Active Scanning       Acquire Infastructure       Valid Accounts       Comportine Accounts       Comportine Accounts       Comportine Infrastructure       Valid Accounts       System Service Discovery       Remote Services       Data Obfuscation       Explication Over Other Alliance       Data Infrastructure       Data Obfuscation       Data Obfuscation       Explication Over Other Alliance       Data Infrastructure       Data Obfuscation       Data Infrastructure       Data Infructure       Data Infructure	Reconnaissance 10 techniques	Resource Developme 7 techniques	ent Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Chronology         Chronology <thchronology< th="" thronology<=""> <thchronology< th="">         &lt;</thchronology<></thchronology<>														
Identifying and second seco	¥			 Windows Management		Valid Accounts							—	
Adde data         Adde data         Find data <t< td=""><td></td><td></td><td></td><td><b>.</b></td><td></td><td></td><td></td><td></td><td>5</td><td></td><td></td><td></td><td></td><td></td></t<>				<b>.</b>					5					
Minimum         Label definition         approximation         Table definition         Attende definition         Attende definition         Attende definition         Description         Contract of the second of		•			Boot or Logon I		Direct Volume Access							-
Open Control         Open Control<					<b>5</b>	•					· · ·			
Infernation         Resc						• •				■ Internal Spearphishing	<b>_</b>			
Grand Stand         Alie of J         Control J         Second Stand S								$\equiv$			· ·			
Image: Second					<b>U</b>			•	·					$\equiv \boxed{ Network Denial of Service } \equiv $
Pressing and providence         Space for each of the sp				≡ Execution	External Remote Services	Access Toke	n Manipulation	∃ Access	System Network	Lateral Tool Transfer	· ·	Ingress Tool Transfer	Exfiltration Over	$\_$ Endpoint Denial of Service $\equiv$
Same di conces         Service di conces         Conces di conces </td <td></td> <td></td> <td>External Remote Services</td> <td>System Services</td> <td></td> <td>Abuse Elevation</td> <td>Control Mechanism</td> <td>■ Steal Web Session Cookie</td> <td>Connections Discovery</td> <td>Taint Shared Content</td> <td>Audio Capture</td> <td></td> <td>Web Service</td> <td>System Shutdown/Reboot</td>			External Remote Services	System Services		Abuse Elevation	Control Mechanism	■ Steal Web Session Cookie	Connections Discovery	Taint Shared Content	Audio Capture		Web Service	System Shutdown/Reboot
Sine Cogener (Selection Delay Delay D			Drive-by Compromise	Command and Scripting	Create Account	Domain Pol	icy Modification	■ Unsecured Credentials	Permission Groups	_ Exploitation of Remote	Video Capture	Traffic Signaling	Automated Exfiltration	Account Access Removal
Turned Concent         Turned Concent         Parter							1	$\equiv$ Credentials from	· · ·	= Services	•		Exfiltration Over	
Send Com         Inter Source	-			Native API	Traffic Signaling	Exploitation for Privilege	Modify Registry	Password Stores	■ File and Directory	Remote Service Session	_ Data from Information	$\equiv$ Dynamic Resolution	Alternative Protocol	•
State         State <th< td=""><td></td><td></td><td></td><td>Inter-Process</td><td></td><td>Escalation</td><td>Trusted Developer Utilities</td><td></td><td></td><td></td><td>= Repositories</td><td>Non-Standard Port</td><td></td><td>•</td></th<>				Inter-Process		Escalation	Trusted Developer Utilities				= Repositories	Non-Standard Port		•
indiantic // control in // col Source         indiantic // control in // control	_			Communication	= Server Software =	≡	Proxy Execution	-   · · ·			Man-in-the-Middle			
winders     Cannard     Velocity     Galdaddial Allow     Marked Frank     Data frank in Nexce     Narked frank       Belge Coultaire     Congorn Schull     Sintee Stand     Sintee Sta				Container Administratior			Traffic Signaling				Archive Collected Data		=	
