THE MITRE ATT&CK AND QRADAR MAPPING

BY IZZMIER IZZUDDIN

TACTICS

1. **TA0043 Reconnaissance**
2. **TA0042 Resource Development**
3. **TA0001 Initial Access**
4. **TA0002 Execution**
5. **TA0003 Persistence**
6. **TA0004 Privilege Escalation**
7. **TA0005 Defense Evasion**
8. **TA0006 Credential Access**
9. **TA0007 Discovery**
10. **TA0008 Lateral Movement**
11. **TA0009 Collection**
12. **TA0011 Command and Control**
13. **TA0010 Exfiltration**
14. **TA0040 Impact**

TECHNIQUES

Reconnaissance

T1595 Active Scanning

.001 Scanning IP Blocks

- **QRadar Use Case: Detect IP scanning activities.**
- **Rules**:
    - Monitor for large numbers of connection attempts to sequential IP addresses.
    - Identify patterns of SYN scanning or other common port scanning methods.
    - Alert on detection of tools known for IP scanning such as Nmap.

.002 Vulnerability Scanning

- **QRadar Use Case: Detect vulnerability scanning activities.**
- **Rules:**
    - Monitor for network traffic indicative of vulnerability scanners (e.g., Nessus, OpenVAS).
    - Detect patterns of traffic attempting to identify known vulnerabilities (specific URI patterns, payloads).
    - Alert on detection of common vulnerability scanning behaviors such as extensive probing of open ports and services.

.003 Wordlist Scanning

- **QRadar Use Case: Detect scanning activities using wordlists.**
- **Rules:**
    - Monitor for login attempts using common username and password combinations (brute force detection).
    - Detect patterns of automated attempts to access web resources or services using known default credentials.
    - Alert on detection of tools and scripts that use wordlists for scanning and attempting to gain access (e.g., Hydra, Burp Suite).

T1592 Gather Victim Host Information

.001 Hardware

- **QRadar Use Case: Detect enumeration of hardware details on victim hosts.**
- **Rules:**
    - Monitor for commands that enumerate hardware information, such as lshw, dmidecode, systeminfo, or wmic.

- Alert on logs that indicate access to hardware management interfaces or tools.

.002 Software

- **QRadar Use Case: Detect enumeration of installed software on victim hosts.**
- **Rules:**
  - Detect commands that list installed software, such as dpkg --list, rpm -qa, wmic product get name, or Get-WmiObject -Class Win32_Product.
  - Monitor for access to software inventory databases or management systems.
  - Alert on logs indicating software enumeration via scripts or management tools.

.003 Firmware

- **QRadar Use Case: Detect attempts to gather firmware details.**
- **Rules:**
  - Monitor for commands that query firmware details, such as dmidecode or fwupdmgr.
  - Alert on logs showing access to firmware update utilities or interfaces.

.004 Client Configurations

- **QRadar Use Case: Detect gathering of client configuration details.**
- **Rules:**
  - Detect commands that retrieve configuration details, such as ipconfig /all, ifconfig, netsh, or nmcli.
  - Monitor for access to configuration files or management consoles.
  - Alert on logs indicating enumeration of network settings, system configurations, or user profiles.

T1589 Gather Victim Identity Information

.001 Credentials

- **QRadar Use Case: Detect attempts to gather or use victim credentials.**
- **Rules:**
  - Monitor for unusual login attempts, such as multiple failed login attempts followed by a successful login (brute force detection).
  - Detect use of credential harvesting tools or scripts.
  - Alert on access to credential stores, such as Windows Credential Manager, macOS Keychain, or Linux keyrings.
  - Monitor for suspicious network traffic patterns, like connections to known phishing domains or data exfiltration that may indicate credential dumping.

.002 Email Addresses

- **QRadar Use Case: Detect gathering or enumeration of victim email addresses.**
- **Rules:**
  - Monitor for large-scale email directory queries or enumeration attempts against directory services (e.g., LDAP queries).
  - Detect access to email harvesting tools or scraping scripts.
  - Alert on outgoing network traffic that may indicate data exfiltration of email address lists.
  - Monitor web server logs for signs of scraping activities targeting contact pages or user directories.

.003 Employee Names

- **QRadar Use Case: Detect gathering of victim employee names.**
- **Rules:**
  - Monitor for large-scale directory queries or searches that enumerate employee names from corporate directories.
  - Detect access to tools or scripts used for harvesting employee names.
  - Alert on network traffic that may indicate the exfiltration of employee name lists.
  - Monitor social media and public-facing websites for automated scraping activities targeting employee information.

T1590 Gather Victim Network Information

.001 Domain Properties

- **QRadar Use Case: Detect enumeration of domain properties.**
- **Rules:**
  - Monitor for LDAP queries that enumerate Active Directory domain properties.
  - Alert on use of tools like dsquery, net group, or Get-ADDomain.
  - Detect access to domain controllers or use of domain enumeration scripts.

.002 DNS

- **QRadar Use Case: Detect DNS enumeration activities.**
- **Rules:**
  - Monitor for DNS query patterns indicative of domain enumeration, such as bulk DNS lookups or zone transfer attempts.
  - Alert on use of tools like nslookup, dig, or fierce.
  - Detect suspicious DNS traffic, such as queries for internal domains from external sources.

.003 Network Trust Dependencies

- **QRadar Use Case: Detect enumeration of network trust relationships.**
- **Rules:**
  - Monitor for commands and tools used to discover network trust relationships, such as net use, net session, or netdom.
  - Alert on abnormal authentication attempts that may indicate trust discovery.
  - Detect network traffic patterns that suggest the mapping of trust relationships between domains or systems.

.004 Network Topology

- **QRadar Use Case: Detect mapping of network topology.**
- **Rules:**
  - Monitor for network scanning tools and techniques used to map the network topology, such as Nmap, traceroute, or pathping.
  - Detect SNMP queries and responses that may indicate network topology discovery.
  - Alert on unusual volumes of ICMP traffic that may suggest network mapping efforts.

.005 IP Addresses

- **QRadar Use Case: Detect attempts to gather IP address information.**
- **Rules:**
  - Monitor for network scanning activities aimed at discovering IP addresses, such as ping sweeps or ARP scans.
  - Detect use of tools like ipconfig, ifconfig, arp, or ip addr.
  - Alert on logs indicating enumeration of IP address ranges or subnets.

.006 Network Security Appliances

- **QRadar Use Case: Detect enumeration of network security appliances.**
- **Rules:**
  - Monitor for commands and tools used to identify network security appliances, such as nmap service scans or specific SNMP queries.
  - Detect access to management interfaces of firewalls, intrusion detection/prevention systems, and other security appliances.
  - Alert on suspicious network traffic patterns that may indicate probing of security devices.

T1591 Gather Victim Org Information

.001 Determine Physical Locations

- **QRadar Use Case: Detect enumeration of physical locations of the organization.**
- **Rules:**
    - Monitor for access to internal databases or documents containing office locations or addresses.
    - Detect queries to geolocation services or GPS-based systems that could indicate attempts to determine physical locations.
    - Alert on abnormal access to location-based information systems or mapping tools.

