed: 28-Jan-2023].

[2] "Threat Assessment/Analysis," *NIST*. [Online]. Available: https://csrc.nist.gov/glossary/term/threat_assessment_analysis. [Accessed: 28-Jan-2023].

[3] "Threat Actor," *NIST*. [Online]. Available: https://csrc.nist.gov/glossary/term/threat_actor. [Accessed: 28-Jan-2023].\

[4] "TTP," *NIST*. [Online]. Available: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures. [Accessed: 28-Jan-2023].

[5] "What is EDR? - endpoint detection and response," *Cisco*, 20-Dec-2022. [Online]. Available: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html. [Accessed: 29-Jan-2023].

[6] "Separation of Duty (SOD)," *NIST*. [Online]. Available: https://csrc.nist.gov/glossary/term/separation_of_duty. [Accessed: 29-Jan-2023].\

[7] "Security Information and Event Management (SIEM) Tool," *NIST*. [Online]. Available: https://csrc.nist.gov/glossary/term/separation_of_duty. [Accessed: 29-Jan-2023].\

[8] "What is SOAR?," *Palo Alto Networks*. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-soar. [Accessed: 29-Jan-2023].

[9] "Software," *MITRE ATT&CK®*. [Online]. Available: https://attack.mitre.org/software/S0002/. [Accessed: 29-Jan-2023].

[10] "Techniques," MITRE ATT&CK®. [Online]. Available: https://attack.mitre.org/techniques/enterprise/. [Accessed: 29-Jan-2023].

[11] "DeTT&CK: Mapping Your Blue Team to MITRE ATT&CK," *MB Secure*. [Online]. Available: https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack. [Accessed: 29-Jan-2023].

[12] "MITIGATIONS," MITRE ATT&CK. [Online], Available: https://attack.mitre.org/mitigations/. [Accessed: 29-Jan-2023].

[13] "Sightings Ecosystem: A Data-driven Analysis of ATT&CK in the Wild," MITRE ENGENUITY. [Online], Available: https://info.mitre-

engenuity.org/hubfs/Center%20for%20Threat%20Informed%20Defense/CTID-Sightings-Ecosystem-Report.pdf. [Accessed: 29-Jan-2023].