NATIONAL SECURITY AGENCY
CYBERSECURITY REPORT

NSA/CSS Technical Cyber Threat Framework v2

A REPORT FROM:
CYBERSECURITY OPERATIONS
THE CYBERSECURITY PRODUCTS AND SHARING DIVISION

29 November 2018

PP-18-0844

(U) DOCUMENT CHANGE HISTORY

DATE	VERSION	DESCRIPTION
08 March 2018	V1	NTCTF_v1 release date
09 November 2018	V2	NTCTF_v2 release date
29 November 2018	V2	Minor revisions

(U) EXECUTIVE SUMMARY

(U) The "NSA/CSS Technical Cyber Threat Framework v2" (NTCTF v2) was developed as a technical extension of the Director of National Intelligence Cyber Threat Framework. Designed to standardize how NSA characterizes and categorizes adversary activity by using a common technical lexicon that is operating system independent and closely aligned with industry definitions. This common technical cyber lexicon supports sharing, product development, operational planning, and knowledge driven operations across the Intelligence Community. Public dissemination of the technical cyber lexicon allows for collaboration with whole-of-community. Use of the NTCTF facilitates organizing and examining adversary activity to support knowledge management and enable analytic efforts.

(U) The Cyber Technical Report entitled "NSA/CSS Technical Cyber Threat Framework v2" provides a baseline of standard definitions to be used as reference for U.S. Government Collaboration with partners and stakeholders in discussing adversary activities throughout the adversary lifecycle.

(U) Notably, in NTCTF v2, the shared technical lexicon has been reduced by 20% with clearer definitions and over 1700 key phrases to help guide the analyst in characterizing adversarial cyber activity using the NTCTF actions. This release has been reviewed to capture recent trends, account for emerging technologies and insider threat, and include operational technology (OT) concepts to support threats to critical infrastructure.

(U) DISCLAIMER OF WARRANTIES AND ENDORSEMENT

(U) The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

(U) CONTACT INFORMATION

Client Requirements and Inquiries or General Cybersecurity Inquiries

CYBERSECURITY REQUIREMENTS CENTER (CRC)

410-854-4200

Cybersecurity_Requests@nsa.gov

THIS PAGE INTENTIONALLY LEFT BLANK

NSA/CSS Technical Cyber Threat Framework (NTCTF v2)

Administration

Planning
- Analyze operation
- Determine strategy and goals
- Issue operational directive
- Produce operational plans
- Receive approval to execute operations
- Select intended victims

Resource Development
- Acquire operational infrastructure
- Build alliances and partnerships
- Create botnet
- Develop capabilities
- Obtain financing
- Seed supply chain
- Staff and train resources

Research
- Gather information
- Identify capability gaps
- Identify information gaps

Preparation

Reconnaissance
- Conduct social engineering
- Gather credentials
- Identify crosstalk
- Map accessible networks
- Scan devices
- Scrape websites
- Select potential victims
- Survey devices
- Use social media

Staging
- Add exploits to application data files
- Allocate operational infrastructure
- Create midpoints
- Establish physical proximity
- Infect or seed website
- Pre-position payload

Engagement

Delivery
- Access via wireless
- Alter communications path
- Compromise supply chain or trusted source
- Connect removable media
- Connect rogue network devices
- Infect via websites
- Inject database command
- Leverage device swapping
- Send malicious email
- Transport via common network infrastructure
- Traverse CDS or MLS
- Use chat services
- Use compromised host
- Use legitimate remote access
- Use physical network bridge

Exploitation
- Abuse protocols
- Access virtual memory
- Conduct social engineering
- Defeat encryption
- Exploit firmware vulnerability
- Exploit local application vulnerability
- Exploit OS vulnerability
- Exploit remote application vulnerability
- Exploit weak access controls
- Hijack
- Impersonate or spoof user
- Launch zero-day exploit
- Leverage exploit packs
- Leverage trusted relationship
- Replay

Presence

Execution
- Create scheduled task
- Execute via service controller
- Execute via third-party software
- Inject into running process
- Leverage authorized user
- Replace existing binary
- Run commands in shell
- Run fileless payload
- Use interpreted scripts
- Use OS APIs
- Use remote services
- Use trusted application to execute untrusted code
- Write to disk

Internal Reconnaissance
- Enumerate accounts and permissions
- Enumerate file system
- Enumerate local network connections
- Enumerate local network settings
- Enumerate OS and software
- Enumerate processes
- Enumerate windows
- Map accessible networks
- Scan connected devices
- Sniff network

Privilege Escalation
- Exploit application vulnerability
- Exploit firmware vulnerability
- Exploit OS vulnerability
- Inject into running process
- Use accessibility features
- Use legitimate credentials

Presence

Credential Access
- Add or modify credentials
- Conduct social engineering
- Crack passwords
- Dump credentials
- Hijack active credential
- Locate credentials
- Log keystrokes

Lateral Movement
- Exploit peer connections
- Logon remotely
- Pass the hash
- Pass the ticket
- Replicate through removable media
- Taint shared content
- Use application-deployment software
- Use remote services
- /rite to remote file shares
- Write to shared webroot

Persistence
- Create new service
- Create scheduled task
- Edit boot record
- Edit file-type associations
- Employ logon scripts
- Leverage path-order execution
- Modify BIOS
- Modify configuration to facilitate launch
- Modify existing services
- Modify links
- Modify service configuration
- Replace service binary
- Set to load at startup
- Use library-search hijack

Effect

Monitor
- Activate recording
- Collect passively
- Enable other operations
- Log keystrokes
- Maintain access
- Take screen capture

Exfiltrate
- Collect crosstalk
- Collect from local system
- Collect from network resources
- Compress data
- Disclose data or information
- Position data
- Run collection script
- Send over C2 channel
- Send over non-C2 channel
- Send over other network medium
- Throttle data
- Transfer via physical means
- Traverse CDS or MLS

Modify
- Alter data
- Alter process outcomes
- Cause physical effects
- Change machine-to-machine communications
- Change run-state of system processes
- Deface websites
- Defeat encryption

Deny
- Corrupt files or applications
- Degrade
- Disrupt or denial of service
- Encrypt data to render unusable

Destroy
- Brick disk or OS (full delete)
- Corrupt disk or OS (partial delete)
- Delete data
- Destroy hardware

Ongoing Processes

Analysis, Evaluation, and Feedback
- Abandon infrastructure
- Conduct effects assessments
- Refine potential victims

Command and Control
- Beacon to midpoints
- Establish peer network
- Relay communications
- Send commands
- Use botnet
- Use chained protocols
- Use peer connections
- Use remote shell
- Use removable media

Evasion
- Access raw disk
- Avoid data-size limits
- Block indicators on host
- Degrade security products
- Delay activity
- Employ anti-forensics measures
- Employ anti-reverse-engineering measures
- Employ rootkit
- Encode data
- Encrypt data
- Impersonate legitimate file
- Manipulate trusted process
- Mimic legitimate traffic
- Modify malware to avoid detection
- Obfuscate data
- Remove logged data
- Remove toolkit
- Sign malicious content
- Store files in unconventional location
- Tailor behavior to environment
- Use signed content

Legend
- Stage
- Objective
- Action

NTCTF V2 STAGE AND OBJECTIVE DEFINITIONS

ADMINISTRATION

Adversary activities that comprise "day-to-day" or standard operations that occur outside of targeted operations. This stage provides the necessary foundational resources and direction to drive targeted operations. During this stage, the adversary derives their operational intent, plans campaigns, performs research and analysis, and develops resources based on their strategy to generate targeted tasking based on their intent.

> PLANNING

Planning is an orderly, analytical process that consists of a logical set of activities to analyze a mission, select the best course of action, and produce operational plans (based on JP 5-0). The adversary plans their operations, typically derived from high level or national strategy. Based upon the resulting plans, the adversary identifies mission needs and requirements.

> RESOURCE DEVELOPMENT

Resource development activities aid with fulfilling the mission needs. Resource types include: infrastructure, software, data, people, and support to conduct operations. Resource development actions include the processes an adversary employs to develop, modify, test, and distribute the resources to support operations, such as capabilities and infrastructure. Resource development also includes activities such as the training and education of people, or cultivating of alliances and partnerships.

> RESEARCH

Research activities are adversary activities performed to identify gaps and ideate ways to fill those gaps, through technical, mechanical, physical, financial, or other means. This set of activities also aims to identify resources to be developed in order to meet the demands of strategic and operational plans.

PREPARATION

Adversary activities to conduct research on target networks and/or entities of interest and set up infrastructure and capabilities to be used during targeted operations. Actions taken by a threat actor to assess the intended victim cyber threat environment and assess success/failure of threat activities in meeting objectives.

> RECONNAISSANCE

Reconnaissance is the act of obtaining and examining information about the activities and resources of a potential target, or capturing data and characteristics of a particular target system or network (derived from JP 1-02, Reference e). An adversary conducts reconnaissance to strategize their targeted operation with the goal of making the intrusion more efficient and to increase the probability of success. Typically reconnaissance is performed via passive or active means using cyber and non-cyber methods.

Passive reconnaissance involves no interaction with the target directly. It includes cyber activities such as open source research to gather publicly available information and drawing on information previously collected as well as non-cyber activities such as dumpster diving, and physical observation.

Active reconnaissance involves attempts to interact with the target directly. Activities include port, network and vulnerability scanning, and network enumeration techniques, such as banner grabbing and TCP fingerprinting. The desired result is a profile and enumeration of target access points, protocols, and vulnerabilities to exploit.

> STAGING

The goal of staging is to position capabilities and infrastructure required to support the operation (derived from JP 3-35, Reference f). This objective includes allocating and preparing supporting infrastructure, such as command and control nodes, hop points, DNS infrastructure, and necessary accounts (email, chat, etc.). During these activities, the adversary ensures tools, infrastructure and communication channels are identified and deliverable. This objective also includes coupling malware with a delivery mechanism.

Pre-positioning of threat actor capabilities to threat actor internally owned/controlled storage locations, whether electronic media or physical hardware (i.e., removable media, bundled hardware/firmware/software corrupted through a cooperative supply chain), to support intended/subsequent cyber threat actions/activities.

NTCTF V2 STAGE AND OBJECTIVE DEFINITIONS

ENGAGEMENT

Adversary activities taken by a threat actor against a specific target/target set prior to gaining, but with the intent to gain, access to the victim's physical or virtual computer or information system(s), network(s), and/or data stores.

> DELIVERY

Deliver a malicious payload to the target via technical, cognitive, or physical means with the goal of exploiting target vulnerabilities in technology, people, or processes. The malicious payload can be as simple as an idea verbally communicated to the target to acquire information or as complex as custom coded malware, and can be delivered to a target in multiple ways. The most commonly used remote methods include spear phishing, malicious websites and via remote exploits, but can also be delivered through social engineering or insider threats.

> EXPLOITATION

Use network, system, physical and/or social vulnerabilities to establish unauthorized access to a target. Adversary activities to leverage vulnerabilities in people, processes, or technology. Exploitation of people typically is achieved using social engineering techniques. Social engineering is defined as the use of influence and persuasion to deceive people for the purpose of obtaining information or persuading the person to perform an action. Social engineering techniques are often employed when constructing messages used in spear-phishing email/text message, social networking sites, and active reconnaissance communication.

> CREDENTIAL ACCESS

Adversarial activities to obtain, create, hijack, and leverage legitimate credentials within a target system or network. These activities include credential dumping, network sniffing with the intent of gaining credentials, keylogging on a target system, leveraging legitimate password recovery techniques, hijacking active authentication tokens, or merely searching file systems for credentials in files.

PRESENCE

Actions taken by the threat actor once access to target/target set physical or virtual computer or information system has been achieved. Adversary activities to ensure ongoing and robust access to the victim and potentially its connected environment

> EXECUTION

Unauthorized threat actor actions (automated or manual) that direct or execute actions or activities using available target's computer(s), information system(s), and/or network(s). Actions taken by an adversary to run malicious or controlled code on a local or remote system.

> INTERNAL RECONNAISSANCE

Activities an adversary performs on the victim network that support traversing the network and compromising additional hosts or connected networks. Activities include internal network scanning, directory walks, active directory dumps, password dumps, and identification of target systems and users.

> PRIVILEGE ESCALATION

Activities an adversary performs on the victim network to support obtaining administrative rights. Adversary uses information from external and/or internal reconnaissance, social engineering, or other means to attempt to obtain administrative rights by using a variety of tools and tactics. Some examples include using password hash exploitation tools, leveraging legitimate account credentials, and using open source or custom exploits.

NTCTF V2 STAGE AND OBJECTIVE DEFINITIONS

PRESENCE

> LATERAL MOVEMENT

Adversarial activities to propagate through the victim environment. An adversary may use information from internal reconnaissance to identify and compromise additional networks, hosts, and connected networks. Within this objective, the adversary may attempt establishing new user credentials to further propagate on the network. These activities that an adversary performs on the victim network support traversing the network to achieve objectives.

> PERSISTENCE

Activities performed to maintain presence on the system, device, and/or network. Activities include creating legitimate credentials, installing rootkits, establishing remote access tools, etc. It is important to note that once initial access is gained to a target, persistence may be established at any time and may consist of multiple techniques

EFFECT

> MODIFY

Activities to modify target systems, networks, resources, or information. These modifications could be changing configuration files, removing data files, sending unauthorized email from a target account, or installing additional malicious files.

> DENY

Activities that result in the denial of target systems, networks, or other resources, as well as denying access to information. These activities may be the result of Denial of Service attacks, or by virtue of modifying or destroying components of the target.

> DESTROY

Activities to destroy target systems, networks, resources, or information. Attacks cause a wide range of consequences ranging from minor to significant damage to the target.

EFFECT

Adversary activities involved in the manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or resident information. Outcomes of threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores.

> MONITOR

Activities such as maintaining presence on a host, establishing a compromised host as a listening post, identifying health and status of the host, and waiting to perform additional operations.

ANALYSIS, EVALUATION, AND FEEDBACK

Activities to continually analyze, evaluate, and update the operation to best perform their mission at any point in the target operation activities. This activity is a similar concept to the Observe Orient Decide Act (OODA) loop for the adversary.

COMMAND AND CONTROL

Activities to direct and receive information from a victim. Activities include the transmission of location, health, or operational status of persistent access capabilities and the remote tasking of access capabilities.

NTCTF V2 STAGE AND OBJECTIVE DEFINITIONS

> EXFILTRATE

Activities to collect and transmit information from a target that enables operations, fulfills tasking requirements or meets mission objectives. Observable activities include gathering files, internally staging those files, obfuscating file types and formats, compressing into archive files, and transmitting files. Transmission could occur through standard protocols, remote access tools, or a variety of other methods such as email, chat, cloud services, and more. The method used will vary based on the adversary, their collection requirements and urgency.

EVASION

Activities to minimize the risk of being caught within a victim host and their environment. An adversary is likely to employ forms of evasion across the various stages of their standard and targeted operations. Evasion techniques can vary, based on the stage, particular Tactics, Techniques, and Procedures (TTP), and sophistication of the adversary. Some examples include saving malware with legitimate file types, using encryption or covert channels for communications, or performing command and control using social networking sites.

NTCTF V2 ACTION DEFINITIONS AND KEY PHRASES

ADMINISTER

> PLANNING

Analyze operation

Steps taken by a threat actor (individual, team or government-sponsored agency), their sponsor, or leadership to establish the overall strategy for, policy limitations of, and the requisite resources and capabilities needed to conduct the intended malicious cyber activity, along with the criteria for evaluating the eventual success or failure of the activity.

Issue operational directive

Steps taken by an individual cyber threat actor, their sponsor, or leadership to decide to execute a planned cyber threat operation.

Receive approval to execute operations

Threat actors receive approval from their leadership to execute operations against identified targets.

Determine strategy and goals

Steps taken by a threat actor, their sponsor, or leadership to determine the portion(s) of national strategy and/or interests that will be supported by the intended cyber activity, or to justify that activity. This includes threat actor perception of programmatic or operational goals, environmental changes, or outcomes that contribute to the overall success of the threat activity.

Produce operational plans

Steps taken to integrate known information on the target, capabilities, and intended outcome into a plan for how to most effectively conduct intended cyber activity.

Select intended victims

The initial step in the planning process that produces a list of intended victim(s), and defines the intent for and desired outcome of the malicious cyber activity.

> RESEARCH

Gather information

Threat actor actions taken to compile and analyze all available information on potential targets.

Identify capability gaps

Threat actor actions to establish requirements for tools, including malware, needed to develop capabilities and/or conduct operations.

Identify information gaps

Threat actor actions to determine the utility of available information related to a potential target and to document intelligence gaps.

NTCTF V2 ACTION DEFINITIONS

> RESOURCE DEVELOPMENT

Acquire operational infrastructure

Steps taken to acquire the facilities and infrastructure required to conduct the intended cyber activity during targeted operations.

Develop capabilities

Steps taken to define, develop, acquire, and test the technology, processes, and tools required to conduct the intended cyber activity.

Seed supply chain

Threat actor action to place compromised software, hardware and/or firmware on partner or organic supply chain.

Build alliances and partnerships

Steps taken to establish relationships with individuals, groups or governments; to acquire or provide co-production and/or contract development of technology, processes and/or tools for use in the intended cyber activity; and to provide support to compromise victim supply chains.

Obtain financing

Steps taken to identify and employ viable sources of financial support required to support staff, infrastructure, and other expenses that occur while conducting cyber activities.

Staff and train resources

Steps taken to select and train the people required to conduct intended activity in areas such as cyber activities, targeting, and data analysis.

Create botnet

Actions taken to establish a virtual network of target computer or information system resources for use in conducting threat actor activities.

PREPARATION

> RECONNAISSANCE

Conduct social engineering

Psychological manipulation of people by threat actor into performing actions or divulging information.

Map accessible networks

The sending of transmissions to the network's possible nodes, examining the responses they receive identify the existence of nodes on the network. The results potentially provide insight to identify security systems and policies on the network.

Select potential victims

Actions taken by a threat actor to identify a specific target or targets from a broader list of potential targets.

Gather credentials

Activities to obtain credentials of unknowing users for the purpose of future engagement.

Scan devices

Active or passive actions taken by the adversary in order to determine the software or firmware currently used by a target, versions of software or firmware, a target's patch status, and configuration (e.g., ports open).

Survey devices

Threat actor actions to collect intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to an identified target.

NTCTF V2 ACTION DEFINITIONS

> RECONNAISSANCE

Identify crosstalk

Any phenomenon by which a signal transmitted on one circuit or channel creates an unintended effect on another circuit or channel that is not physically connected.

Scrape websites

The gathering of information about a potential target by searching open source information such as public forums, conference announcements, bulletin boards, or distribution lists looking for victim information; includes the use of automated tools to overcome protection measures.

