cybersecurity
associates

# Lazarus

## Threat Hunting Report

Dated: 01/09/2023

Written by: Sohaib Saif

This report contains Threat Hunting research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about current and emerging threats to identify countermeasures which can be put into place to thwart the threat.

# Contents

# Lazarus

## Threat Report

### Executive Summary

The purpose of this report is to document the current form and methodologies used by the Lazarus threat actor. The information documented is then used by Cyber Security Associates Ltd (CSA) Cyber Analysts to detect and hunt for the threat within the client environment through the use of our supported SIEM's BorderPoint, Microsoft Sentinel and LogRhythm and advise on counter measures to monitor and detect for the subject threat.

This report documents the threat group Lazarus and their TTPs (Tactics, Techniques and Procedures). Containing recommendations to help detect and mitigate the threat. The report also includes references where information within this report was identified from.

## Summary

Lazarus are a sophisticated Advanced Persistent Threat (APT) organisation that has gathered international attention due to their malicious cyber activity, with evidence likely linking them to be state sponsored by North Korea. This group has been active and highly dangerous since 2009 and are known to exhibit a versatile range of cyber espionage, financial theft and disruptive attacks.

One of the most high-profile attacks attributed to Lazarus is the 2014 Sony Pictures hack. This was a targeted attack at the entertainment company in response to the release of a movie perceived as offensive to North Korea's leader [1]. This attack included data theft, destructive malware and reputational damage strategies.

Lazarus is also responsible for the infamous WannaCry [2] ransomware attack in 2017, this affected hundreds of thousands of computers worldwide many of which were part of the Critical National Infrastructure. Although they have not conducted any attacks of this scale recently, they are making the news every year with the most recent activity seen in August 2023.

The groups techniques have evolved over time, encompassing advanced persistent threats, supply chain attacks and cryptocurrency theft. Lazarus is known for their technical capabilities and stealthy operations. It is for these reasons that a threat report on Lazarus is helpful to understand the current threat they constitute. This report will focus on the most recent Lazarus campaigns that were started or resumed within the last 12 months.

## Tactics, Techniques & Procedures

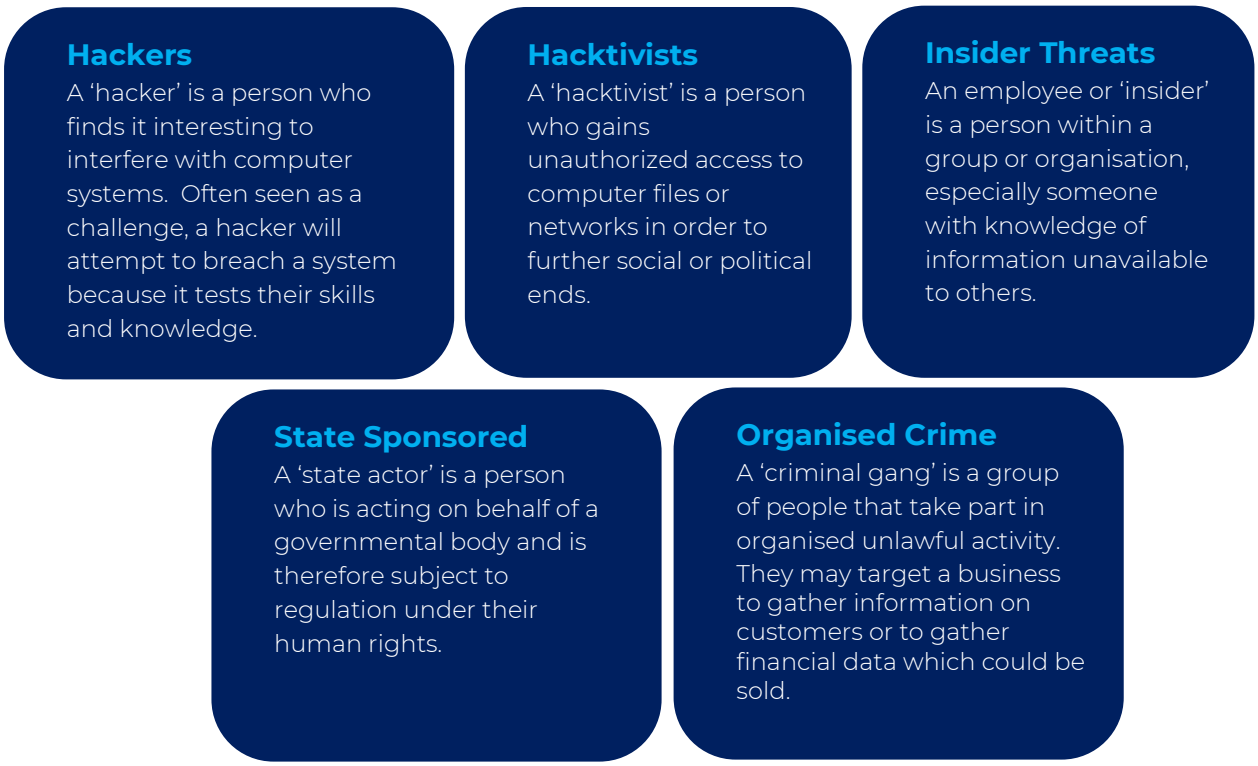
Tactics, Techniques, and Procedures (TTPs) describes the actions, behaviours, processes and strategies used by malicious adversaries that engage in cyber-attacks.

