DDoS - Paketschießstand

SLAC 24.05.2016 Berlin

zeroBS GmbH

Agenda

- $ whoami
  Markus Manzke
  Leiter Technik zeroBS GmbH
  Botnetz-Tracking seit 2007

- zeroBS GmbH
  „scratching the glitter from the cyber“
  Enisa Networking Group

Intro + TOC

- Mirai Mirai on The Wall
  - Überblick über das aktuell populärste IoT-Botnetz
- Abwehrfähigkeit messen
  - kurze Einführung in den DDoS Resiliency Score (DRS)
- Tools der Verteidiger
- Feuer Frei

Mirai

- Betreiber: etablierte Gangs, weltweit
- Motivation/Businessmodell: DDoS, Bitcoins
  - Erpressung
  - DDoS as a Service
- Größe: 20.000 - 50.000 Bots
- Lücke(n):
  - IoT, Kameras, DSL-Router
  - Hardcoded Passwords, alle Services als root, Updates … welche updates?

Mirai

- DDoS:
  - alle Varianten Volumenangriffe sehr effektiv
  - Layer 7 (HTTP, DNS)
  - überwinden von DDoS-Schutzservices möglich
- Command & Control: IRC, Pong-Receiver
- Bots: ELF-basierte Linux-Malware
- Preise: 27$/Tag

