An ATT&CK Review of 200 Hybrid-Analysis Submissions

James Lerud
Manager, Behavior Research Team

Introduction

> Who/What/When/Where/Why

- Scope
- Findings
- Open Questions

James.Lerud @ gmail | verodin .com

@Warlockobama

Dad Joke

Introduction Continued

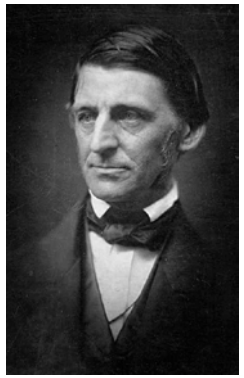
consistent adjective

con·sis·tent | \kən-ˈsi-stənt\

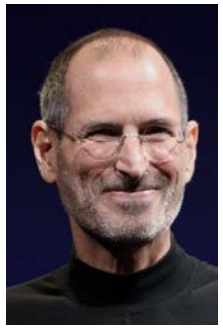
Definition of *consistent*

1 a : marked by harmony, regularity, or steady continuity : free from variation or contradiction

// a consistent style in painting



"A foolish consistency is the hobgoblin of little minds, adored by little statesmen and philosophers and divines."-Ralph Waldo Emerson



"If you want to use a framework to make educated decisions it better be consistent"-Steve Jobs

Introduction Continued

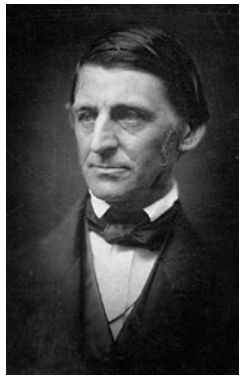
consistent adjective

con·sis·tent | \kən-ˈsi-stənt\

Definition of *consistent*

1 a : marked by harmony, regularity, or steady continuity : free from variation or contradiction

// a *consistent* style in painting



"A foolish consistency is the hobgoblin of little minds, adored by little statesmen and philosophers and divines."-Ralph Waldo Emerson

"If you want to use a framework to make educated decisions it better be consistent"-Me ~~Steve Jobs~~

