



Bundeskriminalamt

# Cybercrime

Bedrohung / Risiken aus polizeilicher Sicht

Abteilung Schwere und Organisierte Kriminalität

SO41 – Nationale Kooperationsstelle Cybercrime

Düsseldorf, 20.04.2016

Aktuelle Phänomene Cybercrime

Lagebild – Herausforderungen

Nationale Kooperationsstelle Cybercrime

Strategie und Auftrag

Kooperationsmodelle

# Phänomen Ransomware

---

- Was ist Ransomware?
- Historie / Entwicklung
- Erfolgreiches kriminelles Geschäftsmodell
- Aktuelle Lage



# Crypto-Ransomware Alte-Version



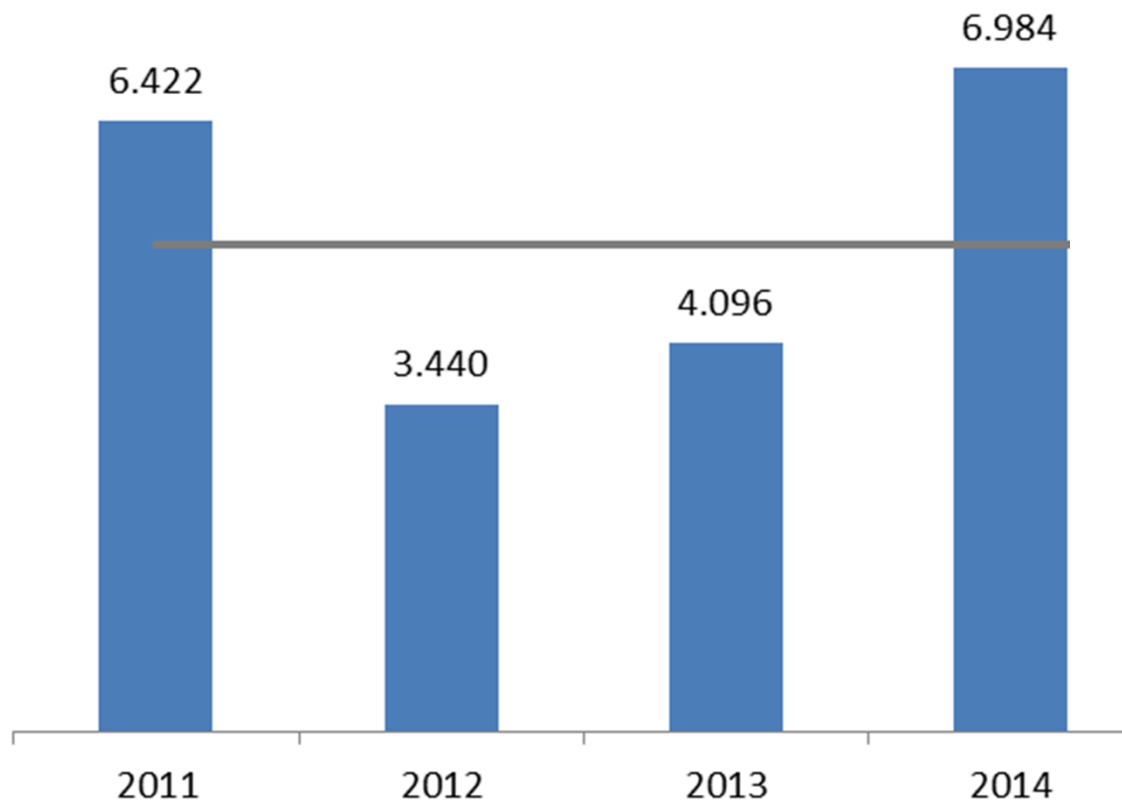


# Crypto-Ransomware neue-Version (Petya)

```
uu$$$$$$$$$$$$uu
uu$$$$$$$$$$$$uu
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$*   *$$$$$*   *$$$$$$$$u
*$$$$$*       u$u       $$$$*
$$$$u         u$u         u$$$
$$$$u         u$$$$u      u$$$
*$$$$$uu$$$$   $$$$uu$$$$*
*$$$$$$$$$*   *$$$$$$$$$*
u$$$$$$$$$u$$$$u
u$*$$$*$$$*$$$*$$$u
$$$$u$ $ $ $ $u$$$
$$$$$$$$uuuu$$$$
*$$$$$$$$$$$$$*
uu$$$$$$$$$$$$
u$$$$$$$$$$$$$$$$uu   *****   uuuu$$$$$$$$$$$$
$$$$$*$$$*$$$$$$$$$$$$uuu   uu$$$$$$$$$$$$$$$$$$$*
***   **$$$$$$$$$$$$$$$$uu   **$***
uuuu   **$$$$$$$$$$$$$$$$uu
u$$$$uuu$$$$$$$$$$$$uu   **$$$$$$$$$$$$$$$$uu$$$$
$$$$$$$$$$$$$$$$$$$*   **$$$$$$$$$$$$$$$$$$$*
*$$$$$$$*   **$$$$$$$*
$$$$$*   PRESS ANY KEY!   $$$$$$*
```



