TeleTrusT
Pioneers in IT security.

Informationstag "IT-Forensik"

Berlin, 12.05.2016

ElasticZombie - Einblicke in ein ElasticSearch - Botnet

Markus Manzke, 8ack GmbH Kiel

Vorstellung

- Markus Manzke - Leiter Technik 8ack GmbH
- Sprecher u.a. SLAC, CeBIT, OWASP
- 8ack
  - sensorbasierte Aufklärung (Honeypots)
  - Fokus auf Datacenter, Cloudprovider, Online-Rechenzentren

Einführung

- serverbasierte Botnetze allgemein
- ElasticSearch - Botnetz im Speziellen
  - Aufbau
  - Betrieb
  - Targets

Warum existieren Botnetze (Techniksicht)

- günstige 24/7 Cloudserver (5$/Monat)
- vorkonfigurierte Instanzen (1-Click-Installation)
- DevOps for Dummies: Funktion über Sicherheit
- „moderne“ Software, unsicher by Design

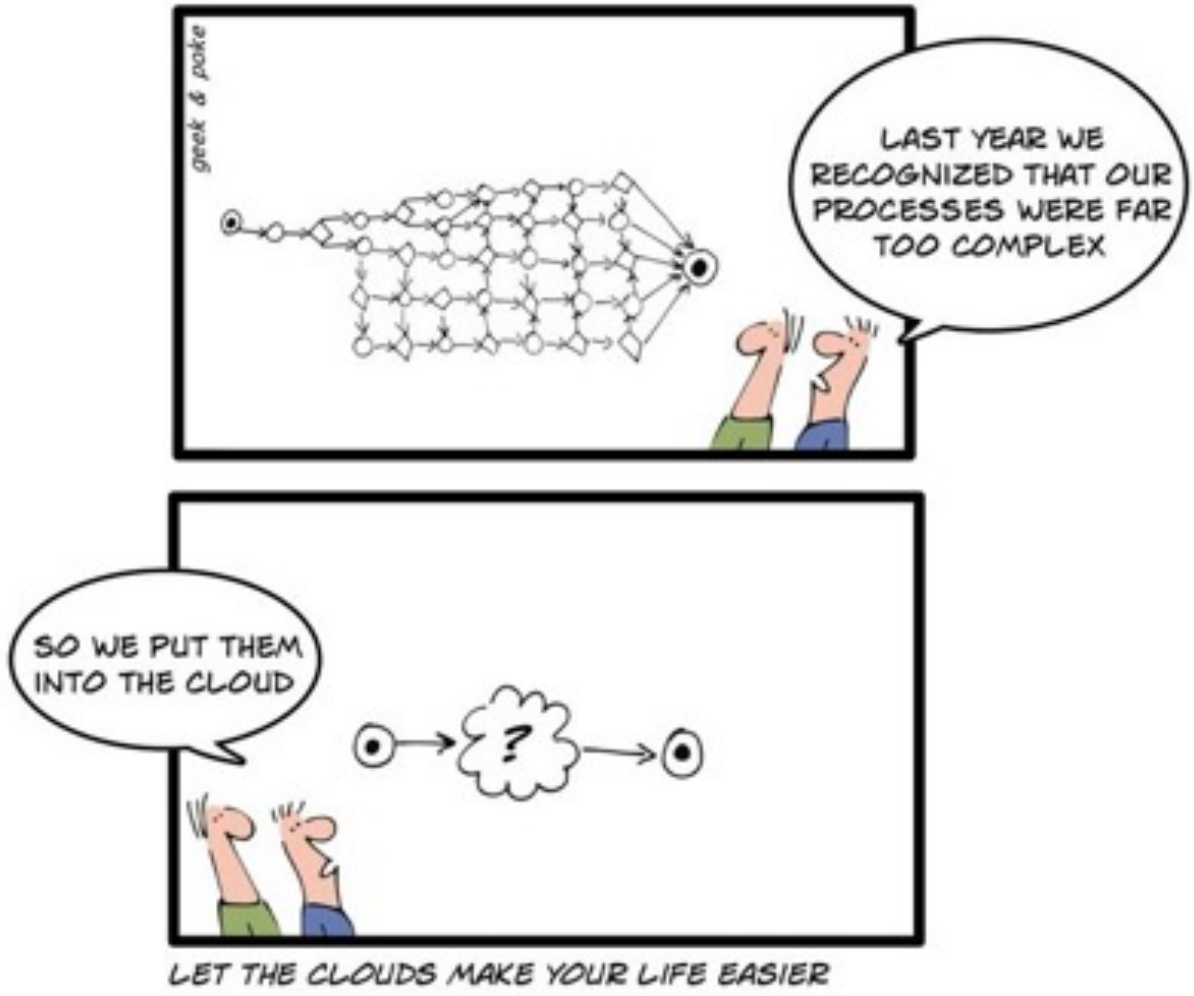
- viele Server + viele Sicherheitslücken == ideales Biotop für Botnetze