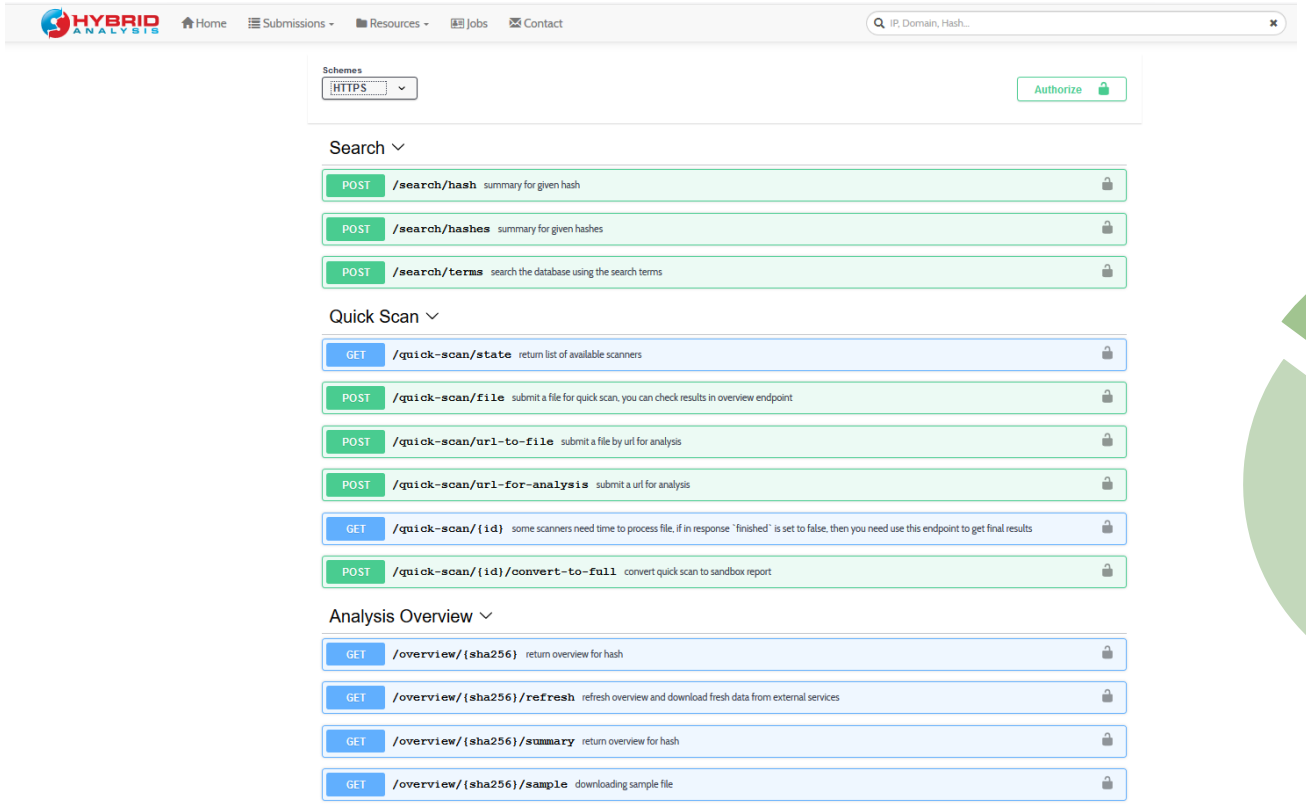
Introduction Continued

+

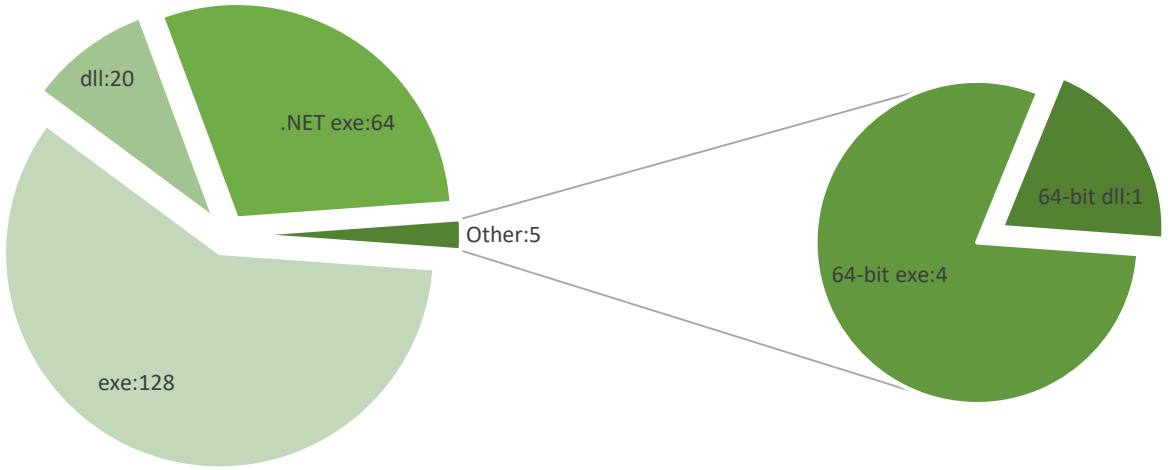
=

ATT&CK ?

