Malware-Traffic-Analysis.net - 2018-02-01 - Quick test-drive of Trickbot (it now has a Monero module)

NOTICE:

- 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.

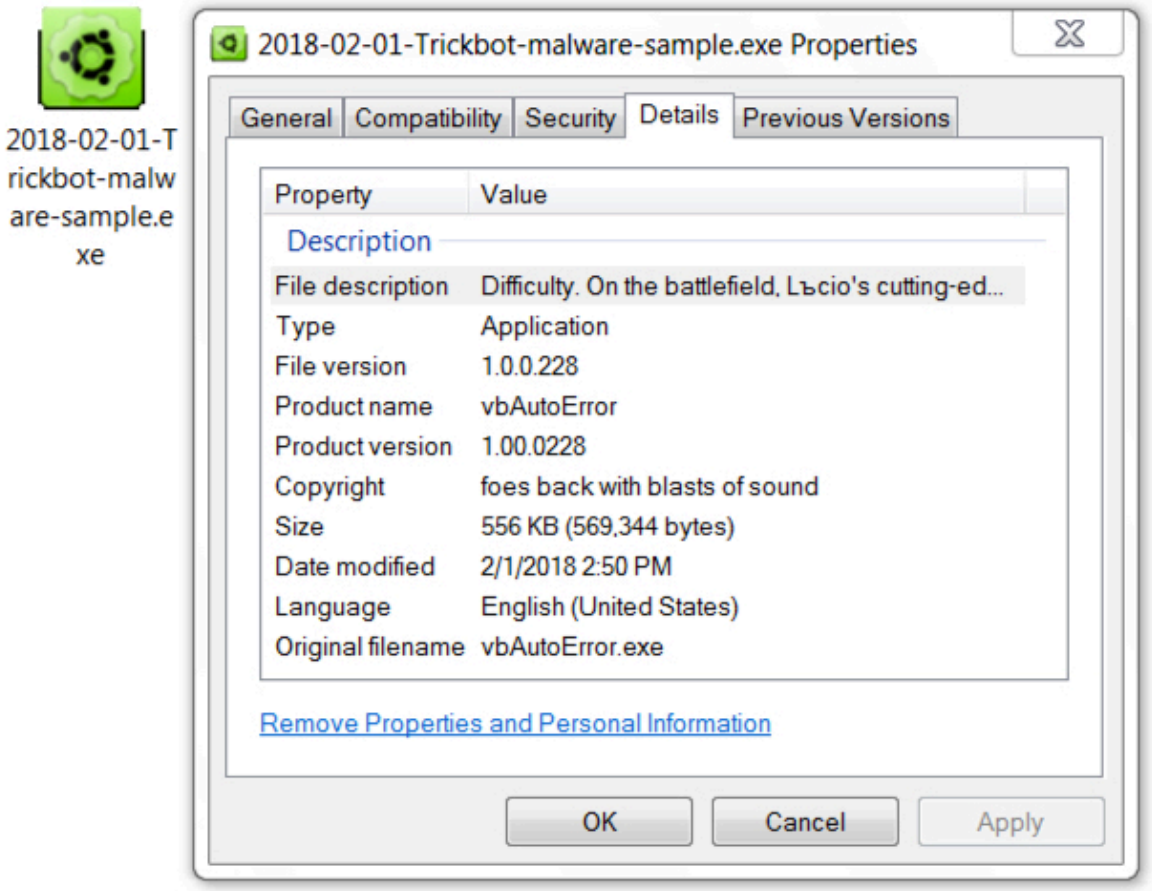
ASSOCIATED FILES:

- 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 542.2 kB (542,161 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.

