

about

TeamTNT (G0139)

Enterprise techniques used by TeamTNT, ATT&CK group G0139 v1.0

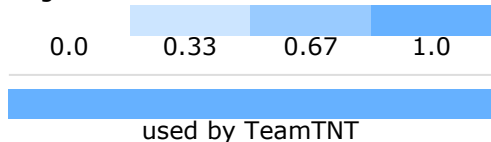
domain

Enterprise ATT&CK v10

platforms

Linux, macOS, Windows, Azure AD, Office 365, SaaS, IaaS, Google Workspace, PRE, Network, Containers

legend



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
<div>Active Scanning</div> <div>Scanning IP Blocks</div> <div>Vulnerability Scanning</div> <div>Gather Victim Host Information</div> <div>Gather Victim Identity Information</div> <div>Gather Victim Network Information</div> <div>Gather Victim Org Information</div> <div>Phishing for Information</div> <div>Search Closed Sources</div> <div>Search Open Websites/Domains</div> <div>Search Victim-Owned Websites</div>	<div>Acquire Infrastructure</div> <div>Domains</div> <div>DNS Server</div> <div>Virtual Private Server</div> <div>Server</div> <div>Botnet</div> <div>Web Services</div> <div>Compromise Accounts</div> <div>Develop Capabilities</div> <div>Malware</div> <div>Code Signing Certificates</div> <div>Digital Certificates</div> <div>Exploits</div> <div>Establish Accounts</div> <div>Obtain Capabilities</div> <div>Stage Capabilities</div> <div>Upload Malware</div> <div>Upload Tool</div> <div>Install Digital Certificate</div> <div>Drive-by Target</div> <div>Link Target</div>	<div>Drive-by Compromise</div> <div>Exploit Public-Facing Application</div> <div>External Remote Services</div> <div>Hardware Additions</div> <div>Phishing</div> <div>Replication Through Removable Media</div> <div>Supply Chain Compromise</div> <div>Trusted Relationship</div> <div>Valid Accounts</div>	<div>Command and Scripting Interpreter</div> <div>PowerShell</div> <div>AppleScript</div> <div>Windows Command Shell</div> <div>Unix Shell</div> <div>Visual Basic</div> <div>Python</div> <div>JavaScript</div> <div>Network Device CLI</div> <div>Container Administration Command</div> <div>Deploy Container</div> <div>Exploitation for Client Execution</div> <div>Inter-Process Communication</div> <div>Native API</div> <div>Scheduled Task/Job</div> <div>Shared Modules</div> <div>Software Deployment Tools</div> <div>System Services</div> <div>User Execution</div> <div>Malicious Link</div> <div>Malicious File</div> <div>Malicious Image</div> <div>Windows Management Instrumentation</div>	<div>Account Manipulation</div> <div>Personal Cloud Credentials</div> <div>Exchange Email Outgoing Permissions</div> <div>Add Office 365 Global Administrator Role</div> <div>Self Authorized Keys</div> <div>BITS Jobs</div> <div>Boot or Logon Automatic Execution</div> <div>Registry Run Keys / Startup Folder</div> <div>Time Providers</div> <div>Windows Helper DLL</div> <div>Security Support Provider</div> <div>Kernel Modules and Extensions</div> <div>Re-opened Applications</div> <div>Time Providers</div> <div>Windows Helper DLL</div> <div>Security Support Provider</div> <div>Kernel Modules and Extensions</div> <div>Re-opened Applications</div> <div>LSASS Driver</div> <div>Shortcut Modification</div> <div>Port Monitors</div> <div>File Modification</div> <div>Host Processors</div> <div>XDG Autostart Entries</div> <div>Port Monitors</div> <div>File Modification</div> <div>Print Processors</div> <div>VNC Autostart Entries</div> <div>Active Setup</div> <div>Login Items</div> <div>Boot or Logon Initialization Scripts</div> <div>Create or Modify System Process</div> <div>Launch Agent</div> <div>Systemd Service</div> <div>Windows Service</div> <div>Launch Daemon</div> <div>Event Triggered Execution</div> <div>External Remote Services</div> <div>Hijack Execution Flow</div> <div>Inject Internal Image</div> <div>Modify Authentication Process</div> <div>Office Application Startup</div> <div>Pre-OS Boot</div> <div>Scheduled Task/Job</div> <div>Server Software Component</div> <div>Traffic Signaling</div> <div>Valid Accounts</div>	<div>Abuse