

Hack the Box — Sherlock Dream Job-1

Sherlock Dream-Job 1

- **Perfil:** Blue Team - Cyber Threat Intelligence
- **Sección:** Threat Intelligence
- **Dificultad:** Muy fácil

En este laboratorio vamos a estar resolviendo un ejercicio correspondiente a la plataforma especializada en ejercicios de ciberseguridad y hacking, Hack the Box, dentro del apartado de sus sherlocks, que son labs de blue team.

Para este ejercicio utilizaremos la herramienta de **MITRE ATT&CK** y la plataforma **VirusTotal** para la inteligencia de amenazas.

Enunciado: *“Eres un analista junior de inteligencia de amenazas en una empresa de ciberseguridad. Se te ha encargado investigar una campaña de ciberespionaje*

conocida como Operación Dream Job. El objetivo es reunir información crucial sobre esta operación”.

Los indicadores de compromiso que se nos deja son los siguientes:

1. 7bb93be636b332d0a142ff11aedb5bf0ff56deabba3aa02520c85bd99258406f
2. adce894e3ce69c9822da57196707c7a15acee11319ccc963b84d83c23c3ea802
3. 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1

DREAM JOB-1—SOLUCIÓN

Task 1:

Who conducted Operation Dream Job?

Lazarus Group

Lo primero que debemos hacer antes de contestar el resto de preguntas es determinar que grupo fue el perpetrador de la campaña “**Operation Dream Job**” una operación de ciberespionaje.

Lo podemos encontrar dentro del framework **MITRE ATT&CK** si buscamos el nombre de la operación.

Operation Dream Job

Operation Dream Job was a cyber espionage operation likely conducted by Lazarus Group that targeted the defense, aerospace, government, and other sectors in the United States, Israel, Australia, Russia, and India. In at least one case, the cyber actors tried to monetize their network access to conduct a business email compromise (BEC) operation. In 2020, security researchers noted overlapping TTPs, to include fake job lures and code similarities, between Operation Dream Job, Operation North Star, and Operation Interception; by 2022 security researchers described Operation Dream Job as an umbrella term covering both Operation Interception and Operation North Star.^{[1][2][3][4]}

Para ponernos en contexto, **Lazarus Group** es un APT de origen norcoreano muy famoso por llevar a cabo ciberataques y operaciones de gran magnitud, donde se destaca el ataque a Sony Pictures en 2014, el robo al banco de Bangladesh en 2016, el ransomware de WannaCry en 2017 y, más recientemente, el hackeo a ByBit en este mismo año, reforzando sus ataques en operaciones relacionadas al robo de criptomonedas, aspecto en el que se han centrado últimamente.

Task 2:

When was this operation first observed?

September 2019

Esta información también se nos brinda de manera muy directa dentro de la misma sección de la operación de la pregunta anterior, indicándonos el mes y el año donde se ejecutó por primera vez la acción delictiva.

Operation Dream Job

Operation Dream Job was a cyber espionage operation likely conducted by Lazarus Group that targeted the defense, aerospace, government, and other sectors in the United States, Israel, Australia, Russia, and India. In at least one case, the cyber actors tried to monetize their network access to conduct a business email compromise (BEC) operation. In 2020, security researchers noted overlapping TTPs, to include fake job lures and code similarities, between Operation Dream Job, Operation North Star, and Operation Interception; by 2022 security researchers described Operation Dream Job as an umbrella term covering both Operation Interception and Operation North Star.^{[1][2][3][4]}

ID: C0022
First Seen: September 2019 ^[3]
Last Seen: August 2020 ^[1]
① Associated Campaigns: Operation North Star, Operation Interception
Version: 1.2
Created: 17 March 2023
Last Modified: 11 April 2024

[Version Permalink](#)

Task 3:

There are 2 campaigns associated with Operation Dream Job. One is Operation North Star, what is the other?

Operation Interception

Nuevamente sin salirnos de esta sección, encontraremos ese segundo nombre debajo.

Associated Campaign Descriptions

Name	Description
Operation North Star	[2][5]
Operation Interception	[3]

Task 4:

During Operation Dream Job, there were the two system binaries used for proxy execution. One was Regsvr32, what was the other?

Rundll32

Para esta pregunta, debemos bajar a observar las tácticas utilizadas por el grupo para ejecutar esta operación.

Se nos describe unas cuantas, pero debemos hacer hincapié particularmente en la técnica de **proxy execution**.