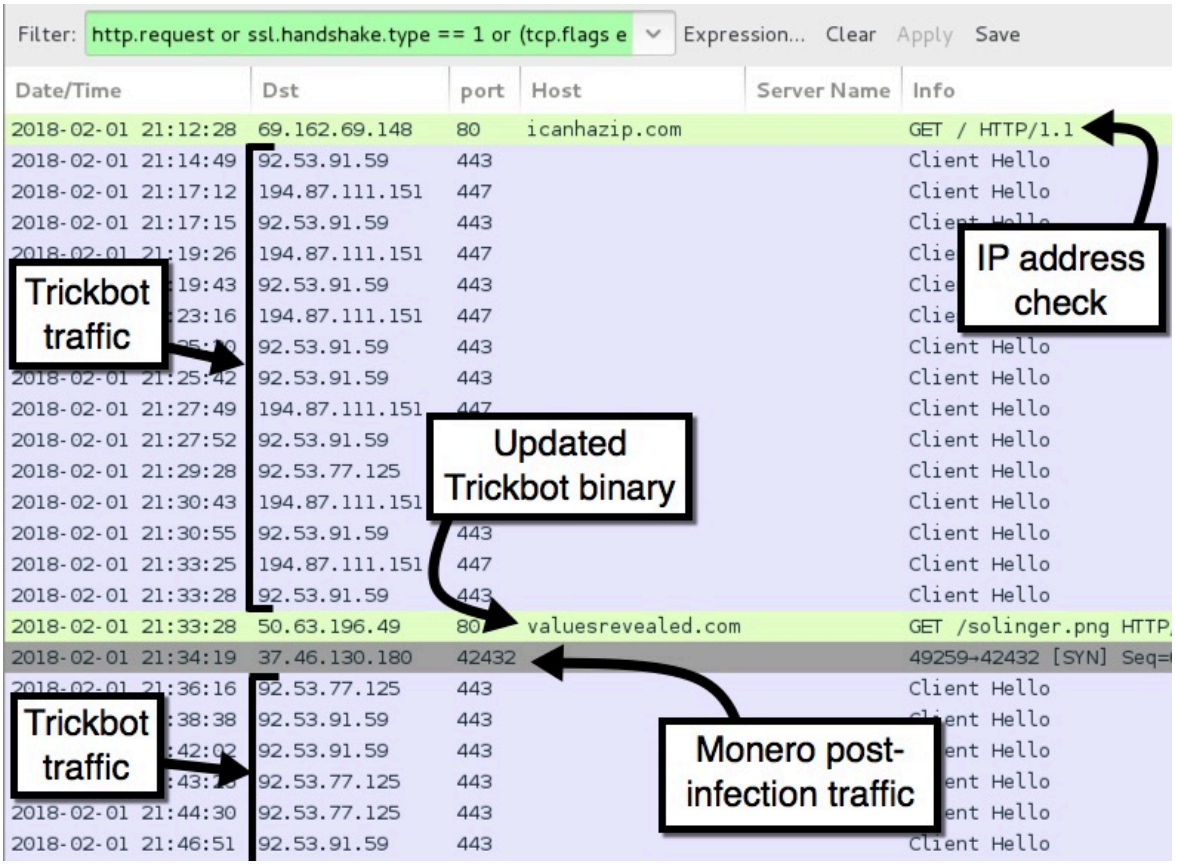


Shown above: Trickbot binary extracted from the Any.run pcap.

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](#).