Tactics will outline the overall goals behind an attack, including the strategies that were followed by the attacker to implement the attack. For example, the goal may be to steal credentials. Understanding the Tactics of an adversary can help in predicting the upcoming attacks and detect those in early stages.

Techniques will show the method that was used to engage in the attack, such as cross-site scripting (XSS), manipulation through social engineering and phishing, to name a few. Identifying the Techniques used during an attack can help discover an organisation's blind spots and implement countermeasures in advance.

Procedures will describe the tools and methods used to produce a step-by-step description of the attack. Procedures can help to create a profile for a threat actor or threat group. The analysis of the procedures used by the adversary can help to understand what the adversary is looking for within their target's infrastructure.

Analysts follow this methodology to analyse and define the TTPs to aid in counterintelligence. TTPs that are described within this research are based of the information which CSA analysts have been able to identify prior to the release of this document. The threat may change and adapt as it matures to increase its likelihood of evading defence.



## Phase 1: Initial Access

Lazarus utilise a variety of sophisticated techniques involving initial access methods to breach target networks. Some of the most known initial access methods used by the APT group include:

### Spear Phishing

Spear phishing is a targeted form of phishing that involves sending a tailored email to specific individuals within an organisation. Lazarus employs this technique to trick employees into giving away sensitive information or clicking malicious attachments. These emails are carefully crafted to appear legitimate and often contain malicious attachments or links that, when clicked, lead to the deployment of malware.

### Watering Hole Attacks

In a watering hole attack, the Lazarus group compromises websites frequently visited by the target organisations employees. By injecting malicious code into these sites, the attackers infect the visitors' systems with malware. When employees visit the compromised sites, their devices become infected, providing Lazarus with a foothold in the network.

### MITRE ATT&CK

MITRE developed the Adversarial Tactics, Techniques and Common Knowledge framework (ATT&CK), which is used to track various techniques attackers use throughout the different stages of cyberattack to infiltrate a network and exfiltrate data.

The framework defines the following tactics that are used in a cyberattack:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

### Exploitation of Zero-Day Vulnerabilities

Lazarus is known to exploit zero-day vulnerabilities in software applications. These are previously unknown vulnerabilities that allow attackers to gain unauthorised access before a patch is developed. By exploiting such vulnerabilities, the group can evade security measures and establish a presence within the target network.

### Supply Chain Attacks

The Lazarus APT group has also been associated with supply chain attacks. This involves targeting trusted third-party vendors or suppliers of the target organisation. This would also create issues for the target organisations without having to target them directly.

### Remote Access Trojans (RATs)

Remote Access Trojans are commonly used by Lazarus. They allow the group to gain unauthorised remote access to compromised systems. Lazarus use RATs to maintain persistence and move laterally within a network and also gather intelligence over a long period of time.