Use social media

The gathering of information about a potential target by searching public social media sites.

> STAGING

Add exploits to application data files

Altering the content of data files to exploit a weakness in the application that parses that type of data file. The change causes that application to perform unintended actions, usually code execution or revealing sensitive information.

Create midpoints

Configure, acquire, compromise, or develop one or more intermediate nodes between source and destination for data exfiltration and command and control.

Infect or seed website

A website that has been created or modified by a threat actor to include malicious code, which can subsequently be used in phishing attacks, drive-by attacks and watering hole attacks.

Allocate operational infrastructure

Threat actor actions taken to put in place facilities and associated infrastructure needed to support development of capabilities for and to support conduct of threat activities.

Establish physical proximity

Threat actor actions taken to obtain facilities and infrastructure in close physical proximity to identified target's computer or information systems, networks, and/or data stores.

Pre-position payload

Pre-positioning of threat actor capabilities on threat actor internally owned/controlled storage locations.

ENGAGEMENT

> DELIVERY

Access via wireless

Wireless access to network communications or a device connected to the network.

Infect via websites

Adversaries embed malicious code into a website that a user visits that infects the computer that connects to it.

Traverse CDS or MLS

Usage of cross domain solutions (CDS) or multi-level solutions (MLS) to maliciously transfer content, or allow adversarial movement from one network to another, whether in a manual or automated manner (through trusted services).

NTCTF V2 ACTION DEFINITIONS

> DELIVERY

Alter communications path

Modify communications paths by altering cache entries or routing tables using a variety of protocols to deliver a payload or redirect victims to fraudulent and malicious web sites and systems.

Compromise supply chain or trusted source

Adding malicious software, hardware, or configurations to items that are trusted to be non-malicious while on their way to the target network.

Connect removable media

The deployment of malicious code via removable media. Removable media can be programmed to auto-run upon insertion of a device, causing malware to be automatically executed.

Connect rogue network devices

The insertion or use of existing rogue interfaces to authorized network devices.

Inject database command

The injection of malicious SQL commands into unchecked input fields, allowing data theft, modifications, or execution of malicious commands.

Leverage device swapping

Any instance in which an information system, either unaccredited or accredited for a specific network, is moved from said network to a secondary network without authorization. Whether the device swapping is accidental or purposeful, it is a cross domain violation.

Send malicious email

Embeds malicious attachments or links within an email message, sent to a target. The user's computer can be 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.

Transport via common network infrastructure

Deliver malicious content via previous adversary-compromised network infrastructure that connects to or transports the target network.

Use chat services

Employ a chat communications protocol allowing the interchange of messages and/or files between devices (mobile, computers, IoT) to communicate with a target.

Use compromised host

The process of delivering malicious code from a previously compromised victim host to a target within the victim's network to be used to gain further access.

Use legitimate remote access

The use of legitimate remote access capabilities without exploiting a vulnerability usually involving the reuse of legitimate credentials that were captured previously to gain access to internal network resources.

Use physical network bridge

Networking hardware that creates an aggregate network from either two or more communication networks, or two or more network segments. Bridging (OSI layer 2) is distinct from routing (OSI layer 3), which allows multiple different networks to communicate independently while remaining separate.

NTCTF V2 ACTION DEFINITIONS

ENGAGEMENT

> EXPLOITATION

Abuse protocols

Threat actor use of standard target system or network protocols to gain unauthorized access through unanticipated use of the protocol.

Access virtual memory

Abusing physical collocation of separate/isolated virtual spaces (e.g., virtual machines, containers, processes) to compromise the integrity or confidentiality of targeted virtual resources.

Conduct social engineering

Psychological manipulation of people by threat actor into performing actions or divulging information.

Defeat encryption

Exploitation of cryptographic algorithms or device implementations of cryptography, or using acquired cryptographic keys to gain access to or manipulate the underlying unencrypted content.

Exploit firmware vulnerability

Exploiting a software vulnerability in firmware to lead to access to a device. This occurs when a programming or logical error is triggered that causes the software to behave in an unintended and insecure way.

Exploit local application vulnerability

Exploiting a software vulnerability in an application by having the exploit triggered locally on the host, often requiring some user interaction to launch and usually leading to user level access on the host. This occurs when a programming or logical error is triggered that causes the software to behave in an unintended and insecure way.

Exploit OS vulnerability

Exploiting a software vulnerability in a default operating system service or kernel. This occurs when a programming or logical error is triggered that causes the OS to behave in an unintended and insecure way. Exploiting OS vulnerabilities often leads directly to privileged access on the host.

Exploit remote application vulnerability

Exploiting a software vulnerability in an application by having the exploit triggered remotely over the network, often without any user interaction and usually leading to user level access on the host. This occurs when a programming error is triggered that causes the software to behave in an unintended and insecure way.

Exploit weak access controls

Exploitation of weak, misconfigured, or missing access controls to gain access to a system or data.

Hijack

Hijacking is a type of network security attack in which the threat actor takes control of a communication between two entities.

Impersonate or spoof user

Adversary poses as an authorized user in order to gain access to target computer system.

Launch zero-day exploit

A zero-day (0-day) exploit is a vulnerability in software that is not publicly disclosed or is unknown to the vendor, which is then exploited by the threat actor before the vendor becomes aware and/or fixes it.

Leverage exploit packs

Threat actor makes use of exploit packs (also called an exploit kit), a toolkit that automates the exploitation of client side vulnerabilities, usually targeting browsers and programs that a website can invoke through the browser.

Leverage trusted relationship

Leverage compromise of a connected peer network or other trusted relationship with another network.

Replay

Threat actors conduct a network attack against a target in which a valid data transmission is maliciously or fraudulently repeated or delayed.

NTCTF V2 ACTION DEFINITIONS

PRESENCE

> INSTALLATION & EXECUTION

Create scheduled task

Task scheduling is used to execute programs on a scheduled basis to persist adversary code or gain SYSTEM privileges. Task scheduling requires administrator privileges, but tasks may be configured to run with SYSTEM privileges, representing an escalation of privilege

Execute via service controller

Execute a binary via the service controller or other methods of interacting with services.

Execute via third-party software

Adversary uses pre-existing third-party applications to execute code within the targeted environment.

Inject into running process

Injecting malicious code into an existing legitimate process. Running code in the context of another process provides many benefits such as access to the process's memory, permissions, and identity. Code injection masks the malicious activity from casual inspection of the task list.

Leverage authorized user

Actions initiated by an authorized user that enable the installation and execution of code.

Replace existing binary

Threat actor actions taken to replace a legitimate or pre-existing binary with a malicious executable in a commonly trusted location, from a legitimate source, or named with a common name to bypass tools that trust executables by relying on file name or path.

Run commands in shell

Invoke individual commands from the command line to run executable code. This can be done locally or remotely - and interactively. Commands that are executed run with current permission level of the command line.

Run commands in shell

Invoke individual commands from the command line to run executable code. This can be done locally or remotely - and interactively. Commands that are executed run with current permission level of the command line.

Run fileless payload

Run fileless payload only in memory without an executable file or script on disk.

Use interpreted scripts

Utilizing a scripting language, adversaries use scripts to execute code in a number of different ways, either with script files or script commands fed directly to the script interpreter.

Use OS APIs

Adversary tools directly use an operating system (OS) application programming interface (API) to execute binaries.

Use remote services

Use remote administrative services to perform execution remotely, or other running services that have implied trust or authentication that can be leveraged by the adversary to maneuver through the network. With valid credentials and the ability to remotely access the features, remote services can be used to read or modify system configuration and data and/or cause code to execute.

Use trusted application to execute untrusted code

Adversary indirectly executes code through a trusted application and avoids triggering security tools.

Write to disk

Store binary data on a disk or network share to be used in further operations.

NTCTF V2 ACTION DEFINITIONS

PRESENCE

> INTERNAL RECONNAISSANCE

Enumerate accounts and permissions

Adversaries attempt to get a listing of all local or domain accounts and their permissions, including reviewing logins or file modification times to identify primary users. Adversaries get a listing of all local groups and their permissions and members.

Enumerate file system

Adversaries enumerate all files and directories in certain areas of a host or remote share or perform a targeted search for specific files or directories; also known as a directory walk.

Enumerate local network connections

Adversaries attempt to get a listing of all network connections.

Enumerate local network settings

Adversaries acquire information about local networks, typically using several utilities that describe local network settings.

Enumerate OS and software

An adversary attempts to get detailed information about the OS including version, patches, hotfixes, service packs, and architecture. Adversaries attempt to get a listing of software or drivers that are installed on the system and their configurations.

Enumerate processes

Adversaries attempt to get information about running processes. This could also include enumerating loaded libraries that are part of the running processes, or registered services.

Enumerate windows

Adversaries attempt to get a listing of all application windows, including invisible windows.

Map accessible networks

The sending of transmissions to the network's possible nodes, examining the responses they receive identify the existence of nodes on the network. The results potentially provide insight to identify security systems and policies on the network.

Scan connected devices

Active or passive actions taken by the adversary in order to determine the software or firmware currently used by a target, versions of software or firmware, a target's patch status, and configuration.

Sniff network

Network sniffing is when the network is monitored to capture credentials. An adversary may place a network interface into promiscuous mode, using a utility to capture traffic in transit over the network or use span ports to capture a larger amount of data.

> PRIVILEGE ESCALATION

Exploit application vulnerability

Exploiting a software vulnerability in an application by having the exploit triggered, often requiring some user interaction to launch that leads to user level access on the host. This occurs when a programming error causes the software to behave in an unintended and insecure way.

Exploit firmware vulnerability

Exploiting a software vulnerability in firmware to lead to access to a device. This occurs when a programming or logical error is triggered that causes the software to behave in an unintended and insecure way.

Exploit OS vulnerability

Exploiting a software vulnerability in an operating system service or kernel. This occurs when a programming error is triggered that causes the software to behave in an unintended and insecure way. Exploiting OS vulnerabilities often leads directly to privileged access on the host.

Inject into running process

Injecting malicious code into an existing legitimate process.

Use accessibility features

An adversary can modify accessibility features that may be launched with a key combination before a user has logged in. An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Use legitimate credentials

Using compromised credentials to leverage legitimate access controls placed on various resources on hosts and within the network to grant an adversary increased privilege to specific systems or access to restricted areas of the network.

NTCTF V2 ACTION DEFINITIONS

PRESENCE

> CREDENTIAL ACCESS

Add or modify credentials

Account creation and manipulation may aid adversaries in maintaining access to credentials and certain permission levels within an environment; an adversary must already have sufficient permissions on the domain or systems. This action includes creating credentials, modifying permissions, adding or changing permission groups, or modifying account settings.

Dump credentials

Credential dumping is obtaining information from weaknesses in operating system or software that can be used to login to the operating system. Utilities do this in many different ways: extracting credential hashes for off-line cracking, extracting plaintext passwords, or finding Kerberos tickets.

Locate credentials

Adversaries search for local file systems, remote file shares, network traffic, and other systems on the network for files or activity containing passwords.

Log keystrokes

Use of software/hardware that records keystrokes and keyboard events.

Conduct social engineering

Psychological manipulation of people by threat actor into performing actions or divulging information.

Hijack active credential

The malicious use of authentication tokens either activated by a legitimate user or while in use without the user's knowledge.

Crack passwords

Adversaries may use password cracking techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained.

> LATERAL MOVEMENT

Exploit peer connections

Exploit connected, peer-to-peer, or mesh network to maneuver and expand presence within a network. The network may be within a single organization or across organizations with trust relationships and authentication agreements.

Replicate through removable media

Adversaries may move between hosts, possibly those on disconnected or air-gapped networks, by copying to removable media and taking advantage of autorun features, by 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.

Use remote services

Use remote administrative services to perform execution remotely, or other running services that have implied trust or authentication that can be leveraged by the adversary to maneuver through the network. With valid credentials and the ability to remotely access the features, they can be used to read or modify data and/or cause code to execute.

Logon remotely

An adversary may use valid credentials to login to a remote host for manual interaction, through a graphical user interface (GUI) or command line interface that is sent back to the initiator of the remote connection. They may then perform action as the logged on user.

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 valid content. Once a user opens the shared content, the tainted content is executed. Adversaries may taint shared content to move laterally.

Write to remote file shares

Writing data to remote hosts via file shares or file hosting to cause a change that results in code execution either directly by overwriting files or configuration data or indirectly by preplacing code that is executed via another mechanism.

NTCTF V2 ACTION DEFINITIONS

Pass the hash

Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. Threat actors use valid, captured password hashes for the account to authenticate as the user.

Use application-deployment software

Adversaries may deploy new software to systems using application deployment systems already employed by site administrators. The permissions required for this action varies by system; local credentials may be sufficient with direct access to the deployment server. However the system may require an administrative user account to log in, or to perform software deployment.

Write to shared webroot

Adversaries may add malicious content to a website through the open file share and then browse to that content with a web browser to cause the server to execute the content. The malicious content will typically run under the context and permissions of the web server process, often resulting in local system or administrative privileges depending on how the web server is configured.

Pass the ticket

Pass the ticket (PtT) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the Kerberos ticket. Threat actors use valid Kerberos tickets for the account that are either captured using a Credential Access technique or generated by the attacker who has the right level of access to generate forged tickets through the golden ticket attack. Kerberos tickets are used with PtH to authenticate as a user. Once authenticated, PtT may be used to logon to remote or local systems.

> PERSISTENCE

Create new service

Create a new service started by the operating system by directly modifying the registry (or similar construct) or by using tools which do so.

Leverage path-order execution

Path interception occurs when an executable is placed in a specially crafted path so that it is executed instead of the intended target.

Modify service configuration

Alter subsequent load processes for service related executables and libraries by modifying the service's configuration information; not configuration of the service manager itself, but services run by it.

Create scheduled task

Task scheduling is used to execute programs on a periodic basis to persist adversary capabilities or gain elevated privileges.

Modify BIOS

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.

Replace service binary

If the file system location of a service executable is modifiable by the user, it may be replaced by another executable. An adversary may use this capability to gain elevated privileges by putting their own executable in place of the service executable.

Edit boot record

The master boot record (MBR) is the section of disk that is first loaded after completing hardware initialization by the BIOS and is the location of the boot loader. If an adversary has raw access to the boot drive, they may modify or overwrite this area diverting execution during startup from the normal bootloader to adversary code. This could also be achieved by modifying the virtual boot record (VBR) or partition table.

Modify configuration to facilitate launch

An adversary causes a file to execute based on a configuration change.

Set to load at startup

An adversary causes the system to automatically load and execute code after the operating system has started.

NTCTF V2 ACTION DEFINITIONS

Edit file-type associations

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. Applications can modify the file handler for a given file extension to call an arbitrary program when a file with the given extension is opened.

Modify existing services

Modify an existing service to run adversary software by using tools that modify the registry or by directly modifying the registry. Modifying existing services may break existing services or may enable services that are disabled/not commonly used.

Use library-search hijack

Adversaries take advantage of the library search order and programs that ambiguously specify libraries to gain privilege escalation.

Employ logon scripts

Logon scripts are run whenever a specific user or users logon to a system. If adversaries can access these scripts, they can insert additional code that allows them to maintain persistence or move laterally within an enclave because it is executed every time the affected user or users 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.

Modify 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.

EFFECT

> MONITOR

Activate recording

Threat actor actions to capture/record audio/video activity within the target's work space.

Enable other operations

Measurable cyber threat activities that indicate, identify and/or establish a foundation for subsequent actions against a target's data, computer(s) and/or information systems.

Maintain access

Process of checking or maintaining accesses into or on targeted networks and hosts. Access can be tracked through the use of automated beacons, or interactive means to provide situational awareness.

Collect passively

Threat actor actions taken to collect information on the target using methods which require no active effort on behalf of the actor and for which the target has limited awareness.

Log keystrokes

Use of software/hardware that records keystrokes and keyboard events.

Take screen capture

Threat actor actions taken to capture target screen shots during target operations.

> EXFILTRATE

Collect crosstalk

Use of any phenomenon by which a signal transmitted on one circuit or channel creates an unintended effect on another circuit or channel that is not physically connected to gather information.

Position data

Data, gathered from one or more sources, is placed in a specified location for exfiltration at a later time. This technique may be used to aggregate files in preparation for exfiltration.

Send over other network medium

Exfiltration occurs over a completely 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, cellular data connection, or Bluetooth. Adversaries may broadcast and connect to their own wireless network specifically for data exfiltration.

NTCTF V2 ACTION DEFINITIONS

Collect from local system

Data is collected from local sources on a host that is accessible from the current system.

Collect from network resources

Data is collected from a network resource that is accessible from the current system.

Compress data

Data is compressed prior to exfiltration to minimize the amount of data sent over the network or to make the contents of the data less obvious. This compression is done separately from the exfiltration channel. The compression may be performed using a custom program or algorithm, or a more common compression library or program.

Disclose data or information

Release data/information to let unauthorized people read data/information to which they are not authorized access to deny integrity.

Run collection script

Data is identified and/or gathered through the use of automated processing or scripting. This may include automated searching of files matching criteria or entire directory structures.

Send over C2 channel

Data exfiltration is performed over the adversary command and control channel. Data is transferred through the channel using the same protocol as command and control communications.

Send 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 not routed through the existing adversary command and control channel. An alternate data connection would be made to transfer the data.

Throttle data

Data is arranged into defined chunks instead of whole files, or packet sizes are limited. This approach may be used to avoid operational limitations dealing with logical or physical transfer constraints related to transmission protocols.

Transfer via physical means

Exfiltration occurs via a physical medium. This medium can be an entire device being lost, stolen, or removed; a component part, or even a non-digital medium such as printed papers. The physical media may be used as the final exfiltration point or as a hop between disconnected devices.

Traverse CDS or MLS

Usage of CDS or MLS to maliciously transfer content, or allow adversarial movement from one network to another. This technique focuses on zero-day unknown or design vulnerabilities in the trusted device or its component parts or software that a system administrator cannot be expected to prevent.

> MODIFY

Alter data

The modification of data within information systems. Data that is modified is not deleted, but changed to influence decisions or cause confusion.

Alter process outcomes

Actions taken to alter process outcomes of target's internal target computer(s), network(s), and/or information system(s).

Cause physical effects

Change machine-to-machine communications

Actions taken to alter communications between processes operating on separate target computer(s), network(s) and/or information system(s).

Change run-state of system processes

Actions taken to alter the state (e.g. running, suspended, stopped) of processes operating on the target's computer(s), network(s), and/or information system(s), to achieve desired outcomes.

Deface websites

Actions to change the visual appearance of a website or webpage.