# Phishing im Onlinebanking





# Ransomware...

---

- Angriffsvektoren
  - Spam
  - Drive-By Infektionen
  - Schwachstellen in Servern
  - Ungeschützte Fernwartungszugänge
- Varianten
  - TeslaCrypt
  - CryptoWall
  - Torrent Locker
  - Petya



# Ransomware...

---

- Aus Sicht der Unternehmen
  - Schlechte Prävention
  - Verhalten der Mitarbeiter
- Schadensseite
  - Eigenschäden
  - Reputationsschäden
  - Fremdschäden



# DDoS-Erpressung

**AMERICAN BANKER** | Bank Technology News  
Wednesday, November 11, 2015 | as of 10:04 AM ET

Today's Paper | Magazine | Video | Web Seminars | White Papers | Women in Banking | FinTech Forum

DEALMAKING & STRATEGY | COMMUNITY BANKING | NATIONAL/REGIONAL | LAW & REGULATION | CONSUMER FINANCE | BANK TECHNOLOGY

Subscriber content, log in or subscribe now to access all American Banker content

---

**bn BANK TECHNOLOGY NEWS**

## Hackers to Bankers: Pay Up or We Attack Your Website

By Penny Crosman  
September 23, 2015

Twitter LinkedIn Facebook Google+ Email Comments Print Reprints

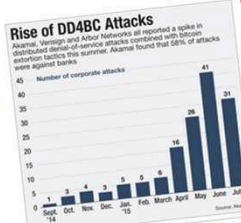
It sounds like a movie plot, but it's all too real: a group with the handle DD4BC tries to hold corporations hostage, threatening distributed denial-of-service attacks unless it is paid a ransom in bitcoins.

Comprehensive data is hard to come by, but security vendor Akamai Technologies reported a spike in such attacks from April through June before they eased a bit in July. Its rivals Arbor Networks and Verisign have detected similar patterns, and the Financial Industry Regulatory Authority recently sent warnings to companies to be on guard.

Casinos and certain other businesses have been dealing with the problem for a decade, but the number of attacks aimed at financial services firms has risen. According to Finra, several financial services and broker-dealer firms were targeted by DD4BC in June alone.

**RELATED**

- Rise of DD4BC Attacks
- Banks Lose Up to \$100K/hour to Shorter, More Intense DDoS Attacks
- What Banks Need to Know from Verizon's Comprehensive Breach Report




Month	Number of attacks
Sept. '14	1
Oct. '14	3
Nov. '14	4
Dec. '14	3
Jan. '15	5
Feb. '15	5
March '15	11
April '15	20
May '15	31
June '15	41
July '15	31

**heute**

Internetkriminalität

## Cybergangster erpressen deutsche Unternehmen



Wer bezahlt wird in Ruhe gelassen. Das Versprechen der Erpresser: "Wir machen böse Dinge, doch wir halten unser Wort." (Quelle: dpa)

Erst kommt der Angriff

Video BKA warnt vor Cyber-Kriminalität

Video Schlechter IT-Schutz in Firmen

Video Studiengang Cybersicherheit

Alfred Krüger

Unbewusst, gefährlich, professionell: Eine Gruppe von Cyberkriminellen ist seit Februar letzten Jahres weltweit Unternehmen. Die Gruppe legt die Opfer lahm und verlangt Schutzgelder. Jetzt sind auch deutsche Dienstleister betroffen.

Schutzgelderpresser treten unter dem Namen DD4BC auf. Das Kürzel steht für "Distributed Denial of Service for Bitcoins". Der Name ist Programm. Denn die fordern ihre Opfer per E-Mail auf, ein Schutzgeld in der virtuellen Währung zu bezahlen. Ansonsten würden ihre Server mit DDoS-Angriffen lahmgelegt.

