Lazarus Group, Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Diamond Sleet, Group G0032

Archived: 2026-04-05 13:09:10 UTC

Enterprise T1134 .002 Access Token Manipulation: Create Process with Token

Lazarus Group keylogger KiloAlfa obtains user tokens from interactive sessions to execute itself with API call `CreateProcessAsUserA` under that user's context.[3][16]

Enterprise T1087 .002 Account Discovery: Domain Account

During Operation Dream Job, Lazarus Group queried compromised victim's active directory servers to obtain the list of employees including administrator accounts.[12]

Enterprise T1098 Account Manipulation

Lazarus Group malware WhiskeyDelta-Two contains a function that attempts to rename the administrator’s account.[3][17]

Enterprise T1583 .001 Acquire Infrastructure: Domains

Lazarus Group has acquired domains related to their campaigns to act as distribution points and C2 channels.[18] [19]

During Operation Dream Job, Lazarus Group registered a domain name identical to that of a compromised company as part of their BEC effort.[12]

.004 Acquire Infrastructure: Server

During Operation Dream Job, Lazarus Group acquired servers to host their malicious tools.[12]

.006 Acquire Infrastructure: Web Services

Lazarus Group has hosted malicious downloads on Github.[18]

During Operation Dream Job, Lazarus Group used file hosting services like DropBox and OneDrive.[13]

Enterprise T1557 .001 Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay

Lazarus Group executed Responder using the command `[Responder file path] -i [IP address] -rPv` on a compromised host to harvest credentials and move laterally.[20]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Lazarus Group has conducted C2 over HTTP and HTTPS.[21][22][23][24][25][26]

During Operation Dream Job, Lazarus Group uses HTTP and HTTPS to contact actor-controlled C2 servers.[14]

Enterprise T1010 Application Window Discovery

Lazarus Group malware IndiaIndia obtains and sends to its C2 server the title of the window for each running process. The KilaAlfa keylogger also reports the title of the window in the foreground.[3][27][16]

Enterprise T1560 Archive Collected Data

Lazarus Group has compressed exfiltrated data with RAR and used RomeoDelta malware to archive specified directories in .zip format, encrypt the .zip file, and upload it to C2. [27][28][21]

.001 Archive via Utility

During Operation Dream Job, Lazarus Group archived victim's data into a RAR file.[12]

.002 Archive via Library

Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is compressed with Zlib, encrypted, and uploaded to a C2 server.[28][21]

.003 Archive via Custom Method

A Lazarus Group malware sample encrypts data using a simple byte based XOR operation prior to exfiltration.[3][27][28][21]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Lazarus Group has maintained persistence by loading malicious code into a startup folder or by adding a Registry Run key.[3][28][21][24]

During Operation Dream Job, Lazarus Group placed LNK files into the victims' startup folder for persistence.[14]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Lazarus Group malware has maintained persistence on a system by creating a LNK shortcut in the user’s Startup folder.[21]

Enterprise T1110 .003 Brute Force: Password Spraying

Lazarus Group malware attempts to connect to Windows shares for lateral movement by using a generated list of usernames, which center around permutations of the username Administrator, and weak passwords.[3][28]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Lazarus Group has used PowerShell to execute commands and malicious code.[19]

During Operation Dream Job, Lazarus Group used PowerShell commands to explore the environment of compromised victims.[12]

.003 Command and Scripting Interpreter: Windows Command Shell

Lazarus Group malware uses cmd.exe to execute commands on a compromised host.[3][17][21][29][25] A Destover-like variant used by Lazarus Group uses a batch file mechanism to delete its binaries from the system.[30]

During Operation Dream Job, Lazarus Group launched malicious DLL files, created new folders, and renamed folders with the use of the Windows command shell.[12][14]

.005 Command and Scripting Interpreter: Visual Basic

Lazarus Group has used VBA and embedded macros in Word documents to execute malicious code.[24][25]

During Operation Dream Job, Lazarus Group executed a VBA written malicious macro after victims download malicious DOTM files; Lazarus Group also used Visual Basic macro code to extract a double Base64 encoded DLL implant.[13][14]

