

Anonymizing VPN Services as a Botnet Monetization Strategy

Analyzing The Bunitu Botnet

Researchers

Hasherezade (@hasherezade), **Malwarebytes**

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

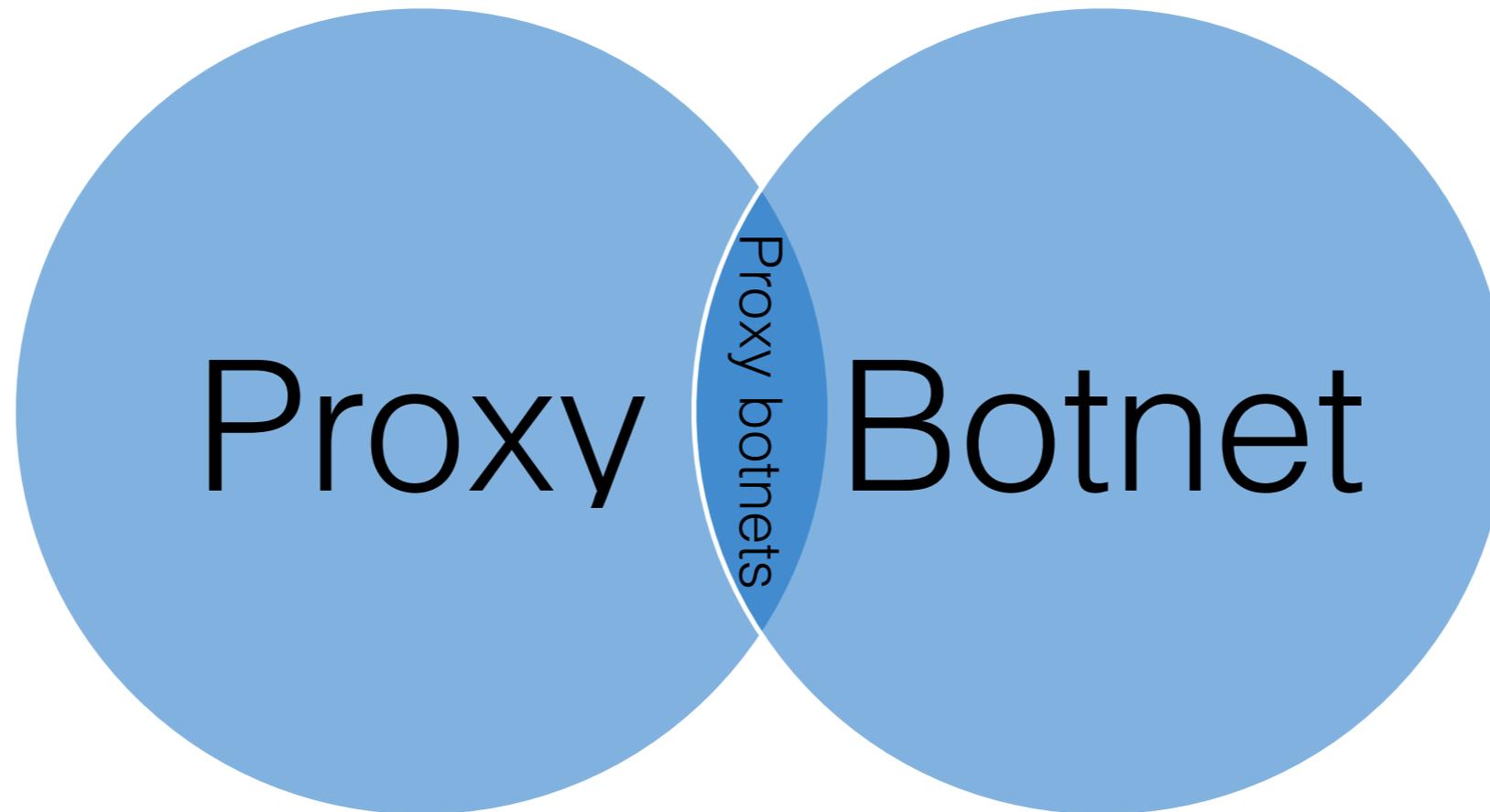


Sentrant
Digital Advertising Integrity



Malwarebytes

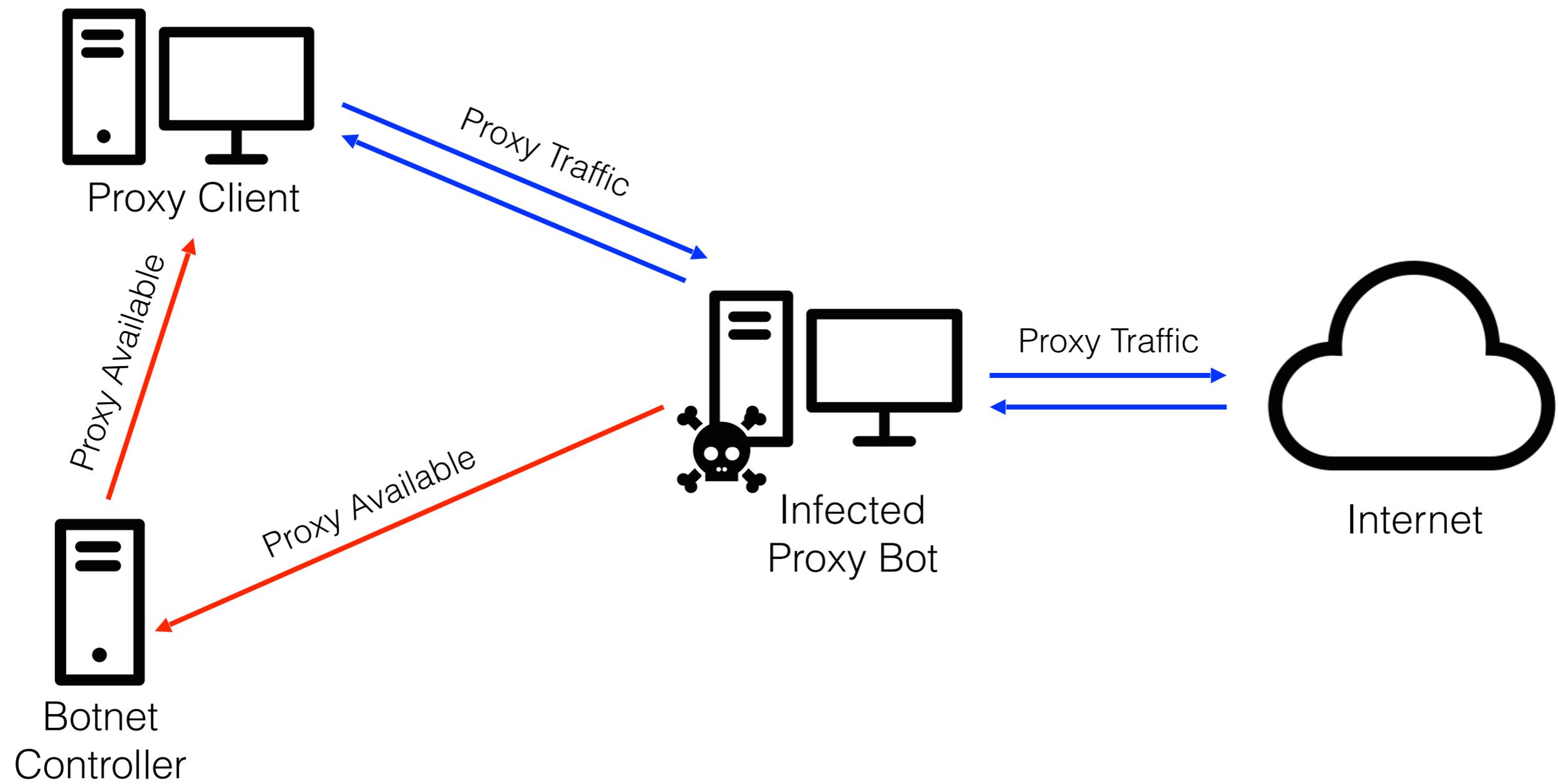
What is a Proxy Botnet



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



What is a Proxy Botnet

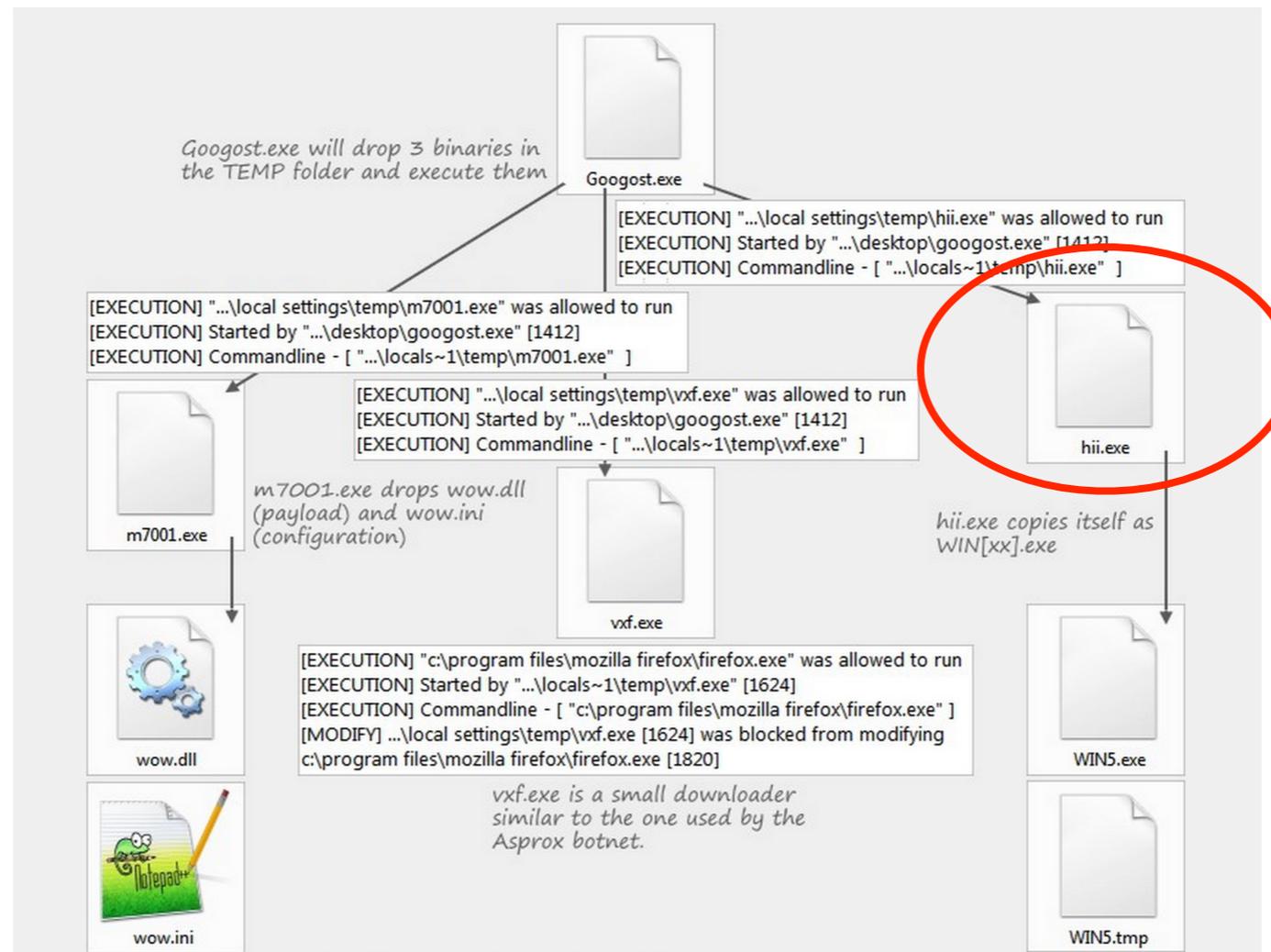


Monetizing Proxy Botnets

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



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



Prior Work: Monetization Via Proxy Sales

The screenshot shows the AWM PROXY website interface. At the top, there's a navigation bar with 'Chat', 'icq 434-929', and links for 'FAQ', 'ARTICLES', 'DOWNLOAD', and 'CONTACTS'. Below this is a user account section with 'Welcome', 'Money: 0.00 USD', 'Add money', 'Cabinet', 'Settings', and 'Quit' buttons. The main content area is divided into four columns: 'HTTP/Socks', 'Exclusive', 'Private HTTP', and 'Browser proxy'. Each column has a 'Description', 'Proxy list', 'Price', and 'FAQ (instruction)' link, along with a 'free Test!' or 'test used' button. To the right, there's a section for 'affiliate program' with a 'Send msg' button and a 'No active subscriptions' notification with a 'Buy Proxy | To take for