Malware-Traffic-Analysis.net - 30 days of Formbook: Day 1, Monday 2023-06-05

NOTICE:

- Of note, the zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

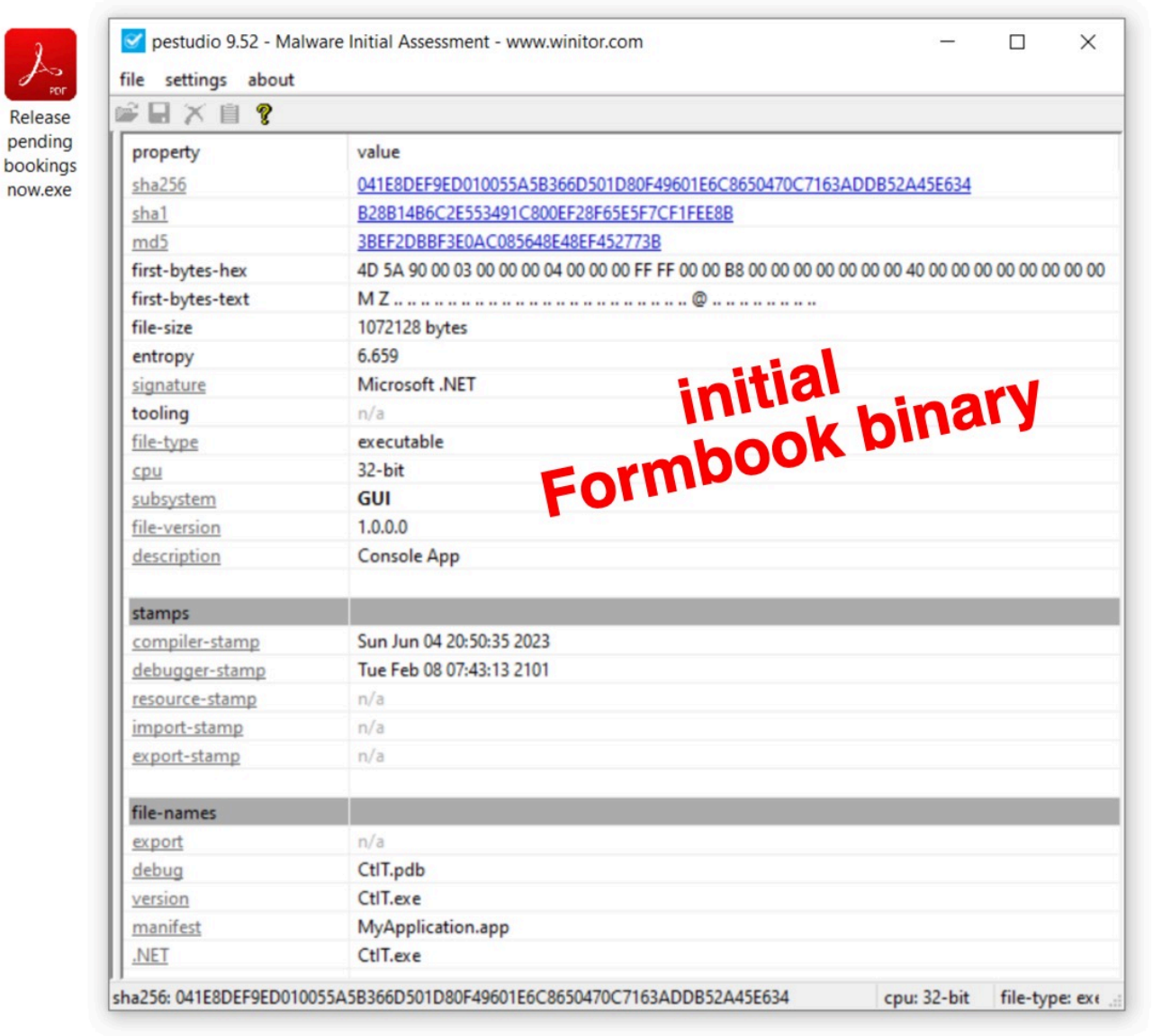
NOTES:

- I'm gathering data on Formbook, so I plan to generate infection runs on new Formbook samples 30 times during the next month or two.
- Today's sample is from a .rar archive submitted to VirusTotal on Sunday 2023-06-04.

