Anonymizing VPN Services as a Botnet Monetization Strategy

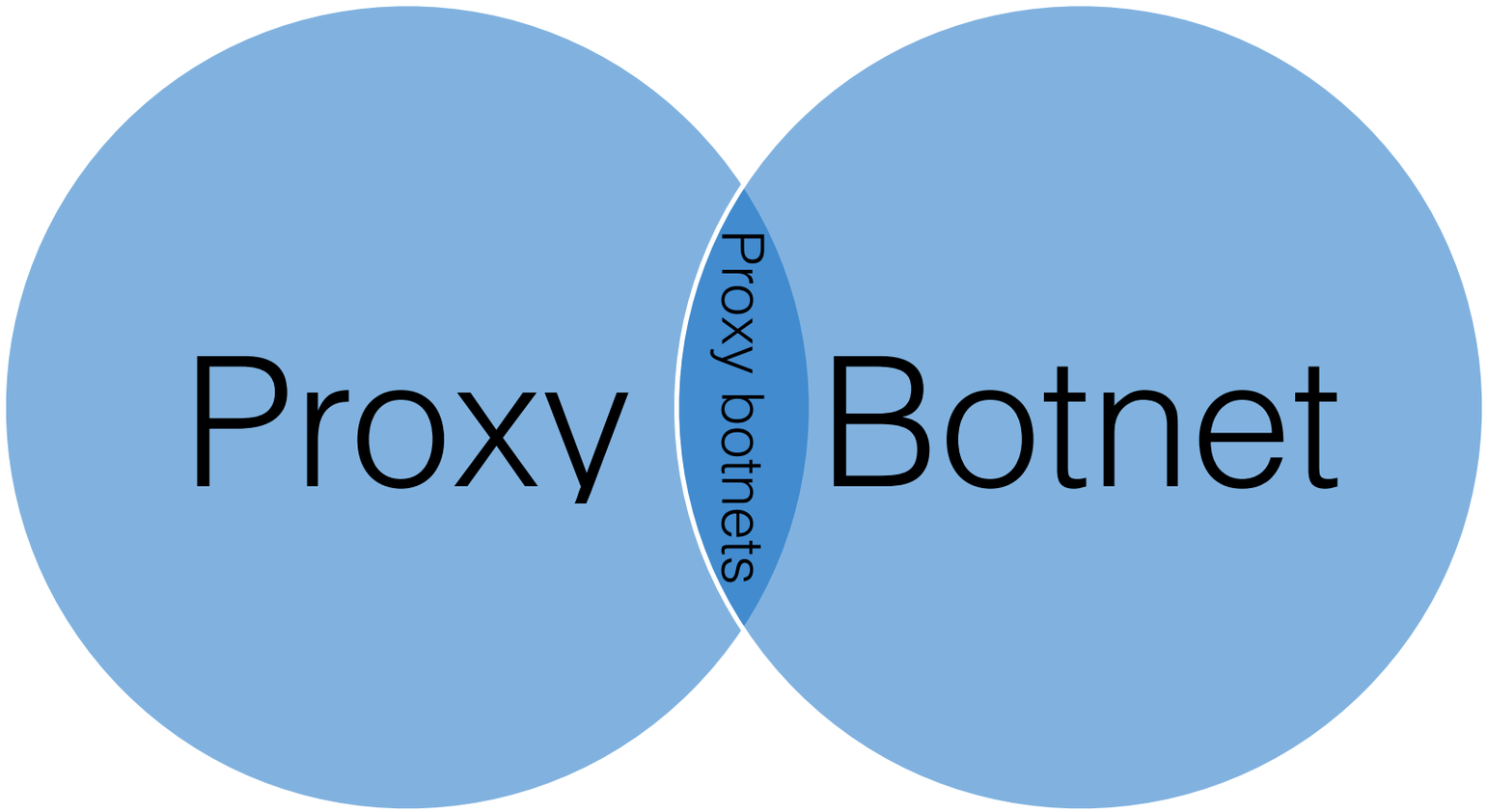
Analyzing The Bunitu Botnet

Researchers

Hasherezade (@hasherezade), **Malwarebytes**

Sergei Frankoff (@herrcore), **Sentrant**

What is a Proxy Botnet

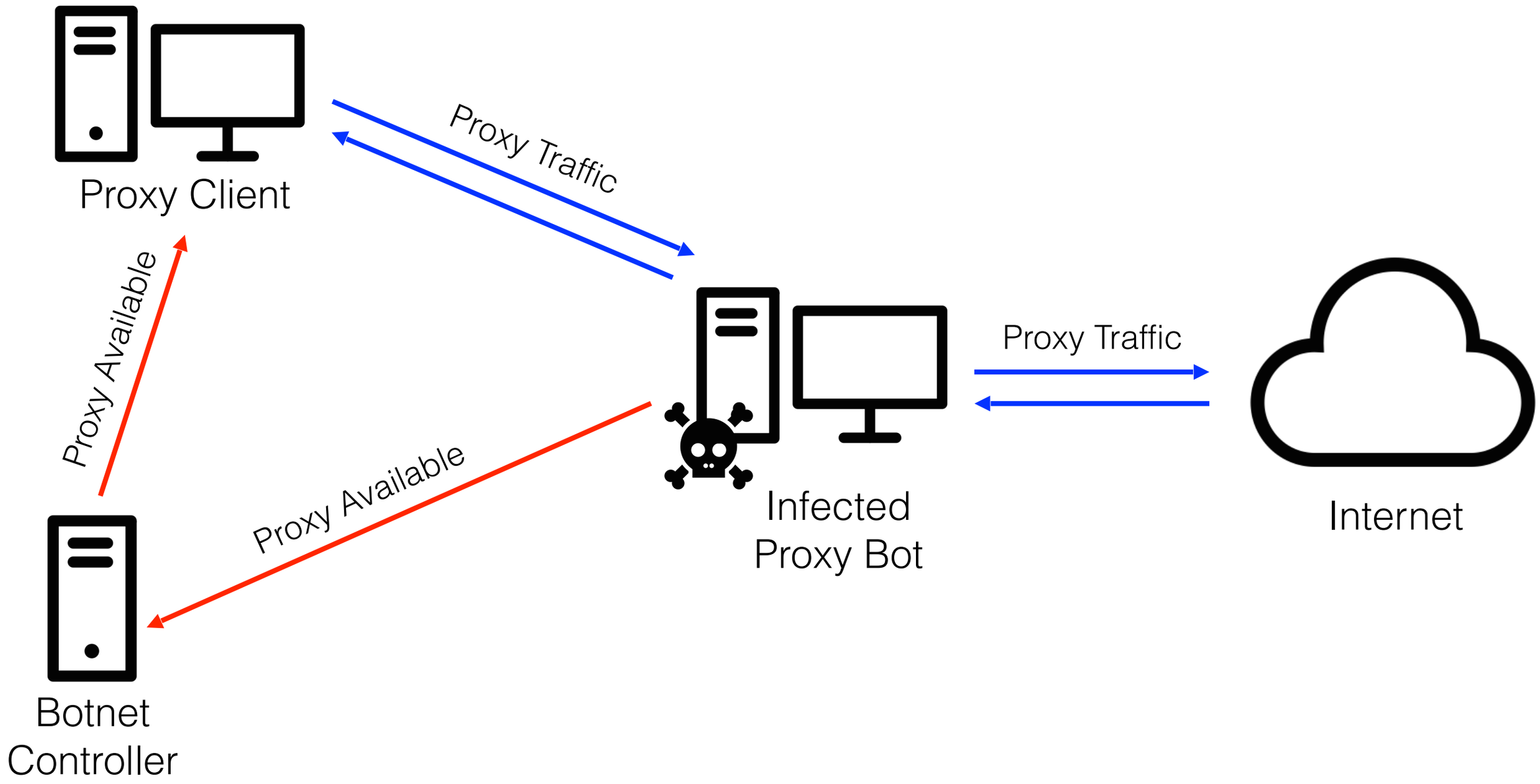


- Used to bypass the traffic
- Covers up the IP of the user
- Network of infected computers
- Used for cybercrime

Sentrant
Digital Advertising Integrity

Malwarebytes

What is a Proxy Botnet



Sentrant
Digital Advertising Integrity

Malwarebytes

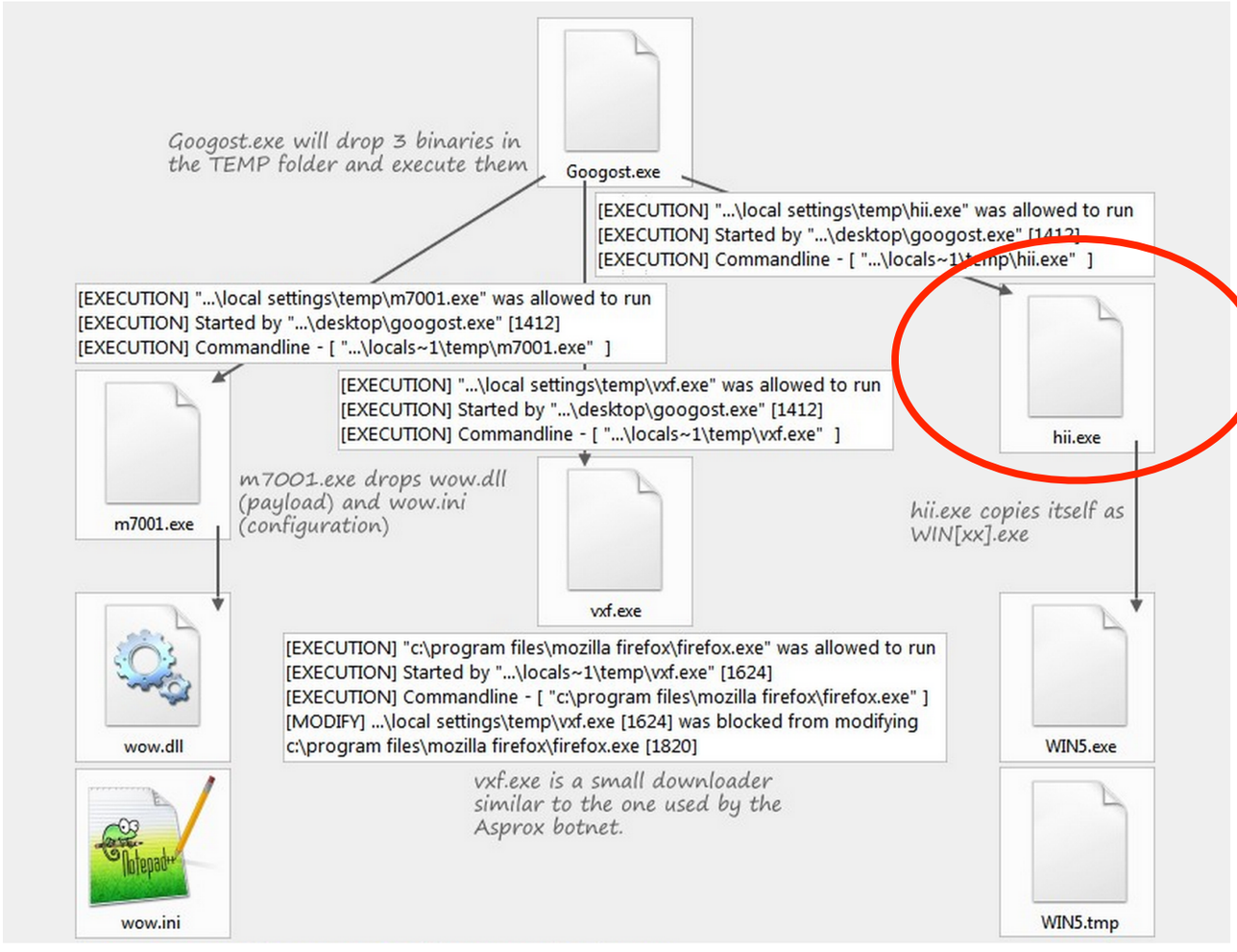
Monetizing Proxy Botnets

- Advertising Fraud
- Re-packaged and sold as VPN/Proxy service

Sentrant
Digital Advertising Integrity

Malwarebytes

Prior Work: Monetization Via Ad-Fraud



stopmalvertising.com (March, 2014) - hii ad-fraud proxy

Prior Work: Monetization Via Ad-Fraud

```
00000000  09 00 19 2e 69 3d d8 00  50 04 5e 17 29 d6 67 35  ....i=.. P.^.).g5
00000010  36 64 65 63 35 39 36 61  65 62 32 38              6dec596a eb28
```