testing' link. Below the navigation, there's a section titled 'The list of urgent proxies HTTP/SOCKS' with a dropdown menu for 'Country of proxy' set to 'ALL (24373)' and a dropdown for 'Amount of proxies displayed on the page' set to 'All'. A table of proxy listings follows, with columns for '#', 'ip', 'Country', 'City', 'Speed', 'Uptime', and 'CTR'. The table contains 12 rows of data. On the right side, there's an 'Archive news' section with three news items dated 31.08.2011, 26.05.2011, and 22.03.2011.

#	ip	Country	City	Speed	Uptime	CTR
1	112.208.113.136	PH	Las Piñ	32 Kbs	3519 min.	92%
2	124.91.16.99	JP	Fpo	7778 Kbs	2638 min.	98%
3	202.86.100.202	ID	Jakarta	8137 Kbs	2386 min.	98%
4	186.100.109.98	--		5972 Kbs	2356 min.	94%
5	118.91.16.28	VN	Ho Chi Minh City	6902 Kbs	2331 min.	96%
6	128.91.161.51	JP	Tokyo	5529 Kbs	2330 min.	87%
7	200.117.104.217	AR	Buenos Aires	5005 Kbs	2327 min.	85%
8	2.81.192	--	Dubai	7753 Kbs	2292 min.	98%
9	211.114.231	TW	Taipei	2718 Kbs	2272 min.	96%
10	208.111.10.83	CL	Santiago	5273 Kbs	2255 min.	98%
11	178.100.10.10	AP		7002 Kbs	2166 min.	95%
12	50.81.10.107	--		5277 Kbs	2158 min.	82%

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



Sentrant
Digital Advertising Integrity



Malwarebytes

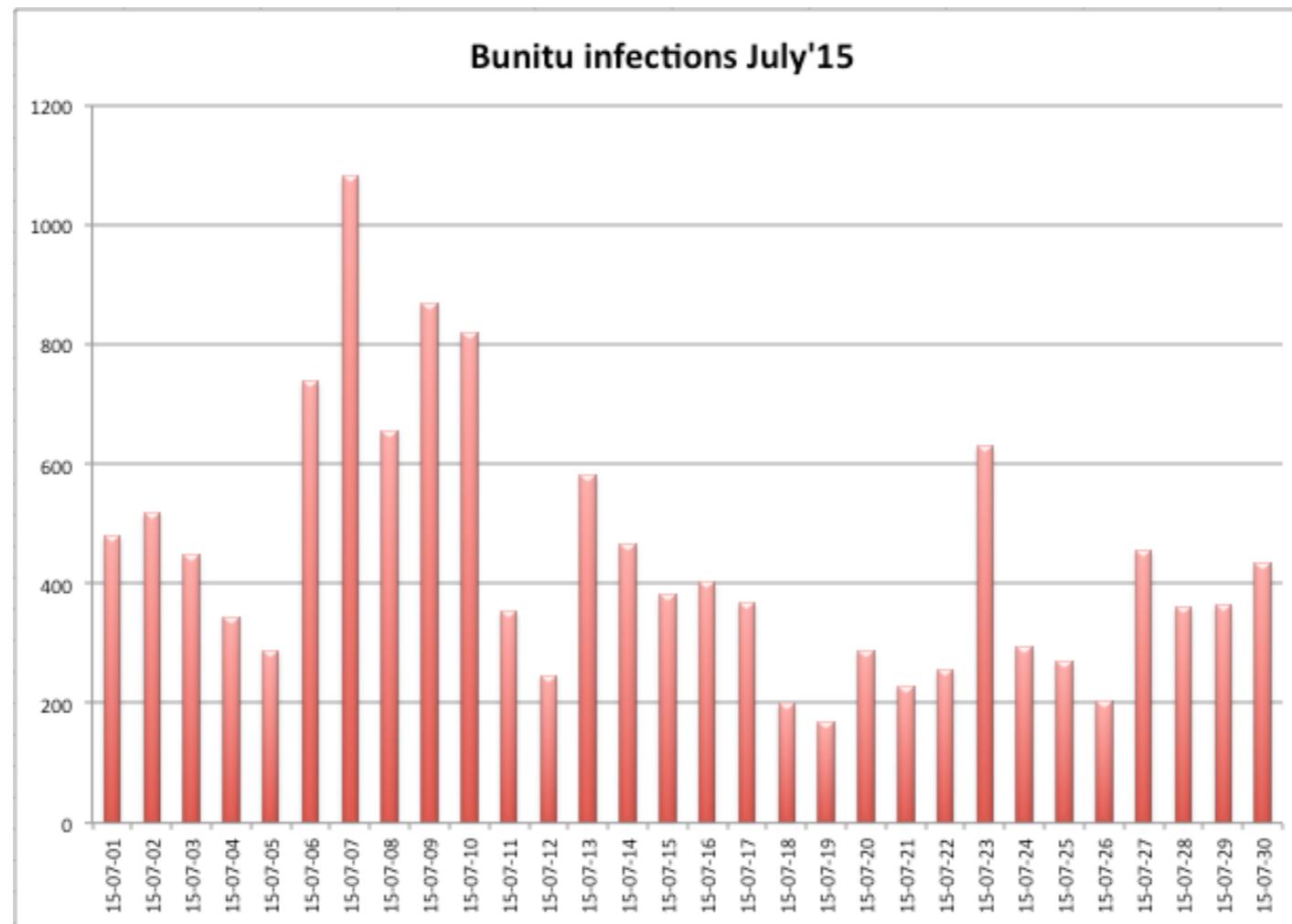
Bunitu

~~Ad fraud~~

Proxy botnet



Bunitu Overview



2013-12-25 : b0a91e1f91078bad48252edc989e868e : mlicnai.dll

...