Botnetz-Infektion Workflow

- Mirai, ElasticZombie

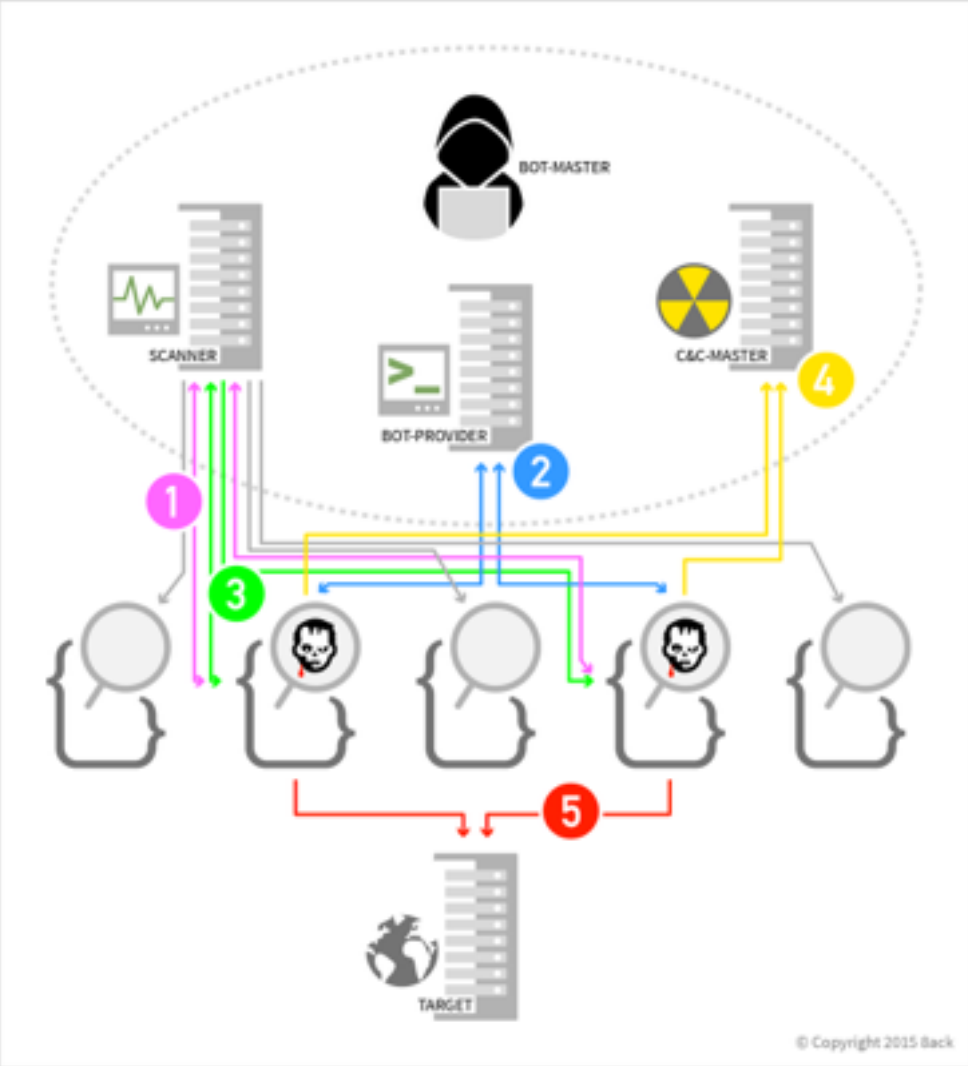
  1. Scan

  2. Exploit + Bot

  3. Bot aktivieren

  4. C&C - Comms

  5. Ziel angreifen



Botnetz - Kaufen

Botnetz - Kaufen

amelia75 | User Profile

View Store
Send Message
Favorite
Blacklist

amelia75(1110) Vendor Level 5 Trust Level 5

Positive feedback (last 12 months): 99%
[How is the feedback score calculated?]

Member since: July 7, 2016
Contracts: 0 in progress, 0 complete

Seller Feedback Ratings ?

	1 month	6 months	12 months
			(last 12 months)
Positive			12
		72	234
Neutral			0
		0	1
Negative			0
		1	1

Buyer Statistics ?

	Since join
	(since join date)
Total disputes / orders	0 / 96
Total spendings	---
Feedback left	67 (97.0% positive)
Last online	

Description | Bids | Feedback | Refund Policy

Listing Feedback

Buyer	Date	Time	Comment
g**e	March 30, 2017	19:25	PERFECT
G**8	March 30, 2017	01:31	Great service, worked like a charm on a deserving target
b**o	March 29, 2017	23:41	Perfect Work
k**7	March 29, 2017	18:18	perfect
k**7	March 29, 2017	18:17	perfect
m**6	March 27, 2017	20:39	Very very good job
s**r	March 27, 2017	20:29	Can penetrate Cloudflare. Amazing.
B**g	March 27, 2017	01:23	Amazing
p**_	March 26, 2017	19:15	Thank you very much! This service is highly recommended!
s**r	March 26, 2017	12:44	Great service as always
s**r	March 24, 2017	13:27	Quick and great execution!
p**_	March 23, 2017	20:20	Perfect service! Thank you!
s**r	March 23, 2017	12:35	Great service. Quick to respond. Highly recommend.
p**_	March 22, 2017	19:56	Great service as always. Thank you!

