1. MỤC TIÊU CHUNG

Tiến hành nghiên cứu toàn diện về nhóm Lazarus Group, tập trung vào chiến thuật, kỹ thuật và thủ tục của họ. Sử dụng khung MITRE ATT&CK để vạch ra các hoạt động của nhóm và cung cấp những hiểu biết có thể hành động. [1]

Phát hiện của bản báo cáo này đóng một vai trò quan trọng trong việc củng cố khả năng phòng thủ chống lại kẻ thù này.

2. Lazarus Group

Lazarus Group là một trong những nhóm tin tặc nguy hiểm và nổi tiếng nhất hiện nay. Nhóm này được cho là có liên hệ chặt chẽ với chính phủ Bắc Triều Tiên, hoạt động ít nhất từ năm 2009 đến nay. Lazarus thường xuyên tiến hành các cuộc tấn công mạng quy mô lớn nhằm vào nhiều mục tiêu khác nhau, bao gồm cả lĩnh vực chính trị, quân sự và tài chính.[1]

2.1 Nguồn gốc và tổ chức

Theo các báo cáo tình báo và phân tích an ninh mạng, Lazarus Group được điều hành bởi **Reconnaissance General Bureau (RGB)** – cơ quan tình báo quân sự của Triều Tiên. Bên trong Lazarus tồn tại nhiều nhánh phụ chuyên trách: [1]

- **BlueNorOff / APT38**: Tập trung vào các cuộc tấn công tài chính, nhắm vào hệ thống ngân hàng và tiền mã hóa.[1]
- **AndAriel**: Thực hiện các chiến dịch gián điệp mạng và tấn công vào hạ tầng quan trọng, đặc biệt tại Hàn Quốc.[1]
- **Hidden Cobra, Guardians of Peace, ZINC, v.v.,** được dùng để che giấu dấu vết và tạo sự nhầm lẫn cho cơ quan điều tra .[1]

2.2 Các vụ tấn công nổi bật

Một số sự kiện tiêu biểu do **Lazarus Group** thực hiện:

- **2014 – Sony Pictures**: Tấn công, đánh cắp dữ liệu và làm rò rỉ thông tin mật, được cho là trả đũa bộ phim The Interview. [2]
- **2016 – Ngân hàng Trung ương Bangladesh**: Lazarus đánh cắp 81 triệu USD qua hệ thống SWIFT. [3]
- **2017 – WannaCry Ransomware**: Mã độc tống tiền toàn cầu, gây ảnh hưởng đến hơn 150 quốc gia.
- **2022 – Ronin Network / Axie Infinity**: Đánh cắp hơn 620 triệu USD tiền mã hóa.
- **2023 – Stake[.]com và Atomic Wallet**: Tổng cộng Lazarus đã lấy hơn 300 triệu USD từ các nền tảng crypto [4]

Điểm đáng chú ý là Lazarus không chỉ triển khai Dream Job như một chiến dịch đơn lẻ. Nó còn liên kết với các hoạt động khác như **Operation North Star** và **Operation Interception**, thể hiện chiến lược lâu dài nhằm vào cá nhân trong lĩnh vực kỹ thuật và an ninh quốc phòng. [5]

2.3 Operation Dream Job

Bài báo cáo này sẽ tập trung vào chiến dịch Operation Dream Job.

Operation Dream Job là một trong những chiến dịch tấn công mạng phức tạp nhất do **Lazarus Group** tiến hành. Chiến dịch này lợi dụng các cơ hội nghề nghiệp giả mạo từ những công ty công nghệ và quốc phòng lớn để dụ dỗ nạn nhân tải về các tài liệu hoặc phần mềm chứa mã độc. Lần đầu tiên chiến dịch này được phát hiện là vào **tháng 9 năm 2019** theo dữ liệu từ MITRE ATT&CK. [5]

