SANS ISC: Recent Dridex activity - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

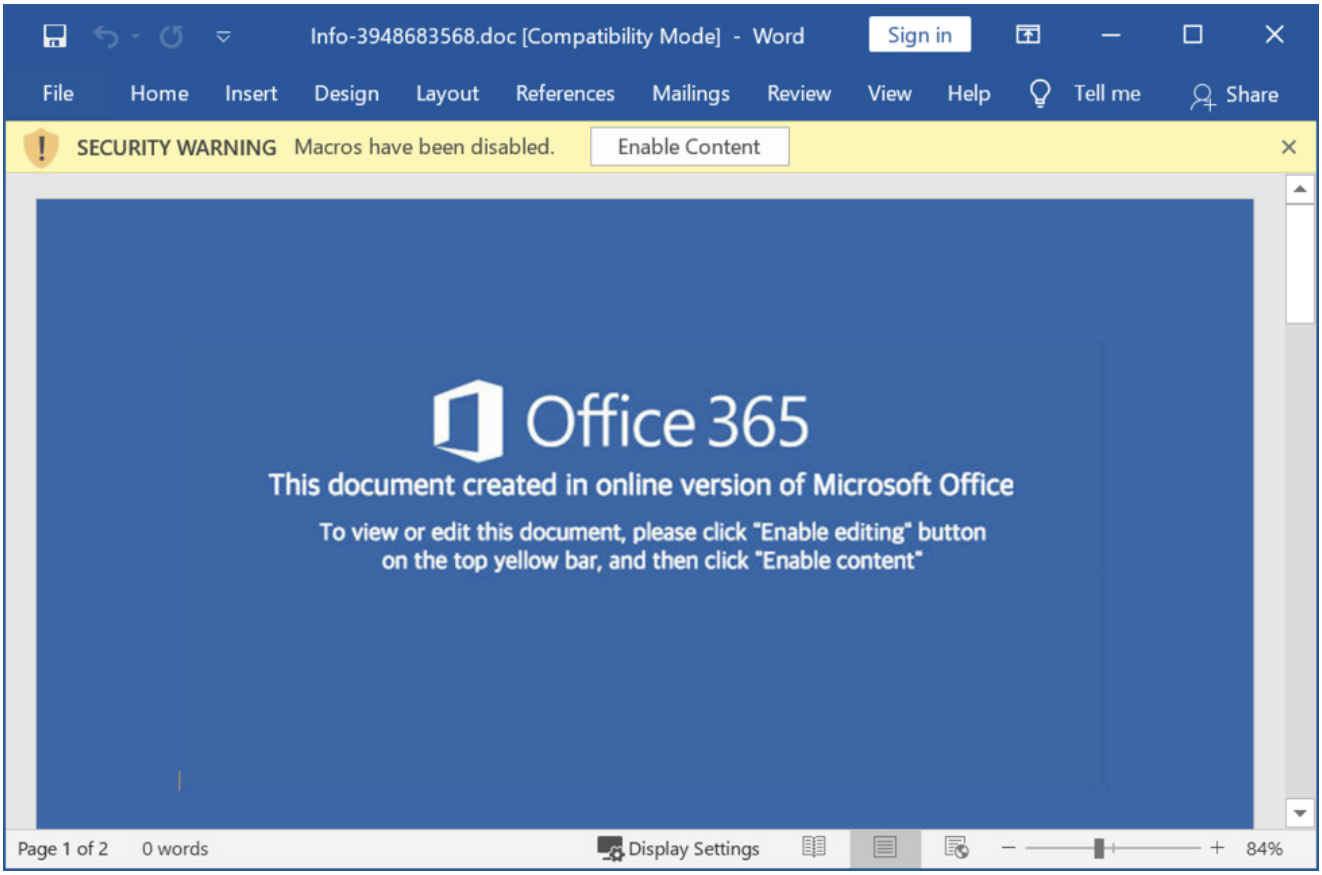
Introduction

For the past month or so, I hadn't had any luck finding active malspam campaigns pushing Dridex malware. That changed starting this week, and I've since found several examples. Today's diary reviews an infection from Wednesday September 9th, 2020.

The Word documents

While searching VirusTotal, I found three documents with the same template that generated the same type of traffic (read: SHA256 hash - name):

- fee5bb973112d58445d9e267e0ceea137d9cc1fb8a7140cf9a67472c9499a30f - Info-3948683568.doc
- 9b747e89874c0b080cf78ed61a1ccbd9c86045dc61b433116461e3e81eee1348 - Inform-34674869.doc'
- 27379612c139d3c4a0c6614ea51d49f2495213c867574354d7851a86fdec2428 - Rep-Sept2020.doc



Shown above: Screenshot with template used by all three of the above listed Word documents.

