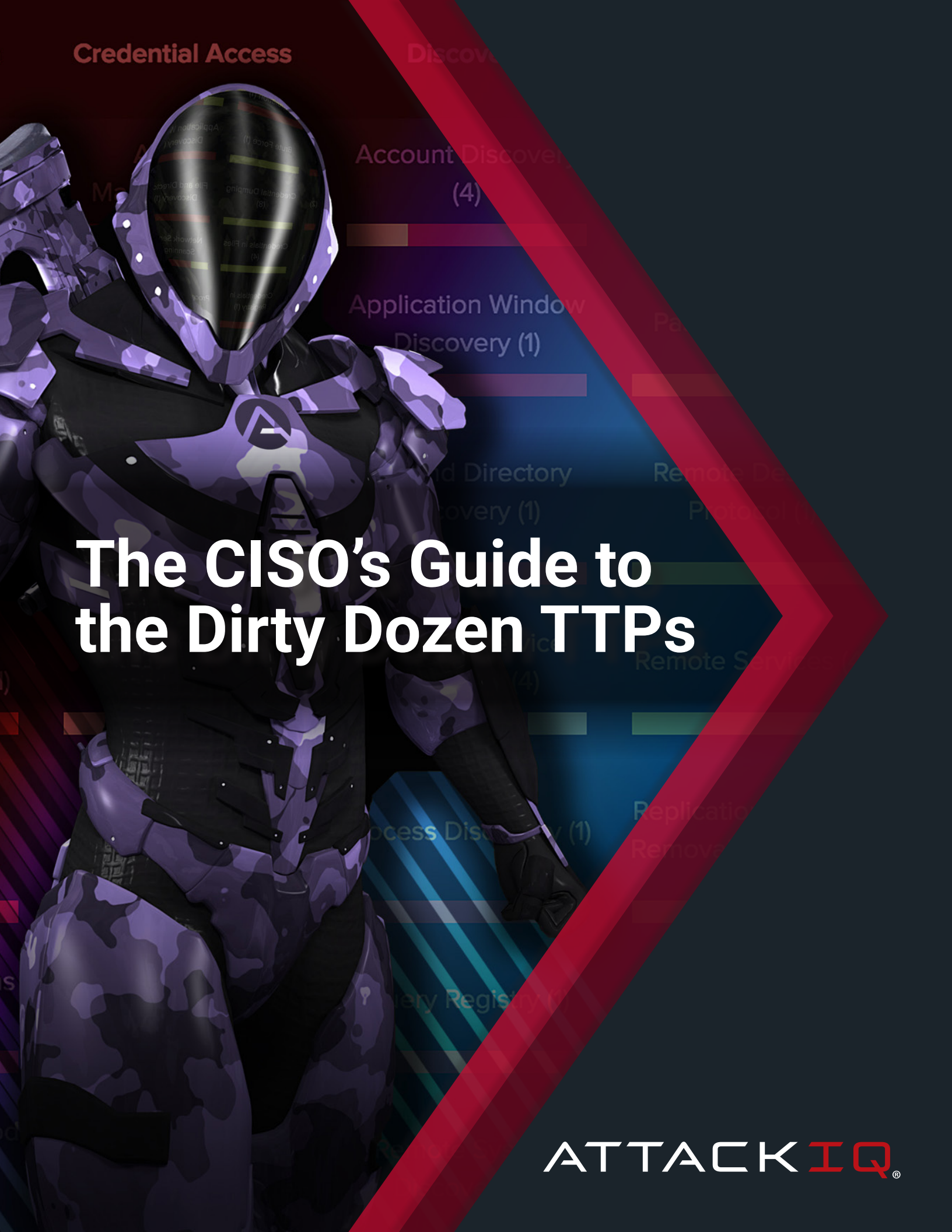


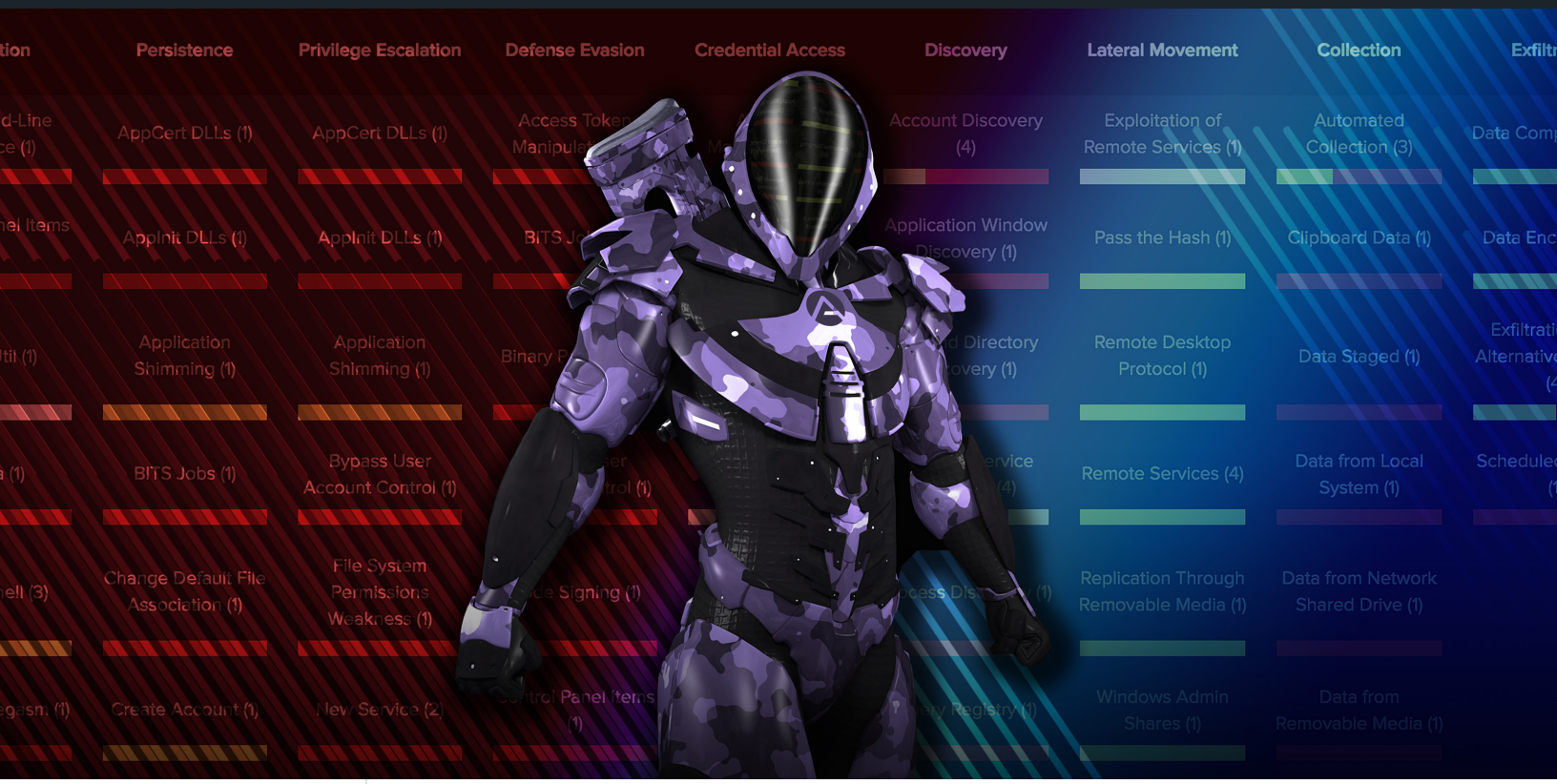
The CISO's Guide to the Dirty Dozen TTPs

ATTACKIQ®

Contents

Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.



Executive Summary

This report, the CISO's Guide to the Dirty Dozen TTPs (Tactics, Techniques, and Procedures) presents research data assembled by AttackIQ. This research report identifies the most prevalent tactics, techniques, and procedures that our data indicate remain viable and unmitigated by security controls present many of the tested installations. Many of these users have the requisite security controls in place to block the use of these techniques but, in quite a few cases, do not have them configured correctly.