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



Bunitu Proxy Services

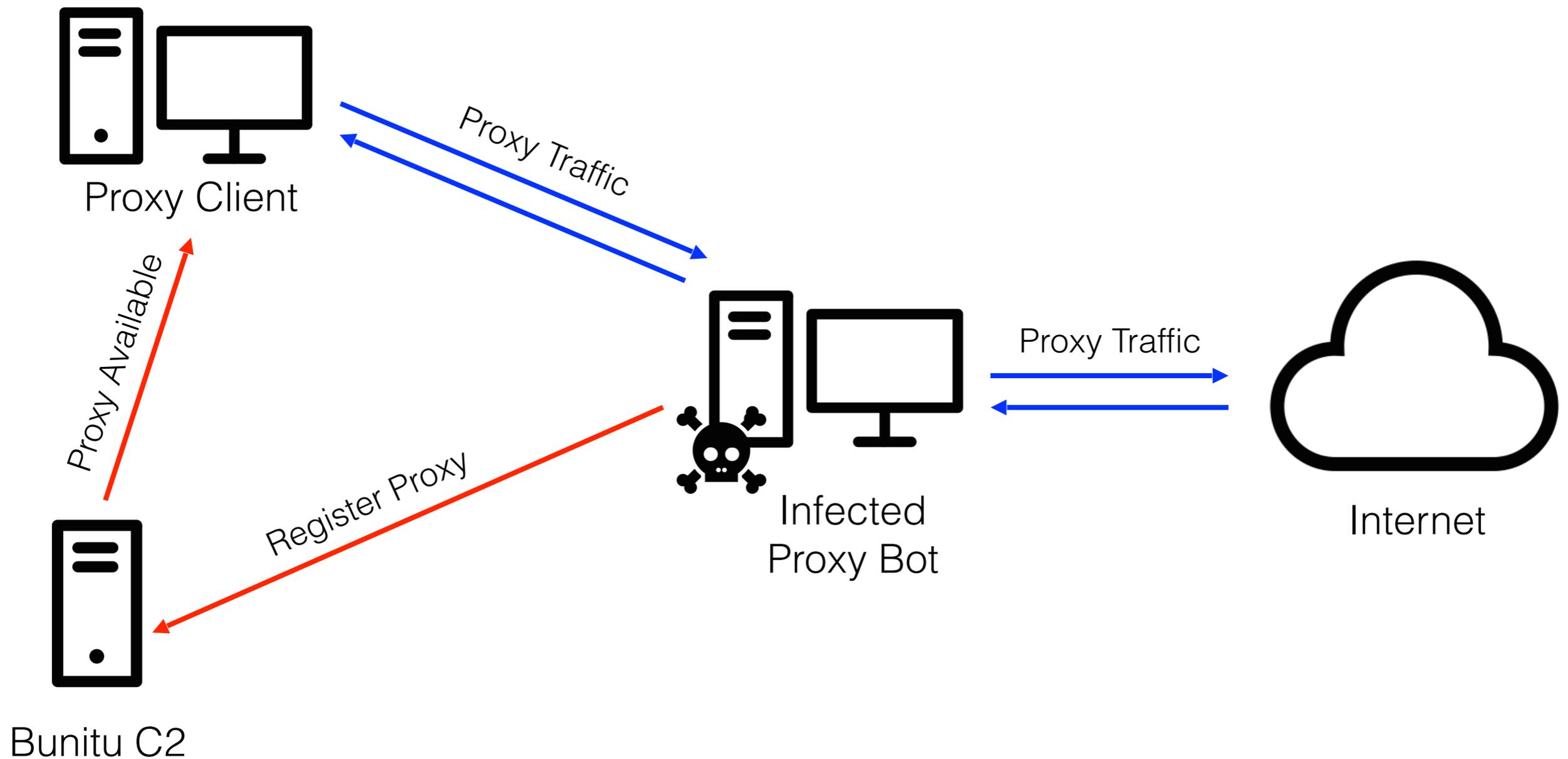
Two types of proxy: Standard and Tunnel

 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

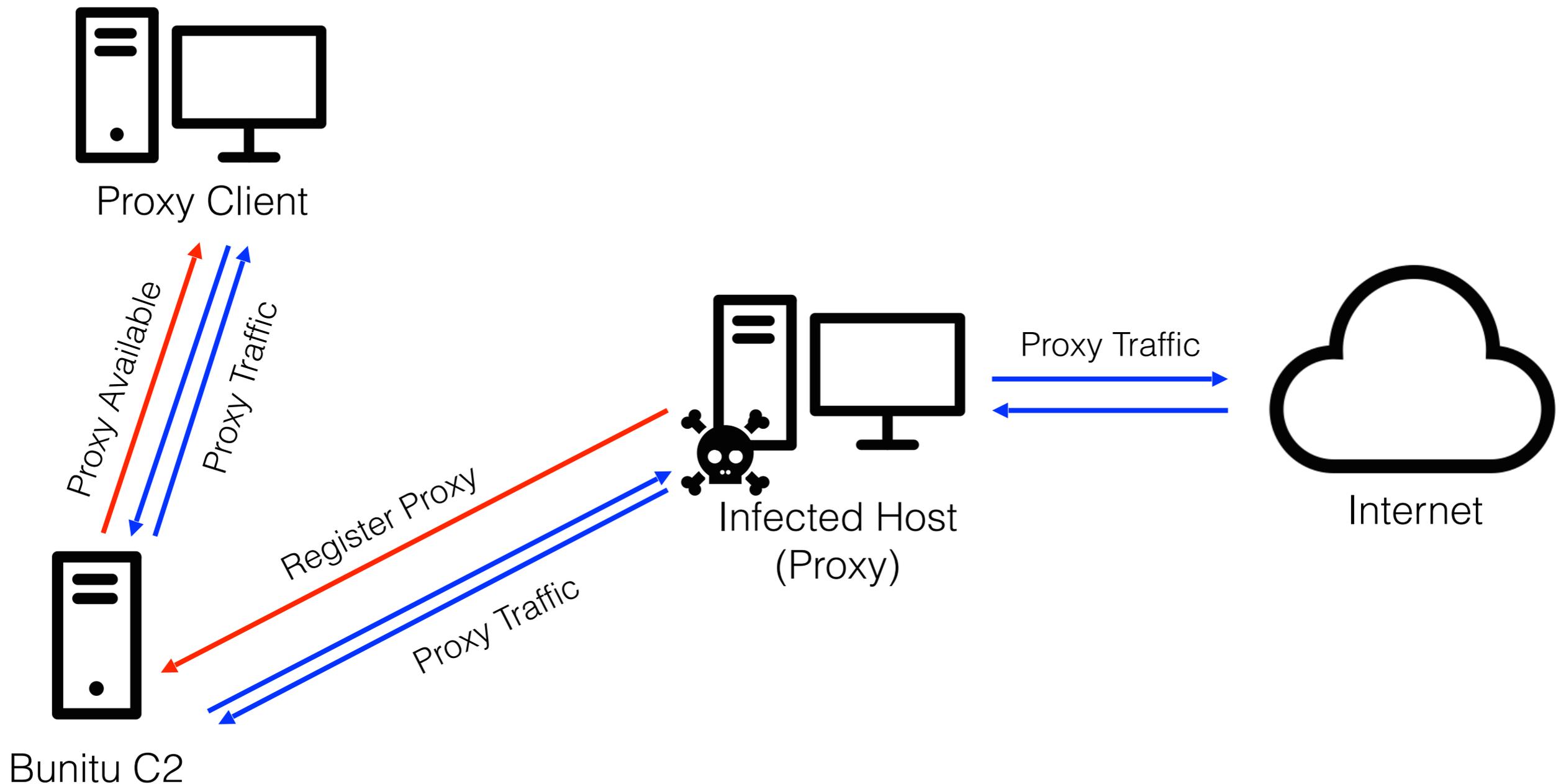
- Standard HTTP proxy and SOCKS proxy services are started by Bunitu on random high ports, client registers them to C&C#1
- Tunnel is operated via C&C#2 – uses it's own protocol to wrap and bypass the traffic