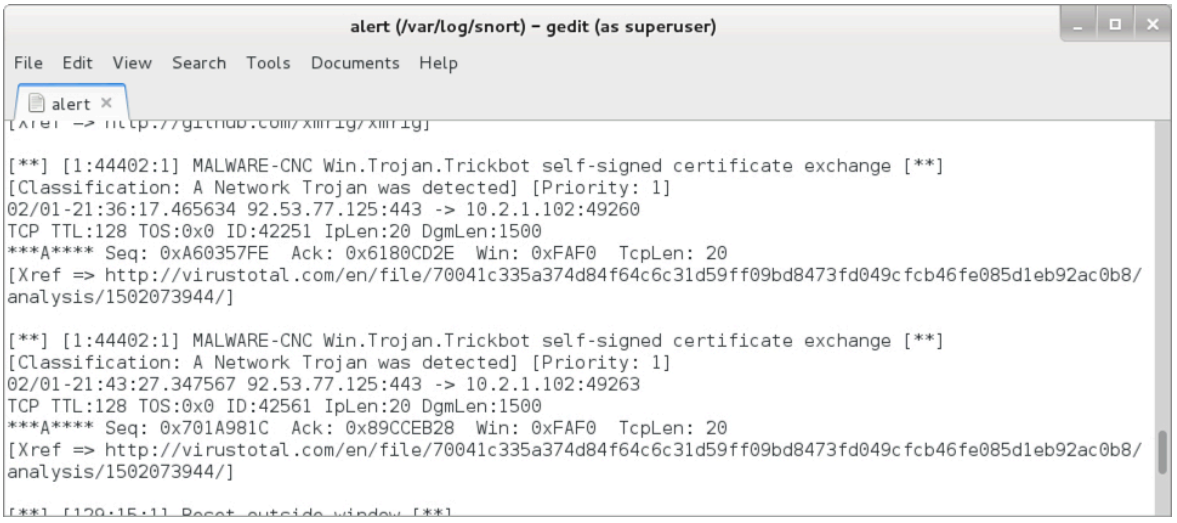
TRICKBOT TRAFFIC

Trickbot network traffic in February 2018 is similar to what I saw 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.

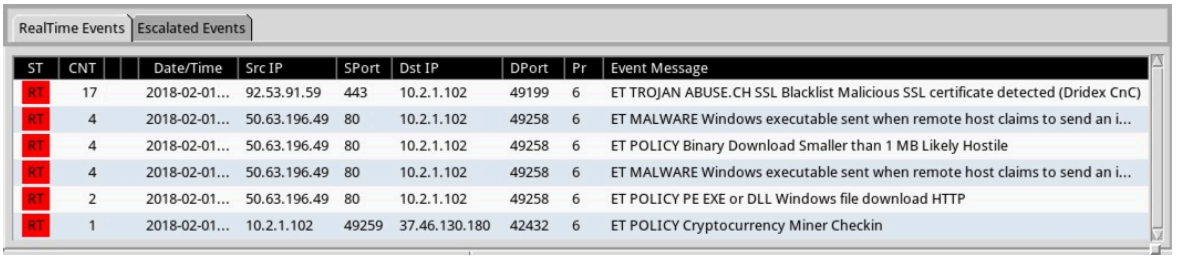


Shown above: Trickbot traffic (from the Trickbot binary) on 2018-02-01.

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.



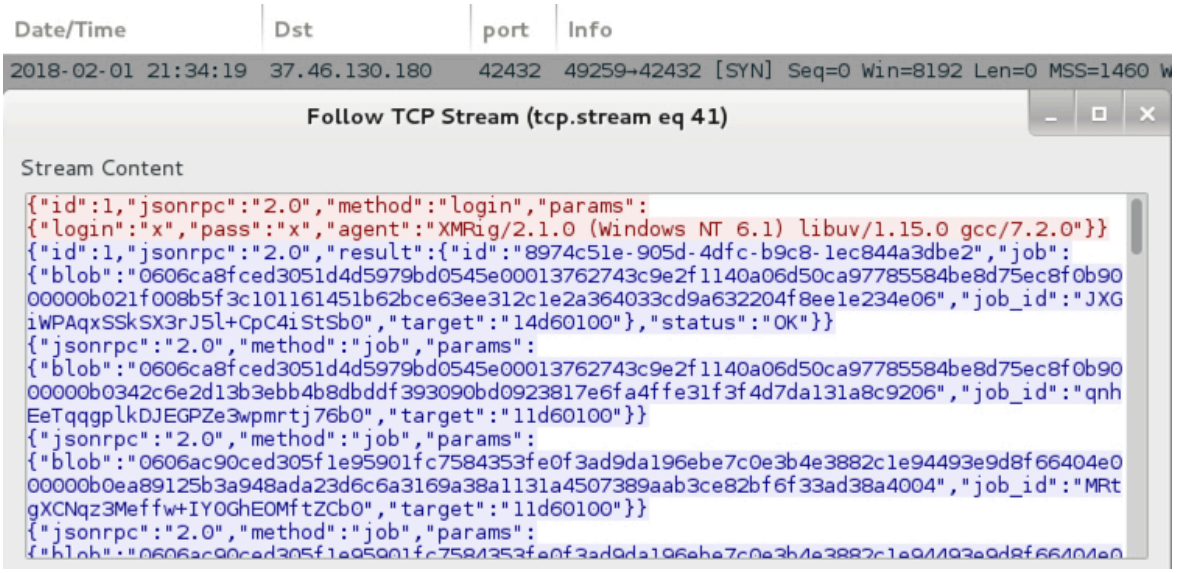
Shown above: Snort alerts on Trickbot certificates in SSL traffic.



