

# Der AV-TEST Sicherheitsreport 2015/2016



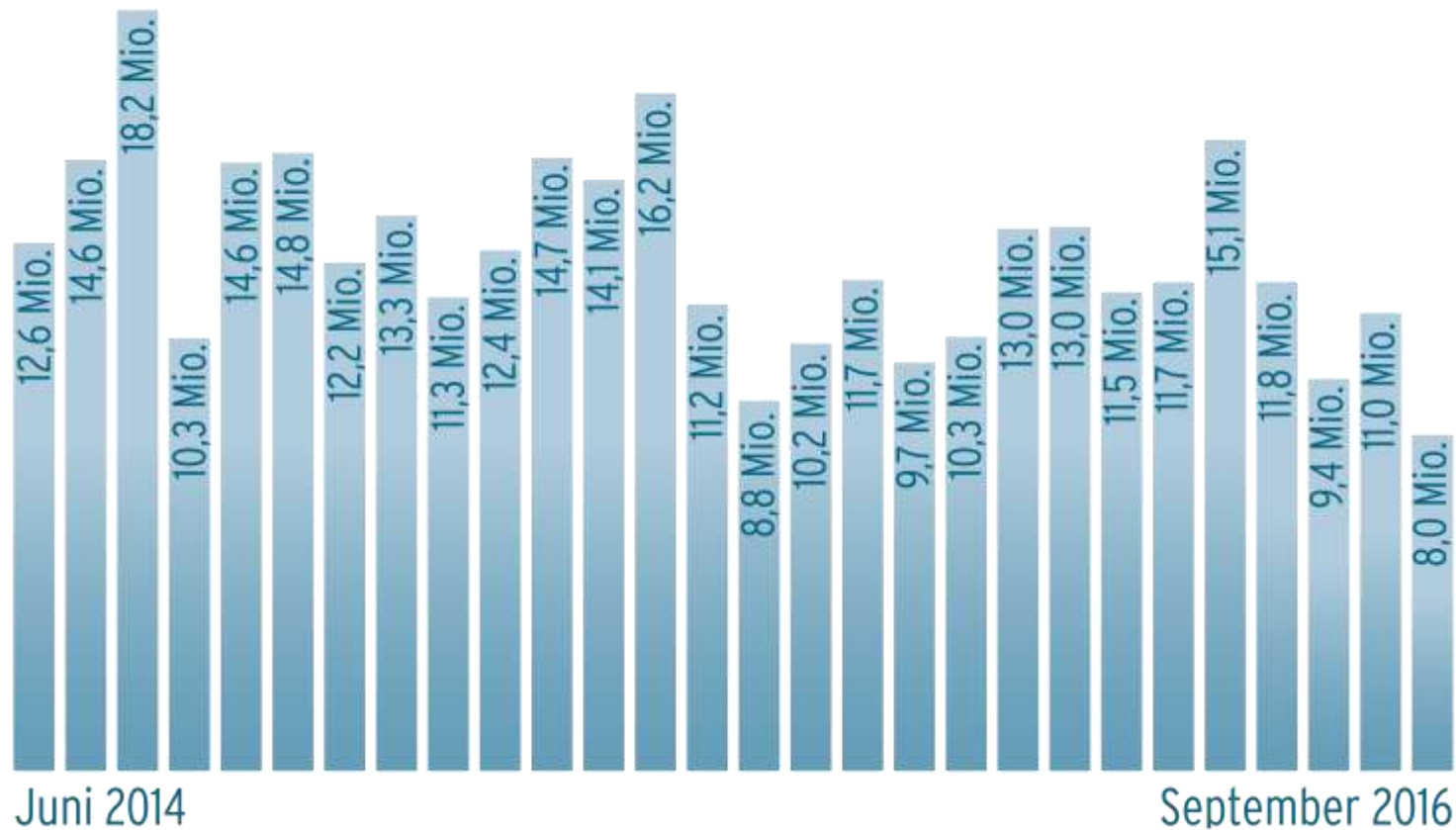
- **Team: über 30 international anerkannte Security-Spezialisten**
- **eine der größten Sammlungen digitaler Schädlinge weltweit**
- **eigene Forschungsabteilung**
- **intensive Zusammenarbeit mit wissenschaftlichen Einrichtungen**
- **selbstentwickelte Analysesysteme**
- **reproduzierbare Testergebnisse für alle gängigen Betriebssysteme und Plattformen**





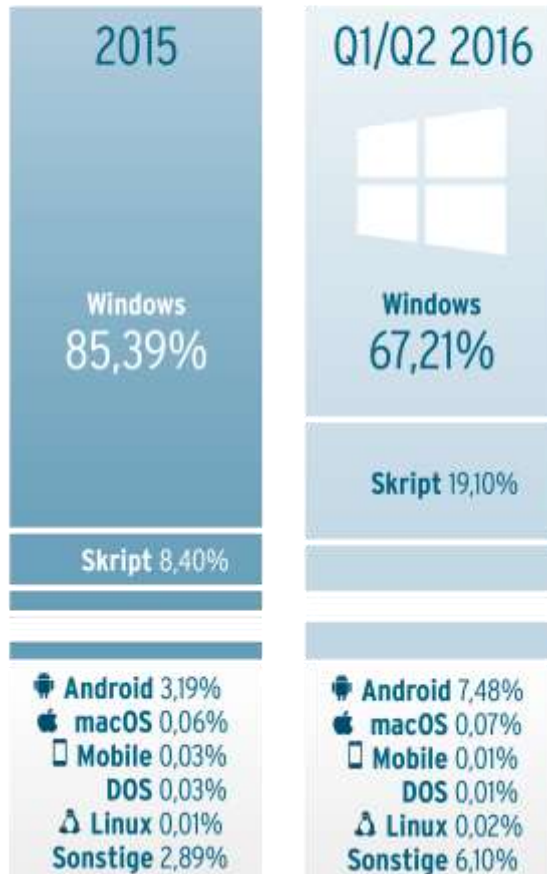
5 NEUE SCHÄDLINGE PRO SEKUNDE!

## Auftreten neuer Malware insgesamt



## VERTEILUNG VON MALWARE

### Malware-Erkennung nach Betriebssystem



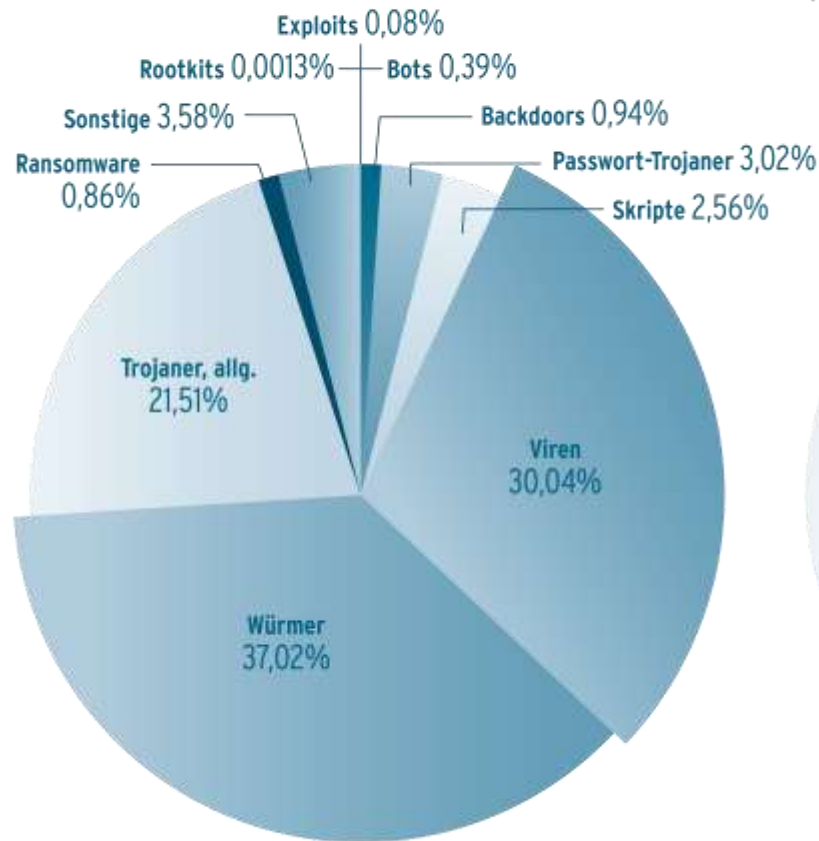
- Hauptangriffsziel Windows
- Android und Skript-Malware holen stark auf



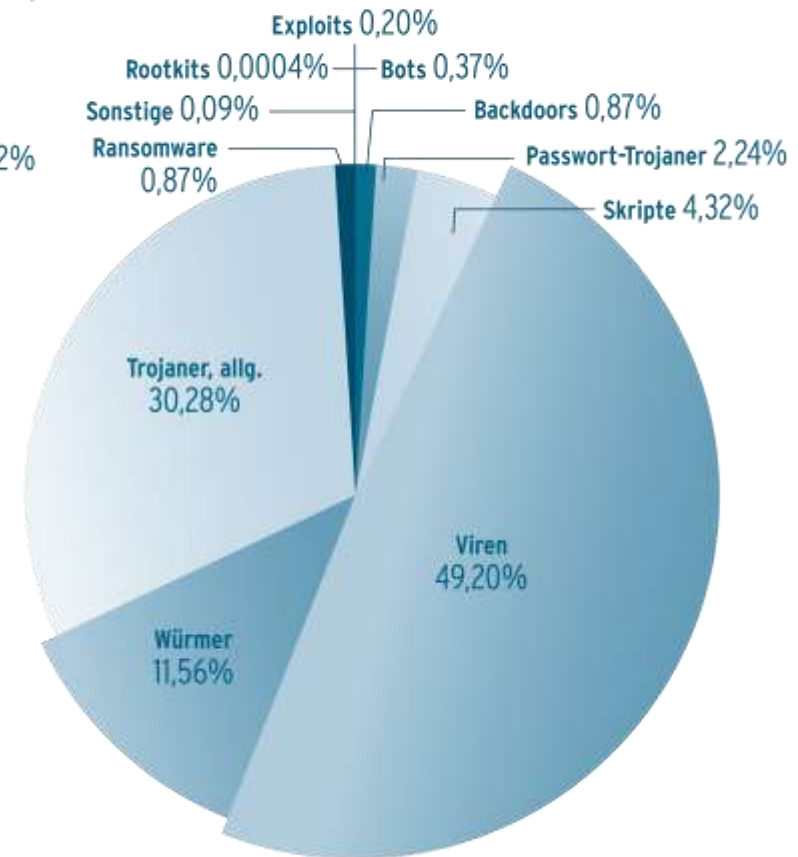
# VIREN UNTER WINDOWS AUF DEM VORMARSCH

## Malware-Verteilung unter Windows

2015



Q1/Q2 2016



## WINDOWS-MALWARE „HIGHLIGHTS“: RANSOMWARE

Betreff: Stefan Friedrich - Bewerbung

Datum: Mon, 05 Dec 2016 08:26:57 +0000

Von: Stefan Friedrich <[s.friedrich@t-online.de](mailto:s.friedrich@t-online.de)> Antwort an: Stefan Friedrich <[s.friedrich@t-online.de](mailto:s.friedrich@t-online.de)>

