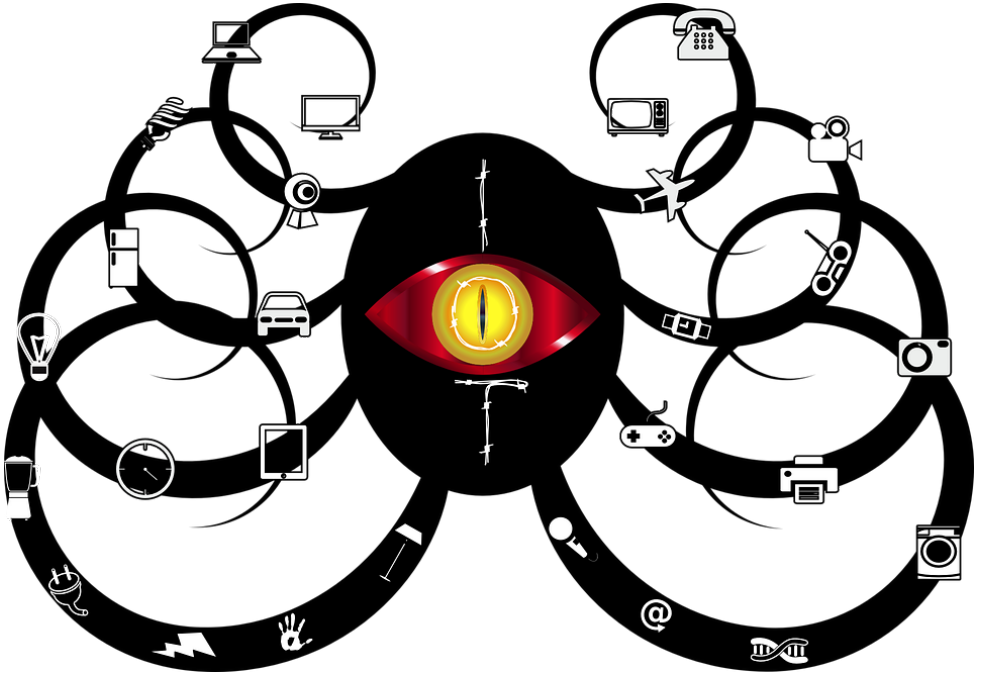
MATHEMA

Rise of the Machines

Wie Sicherheitslücken im IoT das Internet gefährden

Nikolas May

Hristiyan Pehlivanov



Agenda

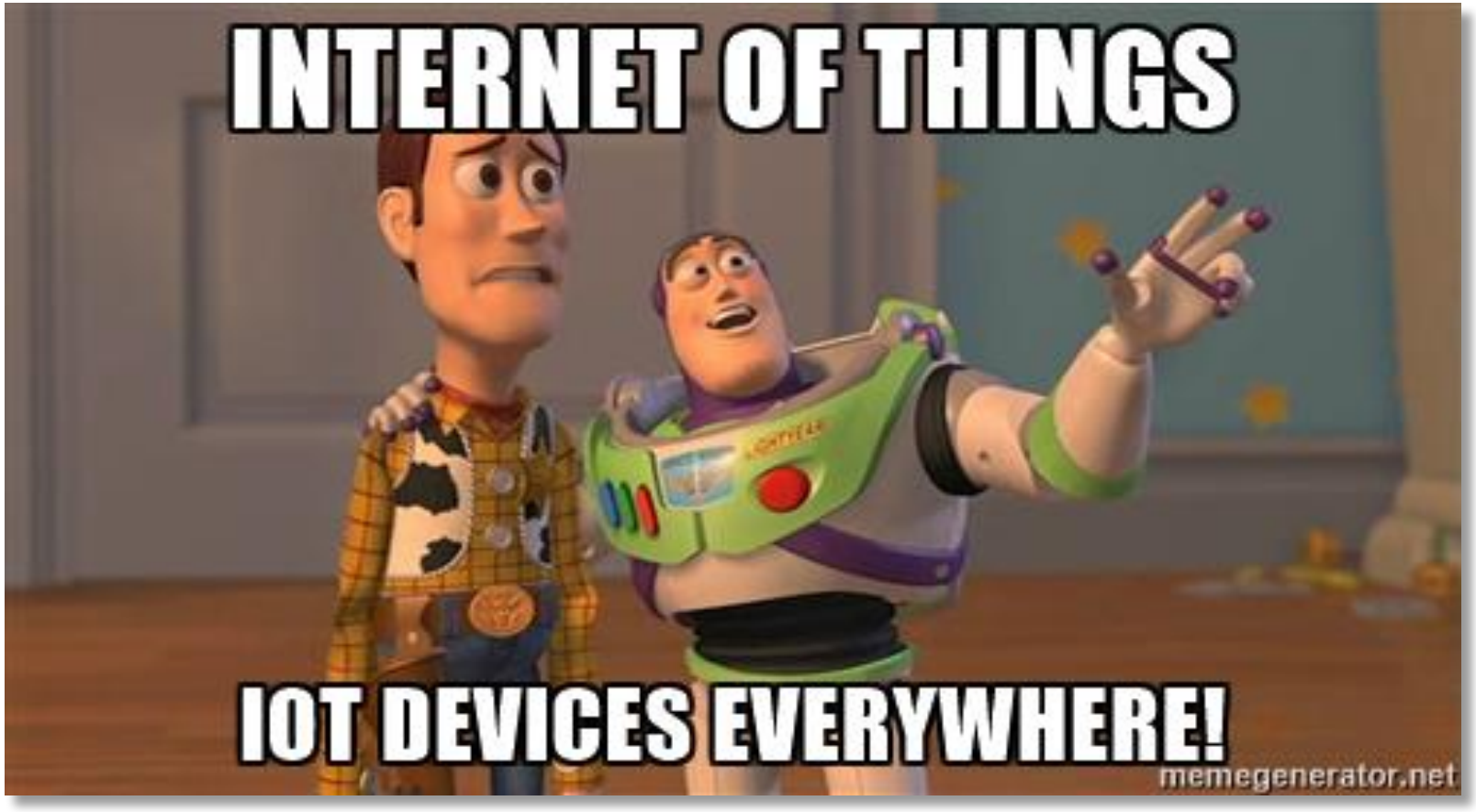
1. Motivation
2. Mirai Botnetz
3. Live Hacking
4. IoT Sicherheitslücken
5. Herkunft von Mirai