Defeat encryption

Exploitation of weak or misconfigured cryptographic algorithms, modifications of configurations, or using acquired cryptographic keys to gain access to or manipulate the underlying unencrypted content.

Causing a physical effect to occur, such as a piece of equipment malfunctioning or turning off power.

NTCTF V2 ACTION DEFINITIONS

> DENY

Corrupt files or applications

Modification of data by an adversary to render the files or applications unusable.

Encrypt data to render unusable

The encrypting of data by an adversary to render the data unusable.

Degrade

Actions taken to decrease capabilities to some degree and/or for a period of time the target's computer, information system, or network.

Disrupt or denial of service

Normal system activities directed at the victim's environment in a magnitude that overwhelms the normal operation of the victim's computer(s), network(s), and/or information system(s), thus severely limiting or precluding normal access. This includes the use of multiple systems to cause a Distributed Denial of Service (DDOS).

> DESTROY

Brick disk or OS (full delete)

Deletion of critical components of an operating system rendering it unusable by the target/victim.

Corrupt disk or OS (partial delete)

Deletion of some components of an operating system rendering it unusable by the target/victim. The system may have some recoverable information.

Delete data

Deletion of data from a hard drive, or computer system, without damaging the operating system or hardware.

Destroy hardware

Permanently, completely and irreparably damage a target's physical computer or information system(s), network(s), and/or data stores.

ANALYSIS, EVALUATION, AND FEEDBACK

Abandon infrastructure

Actions taken to cease use of infrastructure previously allocated for targeted operations.

Conduct effects assessments

Recurring actions taken to assess the success of cyber threat activities/operations in meeting intended objectives. Assessments may occur multiple times during ongoing activities/operations and serves as the starting point for validating/resetting objectives and courses of actions.

Refine potential victims

Actions taken (electronically or physically) to ensure presence and validity of intended target data/information, and/or identify additional potential targets (data, computers, and/or information systems), and that intended tools/processes will achieve intended outcome/result.

NTCTF V2 ACTION DEFINITIONS

C2

Beacon to midpoints

Transmission of location, health, or other operational status of persistent access capabilities to a designated location and/or threat actor.

Establish peer network

Establish a proxied, peer-to-peer or mesh network to manage C2 communications. The network may be within a single organization or across organizations with trust relationships.

Use peer connections

Use a proxied, peer-to-peer or mesh network to manage C2 communications to reduce the number of simultaneous outbound network connections and to provide resiliency upon connection loss.

Send commands

Adversary actions to issue commands to installed malware or implants on compromised hosts.

Use botnet

Send command and control communications to or via a previously created botnet.

Use remote shell

A threat actor uses an application, script, or shell to create unauthorized access.

Relay communications

Adversary actions to transmit malicious data/code through networks from host to host, or manipulating routing infrastructure.

Use chained protocols

Use of various protocols in concert to communicate with a system under their control in a target network to enable the C2 to eventually get to the C2 server over multiple hops. This is often used when certain protocols are allowed inside the network for some connections and then other protocols are allowed from certain compromised devices to leave the network.

Use removable media

Use removable media to spread commands from computer to computer, including on potentially disconnected networks.

EVASION

Access raw disk

Programs with direct drive access may read and write files directly from the drive by analyzing file system data structures. This enables covert storage and avoids operating system visibility.

Employ rootkit

Rootkits are programs that hide the existence of malware by intercepting and modifying OS API calls that supply system information. Rootkit functionality may reside at the user level, kernel level in the OS, or lower, to include a hypervisor, MBR, or the BIOS. Adversaries use rootkits to hide the presence of programs, files, connections, services, and/or drivers.

Obfuscate data

Make data more difficult to analyze by selectively replacing or otherwise concealing its contents; includes executables and network traffic.

Avoid data-size limits

Data being exfiltrated is sent in defined chunks instead of whole files or packet sizes are limited. This approach may be used to avoid triggering network threshold alerts.

Encode data

The process of converting data into another format.

Remove logged data

The deletion or modification of generated log/event files on a host system. This may compromise the integrity of the security solution causing security events to go unreported or impeding incident response.

NTCTF V2 ACTION DEFINITIONS

Block indicators on host

Blocking indicators of host activity from leaving the host machine. In the case of network based reporting of indicators, an adversary may block traffic associated with reporting to prevent central station analysis. This may be accomplished by many means such as stopping a local process to creating a host-based firewall rule to block traffic to a specific server.

Degrade security products

Disable, disrupt, or otherwise evade security tools to avoid detection. This can take the form of killing processes, deleting registry keys so that tools do not start at run time, or other methods to prevent the intended operation.

Delay activity

The use of sleep timers, user interaction, computationally intensive algorithms, and other means to delay malicious behavior execution in order to evade detection by timed behavioral detection technologies.

Employ anti-forensics measures

Threat actor actions to destroy or obfuscate data artifacts (beyond logs and files) that would indicate their presence on target computer(s), information system(s), and/or network(s), and thereby render target-initiated forensic analysis difficult or impossible.

Employ anti-reverse-engineering measures

Use a variety of activities to evade reverse engineering efforts.

Encrypt data

Data is encrypted to hide the target information, increasing inspection difficulty. This action is performed on the data at rest or in transit. Adversaries encrypt data to protect or conceal the specific activities.

Impersonate legitimate file

Placing a file in a commonly trusted location (such as C:\Windows\System32) or naming a file with a common name (such as "explorer.exe" or "svchost.exe") to leverage tools that trust executables by relying on file name or path. This also may be done to deceive defenders and system administrators into thinking a file is benign by name association to something that is known to be legitimate.

Manipulate trusted process

Malicious software may inject into a trusted process to gain elevated privileges without prompting a user.

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 an enclave. C2 commands and results are embedded within the traffic between the client and server.

Modify malware to avoid detection

If malware is detected and quarantined, an adversary may be able to determine why the malware was detected, modify the malware, and send an updated version that is no longer detected by security tools.

Remove toolkit

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. There are tools available from the host operation system to perform cleanup, but adversaries may choose to use other tools as well.

Sign malicious content

Signing malicious code using stolen, self-generated, or compromised private keys, since signed content is either required by the operating system or often trusted by default.

Store files in unconventional location

Data or executables may be stored in file system metadata, slack space, registry, outside logical partition, or some other unconventional location instead of directly in files to evade file monitoring tools. These actions leverage standard disk read/write operations (different from raw access).

Tailor behavior to environment

Detecting the environment where code or scripts are executed and adjusting execution behaviors to avoid detection.

Use signed content

The use of signed content or code for malicious purposes, including computed hash collisions, legitimate signed software for malicious purposes, since signed content is either required or trusted by default.

Appendix A. Key Phrases by NTCTF Action

(U) This table contains a mapping of commonly used phrases to NTCTF Actions.

Stage	Objective	Action	Key Phrases
Administration	Planning	Analyze operation	success criteria
Administration	Planning	Analyze operation	information needs
Administration	Planning	Analyze operation	mission needs
Administration	Planning	Analyze operation	policy
Administration	Planning	Analyze operation	measures of performance
Administration	Planning	Analyze operation	leadership
Administration	Planning	Determine strategy and goals	intentions
Administration	Planning	Determine strategy and goals	strategy
Administration	Planning	Determine strategy and goals	goals
Administration	Planning	Determine strategy and goals	interests
Administration	Planning	Determine strategy and goals	communications between organizational leaders
Administration	Planning	Determine strategy and goals	perception
Administration	Planning	Determine strategy and goals	environmental changes
Administration	Planning	Determine strategy and goals	desired outcomes
Administration	Planning	Determine strategy and goals	operational goals
Administration	Planning	Determine strategy and goals	evaluation
Administration	Planning	Issue operational directive	send tasking
Administration	Planning	Issue operational directive	commands
Administration	Planning	Issue operational directive	execute operation
Administration	Planning	Issue operational directive	leadership decision
Administration	Planning	Produce operational plans	schedule of operations
Administration	Planning	Produce operational plans	planning
Administration	Planning	Produce operational plans	documents
Administration	Planning	Produce operational plans	expected outcomes
Administration	Planning	Receive approval to execute operations	leadership approval
Administration	Planning	Receive approval to execute operations	approval
Administration	Planning	Receive approval to execute operations	authorization
Administration	Planning	Receive approval to execute operations	orders
Administration	Planning	Select intended victims	victim group
Administration	Planning	Select intended victims	victim organization
Administration	Planning	Select intended victims	strategic target list
Administration	Planning	Select intended victims	intent for operation
Administration	Resource Development	Acquire operational infrastructure	cloud hosting
Administration	Resource Development	Acquire operational infrastructure	facilities
Administration	Resource Development	Acquire operational infrastructure	purchase infrastructure
Administration	Resource Development	Acquire operational infrastructure	virtual private server
Administration	Resource Development	Acquire operational infrastructure	register domains
Administration	Resource Development	Acquire operational infrastructure	rent physical space
Administration	Resource Development	Acquire operational infrastructure	set up accounts
Administration	Resource Development	Acquire operational infrastructure	network connection
Administration	Resource Development	Acquire operational infrastructure	lease botnet
Administration	Resource Development	Build alliances and partnerships	contract development
Administration	Resource Development	Build alliances and partnerships	commercial vendors

Administration	Resource Development	Build alliances and partnerships	contracts
Administration	Resource Development	Build alliances and partnerships	supply chain
Administration	Resource Development	Build alliances and partnerships	co-production
Administration	Resource Development	Build alliances and partnerships	relationships
Administration	Resource Development	Create botnet	botnet
Administration	Resource Development	Create botnet	virtual network
Administration	Resource Development	Create botnet	bot
Administration	Resource Development	Create botnet	controller
Administration	Resource Development	Develop capabilities	framework
Administration	Resource Development	Develop capabilities	tools
Administration	Resource Development	Develop capabilities	toolkits
Administration	Resource Development	Develop capabilities	create repo
Administration	Resource Development	Develop capabilities	custom code
Administration	Resource Development	Develop capabilities	0-day exploits
Administration	Resource Development	Develop capabilities	exploits
Administration	Resource Development	Develop capabilities	modules
Administration	Resource Development	Develop capabilities	implants
Administration	Resource Development	Develop capabilities	testing
Administration	Resource Development	Develop capabilities	test malware
Administration	Resource Development	Develop capabilities	malware testing
Administration	Resource Development	Obtain financing	contracts
Administration	Resource Development	Obtain financing	income
Administration	Resource Development	Obtain financing	cryptocurrency
Administration	Resource Development	Obtain financing	funding
Administration	Resource Development	Obtain financing	expenses
Administration	Resource Development	Obtain financing	cryptomining
Administration	Resource Development	Obtain financing	cryptojacking
Administration	Resource Development	Obtain financing	virtual money
Administration	Resource Development	Obtain financing	digital currency
Administration	Resource Development	Seed supply chain	supply chain compromise
Administration	Resource Development	Seed supply chain	compromised partner
Administration	Resource Development	Seed supply chain	software
Administration	Resource Development	Seed supply chain	firmware
Administration	Resource Development	Seed supply chain	hardware
Administration	Resource Development	Staff and train resources	resume
Administration	Resource Development	Staff and train resources	recruit
Administration	Resource Development	Staff and train resources	train
Administration	Resource Development	Staff and train resources	terminate
Administration	Research	Gather information	vulnerabilities
Administration	Research	Gather information	breached credentials
Administration	Research	Gather information	publicly available
Administration	Research	Gather information	websites
Administration	Research	Identify capability gaps	target infrastructure
Administration	Research	Identify capability gaps	requirements
Administration	Research	Identify capability gaps	missing capability
Administration	Research	Identify capability gaps	malware analysis
Administration	Research	Identify information gaps	review data
Administration	Research	Identify information gaps	missing target data
Administration	Research	Identify information gaps	collected information
Preparation	Reconnaissance	Conduct social engineering	social engineering
Preparation	Reconnaissance	Conduct social engineering	manipulate people

Preparation	Reconnaissance	Conduct social engineering	solicit
Preparation	Reconnaissance	Conduct social engineering	ask questions
Preparation	Reconnaissance	Conduct social engineering	gather responses
Preparation	Reconnaissance	Conduct social engineering	vishing
Preparation	Reconnaissance	Conduct social engineering	elicitation
Preparation	Reconnaissance	Gather credentials	obtain credentials
Preparation	Reconnaissance	Gather credentials	site masquerading
Preparation	Reconnaissance	Gather credentials	typo squatting
Preparation	Reconnaissance	Gather credentials	typosquatting
Preparation	Reconnaissance	Gather credentials	page scraping
Preparation	Reconnaissance	Gather credentials	domain squatting
Preparation	Reconnaissance	Gather credentials	cybersquatting
Preparation	Reconnaissance	Gather credentials	password list
Preparation	Reconnaissance	Gather credentials	compromised credentials
Preparation	Reconnaissance	Gather credentials	common passwords
Preparation	Reconnaissance	Gather credentials	usernames and passwords
Preparation	Reconnaissance	Gather credentials	rainbow table
Preparation	Reconnaissance	Gather credentials	email credentials
Preparation	Reconnaissance	Gather credentials	domain credentials
Preparation	Reconnaissance	Gather credentials	account harvesting
Preparation	Reconnaissance	Identify crosstalk	crosstalk
Preparation	Reconnaissance	Identify crosstalk	electromagnetic interference
Preparation	Reconnaissance	Identify crosstalk	twisted pair
Preparation	Reconnaissance	Identify crosstalk	emanations
Preparation	Reconnaissance	Identify crosstalk	audio signals
Preparation	Reconnaissance	Identify crosstalk	video signals
Preparation	Reconnaissance	Map accessible networks	network mapping
Preparation	Reconnaissance	Map accessible networks	subnet
Preparation	Reconnaissance	Map accessible networks	evaluating route statements
Preparation	Reconnaissance	Map accessible networks	ping
Preparation	Reconnaissance	Map accessible networks	ping sweep
Preparation	Reconnaissance	Map accessible networks	active devices
Preparation	Reconnaissance	Map accessible networks	nmap
Preparation	Reconnaissance	Map accessible networks	icmp
Preparation	Reconnaissance	Map accessible networks	traceroute
Preparation	Reconnaissance	Scan devices	active scan
Preparation	Reconnaissance	Scan devices	port scan
Preparation	Reconnaissance	Scan devices	TCP fingerprinting
Preparation	Reconnaissance	Scan devices	banner grabbing
Preparation	Reconnaissance	Scan devices	vulnerability scan
Preparation	Reconnaissance	Scan devices	passive scan
Preparation	Reconnaissance	Scan devices	scanning
Preparation	Reconnaissance	Scan devices	OS fingerprinting
Preparation	Reconnaissance	Scan devices	open ports
Preparation	Reconnaissance	Scan devices	address scan
Preparation	Reconnaissance	Scrape websites	web scraper
Preparation	Reconnaissance	Scrape websites	web forum
Preparation	Reconnaissance	Scrape websites	google dorking
Preparation	Reconnaissance	Scrape websites	bulk retrieval
Preparation	Reconnaissance	Scrape websites	robot.txt
Preparation	Reconnaissance	Scrape websites	conference website

Preparation	Reconnaissance	Scrape websites	bulletin board
Preparation	Reconnaissance	Scrape websites	web search
Preparation	Reconnaissance	Scrape websites	search engine
Preparation	Reconnaissance	Scrape websites	web crawler
Preparation	Reconnaissance	Scrape websites	scraping
Preparation	Reconnaissance	Scrape websites	web scraping
Preparation	Reconnaissance	Scrape websites	spambot
Preparation	Reconnaissance	Select potential victims	target list
Preparation	Reconnaissance	Select potential victims	targeted user
Preparation	Reconnaissance	Select potential victims	targeted network
Preparation	Reconnaissance	Select potential victims	vulnerable host
Preparation	Reconnaissance	Survey devices	analyze targets
Preparation	Reconnaissance	Survey devices	cross check information
Preparation	Reconnaissance	Survey devices	search CVE
Preparation	Reconnaissance	Survey devices	whois
Preparation	Reconnaissance	Survey devices	dig
Preparation	Reconnaissance	Survey devices	finger
Preparation	Reconnaissance	Survey devices	identify crypto
Preparation	Reconnaissance	Survey devices	fuzzing
Preparation	Reconnaissance	Use social media	handle
Preparation	Reconnaissance	Use social media	develop profile
Preparation	Reconnaissance	Use social media	friend request
Preparation	Reconnaissance	Use social media	private message
Preparation	Reconnaissance	Use social media	post
Preparation	Reconnaissance	Use social media	download data
Preparation	Reconnaissance	Use social media	contact list
Preparation	Reconnaissance	Use social media	profile
Preparation	Reconnaissance	Use social media	likes
Preparation	Reconnaissance	Use social media	connections
Preparation	Reconnaissance	Use social media	groups
Preparation	Reconnaissance	Use social media	followers
Preparation	Reconnaissance	Use social media	tweet
Preparation	Reconnaissance	Use social media	feed
Preparation	Staging	Add exploits to application data files	application vulnerability
Preparation	Staging	Add exploits to application data files	exploit
Preparation	Staging	Add exploits to application data files	CVE
Preparation	Staging	Add exploits to application data files	macro
Preparation	Staging	Add exploits to application data files	VBS
Preparation	Staging	Add exploits to application data files	embed
Preparation	Staging	Add exploits to application data files	steganography
Preparation	Staging	Add exploits to application data files	alter content
Preparation	Staging	Add exploits to application data files	javascript
Preparation	Staging	Add exploits to application data files	font
Preparation	Staging	Add exploits to application data files	container
Preparation	Staging	Add exploits to application data files	decoy
Preparation	Staging	Allocate operational infrastructure	manage domains
Preparation	Staging	Allocate operational infrastructure	resolve to IP address
Preparation	Staging	Allocate operational infrastructure	resolve to null IP address
Preparation	Staging	Allocate operational infrastructure	configure hosted infrastructure
Preparation	Staging	Allocate operational infrastructure	update dynamic-DNS
Preparation	Staging	Allocate operational infrastructure	anonymizing infrastructure