An: [REDACTED]

Sehr geehrte Damen und Herren,

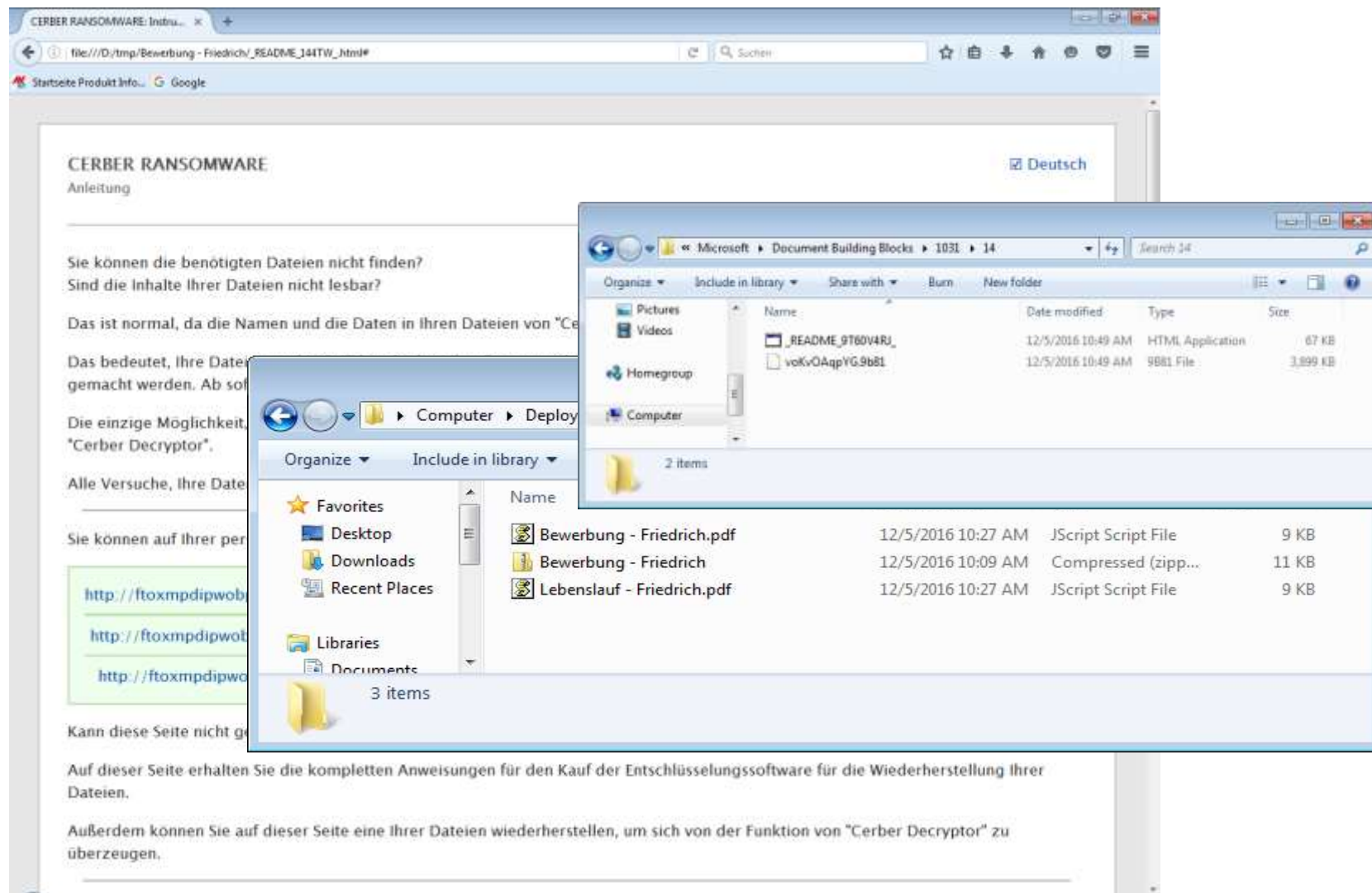
anbei finden Sie meine Bewerbung für Ihre ausgeschriebene Position. Die Stelle entspricht genau meinen Vorstellungen und reizt mich sehr. Da mein Profil und meine bisherigen Erfahrungen gut zu Ihren Anforderungen passen, bin ich davon überzeugt, einen echten Mehrwert leisten zu können. Und das möchte ich!

Ich freue mich, wenn Sie meine Bewerbungsunterlagen im Anhang prüfen und ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit besten Grüßen,

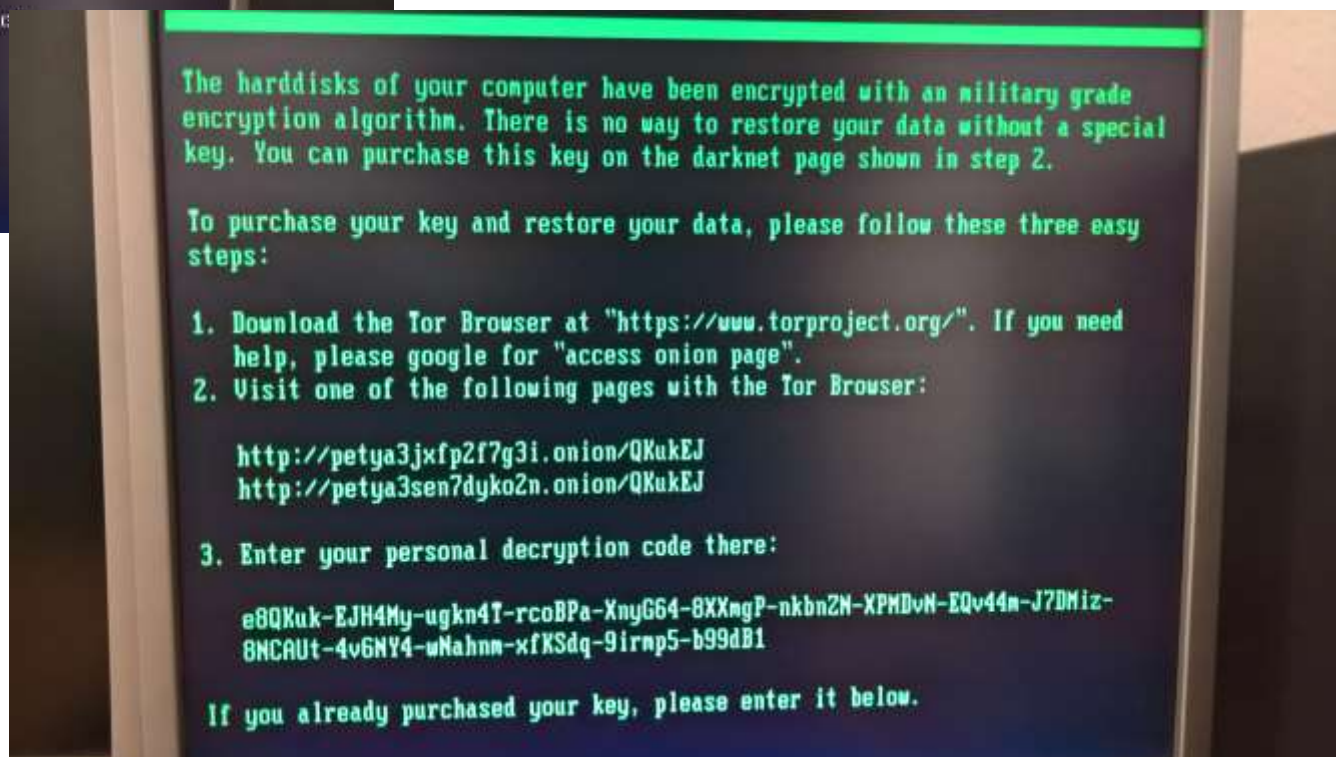
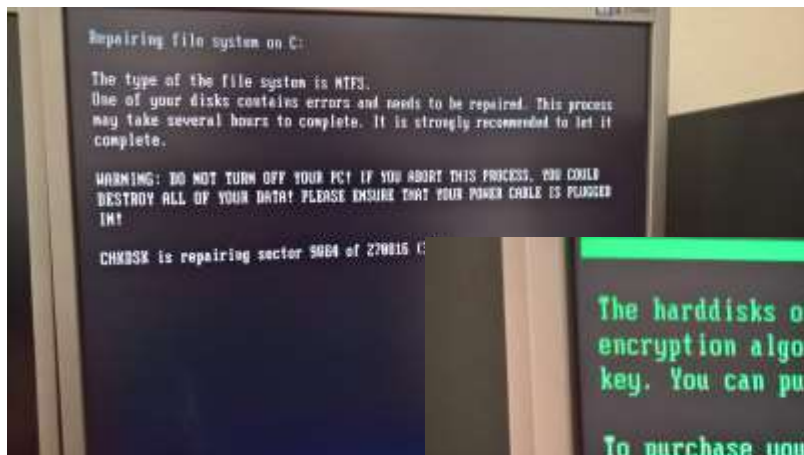
Stefan Friedrich