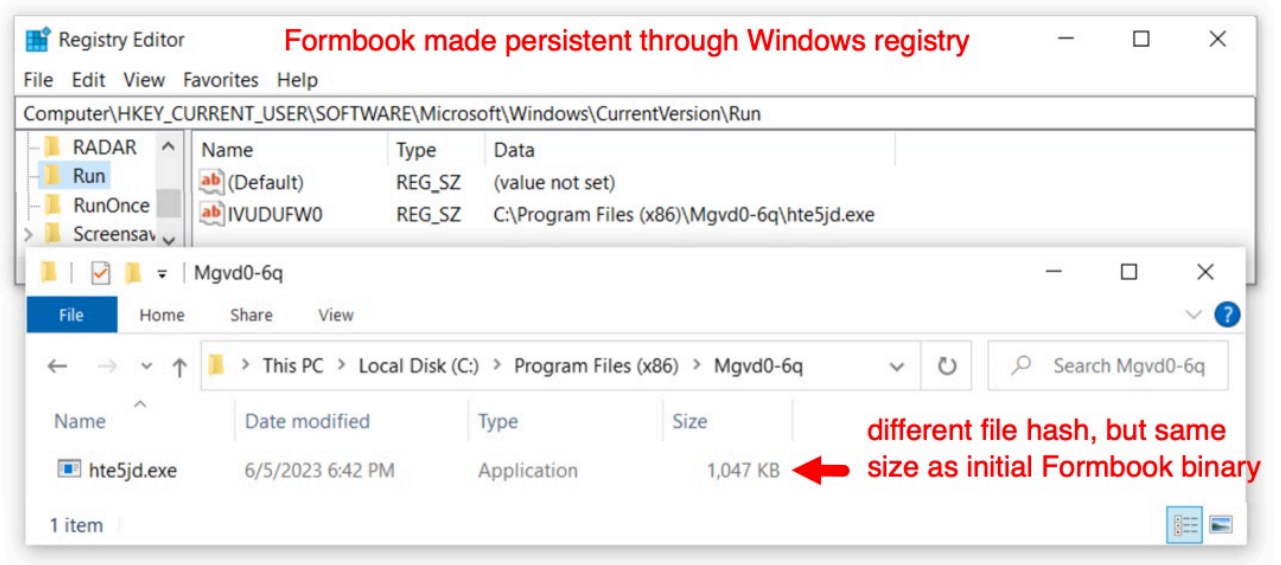
ASSOCIATED FILES:

- 2023-06-05-IOCs-for-Formbook-infection.txt.zip 2.5 kB (2,535 bytes)
- 2023-06-05-Formbook-infection.pcap.zip 3.9 MB (3,898,132 bytes)
- 2023-06-05-Formbook-malware-and-artifacts.zip 1.9 MB (1,919,919 bytes)

