DreamJob-1 Writeup

2025-01-30

Prepared by: ArthurWho, VivisGhost

Machine Author: ArthurWho

Difficulty: Very-Easy

Description

> In this Sherlock, players will be introduced to the MITRE ATT&CK framework, which is a comprehensive tool used to research and understand advanced persistent threat (APT) groups. Specifically, players will focus on the APT group known as Lazarus Group. As they progress, players will get to explore various tactics, techniques, and procedures (TTPs) associated with Lazarus Group.

Scenario

> You are a junior threat intelligence analyst at a Cybersecurity firm. You have been tasked with investigating a Cyber espionage campaign known as Operation Dream Job. Use MITRE ATT&CK to gather crucial information about this operation

Artifacts Provided

- DreamJob1.zip - *fb58f87593fafaf51be524fcb6d1b8760142f7a163f04a9aee2262872a10ed46*

Skills Learnt

- Threat Intelligence
- MITRE ATT&ACK

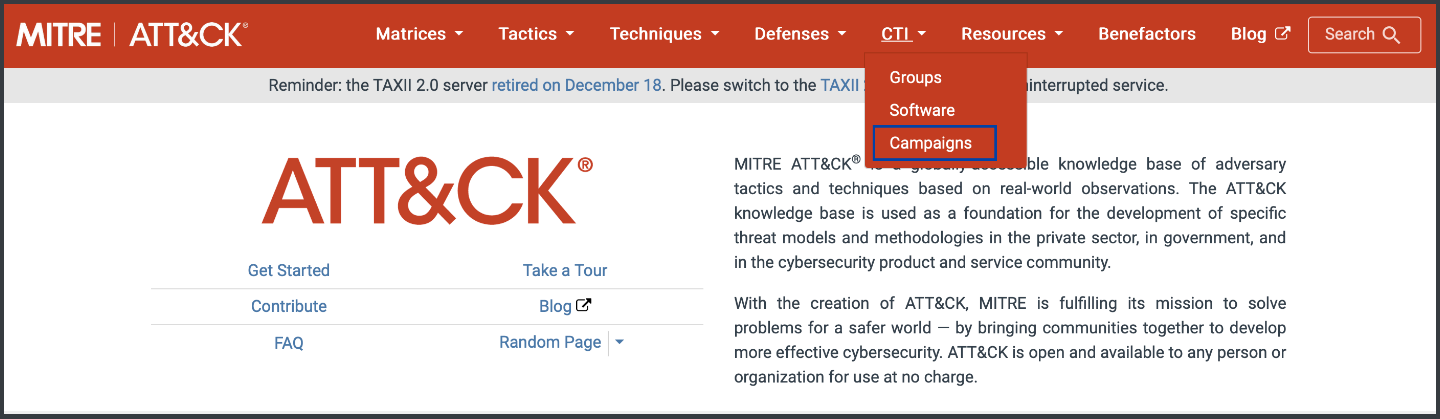
Initial Analysis

To begin the analysis, the password-protected ZIP file was unlocked using the password `hacktheblue`. Inside we will find an `IOCs.txt`. This will be used to answer the final questions.

```
IOCs.txt
1. 7bb93be636b332d0a142ff11aedb5bf0ff56deabba3aa02520c85bd99258406f
2. adce894e3ce69c9822da57196707c7a15acee11319ccc963b84d83c23c3ea802
3. 0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1
```

To answer the following questions we will utilize **MITRE ATT&CK**. **MITRE ATT&CK** is used for threat intelligence, where you can find information about adversaries, groups, campaigns, and the software they use. It's a valuable resource for understanding how cyber threats operate and how to defend against them.

Let's start by going to the **MITRE ATT&CK** page (https://attack.mitre.org) and click on `CTI -> Campaigns`.

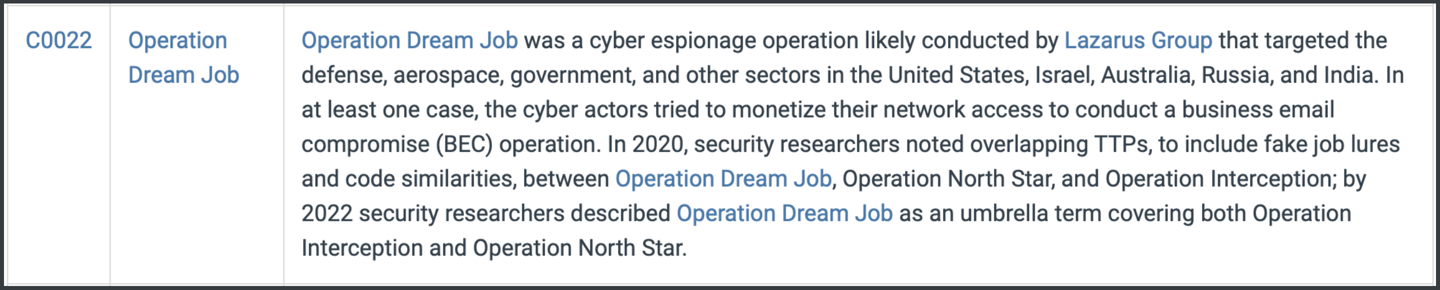


Reminder: the TAXII 2.0 server retired on December 18. Please switch to the TAXII … interrupted service.

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

Once on the page we can scroll down to find `Operation Dream Job`.