.002 Business Relationships

- **QRadar Use Case: Detect enumeration of the organization's business relationships.**
- **Rules:**
    - Monitor for access to CRM systems, partnership databases, or email communication patterns that could reveal business relationships.
    - Detect use of tools or scripts designed to scrape business relationship data from internal or public-facing systems.
    - Alert on abnormal patterns of data access that suggest enumeration of business contacts and partnerships.

.003 Identify Business Tempo

- **QRadar Use Case: Detect attempts to determine the business tempo or operational schedule.**
- **Rules:**
    - Monitor for access to scheduling systems, meeting calendars, or employee attendance records.
    - Detect unusual queries or data exfiltration attempts involving operational schedules or business calendars.
    - Alert on patterns of access to systems containing information about business hours, peak operational periods, or event schedules.

.004 Identify Roles

- **QRadar Use Case: Detect enumeration of roles and responsibilities within the organization.**
- **Rules:**
    - Monitor for access to HR systems, organizational charts, or role-specific directories.
    - Detect use of tools or scripts designed to enumerate user roles and responsibilities.
    - Alert on unusual patterns of data access that suggest enumeration of employee roles, job titles, or departmental responsibilities.

T1598 Phishing for Information

.001 Spearphishing Service

- **QRadar Use Case: Detect spearphishing attempts through spoofed or compromised services.**
- **Rules:**
    - Monitor for inbound emails from suspicious or unknown services, especially those impersonating trusted services.
    - Detect emails containing requests for sensitive information or prompting users to perform actions that are atypical.
    - Alert on patterns of email headers, domains, or content indicative of spearphishing attempts.

.002 Spearphishing Attachment

- **QRadar Use Case: Detect spearphishing attempts using malicious attachments.**
- **Rules:**
    - Monitor for inbound emails with attachments that have suspicious file types (e.g., executable files, macro-enabled documents).
    - Detect the use of common filenames or content within attachments that are often used in spearphishing attacks.
    - Alert on attachment scanning results that indicate malicious or potentially harmful content.
    - Use sandboxing techniques to analyze attachments and detect malicious behavior.

.003 Spearphishing Link

- **QRadar Use Case: Detect spearphishing attempts using malicious links.**
- **Rules:**
    - Monitor for inbound emails containing links to known malicious domains or newly registered/suspicious domains.
    - Detect URL patterns within emails that are shortened or obfuscated to disguise their true destination.
    - Alert on user clicks on suspicious links, especially if they lead to credential harvesting pages or exploit kits.
    - Implement link reputation services to assess the risk of URLs contained in emails.

.004 Spearphishing Voice

- **QRadar Use Case: Detect spearphishing attempts using voice calls.**
- **Rules:**
    - Monitor for unusual patterns of incoming calls, especially those from numbers with a high volume of calls to multiple employees.

    - Detect reported incidents or patterns from employees indicating they received suspicious calls asking for sensitive information.
    - Alert on call metadata that matches known vishing techniques, such as calls from spoofed numbers or numbers linked to previous attacks.
    - Integrate call recording and transcription services to analyze call content for phishing indicators.

T1597 Search Closed Sources

.001 Threat Intel Vendors

- **QRadar Use Case: Detect unauthorized access to or use of threat intelligence from vendors.**
- **Rules:**
    - Monitor for unauthorized access attempts to threat intelligence platforms or vendor portals.
    - Detect unusual download patterns or data exfiltration activities from threat intelligence repositories.
    - Alert on usage of credentials that have been flagged for suspicious activity or are associated with known breaches.
    - Monitor for API key misuse or unusual API call patterns to threat intelligence services.

.002 Purchase Technical Data

- **QRadar Use Case: Detect attempts to purchase technical data from closed sources.**
- **Rules:**
    - Monitor for unusual financial transactions or purchase orders directed towards known sources of technical data.
    - Detect access to internal procurement systems that indicate attempts to buy technical data.
    - Alert on communications or network traffic associated with known vendors of technical data.
    - Integrate dark web monitoring services to detect mentions of the organization's assets being targeted for purchase.

T1596 Search Open Technical Databases

.001 DNS/Passive DNS

- **QRadar Use Case: Detect DNS enumeration activities.**
- **Rules:**
    - Monitor for DNS query patterns indicative of domain enumeration, such as bulk DNS lookups or zone transfer attempts.
    - Alert on the use of tools like nslookup, dig, or fierce.

    - Detect suspicious DNS traffic, such as queries for internal domains from external sources.

.002 WHOIS

- **QRadar Use Case: Detect WHOIS query activities.**
- **Rules:**
    - Monitor for WHOIS queries targeting your organization's domain.
    - Detect patterns of WHOIS queries from known malicious IP addresses.
    - Alert on unusual spikes in WHOIS query activity.

.003 Digital Certificates

- **QRadar Use Case: Detect enumeration of digital certificates.**
- **Rules:**
    - Monitor for access to certificate repositories or management systems.
    - Detect patterns of querying public certificate transparency logs.
    - Alert on unusual requests for digital certificates related to your organization.

.004 CDNs

- **QRadar Use Case: Detect enumeration activities related to Content Delivery Networks (CDNs).**
- **Rules:**
    - Monitor for access to CDN-related resources or configurations.
    - Detect patterns of querying CDN IP ranges or endpoints.
    - Alert on abnormal traffic patterns that may indicate probing of CDN infrastructure.

.005 Scan Databases

- **QRadar Use Case: Detect access to public scan databases.**
- **Rules:**
    - Monitor for access to databases like Shodan or Censys.
    - Detect patterns of querying these databases for your organization's IP ranges or services.
    - Alert on abnormal spikes in access to scan database results.

T1593 Search Open Websites/Domains

.001 Social Media

- **QRadar Use Case: Detect enumeration and information gathering activities on social media.**
- **Rules:**

- Monitor for patterns of access to social media profiles or pages associated with your organization.
- Detect tools or scripts designed to scrape information from social media platforms.
- Alert on unusual spikes in traffic to social media domains that suggest automated scraping or reconnaissance.

.002 Search Engines

- **QRadar Use Case: Detect information gathering activities using search engines.**
- **Rules:**
  - Monitor for patterns of search queries related to your organization that may indicate information gathering.
  - Detect access to search engine results that match known reconnaissance patterns.
  - Alert on unusual search activity that suggests targeting of your organization's public information.

.003 Code Repositories

- **QRadar Use Case: Detect enumeration and information gathering activities in public code repositories.**
- **Rules:**
  - Monitor for access to public code repositories (e.g., GitHub, GitLab) looking for sensitive information.
  - Detect patterns of cloning or downloading repositories that contain your organization's code.
  - Alert on searches or queries within code repositories that match patterns of sensitive information (e.g., API keys, credentials).