Elevation Control Mechanism</div> <div>Access Token Manipulation</div> <div>Boot or Logon Automatic Execution</div> <div>Registry Run Keys / Startup Folder</div> <div>Authentication</div> <div>Security Support Provider</div> <div>Kernel Modules and Extensions</div> <div>Re-opened Applications</div> <div>LSASS Driver</div> <div>Shortcut Modification</div> <div>Port Monitors</div> <div>File Modification</div> <div>Host Processors</div> <div>XDG Autostart Entries</div> <div>Active Setup</div> <div>Login Items</div> <div>Boot or Logon Initialization Scripts</div> <div>Create or Modify System Process</div> <div>Launch Agent</div> <div>Systemd Service</div> <div>Windows Service</div> <div>Launch Daemon</div> <div>Domain Policy Modification</div> <div>Escape to Host</div> <div>Event Triggered Execution</div> <div>Exploitation for Privilege Escalation</div> <div>Hijack Execution Flow</div> <div>Process Injection</div> <div>Scheduled Task/Job</div> <div>Valid Accounts</div>	<div>Abuse Elevation Control Mechanism</div> <div>Access Token Manipulation</div> <div>Build Image on Host</div> <div>Unauthenticated Device Files or Information</div> <div>Deploy Container</div> <div>Direct Volume Access</div> <div>Domain Policy Modification</div> <div>Execution Guardrails</div> <div>Exploitation for Defense Evasion</div> <div>File and Directory Permissions Modification</div> <div>Disable File and Directory Permissions Modification</div> <div>Clear Web Page File and Directory Permissions Modification</div> <div>Hide Artifacts</div> <div>Hijack Execution Flow</div> <div>Injunct Defenses</div> <div>Disable or Modify Tools</div> <div>Disable Windows Event Logging</div> <div>Impair Command History Logging</div> <div>Indicator Blocking</div> <div>Disable or Modify Cloud Firewall</div> <div>Cloud Logs</div> <div>Safe Mode Boot</div> <div>Downgrade Attack</div> <div>Indicator Removal on Host</div> <div>Clear Windows Event Logs</div> <div>Clear User or Mac System Logs</div> <div>Clear Command History</div> <div>File Deletion</div> <div>Network Share Connector Removal</div> <div>Timestamp</div> <div>Indirect Command Execution</div> <div>Hoaxing</div> <div>Modify Authentication Process</div> <div>Modify Local Compute Infrastructure</div> <div>Modify Registry</div> <div>Modify System Image</div> <div>Network Boundary Bridging</div> <div>Offloaded File or Information</div> <div>Binary Padding</div> <div>Software Padding</div> <div>Steganography</div> <div>Compile After Delivery</div> <div>Indicator Removal from Tools</div> <div>HTTP Smuggling</div> <div>Pre-OS Boot</div> <div>Process Injection</div> <div>Reflection Code Loading</div> <div>Rego</div> <div>Domain Controller</div> <div>Rootkit</div> <div>Signed Binary Proxy Execution</div> <div>Signed Script Proxy Execution</div> <div>Subvert Trust Controls</div> <div>Template Injection</div> <div>Traffic Signaling</div> <div>Trusted Developer Utilities Proxy Execution</div> <div>Unused/Unsupported Cloud Regions</div> <div>Use Alternate Authentication Material</div> <div>Valid Accounts</div> <div>Virtualization/Sandbox Evasion</div> <div>Weaken Encryption</div> <div>XSL Script Processing</div>	<div>Adversary-in-the-Middle</div> <div>Brute Force</div> <div>Credentials from Password Store</div> <div>Exploitation for Credential Access</div> <div>Forward Authentication</div> <div>Forge Web Credentials</div> <div>Input Capture</div> <div>Modify Authentication Process</div> <div>Network Sniffing</div> <div>OS Credential Dumping</div> <div>Steal Application Access Token</div> <div>Steal Kerberos Tickets</div> <div>Steal Web Session Cookie</div> <div>Two-Factor Authentication Interception</div> <div>Unmeasured Credentials</div> <div>Credentials in Files</div> <div>Credentials in Registry</div> <div>Bash History</div> <div>Private Keys</div> <div>Cloud Instance Metadata API</div> <div>Group