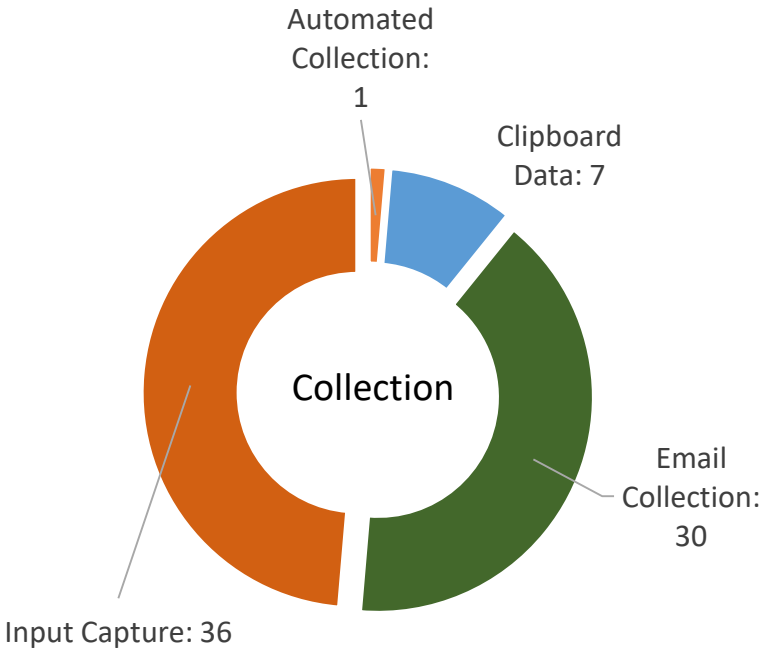
Scope

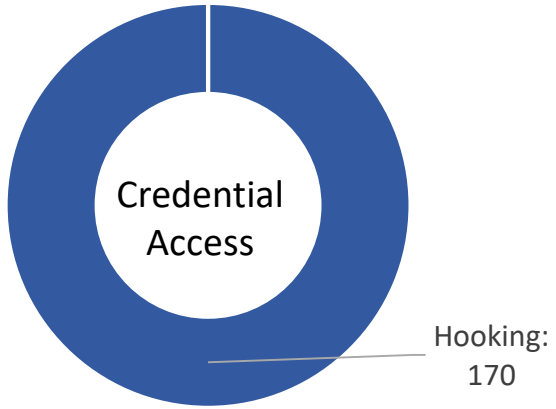


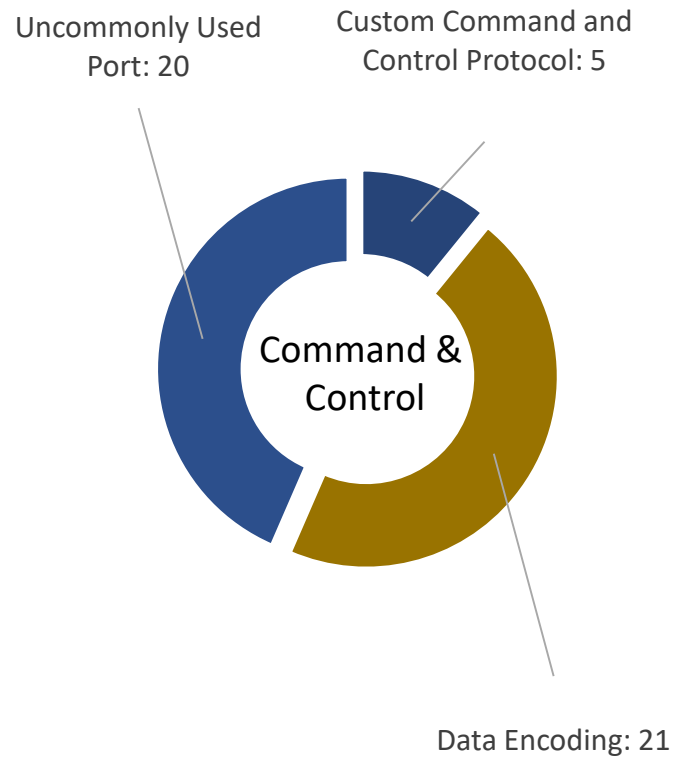
217 Samples



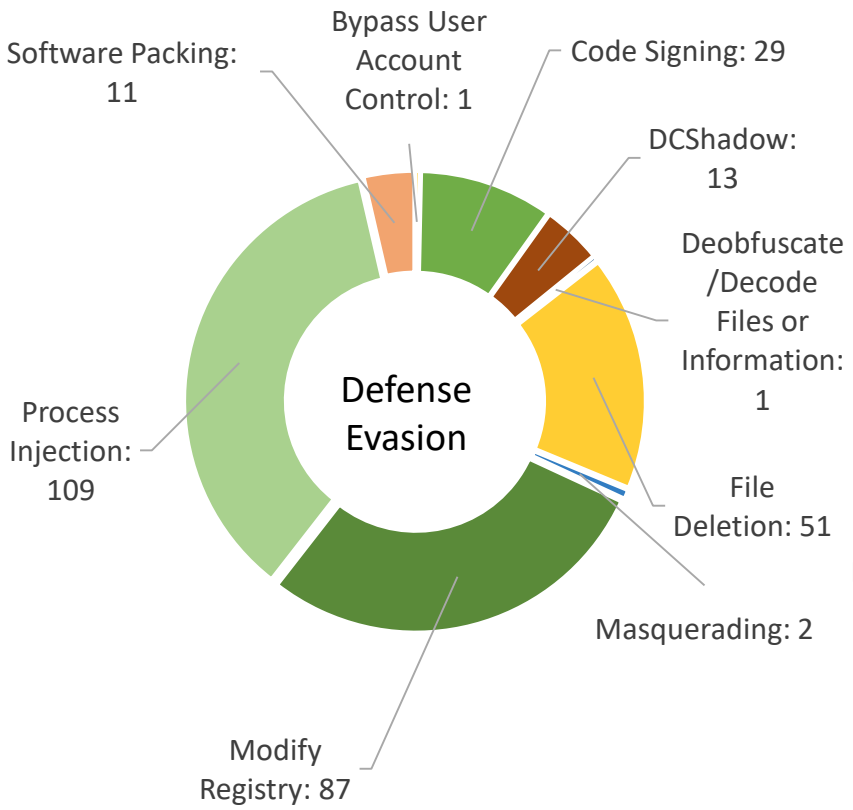