T1594 Search Victim-Owned Websites

- **QRadar Use Case: Detect reconnaissance activities targeting victim-owned websites.**
- **Rules:**
  - Monitor for patterns of access to your organization's websites that may indicate enumeration or information gathering activities.
  - Detect unusual or suspicious user-agent strings, referrer URLs, or other HTTP headers that suggest automated scanning or scraping.
  - Alert on unusual spikes in traffic to certain web pages or endpoints, especially those that contain sensitive information or are less frequently accessed.
  - Monitor for known reconnaissance tools or scripts being used against your website.
  - Detect anomalies in web traffic patterns, such as unexpected POST requests or high-frequency GET requests to certain resources.

- Implement behavioral analysis to identify deviations from normal access patterns, potentially indicating reconnaissance or probing activities.

Resource Development

T1650 Acquire Access

- **QRadar Use Case: Detect attempts to gain unauthorized access to systems, applications, or data.**
- **Rules:**
    - Monitor for brute force attempts on authentication mechanisms (e.g., repeated failed login attempts).
    - Detect the use of stolen or compromised credentials.
    - Alert on the use of default or common passwords, especially on administrative accounts.
    - Monitor for unusual login patterns, such as access from new locations or at unusual times.
    - Detect attempts to exploit vulnerabilities in authentication mechanisms or services.
    - Monitor for signs of social engineering attacks, such as phishing, where credentials may be acquired.
    - Detect unusual account creation or privilege escalation activities.
    - Implement behavioral analysis to identify deviations from normal login patterns, potentially indicating unauthorized access attempts.

T1583 Acquire Infrastructure

.001 Domains

- **QRadar Use Case: Detect the acquisition and use of malicious or suspicious domains.**
- **Rules:**
    - Monitor for domain registration patterns associated with known threat actors.
    - Detect the use of newly registered or rarely used domains in communication.
    - Alert on the use of domains that match known malicious indicators.

.002 DNS Server

- **QRadar Use Case: Detect the setup or use of malicious DNS servers.**
- **Rules:**
    - Monitor for changes in DNS server configurations that may indicate malicious intent.
    - Detect traffic patterns indicative of DNS tunneling or exfiltration.
    - Alert on DNS queries that resolve to known malicious IP addresses.

.003 Virtual Private Server

- **QRadar Use Case: Detect the acquisition and use of VPS for malicious activities.**
- **Rules:**
    - Monitor for access patterns that suggest the use of VPS for command and control (C2) infrastructure.
    - Detect unusual or high-volume traffic to VPS IP ranges associated with known threats.
    - Alert on the use of VPS services known to be abused by cybercriminals.

.004 Server

- **QRadar Use Case: Detect the setup or use of servers for malicious purposes.**
- **Rules:**
    - **Monitor for server configurations and activities that indicate malicious use (e.g., hosting phishing sites, C2 servers).**
    - **Detect unauthorized access or control of servers within your network.**
    - **Alert on the use of server IP addresses known to be associated with malicious activities.**

.005 Botnet

- **QRadar Use Case: Detect the setup or use of botnets.**
- **Rules:**
    - **Monitor for communication patterns typical of botnet C2 traffic.**
    - **Detect attempts to recruit devices within your network into a botnet.**
    - **Alert on the use of IP addresses or domains known to be associated with botnet C2 servers.**

.006 Web Services

- **QRadar Use Case: Detect the acquisition and use of web services for malicious activities.**
- **Rules:**
    - **Monitor for unusual access patterns to web services that may indicate abuse.**
    - **Detect the use of web services for hosting malicious content or as part of a C2 infrastructure.**
    - **Alert on web service usage patterns that match known malicious indicators.**

.007 Serverless

- **QRadar Use Case: Detect the use of serverless computing resources for malicious activities.**
- **Rules:**
    - Monitor for unusual function invocation patterns that may indicate malicious use.

    - Detect the deployment of serverless functions with malicious payloads.
    - Alert on the use of serverless services in ways that deviate from normal usage patterns.

.008 Malvertising

- **QRadar Use Case: Detect the use of malvertising to distribute malware or redirect traffic.**
- **Rules:**
    - Monitor for traffic patterns indicative of malvertising campaigns.
    - Detect redirects from legitimate websites to malicious sites through advertising networks.
    - Alert on the use of advertising domains or URLs known to be associated with malvertising activities.

T1586 Compromise Accounts

.001 Social Media Accounts

- **QRadar Use Case: Detect the compromise and misuse of social media accounts.**
- **Rules:**
    - Monitor for unusual login activity to social media accounts, such as logins from unexpected locations or devices.
    - Detect changes to social media profiles or posts that deviate from normal behavior.
    - Alert on reports of unauthorized access or unusual activity on social media accounts from employees or automated detection systems.

.002 Email Account

- **QRadar Use Case: Detect the compromise and misuse of email accounts.**
- **Rules:**
    - Monitor for unusual login activity to email accounts, including logins from new locations or IP addresses.
    - Detect patterns indicative of email account takeover, such as changes to email forwarding rules or unusual email sending patterns.
    - Alert on reports of phishing attempts or unauthorized access to email accounts.
    - Monitor for email sending behavior that matches known phishing or spam campaigns.

.003 Cloud Account

- **QRadar Use Case: Detect the compromise and misuse of cloud service accounts.**
- **Rules:**

    - Monitor for unusual login activity to cloud accounts, such as logins from new locations or devices.
    - Detect changes to cloud service configurations or resources that deviate from normal usage patterns.
    - Alert on access to sensitive cloud resources by accounts showing signs of compromise.
    - Monitor for the use of cloud services in ways that align with known attack patterns, such as data exfiltration or unauthorized resource provisioning.

T1584 Compromise Infrastructure

.001 Domains

- **QRadar Use Case: Detect and respond to the compromise of domains.**
- **Rules:**
    - Monitor for unauthorized changes to domain registration details.
    - Detect unusual DNS activity or patterns indicative of domain hijacking.
    - Alert on domain name system (DNS) queries or traffic associated with compromised domains.

.002 DNS Server

- **QRadar Use Case: Detect and respond to the compromise of DNS servers.**
- **Rules:**
    - Monitor for unauthorized changes to DNS server configurations.
    - Detect patterns of DNS traffic that suggest unauthorized access or control of DNS servers.
    - Alert on DNS queries that resolve to known malicious IP addresses or that indicate DNS hijacking.

.003 Virtual Private Server

- **QRadar Use Case: Detect and respond to the compromise of VPS.**
- **Rules:**
    - Monitor for unauthorized access or control of VPS within your infrastructure.
    - Detect unusual or malicious activity originating from VPS instances.
    - Alert on VPS IP addresses associated with known threats or malicious activities.

.004 Server

- **QRadar Use Case: Detect and respond to the compromise of servers.**
- **Rules:**
    - Monitor for unauthorized access or control of servers.
    - Detect unusual or malicious activity on servers, such as the presence of malware or unauthorized processes.

    - Alert on server configurations or activities that deviate from normal behavior.

.005 Botnet

- **QRadar Use Case: Detect and respond to the compromise of devices into botnets.**
- **Rules:**
    - Monitor for communication patterns typical of botnet command and control (C2) traffic.
    - Detect attempts to recruit devices within your network into a botnet.
    - Alert on the use of IP addresses or domains known to be associated with botnet C2 servers.