Lazarus initial access can be mapped to the following Mitre ATT&CK techniques [3]:

| Technique | ID | Description |
|---|---|---|
| Phishing | T1566 | Phishing can involve many different tactics. Spear phishing is specifically targeted at certain users. Lazarus is known to use these tactics as part of initial access. |
| Supply Chain Compromise | T1195 | Adversaries may manipulate products prior to it being given to the final consumer or the target organisation. This can include software dependencies and tools but can also include hardware manipulation. |
| Exploit Public Facing Application | T1190 | Adversaries may attempt to exploit a weakness in an internet facing host or system that the target organizations employees often use. This weakness may include a software bug or misconfiguration. |
| Drive-by Compromise | T1189 | Adversaries may gain access to an organizations system through an employee's normal course of browsing the internet. In this technique, the web browser is usually targeted for exploitation, however, adversaries may also use compromised websites for non-exploitation techniques such as acquiring an application access token. |

## Phase 2: Reconnaissance and Privilege Escalation

An investigation of the Lazarus campaign DeathNote, revealed some of the tactics they used to conduct reconnaissance.

### Basic reconnaissance

This included using numerous windows commands to gather basic system information:

- “cmd.exe /c netstat -ano | find TCP”
- “systeminfo”

In one instance, they accessed the default domain controllers policy directly using:

- Cmd.exe /c “Type “Type \\[redacted]SYSVOL\[redacted]\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf

### Finding high-value hosts

To find a connected Remote Desktop host, they utilized Windows commands or queried the saved server list from the registry:

- “cmd.exe /c netstat -ano | findstr 3389”
- “cmd.exe /c reg query HKEY_USERS\S-1-5-[redacted]-1001\Software\Microsoft\Terminal Server Client\Servers”

Utilizing ADFind tool to acquire Active directory information:

- cmd.exe /c “%appdata%\[redacted].xic -b dc=[redacted],dc=[redacted] -f “sAMAccountName=[redacted]” >> %temp%\dm3349.tmp 2>&1"

### Acquiring Logon Credentials

Lazarus used Mimikatz to dump login credentials and also used the Responder tool to capture credentials.

### Lateral Movement

Some common approaches for launching commands on remote hosts that Lazarus have used include SMB connections and the ServiceMove technique.

### Cyber Kill-Chain

The cyber kill chain is a process that traces the stages of a cyberattack. This starts at the early reconnaissance stages that eventually leads to data exfiltration.

The kill chain can help one to understand and combat ransomware, advanced persistent threats (APTs) and security breaches.

The cyber kill-chain defines the following tactics that are used in a cyberattack:

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

## Phase 3: Exfiltration

Once they have gained access to a system and found what they are looking for, they will begin to exfiltrate that data. Lazarus use various methods to do this including the following:

### Command and Control Infrastructure (C2 Servers)

The group often establishes a complex network of command-and-control servers to manage their operations. These servers act as intermediaries for exfiltration, allowing them to maintain persistence within the compromised networks. The group frequently uses compromised legitimate websites or hidden servers on the TOR network to host their C2 infrastructure. This makes it difficult to detect and block the communication channels.

### Data Compression and Encryption

To minimize the volume of data transferred and avoid detection, Lazarus uses compression and encryption techniques. This allows them to disguise the exfiltrated data as benign network traffic which then makes it difficult for security solutions to identify any suspicious activity. By using encryption, they can ensure that even if the data is intercepted, the data remains inaccessible.

Examples of commands using WinRAR to archive files before sending the stolen file via C2 channel can be seen below for Lazarus:

- adobearm.exe a -hp1q2w3e4 -m5 -v2000000k “%Local AppData%\Adobe\SYSVOL800.CHK” “\\[redacted]FILE02.[redacted]\Projects\[redacted] Concept Demonstrator”
- %appdata%\USOShared\USOShared.LOG1 a -hpb61de03de6e0451e834db6f185522bff -m5 “%appdata%\USOShared\USOShared.LOG2” “%appdata%\ntuser.001.dat”