The user base surveyed is confidential but includes a broad international mix of government agencies, commercial enterprise customers, channel partners, and managed security service providers using a breach and attack simulation platform.

The tactics, techniques, and procedures are categorized by the current MITRE ATT&CK matrix. These were then operationalized by the AttackIQ breach and attack simulation (BAS) platform which provided the results in this report. The AttackIQ platform enables you to operationalize and automate the MITRE ATT&CK matrix for continuous breach and attack simulation (BAS).

Our report will also share information about suggested mitigations, map these techniques to known threat groups, and provide a brief overview of MITRE ATT&CK. Finally, we will also share an overview of our BAS platform and the benefits it provides. You can also review a summary of the report contents in an 18-minute video presented by our engineering team, available here on youtube: **https://www.youtube.com/watch?v=79G17TOG00k&t=8s**

An Introduction to MITRE ATT&CK™

MITRE ATT&CK is, in both depth and breadth, the largest attack knowledge base, providing suggested mitigation techniques, detection procedures, and other important technical information. MITRE has expanded the Kill Chain to include the widest variety of tactics that are then supported by detailed techniques. This organized approach enables you to methodically select and analyze attacks and to compare them to the capabilities of your security controls so that you can understand the gaps. Once understood, you can then rationally expand your security controls and adjust your budgets.

MITRE ATT&CK is the largest, most in-depth, organized, and strongly supported knowledge base of adversarial behavior. You can review your security controls and gain visibility into gaps in your defenses. Security management can rapidly and easily identify critical problems for remediation. This objective assessment provides a data-driven approach to prioritizing and scaling your cybersecurity program and budget.

The MITRE ATT&CK enterprise matrix provides a tabular view of all attacker tactics and techniques that might leverage Windows, Mac, and Linux environments. Across the top are headings listing the 12 tactics defined by MITRE ATT&CK. Listed below each of the 12 tactics is a column that shows nine to 67 techniques that might be used to implement a particular tactic. It is often that case that several techniques are used in one or more tactics. A tactic clearly defines the goals of the attacker. A technique describes the different ways that a cyber attacker can achieve the end goals of the tactic.

Operationalizing MITRE ATT&CK With Breach and Attack Simulation Platforms

Breach and Attack Simulation platforms allow enterprises to automatically simulate the full attack and expanded kill chain used by cyber attackers against enterprise infrastructure using software test points that allow testing across roaming laptops, user desktops, virtual machines or cloud infrastructure. The result is detailed reports of the status and performance of your security controls and processes as well as the personnel that support them. Once BAS allows you to find the performance gaps, you can strengthen your security posture and improve your incident response capabilities. BAS can validate that your enterprise security systems are performing against known attacker behaviors.

Most important, BAS platforms provide automation that enables the platforms to work autonomously and to scale to support the largest global enterprise. Support for live production environments enables you to see in real-time how changes to configurations or administration can open new vulnerabilities in your cyberdefense.

AttackIQ's BAS platform provides the setup of scenarios that are used to test your technology controls, validate your security posture, and instrument your environment. Scenarios will mimic malware and attack vectors so that you can confirm that your security controls are working as expected. The fast path to productivity is to test your existing security controls to validate they are performing as you expect.