# WINDOWS-MALWARE „HIGHLIGHTS“: BANKING-TROJANER





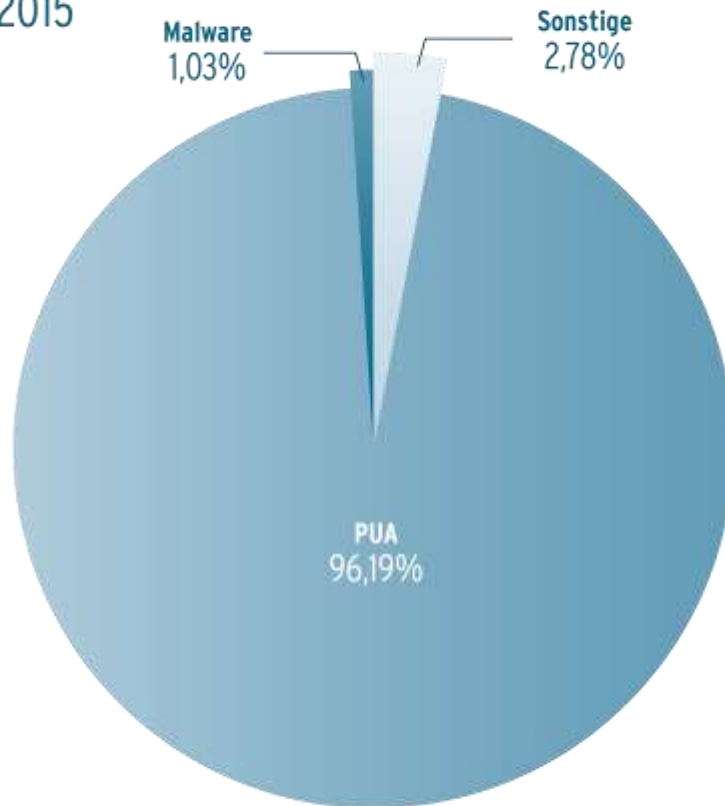
# WINDOWS-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



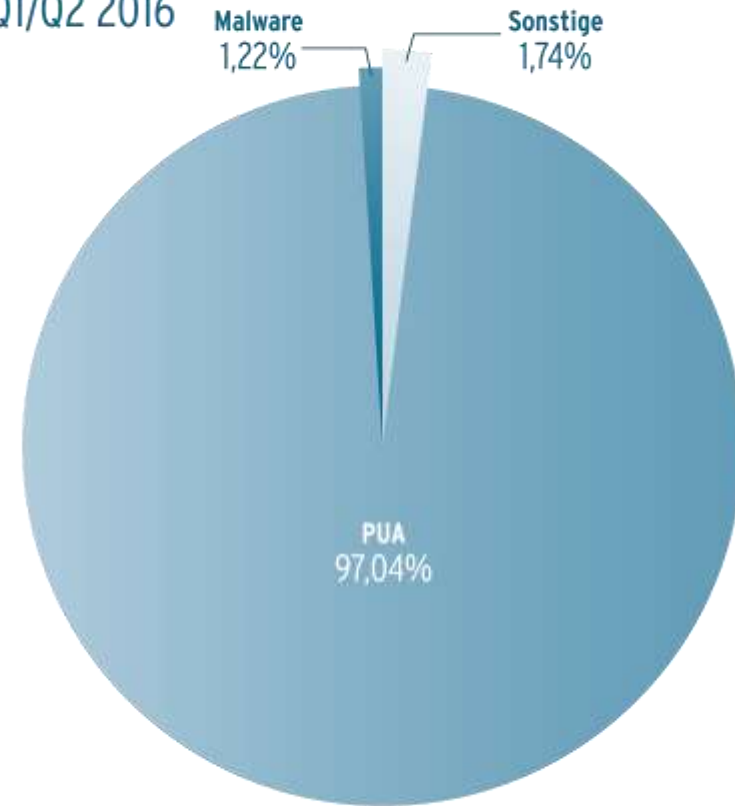
# GEFAHRENLAGE FÜR MAC-NUTZER

## Schädlinge macOS

2015



Q1/Q2 2016



# Schädlinge Android versus Mobil

**Android 2015**

99,18%

**Android Q1/Q2 2016**

99,87%

**Mobile 2015**

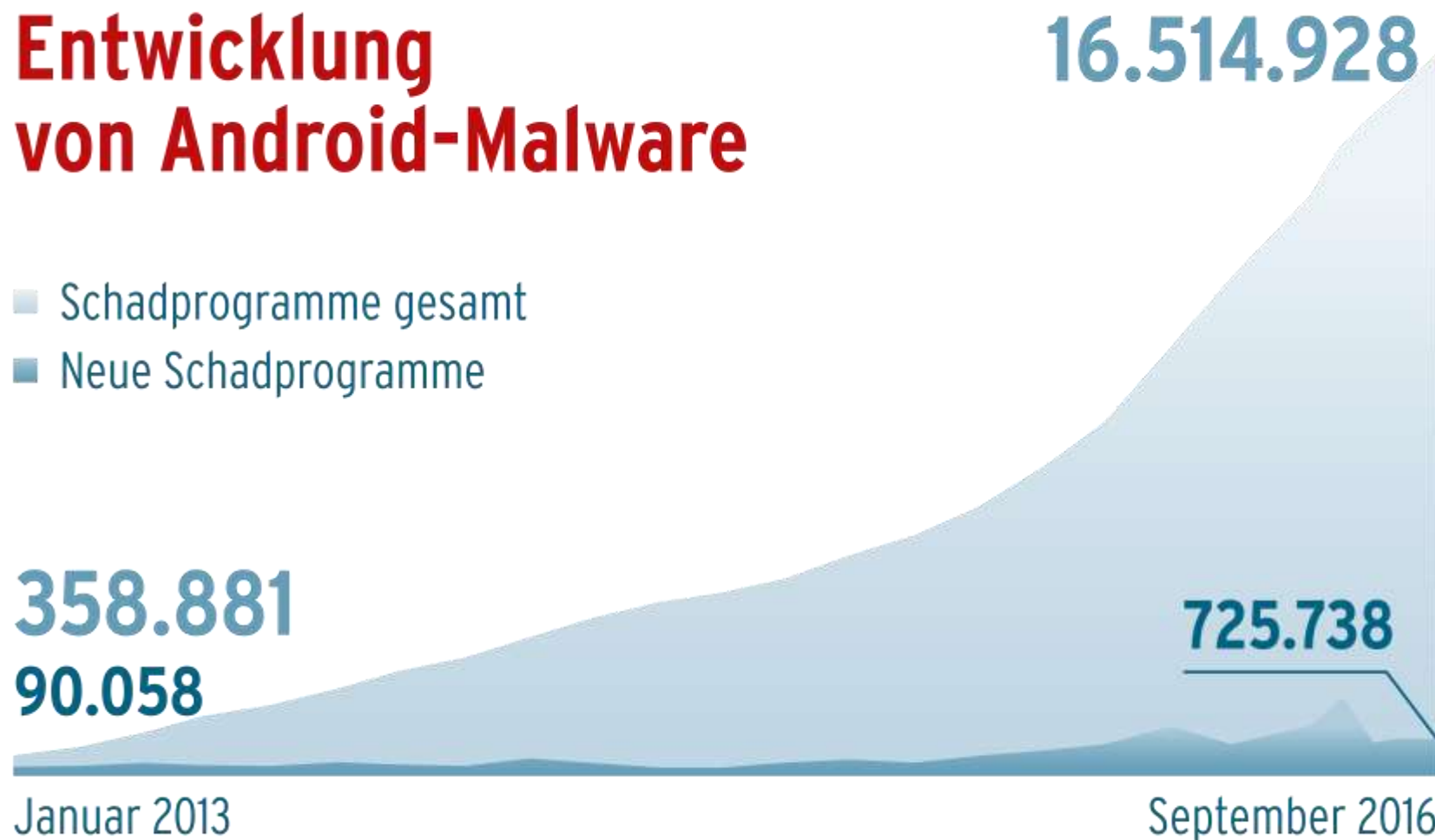
0,82%

**Mobile Q1/Q2 2016**

0,13%

## Entwicklung von Android-Malware

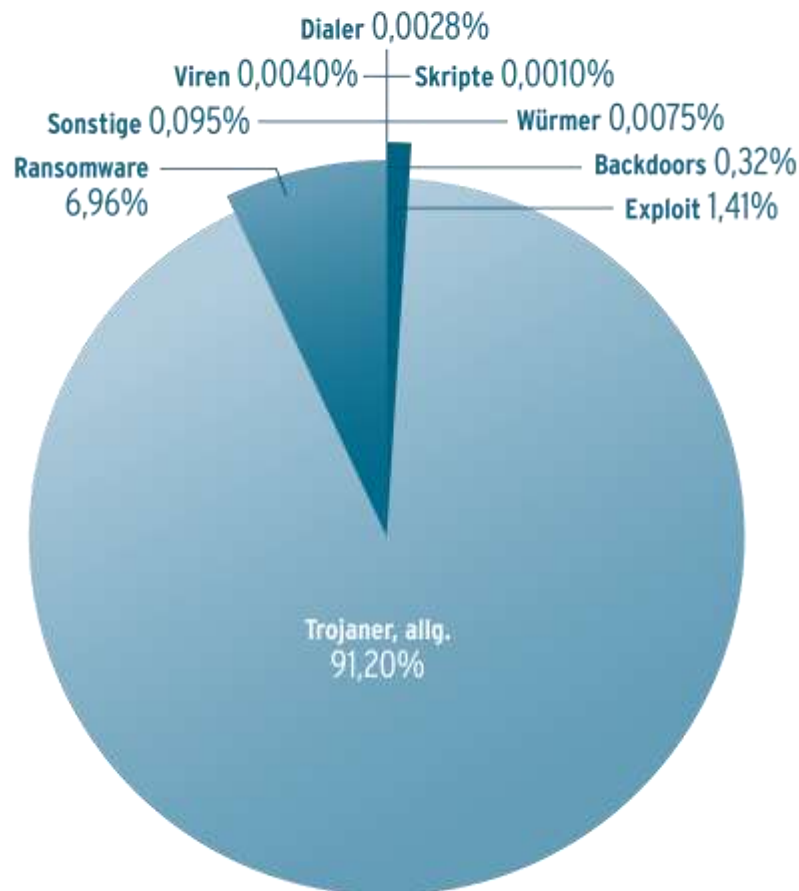
- Schadprogramme gesamt
- Neue Schadprogramme