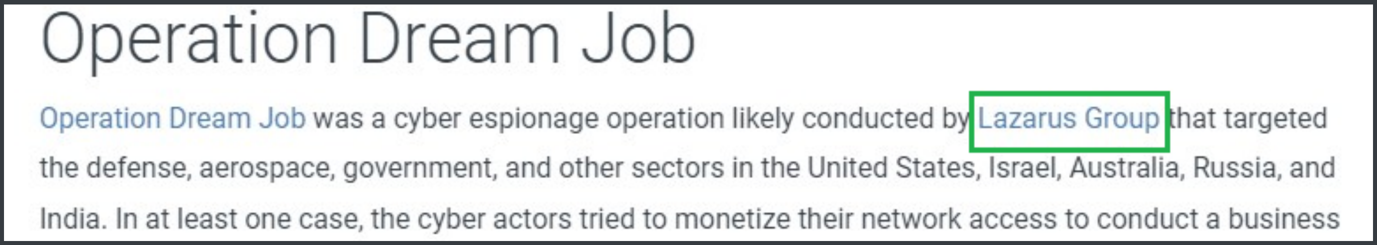


C0022	Operation Dream Job	Operation Dream Job was a cyber espionage operation likely conducted by Lazarus Group that targeted the defense, aerospace, government, and other sectors in the United States, Israel, Australia, Russia, and India. In at least one case, the cyber actors tried to monetize their 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.

Questions

1. **Who conducted Operation Dream Job?**

   For the first question we will go to the MITRE campaign page to find information about the operation https://attack.mitre.org/campaigns/C0022/



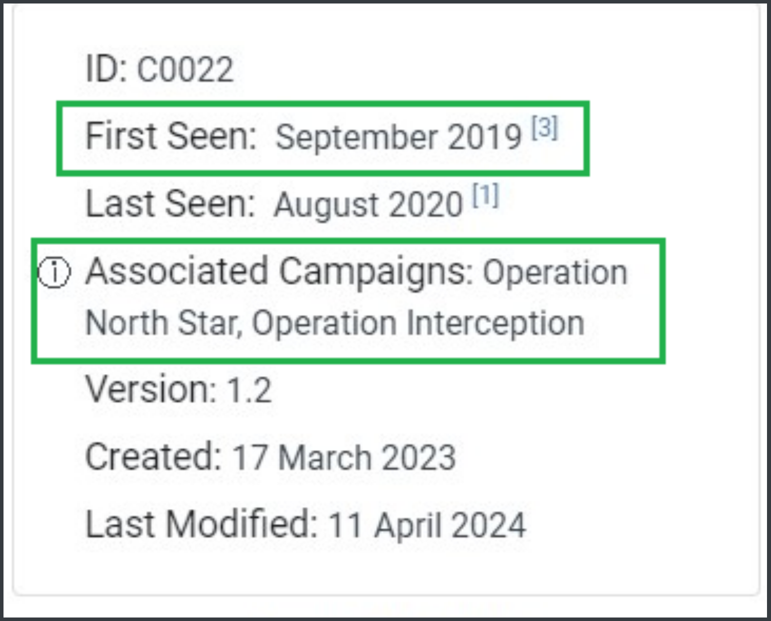
Operation Dream Job

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

Answer: `Lazarus Group`

2. **When was this operation first observed?**

   On the right side of the same page you will see a block which contains the operation id, first seen and last seen along with associated campaigns.



ID: C0022

First Seen: September 2019 [3]

Last Seen: August 2020 [1]

Associated Campaigns: Operation North Star, Operation Interception

Version: 1.2

Created: 17 March 2023

Last Modified: 11 April 2024

Answer: `September 2019`

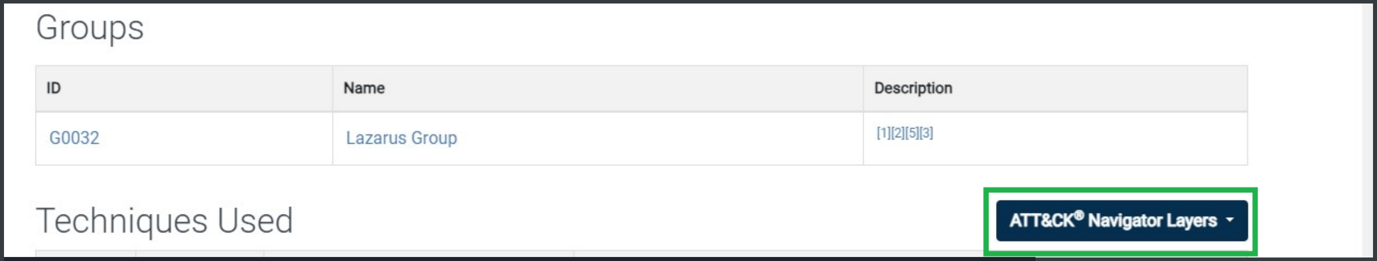
3. **There are 2 campaigns associated with Operation Dream Job. One is `Operation North Star`, what is the other?**

   Found in screenshot from Question #2.