.006 Web Services

- **QRadar Use Case: Detect and respond to the compromise of web services.**
- **Rules:**
    - Monitor for unauthorized access or control of web services.
    - Detect unusual or malicious activity on web services, such as the hosting of phishing sites or malware.
    - Alert on web service configurations or activities that deviate from normal behavior.

.007 Serverless

- **QRadar Use Case: Detect and respond to the compromise of serverless computing resources.**
- **Rules:**
    - Monitor for unauthorized access or control of serverless functions.
    - Detect unusual function invocation patterns that suggest malicious activity.
    - Alert on the deployment of serverless functions with malicious payloads.

.008 Network Devices

- **QRadar Use Case: Detect and respond to the compromise of network devices.**
- **Rules:**
    - Monitor for unauthorized access or control of network devices, such as routers, switches, and firewalls.
    - Detect changes to network device configurations that indicate compromise.
    - Alert on network traffic patterns that suggest malicious activity originating from or targeting network devices.

T1587 Develop Capabilities

.001 Malware

- **QRadar Use Case: Detect the development or deployment of malware within the organization.**
- **Rules:**
    - Monitor for the presence of known malware signatures and behaviors.
    - Detect unusual file creations or modifications that suggest the development or staging of malware.
    - Alert on the use of tools and environments commonly associated with malware development, such as specific compilers or packers.
    - Monitor for network traffic indicative of malware communication or exfiltration.

.002 Code Signing Certificates

- **QRadar Use Case: Detect the acquisition and misuse of code signing certificates.**
- **Rules:**
    - Monitor for attempts to acquire code signing certificates from public or private sources.
    - Detect the use of code signing certificates that deviate from normal usage patterns, such as certificates signed by unknown or suspicious authorities.
    - Alert on the signing of executable files or software with certificates that match known malicious indicators.

.003 Digital Certificates

- **QRadar Use Case: Detect the acquisition and misuse of digital certificates.**
- **Rules:**
    - Monitor for unauthorized access to certificate authorities (CAs) or certificate management systems.
    - Detect the issuance or use of digital certificates that deviate from normal behavior, such as certificates issued to unusual domain names.
    - Alert on the use of digital certificates associated with known malicious activities.

.004 Exploits

- **QRadar Use Case: Detect the development or use of exploits within the organization.**
- **Rules:**
    - Monitor for the presence of exploit code or tools within the network.
    - Detect patterns of activity indicative of exploit development or testing, such as the use of specific debuggers or fuzzing tools.
    - Alert on network traffic or system behavior that matches known exploit patterns, such as specific vulnerability scans or unusual process activity.

T1585 Establish Accounts

0.001 Social Media Accounts

- **QRadar Use Case: Detect the creation and use of unauthorized social media accounts.**
- **Rules:**
    - Set up alerts for network traffic patterns that indicate access to social media platforms commonly used for account creation.
    - Use web proxy logs to identify attempts to create new accounts on social media sites from within the organization's network.
    - Detect and alert on patterns of activity associated with the use of new social media accounts, such as high-frequency posting or connections to known suspicious accounts.
    - Monitor for any communication or mentions of the organization that seem unusual or unauthorized.

0.002 Email Accounts

- **QRadar Use Case: Detect the creation and use of unauthorized email accounts.**
- **Rules:**
    - Set up alerts for network traffic patterns indicating access to popular email service providers used for creating new accounts.
    - Monitor DNS queries and HTTP requests associated with common email service providers (e.g., Gmail, Yahoo, Outlook).
    - Analyze email traffic for signs of phishing campaigns or other malicious activities originating from newly created email accounts.
    - Set alerts for unusual login attempts to corporate email systems that may indicate the use of unauthorized accounts.

0.003 Cloud Accounts

- **QRadar Use Case: Detect the creation and use of unauthorized cloud accounts.**
- **Rules:**
    - Track API calls and web traffic to cloud service providers (e.g., AWS, Azure, Google Cloud) to detect the creation of new accounts.
    - Use logs from cloud management platforms to identify account creation events.
    - Detect and alert on unusual activity patterns in cloud environments, such as large data transfers or changes in configurations that could indicate unauthorized access.
    - Monitor cloud access logs for signs of anomalous behavior from new or rarely used accounts.

T1588 Obtain Capabilities

0.001 Malware

- **QRadar Use Case: Detect the acquisition and use of malware.**
- **Rules:**
  - Set up alerts for network traffic patterns that indicate downloads from known malware repositories or suspicious sources.
  - Use threat intelligence feeds to update blacklists of known malicious domains and IP addresses.
  - Analyze file creation and modification events to detect the introduction of new, potentially malicious files.
  - Utilize antivirus and endpoint detection and response (EDR) solutions to identify malware signatures.

0.002 Tool

- **Radar Use Case: Detect the acquisition and use of hacking tools.**
- **Rules:**
  - Track network traffic for downloads from websites known to host hacking tools.
  - Use proxy logs and threat intelligence to identify access to tool repositories.
  - Detect and alert on the execution of known hacking tools within the network.
  - Analyze command-line activity for patterns associated with the use of hacking tools.

0.003 Code Signing Certificates

- **QRadar Use Case: Detect attempts to acquire code signing certificates.**
- **Rules:**
  - Track network traffic and logs for requests to certificate authorities (CAs) that could indicate attempts to acquire code signing certificates.
  - Set alerts for suspicious patterns of certificate requests or renewals.
  - Analyze logs for the use of newly obtained certificates to sign code, especially if the certificate use does not match the expected patterns.
  - Alert on certificates used by unauthorized entities or in unexpected contexts.

0.004 Digital Certificates

- **QRadar Use Case: Detect attempts to acquire digital certificates.**
- **Rules:**
  - Track network and system logs for attempts to obtain digital certificates from internal or external CAs.
  - Set alerts for unusual patterns of certificate requests or abnormal CA access.

    - Detect and alert on the deployment of newly obtained certificates, particularly if associated with suspicious activities or entities.
    - Analyze network traffic for the use of digital certificates in encrypted communications, focusing on anomalies.

0.005 Exploits

- **QRadar Use Case: Detect the acquisition and use of exploits.**
- **Rules:**
    - Track network traffic for downloads from known exploit kit repositories or suspicious domains.
    - Use threat intelligence to identify sources of known exploits.
    - Analyze system and application logs for indicators of exploit attempts, such as unusual crashes or application behaviors.
    - Set alerts for known exploit signatures or anomalous system calls.

0.006 Vulnerabilities

- **QRadar Use Case: Detect attempts to obtain information on vulnerabilities.**
- **Rules:**
    - Detect and alert on network traffic indicative of vulnerability scanning activities.
    - Use intrusion detection systems (IDS) and vulnerability management tools to identify scanning patterns.
    - Monitor access to internal and external vulnerability databases, focusing on unusual or unauthorized queries.
    - Set alerts for large volumes of vulnerability data downloads or access from suspicious entities.