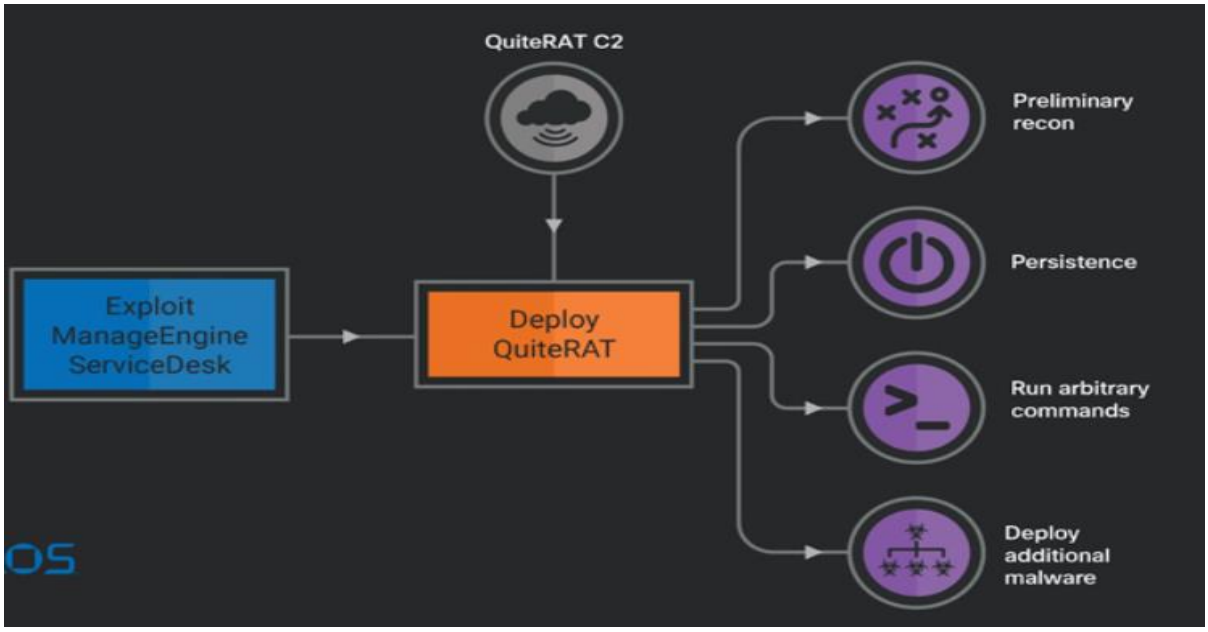
### Exfiltration over Unencrypted Non C2 Protocol

The Lazarus group has previously used exfiltration through the SMTP protocol. This was done with their malware SierraBravo-Two. An email message via SMTP would be sent containing information about newly infected victims. This would allow the group to exfiltrate data without raising too much suspicion.

## Latest News

Whilst this report has mainly focused on the continuation of DeathNote in 2023 by Lazarus, they have recently made the news again for their malicious activities. On this occasion, they managed to exploit a critical Zoho ManageEngine Flaw to deploy a stealthy QuiteRAT malware [4]. Although this flaw has now been patched, ManageEngine's solutions power over 200,000 companies around the world so it is important to understand what recently occurred.

This attack involved the exploitation of the vulnerability CVE-2022-47966 [5]. ServiceDesk Plus, one of ManageEngine's solutions, allowed remote code execution due to the use of Apache xmlsec. This was because xmlsec made the application responsible for certain security protections and the ManageEngine applications did not provide those protections.




QuiteRAT has shown many capabilities of the Lazarus Group's better known MagicRAT malware. However, the file size of QuiteRAT is significantly smaller. The development of these Remote Access Trojans shows that the Lazarus Group is shifting its tactics whilst also looking to exploit new vulnerabilities.

## Conclusion:

This report has looked at the threat posed by the Lazarus Group and some of the TTPs they use. Although the WannaCry cyber attack was over 5 years ago, Lazarus should not be overlooked as they are still active and developing their tools and techniques for further malicious activity.

## Advice:

### Training and Awareness

Like many other APT groups, Lazarus relies on social engineering as an initial attack vector. Therefore, educating employees as to the dangers of spear phishing is crucial. This should include phishing emails as well as phishing through social media. This is because an attacker might gain access to sensitive information that can be used to further social engineer remote access to a network.