   Answer: `Operation Interception`

4. **During Operation Dream Job, there were the two system binaries used for proxy execution. One was `regsvr32`, what was the other?**

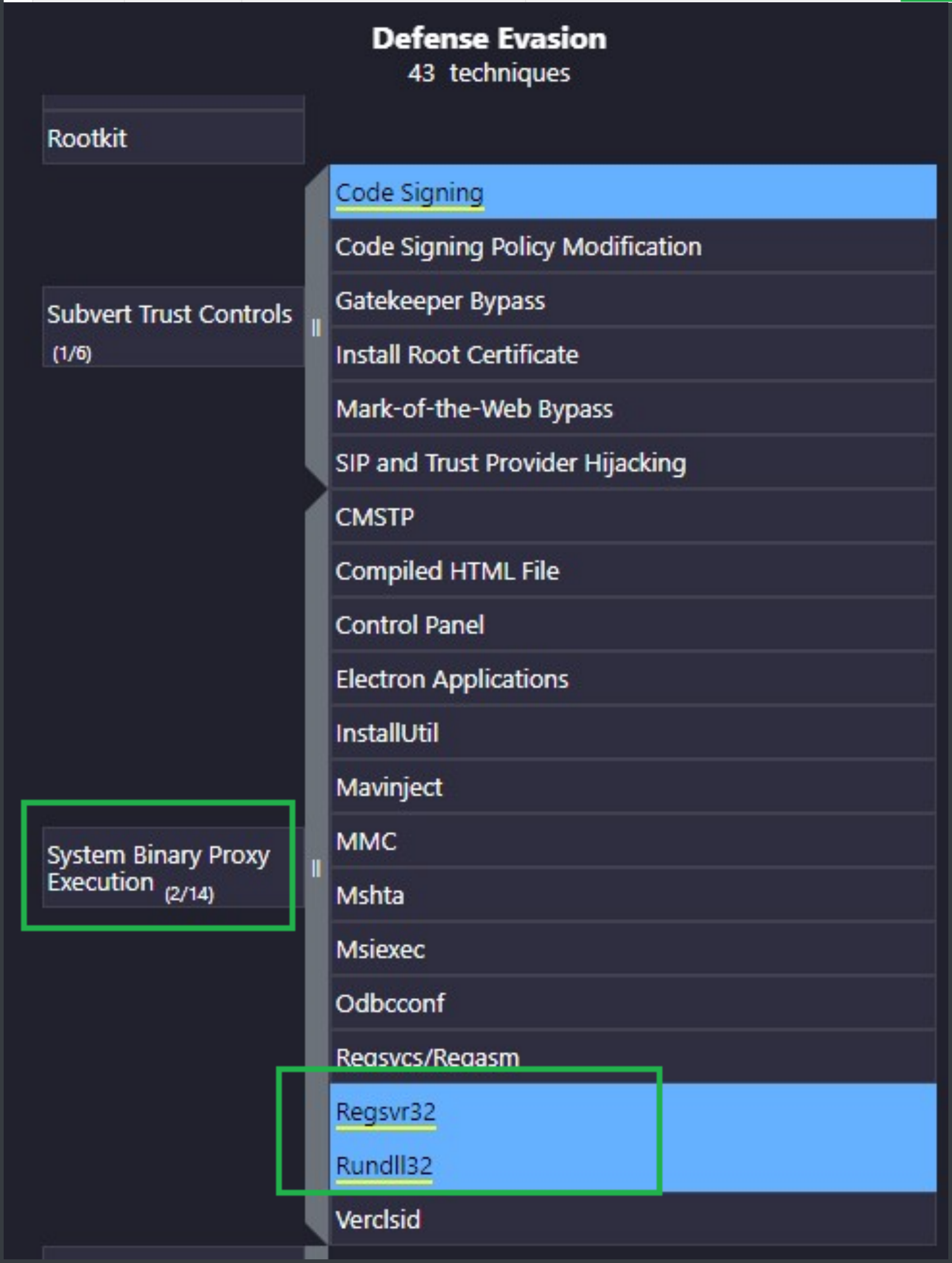
   For this we will look into the **MITRE ATT&CK** navigate layer present on the same page. In Navigate layer we will look for **Defense Evasion technique** there we will find **System Binary Proxy Execution**.



Groups

ID	Name	Description
G0032	Lazarus Group	[1][2][5][3]

Techniques Used

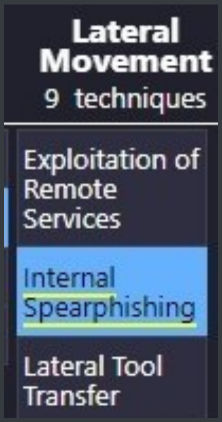


MITRE ATT&CK Navigator is a tool used to explore and visualize the MITRE ATT&CK framework. It helps you map out tactics, techniques, and procedures (TTPs) used by cyber adversaries, making it easier to analyze and plan defenses against cyber threats.