Warum existieren Botnetze (Techniksicht)

- neue Technologien erleichtern Botmastern das Leben:
  - shodan => weltweite Scan/Indizierungsengine
  - „moderne“ Technologien bedingen häufig manuelles Setup -> keine automatischen Updates
  - zmap, masscan: internetweite Scans in 4-24h
- Automatisierung: mehrer 100 Scans/Exploitversuche pro Tag und IP, Gießkannenmethode

Warum existieren Botnetze

- die Realität:



Zahlen

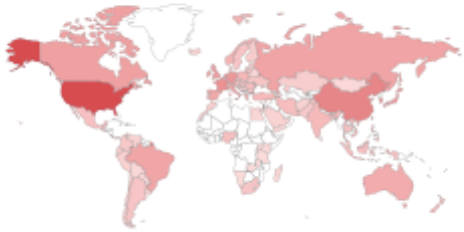
- ElasticSearch: 150.000 exploitbare Instanzen
- Redis: 40.000 exploitbare Instanzen
- MongoDB: 20.000 exploitbare Instanzen

- 60% der im Internet betriebenen Applikationen haben Sicherheitslücken

- POC: 5000 Server in 24h
- ca 200.000 Server in Botnetzen aktiv

Zahlen

TOP COUNTRIES



Hong Kong	170,140
United States	35,958
China	4,349
France	2,486
Germany	1,842

Total results: 230,950

54.173.139.217

ec2-54-173-139-217.compute-1.amazonaws.com

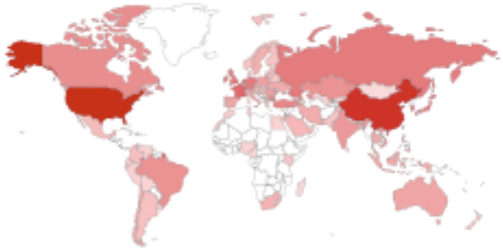
AMAZON

Added on 2016-05-10 11:28:42 GMT

United States, Ashburn

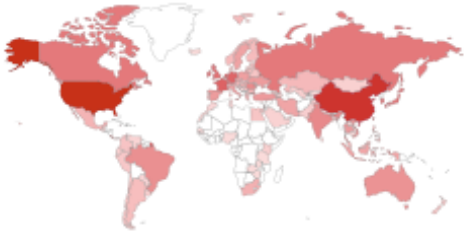
Details

TOP COUNTRIES



United States	24,794
China	16,228
Netherlands	2,628
France	2,546
United Kingdom	1,349

TOP COUNTRIES



United States	10,718
China	6,091
Netherlands	1,497
France	1,415
Singapore	1,277

Total results: 30,861

37.139.2.8

Cloud Hosting

Added on 2016-05-10 11:28:42 GMT

Netherlands, Amsterdam

Details

832.0 MB	6 Databases

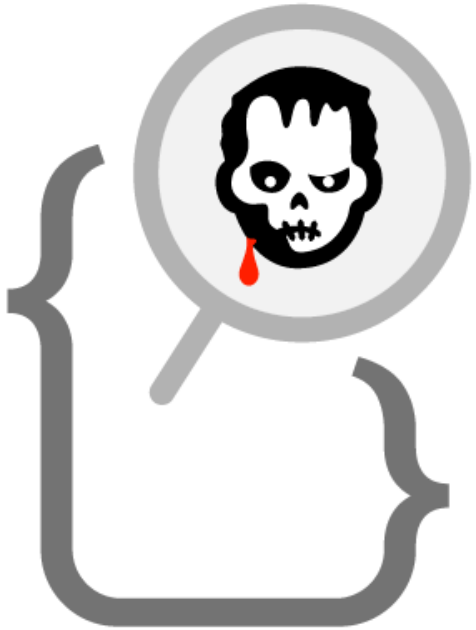
Database Name	Size
Weather	208.0 MB
TTKCities	208.0 MB