Mirai - Was bisher geschah

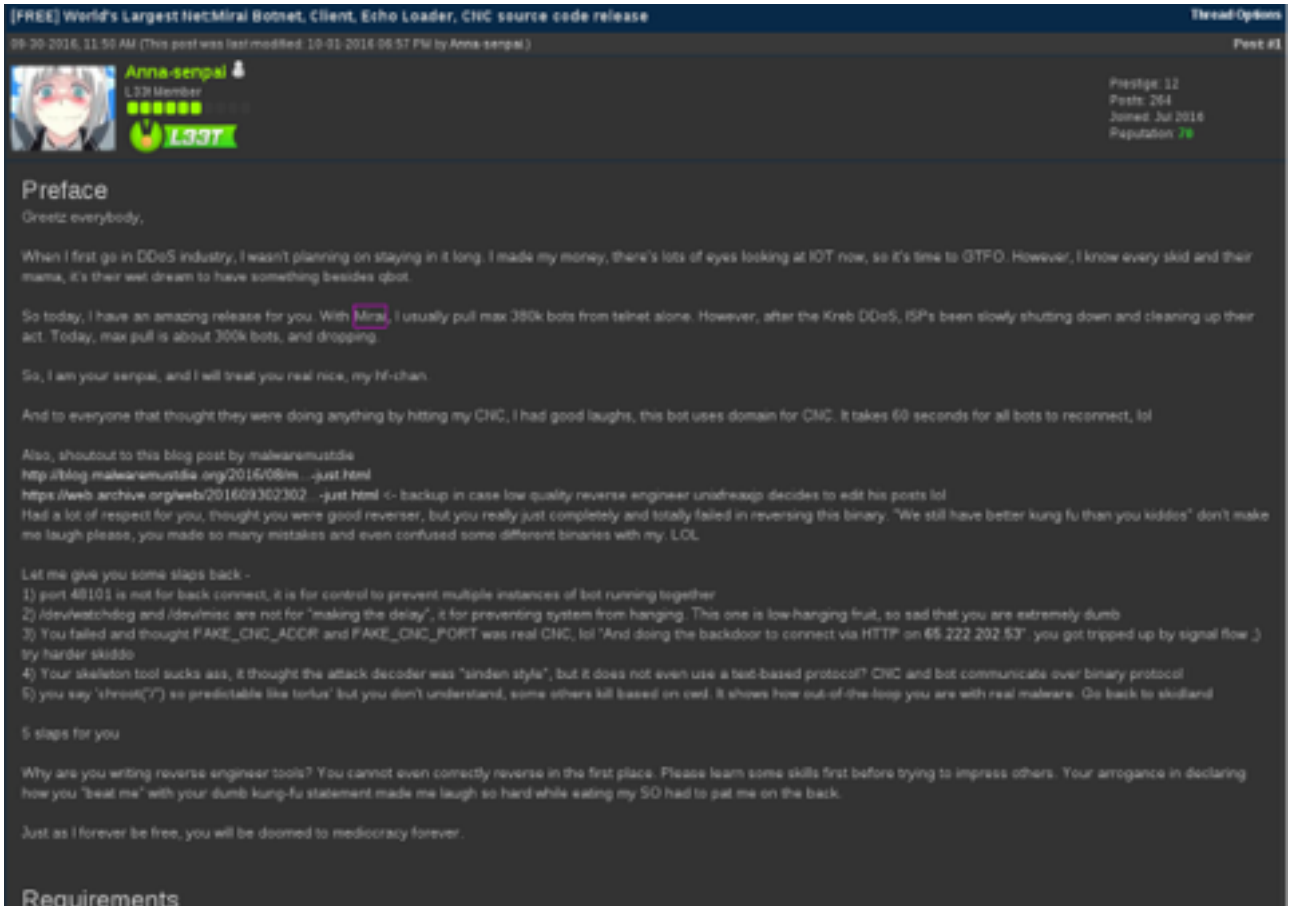
- Aug 2016. - BigBrother Attack
- 3-Wochen-Kampagne gegen Online-Möbelhändler
- von uns analysiert: alles CCTV-Kameras

Mirai - Was bisher geschah

- 21. 09. - Angriff auf KrebsOnSecurity - Akamai gibt auf

Mirai - Was bisher geschah

- 30.09. - Mirai-Release



[FREE] World's Largest NetMirai Botnet, Client, Echo Loader, CNC source code release

Thread Options

09-30-2016, 11:50 AM (This post was last modified: 10-01-2016 06:57 PM by Anna-senpai.)

