Internet Storm Center

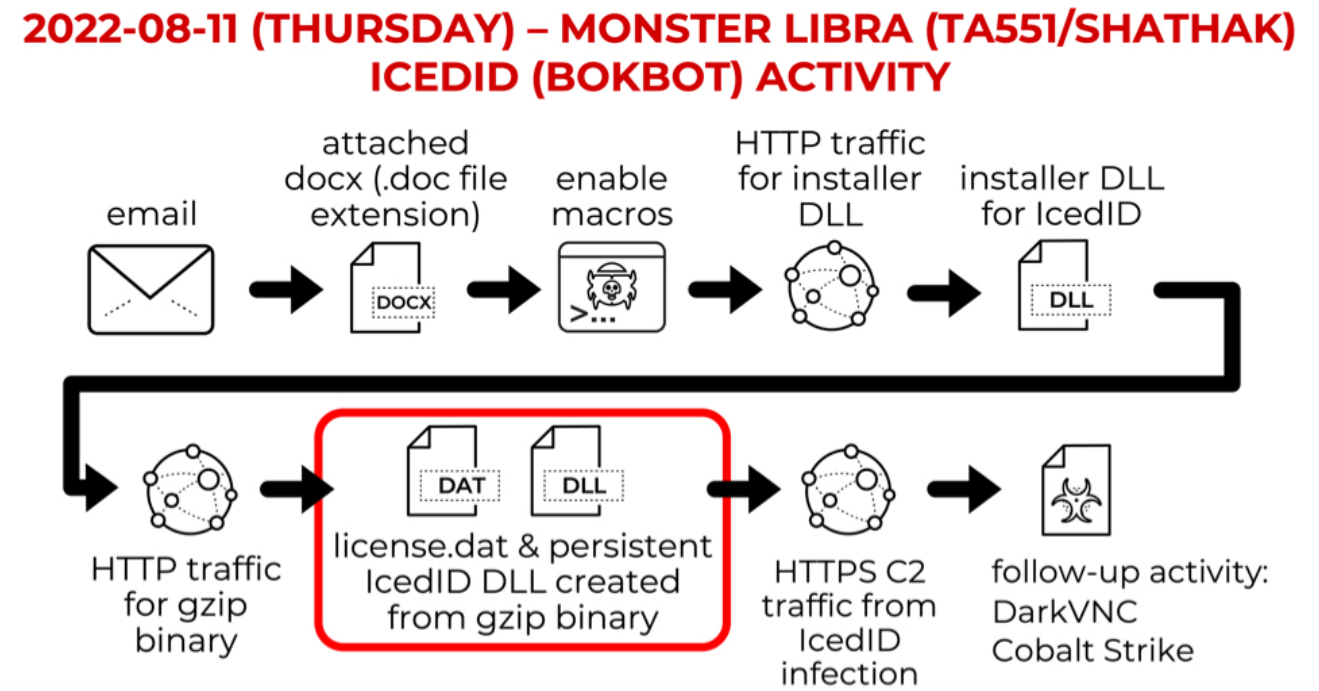
isc.sans.edu/diary/rss/28934

Monster Libra (TA551/Shathak) pushes IcedID (Bokbot) with Dark VNC and Cobalt Strike

Published: 2022-08-12
Last Updated: 2022-08-12 00:52:37 UTC
by Brad Duncan (Version: 1)
0 comment(s)