Bunitu Standard Proxy

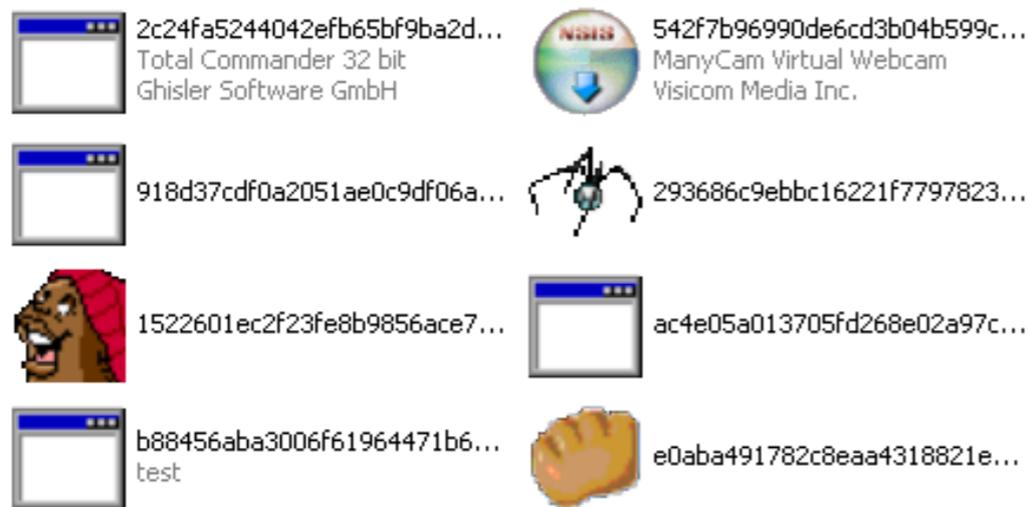


Bunitu Tunneled Proxy



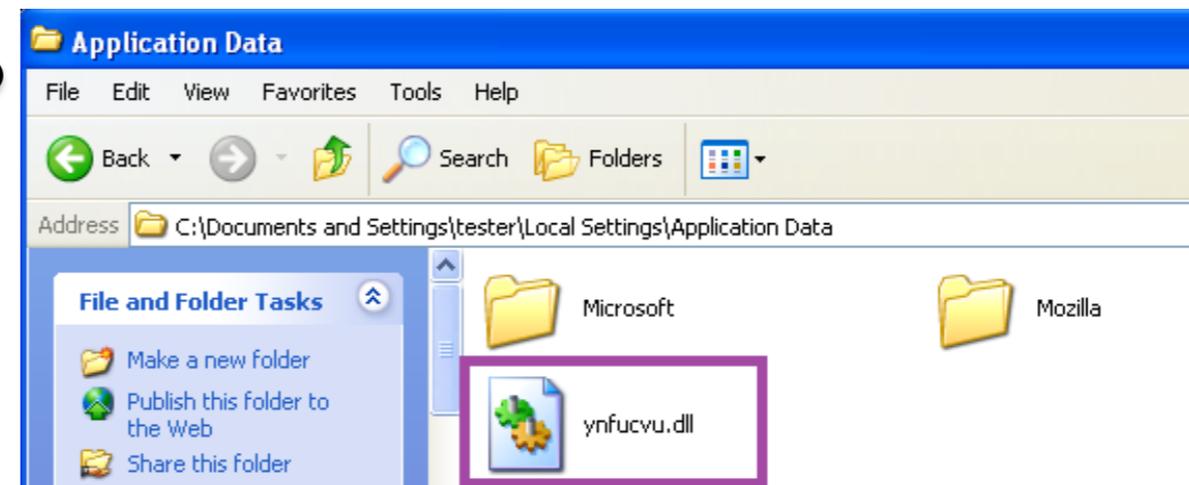
Bunitu Trojan overview

Always a DLL installed by dedicated dropper



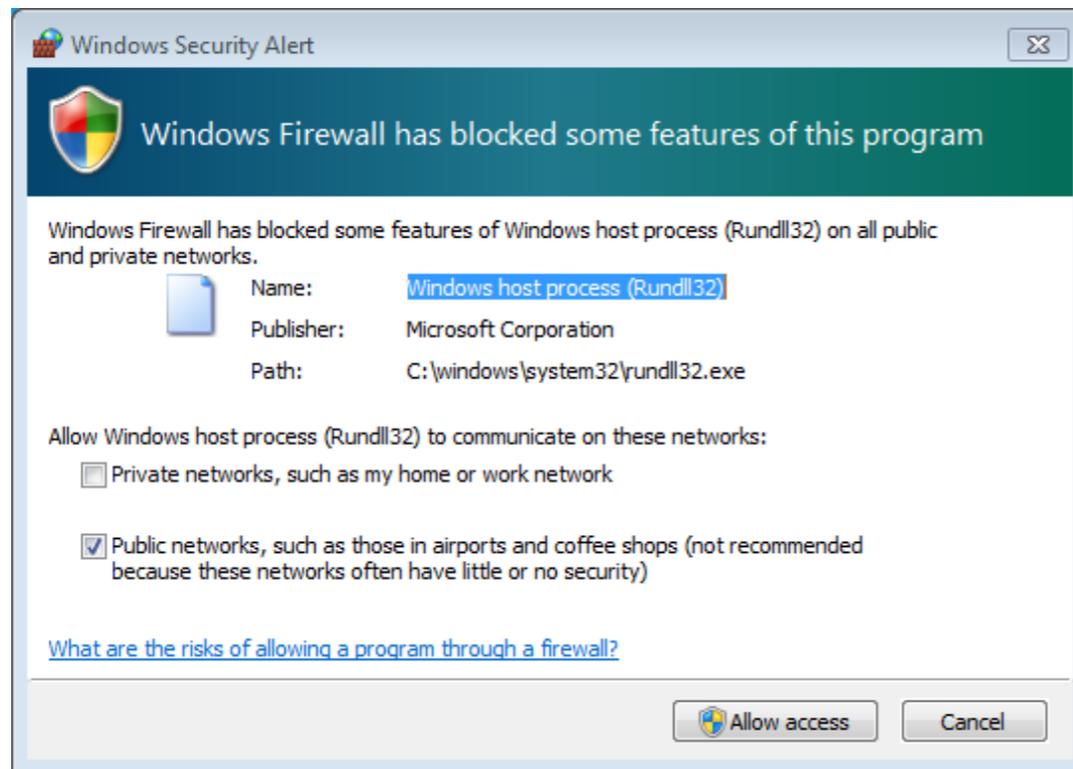
Droppers' Gallery

Constant naming convention:
[a-z]{7}.dll



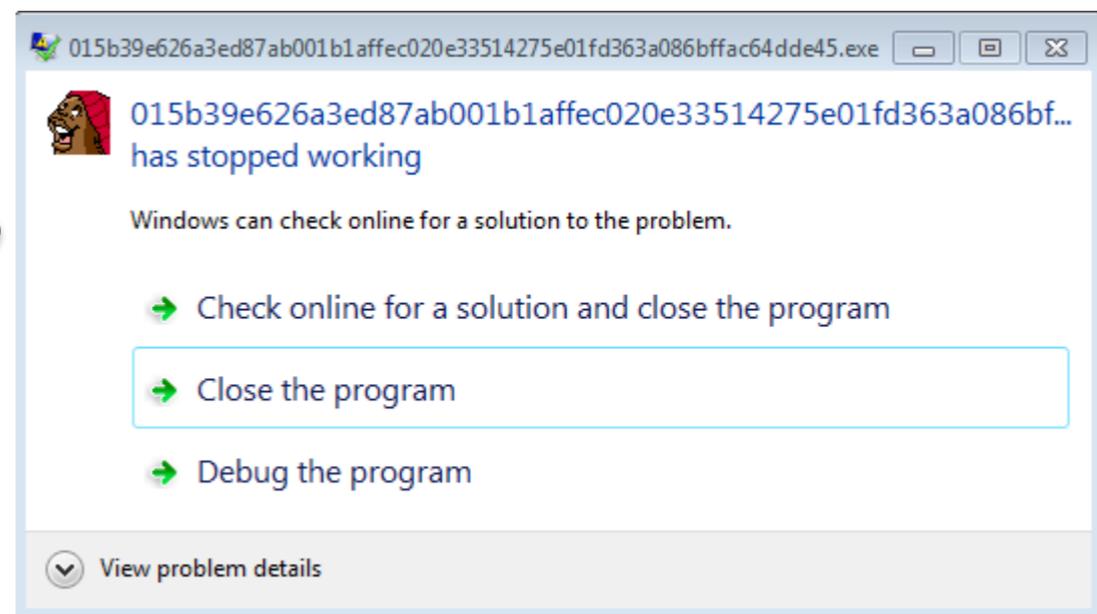
https://github.com/hasherezade/bunitu_tests/wiki/Bunitu-Gallery