Warum existieren Botnetze - Botmaster-POV

- Botnetze offerieren lohnende Geschäftsmodelle
  - DDoS as a Service (Booter/Stresser)
  - Erpressung mit DDoS (Armada, DD4BC)
  - SPAM-Versand
  - Vermietung

ElasticZombie

- Aufbau eines weltweit verteilen Honeypot-Netzwerks zum Fangen und Analysieren von BotWare
- eigene Honeypot- und Analyse-software (Codeanalyse & Sandbox)
- August 2015-Mai 2016: 650Bots gefangen, 50 unique Bots, 2 Bot-Familien, 8 C&C



ElasticZombie - The Grunge

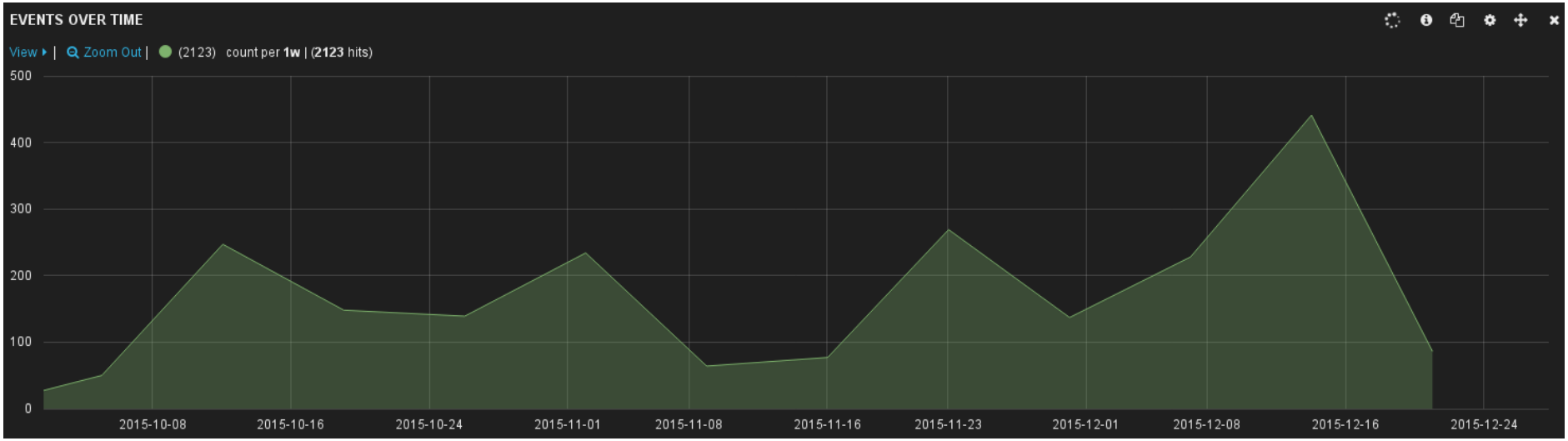
Dashboard :: total: 192

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

ElasticZombie - Daten

- Bots: ELF-Malware mit hardcodierten C&C-Servern, 40% nicht (mehr) lauffähig, da zu alt