2.3.1 Phương thức tấn công

2.3.1.1. Kỹ thuật lợi dụng hệ thống hợp pháp

Trong chiến dịch này, Lazarus đã khai thác các binary hợp pháp của Windows như **Regsvr32** và **Rundll32** để thực hiện proxy execution. Đây là kỹ thuật "Living off the Land" (LOLBin) thường thấy, giúp kẻ tấn công ngụy trang hoạt động của mình dưới lớp vỏ hợp pháp, khó bị phát hiện bởi các hệ thống phòng thủ truyền thống. [5]

2.3.1.2. Kỹ thuật di chuyển ngang

Sau khi xâm nhập ban đầu, Lazarus sử dụng kỹ thuật **Internal Spearphishing** để mở rộng phạm vi kiểm soát trong cùng một tổ chức. Kỹ thuật này được MITRE định danh là **T1534**. Điều này cho phép kẻ tấn công mở rộng quyền truy cập mà không cần phải khai thác thêm nhiều lỗ hổng. [5]

2.3.1.3. Phần mềm độc hại

Một RAT (Remote Access Trojan) quan trọng trong chiến dịch này là **DRATzarus**. Đây là công cụ giúp Lazarus duy trì truy cập từ xa, thực hiện các lệnh và đánh cắp dữ liệu. **DRATzarus** sử dụng **Native API** để thực thi trực tiếp trên hệ thống, đồng thời áp dụng kỹ thuật **Time-Based Evasion** nhằm tránh bị sandbox phân tích trong môi trường ảo. [6] [7]

2.3.2 Operation Dream Job Techniques Used [5]

Domain	ID		Name	Use
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.
Enterprise	T1583	.001	Acquire Infrastructure: Domains	During Operation Dream Job, Lazarus Group registered a domain name identical to that of a compromised company as part of their BEC effort.
		.004	Acquire Infrastructure: Server	During Operation Dream Job, Lazarus Group acquired servers to host their malicious tools.
		.006	Acquire Infrastructure: Web Services	During Operation Dream Job, Lazarus Group used file hosting services like DropBox and OneDrive.
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	During Operation Dream Job, Lazarus Group uses HTTP and HTTPS to contact actor-controlled C2 servers.
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	During Operation Dream Job, Lazarus Group uses HTTP and HTTPS to contact actor-controlled C2 servers.
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	During Operation Dream Job, Lazarus Group archived victim's data into a RAR file.

Enterprise	T1110		Brute Force	During Operation Dream Job, Lazarus Group placed LNK files into the victims' startup folder for persistence.
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	During Operation Dream Job, Lazarus Group used PowerShell commands to explore the environment of compromised victims.
		.003	Command and Scripting Interpreter: Windows Command Shell	During Operation Dream Job, Lazarus Group launched malicious DLL files, created new folders, and renamed folders with the use of the Windows command shell.
		.005	Command and Scripting Interpreter: Visual Basic	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.
Enterprise	T1584	.001	Compromise Infrastructure: Domains	For Operation Dream Job, Lazarus Group compromised domains in Italy and other countries for their C2 infrastructure.
		.004	Compromise Infrastructure: Server	For Operation Dream Job, Lazarus Group compromised servers to host their malicious tools
Enterprise	T1005		Data from Local System	During Operation Dream Job, Lazarus Group used malicious Trojans and DLL files to exfiltrate data from an infected host.
Enterprise	T1622		Debugger Evasion	During Operation Dream Job, Lazarus Group used tools that used the IsDebuggerPresent call to detect debuggers.

Enterprise	T1587	.001	Develop Capabilities: Malware	For Operation Dream Job, Lazarus Group developed custom tools such as Sumarta, DBLL Dropper, Torisma, and DRATzarus for their operations.
		.002	Develop Capabilities: Code Signing Certificates	During Operation Dream Job, Lazarus Group digitally signed their malware and the dbxcli utility.
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	During Operation Dream Job, Lazarus Group used an AES key to communicate with their C2 server.
Enterprise	T1585	.001	Establish Accounts: Social Media Accounts	For Operation Dream Job, Lazarus Group created fake LinkedIn accounts for their targeting efforts.
		.002	Establish Accounts: Email Accounts	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.
Enterprise	T1041		Exfiltration Over C2 Channel	During Operation Dream Job, Lazarus Group exfiltrated data from a compromised host to actor-controlled C2 servers.
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.
Enterprise	T1083		File and Directory Discovery	During Operation Dream Job, Lazarus Group conducted word searches within documents on a compromised host in search of security and financial matters.