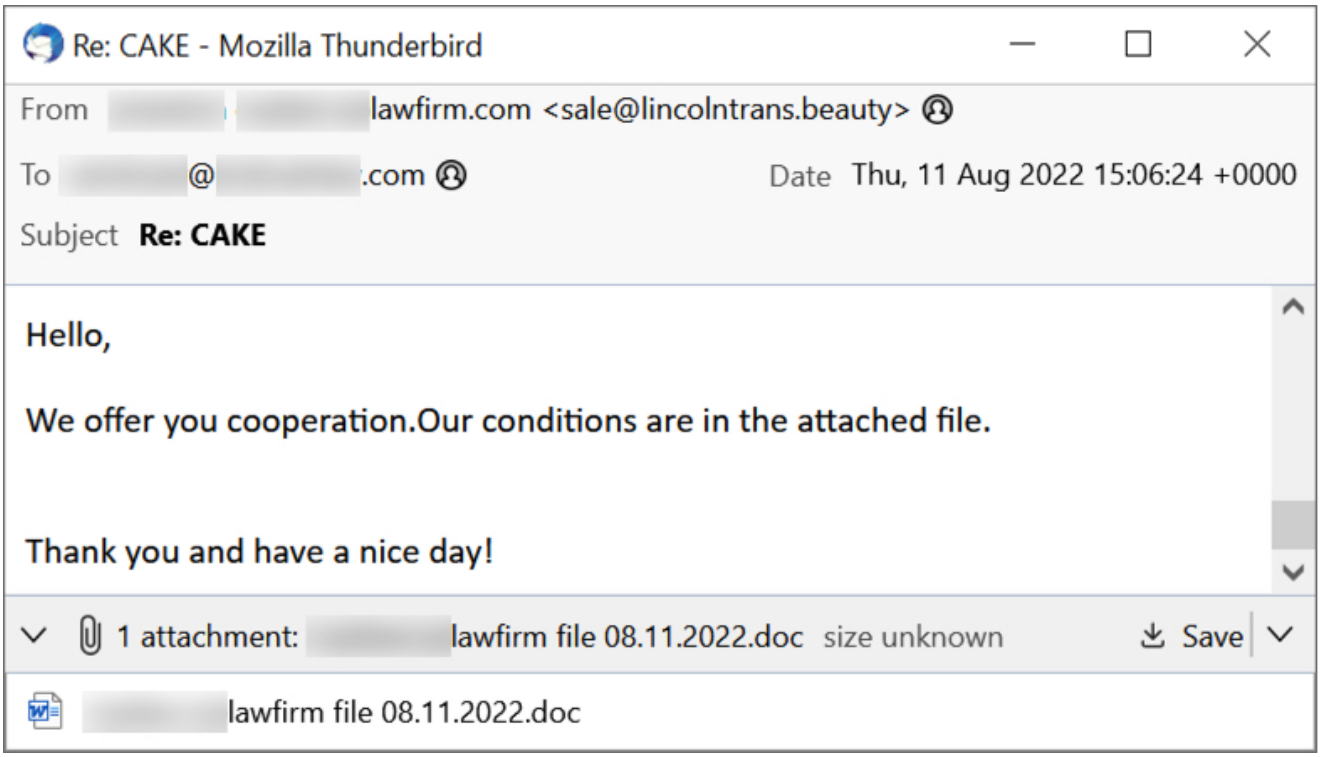
Introduction

Since 2019, threat actor Monster Libra (also known as TA551 or Shathak) has pushed different families of malware. During the past few months, Monster Libra has primarily pushed SVCready or IcedID. Today's diary reviews an example of Monster Libra pushing IcedID on Thursday 2022-08-11, and that IcedID infection led to Dark VNC activity and Cobalt Strike.

