



Betrugsschutz beim Online-Banking

Symposium und Präsentation der Arbeitsergebnisse

Oliver Wolf – April 2017

4487821
total threats



Agenda = Arbeitspakete

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





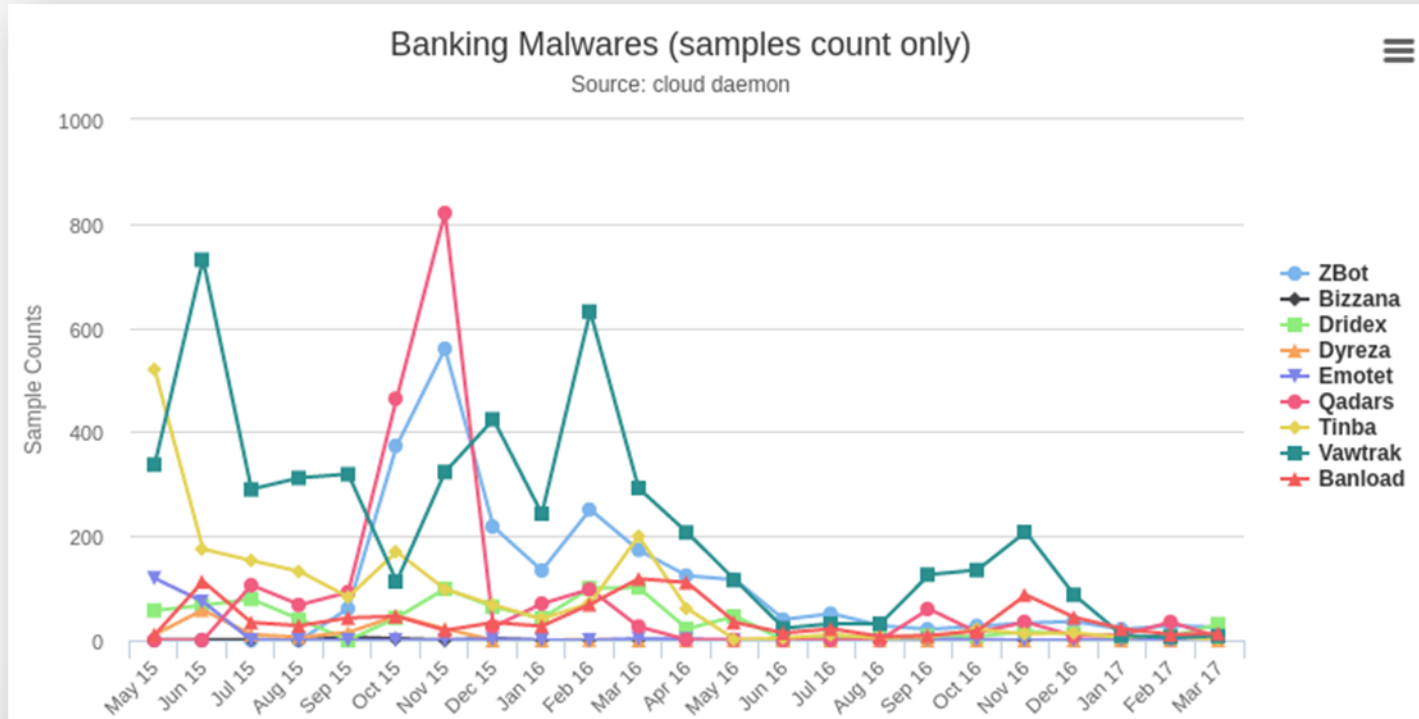
Analyse der Banking-Trojaner

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



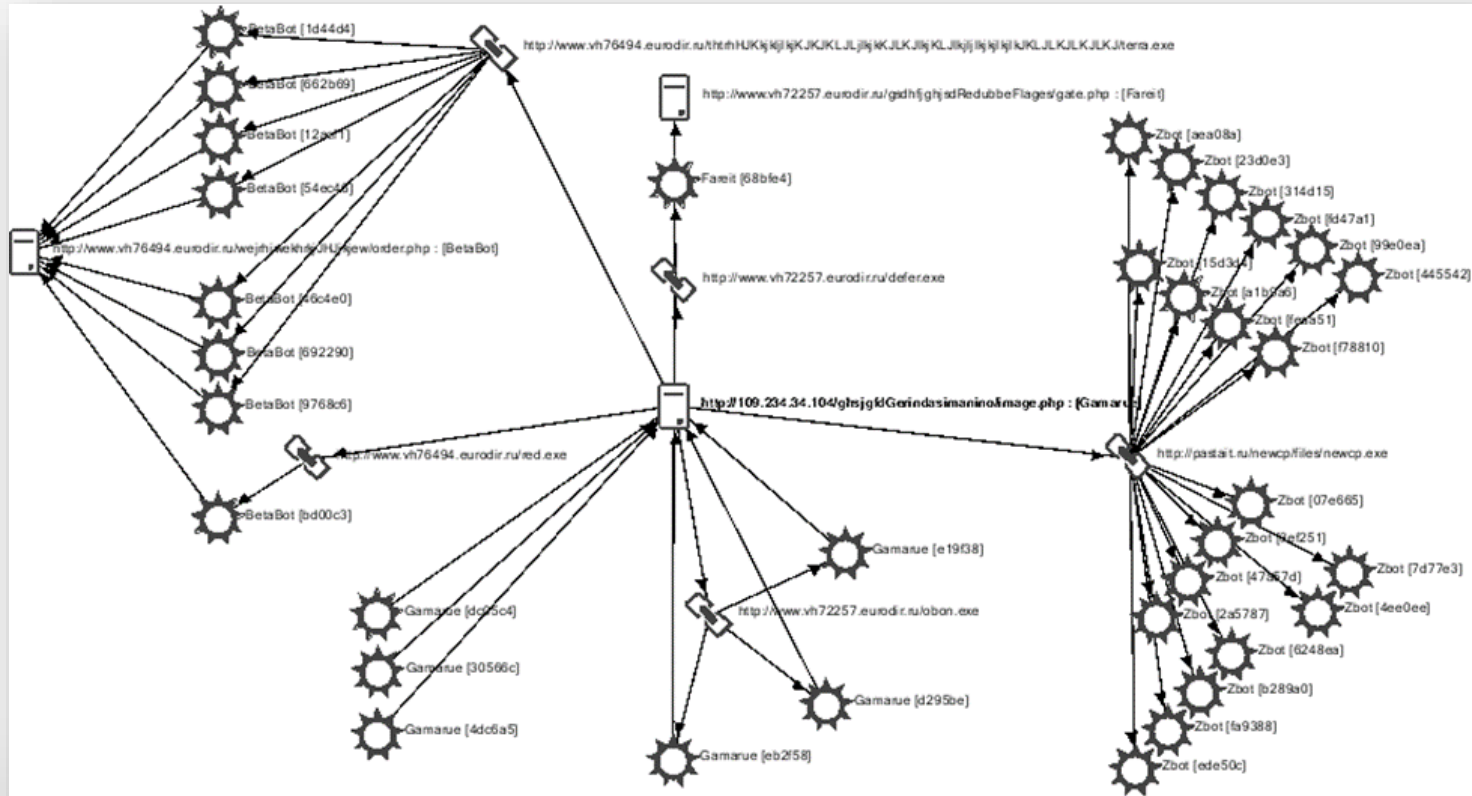
Analyse der Banking-Trojaner



(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 werden die Schreibrechte des Handles entfernt
 - Installation von Malware wird dadurch nicht verhindert, letzte Maßnahme um die Daten des Kunden zu schützen











Erforschung neuartiger Alerting Schutzmechanismen

Erforschung neuer Alerting Schutzmechanismen

- Methoden von Phishing Angriffen
 - Punycode-Domainnamen

sparkasse.de 	 Germany	 Registered
sparkasse.de 	 Germany	 Available

- Nachgestelltes Bankenlayout

Beispiel: nachgestelltes Bankenlayout

The image shows a browser window displaying the website **bankpage.net**. The page is for Sparkasse GiroPRIVILEG and features a registration form for online banking. The layout includes a top navigation bar, a left sidebar with menu items, a main content area with a form, and a footer with utility links.

Navigation and Header:

- Top bar: Home, Kontakt, Service, Karriere, Unsere Berater, Media Center, Suchbegriff
- Header: Sparkasse SEPA-Umstellung, GiroPRIVILEG