Enterprise	T1589		Gather Victim Identity Information	For Operation Dream Job, Lazarus Group conducted extensive reconnaissance research on potential targets.
Enterprise	T1591		Gather Victim Org Information	For Operation Dream Job, Lazarus Group gathered victim organization information to identify specific targets.
		.004	Identify Roles	During Operation Dream Job, Lazarus Group targeted specific individuals within an organization with tailored job vacancy announcements.
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.
Enterprise	T1070	.004	Indicator Removal: File Deletion	During Operation Dream Job, Lazarus Group removed all previously delivered files from a compromised computer.
Enterprise	T1105		Ingress Tool Transfer	During Operation Dream Job, Lazarus Group downloaded multistage malware and tools onto a compromised host.
Enterprise	T1534		Internal Spearphishing	During Operation Dream Job, Lazarus Group conducted internal spearphishing from within a compromised organization.
Enterprise	T1036	.008	Masquerading: Masquerade File Type	During Operation Dream Job, Lazarus Group disguised malicious template files as JPEG files to avoid detection.
Enterprise	T1106		Native API	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.
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	During Operation Dream Job, Lazarus Group packed malicious .db files with Themida to evade detection.
		.013	Obfuscated Files or Information: Encrypted/Encoded File	During Operation Dream Job, Lazarus Group encrypted malware such as DRATzarus with XOR and DLL files with base64.
Enterprise	T1588	.002	Obtain Capabilities: Tool	For Operation Dream Job, Lazarus Group obtained tools such as Wake-On-Lan, Responder, ChromePass, and dbxcli.
		.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.
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	During Operation Dream Job, Lazarus Group sent emails with malicious attachments to gain unauthorized access to targets' computers.
		.002	Phishing: Spearphishing Link	During Operation Dream Job, Lazarus Group sent malicious OneDrive links with fictitious job offer advertisements via email.
		.003	Phishing: Spearphishing via Service	During Operation Dream Job, Lazarus Group sent victims spearphishing messages via LinkedIn concerning fictitious jobs.
Enterprise	T1010	.005	Scheduled Task/Job:	During Operation Dream Job, Lazarus Group created scheduled

	53		Scheduled Task	tasks to set a periodic execution of a remote XSL script.
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.
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.
Enterprise	T1608	.001	Stage Capabilities: Upload Malware	For Operation Dream Job, Lazarus Group used compromised servers to host malware.
		.002	Stage Capabilities: Upload Tool	For Operation Dream Job, Lazarus Group used multiple servers to host malicious tools.
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	During Operation Dream Job, Lazarus Group digitally signed their own malware to evade detection.
Enterprise	T1218	.010	System Binary Proxy Execution: Regsvr32	During Operation Dream Job, Lazarus Group used regsvr32 to execute malware.
		.011	System Binary Proxy Execution: Rundll32	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.
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.
Enterprise	T1221		Template Injection	During Operation Dream Job, Lazarus Group used DOCX files to retrieve a malicious document template/DOTM file.
Enterprise	T1204		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.
			User Execution: Malicious File	During Operation Dream Job, Lazarus Group lured victims into executing malicious documents that contained "dream job" descriptions from defense, aerospace, and other sectors.
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.
		.003	Virtualization/Sandbox Evasion: Time Based Evasion	During Operation Dream Job, Lazarus Group used tools that collected GetTickCount and GetSystemTimeAsFileTime data to detect sandbox or VMware services.
Enterprise	T1047		Windows Management Instrumentation	During Operation Dream Job, Lazarus Group used WMIC to executed a remote XSL script.

