Bundesamt
für Sicherheit in der
Informationstechnik

Erfahrungen aus Cyber-Angriffen und Anforderungen an die Netzsicherheit

Dirk Häger

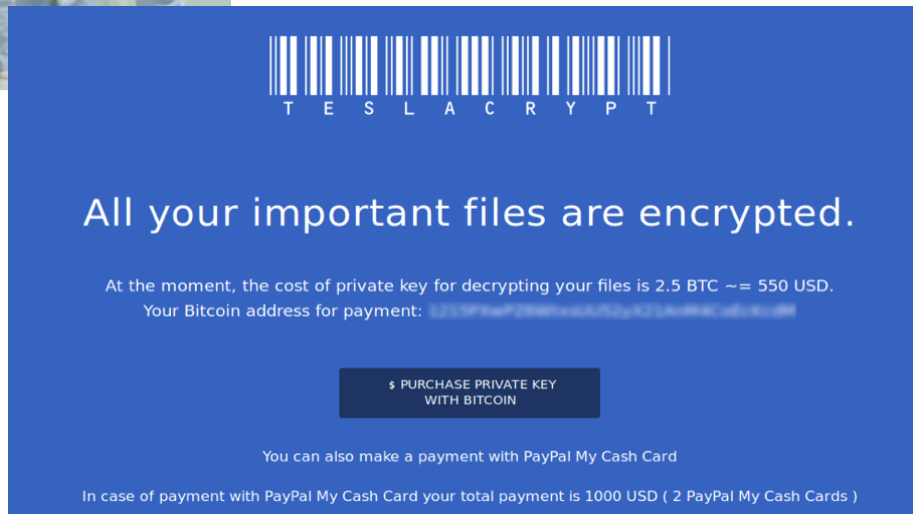
Anwendertag Forensik 2017
Fraunhofer SIT

Ransomware

IT-Sicherheit

Computervirus legt Krankenhäuser lahm

Befunde mussten per Telefon oder Fax übermittelt werden: Ein Computervirus hat die Abläufe im Krankenhaus Arnsberg gestört. Es ist nicht der einzige Vorfall dieser Art in Nordrhein-Westfalen.



Vorgehen bei der Analyse

- Ausgangspunkt: verschlüsselte Dateien und Erpressertext
  - kein Schadprogramm; kein Angriffsvektor bekannt
  - alle Systeme runtergefahren

- Analyseansätze
  - Logging auf AD hochdrehen; bereinigte Server starten und auf Neu-Infektion warten
  - Antivirendatenbanken nach Erpressertext durchsuchen (oder Google)
  - Analyse Firewall-Logs

Botnet Takedown am 30.11.2016

CERT Bund

BSI ermöglicht Zerschlagung der Botnetz-Infrastruktur Avalanche

Hilfestellung für Betroffene unter › www.bsi-fuer-buerger.de/botnetz

Ort Bonn
Datum 01.12.2016

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt nach einem Amtshilfeersuchen die Zentrale Kriminalinspektion der Polizeidirektion Lüneburg (ZKI) sowie die Staatsanwaltschaft Verden/Aller bei der Analyse und Zerschlagung der Botnetz-Infrastruktur Avalanche.

'AVALANCHE' NETWORK DISMANTLED IN INTERNATIONAL CYBER OPERATION

01 December 2016

Press Release

On 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Lüneburg Police (Germany) in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust and global partners, dismantled an international criminal infrastructure platform known as 'Avalanche'.