The Dirty Dozen Scenario List

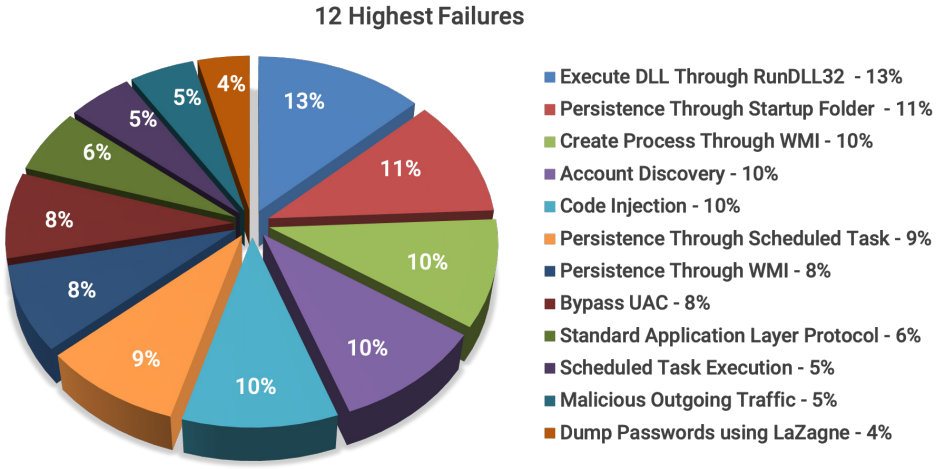
These following 12 tactics, techniques, and procedures (TTPs) are those which were most often not successfully mitigated by security controls that had the capability to do so. These 12 TTPs were structured as scenarios that were emulated and tested by our BAS platform.

This data is as reported by our cloud telemetry in our BAS platform. Each scenario can include more than one technique. Some attacks will require multiple steps to unfold.

These "Dirty Dozen" BAS scenarios include:

1. Execute DLL Through RunDLL32
2. Persistence Through Startup Folder
3. Create Process Through WMI
4. Account Discovery
5. Code Injection
6. Persistence Through Scheduled Task
7. Persistence Through WMI
8. Bypass UAC
9. Standard Application Layer Protocol
10. Scheduled Task Execution
11. Malicious Outgoing Traffic
12. Dump Passwords using LaZagne

This graph below shows the distribution among these 12 highest failure scenarios.



The Dirty Dozen - Technique IDs

These scenarios were then mapped back to the MITRE ATT&CK technique ID. This included 16 unique MITRE ATT&CK technique ID's that we feel that our user base should focus on mitigating.

These techniques and descriptions were extracted from the MITRE ATT&CK copyright materials and include:

TECHNIQUE ID	NAME	DESCRIPTION
T1085	Rundll32	The rundll32.exe program can be called to execute an arbitrary binary. Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor the execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe for normal operations.
T1060	Registry Run Keys/ Startup Folder	Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.
T1047	Windows Management Instrumentation	Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access. RPCS operates over port 135. An adversary can use WMI to interact with local and remote systems and use it as a means to perform many tactic functions, such as gathering information for Discovery and remote Execution of files as part of Lateral Movement.

T1218	Signed Binary Proxy Execution	Binaries signed with trusted digital certificates can execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files. This behavior may be abused by adversaries to execute malicious files that could bypass application whitelisting and signature validation on systems. This technique accounts for proxy execution methods that are not already accounted for within the existing techniques.
T1087	Account Discovery	Adversaries may attempt to get a listing of local system or domain accounts. For example, in Windows, commands that can acquire this information are net user, net group, and net localgroup using the Net utility or through the use of dsquery. If adversaries attempt to identify the primary user, currently logged-in user, or set of users that commonly uses a system, System Owner/User Discovery may apply. In Linux, local users can be enumerated through the use of the /etc/passwd file which is readable. In Mac, this same file is only used in single-user mode in addition to the /etc/master.passwd file.
T1055	Process Injection	Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/ network resources, and elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. In Windows, there are multiple approaches to injecting code into a live process. Windows implementations include Dynamic-link library (DLL) injection, Portable execution injection, Thread Execution hijacking, Asynchronous Procedure Call (APC) injection, and Thread Local Storage (TLS) callback injection.

T1053	Scheduled Task	Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a particular date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically requires being a member of the Administrators group on the remote system. An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.
T1084	Windows Management Instrumentation Event Subscription	Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system. Adversaries may attempt to evade detection of this technique by compiling WMI scripts into Windows Management Object (MOF) files (.mof extension). Examples of events that may be subscribed to are the wall clock time or the computer's uptime. Several threat groups have reportedly used this technique to maintain persistence.