**Erpresser: "Wir machen böse Dinge"**


Bei solchen Angriffen werden die Server eines Unternehmens mit Anfragen überflutet, bis sie unter dieser Last zusammenbrechen und nicht mehr erreichbar sind. Die Angriffe

**heise Security** News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2015 > KW 39 > DD4BC: DDoS-Erpresser drohen deutschen Banken

## DD4BC: DDoS-Erpresser drohen deutschen Banken

22.09.2015 16:24 Uhr - Fabian A. Scherschel



(Bild: Florian Golchert, CC BY-SA 2.0 und Norlando Pobre, CC BY 2.0)

**Eine berühmte Erpressergruppe hat sich die deutsche Finanzindustrie vorgenommen. Sie droht mit massiven DDoS-Angriffen und verlangt fünfstelligen Beträge in Bitcoins als Lösegeld.**

Eine Gruppe von Angreifern, die sich **DD4BC (DDoS for Bitcoins)** nennt, erpresst seit mindestens November 2014 die Betreiber von unzähligen Webseiten. Die Drohung lautet immer gleich: Zahlt uns ein Lösegeld in Bitcoins, oder wir legen Eure Seite derart mit Traffic lahm, dass Eure Kunden in die Röhre schauen. Dabei erpressen sie nicht einfach irgendwen, sondern recherchieren lukrative Ziele. Seit einigen Tagen soll besonders die deutsche Finanzbranche erneut im Visier der Erpresser sein.



# DDoS-Erpressung...



## **Digitale Agenda**

Der Staat steht auch in der vernetzten Welt in der Verantwortung, Gefahren und Kriminalität im Internet wirksam abzuwehren. Wir nehmen diese Verantwortung für die öffentliche IT-Sicherheit an und wollen unserer Aufgaben des Schutzes der Gesellschaft und Wirtschaft im digitalen Zeitalter gerecht werden. Dazu bedarf es einer strategischen Neuausrichtung der Cyber-Sicherheitsarchitektur ebenso wie einer besseren Ausstattung der Sicherheitsbehörden in technischer und personeller Hinsicht.

## **§ 4 Strafverfolgung**

(1) Das Bundeskriminalamt nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr (...)

in den Fällen von Straftaten nach den §§ 202a, 202b, 202c, 263a, 303a und 303b des Strafgesetzbuches, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass die Tat sich gegen

a) die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder

b) Behörden oder Einrichtungen des Bundes oder sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind, richtet.



Bundeskriminalamt

# Polizeiliches/behördliches Netzwerk



Bundesamt  
für Sicherheit in der  
Informationstechnik



Zentrale Ansprechstellen Cybercrime  
der Polizeien der Länder und des Bundes  
für die Wirtschaft



# Handlungsempfehlungen

einschl. Ansprechpartner

The screenshot shows the BKA website with the following elements:

- Search Bar:** Located at the top left, with the text "Suchbegriff eingeben" and "Erweiterte Suche".
- Sidebar:** A list of crime categories on the left side, including "Arzneimittelkriminalität", "Betrügerische Gewinnversprechen am Telefon (Call-Center-Betrug)", "Falschgeld", "Geldwäsche (FIU)", "Internetkriminalität", "Internetrecherche - ZaRD", "Identitätsdiebstahl", "SPAM", "Hoaxes (Falschmeldungen)", "Hacktivismus", "Internet-Sicherheit", "Cyber-Sicherheitsstrategie", "Lagebilder Cybercrime", "Handlungsempfehlungen für die Wirtschaft", "69. Deutscher Juristentag", "Kfz-Kriminalität", "Kinderpornographie", "Kindersextourismus", "Korruption", "Menschenhandel", "Organisierte Kriminalität", "Rauschgiftkriminalität", "Schleusungskriminalität", "Terrorismus/ Extremismus", "Waffen", "Wirtschaftskriminalität", "Zahlungskartenkriminalität", "DNA-Analyse", "Elektronische Fahndungs- und Informationssysteme", and "Erkennungsdienst".
- Main Content Area:** The title "Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime" is prominently displayed. Below it, there is a detailed text block discussing the results of a survey conducted by the IHK Nord in 2013, highlighting the prevalence of cyberattacks on businesses. A graphic titled "Cybercrime" is also visible, showing various types of cyber threats like "Trojaner", "Viren", "Phishing", "Hacker", "Manipulation", "Sabotage", "DDoS-Angriff", "Betrug", "Fälschung", "Aushebeln", "Datenklau", and "Online-Erpressung".
- Footer:** The page includes a "Seite drucken" button and a copyright notice "© Bundeskriminalamt - 2016".

- [www.bka.de](http://www.bka.de)
- Im Suchfeld „Handlungsempfehlungen“ eingeben



Bundeskriminalamt

# Danke für die Aufmerksamkeit!



SO41 - Nationale Kooperationsstelle Cybercrime (NKC)

[so41-nkc@bka.bund.de](mailto:so41-nkc@bka.bund.de)

0611 – 55 15037