Enterprise	T1218	.010	System Binary Proxy Execution: Regsvr32	During Operation Dream Job, Lazarus Group used <code>regsvr32</code> to execute malware.[3]
		.011	System Binary Proxy Execution: Rundll32	During Operation Dream Job, Lazarus Group executed malware with <code>C:\\windows\\system32\\rundll32.exe "C:\\ProgramData\\ThumbNail\\thumbnail.db", CtrlPanel S-6-81-3811-75432205-060098-6872 0 0 905.[1][3][2]</code>

El **Rundll32** es un archivo ejecutable legítimo de Windows y su función principal es permitir que los archivos DLL puedan ejecutarse como si fueran programas independientes.

Task 5:

What lateral movement technique did the adversary use?

Internal Spearphishing

Un **spearphishing** puede ser una táctica de **movimiento lateral** en el contexto de un ciberataque porque permite a un atacante comprometer cuentas específicas

dentro de una red y luego utilizar esas credenciales o accesos para desplazarse a otros sistemas o recursos dentro de la misma infraestructura.

Enterprise	T1534	Internal Spearphishing	During Operation Dream Job, Lazarus Group conducted internal spearphishing from within a compromised organization. ^[1]
------------	-------	------------------------	---

Al fin y al cabo, el spearphishing actuaría como una puerta de entrada, de modo tal que luego se produzcan las acciones maliciosas, como el robo de credenciales, explotación de directorios internos e incluso ir más allá y aplicar pivoting.

Task 6:

What is the technique ID for the previous answer?

T1534

Enterprise	T1534	Internal Spearphishing	During Operation Dream Job, Lazarus Group conducted internal spearphishing from within a compromised organization. ^[1]
------------	-------	------------------------	---

Task 7:

What Remote Access Trojan did the Lazarus Group use in Operation Dream Job?

DRATzarus

Ahora debemos determinar cuál **RAT** fue utilizado por el grupo norcoreano para el trabajo malicioso.

Para ello nos dirigiremos a la sección de software usados en esta operación.

Software

ID	Name	Description
S0694	DRATzarus	During Operation Dream Job, Lazarus Group used DRATzarus to deploy open source software and partly commodity software such as Responder, Wake-On-Lan, and ChromePass to target infected hosts. ^[1]
S0174	Responder	^[1]
S0678	Torisma	During Operation Dream Job, Lazarus Group used Torisma to actively monitor for new drives and remote desktop connections on an infected system. ^{[2][5]}

DRATzarus

DRATzarus is a remote access tool (RAT) that has been used by Lazarus Group to target the defense and aerospace organizations globally since at least summer 2020. DRATzarus shares similarities with Bankshot, which was used by Lazarus Group in 2017 to target the Turkish financial sector.^[1]

Task 8:

What technique did the malware use for execution?

Native API

Vamos a fijarnos ahora en las técnicas utilizadas únicamente por este troyano de acceso remoto.

Enterprise	T1106	Native API	DRATzarus can use various API calls to see if it is running in a sandbox. ^[1]
------------	-------	------------	--

Esto sugiere que el análisis ha identificado que el malware (**DRATzarus**) está utilizando **APIs nativas** del sistema operativo (como las de Windows, por ejemplo) para ejecutar sus funciones.

También se indica que el malware tiene la capacidad de detectar si está siendo ejecutado en un entorno controlado o de análisis, como una máquina virtual o un entorno de sandbox.

Task 9:

What technique did the malware use to avoid detection in a sandbox?

Time Based Evasion

Esta técnica le permite al software malicioso poder evitar ser detectado dentro de un entorno controlado, haciendo uso de dos APIs que se mencionan.

Además, puede apagarse en ciertos momentos y/o condiciones para mejorar sus capacidades de camuflaje dentro del sistema infectado.

Enterprise	T1497	.003	Virtualization/Sandbox Evasion: Time Based Evasion	DRATzarus can use the <code>GetTickCount</code> and <code>GetSystemTimeAsFileTime</code> API calls to measure function timing. ^[1] DRATzarus can also remotely shut down into sleep mode under specific conditions to evade detection. ^[1]
------------	-------	------	---	--

GetTickCount y **GetSystemTimeAsFileTime** son funciones de la API de Windows que proporcionan información sobre el tiempo en un sistema.

Son comúnmente utilizadas, en un contexto malicioso, para detectar entornos de análisis como sandboxes.

- Si `GetTickCount` devuelve un valor muy bajo (indicando que el sistema “acaba de iniciarse”), el malware podría sospechar de un entorno virtual.
- Si `GetSystemTimeAsFileTime` muestra una fecha inconsistente (como 1970 o una fecha futura en un sandbox mal configurado), el malware podría interpretarlo como una señal de análisis.

Task 10:

To answer the remaining questions, utilize VirusTotal and refer to the IOCs.txt file. What is the name associated with the first hash provided in the IOC file?

IEXPLORE.EXE

Nos movemos hacia otra plataforma de análisis llamada **VirusTotal**, muy popular para la investigación de archivos, URL, hashes, entre otros IoC.