T1088	Bypass User Account Control	Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs are allowed to elevate privileges or execute some elevated COM objects without prompting the user through the UAC notification box. An example of this is the use of rundll32.exe to load a specifically crafted DLL which loads an auto-elevated COM object and performs a file operation in a protected directory that would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user. Adversaries can use these techniques to elevate privileges to administrator if the target process is unprotected. Many methods have been discovered to bypass UAC. The Github readme page for UACMe contains an extensive list of methods that have been discovered and implemented within UACMe, but it may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as: › **eventvwr.exe can auto-elevate and execute a specified binary or script.** Another bypass is possible through some Lateral Movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on lateral systems and default to high integrity.

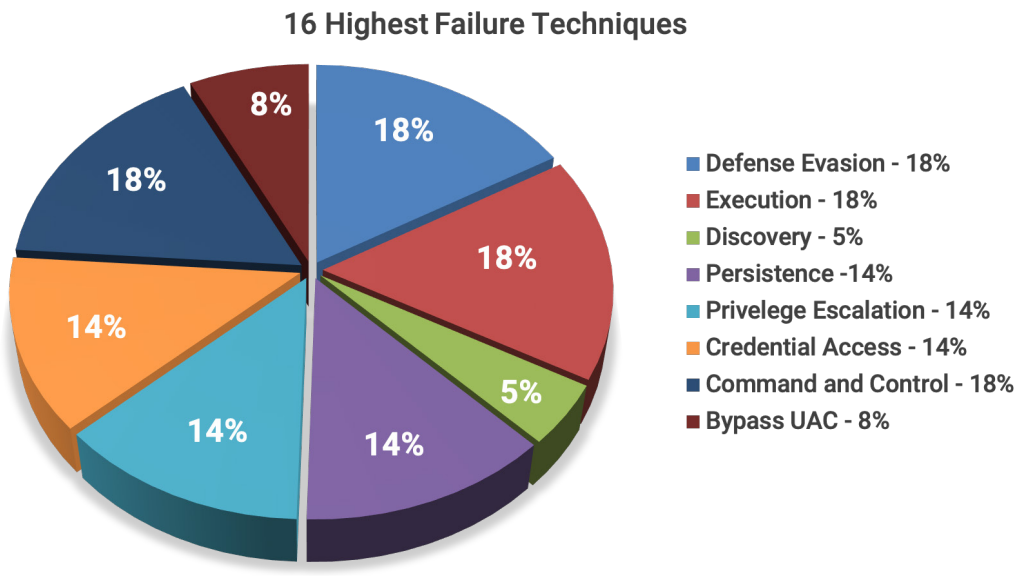
T1043	Commonly Used Port	Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as: › TCP:80 (HTTP) › TCP:443 (HTTPS) › TCP:25 (SMTP) › TCP/UDP:53 (DNS) They may use the protocol associated with the port or a completely different protocol. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are › TCP/UDP:135 (RPC) › TCP/UDP:22 (SSH) › TCP/UDP:3389 (RDP)
T1071	Standard Application Layer Protocol	Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
T1065	Uncommonly Used Port	Adversaries may conduct C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.

T1090	Connection Proxy	Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. Adversaries use these types of proxies to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resilience in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. External connection proxies are used to mask the destination of C2 traffic and are typically implemented with port redirectors. Compromised systems outside of the victim environment may be used for these purposes, as well as purchased infrastructure such as cloud-based resources or virtual private servers. Proxies may be chosen based on the low likelihood that a connection to them from a compromised system would be investigated. Victim systems would communicate directly with the external proxy on the internet and then the proxy would forward communications to the C2 server. Internal connection proxies can be used to consolidate internal connections from compromised systems. Adversaries may use a compromised internal system as a proxy in order to conceal the true destination of C2 traffic. The proxy can redirect traffic from compromised systems inside the network to an external C2 server, making the discovery of malicious traffic difficult. Additionally, the network can be used to relay information from one system to another in order to avoid broadcasting traffic to all systems.