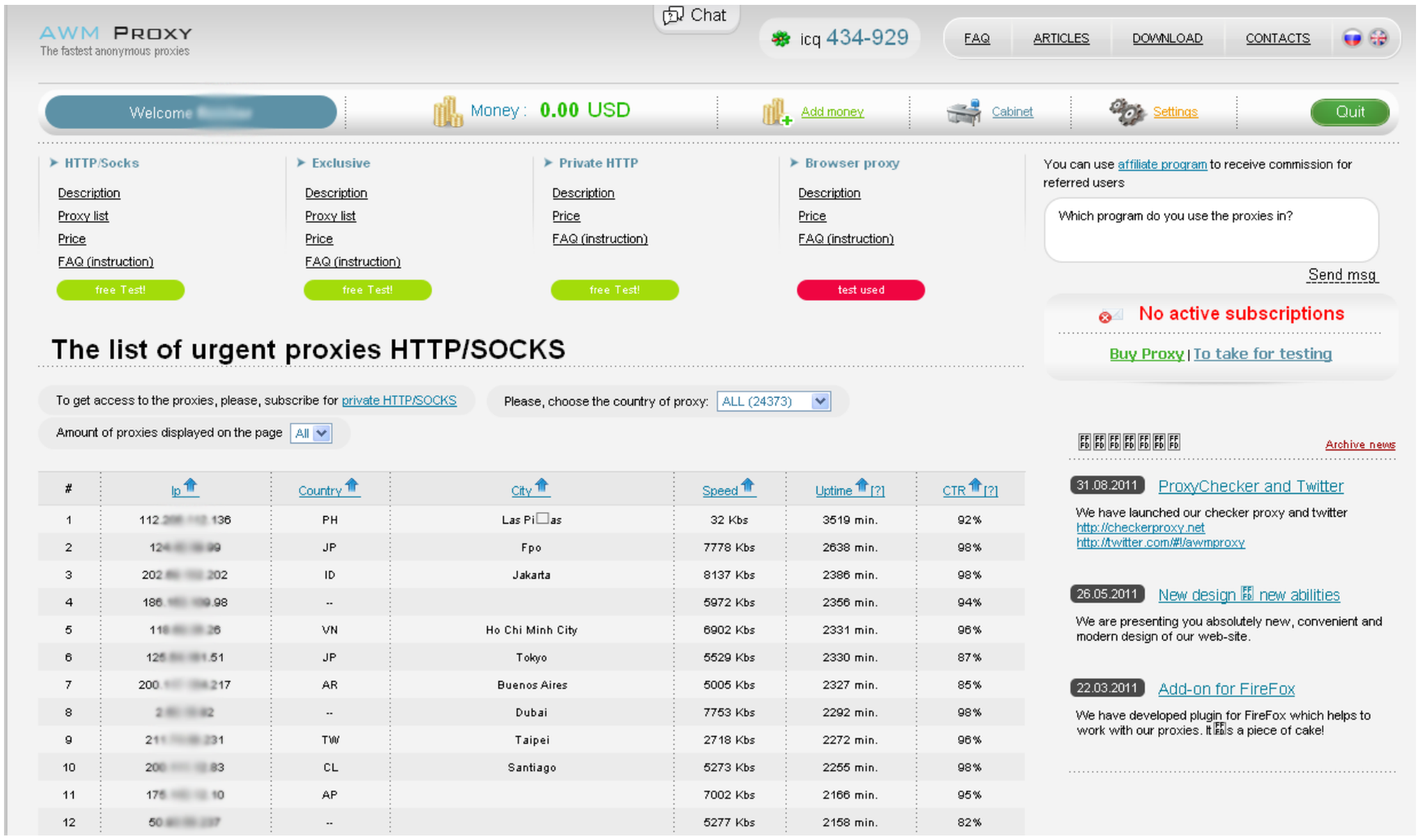
Proxy command = 09
Argument length = 00 19 = 25
Proxy IP = 2e 69 3d d8 = 46.105.61.216
Proxy port = 00 50 = 80
IP address type = 04 = IPv4
Destination IP = 5e 17 29 d6 = 94.23.41.214
Destination port = 67 35 = 26421
Proxy key = 36 64 65 63 35 39 36 61 65 62 32 38

hii ad-fraud proxy registration protocol

Sentrant
Digital Advertising Integrity

Malwarebytes

Prior Work: Monetization Via Proxy Sales



#	Ip	Country	City	Speed	Uptime [?]	CTR [?]
1	112.[redacted].136	PH	Las Pi□as	32 Kbs	3519 min.	92%
2	124.[redacted].89	JP	Fpo	7778 Kbs	2638 min.	98%
3	202.[redacted].202	ID	Jakarta	8137 Kbs	2386 min.	98%
4	186.[redacted].98	--		5972 Kbs	2356 min.	94%
5	118.[redacted].26	VN	Ho Chi Minh City	6902 Kbs	2331 min.	96%
6	125.[redacted].51	JP	Tokyo	5529 Kbs	2330 min.	87%
7	200.[redacted].217	AR	Buenos Aires	5005 Kbs	2327 min.	85%
8	2.[redacted].92	--	Dubai	7753 Kbs	2292 min.	98%
9	211.[redacted].231	TW	Taipei	2718 Kbs	2272 min.	96%
10	200.[redacted].83	CL	Santiago	5273 Kbs	2255 min.	98%
11	175.[redacted].10	AP		7002 Kbs	2166 min.	95%
12	50.[redacted].237	--		5277 Kbs	2158 min.	82%

Kaspersky Research (June 27, 2011) - TDSS Proxy For Hire

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu

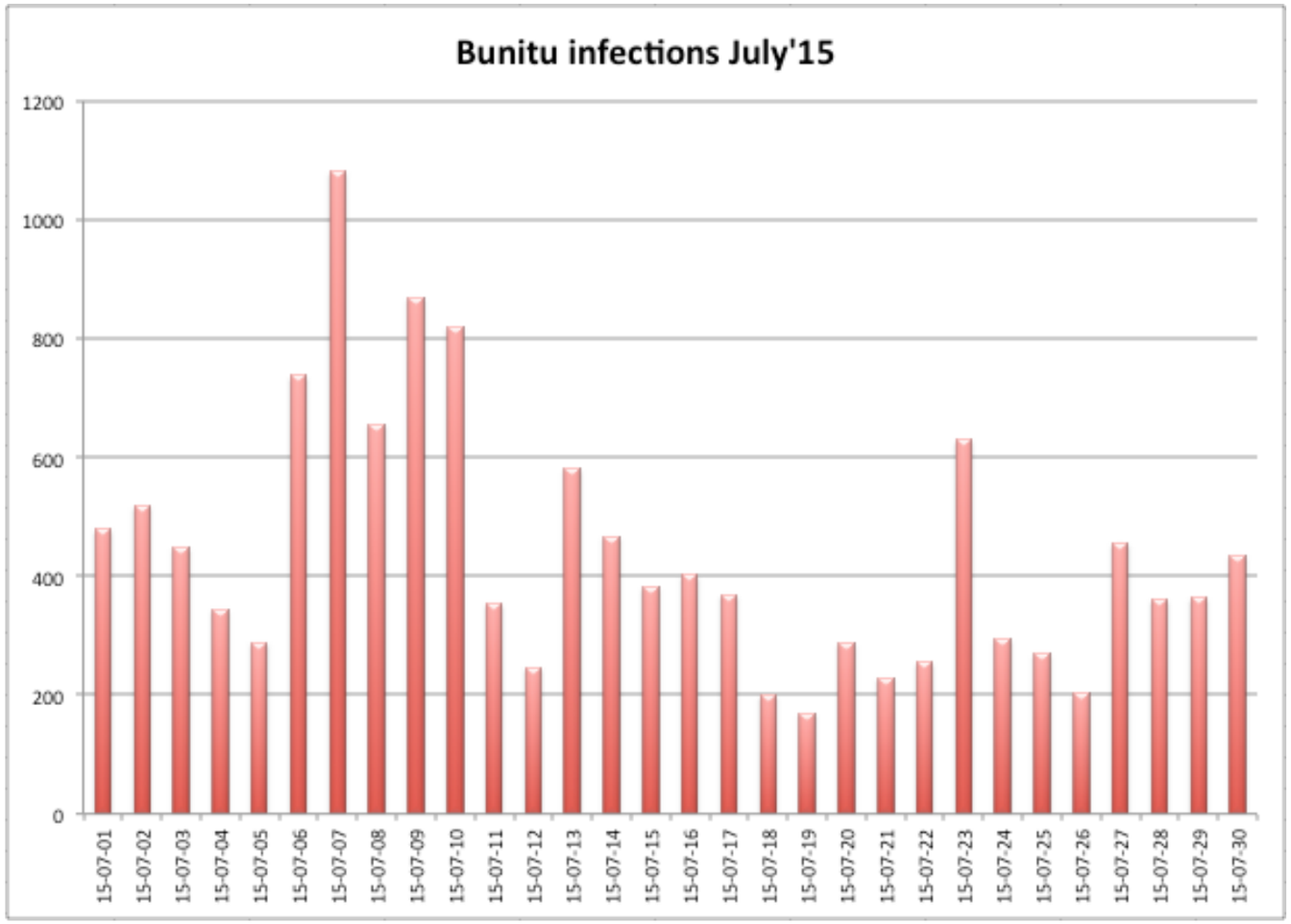
~~Ad fraud~~

Proxy botnet

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Overview



2013-12-25 : b0a91e1f91078bad48252edc989e868e : mlicnai.dll

...

2015-09-16 : 85ae39ee4fed066797fed137fc1fc332 : naukgol.dll

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Proxy Services

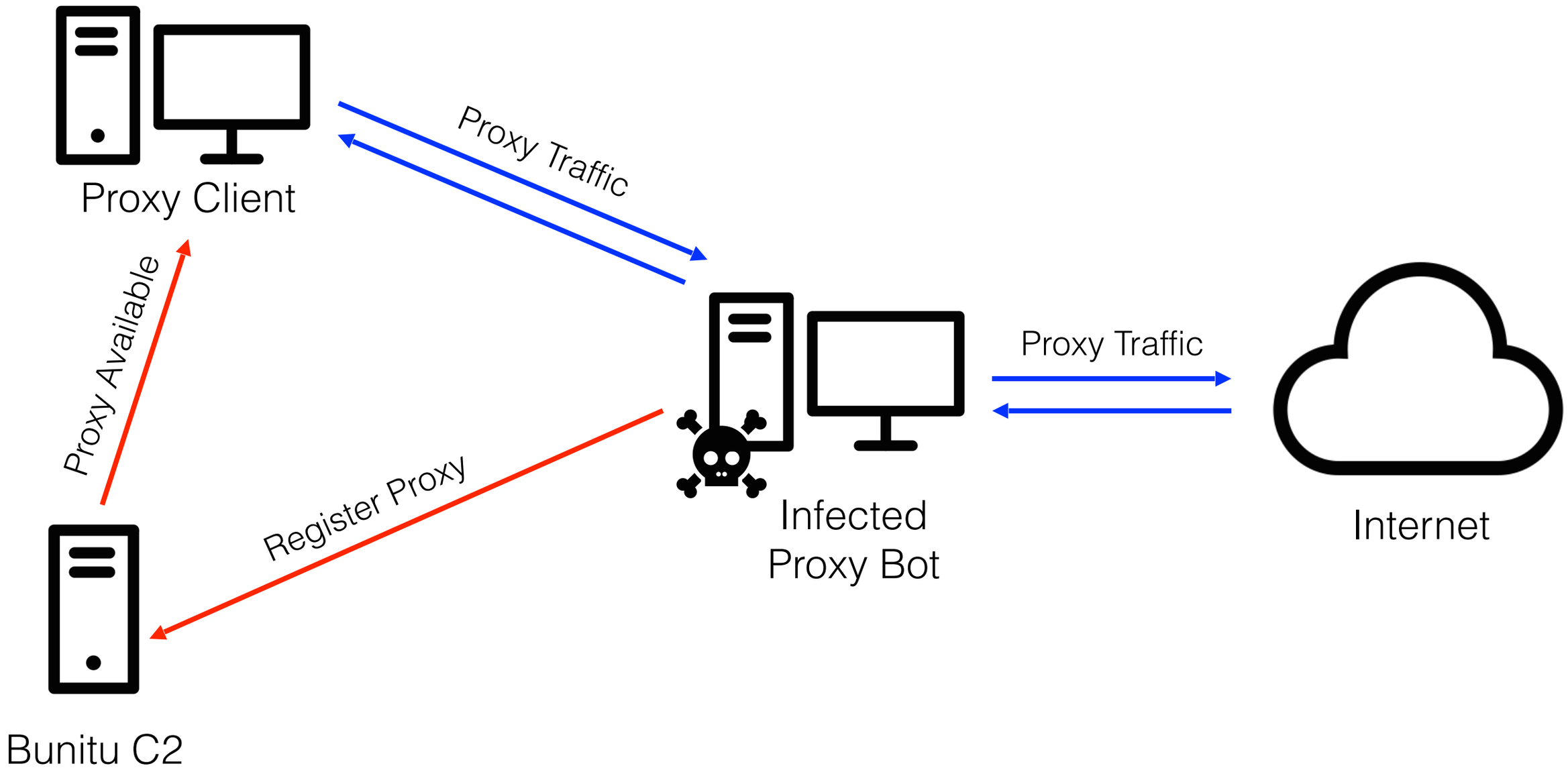
Two types of proxy: Standard and Tunnel

rundll32.exe	628	TCP	0.0.0.0	17133	0.0.0.0	0	LISTENING
rundll32.exe	628	TCP	0.0.0.0	17369	0.0.0.0	0	LISTENING
rundll32.exe	628	TCP	10.0.2.15	49164	95.211.178.145	53	ESTABLISHED