Left Sidebar (Navigation):

- Online-Banking
 - Anmelden
 - Barrierefreies Online-Banking
 - Online-Banking Testzugang
 - Online-Banking beantragen
 - Sicherheit im Internet
 - Sparkassenshop
 - Download-Center
 - App-Center
 - Hilfe
- Privatkunden
- GiroPRIVILEG
- Private Banking
- Firmenkunden
- Ihre Sparkasse
 - Förderengagement
- Service

Main Content Area:

Persönlich Daten Überprüfung

Bitte bestätigen Sie Ihre persönlichen Daten, um die Genauigkeit zu gewährleisten.

1 Daten eingeben **2 Bestätigung**

Ihr Antrag: Online-Kunde werden

Persönliche Angaben (Teilnehmer)

Anrede* --- Bitte auswählen ---	Titel: ---
Vorname* <input type="text"/>	Name* <input type="text"/>
Straße, Hausnr.* <input type="text"/>	Wohnort* <input type="text"/>
PLZ* <input type="text"/>	Ihrer Sparkasse BLZ* <input type="text"/>
Geburtsdatum (TT.MM.JJJJ)* <input type="text"/>	E-Mail* <input type="text"/>
Telefon* <input type="text"/>	Mobiletelefon* <input type="text"/>
Karten-Nr.* <input type="text"/>	Gültig bis* <input type="text"/>
IBAN oder Konto* <input type="text"/>	

* Pflichtfeld

Weitere Infos:

- Service-Telefon 04131 131-004
- E-Mail schreiben
- Filiale finden
- Nottalnummern
- Online-Banking Demo

Footer:

Finanzstatus | Seite drucken | Impressum | AGB | Datenschutz | Preise und Hinweise | Seitenanfang



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