Post #1

Anna-senpai

L33t Member

L33T

Prestige: 12
Posts: 264
Joined: Jul 2016
Reputation: 76

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's time to GTFO. However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, ISP's been slowly shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

And to everyone that thought they were doing anything by hitting my CNC, I had good laughs, this bot uses domain for CNC. It takes 60 seconds for all bots to reconnect, lol

Also, shoutout to this blog post by malwaremustdie
http://blog.malwaremustdie.org/2016/08/m...-just.html
https://web.archive.org/web/20160930230230...-just.html <- backup in case low quality reverse engineer unixfreaxjp decides to edit his posts lol
Had a lot of respect for you, thought you were good reverser, but you really just completely and totally failed in reversing this binary. "We still have better kung fu than you kiddos" don't make me laugh please, you made so many mistakes and even confused some different binaries with my. LOL

Let me give you some slaps back -
1) port 48101 is not for back connect, it is for control to prevent multiple instances of bot running together
2) /dev/watchdog and /dev/misc are not for "making the delay", it for preventing system from hanging. This one is low-hanging fruit, so sad that you are extremely dumb
3) You failed and thought FAKE_CNC_ADDR and FAKE_CNC_PORT was real CNC, lol "And doing the backdoor to connect via HTTP on 65.222.202.53" you got tripped up by signal flow ;) try harder skiddo
4) Your skeleton tool sucks ass, it thought the attack decoder was "sinden style", but it does not even use a text-based protocol? CNC and bot communicate over binary protocol
5) you say 'chroot("/") so predictable like torlus' but you don't understand, some others kill based on cwd. It shows how out-of-the-loop you are with real malware. Go back to skiddiland

5 slaps for you

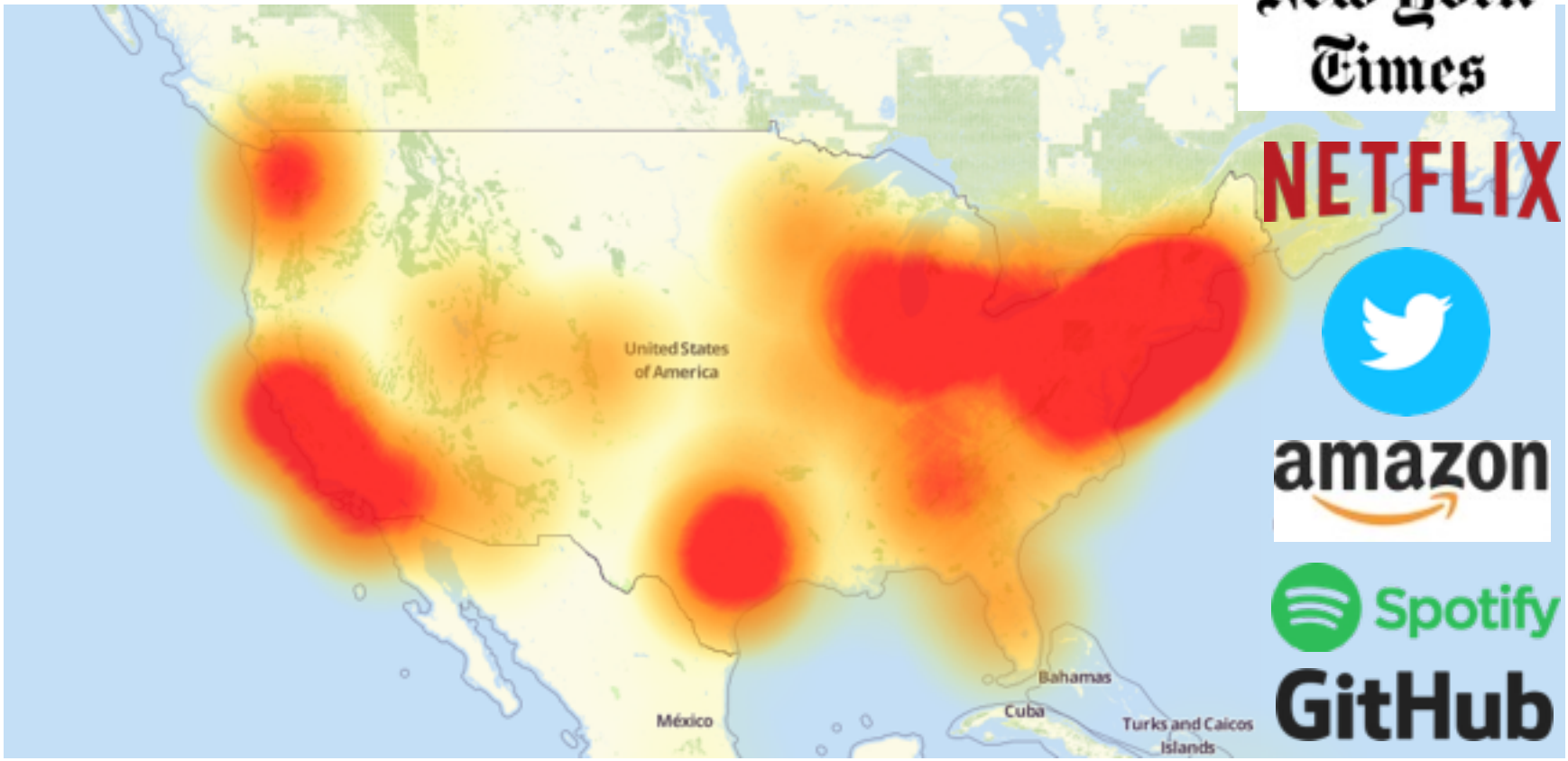
Why are you writing reverse engineer tools? You cannot even correctly reverse in the first place. Please learn some skills first before trying to impress others. Your arrogance in declaring how you "beat me" with your dumb kung-fu statement made me laugh so hard while eating my SO had to pat me on the back.