- Standard HTTP proxy and SOCKS proxy services are started by Bunitu on random high ports, client registers them to C&C#1

- Tunnel is operated via C&C#2 – uses it's own protocol to wrap and bypass the traffic

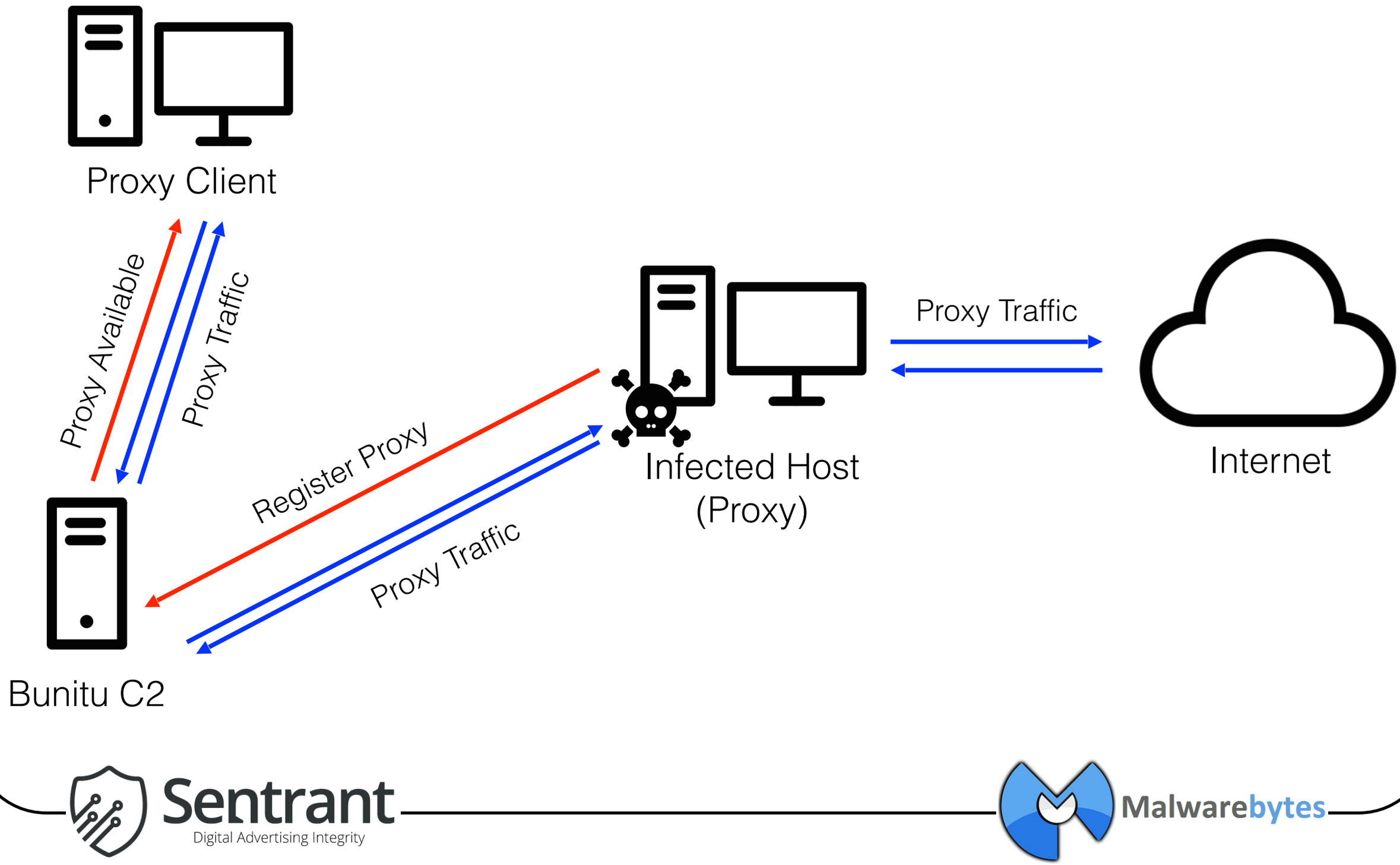
Bunitu Standard Proxy



Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Tunneled Proxy

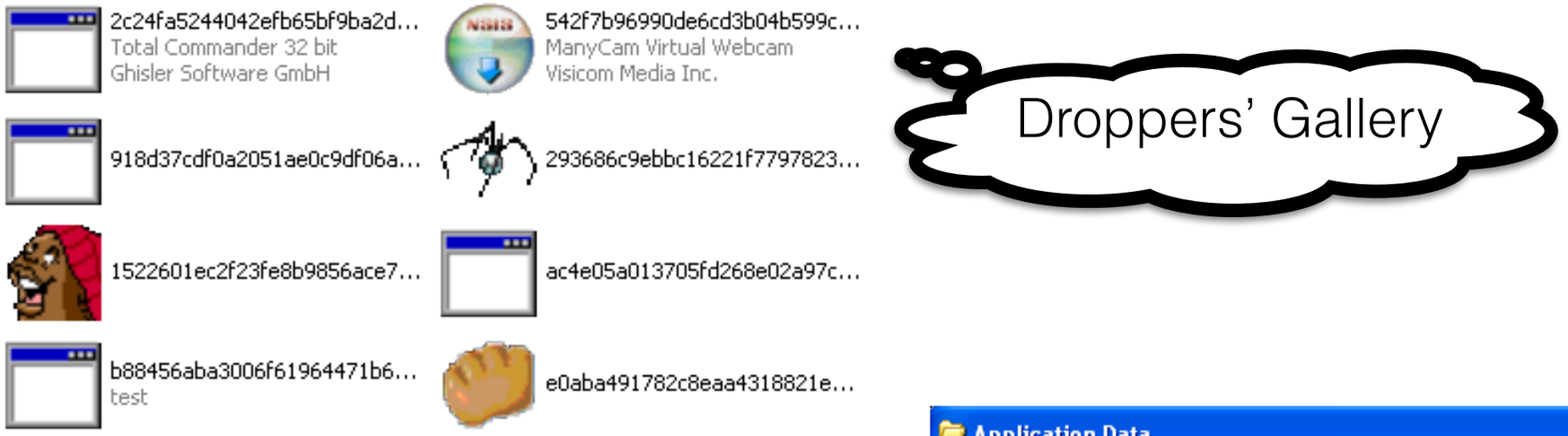


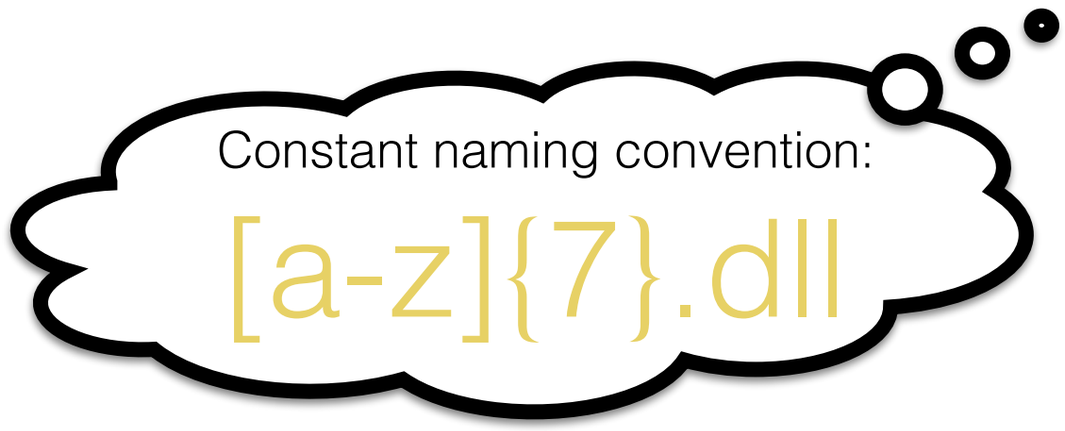
Sentrant
Digital Advertising Integrity

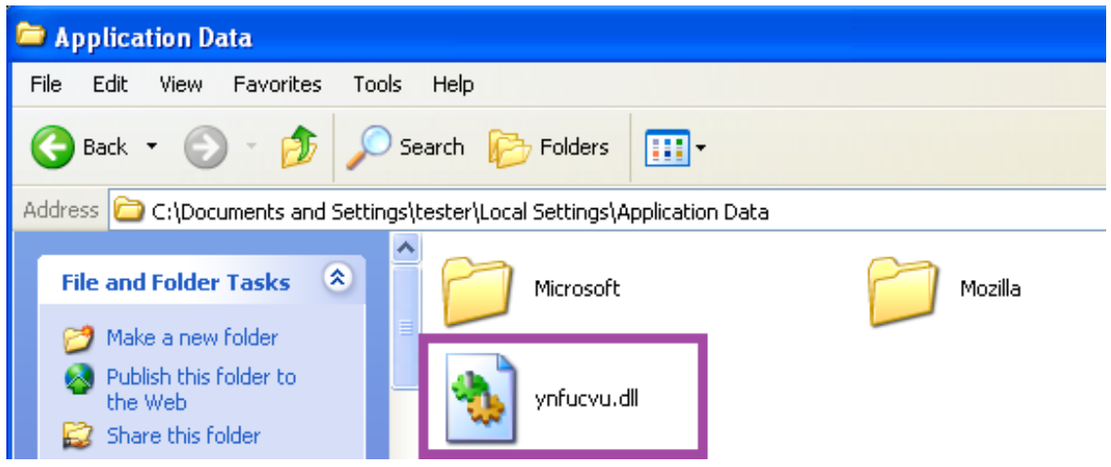
Malwarebytes

Bunitu Trojan overview

Always a DLL installed by dropper





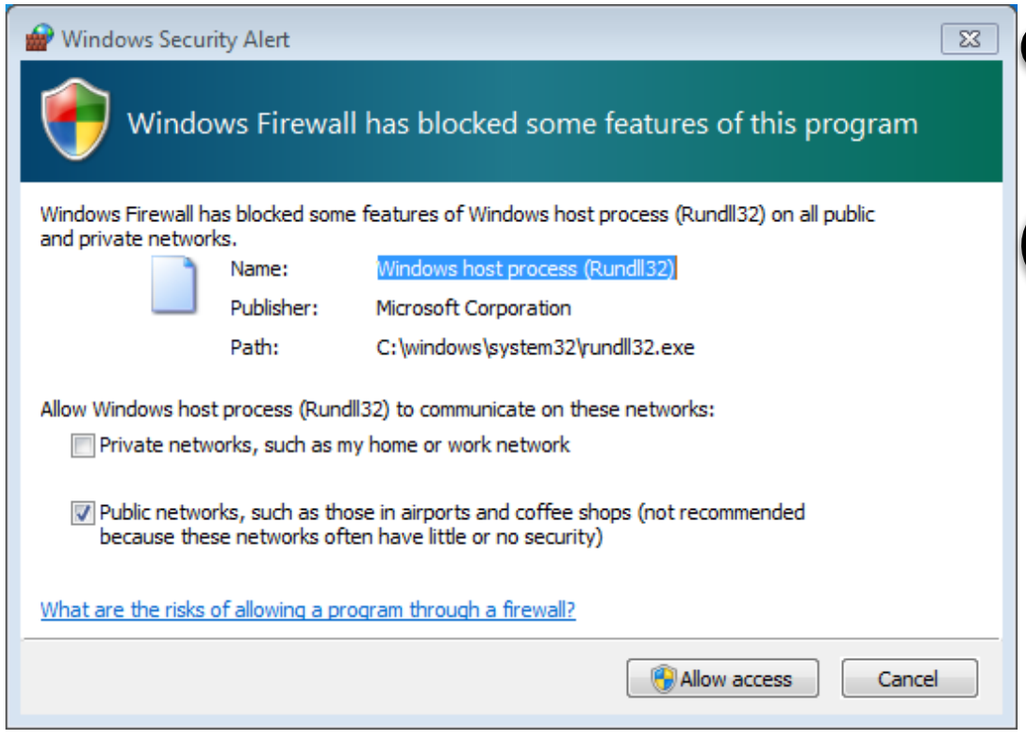


https://github.com/hasherezade/bunitu_tests/wiki/Bunitu-Gallery

Sentrant
Digital Advertising Integrity

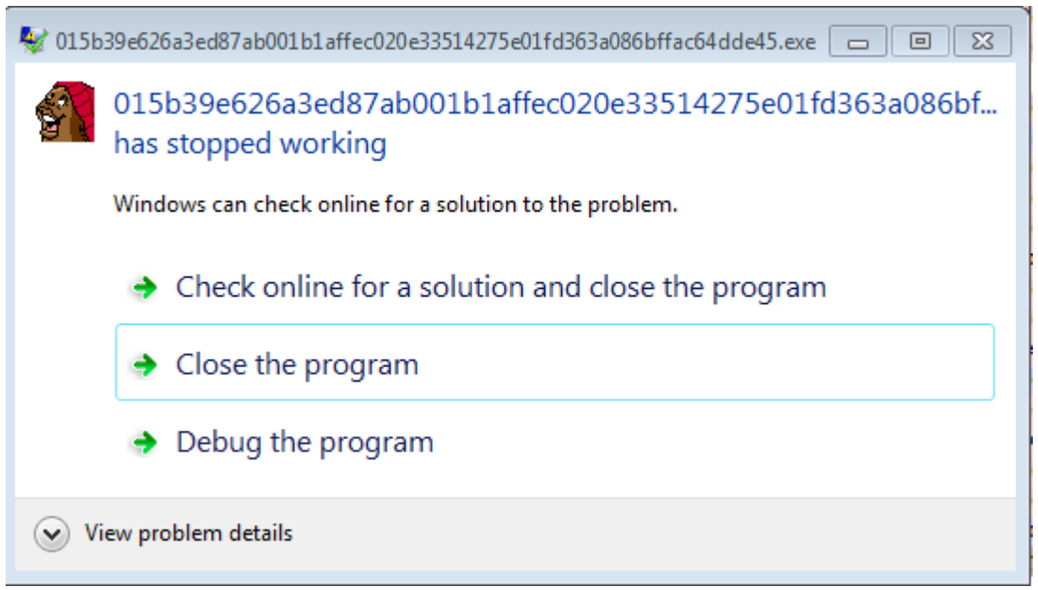
Malwarebytes

Bunitu Installation



The standard proxy services require inbound connections. There is no privilege elevation exploit to silence this.