Depky Commer     incompose (lind)     Success Manuelli, Marce Meldice     Records Manuelli, Marce Meldice     Success Manuelli, MarceeMeldice     Success Manuelli, MarceeMeldice				Command	Pre-OS Boot		Signed Script Proxy	_ Steal Application Access	Network Share Discovery					
Load         Order         Degree Dorand         Control         Quark Under         Quark Un				Deploy Container	Compromise Client		Execution	= Token	Password Policy Discovery					
Indext during the conduct intrace     Indext during the conduct interval     During the conduct interval     During the conduct interval     During the conduct interval       Solution     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     Solution     During the local     During the local     During the local       Present     During the local     During the local     During the local     During the local       Present     During the local     During the local     During the local       Present     During the l	Has sub-techniques				Software Binary		Rogue Domain Controller	Man-in-the-Middle			Data from Cloud			
Notify Authentication     Execution     Nitruitation/shallows     Luta form Configuration       Notesia     Stable Thoreaching     Conditional     Luta form Configuration       Stable Thoreaching     Conditional     Conditional     Luta form Configuration       Notesia     Notesia     Conditional     Luta form Configuration       Notesia     Notesia     Conditional     Luta form Configuration       Notesia     Notesia     Notesia     Notesia	•				Implant Container Image		Indirect Command	Forge Web Credentials	■ Discovery					
XXL-Script Modsling     Could serve Databaid       Ineplate injection     Schore Discovery       Nemistors Modsling     Oney Registry       Nemistors Modsling     Network Seven Discovery       Virtualizators Andbox     Network Seven Discovery       Virtualizators Andbox     Network Seven Discovery       Under Adjumported     System Normalia       Discovery     System Normalia       Under Adjumported     Discovery       Discovery     System Normalia       National State Normalia     System Normalia       Discovery     Discovery       National State Normalia     System Normalia       Discovery     Discovery       National State Normalia     System Normalia       Discovery     Discovery       National Discovery     Discovery       National Discovery     Discovery       Discovery     Dispret Nist Control       System Disco					Modify Authentication	_	Execution		Virtualization/Sandbox	_				
SXS.Sorg invosening     Coud serve Databand       Lengiste rijstom     Sofware Databand       He and Usectory     Dobry Riggity       He and Usectory     Network Kervis Sustaming       Vir utation Softwork     Network Kervis Sustaming       Doald Regions     Network Kervis Sustaming       Doald Regions     Region Softwork       Coud Regions     System Former       Lengiste Rights     System Former       Lengiste Rights     System Former       Lengiste Rights     System Former       Lengiste Rights     System Former       Link Artistik     Coud Regions       Doald Intervery     Diatation       Link Artistik     Coud Strenery       Link Artistik     Coud Strenery       Doald Intervery     Diatation       Link Artistik     Coud Strenery       Link Artistik     Coud Strenery       Doald Intervery     Diatation       Coud Strenery     Diatation       Link Artistik     Coud Strenery       Doald Intervery     Diatation       Coud Strenery     Diatation       Link Artistik     Diatation       Doatation     Diatation       Coud Strenery     Diatation       Strenery     Diatation       Diatation     Diatation       Diatati					Process	=	BITS Jobs		Evasion	=	Repository	_		
File and DirectoryCuary RegistryPrivide ModificationHender System DiscoveryVirtualization/SandoxNetwork Service ScanningEvolutionPrice Notice WaryDirisof UnsuperitySystem InformationDirisof UnsuperityConstrained Price Notice WaryInformationConstrained Price Notice WaryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern DiscoveryInformationSubern Discovery </td <td></td> <td></td> <td></td> <td></td> <td></td> <td>XSL Script Processing</td> <td></td> <td>Cloud Service Dashboard</td> <td></td> <td></td> <td></td> <td></td> <td></td>							XSL Script Processing		Cloud Service Dashboard					