0.007 Artificial Intelligence

- **QRadar Use Case: Detect the acquisition and use of artificial intelligence capabilities for malicious purposes.**
- **Rules:**
    - Track network traffic for downloads from known repositories of AI tools or libraries.
    - Use proxy logs and threat intelligence to identify access to AI resources.
    - Analyze system and application logs for the use of AI tools or models in unexpected contexts.
    - Set alerts for patterns of activity indicative of AI-based attacks or data manipulation.

T1608 Stage Capabilities

0.001 Upload Malware

- **QRadar Use Case: Detect the upload of malware to internal or external systems.**
- **Rules:**
    - Set up alerts for file transfer protocols (FTP, SFTP) and HTTP uploads of files to external servers or cloud storage.
    - Use antivirus and EDR solutions to scan files uploaded to internal servers or shared storage.
    - Analyze file creation and modification events to identify potentially malicious files.
    - Set alerts for known malware signatures and unusual file behavior.

0.002 Upload Tool

- **QRadar Use Case: Detect the upload of hacking tools to internal or external systems.**
- **Rules:**
    - Track network traffic for uploads to known repositories or suspicious destinations.
    - Use web proxy logs to identify access to sites where hacking tools are commonly uploaded.
    - Detect and alert on the execution of newly uploaded tools within the network.
    - Analyze command-line activity for patterns associated with the use of hacking tools.

0.003 Install Digital Certificate

- **QRadar Use Case: Detect the installation of unauthorized digital certificates.**
- **Rules:**
    - Track system logs for events related to the installation of new digital certificates.
    - Set alerts for certificate installation on critical systems or in unusual contexts.
    - Analyze network traffic for the use of new certificates in encrypted communications.
    - Alert on certificates used by unauthorized entities or in unexpected ways.

0.004 Drive-by Target

- **QRadar Use Case: Detect attempts to stage drive-by attacks on targeted systems.**
- **Rules:**
    - Track network traffic for access to compromised websites known for hosting drive-by downloads.

    - Use web filtering and threat intelligence feeds to block and alert on access to malicious sites.
    - Analyze system and application logs for indicators of exploit delivery via drive-by downloads.
    - Set alerts for unusual behaviors such as sudden crashes or anomalous application activity.

0.005 Link Target

- **QRadar Use Case: Detect attempts to stage malicious links targeting users.**
- **Rules:**
    - Track email and web traffic for the presence of suspicious or known malicious links.
    - Use threat intelligence and URL filtering to identify and block harmful links.
    - Detect and alert on users clicking on links that lead to malicious sites.
    - Analyze email logs for phishing attempts and the distribution of malicious links.

0.006 SEO Poisoning

- **QRadar Use Case: Detect attempts to use SEO poisoning to stage malicious capabilities.**
- **Rules:**
    - Track network traffic for access to search engines and identify patterns indicative of SEO poisoning attempts.
    - Use threat intelligence to detect known malicious sites that use SEO poisoning techniques.
    - Analyze web traffic for redirects to malicious content following search engine queries.
    - Set alerts for access to sites flagged for SEO poisoning and unusual browsing patterns.

