Betrugsschutz beim Online-Banking

Symposium und Präsentation der Arbeitsergebnisse

Oliver Wolf – April 2017


4487821
total threats
TOP PRODUCT
PRODUCT OF THE YEAR
2016
BEST OVERALL SPEED 2016
GOLD
FILE DETECTION 2016
GOLD
REAL-WORLD PROTECTION 2016
SILVER
MALWARE REMOVAL 2016
SILVER
AWARD

Agenda = Arbeitspakete

- Analyse der Banking Trojaner
- Nutzerseitige Schutzlösungen vor Banking Trojaner
- Erforschung neuartiger Alerting-Schutzmechanismus

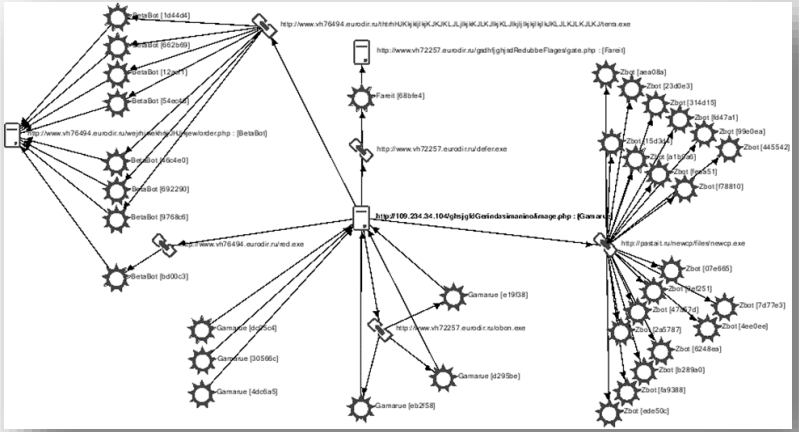
Analyse der Banking-Trojaner

Analyse der Banking-Trojaner

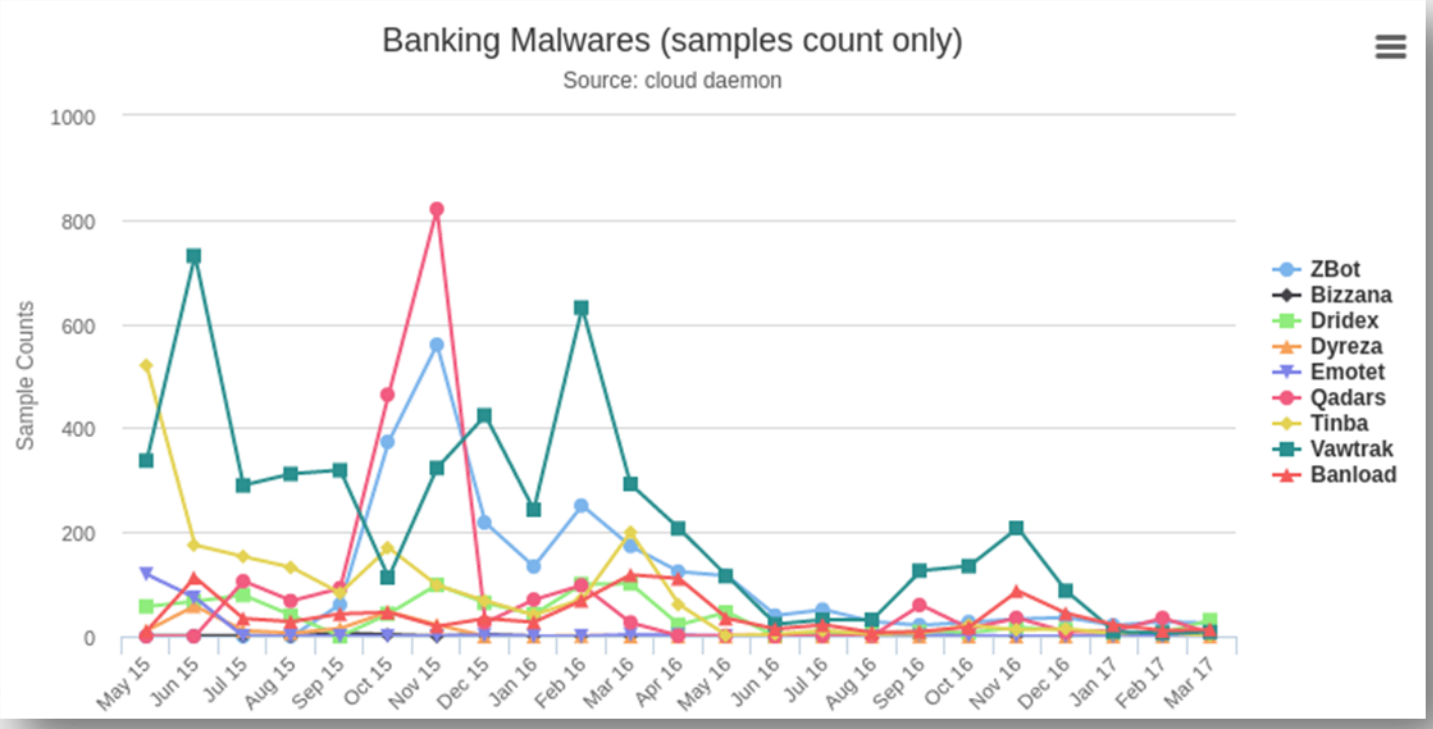
- Analyse der häufigsten Banking-Trojaner
  - Zbot, Bizzana, Dridex, Dyreza, Emotet, Qadars, Tinba, Vawtrak, Banload
- Entfernen der Kryptolayer
- Analyse und Implementierung des Kommunikationsprotokoll
  - Nachstellung des Originals
  - Überwachung der Trojaner Kommunikation im Botnetz