Enterprise T1584 .001 Compromise Infrastructure: Domains

For Operation Dream Job, Lazarus Group compromised domains in Italy and other countries for their C2 infrastructure.[14][15]

.004 Compromise Infrastructure: Server

Lazarus Group has compromised servers to stage malicious tools.[20]

For Operation Dream Job, Lazarus Group compromised servers to host their malicious tools.[13][12][14]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Several Lazarus Group malware families install themselves as new services.[3][17]

Enterprise T1485 Data Destruction

Lazarus Group has used a custom secure delete function to overwrite file contents with data from heap memory.[3]

Enterprise T1132 .001 Data Encoding: Standard Encoding

A Lazarus Group malware sample encodes data with base64.[21]

Enterprise T1005 Data from Local System

Lazarus Group has collected data and files from compromised networks.[3][27][28][20]

During Operation Dream Job, Lazarus Group used malicious Trojans and DLL files to exfiltrate data from an infected host.[13][14]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

Lazarus Group malware also uses a unique form of communication encryption known as FakeTLS that mimics TLS but uses a different encryption method, potentially evading SSL traffic inspection/decryption.[3][17][21][31]

Enterprise T1074 .001 Data Staged: Local Data Staging

Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is saved in the %TEMP% directory, then compressed, encrypted, and uploaded to a C2 server.[3][27]

Enterprise T1622 Debugger Evasion

During Operation Dream Job, Lazarus Group used tools that used the `IsDebuggerPresent` call to detect debuggers.[13]

Enterprise T1491 .001 Defacement: Internal Defacement

Lazarus Group replaced the background wallpaper of systems with a threatening image after rendering the system unbootable with a Disk Structure Wipe.[17]

Enterprise T1140 Deobfuscate/Decode Files or Information

Lazarus Group has used shellcode within macros to decrypt and manually map DLLs and shellcode into memory at runtime.[24][25]

Enterprise T1587 .001 Develop Capabilities: Malware

Lazarus Group has developed custom malware for use in their operations.[18][19]

For Operation Dream Job, Lazarus Group developed custom tools such as Sumarta, DBLL Dropper, Torisma, and DRATzarus for their operations.[13][12][14][15]

.002 Develop Capabilities: Code Signing Certificates

During Operation Dream Job, Lazarus Group digitally signed their malware and the dbxcli utility.[12]

Enterprise T1561 .001 Disk Wipe: Disk Content Wipe

Lazarus Group has used malware like WhiskeyAlfa to overwrite the first 64MB of every drive with a mix of static and random buffers. A similar process is then used to wipe content in logical drives and, finally, attempt to wipe every byte of every sector on every drive. WhiskeyBravo can be used to overwrite the first 4.9MB of physical drives. WhiskeyDelta can overwrite the first 132MB or 1.5MB of each drive with random data from heap memory.[17]

.002 Disk Wipe: Disk Structure Wipe

Lazarus Group malware SHARPKNOT overwrites and deletes the Master Boot Record (MBR) on the victim's machine and has possessed MBR wiper malware since at least 2009.[29][3]

Enterprise T1189 Drive-by Compromise

Lazarus Group delivered RATANKBA and other malicious code to victims via a compromised legitimate website.[32][19]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Several Lazarus Group malware families encrypt C2 traffic using custom code that uses XOR with an ADD operation and XOR with a SUB operation. Another Lazarus Group malware sample XORs C2 traffic. Other Lazarus Group malware uses Caracachs encryption to encrypt C2 payloads. Lazarus Group has also used AES to encrypt C2 traffic.[3][17][21][30]

During Operation Dream Job, Lazarus Group used an AES key to communicate with their C2 server.[14]

Enterprise T1585 .001 Establish Accounts: Social Media Accounts

Lazarus Group has created new Twitter accounts to conduct social engineering against potential victims.[19]

For Operation Dream Job, Lazarus Group created fake LinkedIn accounts for their targeting efforts.[13][12]

