MALWARE-TRAFFIC-ANALYSIS.NET

2021-04-29 (THURSDAY) - TA551 (SHATHAK) PUSHES ICEDID (BOKBOT)

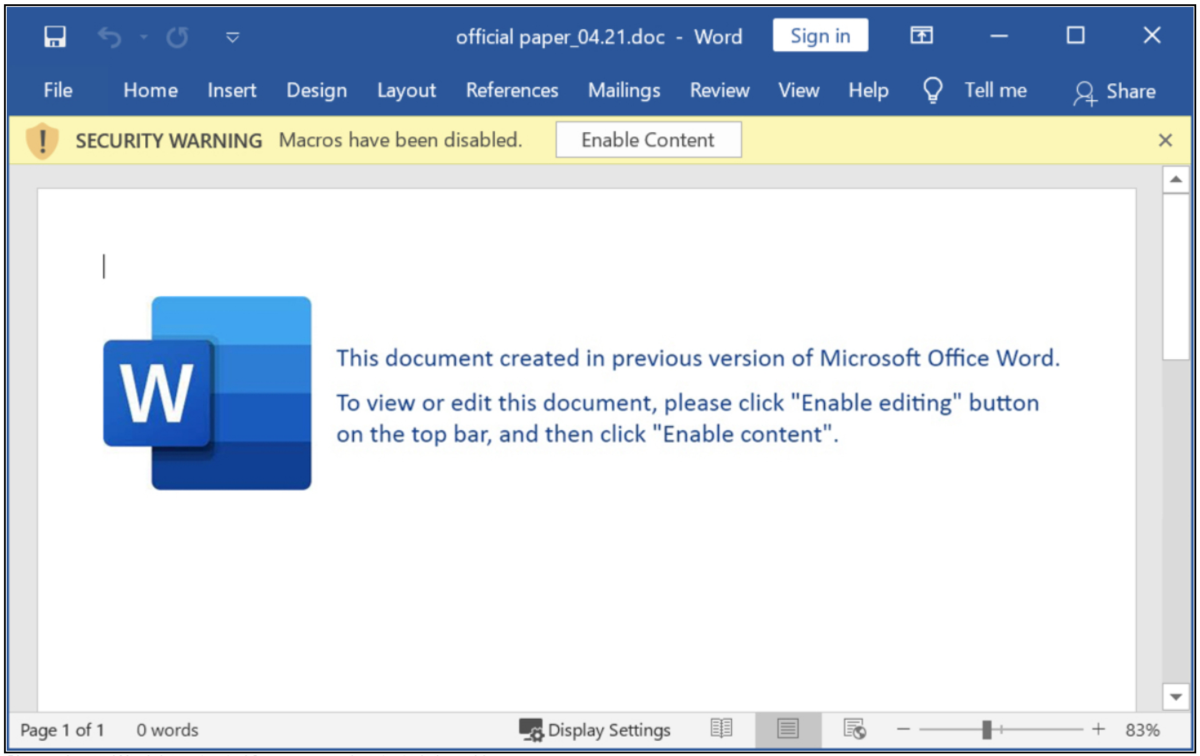
ASSOCIATED FILES:

- **2021-04-29-TA551-IcedID-IOCs.txt.zip** 2.0 kB (1,971 bytes)
- **2021-04-29-TA551-IcedID-infection-traffic.pcap.zip** 1.1 MB (1,081,098 bytes)
- **2021-04-29-TA551-IcedID-malware-and-artifacts.zip** 1.2 MB (1,205,559 bytes)

NOTES:

- All zip archives on this site are password-protected. If you don't know the password, see the "about" page of this website.