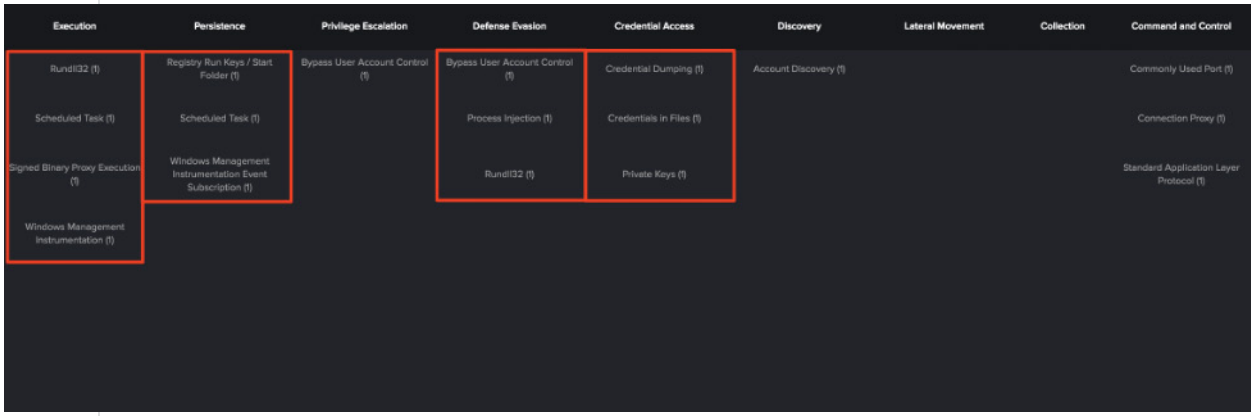
T1081	Credentials in Files	Adversaries may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords. It is possible to extract passwords from backups or saved virtual machines through Credential Dumping. Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller. In cloud environments, authenticated user credentials are often stored in local configuration and credential files. In some cases, these files can be copied and reused on another machine or the contents can be read and then used to authenticate without needing to copy any files.
T1145	Private Keys	Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures. Adversaries may gather private keys from compromised systems for use in authenticating to Remote Services like SSH or for use in decrypting other collected files such as email. Common key and certificate file extensions include .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, and .asc. Adversaries may also look in common key directories, such as ~/.ssh for SSH keys on * nix-based systems or C:\ Users(username).ssh\ on Windows. Private keys should require a password or passphrase for operation, so an adversary may also use Input Capture for keylogging or attempt to Brute Force the passphrase off-line. Adversary tools have been discovered that search compromised systems for file extensions relating to cryptographic keys and certificates.

T1003	Credential Dumping	Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information. Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well. Attackers may use the Windows Security Accounts Manager (SAM), Cached Credentials, Local System Authority (LSA) Secrets, NTDS from Domain Controller, Group Policy Preference (GPP) Files, Service Principal Names (SPNs), and Plain Text Credentials, and DCSync.

This graph below shows the distribution among the 16 highest failure techniques.



You can also see here below how these map to the tactics in the MITRE ATT&CK matrix. Here we can also see the tactics. Credential access is the area where we have noted the most misconfiguration and failure due to credential theft.