RealTime Events | Escalated Events

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

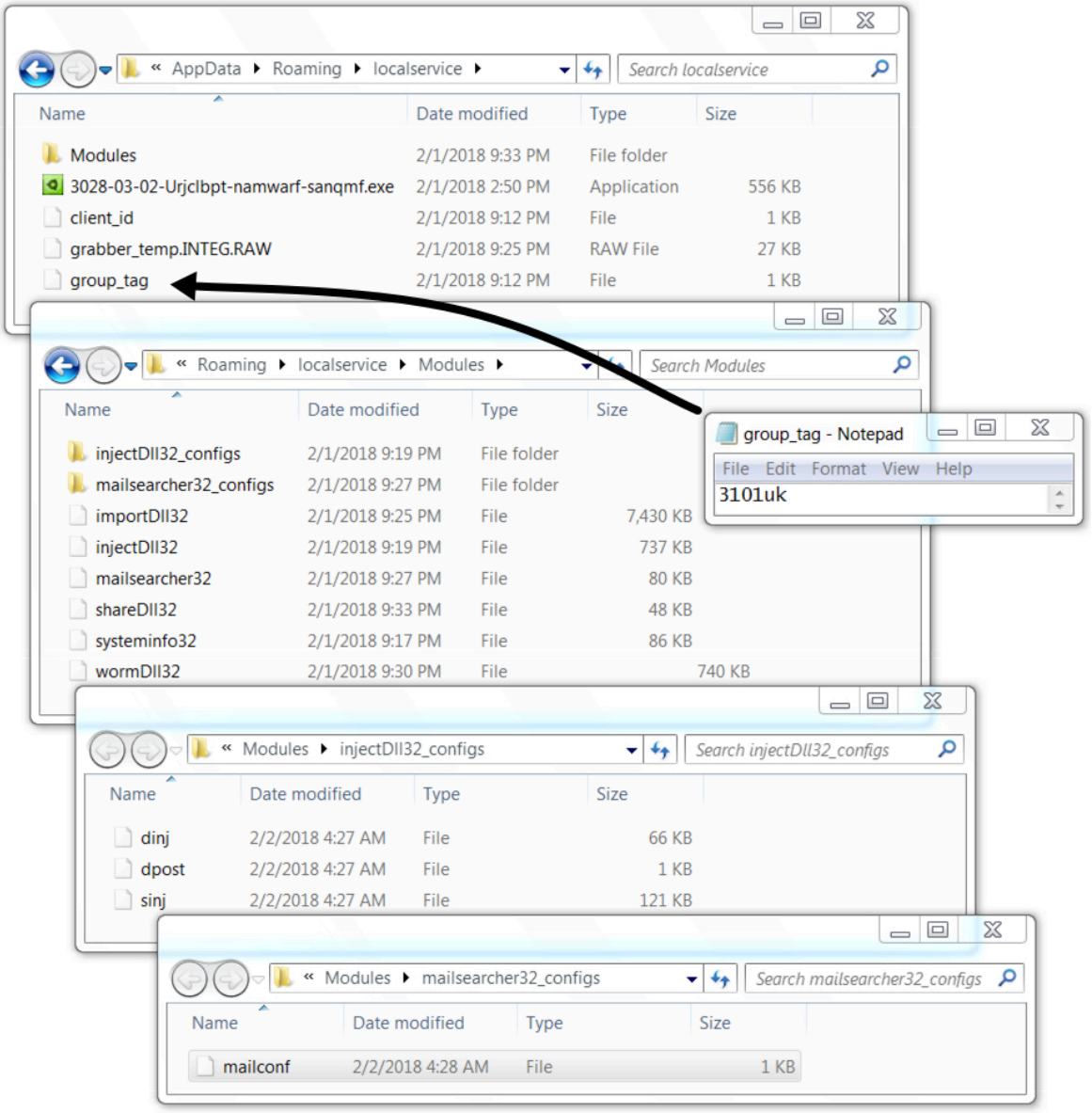
Shown above: Emerging Threats alerts on the infection traffic from Sguil using Suricata on Security Onion.