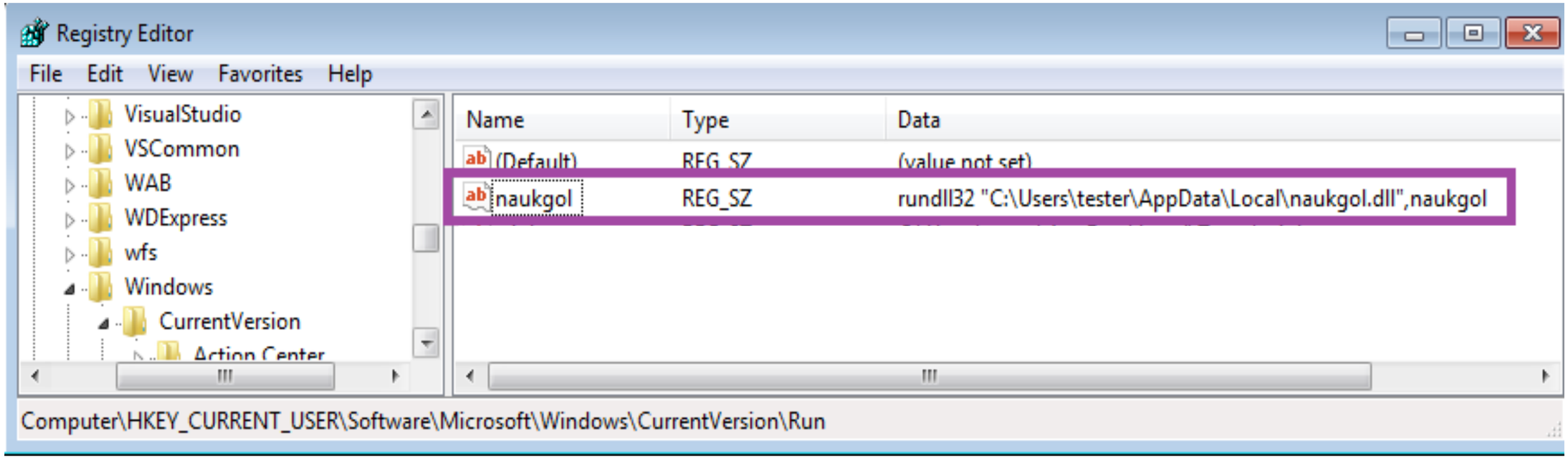
The installer often crashes at the end



Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Host Persistence



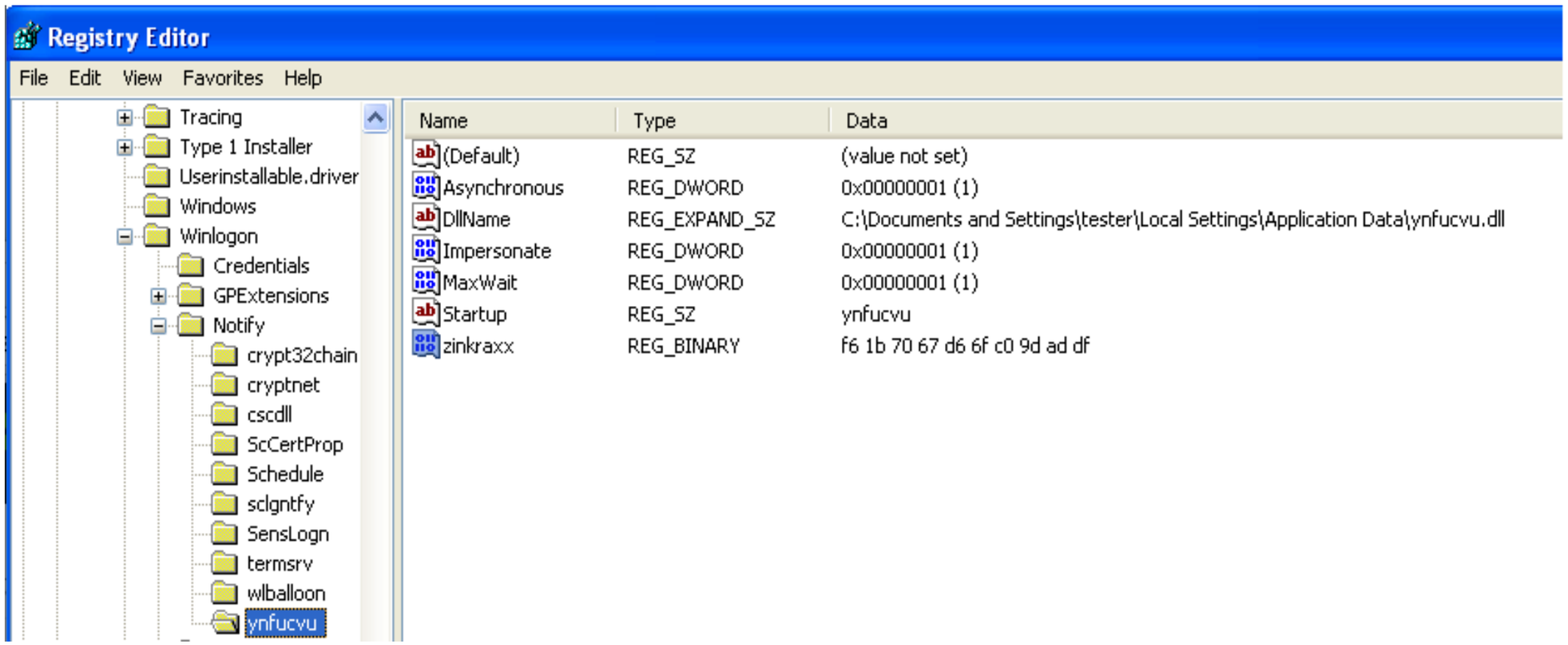
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu BotID

During installation an unique bot ID is generated, and stored in the registry



HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\

BotID = **fb1b7067d66fc09daddf**

Sentrant
Digital Advertising Integrity

Malwarebytes

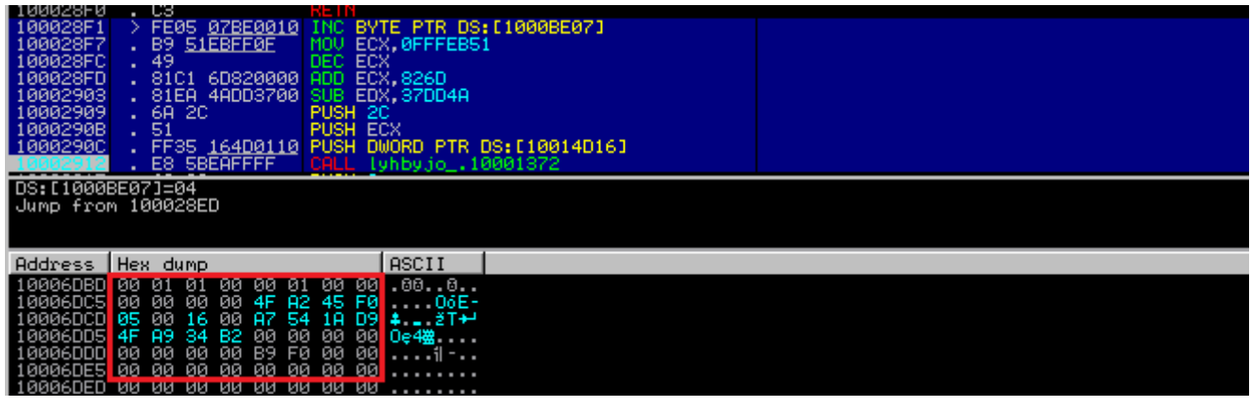
Bunitu C2 Server Domains

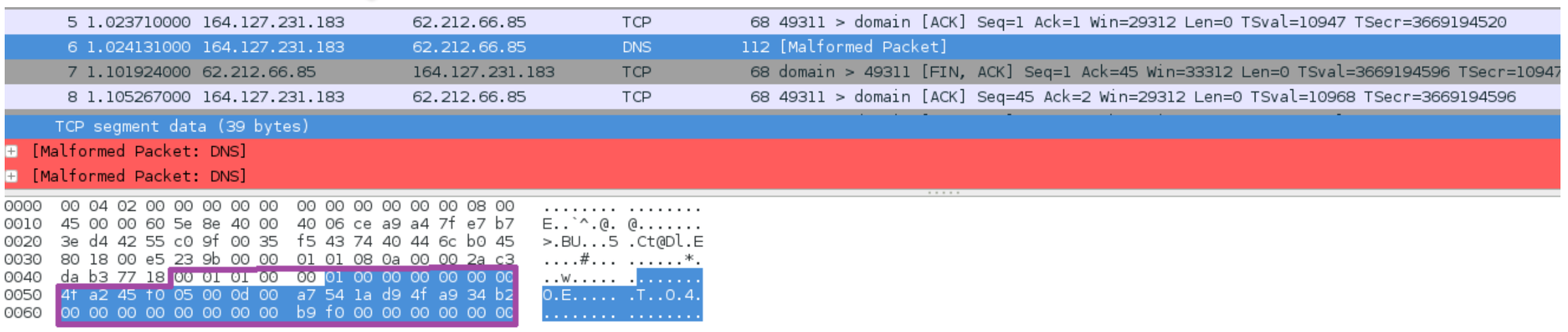
```
if ( arg_flag_get_ip_from_dns )
{
  var_dns_ip = ptr_0_ws2_32_gethostbyname((char *)&unk_7FFE0000 - 1878896220);
  if ( !var_dns_ip )
    goto close_and_clean_up;
  var_real_ip = ***(_DWORD ***)(var_dns_ip + 12) ^ 0x16EC1A31;
}
else
{
  var_real_ip = arg_ip;
}
var_ptr_real_ip = var_real_ip;
var_hardcoded_port_real_ip_struct = 0x35000002;// port 53
```

C2 domains are hard coded in binary.

IPs these domains resolve to must be XOR with key to get real IPs.