Bunitu Installation

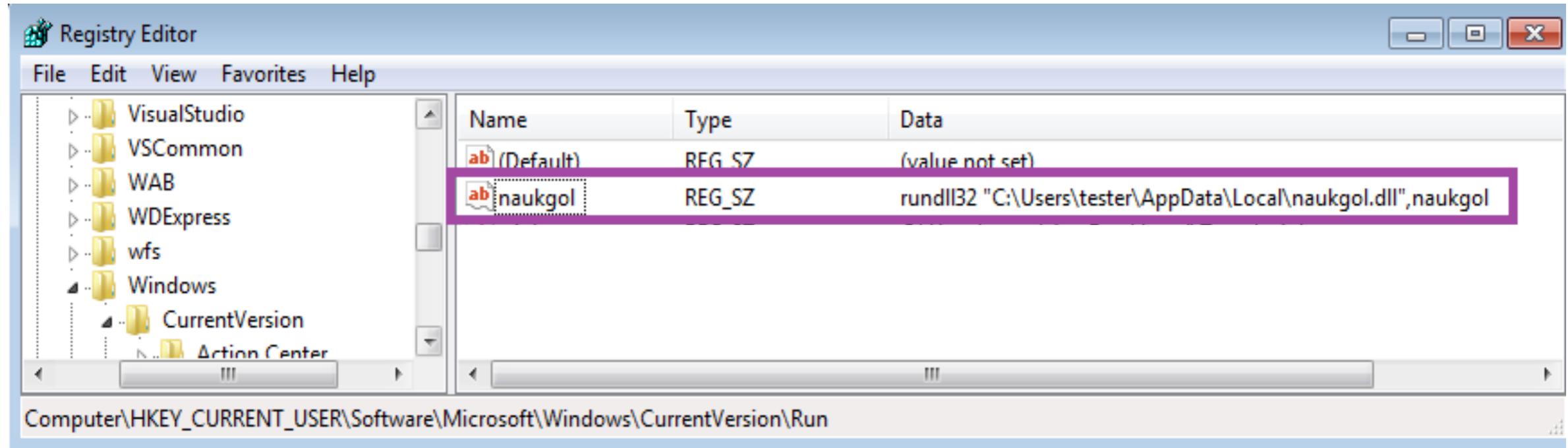


The standard proxy services require inbound connections. There is no privilege elevation exploit to silence this.

The installer often crashes at the end



Bunitu Host Persistence

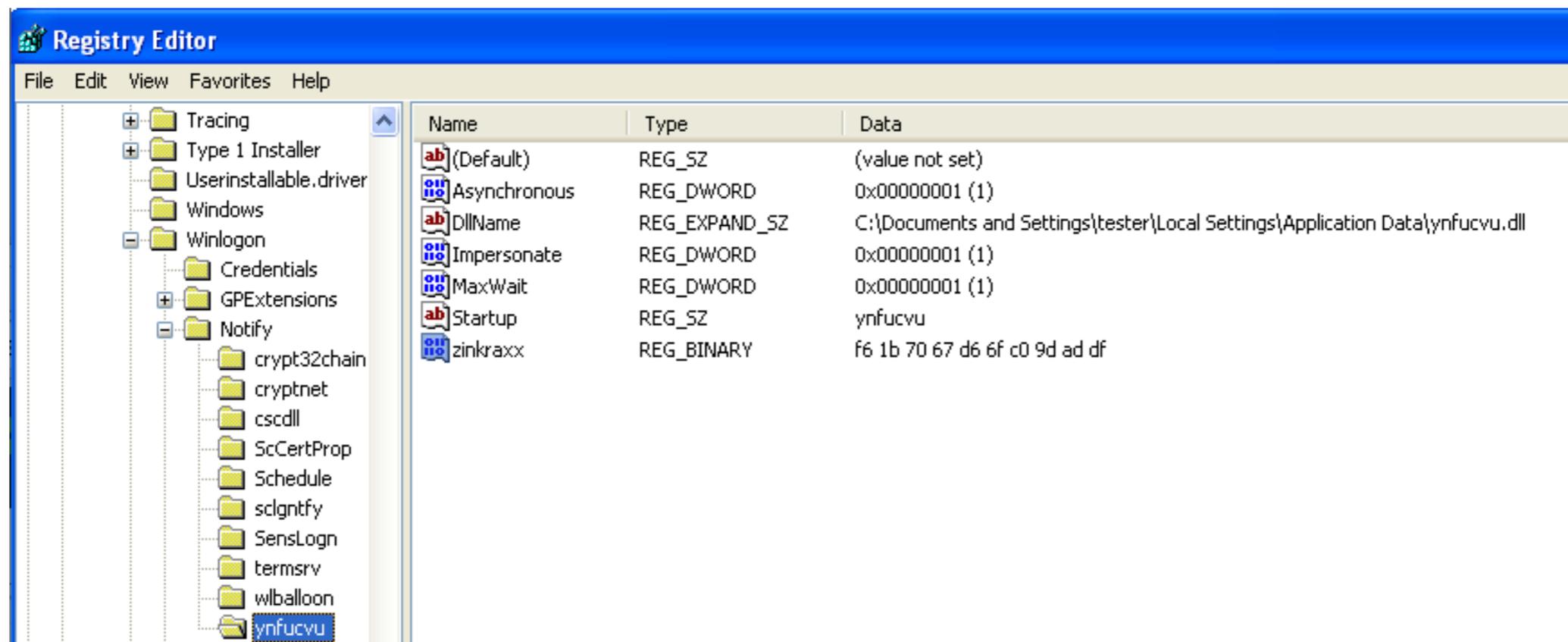


HKCU\Software\Microsoft\Windows\CurrentVersion\Run



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**



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

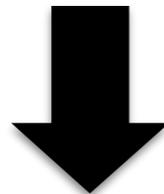
```

100028F0 . C3 RETN
100028F1 > FE05 07BE0010 INC BYTE PTR DS:[1000BE07]
100028F7 . B9 51E8FF0E MOV ECX,0FFFE851
100028FC . 49 DEC ECX
100028FD . 81C1 60820000 ADD ECX,8260
10002903 . 81EA 4A0D3700 SUB EDX,37DD4A
10002909 . 6A 2C PUSH 2C
1000290B . 51 PUSH ECX
1000290C . FF35 164D0110 PUSH DWORD PTR DS:[10014D16]
10002914 . E8 5BEAFFFF CALL lyhbyjo_.10001372

```

DS:[1000BE07]=04
Jump from 100028ED

Address	Hex dump	ASCII
10006D8D	00 01 01 00 00 01 00 00	.00..0..
10006DC5	00 00 00 00 4F A2 45 F0	...0&E-
10006DCD	05 00 16 00 A7 54 1A D9	↓...3T↓
10006DD5	4F A9 34 B2 00 00 00 00	0e4端...
10006DD0	00 00 00 00 B9 F0 00 00
10006DE5	00 00 00 00 00 00 00 00
10006DED	00 00 00 00 00 00 00 00



5	1.023710000	164.127.231.183	62.212.66.85	TCP	68 49311 > domain [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=10947 TSecr=3669194520
6	1.024131000	164.127.231.183	62.212.66.85	DNS	112 [Malformed Packet]
7	1.101924000	62.212.66.85	164.127.231.183	TCP	68 domain > 49311 [FIN, ACK] Seq=1 Ack=45 Win=33312 Len=0 TSval=3669194596 TSecr=10947
8	1.105267000	164.127.231.183	62.212.66.85	TCP	68 49311 > domain [ACK] Seq=45 Ack=2 Win=29312 Len=0 TSval=10968 TSecr=3669194596

TCP segment data (39 bytes)

+ [Malformed Packet: DNS]

+ [Malformed Packet: DNS]

0000	00 04 02 00 00 00 00 00	00 00 00 00 00 00 08 00
0010	45 00 00 60 5e 8e 40 00	40 06 ce a9 a4 7f e7 b7	E..^.@. @.....
0020	3e d4 42 55 c0 9f 00 35	f5 43 74 40 44 6c b0 45	>.BU...5 .Ct@dl.E
0030	80 18 00 e5 23 9b 00 00	01 01 08 0a 00 00 2a c3#... ..*.
0040	da b3 77 18 00 01 01 00	00 01 00 00 00 00 00 00	..w.....
0050	4f a2 45 f0 05 00 0d 00	a7 54 1a d9 4f a9 34 b2	0.E..... .T..0.4.
0060	00 00 00 00 00 00 00 00	b9 f0 00 00 00 00 00 00



Bunitu Standard Proxy Registration Protocol

```

49 387.58834600( infected machine IP 130.185.108.130 TCP 76 57296 > domain [SYN
50 387.67663000( 130.185.108.130 infected machine IP TCP 76 domain > 57296 [SYN
51 387.67668700( infected machine IP 130.185.108.130 TCP 68 57296 > domain [ACK
52 387.67809900( infected machine IP 130.185.108.130 DNS 112 [Malformed Packet]
.....

TCP segment data (39 bytes)
+ [Malformed Packet: DNS]
+ [Malformed Packet: DNS]
.....

0000 00 04 02 00 00 00 00 00 00 00 00 00 00 08 00 .....
0010 45 00 00 60 1e 84 40 00 40 06 cd 6e 6d f3 f1 76 E..`..@. @..nm..v
0020 82 b9 6c 82 df d0 00 35 24 49 75 9f 95 1a fd 4f ..l....5 $Iu....0
0030 80 18 00 e5 e9 a6 00 00 01 01 08 0a 00 09 6b 33 .....k3
0040 8b c7 b8 b7 00 01 01 00 00 01 00 00 00 00 00 .....
0050 67 ab a0 32 05 00 3a 02 f6 1b 70 67 d6 6f c0 9d g..2... ..pg.o..
0060 ad df 00 00 00 00 00 00 8d f0 00 00 00 00 00 00 .....