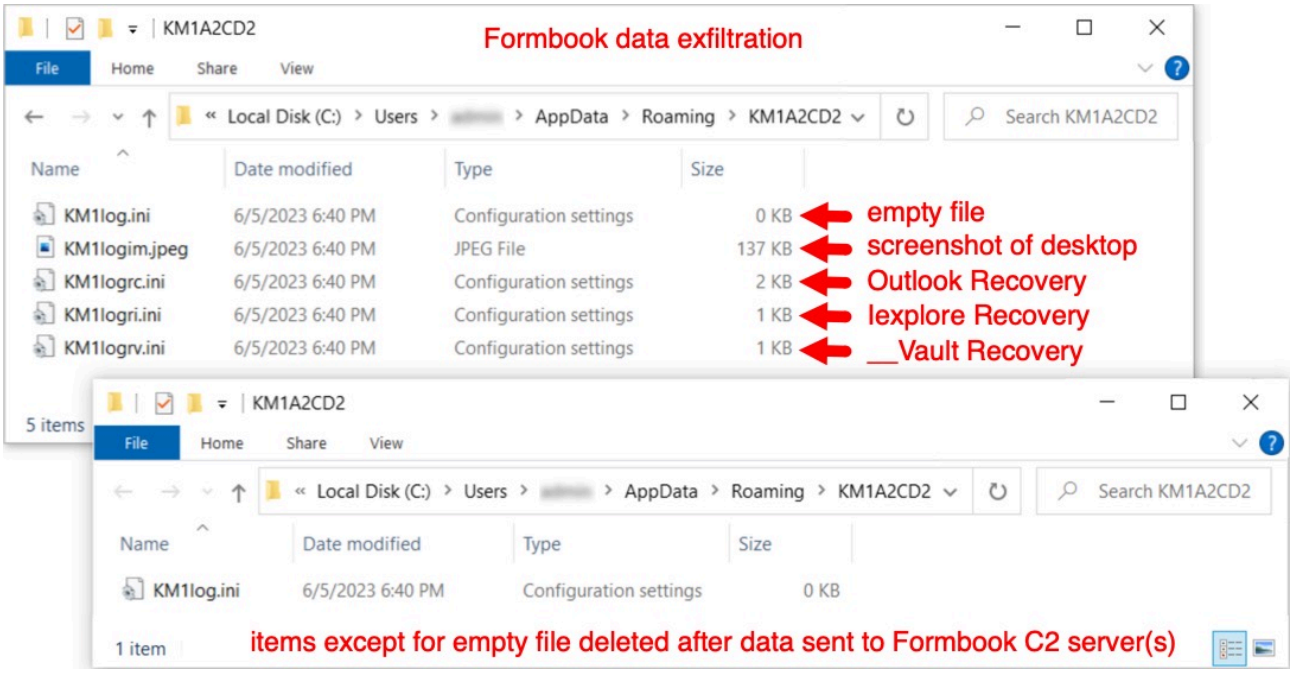
IMAGES



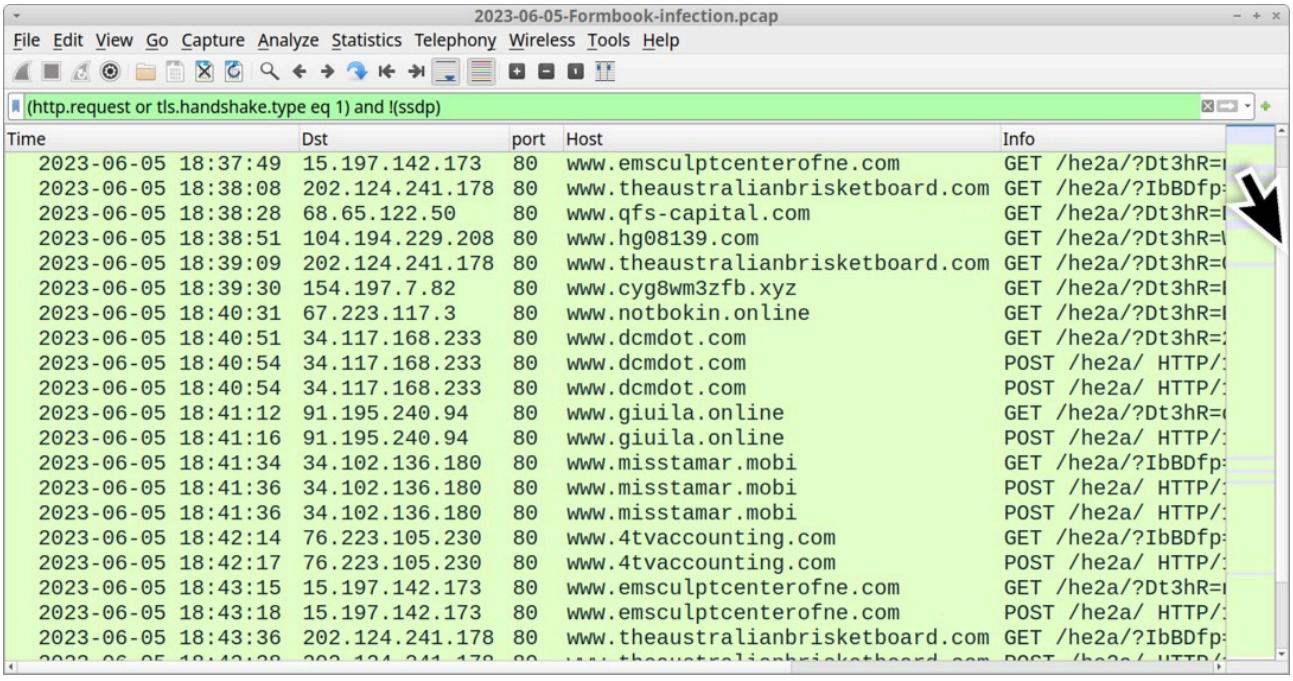
Shown above: Initial Formbook binary (Windows EXE file) submitted to VirusTotal.