Bundesamt für Sicherheit in der Informationstechnik

Avalanche Takedown 30.11.2016

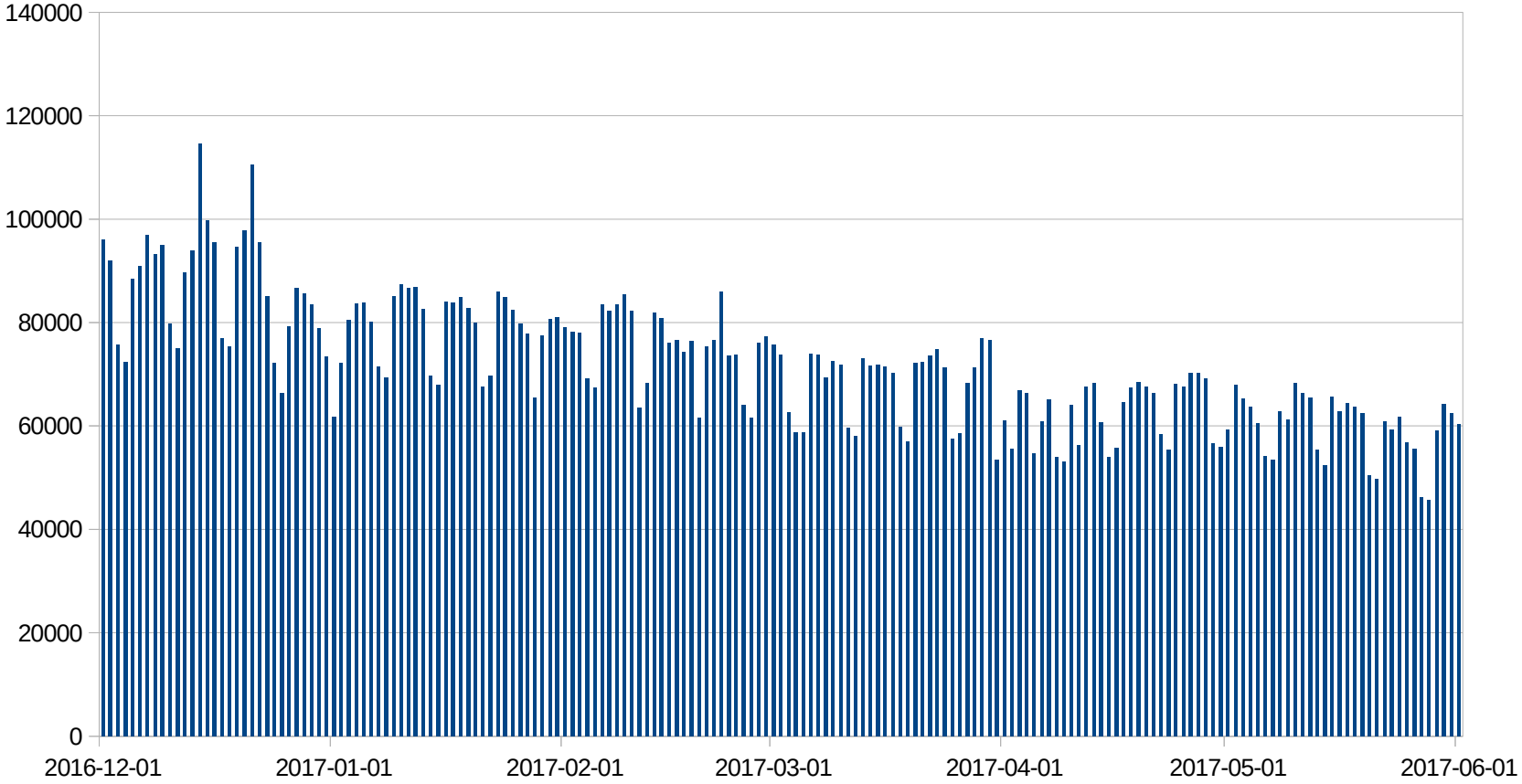
- 5 Festnahmen, 37 Durchsuchungen, 39 Server beschlagnahmt (C&C-Server, 2nd-Level-Proxy-Server), 221 1st-Level Proxies abgeschaltet (Abuse-Meldungen). Umleitung Domänen für Sinkholing
- Beteiligt 62 TLDs (Top-Level-Domains), 44 Registries in 24 Ländern:
  839.000 Domänen, davon zeigen aktuell >60.000 Domänen auf das Sinkhole-System.
- Analyse Sinkhole (weltweite Verteilung durch BSI):
  - IPs aus 190 Ländern, ca. 85.000 unique pro Tag weltweit, durchschnittlich 5.000 Bots pro Tag aus DE (Maximum 13.000).

Botnetz-Familien

Andomeda (D)
Bolek (B)
Citadel (B)
CoreBot (B)
Dofoil (D)
Gozi/GozNym (B)
KINS (B)
Marcher (B,A)
Matsnu (D)
Nymaim (D)
Pandabanker (B)
Ranbyus (B)
Rovnix (B)
Smart App (B, A)
Teslacrypt (B)
Tinybanker (B)
Trusteer App (B,A)
URLzone (B)
Vawtrak (B)
Xswkit (D)