Answer: `Rundll32`

5. **What lateral movement technique did the adversary use?**

   In the Navigate layer go to Lateral Movement technique. Put your cursor on the technique and you will see its ID

   Lateral Movement

   9 techniques

   Exploitation of Remote Services

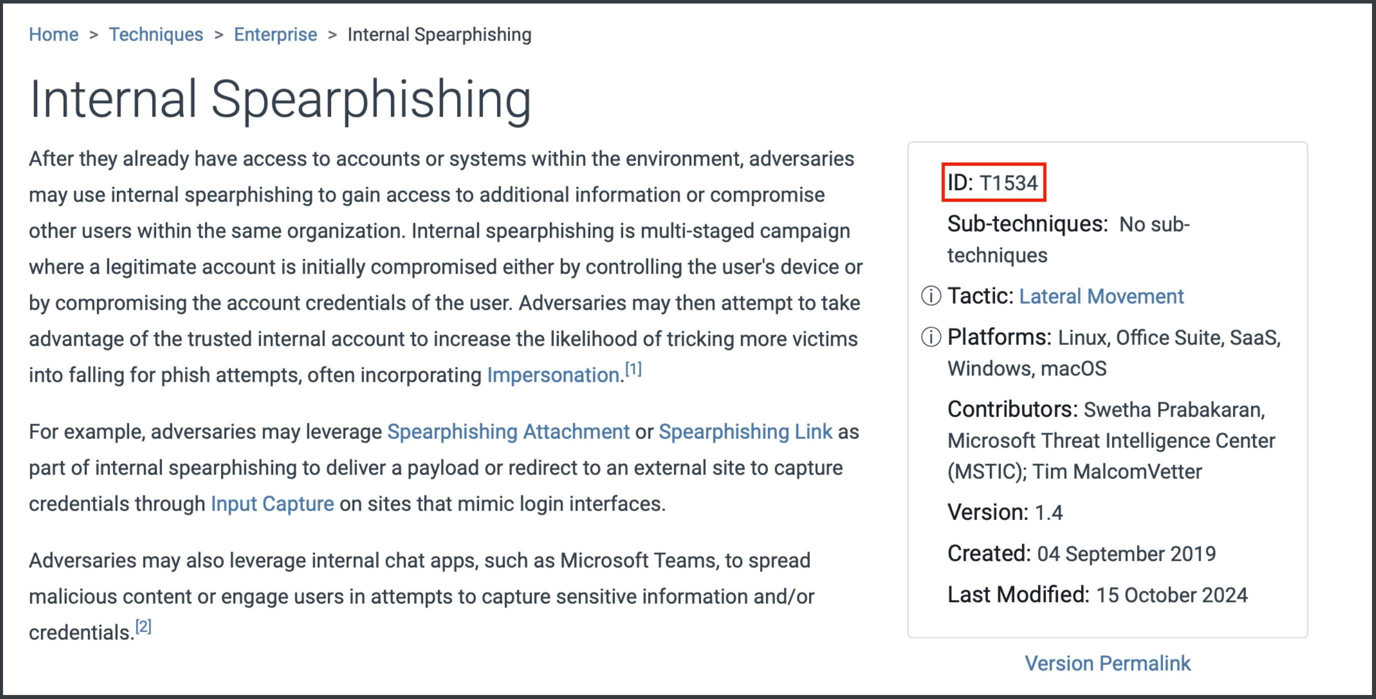
   Internal Spearphishing

   Lateral Tool Transfer

   MITRE uses technique IDs to identify specific methods that cyber attackers use. Each technique has a unique ID

   Answer: `Internal Spearphishing`

6. **What is the technique ID for the previous answer?**



Home > Techniques > Enterprise > Internal Spearphishing

Internal Spearphishing

After they already have access to accounts or systems within the environment, adversaries may use internal spearphishing to gain access to additional information or compromise other users within the same organization. Internal spearphishing is multi-staged campaign where a legitimate account is initially compromised either by controlling the user's device or by compromising the account credentials of the user. Adversaries may then attempt to take advantage of the trusted internal account to increase the likelihood of tricking more victims into falling for phish attempts, often incorporating Impersonation.[1]

For example, adversaries may leverage Spearphishing Attachment or Spearphishing Link as part of internal spearphishing to deliver a payload or redirect to an external site to capture credentials through Input Capture on sites that mimic login interfaces.

Adversaries may also leverage internal chat apps, such as Microsoft Teams, to spread malicious content or engage users in attempts to capture sensitive information and/or credentials.[2]

ID: T1534

Sub-techniques: No sub-techniques

ⓘ Tactic: Lateral Movement

ⓘ Platforms: Linux, Office Suite, SaaS, Windows, macOS

Contributors: Swetha Prabakaran, Microsoft Threat Intelligence Center (MSTIC); Tim MalcomVetter

