

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 of Execution Control Mechanism	Abuse of Execution 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	ABP Cache Poisoning	Anonymous Account	Internal Spearphishing	ABP Cache Poisoning	DNS	Data Transfer Size Limits	Data Destruction
Exploit	Python	Kernel Modules and Extensions	Logon Autostart Execution	Deobfuscate/Decode Files or Information	DHCP Spoofing	Anonymous 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	Credential Access	Browser Information Discovery	Remote Service Session Hijacking	Archive Collected Data	Mail Protocols	Exfiltration Over Asymmetric Cryptography	Data Manipulation
External Remote Services	Visual Basic	Boot or Logon Initialization Scripts	XDG Autostart Entries	Debugger Evasion	Password Guessing	Device Driver Discovery	SSH	Archive via Custom Method	Communication Through Hard-to-Reach Media	Exfiltration Over Encrypted Non-C2 Channel	Defacement
Hardware Additions	Exploitation by Client Execution	Browser Extensions	Event Triggered Execution	Hide Artifacts	Password Spraying	File and Directory Discovery	Software Deployment Tools	Archive via Library	Content Injection	Exfiltration Over C2 Channel	Internal Defacement
Phishing	Inter-Process Communication	Compromise Host Software Binary	Create or Modify System Process	Email Hiding Rules	Credentials from Password Stores	Log Enumeration	Taint Shared Content	Audio Capture	Data Encoding	Exfiltration Over Other Network Medium	Disk Wipe
Spearphishing Attachment	Native API	Create Account	System Service	File Path Exclusions	Exploitation for Credential Access	Network Service Discovery		Automated Collection	Non-Standard Encrypted Channel	Exfiltration Over Physical Medium	Disk Contents Wipe
Spearphishing Link	Scheduled Task/job	Create or Modify System Process	Escape to Host	Hidden File System	Forge Web Credentials	Network Share Discovery		Clipboard Data	Standard Encrypted Channel	Exfiltration Over Web Service	Disk Structure Wipe
Spearphishing Web Service	At	System Service	Event Triggered Execution	Hidden File System	Input Capture	Network Sniffing		Data from Information Repositories	Data Obfuscation	Exfiltration Over Webhook	Endpoint Denial of Service
Spearphishing Voice	Cron	External Remote Services	Hijack Execution Flow	Hidden File System	GUI Input Capture	Password Policy Discovery		Data from Local System	Junk Data	Exfiltration to Cloud Storage	Financial Theft
Supply Chain Compromise	System Timers	Hijack Execution Flow	Dynamic Linker Hijacking	Run Virtual Instance	Keylogging	Peripheral Device Discovery		Data from Network Shared	Protocol Interception	Exfiltration to Code Repository	Firmware Corruption
Trusted Relationship	Shared Modules	Path Interception by PATH Environment Variable	Dynamic Linker Hijacking	VMA Stomping	Web Proxy	Permission Groups Discovery		Data from Removable Media	Steganography	Exfiltration to Test Storage Sites	Inhibit System Recovery
Valid Accounts	Software Deployment Tools	Path Interception by PATH Environment Variable	Process Injection	Hijack Execution Flow	Modify Authentication Process	Process Discovery		Data Staged	Dynamic Resolution	Scheduled Transfer	Network Denial of Service
	System Services	Modify Authentication Process	Proc Memory	Dynamic Linker Hijacking	Multi-Factor Authentication Interception	Remote System Discovery		Local Data Stage	Encrypted Channel		Resource Hijacking
	User Execution	Power Settings	Process System Calls	Dynamic Linker Hijacking	Multi-Factor Authentication Request Generation	Software Discovery		Remote Data Stage	Asymmetric Cryptography		Service Stop
	Malicious File	Pre-OS Boot	VDSO Hijacking	Dynamic Linker Hijacking	Network Sniffing	System Information Discovery		Email Collection	Symmetric Cryptography		System Shutdown/Reboot
	Malicious Link	Bootkit	Scheduled Task/job	Impair Defenses	OS Credential Dumping	System Location Discovery		Input Capture	Fallback Channels		
		Component Firmware	At	Disable or Modify Linux Audit System	Steal or Forge Authentication Certificates	System Language Discovery		GUI Input Capture	Ingress Tool Transfer		
		Scheduled Task/job	Cron	Disable or Modify System Firewall	Steal or Forge Kerberos Tickets	System Network Configuration Discovery		Keylogging	Multi-Stage Channels		
		At	System Timers	Disable or Modify Tools	Steal Web Session Cookie	System Network Connections Discovery		Web Portal Capture	Non-Application Layer Protocol		
		Cron	Valid Accounts	Downgrade Attack	Unsecured Credentials	System Owner/User Discovery		Screen Capture	Non-Standard Port		
		System Timers		Inspiral		System Service Discovery		Video Capture	Protocol Tunneling		
		Server Software Component		Commanded History Logging		System Time Discovery			Proxy		
		SQL Stored Procedures		Indicator Blocking		Virtualization/Sandbox Evasion			Domain Fronting		
		Transport Agent		Spoof Security Alerting		System Checks			External Proxy		
		Web Shell		Indicator Removal		Time Based Evasion			Internal Proxy		
		Traffic Signaling		Clear Command History		User Activity Based Checks			Multi-hop Proxy		
		Valid Accounts		Clear Linux or Mac System Logs					Remote Access Software		
				Clear Mailbox Data					Traffic Signaling		
				Clear Network Connection History and Configurations					Web Service		
				Clear Persistence					Bi-directional Escalation		
				File Deletion					Jump Host Resolver		
				Timestamping					Anonymous Communication		
				Masquerading							
				Break Process Trees							
				Impersonate File Type							
				Impersonate Task or Service							
				Watch 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							
				HTTP 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							
				Rookit							
				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							