Shown above: Formbook persistent on the infected Windows host.



Shown above: Stolen data temporarily stored to disk, which is deleted after data is accepted by a Formbook C2 server.



Shown above: Traffic from the infection filtered in Wireshark.

```
30 DAYS OF FORMBOOK: DAY 1, MONDAY 2023-06-05

INFECTION CHAIN:

- Unknown vector, possibly distributed as email attachment.

FORMBOOK SAMPLE:
```

- SHA256 hash: 4d86ca8f4deaffa4779027e6aa03ddd63b8b7b035e1344a609ea1fadbd1040bb
- File size: 620,684 bytes
- File name: Release_pending_bookings_now.rar
- File type: RAR archive data, v4, os: Win32
- File description: RAR archive containing Formbook EXE
- Earliest Contents Modification: 2023-06-04 21:50:35 UTC

- SHA256 hash: 041e8def9ed010055a5b366d501d80f49601e6c8650470c7163addb52a45e634
- File size: 1,072,128 bytes
- File name: Release pending bookings now.exe
- File type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
- File description: Formbook EXE with Adobe PDF-style icon
- Creation Time: 2023-06-04 20:50:35 UTC

- SHA256 hash: 5a48b39e1031dc42091ea074e632b3e8cc22a887b16c909b2dcd66490a8cf377
- File size: 1,072,128 bytes
- File location: C:\Program Files (x86)\Mgvd0-6q\hte5jd.exe
- File type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
- File description: Formbook from the above sample, persistent on the infected Windows host

FORMBOOK PERSISTENCE:

- Windows Registry key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Value name: IVUDUFW0
- Value type: REG_SZ
- Value Data: C:\Program Files (x86)\Mgvd0-6q\hte5jd.exe

DATA STORED FOR EXFILTRATION TO FORMBOOK C2 SERVER:

- C:\Users\[username]\AppData\Roaming\KM1A2CD2\KM1log.ini - 0 bytes
- C:\Users\[username]\AppData\Roaming\KM1A2CD2\KM1logim.jpeg - 137 kB (screenshot of desktop)
- C:\Users\[username]\AppData\Roaming\KM1A2CD2\KM1logrc.ini - 2 kB (Outlook Recovery)
- C:\Users\[username]\AppData\Roaming\KM1A2CD2\KM1logri.ini - 1 kB (Iexplore Recovery)
- C:\Users\[username]\AppData\Roaming\KM1A2CD2\KM1logrv.ini - 1 kB (__Vault Recovery)

- Note: All the above files were deleted after data exfiltation, except for first file at 0 bytes na

FORMBOOK HTTP GET AND POST REQUESTS:

- GET /he2a/?[string of alphanumeric characters with the following mixed in: = _ + and /]
- POST /he2a/

FORMBOOK DOMAINS THAT DID NOT RESOLVE:

- DNS query for www.24eu-ru-startup[.]xyz - No such name
- DNS query for www.b-store[.]shop - No such name
- DNS query for www.bavrnimn[.]site - No such name

- DNS query for www.connectioncompass[.]store - No such name
- DNS query for www.hfaer4[.]xyz - No such name
- DNS query for www.lb92[.]tech - No such name
- DNS query for www.meet-friends[.]online - No such name
- DNS query for www.myjbtest[.]net - No such name
- DNS query for www.narcisme[.]coach - No such name
- DNS query for www.pagosmultired[.]online - no response from DNS
- DNS query for www.redtopassociates[.]com - No such name
- DNS query for www.smokintires[.]net - No such name
- DNS query for www.wealthjigsaw[.]xyz - No such name