- Wellen: 10-60 Scans („Infektionen“) / Tag / Sensor



ElasticZombie - Bots klassifiziert

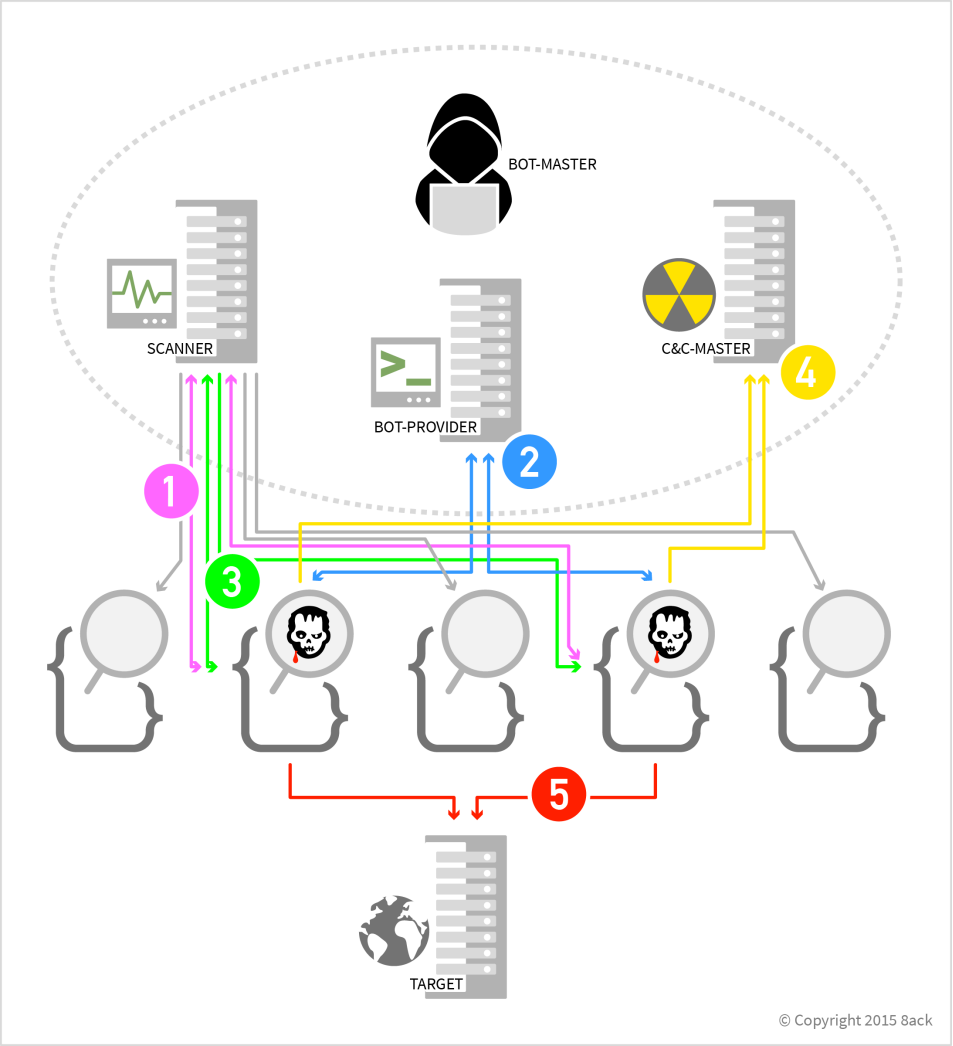
- 2 Arten / 1. Typ:
  - Fire & Forget - Bots (BillGates - Family, 2013)
  - keine Installation
  - nach Drop -> melden sich beim C&C und warten auf Befehle
  - TCP/SynFloods, Reflection/Amplification mit dynamisch aktualisierten Reflection-Zielen
  - unverschlüsselte Kommunikation

ElasticZombie - Bots klassifiziert

- 2. Typ:
  - intelligente(re) Bots (IptabLex/IptabLes, 2014)
  - systemweite Installation, überlebt Reboot
  - erweiteres CommandSet, kann DDoS, Scannen, individuelle Befehle ausführen
  - verschlüsselte Kommunikation

ElasticZombie - von der Infektion zum Angriff

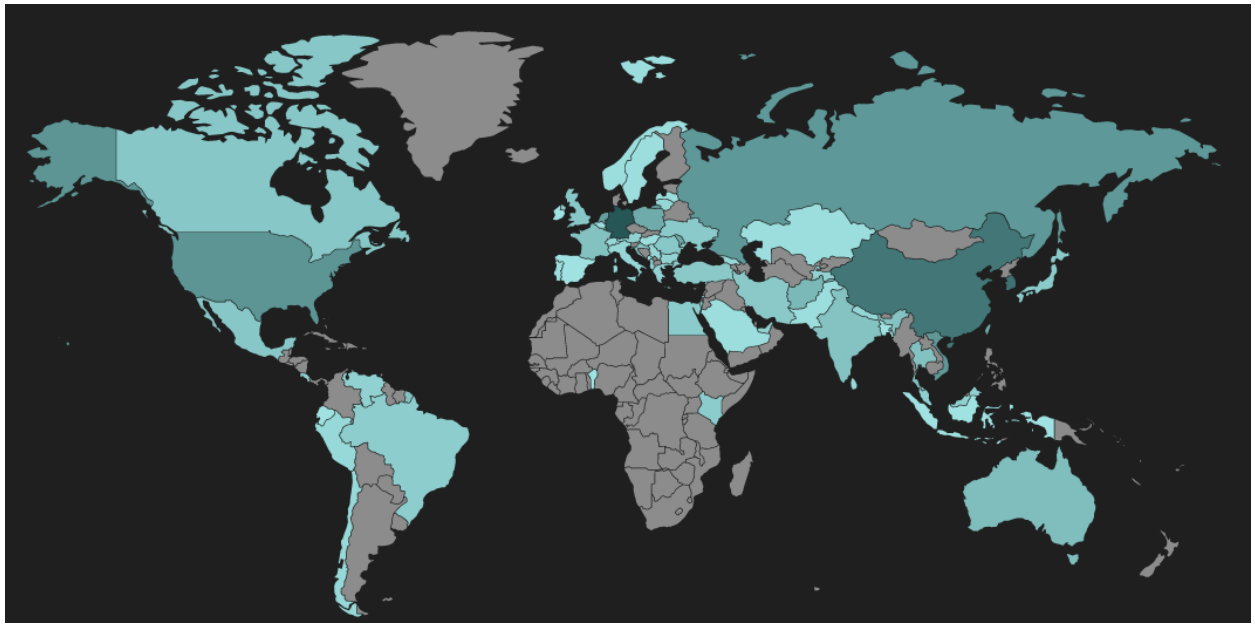
- 1 - Scan
- 2 - Bot Download
- 3 - Bot Execution
- 4 - C&C-Comms
- 5 - Angriff