A Look @ Results

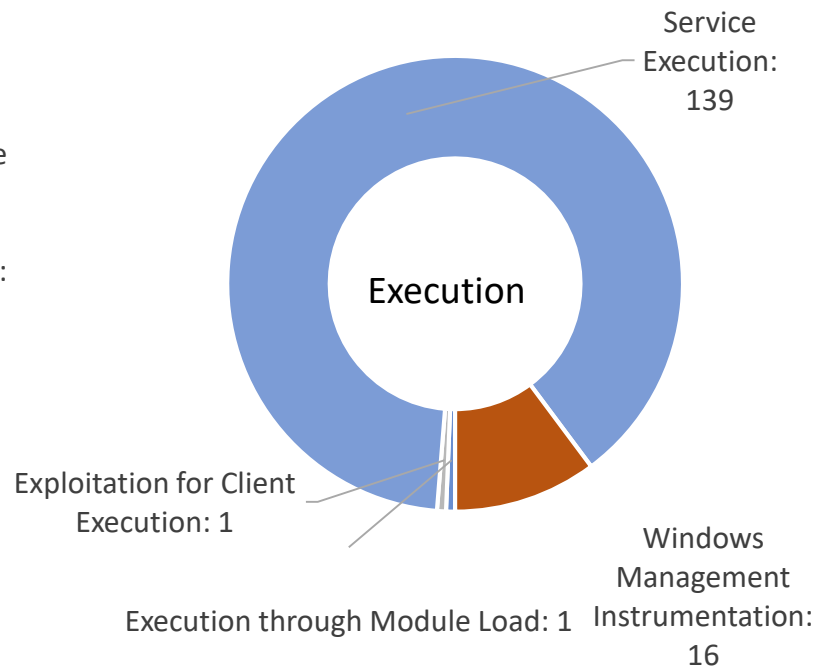


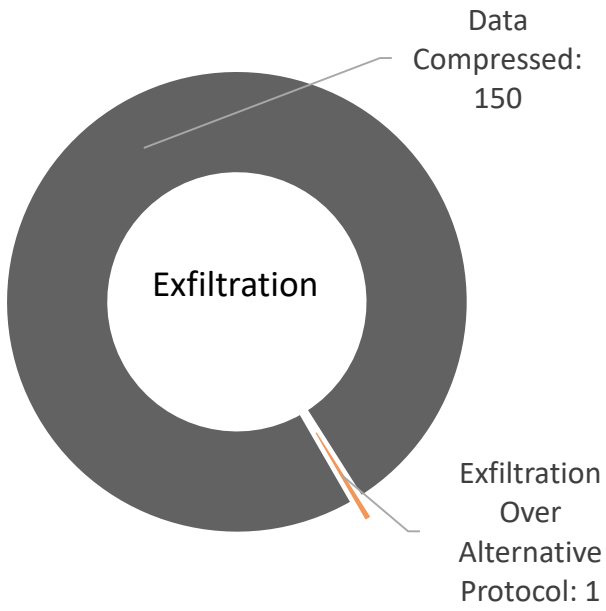




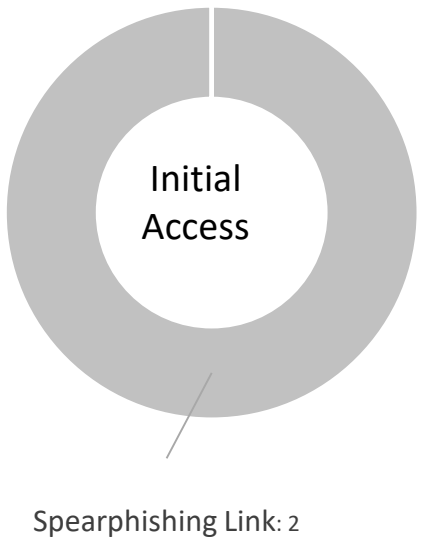
A Look @ Results

