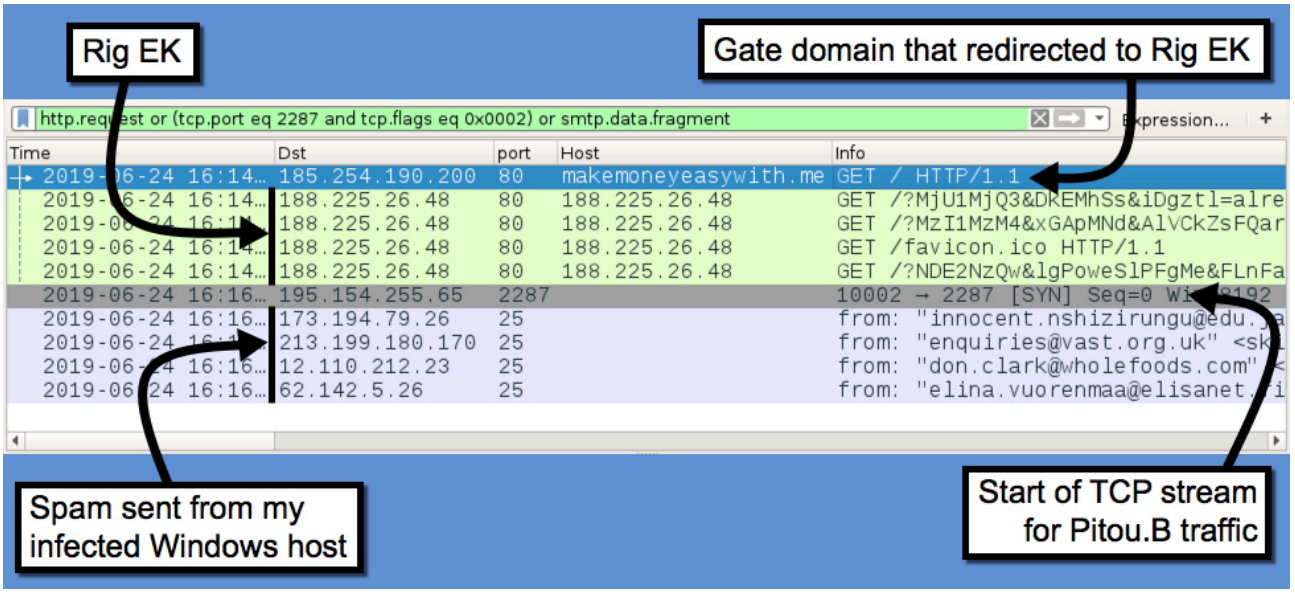
Rig Exploit Kit sends Pitou.B Trojan - SANS ISC

By SANS Internet Storm Center

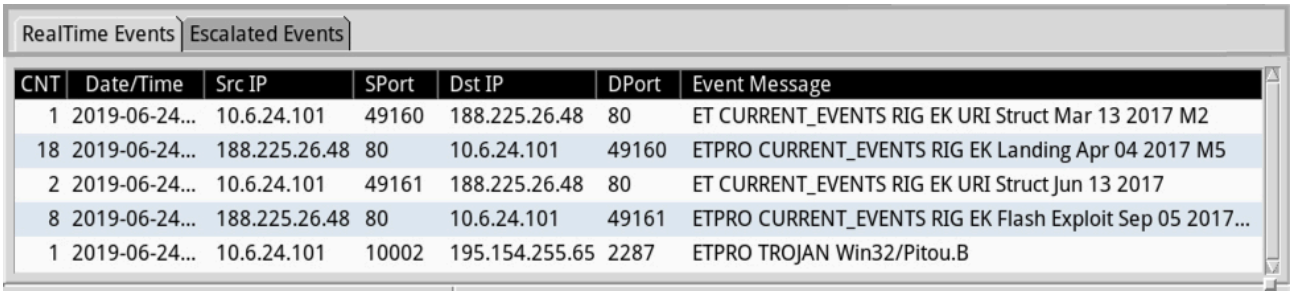
Archived: 2026-04-05 19:51:04 UTC

Introduction

As I mentioned last week, Rig exploit kit (EK) is one of a handful of EKs still active in the wild. Today's diary examines another recent example of an infection caused by Rig EK on Monday 2019-06-24.