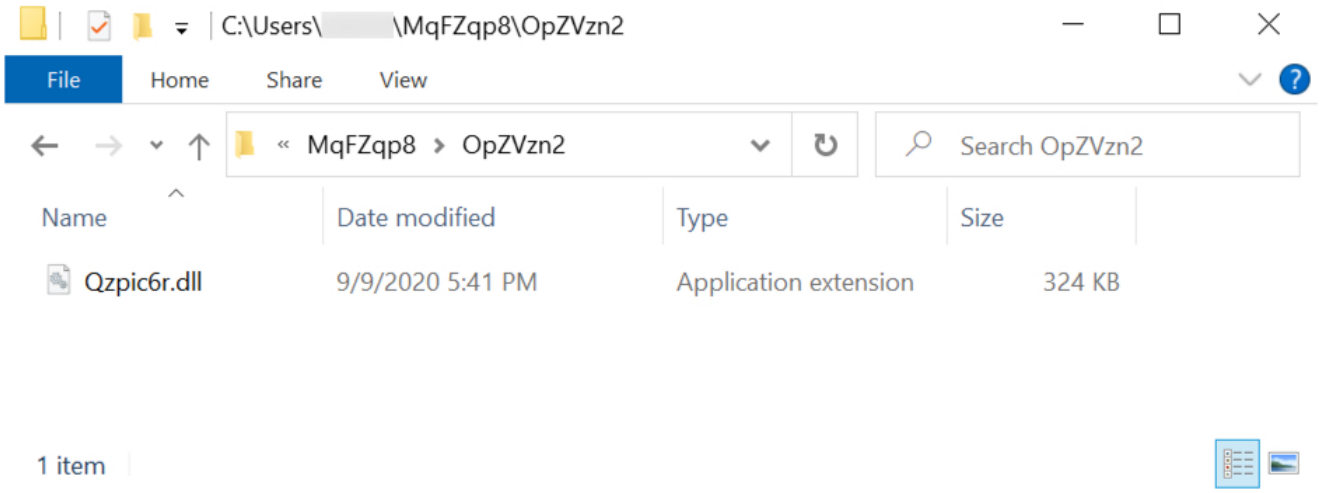
My lab environment revealed these documents are designed to infect a vulnerable Windows host with Dridex.

Enabling macros caused Powershell to retrieve a DLL file from one of the following URLs over encrypted HTTPS traffic:

```
hxxps://teworhfoundation[.]com/4jvmow.zip
hxxps://teworhfoundation[.]com/zd0pcc.rar
hxxps://thecandidtales[.]com/doakai.zip
hxxps://safaktasarim[.]com/7zcsfo.txt
hxxps://thecandidtales[.]com/wuom4a.rar
```

After the DLL was saved under the victim's profile, it was run using rundll32.exe. The DLL is an installer for Dridex, and it was run using the following command:

```
"C:\Windows\system32\rundll32.exe" C:\Users\[username]\Mqfzqp8\Opzvzn2\Qzpic6r.dll 0
```



Shown above: Location of the initial DLL to install Dridex on an infected Windows host.

Dridex infection traffic

Dridex post-infection traffic is all HTTPS. In this case, we saw HTTPS traffic over the following IP addresses and ports:

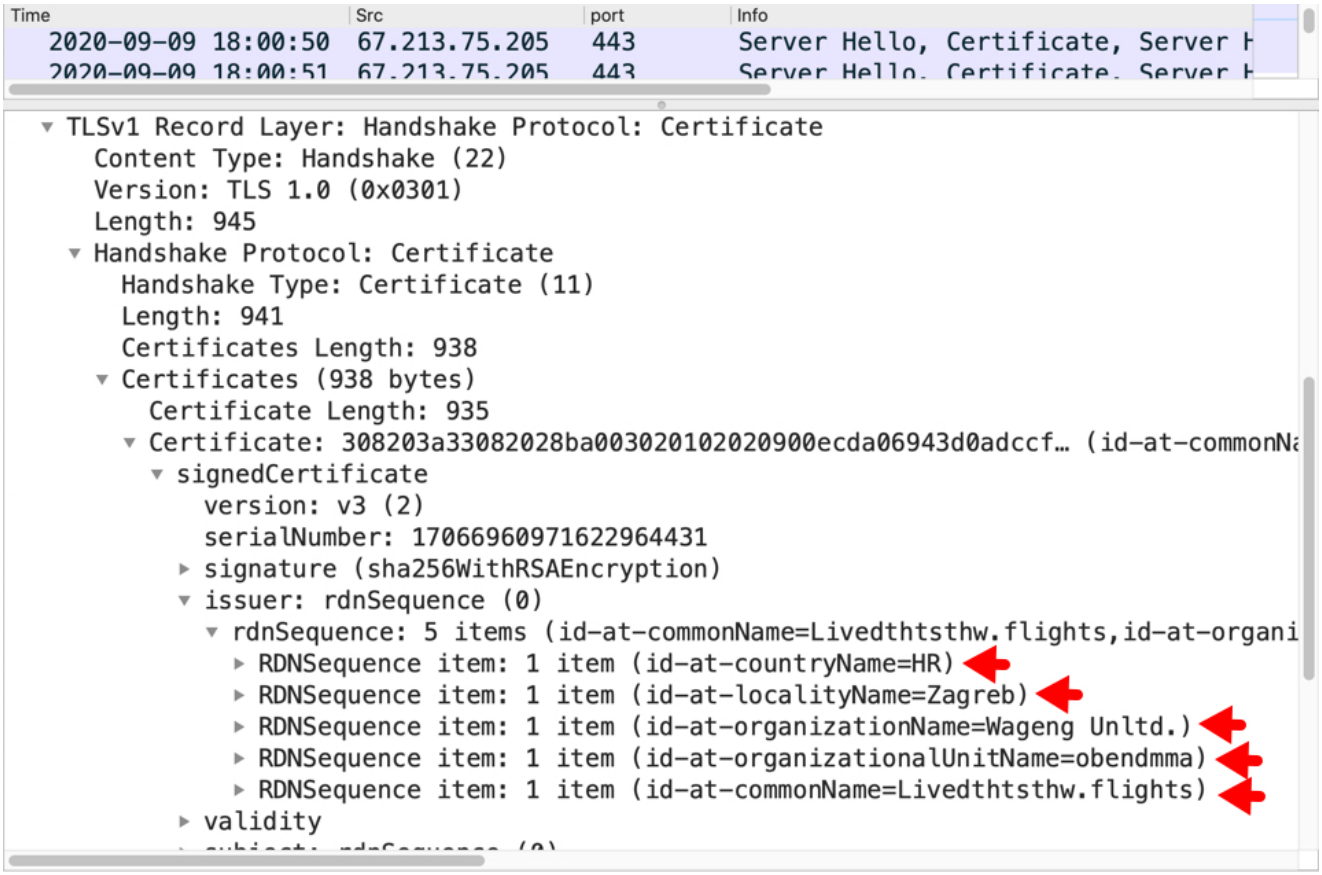
```
67.213.75[.]205 port 443
54.39.34[.]26 port 453
```

Time	Dst	port	Host	Info
2020-09-09 17:41:53	3.8.100.163	443	teworhfoundation.com	Client Hello
2020-09-09 18:00:49	67.213.75.205	443		Client Hello
2020-09-09 18:00:51	67.213.75.205	443		Client Hello
2020-09-09 18:00:56	67.213.75.205	443		Client Hello
2020-09-09 18:01:04	67.213.75.205	443		Client Hello
2020-09-09 18:05:41	54.39.34.26	453		Client Hello
2020-09-09 18:05:42	54.39.34.26	453		Client Hello
2020-09-09 18:05:48	54.39.34.26	453		Client Hello
2020-09-09 18:05:54	54.39.34.26	453		Client Hello
2020-09-09 18:41:28	54.39.34.26	453		Client Hello
2020-09-09 18:41:29	54.39.34.26	453		Client Hello
2020-09-09 18:41:37	54.39.34.26	453		Client Hello
2020-09-09 19:02:53	54.39.34.26	453		Client Hello
2020-09-09 19:02:59	54.39.34.26	453		Client Hello

