MITRE ATT&CK COVERAGE

SNAP DEFENSE AGB CYBER DIVISION

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND AND CONTROL
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multilayer Encryption
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Port Knocking
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Remote Access Tools
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote File Copy
	PowerShell	Dylib Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Standard Application Layer Protocol
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Cryptographic Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Non-Application Layer Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Uncommonly Used Port
	Scheduled Task	Hooking	SID-History Injection	File Permissions Modification		System Time Discovery				Web Service
	Scripting	Hypervisor	Scheduled Task	File System Logical Offsets						
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	HISTCONTROL						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Hidden Files and Directories						
	Source	LSASS Driver	Sudo	Hidden Users						
	Space after Filename	Launch Agent	Sudo Caching	Hidden Window						
	Third-party Software	Launch Daemon	Valid Accounts	Image File Execution Options Injection						
	Trap	Launchctl	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Local Job Scheduling		Indicator Removal from Tools						
	User Execution	Login Item		Indicator Removal on Host						
	Windows Management Instrumentation	Logon Scripts		Indirect Command Execution						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUtil						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		Launchctl						
		Path Interception		Masquerading						
		Plist Modification		Modify Registry						
		Port Knocking		Mshta						
		Port Monitors		NTFS File Attributes						
		Rc.common		Network Share Connection Removal						
		Re-opened Applications		Obfuscated Files or Information						
		Redundant Access		Plist Modification						
		Registry Run Keys / Startup Folder		Port Knocking						
		SIP and Trust Provider Hijacking		Process Doppelgänging						
		Scheduled Task		Process Hollowing						
		Screensaver		Process Injection						
		Security Support Provider		Redundant Access						
		Service Registry Permissions Weakness		Regsvcs/Regasm						
		Setuid and Setgid		Regsvr32						
		Shortcut Modification		Rootkit						
		Startup Items		Rundll32						
		System Firmware		SIP and Trust Provider Hijacking						
		Time Providers		Scripting						
		Trap		Signed Binary Proxy Execution						
		Valid Accounts		Signed Script Proxy Execution						
		Web Shell		Software Packing						
		Windows Management Instrumentation Event Subscription		Space after Filename						
		Winlogon Helper DLL		Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						
				XSL Script Processing						

= supported by SNAP-Defense

WWW.AGBCYBER.COM For more information on MITRE ATT&CK framework: atack.mitre.org

EXECUTION 79%

- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- LSASS Driver
- Launchctl
- Local Job Scheduling
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

PERSISTENCE 50%

- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- LC_LOAD_DYLIB Addition
- LSASS Driver
- Launch Agent
- Launch Daemon
- Launchctl
- Local Job Scheduling
- Login Item
- Logon Scripts
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Startup Folder
- SIP and Trust Provider Hijacking
- Scheduled Task
- Screensaver
- Security Support Provider
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- Startup Items
- System Firmware
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

= supported by SNAP-Defense

AGB CYBER DIVISION

WWW.AGBCYBER.COM

INITIAL ACCESS 90%	PRIVILEGE ESCALATION 54%	CREDENTIAL ACCESS 68%	DISCOVERY 100%
Drive-by Compromise	Access Token Manipulation	Account Manipulation	Account Discovery
Exploit Public-facing Application	Accessibility Features	Bash History	Application Window Discovery
Hardware Additions	AppCert DLLs	Brute Force	Browser Bookmark Discovery
Replication Through Removable Media	AppInit DLLs	Credential Dumping	File and Directory Discovery
Spearphishing Attachment	Application Shimming	Credentials in Files	Network Service Scanning
Spearphising Link	Bypass User Account Control	Credentials in Registry	Network Share Discovery
Spearphishing via Service	DLL Search Order Hijacking	Exploitation for Credential Access	Network Sniffling
Supply Chain Compromise	Dylib Hijacking	Forced Authentication	Password Policy Discovery
Trusted Relationship	Exploitation for Privilege Escalation	Hooking	Peripheral Device Discovery
Valid Accounts	Extra Window Memory Injection	Input Capture	Permission Groups Discovery
	File System Permissions Weakness	Input Prompt	Process Discovery
	Hooking	Kerberoasting	Query Registry
	Image File Execution Options Injection	Keychain	Remote System Discovery
	Launch Daemon	LLMNR/NBT-NS Poisoning Network Sniffling	Security Software Discovery
	New Service	Password Filter DLL	System Information Discovery
	Path Interception	Private Keys	System Network Configuration Discovery
	Plist Modification	Securityd Memory	System Network Connections Discovery
	Port Monitors	Two-Factor Authentication Interception	System Owner/User Discovery
	Process Injection		System Service Discovery
	SID-History Injection		System Time Discovery
	Scheduled Task		
	Service Registry Permissions Weakness		
	Setuid and Setgid		
	Startup Items		
	Sudo Caching		
	Sudo		
	Valid Accounts		
	Web Shell		

= supported by SNAP-Defense

WWW.AGBCYBER.COM

DEFENSE EVASION 71%

- Access Token Manipulation
- BITS Jobs
- Binary Padding
- Bypass User Account Control
- CMSTP
- Clear Command History
- Code Signing
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- DLL Search Order Hijacking
- DLL Side-Loading
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File Permissions Modification
- File System Logical Offsets
- Gatekeeper Bypass
- HISTCONTROL
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- LC_MAIN Hijacking
- Launchctl
- Masquerading
- Modify Registry
- Mshta
- NTFS File Attributes
- Network Share Connection Removal
- Obfuscated Files or Information
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- SIP and Trust Provider Hijacking
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Web Service
- XSL Script Processing

LATERAL MOVEMENT 88%

- AppleScript
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- SSH Hijacking
- Shared Webroot
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

COLLECTION 69%

- Audio Capture
- Automated Collection
- Clipboard Data
- Data Staged
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

= supported by SNAP-Defense

AGB CYBER DIVISION

WWW.AGBCYBER.COM

EXFILTRATION 100%

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

COMMAND AND CONTROL 86%

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Fallback Channels
- Multi-Stage Channels
- Multi-hop Proxy
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

= supported by SNAP-Defense

AGB CYBER DIVISION

WWW.AGBCYBER.COM