

# 2018-02-01 - QUICK TEST DRIVE OF TRICKBOT (IT NOW HAS A MONERO MODULE)

---

malware-traffic-analysis.net/2018/02/01/

## ASSOCIATED FILES:

- Zip archive of the pcaps: [2018-02-01-Trickbot-infection-traffic.pcap.zip](#) 9.5 MB (9,472,261 bytes)
- Zip archive of the malware: [2018-02-01-Trickbot-malware-samples.zip](#) 542 kB (541,817 bytes)

## INTRODUCTION

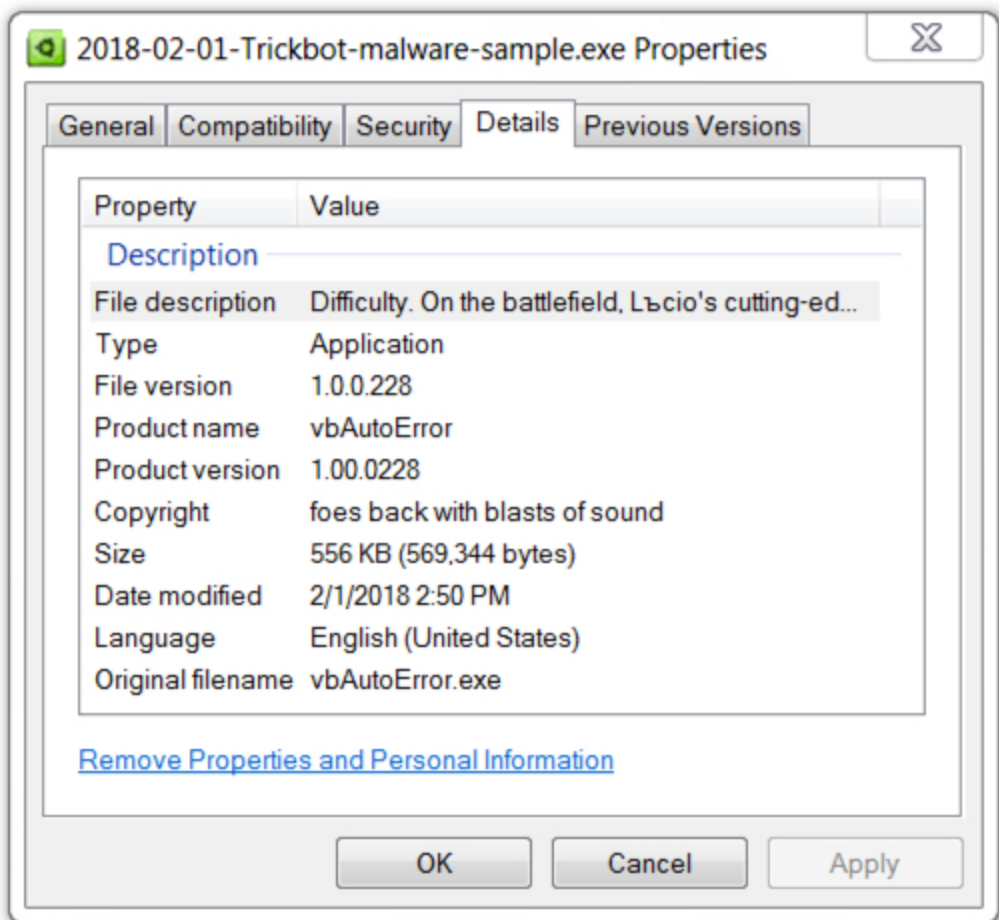
---

I infected a Windows host with the Trickbot malware from 2018-02-01 mentioned in [this blog post](#) from My Online Security. I extracted the Trickbot binary located in a pcap from the [Any.run analysis of the associated malicious Word document](#).

The chain of events led from the email to --> link to a Word document --> enable Word document macro --> Smoke Loader --> Trickbot.



2018-02-01-Trickbot-malware-sample.exe



Shown above: Trickbot binary extracted from the Any.run pcap.

I wanted to see what the Trickbot binary was doing, since I haven't looked at it in a while. This blog post only reviews traffic and artifacts from a Windows host infected with the Trickbot binary, SHA256 hash [91f78068e996b1b32a3539746b6b683f5fa40e7be009b779c56e215b521df6c5](#).