Shown above: Traffic from the infection filtered in Wireshark.



CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Event Message
1	2019-06-24...	10.6.24.101	49160	188.225.26.48	80	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
18	2019-06-24...	188.225.26.48	80	10.6.24.101	49160	ETPRO CURRENT_EVENTS RIG EK Landing Apr 04 2017 M5
2	2019-06-24...	10.6.24.101	49161	188.225.26.48	80	ET CURRENT_EVENTS RIG EK URI Struct Jun 13 2017
8	2019-06-24...	188.225.26.48	80	10.6.24.101	49161	ETPRO CURRENT_EVENTS RIG EK Flash Exploit Sep 05 2017...
1	2019-06-24...	10.6.24.101	10002	195.154.255.65	2287	ETPRO TROJAN Win32/Pitou.B

Shown above: Some of the alerts generated by this infection using Security Onion with Suricata and the EmergingThreats Pro ruleset viewed in Sguil.

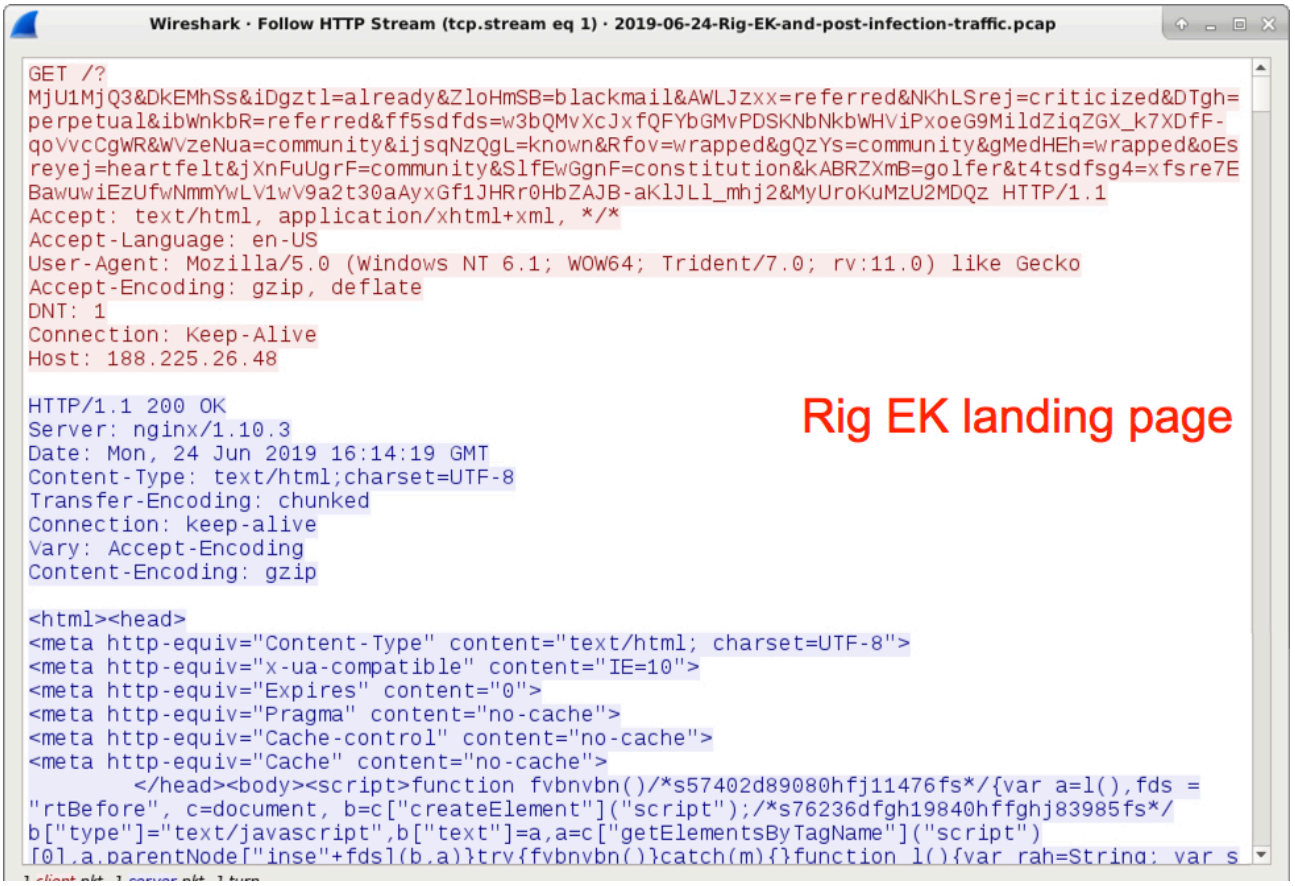
Malvertising campaign redirect domain

EK-based malvertising campaigns have "gate" domains that redirect to an EK. In this case, the gate domain was makemoneyeasywith[.]me. According to Domaintools, this domain was registered on 2019-06-19, and indicators of this domain redirecting to Rig EK were reported as early as 2019-06-21.

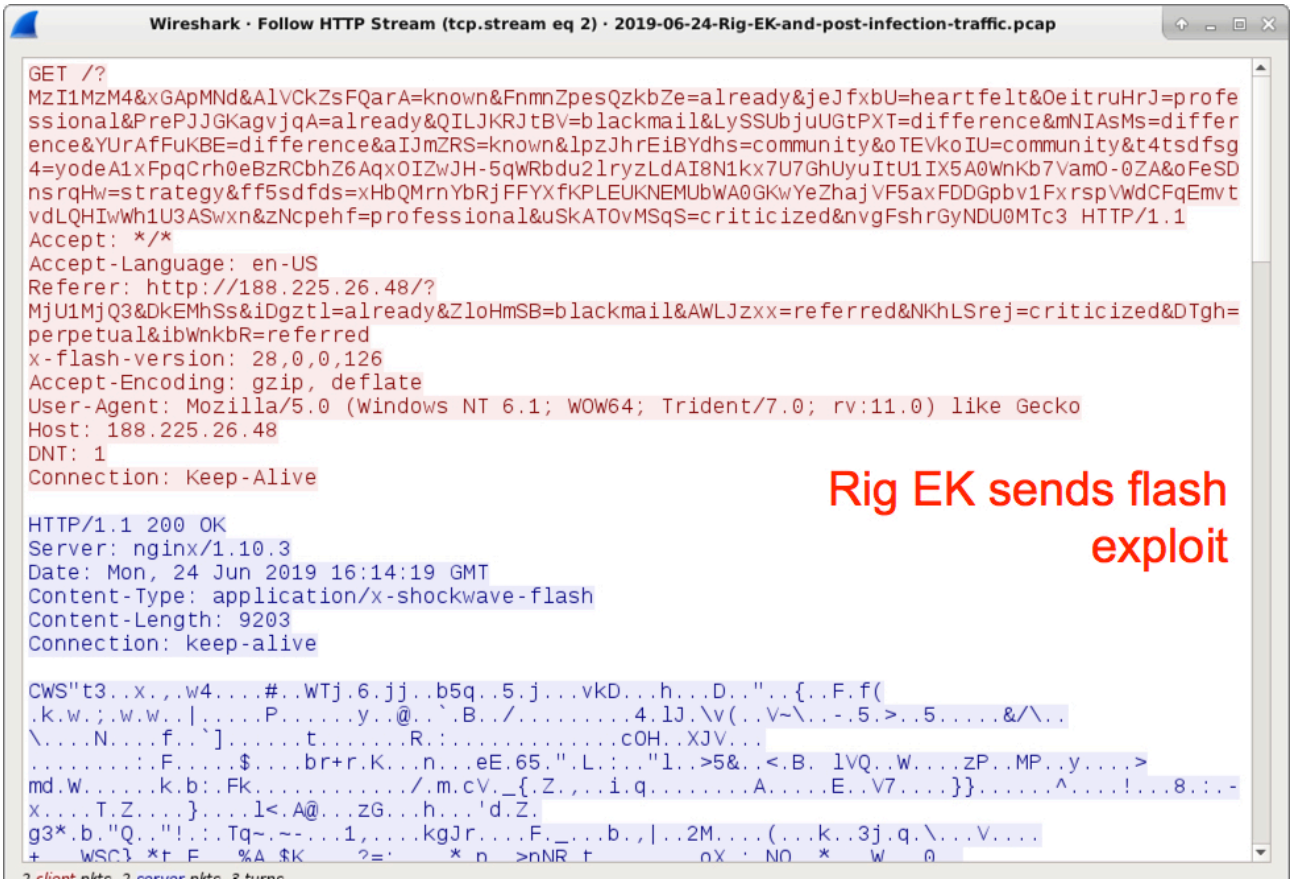
Shown above: makemoneyeasywith[.]me redirecting to Rig EK landing page on 2019-06-24.

