SOC ANALYST TRANING REPORT

ON

Lazarus Group Malware Analysis Report

Using Mitre Attack Framework

ANALYSED AND REPORTED

BY

ALI CHINASA JULIET

INSTRUCTOR: MR OLA OLAITAN

DATE: September 2024

Introduction

The Lazarus Group is a well-known cyber threat actor linked to the North Korean government. This gang, well-known for its sophisticated cyber operations, has been implicated in a number of high-profile attacks, ranging from disruptive operations to money theft. This report uses the MITRE ATT&CK framework to map the tactics, methods, and procedures (TTPs) of the Lazarus Group in order to present a thorough profile of their malware. Finding weak points in our organization's defenses and offering helpful suggestions to lessen the likelihood of an attack are the objectives.

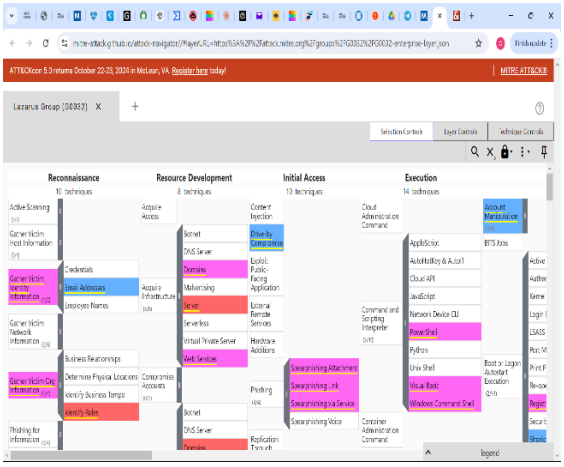
Executive Summary

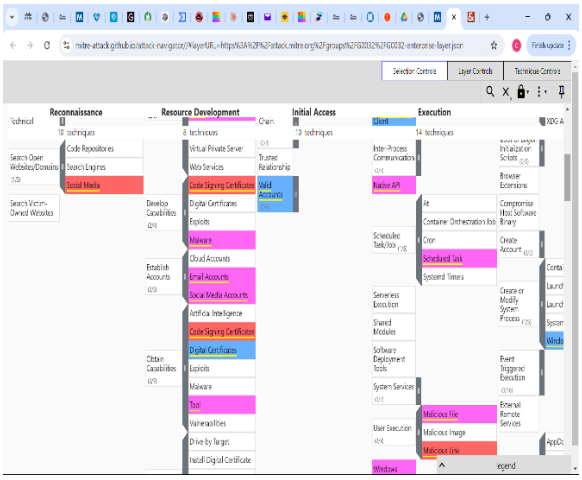
This analysis delves into the Lazarus Group's malware activities, utilizing the MITRE ATT&CK framework to dissect their tactics, techniques, and procedures (TTPs). Our goal is to fortify our organization's cybersecurity defenses against this advanced persistent threat (APT) group.