Enterprise	T1220	XSL Script Processing	During Operation Dream Job, Lazarus Group used a remote XSL script to download a Base64-encoded DLL custom downloader.

3. Lazarus Group Techniques Used [1]

Domain	ID		Name	Use
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.
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.
Enterprise	T1098		Account Manipulation	Lazarus Group malware WhiskeyDelta-Two contains a function that attempts to rename the administrator’s account.
Enterprise	T1583	.001	Acquire Infrastructure: Domains	Lazarus Group has acquired domains related to their campaigns to act as distribution points and C2 channels. During Operation Dream Job, Lazarus Group registered a domain name identical to that of a compromised company as part of their BEC effort.
		.004	Acquire Infrastructure: Server	During Operation Dream Job, Lazarus Group acquired servers to host their malicious tools.

		.006	Acquire Infrastructure: Web Services	Lazarus Group has hosted malicious downloads on Github. During Operation Dream Job, Lazarus Group used file hosting services like DropBox and OneDrive.
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.
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Lazarus Group has conducted C2 over HTTP and HTTPS. During Operation Dream Job, Lazarus Group uses HTTP and HTTPS to contact actor-controlled C2 servers.
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.
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.
		.001	Archive via Utility	During Operation Dream Job, Lazarus Group archived victim's data into a RAR file.
		.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.
		.003	Archive via Custom Method	A Lazarus Group malware sample encrypts data using a simple byte based XOR operation prior to exfiltration.
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. During Operation Dream Job, Lazarus Group placed LNK files into the victims' startup folder for persistence.
		.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.
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.
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Lazarus Group has used PowerShell to execute commands and malicious code. During Operation Dream Job, Lazarus Group used PowerShell commands to explore the environment of compromised victims.
		.003	Command and Scripting Interpreter:	Lazarus Group malware uses cmd.exe to execute commands on a compromised host. A Destover-

			Windows Command Shell	like variant used by Lazarus Group uses a batch file mechanism to delete its binaries from the system. During Operation Dream Job, Lazarus Group launched malicious DLL files, created new folders, and renamed folders with the use of the Windows command shell.
		.005	Command and Scripting Interpreter: Visual Basic	Lazarus Group has used VBA and embedded macros in Word documents to execute malicious code. 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.
Enterprise	T1584	.001	Compromise Infrastructure: Domains	For Operation Dream Job, Lazarus Group compromised domains in Italy and other countries for their C2 infrastructure.
		.004	Compromise Infrastructure: Server	Lazarus Group has compromised servers to stage malicious tools. For Operation Dream Job, Lazarus Group compromised servers to host their malicious tools.
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Several Lazarus Group malware families install themselves as new services.

Enterprise	T1485		Data Destruction	Lazarus Group has used a custom secure delete function to overwrite file contents with data from heap memory.
Enterprise	T1132	.001	Data Encoding: Standard Encoding	A Lazarus Group malware sample encodes data with base64.
Enterprise	T1005		Data from Local System	Lazarus Group has collected data and files from compromised networks. During Operation Dream Job, Lazarus Group used malicious Trojans and DLL files to exfiltrate data from an infected host.
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.
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.

4. References

[1] Lazarus Group. https://attack.mitre.org/groups/G0032/

[2] Cyber Security NCC Group Resource Hub articles, The Lazarus group: North Korean scourge for +10 years. https://www.nccgroup.com/the-lazarus-group-north-korean-scourge-for-plus10-years

[3] Lazarus Group, The APT with countless lives. https://eurepoc.eu/wp-content/uploads/2024/02/Advanced-Persistent-Threat-Profile-Lazarus-February-2024.pdf

[4] Inside Lazarus Group: Analyzing North Korea's Most Infamous Crypto Hacks. https://hacken.io/discover/lazarus-group/

[5] Operation Dream Job. https://attack.mitre.org/campaigns/C0022/

[6] Native API. https://attack.mitre.org/techniques/T1106/

[7] Virtualization/Sandbox Evasion: Time Based Evasion. https://attack.mitre.org/techniques/T1497/003/