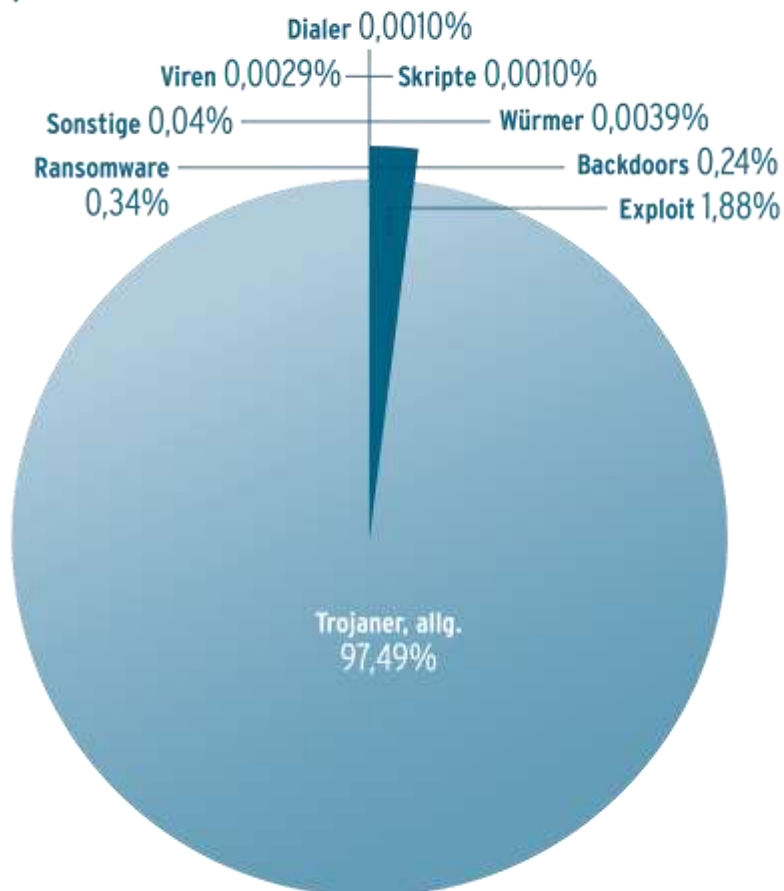
# TROJANER-ATTACKEN AUF ANDROID

## Malware-Verteilung Android

2015

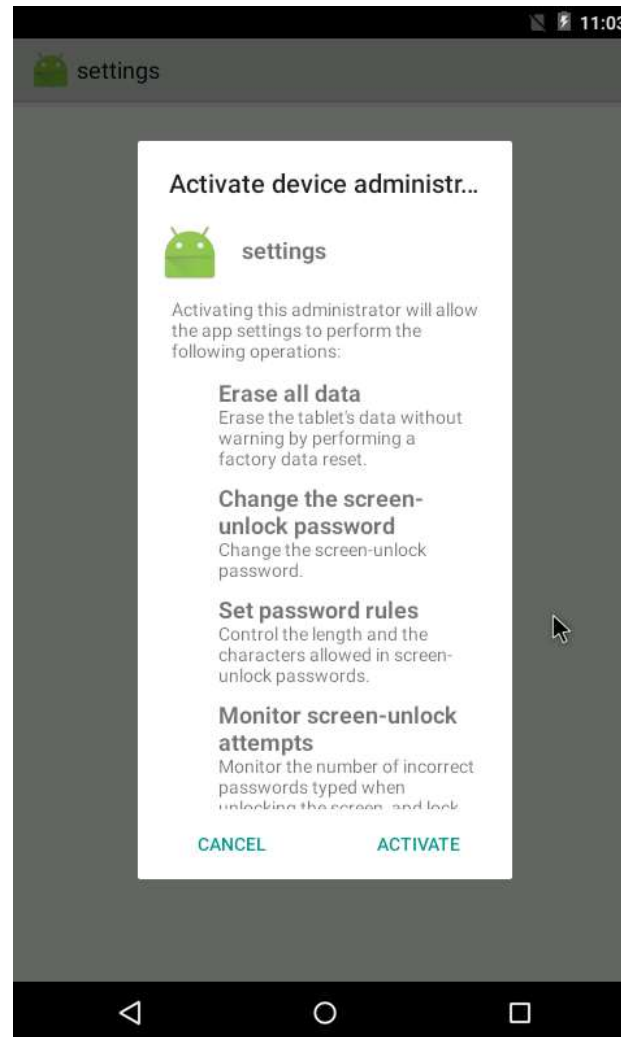


Q1/Q2 2016





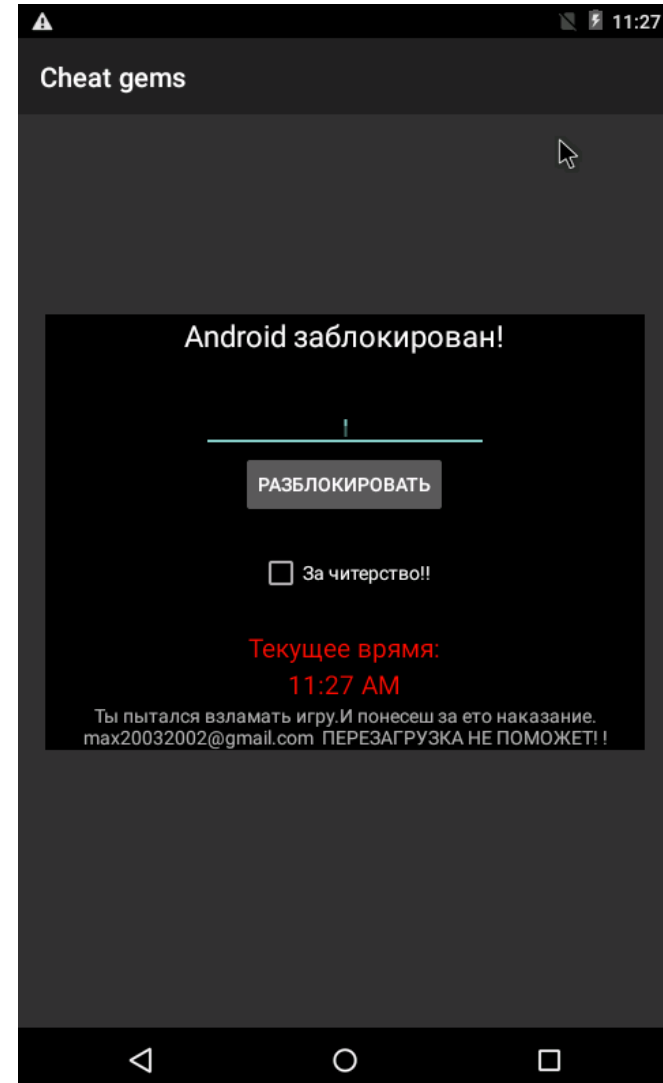
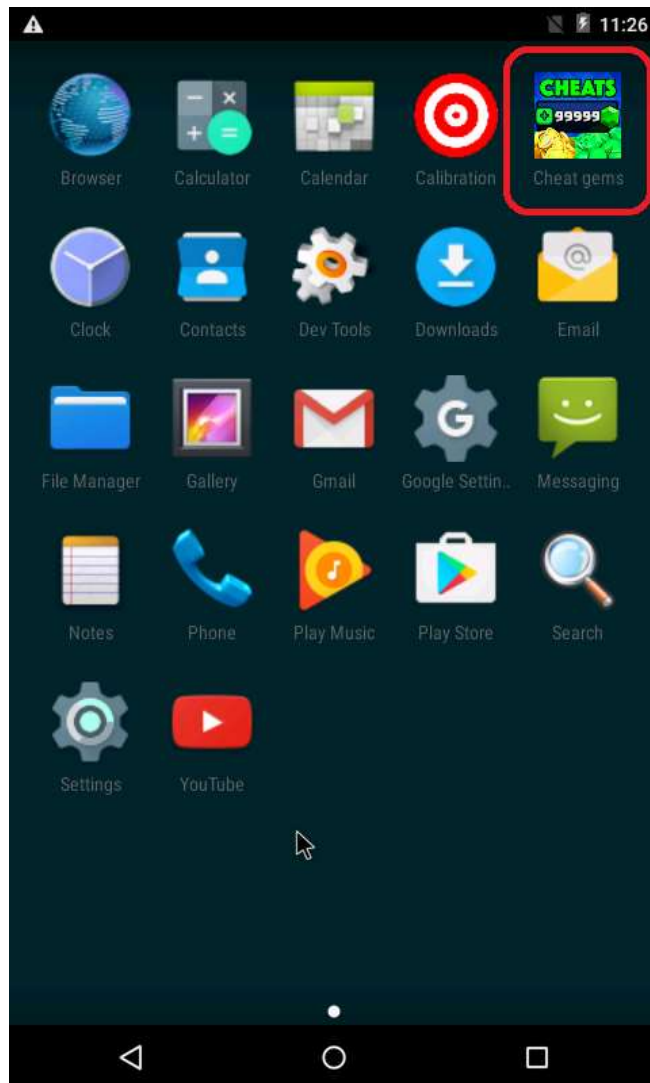
# ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER



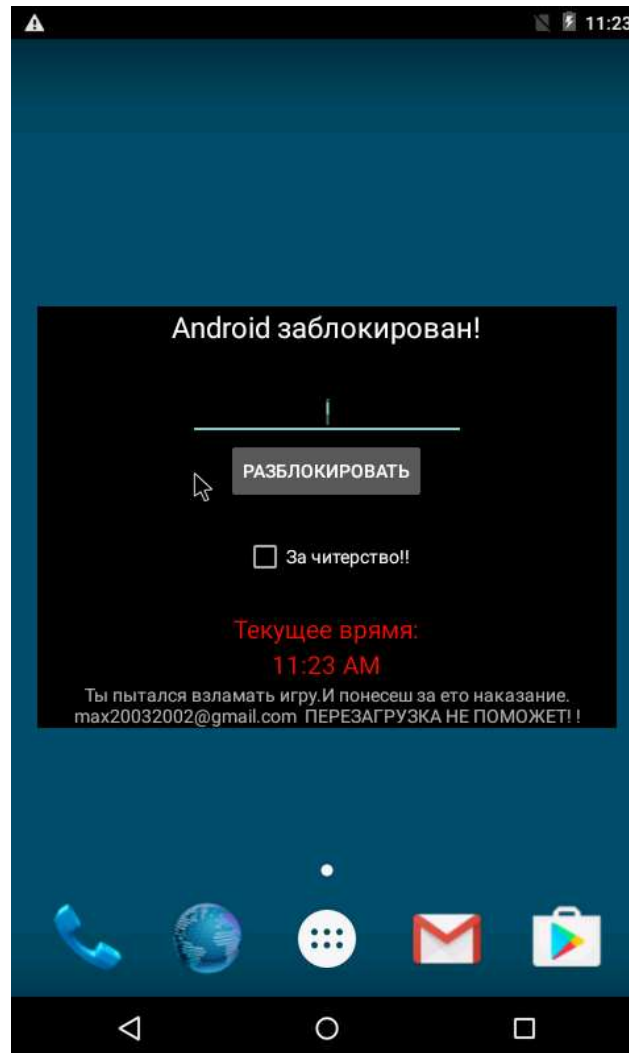
## ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER



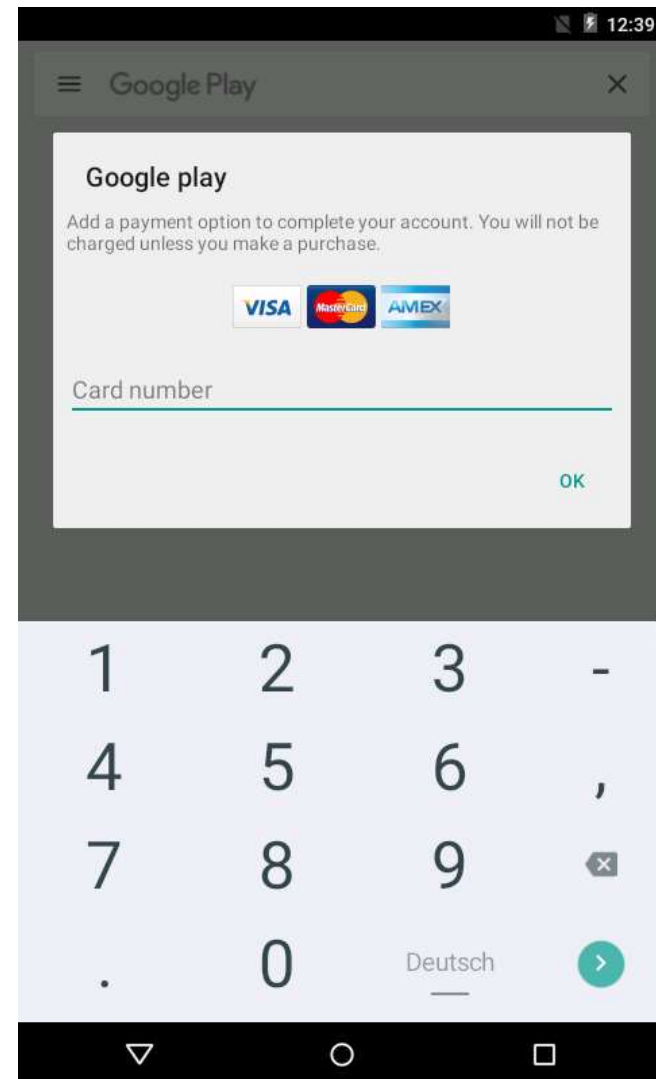
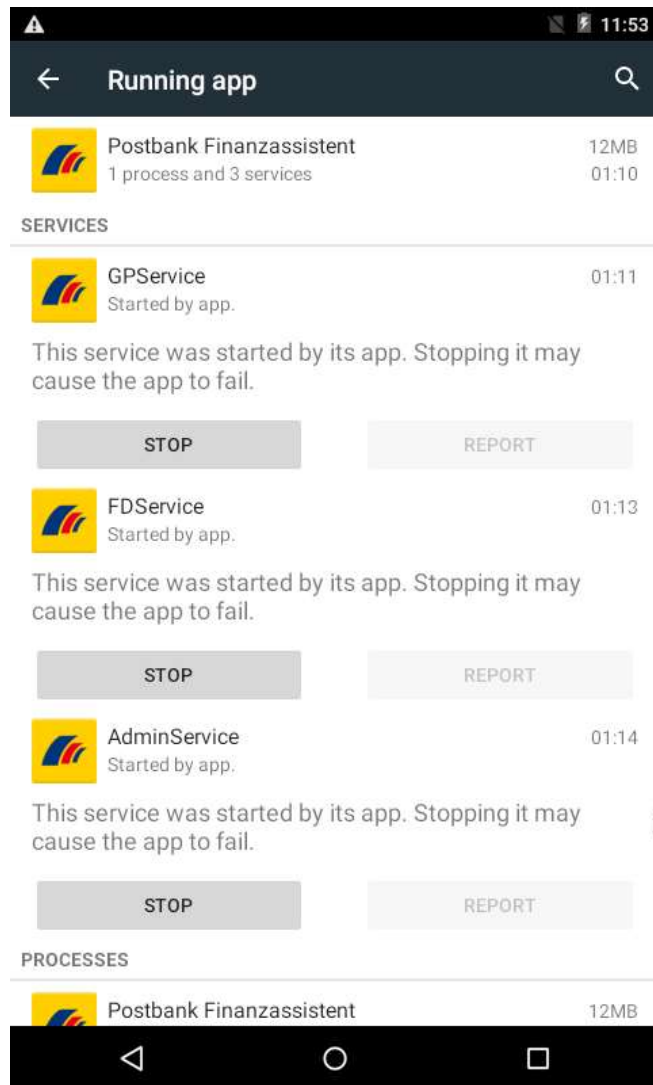
## ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER



## ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER

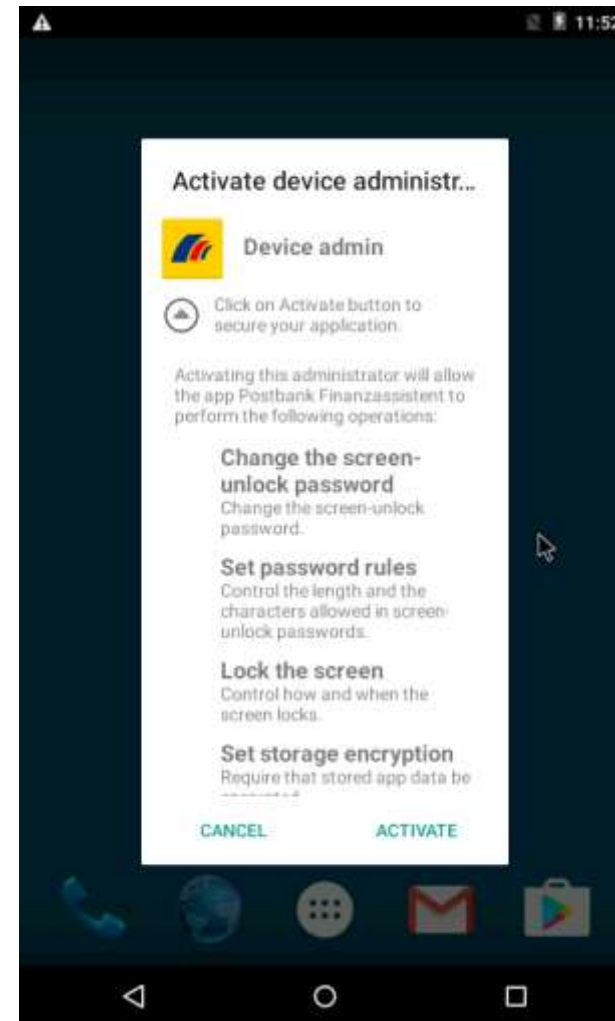
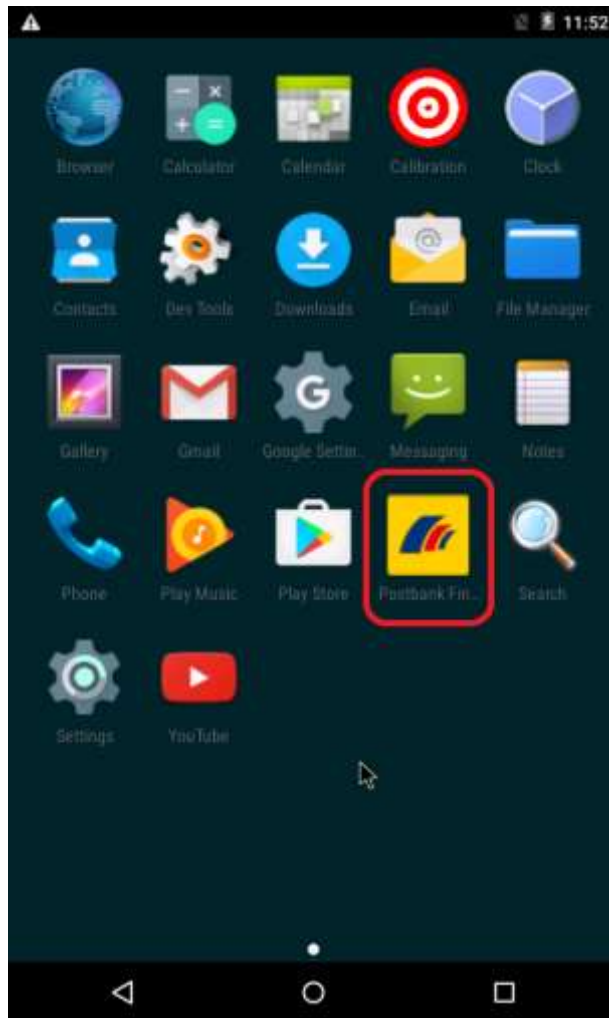


# ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER

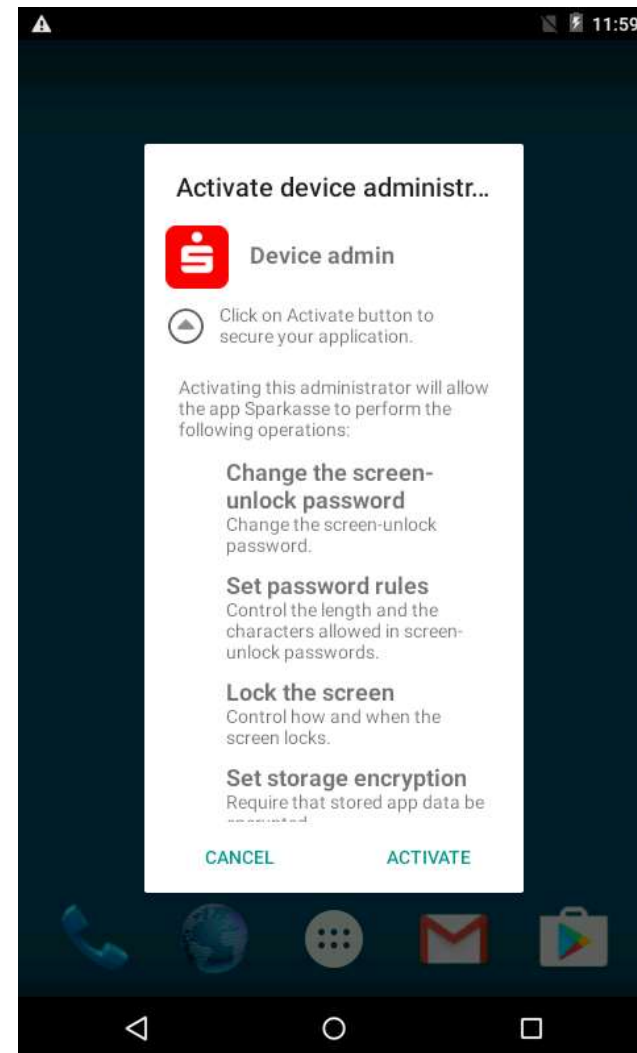
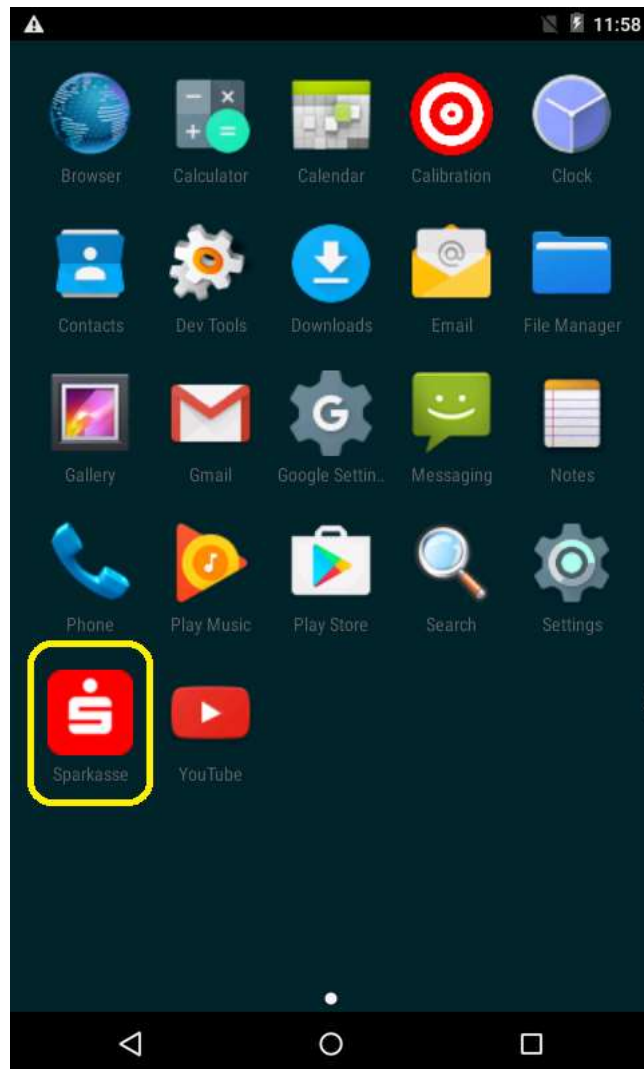




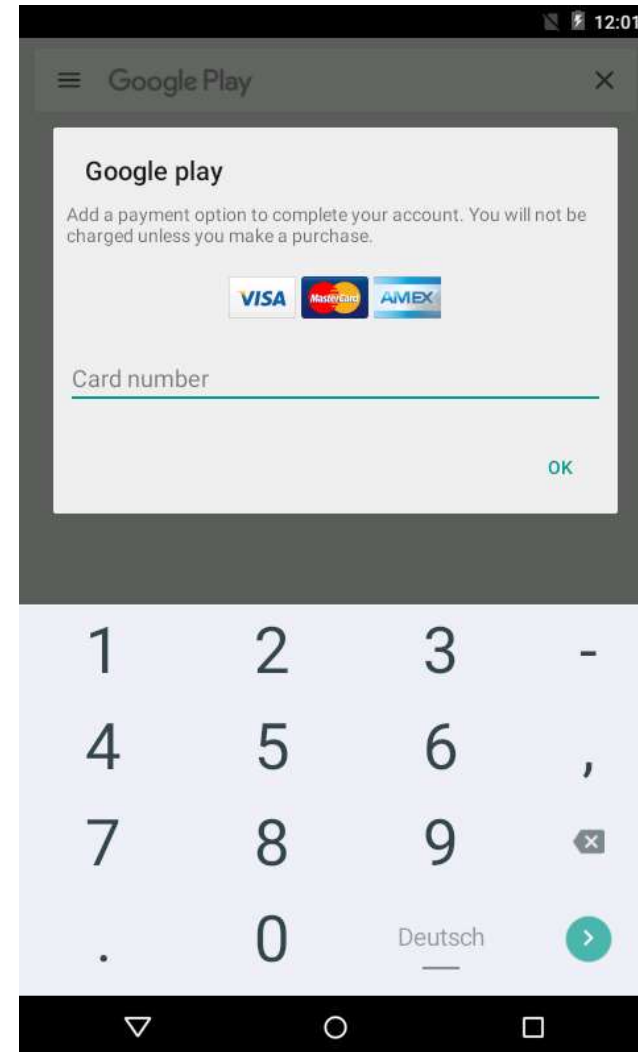
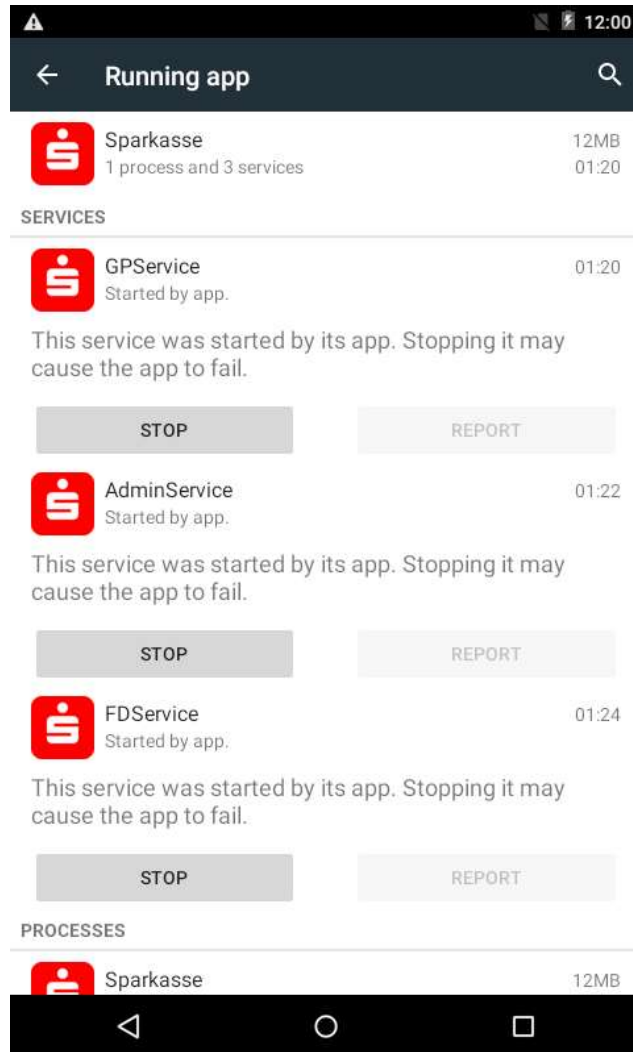
# ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



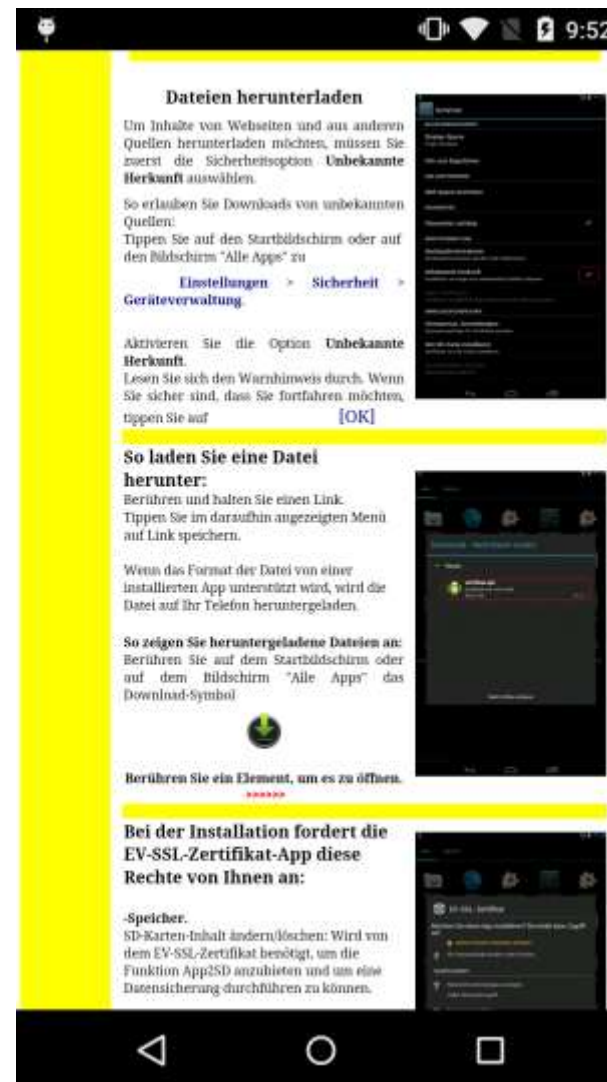
# ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