Si recordamos, se nos ha provisto de tres hashes que vinculan a archivos maliciosos para su respectiva observación.

55/72 security vendors flagged this file as malicious

7bb93be636b332d0a142ff11aedb5bf0ff56deabba3aa02520c85bd99258406f

Size: 181.50 KB | Last Analysis Date: 2 days ago

Community Score: 55/72

File Name: IEXPLORE.EXE

peexe assembly 64bits spreader

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.nukesped/agentb | Threat categories: trojan | Family labels: nukesped, agentb, comebacker

Security vendors' analysis

Vendor	Detection	Vendor	Detection
AhnLab-V3	Backdoor.Win32.Agent.R346780	Alibaba	Trojan.Win64/Comebacker.004ddb3e
AliCloud	Trojan:Win/NukeSped.CK	ALYac	Trojan.Agent.185344L
Antiy-AVL	Trojan[APT]/Win32.Lazarus	Arcabit	Trojan.Generic.D20B2A96
Avast	Win64:Trojan-gen	AVG	Win64:Trojan-gen

Task 11:

When was the file associated with the second hash in the IOC first created?

2020-05-12 19:26:17

Se nos solicita la fecha exacta de cuando se creó el archivo asociado al segundo hash.

Esto lo podemos hallar dentro de la sección de detalles.

History ⓘ

Creation Time	2020-05-12 19:26:17 UTC
First Seen In The Wild	2020-08-13 08:44:50 UTC
First Submission	2020-06-05 09:20:22 UTC
Last Submission	2022-11-26 16:01:01 UTC
Last Analysis	2025-03-12 22:11:55 UTC

Task 12:

What is the name of the parent execution file associated with the second hash in the IOC?

BAE_HPC_SE.iso

Un **parent execution file** se refiere al archivo ejecutable (generalmente un programa o proceso) que inicia o "engendra" otro proceso en un sistema operativo.

En términos sencillos, es el proceso padre que crea un proceso hijo al ejecutarse.

En este caso, se nos pregunta el parent execution file asociado al archivo que refiere el segundo hash.

La respuesta la encontramos en la sección de relaciones.

Execution Parents (1) ⓘ

Scanned	Detections	Type	Name
2024-12-05	37 / 61	ISO image	BAE_HPC_SE.iso

Task 13:

Examine the third hash provided. What is the file name likely used in the campaign that aligns with the adversary's known

tactics?

Salary_Lockheed_Martin_job_opportunities_confidential.doc

En este caso, se nos pregunta qué otro nombre tiene este archivo que se relaciona con la campaña que hemos estado investigando y que además se alinea con las tácticas conocidas del atacante.

Para ello, debemos ir hacia el apartado de nombres ubicado en la sección de detalles.

Names ⓘ

z00TN6TzKIO8HWOFvYH12h7mUJOIP2

malware_sample_003

lazarus.doc

0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1.doc

Salary_Lockheed_Martin_job_opportunities_confidential.doc

output.191053719.txt

125.vir

829050.doc

0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1.bin

No hace falta ser muy inteligente para darnos cuenta que probablemente se utiliza este nombre para que se pueda colar como un **phishing**, y así aumentar las probabilidades de que un usuario lo ejecute.

Task 14:

Which URL was contacted on 2022-08-03 by the file associated with the third hash in the IOC file?

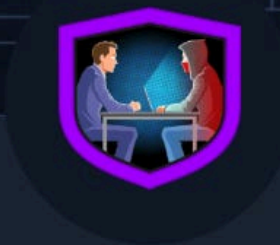
https://markettrendingcenter[.]com/lk_job_oppor.docx (URL MALICIOSA, BORRAR LOS CORCHETES)

Se nos pregunta qué dirección fue contactada en la fecha mencionada por parte de ese archivo.

Contacted URLs (10) ⓘ

Scanned	Detections	Status	URL
2025-02-26	0 / 96	200	http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
2025-03-11	12 / 96	-	https://markettrendingcenter.com/
2022-08-03	14 / 88	200	https://markettrendingcenter.com/lk_job_oppor.docx
2022-09-13	11 / 88	404	https://markettrendingcenter.com/member.htm
2022-09-13	0 / 88	200	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?86057a3ba45eb9ff
2025-02-26	0 / 96	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2025-03-13	0 / 96	200	http://x1.i.lencr.org/
2025-01-22	10 / 96	400	http://markettrendingcenter.com:443/
2025-02-26	0 / 96	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c
2025-02-26	0 / 96	200	http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt

¡Ejercicio completado!



Dream Job-1 has been Solved

TiziMass has successfully solved Dream Job-1 from Hack The Box

#384 SHERLOCK RANK	13 Mar 2025 SOLVE DATE
------------------------------	----------------------------------