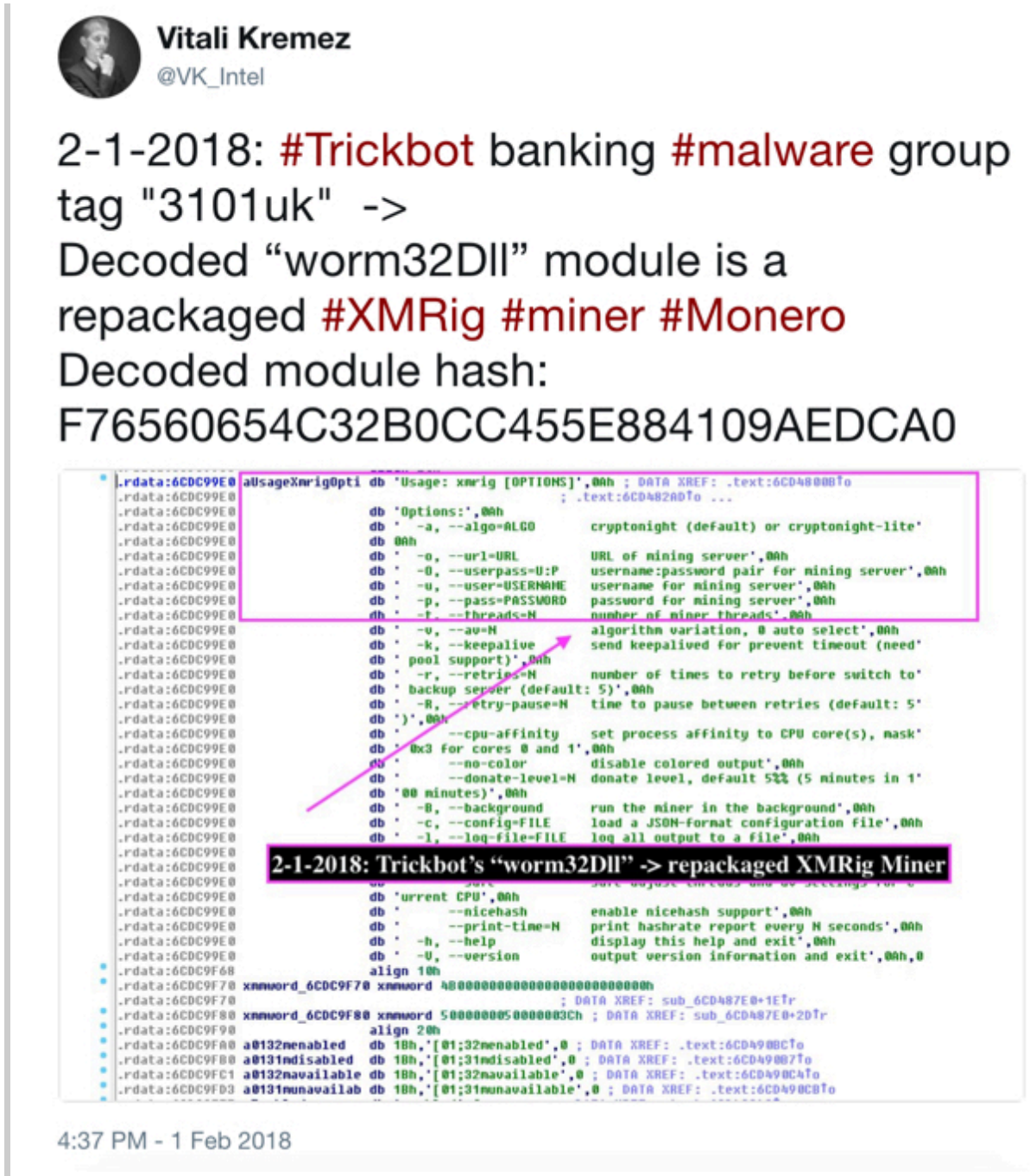
Shown above: Post-infection traffic caused by malware based on Monero (XMRig) coin miner.

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.



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.

Click here to return to the main page.

Source: http://www.malware-traffic-analysis.net/2018/02/01/