about

Fleury REvil

domain

Enterprise ATT&CK v9

platforms

Windows, Office 365, SaaS, IaaS, PRE, Network

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	**Acquire Infrastructure**	Drive-by Compromise	**Command and Scripting Interpreter**	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	**Exploitation of Remote Services**	Archive Collected Data	Application Layer Protocol	**Automated Exfiltration**	Account Access Removal
Gather Victim Host Information	**Compromise Accounts**	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	**Data Encrypted for Impact**
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	**Remote Service Session Hijacking**	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	**Phishing**	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Forge Web Credentials	Cloud Service Dashboard	**Remote Services**	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	**Domain Policy Modification**	**Domain Policy Modification**	Input Capture	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository	**Encrypted Channel**	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Software Deployment Tools	Create Account	Escape to Host	Execution Guardrails	Man-in-the-Middle	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	System Services	Create or Modify System Process	Event Triggered Execution	Exploitation for Defense Evasion	Modify Authentication Process	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		**Valid Accounts**	User Execution	Event Triggered Execution	Exploitation for Privilege Escalation	File and Directory Permissions Modification	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow	Hide Artifacts	OS Credential Dumping	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
				Hijack Execution Flow	Process Injection	Hijack Execution Flow	Steal Application Access Token	Network Sniffing		Data Staged	Non-Standard Port		**Resource Hijacking**
				Implant Internal Image	Scheduled Task/Job	Impair Defenses	Steal or Forge Kerberos Tickets	Password Policy Discovery		Email Collection	Protocol Tunneling		Service Stop
				Modify Authentication Process	**Valid Accounts**	Indicator Removal on Host	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture	Proxy		System Shutdown/Reboot
				Office Application Startup		Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery		Man in the Browser	**Remote Access Software**		
				Pre-OS Boot		Masquerading	Unsecured Credentials	Process Discovery		Man-in-the-Middle	Traffic Signaling		
				Scheduled Task/Job		Modify Authentication Process		Query Registry		Screen Capture	Web Service		
				Server Software Component		Modify Cloud Compute Infrastructure		Remote System Discovery		Video Capture			
				Traffic Signaling		**Modify Registry**		Software Discovery					
				Valid Accounts		Modify System Image		System Information Discovery					
						Network Boundary Bridging		System Location Discovery					
						Obfuscated Files or Information		System Network Configuration Discovery					
						Pre-OS Boot		System Network Connections Discovery					
						Process Injection		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Signed Binary Proxy Execution		Virtualization/Sandbox Evasion					
						Signed Script Proxy Execution							
						Subvert Trust Controls							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							