Just as I forever be free, you will be doomed to mediocracy forever.

Requirements

Mirai - Was bisher geschah

- 21. 10. - Angriff auf DYN



Mirai

- Wie groß ist Mirai?
  - 8ack: 20k
  - Akamai: 45k
  - Dyn: 50k
  - Palo Alto: 12k
- Apr 2017
  - 8 Mirai-Varianten im Tracking

Was bisher geschah

- Wieso ist Mirai solch ein Problem?
  - primär Layer 7 / Applikation
  - bewährte Verteidigungsmechanismen wirkungslos
  - Size DOES matter
  - IoT == private DSL-Anschlüsse
    == neue IPs alle 24h
  - Bedrohung für alle von
    DRS 3/4 auf DRS 5

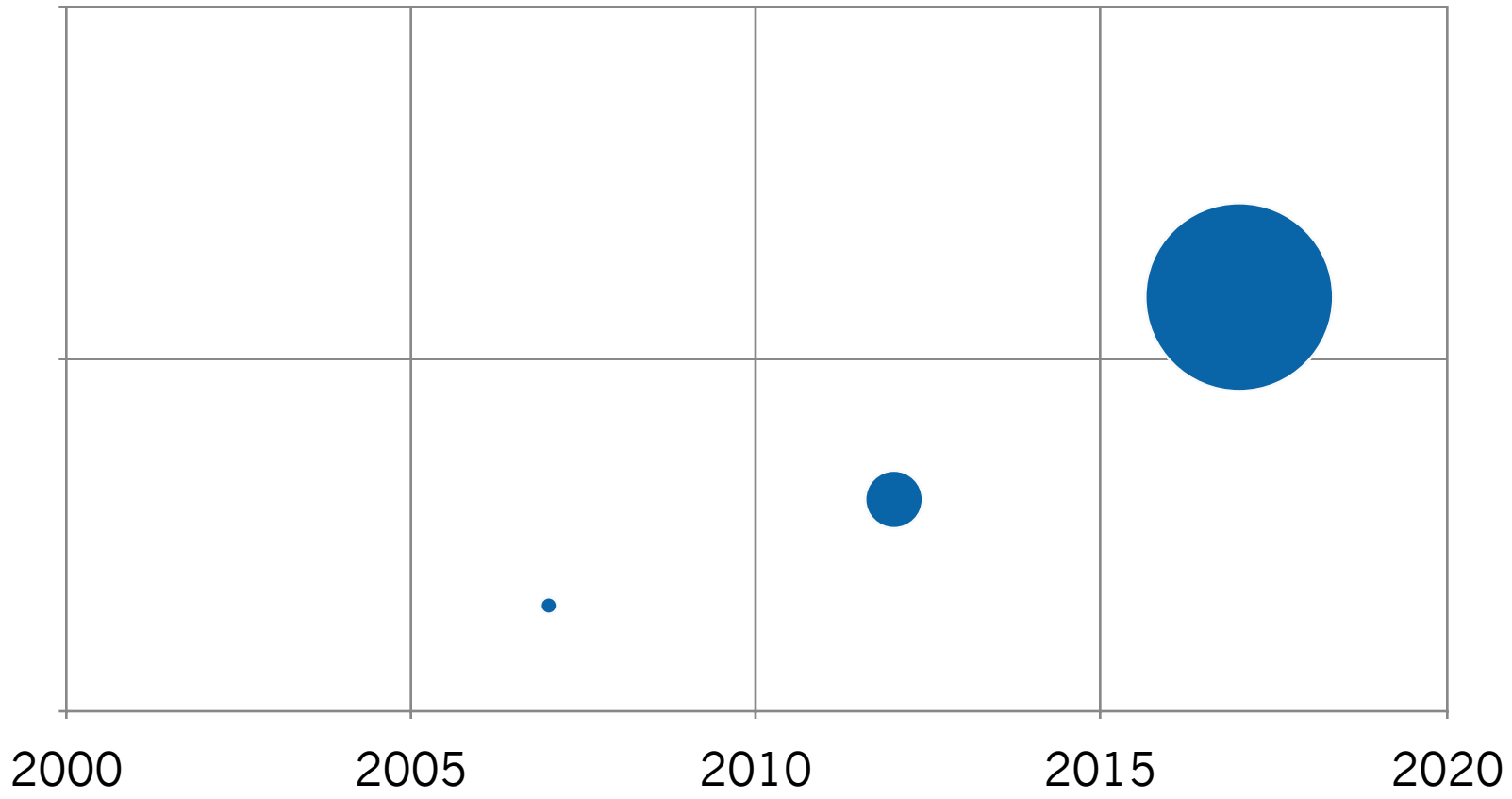
Evolution der Botnetze

	vor 2016	ab 2016
Größe (AVG)	1000 - 20.000	5000 - 50.000
Durchsatz	viel Traffic/Bot	wenig Traffic/Bot
Layer	primär 3/4 (Volumen) Layer 7 eher Ausnahme	alle Layer vermehrt Layer 7
Verteidigung	eher einfach Statistik	eher schwierig Verhalten
Time-To-Exploit	7d	< 24h

Evolution der Botnetze

	vor 2016	ab 2016
Preise	50$/h	25$/Tag
globale Bedrohung	abstrakt	real
Player	wenige, Covert	mehrere, Overt
Aussicht	alles im Griff	problematisch

