Collection, Tactic TA0009 - Enterprise

Archived: 2026-04-05 15:26:56 UTC

T1557 Adversary-in-the-Middle Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions. .001 LLMNR/NBT-NS Poisoning and SMB Relay By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials. .002 ARP Cache Poisoning Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. .003 DHCP Spoofing Adversaries may redirect network traffic to adversary-owned systems by spoofing Dynamic Host Configuration Protocol (DHCP) traffic and acting as a malicious DHCP server on the victim network. By achieving the adversary-in-the-middle (AiTM) position, adversaries may collect network communications, including passed credentials, especially those sent over insecure, unencrypted protocols. This may also enable follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. .004 Evil Twin Adversaries may host seemingly genuine Wi-Fi access points to deceive users into connecting to malicious networks as a way of supporting follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or Input Capture. T1560 Archive Collected Data An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. .001 Archive via Utility Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport. .002 Archive via Library An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party libraries. Many libraries exist that can archive data, including Python rarfile , libzip , and zlib . Most libraries include functionality to encrypt and/or compress data. .003 Archive via Custom Method An adversary may compress or encrypt data that is collected prior to exfiltration using a custom method. Adversaries may choose to use custom archival methods, such as encryption with XOR or stream ciphers implemented with no external library or utility references. Custom implementations of well-known compression algorithms have also been used. T1123 Audio Capture An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. T1119 Automated Collection Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a Command and Scripting Interpreter to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. T1185 Browser Session Hijacking Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to

change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques. T1115 Clipboard Data Adversaries may collect data stored in the clipboard from users copying information within or between applications. T1530 Data from Cloud Storage Adversaries may access data from cloud storage. T1602 Data from Configuration Repository Adversaries may collect data related to managed devices from configuration repositories. Configuration repositories are used by management systems in order to configure, manage, and control data on remote systems. Configuration repositories may also facilitate remote access and administration of devices. .001 SNMP (MIB Dump) Adversaries may target the Management Information Base (MIB) to collect and/or mine valuable information in a network managed using Simple Network Management Protocol (SNMP). .002 Network Device Configuration Dump Adversaries may access network configuration files to collect sensitive data about the device and the network. The network configuration is a file containing parameters that determine the operation of the device. The device typically stores an in-memory copy of the configuration while operating, and a separate configuration on non-volatile storage to load after device reset. Adversaries can inspect the configuration files to reveal information about the target network and its layout, the network device and its software, or identifying legitimate accounts and credentials for later use. T1213 Data from Information Repositories Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, such as Credential Access, Lateral Movement, or Defense Evasion, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization (i.e., Transfer Data to Cloud Account). .001 Confluence Adversaries may leverage Confluence repositories to mine valuable information. Often found in development environments alongside Atlassian JIRA, Confluence is generally used to store development-related documentation, however, in general may contain more diverse categories of useful information, such as: .002 Sharepoint Adversaries may leverage the SharePoint repository as a source to mine valuable information. SharePoint will often contain useful information for an adversary to learn about the structure and functionality of the internal network and systems. For example, the following is a list of example information that may hold potential value to an adversary and may also be found on SharePoint: .003 Code Repositories Adversaries may leverage code repositories to collect valuable information. Code repositories are tools/services that store source code and automate software builds. They may be hosted internally or privately on third party sites such as Github, GitLab, SourceForge, and BitBucket. Users typically interact with code repositories through a web application or command-line utilities such as git. .004 Customer Relationship Management Software Adversaries may leverage Customer Relationship Management (CRM) software to mine valuable information. CRM software is used to assist organizations in tracking and managing customer interactions, as well as storing customer data. .005 Messaging Applications Adversaries may leverage chat and messaging applications, such as Microsoft Teams, Google Chat, and Slack, to mine valuable information. .006 Databases Adversaries may leverage databases to mine valuable information. These databases may be hosted on-premises or in the cloud (both in platform-as-a-service and software-as-a-service environments). T1005 Data from Local System Adversaries may search local system sources, such as file systems, configuration files, local databases, virtual machine files, or process memory, to find files of interest and sensitive data prior to Exfiltration. T1039 Data from Network Shared Drive Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within cmd may be used to

gather information. T1025 Data from Removable Media Adversaries may search connected removable media on computers they have compromised to find files of interest. Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration. Interactive command shells may be in use, and common functionality within cmd may be used to gather information. T1074 Data Staged Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data. Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location. .001 Local Data Staging Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data. Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location. .002 Remote Data Staging Adversaries may stage data collected from multiple systems in a central location or directory on one system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data. Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location. T1114 Email Collection Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Emails may also contain details of ongoing incident response operations, which may allow adversaries to adjust their techniques in order to maintain persistence or evade defenses. Adversaries can collect or forward email from mail servers or clients. .001 Local Email Collection Adversaries may target user email on local systems to collect sensitive information. Files containing email data can be acquired from a user’s local system, such as Outlook storage or cache files. .002 Remote Email Collection Adversaries may target an Exchange server, Office 365, or Google Workspace to collect sensitive information. Adversaries may leverage a user's credentials and interact directly with the Exchange server to acquire information from within a network. Adversaries may also access externally facing Exchange services, Office 365, or Google Workspace to access email using credentials or access tokens. Tools such as MailSniper can be used to automate searches for specific keywords. .003 Email Forwarding Rule Adversaries may setup email forwarding rules to collect sensitive information. Adversaries may abuse email forwarding rules to monitor the activities of a victim, steal information, and further gain intelligence on the victim or the victim’s organization to use as part of further exploits or operations. Furthermore, email forwarding rules can allow adversaries to maintain persistent access to victim's emails even after compromised credentials are reset by administrators. Most email clients allow users to create inbox rules for various email functions, including forwarding to a different recipient. These rules may be created through a local email application, a web interface, or by command-line interface. Messages can be forwarded to internal or external recipients, and there are no restrictions limiting the extent of this rule. Administrators may also create forwarding rules for user accounts with the same considerations and outcomes. T1056 Input Capture Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture). .001 Keylogging Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when OS Credential Dumping efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. In order to increase the likelihood of

capturing credentials quickly, an adversary may also perform actions such as clearing browser cookies to force users to reauthenticate to systems. .002 GUI Input Capture Adversaries may mimic common operating system GUI components to prompt users for credentials with a seemingly legitimate prompt. When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: Bypass User Account Control). .003 Web Portal Capture Adversaries may install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. For example, a compromised login page may log provided user credentials before logging the user in to the service. .004 Credential API Hooking Adversaries may hook into Windows application programming interface (API) functions and Linux system functions to collect user credentials. Malicious hooking mechanisms may capture API or function calls that include parameters that reveal user authentication credentials. Unlike Keylogging, this technique focuses specifically on API functions that include parameters that reveal user credentials. T1113 Screen Capture Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`. T1125 Video Capture An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.