.002 Establish Accounts: Email Accounts

Lazarus Group has created new email accounts for spearphishing operations.[20]

During Operation Dream Job, Lazarus Group created fake email accounts to correspond with fake LinkedIn personas; Lazarus Group also established email accounts to match those of the victim as part of their BEC attempt.[12]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

Lazarus Group malware SierraBravo-Two generates an email message via SMTP containing information about newly infected victims.[3][28]

Enterprise T1041 Exfiltration Over C2 Channel

Lazarus Group has exfiltrated data and files over a C2 channel through its various tools and malware.[3][27][21]

During Operation Dream Job, Lazarus Group exfiltrated data from a compromised host to actor-controlled C2 servers.[13]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

During Operation Dream Job, Lazarus Group used a custom build of open-source command-line dbxcli to exfiltrate stolen data to Dropbox.[12][13]

Enterprise T1203 Exploitation for Client Execution

Lazarus Group has exploited Adobe Flash vulnerability CVE-2018-4878 for execution.[33]

Enterprise T1008 Fallback Channels

Lazarus Group malware SierraAlfa sends data to one of the hard-coded C2 servers chosen at random, and if the transmission fails, chooses a new C2 server to attempt the transmission again.[3][28]

Enterprise T1083 File and Directory Discovery

Lazarus Group malware can use a common function to identify target files by their extension, and some also enumerate files and directories, including a Destover-like variant that lists files and gathers information for all drives.[3][30][24][25]

During Operation Dream Job, Lazarus Group conducted word searches within documents on a compromised host in search of security and financial matters.[13]

Enterprise T1589 .002 Gather Victim Identity Information: Email Addresses

Lazarus Group collected email addresses belonging to various departments of a targeted organization which were used in follow-on phishing campaigns.[20]

Enterprise T1591 Gather Victim Org Information

Lazarus Group has studied publicly available information about a targeted organization to tailor spearphishing efforts against specific departments and/or individuals.[20]

For Operation Dream Job, Lazarus Group gathered victim organization information to identify specific targets.[13]

.004 Identify Roles

During Operation Dream Job, Lazarus Group targeted specific individuals within an organization with tailored job vacancy announcements.[13][12]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Lazarus Group has used a VBA Macro to set its file attributes to System and Hidden and has named files with a dot prefix to hide them from the Finder application.[21][22][23][24]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Lazarus Group has replaced `win_fw.dll`, an internal component that is executed during IDA Pro installation, with a malicious DLL to download and execute a payload.[26] Lazarus Group utilized DLL side-loading to execute malicious payloads through abuse of the legitimate processes `wsmprovhost.exe` and `dfrgui.exe`.[34]

.013 Hijack Execution Flow: KernelCallbackTable

Lazarus Group has abused the `KernelCallbackTable` to hijack process control flow and execute shellcode.[24][25]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Lazarus Group malware TangoDelta attempts to terminate various processes associated with McAfee. Additionally, Lazarus Group malware SHARPKNOT disables the Microsoft Windows System Event Notification and Alerter services.[3][27][16][29].

.004 Impair Defenses: Disable or Modify System Firewall

Various Lazarus Group malware modifies the Windows firewall to allow incoming connections or disable it entirely using netsh. [3][27][16]

Enterprise T1656 Impersonation

During Operation Dream Job, Lazarus Group impersonated HR hiring personnel through LinkedIn messages and conducted interviews with victims in order to deceive them into downloading malware.[13][12][35]

Enterprise T1070 Indicator Removal

Lazarus Group has restored malicious KernelCallbackTable code to its original state after the process execution flow has been hijacked.[24]

.003 Clear Command History

Lazarus Group has routinely deleted log files on a compromised router, including automatic log deletion through the use of the logrotate utility.[20]

.004 File Deletion

Lazarus Group malware has deleted files in various ways, including "suicide scripts" to delete malware binaries from the victim. Lazarus Group also uses secure file deletion to delete files from the victim.[3][30]

During Operation Dream Job, Lazarus Group removed all previously delivered files from a compromised computer.[12]