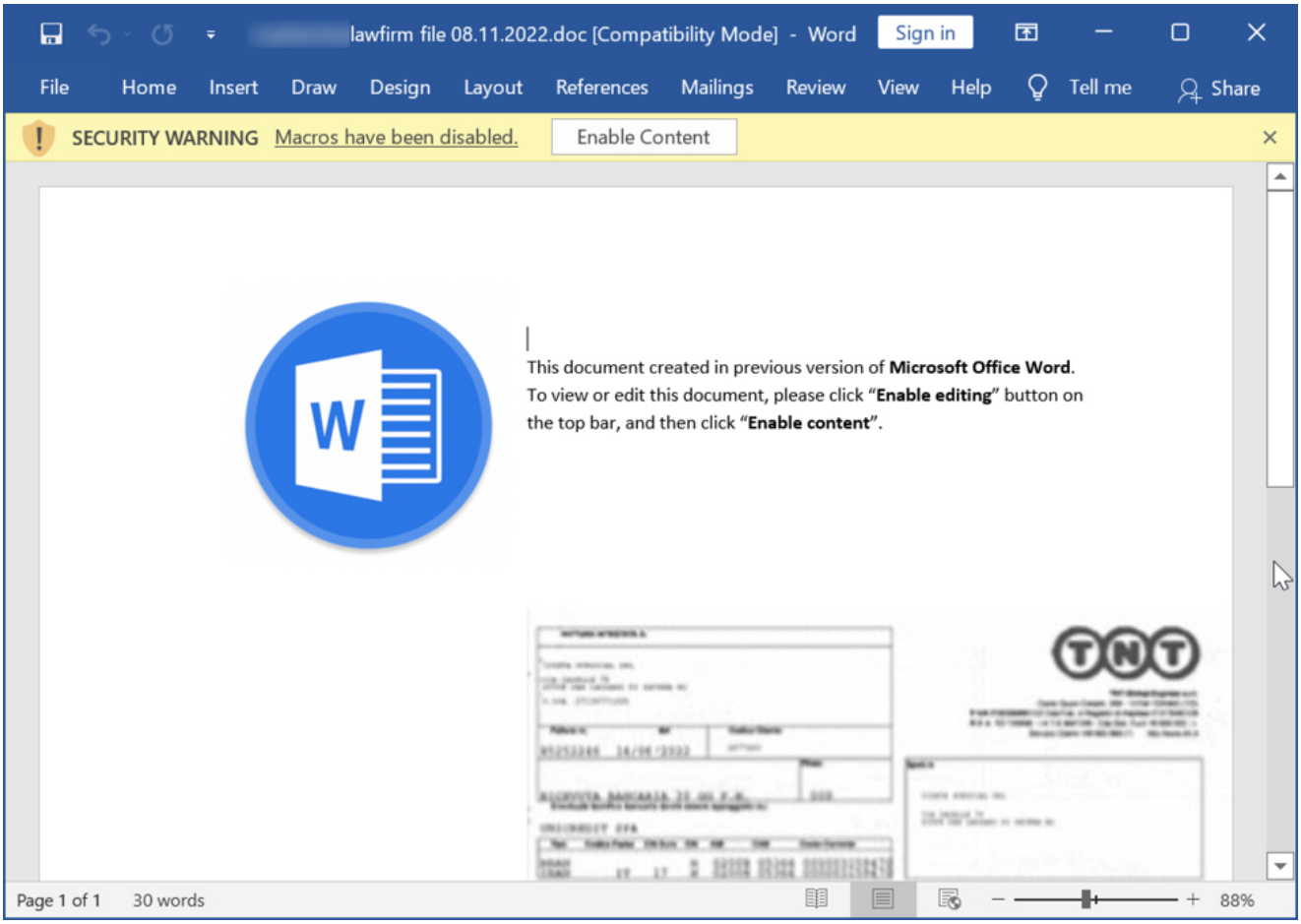


Shown above: Chain of events for IcedID infection distributed through Monster Libra.