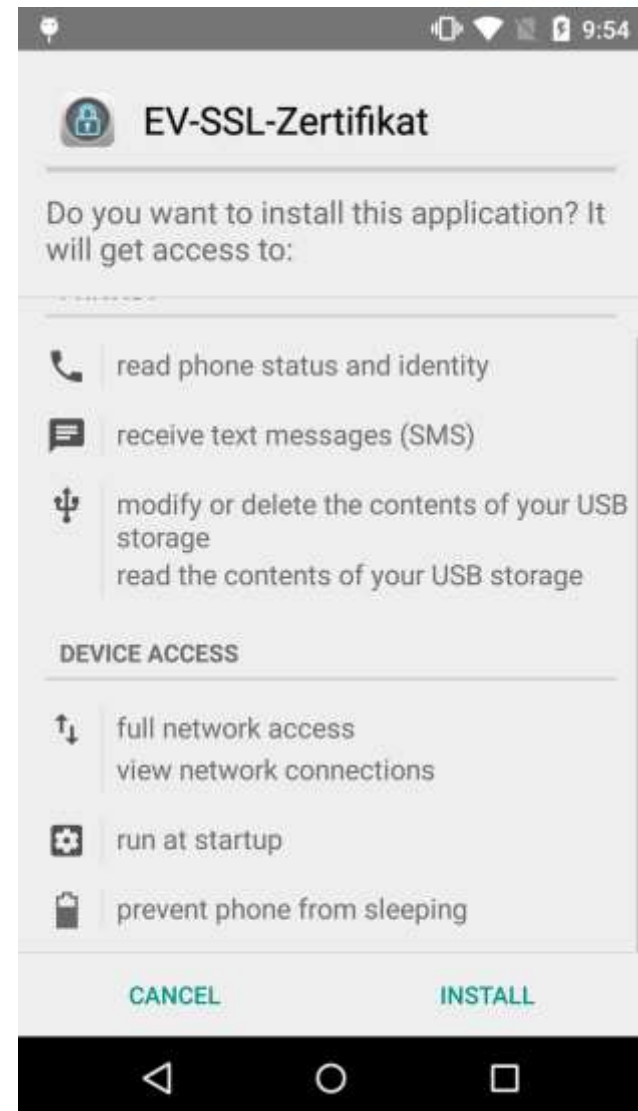
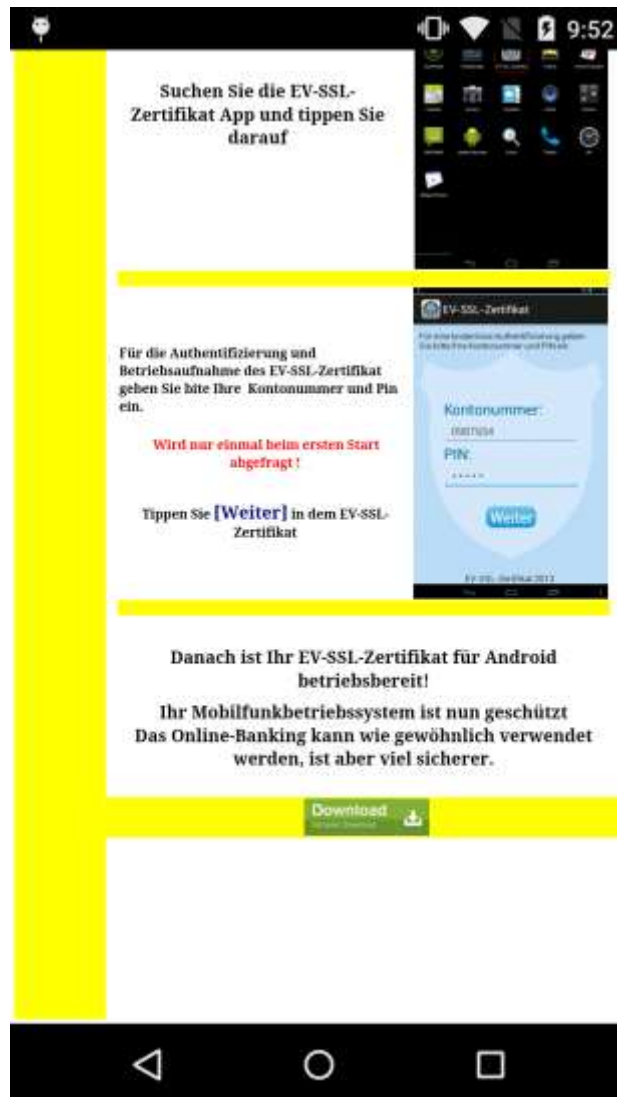
# ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



# ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



# ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



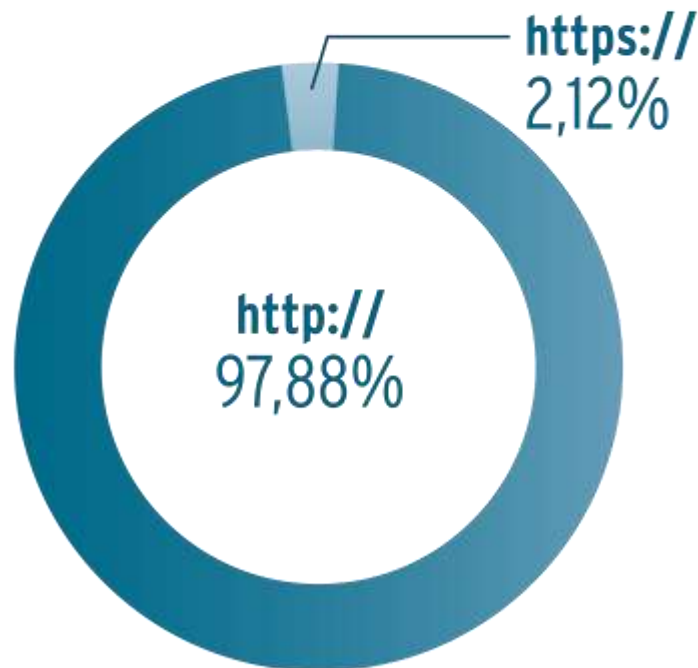


# ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER

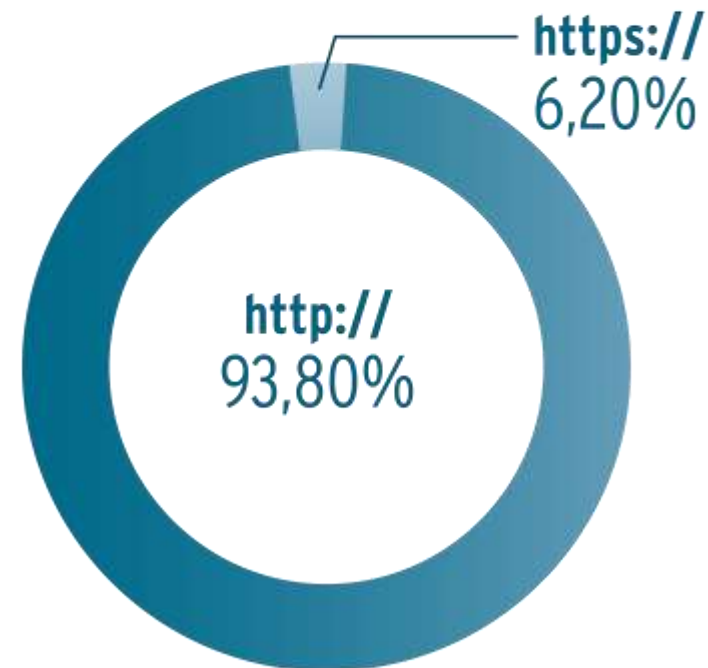


## Malware-Verteilung über verschlüsselte und unverschlüsselte Internetseiten

2015



Q1/Q2 2016



## TOP 10 Malware-Domains 2015

<b>1</b>	COM	47,68%
<b>2</b>	RU	13,15%
<b>3</b>	SU	10,06%
<b>4</b>	NET	5,89%
<b>5</b>	ORG	3,97%
<b>6</b>	TR	1,90%
<b>7</b>	IT	1,16%
<b>8</b>	DE	1,15%
<b>9</b>	PL	0,89%
<b>10</b>	INFO	0,71%

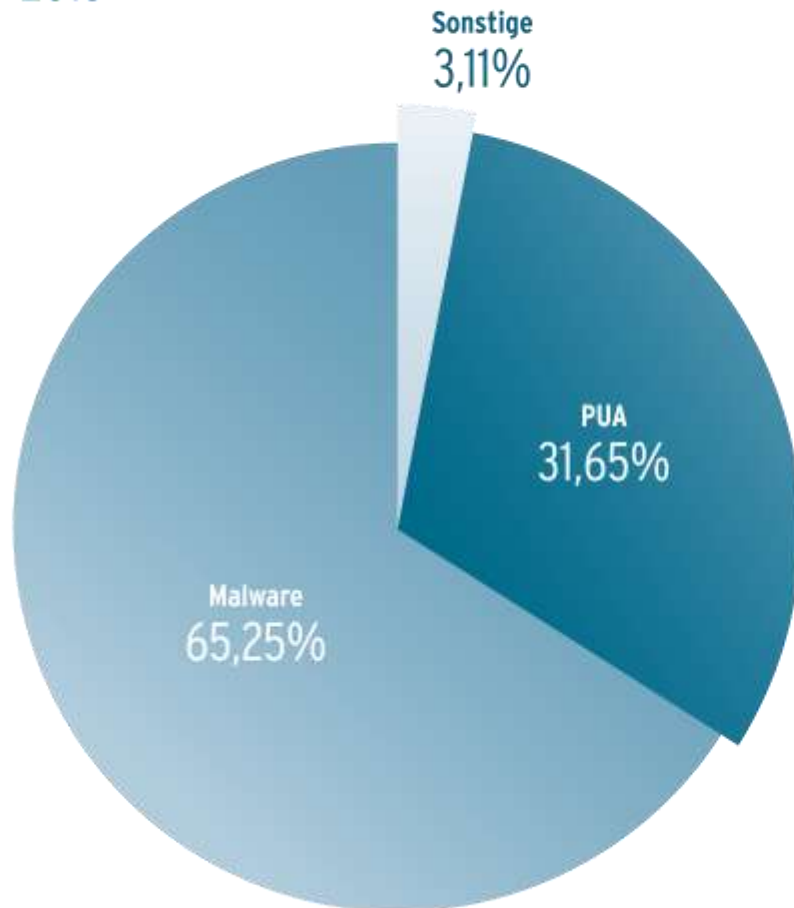
### TOP 10 File Extensions Malware 2015

1	EXE	37,90%
2	HTML	35,12%
3	ZIP	11,08%
4	RAR	5,80%
5	PHP	4,03%
6	SWF	2,32%
7	ASP	1,67%
8	HTM	1,28%
9	PDF	0,22%
10	ASPX	0,15%