Bunitu Standard Proxy Registration Protocol

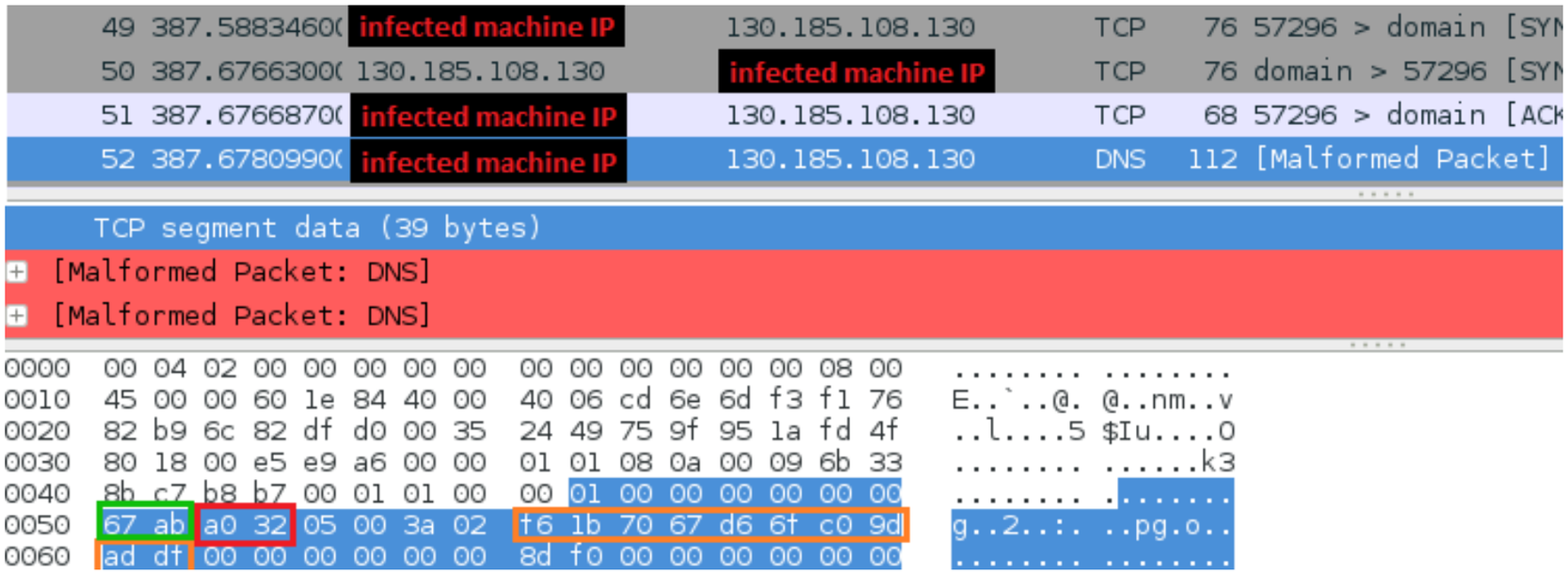




Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Standard Proxy Registration Protocol

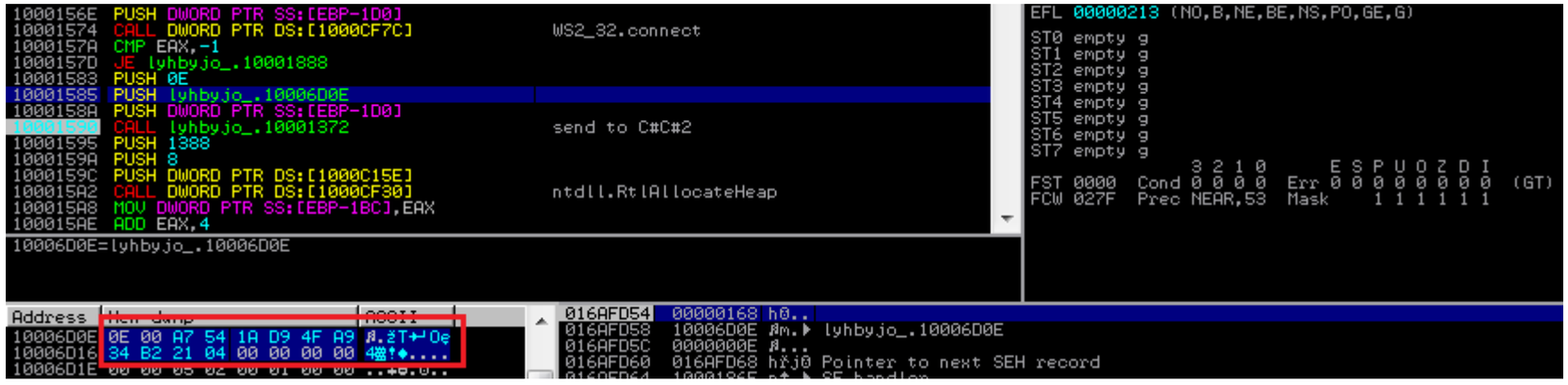


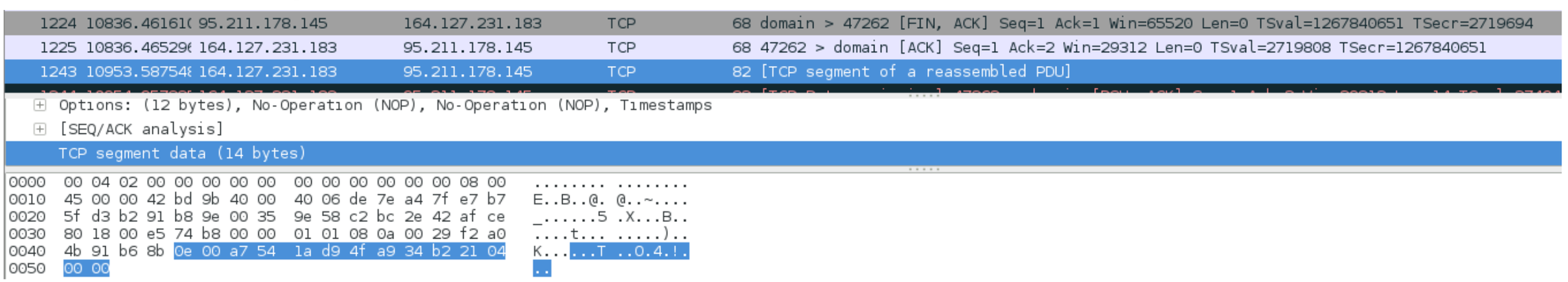
00010100 00010000 00000000 = header (hardcoded)
67 ab = socks proxy port (little endian -> **0xab67** = 43879)
a0 32 = http proxy port (little endian -> **0x32ab** = 12971)
05 00 = hard coded value
3a = minutes since last reboot
02 = hours since last reboot
fb1b7067d66fc09daddf = botID
8d f0 = hard coded unique to each version of the malware

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Tunneled Proxy Protocol

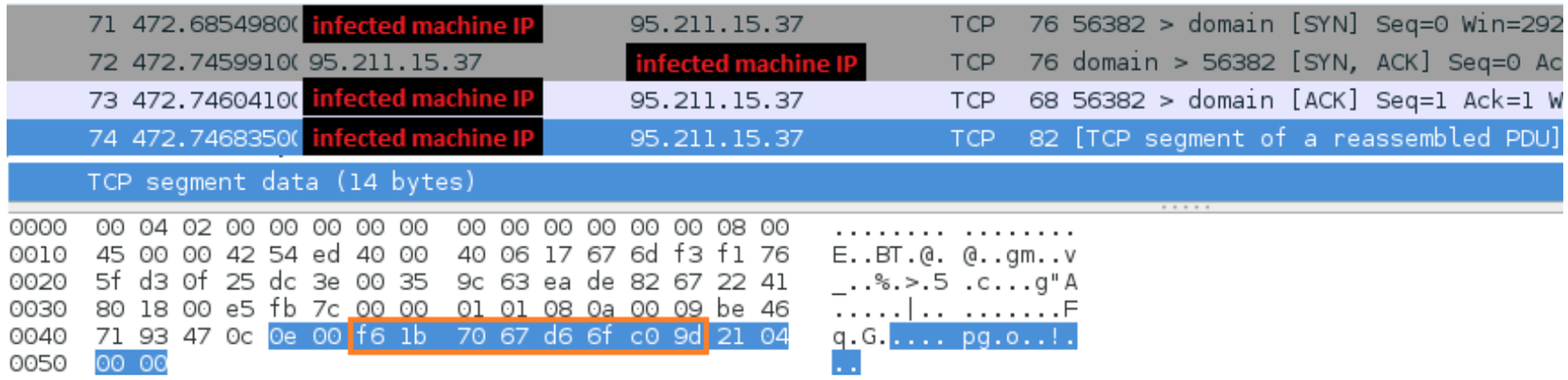




Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Tunneled Proxy Protocol - Registration



0e 00 = Length of the message (little endian) -> 0x00e0 -> 14
fb 1b 70 67 d6 6f c0 9d = bot ID, truncated (without last WORD)
21 04 00 00 = command (0x0421) *start the proxy*

Bunitu Tunneled Proxy Protocol - Initialization

After registration C&C tests a bot by ordering it to query Google

77	799.759486000	95.211.15.37	infected machine IP	TCP 1	118 [TCP segment of a reassembled PDU]
78	799.759557000	infected machine IP	95.211.15.37	TCP	68 49643 > domain [ACK] Seq=15 Ack=51 Win=29312 Le
79	799.763614000	infected machine IP	89.108.202.21	DNS 2	72 Standard query 0xb289 A google.com
80	799.801820000	89.108.202.21	infected machine IP	DNS	88 Standard query response 0xb289 A 216.58.209.78
81	799.803705000	infected machine IP	216.58.209.78	TCP	76 43396 > http [SYN] Seq=0 Win=29200 Len=0 MSS=14
82	799.843613000	216.58.209.78	infected machine IP	TCP	76 http > 43396 [SYN, ACK] Seq=0 Ack=1 Win=42540 L
83	799.843698000	infected machine IP	216.58.209.78	TCP	68 43396 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0
84	799.845141000	infected machine IP	95.211.15.37	TCP 3	105 [TCP segment of a reassembled PDU]
85	799.983446000	95.211.15.37	infected machine IP	TCP 4	105 [TCP segment of a reassembled PDU]

TCP segment data (50 bytes)

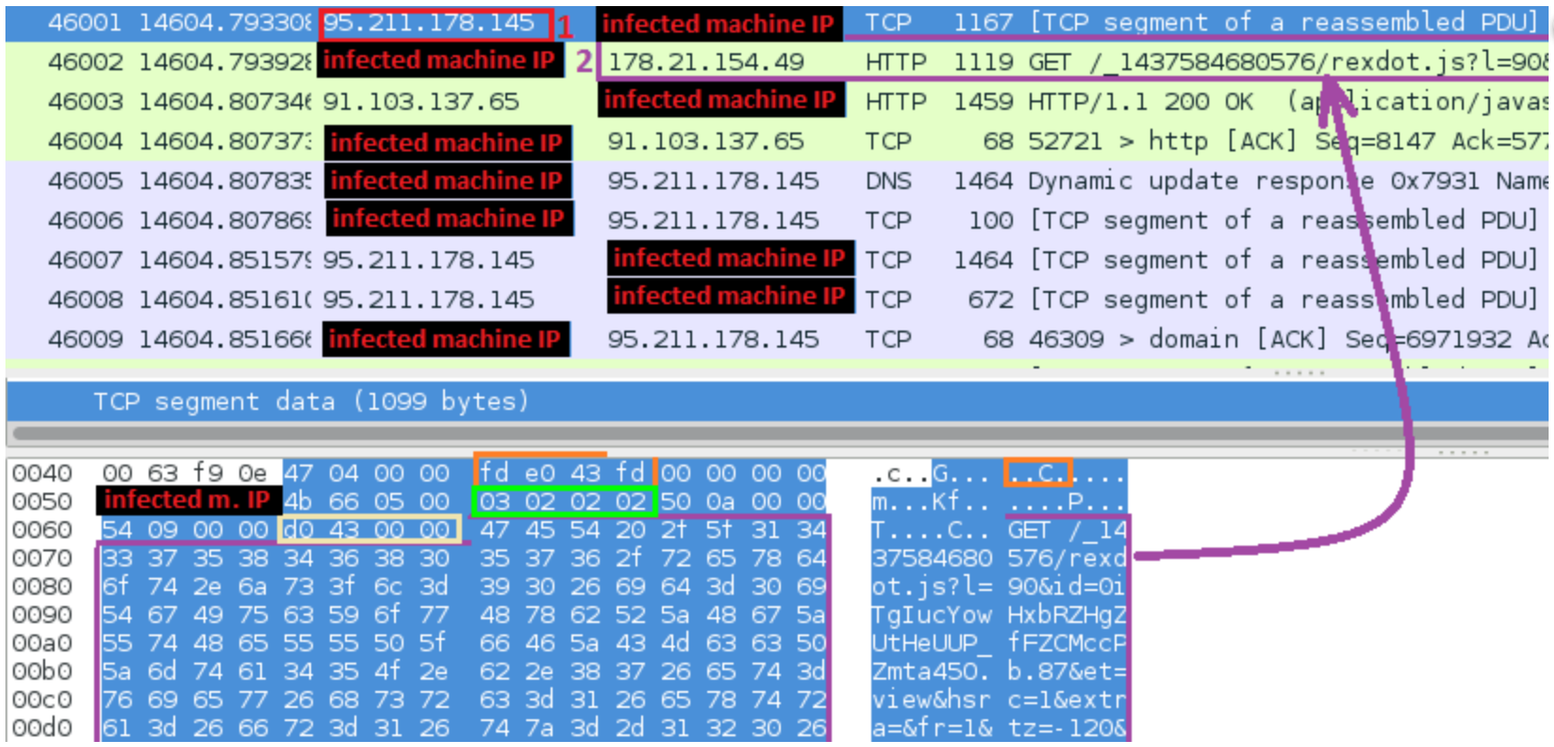
```
0000  00 00 02 00 00 00 00 00  00 00 00 00 00 00 08 00   ........ ........
0010  45 00 00 66 6e 02 40 00  37 06 ec 21 5f d3 0f 25   E..fn.@. 7..!_..%
0020  a4 7f d5 f6 00 35 c1 eb  20 cd 89 4e 7a 22 00 1c   .....5.. ..Nz"..
0030  80 18 04 11 09 f7 00 00  01 01 08 0a 89 f0 4e 2b   ........ ......N+
0040  00 15 5d a9 2e 00 00 00  f6 1b 70 67 00 00 00 00   ..].....  ..pg....
0050  00 00 00 00 00 00 00 00  01 00 00 01 00 00 00 00   ........ ........
0060  00 00 00 00 4c 16 23 3c  01 67 6f 6f 67 6c 65 2e   ....L.#< .google.
0070  63 6f 6d 00 50 00                                 com.P.
```