Rig EK

The Rig EK activity I saw on 2019-06-24 was similar to Rig EK traffic I documented in an ISC diary last week. See the images below for details.



Shown above: Rig EK landing page.



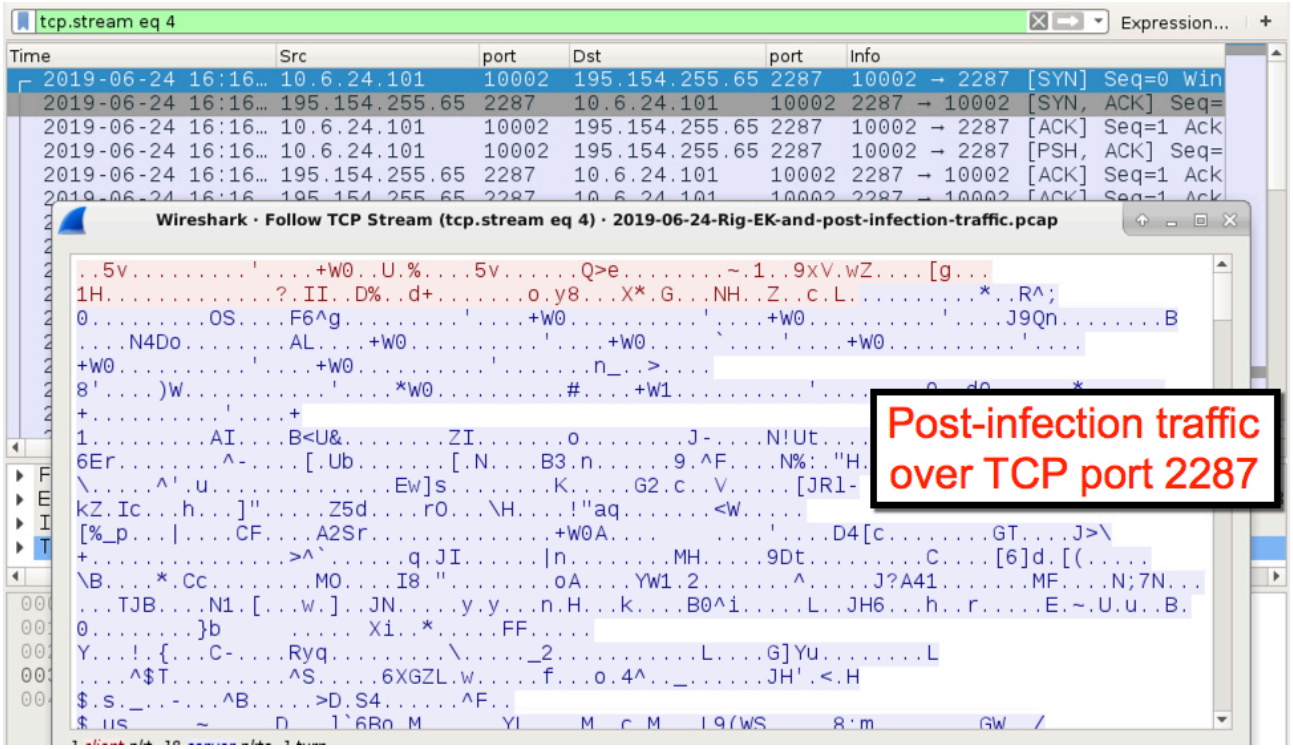
Shown above: Rig EK sends a Flash exploit.

Shown above: Rig EK sends a malware payload.