Analyse der Banking-Trojaner

- Erstellen eines Extraktors
  - Überwachung der CnC-Server
  - Webinjects
  - Verschlüsselung & Keys etc.
- Fortlaufende Überwachung des Botnets

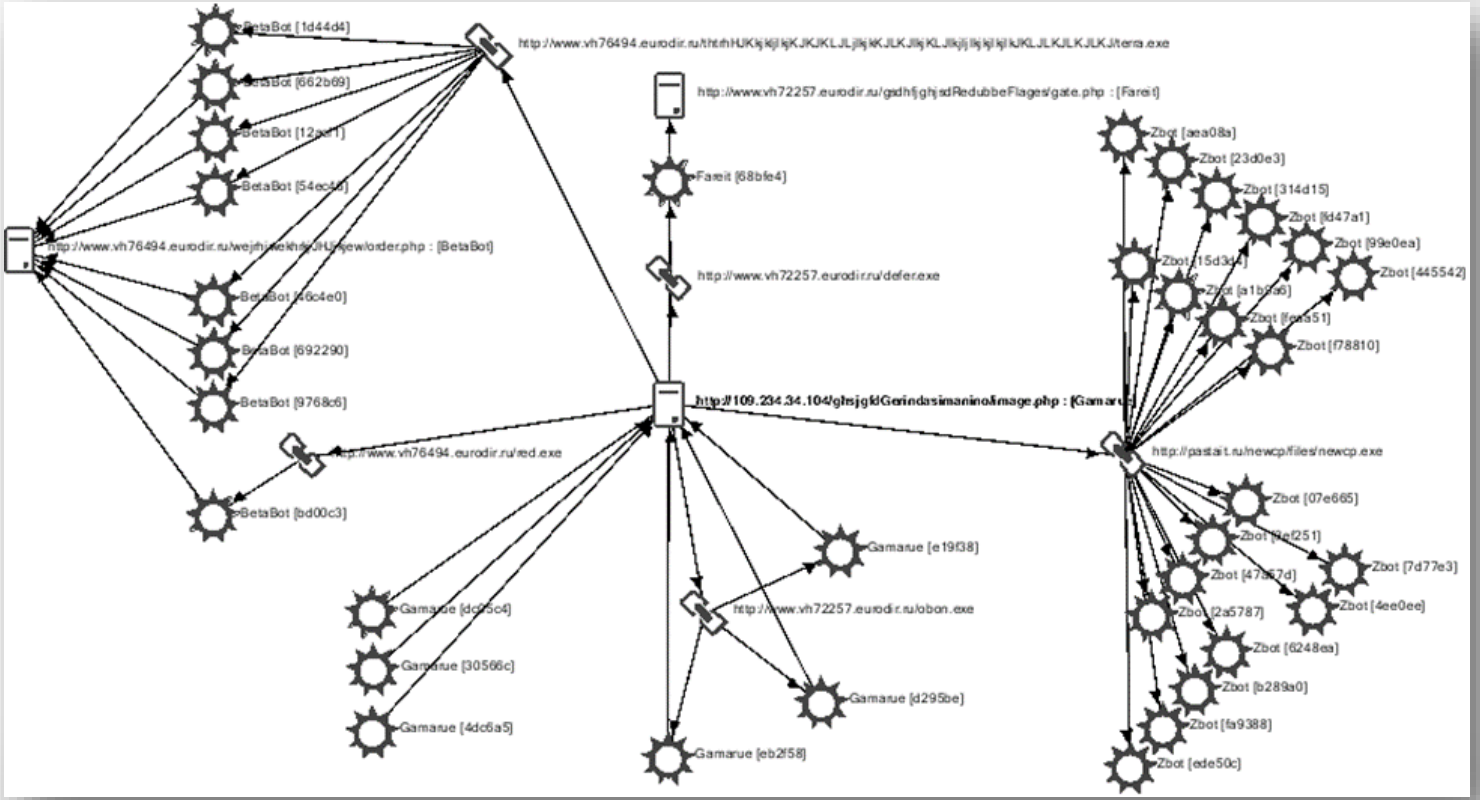


Analyse der Banking-Trojaner



(Source: Cloud Daemon)

Analyse der Banking-Trojaner



(Botchecker: Gamarue C&C Kommunikation)

Nutzerseitige Schutzlösungen

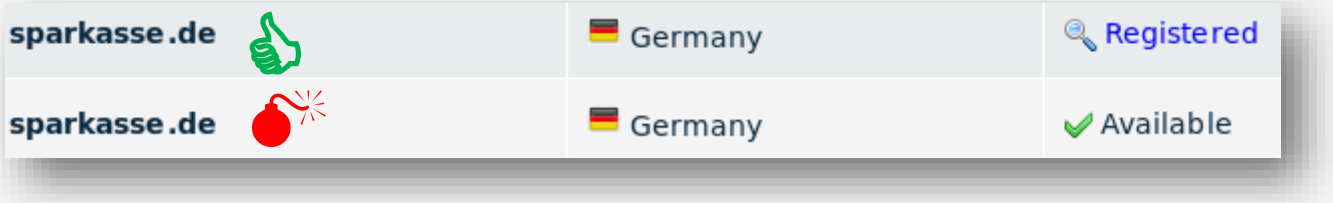
Nutzerseitige Schutzlösungen

- Banking-Trojaner injizieren sich in den Browser
  - Abfangen von Nutzereingaben (Formgrabbing)
  - Injizieren von eigenen HTML-Elementen (Webinjects)
  - Phishing
- Lösungsvorschlag: Blockieren der Injizierung durch Implementierung eines Treibers (Watchdog)
  - Beim Öffnen des Prozesses warden die Schreibrechte des Handles entfern
  - Installation von Malware wird dadurch nicht verhindert tzte Maßnahme um die Daten des Kunden zu schützen