Permixtam Modif.chimItendre System DiscoveryVirtualization SandboxProcess DiscoveryUnusci/UnusupportdSystem InformationCload RegionDiscoveryUie AttenateCould RegionAuthentication MaterialSystem Time DiscoveryHide ArtifactsCould System Time DiscoveryHide ArtifactsCould System Time DiscoveryHide ArtifactsCload Sevice Sistem Time DiscoveryBase ProveCload Sevice Sistem Time DiscoveryBase ProveCload Sevice Sistem Time DiscoveryBase ProveCload Sevice Sistem Time DiscoverySystem Time DiscoveryCload Sevice Sistem Time DiscoveryBase ProveCload Sevice Sistem Time DiscoverySystem Time DiscoveryCload Sevice Sistem Time DiscoverySystem Time DiscoveryCload Sevice Sistem Time DiscoverySystem Time DiscoveryCload Sevice Sistem Cload Sevice Sistem Cloa							Template Injection		Software Discovery	$\equiv$				
Permissions Modification     Renote System Discovery       Virualization/Sandbez     Process Discovery       System Information     Discovery       Unuscification     Discovery       Lie Attenute     Authentication Modified       Authentication     Discovery       Ipper Ministricture     Discovery       Isper Ministricture     Discovery       Ipper Ministrict							File and Directory	=	Query Registry					
Fixedin       Process Discovery         Chune of Vingeri Vin							Permissions Modification	_						
Unsed/Insupported Cloud RegionsSystem Information DiscoveryUe A Iternate Authentication Nuterial Impar Defenses Authentication Nuterial Hide ArtifartsAccount Discovery Domain Trust DiscoveryHide ArtifartsCloud Server Domain Trust DiscoveryMasquerading Dechloractification for Defense Execution Cloud Infrastructure DiscoveryDiscovery DiscoverySystem Information Dechloractification for Defense Evaluation for Defense 							Virtualization/Sandbox	_	Network Service Scanning					
Cloud Regions     Diceowy       Uxe Aternate     Cound Diccowy       Amheniteation Material     System Time Discowy       Impair Defences     Cound Diccowy       Hide Artifacts     Cound Diccowy       Hide Artifacts     Cound Diccowy       Hide Artifacts     Cound Diccowy       System Time Discowy     Cound Diccowy       Hide Artifacts     Cound Diccowy       System Time Discowy     Cound Diccowy       Debthisrate/Picede Files     Discowy       Cloud Instarture Lue     Discowy       Signed Binary Novy     Signed Binary Novy       Signed Binary Novy     Signed Binary Novy       Signed Tinary Consult     Signed Binary Novy <t< td=""><td></td><td></td><td></td><td></td><td></td><td>Evasion</td><td>—</td><td>Process Discovery</td><td></td><td></td><td></td><td></td><td></td></t<>							Evasion	—	Process Discovery					
Use Alternate Account Discovery   Impair Defenses Domain Trust Discovery   Impair Defenses Domain Trust Discovery   Hide Artifacts Cound Service Discovery   Hide Artifacts Cound Service Discovery   Deedbracater Decode Files Cound Service Discovery   Deedbracater Decode Files Cound Service Discovery   Signed Binary Proxy Discovery   Exploitation for Defense Discovery   Evaluation Exploitation for Defense							Unused/Unsupported		System Information					
Autheritartion MaterialSystem Time DiscoveryImpair DefinesDemain Trust DiscoveryHide ArtifactsCloud Service DiscoveryMasqueradingCanCainer and ResourceDeabfuscatie/Decede FilesDiscoveryor InformationCloud InfrastructureSigned Simary PhonyDiscoveryExecution CaurdrailsSystem Location DiscoveryExecution GuardrailsExecution GuardrailsModify Cloud ComputeInfrastructurePre-OS BootExecution GuardrailsSubver Trust ControlsESubver Trust ControlsEBuild mage on HostEDeptor Subver Trust ControlsEDeptor Subver Trust ControlsEBuild mage on HostEDeptor Subver Trust ControlsEDeptor Sub							Cloud Regions		Discovery					