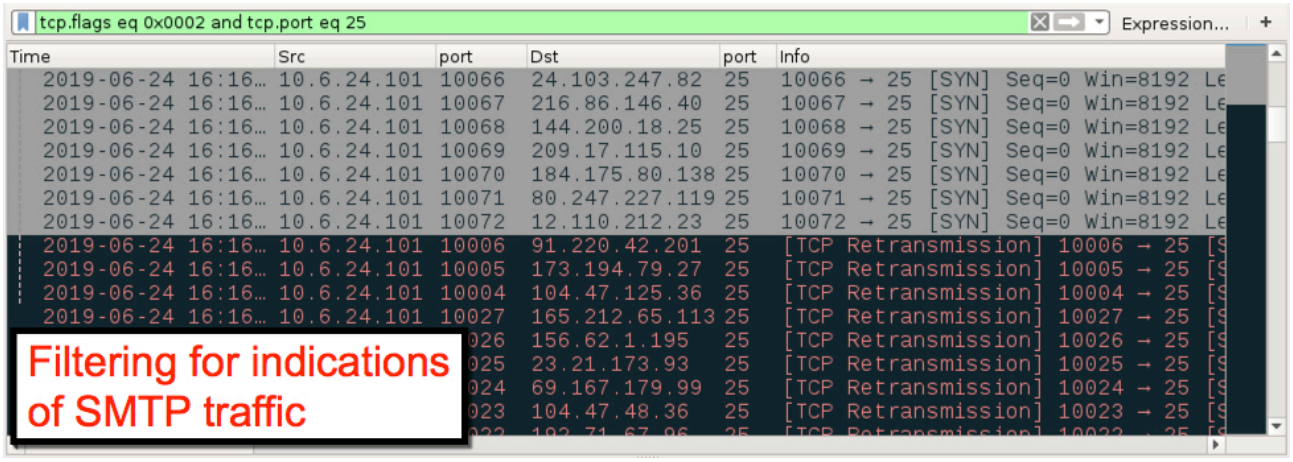
The malware payload

The malware payload sent by this example of Rig EK appears to be Pitou.B. In my post-infection activity, I saw several attempts at malspam, but I didn't find DNS queries for any of the mail servers associated with this spam traffic.

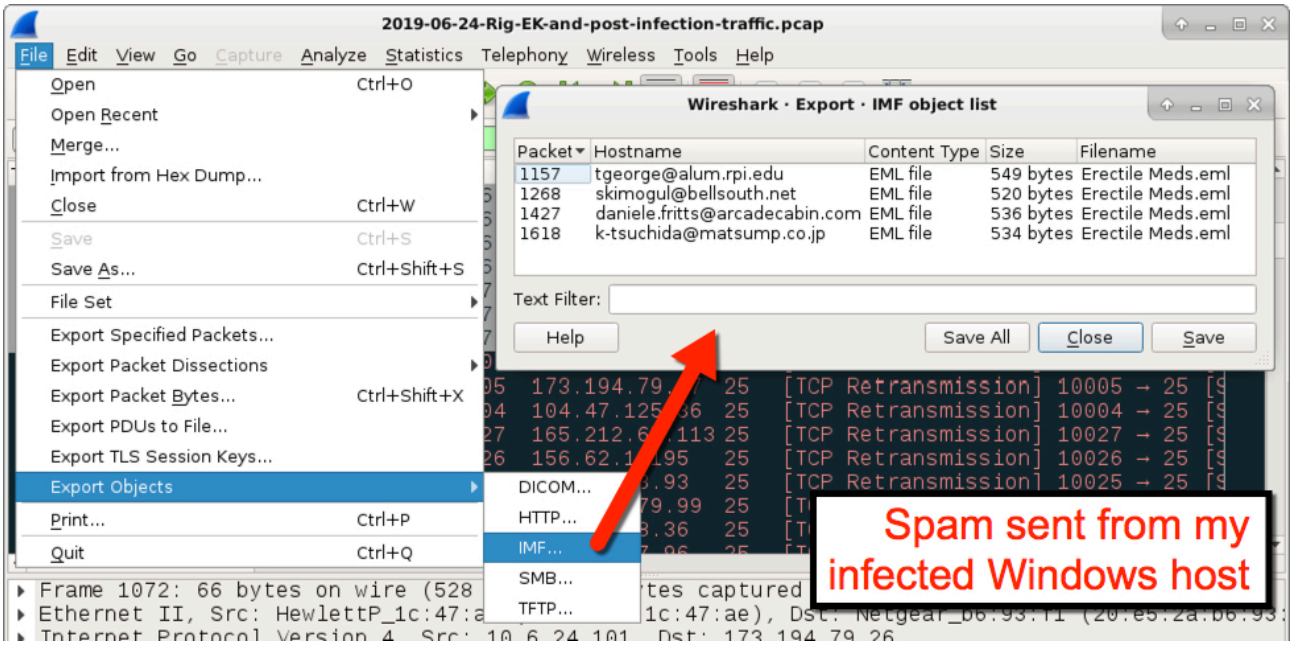
Prior to the spam activity, I saw traffic over TCP port 2287 which matched a signature for ETPRO TROJAN Win32/Pitou.B, and it also fit the description for Pitou.B provided by Symantec from 2016. I didn't let my infected Windows host run long enough to generate DNS queries for remote locations described in Symantec's Technical Description for this Trojan. However, Any.Run's sandbox analysis of this malware shows DNS queries similar to the Symantec description that happened approximately 9 to 10 minutes after the initial infection activity.