Initial Access

T1659 Content Injection

T1189 Drive-by Compromise

T1190 Exploit Public-Facing Application

T1133 External Remote Services

T1200 Hardware Additions

T1566 Phishing

0.001 Spearphishing Attachment

0.002 Spearphishing Link

0.003 Spearphishing via Service

0.004 Spearphishing Voice

T1091 Replication Through Removable Media

T1195 Supply Chain Compromise

0.001 Compromise Software Dependencies and Development Tools

0.002 Compromise Software Supply Chain

0.003 Compromise Hardware Supply Chain

T1199 Trusted Relationship

T1078 Valid Accounts

0.001 Default Accounts

0.002 Domain Accounts

0.003 Local Accounts

0.004 Cloud Accounts

Execution

T1651 Cloud Administration Command

T1059 Command and Scripting Interpreter

0.001 PowerShell

0.002 AppleScript

0.003 Windows Command Shell

0.004 Unix Shell

0.005 Visual Basic

0.006 Python

0.007 JavaScript

0.008 Network Device CLI

0.009 Cloud API

0.010 AutoHotKey & AutoIT

T1609 Container Administration Command

T1610 Deploy Container

T1203 Exploitation for Client Execution

T1559 Inter-Process Communication

0.001 Component Object Model

0.002 Dynamic Data Exchange

0.003 XPC Services

T1106 Native API

T1053 Scheduled Task/Job

0.002 At

0.003 Cron

0.005 Scheduled Task

0.006 Systemd Timers

0.007 Container Orchestration Job

T1648 Serverless Execution

T1129 Shared Modules

T1072 Software Deployment Tools

T1569 System Services

0.001 Launchctl

0.002 Service Execution

T1204 User Execution

0.001 Malicious Link

0.002 Malicious File

0.003 Malicious Image

T1047 Windows Management Instrumentation

Persistence

T1098 Account Manipulation

0.001 Additional Cloud Credentials

0.002 Additional Email Delegate Permissions

0.003 Additional Cloud Roles

0.004 SSH Authorized Keys

0.005 Device Registration

0.006 Additional Container Cluster Roles

T1197 BITS Jobs

T1547 Boot or Logon Autostart Execution

0.001 Registry Run Keys / Startup Folder

0.002 Authentication Package

0.003 Time Providers

0.004 Winlogon Helper DLL

0.005 Security Support Provider

0.006 Kernel Modules and Extensions

0.007 Re-opened Applications

0.008 LSASS Driver

0.009 Shortcut Modification

0.010 Port Monitors

0.012 Print Processors

0.013 XDG Autostart Entries

0.014 Active Setup

0.015 Login Items

T1037 Boot or Logon Initialization Scripts

0.001 Logon Script (Windows)

0.002 Login Hook

0.003 Network Logon Script

0.004 RC Scripts

0.005 Startup Items

T1176 Browser Extensions

T1554 Compromise Host Software Binary

T1136 Create Account

0.001 Local Account

0.002 Domain Account

0.003 Cloud Account

T1543 Create or Modify System Process

0.001 Launch Agent

0.002 Systemd Service

0.003 Windows Service

0.004 Launch Daemon

0.005 Container Service

T1546 Event Triggered Execution

0.001 Change Default File Association

0.002 Screensaver

0.003 Windows Management Instrumentation Event Subscription

0.004 Unix Shell Configuration Modification

0.005 Trap

0.006 LC_LOAD_DYLIB Addition

0.007 Netsh Helper DLL

0.008 Accessibility Features

0.009 AppCert DLLs

0.010 AppInit DLLs

0.011 Application Shimming

0.012 Image File Execution Options Injection

0.013 PowerShell Profile

0.014 Emond

0.015 Component Object Model Hijacking

0.016 Installer Packages

T1133 External Remote Services

T1574 Hijack Execution Flow

0.001 DLL Search Order Hijacking

0.002 DLL Side-Loading

0.004 Dylib Hijacking

0.005 Executable Installer File Permissions Weakness

0.006 Dynamic Linker Hijacking

0.007 Path Interception by PATH Environment Variable

0.008 Path Interception by Search Order Hijacking

0.009 Path Interception by Unquoted Path

0.010 Services File Permissions Weakness

0.011 Services Registry Permissions Weakness

0.012 COR_PROFILER

0.013 KernelCallbackTable

0.014 AppDomainManager

T1525 Implant Internal Image

T1556 Modify Authentication Process

0.001 Domain Controller Authentication

0.002 Password Filter DLL

0.003 Pluggable Authentication Modules

0.004 Network Device Authentication

0.005 Reversible Encryption

0.006 Multi-Factor Authentication

0.007 Hybrid Identity

0.008 Network Provider DLL

0.009 Conditional Access Policies

T1137 Office Application Startup

0.001 Office Template Macros

0.002 Office Test

0.003 Outlook Forms

0.004 Outlook Home Page

0.005 Outlook Rules

0.006 Add-ins

T1653 Power Settings

T1542 Pre-OS Boot

0.001 System Firmware

0.002 Component Firmware

0.003 Bootkit

0.004 ROMMONkit

0.005 TFTP Boot

T1053 Scheduled Task/Job

0.002 At

0.003 Cron

0.005 Scheduled Task

0.006 Systemd Timers

0.007 Container Orchestration Job

T1505 Server Software Component

0.001 SQL Stored Procedures

0.002 Transport Agent

0.003 Web Shell

0.004 IIS Components

0.005 Terminal Services DLL

T1205 Traffic Signaling

0.001 Port Knocking

0.002 Socket Filters

T1078 Valid Accounts

0.001 Default Accounts

0.002 Domain Accounts

0.003 Local Accounts

0.004 Cloud Accounts

Privilege Escalation

T1548 Abuse Elevation Control Mechanism

0.001 Setuid and Setgid

0.002 Bypass User Account Control

0.003 Sudo and Sudo Caching

0.004 Elevated Execution with Prompt

0.005 Temporary Elevated Cloud Access

0.006 TCC Manipulation

T1134 Access Token Manipulation

0.001 Token Impersonation/Theft

0.002 Create Process with Token

0.003 Make and Impersonate Token

0.004 Parent PID Spoofing

0.005 SID-History Injection

T1098 Account Manipulation

0.001 Additional Cloud Credentials

0.002 Additional Email Delegate Permissions

0.003 Additional Cloud Roles

0.004 SSH Authorized Keys

0.005 Device Registration

0.006 Additional Container Cluster Roles

T1547 Boot or Logon Autostart Execution

0.001 Registry Run Keys / Startup Folder

0.002 Authentication Package

0.003 Time Providers

0.004 Winlogon Helper DLL

0.005 Security Support Provider

0.006 Kernel Modules and Extensions

0.007 Re-opened Applications

0.008 LSASS Driver

0.009 Shortcut Modification

0.010 Port Monitors

0.012 Print Processors

0.013 XDG Autostart Entries

0.014 Active Setup

0.015 Login Items

T1037 Boot or Logon Initialization Scripts

0.001 Logon Script (Windows)

0.002 Login Hook

0.003 Network Logon Script

0.004 RC Scripts

0.005 Startup Items

T1543 Create or Modify System Process

0.001 Launch Agent

0.002 Systemd Service

0.003 Windows Service

0.004 Launch Daemon

0.005 Container Service

T1484 Domain or Tenant Policy Modification

0.001 Group Policy Modification

0.002 Trust Modification

T1611 Escape to Host

T1546 Event Triggered Execution

0.001 Change Default File Association

0.002 Screensaver

0.003 Windows Management Instrumentation Event Subscription

0.004 Unix Shell Configuration Modification

0.005 Trap

0.006 LC_LOAD_DYLIB Addition

0.007 Netsh Helper DLL

0.008 Accessibility Features

0.009 AppCert DLLs

0.010 AppInit DLLs

0.011 Application Shimming

0.012 Image File Execution Options Injection

0.013 PowerShell Profile

0.014 Emond

0.015 Component Object Model Hijacking

0.016 Installer Packages

T1068 Exploitation for Privilege Escalation

T1574 Hijack Execution Flow

0.001 DLL Search Order Hijacking

0.002 DLL Side-Loading

0.004 Dylib Hijacking

0.005 Executable Installer File Permissions Weakness

0.006 Dynamic Linker Hijacking