B: Banking
D: Downloader
A: Android

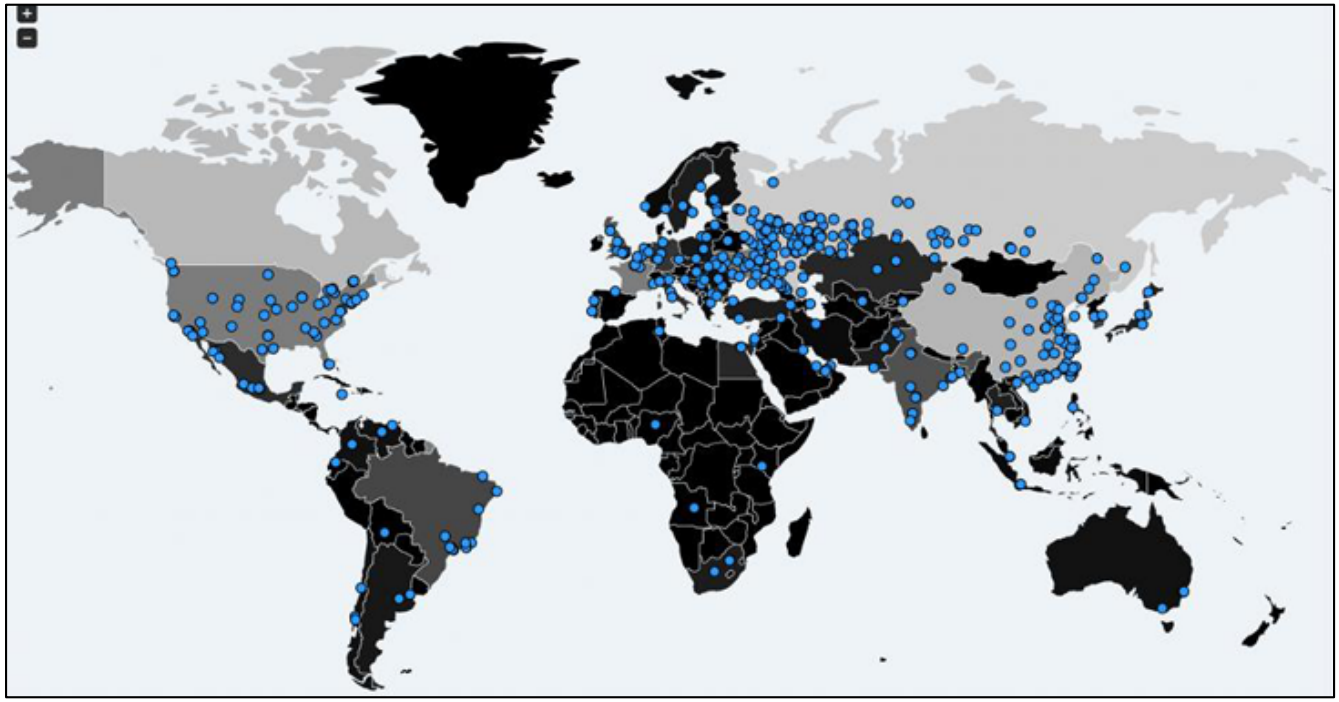
Sinkhole-Statistik
Anzahl unique IPs pro Tag global



Anzeigetafeln der Deutschen Bahn

Bild: Twitter

WannaCry Verteilung



Länderverteilung Top 20:

25875	Russian Federation
22991	China
7626	Taiwan
5966	Ukraine
4613	United States
3165	Canada
2224	Korea
1803	France
1400	India
1142	Brazil
1057	Hong Kong
730	Japan
604	**Germany**
578	United Kingdom
521	Poland
514	Chile
480	Mexico
438	Vietnam
430	Kazakhstan
404	Armenia

Bundesamt
für Sicherheit in der
Informationstechnik

Erkenntnisse aus WannyCry und NotPetya

- Methoden gezielter Angriffe sind automatisiert worden: neue Breitenwirkung
- Netzwerksegmentierung scheinbar kaum vorhanden
- Cybersicherheitswarnungen erreichen viele Adressaten nicht
- Gutes Krisenmanagement essentiell für Schadensminimierung

- Motivation der Täter unklar: eventuell kein CyberCrime

- Staatliches Cyber-Waffenarsenal muss besser geschützt werden.