Moderne IoT-Geräte haben

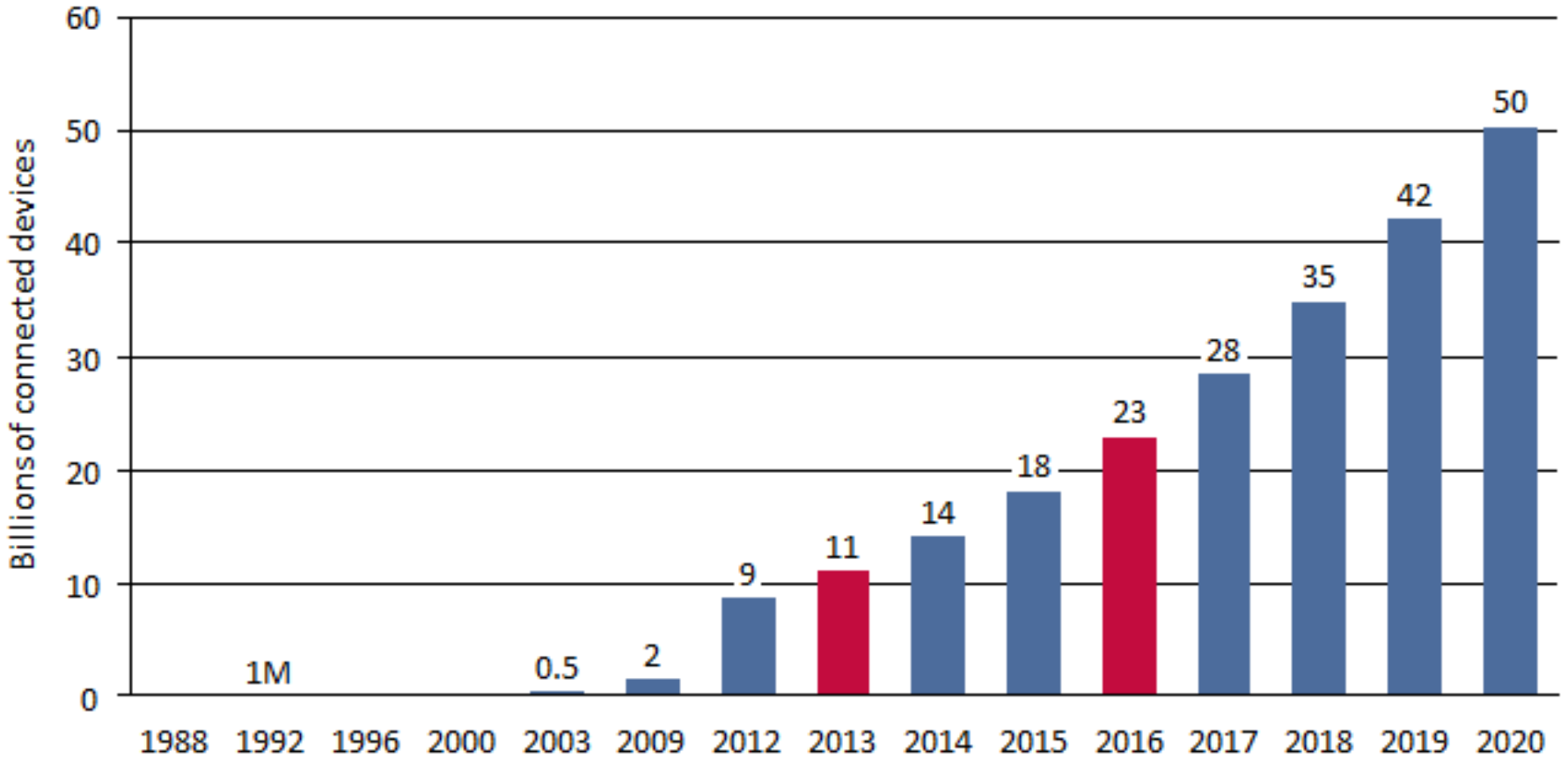
- WiFi
- Kamera
- Licht
- Skype

- http://www.svakom.net/Siime-Eye/

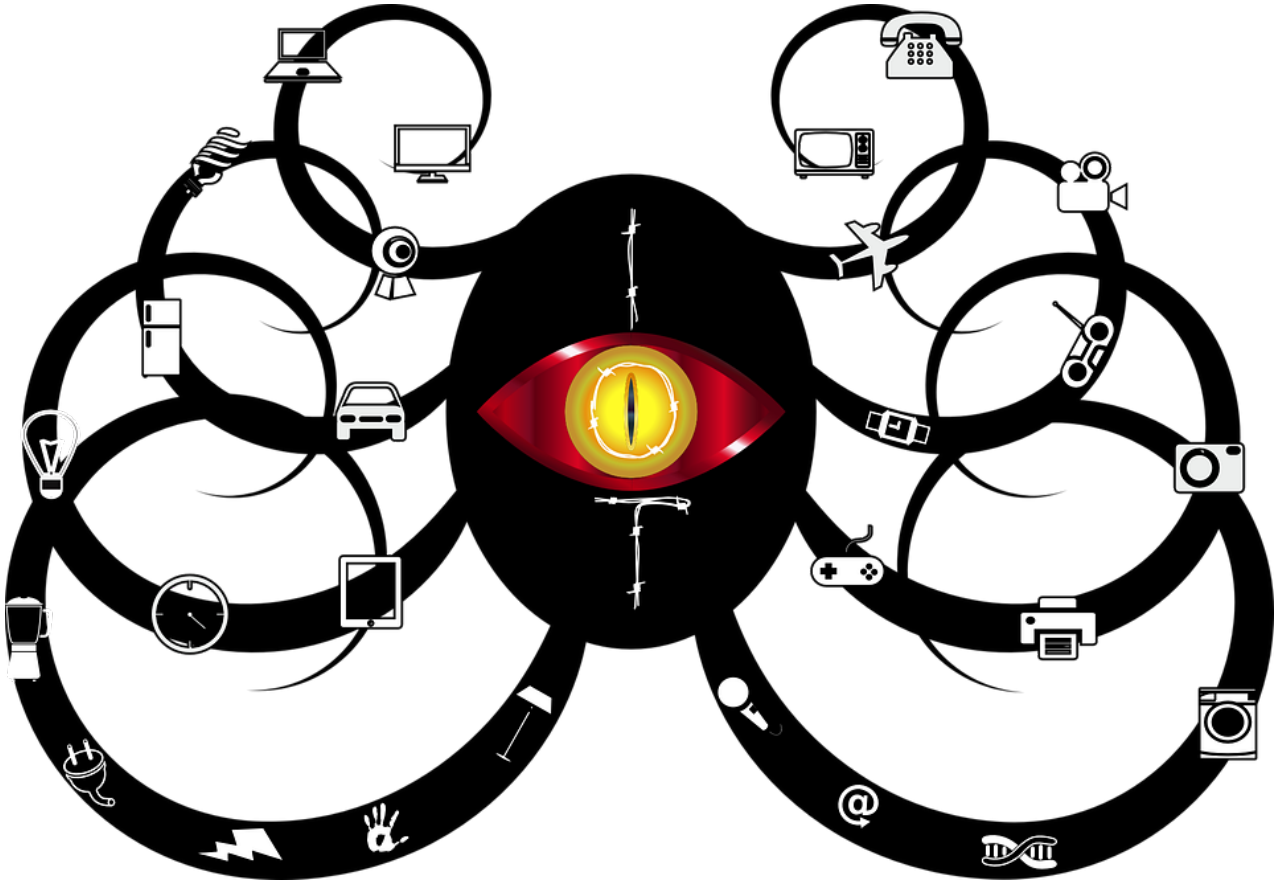
Motivation



Motivation

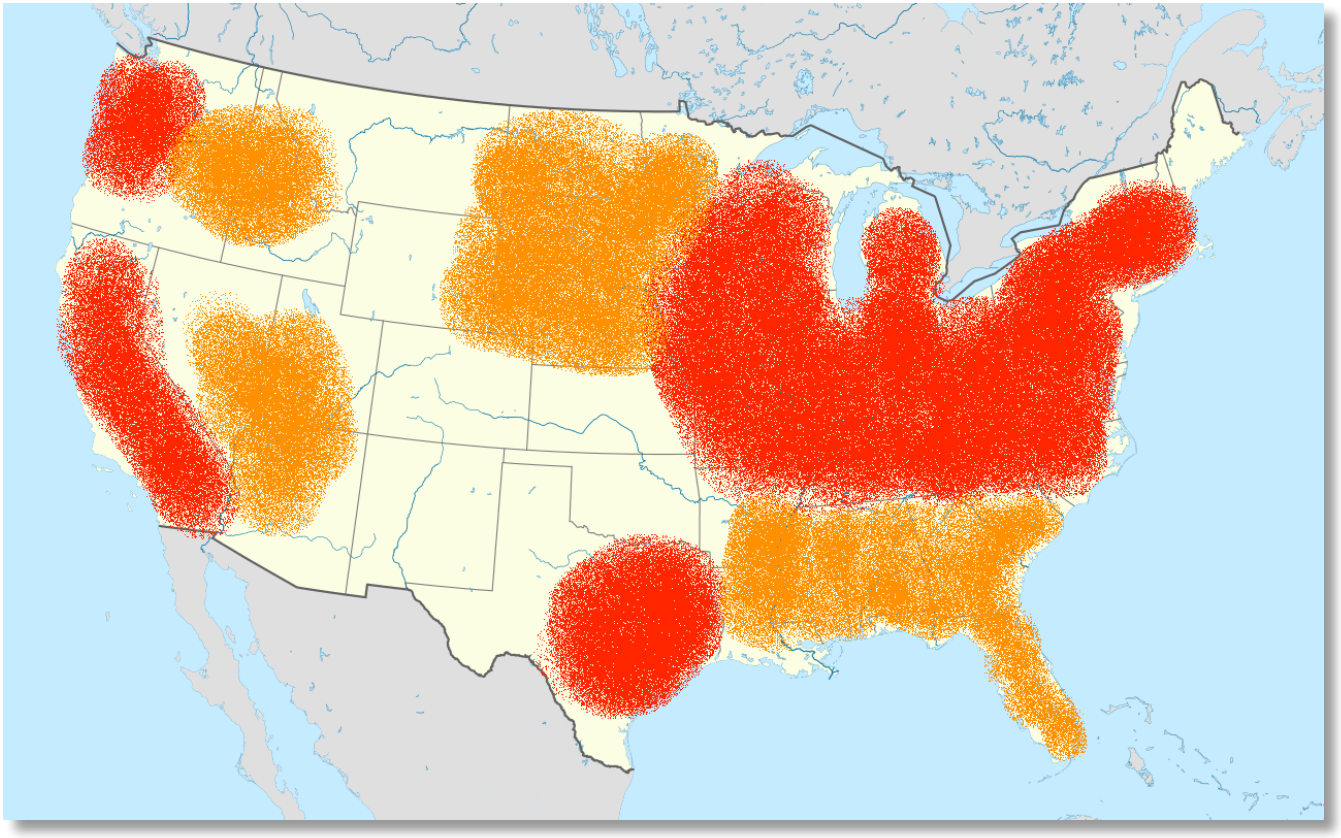


Mirai Botnetz

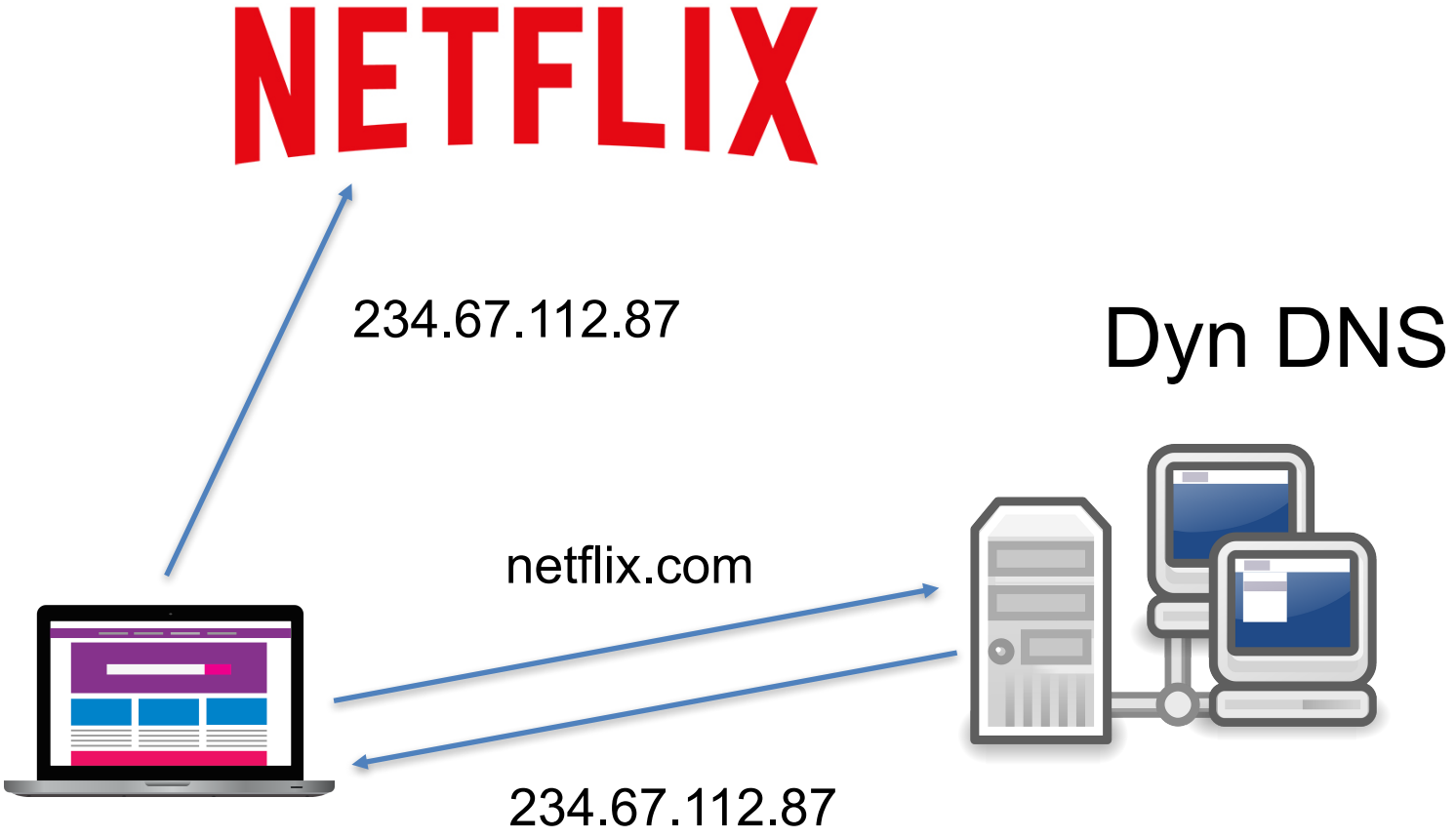


Mirai – Angriff auf Dyn

- PayPal
- Twitter
- Reddit
- GitHub
- Amazon
- Netflix
- Spotify



Mirai – Angriff auf Dyn



Mirai – Angriff auf Telekom

Angriffskapazität des Botnetz

- Dyn (21.10.2016)
  - ca. 100 000 Endpoints
  - Bis zu 1 Tbps (unbestätigt)