IMAGES

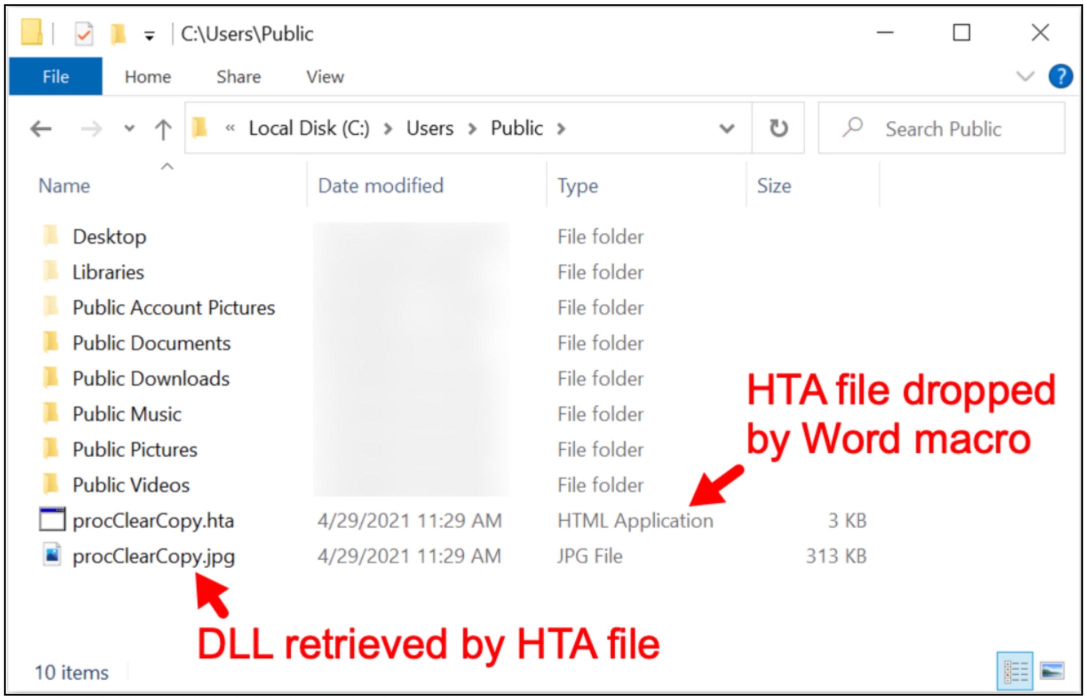


SECURITY WARNING Macros have been disabled.

This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content".

Shown above: Word doc extracted from password-protected zip archive.

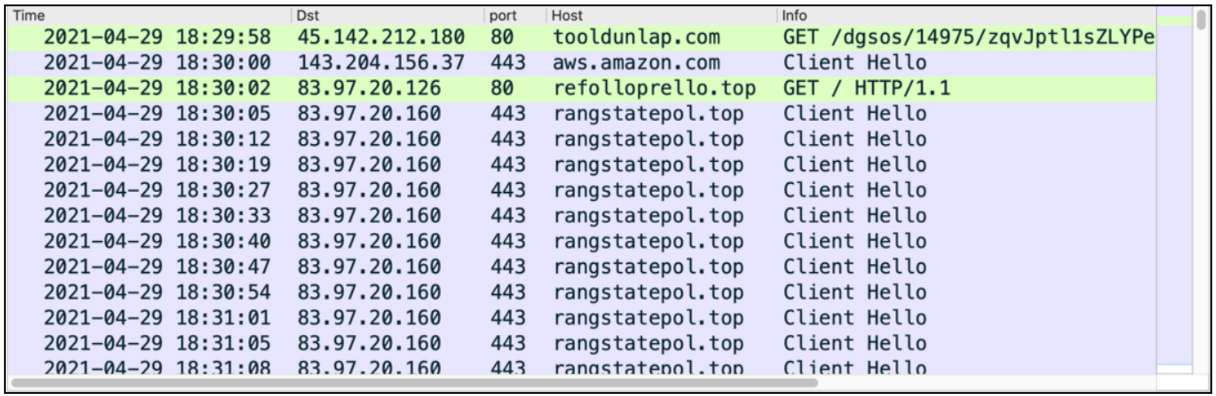


Name	Date modified	Type	Size
Desktop		File folder	
Libraries		File folder	
Public Account Pictures		File folder	
Public Documents		File folder	
Public Downloads		File folder	
Public Music		File folder	
Public Pictures		File folder	
Public Videos		File folder	
procClearCopy.hta	4/29/2021 11:29 AM	HTML Application	3 KB
procClearCopy.jpg	4/29/2021 11:29 AM	JPG File	313 KB