Preparation	Staging	Allocate operational infrastructure	domain shadowing
Preparation	Staging	Allocate operational infrastructure	create subdomain
Preparation	Staging	Create midpoints	log into hosting accounts
Preparation	Staging	Create midpoints	hop point
Preparation	Staging	Create midpoints	virtual private server
Preparation	Staging	Create midpoints	VPS
Preparation	Staging	Create midpoints	jump box
Preparation	Staging	Create midpoints	relay
Preparation	Staging	Create midpoints	deploy software on hosted device
Preparation	Staging	Create midpoints	update software
Preparation	Staging	Establish physical proximity	local infrastructure
Preparation	Staging	Establish physical proximity	insider threat
Preparation	Staging	Establish physical proximity	minimize latency
Preparation	Staging	Establish physical proximity	enable wireless access
Preparation	Staging	Establish physical proximity	improve OPSEC
Preparation	Staging	Establish physical proximity	physical office
Preparation	Staging	Establish physical proximity	data center location
Preparation	Staging	Infect or seed website	phishing
Preparation	Staging	Infect or seed website	web shell
Preparation	Staging	Infect or seed website	webshell
Preparation	Staging	Infect or seed website	modify existing website
Preparation	Staging	Infect or seed website	malvertising
Preparation	Staging	Infect or seed website	watering hole
Preparation	Staging	Infect or seed website	drive-by download
Preparation	Staging	Infect or seed website	fuzzing
Preparation	Staging	Pre-position payload	pre-positioning
Preparation	Staging	Pre-position payload	cloud document hosting services
Preparation	Staging	Pre-position payload	accessible data storage
Engagement	Delivery	Access via wireless	wifi
Engagement	Delivery	Access via wireless	WPA
Engagement	Delivery	Access via wireless	WEP
Engagement	Delivery	Access via wireless	access point
Engagement	Delivery	Access via wireless	AP
Engagement	Delivery	Access via wireless	mircowave
Engagement	Delivery	Access via wireless	bluetooth
Engagement	Delivery	Access via wireless	wireless card
Engagement	Delivery	Access via wireless	cellular
Engagement	Delivery	Access via wireless	IR
Engagement	Delivery	Access via wireless	inductive coupling
Engagement	Delivery	Access via wireless	RF
Engagement	Delivery	Access via wireless	airdrop
Engagement	Delivery	Access via wireless	BLE
Engagement	Delivery	Access via wireless	bluejacking
Engagement	Delivery	Access via wireless	bluesnarfing
Engagement	Delivery	Alter communications path	change route
Engagement	Delivery	Alter communications path	cache poisoning
Engagement	Delivery	Alter communications path	DNS poisoning
Engagement	Delivery	Alter communications path	route poisoning
Engagement	Delivery	Alter communications path	route injection
Engagement	Delivery	Alter communications path	ARP poisoning
Engagement	Delivery	Alter communications path	race condition

Engagement	Delivery	Alter communications path	man-in-the-middle
Engagement	Delivery	Alter communications path	man-on-the-side
Engagement	Delivery	Alter communications path	poison cache
Engagement	Delivery	Alter communications path	false URL
Engagement	Delivery	Alter communications path	cached URL
Engagement	Delivery	Compromise supply chain or trusted source	trusted vendor list
Engagement	Delivery	Compromise supply chain or trusted source	supplier
Engagement	Delivery	Compromise supply chain or trusted source	install malicious software
Engagement	Delivery	Compromise supply chain or trusted source	modify firmware
Engagement	Delivery	Compromise supply chain or trusted source	modify hardware
Engagement	Delivery	Compromise supply chain or trusted source	install malicious hardware
Engagement	Delivery	Compromise supply chain or trusted source	redirect shipment
Engagement	Delivery	Compromise supply chain or trusted source	supply chain compromise
Engagement	Delivery	Connect removable media	insert removable media
Engagement	Delivery	Connect removable media	USB
Engagement	Delivery	Connect removable media	flash drive
Engagement	Delivery	Connect removable media	CD
Engagement	Delivery	Connect removable media	external hard drive
Engagement	Delivery	Connect removable media	auto-run
Engagement	Delivery	Connect removable media	.ini
Engagement	Delivery	Connect removable media	replication through removable media
Engagement	Delivery	Connect rogue network devices	create access point
Engagement	Delivery	Connect rogue network devices	rogue access point
Engagement	Delivery	Connect rogue network devices	extra network interface card
Engagement	Delivery	Connect rogue network devices	NIC
Engagement	Delivery	Connect rogue network devices	embedded infrared
Engagement	Delivery	Connect rogue network devices	bluetooth
Engagement	Delivery	Connect rogue network devices	wifi
Engagement	Delivery	Connect rogue network devices	cellular modem
Engagement	Delivery	Connect rogue network devices	hot spot
Engagement	Delivery	Connect rogue network devices	hardware additions
Engagement	Delivery	Infect via websites	watering hole
Engagement	Delivery	Infect via websites	advertisement
Engagement	Delivery	Infect via websites	malvertising
Engagement	Delivery	Infect via websites	embedded
Engagement	Delivery	Infect via websites	iframe
Engagement	Delivery	Infect via websites	legitimate website
Engagement	Delivery	Infect via websites	compromised website
Engagement	Delivery	Infect via websites	spoofed website
Engagement	Delivery	Infect via websites	whitelisted
Engagement	Delivery	Infect via websites	download
Engagement	Delivery	Infect via websites	cross site scripting
Engagement	Delivery	Infect via websites	cross-site scripting
Engagement	Delivery	Infect via websites	XSS
Engagement	Delivery	Infect via websites	drive-by compromise
Engagement	Delivery	Infect via websites	spearphishing link
Engagement	Delivery	Infect via websites	spearphishing via service
Engagement	Delivery	Infect via websites	adware
Engagement	Delivery	Infect via websites	cookie
Engagement	Delivery	Infect via websites	scareware
Engagement	Delivery	Inject database command	SQL injection

Engagement	Delivery	Inject database command	web interface
Engagement	Delivery	Inject database command	fuzzing
Engagement	Delivery	Inject database command	error handling
Engagement	Delivery	Inject database command	form handling
Engagement	Delivery	Inject database command	URL parameters
Engagement	Delivery	Inject database command	encoding
Engagement	Delivery	Inject database command	web server error messages
Engagement	Delivery	Inject database command	exploit public-facing application
Engagement	Delivery	Leverage device swapping	unauthorized device
Engagement	Delivery	Leverage device swapping	insider threat
Engagement	Delivery	Leverage device swapping	cross-domain movement
Engagement	Delivery	Leverage device swapping	close access
Engagement	Delivery	Leverage device swapping	security domain
Engagement	Delivery	Leverage device swapping	charge mobile device
Engagement	Delivery	Leverage device swapping	swap RAM
Engagement	Delivery	Leverage device swapping	hardware additions
Engagement	Delivery	Send malicious email	spear-phishing
Engagement	Delivery	Send malicious email	whaling
Engagement	Delivery	Send malicious email	phishing
Engagement	Delivery	Send malicious email	spam
Engagement	Delivery	Send malicious email	malicious attachment
Engagement	Delivery	Send malicious email	malicious link
Engagement	Delivery	Send malicious email	URL
Engagement	Delivery	Send malicious email	embedded code
Engagement	Delivery	Send malicious email	embedded HTML iFrame
Engagement	Delivery	Send malicious email	iFrame
Engagement	Delivery	Send malicious email	spearphishing attachment
Engagement	Delivery	Send malicious email	spearphishing link
Engagement	Delivery	Send malicious email	spearphishing via service
Engagement	Delivery	Transport via common network infrastructure	compromised network
Engagement	Delivery	Transport via common network infrastructure	trusted network relationship
Engagement	Delivery	Transport via common network infrastructure	connected network
Engagement	Delivery	Transport via common network infrastructure	subnet
Engagement	Delivery	Transport via common network infrastructure	provider network
Engagement	Delivery	Transport via common network infrastructure	trusted relationship
Engagement	Delivery	Traverse CDS or MLS	automated transport services
Engagement	Delivery	Traverse CDS or MLS	cross domain solution
Engagement	Delivery	Traverse CDS or MLS	multi-level solution
Engagement	Delivery	Traverse CDS or MLS	network guard
Engagement	Delivery	Traverse CDS or MLS	trusted services
Engagement	Delivery	Traverse CDS or MLS	misconfigured CDS
Engagement	Delivery	Traverse CDS or MLS	misconfigured MLS
Engagement	Delivery	Traverse CDS or MLS	low-to-high
Engagement	Delivery	Traverse CDS or MLS	pathway
Engagement	Delivery	Traverse CDS or MLS	insider threat
Engagement	Delivery	Traverse CDS or MLS	compromise trusted services
Engagement	Delivery	Traverse CDS or MLS	dual-homed
Engagement	Delivery	Traverse CDS or MLS	trusted relationship
Engagement	Delivery	Use chat services	send message
Engagement	Delivery	Use chat services	sms
Engagement	Delivery	Use chat services	messaging

Engagement	Delivery	Use chat services	mms
Engagement	Delivery	Use chat services	chatroom
Engagement	Delivery	Use chat services	chat session
Engagement	Delivery	Use chat services	spearphishing via service
Engagement	Delivery	Use compromised host	previously compromised victim
Engagement	Delivery	Use compromised host	toolkit
Engagement	Delivery	Use compromised host	download tool
Engagement	Delivery	Use compromised host	download toolkit
Engagement	Delivery	Use compromised host	second stage malware
Engagement	Delivery	Use compromised host	victim host
Engagement	Delivery	Use compromised host	trojan
Engagement	Delivery	Use compromised host	remote shell
Engagement	Delivery	Use compromised host	insider threat
Engagement	Delivery	Use compromised host	trusted relationship
Engagement	Delivery	Use compromised host	backdoor
Engagement	Delivery	Use compromised host	implant
Engagement	Delivery	Use compromised host	spyware
Engagement	Delivery	Use legitimate remote access	remote access to host
Engagement	Delivery	Use legitimate remote access	legitimate credentials
Engagement	Delivery	Use legitimate remote access	VPN
Engagement	Delivery	Use legitimate remote access	RDP
Engagement	Delivery	Use legitimate remote access	ssh
Engagement	Delivery	Use legitimate remote access	telnet
Engagement	Delivery	Use legitimate remote access	ftp
Engagement	Delivery	Use legitimate remote access	WMI
Engagement	Delivery	Use legitimate remote access	webmail
Engagement	Delivery	Use legitimate remote access	insider threat
Engagement	Delivery	Use legitimate remote access	valid accounts
Engagement	Delivery	Use physical network bridge	bridging
Engagement	Delivery	Use physical network bridge	cabling
Engagement	Delivery	Use physical network bridge	switch
Engagement	Delivery	Use physical network bridge	hub
Engagement	Delivery	Use physical network bridge	connect networks
Engagement	Delivery	Use physical network bridge	bridge networks
Engagement	Delivery	Use physical network bridge	subnet
Engagement	Delivery	Use physical network bridge	network segment
Engagement	Delivery	Use physical network bridge	hardware additions
Engagement	Exploitation	Abuse protocols	unanticipated use
Engagement	Exploitation	Abuse protocols	protocol abuse
Engagement	Exploitation	Abuse protocols	RFC compliance
Engagement	Exploitation	Abuse protocols	legacy field
Engagement	Exploitation	Abuse protocols	legacy protocol
Engagement	Exploitation	Abuse protocols	undocumented field
Engagement	Exploitation	Abuse protocols	undocumented command
Engagement	Exploitation	Abuse protocols	slack space
Engagement	Exploitation	Abuse protocols	unexpected protocol
Engagement	Exploitation	Abuse protocols	port protocol mismatch
Engagement	Exploitation	Access virtual memory	abuse physical location of virtual spaces
Engagement	Exploitation	Access virtual memory	collocation
Engagement	Exploitation	Access virtual memory	virtual spaces
Engagement	Exploitation	Access virtual memory	virtual machines

Engagement	Exploitation	Access virtual memory	VM
Engagement	Exploitation	Access virtual memory	container
Engagement	Exploitation	Access virtual memory	hypervisor
Engagement	Exploitation	Access virtual memory	memory cache of isolated virtual machines
Engagement	Exploitation	Access virtual memory	race condition
Engagement	Exploitation	Access virtual memory	return memory contents
Engagement	Exploitation	Access virtual memory	Heartbleed
Engagement	Exploitation	Access virtual memory	malicious payload in virtual memory
Engagement	Exploitation	Access virtual memory	virtual machine escape
Engagement	Exploitation	Access virtual memory	VM escape
Engagement	Exploitation	Conduct social engineering	social engineering
Engagement	Exploitation	Conduct social engineering	manipulate people
Engagement	Exploitation	Conduct social engineering	entice a user to view
Engagement	Exploitation	Conduct social engineering	entice a user to click
Engagement	Exploitation	Conduct social engineering	click bait
Engagement	Exploitation	Conduct social engineering	post QR code
Engagement	Exploitation	Conduct social engineering	themes
Engagement	Exploitation	Conduct social engineering	craft legitimate email
Engagement	Exploitation	Conduct social engineering	enticing email
Engagement	Exploitation	Conduct social engineering	decoy
Engagement	Exploitation	Conduct social engineering	USB drop
Engagement	Exploitation	Conduct social engineering	human-enabled technical operation
Engagement	Exploitation	Defeat encryption	improperly implemented crypto
Engagement	Exploitation	Defeat encryption	exploit crytographic algorithms
Engagement	Exploitation	Defeat encryption	exploit device implementation of cryptography
Engagement	Exploitation	Defeat encryption	misconfigured crypto
Engagement	Exploitation	Defeat encryption	generate keys
Engagement	Exploitation	Defeat encryption	brute force
Engagement	Exploitation	Defeat encryption	crack encryption
Engagement	Exploitation	Defeat encryption	obtain key material
Engagement	Exploitation	Defeat encryption	dictionary attack
Engagement	Exploitation	Exploit firmware vulnerability	firmware
Engagement	Exploitation	Exploit firmware vulnerability	embedded devices
Engagement	Exploitation	Exploit firmware vulnerability	CVE
Engagement	Exploitation	Exploit firmware vulnerability	phlashing
Engagement	Exploitation	Exploit local application vulnerability	open malicious file
Engagement	Exploitation	Exploit local application vulnerability	software
Engagement	Exploitation	Exploit local application vulnerability	application
Engagement	Exploitation	Exploit local application vulnerability	buffer overflow
Engagement	Exploitation	Exploit local application vulnerability	user interaction
Engagement	Exploitation	Exploit local application vulnerability	insider threat
Engagement	Exploitation	Exploit local application vulnerability	CVE
Engagement	Exploitation	Exploit local application vulnerability	exploitation for client execution
Engagement	Exploitation	Exploit OS vulnerability	operating system
Engagement	Exploitation	Exploit OS vulnerability	os vulnerability
Engagement	Exploitation	Exploit OS vulnerability	CVE
Engagement	Exploitation	Exploit OS vulnerability	protocol implementation
Engagement	Exploitation	Exploit OS vulnerability	exploitation for client execution
Engagement	Exploitation	Exploit OS vulnerability	LSASS driver
Engagement	Exploitation	Exploit OS vulnerability	space after filename
Engagement	Exploitation	Exploit remote application vulnerability	webmail

Engagement	Exploitation	Exploit remote application vulnerability	web application
Engagement	Exploitation	Exploit remote application vulnerability	software
Engagement	Exploitation	Exploit remote application vulnerability	application
Engagement	Exploitation	Exploit remote application vulnerability	network traffic
Engagement	Exploitation	Exploit remote application vulnerability	CVE
Engagement	Exploitation	Exploit remote application vulnerability	exploit public-facing application
Engagement	Exploitation	Exploit remote application vulnerability	exploitation for client execution
Engagement	Exploitation	Exploit weak access controls	password spraying
Engagement	Exploitation	Exploit weak access controls	anonymous FTP
Engagement	Exploitation	Exploit weak access controls	anonymous telnet login
Engagement	Exploitation	Exploit weak access controls	misconfigured router ACL
Engagement	Exploitation	Exploit weak access controls	default password
Engagement	Exploitation	Exploit weak access controls	missing access control
Engagement	Exploitation	Exploit weak access controls	brute force
Engagement	Exploitation	Hijack	control communication
Engagement	Exploitation	Hijack	man-in-the-middle
Engagement	Exploitation	Hijack	BGP hijacking
Engagement	Exploitation	Hijack	redirect route
Engagement	Exploitation	Hijack	session hijacking
Engagement	Exploitation	Hijack	route
Engagement	Exploitation	Hijack	connection hijacking
Engagement	Exploitation	Impersonate or spoof user	request user account
Engagement	Exploitation	Impersonate or spoof user	ssh masquerade
Engagement	Exploitation	Impersonate or spoof user	telnet masquerade
Engagement	Exploitation	Impersonate or spoof user	password reset
Engagement	Exploitation	Impersonate or spoof user	domain spoofing
Engagement	Exploitation	Impersonate or spoof user	email spoofing
Engagement	Exploitation	Impersonate or spoof user	fake profile
Engagement	Exploitation	Impersonate or spoof user	valid accounts
Engagement	Exploitation	Impersonate or spoof user	operational account
Engagement	Exploitation	Impersonate or spoof user	impersonating
Engagement	Exploitation	Impersonate or spoof user	DNS spoofing
Engagement	Exploitation	Impersonate or spoof user	piggybacking
Engagement	Exploitation	Impersonate or spoof user	mimicking
Engagement	Exploitation	Launch zero-day exploit	0-day exploit
Engagement	Exploitation	Launch zero-day exploit	undisclosed vulnerability
Engagement	Exploitation	Launch zero-day exploit	zero day
Engagement	Exploitation	Launch zero-day exploit	zero-day
Engagement	Exploitation	Launch zero-day exploit	undocumented vulnerability
Engagement	Exploitation	Launch zero-day exploit	exploit public-facing application
Engagement	Exploitation	Leverage exploit packs	exploit packs
Engagement	Exploitation	Leverage exploit packs	exploit kit
Engagement	Exploitation	Leverage exploit packs	exploit public-facing application
Engagement	Exploitation	Leverage trusted relationship	trusted network relationship
Engagement	Exploitation	Leverage trusted relationship	peer network
Engagement	Exploitation	Leverage trusted relationship	compromised network
Engagement	Exploitation	Leverage trusted relationship	trusted relationship
Engagement	Exploitation	Leverage trusted relationship	trusted domain
Engagement	Exploitation	Leverage trusted relationship	trusted host
Engagement	Exploitation	Replay	retransmit traffic
Engagement	Exploitation	Replay	send traffic again