Botnetz-Größe über die Jahre



Evolution der Botnetze

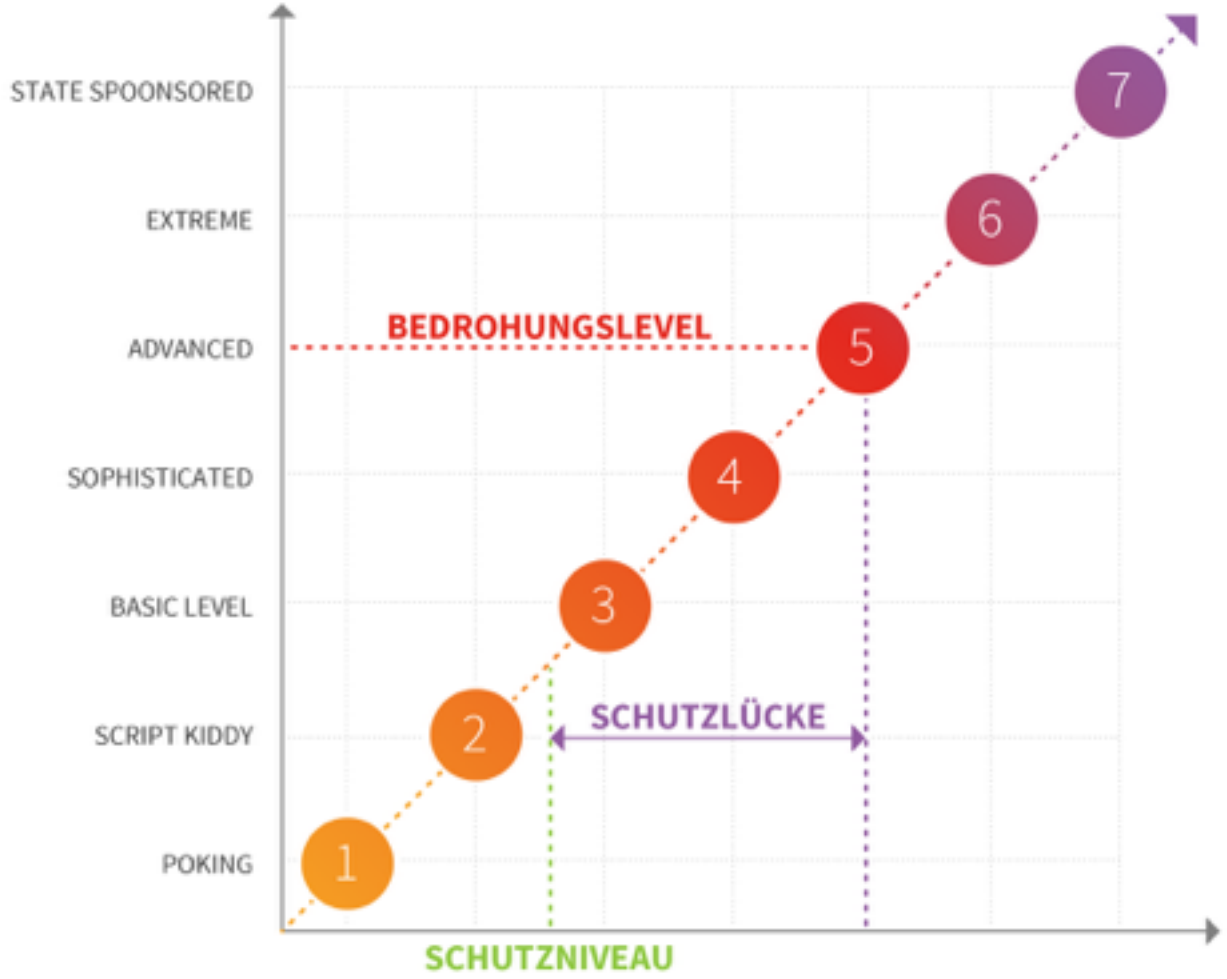
- hohe Professionalisierung des „Business“
- gute Erträge
- Kampf um knappe Ressourcen
- gute Codequalität
- Time-To-Exploit: < 24h

DDoS - Schutzlevel messen

- DDoS-Resilience-Score

Level	Bezeichnung	Volumen	RPS	Vektoren
1	Poking, Anklopfen	< 10MBit	1000	1
2	ScriptKiddy, Booter-Services	< 100 MBit	5000	2
3	Basic Level Professionals	< 1GBit	10000	5
4	Sophisticated Professional	< 10 GBit	100000	10
5	Advanced Professionals	< 100 GBit	1 Mio	no limit
6	Extreme Professionals	no limit	no limit	no limit
7	State Sponsored	no limit	no limit	no limit