- Absicherung von Updateprozessen muss neu bewertet werden (Hersteller in der Pflicht)

Webhacking

- Webserver eines Bundesamtes wird „gehackt“
  - Per Javascript wird auf Schadprogramm verlinkt
- Webseite wird bereinigt – Problem damit beseitigt
  - Wie wurde der Angriff denn durchgeführt?
- Webserver wird erneut gehackt
  - Upps!
  - Config-Änderungen
- Webserver wird zum vierten Mal gehackt!
  - Hiiilfe!!!!!
  - Rechner wird abgeschaltet
  - BSI bekommt Logdaten

Analyseergebnisse

- SQL-Injection (Versuche in den Logs zu sehen)
- Nachladen von Zeus (Zbot)
- Angreifer installierte PHP Shell

- Teilweise Automatisierung der SQL-Tests
  - User-Agent: Microsoft URL Control – 6.[...]
  - 180 Versuche in 3 Minuten von einer IP
- Teamarbeit? Tor-User?
  - SQL-Injection von 4 IP-Adressen
  - 3 Stunden und 243 Versuche
  - Insgesamt Zugriffe von 9 völlig unterschiedlichen IP-Adressen (hauptsächlich aus Russland)

IT-Vorfall in einem Parlament

- Diverse Auffälligkeiten führten zur schnellen Entdeckung
- Bereinigungsversuche erfolglos

- Suche nach infizierten Systemen
  - Signaturbasierte Suche auf den internen Systemen („spezieller Virenscanner“)
  - Analyse der Firewalllogs

Loganalyse

- Datenabfluss **MUSS** Spuren in den Logs hinterlassen haben!

- Sortieren der HTTP-Daten
  - Verbindungslänge
  - Menge der versendeten Daten
  - Top-Talker (Anzahl Verbindungsaufbauten)

- Fleißaufgabe
  - Problem: HTTPS-Seiten (ohne Reverse DNS)
  - Keine/kaum Kenntnisse der internen Strukturen/Prozesse
  - Werkzeug: Kommandozeile!!

- Weiterer guter Indikator: Verwendung einer IP-Adresse statt Hostname

Fakten?

Integration fängt damit an, daß Sie als Deutscher mal türkisch lernen!

Renate Künast, Die Grünen Sendung Beckmann 30.8.2010

Satireseiten Moselkurier?

- Unglaublich was sich die Politiker raus nehmen. Deutschland sollte umbenannt werden in Absurdistan.
- Die hat nicht mal einen Twitteraccount
- Ich wünsche keiner Frau, dass sie vergewaltigt wird. Der Frau Petra Klamm wünsche ich geradezu, dass ihr das schon bald auch blüht und aber hoffentlich am Leben gelassen wird.

Politics by Numbers

On Twitter, Trump bots are out-tweeting Clinton bots 7 to 1

Trump's social media popularity is rigged, too.

BY APRIL GLASER | @APRILASER | NOV 1, 2016, 4:22PM EDT

Social Bots

SPIEGEL Plus

Wie digitale Dreckschleudern Meinung machen

Automatische Bots verzerren politische Diskussionen in sozialen Netzwerken und können Wahlen beeinflussen. Die Kanzlerin hält sie für gefährlich, doch die AfD will sie einsetzen.

Analyse sozialer Netze

Bundestagswahl 2017: Social-Media-Angriff auf das #kanzlerduell?

ALLGEMEIN CHRISTIAN GRIMME 6. SEPTEMBER 2017

Das Projekt PropStop hat im Kontext des Bundestagswahlkampfs 2017 die Aktivitäten rund um den Abend des TV-Duells zwischen Bundeskanzlerin Angela Merkel (CDU) und ihrem Herausforderer Martin Schulz (SPD) untersucht. Dabei konnte der Versuch beobachtet werden, das Hashtag #kanzlerduell für die Verbreitung zweier anderer Hashtags koordiniert zu missbrauchen. Hier geht es zum detaillierten Bericht über die Beobachtungen während des TV-Duells.

Aktuelle Gefährdungslage

- Ransomware lässt nicht nach → **Backups**
- Angriffe gelegentlich erfolgreich → Nachvollziehbarkeit durch Logging

- Gegenmaßnahmen
  - Firewall
  - Netzseparierung und Härtung der Betriebssysteme
  - Red Forest (Schutz des AD)
  - AV-Programme
  - Blacklisting von bösartigen Domains
  - IDS und Honeypots

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Dr. Dirk Häger
dirk.haeger@bsi.bund.de
Tel. +49 (0) 228 9582 5304
Fax +49 (0) 228 10 9582 5304

Bundesamt für Sicherheit in der Informationstechnik
Fachbereich CK2 – Operative Cyber-Sicherheit
Godesberger Allee 185 - 189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik