CYBER THREAT ATTRIBUTION LEXICON

BACKGROUND

The characterization of cyber threats in a consistent, repeatable, and transparent fashion remains a critical challenge for timely and effective sharing of actionable cyber threat information. Advanced polymorphic malware and file-less intrusion methods, combined with evolving command and control methodologies based in social media or embedded in legitimate traffic, make descriptions and attribution of malicious cyber activity an increasingly difficult task. Understanding these threats and sharing actionable descriptions is critical for providing early warnings, protections for critical infrastructure, and attribution of the origin and responsibility for malicious cyber activity.

Sharing descriptive cyber threat activity and the utility of the collected/reported data is greatly enhanced when based on a common approach – a framework – that enables consistent and repeatable groupings of data while supporting individual use cases (or consumer needs).

A number of cybersecurity-related frameworks exist in government and private industry. Each framework reflects the priorities and interests of its organization, however, disparities across frameworks make it difficult to facilitate efficient sharing and/or situational analysis based on objective data.

To facilitate government communication on cyber threats, the Office of the Director of National Intelligence (ODNI) led an effort among federal agencies to codify best practices in a common cyber threat framework (CTF)[1] that serves as a translator to normalize disparate models and facilitate the exchange of threat data. Subsequently, the National Security Agency leveraged the CTF as the basis for its Technical Cyber Threat Framework.[2]

To further connect government frameworks with those in common use in the private sector, a public-private working group, convened under DHS's Critical Infrastructure and Partnership Advisory Council authority, was chartered to create shared lexicon. The group assessed existing cyber threat information methodologies, developed a matrix comprising a correlation of Tactics, Techniques, and Procedures (TTPs), and crafted a *Cyber Threat Attribution Lexicon* that captures shared characteristics of the TTPs.

Organizations that contributed to this effort include: DHS, FBI, NSA, ODNI, USCC, AT&T, IBM, Intel, Leidos, KMB Strategies, McAfee, Microsoft, MITRE, and Symantec.

---

[1] https://www.dni.gov/index.php/cyber-threat-framework

[2] https://media.defense.gov/2019/Jul/16/2002158108/-1/-1/0/CTR_NSA-CSS-TECHNICAL-CYBER-THREAT-FRAMEWORK_V2.PDF

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
AppCert DLLs	Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key KEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager are loaded into every process that calls the ubiquitously used application programming interface (API) functions CreateProcess, CreateProcessAsUser,CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec.	**ATT&CK**: T1182-AppCert DLLs **NTCTF**: Modify configuration to facilitate launch
Access Raw Data	Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools.	**ATTC&K**: T1006-File System Logical Offsets **NTCTF**: Access Raw Disk
Account Manipulation	Account manipulation may aid adversaries in maintaining access to credentials and maintaining certain permissions within an environment. It can consist of modifying permissions, modifying credentials, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.	**ATT&CK**: T1098-Account Manipulation **NTCTF**: Add or modify credentials
Application Deployment Software	Attempts to deploy new software to systems using application deployment systems already employed by site administrators. The permissions required for this action varies by configuration; however, local credentials may be sufficient for direct access to the deployment server.	**ATT&CK**: T1017-Application deployment software **NTCTF**: Use application deployment software
Application Shimming	The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses Hooking to redirect the code as necessary in order to communicate with the OS.	**ATT&CK:** T1138-Application Shimming **NTCTF**: Modify configuration to facilitate launch
Application Windows Discovery	Attempts to obtain a list of all application windows, both visible and invisible.	**ATT&CK**: T1010-Application Window Discovery **NTCTF**: Enumerate Windows
Applnit Dynamic-Link Libraries (DLL)	DLLs that are specified in the AppInit_DLLs value in the Registry keys HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows or HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program,	**ATT&CK**: T1103-Applnit DLLs **NTCTF:** Modify configuration to facilitate launch

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
	since user32.dll is a very common library. Similar to Process Injection, these values can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.	
Authentication Package Load at Startup	Windows Authentication Package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.	**ATT&CK:** T1131-Authentication Package **NTCTF**: Set to load at startup
Automated Collection	Use of automated techniques to search, identify, or obtain data. An example technique is the use or automated scripting designed to search for and copy data matching certain criterion at specific times.	**ATT&CK**: T1119-Automate Collection **NTCTF**: Run Collection Script
BITS Jobs	Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM). BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.	**ATT&CK**: T1197-BITS Jobs **NTCTF**: Modify configuration to facilitate launch
Capture Audio	An adversary's use of a computer's peripheral devices (i.e. microphones and webcams) or applications such as voice and video call services to capture audio recordings for the purpose of listening into sensitive conversations to gather information.	**ATT&CK**: T1123-Audio Capture **NTCTF**: Active Recording
Capture Screenshots	Actions to capture screen shots of desktop to gather information over the course of an operation. Example: Screen capturing functionality may be included as a valid feature of a remote access.	**ATT&CK**: T1113-Screen Capture **NTCTF**: Take Screen Capture
Capture Video	Actions to use of a computer's peripheral devices (i.e. integrated cameras or webcams) or applications such as video call services to capture video files or images to gather information.	**ATT&CK**: T1125-Video Capture **NTCTF**: Activate recording
Change File Association	Malicious use of applications to modify the file handler for a given file extension to call an arbitrary program when a file with the given extension is opened. Illustration: when a file is opened, its file extension or header is checked to determine which program opens the file. In Windows, these defaults are stored in the registry and can be edited by programs that have registry access.	**ATT&CK**: T1042-Change Default File Association **NTCTF**: Edit file-type associations
CMSTP	The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.	**ATT&CK**: T1191-CMSTP **NTCTF**: User trusted application to execute untrusted code

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Code Signing	Use of certificates (that were forged, stolen or created by the adversary) during an operation. Illustration: Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. However, adversaries are known to use code signing certificates to masquerade malware and tools as legitimate binaries.	**ATT&CK**: T1116- Code Signing **NTCTF**: Sign malicious content
Complied HTML File	Compiled HTML files (.chm) are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. CHM content is displayed using underlying components of the Internet Explorer browser loaded by the HTML Help executable program (hh.exe).	**ATT&C:**; T1223-Complied HTML File **NTCTF:** User trusted application to execute untrusted code
Component Object Model (COM) Hijacking	COM is a system within Windows to enable interaction between software components through the operating system. Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead. An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.	**ATT&CK**: T1122- Component Object Model Hijacking **NTCTF**: Modify configuration to facilitate launch
Compromise Supply Chain	Manipulation of trusted product(s) and/or product delivery mechanisms- by adding malicious software, hardware, or configurations- for the purpose of data or system compromise to the target network.	**ATT&CK**: T1195-Supply Chain Compromise **NTCTF**: Compromise Supply Chain or Trusted Source
Conduct Social Engineering	Psychological manipulation of users by a threat actor into performing actions or divulging information. This type of manipulation may lead to other execution techniques frequently occurring shortly after Initial Access or occurring at other phases of intrusion Examples of such manipulation include direct code or via Spearphishing attachments	**ATT&CK**: T1195-Supply Chain Compromise **NTCTF**: Compromise Supply Chain or Trusted Source
Connect Removable Media	Deployment of malicious code via removable media (programmed to auto-run/ automatically execute upon insertion in a device) containing modified executable files, media firmware, or media initially formatted using compromised systems.	**ATT&CK**: T1091-Replication Through Removable Media **NTCTF**: Connect Removable Media
Connect Rogue Network Devices	The insertion or use of existing rogue interfaces- computer accessories, computers, or network hardware-used to gain execution capabilities.	**ATT&CK:** T1200-Hardware Additions **NTCTF:** Connect Rogue Network Devices

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Crack Passwords	Use of password cracking techniques to access to accounts. An example technique is brute force to attempt access to accounts when passwords are unknown or when password hashes are obtained.	**ATTC&K**: T1110-Brute Force **NTCTF**: Crack passwords
Create New Service	Creating a new service to be started by the operating system by directly modifying the registry (or similar construct) or by using tools which do so.	**ATT&CK**: T1035 - Service Execution, T1050 - New Service **NTCTF**: Execute via service controller, Create new service
Credential Dumping	The process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.	**ATT&CK**: T1003-Credential Dumping **NTCTF**: Dump Credentials
Credential in Fields	Attempt to search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.	**ATT&CK**: T1081-Credential in Fields **NTCTF**: Locate Credentials
Credentials in Registry	The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.	**ATT&CK:** T1214-Credentials in Registry **NTCTF:** Locate credential
Enumerate Accounts and Permissions	Adversary attempts to obtain a list of all local and domain accounts, their permissions, members, and login and file modification times.	**ATT&CK:** T1069-Permission Groups Discovery, T1087-Account Discover **NTCTF**: Enumerate accounts and permissions
Execute Arbitrary Binaries	Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries.	**ATT&CK**: T1117- Regsvr32 **NTCTF**: User trusted application to execute untrusted code
Execute Service	Adversaries may execute a binary, a command, or a script via processes that interact with native (OS) as well as other services –such as the Service Control Manager. The intent is to create a new service or modify an existing service. This may be achieved, by performing the Execute technique in conjunction with the Create New Service or Modify Existing Service technique.	**ATT&CK**: T1035 - Service Execution, T1050 - New Service, T1031 - Modify Existing Service **NTCTF**: Execute via service controller, Create new service, Modify existing service
Execute via Third Party Software	Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, VNC, HBSS, Altiris, etc.). If an adversary gains access to these systems, then they may be able to execute code.	**ATT&CK**: T1072- Third-Party Software **NTCTF**: Execute Via Third Party Software

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Execution Through API	Adversarial use of the operating system (OS) application programming interface (API) to execute binaries. Example: Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters.	**ATT&CK**: T1106- Execution through API **NTCTF**: User OS APIs
Exfiltration over C2 Channel	Data exfiltration is performed over the Command and Control channel. Data is encoded into the normal communications channel using the same protocol as command and control communications	**ATT&CK**: T1041- Exfiltration Over Command Control Channel **NTCTF**: Send over C2 Channel
Exfiltration over Non- C2 Channel	Data exfiltration is performed over the same network as the adversary command and control channel, or other directly connected networks, but data is likely to be routed through an alternative network location from the main command and control server.	**ATT&CK**: T1048- Exfiltration over Alternate Protocol **NTCTF**: Send over Non C2 Channel
Exfiltration Over Other Network Medium	Data exfiltration is performed over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel.	**ATT&CK**: T1011-Exfiltration Over Other Network Medium **NTCTF**: Send over Other Network Medium
Exfiltration over Physical Medium	In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to move between otherwise disconnected systems.	**ATT&CK**: T1052- Exfiltration over Physical Medium **NTCTF**: Transfer via Physical Means
Exploit Public-Facing Application	Using software, data, or commands to take advantage of a weakness (i.e. bug, a glitch, or design vulnerability) in a public-facing computer system/program/service for the purpose of causing unintended or unanticipated behavior. The most common example of this technique is the injection of malicious SQL commands into unchecked input fields, allowing data theft, modification, or execution of malicious commands.	**ATT&CK**: T1190-Exploit Public-Facing Application **NTCTF**: Inject Database Command
Exploiting Application Software Vulnerability	Adversaries' execution of an exploit of a vulnerability in software on the target system.	**ATT&CK**: T1068- Exploitation for Privilege Escalation **NTCTF**: Exploit application vulnerability
Exploiting OS or Software Services Vulnerability	Adversaries' execution of an exploit of a vulnerability in the OS or supporting software services on the target system.	**ATT&CK**: T106- Exploitation for Privilege Escalation **NTCTF**: Exploit OS or service vulnerability

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
File Deletion	Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces behind as to what was done within a network and how. Adversaries may remove these files over the course of an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process.	**ATT&CK**: T1107-File Deletion **NTCTF**: Remove toolkit
File System and Network Share Discovery	Attempts to create a list of accessible files and directories on the system. These may include all or selected files on the local system or via network shares.	**ATT&CK**: T1083-File and Directory Discovery, T1135-Network Share Discovery **NTCTF**: Enumerate file system
File System Permissions Weakness	Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.	**ATT&CK**: T1044- File System Permissions Weakness **NTCT**F: Replace Service Binary
Forced Authentication	The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. This behavior is typical in enterprise environments so users do not need to enter credentials to access network resources. Web Distributed Authoring and Versioning (WebDAV) is typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443.	**ATT&CK**: T1187 - Forced Authentication **NTCTF**: Social engineering
Hijack Active Credentials	Malicious interception of authentication tokens that a legitimate user has activated or that are being used without the user's knowledge. Examples include adversaries targeting authentication mechanisms, such as smart cards and valid Kerberos ticket-granting tickets (TGT), to gain access to systems, services, and network resources	**ATT&CK**: T1111-Two Factor Authentication Interception **NTCTF**: Hijack active credentials
Image File Execution Options (IFEO) Injection	IFEO enables a developer to attach a debugger to an application. When a process is created, a debugger present in an application's IFEO will be prepended to the application's name, effectively launching the new process under the debugger (e.g., "C:\dbg\ntsd.exe -g notepad.exe").	**ATT&CK**: T1183-Image File Execution Options Injection **NTCTF**: Modify configuration to facilitate launch
Indicator Blocking	Attempts to block indicators or events typically captured by sensors from being gathered and analyzed. This could include modifying sensor settings stored in configuration files and/or Registry keys to disable or maliciously redirect event telemetry.	**ATT&CK**: T1054-Indicator Blocking **NTCTF**: Blocks indicators on host
Infect via Website	Embedding malicious code into a website to gain access to a user's system upon visiting.	**ATT&CK**: T1189-Drive-by Compromise **NTCTF**: Infect via websites

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Inject Code into Running Process	Attempts to inject foreign code into an existing process or into memory.	**ATT&CK**: T1055-Process Injection **NTCTF**: Inject into running process
Input Capture	Using methods of capturing user input for obtaining credentials for Valid Accounts and Information Collection that include keylogging and user input field interception.	**ATT&CK**: T1056-Input Capture **NTCTF**: Log Keystrokes
InstallUtil	InstallUtil, a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. InstallUtil is located in the .NET directories on a Windows system: *C:\Windows\Microsoft.NET\Framework\v\InstallUtil.exe* and *C:\Windows\Microsoft.NET\Framework64\v\InstallUtil.exe*. The *InstallUtil.exe* is digitally signed by Microsoft.	**ATT&CK**: T1118-InstallUtil **NTCTF**: User trusted application to execute untrusted code
Leverage Authorized Users	Reliance upon specific actions by an authorized user in order to gain installation and execution of code. Examples include direct code execution when a user opens a malicious executable delivered via Spearphishing Attachments or Spearphishing Links.	**ATT&CK**: T1024- User Execution **NTCTF**: Leverage Authorized User
Leverage Scripting Language	Using scripts to aid in operating and performing multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Examples include VBScript, PowerShell, and command-line batch scripts.	**ATT&CK**: T1064- Scripting, T1086- PowerShell, T1059- Command Line Interface **NTCTF**: User Interpreted Scripts, Run Commands in Shell
Library Search Order Hijacking	Taking advantage of the library search order and programs that ambiguously specify libraries to gain privilege escalation and persistence Example-Windows systems use a common method to look for required DLLs to load into a program.	**ATT&CK**: T1038- DLL Search Order Hijacking **NTCTF**: Use library-search hijack
Logon Scripts	Use of logon scripts to insert additional code that allows maintaining persistence or moving laterally within an enclave because it is executed each time the affected user(s) logon to a computer. Modifying logon scripts can effectively bypass workstation and enclave firewalls. Depending on the access configuration of the logon scripts, either local credentials or a remote administrative account may be necessary.	**ATT&CK**: T1037-Logon Scripts **NTCTF**: Employ Logon Scripts
LSA Subsystem Services (LSASS) Driver	The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple DLLs associated with various other security functions, all of which run in the context LSASS (lsass.exe) process.	**ATT&CK**; T1177-LSASS Driver **NTCTF**; Modify configuration to facilitate launch

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Map Accessible Networks	Attempts to obtain a map of the networks, systems, and processes accessible from a device. This may require sending messages on those networks and analyzing the responses	**ATT&CK**: T1018-Remote System Discovery **NTCTF**: Map accessible networks
Mimic Legitimate Traffic	Actions to avoid detection by blending in with existing traffic. This could include using standard protocols and ports, similar volume, same time of day, source and destinations, and types of traffic that occur internally within enclave. C2 commands and results are embedded within the traffic between the client and server.	**ATT&CK: T1032-**Standard Cryptographic Protocol, T1071-Standard Application Layer Protocol, T1095-Stardard Non-Application Layer Protocol, T1102-Web Services **NTCTF**: Mimic Legitimate Traffic
Misuse of accessibility features	An adversary can launch/modify accessibility features to obtain a system access without logging in to the system.	**ATT&CK**: T1015-Accessibility Features **NTCTF**: Use accessibility features
Modify Existing Services	Windows service configuration information, including the path to the services' executable and recovery programs/commands, is stored in the Windows Registry. Service configurations can be modified using utilities such as sc.exe and Reg. Adversaries may also use these utilities or custom tools to modify and execute an existing service or to directly modify the Registry. Such modifications may interrupt the functionality of existing services or enable services that are generally disabled or not commonly used.	**ATT&CK**: T1035 - Service Execution, T1031 – Modify Existing Service **NTCTF**: Execute via service controller, Modify existing service
Modify Registry	Interaction with the Operating Systems (OS) 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.	**ATT&CK**, T1112-Modify Registry **NTCTF**, Employ anti-forensics measures
Modify Service Configuration	The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, PowerShell, or Reg. Access to Registry keys is controlled through Access Control Lists and permissions.	**ATT&CK**: T1058- Service Registry Permissions Weakness **NTCTF**: Modify Service Configuration
Modify Shortcut Links	Links redirect from one location to another location. The adversary may edit or create a link so that data or execution occurs in an alternate location than intended to maintain persistence or escalate privileges.	**ATT&CK**: T1023- Shortcut Modification **NTCTF**: Modify Links
Map Accessible Networks	Attempts to obtain a map of the networks, systems, and processes accessible from a device. This may require sending messages on those networks and analyzing the responses	**ATT&CK**: T1018-Remote System Discovery **NTCTF**: Map accessible networks

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Modify System Firmware	The BIOS (Basic Input/Output System) or Unified Extensible Firmware Interface (UEFI), which underlies the functionality of a computer or other device, may be modified to perform or assist in malicious activity.	**ATT&CK**: T1019- System Firmware **NTCTF**: Modify BIOS
Modify Timestamp	Modification of timestamps of a file to mimic that of files in the same folder in order that compromised files modified or created by the adversary does not appear conspicuous to forensic investigators or file analysis tools. Example is using this Timestamping technique along with file name Masquerading to hide malware and tools.	**ATT&CK**: T1099-Timestomp **NTCTF**: Employ anti-forensics measures
Mshta	Mshta.exe is a utility that executes Microsoft HTML Applications (HTA). HTA files have the file extension .hta. HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser.	**ATT&CK**; T1170-Mshta **NTCTF**: User trusted application to execute untrusted code
Netsh Helper DL	Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility. The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at HKLM\SOFTWARE\Microsoft\Netsh.	**ATT&CK**: T1128-Netsh Helper DLL **NTCTF**: Modify configuration to facilitate launch
Network Connections Ports & Protocols	Adversary attempts to identify the set of all network connections into and out of a system. Includes monitoring privilege access to the Boundary Control Device (BCD).	**ATT&CK**: T1049-System Network Connections Discovery **NTCTF**: Enumerate Local Network Connections
Network Sniffing	Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.	**ATT&CK**: T1040- Network Sniffing **NTCTF**: Sniff Network
Obfuscated Data and Information	Attempts 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.	**ATT&CK**: T1027- Obfuscated Files or Information **NTCTF**: Obfuscate data
Office Application Startup	Multiple mechanisms may be used with Microsoft Office (a fairly common application suite on Windows-based operating systems) within an enterprise network for persistence when an Office-based application is started.	**ATT&CK**: T1137- Office Application Startup **NTCTF**: Modify configuration to facilitate launch
OS and System Information Discovery	Adversary attempts to obtain detailed information about the OS version, application packages, patches, hotfixes, service packs, architecture, configuration, and drivers.	**ATT&CK**: T1082 **NTCTF**: Enumerate OS and software

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Pass the Hash	A method used to bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with Pass the Hash (PtH) to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.	**ATT&CK**: T1075-Pass the Hash **NTCTF**: Pass the hash
Pass the Ticket	A method used to bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the Kerberos ticket. In this technique valid Kerberos tickets for the account are either captured using a Credential Access techniques or generated by an attacker who has the right level of access to generate forged tickets through the golden ticket attacked. Kerberos tickets are used with Pass the hash (PtH) to authenticate as a user. Once authenticated, PtT may be used to logon to remote or local systems.	**ATT&CK**: T1097-Pass the Ticket **NTCTF**: Pass the ticket
Path Interception	Occurs when an executable is placed in a specific path so that it is executed by an application instead of the intended target. Example is the use of a copy of cmd in the current working directory of a vulnerable application that loads a CMD or BAT file with the CreateProcess function.	**ATT&CK**: T1034- Path Interception **NTCTF**: Leverage path-order execution
Port Monitors	Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Registry. Service configurations can be modified using utilities such as sc.exe and Reg.	**ATT&CK**: T1013-Port Monitors **NTCTF**: Set to load at startup
Private Keys	Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures.	**ATT&CK**: T1145-Private Keys **NTCTF**: Locate credentials
Process discovery	Enumeration of global libraries and APIs. Adversary attempts to obtain information about the system's running processes and registered services, including any shared libraries they use.	**ATT&CK:** T1057-Process Discovery **NTCTF:** Enumerate Processes
Process Injection	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. Example - Malicious software may inject into a trusted process to gain elevated privileges without prompting a user.	**ATTC&K**: T1055-Process Injection **NTCTF**: Manipulate trusted process
Proxy Execute of Binaries	Using binaries signed with trusted digital certificates to 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. This behavior may be abused by adversaries to execute malicious files that could bypass application whitelisting and signature validation on systems. This technique	**ATT&CK**: T1218- Signed Binary Proxy Execution

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
	accounts for proxy execution methods that are not already accounted for within the existing techniques	**NTCTF**: User trusted application to execute untrusted code
Proxy Execute of Malicious Files	Using scripts signed with trusted certificates to proxy execute malicious files. This behavior may bypass signature validation restrictions and application whitelisting solutions that do not account for use of these scripts.	**ATT&CK**: T1216- Signed Script Proxy Execution **NTCTF**: User trusted application to execute untrusted code
Regsvcs/Rregasm	Regsvcs and Regasm are Windows command-line utilities used to register .NET Component Object Model (COM) assemblies. Both utilities are digitally signed by Microsoft.	**ATT&CK**: T1121-Regsvcs/Rregasm **NTCTF**: User trusted application to execute untrusted code
Remote File Access/Read/Write	Files may be copied from one system to another to stage adversary tools or other files over the course of an operation. Files may be copied from an external adversary-controlled system through the Command and Control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP.	**ATT&CK:**T1105-Remote File Copy, T1077-Windows Admin Share **NTCTF**: Write to remote file shares
Remote Login	Maliciously using valid credentials to login to a remote host for manual interactions, through a GUI or command line interface that is sent back to the initiator of the remote connection. Actions may then be performed as an authenticated, logged on user. Example is remote desktop, a common feature in operating systems which allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).	**ATT&CK**: T11076-Remote Desktop Protocol, T1077-Windows Admin shares **NTCTF**: Logon remotely
Remote Services	Using Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. Adversarial access may then be used to perform actions as an authenticated, logged-on user.	**ATT&CK**: T1028-Windows Remote Management, T1021-Remote Services, T1175-Distributed Component Object Model, T1077-Windows Admin Shares **NTCTF**: Use remote services
Removal of Indicator(s) from Host	Deleting or altering generated artifacts on a host system, including logs and potentially captured files such as quarantined malware. Locations and format of logs will vary.	**ATTC&K**: T1070- Indicator Removal from Host **NTCTF**: Remove logged data
Remove Files	Removing files that leave traces of an attack in order to lessen or remove an adversaries' footprint at the end of an intrusion. Examples include malware, tools, or other non-native files that may have been created on dropped during the course of an attack.	**ATT&CK**: T1107-File Deletion **NTCTF**: Employ anti-forensics measures

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Remove Indicators from Host	Deleting or altering operation system (OS) generated artifacts on a host system, including logs and potentially captured files such as quarantined malware. Locations and format of logs will vary with operation system.	**ATT&CK**: T1070-Indicator Removal from Host **NTCTF**: Employ anti-forensics measures
Replicate through Removable Media	Using Autorun features to copy malware onto removable media, thin inserting and executing media into a system. Especially on disconnected systems or air-gapped networks, by copying malware to removable media and Examples include 1) modifying executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system and 2) manually manipulating media or modifying of systems used to initially format the media, or modification to the media's firmware itself	**ATT&CK**: T1091-Replication Through Removal Media **NTCTF**: Replicate through removable media
Rootkits	Rootkits are programs that hide the existence of malware by intercepting (i.e., Hooking) and modifying operating system API calls that supply system information. Rootkits or rootkit enabling functionality may reside at the user or kernel level of the operating system or lower, to include a Hypervisor, Master Boot Record, or the System Firmware. Adversaries may use rootkits to hide the presence of programs, files, connections, services, and/or drivers.	**ATT&CK**: T1014-Roolkit **NTCTF**: Employ Rootkit
Schedule Task	Utilities such as *at* and, along with the Windows Task Scheduler, can be used to schedule tasks or to execute programs/scripts at a specified date and time for the purpose of persisting adversary code or gaining SYSTEM privileges. Task scheduling typically requires administrator privileges on local systems, but may be configured to run with SYSTEM privileges. Task scheduling on a remote system typically requires proper authentication to use RPC, file/printer sharing be turned on, and administrator privileges on the remote system.	**ATT&CK**: T1058- Scheduled Tasks **NTCTF**: Create Scheduled Tasks
Security Hardware and Software Discovery	Attempts to obtain detailed information about security software, defensive tools, sensors, and configurations installed on the system. Examples include local firewall rules, anti-virus, IDS/IPS, VPN, virtualization, etc.	**ATT&CK:** T1063 **NTCTF:** Enumerate OS and software
Set to Load at Startup	Causing the system to automatically load and execute code after the operating system has started.	**ATT&CK**: T1131-Authentication Package, T1101-Security Support Provider, T1209-Time Providers **NTCT:** Set to load at startup
SIP and Trust Provider Hijacking	In user mode, Windows Authenticode digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust API function, which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature.	**ATT&CK:** T1198-SIP and Trust Provider Hijacking **NTCTF:** Modify configuration to facilitate launch
Spearphishing	Embedding malware via use of links to down load or attachments within an email message, sent to a target. Target is compromised after opening or executing the attached file, upon clicking the link or upon loading the email itself, and potentially providing access to a malicious actor.	**ATT&CK**: T1193-Spearphishing Attachment, T1192-Spearphishing Link **NTCTF**: Send malicious email

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Staged Data	Data, collected from one or more sources, is maintained and staged in a central location prior to exfiltration. Data may have been aggregated into one file by using techniques such as data compression or data encryption.	**ATT&CK**: T1074-Data Staged **NTCTF**: Position Data
Stores Files in Unconventional Location	Data or executables may be stored in file system metadata, slack space, registries, outside logical partition, or some other conventional location instead of directly in files to evade file monitoring tools. These actions leverage standard disk read/write operations (different from raw access).	**ATT&CK**: T1158-Hidden Files and Directories **NTCTF**: Stores files in unconventional location
Schedule Task	Utilities such as *at* and, along with the Windows Task Scheduler, can be used to schedule tasks or to execute programs/scripts at a specified date and time for the purpose of persisting adversary code or gaining SYSTEM privileges. Task scheduling typically requires administrator privileges on local systems, but may be configured to run with SYSTEM privileges. Task scheduling on a remote system typically requires proper authentication to use RPC, file/printer sharing be turned on, and administrator privileges on the remote system.	**ATT&CK**: T1058- Scheduled Tasks **NTCTF**: Create Scheduled Tasks
Security Hardware and Software Discovery	Attempts to obtain detailed information about security software, defensive tools, sensors, and configurations installed on the system. Instances include local firewall rules, anti-virus, IDS/IPS, VPN, virtualization, etc.	**ATT&CK:** T1063 **NTCTF:** Enumerate OS and software
Set to Load at Startup	Causing the system to automatically load and execute code after the operating system has started.	**ATT&CK**: T1131-Authentication Package, T1101-Security Support Provider, T1209-Time Providers **NTCT:** Set to load at startup
SIP and Trust Provider Hijacking	In user mode, Windows Authenticode digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust API function, which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature.	**ATT&CK:** T1198-SIP and Trust Provider Hijacking **NTCTF:** Modify configuration to facilitate launch
Taint Shared Content	Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. The adversary may use tainted shared content to move laterally or may use the malicious portion of the tainted shared content to run code on a remote system once a user has opened it.	**ATT&CK**: T1080-Taint shared content **NTCTF:** Taint shared content
Time Providers	The Windows Time service (W32Time) enables time synchronization across and within domains. W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients.	**ATT&CK**: T1209-Time Providers **NTCTF**: Set to load at startup
Trusted Developer Utilities	There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering. These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted	**ATT&CK**: T1127- Trusted Developer Utilities

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
	process that effectively bypasses application whitelisting defensive solutions.	**NTCTF:** User trusted application to execute untrusted code
Trusted Relationship	Breach or otherwise leverage of organizations who have access to the adversaries' intended victims. This access through trusted third party relationships exploit an existing connection that may not be protected or that may receive less scrutiny than standard mechanisms required to gain access to a network.	**ATT&CK:** T1199-Trusted Relationship **NTCTF:** Leverage Trusted Relationship
Unwarranted window memory extension	Attempts to access and extend memory allocation for Windows-based process.	**ATT&CK:** T118-Extra Window Memory Injection **NTCTF:** Inject into running process
Use of Legitimate Credentials	Theft of a specific user's credentials or service accounts; using credential access techniques or capturing credentials earlier in their reconnaissance process through social engineering with the intent of gaining access to a system or resources. An example is an adversary leveraging legitimate access controls to obtain entry to restricted areas within a network or to obtain escalated privileges with the intent of accessing resources on a specific system.	**ATT&CK**: T1078- Valid accounts **NTCTF:** Impersonate or spoof user, User legitimate credentials
Used Signed Content	Use of a signed content or code for malicious purposes, including computed has collisions, legitimate signed software for malicious purposes, since signed content is either required or trusted by default.	**ATT&CK:** T1218-Signed Binary Proxy Execution **NTCTF:** Used Signed Content
Using A Common Application Layer Protocol for C2	Use of a common, standardized application layer protocol (e.g., HTTP, SMTP, DNS, etc.) to relay command and control data to a compromised system.	**ATT&CK**: T1071 **NTCTF:** Mimic legitimate traffic
Using a Legitimate Web Service for C2	Use of an existing, valid web services to relay command and control data to a compromised system.	**ATT&CK:** T1102 **NTCTF:** Mimic legitimate traffic
Using a Non-application Layer Protocol for C2	Use of a non-application layer protocol (e.g., ICMP, SOSCK, UDP, tunneling protocols, etc.) to relay command and control data to a compromised system.	**ATT&CK**: T1095- Standard Non-Application Layer Protocol **NTCTF**: Mimic legitimate traffic
Using Encryption to Conceal	Use of a known encryption algorithm (DES, AES, etc.) to relay command and control data to a compromised system.	**ATT&CK**: T1032 **NTCTF**: Mimic legitimate traffic

ATTRIBUTE (TECHNIQUE)	DESCRIPTION	REFERENCES
Using Removable Media to Propagate Files	Use of a removable media to propagate malware or other attack files from one system to another.	**ATT&CK**: T1092 **NTCTF**; Use removable media
Windows Remote Management (WinRM)	WinRM is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, and modify services). It may be called with the winrm command or by any number of programs such as PowerShell.	**ATT&CK**: T1028-Windows Remote Management **NTCTF**: Use remote services
Windows Security Support Provider (SSP)	SSP DLLs are loaded into the Local Security Authority (LSA) process at system startup. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords stored in Windows. The SSP configuration is stored in two Registry keys which the adversary may modify to add new SSPs. These SSPs will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called. The two Registry keys are: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages and HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages.	**ATT&CK:** T1101-Security Support Provider **NTCTF:** Set to load at startup
Write to Shared Webroot	Adversaries may add malicious content to a website through the open file share and then browse to that content via a web browser to cause the server to execute the content. This malicious content will typically run under the context and permissions of the web server process, often resulting in local system or administrative privileges -based on the webserver's configuration.	**ATT&CK**: T1051-Shared webroot **NTCTF**: Write to shared webroot
XSL Script Processing	Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages.	**ATT&CK:** T1220- XSL Script Processing **NTCTF**: User trusted application to execute untrusted code

**Exercise revealed ~80% Correlation between ATT&CK and NTCTF Frameworks