Discovery, Tactic TA0007 - Enterprise

Archived: 2026-04-05 13:11:47 UTC

T1087 Account Discovery Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., Valid Accounts). .001 Local Account Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior. .002 Domain Account Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior such as targeting specific accounts which possess particular privileges. .003 Email Account Adversaries may attempt to get a listing of email addresses and accounts. Adversaries may try to dump Exchange address lists such as global address lists (GALs). .004 Cloud Account Adversaries may attempt to get a listing of cloud accounts. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. T1010 Application Window Discovery Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used. For example, information about application windows could be used identify potential data to collect as well as identifying security tooling (Security Software Discovery) to evade. T1217 Browser Information Discovery Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure. T1580 Cloud Infrastructure Discovery An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services. T1538 Cloud Service Dashboard An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, review findings of potential security risks, and run additional queries, such as finding public IP addresses and open ports. T1526 Cloud Service Discovery An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Entra ID, etc. They may also include security services, such as AWS GuardDuty and Microsoft Defender for Cloud, and logging services, such as AWS CloudTrail and Google Cloud Audit Logs. T1619 Cloud Storage Object Discovery Adversaries may enumerate objects in cloud storage infrastructure. Adversaries may use this information during automated discovery to shape follow-on behaviors, including requesting all or specific objects from cloud storage. Similar to File and Directory Discovery on a local host, after identifying available storage services (i.e. Cloud Infrastructure Discovery) adversaries may access the contents/objects stored in cloud infrastructure. T1613 Container and Resource Discovery Adversaries may attempt to discover containers and other

resources that are available within a containers environment. Other resources may include images, deployments, pods, nodes, and other information such as the status of a cluster. T1622 Debugger Evasion Adversaries may employ various means to detect and avoid debuggers. Debuggers are typically used by defenders to trace and/or analyze the execution of potential malware payloads. T1652 Device Driver Discovery Adversaries may attempt to enumerate local device drivers on a victim host. Information about device drivers may highlight various insights that shape follow-on behaviors, such as the function/purpose of the host, present security tools (i.e. Security Software Discovery) or other defenses (e.g., Virtualization/Sandbox Evasion), as well as potential exploitable vulnerabilities (e.g., Exploitation for Privilege Escalation). T1482 Domain Trust Discovery Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain. Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct SID-History Injection, Pass the Ticket, and Kerberoasting. Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP. The Windows utility Nltest is known to be used by adversaries to enumerate domain trusts. T1083 File and Directory Discovery Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. T1615 Group Policy Discovery Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment. Group Policy allows for centralized management of user and computer settings in Active Directory (AD). Group policy objects (GPOs) are containers for group policy settings made up of files stored within a predictable network path `\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`. T1680 Local Storage Discovery Adversaries may enumerate local drives, disks, and/or volumes and their attributes like total or free space and volume serial number. This can be done to prepare for ransomware-related encryption, to perform Lateral Movement, or as a precursor to Direct Volume Access. T1654 Log Enumeration Adversaries may enumerate system and service logs to find useful data. These logs may highlight various types of valuable insights for an adversary, such as user authentication records (Account Discovery), security or vulnerable software (Software Discovery), or hosts within a compromised network (Remote System Discovery). T1046 Network Service Discovery Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port, vulnerability, and/or wordlist scans using tools that are brought onto a system. T1135 Network Share Discovery Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network. T1040 Network Sniffing Adversaries may passively sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data. T1201 Password Policy Discovery Adversaries may attempt to access detailed information about the password policy used within an enterprise

network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through Brute Force. This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts). T1120 Peripheral Device Discovery Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions. T1069 Permission Groups Discovery Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions. .001 Local Groups Adversaries may attempt to find local system groups and permission settings. The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group. .002 Domain Groups Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators. .003 Cloud Groups Adversaries may attempt to find cloud groups and permission settings. The knowledge of cloud permission groups can help adversaries determine the particular roles of users and groups within an environment, as well as which users are associated with a particular group. T1057 Process Discovery Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better process details. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. T1012 Query Registry Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. T1018 Remote System Discovery Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as Ping, `net view` using Net, or, on ESXi servers, `esxcli network diag ping`. T1518 Software Discovery Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. .001 Security Software Discovery Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. This may include things such as cloud monitoring agents and anti-virus. Adversaries may use the information from Security Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. .002 Backup Software Discovery Adversaries may attempt to get a listing of backup software or configurations that are installed on a system. Adversaries may use this information to shape follow-on behaviors, such as Data Destruction, Inhibit System Recovery, or Data Encrypted for Impact. T1082

System Information Discovery An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use this information to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. This behavior is distinct from Local Storage Discovery which is an adversary's discovery of local drive, disks and/or volumes. T1614 System Location Discovery Adversaries may gather information in an attempt to calculate the geographical location of a victim host. Adversaries may use the information from System Location Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. .001 System Language Discovery Adversaries may attempt to gather information about the system language of a victim in order to infer the geographical location of that host. This information may be used to shape follow-on behaviors, including whether the adversary infects the target and/or attempts specific actions. This decision may be employed by malware developers and operators to reduce their risk of attracting the attention of specific law enforcement agencies or prosecution/scrutiny from other entities. T1016 System Network Configuration Discovery Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route. .001 Internet Connection Discovery Adversaries may check for Internet connectivity on compromised systems. This may be performed during automated discovery and can be accomplished in numerous ways such as using Ping, `tracert`, and GET requests to websites, or performing initial speed testing to confirm bandwidth. .002 Wi-Fi Discovery Adversaries may search for information about Wi-Fi networks, such as network names and passwords, on compromised systems. Adversaries may use Wi-Fi information as part of Account Discovery, Remote System Discovery, and other discovery or Credential Access activity to support both ongoing and future campaigns. T1049 System Network Connections Discovery Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. T1033 System Owner/User Discovery Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using OS Credential Dumping. The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from System Owner/User Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. T1007 System Service Discovery Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may also gather information about schedule tasks via commands such as `schtasks` on Windows or `crontab -l` on Linux and macOS. T1124 System Time Discovery An adversary may gather the system time and/or time zone settings from a local or remote system. The system time is set and stored by services, such as the Windows Time Service on Windows or `systemsetup` on macOS. These time settings may also be synchronized between systems and services in an enterprise network, typically accomplished with a network time server within a domain. T1673 Virtual Machine Discovery An adversary may attempt to enumerate running virtual machines (VMs) after gaining access to a host or hypervisor. For example, adversaries may enumerate a list of VMs on an ESXi hypervisor using a Hypervisor CLI such as `esxcli` or

`vim-cmd` (e.g. `esxcli vm process list or vim-cmd vmsvc/getallvms`). Adversaries may also directly leverage a graphical user interface, such as VMware vCenter, in order to view virtual machines on a host. T1497 Virtualization/Sandbox Evasion Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors. .001 System Checks Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors. .002 User Activity Based Checks Adversaries may employ various user activity checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors. .003 Time Based Checks Adversaries may employ various time-based methods to detect virtualization and analysis environments, particularly those that attempt to manipulate time mechanisms to simulate longer elapses of time. This may include enumerating time-based properties, such as uptime or the system clock.
