about _____

domain

Enterprise ATT&CK v14

 1.0 1.2 1.4 1.6 1.8 2.0

			J			J				J			
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 Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Extitration	Account Access Removal
Gather Victim	Acquire	Drive-by	Command and	BITS Jobs	Access Token	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive	Communication Through Removable Media	Data Transfer	Data
Host Information Gather Victim	Infrastructure Compromise	Compromise Exploit Public-Facing	Scripting Interpreter Container	Boot or Logon	Manipulation Account		Credentials from	Window Discovery Browser Information	Lateral	Collected Data	Content	Size Limits Exhibitation Over	Destruction Data Encrypted
Identity Information	Accounts	Application	Administration Command	Autostart Execution	Manipulation	BITS Jobs	Password Stores	Discovery	Tool Transfer	Audio Capture	Injection	Alternative Protocol	for Impact
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Org Information Phishing for	Capabilities Exhibitish		Client Execution	Compromise Client	Initialization Scripts Create or Modify	Evasion Deobfuscate/Decode	Forge Web	Cloud Service	Replication Through		Obtuscation Dynamic	Other Network Medium Exfiltration Over	
Information	Accounts	Phishing	Communication	Software Binary	System Process	Files or Information	Credentials	Discovery	Removable Media	Clipboard Data	Resolution	Physical Medium	Disk Wipe
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Native AP1	Create Account	Domain Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases	Stage Capabilities	Supply Chain	Scheduled Task/Job	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration	Falback Channels	Scheduled Transfer	Financial Theft
Search Open	Capabilities	Compromise Trusted	Serverless	Event Triggered	Event Triggered	Domain Policy	Multi-Factor Authentication	Debugger	Shared Content Use Alternate Authentication Material	Repository Data from Information	Ingress	Transfer Data	Firmware
Websites/Domains Search Victim-Owned	-	Relationship	Execution	Execution	Execution Exploitation for	Modification		Evasion Device Driver	Material Material	Repositories Data from	Tool Transfer	to Cloud Account	Corruption Inhibit System
Search Victim-Owned Websites		Valid Accounts	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardralia	Multi-Factor Authentication Request Generation	Discovery		Local System	Multi-Stage Channels		Recovery
	-		Software Deployment Tools	Hjack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application		Network Denial of Service
			System	Implant	Process	File and Directory Permissions Modification	OS Credential	File and Directory	1	Data from	Layer Protocol Non-Standard		Resource
			Services	Internal Image Modify Authentication	Injection Scheduled	Modification	Dumping Steal Application	Discovery Group Policy	-	Removable Media	Port		Hijacking
			User Execution	Process	Scheduled TaskUob	Hide Artifacts	Access Token	Group Policy Discovery		Data Staged	Protocol Turneling		Service Stop
			Windows Management	Office Application	Valid Accounts	Hjack	Steal or Forge Authentication	Log		Ernal	Proxy	1	System
			nuovitensison	Startup		Execution Flow Impair	Certificates Steal or Forge	Enumeration Network Service		Collection	Remote Access	1	Shutdown/Reboot
				Power Settings	_	Defenses	Kerberos Tickets	Discovery		Input Capture	Software	-	
				Pre-OS Boot		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling		
				Scheduled Yask/Job		Indicator Removal	Unsecured Credentials	Network Sniffing		Video Capture	Web Service		
				Task/Job Server Software	1	Indirect Command	CHARTES	Password Policy	1				
				Component	-	Execution	4	Discovery	-				
				Traffic Signaling		Manquerading		Device Discovery					
				Valid Accounts		Modify Authentication Process		Permission Groups Discovery					
						Modify Cloud Compute	1	Process					
						Infrastructure Modify	-	Discovery	_				
						Registry		Query Registry					
						Modify System Image		Remote System Discovery					
						Network Boundary	1	Software					
						Bridging Obfuscated Files	-	Discovery System Information					
						or Information		Discovery					
						Plat File Modification		System Location Discovery					
						Pre-OS Boot	1	System Network Configuration Discovery	1				
						Pre-OS Boot Process	-	Discovery System Network	-				
						Injection		Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domein	1	System Service	1				
						Controller	-	Discovery System	-				
						Rootkit		Time Discovery					
						Subvert Trust Controls		Virtualization/Sandbox Evasion					
						System Binary	1		_				
						Proxy Execution System Script	-						
						Proxy Execution							
						Yemptate Injection							
						Traffic	1						
						Signaling Trusted	-						
						Developer Utilities Proxy Execution							
						Unused Unsupported Cloud Regions							
						Use Alterrate Authentication Material	1						
						Maderial Maderial	-						
						Valid Accounts							
						Virtualization/Sandbox Evasion	1						
						Evasion Weaken	+						
						Encryption	4						
						XSL Script							