

about

Lazarus Group (G0032)

Enterprise techniques used by Lazarus Group, ATT&CK group G0032 (v4.0)

domain

Enterprise ATT&CK v15

platforms

Linux

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Content Injection	Command and Scripting Interpreter	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 Exfiltration	Account Access Removal
Drive-by Compromise	Javascript	Boot or Logon Autostart Execution	Account Manipulation	Debugger Evasion	ARP Cache Poisoning	Domain Account	Internal Spearphishing	ARP Cache Poisoning	DNS	Data Transfer Size Limits	Data Destruction
Exploit	Python	Kernel Modules and Extensions	Boot or Logon Autostart Execution	Deobfuscate/Decode Files or Information	DHCP Spoofing	Local Account	Lateral Tool Transfer	DHCP Spoofing	File Transfer Protocols	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Public Facing Application	Unix Shell	XDG Autostart Entries	Kernel Modules and Extensions	Execution Guardrails	Brute Force	Application Window Discovery	Remote Service Session Hijacking	Archive Collected Data	Mail Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Data Manipulation
External Remote Services	Visual Basic	Boot or Logon Initialization Scripts	XDG Autostart Entries	Exploitation for Defense Evasion	Credential Stuffing	Browser Information Discovery	Remote Services	Archive via Custom Method	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Defacement
Hardware Additions	Exploitation by Client Execution	Browser Extensions	Logon Initialization Scripts	File and Directory Permissions Modification	Password Cracking	Debugger Evasion	SSH	Archive via Library	Communication Through Removable Media	Exfiltration Over Encrypted Non-C2 Protocol	Internal Defacement
Phishing	Inter Process Communication	Compromise Host Software Binary	Create or Modify System Process	Hide Artifacts	Password Guessing	Device Driver Discovery	VNC	Archive via Utility	Content Injection	Exfiltration Over C2 Channel	Internal Defacement
Spearphishing Attachment	Native API	Create Account	System Service	Email Hiding Rules	Password Spraying	File and Directory Discovery	Software Deployment Tools		Data Encoding	Exfiltration Over Other Network Medium	Disk Wipe
Spearphishing Link	Scheduled Task/job	Create or Modify System Process	Escape to Host	File/Path Exclusions		Log Enumeration	Taint Shared Content	Audio Capture	Automated Collection	Exfiltration Over Physical Medium	Disk Contents Wipe
Spearphishing Web Service	At	System Service	Event Triggered Execution	Hidden File System	Credentials from Password Stores	Network Service Discovery		Clipboard Data	Non-Standard Encoding	Exfiltration Over Web Service	Disk Structure Wipe
Spearphishing Voice	Cron	System Service	Event Triggered Execution	Hidden Files and Directories	Exploitation for Credential Access	Network Share Discovery		Data from Information Repositories	Standard Encoding	Exfiltration Over Webhook	Endpoint Denial of Service
Supply Chain Compromise	Systemd Timers	External Remote Services	Hijack Execution Flow	Hidden Users	Forge Web Credentials	Network Sniffing		Data from Local System	Data Obfuscation	Exfiltration Over Code Storage	Financial Theft
Trusted Relationship		Hijack Execution Flow	Dynamic Linker Hijacking	Hidden Window	Input Capture	Password Policy Discovery		Data from Network Shared Drive	Junk Data	Exfiltration to Code Repository	Firmware Corruption
Valid Accounts	Shared Modules	Path Interception by PATH Environment Variable	Path Interception by PATH Environment Variable	Ignore Process Integrity	GUI Input Capture	Peripheral Device Discovery		Data from Removable Media	Protocol Impersonation	Exfiltration to Test Storage Sites	Inhibit System Recovery
	Software Deployment Tools	Process Injection	Process Injection	Run Virtual Instance	Keylogging	Permission Groups Discovery		Data Staged	Steganography	Scheduled Transfer	Network Denial of Service
	System Services	Modify Authentication Process	Proc Memory	VMA Stomping	Web Portal Capture	Process Discovery		Local Data Staging	Dynamic Resolution		Resource Hijacking
	User Execution	Power Settings	Process System Calls	Hijack Execution Flow	Modify Authentication Process	Remote System Discovery		Remote Data Staging	Encrypted Channel		Service Stop
	Malicious File	Pre-OS Boot	VDSO Hijacking	Dynamic Linker Hijacking	Multi-Factor Authentication Interception	Software Discovery		Email Collection	Asymmetric Cryptography		System Shutdown/Reboot
	Malicious Link	Bootkit	Scheduled Task/job	Path Interception by PATH Environment Variable	Multi-Factor Authentication Request Generation	System Information Discovery		Input Capture	Symmetric Cryptography		
		Component Firmware	At	Impair Defenses	Network Sniffing	System Location Discovery		GUI Input Capture	Fallback Channels		
		Scheduled Task/job	Cron	Disable or Modify Linux Audit System	OS Credential Dumping	System Network Configuration Discovery		Web Portal Capture	Hide Infrastructure		
		At	Systemd Timers	Disable or Modify System Firewall	Steal or Forge Authentication Certificates	System Owner/User Discovery	System Language Discovery	Screen Capture	Ingress Tool Transfer		
		Cron	Valid Accounts	Disable or Modify Tools	Steal or Forge Kerberos Tickets	System Network Connections Discovery	System Network Configuration Discovery	Video Capture	Multi-Stage Channels		
		Systemd Timers		Downgrade Attack	Steal Web Session Cookie	System Owner/User Discovery	System Owner/User Discovery		Non-Application Layer Protocol		
		Server Software Component		Inspiral	Unsecured Credentials	System Service Discovery	System Service Discovery		Non-Standard Port		
		SQL Stored Procedures		Indicator Blocking		System Time Discovery	System Time Discovery		Protocol Tunneling		
		Transport Agent		Spoof Security Alerting		Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		Proxy		
		Web Shell		Impersonation		System Checks	System Checks		Domain Fronting		
		Traffic Signaling		Indicator Removal		Time Based Evasion	Time Based Evasion		Internal Proxy		
		Valid Accounts		Clear Command History		User Activity Based Checks	User Activity Based Checks		External Proxy		
				Clear Linux or Mac System Logs					Multi-hop Proxy		
				Clear Mailbox Data					Remote Access Software		
				Clear Network Connection History and Configurations					Traffic Signaling		
				Clear Persistence					Web Service		
				File Deletion					Bi-directional Communication		
				Timestamp					Dead Drop Resolver		
				Masking					One-Way Communication		
				Break Process Trees							
				Masked File Type							
				Masked Task or Service							
				Match Legitimate Name or Location							
				Rename System Utilities							
				Right-to-Left Override							
				Space after Filename							
				Modify Authentication Process							
				Obfuscated Files or Information							
				Binary Padding							
				Command Obfuscation							
				Compile After Delivery							
				Embedded Payloads							
				Encrypted/Encoded File							
				HTML Smuggling							
				Indicator Removal from Tools							
				Software Packing							
				Steganography							
				Stripped Payloads							
				Pre-OS Boot							
				Bootkit							
				Component Firmware							
				Process Injection							
				Proc Memory							
				Process System Calls							
				VDSO Hijacking							
				Reflective Code Loading							
				Rootkit							
				Subvert Trust Controls							
				Install Root Certificate							
				System Binary Proxy Execution							
				Electron Applications							
				Traffic Signaling							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				System Checks							
				Time Based Evasion							
				User Activity Based Checks							