Observation of ATT&CK techniques in Windows malware

From: Oosthoek, K., & Doerr, C. (2019). SoK: ATT&CK Techniques and Trends in Windows Malware. Proceedings of SecureComm 2019, 15th EAI International Conference on Security and Privacy in Communication Networks

Initial Access	Execution	Persistence (1)	Persistence (2)	Privilege Escalation	Defence Evasion (1)	Defence Evasion (2)	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Drive-by Compromise	CMSTP	Accessibility Features	Logon Scripts	Access Token Manipulation	Access Token Manipulation	Install Root Certificate	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	LSASS Driver	Accessibility Features	Binary Padding	InstallUtil	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	Modify Existing Service	AppCert DLLs	BITS Jobs	Masquerading	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Netsh Helper DLL	AppInit DLLs	Bypass User Account Control	Modify Registry	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	New Service	Application Shimming	CMSTP	Mshta	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Office Application Startup	Bypass User Account Control	Code Signing	Network Share Connection Removal	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	Path Interception	DLL Search Order Hijacking	Compiled HTML File	NTFS File Attributes	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Port Monitors	Exploitation for Privilege Escalation	Component Firmware	Obfuscated Files or Information	Hooking	Password Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Redundant Access	Extra Window Memory Injection	Component Object Model Hijacking	Process Doppelgänging	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Registry Run Keys / Startup Folder	File System Permissions Weakness	Control Panel Items	Process Hollowing	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	LSASS Driver	Component Firmware	Scheduled Task	Hooking	DCShadow	Process Injection	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Screensaver	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Redundant Access	Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Multiband Communication
	PowerShell	Create Account	Security Support Provider	New Service	Disabling Security Tools	Regsvcs/Regasm	Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvcs/Regasm	DLL Search Order Hijacking	Service Registry Permissions Weakness	Path Interception	DLL Search Order Hijacking	Regsvr32	Private Keys	Security Software Discovery	Windows Admin Shares			Remote Access Tools
	Regsvr32	External Remote Services	Shortcut Modification	Port Monitors	DLL Side-Loading	Rootkit	Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Remote File Copy
	Rundll32	File System Permissions Weakness	SIP and Trust Provider Hijacking	Process Injection	Exploitation for Defense Evasion	Rundll32		System Network Configuration Discovery				Standard Application Layer Protocol
	Scheduled Task	Hidden Files and Directories	System Firmware	Scheduled Task	Extra Window Memory Injection	Scripting		System Network Connections Discovery				Standard Cryptographic Protocol
	Scripting	Hooking	Time Providers	Service Registry Permissions Weakness	File Deletion	Signed Binary Proxy Execution		System Owner/User Discovery				Standard Non-Application Layer Protocol
	Service Execution	Hypervisor	Valid Accounts	SID-History Injection	File Permissions Modification	Signed Script Proxy Execution		System Service Discovery				Uncommonly Used Port
	Signed Binary Proxy Execution	Image File Execution Options Injection	Web Shell	Valid Accounts	File System Logical Offsets	SIP and Trust Provider Hijacking		System Time Discovery				Web Service
	Signed Script Proxy Execution		Windows Management Instrumentation Event Subscription	Web Shell	Hidden Files and Directories	Software Packing						
	Third-party Software		Winlogon Helper DLL		Image File Execution Options Injection	Template Injection						
	Trusted Developer Utilities				Indicator Blocking	Timestomp						
	User Execution				Indicator Removal from Tools	Trusted Developer Utilities						
	Windows Management Instrumentation				Indicator Removal on Host	Valid Accounts						
	Windows Remote Management				Indirect Command Execution	Web Service						
	XSL Script Processing					XSL Script Processing						

Legend
950 observations
450 observations
300 observations
50 observations
10 observations

MITRE | ATT&CK™

krisk.io