## TRICKBOT TRAFFIC

Trickbot network traffic in February 2018 are similar to what I in [this ISC diary I wrote in August 2017](#). The only difference is a Monero cryptocurrency miner (coin miner) in post-infection traffic in February 2018, which I hadn't noticed before.

Filter: `http.request or ssl.handshake.type == 1 or (tcp.flags e` Expression... Clear Apply Save

Date/Time	Dst	port	Host	Server Name	Info
2018-02-01 21:12:28	69.162.69.148	80	icanhazip.com		GET / HTTP/1.1
2018-02-01 21:14:49	92.53.91.59	443			Client Hello
2018-02-01 21:17:12	194.87.111.151	447			Client Hello
2018-02-01 21:17:15	92.53.91.59	443			Client Hello
2018-02-01 21:19:26	194.87.111.151	447			Client Hello
2018-02-01 21:19:43	92.53.91.59	443			Client Hello
2018-02-01 21:23:16	194.87.111.151	447			Client Hello
2018-02-01 21:25:10	92.53.91.59	443			Client Hello
2018-02-01 21:25:42	92.53.91.59	443			Client Hello
2018-02-01 21:27:49	194.87.111.151	447			Client Hello
2018-02-01 21:27:52	92.53.91.59	443			Client Hello
2018-02-01 21:29:28	92.53.77.125	443			Client Hello
2018-02-01 21:30:43	194.87.111.151	447			Client Hello
2018-02-01 21:30:55	92.53.91.59	443			Client Hello
2018-02-01 21:33:25	194.87.111.151	447			Client Hello
2018-02-01 21:33:28	92.53.91.59	443			Client Hello
2018-02-01 21:33:28	50.63.196.49	80	valuesrevealed.com		GET /solinger.png HTTP/1.1
2018-02-01 21:34:19	37.46.130.180	42432			49259-42432 [SYN] Seq=
2018-02-01 21:36:16	92.53.77.125	443			Client Hello
2018-02-01 21:38:38	92.53.91.59	443			Client Hello
2018-02-01 21:42:02	92.53.91.59	443			Client Hello
2018-02-01 21:43:13	92.53.77.125	443			Client Hello
2018-02-01 21:44:30	92.53.77.125	443			Client Hello
2018-02-01 21:46:51	92.53.91.59	443			Client Hello

Shown above: Trickbot traffic (from the Trickbot binary) on 2018-02-01.

Trickbot SSL traffic is somewhat similar to what we've seen with Dridex SSL traffic in recent weeks. Today's Trickbot traffic triggered Emerging Threats alerts for ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificates detected (Dridex CnC), which I've seen with Trickbot traffic before. More importantly, rules from the Snort subscriber's ruleset detected Trickbot SSL certificates, which better fits what I saw on 2018-02-01.

```

alert (/var/log/snort) - gedit (as superuser)
File Edit View Search Tools Documents Help
alert x
[Alert -> http://77gctnab.com/xiirig/xiirig]

[**] [1:44402:1] MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange [**]
[Classification: A Network Trojan was detected] [Priority: 1]
02/01-21:36:17.465634 92.53.77.125:443 -> 10.2.1.102:49260
TCP TTL:128 TOS:0x0 ID:42251 Iplen:20 Dgmlen:1500
***A*** Seq: 0xA60357FE Ack: 0x6180CD2E Win: 0xFAF0 TcpLen: 20
[Xref => http://virustotal.com/en/file/70041c335a374d84f64c6c31d59ff09bd8473fd049cfcb46fe085d1eb92ac0b8/analysis/1502073944/]

[**] [1:44402:1] MALWARE-CNC Win.Trojan.Trickbot self-signed certificate exchange [**]
[Classification: A Network Trojan was detected] [Priority: 1]
02/01-21:43:27.347567 92.53.77.125:443 -> 10.2.1.102:49263
TCP TTL:128 TOS:0x0 ID:42561 Iplen:20 Dgmlen:1500
***A*** Seq: 0x701A981C Ack: 0x89CCEB28 Win: 0xFAF0 TcpLen: 20
[Xref => http://virustotal.com/en/file/70041c335a374d84f64c6c31d59ff09bd8473fd049cfcb46fe085d1eb92ac0b8/analysis/1502073944/]

[**] [120:15:1] Reset outside window [**]

```

Shown above: Snort alerts on Trickbot certificates in SSL traffic.