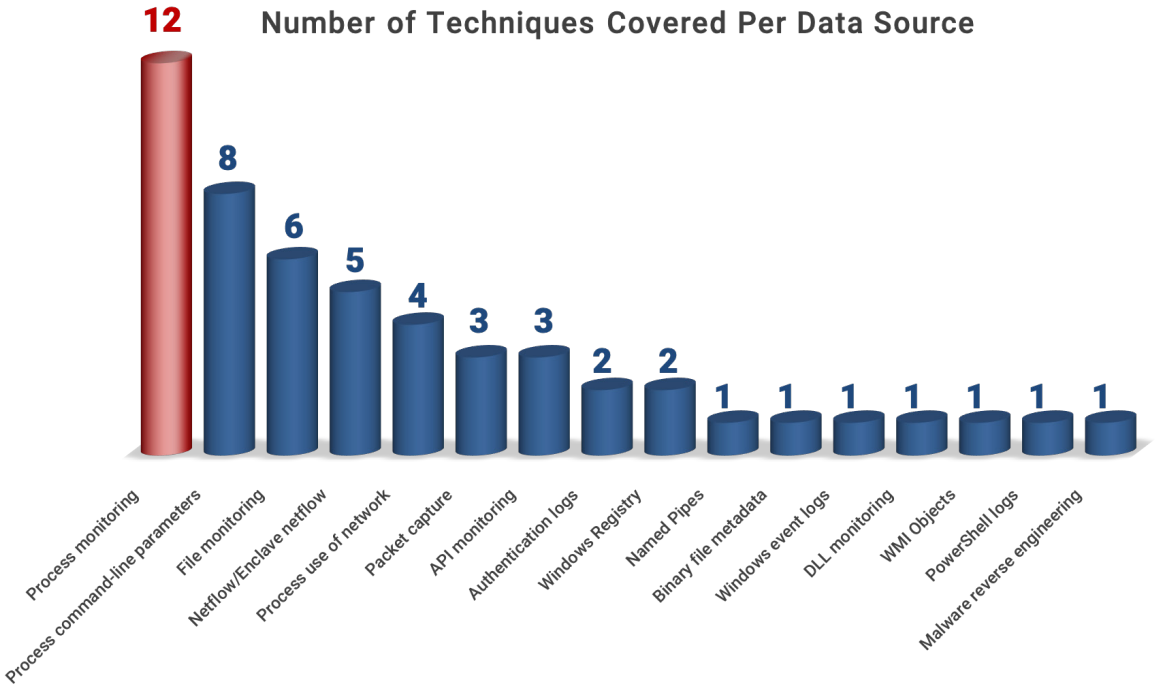


Data Sources to Identify Activity

We also show the data sources which you as an organization can use to identify this activity. For example, out of the 16 techniques, **process monitoring covers 12 of the 16 techniques**.

DATA SOURCES	NUMBER OF TECHNIQUES COVERED
Process monitoring	12
Process command-line parameters	8
File monitoring	6
Netflow/Enclave netflow	5
Process use of network	4
Packet capture	3
API monitoring	3
Authentication logs	2
Windows Registry	2
Named Pipes	1
Binary file metadata	1
Windows event logs	1
DLL monitoring	1
WMI Objects	1
PowerShell logs	1
Malware reverse engineering	1
System calls	1

Here you can see this graphically:



If you are just monitoring basic processes or syslog and using that as a basis to create rules, you will have pretty effective coverage of these techniques that most users are not effectively covering today. Customers are beginning to ingest syslog, windows event logs, and windows API logs and are writing rule sets around these. You can get good rules from the user community in Github that can help you to mitigate these techniques.

You can also see which attack groups are known to use various techniques. It is useful to identify those actors that are most prevalent to your organization and industry based on current events and the threat intelligence you possess.

Recommendations

Review the Dirty Dozen MITRE ATT&CK technique IDs that are being used by the largest number of bad actors and determine if your security controls are configured to mitigate against these techniques. This will reduce your risk and improve the resilience of your cyber defenses.

As mentioned earlier, they are:

- Execute DLL Through RunDLL32
- Persistence Through Startup Folder
- Create Process Through WMI
- Account Discovery
- Code Injection
- Persistence Through Scheduled Task
- Persistence Through WMI
- Bypass UAC
- Standard Application Layer Protocol
- Scheduled Task Execution
- Malicious Outgoing Traffic
- Dump Passwords using LaZagne

AttackIQ Breach and Attack Simulation provide a powerful platform with which to implement and operationalize MITRE ATT&CK. The value provided by a BAS platform can be compelling for you and your organization and will enable you to continuously validate the performance of your production security controls, as configured, against these scenarios and many more.

To find out more about how to operationalize MITRE ATT&CK using AttackIQ BAS, please reach out to **info@attackiq.com** or visit us at **www.attackiq.com**.

ATTACKIQ
U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

AttackIQ, a leader in the emerging market of breach and attack simulation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ® supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit **www.attackiq.com**. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.