0.007 Path Interception by PATH Environment Variable

0.008 Path Interception by Search Order Hijacking

0.009 Path Interception by Unquoted Path

0.010 Services File Permissions Weakness

0.011 Services Registry Permissions Weakness

0.012 COR_PROFILER

0.013 KernelCallbackTable

0.014 AppDomainManager

T1055 Process Injection

0.001 Dynamic-link Library Injection

0.002 Portable Executable Injection

0.003 Thread Execution Hijacking

0.004 Asynchronous Procedure Call

0.005 Thread Local Storage

0.008 Ptrace System Calls

0.009 Proc Memory

0.011 Extra Window Memory Injection

0.012 Process Hollowing

0.013 Process Doppelgänging

0.014 VDSO Hijacking

0.015 ListPlanting

T1053 Scheduled Task/Job

0.002 At

0.003 Cron

0.005 Scheduled Task

0.006 Systemd Timers

0.007 Container Orchestration Job

T1078 Valid Accounts

0.001 Default Accounts

0.002 Domain Accounts

0.003 Local Accounts

0.004 Cloud Accounts

Defense Evasion

T1548 Abuse Elevation Control Mechanism

0.001 Setuid and Setgid

0.002 Bypass User Account Control

0.003 Sudo and Sudo Caching

0.004 Elevated Execution with Prompt

0.005 Temporary Elevated Cloud Access

0.006 TCC Manipulation

T1134 Access Token Manipulation

0.001 Token Impersonation/Theft

0.002 Create Process with Token

0.003 Make and Impersonate Token

0.004 Parent PID Spoofing

0.005 SID-History Injection

T1197 BITS Jobs

T1612 Build Image on Host

T1622 Debugger Evasion

T1140 Deobfuscate/Decode Files or Information

T1610 Deploy Container

T1006 Direct Volume Access

T1484 Domain or Tenant Policy Modification

0.001 Group Policy Modification

0.002 Trust Modification

T1480 Execution Guardrails

0.001 Environmental Keying

T1211 Exploitation for Defense Evasion

T1222 File and Directory Permissions Modification

0.001 Windows File and Directory Permissions Modification

0.002 Linux and Mac File and Directory Permissions Modification

T1564 Hide Artifacts

0.001 Hidden Files and Directories

0.002 Hidden Users

0.003 Hidden Window

0.004 NTFS File Attributes

0.005 Hidden File System

0.006 Run Virtual Instance

0.007 VBA Stomping

0.008 Email Hiding Rules

0.009 Resource Forking

0.010 Process Argument Spoofing

0.011 Ignore Process Interrupts

0.012 File/Path Exclusions

T1574 Hijack Execution Flow

0.001 DLL Search Order Hijacking

0.002 DLL Side-Loading

0.004 Dylib Hijacking

0.005 Executable Installer File Permissions Weakness

0.006 Dynamic Linker Hijacking

0.007 Path Interception by PATH Environment Variable

0.008 Path Interception by Search Order Hijacking

0.009 Path Interception by Unquoted Path

0.010 Services File Permissions Weakness

0.011 Services Registry Permissions Weakness

0.012 COR_PROFILER

0.013 KernelCallbackTable

0.014 AppDomainManager

T1562 Impair Defenses

0.001 Disable or Modify Tools

0.002 Disable Windows Event Logging

0.003 Impair Command History Logging

0.004 Disable or Modify System Firewall

0.006 Indicator Blocking

0.007 Disable or Modify Cloud Firewall

0.008 Disable or Modify Cloud Logs

0.009 Safe Mode Boot

0.010 Downgrade Attack

0.011 Spoof Security Alerting

0.012 Disable or Modify Linux Audit System

T1656 Impersonation

T1070 Indicator Removal

0.001 Clear Windows Event Logs

0.002 Clear Linux or Mac System Logs

0.003 Clear Command History

0.004 File Deletion

0.005 Network Share Connection Removal

0.006 Timestomp

0.007 Clear Network Connection History and Configurations

0.008 Clear Mailbox Data

0.009 Clear Persistence

T1202 Indirect Command Execution

T1036 Masquerading

0.001 Invalid Code Signature

0.002 Right-to-Left Override

0.003 Rename System Utilities

0.004 Masquerade Task or Service

0.005 Match Legitimate Name or Location

0.006 Space after Filename

0.007 Double File Extension

0.008 Masquerade File Type

0.009 Break Process Trees

T1556 Modify Authentication Process

0.001 Domain Controller Authentication

0.002 Password Filter DLL

0.003 Pluggable Authentication Modules

0.004 Network Device Authentication

0.005 Reversible Encryption

0.006 Multi-Factor Authentication

0.007 Hybrid Identity

0.008 Network Provider DLL

0.009 Conditional Access Policies

T1578 Modify Cloud Compute Infrastructure

0.001 Create Snapshot

0.002 Create Cloud Instance

0.003 Delete Cloud Instance

0.004 Revert Cloud Instance

0.005 Modify Cloud Compute Configurations

T1112 Modify Registry

T1601 Modify System Image

0.001 Patch System Image

0.002 Downgrade System Image

T1599 Network Boundary Bridging

0.001 Network Address Translation Traversal

T1027 Obfuscated Files or Information

0.001 Binary Padding

0.002 Software Packing

0.003 Steganography

0.004 Compile After Delivery

0.005 Indicator Removal from Tools

0.006 HTML Smuggling

0.007 Dynamic API Resolution

0.008 Stripped Payloads

0.009 Embedded Payloads

0.010 Command Obfuscation

0.011 Fileless Storage

0.012 LNK Icon Smuggling

0.013 Encrypted/Encoded File

T1647 Plist File Modification

T1542 Pre-OS Boot

0.001 System Firmware

0.002 Component Firmware

0.003 Bootkit

0.004 ROMMONkit

0.005 TFTP Boot

T1055 Process Injection

0.001 Dynamic-link Library Injection

0.002 Portable Executable Injection

0.003 Thread Execution Hijacking

0.004 Asynchronous Procedure Call

0.005 Thread Local Storage

0.008 Ptrace System Calls

0.009 Proc Memory

0.011 Extra Window Memory Injection

0.012 Process Hollowing

0.013 Process Doppelgänging

0.014 VDSO Hijacking

0.015 ListPlanting

T1620 Reflective Code Loading

T1207 Rogue Domain Controller

T1014 Rootkit

T1553 Subvert Trust Controls

0.001 Gatekeeper Bypass

0.002 Code Signing

0.003 SIP and Trust Provider Hijacking

0.004 Install Root Certificate

0.005 Mark-of-the-Web Bypass

0.006 Code Signing Policy Modification

T1218 System Binary Proxy Execution

0.001 Compiled HTML File

0.002 Control Panel

0.003 CMSTP

0.004 InstallUtil

0.005 Mshta

0.007 Msiexec

0.008 Odbcconf

0.009 Regsvcs/Regasm

0.010 Regsvr32

0.011 Rundll32

0.012 Verclsid

0.013 Mavinject

0.014 MMC

0.015 Electron Applications

T1216 System Script Proxy Execution

0.001 PubPrn

0.002 SyncAppvPublishingServer

T1221 Template Injection

T1205 Traffic Signaling

0.001 Port Knocking

0.002 Socket Filters

T1127 Trusted Developer Utilities Proxy Execution

0.001 MSBuild

T1535 Unused/Unsupported Cloud Regions

T1550 Use Alternate Authentication Material

0.001 Application Access Token

0.002 Pass the Hash

0.003 Pass the Ticket

0.004 Web Session Cookie

T1078 Valid Accounts

0.001 Default Accounts

0.002 Domain Accounts

0.003 Local Accounts

0.004 Cloud Accounts

T1497 Virtualization/Sandbox Evasion

0.001 System Checks

0.002 User Activity Based Checks

0.003 Time Based Evasion

T1600 Weaken Encryption

0.001 Reduce Key Space

0.002 Disable Crypto Hardware

T1220 XSL Script Processing

Credential Access

T1557 Adversary-in-the-Middle

0.001 LLMNR/NBT-NS Poisoning and SMB Relay

0.002 ARP Cache Poisoning

0.003 DHCP Spoofing

T1110 Brute Force

0.001 Password Guessing

0.002 Password Cracking

0.003 Password Spraying

0.004 Credential Stuffing

T1555 Credentials from Password Stores

0.001 Keychain

0.002 Securityd Memory

0.003 Credentials from Web Browsers

0.004 Windows Credential Manager

0.005 Password Managers