Policy Preferences</div> <div>Container API</div>	<div>Account Discovery</div> <div>Application Window Discovery</div> <div>Browser Autocomplete Discovery</div> <div>Cloud Infrastructure Discovery</div> <div>Cloud Service Dashboard</div> <div>Cloud Service Discovery</div> <div>Cloud Storage Object Discovery</div> <div>Container and Regional Discovery</div> <div>Domain Trust Discovery</div> <div>Group Policy Discovery</div> <div>Network Service Scanning</div> <div>Network Share Discovery</div> <div>Network Sniffing</div> <div>Peripheral Device Discovery</div> <div>Permission Group Discovery</div> <div>Process Discovery</div> <div>Query Registry</div> <div>Remote Device Discovery</div> <div>Software Discovery</div> <div>Security Software Discovery</div> <div>System Information Discovery</div> <div>System Location Discovery</div> <div>System Network Configuration Discovery</div> <div>System Network Connections Discovery</div> <div>System Owner/User Discovery</div> <div>System Service Discovery</div> <div>System Time Discovery</div> <div>Virtualization/Sandbox Evasion</div>	<div>Exploitation of Remote Services</div> <div>Internal Spearphishing</div> <div>Lateral Tool Transfer</div> <div>Remote Service Session Hijacking</div> <div>Remote Services</div> <div>Remote Desktop Protocol</div> <div>SSH/Windows Admin Shares</div> <div>Distributed Component Object Model</div> <div>SSM</div> <div>Windows Remote Management</div> <div>Replication Through Removable Media</div> <div>Software Deployment Tools</div> <div>Taint Shared Content</div> <div>Use Alternate Authentication Material</div>	<div>Adversary-in-the-Middle</div> <div>Archive</div> <div>Collected Data</div> <div>Audio Capture</div> <div>Automated Collection</div> <div>Browser Session Hijacking</div> <div>Clipboard Data</div> <div>Data from Cloud Storage Object</div> <div>Data from Configuration Repository</div> <div>Data from Information Repositories</div> <div>Data from Local System</div> <div>Data from Network Shared Drive</div> <div>Data from Removable Media</div> <div>Data Staged</div> <div>Email Collection</div> <div>Input Capture</div> <div>Screen Capture</div> <div>Video Capture</div>	<div>Application Layer Protocol</div> <div>Web Protocols</div> <div>File Transfer Protocol</div> <div>Mail Protocols</div> <div>DNS</div> <div>Communication Through Removable Media</div> <div>Data Encoding</div> <div>Data Obfuscation</div> <div>Dynamic Resolution</div> <div>Encrypted Channel</div> <div>Fallback Channels</div> <div>Ingress Tool Transfer</div> <div>Multi-Stage Channels</div> <div>Non-Application Layer Protocol</div> <div>Non-Standard Port</div> <div>Protocol Tunneling</div> <div>Proxy</div> <div>Remote Access Software</div> <div>Traffic Signaling</div> <div>Web Service</div>	<div>Automated Exfiltration</div> <div>Data Transfer</div> <div>Size Limits</div> <div>Exfiltration Over Alternative Protocol</div> <div>Exfiltration Over C2 Channel</div> <div>Exfiltration Over Other Network Medium</div> <div>Exfiltration Over Physical Medium</div> <div>Exfiltration Over Web Service</div> <div>Scheduled Transfer</div> <div>Transfer Data to Cloud Account</div> <div>Inhibit System Recovery</div> <div>Network Denial of Service</div> <div>Firmware Corruption</div> <div>Resource Hijacking</div> <div>Service Stop</div> <div>System Shutdown/Reboot</div>	<div>Account Access Removal</div> <div>Data Destruction</div> <div>Data Encrypted for Impact</div> <div>Data Manipulation</div> <div>Data Removal</div> <div>Denial of Service</div> <div>Endpoint Denial of Service</div> <div>Network Denial of Service</div> <div>Scheduled Transfer</div> <div>Transfer Data to Cloud Account</div> <div>Inhibit System Recovery</div> <div>Network Denial of Service</div> <div>Firmware Corruption</div> <div>Resource Hijacking</div> <div>Service Stop</div> <div>System Shutdown/Reboot</div>