Erforschung neuartiger Alerting Schutzmechanismen

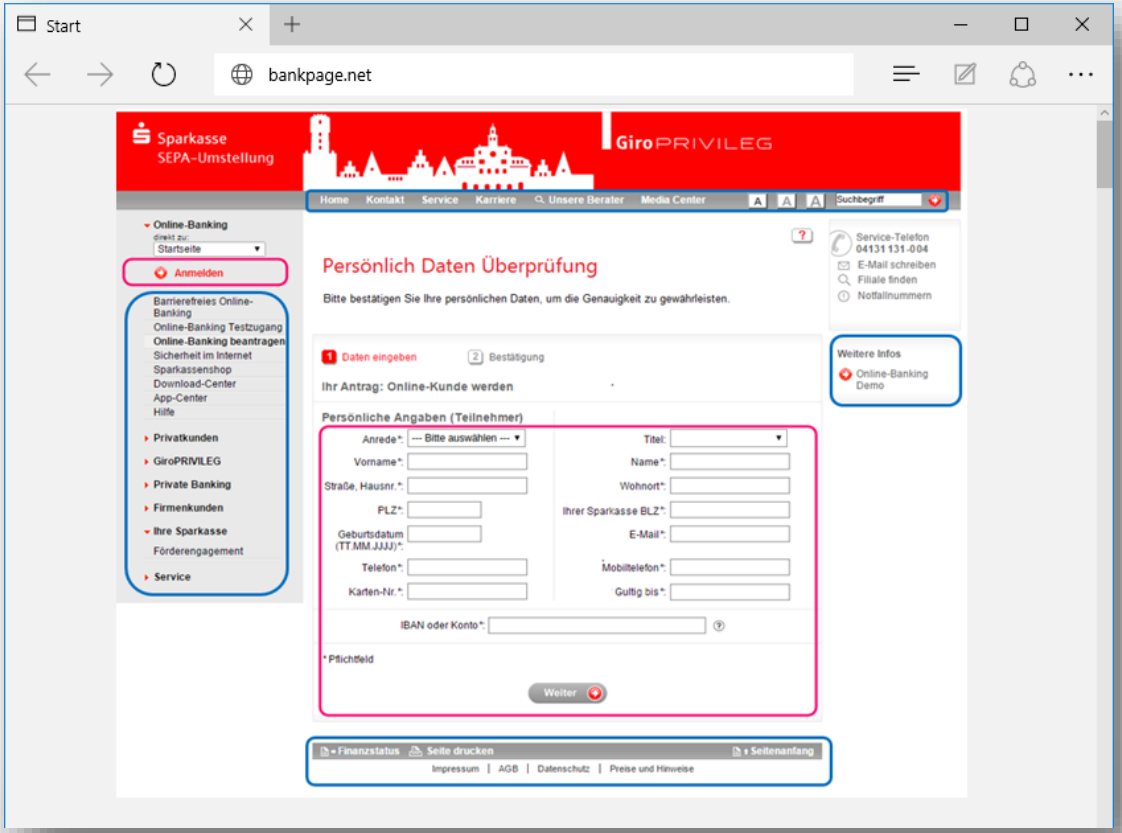
Erforschung neuer Alerting Schutzmechanismen

- Methoden von Phishing Angriffen
  - Punycode-Domainnamen



- Nachgestelltes Bankenlayout

Beispiel: nachgestelltes Bankenlayout



Erforschung neuer Alerting Schutzmechanismen

- Erkennung von Phishing Webseiten
  - Ähnlichkeiten des Webseitenaufbaus
  - Muster in den Domainnamen
  - Bankdomain als SubDomain

http://www.ubibanca.com.arlyihetrgk<...snipped....>.com/index.php

Erforschung neuer Alerting Schutzmechanismen

target	keyword	total phish URL	keyword in URL	domain name in URL
wellsfargo.com	wellsfargo	28.808	6.405 (22%)	2.875 (10%)
sparkasse.de	sparkasse	832	134 (16%)	24 (3%)
vrbank.de	vrbank	31	28 (90%)	28 (90%)

© Avira