.006 Timestomp

Several Lazarus Group malware families use timestomping, including modifying the last write timestamp of a specified Registry key to a random date, as well as copying the timestamp for legitimate .exe files (such as calc.exe or mspaint.exe) to its dropped files.[3][17][27][30]

Enterprise T1202 Indirect Command Execution

Lazarus Group persistence mechanisms have used `forfiles.exe` to execute .htm files.[25]

Enterprise T1105 Ingress Tool Transfer

Lazarus Group has downloaded files, malware, and tools from its C2 onto a compromised host.[3][17][27][22][23][20][19][24][25][26]

During Operation Dream Job, Lazarus Group downloaded multistage malware and tools onto a compromised host.[13][12][14]

Enterprise T1056 .001 Input Capture: Keylogging

Lazarus Group malware KiloAlfa contains keylogging functionality.[3][16]

Enterprise T1534 Internal Spearphishing

During Operation Dream Job, Lazarus Group conducted internal spearphishing from within a compromised organization.[13]

Enterprise T1680 Local Storage Discovery

A Destover-like variant used by Lazarus Group collects disk space information and sends it to its C2 server.[3][17][27][21][30][24]

Enterprise T1036 .003 Masquerading: Rename Legitimate Utilities

Lazarus Group has renamed system utilities such as `wscript.exe` and `mshta.exe`.[25]

.004 Masquerading: Masquerade Task or Service

Lazarus Group has used a scheduled task named `SRCheck` to mask the execution of a malicious .dll.[26]

.005 Masquerading: Match Legitimate Resource Name or Location

Lazarus Group has renamed malicious code to disguise it as Microsoft's narrator and other legitimate files.[36][25]

.008 Masquerading: Masquerade File Type

During Operation Dream Job, Lazarus Group disguised malicious template files as JPEG files to avoid detection.[14][12]

Enterprise T1104 Multi-Stage Channels

Lazarus Group has used multi-stage malware components that inject later stages into separate processes.[24]

Enterprise T1106 Native API

Lazarus Group has used the Windows API `ObtainUserAgentString` to obtain the User-Agent from a compromised host to connect to a C2 server.[14] Lazarus Group has also used various, often lesser known, functions to perform various types of Discovery and Process Injection.[24][25]

During Operation Dream Job, Lazarus Group used Windows API `ObtainUserAgentString` to obtain the victim's User-Agent and used the value to connect to their C2 server.[14]

Enterprise T1046 Network Service Discovery

Lazarus Group has used nmap from a router VM to scan ports on systems within the restricted segment of an enterprise network.[20]

Enterprise T1571 Non-Standard Port

Some Lazarus Group malware uses a list of ordered port numbers to choose a port for C2 traffic, creating port-protocol mismatches.[3][28]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

During Operation Dream Job, Lazarus Group packed malicious .db files with Themida to evade detection.[13][14][15]

.007 Obfuscated Files or Information: Dynamic API Resolution

Lazarus Group has used a custom hashing method to resolve APIs used in shellcode.[24]

.009 Obfuscated Files or Information: Embedded Payloads

Lazarus Group has distributed malicious payloads embedded in PNG files.[37]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Lazarus Group has used multiple types of encryption and encoding for their payloads, including AES, Caracachs, RC4, XOR, Base64, and other tricks such as creating aliases in code for Native API function names.[3][27][28][21][23][24][25]

During Operation Dream Job, Lazarus Group encrypted malware such as DRATzarus with XOR and DLL files with base64.[13][12][14][15]

Enterprise T1588 .002 Obtain Capabilities: Tool

Lazarus Group has obtained a variety of tools for their operations, including Responder and PuTTy PSCP.[20]

For Operation Dream Job, Lazarus Group obtained tools such as Wake-On-Lan, Responder, ChromePass, and dbxcli.[13][12]

.003 Obtain Capabilities: Code Signing Certificates

During Operation Dream Job, Lazarus Group used code signing certificates issued by Sectigo RSA for some of its malware and tools.[12]