Engagement	Exploitation	Replay	valid data transmission
Engagement	Exploitation	Replay	repeat traffic
Engagement	Exploitation	Replay	delayed transmission
Presence	Execution	Create scheduled task	execute programs
Presence	Execution	Create scheduled task	schedule
Presence	Execution	Create scheduled task	at
Presence	Execution	Create scheduled task	schtasks
Presence	Execution	Create scheduled task	cron
Presence	Execution	Create scheduled task	cronjob
Presence	Execution	Create scheduled task	local job scheduling
Presence	Execution	Create scheduled task	scheduled task
Presence	Execution	Execute via service controller	service controller
Presence	Execution	Execute via service controller	execute binary
Presence	Execution	Execute via service controller	service control module
Presence	Execution	Execute via service controller	daemons
Presence	Execution	Execute via service controller	inetd
Presence	Execution	Execute via service controller	xinetd
Presence	Execution	Execute via service controller	service control manager
Presence	Execution	Execute via service controller	sc
Presence	Execution	Execute via service controller	regsvr32
Presence	Execution	Execute via service controller	service execution
Presence	Execution	Execute via service controller	regsvcs/regasm
Presence	Execution	Execute via third-party software	pre-existing third-party applications
Presence	Execution	Execute via third-party software	unauthorized updates
Presence	Execution	Execute via third-party software	peer-to-peer network administration tools
Presence	Execution	Execute via third-party software	graphical user interface
Presence	Execution	Execute via third-party software	installutil
Presence	Execution	Execute via third-party software	third-party software
Presence	Execution	Execute via third-party software	trusted developer utilities
Presence	Execution	Inject into running process	process injection
Presence	Execution	Inject into running process	code injection
Presence	Execution	Inject into running process	context of another process
Presence	Execution	Inject into running process	process memory
Presence	Execution	Inject into running process	process permissions
Presence	Execution	Inject into running process	DLL sideloading
Presence	Execution	Inject into running process	DLL side-loading
Presence	Execution	Inject into running process	tasklist
Presence	Execution	Inject into running process	loader
Presence	Execution	Inject into running process	DLL injection
Presence	Execution	Inject into running process	process hollowing
Presence	Execution	Inject into running process	execution through module load
Presence	Execution	Leverage authorized user	user interaction
Presence	Execution	Leverage authorized user	open file
Presence	Execution	Leverage authorized user	click link
Presence	Execution	Leverage authorized user	enable macros
Presence	Execution	Leverage authorized user	change security settings
Presence	Execution	Leverage authorized user	insider threat
Presence	Execution	Leverage authorized user	user execution
Presence	Execution	Leverage authorized user	human-enabled technical operation
Presence	Execution	Replace existing binary	appear legitimate
Presence	Execution	Replace existing binary	commonly trusted location

Presence	Execution	Replace existing binary	legitimate source
Presence	Execution	Replace existing binary	common name
Presence	Execution	Replace existing binary	legitimate file name
Presence	Execution	Replace existing binary	common path
Presence	Execution	Replace existing binary	local patch updating mechanism
Presence	Execution	Replace existing binary	benign by name
Presence	Execution	Replace existing binary	replace legitimate binary
Presence	Execution	Replace existing binary	signed binary proxy execution
Presence	Execution	Run commands in shell	commands
Presence	Execution	Run commands in shell	command line
Presence	Execution	Run commands in shell	remote shell
Presence	Execution	Run commands in shell	interactive
Presence	Execution	Run commands in shell	cmd.exe
Presence	Execution	Run commands in shell	RDP
Presence	Execution	Run commands in shell	reverse shell
Presence	Execution	Run commands in shell	bash
Presence	Execution	Run commands in shell	powershell command line
Presence	Execution	Run commands in shell	python shell
Presence	Execution	Run commands in shell	web shell
Presence	Execution	Run commands in shell	webshell
Presence	Execution	Run commands in shell	command-line interface
Presence	Execution	Run fileless payload	in memory code
Presence	Execution	Run fileless payload	resident in memory
Presence	Execution	Run fileless payload	memory resident
Presence	Execution	Run fileless payload	no file
Presence	Execution	Use interpreted scripts	scripting language
Presence	Execution	Use interpreted scripts	scripts
Presence	Execution	Use interpreted scripts	script file
Presence	Execution	Use interpreted scripts	script commands
Presence	Execution	Use interpreted scripts	script interpreter
Presence	Execution	Use interpreted scripts	powershell
Presence	Execution	Use interpreted scripts	vbscript
Presence	Execution	Use interpreted scripts	javascript
Presence	Execution	Use interpreted scripts	.net
Presence	Execution	Use interpreted scripts	java
Presence	Execution	Use interpreted scripts	sequenced commands
Presence	Execution	Use interpreted scripts	perl
Presence	Execution	Use interpreted scripts	python
Presence	Execution	Use interpreted scripts	JIT compiled languages
Presence	Execution	Use interpreted scripts	bash script
Presence	Execution	Use interpreted scripts	shell script
Presence	Execution	Use interpreted scripts	WMI script
Presence	Execution	Use interpreted scripts	applescript
Presence	Execution	Use interpreted scripts	scripting
Presence	Execution	Use OS APIs	operating system
Presence	Execution	Use OS APIs	application programming interfaces
Presence	Execution	Use OS APIs	CreateProcess
Presence	Execution	Use OS APIs	copy into expected location to run
Presence	Execution	Use OS APIs	OS functions
Presence	Execution	Use OS APIs	control panel items
Presence	Execution	Use OS APIs	execution through API

Presence	Execution	Use OS APIs	mshta
Presence	Execution	Use remote services	remote administrative services
Presence	Execution	Use remote services	remote access
Presence	Execution	Use remote services	windows management instrumentation
Presence	Execution	Use remote services	WMI
Presence	Execution	Use remote services	windows remote management
Presence	Execution	Use remote services	WinRM
Presence	Execution	Use remote services	RPC
Presence	Execution	Use remote services	remote desktop services
Presence	Execution	Use remote services	mstsc
Presence	Execution	Use remote services	windows terminal services
Presence	Execution	Use remote services	mmc
Presence	Execution	Use remote services	Microsoft Management Console
Presence	Execution	Use remote services	implied trust
Presence	Execution	Use remote services	valid credentials
Presence	Execution	Use trusted application to execute untrusted code	trusted application
Presence	Execution	Use trusted application to execute untrusted code	Rundll32
Presence	Execution	Use trusted application to execute untrusted code	arbitrary DLL
Presence	Execution	Use trusted application to execute untrusted code	ignored by security tools
Presence	Execution	Use trusted application to execute untrusted code	evade detection
Presence	Execution	Use trusted application to execute untrusted code	bypass process monitoring
Presence	Execution	Use trusted application to execute untrusted code	insmod
Presence	Execution	Use trusted application to execute untrusted code	inject code into the kernel
Presence	Execution	Write to disk	disk
Presence	Execution	Write to disk	network share
Presence	Execution	Write to disk	dropped files
Presence	Execution	Write to disk	configuration file
Presence	Execution	Write to disk	log file
Presence	Execution	Write to disk	save file
Presence	Execution	Write to disk	file created
Presence	Execution	Write to disk	copy
Presence	Execution	Write to disk	application shimming
Presence	Execution	Write to disk	edit registry
Presence	Execution	Write to disk	add registry key
Presence	Execution	Write to disk	modify registry
Presence	Execution	Write to disk	upload
Presence	Internal Reconnaissance	Enumerate accounts and permissions	domain account
Presence	Internal Reconnaissance	Enumerate accounts and permissions	account list
Presence	Internal Reconnaissance	Enumerate accounts and permissions	permissions
Presence	Internal Reconnaissance	Enumerate accounts and permissions	review logins
Presence	Internal Reconnaissance	Enumerate accounts and permissions	identify primary users
Presence	Internal Reconnaissance	Enumerate accounts and permissions	local groups
Presence	Internal Reconnaissance	Enumerate accounts and permissions	group permission
Presence	Internal Reconnaissance	Enumerate accounts and permissions	group members
Presence	Internal Reconnaissance	Enumerate accounts and permissions	local account
Presence	Internal Reconnaissance	Enumerate accounts and permissions	net user
Presence	Internal Reconnaissance	Enumerate accounts and permissions	quser
Presence	Internal Reconnaissance	Enumerate accounts and permissions	dsquery
Presence	Internal Reconnaissance	Enumerate accounts and permissions	whoami
Presence	Internal Reconnaissance	Enumerate accounts and permissions	dir /a ntuser.dat
Presence	Internal Reconnaissance	Enumerate accounts and permissions	net localgroup

Presence	Internal Reconnaissance	Enumerate accounts and permissions	account discovery
Presence	Internal Reconnaissance	Enumerate accounts and permissions	permission groups discovery
Presence	Internal Reconnaissance	Enumerate accounts and permissions	password policy discovery
Presence	Internal Reconnaissance	Enumerate accounts and permissions	system owner/user discovery
Presence	Internal Reconnaissance	Enumerate file system	enumerate files
Presence	Internal Reconnaissance	Enumerate file system	directory walk
Presence	Internal Reconnaissance	Enumerate file system	search files
Presence	Internal Reconnaissance	Enumerate file system	search directories
Presence	Internal Reconnaissance	Enumerate file system	dir
Presence	Internal Reconnaissance	Enumerate file system	ls
Presence	Internal Reconnaissance	Enumerate file system	findstr
Presence	Internal Reconnaissance	Enumerate file system	SMB
Presence	Internal Reconnaissance	Enumerate file system	NFS
Presence	Internal Reconnaissance	Enumerate file system	CIFS
Presence	Internal Reconnaissance	Enumerate file system	file and directory discovery
Presence	Internal Reconnaissance	Enumerate file system	network share discovery
Presence	Internal Reconnaissance	Enumerate local network connections	list network connections
Presence	Internal Reconnaissance	Enumerate local network connections	netstat
Presence	Internal Reconnaissance	Enumerate local network connections	net user
Presence	Internal Reconnaissance	Enumerate local network connections	net session
Presence	Internal Reconnaissance	Enumerate local network connections	net view
Presence	Internal Reconnaissance	Enumerate local network connections	arp
Presence	Internal Reconnaissance	Enumerate local network connections	route
Presence	Internal Reconnaissance	Enumerate local network connections	nbtstat
Presence	Internal Reconnaissance	Enumerate local network connections	lsof
Presence	Internal Reconnaissance	Enumerate local network connections	ss
Presence	Internal Reconnaissance	Enumerate local network connections	system network connections discovery
Presence	Internal Reconnaissance	Enumerate local network settings	network settings
Presence	Internal Reconnaissance	Enumerate local network settings	local network
Presence	Internal Reconnaissance	Enumerate local network settings	ipconfig
Presence	Internal Reconnaissance	Enumerate local network settings	ip
Presence	Internal Reconnaissance	Enumerate local network settings	ifconfig
Presence	Internal Reconnaissance	Enumerate local network settings	configuration files
Presence	Internal Reconnaissance	Enumerate local network settings	subnet
Presence	Internal Reconnaissance	Enumerate local network settings	network diagram
Presence	Internal Reconnaissance	Enumerate local network settings	system network configuration discovery
Presence	Internal Reconnaissance	Enumerate OS and software	OS details
Presence	Internal Reconnaissance	Enumerate OS and software	version
Presence	Internal Reconnaissance	Enumerate OS and software	patch
Presence	Internal Reconnaissance	Enumerate OS and software	hotfixes
Presence	Internal Reconnaissance	Enumerate OS and software	service packs
Presence	Internal Reconnaissance	Enumerate OS and software	architecture
Presence	Internal Reconnaissance	Enumerate OS and software	software list
Presence	Internal Reconnaissance	Enumerate OS and software	drivers
Presence	Internal Reconnaissance	Enumerate OS and software	configuration
Presence	Internal Reconnaissance	Enumerate OS and software	version
Presence	Internal Reconnaissance	Enumerate OS and software	uname
Presence	Internal Reconnaissance	Enumerate OS and software	systeminfo
Presence	Internal Reconnaissance	Enumerate OS and software	netsh
Presence	Internal Reconnaissance	Enumerate OS and software	reg query
Presence	Internal Reconnaissance	Enumerate OS and software	dir

Presence	Internal Reconnaissance	Enumerate OS and software	tasklist
Presence	Internal Reconnaissance	Enumerate OS and software	adware
Presence	Internal Reconnaissance	Enumerate OS and software	detect security software
Presence	Internal Reconnaissance	Enumerate OS and software	antivirus
Presence	Internal Reconnaissance	Enumerate OS and software	browser bookmark discovery
Presence	Internal Reconnaissance	Enumerate OS and software	query registry
Presence	Internal Reconnaissance	Enumerate OS and software	reggquery
Presence	Internal Reconnaissance	Enumerate OS and software	security software discovery
Presence	Internal Reconnaissance	Enumerate OS and software	system information discovery
Presence	Internal Reconnaissance	Enumerate OS and software	system time discovery
Presence	Internal Reconnaissance	Enumerate processes	process list
Presence	Internal Reconnaissance	Enumerate processes	top
Presence	Internal Reconnaissance	Enumerate processes	running processes
Presence	Internal Reconnaissance	Enumerate processes	lodaded libraries
Presence	Internal Reconnaissance	Enumerate processes	mutex
Presence	Internal Reconnaissance	Enumerate processes	registered services
Presence	Internal Reconnaissance	Enumerate processes	tasklist
Presence	Internal Reconnaissance	Enumerate processes	ps
Presence	Internal Reconnaissance	Enumerate processes	tasklist /svc
Presence	Internal Reconnaissance	Enumerate processes	sc
Presence	Internal Reconnaissance	Enumerate processes	net start
Presence	Internal Reconnaissance	Enumerate processes	init
Presence	Internal Reconnaissance	Enumerate processes	services
Presence	Internal Reconnaissance	Enumerate processes	search registry
Presence	Internal Reconnaissance	Enumerate processes	process discovery
Presence	Internal Reconnaissance	Enumerate processes	system service discovery
Presence	Internal Reconnaissance	Enumerate windows	application window
Presence	Internal Reconnaissance	Enumerate windows	invisible window
Presence	Internal Reconnaissance	Enumerate windows	pixel
Presence	Internal Reconnaissance	Enumerate windows	application window discovery
Presence	Internal Reconnaissance	Map accessible networks	network mapping
Presence	Internal Reconnaissance	Map accessible networks	ping
Presence	Internal Reconnaissance	Map accessible networks	ping sweep
Presence	Internal Reconnaissance	Map accessible networks	active devices
Presence	Internal Reconnaissance	Map accessible networks	nmap
Presence	Internal Reconnaissance	Map accessible networks	icmp
Presence	Internal Reconnaissance	Map accessible networks	traceroute
Presence	Internal Reconnaissance	Map accessible networks	local network
Presence	Internal Reconnaissance	Scan connected devices	local network
Presence	Internal Reconnaissance	Scan connected devices	active scan
Presence	Internal Reconnaissance	Scan connected devices	port scan
Presence	Internal Reconnaissance	Scan connected devices	TCP fingerprinting
Presence	Internal Reconnaissance	Scan connected devices	banner grabbing
Presence	Internal Reconnaissance	Scan connected devices	vulnerability scan
Presence	Internal Reconnaissance	Scan connected devices	passive scan
Presence	Internal Reconnaissance	Scan connected devices	scanning
Presence	Internal Reconnaissance	Scan connected devices	OS fingerprinting
Presence	Internal Reconnaissance	Scan connected devices	open ports
Presence	Internal Reconnaissance	Scan connected devices	address scan
Presence	Internal Reconnaissance	Scan connected devices	private network
Presence	Internal Reconnaissance	Scan connected devices	network service scanning

Presence	Internal Reconnaissance	Scan connected devices	peripheral device discovery
Presence	Internal Reconnaissance	Scan connected devices	remote system discovery
Presence	Internal Reconnaissance	Sniff network	network interface
Presence	Internal Reconnaissance	Sniff network	monitor network
Presence	Internal Reconnaissance	Sniff network	analyze traffic
Presence	Internal Reconnaissance	Sniff network	packet analysis
Presence	Internal Reconnaissance	Sniff network	promiscuous mode
Presence	Internal Reconnaissance	Sniff network	packet capture
Presence	Internal Reconnaissance	Sniff network	span port
Presence	Internal Reconnaissance	Sniff network	network sniffing
Presence	Internal Reconnaissance	Sniff network	sniffer
Presence	Internal Reconnaissance	Sniff network	PCAP
Presence	Internal Reconnaissance	Sniff network	tcpdump
Presence	Privilege Escalation	Exploit application vulnerability	open malicious file
Presence	Privilege Escalation	Exploit application vulnerability	software
Presence	Privilege Escalation	Exploit application vulnerability	application
Presence	Privilege Escalation	Exploit application vulnerability	buffer overflow
Presence	Privilege Escalation	Exploit application vulnerability	user interaction
Presence	Privilege Escalation	Exploit application vulnerability	insider threat
Presence	Privilege Escalation	Exploit application vulnerability	CVE
Presence	Privilege Escalation	Exploit application vulnerability	webmail
Presence	Privilege Escalation	Exploit application vulnerability	web application
Presence	Privilege Escalation	Exploit application vulnerability	network traffic
Presence	Privilege Escalation	Exploit application vulnerability	XSS
Presence	Privilege Escalation	Exploit application vulnerability	CSRF
Presence	Privilege Escalation	Exploit application vulnerability	code execution
Presence	Privilege Escalation	Exploit application vulnerability	command execution
Presence	Privilege Escalation	Exploit application vulnerability	escalate current process
Presence	Privilege Escalation	Exploit application vulnerability	higher privilege
Presence	Privilege Escalation	Exploit application vulnerability	bypass security mechanism
Presence	Privilege Escalation	Exploit application vulnerability	AppCert DLLs
Presence	Privilege Escalation	Exploit application vulnerability	AppInit DLLs
Presence	Privilege Escalation	Exploit application vulnerability	exploitation for privilege escalation
Presence	Privilege Escalation	Exploit application vulnerability	web shell
Presence	Privilege Escalation	Exploit application vulnerability	webshell
Presence	Privilege Escalation	Exploit firmware vulnerability	firmware
Presence	Privilege Escalation	Exploit firmware vulnerability	embedded device
Presence	Privilege Escalation	Exploit firmware vulnerability	embedded software
Presence	Privilege Escalation	Exploit firmware vulnerability	IoT device
Presence	Privilege Escalation	Exploit firmware vulnerability	CVE
Presence	Privilege Escalation	Exploit firmware vulnerability	exploitation for privilege escalation
Presence	Privilege Escalation	Exploit OS vulnerability	application shimming
Presence	Privilege Escalation	Exploit OS vulnerability	operating system
Presence	Privilege Escalation	Exploit OS vulnerability	os vulnerability
Presence	Privilege Escalation	Exploit OS vulnerability	CVE
Presence	Privilege Escalation	Exploit OS vulnerability	protocol implementation
Presence	Privilege Escalation	Exploit OS vulnerability	code execution
Presence	Privilege Escalation	Exploit OS vulnerability	command execution
Presence	Privilege Escalation	Exploit OS vulnerability	escalate current process
Presence	Privilege Escalation	Exploit OS vulnerability	higher privilege
Presence	Privilege Escalation	Exploit OS vulnerability	bypass security mechanism