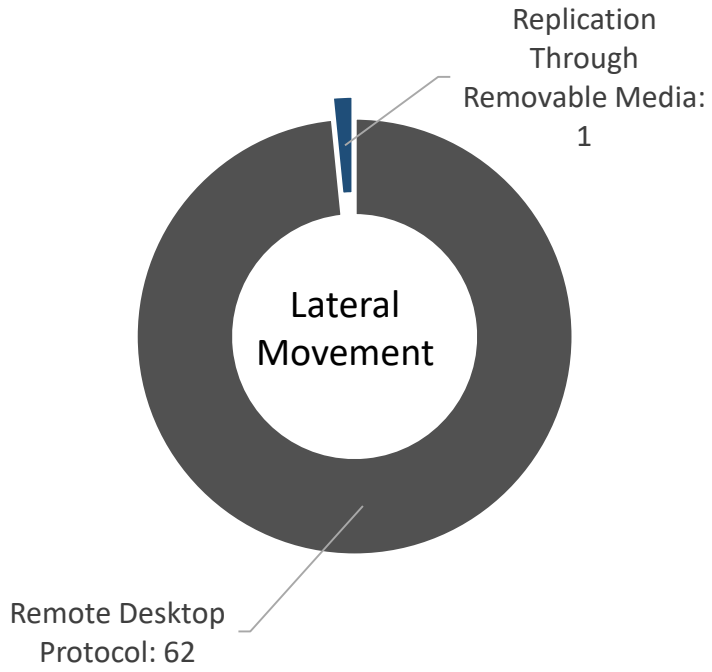


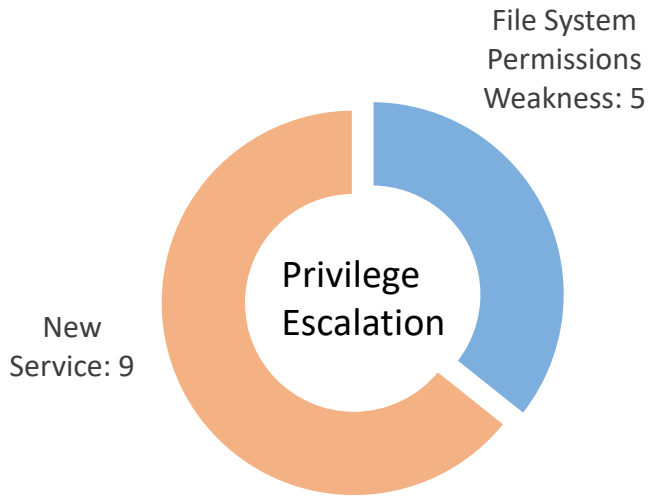




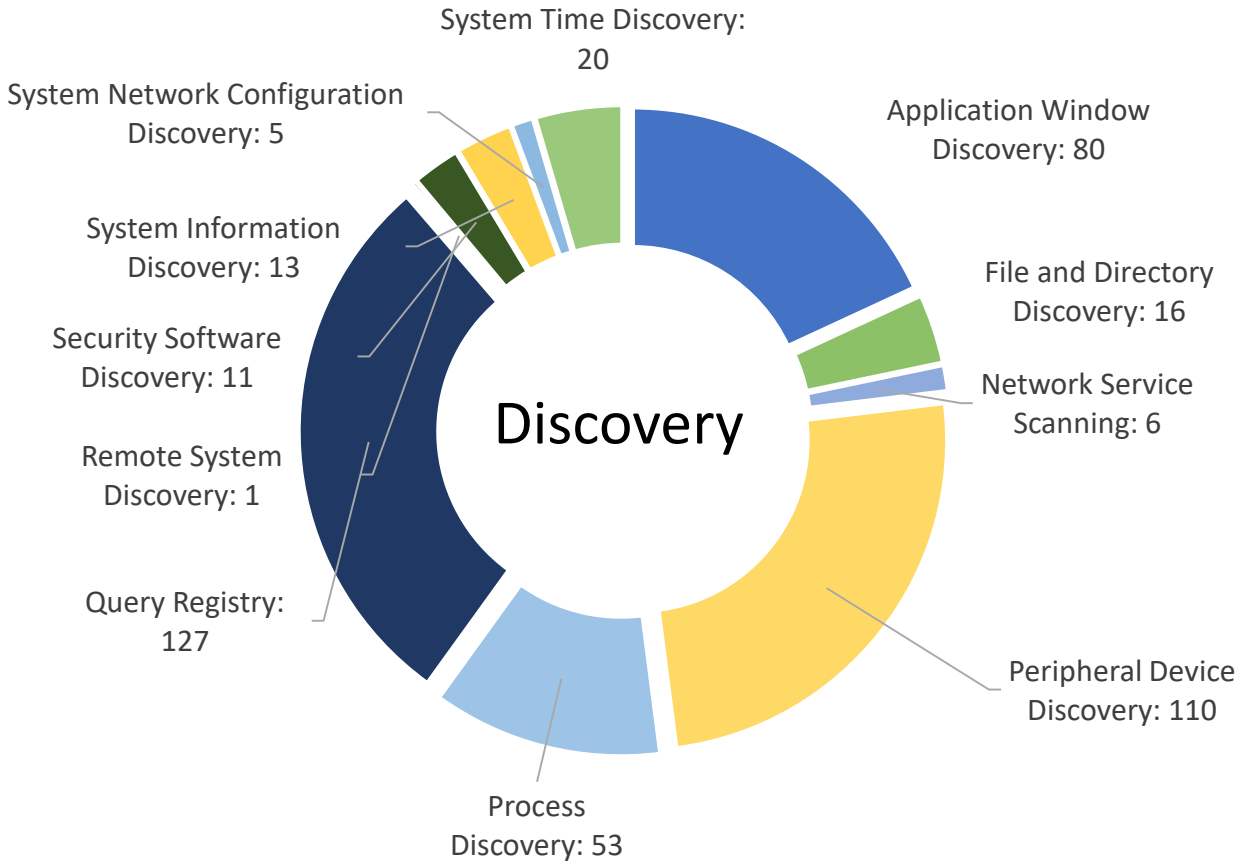
A Look @ Results … Continued