- Krebsonsecurity.com (20.09.2016)
  - 620 Gbps
- OVH, franz. Web Host (19.09.2016)
  - ca. 150 000 Endpoints
  - 1 Tbps
- Gesamtbotnetz (2016)
  - 300 000 – 500 000 Endpoints

Mirai – geographische Verteilung

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Welche Sicherheitslücken nutzt Mirai aus?

root/xc3511	root/vizxv	root/admin
admin/admin	root/888888	root/xmhdipc
root/default	root/juantech	root/123456
root/54321	support/support	root/(none)
admin/password	root/root	root/12345
user/user	admin/(none)	root/pass
admin/admin1234	root/1111	admin/smcadmin
admin/1111	root/666666	root/password
root/1234	root/klv123	Administrator/admin
service/service	supervisor/supervisor	guest/guest
guest/12345	guest/12345	admin1/password
administrator/1234	666666/666666	888888/888888
ubnt/ubnt	root/klv1234	root/Zte521
root/hi3518	root/jvbzd	root/anko
root/zlxx.	root/7ujMko0vizxv	root/7ujMko0admin
root/system	root/ikwb	root/dreambox
root/user	root/realtek	root/00000000
admin/1111111	admin/1234	admin/12345
admin/54321	admin/123456	admin/7ujMko0admin
admin/1234	admin/pass	admin/meinsm
tech/tech	mother/fu[redacted]r	