ElasticZombie - Infrastruktur

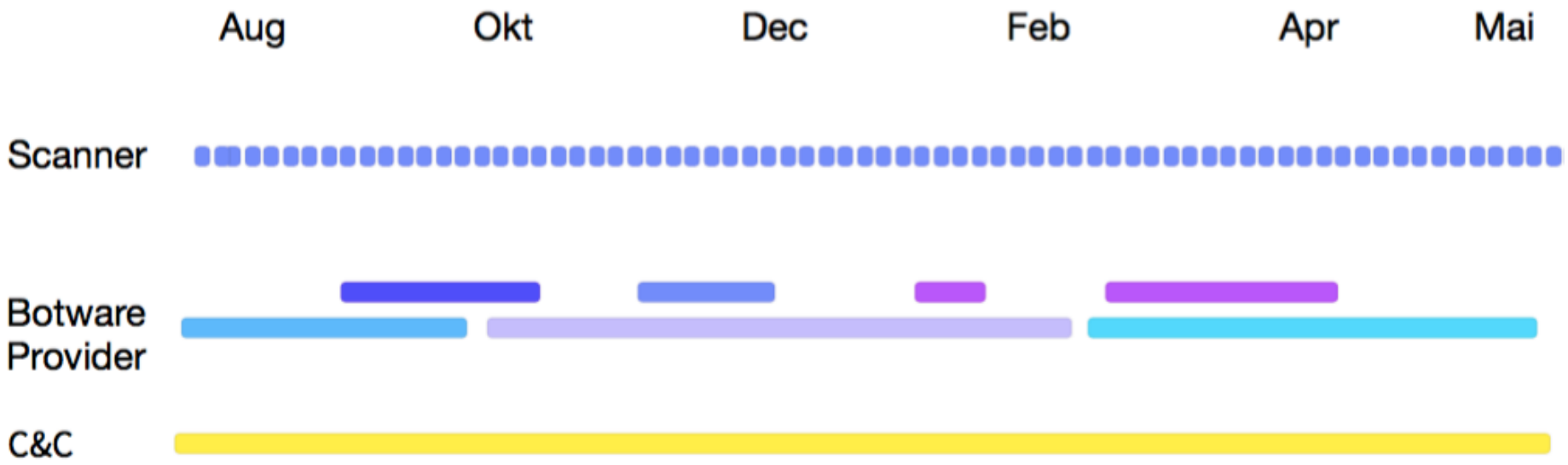
- Scanner / Botware-Provider:
  - gehackte Server, häufiger Wechsel (1-2 Tage), Provider mehrere Wochen, weltweit