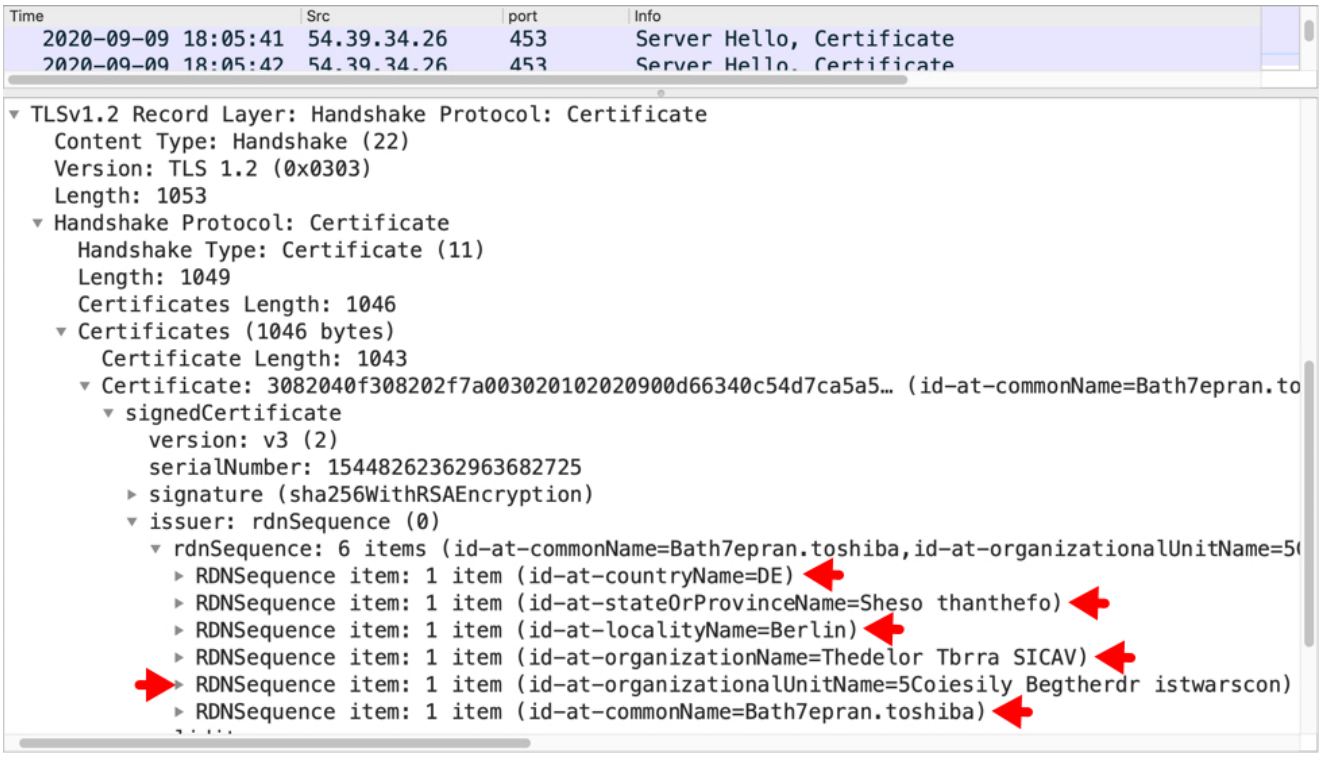
Shown above: Traffic from the Dridex infection filtered in Wireshark.

Most of the Dridex post-infection traffic I've seen uses IP addresses without domain names, and issuer data for the SSL/TLS certificates is somewhat unusual. Certificate issuer data for the Dridex post-infection traffic:

```
CERTIFICATE ISSUER DATA FOR HTTPS TRAFFIC TO 67.213.75[.]205 OVER TCP PORT 443:

id-at-countryName=HR
id-at-localityName=Zagreb
id-at-organizationName=Wageng Unltd.
id-at-organizationalUnitName=obendmma
id-at-commonName=Livedthtsthw.flights

CERTIFICATE ISSUER DATA FOR HTTPS TRAFFIC TO 54.39.34[.]26 OVER TCP PORT 453:

id-at-countryName=DE
id-at-stateOrProvinceName=Sheso thanthefo
id-at-localityName=Berlin
id-at-organizationName=Thedelor Tbrra SICAV
id-at-organizationalUnitName=5Coiesily Begtherdr istwarscon
id-at-commonName=Bath7epran.toshiba
```



Shown above: Certificate issuer data for HTTPS traffic to 67.213.75[.]205 over TCP port 443 found in Wireshark.



Shown above: Certificate issuer data for HTTPS traffic to 54.39.34[.]26 *over TCP port 453 found in Wireshark.*

Dridex persistent on an infected Windows host

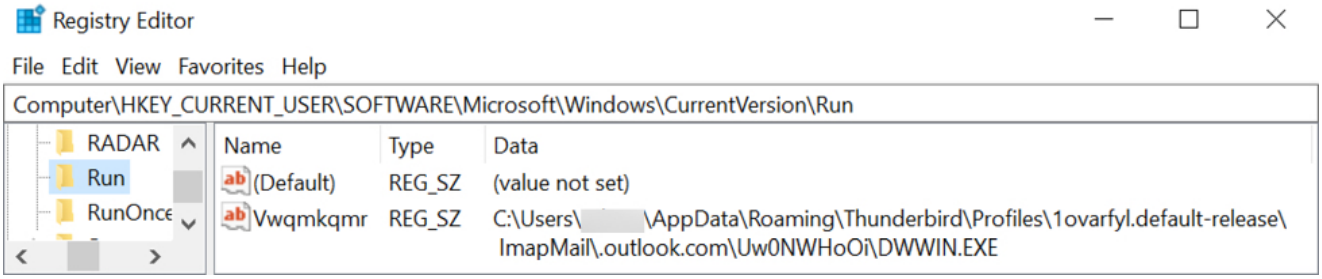
Dridex is made persistent on an infected Windows host using 3 methods simultaneously:

- Windows registry update
- Scheduled task
- Windows startup menu shortcut

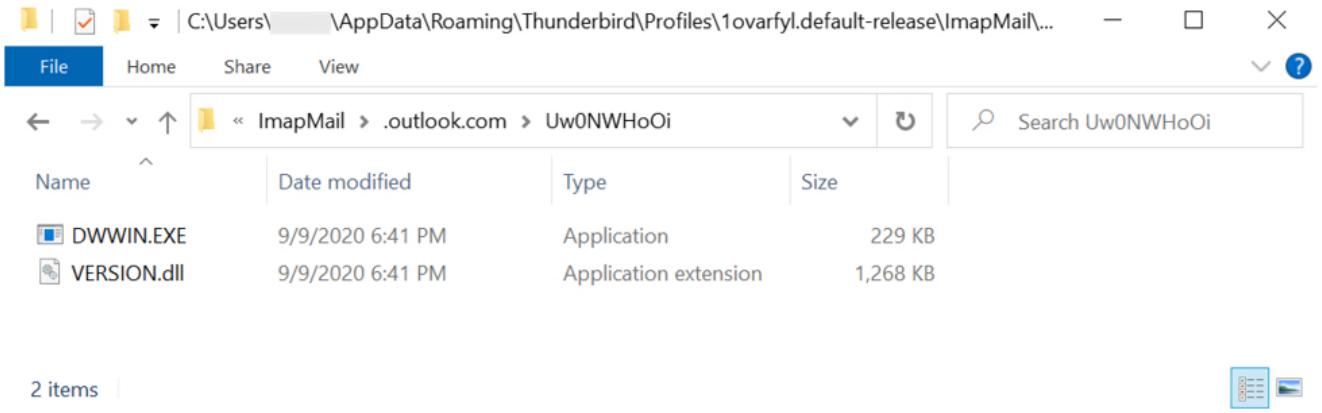
Dridex uses copies of legitimate Windows system files (EXEs) to load and run malware. Dridex DLL files are named as DLLs that would normally be run by these copied system EXEs.

For this infection, all of the persistent Dridex DLL files were 64-bit DLL files.

```
WINDOWS REGISTRY UPDATE:

- Registry Key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Value name: Vwqmkqmr
- Value type: REG_SZ
- Value data: C:\Users\
[username]\AppData\Roaming\Thunderbird\Profiles\1ovarfyl.default-release\
             ImapMail\.outlook.com\Uw0NWHoOi\DWWIN.EXE

NOTE: DWWIN.EXE loads and runs a Dridex DLL file named VERSION.dll in the same
directory.
```