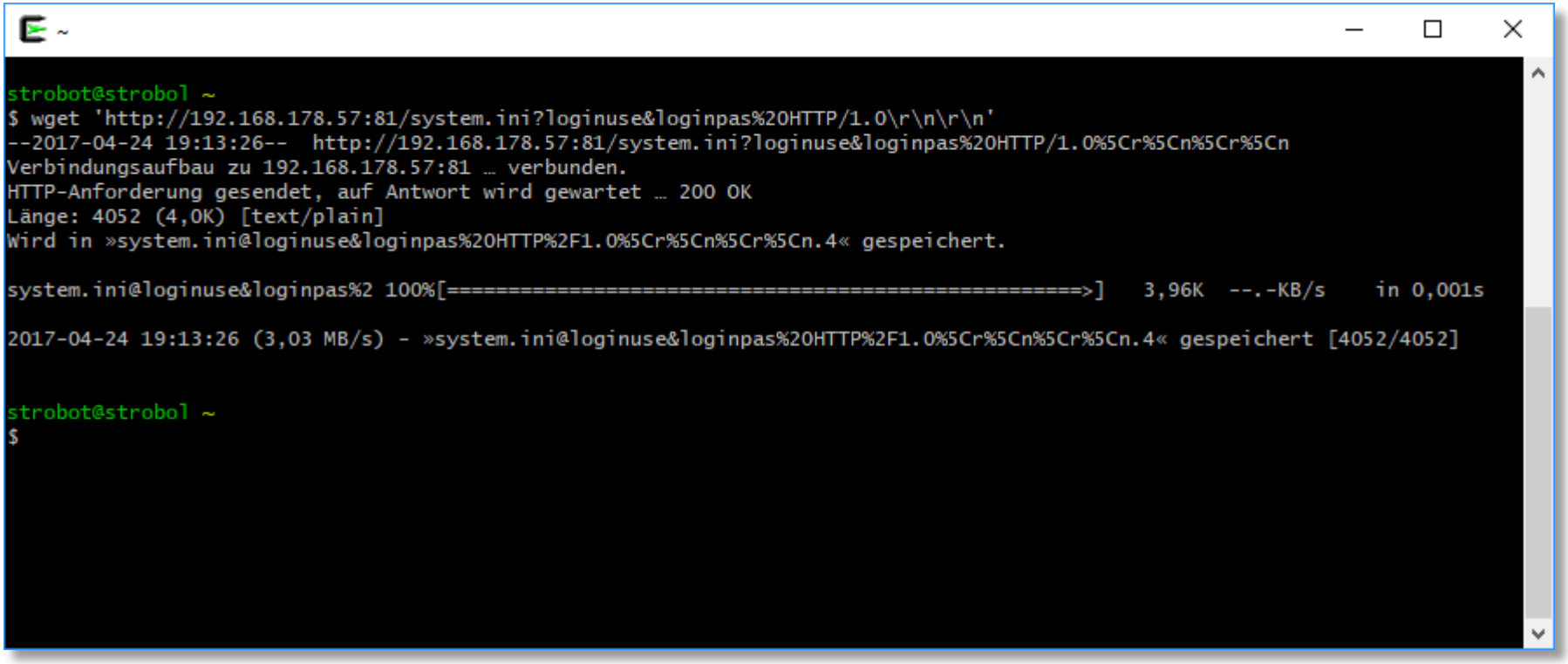
Mirai's built-in password dictionary.

Wie funktioniert Mirai?

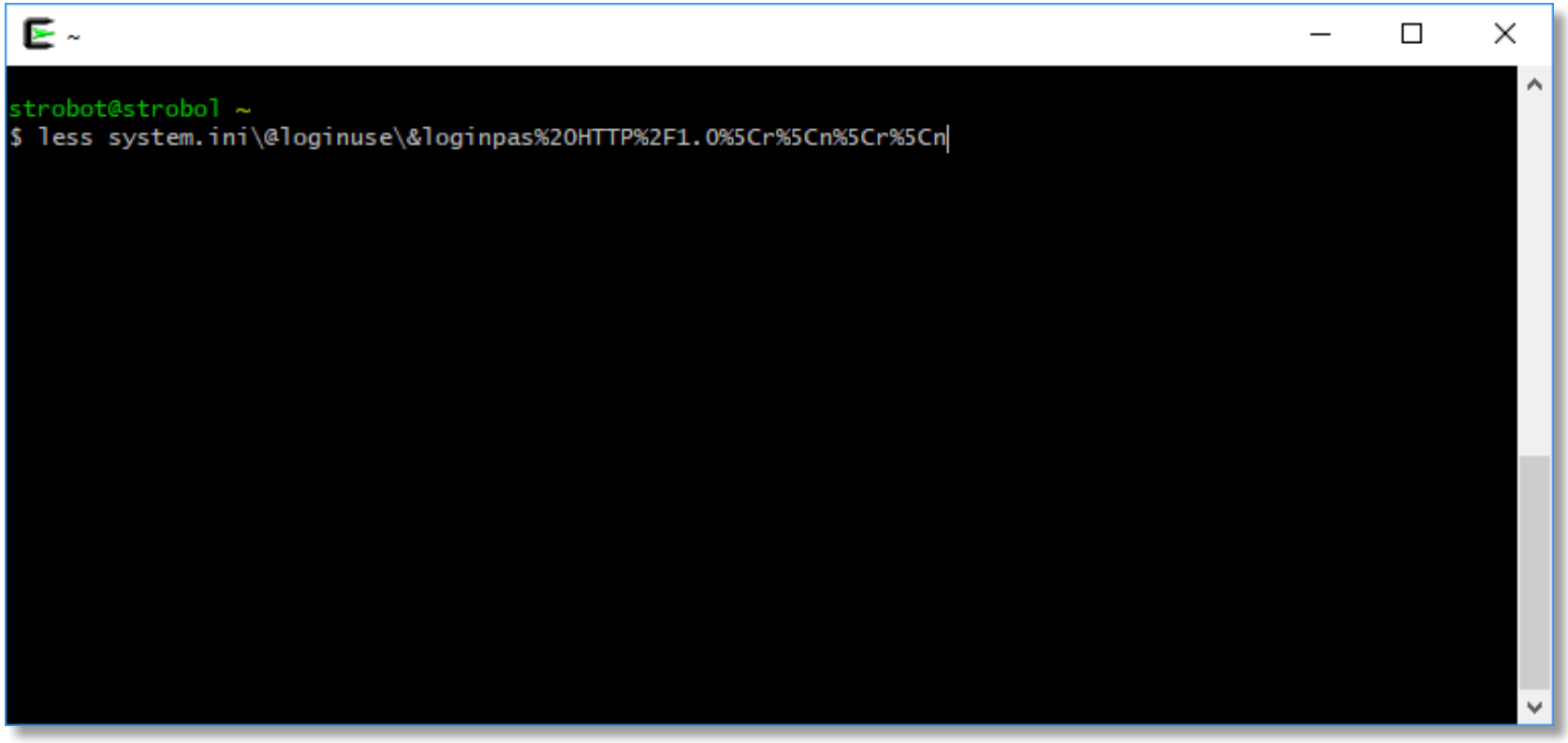
- Call-Home System
  - verbindet Bots zu Command und Control Servern
- Angriffsroutinen
  - HTTP, UDP, SYN, ACK Flooding, etc.
- Network scanner
  - Durchsucht zufällige IP-Adressen und infiziert Geräte