2e 00 = Length of the message (little endian) -> 0x002e -> 46
fb 1b 70 67 = bot ID, truncated (without last WORD)
01 00 00 01 = command *test given domain*
4c 16 23 3c = session constant
01 = number of queries
google.com = domain to test
50 00 = port to query (little endian) 0x0050 -> 80

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Tunneled Proxy Protocol - Request



C&C orders a bot to perform a GET request

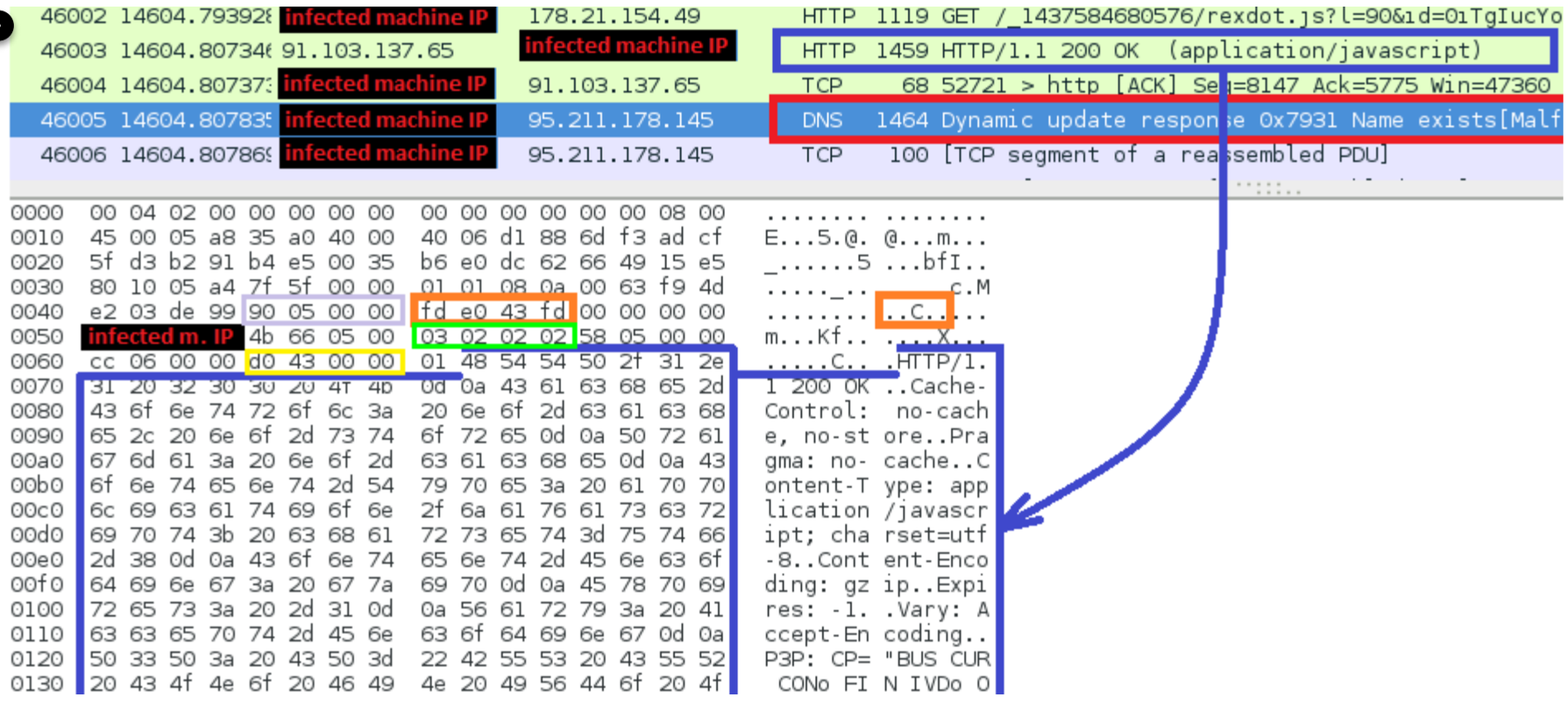
47 04 = Length of the message (little endian) -> 0x0447 -> 1095
fd e0 43 fd = bot ID, truncated (without last WORD)
03 02 02 02 = command *HTTP request*
d0 43 00 00 = proxy client ID
GET / … = request data

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Tunneled Proxy Protocol - Response

Bot performs ordered request, packs it in the internal protocol and sends back to the C&C



90 05 = Length of the message (little endian) -> 0x0590 -> 1424
fd e0 43 fd = bot ID, truncated (without last WORD)
03 02 02 02 = command *HTTP request*
d0 43 00 00 = proxy client ID
HTTP /1.1 … = response data

Sentrant
Digital Advertising Integrity

Malwarebytes

A proxy but for what?

Who is using this and why?

Sentrant
Digital Advertising Integrity

Malwarebytes

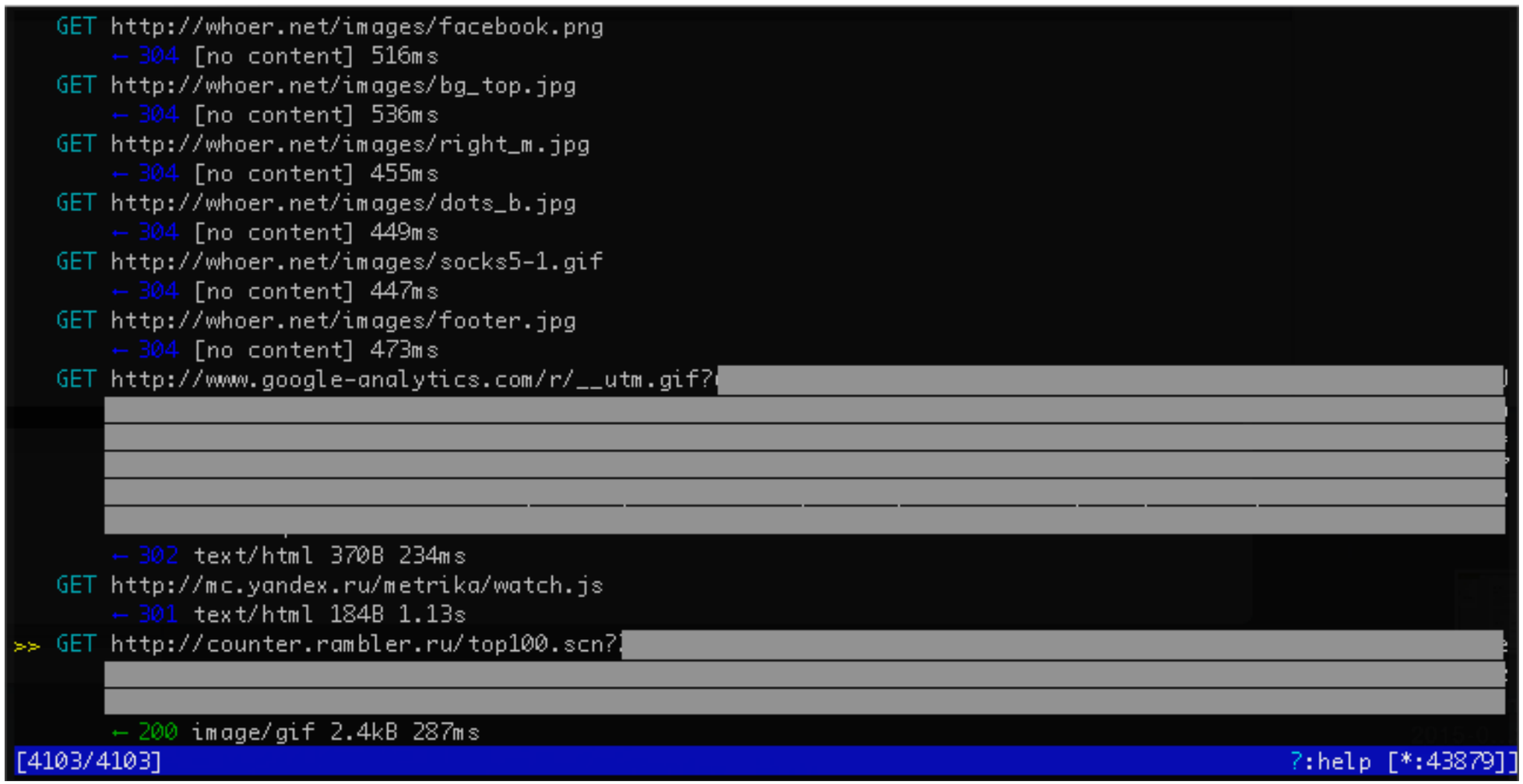
Proxy Honeypot

1. Reimplement proxy registration protocol in script
2. Find a good proxy intercept tool (mitmproxy)
3. Build our own proxy honeypot
4. :))

Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Proxy Traffic



Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Proxy Traffic… So Bad

Crime Forums
crdclub.so, verified.mn, etc

Testing Stolen Credentials
paypal, alibaba.com, royalbank.com, etc

Building Fake Dating Profiles
jdate.com, datehookup.com, match.com, etc.