### Strengthening security posture via a Security Operations Centre (SOC)

Some organisations may benefit from the use of a Security Operations Centre (SOC). Some benefits of a SOC [6] include preventing cyber security incidents through proactive measures such as scanning for vulnerabilities and deploying automated playbooks in the event of an incident. The use of a SOC also allows analysis of potential intrusions in real time by using a variety of data sources.

### Multifactor authentication (MFA)

Organisations should ensure that MFA is enabled and enforced for all users. This would help as even if an attacker was able to get hold of credentials, they would not be able to pass MFA. The enforcement of conditional access policies may also be useful to stop sign-ins from locations that are not expected.

### Enforcing the principle of least privilege

We have seen in this report that one way Lazarus is able to conduct its activities is through the use of administrator credentials. Administrators should only have access to the resources that are necessary for their roles [7]. This will limit the amount of damage an attacker could do if they can get access to administrator credentials.

# Indicators of Compromise

## DeathNote Campaign [8]

### Malicious Documents

265f407a157ab0ed017dd18cae0352ae

7a73a2261e20bdb8d24a4fb252801db7

7a307c57ec33a23ce9b5c84659f133cc

ced38b728470c63abcf4db013b09cff7

9121f1c13955506e33894ffd780940cd

50b2154de64724a2a930904354b5d77d

8a05f6b3f1eb25bcbceb717aa49999cd

ee73a772b72a5f3393d4bf577fc48efe

### Downloader

d1c652b4192857cb08907f0ba1790976

25b37c971fd7e9e50e45691aa86e5f0a

0493f40628995ae1b7e3ffacd675ba5f

8840f6d2175683c7ed8ac2333c78451a

c278d6468896af3699e058786a8c3d62

9fd35bad075c2c70678c65c788b91bc3

59cb8474930ae7ea45b626443e01b66d

7af59d16cfd0802144795ca496e8111c

cd5357d1045948ba62710ad8128ae282

77194024294f4fd7a4011737861cce3c

e9d89d1364bd73327e266d673d6c8acf

0d4bdfec1e657d6c6260c42ffdbb8cab

5da86adeec6ce4556f477d9795e73e90

706e55af384e1d8483d2748107cbd57c

### Manipulated Installer

dd185e2bb02b21e59fb958a4e12689a7

### Installer

4088946632e75498d9c478da782aa880 C:\Windows\igfxmon.exe

### Injector

dc9244206e72a04d30eeadef23713778 C:\Windows\system32\[random 2 bytes]proc.exe

### Backdoor

735afcd0f6821cbd3a2db510ea8feb22 C:\Windows\system32\[random 2 bytes]svc.dll

### Shifting focus to the defence industry

### Malicious documents

4c239a926676087e31d82e79e838ced1 pubmaterial.docx

183ad96b931733ad37bb627a958837db Boeing_PMS.docx

9ea365c1714eb500e5f4a749a3ed0fe7 Boeing_DSS_SE.docx

2449f61195e39f6264d4244dfa1d1613 Senior_Design_Engineer.docx

880b263b4fd5de0ae6224189ea611023 LM_IFG_536R.docx.docx

e7aa0237fc3db67a96ebd877806a2c88 Boeing_AERO_GS.docx

56470e113479eacda081c2eeead153bf boeing_spectrolab.docx

### Fetched Template

2efbe6901fc3f479bc32aaf13ce8cf12 pubmaterial.dotm

65df11dea0c1d0f0304b376787e65ccb 43.dotm

0071b20d27a24ae1e474145b8efc9718 17.dotm

1f254dd0b85edd7e11339681979e3ad6 61.dotm

### DeathNote Downloader

f4b55da7870e9ecd5f3f565f40490996 onenote.db, thumbnail.db

2b02465b65024336a9e15d7f34c1f5d9 wsuser.db

11fdc0be9d85b4ff1faf5ca33cc272ed onenote.db

f6d6f3580160cd29b285edf7d0c647ce

78d42cedb0c012c62ef5be620c200d43 wsuser.db

92657b98c2b4ee4e8fa1b83921003c74

075fba0c098d86d9f22b8ea8c3033207 wsdts.db

8fc7b0764541225e5505fa93a7376df4