Presence	Privilege Escalation	Exploit OS vulnerability	domain user permissions
Presence	Privilege Escalation	Exploit OS vulnerability	exploitation for privilege escalation
Presence	Privilege Escalation	Exploit OS vulnerability	extra window memory injection
Presence	Privilege Escalation	Exploit OS vulnerability	file system permissions weakness
Presence	Privilege Escalation	Exploit OS vulnerability	launch daemon
Presence	Privilege Escalation	Exploit OS vulnerability	local port monitor
Presence	Privilege Escalation	Exploit OS vulnerability	new service
Presence	Privilege Escalation	Exploit OS vulnerability	path interception
Presence	Privilege Escalation	Exploit OS vulnerability	plist modification
Presence	Privilege Escalation	Exploit OS vulnerability	port monitors
Presence	Privilege Escalation	Exploit OS vulnerability	service registry permissions weakness
Presence	Privilege Escalation	Exploit OS vulnerability	setuid and setgid
Presence	Privilege Escalation	Exploit OS vulnerability	SID-History injection
Presence	Privilege Escalation	Exploit OS vulnerability	startup items
Presence	Privilege Escalation	Exploit OS vulnerability	sudo caching
Presence	Privilege Escalation	Inject into running process	escalate privilege
Presence	Privilege Escalation	Inject into running process	rundlll32
Presence	Privilege Escalation	Inject into running process	process injection
Presence	Privilege Escalation	Inject into running process	code injection
Presence	Privilege Escalation	Inject into running process	context of another process
Presence	Privilege Escalation	Inject into running process	process memory
Presence	Privilege Escalation	Inject into running process	process permissions
Presence	Privilege Escalation	Inject into running process	DLL sideloading
Presence	Privilege Escalation	Inject into running process	tasklist
Presence	Privilege Escalation	Inject into running process	loader
Presence	Privilege Escalation	Inject into running process	DLL injection
Presence	Privilege Escalation	Inject into running process	process hollowing
Presence	Privilege Escalation	Inject into running process	DLL search order hijacking
Presence	Privilege Escalation	Inject into running process	dylib hijacking
Presence	Privilege Escalation	Inject into running process	hooking
Presence	Privilege Escalation	Inject into running process	image file execution options injection
Presence	Privilege Escalation	Use accessibility features	hot keys
Presence	Privilege Escalation	Use accessibility features	key combination
Presence	Privilege Escalation	Use accessibility features	launch accessibility programs
Presence	Privilege Escalation	Use accessibility features	command prompt
Presence	Privilege Escalation	Use accessibility features	backdoor
Presence	Privilege Escalation	Use accessibility features	shift key
Presence	Privilege Escalation	Use accessibility features	on screen keyboard
Presence	Privilege Escalation	Use accessibility features	mouse
Presence	Privilege Escalation	Use accessibility features	accessibility features
Presence	Privilege Escalation	Use legitimate credentials	legitimate access control
Presence	Privilege Escalation	Use legitimate credentials	compromised credentials
Presence	Privilege Escalation	Use legitimate credentials	Run as
Presence	Privilege Escalation	Use legitimate credentials	Psexec
Presence	Privilege Escalation	Use legitimate credentials	switch user
Presence	Privilege Escalation	Use legitimate credentials	higher privilege
Presence	Privilege Escalation	Use legitimate credentials	access restricted area
Presence	Privilege Escalation	Use legitimate credentials	access token manipulation
Presence	Privilege Escalation	Use legitimate credentials	bypass user access control
Presence	Privilege Escalation	Use legitimate credentials	sudo
Presence	Privilege Escalation	Use legitimate credentials	su root

Presence	Privilege Escalation	Use legitimate credentials	su -
Presence	Privilege Escalation	Use legitimate credentials	valid accounts
Presence	Privilege Escalation	Use legitimate credentials	authentication package
Presence	Credential Access	Add or modify credentials	change credentials
Presence	Credential Access	Add or modify credentials	create account
Presence	Credential Access	Add or modify credentials	modify account
Presence	Credential Access	Add or modify credentials	modify permission
Presence	Credential Access	Add or modify credentials	add permission group
Presence	Credential Access	Add or modify credentials	change permission group
Presence	Credential Access	Add or modify credentials	domain permission
Presence	Credential Access	Add or modify credentials	account manipulation
Presence	Credential Access	Add or modify credentials	LLMNR/NBT-NS poisoning
Presence	Credential Access	Add or modify credentials	exploitation for privilege escalation
Presence	Credential Access	Conduct social engineering	social engineering
Presence	Credential Access	Conduct social engineering	manipulate people
Presence	Credential Access	Conduct social engineering	entice a user to view
Presence	Credential Access	Conduct social engineering	UAC prompt
Presence	Credential Access	Conduct social engineering	credential pharming
Presence	Credential Access	Conduct social engineering	pharming
Presence	Credential Access	Conduct social engineering	direct to credential pharming site
Presence	Credential Access	Conduct social engineering	credentials from user
Presence	Credential Access	Conduct social engineering	enabled by user
Presence	Credential Access	Conduct social engineering	forced authentication
Presence	Credential Access	Conduct social engineering	input prompt
Presence	Credential Access	Crack passwords	password cracking
Presence	Credential Access	Crack passwords	password recovery
Presence	Credential Access	Crack passwords	rainbow table
Presence	Credential Access	Crack passwords	password spraying
Presence	Credential Access	Crack passwords	guess password
Presence	Credential Access	Crack passwords	compute hash
Presence	Credential Access	Crack passwords	brute force
Presence	Credential Access	Crack passwords	guess successful logins
Presence	Credential Access	Crack passwords	hash table
Presence	Credential Access	Crack passwords	known password
Presence	Credential Access	Crack passwords	possible password
Presence	Credential Access	Crack passwords	common passwords
Presence	Credential Access	Crack passwords	crack hash
Presence	Credential Access	Crack passwords	kerberoasting
Presence	Credential Access	Crack passwords	cracking
Presence	Credential Access	Crack passwords	dictionary attack
Presence	Credential Access	Dump credentials	credential dumping
Presence	Credential Access	Dump credentials	extract credential hash
Presence	Credential Access	Dump credentials	extract plaintext password
Presence	Credential Access	Dump credentials	find kerberos ticket
Presence	Credential Access	Dump credentials	memory dump
Presence	Credential Access	Dump credentials	password dumping
Presence	Credential Access	Dump credentials	extract passwords
Presence	Credential Access	Dump credentials	LSASS
Presence	Credential Access	Dump credentials	local security authority subsystem service
Presence	Credential Access	Dump credentials	access virtual memory
Presence	Credential Access	Dump credentials	password filter DLL

Presence	Credential Access	Dump credentials	replication through removable media
Presence	Credential Access	Dump credentials	credential harvesting
Presence	Credential Access	Hijack active credential	malicious use of authenticated credentials
Presence	Credential Access	Hijack active credential	authentication token
Presence	Credential Access	Hijack active credential	hardware authentication token
Presence	Credential Access	Hijack active credential	in use by legitimate user
Presence	Credential Access	Hijack active credential	without user knowledge
Presence	Credential Access	Hijack active credential	hijack authenticated session
Presence	Credential Access	Hijack active credential	two-factor authentication interception
Presence	Credential Access	Locate credentials	search for credentials
Presence	Credential Access	Locate credentials	find credentials
Presence	Credential Access	Locate credentials	password file
Presence	Credential Access	Locate credentials	passwd
Presence	Credential Access	Locate credentials	shadow
Presence	Credential Access	Locate credentials	log with plaintext password
Presence	Credential Access	Locate credentials	shared credential store
Presence	Credential Access	Locate credentials	configuration files containing passwords
Presence	Credential Access	Locate credentials	source code with password
Presence	Credential Access	Locate credentials	extract from backup
Presence	Credential Access	Locate credentials	extract from saved virtual machine
Presence	Credential Access	Locate credentials	bash history
Presence	Credential Access	Locate credentials	credentials in file
Presence	Credential Access	Locate credentials	credentials in registry
Presence	Credential Access	Locate credentials	keychain
Presence	Credential Access	Locate credentials	private keys
Presence	Credential Access	Locate credentials	securityd memory
Presence	Credential Access	Log keystrokes	keylogger
Presence	Credential Access	Log keystrokes	record keystrokes
Presence	Credential Access	Log keystrokes	record keyboard events
Presence	Credential Access	Log keystrokes	keylogging
Presence	Credential Access	Log keystrokes	save keystrokes
Presence	Credential Access	Log keystrokes	input capture
Presence	Lateral Movement	Exploit peer connections	authentication agreement
Presence	Lateral Movement	Exploit peer connections	mesh network
Presence	Lateral Movement	Exploit peer connections	peer-to-peer
Presence	Lateral Movement	Exploit peer connections	domain trust relationships
Presence	Lateral Movement	Exploit peer connections	connected hosts
Presence	Lateral Movement	Exploit peer connections	maneuver
Presence	Lateral Movement	Exploit peer connections	expand within network
Presence	Lateral Movement	Logon remotely	logon
Presence	Lateral Movement	Logon remotely	interactive logon
Presence	Lateral Movement	Logon remotely	valid credentials
Presence	Lateral Movement	Logon remotely	remote host
Presence	Lateral Movement	Logon remotely	manual interaction
Presence	Lateral Movement	Logon remotely	successfully logged on
Presence	Lateral Movement	Logon remotely	logoff
Presence	Lateral Movement	Logon remotely	graphical user interface
Presence	Lateral Movement	Logon remotely	GUI
Presence	Lateral Movement	Logon remotely	VPN
Presence	Lateral Movement	Logon remotely	RDP
Presence	Lateral Movement	Logon remotely	remote desktop protocol

Presence	Lateral Movement	Logon remotely	command line interface
Presence	Lateral Movement	Logon remotely	CLI
Presence	Lateral Movement	Logon remotely	VNC
Presence	Lateral Movement	Logon remotely	telnet
Presence	Lateral Movement	Logon remotely	ssh
Presence	Lateral Movement	Logon remotely	remote desktop services
Presence	Lateral Movement	Logon remotely	windows terminal services
Presence	Lateral Movement	Logon remotely	applescript
Presence	Lateral Movement	Logon remotely	exploitation for privilege escalation
Presence	Lateral Movement	Pass the hash	pass the hash
Presence	Lateral Movement	Pass the hash	pass-the-hash
Presence	Lateral Movement	Pass the hash	PtH
Presence	Lateral Movement	Pass the hash	bypass authentication
Presence	Lateral Movement	Pass the hash	valid password hash
Presence	Lateral Movement	Pass the hash	no cleartext password
Presence	Lateral Movement	Pass the hash	captured hash
Presence	Lateral Movement	Pass the ticket	pass the ticket
Presence	Lateral Movement	Pass the ticket	pass-the-ticket
Presence	Lateral Movement	Pass the ticket	PtT
Presence	Lateral Movement	Pass the ticket	bypass authentication
Presence	Lateral Movement	Pass the ticket	valid Kerberos ticket
Presence	Lateral Movement	Pass the ticket	no cleartext password
Presence	Lateral Movement	Pass the ticket	generate ticket
Presence	Lateral Movement	Pass the ticket	captured ticket
Presence	Lateral Movement	Pass the ticket	golden ticket
Presence	Lateral Movement	Replicate through removable media	insider threat
Presence	Lateral Movement	Replicate through removable media	air-gapped network
Presence	Lateral Movement	Replicate through removable media	disconnected network
Presence	Lateral Movement	Replicate through removable media	copy to removable media
Presence	Lateral Movement	Replicate through removable media	autorun
Presence	Lateral Movement	Replicate through removable media	.ini
Presence	Lateral Movement	Replicate through removable media	modify executables on removable media
Presence	Lateral Movement	Replicate through removable media	copy malware from removable media
Presence	Lateral Movement	Replicate through removable media	USB drop
Presence	Lateral Movement	Replicate through removable media	close access
Presence	Lateral Movement	Replicate through removable media	replication through removable media
Presence	Lateral Movement	Taint shared content	shared network drive
Presence	Lateral Movement	Taint shared content	shared file
Presence	Lateral Movement	Taint shared content	add malicious programs
Presence	Lateral Movement	Taint shared content	embedded scripts
Presence	Lateral Movement	Taint shared content	add exploit to file
Presence	Lateral Movement	Taint shared content	peer-to-peer
Presence	Lateral Movement	Taint shared content	taint shared content
Presence	Lateral Movement	Use application-deployment software	application deployment software
Presence	Lateral Movement	Use application-deployment software	application deployment system
Presence	Lateral Movement	Use application-deployment software	deployment server
Presence	Lateral Movement	Use application-deployment software	system administrator action
Presence	Lateral Movement	Use application-deployment software	malicious update
Presence	Lateral Movement	Use application-deployment software	malicious patch
Presence	Lateral Movement	Use application-deployment software	HBSS
Presence	Lateral Movement	Use application-deployment software	admin tool

Presence	Lateral Movement	Use application-deployment software	administration tool
Presence	Lateral Movement	Use remote services	remote execution
Presence	Lateral Movement	Use remote services	legitimate credentials
Presence	Lateral Movement	Use remote services	remote administrative services
Presence	Lateral Movement	Use remote services	remote access
Presence	Lateral Movement	Use remote services	windows management instrumentation
Presence	Lateral Movement	Use remote services	WMI
Presence	Lateral Movement	Use remote services	wmic
Presence	Lateral Movement	Use remote services	windows remote management
Presence	Lateral Movement	Use remote services	WinRM
Presence	Lateral Movement	Use remote services	RPC
Presence	Lateral Movement	Use remote services	netbios
Presence	Lateral Movement	Use remote services	remote desktop services
Presence	Lateral Movement	Use remote services	mstsc
Presence	Lateral Movement	Use remote services	windows terminal services
Presence	Lateral Movement	Use remote services	mmc
Presence	Lateral Movement	Use remote services	Microsoft Management Console
Presence	Lateral Movement	Use remote services	powershell
Presence	Lateral Movement	Use remote services	implied trust
Presence	Lateral Movement	Use remote services	valid credentials
Presence	Lateral Movement	Use remote services	remote services
Presence	Lateral Movement	Use remote services	exploitation of remote services
Presence	Lateral Movement	Write to remote file shares	writing data to remote hosts via file shares
Presence	Lateral Movement	Write to remote file shares	remote file copy
Presence	Lateral Movement	Write to remote file shares	file hosting
Presence	Lateral Movement	Write to remote file shares	code execution
Presence	Lateral Movement	Write to remote file shares	overwrite files
Presence	Lateral Movement	Write to remote file shares	change configuration
Presence	Lateral Movement	Write to remote file shares	embed code
Presence	Lateral Movement	Write to remote file shares	hidden network shares
Presence	Lateral Movement	Write to remote file shares	admin shares
Presence	Lateral Movement	Write to remote file shares	windows admin shares
Presence	Lateral Movement	Write to remote file shares	C$
Presence	Lateral Movement	Write to remote file shares	ADMIN$
Presence	Lateral Movement	Write to remote file shares	IPC$
Presence	Lateral Movement	Write to remote file shares	logon script
Presence	Lateral Movement	Write to remote file shares	SMB
Presence	Lateral Movement	Write to remote file shares	CIFS
Presence	Lateral Movement	Write to remote file shares	NFS
Presence	Lateral Movement	Write to remote file shares	FTP
Presence	Lateral Movement	Write to remote file shares	TFTP
Presence	Lateral Movement	Write to remote file shares	move
Presence	Lateral Movement	Write to remote file shares	copy
Presence	Lateral Movement	Write to remote file shares	net.exe
Presence	Lateral Movement	Write to remote file shares	net use
Presence	Lateral Movement	Write to remote file shares	net time
Presence	Lateral Movement	Write to remote file shares	ssh
Presence	Lateral Movement	Write to remote file shares	mount
Presence	Lateral Movement	Write to remote file shares	psexec
Presence	Lateral Movement	Write to remote file shares	distributed component object model
Presence	Lateral Movement	Write to shared webroot	shared webroot

Presence	Lateral Movement	Write to shared webroot	malicious content on website
Presence	Lateral Movement	Write to shared webroot	web shell
Presence	Lateral Movement	Write to shared webroot	webshell
Presence	Lateral Movement	Write to shared webroot	open file share
Presence	Lateral Movement	Write to shared webroot	browse to content with a web browser
Presence	Lateral Movement	Write to shared webroot	execute content in browser
Presence	Lateral Movement	Write to shared webroot	web server process
Presence	Lateral Movement	Write to shared webroot	web server configuration
Presence	Lateral Movement	Write to shared webroot	transfer file
Presence	Lateral Movement	Write to shared webroot	run as current privilege
Presence	Persistence	Create new service	create service
Presence	Persistence	Create new service	start new service
Presence	Persistence	Create new service	modify registry
Presence	Persistence	Create new service	system permission
Presence	Persistence	Create new service	root permission
Presence	Persistence	Create new service	service-level privileges
Presence	Persistence	Create scheduled task	execute programs
Presence	Persistence	Create scheduled task	schedule
Presence	Persistence	Create scheduled task	at
Presence	Persistence	Create scheduled task	schtasks
Presence	Persistence	Create scheduled task	cron
Presence	Persistence	Create scheduled task	cronjob
Presence	Persistence	Edit boot record	master boot record
Presence	Persistence	Edit boot record	MBR
Presence	Persistence	Edit boot record	boot loader
Presence	Persistence	Edit boot record	raw access to the boot drive
Presence	Persistence	Edit boot record	overwrite MBR
Presence	Persistence	Edit boot record	modify MBR
Presence	Persistence	Edit boot record	bootkit
Presence	Persistence	Edit boot record	virtual boot record
Presence	Persistence	Edit boot record	VBR
Presence	Persistence	Edit boot record	partition table
Presence	Persistence	Edit file-type associations	open file in application
Presence	Persistence	Edit file-type associations	file extension
Presence	Persistence	Edit file-type associations	registry entry
Presence	Persistence	Edit file-type associations	file handler
Presence	Persistence	Edit file-type associations	set new program
Presence	Persistence	Edit file-type associations	change default file association
Presence	Persistence	Employ logon scripts	logon script
Presence	Persistence	Employ logon scripts	modify logon script
Presence	Persistence	Employ logon scripts	configure logon
Presence	Persistence	Employ logon scripts	logon event
Presence	Persistence	Leverage path-order execution	unquoted path
Presence	Persistence	Leverage path-order execution	path interception
Presence	Persistence	Leverage path-order execution	specially crafted path to execute
Presence	Persistence	Leverage path-order execution	misconfiguration of path environment variable
Presence	Persistence	Leverage path-order execution	path environment variable
Presence	Persistence	Leverage path-order execution	search order hijacking
Presence	Persistence	Leverage path-order execution	DLL search order hijacking
Presence	Persistence	Leverage path-order execution	dylib hijacking
Presence	Persistence	Leverage path-order execution	full program paths