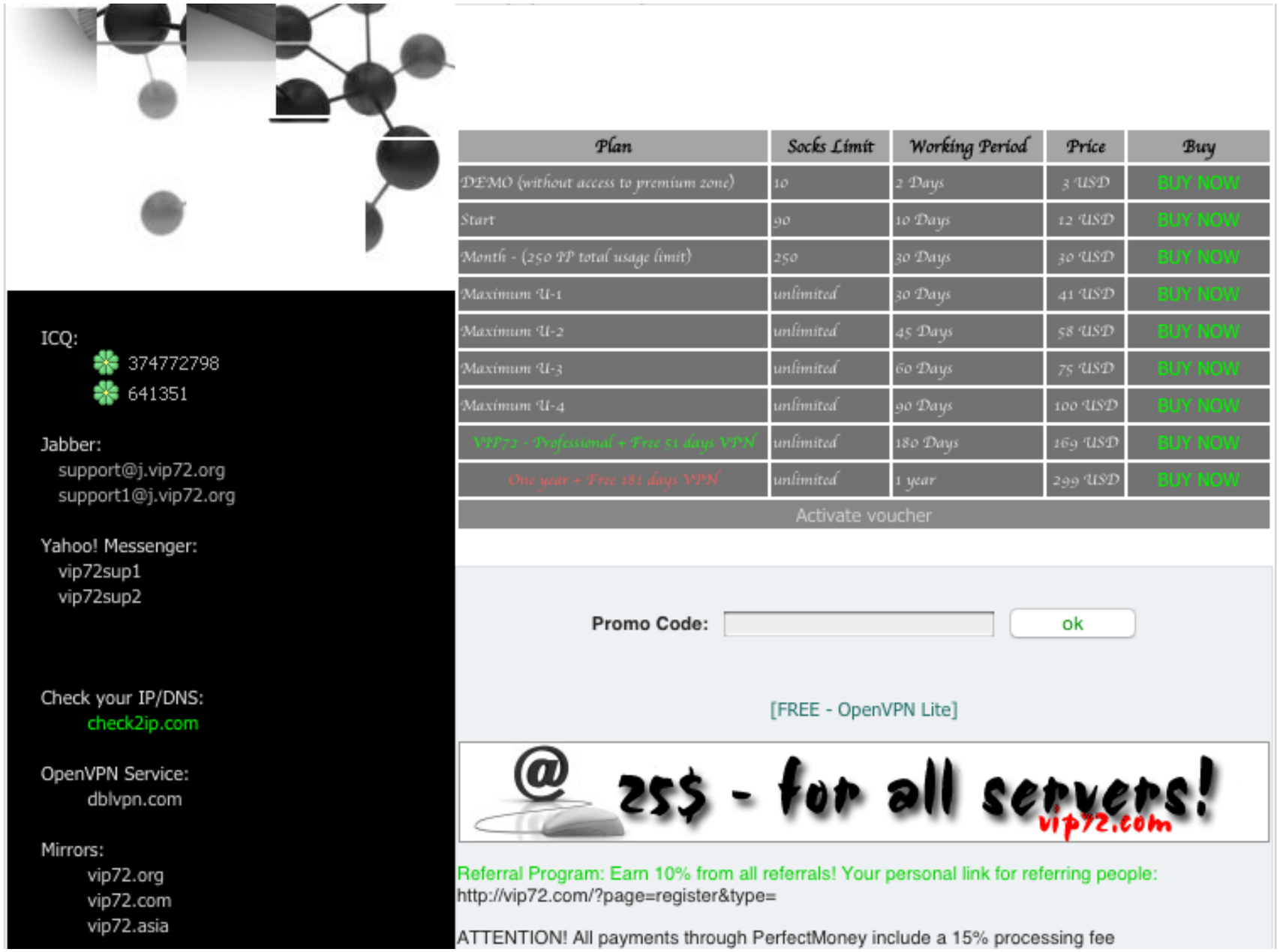
Sentrant
Digital Advertising Integrity

Malwarebytes

Bunitu Link to VIP72

```
    ← 200 image/x-icon 12.12kB 255ms
GET http://www.google-analytics.com/collect?v=1&_v=j39&a=840972276&t=pageview&_s=1&dl=http%3A%2F%2Frencont
    re.sexy.easyflirt.fr%2Ff%2Fpublic&dp=%2Ff%2Fpublic&ul=en-us&de=UTF-8&dt=Sexy&sd=24-bit&sr=2560x1440&vp
    =1333x794&je=1&_u=SCCAiEABF~&jid=&cid=1061364277.1442732901&tid=UA-1775268-1&cd1=2&cd6=tmpl_video_moza
    ic&cd7=&z=1099427177
    ← 200 image/gif 35B 106ms
GET http://check2ip.com/
    ← 200 text/html 3.63kB 760ms
GET http://46241382.vip72.info/xxx.img
    ← ProxyError(NetLibError('Error connecting to "46241382.vip72.info": [Errno 8] nodename nor servname
      provided, or not known',),)
GET http://check2ip.com/flash.swf?xxx=56801897
    ← 200 application/x-shockwave-flash 3.91kB 89ms
GET http://check2ip.com/who.php
    ← 200 image/jpeg 12.06kB 30.2s
GET http://check2ip.com/leftw.gif
    ← 304 [no content] 30.1s
GET http://check2ip.com/xw.jpg
    ← 304 [no content] 118ms
GET http://check2ip.com/rightw.gif
    ← 304 [no content] 30.1s
GET http://check2ip.com/?prm=46241382
    ← 200 text/html 127B 2.23s
>> GET http://check2ip.com/?prm=56801897
    ← 200 text/html 20B 14.2s
[4221/4221]                                                          ?:help [*:43879]]
```

What is VIP72



ICQ:
374772798
641351

Jabber:
support@j.vip72.org
support1@j.vip72.org

Yahoo! Messenger:
vip72sup1
vip72sup2

Check your IP/DNS:
check2ip.com

OpenVPN Service:
dblvpn.com

Mirrors:
vip72.org
vip72.com
vip72.asia

Plan	Socks Limit	Working Period	Price	Buy
DEMO (without access to premium zone)	10	2 Days	3 USD	BUY NOW
Start	90	10 Days	12 USD	BUY NOW
Month - (250 PP total usage limit)	250	30 Days	30 USD	BUY NOW
Maximum U-1	unlimited	30 Days	41 USD	BUY NOW
Maximum U-2	unlimited	45 Days	58 USD	BUY NOW
Maximum U-3	unlimited	60 Days	75 USD	BUY NOW
Maximum U-4	unlimited	90 Days	100 USD	BUY NOW
VIP72 - Professional + Free 51 days VPN	unlimited	180 Days	169 USD	BUY NOW
One year + Free 181 days VPN	unlimited	1 year	299 USD	BUY NOW
Activate voucher				

Promo Code: ok

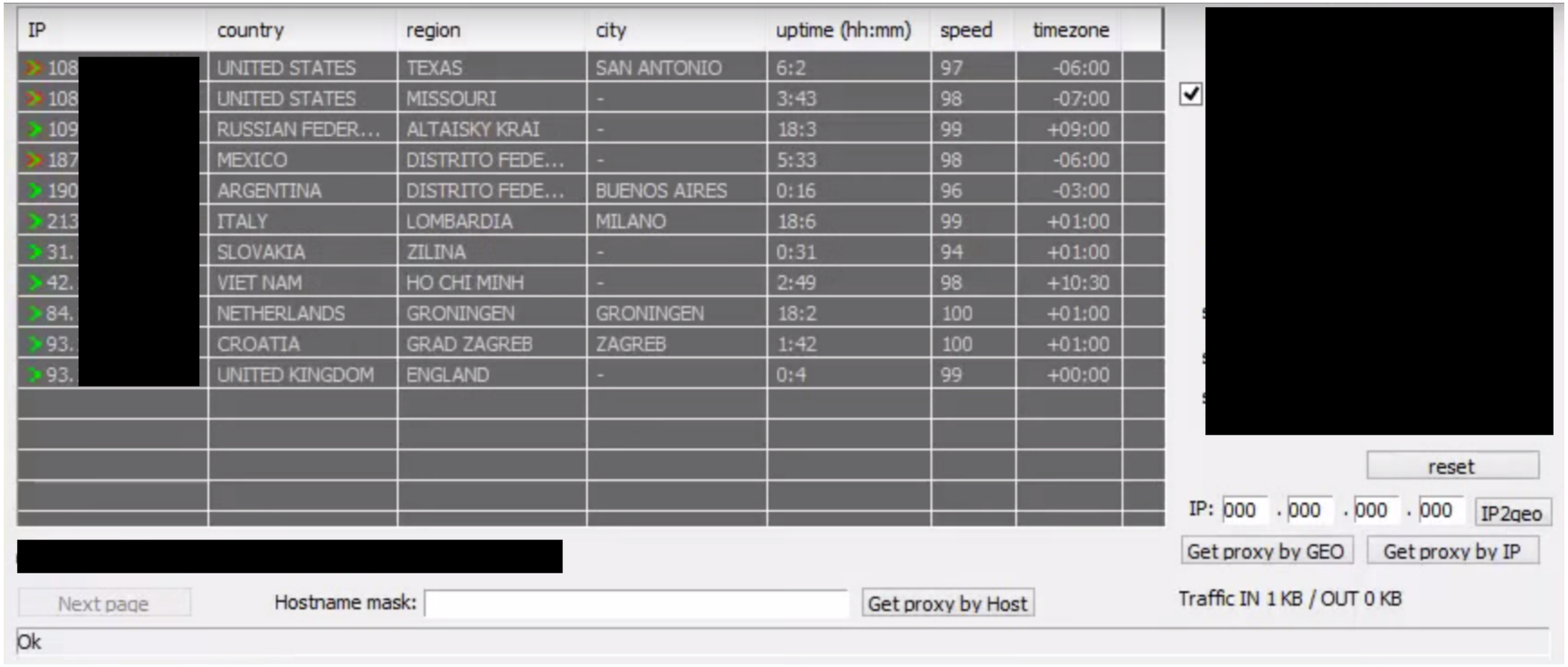
[FREE - OpenVPN Lite]

@ 25$ - for all servers! vip72.com

Referral Program: Earn 10% from all referrals! Your personal link for referring people:
http://vip72.com/?page=register&type=

ATTENTION! All payments through PerfectMoney include a 15% processing fee

What is VIP72

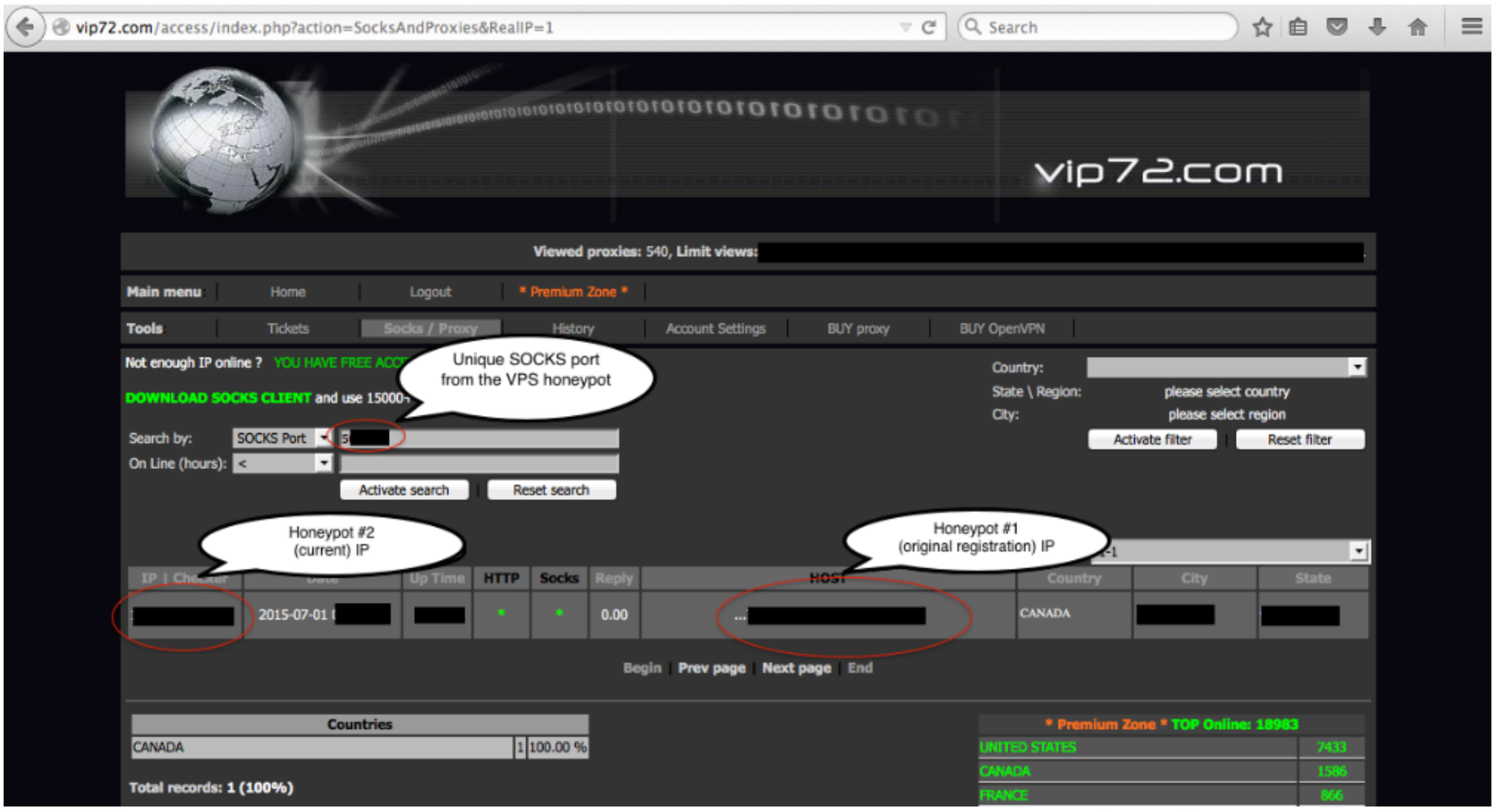


VIP72 VPN Client

Sentrant
Digital Advertising Integrity

Malwarebytes

Confirming VIP72 Resale of Bunitu Proxy Services



Sentrant
Digital Advertising Integrity

Malwarebytes

Other VPN Services Involved

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
System	4	UDP	testmachine	microsoft-ds	*	*					
winlogon.exe	612	TCP	testmachine	12960	testmachine	0	LISTENING				
winlogon.exe	612	TCP	testmachine	43879	testmachine	0	LISTENING				
winlogon.exe	612	TCP	testmachine	1036	server6032.megahoster.net	domain	ESTABLISHED	8,965	14,995,532	3,010	1,315,544
winlogon.exe	612	TCP	testmachine	1068	counter.rambler.ru	http	CLOSE_WAIT	2	894	8	9,826
winlogon.exe	612	TCP	testmachine	1069	counter.rambler.ru	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1138	68.232.34.191	https	CLOSE_WAIT	4	719	24	33,384
winlogon.exe	612	TCP	testmachine	1141	68.232.34.191	https	CLOSE_WAIT	3	510	16	20,812
winlogon.exe	612	TCP	testmachine	1146	68.232.34.191	https	CLOSE_WAIT	4	719	22	31,271
winlogon.exe	612	TCP	testmachine	1143	68.232.34.191	https	CLOSE_WAIT	4	718	11	12,755
winlogon.exe	612	TCP	testmachine	1154	ip-8.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT	2	702	23	33,732
winlogon.exe	612	TCP	testmachine	1159	ip-8.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT	1	371	1	574
winlogon.exe	612	TCP	testmachine	1192	pl-web1.pl.mediainter.net	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1180	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT	1	399	8	10,373
winlogon.exe	612	TCP	testmachine	1188	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1176	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1184	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT	1	454	1	2,054
winlogon.exe	612	TCP	testmachine	1181	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT			45	72,810
winlogon.exe	612	TCP	testmachine	1189	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1185	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1193	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1177	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT			4	7,039
winlogon.exe	612	TCP	testmachine	1186	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1182	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT			2	1,817
winlogon.exe	612	TCP	testmachine	1190	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT	1	454	5	6,192
winlogon.exe	612	TCP	testmachine	1178	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT			10	17,155
winlogon.exe	612	TCP	testmachine	1191	pl-web1.pl.mediainter.net	http	CLOSE_WAIT			1	574
winlogon.exe	612	TCP	testmachine	1183	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1179	ip-4.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT			6	8,027
winlogon.exe	612	TCP	testmachine	1187	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1199	rtax.criteo.com	http	CLOSE_WAIT	1	392	1	469
winlogon.exe	612	TCP	testmachine	1204	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT	1	454	4	6,629
winlogon.exe	612	TCP	testmachine	1203	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT	1	470	31	51,382
winlogon.exe	612	TCP	testmachine	1208	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1209	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1210	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1206	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1211	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1207	ip-6.213-189-55-112.net.eco.atman.pl	http	CLOSE_WAIT				
winlogon.exe	612	TCP	testmachine	1224	cdn1.bbmedia.cz	http	CLOSE_WAIT	1	357	7	11,104
winlogon.exe	612	TCP	testmachine	1215	185.31.25.89	https	CLOSE_WAIT	3	1,021	56	101,004
winlogon.exe	612	TCP	testmachine	1227	cdn3.bbmedia.cz	http	CLOSE_WAIT	1	354	1	807
winlogon.exe	612	TCP	testmachine	1221	185.31.25.89	https	CLOSE_WAIT	3	1,069	5	5,142
winlogon.exe	612	TCP	testmachine	1228	185.31.25.90	https	CLOSE_WAIT	3	1,030	10	10,975