Live Hacking

Live Hacking

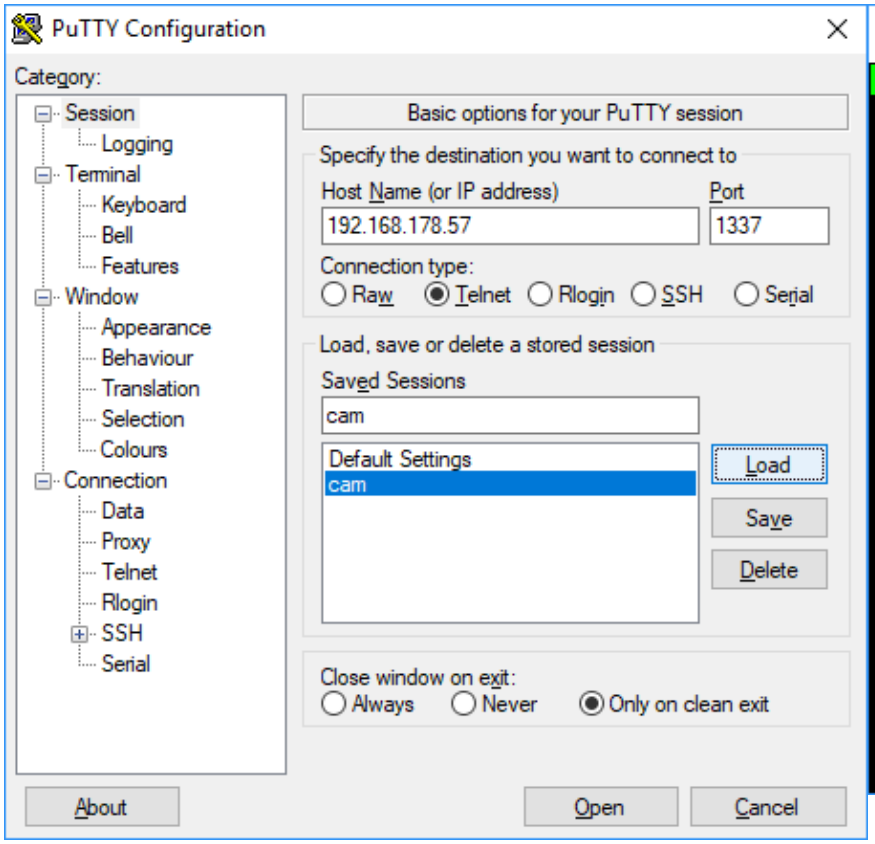


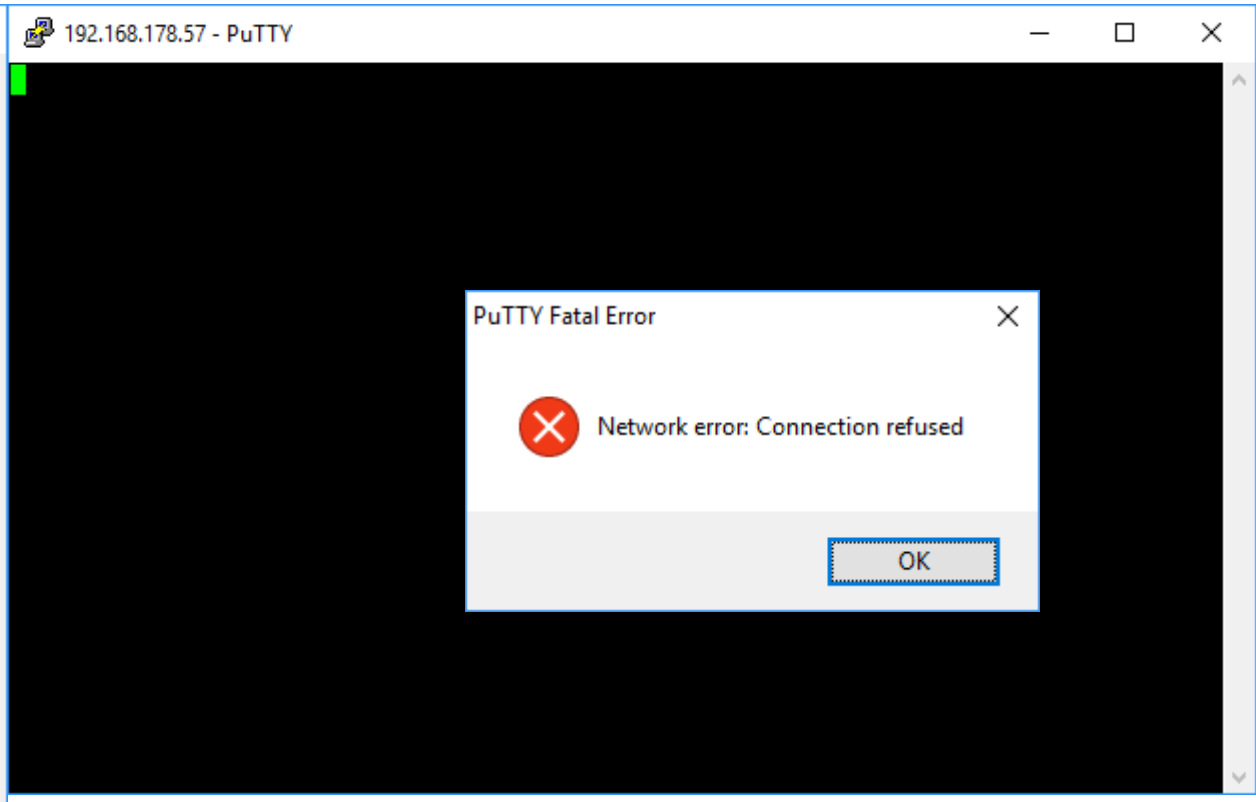
Live Hacking



Live Hacking

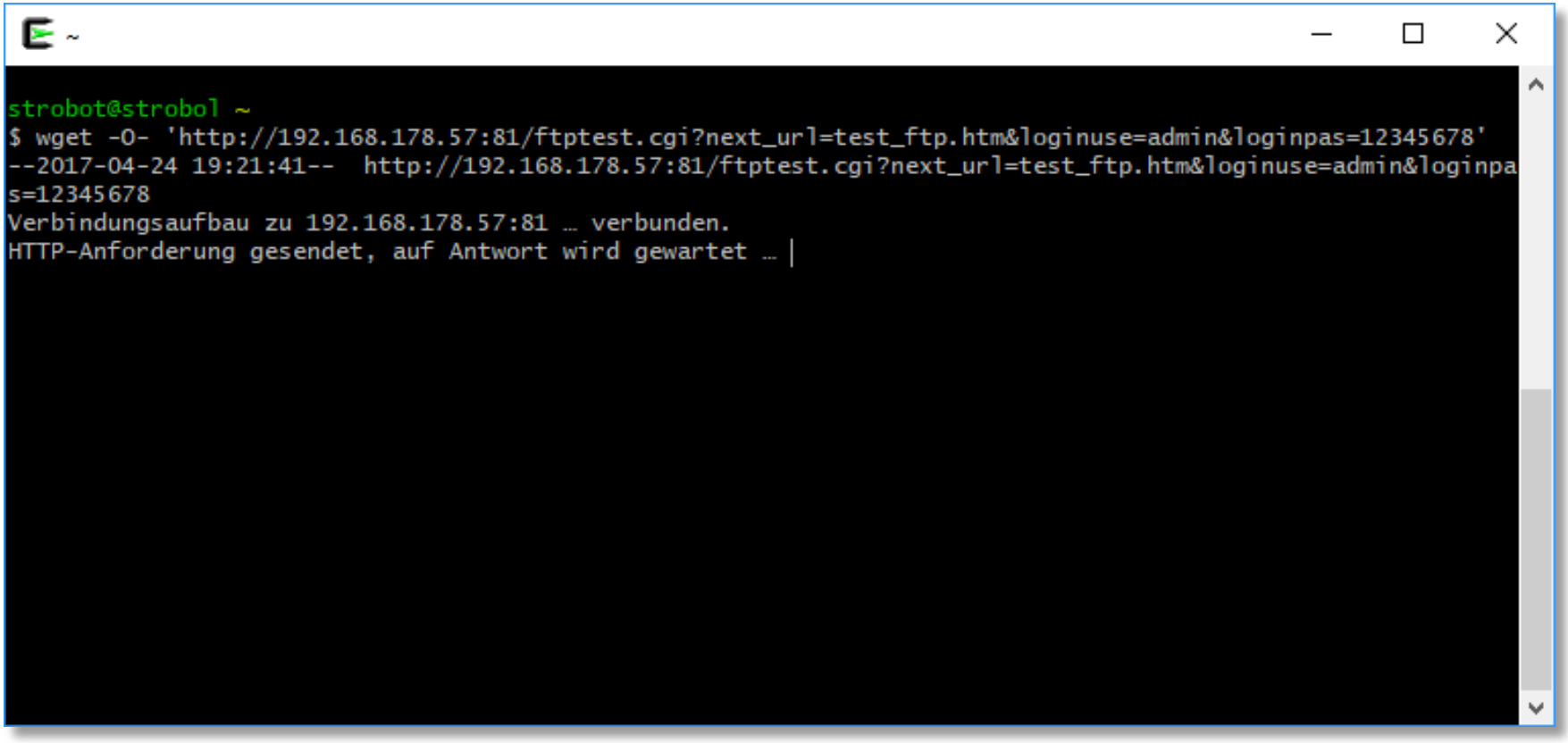
Live Hacking



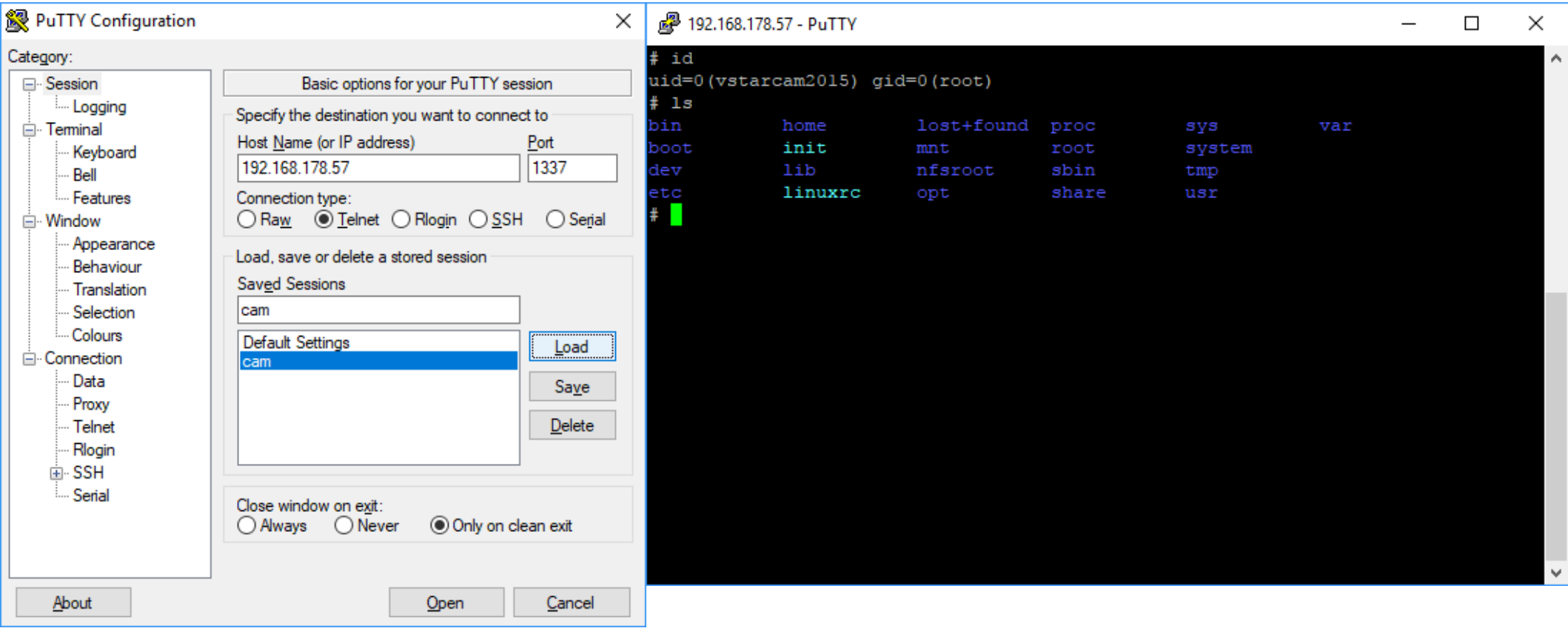


Live Hacking

Live Hacking

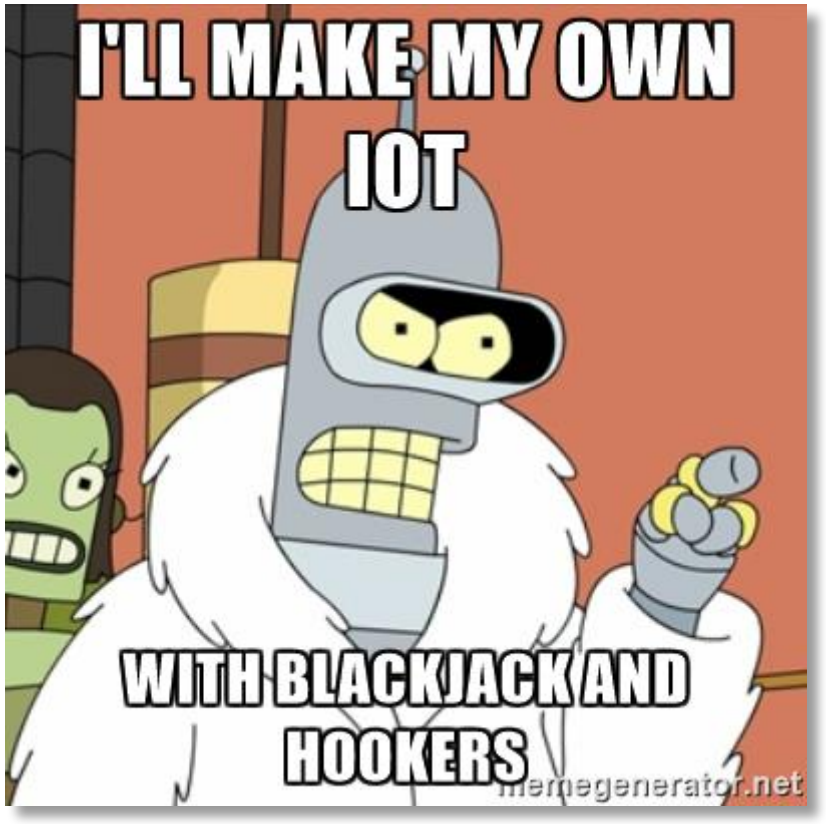


Live Hacking



Live Hacking

IoT Sicherheitslücken



- Offene Netze
- Schlechte Passwörter
- Stripped Linux
- Schlechter Code
- Keine Standards
- „Cloudservices“

Was würden Sie machen?

Sicherheit

- Braucht das Gerät wirklich Internet
- Separates Netzwerk
- Passwörter ändern
- Unterschiedliche Passwörter
- UPnP ausschalten
- Firmware-Updates
- Cloudservices vermeiden
- Netzwerkverkehr im Auge behalten

Lösungsvorschläge

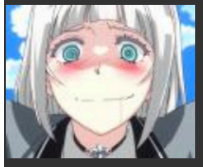
VS

Herkunft von Mirai

- Mirai wird Open-Source

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

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by **Anna-senpai**.)



Anna-senpai
L33t Member

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
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,