Presence	Persistence	Leverage path-order execution	unspecified program path
Presence	Persistence	Modify BIOS	BIOS
Presence	Persistence	Modify BIOS	basic input output system
Presence	Persistence	Modify BIOS	unified extensible firmware interface
Presence	Persistence	Modify BIOS	UEFI
Presence	Persistence	Modify BIOS	redirect to a different partition
Presence	Persistence	Modify BIOS	replace BIOS
Presence	Persistence	Modify BIOS	replace UEFI
Presence	Persistence	Modify BIOS	insert code into the boot process
Presence	Persistence	Modify BIOS	bootkit
Presence	Persistence	Modify configuration to facilitate launch	change configuration
Presence	Persistence	Modify configuration to facilitate launch	change initialization script
Presence	Persistence	Modify configuration to facilitate launch	change default shell
Presence	Persistence	Modify configuration to facilitate launch	edit environment variables
Presence	Persistence	Modify configuration to facilitate launch	browser extenstions
Presence	Persistence	Modify configuration to facilitate launch	accessibility features
Presence	Persistence	Modify existing services	existing service
Presence	Persistence	Modify existing services	modify the registry
Presence	Persistence	Modify existing services	sc
Presence	Persistence	Modify existing services	regedit
Presence	Persistence	Modify existing services	run malicious binary
Presence	Persistence	Modify existing services	application shimming
Presence	Persistence	Modify existing services	change service
Presence	Persistence	Modify links	redirect link
Presence	Persistence	Modify links	link modification
Presence	Persistence	Modify links	edit link
Presence	Persistence	Modify links	create link
Presence	Persistence	Modify links	hard link
Presence	Persistence	Modify links	soft link
Presence	Persistence	Modify links	shortcut
Presence	Persistence	Modify links	symbolic link
Presence	Persistence	Modify links	execute program when shortcut is clicked
Presence	Persistence	Modify links	redirect to a different application
Presence	Persistence	Modify service configuration	alter load process
Presence	Persistence	Modify service configuration	service-related executables
Presence	Persistence	Modify service configuration	service-related libraries
Presence	Persistence	Modify service configuration	/etc
Presence	Persistence	Modify service configuration	/opt
Presence	Persistence	Modify service configuration	services run by the service manager
Presence	Persistence	Replace service binary	replace service executable
Presence	Persistence	Replace service binary	overwrite service executable
Presence	Persistence	Replace service binary	modifiable service executable
Presence	Persistence	Replace service binary	gain elevated privileges
Presence	Persistence	Replace service binary	non-standard service binary storage location
Presence	Persistence	Set to load at startup	automatically load and execute code
Presence	Persistence	Set to load at startup	autorun
Presence	Persistence	Set to load at startup	AddMonitor
Presence	Persistence	Set to load at startup	registry run keys
Presence	Persistence	Set to load at startup	WMI event subscriptions
Presence	Persistence	Set to load at startup	WinLogon Helper DLL
Presence	Persistence	Set to load at startup	AppInit

Presence	Persistence	Set to load at startup	AppInit DLLs
Presence	Persistence	Set to load at startup	AppCert DLLs
Presence	Persistence	Set to load at startup	DLLs
Presence	Persistence	Set to load at startup	modify default shell
Presence	Persistence	Set to load at startup	rc script
Presence	Persistence	Set to load at startup	LDPRELOAD
Presence	Persistence	Set to load at startup	bashrc
Presence	Persistence	Use library-search hijack	library search order
Presence	Persistence	Use library-search hijack	gain elevated privileges
Presence	Persistence	Use library-search hijack	ambiguously specify libraries
Presence	Persistence	Use library-search hijack	DLL
Presence	Persistence	Use library-search hijack	DLL pre-loading
Presence	Persistence	Use library-search hijack	modify how a program loads DLLs
Presence	Persistence	Use library-search hijack	.manifest
Presence	Persistence	Use library-search hijack	.local
Presence	Persistence	Use library-search hijack	side-loading
Presence	Persistence	Use library-search hijack	DLL sideloading
Presence	Persistence	Use library-search hijack	path hijacking
Effect	Monitor	Activate recording	record target environment
Effect	Monitor	Activate recording	capture audio
Effect	Monitor	Activate recording	audio capture
Effect	Monitor	Activate recording	capture video
Effect	Monitor	Activate recording	screen capture
Effect	Monitor	Activate recording	video capture
Effect	Monitor	Activate recording	hot mic
Effect	Monitor	Activate recording	hot camera
Effect	Monitor	Activate recording	record ambiant noise
Effect	Monitor	Collect passively	monitor email
Effect	Monitor	Collect passively	collect target information
Effect	Monitor	Collect passively	monitor documents
Effect	Monitor	Collect passively	monitor chat channels
Effect	Monitor	Collect passively	packet sniffing
Effect	Monitor	Collect passively	cleartext sniffing
Effect	Monitor	Collect passively	shoulder surfing
Effect	Monitor	Collect passively	automated collection
Effect	Monitor	Enable other operations	use as future infrastructure
Effect	Monitor	Enable other operations	maintain botnet
Effect	Monitor	Enable other operations	check operational status
Effect	Monitor	Enable other operations	create foothold
Effect	Monitor	Log keystrokes	keylogger
Effect	Monitor	Log keystrokes	record keystrokes
Effect	Monitor	Log keystrokes	record keyboard events
Effect	Monitor	Log keystrokes	keylogging
Effect	Monitor	Log keystrokes	save keystrokes
Effect	Monitor	Log keystrokes	input capture
Effect	Monitor	Maintain access	monitor access
Effect	Monitor	Maintain access	track access
Effect	Monitor	Maintain access	check access
Effect	Monitor	Maintain access	check health and status of tools
Effect	Monitor	Maintain access	check implants
Effect	Monitor	Take screen capture	screen grab

Effect	Monitor	Take screen capture	screenshot
Effect	Monitor	Take screen capture	screen capture
Effect	Monitor	Take screen capture	snip
Effect	Monitor	Take screen capture	print screen
Effect	Exfiltrate	Collect crosstalk	crosstalk
Effect	Exfiltrate	Collect crosstalk	electromagnetic interference
Effect	Exfiltrate	Collect crosstalk	twisted pair
Effect	Exfiltrate	Collect crosstalk	emanations
Effect	Exfiltrate	Collect crosstalk	audio signals
Effect	Exfiltrate	Collect crosstalk	video signals
Effect	Exfiltrate	Collect crosstalk	emanation
Effect	Exfiltrate	Collect crosstalk	emanate
Effect	Exfiltrate	Collect from local system	local host file system
Effect	Exfiltrate	Collect from local system	local processes
Effect	Exfiltrate	Collect from local system	system configuration
Effect	Exfiltrate	Collect from local system	copy data
Effect	Exfiltrate	Collect from local system	copy file
Effect	Exfiltrate	Collect from local system	clone drive
Effect	Exfiltrate	Collect from local system	clipboard data
Effect	Exfiltrate	Collect from local system	clone system configuration
Effect	Exfiltrate	Collect from local system	data from local system
Effect	Exfiltrate	Collect from local system	data from removable media
Effect	Exfiltrate	Collect from local system	end-point collection
Effect	Exfiltrate	Collect from network resources	copy from shared drive
Effect	Exfiltrate	Collect from network resources	data from network shared drive
Effect	Exfiltrate	Collect from network resources	data from information repositories
Effect	Exfiltrate	Collect from network resources	clone shared drive
Effect	Exfiltrate	Collect from network resources	copy from file server
Effect	Exfiltrate	Collect from network resources	clone file server
Effect	Exfiltrate	Collect from network resources	copy from mail server
Effect	Exfiltrate	Collect from network resources	clone mail server
Effect	Exfiltrate	Collect from network resources	email collection
Effect	Exfiltrate	Collect from network resources	copy from web server
Effect	Exfiltrate	Collect from network resources	clone web server
Effect	Exfiltrate	Collect from network resources	man in the browser
Effect	Exfiltrate	Collect from network resources	copy from virtual machine
Effect	Exfiltrate	Collect from network resources	clone virtual machine
Effect	Exfiltrate	Collect from network resources	exfil over network resources
Effect	Exfiltrate	Collect from network resources	hosted resource
Effect	Exfiltrate	Collect from network resources	web-based email
Effect	Exfiltrate	Collect from network resources	cloud storage
Effect	Exfiltrate	Collect from network resources	hosted storage
Effect	Exfiltrate	Compress data	data compression
Effect	Exfiltrate	Compress data	compressed data
Effect	Exfiltrate	Compress data	data compressed
Effect	Exfiltrate	Compress data	deflate
Effect	Exfiltrate	Compress data	archive file
Effect	Exfiltrate	Compress data	makecab
Effect	Exfiltrate	Compress data	7zip
Effect	Exfiltrate	Compress data	gzip
Effect	Exfiltrate	Compress data	rar

Effect	Exfiltrate	Compress data	zip
Effect	Exfiltrate	Compress data	zlib
Effect	Exfiltrate	Compress data	compression algorithm
Effect	Exfiltrate	Compress data	encode data
Effect	Exfiltrate	Compress data	encoded
Effect	Exfiltrate	Disclose data or information	Release information to unauthorized user
Effect	Exfiltrate	Disclose data or information	release to a public website
Effect	Exfiltrate	Disclose data or information	change permissions to allow broad access
Effect	Exfiltrate	Disclose data or information	send to unauthorized user
Effect	Exfiltrate	Disclose data or information	shoulder surfing
Effect	Exfiltrate	Disclose data or information	data breach
Effect	Exfiltrate	Position data	gather files
Effect	Exfiltrate	Position data	store files to be exfiltrated
Effect	Exfiltrate	Position data	create directory
Effect	Exfiltrate	Position data	aggregate files
Effect	Exfiltrate	Position data	add files to archive
Effect	Exfiltrate	Position data	move files
Effect	Exfiltrate	Position data	staged data
Effect	Exfiltrate	Position data	data staged
Effect	Exfiltrate	Run collection script	automated search
Effect	Exfiltrate	Run collection script	automated processing
Effect	Exfiltrate	Run collection script	scripted collection
Effect	Exfiltrate	Run collection script	scripted search
Effect	Exfiltrate	Run collection script	automated exfiltration
Effect	Exfiltrate	Run collection script	scripted exfiltration
Effect	Exfiltrate	Send over C2 channel	data exfiltration
Effect	Exfiltrate	Send over C2 channel	use existing connection
Effect	Exfiltrate	Send over C2 channel	use C2 protocol
Effect	Exfiltrate	Send over C2 channel	use C2 channel
Effect	Exfiltrate	Send over C2 channel	exfiltration over command and control channel
Effect	Exfiltrate	Send over non-C2 channel	alternate data connection
Effect	Exfiltrate	Send over non-C2 channel	use different session
Effect	Exfiltrate	Send over non-C2 channel	use different connection
Effect	Exfiltrate	Send over non-C2 channel	use non-C2 protocol
Effect	Exfiltrate	Send over non-C2 channel	data exfiltration
Effect	Exfiltrate	Send over non-C2 channel	exfiltration over alternative protocol
Effect	Exfiltrate	Send over other network medium	alternate network connection
Effect	Exfiltrate	Send over other network medium	use different network medium
Effect	Exfiltrate	Send over other network medium	data exfiltration
Effect	Exfiltrate	Send over other network medium	backup network connection
Effect	Exfiltrate	Send over other network medium	exfiltration over other network medium
Effect	Exfiltrate	Throttle data	arrange data into smaller size
Effect	Exfiltrate	Throttle data	low and slow
Effect	Exfiltrate	Throttle data	limit transfer speed
Effect	Exfiltrate	Throttle data	slowing transfer
Effect	Exfiltrate	Throttle data	small packet size
Effect	Exfiltrate	Throttle data	avoid size limits
Effect	Exfiltrate	Throttle data	chunks of data
Effect	Exfiltrate	Throttle data	bandwidth monitoring
Effect	Exfiltrate	Throttle data	noise floor
Effect	Exfiltrate	Throttle data	packet flow

Effect	Exfiltrate	Throttle data	physical transfer constraints
Effect	Exfiltrate	Throttle data	chunked files
Effect	Exfiltrate	Throttle data	evade detection of exfiltration
Effect	Exfiltrate	Throttle data	data transfer size limits
Effect	Exfiltrate	Transfer via physical means	physical media
Effect	Exfiltrate	Transfer via physical means	lost device
Effect	Exfiltrate	Transfer via physical means	stolen device
Effect	Exfiltrate	Transfer via physical means	removed device
Effect	Exfiltrate	Transfer via physical means	hard copy
Effect	Exfiltrate	Transfer via physical means	printed papers
Effect	Exfiltrate	Transfer via physical means	external hard drive
Effect	Exfiltrate	Transfer via physical means	USB
Effect	Exfiltrate	Transfer via physical means	USB drive
Effect	Exfiltrate	Transfer via physical means	flash drive
Effect	Exfiltrate	Transfer via physical means	cellular phone
Effect	Exfiltrate	Transfer via physical means	MP3 player
Effect	Exfiltrate	Transfer via physical means	sneakernet
Effect	Exfiltrate	Transfer via physical means	send information to a remote printer
Effect	Exfiltrate	Transfer via physical means	exfiltration over physical medium
Effect	Exfiltrate	Traverse CDS or MLS	automated transport services
Effect	Exfiltrate	Traverse CDS or MLS	cross domain solution
Effect	Exfiltrate	Traverse CDS or MLS	multi-level solution
Effect	Exfiltrate	Traverse CDS or MLS	network guard
Effect	Exfiltrate	Traverse CDS or MLS	trusted services
Effect	Exfiltrate	Traverse CDS or MLS	misconfigured CDS
Effect	Exfiltrate	Traverse CDS or MLS	misconfigured MLS
Effect	Exfiltrate	Traverse CDS or MLS	high-to-low
Effect	Exfiltrate	Traverse CDS or MLS	pathway
Effect	Exfiltrate	Traverse CDS or MLS	insider threat
Effect	Exfiltrate	Traverse CDS or MLS	compromise trusted services
Effect	Modify	Alter data	change data
Effect	Modify	Alter data	modify access control
Effect	Modify	Alter data	modify privilege
Effect	Modify	Alter data	change data in databases
Effect	Modify	Alter data	change data in files
Effect	Modify	Alter data	modify status shown in dashboards
Effect	Modify	Alter data	alteration
Effect	Modify	Alter process outcomes	change process
Effect	Modify	Alter process outcomes	hijack process
Effect	Modify	Alter process outcomes	filter process input
Effect	Modify	Alter process outcomes	filter process output
Effect	Modify	Alter process outcomes	modify process input
Effect	Modify	Alter process outcomes	modify process output
Effect	Modify	Cause physical effects	physical change
Effect	Modify	Cause physical effects	equipment malfunction
Effect	Modify	Cause physical effects	power loss
Effect	Modify	Change machine-to-machine communications	alter communications processes
Effect	Modify	Change machine-to-machine communications	route poisoning
Effect	Modify	Change machine-to-machine communications	protocol downgrade
Effect	Modify	Change machine-to-machine communications	filter traffic
Effect	Modify	Change machine-to-machine communications	dropping router traffic

Effect	Modify	Change run-state of system processes	alter process state
Effect	Modify	Change run-state of system processes	change access controls
Effect	Modify	Change run-state of system processes	change privileges
Effect	Modify	Change run-state of system processes	restart process
Effect	Modify	Change run-state of system processes	halt process
Effect	Modify	Change run-state of system processes	SIGKILL
Effect	Modify	Change run-state of system processes	taskkill
Effect	Modify	Change run-state of system processes	running process
Effect	Modify	Change run-state of system processes	suspended process
Effect	Modify	Change run-state of system processes	stop process
Effect	Modify	Deface websites	change visual appearance
Effect	Modify	Deface websites	add content to webpage
Effect	Modify	Deface websites	modify function of website
Effect	Modify	Defeat encryption	exploit weak cryptographic implementation
Effect	Modify	Defeat encryption	exploit misconfigured crypto
Effect	Modify	Defeat encryption	modify encryption configuration
Effect	Modify	Defeat encryption	use aquired cryptographic key
Effect	Modify	Defeat encryption	crypto
Effect	Modify	Defeat encryption	manipulate unencrypted content
Effect	Modify	Defeat encryption	downgrade SSL version
Effect	Modify	Defeat encryption	force misconfiguration of encryption scheme
Effect	Modify	Defeat encryption	dictionary attack
Effect	Modify	Defeat encryption	rainbow attack
Effect	Modify	Defeat encryption	plain-text attack
Effect	Modify	Defeat encryption	decrypt
Effect	Modify	Defeat encryption	decryption
Effect	Modify	Defeat encryption	side channel attack
Effect	Deny	Corrupt files or applications	render files or applications unusable
Effect	Deny	Corrupt files or applications	munge file headers
Effect	Deny	Corrupt files or applications	delete portions of application files
Effect	Deny	Corrupt files or applications	flip bits of data files to make them unusable
Effect	Deny	Corrupt files or applications	bit flip
Effect	Deny	Degrade	decrease throughput
Effect	Deny	Degrade	increase latency
Effect	Deny	Degrade	decrease capability for a period of time
Effect	Deny	Degrade	decrease capability to some degree
Effect	Deny	Degrade	degrade communications
Effect	Deny	Disrupt or denial of service	dos
Effect	Deny	Disrupt or denial of service	service disruption
Effect	Deny	Disrupt or denial of service	SYN flood
Effect	Deny	Disrupt or denial of service	flooding
Effect	Deny	Disrupt or denial of service	disable network services on a host
Effect	Deny	Disrupt or denial of service	overwhelming volume of connection requests
Effect	Deny	Disrupt or denial of service	smurf attack
Effect	Deny	Disrupt or denial of service	reflection attack
Effect	Deny	Disrupt or denial of service	ddos
Effect	Deny	Disrupt or denial of service	amplification attack
Effect	Deny	Disrupt or denial of service	multiple systems overwhelm a targeted victim
Effect	Deny	Disrupt or denial of service	flooding
Effect	Deny	Disrupt or denial of service	use botnet to overwhelm victim
Effect	Deny	Disrupt or denial of service	coordinated denial of service