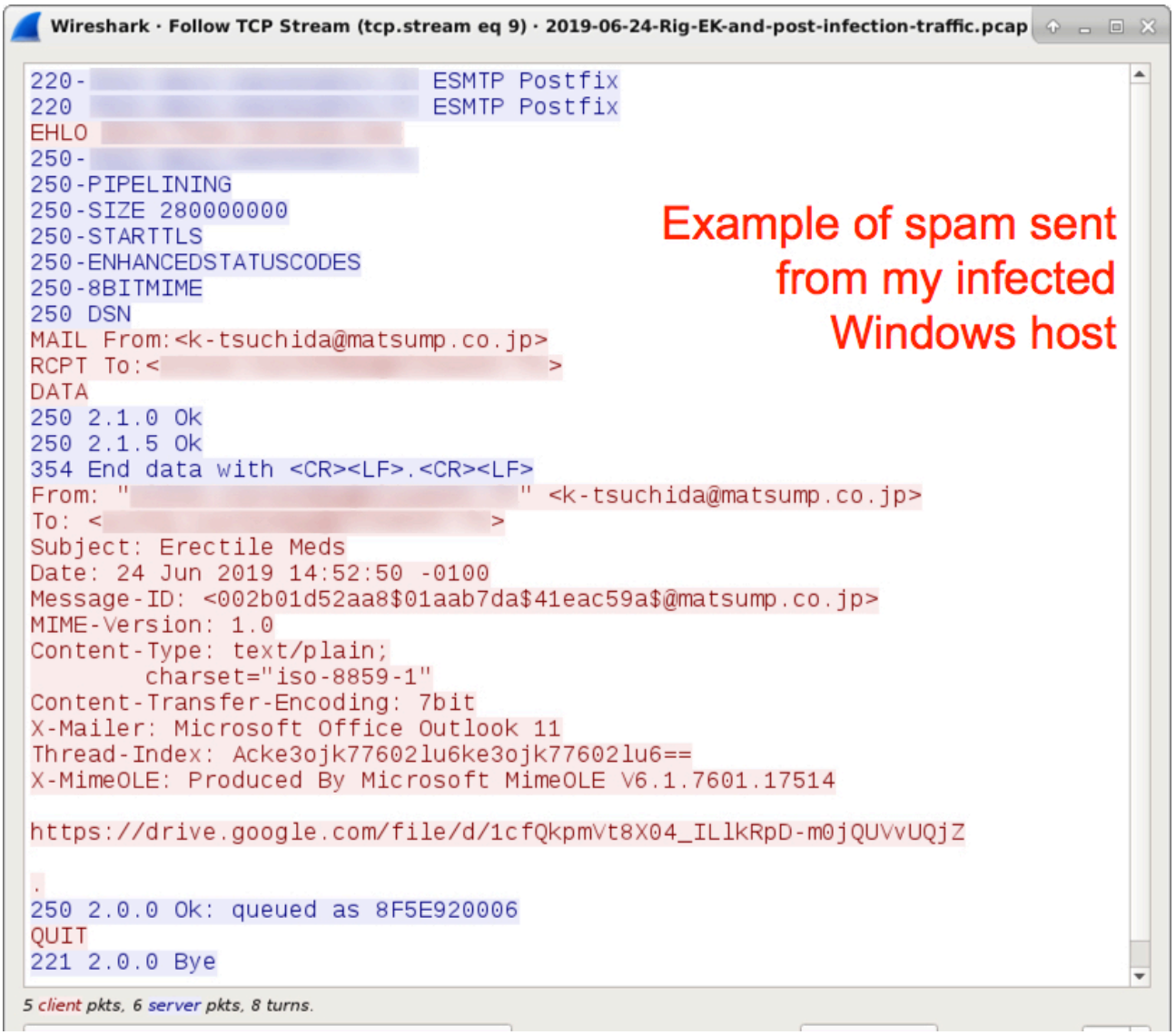
Shown above: Post-infection traffic over TCP port 2287.