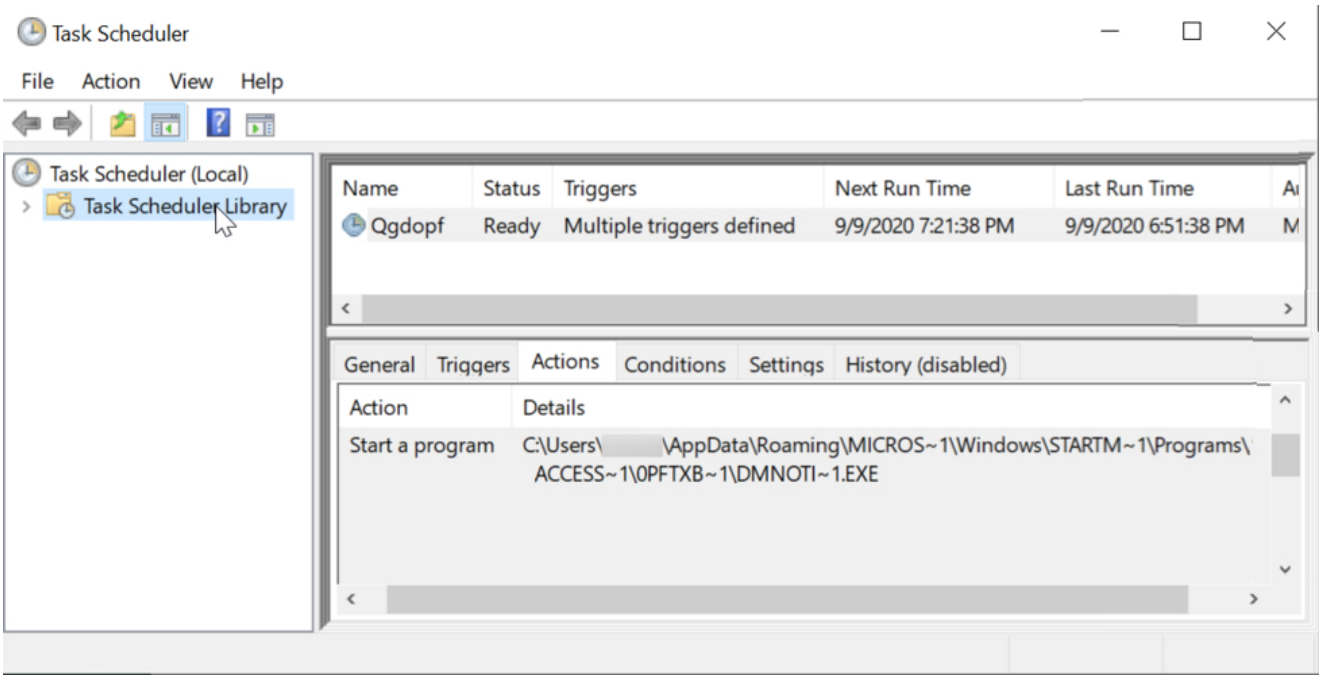


Shown above: Windows registry update used to keep Dridex persistent on an infected host.

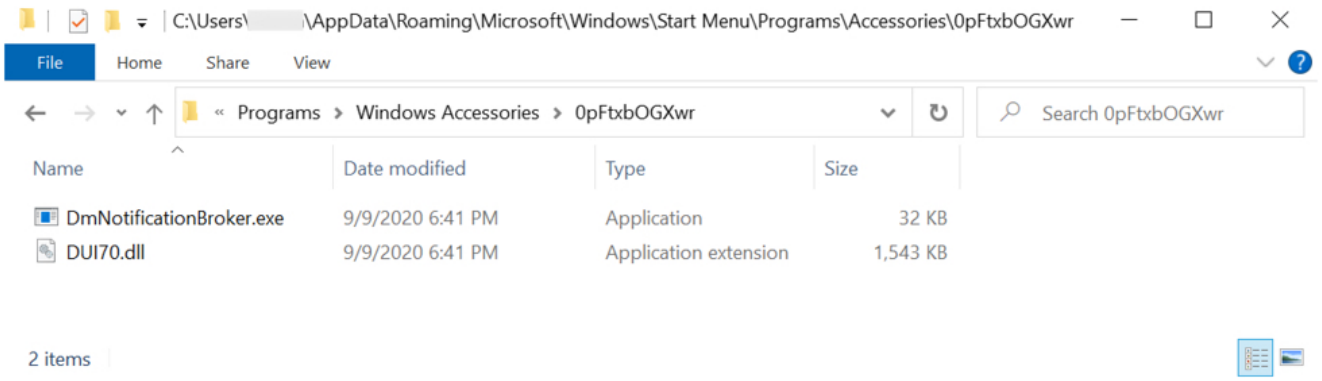


Shown above: Legitimate EXE called by registry update, and Dridex DLL in the same directory.

```
SCHEDULED TASK:

- Task name: Qgdopf
- Action: Start a program
- Details: C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\
          0pFtxbOGXwr\DmNotificationBroker.exe

NOTE: DmNotificationBroker.exe loads and runs a Dridex DLL file named DUI70.dll in
the same directory.
```