.004 Obtain Capabilities: Digital Certificates

Lazarus Group has obtained SSL certificates for their C2 domains.[18]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Lazarus Group has targeted victims with spearphishing emails containing malicious Microsoft Word documents.[33][20][24][25]

During Operation Dream Job, Lazarus Group sent emails with malicious attachments to gain unauthorized access to targets' computers.[13][14]

.002 Phishing: Spearphishing Link

Lazarus Group has sent malicious links to victims via email.[20]

During Operation Dream Job, Lazarus Group sent malicious OneDrive links with fictitious job offer advertisements via email.[13][12]

.003 Phishing: Spearphishing via Service

Lazarus Group has used social media platforms, including LinkedIn and Twitter, to send spearphishing messages.[19]

During Operation Dream Job, Lazarus Group sent victims spearphishing messages via LinkedIn concerning fictitious jobs.[13][12]

Enterprise T1542 .003 Pre-OS Boot: Bootkit

Lazarus Group malware WhiskeyAlfa-Three modifies sector 0 of the Master Boot Record (MBR) to ensure that the malware will persist even if a victim machine shuts down.[3][17]

Enterprise T1057 Process Discovery

Several Lazarus Group malware families gather a list of running processes on a victim system and send it to their C2 server. A Destover-like variant used by Lazarus Group also gathers process times.[3][27][21][30][23][24]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

A Lazarus Group malware sample performs reflective DLL injection.[21][24]

Enterprise T1090 .001 Proxy: Internal Proxy

Lazarus Group has used a compromised router to serve as a proxy between a victim network's corporate and restricted segments.[20]

.002 Proxy: External Proxy

Lazarus Group has used multiple proxies to obfuscate network traffic from victims.[38][23]

Enterprise T1012 Query Registry

Lazarus Group malware IndiaIndia checks Registry keys within HKCU and HKLM to determine if certain applications are present, including SecureCRT, Terminal Services, RealVNC, TightVNC, UltraVNC, Radmin, mRemote, TeamViewer, FileZilla, pcAnyware, and Remote Desktop. Another Lazarus Group malware sample checks for the presence of the following Registry key: `HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt`.[3][27] [21]

Enterprise T1620 Reflective Code Loading

Lazarus Group has changed memory protection permissions then overwritten in memory DLL function code with shellcode, which was later executed via KernelCallbackTable hijacking. Lazarus Group has also used shellcode within macros to decrypt and manually map DLLs into memory at runtime.[24][25]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Lazarus Group malware SierraCharlie uses RDP for propagation.[3][28]

.002 Remote Services: SMB/Windows Admin Shares

Lazarus Group malware SierraAlfa accesses the `ADMIN$` share via SMB to conduct lateral movement.[3][28]

.004 Remote Services: SSH

Lazarus Group used SSH and the PuTTy PSCP utility to gain access to a restricted segment of a compromised network.[20]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Lazarus Group has used `schtasks` for persistence including through the periodic execution of a remote XSL script or a dropped VBS payload.[25][26]

During Operation Dream Job, Lazarus Group created scheduled tasks to set a periodic execution of a remote XSL script.[12]

Enterprise T1593 .001 Search Open Websites/Domains: Social Media

For Operation Dream Job, Lazarus Group used LinkedIn to identify and target employees within a chosen organization.[12]

Enterprise T1505 .004 Server Software Component: IIS Components

During Operation Dream Job, Lazarus Group targeted Windows servers running Internet Information Systems (IIS) to install C2 components.[14]

Enterprise T1489 Service Stop

Lazarus Group has stopped the MSExchangeIS service to render Exchange contents inaccessible to users.[17]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

For Operation Dream Job, Lazarus Group used compromised servers to host malware.[13][12][14][15]

.002 Stage Capabilities: Upload Tool

For Operation Dream Job, Lazarus Group used multiple servers to host malicious tools.[12]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Lazarus Group has digitally signed malware and utilities to evade detection.[24]