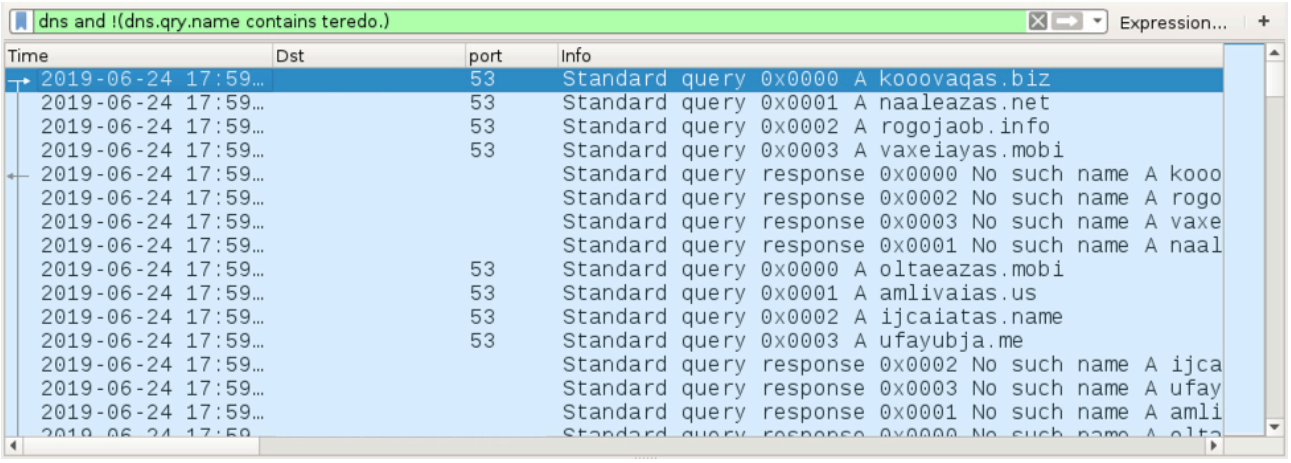
Shown above: Filtering for indications of SMTP traffic in the pcap.



*Shown above: Using the **Export Objects** function in Wireshark to see successfully sent spam.*



Shown above: An example of spam sent from my infected Windows host.



Shown above: DNS queries seen from the [Any.Run analysis of this Pitou.B sample](#).

Indicators of Compromise (IoCs)

The following are IP addresses and domains associated with this infection:

- 185.254.190[.]200 port 80 - ***makemoneyeasywith[.]me*** - Gate domain that redirected to Rig EK
- 188.225.26[.]48 port 80 - ***188.225.26[.]48*** - Rig EK traffic
- 195.154.255[.]65 port 2287 - Encoded/encrypted traffic caused by the Pitou.B Trojan
- various IP addresses over TCP port 25 - spam traffic from the infected Windows host
- various domains in DNS queries seen from the Any.Run analysis of this Pitou.B sample

The following are files associated with this infection:

SHA256 hash: 9c569f5e6dc2dd3cf1618588f8937513669b967f52b3c19993237c4aa4ac58ea

- File size: 9,203 bytes
- File description: Flash exploit sent by Rig EK on 2019-06-24

SHA256 hash: 835873504fdaa37c7a6a2df33828a3dcfc95ef0a2ee7d2a078194fd23d37cf64

- File size: 827,904 bytes
- File description: Pitou.B malware sent by Rig EK on 2019-06-24

Final words

A pcap of the infection traffic along with the associated malware and artifacts can be found here.

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