```

- 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

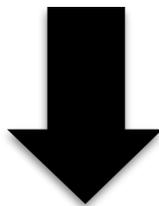


Bunitu Tunneled Proxy Protocol

```
1000156E PUSH DWORD PTR SS:[EBP-100]
10001574 CALL DWORD PTR DS:[1000CF7C] WS2_32.connect
1000157A CMP EAX,-1
1000157D JF lyhbyjo_.10001898
10001583 PUSH 0E
10001585 PUSH lyhbyjo_.10006D0E
1000158A PUSH DWORD PTR SS:[EBP-100]
1000158E CALL lyhbyjo_.10001372 send to C#C#2
10001595 PUSH 1388
1000159A PUSH 8
1000159C PUSH DWORD PTR DS:[1000C15E]
100015A2 CALL DWORD PTR DS:[1000CF30] ntdll.RtlAllocateHeap
100015A8 MOV DWORD PTR SS:[EBP-1BC],EAX
100015AE ADD EAX,4
10006D0E=lyhbyjo_.10006D0E
```

```
EFL 00000213 (NO,B,NE,BE,NS,PO,GE,G)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
```

Address	Hex Dump	ASCII	Comment
10006D0E	0E 00 A7 54 1A D9 4F A9	.#.T+.0e	016AFD54 00000168 h0..
10006D16	34 B2 21 04 00 00 00 00	##!+....	016AFD58 10006D0E #m.. lyhbyjo_.10006D0E
10006D1E	00 00 00 00 00 00 00 00	016AFD5C 00000000 #...
			016AFD60 016AFD68 hXj0 Pointer to next SEH record
			016AFD64 10001375 #t.. CF handler



```
1224 10836.46161( 95.211.178.145 164.127.231.183 TCP 68 domain > 47262 [FIN, ACK] Seq=1 Ack=1 Win=65520 Len=0 TSval=1267840651 TSecr=2719694
1225 10836.46529( 164.127.231.183 95.211.178.145 TCP 68 47262 > domain [ACK] Seq=1 Ack=2 Win=29312 Len=0 TSval=2719808 TSecr=1267840651
1243 10953.58754( 164.127.231.183 95.211.178.145 TCP 82 [TCP segment of a reassembled PDU]
1244 10954.05700( 164.127.231.183 95.211.178.145 TCP 82 [TCP segment of a reassembled PDU]
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP segment data (14 bytes)
0000 00 04 02 00 00 00 00 00 00 00 00 00 08 00 .....
0010 45 00 00 42 bd 9b 40 00 40 06 de 7e a4 7f e7 b7 E..B..@. @..~....
0020 5f d3 b2 91 b8 9e 00 35 9e 58 c2 bc 2e 42 af ce _.....5 .X...B..
0030 80 18 00 e5 74 b8 00 00 01 01 08 0a 00 29 f2 a0 ....t... ..)....
0040 4b 91 b6 8b 0e 00 a7 54 1a d9 4f a9 34 b2 21 04 K...T ..0.4.!..
0050 00 00 ..
```

Bunitu Tunneled Proxy Protocol - Registration

71	472.68549800	infected machine IP	95.211.15.37	TCP	76	56382 > domain [SYN] Seq=0 Win=292
72	472.74599100	95.211.15.37	infected machine IP	TCP	76	domain > 56382 [SYN, ACK] Seq=0 Ac
73	472.74604100	infected machine IP	95.211.15.37	TCP	68	56382 > domain [ACK] Seq=1 Ack=1 W
74	472.74683500	infected machine IP	95.211.15.37	TCP	82	[TCP segment of a reassembled PDU]

TCP segment data (14 bytes)

0000	00 04 02 00 00 00 00 00 00 00 00 00 00 00 08 00
0010	45 00 00 42 54 ed 40 00 40 06 17 67 6d f3 f1 76	E..BT.@. @..gm..v
0020	5f d3 0f 25 dc 3e 00 35 9c 63 ea de 82 67 22 41	..%.>.5 .c...g"A
0030	80 18 00 e5 fb 7c 00 00 01 01 08 0a 00 09 be 46F
0040	71 93 47 0c 0e 00 f6 1b 70 67 d6 6f c0 9d 21 04	q.G..... pg.o...!
0050	00 00	..

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 Len=0
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=1460
82	799.843613000	216.58.209.78	infected machine IP	TCP	76	http > 43396 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0
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
0020	a4 7f d5 f6 00 35 c1 eb 20 cd 89 4e 7a 22 00 1c
0030	80 18 04 11 09 f7 00 00 01 01 08 0a 89 f0 4e 2b
0040	00 15 5d a9 2e 00 00 00 f6 1b 70 67 00 00 00 00
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
0070	63 6f 6d 00 50 00

- 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

Bunitu Tunneled Proxy Protocol - Request

```

46001 14604.793308 95.211.178.145 1 infected machine IP TCP 1167 [TCP segment of a reassembled PDU]
46002 14604.793928 infected machine IP 2 178.21.154.49 HTTP 1119 GET /_1437584680576/rexdot.js?l=90
46003 14604.807346 91.103.137.65 infected machine IP HTTP 1459 HTTP/1.1 200 OK (application/javas
46004 14604.807373 infected machine IP 91.103.137.65 TCP 68 52721 > http [ACK] Seq=8147 Ack=57
46005 14604.807835 infected machine IP 95.211.178.145 DNS 1464 Dynamic update response 0x7931 Name
46006 14604.807865 infected machine IP 95.211.178.145 TCP 100 [TCP segment of a reassembled PDU]
46007 14604.851579 95.211.178.145 infected machine IP TCP 1464 [TCP segment of a reassembled PDU]
46008 14604.851610 95.211.178.145 infected machine IP TCP 672 [TCP segment of a reassembled PDU]
46009 14604.851666 infected machine IP 95.211.178.145 TCP 68 46309 > domain [ACK] Seq=6971932 Ac

TCP segment data (1099 bytes)

0040 00 63 f9 0e 47 04 00 00 fd e0 43 fd 00 00 00 00 .c..G... ..C....
0050 infected m. IP 4b 66 05 00 03 02 02 02 50 0a 00 00 m...Kf... ..P...
0060 54 09 00 00 d0 43 00 00 47 45 54 20 2f 5f 31 34 T...C.. GET /_14
0070 33 37 35 38 34 36 38 30 35 37 36 2f 72 65 78 64 37584680 576/rexd
0080 6f 74 2e 6a 73 3f 6c 3d 39 30 26 69 64 3d 30 69 ot.js?l= 90&id=0i
0090 54 67 49 75 63 59 6f 77 48 78 62 52 5a 48 67 5a TgIucYow HxbRZHgZ
00a0 55 74 48 65 55 50 5f 66 46 5a 43 4d 63 63 50 UtHeUUP_ fFZCMccF
00b0 5a 6d 74 61 34 35 4f 2e 62 2e 38 37 26 65 74 3d Zmta450. b.87&et=
00c0 76 69 65 77 26 68 73 72 63 3d 31 26 65 78 74 72 view&hsr c=1&extr
00d0 61 3d 26 66 72 3d 31 26 74 7a 3d 2d 31 32 30 26 a=&fr=1& tz=-120&
  
```

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

Bunitu Tunneled Proxy Protocol - Response

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

```

46002 14604.793928 infected machine IP 178.21.154.49 HTTP 1119 GET /_1437584680576/rexdot.js?l=90&id=01TgIucYo
46003 14604.807346 91.103.137.65 infected machine IP HTTP 1459 HTTP/1.1 200 OK (application/javascript)
46004 14604.807373 infected machine IP 91.103.137.65 TCP 68 52721 > http [ACK] Seq=8147 Ack=5775 Win=47360
46005 14604.807839 infected machine IP 95.211.178.145 DNS 1464 Dynamic update response Ox7931 Name exists[Malf
46006 14604.807869 infected machine IP 95.211.178.145 TCP 100 [TCP segment of a reassembled PDU]

0000 00 04 02 00 00 00 00 00 00 00 00 00 00 00 08 00 .....
0010 45 00 05 a8 35 a0 40 00 40 06 d1 88 6d f3 ad cf E...5.@. @...m...
0020 5f d3 b2 91 b4 e5 00 35 b6 e0 dc 62 66 49 15 e5 _.....5 ...bfI..
0030 80 10 05 a4 7f 5f 00 00 01 01 08 0a 00 63 f9 4d ..... c.M
0040 e2 03 de 99 90 05 00 00 fd e0 43 fd 00 00 00 00 ..... ..C...
0050 infected m. IP 4b 66 05 00 03 02 02 02 58 05 00 00 m...Kf.. ...X...
0060 cc 06 00 00 d0 43 00 00 01 48 54 54 50 2f 31 2e .....C... HTTP/1.
0070 31 20 32 30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d I 200 OK ..Cache-
0080 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 Control: no-cach
0090 65 2c 20 6e 6f 2d 73 74 6f 72 65 0d 0a 50 72 61 e, no-st ore..Pra
00a0 67 6d 61 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 gma: no-cache..C
00b0 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 ontent-T ype: app
00c0 6c 69 63 61 74 69 6f 6e 2f 6a 61 76 61 73 63 72 lication /javascr
00d0 69 70 74 3b 20 63 68 61 72 73 65 74 3d 75 74 66 ipt; cha rset=utf
00e0 2d 38 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e 63 6f -8..Cont ent-Enco
00f0 64 69 6e 67 3a 20 67 7a 69 70 0d 0a 45 78 70 69 ding: gz ip..Expi
0100 72 65 73 3a 20 2d 31 0d 0a 56 61 72 79 3a 20 41 res: -1. .Vary: A
0110 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 0d 0a ccept-En coding..
0120 50 33 50 3a 20 43 50 3d 22 42 55 53 20 43 55 52 P3P: CP= "BUS CUR
0130 20 43 4f 4e 6f 20 46 49 4e 20 49 56 44 6f 20 4f CONo FI N IVDo 0
  
```

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



A proxy but for what?