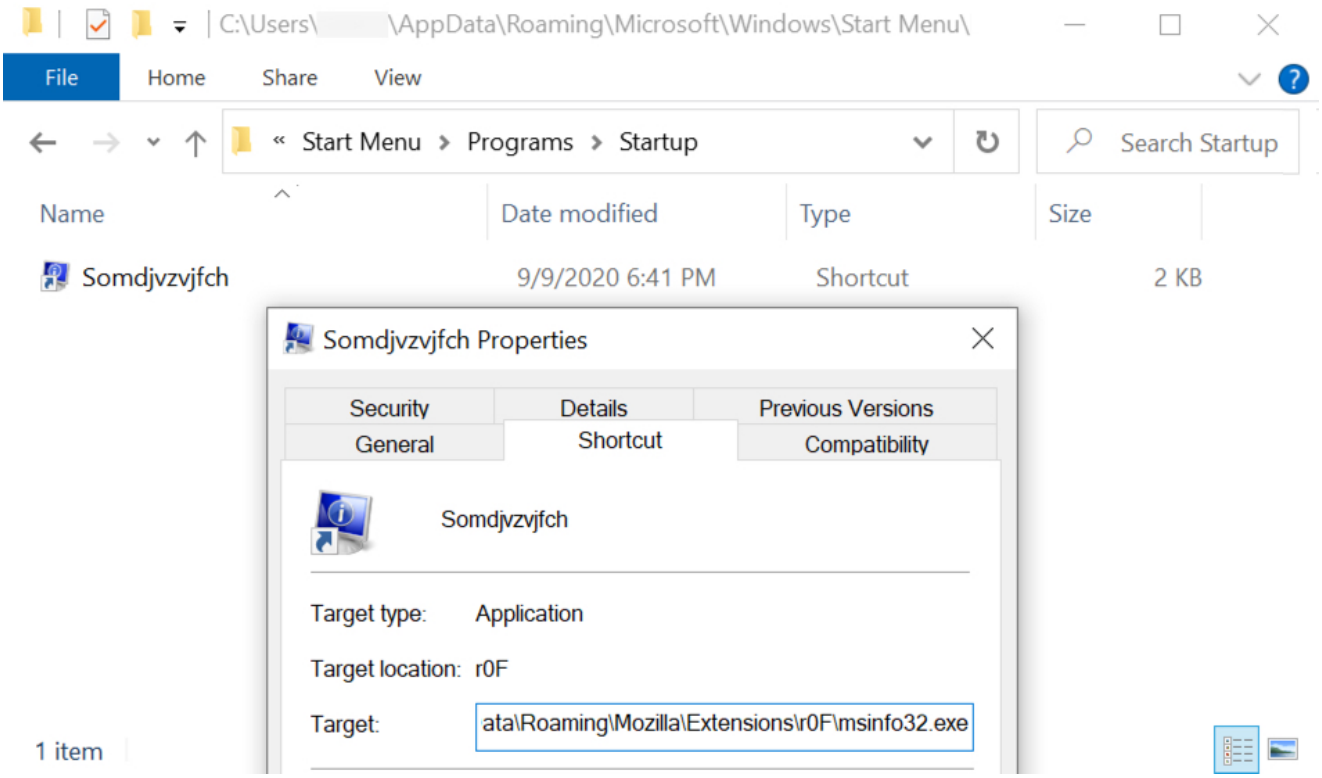


Shown above: Scheduled task on the same infected Windows host also used to keep Dridex persistent.

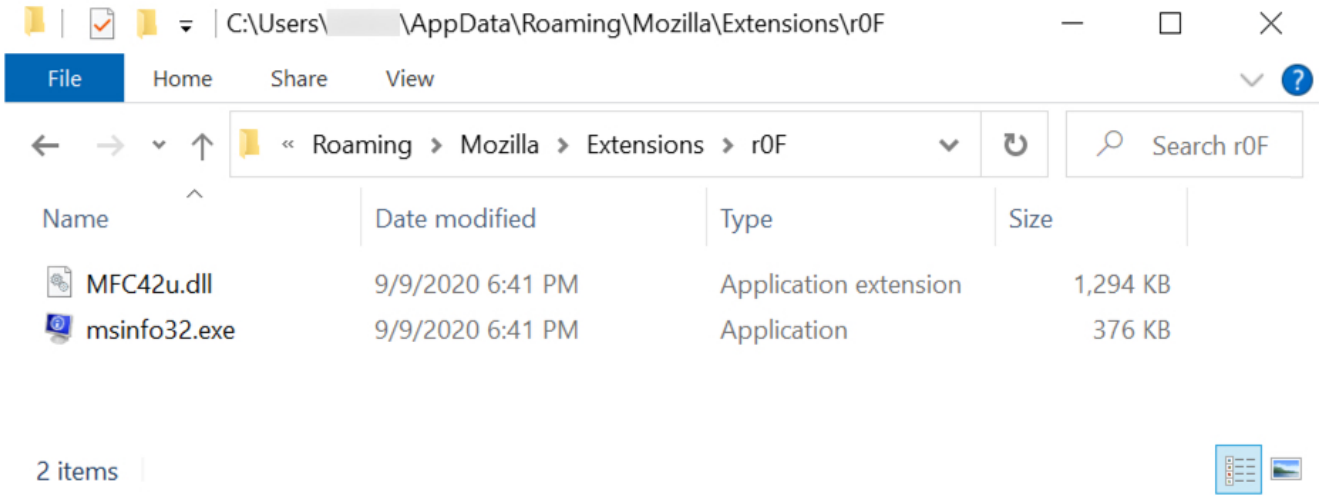


Shown above: Legitimate EXE called by scheduled task, and Dridex DLL in the same directory.

```
WINDOWS STARTUP MENU SHORTCUT:

Shortcut: C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start
Menu\Somdjvzvjfch.lnk
Target: C:\Users\[username]\AppData\Roaming\Mozilla\Extensions\r0F\msinfo32.exe

NOTE: msinfo32.exe loads and runs a Dridex DLL file named MFC42u.dll in the same
directory.
```



Shown above: Windows start menu shortcut also used to keep Dridex persistent on the same infected Windows host.