.ru

.pl

.cz

Observations from PL client

Sentrant
Digital Advertising Integrity

Malwarebytes

Other Anonymizing VPN Services Involved

Filter: http.request.method == "POST" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Lengtl	Info
29370	3442.280749(	infected machine IP	5.134.210.132	HTTP	653	POST /NewItem/Preview.php HTTP/1.1
34138	3466.568687(		23.52.59.27	OCSP	500	Request
34151	3466.678562(		23.52.59.27	OCSP	500	Request
34287	3470.236171(		23.52.59.27	OCSP	500	Request

Hypertext Transfer Protocol

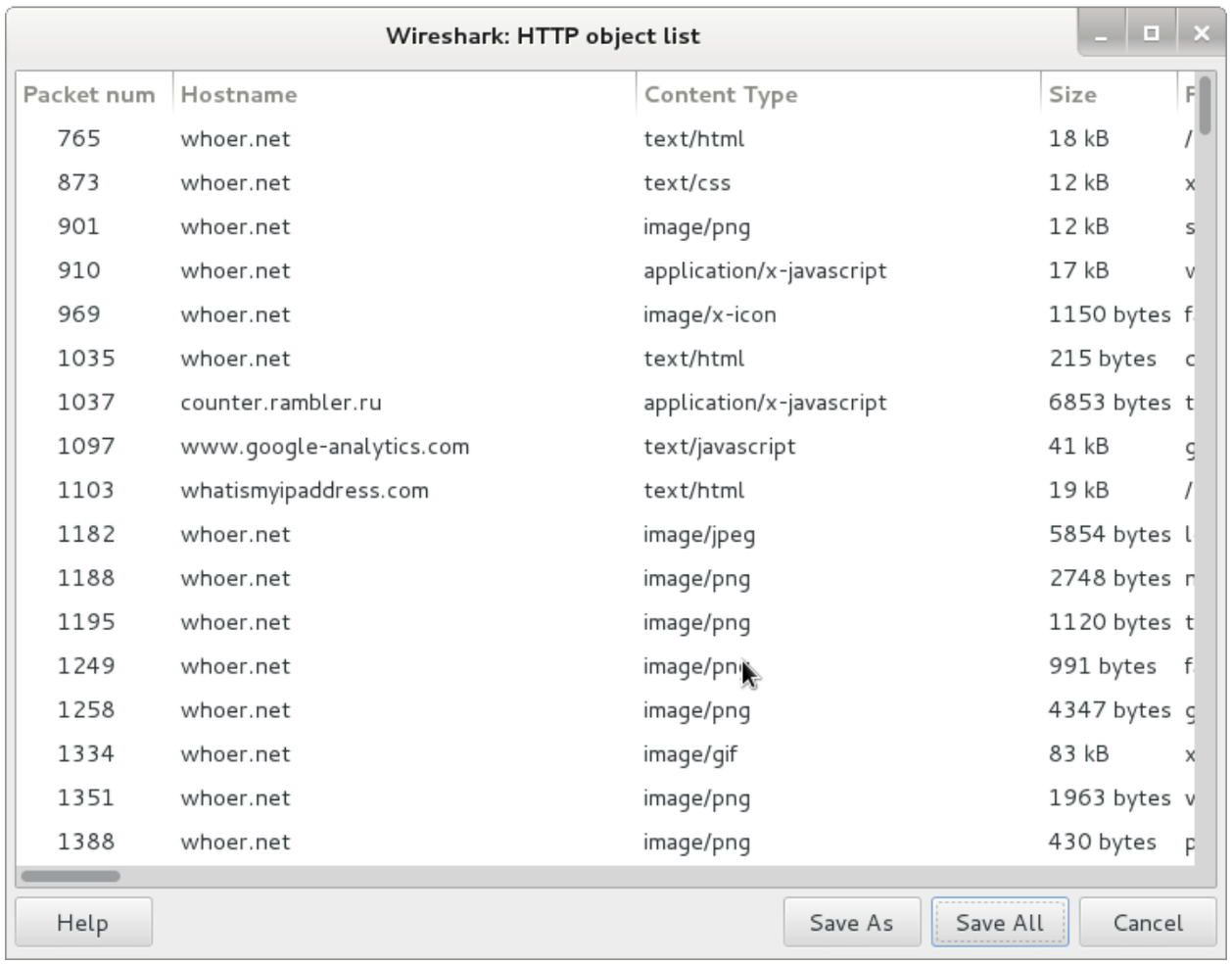
```
POST /NewItem/Add.php/process HTTP/1.1\r\n
Host: allegro.pl\r\n
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:38.0) Gecko/20100101 Firefox/38.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: pl,en-US;q=0.7,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://allegro.pl/NewItem/Preview.php\r\n
[truncated] Cookie: allcg=c1a8cc; __gfp_64b=-TURNEDOFF; cartUserId=
```

Client's browser using Polish locale (code: pl)

Sentrant
Digital Advertising Integrity

Malwarebytes

Other Anonymizing VPN Services Involved



Users often start surfing by checking their new IP address

Sentrant
Digital Advertising Integrity

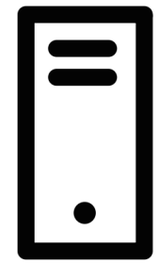
Malwarebytes

Distributors (Theory)

Infected
Proxy Bot

1) Register the bot

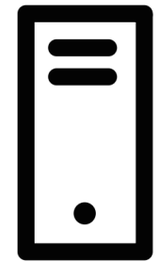
4) Send command from
the distributor



Bunitu C2
(Middleman)

3) Send commands to
my bots

2) Notify appropriate
distributor (based
on bot's geolocation)



Distributor
(ie. VIP72)

Sentrant
Digital Advertising Integrity

Malwarebytes

Risks on both ends

Infected machine owner:

- can be framed in a crime;
- have resources used without the permission

Proxy Customer:

- vulnerable for data theft and privacy violation;
- his/her traffic may be poisoned on the way

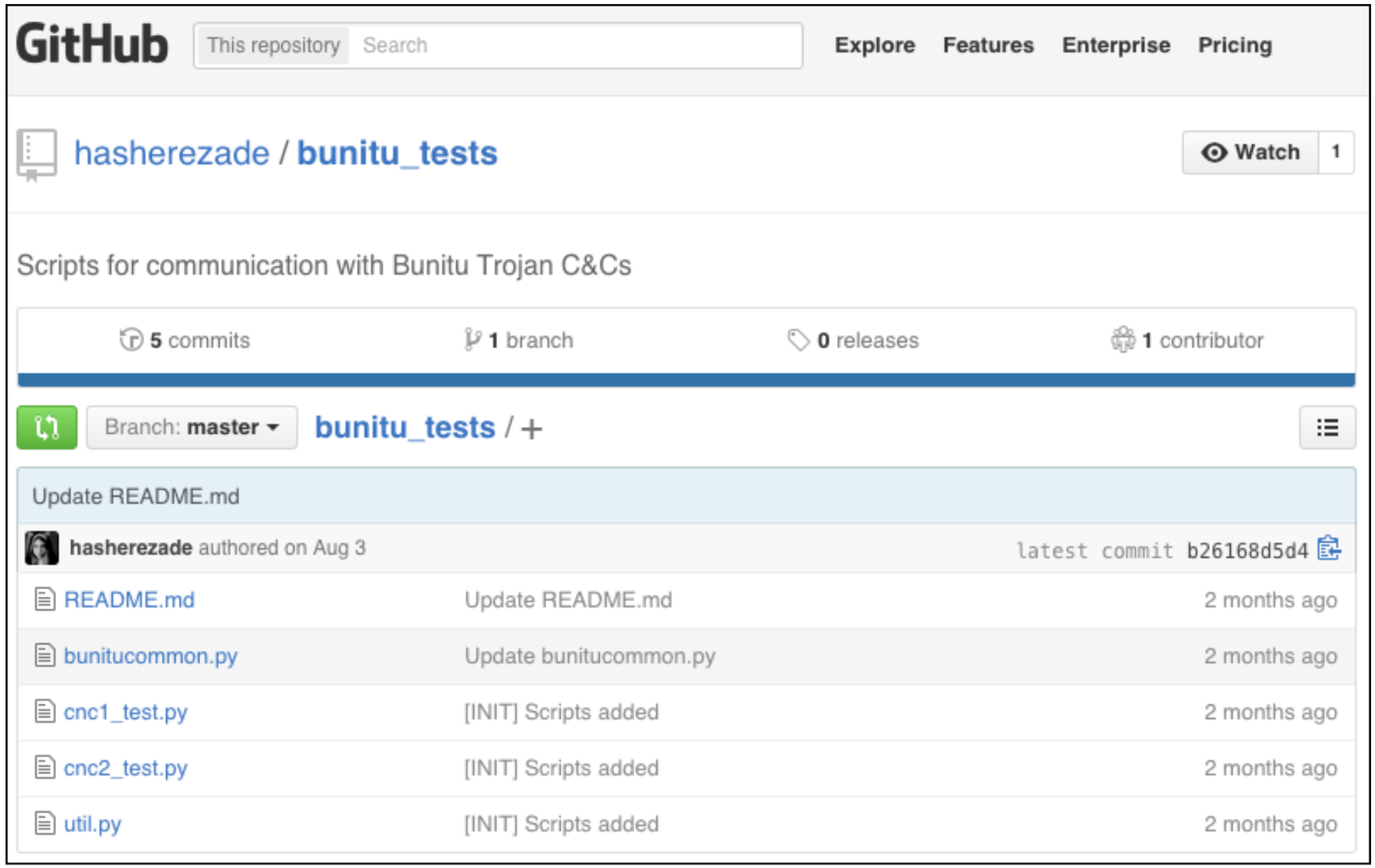
The (lack of) Evolution in Bunitu/VIP72

We first published a report on this malware on **August 5, 2015** there has been no change from either VIP72 or Bunitu

Sentrant
Digital Advertising Integrity

Malwarebytes

Building On Our Research



All of our tools are available on GitHub!

Sentrant
Digital Advertising Integrity

Malwarebytes

Building On Our Research

```
tester@kali:~/code/bunitu_tests$ ./cnc2_test.py --host cld1.adsertnet.com --xorv
al 0x32BC236F
Bot ID:
06 e0 1c eb 18 80 73 ac 31 00
#
XOR = 32bc236f
C&C#2 (Tunnel): 5.61.40.13:53
RESPONSE, len: 75
2e 00 00 00 06 e0 1c eb 00 00 00 00 00 00 00 00 00 00 00 01 00 00 01 00 00 00
 00 00 00 00 00 ec 7f 1a 3b 01 67 6f 6f 67 6c 65 2e 63 6f 6d 00 50 00 15 00 00 0
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 ff ff ff ff
LEN : 2e = 46
LEN : 15 = 21
Packages: 2
> DNS_QUERY: google.com
True
```

https://github.com/hasherezade/bunitu_tests/wiki

Sentrant
Digital Advertising Integrity

Malwarebytes

Contact Us

Hasherezade (@hasherezade), **Malwarebytes**

Sergei Frankoff (@herrcore), **Sentrant**

Sentrant
Digital Advertising Integrity

Malwarebytes

Image Attribution

- desktop computer by Creative Stall from the Noun Project
- Cloud by Golden Roof from the Noun Project
- Skull and Crossbones by Ricardo Moreira from the Noun Project
- Surveillance by Luis Prado from the Noun Project
- about by Amr Fakhri from the Noun Project

Sentrant
Digital Advertising Integrity

Malwarebytes