Who is using this and why?



Sentrant
Digital Advertising Integrity



Malwarebytes

Proxy Honeyypot

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



Bunitu Proxy Traffic

```
GET http://whoer.net/images/facebook.png
  → 304 [no content] 516ms
GET http://whoer.net/images/bg_top.jpg
  → 304 [no content] 536ms
GET http://whoer.net/images/right_m.jpg
  → 304 [no content] 455ms
GET http://whoer.net/images/dots_b.jpg
  → 304 [no content] 449ms
GET http://whoer.net/images/socks5-1.gif
  → 304 [no content] 447ms
GET http://whoer.net/images/footer.jpg
  → 304 [no content] 473ms
GET http://www.google-analytics.com/r/__utm.gif?
  → 302 text/html 370B 234ms
GET http://mc.yandex.ru/metrika/watch.js
  → 301 text/html 184B 1.13s
>> GET http://counter.rambler.ru/top100.scn?
  → 200 image/gif 2.4kB 287ms
[4103/4103] ? :help [*:43879]
```



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.

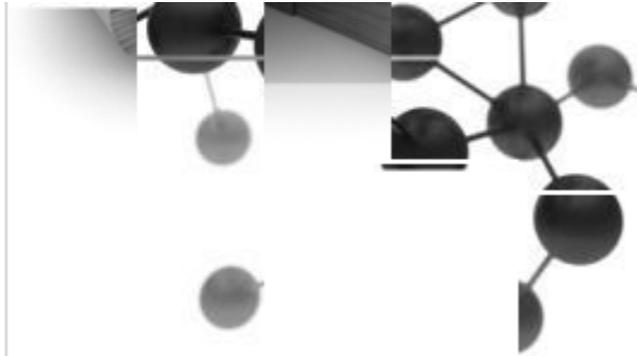


Bunitu Link to VIP72

```
→ 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%2F%2Fpublic&dp=%2F%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_mozai
c&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 31 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:

[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



Sentrant
Digital Advertising Integrity



Malwarebytes

What is VIP72

IP	country	region	city	uptime (hh:mm)	speed	timezone	
> 108	UNITED STATES	TEXAS	SAN ANTONIO	6:2	97	-06:00	
> 108	UNITED STATES	MISSOURI	-	3:43	98	-07:00	<input checked="" type="checkbox"/>
> 109	RUSSIAN FEDER...	ALTAISKY KRAI	-	18:3	99	+09:00	
> 187	MEXICO	DISTRITO FEDE...	-	5:33	98	-06:00	
> 190	ARGENTINA	DISTRITO FEDE...	BUENOS AIRES	0:16	96	-03:00	
> 213	ITALY	LOMBARDIA	MILANO	18:6	99	+01:00	
> 31.	SLOVAKIA	ZILINA	-	0:31	94	+01:00	
> 42.	VIET NAM	HO CHI MINH	-	2:49	98	+10:30	
> 84.	NETHERLANDS	GRONINGEN	GRONINGEN	18:2	100	+01:00	
> 93.	CROATIA	GRAD ZAGREB	ZAGREB	1:42	100	+01:00	
> 93.	UNITED KINGDOM	ENGLAND	-	0:4	99	+00:00	

reset

IP: 000 . 000 . 000 . 000 IP2geo

Get proxy by GEO Get proxy by IP

Traffic IN 1 KB / OUT 0 KB

Next page Hostname mask: Get proxy by Host

Ok

VIP72 VPN Client



Sentrant
Digital Advertising Integrity



Malwarebytes

Confirming VIP72 Resale of Bunitu Proxy Services

The screenshot shows the vip72.com website interface. The browser address bar displays `vip72.com/access/index.php?action=SocksAndProxies&RealIP=1`. The page header includes a search bar and navigation icons. Below the header, there's a main menu with options like Home, Logout, and Premium Zone. A secondary menu includes Tickets, Socks / Proxy, History, Account Settings, BUY proxy, and BUY OpenVPN. The main content area features a search filter for SOCKS ports, with a callout pointing to a specific port value. Below the search filters is a table of proxy results. A callout points to a specific IP address in the table, identifying it as 'HoneyPot #2 (current) IP'. Another callout points to the 'HOST' column of the same row, identifying it as 'HoneyPot #1 (original registration) IP'. The table has columns for IP, Checker, Date, Up Time, HTTP, Socks, Reply, HOST, Country, City, and State. The bottom of the page shows a summary of countries and a 'Premium Zone' status.

Viewed proxies: 540, Limit views: [redacted]

Main menu: Home, Logout, * Premium Zone *

Tools: Tickets, Socks / Proxy, History, Account Settings, BUY proxy, BUY OpenVPN

Not enough IP online ? YOU HAVE FREE ACCT
DOWNLOAD SOCKS CLIENT and use 15000-

Search by: SOCKS Port: [redacted] [redacted]
On Line (hours): < [redacted]

Country: [redacted]
State \ Region: please select country
City: please select region

Activate filter | Reset filter

Activate search | Reset search

HoneyPot #2 (current) IP

HoneyPot #1 (original registration) IP

IP Checker	Date	Up Time	HTTP	Socks	Reply	HOST	Country	City	State
[redacted]	2015-07-01 [redacted]	[redacted]	[redacted]	[redacted]	0.00	[redacted]	CANADA	[redacted]	[redacted]

Begin | Prev page | Next page | End

Countries

Country	Count	Percentage
CANADA	1	100.00 %

Total records: 1 (100%)

* Premium Zone * TOP Online: 18983

UNITED STATES	7433
CANADA	1586
FRANCE	866



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.medianter.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.medianter.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

Observations from PL client



Other Anonymizing VPN Services Involved

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

No.	Time	Source	Destination	Protocol	Length	Info
29370	3442.2807490	[REDACTED]	5.134.210.132	HTTP	653	POST /NewItem/Preview.php HTTP/1.1
34138	3466.5686870	infected machine IP	23.52.59.27	OCSP	500	Request
34151	3466.6785620	infected machine IP	23.52.59.27	OCSP	500	Request
34287	3470.2361710	infected machine IP	23.52.59.27	OCSP	500	Request...

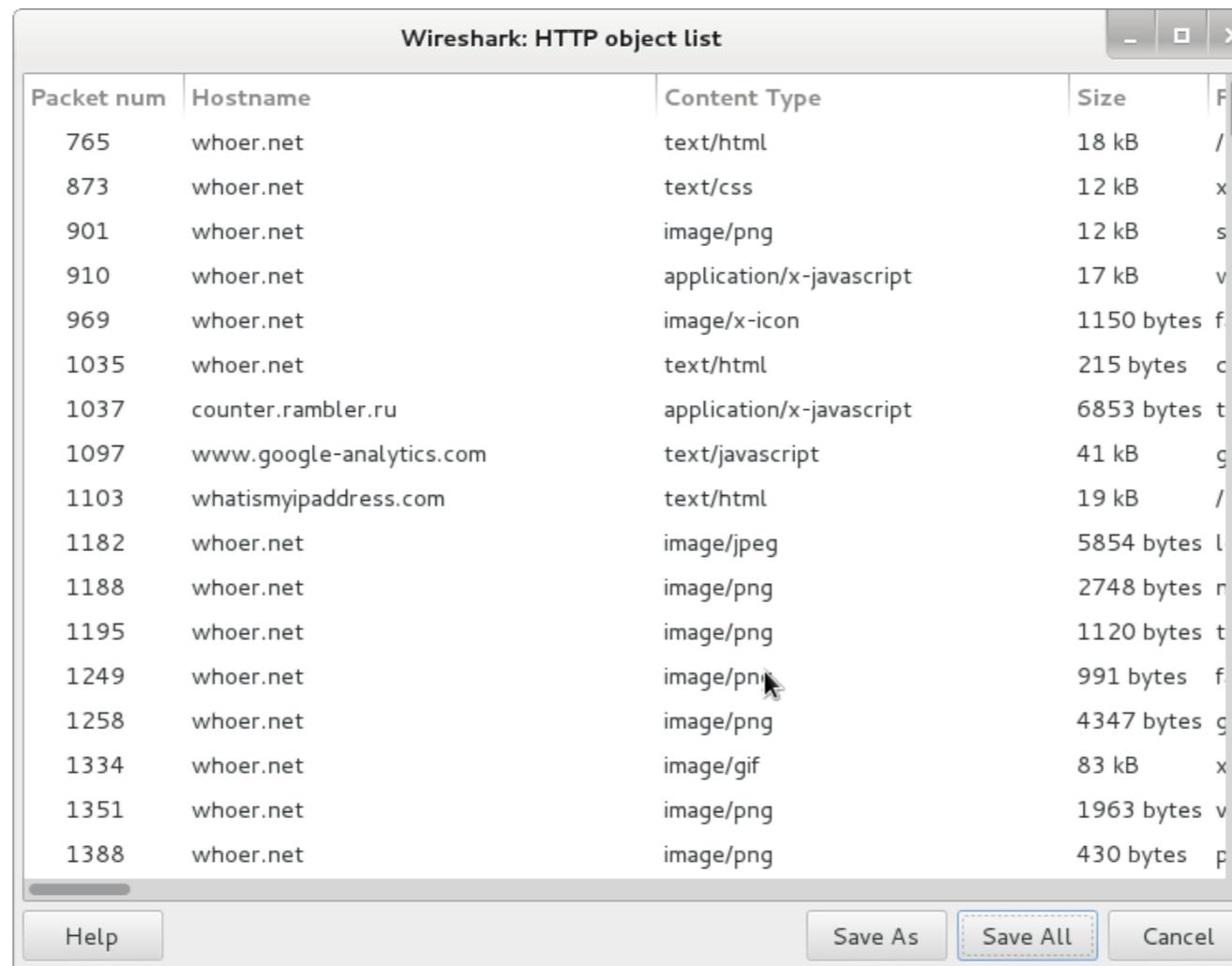
Hypertext Transfer Protocol