7d204793e75bb49d857bf4dbc60792d3 2.dll

eb2dc282ad3ab29c1853d4f6d09bec4f

ca6658852480c70118feba12eb1be880 thumbnail.db

c0a8483b836efdbae190cc069129d5c3 wsdts.db

14d79cd918b4f610c1a6d43cadeeff7b wsuser.db

1bd0ca304cdecfa3bd4342b261285a72

### Trojanized PDF viewer

cbc559ea38d940bf0b8307761ee4d67b SumatraPDF.exe

da1dc5d41de5f241cabd7f79fbc407f5 internal pdf viewer.exe

### Expanded target and adoption of new infection vector

### Racket Downloader

b3a8c88297daecdb9b0ac54a3c107797 SCSKAppLink.dll

### BLIDINGCAN

b23b0de308e55cbf14179d59adee5fcb

64e5acf43613cd10e96174f36cb1d680

### COPPERHEDGE Loader

a43bdc197d6a273102e90cdc0983b0b9

### COPPERHEDGE

97336f5ce811d76b28e23280fa7320b5

### Downloader Loader

f821ca4672851f02bead3c4bd23bed84 c:\officecache\officecert.ocx

### Racket Downloader

b974bc9e6f375f301ae2f75d1e8b6783 %public%\Libraries\SCSKAppLink.dll

eb061dfacb3667cf65d250911179235d

### Stealer

fe549a0185813e4e624104d857f9277b %ProgramData%\GenICam\GenICamKDR.gic

### Backdoor Loader

7b8960e2a22c8321789f107a7b83aa59 %ProgramData%\xilinx\xilinx.pkg

0ac90c7ad1be57f705e3c42380cbcccd %ProgramData%\USOShared\USOShare.cpl

### Mimikatz Loader

adf0d4bbefccf342493e02538155e611 %ProgramData%\USOShared\log.dll

d4d654c1b27ab90d2af8585052c77f33

## An ongoing attack targeting a defense contractor with updated infection tactics

### Loader

2bcf464a333d67afeb80360da4dfd5bb
C:\Windows\system32\perceptionsimulation\devobj.dll

83dd9b600ed33682aa21f038380a6eab
C:\Windows\system32\perceptionsimulation\devobj.dll

### ForestTiger(Backdoor)

97524091ac21c327bc783fa5ffe9cd66
ProgramData\adobe\arm\lockhostingframework.dll

9b09ebf52660a9d6deca21965ce52ca1 %appdata%\adobe\arm\DUI70.dll

26c0f0ce33f5088754d88a1db1e6c4a9

### Trojanized PDF reader

84cd4d896748e2d52e2e22d1a4b9ee46 SecurePDF.exe

## Lazarus QuiteRat Malware [9]

### Collection Rat

ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6

db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984

773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df

05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d

e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe

146.4.21.94

109.248.150.13

108.61.186.55:443

http://146.4.21.94/tmp/tmp/comp.dat

http://146.4.21.94/tmp/tmp/log.php

http://146.4.21.94/tmp/tmp/logs.php

http://ec2-15-207-207-64.ap-south-1.compute.amazonaws.com/resource/main/rawmail.php

http://109.248.150.13/EsaFin.exe

http://146.4.21.94/boards/boardindex.php

http://146.4.21.94/editor/common/cmod

### Quite Rat

ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6

http://146.4.21.94/tmp/tmp/comp.dat

http://146.4.21.94/tmp/tmp/log.php

http://146.4.21.94/tmp/tmp/logs.php

http://ec2-15-207-207-64.ap-south-1.compute.amazonaws.com/resource/main/rawmail.php

## References


[1] https://www.nccgroup.com/uk/the-lazarus-group-north-korean-scourge-for-plus10-years/

[2] https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

[3] https://attack.mitre.org/tactics/TA0001/

[4] https://blog.talosintelligence.com/lazarus-quiterat/

[5] https://nvd.nist.gov/vuln/detail/cve-2022-47966

[6] https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

[7] https://www.cyberark.com/what-is/least-privilege/

[8] https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

[9] https://github.com/Cisco-Talos/IOCs/tree/main/2023/08