Shown above: Legitimate EXE called by start menu shortcut, and Dridex DLL in the same directory.

Indicators of Compromise (IOCs)

Three examples of Microsoft Word documents with macros for Dridex:

SHA256 hash: fee5bb973112d58445d9e267e0ceea137d9cc1fb8a7140cf9a67472c9499a30f

- File size: 136,262 bytes
- File name: Info-3948683568.doc

SHA256 hash:
9b747e89874c0b080cf78ed61a1ccbd9c86045dc61b433116461e3e81eee1348

- File size: 136,182 bytes
- File name: Inform-34674869.doc

SHA256 hash:
27379612c139d3c4a0c6614ea51d49f2495213c867574354d7851a86fdec2428

- File size: 135,053 bytes
- File name: Rep-Sept2020.doc

Installer DLL for Dridex called by Word macro:

SHA256 hash:
790b0d9e2b17f637c3e03e410aa22d16eccfefd28d74b226a293c9696edb60ad

- File size: 331,776 bytes
- File location: hxxps://thecandidtales[.]com/doakai.zip
- File location: C:\Users*[username]*\MqFZqp8\OpZVzn2\Qzpic6r.dll
- Run method: rundll32.exe [file name] 0

Dridex 64-bit DLL files persistent on the infected Windows host:

SHA256 hash: fd8049d573c056b92960ba7b0949d9f3a97416d333fa602ce683ef822986ad58

- File size: 1,580,032 bytes
- File location: C:\Users*[username]*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\0pFtxbOGXwr\DUI70.dll
- Run method: Loaded and run by legitimate system file DmNotificationBroker.exe in the same directory
- Note: Made persistent through scheduled task

SHA256 hash: 719a8634a16beb77e6d5c6bb7f82a96c6a49d5cfa64463754fd5f0e5eb0581be

- File size: 1,325,056 bytes
- File location: C:\Users\ *[username]*\AppData\Roaming\Mozilla\Extensions\r0F\MFC42u.dll
- Run method: Loaded and run by legitimate system file msinfo32.exe in the same directory
- Note: Made persistent through start menu shortcut

SHA256 hash:
4d7d8d1790d494a1a29dae42810a3a10864f7c38148c3600c76491931c767c5c

- File size: 1,297,920 bytes

- File location: C:\Users\ *[username]*\AppData\Roaming\Thunderbird\Profiles\1ovarfyl.default-release\ImapMail\.outlook.com\Uw0NWHoOi\VERSION.dll
- Run method: Loaded and run by legitimate system file DWWIN.EXE in the same directory
- Note: Made persistent through Windows registry update

URLs from Word macro to retrieve Dridex DLL installer:

- hxxps://teworhfoundation[.]com/4jvmow.zip
- hxxps://teworhfoundation[.]com/zd0pcc.rar
- hxxps://thecandidtales[.]com/doakai.zip
- hxxps://safaktasarim[.]com/7zcsfo.txt
- hxxps://thecandidtales[.]com/wuom4a.rar

Certificate data for Dridex HTTPS traffic to 67.213.75[.]205 port 443:

- id-at-countryName=HR
- id-at-localityName=Zagreb
- id-at-organizationName=Wageng Unltd.
- id-at-organizationalUnitName=obendmma
- id-at-commonName=Livedthtsthw.flights

Certificate data for Dridex HTTPS traffic to 54.39.34[.]26 port 453:

- id-at-countryName=DE
- id-at-stateOrProvinceName=Sheso thanthefo
- id-at-localityName=Berlin
- id-at-organizationName=Thedelor Tbrra SICAV
- id-at-organizationalUnitName=5Coiesily Begtherdr istwarscon
- id-at-commonName=Bath7epran.toshiba

Final words

After a period of inactivity, malspam pushing Dridex malware is back, so this blog post reviewed traffic and malware from an infected Windows host. While not much has changed, it's always good to have a refresher.

As usual, up-to-date Windows hosts with the latest security patches and users who follow best security practices are not likely to get infected with this malware. However, I've seen so much come through in the past two or three days that even a small percentage of success will likely be profitable for the criminals behind it.

Brad Duncan
brad [at] malware-traffic-analysis.net

Brad

433 Posts
ISC Handler
Sep 10th 2020