0.006 Cloud Secrets Management Stores

T1212 Exploitation for Credential Access

T1187 Forced Authentication

T1606 Forge Web Credentials

0.001 Web Cookies

0.002 SAML Tokens

T1056 Input Capture

0.001 Keylogging

0.002 GUI Input Capture

0.003 Web Portal Capture

0.004 Credential API Hooking

T1556 Modify Authentication Process

0.001 Domain Controller Authentication

0.002 Password Filter DLL

0.003 Pluggable Authentication Modules

0.004 Network Device Authentication

0.005 Reversible Encryption

0.006 Multi-Factor Authentication

0.007 Hybrid Identity

0.008 Network Provider DLL

0.009 Conditional Access Policies

T1111 Multi-Factor Authentication Interception

T1621 Multi-Factor Authentication Request Generation

T1040 Network Sniffing

T1003 OS Credential Dumping

0.001 LSASS Memory

0.002 Security Account Manager

0.003 NTDS

0.004 LSA Secrets

0.005 Cached Domain Credentials

0.006 DCSync

0.007 Proc Filesystem

0.008 /etc/passwd and /etc/shadow

T1528 Steal Application Access Token

T1649 Steal or Forge Authentication Certificates

T1558 Steal or Forge Kerberos Tickets

0.001 Golden Ticket

0.002 Silver Ticket

0.003 Kerberoasting

0.004 AS-REP Roasting

T1539 Steal Web Session Cookie

T1552 Unsecured Credentials

0.001 Credentials In Files

0.002 Credentials in Registry

0.003 Bash History

0.004 Private Keys

0.005 Cloud Instance Metadata API

0.006 Group Policy Preferences

0.007 Container API

0.008 Chat Messages

Discovery

T1087 Account Discovery

0.001 Local Account

0.002 Domain Account

0.003 Email Account

0.004 Cloud Account

T1010 Application Window Discovery

T1217 Browser Information Discovery

T1580 Cloud Infrastructure Discovery

T1538 Cloud Service Dashboard

T1526 Cloud Service Discovery

T1619 Cloud Storage Object Discovery

T1613 Container and Resource Discovery

T1622 Debugger Evasion

T1652 Device Driver Discovery

T1482 Domain Trust Discovery

T1083 File and Directory Discovery

T1615 Group Policy Discovery

T1654 Log Enumeration

T1046 Network Service Discovery

T1135 Network Share Discovery

T1040 Network Sniffing

T1201 Password Policy Discovery

T1120 Peripheral Device Discovery

T1069 Permission Groups Discovery

0.001 Local Groups

0.002 Domain Groups

0.003 Cloud Groups

T1057 Process Discovery

T1012 Query Registry

T1018 Remote System Discovery

T1518 Software Discovery

0.001 Security Software Discovery

T1082 System Information Discovery

T1614 System Location Discovery

0.001 System Language Discovery

T1016 System Network Configuration Discovery

0.001 Internet Connection Discovery

0.002 Wi-Fi Discovery

T1049 System Network Connections Discovery

T1033 System Owner/User Discovery

T1007 System Service Discovery

T1124 System Time Discovery

T1497 Virtualization/Sandbox Evasion

0.001 System Checks

0.002 User Activity Based Checks

0.003 Time Based Evasion

Lateral Movement

T1210 Exploitation of Remote Services

T1534 Internal Spearphishing

T1570 Lateral Tool Transfer

T1563 Remote Service Session Hijacking

0.001 SSH Hijacking

0.002 RDP Hijacking

T1021 Remote Services

0.001 Remote Desktop Protocol

0.002 SMB/Windows Admin Shares

0.003 Distributed Component Object Model

0.004 SSH

0.005 VNC

0.006 Windows Remote Management

0.007 Cloud Services

0.008 Direct Cloud VM Connections

T1091 Replication Through Removable Media

T1072 Software Deployment Tools

T1080 Taint Shared Content

T1550 Use Alternate Authentication Material

0.001 Application Access Token

0.002 Pass the Hash

0.003 Pass the Ticket

0.004 Web Session Cookie

Collection

T1557 Adversary-in-the-Middle

0.001 LLMNR/NBT-NS Poisoning and SMB Relay

0.002 ARP Cache Poisoning

0.003 DHCP Spoofing

T1560 Archive Collected Data

0.001 Archive via Utility

0.002 Archive via Library

0.003 Archive via Custom Method

T1123 Audio Capture

T1119 Automated Collection

T1185 Browser Session Hijacking

T1115 Clipboard Data

T1530 Data from Cloud Storage

T1602 Data from Configuration Repository

0.001 SNMP (MIB Dump)

0.002 Network Device Configuration Dump

T1213 Data from Information Repositories

0.001 Confluence

0.002 Sharepoint

0.003 Code Repositories

T1005 Data from Local System

T1039 Data from Network Shared Drive

T1025 Data from Removable Media

T1074 Data Staged

0.001 Local Data Staging

0.002 Remote Data Staging

T1114 Email Collection

0.001 Local Email Collection

0.002 Remote Email Collection

0.003 Email Forwarding Rule

T1056 Input Capture

0.001 Keylogging

0.002 GUI Input Capture

0.003 Web Portal Capture

0.004 Credential API Hooking

T1113 Screen Capture

T1125 Video Capture

Command and Control

T1071 Application Layer Protocol

0.001 Web Protocols

0.002 File Transfer Protocols

0.003 Mail Protocols

0.004 DNS

T1092 Communication Through Removable Media

T1659 Content Injection

T1132 Data Encoding

0.001 Standard Encoding

0.002 Non-Standard Encoding

T1001 Data Obfuscation

0.001 Junk Data

0.002 Steganography

0.003 Protocol Impersonation

T1568 Dynamic Resolution

0.001 Fast Flux DNS

0.002 Domain Generation Algorithms

0.003 DNS Calculation

T1573 Encrypted Channel

0.001 Symmetric Cryptography

0.002 Asymmetric Cryptography

T1008 Fallback Channels

T1665 Hide Infrastructure

T1105 Ingress Tool Transfer

T1104 Multi-Stage Channels

T1095 Non-Application Layer Protocol

T1571 Non-Standard Port

T1572 Protocol Tunneling

T1090 Proxy

0.001 Internal Proxy

0.002 External Proxy

0.003 Multi-hop Proxy

0.004 Domain Fronting

T1219 Remote Access Software

T1205 Traffic Signaling

0.001 Port Knocking

0.002 Socket Filters

T1102 Web Service

0.001 Dead Drop Resolver

0.002 Bidirectional Communication

0.003 One-Way Communication

Exfiltration

T1020 Automated Exfiltration

0.001 Traffic Duplication

T1030 Data Transfer Size Limits

T1048 Exfiltration Over Alternative Protocol

0.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol

0.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

0.003 Exfiltration Over Unencrypted Non-C2 Protocol

T1041 Exfiltration Over C2 Channel

T1011 Exfiltration Over Other Network Medium

0.001 Exfiltration Over Bluetooth

T1052 Exfiltration Over Physical Medium

0.001 Exfiltration over USB

T1567 Exfiltration Over Web Service

0.001 Exfiltration to Code Repository

0.002 Exfiltration to Cloud Storage

0.003 Exfiltration to Text Storage Sites

0.004 Exfiltration Over Webhook

T1029 Scheduled Transfer

T1537 Transfer Data to Cloud Account

Impact

T1531 Account Access Removal

T1485 Data Destruction

T1486 Data Encrypted for Impact

T1565 Data Manipulation

0.001 Stored Data Manipulation

0.002 Transmitted Data Manipulation

0.003 Runtime Data Manipulation

T1491 Defacement

0.001 Internal Defacement

0.002 External Defacement

T1561 Disk Wipe

0.001 Disk Content Wipe

0.002 Disk Structure Wipe

T1499 Endpoint Denial of Service

0.001 OS Exhaustion Flood

0.002 Service Exhaustion Flood

0.003 Application Exhaustion Flood

0.004 Application or System Exploitation

T1657 Financial Theft

T1495 Firmware Corruption

T1490 Inhibit System Recovery

T1498 Network Denial of Service

0.001 Direct Network Flood

0.002 Reflection Amplification

T1496 Resource Hijacking

T1489 Service Stop

T1529 System Shutdown/Reboot