Impair DefensesImpair DefensesImpair DefensesHide AcqueradingImpair DefenseCondia Struct DiscoveryMacqueradingImpair DefenseDebolits scarceDebolits conceryDiscoveryDiscoveryDebolits conceryDiscoveryDiscoverySigned Binary ProxyDiscoveryDiscoveryDecontineExecution DiscoveryDiscoverySigned Binary ProxyExecution DiscoveryDiscoveryExecution GuardallsExecution DiscoverySystem Location DiscoveryPrev-OS BootImpair DefenseExecution DiscoverySubvert Trust ContolbEEBuild Image en HostDebolot ContainerE							Use Alternate	_	Account Discovery					
Hide Artifacts = Cloud Service Discovery   Masquerading =   Dobulsucate/Decode Files Discovery   or Information Cloud Infostructure   Signed Binary Proxy Execution   Execution =   Execution Clouder Files Discovery   System Location Discovery System Location Discovery   Kaster Cloud Infostructure Discovery   Execution =   Execution Clouder Files Discovery   Execution Clouder Files Execution Clouder Files   Files Clouder Files Execution Clouder Files   Files Clouder Files Execution Clouder Files   Subwert Trust Controls =   Build Image on Host Execution Clouder Files   Execution Clouder Files Execution Clouder Files   Execution Clouder Files Execution Clouder Files   Execution Clouder Files Execution Clou							Authentication Material	_	System Time Discovery					
MasqueradingContainer and Resource Deobfuscate//RecordDeobfuscate//RecordCloud InfrastructureSigned Binary ProxyDiscoverySigned Dinor for Defense EvalorSystem Location DiscoveryExecution GuardrallsEModify Cloud Compute Infrastructure Infrastructure DiscoverySystem Location DiscoveryPre-OS BootESubvert Trust ContolsEBubled mode Deploy ContainerE							Impair Defenses	$\equiv$	Domain Trust Discovery					
Deobfuscate/Decode Files or informationDiscovery Cloud InformationSigned Binary Proxy ExecutionExecutionExploitation for Defense EvasionSystem Location DiscoveryExecution GuardrailsE Modify Cloud Compute InfrastructurePre-OS BootE Buildinge on Host Deploy Container							Hide Artifacts	$\equiv$	Cloud Service Discovery					
or informationCloud InfrastructureSigned Binary ProxyDiscoveryExecutionDiscoveryExploitation for DefenseExecution GuardrallsExecution GuardrallsModify Cloud ComputeInfrastructurePre-OS BootBuilder Trust ControlsBuilder Trust ControlsBuilder Trust ControlsBuilder Trust ControlsDeploy Container-							Masquerading	$\equiv$	Container and Resource					
Since Biary Proxy   Signed Biary Proxy   Execution   Execution for Defense   Exacution for Defense   Evacution Guardraits   Execution Guardraits   Infastructure   Pre-OS Boot   SubvertTrustControls   Build Hange on Host   Discovery							Deobfuscate/Decode Files							
System Location DiscoveryExecution for Defense EvasionExecution GuardrailsExecution GuardrailsExecution GuardrailsInfrastructure InfrastructurePre-OS BootSubid Imag on HostEukid Imag on HostDeploy Container							or Information							
Exploitation for Defense Evasion Evasion Evacution Guardrails = Molfy Cloud Compute Infrastructure Pre-OS Boot = Subvert Trost Controls = Build Image on Host Deploy Container							Signed Binary Proxy	_		· · · · · · · · · · · · · · · · · · ·				
EvasionExecution Guardrails=Modify Cloud Compute Infrastructure=Preso=Subvert Trust Controls=Build Image on Host Deploy Container=									System Location Discovery					
Execution Guardrails=Modify Cloud Compute Infrastructure=Pre-OS Boot=Subvert Trust Controls=Build Image on Host Deploy Container=							Exploitation for Defense							
Modify Cloud Compute Infrastructure=Pre-OS Boot=Subvert Trust Controls=Build Image on Host Deploy Container=														
Infrastructure   Pre-OS Boot   Subvert Trust Controls   Build Image on Host   Deploy Container														
Pre-OS Boot       ■         Subvert Trust Controls       ■         Build Image on Host       ■         Deploy Container       ■								$\equiv$						
Subvert Trust Controls       ≡         Build Image on Host														
Build Image on Host Deploy Container														
Deploy Container														
Modify System Image $\equiv$														
							Modify System Image					R		

Network Boundary

Weaken Encryption

Bridging

© 2021 MITRE Matrix current as of June 2021

\_\_\_\_\_

## MITRE ATT&CK Enterprise Framework

attack.mitre.org