During Operation Dream Job, Lazarus Group digitally signed their own malware to evade detection.[12]

Enterprise T1218 System Binary Proxy Execution

Lazarus Group lnk files used for persistence have abused the Windows Update Client (`wuauclt.exe`) to execute a malicious DLL.[24][25]

.005 Mshta

Lazarus Group has used `mshta.exe` to execute HTML pages downloaded by initial access documents.[24][25]

.010 Regsvr32

During Operation Dream Job, Lazarus Group used `regsvr32` to execute malware.[12]

.011 Rundll32

Lazarus Group has used rundll32 to execute malicious payloads on a compromised host.[26]

During Operation Dream Job, Lazarus Group executed malware with `C:\\windows\system32\rundll32.exe "C:\ProgramData\ThumbNail\thumbnail.db"` , `CtrlPanel S-6-81-3811-75432205-060098-6872 0 0 905` .[13][12][14]

Enterprise T1082 System Information Discovery

Several Lazarus Group malware families collect information on the type and version of the victim OS, as well as the victim computer name and CPU information.[3][17][27][21][30][24]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

During Operation Dream Job, Lazarus Group deployed malware designed not to run on computers set to Korean, Japanese, or Chinese in Windows language preferences.[13]

Enterprise T1016 System Network Configuration Discovery

Lazarus Group malware IndiaIndia obtains and sends to its C2 server information about the first network interface card’s configuration, including IP address, gateways, subnet mask, DHCP information, and whether WINS is

available.[3][27]

Enterprise T1049 System Network Connections Discovery

Lazarus Group has used `net use` to identify and establish a network connection with a remote host.[20]

Enterprise T1033 System Owner/User Discovery

Various Lazarus Group malware enumerates logged-on users.[3][17][27][28][21][22][24]

Enterprise T1529 System Shutdown/Reboot

Lazarus Group has rebooted systems after destroying files and wiping the MBR on infected systems.[29]

Enterprise T1124 System Time Discovery

A Destover-like implant used by Lazarus Group can obtain the current system time and send it to the C2 server.[30]

Enterprise T1221 Template Injection

During Operation Dream Job, Lazarus Group used DOCX files to retrieve a malicious document template/DOTM file.[13][14]

Enterprise T1204 .001 User Execution: Malicious Link

During Operation Dream Job, Lazarus Group lured users into executing a malicious link to disclose private account information or provide initial access.[13][12]

.002 User Execution: Malicious File

Lazarus Group has attempted to get users to launch a malicious Microsoft Word attachment delivered via a spearphishing email.[33][20][24][25]

During Operation Dream Job, Lazarus Group lured victims into executing malicious documents that contained "dream job" descriptions from defense, aerospace, and other sectors.[13][14]

Enterprise T1078 Valid Accounts

Lazarus Group has used administrator credentials to gain access to restricted network segments.[20]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

During Operation Dream Job, Lazarus Group used tools that conducted a variety of system checks to detect sandboxes or VMware services.[13]

.003 Virtualization/Sandbox Evasion: Time Based Checks

During Operation Dream Job, Lazarus Group used tools that collected `GetTickCount` and `GetSystemTimeAsFileTime` data to detect sandbox or VMware services.[13]

Enterprise T1102 .002 Web Service: Bidirectional Communication

Lazarus Group has used GitHub as C2, pulling hosted image payloads then committing command execution output to files in specific directories.[24]

Enterprise T1047 Windows Management Instrumentation

Lazarus Group has used WMIC for discovery as well as to execute payloads for persistence and lateral movement. [3][28][20][25]

During Operation Dream Job, Lazarus Group used WMIC to executed a remote XSL script.[12]

Enterprise T1220 XSL Script Processing

During Operation Dream Job, Lazarus Group used a remote XSL script to download a Base64-encoded DLL custom downloader.[12]

ICS T0865 Spearphishing Attachment

Lazarus Group has been observed targeting organizations using spearphishing documents with embedded malicious payloads. [39] Highly targeted spear phishing campaigns have been conducted against a U.S. electric grid company. [40]