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	17	2018-02-01...	92.53.91.59	443	10.2.1.102	49199	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)
RT	4	2018-02-01...	50.63.196.49	80	10.2.1.102	49258	6	ET MALWARE Windows executable sent when remote host claims to send an i...
RT	4	2018-02-01...	50.63.196.49	80	10.2.1.102	49258	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	4	2018-02-01...	50.63.196.49	80	10.2.1.102	49258	6	ET MALWARE Windows executable sent when remote host claims to send an i...
RT	2	2018-02-01...	50.63.196.49	80	10.2.1.102	49258	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	2018-02-01...	10.2.1.102	49259	37.46.130.180	42432	6	ET POLICY Cryptocurrency Miner Checkin

Shown above: Emerging Threats alerts on the infection traffic from Squil using Suricata on Security Onion.

Date/Time	Dst	port	Info
2018-02-01 21:34:19	37.46.130.180	42432	49259-42432 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W

**Follow TCP Stream (tcp.stream eq 41)**

Stream Content

```

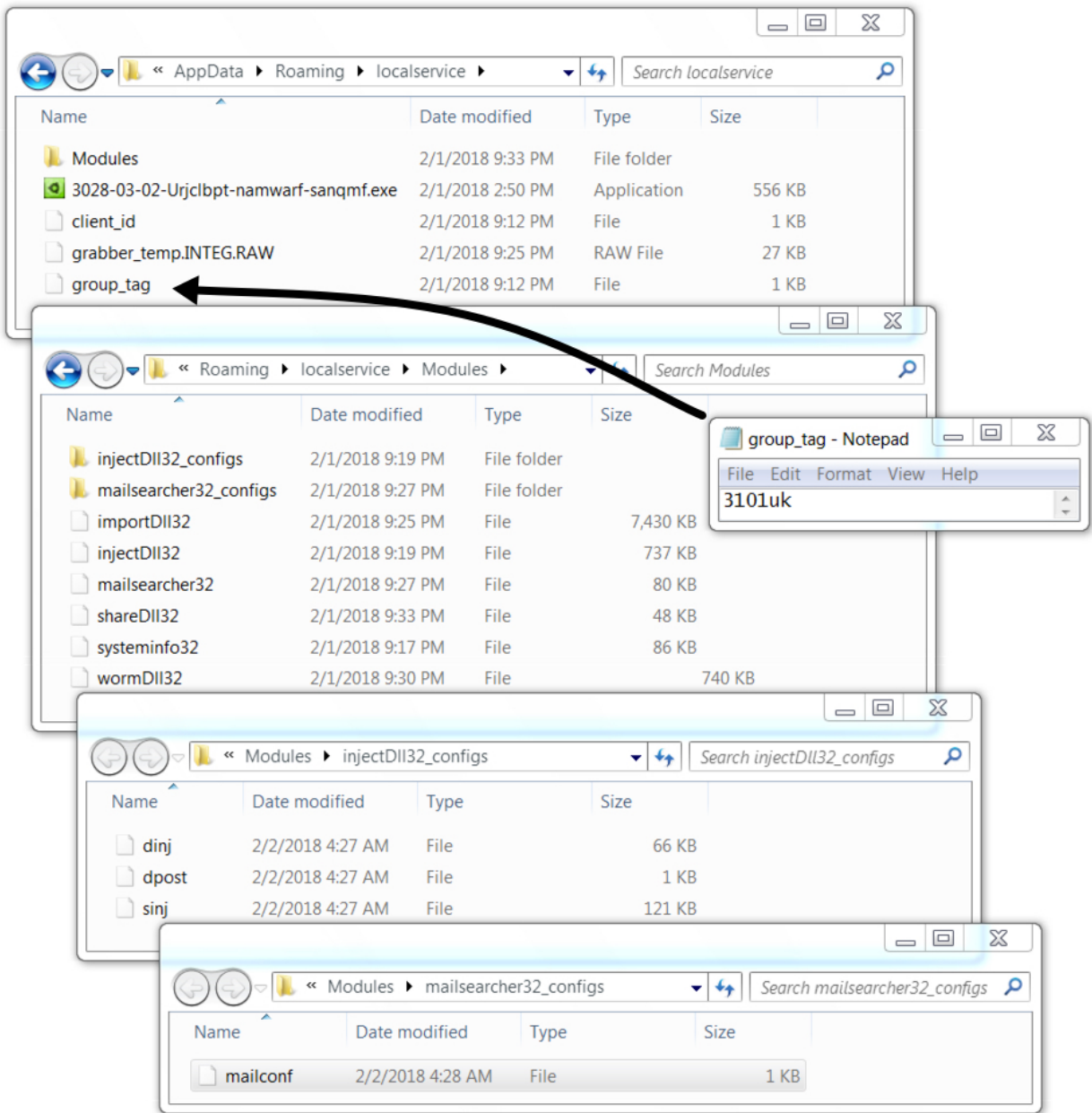