- C&C - Server
  - China, seit 2014/15
  - immernoch aktiv

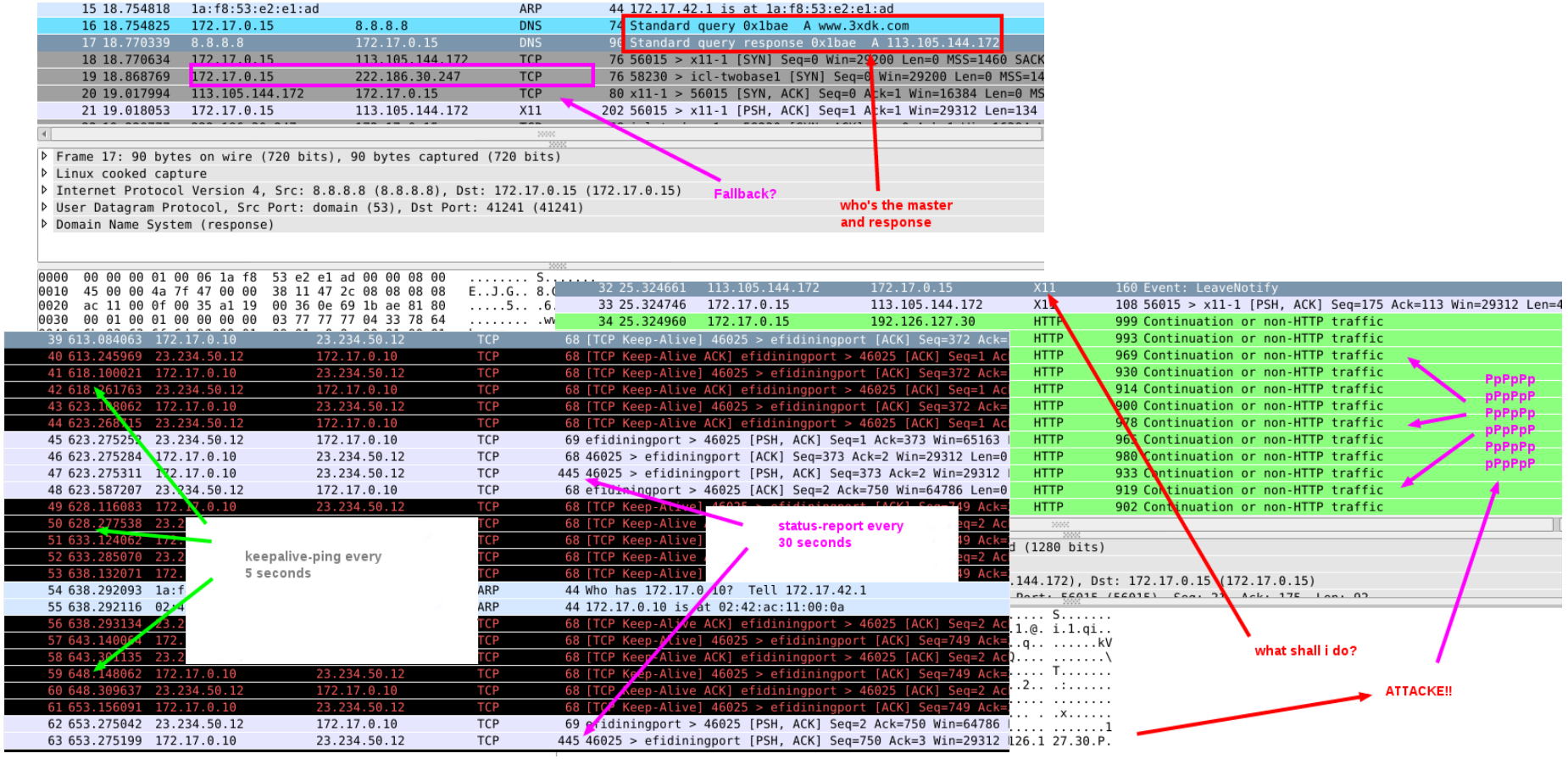


ElasticZombie - Infrastruktur

- zeitlicher Verlauf



ElasticZombie - Exploit / C&C-Comms



ElasticZombie - Angriffswerte

- 1-10 Angriffe / Tag
- bis zu 3 Tagen idle-Time zwischen Angriffen
- kürzester Angriff: 30 Minuten
- längster Angriff: 15 Tage
- kein Booter-Service, wahrscheinlich DDoS-Erpressergruppe
- Ziele: 70% asiatischer Raum, 30% Nordamerika
- Hoster, Gaming-Provider, ISPs

ElasticZombie - Analyse des Botmaster-Verhaltens

- keinerlei Vorsichtsmaßnahmen
- Bots können jederzeit und überall ausgeführt werden
- schwache Obfuscation der C&C-IPs & Hostnamen

ElasticZombie

Fragen ?