Effect	Deny	Encrypt data to render unusable	encrypt file system
Effect	Deny	Encrypt data to render unusable	ransomware
Effect	Deny	Encrypt data to render unusable	unknown key
Effect	Deny	Encrypt data to render unusable	bulk encrypt
Effect	Destroy	Brick disk or OS (full delete)	delete critical components of OS
Effect	Destroy	Brick disk or OS (full delete)	overwrite OS
Effect	Destroy	Brick disk or OS (full delete)	delete OS
Effect	Destroy	Brick disk or OS (full delete)	delete BIOS
Effect	Destroy	Brick disk or OS (full delete)	bricking
Effect	Destroy	Corrupt disk or OS (partial delete)	disk corruption
Effect	Destroy	Corrupt disk or OS (partial delete)	delete some components of OS
Effect	Destroy	Corrupt disk or OS (partial delete)	overwrite some components of OS
Effect	Destroy	Corrupt disk or OS (partial delete)	partially recoverable
Effect	Destroy	Corrupt disk or OS (partial delete)	partially delete
Effect	Destroy	Delete data	data deletion
Effect	Destroy	Delete data	wipe hard drive
Effect	Destroy	Delete data	delete hard drive
Effect	Destroy	Delete data	data clearing
Effect	Destroy	Delete data	data-deletion attack
Effect	Destroy	Delete data	data erasure
Effect	Destroy	Delete data	data wiping
Effect	Destroy	Delete data	wipe data
Effect	Destroy	Delete data	data loss
Effect	Destroy	Delete data	erasure
Effect	Destroy	Destroy hardware	destruction
Effect	Destroy	Destroy hardware	damage hardware
Effect	Destroy	Destroy hardware	corrupt firmware
Effect	Destroy	Destroy hardware	overwrite firmware
Effect	Destroy	Destroy hardware	wipe firmware
Effect	Destroy	Destroy hardware	wipe system
Effect	Destroy	Destroy hardware	permanent loss
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	unused infrastructure
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	unallocate infrastructure
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	assign domains to null IP address
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	not renew leased domain
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	not renew leased infrastructure
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	public exposure
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	anonymity concern
AEF	Analysis, Evaluation, and Feedback	Abandon infrastructure	burn infrastructure
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	assess operations
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	update infrastructure
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	change course of action
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	validate capabilities
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	reset objectives
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	trend analysis
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	analyze trends
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	review outcomes
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	measure success
AEF	Analysis, Evaluation, and Feedback	Conduct effects assessments	damage assessment
AEF	Analysis, Evaluation, and Feedback	Refine potential victims	update target list
AEF	Analysis, Evaluation, and Feedback	Refine potential victims	validate targets

AEF	Analysis, Evaluation, and Feedback	Refine potential victims	start new operations
AEF	Analysis, Evaluation, and Feedback	Refine potential victims	learn from previous operations
AEF	Analysis, Evaluation, and Feedback	Refine potential victims	shift targets
AEF	Analysis, Evaluation, and Feedback	Refine potential victims	identify new targets
AEF	Analysis, Evaluation, and Feedback	Refine potential victims	remove target
C2	Command and Control	Beacon to midpoints	beaconing
C2	Command and Control	Beacon to midpoints	periodic packet
C2	Command and Control	Beacon to midpoints	send packet to mid-point
C2	Command and Control	Beacon to midpoints	send message to C2 infrastructure
C2	Command and Control	Beacon to midpoints	send to C2
C2	Command and Control	Beacon to midpoints	communicate with controller
C2	Command and Control	Beacon to midpoints	send packet on demand
C2	Command and Control	Beacon to midpoints	beacons to
C2	Command and Control	Beacon to midpoints	beaconed
C2	Command and Control	Beacon to midpoints	callback
C2	Command and Control	Beacon to midpoints	call back
C2	Command and Control	Beacon to midpoints	calls back
C2	Command and Control	Beacon to midpoints	keep alive beaconing
C2	Command and Control	Beacon to midpoints	beacon out
C2	Command and Control	Beacon to midpoints	beacon payload
C2	Command and Control	Beacon to midpoints	keep-alive beacon
C2	Command and Control	Establish peer network	create proxy network
C2	Command and Control	Establish peer network	peer-to-peer
C2	Command and Control	Establish peer network	peer to peer
C2	Command and Control	Establish peer network	mesh network
C2	Command and Control	Establish peer network	entry node
C2	Command and Control	Establish peer network	exit node
C2	Command and Control	Establish peer network	.onion
C2	Command and Control	Establish peer network	trusted network relationship
C2	Command and Control	Relay communications	transmit through network
C2	Command and Control	Relay communications	connection proxy
C2	Command and Control	Relay communications	proxy
C2	Command and Control	Relay communications	port redirect
C2	Command and Control	Relay communications	stunnel
C2	Command and Control	Relay communications	netcat
C2	Command and Control	Relay communications	custom code
C2	Command and Control	Relay communications	SSH tunneling
C2	Command and Control	Relay communications	tunneling
C2	Command and Control	Relay communications	tunnel
C2	Command and Control	Relay communications	VPN
C2	Command and Control	Relay communications	GRE tunnel
C2	Command and Control	Relay communications	PPTP
C2	Command and Control	Relay communications	L2TP
C2	Command and Control	Relay communications	modify route
C2	Command and Control	Send commands	issue command
C2	Command and Control	Send commands	controller to implant
C2	Command and Control	Send commands	controller send command
C2	Command and Control	Send commands	remote access tool
C2	Command and Control	Send commands	RAT
C2	Command and Control	Send commands	send packet
C2	Command and Control	Send commands	execute command

C2	Command and Control	Use botnet	send commands to botnet
C2	Command and Control	Use botnet	bot herder
C2	Command and Control	Use botnet	IP addresses used by the botnet
C2	Command and Control	Use botnet	botnet command and control
C2	Command and Control	Use botnet	botnet C2
C2	Command and Control	Use chained protocols	protocol chaining
C2	Command and Control	Use chained protocols	multi-hop proxy
C2	Command and Control	Use chained protocols	mulitple protocols
C2	Command and Control	Use chained protocols	protocol encapsulation
C2	Command and Control	Use peer connections	use proxy network
C2	Command and Control	Use peer connections	send to peer
C2	Command and Control	Use peer connections	peer-to-peer
C2	Command and Control	Use peer connections	peer to peer
C2	Command and Control	Use peer connections	connect to peer
C2	Command and Control	Use peer connections	multi-hop proxy
C2	Command and Control	Use remote shell	powershell
C2	Command and Control	Use remote shell	cmd.exe
C2	Command and Control	Use remote shell	bash
C2	Command and Control	Use remote shell	tcsh
C2	Command and Control	Use remote shell	ksh
C2	Command and Control	Use remote shell	csh
C2	Command and Control	Use remote shell	sh
C2	Command and Control	Use remote shell	/dev/tcp
C2	Command and Control	Use remote shell	reverse shell
C2	Command and Control	Use remote shell	remote access tools
C2	Command and Control	Use remote shell	network socket
C2	Command and Control	Use removable media	spread commands
C2	Command and Control	Use removable media	communication through removable media
C2	Command and Control	Use removable media	Use USB to perform commands
C2	Command and Control	Use removable media	run commands from USB
C2	Command and Control	Use removable media	autorun
Evasion	Evasion	Access raw disk	direct drive access
Evasion	Evasion	Access raw disk	read and write files directly
Evasion	Evasion	Access raw disk	covert storage on disk
Evasion	Evasion	Avoid data-size limits	chunks of data
Evasion	Evasion	Avoid data-size limits	process data on host
Evasion	Evasion	Avoid data-size limits	low and slow
Evasion	Evasion	Avoid data-size limits	avoid size limits
Evasion	Evasion	Avoid data-size limits	compress file size
Evasion	Evasion	Avoid data-size limits	chunked
Evasion	Evasion	Avoid data-size limits	dechunked
Evasion	Evasion	Avoid data-size limits	split
Evasion	Evasion	Block indicators on host	indicators of host activity leaving the host
Evasion	Evasion	Block indicators on host	indicator blocking
Evasion	Evasion	Block indicators on host	indicator removal on tools
Evasion	Evasion	Block indicators on host	indicator removal on host
Evasion	Evasion	Block indicators on host	block traffic associated with reporting
Evasion	Evasion	Block indicators on host	stop local process
Evasion	Evasion	Block indicators on host	create host-based firewall rule
Evasion	Evasion	Block indicators on host	block traffic to server
Evasion	Evasion	Block indicators on host	prevent GUI window creation

Evasion	Evasion	Block indicators on host	block pop-up
Evasion	Evasion	Block indicators on host	disable pop-up
Evasion	Evasion	Degrade security products	disable security product
Evasion	Evasion	Degrade security products	disabling security tools
Evasion	Evasion	Degrade security products	disrupt security product
Evasion	Evasion	Degrade security products	avoid detection
Evasion	Evasion	Degrade security products	enable security product
Evasion	Evasion	Degrade security products	disable logging
Evasion	Evasion	Degrade security products	enable logging
Evasion	Evasion	Degrade security products	alter signature store
Evasion	Evasion	Degrade security products	alter signature hashes
Evasion	Evasion	Degrade security products	alter signature repository
Evasion	Evasion	Degrade security products	delete registry key for security tools
Evasion	Evasion	Degrade security products	stop security product
Evasion	Evasion	Degrade security products	start security product
Evasion	Evasion	Delay activity	time delay
Evasion	Evasion	Delay activity	sleep timers
Evasion	Evasion	Delay activity	wait for user
Evasion	Evasion	Delay activity	wait for user activity
Evasion	Evasion	Delay activity	delay execution
Evasion	Evasion	Delay activity	random execution
Evasion	Evasion	Employ anti-forensics measures	make forensic analysis difficult
Evasion	Evasion	Employ anti-forensics measures	set timestamps to match system files
Evasion	Evasion	Employ anti-forensics measures	alter timestamp
Evasion	Evasion	Employ anti-forensics measures	modify timestamp
Evasion	Evasion	Employ anti-forensics measures	clean cache
Evasion	Evasion	Employ anti-forensics measures	clean registry
Evasion	Evasion	Employ anti-forensics measures	destroy log
Evasion	Evasion	Employ anti-forensics measures	clear log
Evasion	Evasion	Employ anti-forensics measures	alter log
Evasion	Evasion	Employ anti-forensics measures	timestomp
Evasion	Evasion	Employ anti-forensics measures	hidden files and directories
Evasion	Evasion	Employ anti-forensics measures	file deletion
Evasion	Evasion	Employ anti-forensics measures	network share connection removal
Evasion	Evasion	Employ anti-reverse-engineering measures	evade reverse engineering
Evasion	Evasion	Employ anti-reverse-engineering measures	API imports
Evasion	Evasion	Employ anti-reverse-engineering measures	dynamic API import resolution
Evasion	Evasion	Employ anti-reverse-engineering measures	overlapping instructions
Evasion	Evasion	Employ anti-reverse-engineering measures	stack manipulation
Evasion	Evasion	Employ anti-reverse-engineering measures	get tick count
Evasion	Evasion	Employ anti-reverse-engineering measures	script obfuscation
Evasion	Evasion	Employ anti-reverse-engineering measures	anti-stack backtracing
Evasion	Evasion	Employ anti-reverse-engineering measures	string munging
Evasion	Evasion	Employ anti-reverse-engineering measures	trampoline
Evasion	Evasion	Employ anti-reverse-engineering measures	avoid installation
Evasion	Evasion	Employ anti-reverse-engineering measures	check for debuggers
Evasion	Evasion	Employ anti-reverse-engineering measures	software packing
Evasion	Evasion	Employ anti-reverse-engineering measures	code signing
Evasion	Evasion	Employ anti-reverse-engineering measures	obscure code execution flow
Evasion	Evasion	Employ anti-reverse-engineering measures	exception handling
Evasion	Evasion	Employ rootkit	install rootkit

Evasion	Evasion	Employ rootkit	rootkit
Evasion	Evasion	Employ rootkit	modify OS API calls
Evasion	Evasion	Employ rootkit	hooking API
Evasion	Evasion	Employ rootkit	intercept API
Evasion	Evasion	Employ rootkit	SSDT
Evasion	Evasion	Employ rootkit	kernel module
Evasion	Evasion	Employ rootkit	kernel driver
Evasion	Evasion	Employ rootkit	stealth
Evasion	Evasion	Employ rootkit	subvert kernel
Evasion	Evasion	Employ rootkit	non-modular code
Evasion	Evasion	Employ rootkit	user level
Evasion	Evasion	Employ rootkit	kernel level
Evasion	Evasion	Employ rootkit	hypervisor rootkit
Evasion	Evasion	Employ rootkit	hide existence of malware
Evasion	Evasion	Encode data	converting data
Evasion	Evasion	Encode data	encoding
Evasion	Evasion	Encode data	encoded data
Evasion	Evasion	Encode data	data encoding
Evasion	Evasion	Encode data	compiled data
Evasion	Evasion	Encode data	compressed data
Evasion	Evasion	Encode data	convert file
Evasion	Evasion	Encode data	file conversion
Evasion	Evasion	Encode data	data conversion
Evasion	Evasion	Encode data	base64
Evasion	Evasion	Encode data	encapsulate
Evasion	Evasion	Encode data	encapsulation
Evasion	Evasion	Encode data	uuencode
Evasion	Evasion	Encode data	uudecode
Evasion	Evasion	Encrypt data	algorithm
Evasion	Evasion	Encrypt data	encrypted data
Evasion	Evasion	Encrypt data	data encrypted
Evasion	Evasion	Encrypt data	data at rest
Evasion	Evasion	Encrypt data	data in transit
Evasion	Evasion	Encrypt data	RC4
Evasion	Evasion	Encrypt data	PGP
Evasion	Evasion	Encrypt data	decoder
Evasion	Evasion	Encrypt data	private key
Evasion	Evasion	Encrypt data	public key
Evasion	Evasion	Encrypt data	digital signature
Evasion	Evasion	Encrypt data	PKI
Evasion	Evasion	Encrypt data	encryption scheme
Evasion	Evasion	Encrypt data	encrypted protocol
Evasion	Evasion	Encrypt data	HTTPS
Evasion	Evasion	Encrypt data	SFTP
Evasion	Evasion	Encrypt data	encryption
Evasion	Evasion	Impersonate legitimate file	save file in a commonly trusted location
Evasion	Evasion	Impersonate legitimate file	process doppleganging
Evasion	Evasion	Impersonate legitimate file	commonly trusted location
Evasion	Evasion	Impersonate legitimate file	use common name
Evasion	Evasion	Impersonate legitimate file	benign name
Evasion	Evasion	Manipulate trusted process	inject into a trusted process

Evasion	Evasion	Manipulate trusted process	bypass user account control
Evasion	Evasion	Manipulate trusted process	component object model hijacking
Evasion	Evasion	Mimic legitimate traffic	mimic legitimate
Evasion	Evasion	Mimic legitimate traffic	blend in with existing traffic
Evasion	Evasion	Mimic legitimate traffic	standard protocols
Evasion	Evasion	Mimic legitimate traffic	standard ports
Evasion	Evasion	Mimic legitimate traffic	similar volume
Evasion	Evasion	Mimic legitimate traffic	mimic frequency
Evasion	Evasion	Mimic legitimate traffic	source and destination
Evasion	Evasion	Modify malware to avoid detection	change malware
Evasion	Evasion	Modify malware to avoid detection	update malware
Evasion	Evasion	Modify malware to avoid detection	binary padding
Evasion	Evasion	Modify malware to avoid detection	increase executable size
Evasion	Evasion	Modify malware to avoid detection	change MD5
Evasion	Evasion	Modify malware to avoid detection	modify file hash
Evasion	Evasion	Modify malware to avoid detection	recompile
Evasion	Evasion	Modify malware to avoid detection	software packing
Evasion	Evasion	Obfuscate data	replace contents
Evasion	Evasion	Obfuscate data	overlapping instructions
Evasion	Evasion	Obfuscate data	conceal contents
Evasion	Evasion	Obfuscate data	dynamic obfuscation
Evasion	Evasion	Obfuscate data	data obfuscation
Evasion	Evasion	Obfuscate data	obfuscated files or information
Evasion	Evasion	Obfuscate data	deobfuscate/decode files or information
Evasion	Evasion	Obfuscate data	steganography
Evasion	Evasion	Remove logged data	modify log
Evasion	Evasion	Remove logged data	alter log
Evasion	Evasion	Remove logged data	replace log
Evasion	Evasion	Remove logged data	delete log
Evasion	Evasion	Remove logged data	file deletion
Evasion	Evasion	Remove logged data	destroy log
Evasion	Evasion	Remove logged data	clear log
Evasion	Evasion	Remove toolkit	remove tools
Evasion	Evasion	Remove toolkit	delete tools
Evasion	Evasion	Remove toolkit	file deletion
Evasion	Evasion	Remove toolkit	DEL
Evasion	Evasion	Remove toolkit	sysinternals sdelete
Evasion	Evasion	Remove toolkit	file deletion tool
Evasion	Evasion	Remove toolkit	clean-up
Evasion	Evasion	Remove toolkit	cleanup
Evasion	Evasion	Remove toolkit	cover tracks
Evasion	Evasion	Sign malicious content	X.509
Evasion	Evasion	Sign malicious content	code signing
Evasion	Evasion	Sign malicious content	stolen certificate
Evasion	Evasion	Sign malicious content	self-generated key
Evasion	Evasion	Sign malicious content	compromised certificate
Evasion	Evasion	Sign malicious content	forged certificate
Evasion	Evasion	Sign malicious content	self-signed
Evasion	Evasion	Store files in unconventional location	file system metadata
Evasion	Evasion	Store files in unconventional location	extended attributes in NTFS
Evasion	Evasion	Store files in unconventional location	NTFS file attributes

Evasion	Evasion	Store files in unconventional location	slack space
Evasion	Evasion	Store files in unconventional location	registry
Evasion	Evasion	Store files in unconventional location	blob
Evasion	Evasion	Store files in unconventional location	registry key
Evasion	Evasion	Store files in unconventional location	files in registry
Evasion	Evasion	Store files in unconventional location	outside logical partition
Evasion	Evasion	Store files in unconventional location	alternate data streams
Evasion	Evasion	Store files in unconventional location	temp
Evasion	Evasion	Tailor behavior to environment	detect environment
Evasion	Evasion	Tailor behavior to environment	detect sandbox
Evasion	Evasion	Tailor behavior to environment	detect VM
Evasion	Evasion	Tailor behavior to environment	adjust behavior
Evasion	Evasion	Use signed content	X.509
Evasion	Evasion	Use signed content	legitimate signed software
Evasion	Evasion	Use signed content	vulnerable drivers
Evasion	Evasion	Use signed content	signed content for malicious

Appendix B. References and License Information

MITRE

Portions of the "NSA/CSS Technical Cyber Threat Framework" were derived from the MITRE ATT&CK™ threat model framework and MITRE ATT&CK Matrix™ (https://attack.mitre.org). Copyright ©2016, The MITRE Corporation. ATT&CK and ATT&CK Matrix are trademarks of The MITRE Corporation.

LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

Office of the Director of National Intelligence (ODNI)

The ODNI Cyber Threat Framework (CTF) was developed by the US Government to enable consistent categorization and characterization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. This framework can be found at https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework_Overview.pdf.