{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"x","pass":"x","agent":"XMRig/2.1.0 (Windows NT 6.1) libuv/1.15.0 gcc/7.2.0"}}
{"id":1,"jsonrpc":"2.0","result":{"id":"8974c51e-905d-4dfc-b9c8-1ec844a3dbe2","job":
{"blob":"0606ca8fced3051d4d5979bd0545e00013762743c9e2f1140a06d50ca97785584be8d75ec8f0b90
00000b021f008b5f3c101161451b62bce63ee312c1e2a364033cd9a632204f8ee1e234e06","job_id":"JXG
iWPAqxSSkSX3rJ5l+CpC4iStSb0","target":"1d60100"},"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0606ca8fced3051d4d5979bd0545e00013762743c9e2f1140a06d50ca97785584be8d75ec8f0b90
00000b0342c6e2d13b3ebb4b8dbddf393090bd0923817e6fa4ffe31f3f4d7da131a8c9206","job_id":"qnh
EeTqqgplkDJEGPZe3wpmrtj76b0","target":"1d60100"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0606ac90ced305f1e95901fc7584353fe0f3ad9da196ebe7c0e3b4e3882c1e94493e9d8f66404e0
00000b0ea89125b3a948ada23d6c6a3169a38a1131a4507389aab3ce82bf6f33ad38a4004","job_id":"MRT
gXCNqz3Meffw+IYOGhEOMftZCb0","target":"1d60100"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0606ac90ced305f1e95901fc7584353fe0f3ad9da196ebe7c0e3b4e3882c1e94493e9d8f66404e0