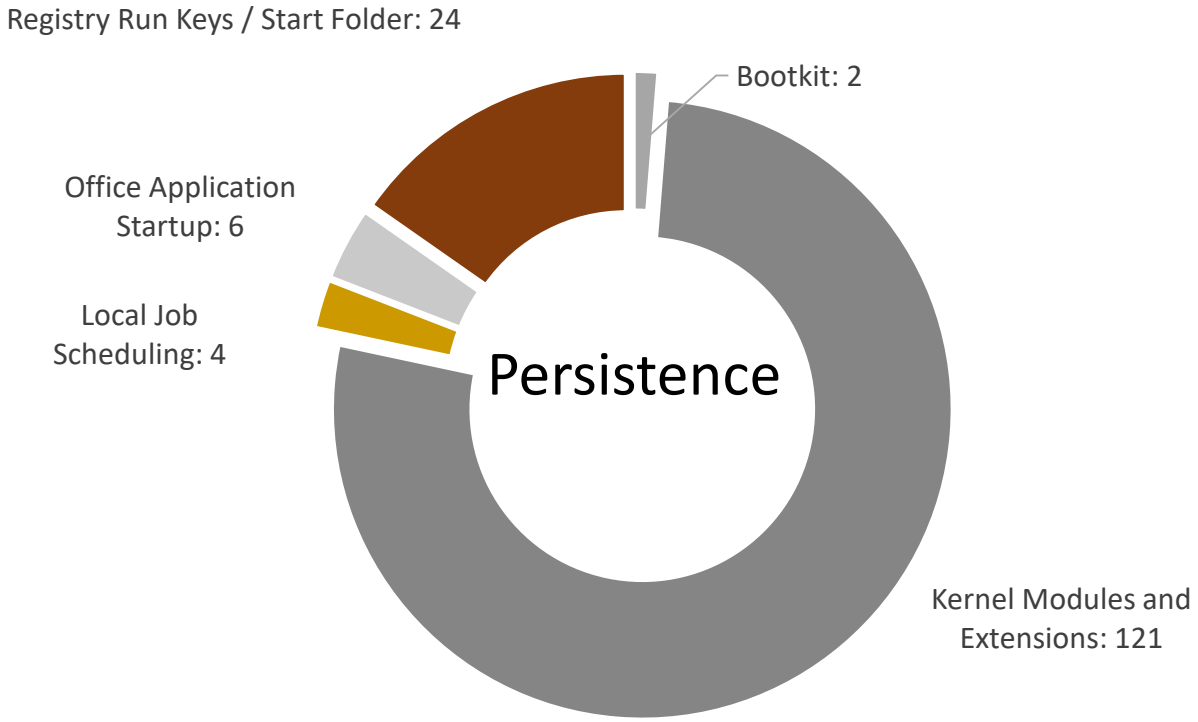






A Look @ Results … Continued





Matrix View

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


VERODIN
Take-Aways, Questions