FORMBOOK DOMAINS THAT RESOLVED, BUT NO CONNECTION TO SERVER:

- 156.239.77[.]249 port 80 - www.paintellensburg[.]com - TCP SYN segments only, no response or RST f
- 3.36.26[.]167 port 80 - www.6o20r[.]beauty - TCP SYN segments only, no response or RST from server

FORMBOOK GET URLS ONLY:

- Note: Most of these are parked domain pages, although some appear to be legitimate websites.

- 13.248.243[.]5 port 80 - www.4tvaccounting[.]com
- 115.126.35[.]194 port 80 - www.678ap[.]com
- 217.70.184[.]50 port 80 - www.adept-expert-comptable[.]net
- 50.87.146[.]73 port 80 - www.arsajib[.]com
- 34.102.136[.]180 port 80 - www.avaturre[.]biz
- 198.54.117[.]216 port 80 - www.botfolk[.]com
- 154.219.175[.]99 port 80 - www.cpohlelaw[.]com
- 154.197.7[.]82 port 80 - www.cyg8wm3zfb[.]xyz
- 75.2.115[.]196 port 80 - www.dp77[.]shop
- 72.167.69[.]17 port 80 - www.dtslogs[.]com
- 103.224.182[.]210 port 80 - www.eletrobrasilvendas[.]com
- 169.239.218[.]55 port 80 - www.epeople[.]store
- 198.54.117[.]215 or 198.54.117[.]218 port 80 - www.guninfo[.]guru
- 104.194.229[.]208 port 80 - www.hg08139[.]com
- 34.102.136[.]180 port 80 - www.mamaeconomics[.]net
- 172.67.160[.]165 port 80 - www.mathews[.]buzz
- 172.67.147[.]23 port 80 - www.mimi2023[.]monster
- 154.31.55[.]249 port 80 - www.mybet668[.]com
- 34.69.160[.]147 port 80 - www.pf326[.]com
- 103.181.194[.]5 port 80 - www.pittalam[.]com
- 204.188.203[.]154 port 80 - www.saledotfate[.]live
- 198.185.159[.]144 port 80 - www.theoregondog[.]com
- 91.238.163[.]179 port 80 - www.totneshotdesk[.]com
- 217.70.184[.]50 port 80 - www.xn--groupe-gorg-lbb[.]com
- 107.148.151[.]12 port 80 - www.yuwangjing[.]com
- 172.67.147[.]73 port 80 - www.zamupoi[.]fun
- 104.21.75[.]135 port 80 - www.zekicharge[.]com

```
DOMAINS USING FORMBOOK GET AND POST URLS:

- Note: These appear to be legitimate websites or parked domain pages.

- 76.223.105[.]230 port 80 - www.4tvaccounting[.]com
- 15.197.142[.]173 port 80 - www.cyberlegion[.]group
- 34.117.168[.]233 port 80 - www.dcmdot[.]com **
- 15.197.142[.]173 port 80 - www.emsculptcenterofne[.]com
- 91.195.240[.]94 port 80 - www.giuila[.]online
- 34.102.136[.]180 port 80 - www.matrix-promotions[.]com
- 104.21.28[.]185 port 80 - www.mimi2023[.]monster **
- 34.102.136[.]180 port 80 - www.misstamar[.]mobi **
- 67.223.117[.]3 port 80 - www.notbokin[.]online **
- 68.65.122[.]50 port 80 - www.qfs-capital[.]com !!
- 64.98.135[.]49 port 80 - www.taylorranchtrail[.]com **
- 202.124.241[.]178 port 80 - www.theaustralianbrisketboard[.]com

  ** - Full stolen data (encoded) sent through HTTP POST request.

  !! - Domain www.qfs-capital[.]com appears to be a legitimate site, but response headers from the P
       it accepted the stolen data.
```

Click here to return to the main page.