DDos Resiliency Score - DDoS - Schutzlevel messen



State of DDoS

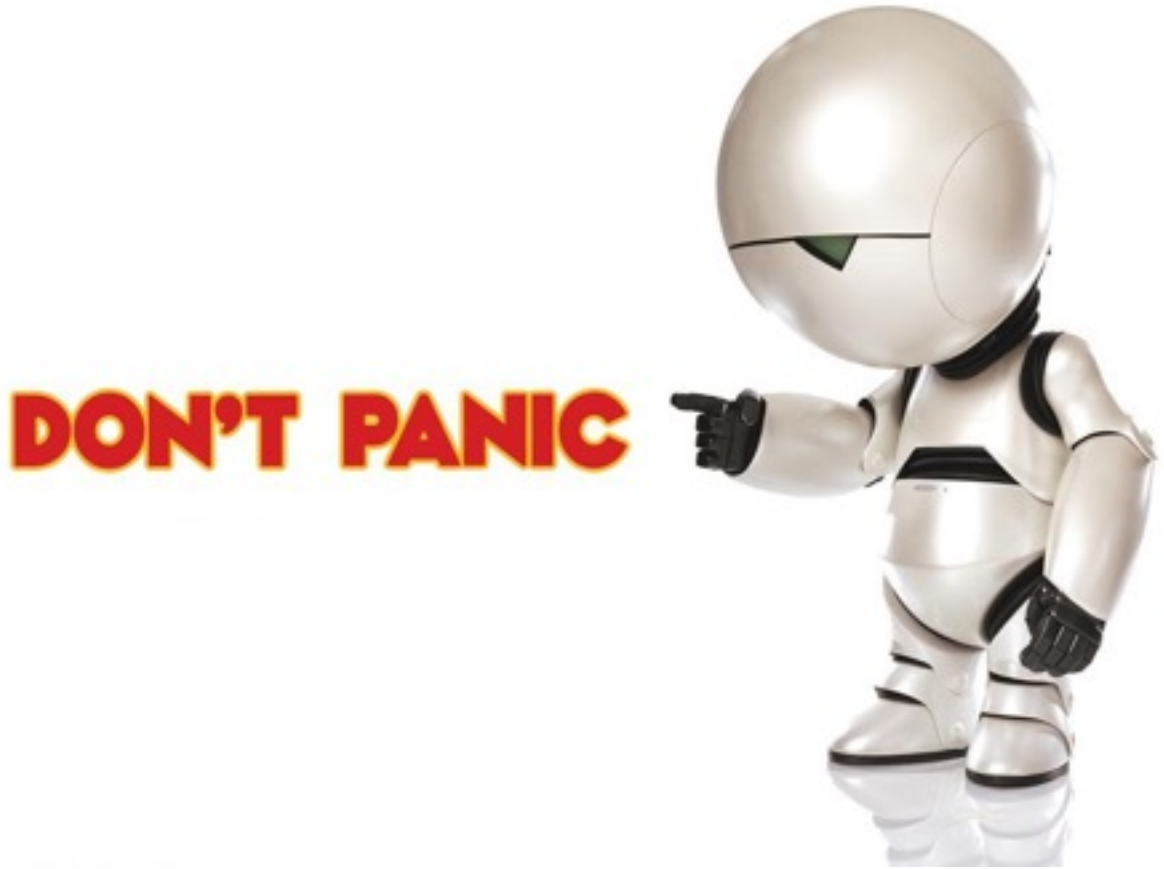
- die aktuellen großen DDoS-Botnetze sind in der Lage, nationale und internationale Internet-Infrastruktur zu gefährden

Ausblick

- weitere Zunahme der Layer-7-Angriffe (aktuell: 40%)
- Ausfall von Teilen des Internet
- irgendwann wird es jeden getroffen haben

- Verteidigung wird mit jedem großen Angriff besser
- heute + 5 Jahre wird die gesamte kommerzielle Kommunikation geschützt sein MÜSSEN

letzte Worte



Fragen?

slac@zero.bs