```
POST /NewItem/Add.php/process HTTP/1.1\r\nHost: allegro.pl\r\nUser-Agent: Mozilla/5.0 (Windows NT 5.1; rv:38.0) Gecko/20100101 Firefox/38.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: pl,en-US;q=0.7,en;q=0.3\r\nAccept-Encoding: gzip, deflate\r\nReferer: http://allegro.pl/NewItem/Preview.php\r\n[truncated] Cookie: allcg=cla8cc; __gfp_64b=-TURNEDOFF; cartUserId=
```

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



Other Anonymizing VPN Services Involved



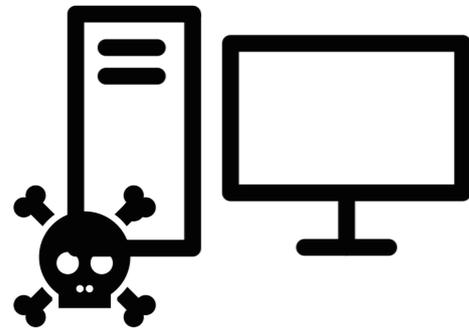
The image shows a screenshot of the 'Wireshark: HTTP object list' window. The window contains a table with the following columns: Packet num, Hostname, Content Type, Size, and File Name. The data is as follows:

Packet num	Hostname	Content Type	Size	File Name
765	whoer.net	text/html	18 kB	/
873	whoer.net	text/css	12 kB	x
901	whoer.net	image/png	12 kB	s
910	whoer.net	application/x-javascript	17 kB	v
969	whoer.net	image/x-icon	1150 bytes	f
1035	whoer.net	text/html	215 bytes	c
1037	counter.rambler.ru	application/x-javascript	6853 bytes	t
1097	www.google-analytics.com	text/javascript	41 kB	g
1103	whatismyipaddress.com	text/html	19 kB	/
1182	whoer.net	image/jpeg	5854 bytes	l
1188	whoer.net	image/png	2748 bytes	r
1195	whoer.net	image/png	1120 bytes	t
1249	whoer.net	image/png	991 bytes	f
1258	whoer.net	image/png	4347 bytes	g
1334	whoer.net	image/gif	83 kB	x
1351	whoer.net	image/png	1963 bytes	v
1388	whoer.net	image/png	430 bytes	p

Users often start surfing by checking their new IP address



Distributors (Theory)



Infected Proxy Bot

1) Register the bot

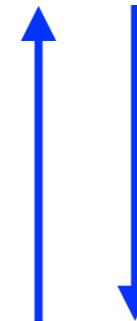


4) Send command from the distributor



Bunitu C2 (Middleman)

3) Send commands to my bots



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



Distributor (ie. VIP72)



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

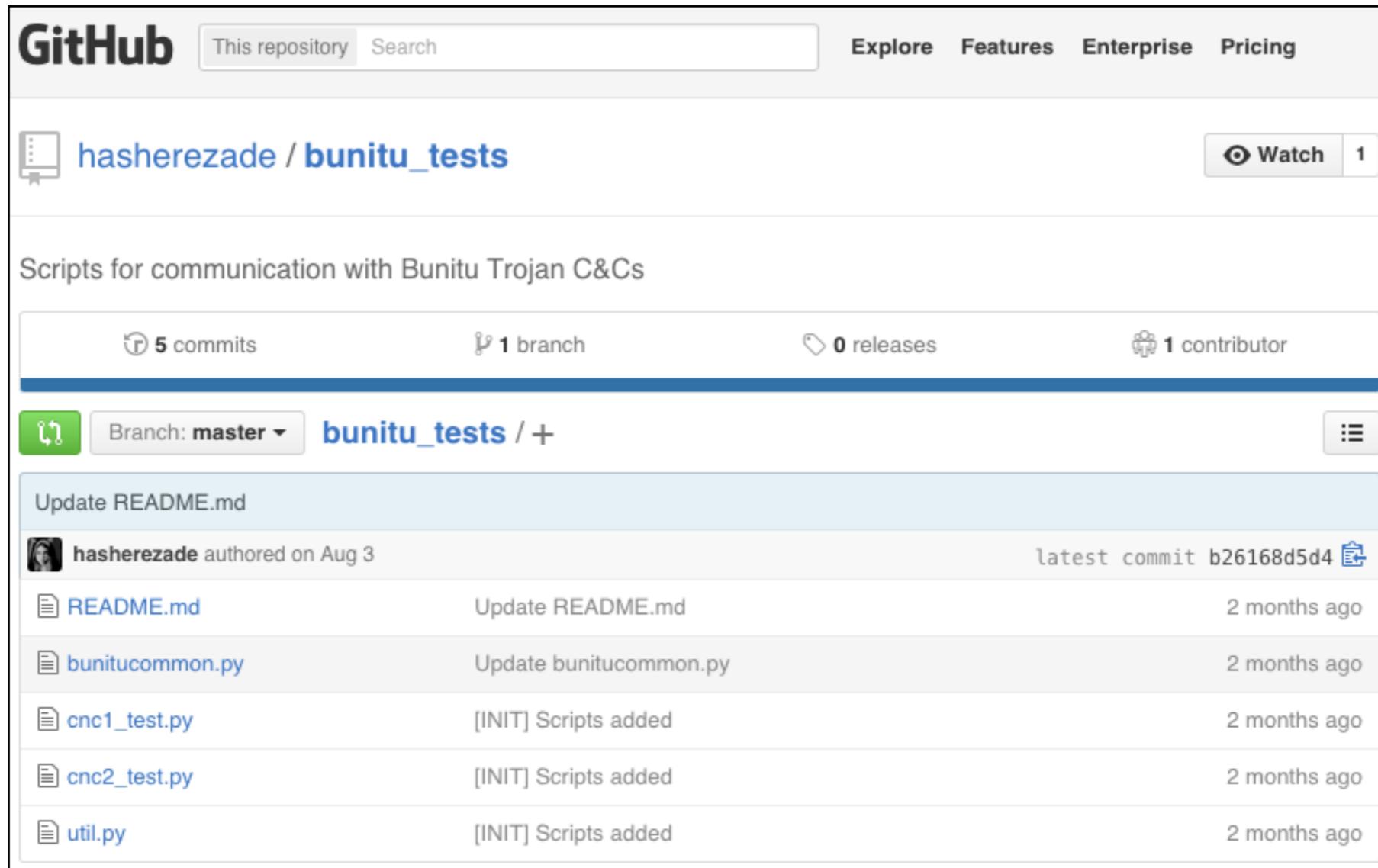


The (lack of) Evolution in Bunitu/VIP72

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



Building On Our Research



The screenshot shows the GitHub interface for the repository 'hasherezade / bunitu_tests'. The repository is described as 'Scripts for communication with Bunitu Trojan C&Cs'. It has 5 commits, 1 branch, 0 releases, and 1 contributor. The current branch is 'master'. The commit history shows a recent update to 'README.md' by 'hasherezade' on August 3, with the latest commit ID 'b26168d5d4'. Below this, a list of files is shown with their commit messages and dates:

File	Commit Message	Time
README.md	Update README.md	2 months ago
bunitucommon.py	Update bunitucommon.py	2 months ago
cnc1_test.py	[INIT] Scripts added	2 months ago
cnc2_test.py	[INIT] Scripts added	2 months ago
util.py	[INIT] Scripts added	2 months ago

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
a1 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 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 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