```

Shown above: Post-infection traffic caused by malware based on Monero (XMRig) coin miner.

## FORENSICS ON THE INFECTED WINDOWS HOST

My Trickbot binary was named **2018-02-01-Trickbot-malware-sample.exe**, and I ran it from the user's **AppData\Local\Temp** directory. As we saw with Trickbot back in August 2017, the malware copied itself to a new folder in the user's **AppData\Roaming** directory. Today's file was re-named, with some (but not all) of the characters in the file name shifted one character. Like we saw back in August 2017, there's a file named **group\_tag**. This time, it contained the text: **3101uk**. Below are images showing some of the artifacts.



Shown above: Artifacts on the infected Windows host.





Vitali Kremez

@VK\_Intel

2-1-2018: #Trickbot banking #malware group tag "3101uk" ->

Decoded "worm32Dll" module is a repackaged #XMRig #miner #Monero

Decoded module hash:

F76560654C32B0CC455E884109AEDCA0

```

.rdata:6CDC99E0 aUsageXmrigOpti db 'Usage: xmrig [OPTIONS]',0Ah ; DATA XREF: .text:6CD48007o
.rdata:6CDC99E0 db 'Options:',0Ah ; .text:6CD482AD7o ...
.rdata:6CDC99E0 db ' -a, --algo=ALGO          cryptonight (default) or cryptonight-lite'
.rdata:6CDC99E0 db 0Ah
.rdata:6CDC99E0 db ' -o, --url=URL            URL of mining server',0Ah
.rdata:6CDC99E0 db ' -O, --userpass=U:P       username:password pair for mining server',0Ah
.rdata:6CDC99E0 db ' -u, --user=USERNAME      username for mining server',0Ah
.rdata:6CDC99E0 db ' -p, --pass=PASSWORD      password for mining server',0Ah
.rdata:6CDC99E0 db ' -t, --threads=N          number of miner threads',0Ah
.rdata:6CDC99E0 db ' -v, --av=N               algorithm variation, 0 auto select',0Ah
.rdata:6CDC99E0 db ' -k, --keepalive          send keepalived for prevent timeout (need
.rdata:6CDC99E0 db ' pool support)',0Ah
.rdata:6CDC99E0 db ' -r, --retries=N          number of times to retry before switch to'
.rdata:6CDC99E0 db ' backup server (default: 5)',0Ah
.rdata:6CDC99E0 db ' -R, --retry-pause=N      time to pause between retries (default: 5'
.rdata:6CDC99E0 db ')',0Ah
.rdata:6CDC99E0 db ' --cpu-affinity           set process affinity to CPU core(s), mask'
.rdata:6CDC99E0 db ' 0x3 for cores 0 and 1',0Ah
.rdata:6CDC99E0 db ' --no-color               disable colored output',0Ah
.rdata:6CDC99E0 db ' --donate-level=N         donate level, default 5%% (5 minutes in 1'
.rdata:6CDC99E0 db ' 00 minutes)',0Ah
.rdata:6CDC99E0 db ' -B, --background        run the miner in the background',0Ah
.rdata:6CDC99E0 db ' -c, --config=FILE       load a JSON-format configuration file',0Ah
.rdata:6CDC99E0 db ' -l, --log-file=FILE     log all output to a file',0Ah
.rdata:6CDC99E0 db ' --current CPU',0Ah
.rdata:6CDC99E0 db ' --nicehash               enable nicehash support',0Ah
.rdata:6CDC99E0 db ' --print-time=N          print hashrate report every N seconds',0Ah
.rdata:6CDC99E0 db ' -h, --help              display this help and exit',0Ah
.rdata:6CDC99E0 db ' -V, --version           output version information and exit',0Ah,0
.rdata:6CDC9F68 align 10h
.rdata:6CDC9F70 xnmword_6CDC9F70 xnmword 48000000000000000000000000000000
.rdata:6CDC9F70 ; DATA XREF: sub_6CD487E0+1ETr
.rdata:6CDC9F80 xnmword_6CDC9F80 xnmword 5000000050000003Ch ; DATA XREF: sub_6CD487E0+20Tr
.rdata:6CDC9F90 align 20h
.rdata:6CDC9FA0 a0132nenabled db 1Bh,'[01:32nenabled',0 ; DATA XREF: .text:6CD490BC7o
.rdata:6CDC9FB0 a0131ndisabled db 1Bh,'[01:31ndisabled',0 ; DATA XREF: .text:6CD490B77o
.rdata:6CDC9FC1 a0132navailable db 1Bh,'[01:32navailable',0 ; DATA XREF: .text:6CD490C47o
.rdata:6CDC9FD3 a0131nunavailab db 1Bh,'[01:31nunavailable',0 ; DATA XREF: .text:6CD490C87o

```

2-1-2018: Trickbot's "worm32Dll" -> repackaged XMRig Miner

4:37 PM - 1 Feb 2018

Shown above: Per @VK\_Intel, decoded Worm32Dll module is a Monero coin miner (link).

## FINAL WORDS

Looks like Trickbot has changed a bit since I last examined it. Traffic and artifacts familiar, but Trickbot has apparently jumped on the cryptocurrency bandwagon by adding a Monero (XMRig) coin mining module. I imagine someone will do a more in-depth write-up on the new Trickbot, but I wanted to get some traffic and malware samples out.

Once again, here are the associated files:

- Zip archive of the pcaps: [2018-02-01-Trickbot-infection-traffic.pcap.zip](#) 9.5 MB (9,472,261 bytes)
- Zip archive of the malware: [2018-02-01-Trickbot-malware-samples.zip](#) 542 kB (541,817 bytes)

All zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

[Click here](#) to return to the main page.