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.

Wer ist der Autor?

Anna-senpai?

Paras Jha 2nd

President at ProTraf Solutions, LLC

Greater New York City Area | Computer & Network Security

Current ProTraf Solutions

Education Rutgers University-New Brunswick

Following

295 followers

https://www.linkedin.com/in/paras-jha-561ba110a

Background

Summary

Paras is a passionate entrepreneur driven by the want to create. Highly self-motivated, in 7th grade he began to teach himself to program in a variety of languages. Today, his skillset for software development includes C#, Java, Golang, C, C++, PHP, x86 ASM, not to mention web "browser languages" such as Javascript and HTML/CSS.

He brings all of these skills to the table at ProTraf Solutions, a DDoS mitigation firm that has a proven track record in mitigating DDoS attacks that competitors cannot.

Experience

President

ProTraf Solutions

March 2015 – Present (1 year 11 months)

DDoS Mitigation services for remote networks and existing network infrastructure. Our filtering appliances are developed in-house, allowing for fine-tuned control of mitigation capabilities to your network's exact needs

DDoS gegen Minecraft-Server

Vielen Dank!

hristiyan.pehlivanov@mathema.de

nikolas.may@mathema.de

Referenzen

- Siime Eye – http://www.svakom.net/Siime-Eye/
- Wachstum des IoTs – https://www.weforum.org/agenda/2015/11/is-this-future-of-the-internet-of-things
- Mirai – http://news.softpedia.com/news/dyn-ddos-attack-powered-mainly-by-mirai-botnet-509541.shtml
- Mirai – Angriff auf Dyn – https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
- Mirai – geographische Verteilung – https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
- Telekom – https://www.engadget.com/2016/11/29/mirai-botnet-targets-deutsche-telekom-routers-in-global-cyberatt/
- Brickerbot – https://blog.radware.com/security/attack-types-and-vectors/
- Wer ist der Autor – https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
- http://www.insecam.org/
- https://www.safegadget.com/139/hacked-internet-things-database/
- https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html
- https://ww.cybereason.com/ip-cameras/