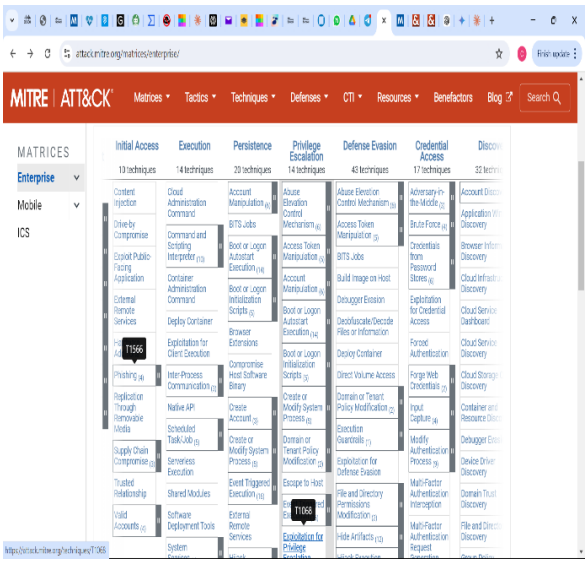
Background

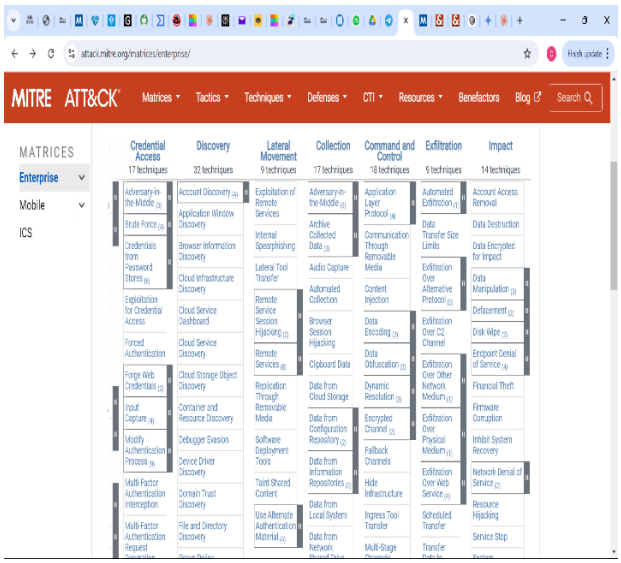
The Lazarus Group, also known as HIDDEN COBRA or APT38, is a North Korean state-sponsored threat actor. They've made headlines with high-profile attacks on financial institutions, government organizations, and critical infrastructure worldwide. Their persistence and evolving tactics make them a top-tier cyber adversary.

MITRE ATT&CK Analysis









Initial Access

- T1566: Phishing
- T1190: Exploit Public-Facing Application

Execution

- T1059: Command and Scripting Interpreter
- T1204: User Execution

Persistence

- T1547: Boot or Logon Autostart Execution
- T1543: Create or Modify System Process

Privilege Escalation

- T1068: Exploitation for Privilege Escalation

Defense Evasion

- T1027: Obfuscated Files or Information
- T1140: Deobfuscate/Decode Files or Information

Credential Access

- T1555: Credentials from Password Stores
- T1056: Input Capture

- T1557: Man-in-the-Middle
- T1110: Brute Force

Discovery

- T1082: System Information Discovery
- T1016: System Network Configuration Discovery
- T1083: File and Directory Discovery
- T1018: Remote System Discovery

Lateral Movement

- T1021: Remote Services
- T1091: Replication Through Removable Media
- T1570: Lateral Tool Transfer
- T1563: Remote Service Session Hijacking

Collection

- T1113: Screen Capture
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1074: Data Staged

Command and Control

- T1071: Application Layer Protocol
- T1573: Encrypted Channel
- T1090: Proxy
- T1572: Protocol Tunneling

Exfiltration

- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1029: Scheduled Transfer
- T1020: Automated Exfiltration

Impact

- T1485: Data Destruction
- T1489: Service Stop
- T1565: Data Manipulation
- T1499: Endpoint Denial of Service

Highlighting the Impact

The Lazarus Group's attacks had the following consequences:

1. Financial Losses: Their heists have resulted in millions of dollars stolen from banks and cryptocurrency exchanges.
2. Data Breaches: Sensitive information exfiltration leads to reputational damage and potential regulatory fines.
3. Operational Disruption: Their destructive malware can cripple an organization's IT infrastructure.
4. Intellectual Property Theft: Targeted attacks on research institutions and tech companies can lead to loss of competitive advantage.
5. National Security Threats: Attacks on government systems pose risks to national security and critical infrastructure.

Recommendations

Short-term Actions

1. Conduct an immediate vulnerability assessment and patch critical systems.
2. Implement strict email filtering rules to combat phishing attempts.
3. Enable multi-factor authentication across all systems and applications.
4. Review and tighten access controls, especially for privileged accounts.
5. Conduct targeted threat hunting exercises based on known Lazarus Group IOCs.

Long-term Strategies

1. Develop a comprehensive security awareness training program.
2. Implement network segmentation to limit potential lateral movement.
3. Deploy and maintain advanced endpoint detection and response (EDR) solutions.
4. Establish a robust incident response plan with regular drills.
5. Engage in threat intelligence sharing with industry peers and relevant government agencies.
6. Implement a zero-trust architecture across the organization.
7. Develop and maintain an asset inventory and vulnerability management program.

Conclusion

The Lazarus Group isn't just another name on a threat feed - they're a clear and present danger to our digital assets and operations. Their sophisticated tactics demand an equally sophisticated defense. By implementing these recommendations and staying vigilant, we're not just protecting data; we're safeguarding our organization's future.