Version: 1.4

Created: 04 September 2019

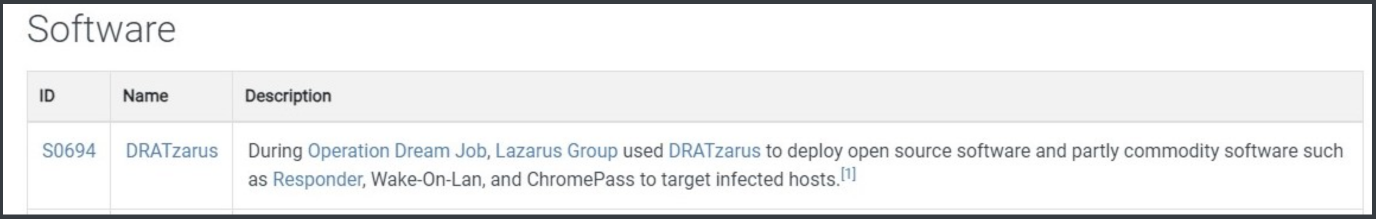
Last Modified: 15 October 2024

Version Permalink

Answer: `T1534`

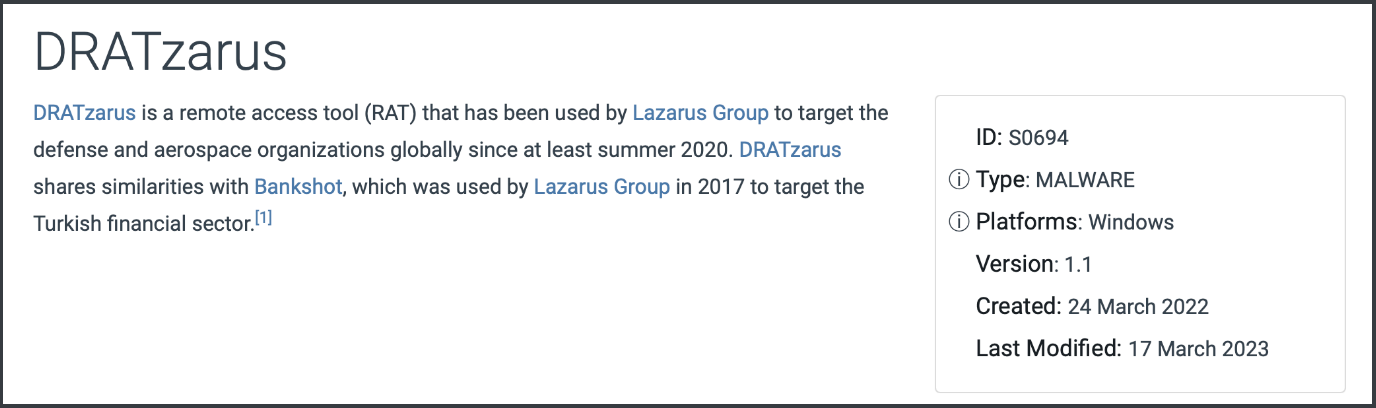
7. **What Remote Access Tool did the Lazarus Group use in Operation Dream Job?**

In the MITRE page scroll down to the **Software** section.



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]



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]

ID: S0694

ⓘ Type: MALWARE

ⓘ Platforms: Windows

Version: 1.1

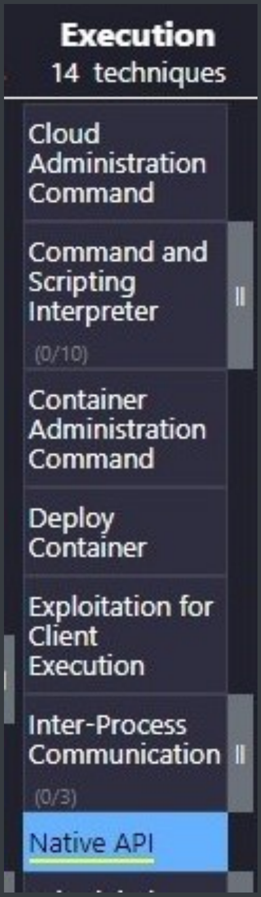
Created: 24 March 2022

Last Modified: 17 March 2023

Answer: `DRATzarus`

8. **What technique did the malware use for execution?**

   Click on `DRATzarus` and go to its ATT&CK navigate layer. You will find the answer under the **Execution** Technique



Execution
14 techniques

Cloud Administration Command

Command and Scripting Interpreter
(0/10)

Container Administration Command

Deploy Container

Exploitation for Client Execution

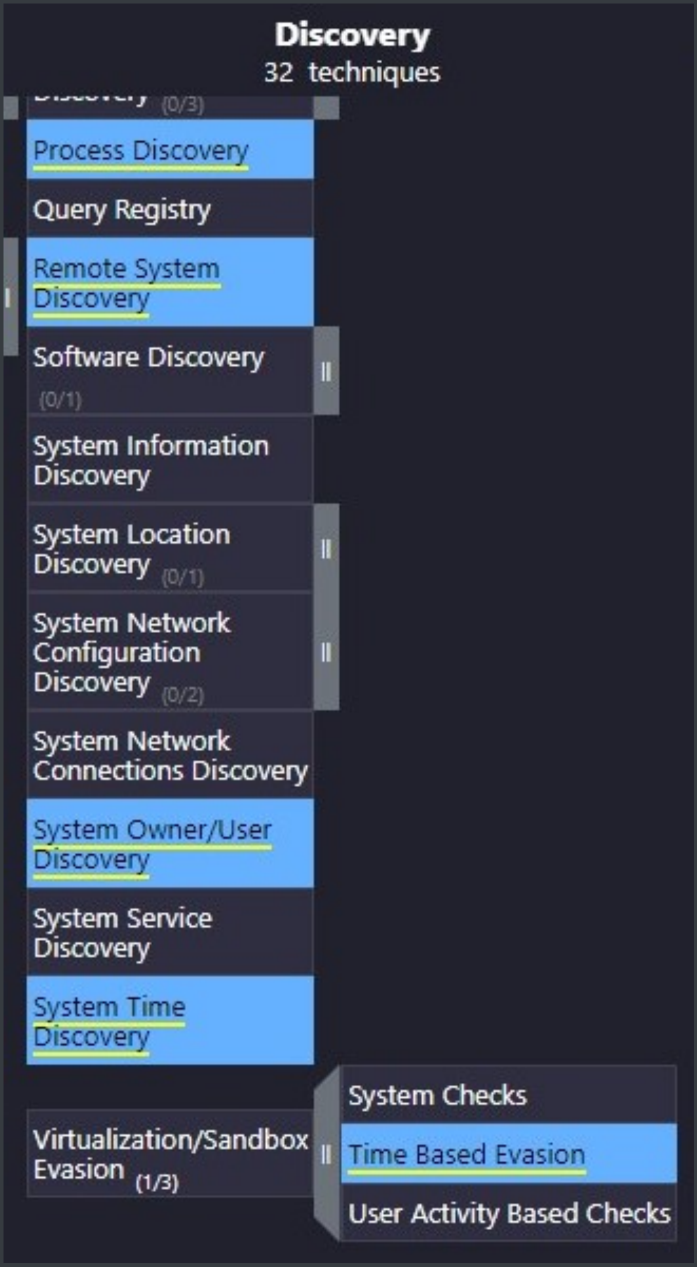
Inter-Process Communication
(0/3)

Native API

Answer: `Native API`

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

   In the navigate layer look under the **Discovery** Technique, the answer is in the **Virtualization/Sandbox** Evasion section.



Discovery
32 techniques

Discovery (0/3)

Process Discovery

Query Registry

Remote System Discovery

Software Discovery (0/1)

System Information Discovery

System Location Discovery (0/1)

System Network Configuration Discovery (0/2)

System Network Connections Discovery

System Owner/User Discovery

System Service Discovery

System Time Discovery

Virtualization/Sandbox Evasion (1/3)

System Checks

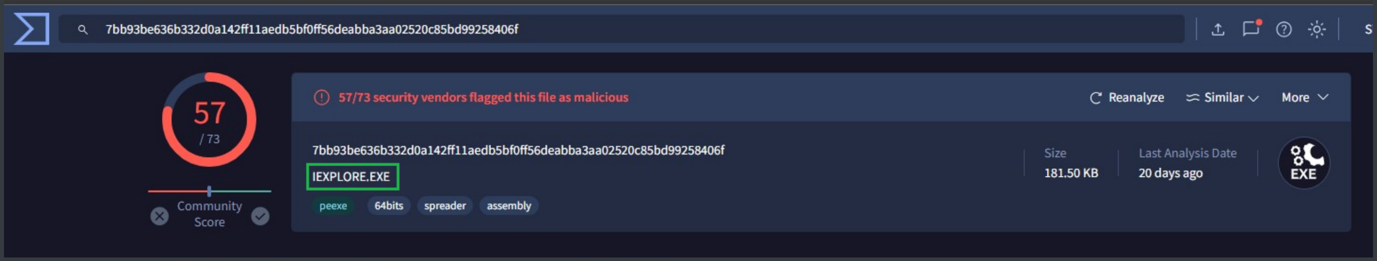
Time Based Evasion

User Activity Based Checks

Answer: `Time Based Evasion`

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?**

    For this we will copy the hash from the file and look it up on VirusTotal.



7bb93be636b332d0a142ff11aedb5bf0ff56deabba3aa02520c85bd99258406f

57 / 73

Community Score

57/73 security vendors flagged this file as malicious

7bb93be636b332d0a142ff11aedb5bf0ff56deabba3aa02520c85bd99258406f

IEXPLORE.EXE

peexe 64bits spreader assembly

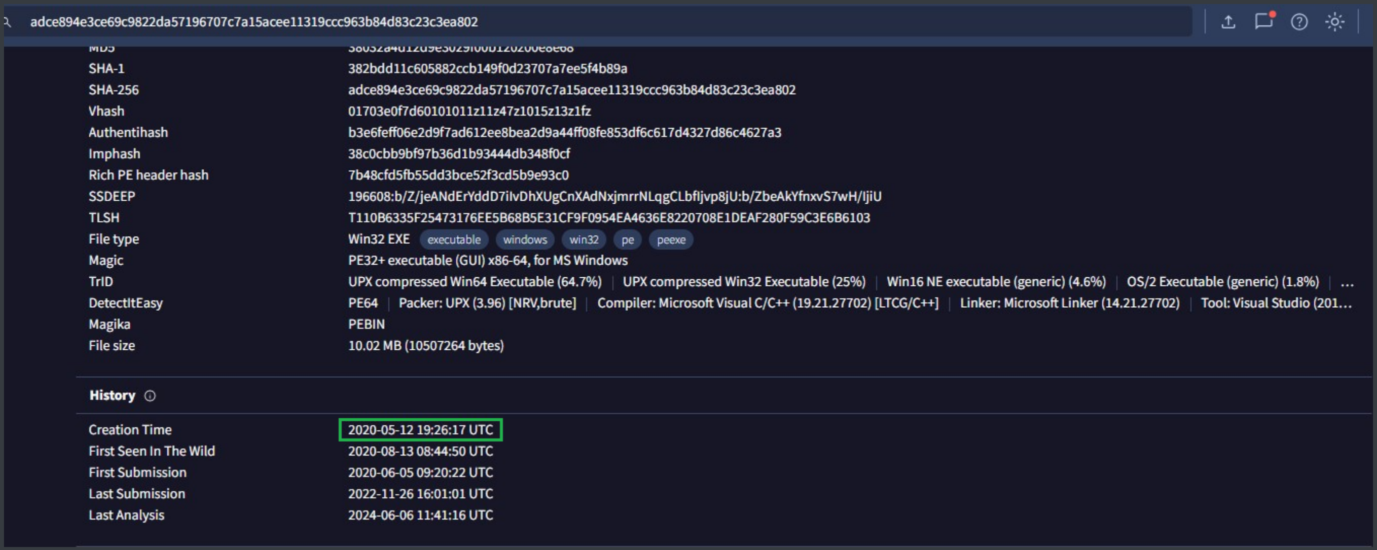
Size	Last Analysis Date
181.50 KB	20 days ago

VirusTotal is an online service that analyzes files and URLs for potential threats by scanning them with multiple antivirus engines. It helps users quickly identify malware, phishing sites, and other malicious content.

Answer: `IEXPLORE.exe`

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

    Same process we will search the hash on virus total. Look in the **Details** tab in the history section we will find our answer.



adce894e3ce69c9822da57196707c7a15acee11319ccc963b84d83c23c3ea802

MD5	
SHA-1	382bdd11c605882ccb149f0d23707a7ee5f4b89a
SHA-256	adce894e3ce69c9822da57196707c7a15acee11319ccc963b84d83c23c3ea802
Vhash	01703e0f7d60101011z11z47z1015z13z1fz
Authentihash	b3e6feff06e2d9f7ad612ee8bea2d9a44ff08fe853df6c617d4327d86c4627a3
Imphash	38c0cbb9bf97b36d1b93444db348f0cf
Rich PE header hash	7b48cfd5fb55dd3bce52f3cd5b9e93c0
SSDEEP	196608:b/Z/jeANdErYddD7ilvDhXUgCnXAdNxjmrrNLqgCLbfljvp8jU:b/ZbeAkYfnxvS7wH/IjiU
TLSH	T110B6335F25473176EE5B68B5E31CF9F0954EA4636E8220708E1DEAF280F59C3E6B6103
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (GUI) x86-64, for MS Windows
TrID	UPX compressed Win64 Executable (64.7%) | UPX compressed Win32 Executable (25%) | Win16 NE executable (generic) (4.6%) | OS/2 Executable (generic) (1.8%) | ...
DetectItEasy	PE64 | Packer: UPX (3.96) [NRV,brute] | Compiler: Microsoft Visual C/C++ (19.21.27702) [LTCG/C++] | Linker: Microsoft Linker (14.21.27702) | Tool: Visual Studio (201...
Magika	PEBIN
File size	10.02 MB (10507264 bytes)

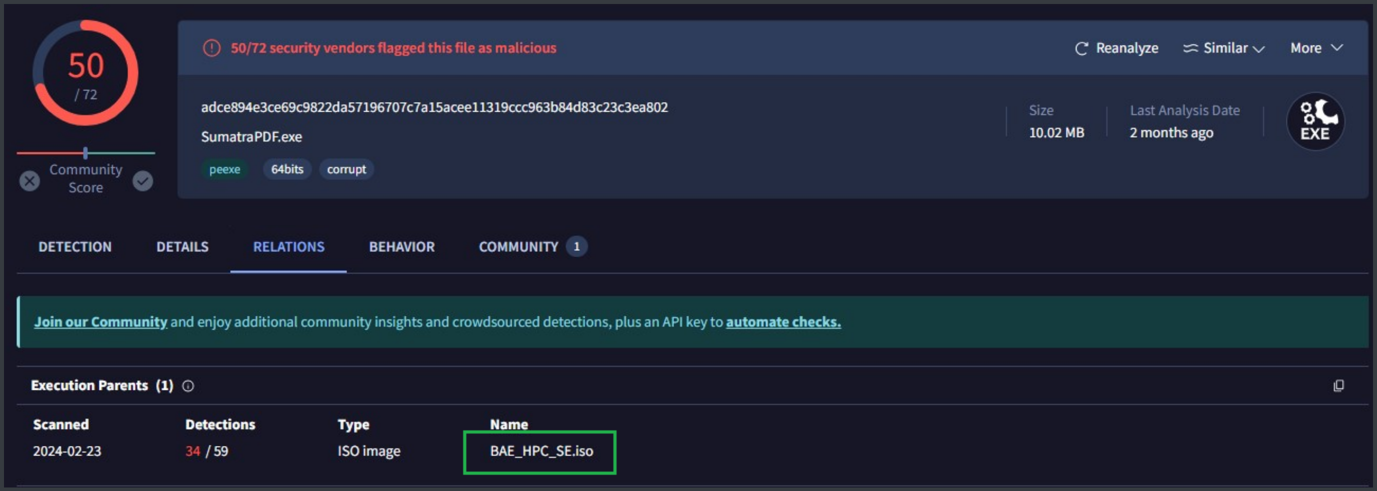
History

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	2024-06-06 11:41:16 UTC

Answer: `2020-05-12 19:26:17`

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

    Again same process search the hash in VirusTotal, this time look in the `Relations` tab under the `Execution Parent` section we will find our answer.

    50/72 security vendors flagged this file as malicious

    adce894e3ce69c9822da57196707c7a15acee11319ccc963b84d83c23c3ea802
    SumatraPDF.exe
    peexe 64bits corrupt

    Size 10.02 MB
    Last Analysis Date 2 months ago

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

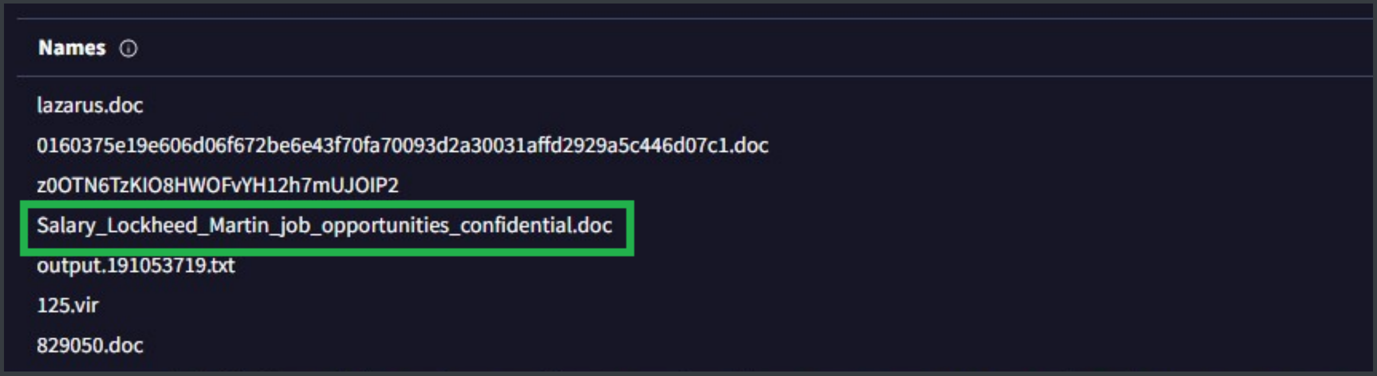
    Execution Parents (1)

Scanned	Detections	Type	Name
2024-02-23	34 / 59	ISO image	BAE_HPC_SE.iso

    Answer: `BAE_HPC_SE.iso`

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

    We will find this answer in the **Details** tab under the **Names** section. As we know, the victims of this operation were job seekers so the most appropriate answer would be.

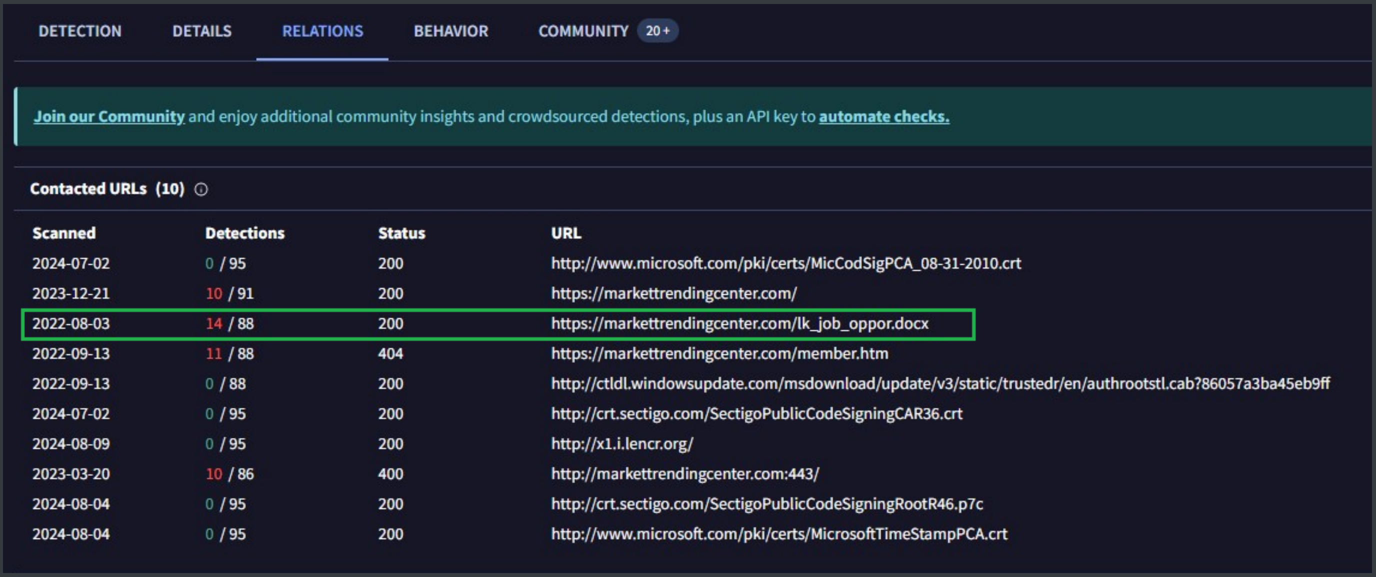
    Names

    lazarus.doc
    0160375e19e606d06f672be6e43f70fa70093d2a30031affd2929a5c446d07c1.doc
    z0OTN6TzKIO8HWOFvYH12h7mUJOIP2
    Salary_Lockheed_Martin_job_opportunities_confidential.doc
    output.191053719.txt
    125.vir
    829050.doc

Answer: `Salary_Lockheed_Martin_job_opportunities_confidential.doc`

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

Again, utilizing VirusTotal we will find the answer in the `Relations` tab under **Contacted URLs** section.



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

Contacted URLs (10)

Scanned	Detections	Status	URL
2024-07-02	0 / 95	200	http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
2023-12-21	10 / 91	200	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
2024-07-02	0 / 95	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2024-08-09	0 / 95	200	http://x1.i.lencr.org/
2023-03-20	10 / 86	400	http://markettrendingcenter.com:443/
2024-08-04	0 / 95	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c
2024-08-04	0 / 95	200	http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt

Answer: `https://markettrendingcenter.com/lk_job_oppor.docx`