HTA file dropped by Word macro

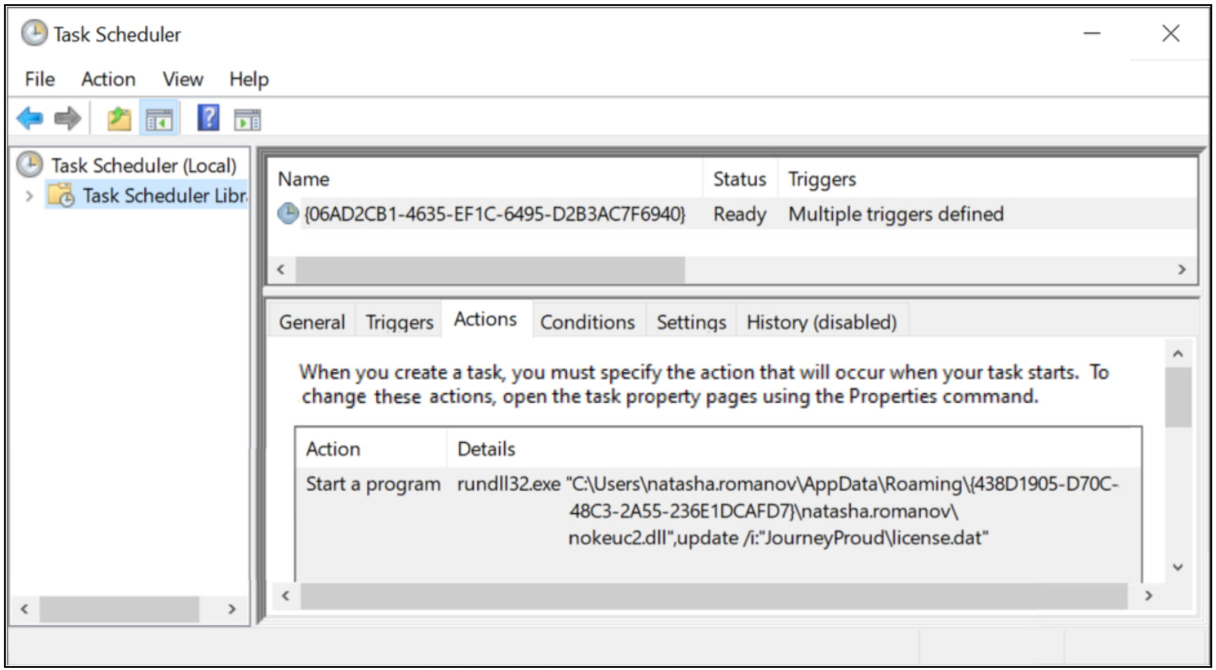
DLL retrieved by HTA file

Shown above: Artifacts seen after enabling macros on the Word doc.



```
Time                 Dst             port  Host               Info
2021-04-29 18:29:58  45.142.212.180  80    tooldunlap.com     GET /dgsos/14975/zqvJptl1sZLYPe
2021-04-29 18:30:00  143.204.156.37  443   aws.amazon.com     Client Hello
2021-04-29 18:30:02  83.97.20.126    80    refolloprello.top  GET / HTTP/1.1
2021-04-29 18:30:05  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:30:12  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:30:19  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:30:27  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:30:33  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:30:40  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:30:47  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:30:54  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:31:01  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:31:05  83.97.20.160    443   rangstatepol.top   Client Hello
2021-04-29 18:31:08  83.97.20.160    443   rangstatepol.top   Client Hello
```

Shown above: Traffic from the infection filtered in Wireshark.



Name	Status	Triggers
{06AD2CB1-4635-EF1C-6495-D2B3AC7F6940}	Ready	Multiple triggers defined

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	rundll32.exe "C:\Users\natasha.romanov\AppData\Roaming\{438D1905-D70C-48C3-2A55-236E1DCAFD7}\natasha.romanov\nokeuc2.dll",update /i:"JourneyProud\license.dat"

Shown above: Scheduled task to keep IcedID malware persistent on the infected Windows host.

Click here to return to the main page.