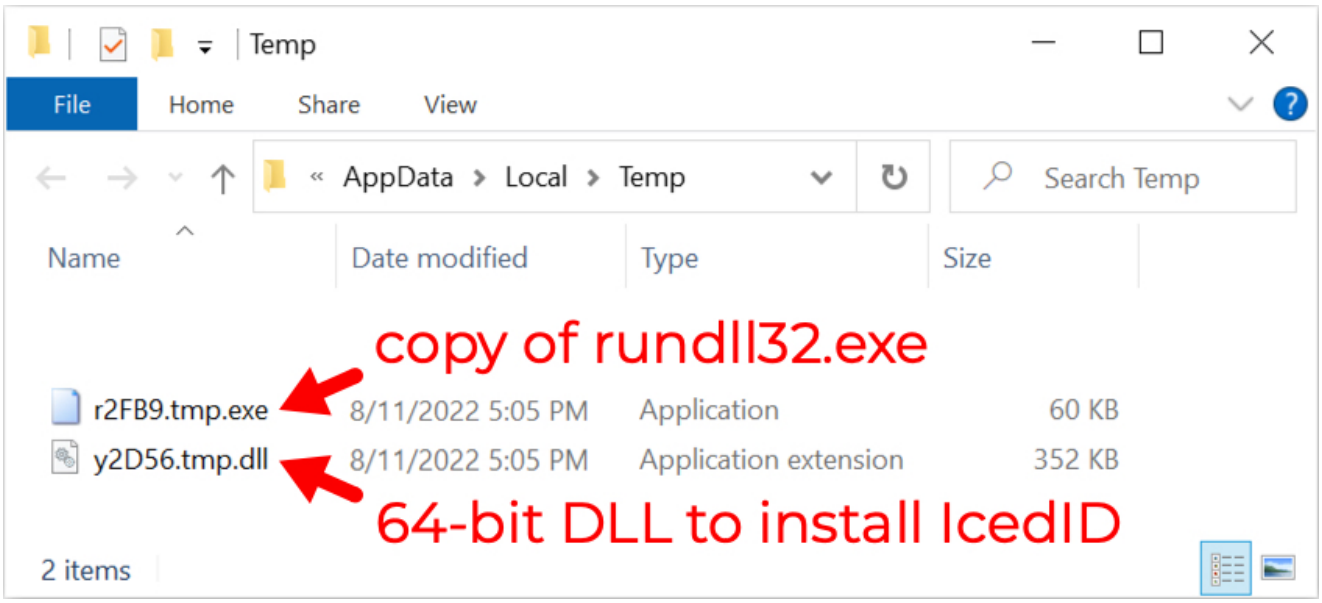
Images From the Infection



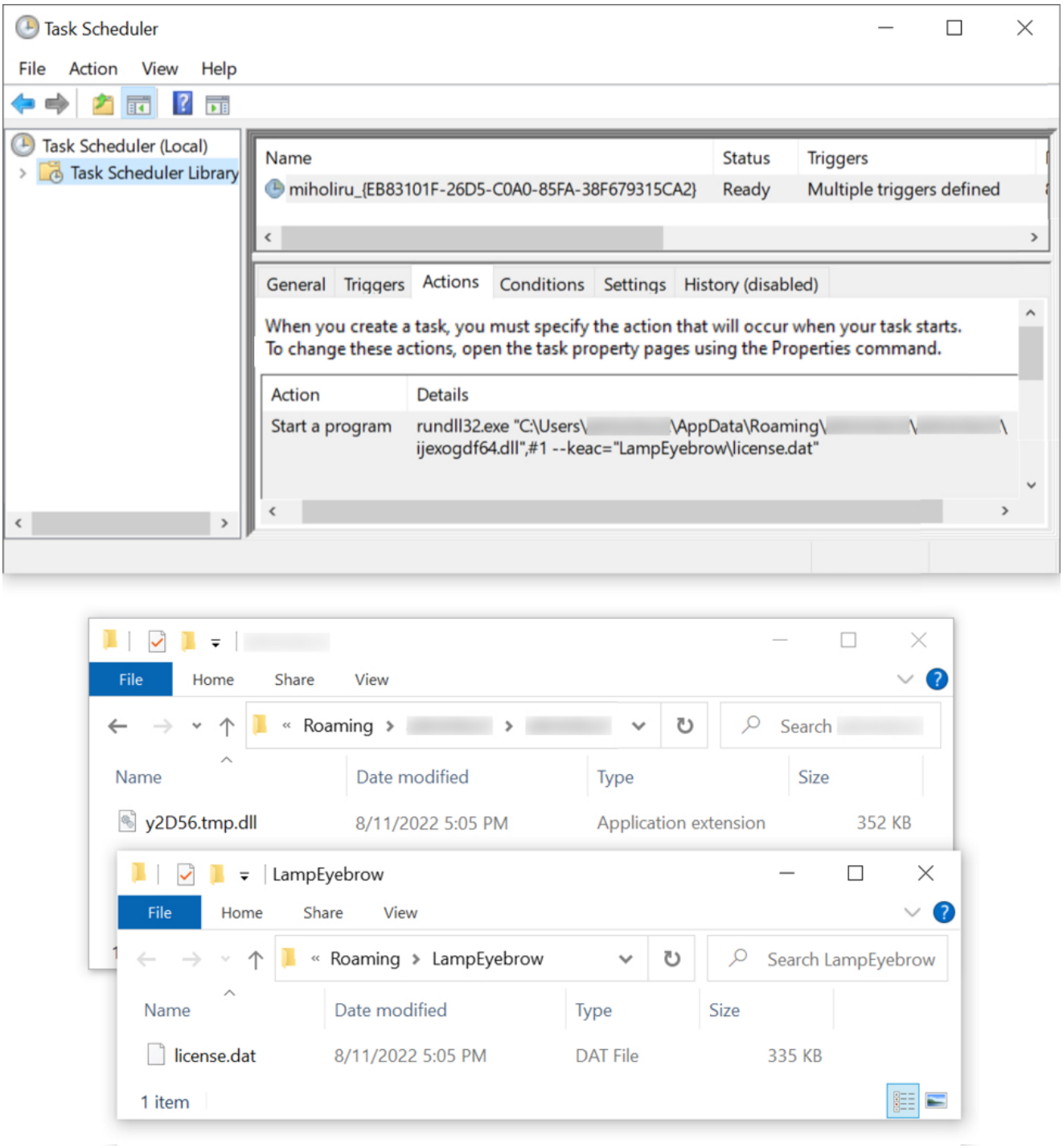
Shown above: Screenshot of a Monster Libra email.



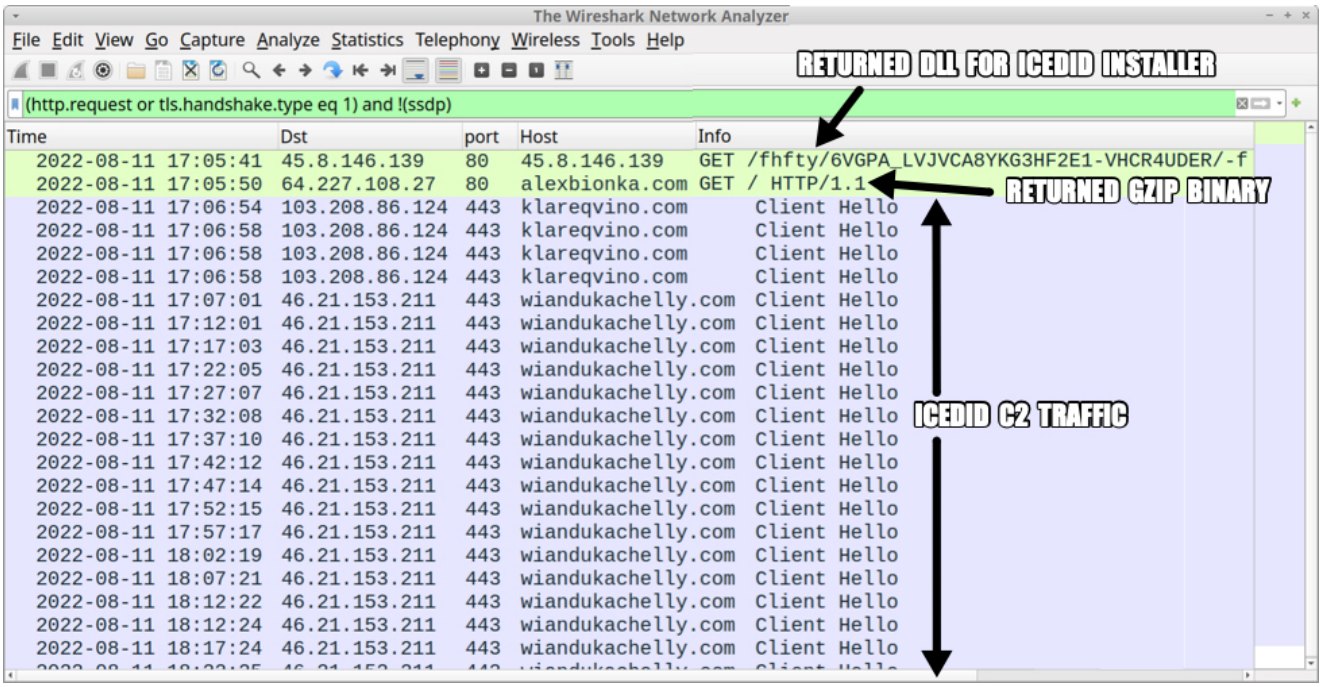
Shown above: Screenshot of the attached Word document.



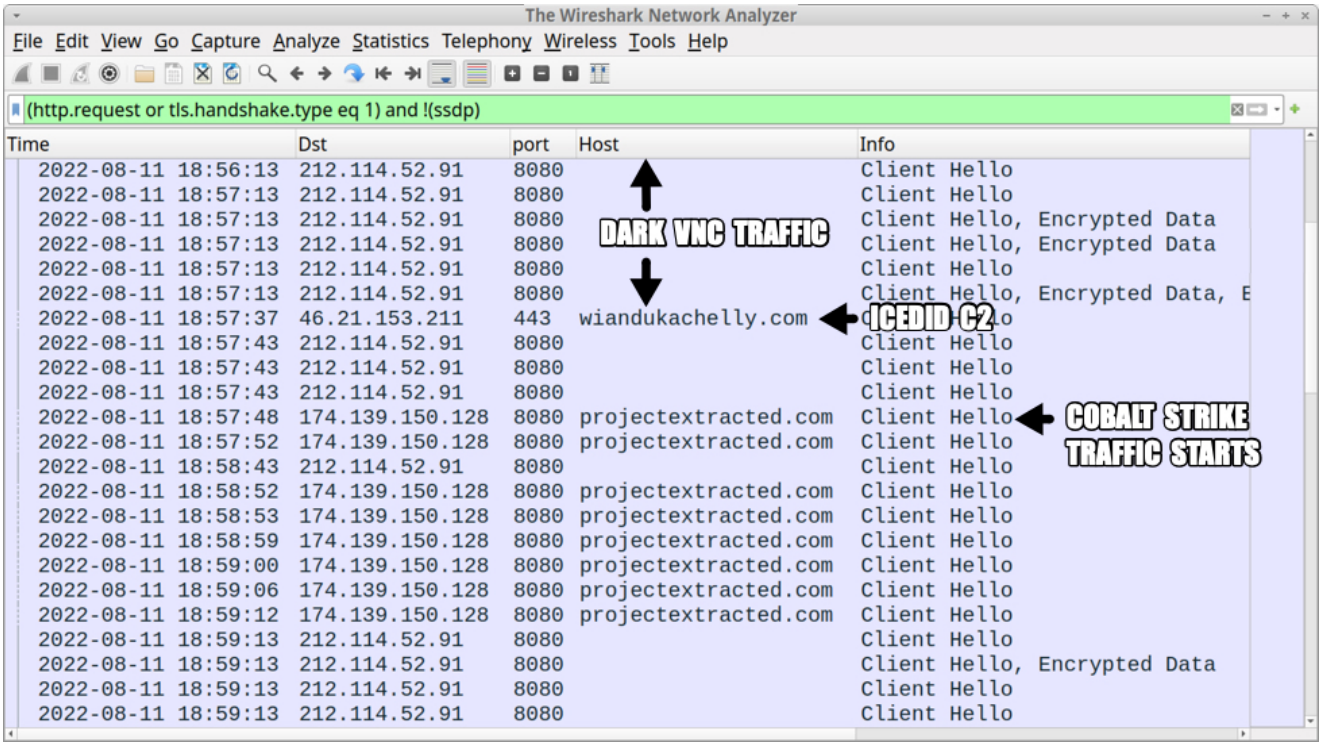
Shown above: Files that appeared after enabling macros



Shown above: Scheduled task for persistent IcedID infection.



Shown above: Traffic from an infection filtered in Wireshark (image 1 of 2).



Shown above: Traffic from an infection filtered in Wireshark (image 2 of 2).

Indicators of Compromise (IOCs)

20 Word docs found on VT:

- 2,316,894 bytes - *[name removed]* doc 08.11.2022.doc
- 2,343,230 bytes - *[name removed]* doc 08.11.2022.doc
- 2,349,822 bytes - *[name removed]* doc 08.11.doc
- 2,316,250 bytes - *[name removed]* file 08.11.2022.doc
- 2,365,937 bytes - *[name removed]* file 08.11.22.doc
- 2,298,962 bytes - *[name removed]* invoice 08.11.22.doc
- 2,343,139 bytes - *[name removed]*,doc,08.11.22.doc
- 2,365,983 bytes - *[name removed]*,document,08.11.22.doc
- 2,298,458 bytes - *[name removed]*,file,08.11.2022.doc
- 2,298,562 bytes - *[name removed]*,file,08.11.22.doc
- 2,297,841 bytes - *[name removed]*-doc-08.11.2022.doc
- 2,350,727 bytes - *[name removed]*-invoice-08.11.22.doc
- 2,315,700 bytes - *[name removed]*.doc.08.11.22.doc
- 2,316,502 bytes - *[name removed]*.document.08.11.2022.doc
- 2,316,883 bytes - *[name removed]*.document.08.11.2022.doc
- 2,316,402 bytes - *[name removed]*.invoice.08.11.2022.doc
- 2,351,271 bytes - *[name removed]*doc08.11.doc
- 2,366,716 bytes - *[name removed]*document08.11.22.doc
- 2,298,836 bytes - *[name removed]*document08.11.doc
- 2,349,614 bytes - *[name removed]*file08.11.22.doc

SHA256 hashes of the 20 Word docs:

Files from an infected Windows host:

SHA256 hash: 6cbe0e1f046b13b29bfa26f8b368281d2dda7eb9b718651d5856f22cc3e02910

- File size: 61,440 bytes
- File location: C:\Windows\SysWOW64\rundll32.exe
- File location: C:\Users*[username]*\AppData\Local\Temp\r2FB9.tmp.exe
- File description: Copy of legitimate Microsoft system file rundll32.exe. This is *not* inherently malicious.

SHA256 hash: 8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6

- File size: 360,448 bytes
- File location: hxxp://45.8.146[.]139/fhfty/6VGPA_LVJVCA8YKG3HF2E1-VHCR4UDER/-f
- File location: C:\Users*[username]*\AppData\Local\Temp\y2D56.tmp.dll
- File description: 64-bit DLL to install IcedID retrieved by Word macro
- Run method: rundll32.exe *[filename]*,#1

SHA256 hash: 5af2d2e245b36447fffff463b66164807f505dc9efcbe7fadfe4d450b1715c46

- File size: 688,572 bytes
- File location: hxxp://alexbionka[.]com/
- File description: gzip from alexbionka[.]com, used to create license.dat and persistent IcedID DLL

SHA256 hash: 1de8b101cf9f0fabc9f086bddb662c89d92c903c5db107910b3898537d4aa8e7

- File size: 342,218 bytes
- File name: C:\Users*[username]*AppData\Roaming\LampEyebrow\license.dat
- File description: Data binary used to run persistent IcedID DLL

SHA256 hash: d45c78fa400b32c11443061dcd1c286d971881ddf35a47143e4d426a3ec6bffd

- File size: 345,600 bytes
- File name: C:\Users*[username]*\AppData\Roaming*[username]**[username]*ijexogdf64.dll
- File description: Persistent 64-bit DLL for IcedID
- Run method: rundll32.exe *[filename]*,#1 --keac="*[path to license.dat]*"

Note: No binaries were saved to disk for DarkVNC or Cobalt Strike.

Traffic for IcedID installer DLL:

> hxxp://45.8.146[.]139/fhfty/6VGPA_LVJVCA8YKG3HF2E1-VHCR4UDER/-f

Traffic for gzip binary:

> 64.227.108[.]27:80 - ***alexbionka[.]com*** - GET / HTTP/1.1

IcedID C2 activity:

- 103.208.86[.]124:443 - ***klareqvino[.]com*** - HTTPS traffic
- 46.21.153[.]211:443 - ***wiandukachelly[.]com*** - HTTPS traffic
- 84.32.188[.]164:443 - ***ultomductingbig[.]pro*** - HTTPS traffic

DarkVNC activity:

> 212.114.52[.]91:8080 - encoded/encrypted TCP traffic

Cobalt Strike activity:

> 174.139.150[.]128:8080 - ***projectextracted[.]com*** - HTTPS traffic

Final Words

IcedID continues to be an active malware in our current threat landscape. Threat actors like Monster Libra continue to push IcedID through malspam-based campaigns as described in this diary. We expect to find more of this activity in the coming weeks.

Brad Duncan
brad [at] malwre-traffic-analysis.net
Keywords: Bokbot Cobalt Strike Dark VNC IcedID
0 comment(s)

Top of page
×

Diary Archives