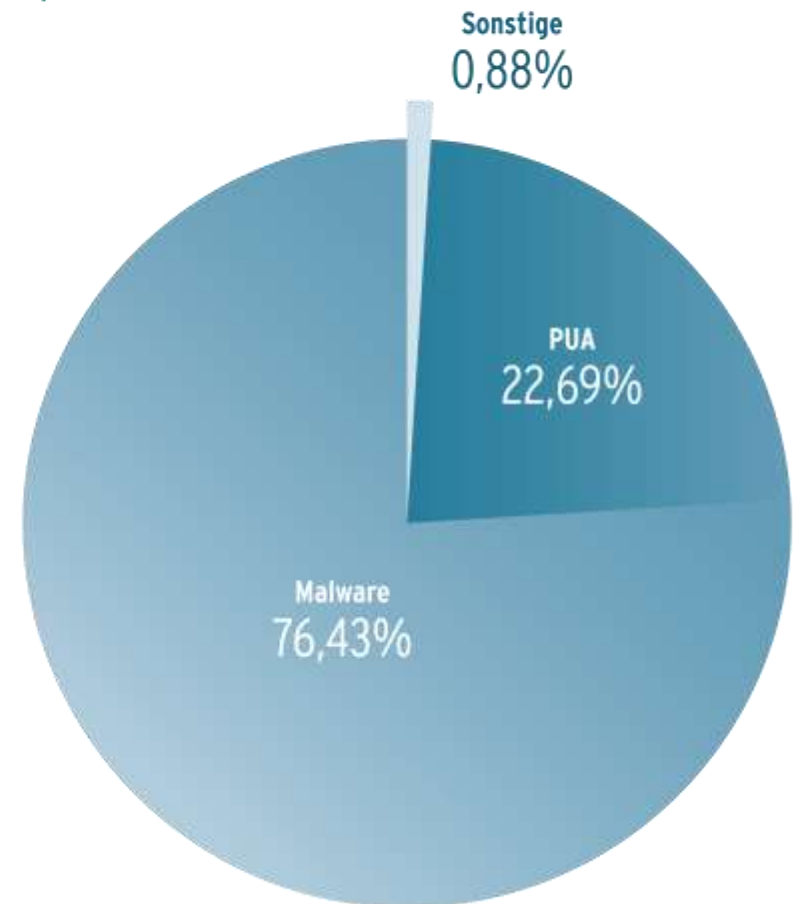
## PUA – DIE WACHSENDE GEFAHR

### PUA-Erkennung gesamt

2015



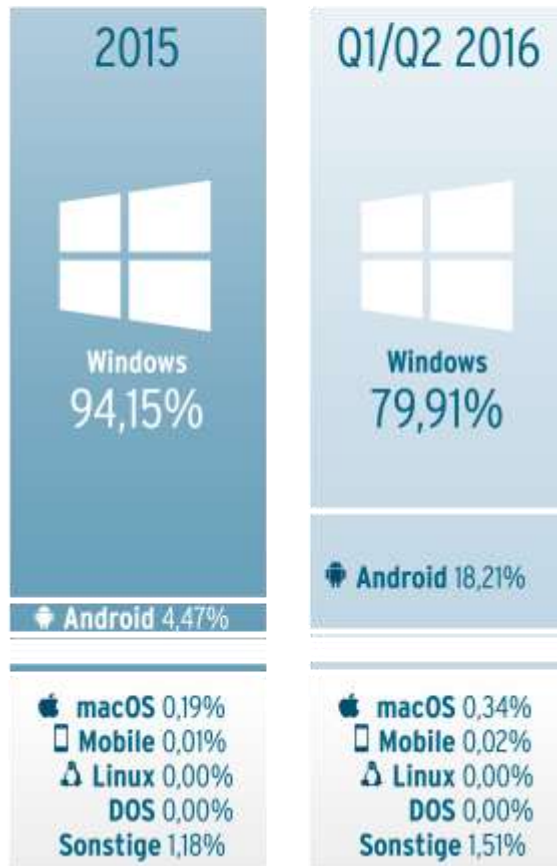
Q1/Q2 2016





## PUA – DIE WACHSENDE GEFAHR

### PUA-Erkennung nach Betriebssystem



- Windows ist Hauptangriffsziel
- PUA für Android nimmt stark zu
- Im Unterschied zu Malware gibt es massenhaft PUA für macOS

Suche Sie Ihr Suchbegriff hier...

Home Aktuelle Kinofilme Filme Serien FAQ Tools RSS feed

**MyKino.to**  
Filme und Serien kostenlos!

Wusstest du schon das MyKino.to auch am iPad verfügbar ist?  
Einfach [www.mykino.to](http://www.mykino.to) aufrufen, Lesezeichen speichern und streams genießen.

**Independence Day: Wiederkehr** STREAM in HD

**Jahr:** 2016 **Länge:** 120 min.  
**Genre:** Sci-Fi, Action, Aktuelle Kinofilme  
**IMDb Wertung:** 5.3/10 102570 votes  
**Land:** N/A  
**Regie:** Roland Emmerich  
**Schauspieler:** Liam Hemsworth, Jeff Goldblum, Jesse Usher, Bill Pullman, Minka Monroe, Selo Ward, William Fichtner, Judd Hirsch

**STREAM in HD NOW**

20 Jahre ist es her, dass Aliens die Erde attackierten und die Hälfte der Bevölkerung auslöschten. Vor allem der mutigen Mission des Piloten Steven Hiller und des Satellitentechnikers David Levinson verdanken wir es, dass die Außerirdischen 1996 besiegt wurden – tragischerweise kam Hiller dann 2007 ums Leben, als er einen Alien-Hybrid-Fighter testete. Und 2016 wird er umso mehr vermisst, als sich die Warnung des Ex-Präsidenten Whitmore bewahrheitet und die Außerirdischen einen neuen, noch verheerenden Angriff starten! Die Menschheit, die in bis dato die gekanntest Einigkeit ein mit Alien-Technologie erweitertes Verteidigungssystem schuf, steht vor ihrer größten Herausforderung. Die Hoffnungen ruhen auf den jungen Kampfpiloten Jake und Dylan, dem Sohn des verstorbenen Steven Hiller.

**Download** **Jetzt Anschauen**

Anbieter Auswahl für Independence Day: Wiederkehr MyKino.to speichert keine Filme selbst!

**StreamCloud** **Newvideo.ch** **Shared.sx** **Flashix.tv**

HD-Stream	Mirror: #1	Mirror: #2	Mirror: #3	Mirror: #4	Mirror: #5
PLAY NOW	PLAY NOW	PLAY NOW	PLAY NOW	PLAY NOW	PLAY NOW
Mirror: #6	Mirror: #7	Mirror: #8	Mirror: #9	Mirror: #10	
PLAY NOW	PLAY NOW	PLAY NOW	PLAY NOW	PLAY NOW	

**Share** **Senden** **Tweet** **Google** **Pinterest** **Email**

Empfohlene Einträge für "Independence Day: Wiederkehr"

**Genres**

Filme	Serien
ABENTEUER	ACTION
BIOGRAPHIE	DRAMA
FAMILIE	FANTASY
HORROR	KOMÖDIE
KRIMI	ROMANTIK
SCI-FI	THRILLER
TRICKFILM	WESTERN
KRIEG	SPORT

**Unsere Fanseite**

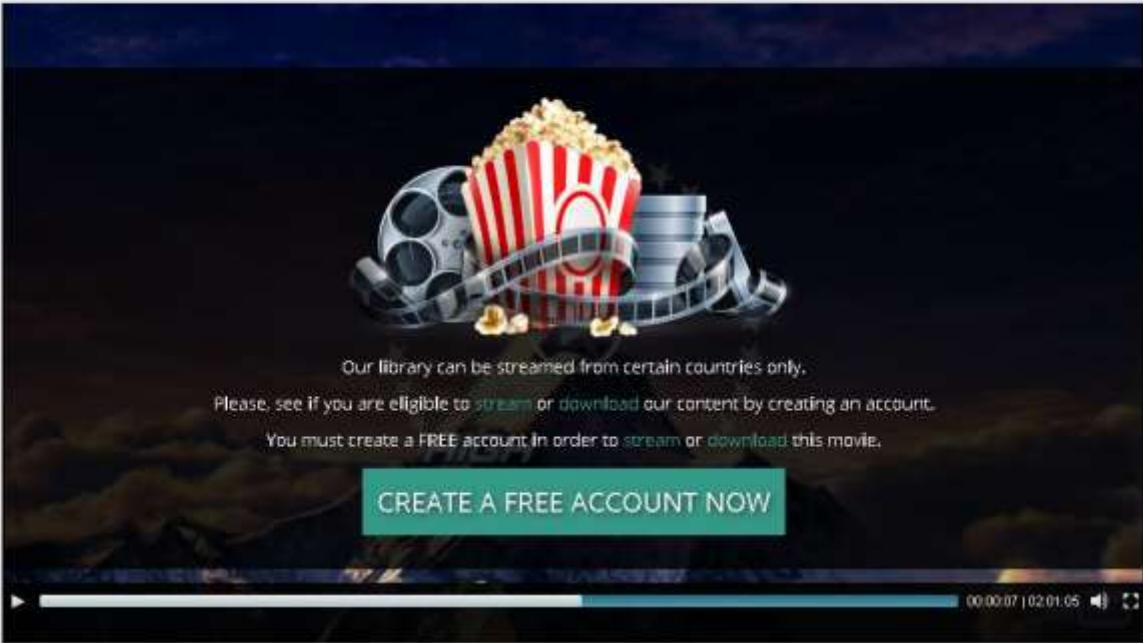
**MyKino.to**  
Sei der Erste deiner Freunde, dem/der das gefällt

**Meistgesehene**

# PUA – DIE WACHSENDE GEFAHR

INDEPENDENCE DAY: WIEDERKEHR (2016)  
120 min | 4K ULTRAHD | FULL HD (1080p) | SD

f 2.5M s 1.1M t 21k




Our library can be streamed from certain countries only.  
Please, see if you are eligible to [stream](#) or [download](#) our content by creating an account.  
You must create a **FREE** account in order to [stream](#) or [download](#) this movie.

**CREATE A FREE ACCOUNT NOW**

AVAILABLE FORMATS

**4K ULTRAHD** ultra high definition  
**FULL HD** 1080p  
**SD** 480p  
FLV  
Mobile  
TV

 **DOWNLOAD**

# INTERNET DER DINGE: ALLES SMART, ODER NICHT?



[www.thefuturesagency.com](http://www.thefuturesagency.com), update: January 20, 2015



# BEISPIEL IP-KAMERAS: SORGEN FÜR SICHERHEIT



# BEISPIEL IP-KAMERAS: INSECAM

https://www.insecam.org/en/yourcountry/DE/?page=12

IP cameras: Germany

Facebook Twitter + More

IT Wartung für EMC Post Warranty - End of Life Wartung Allera Credit Effect

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 ... 114

Watch Vivitek camera in Germany, Karsburg

Watch Vivitek camera in Germany, Rütenscheid

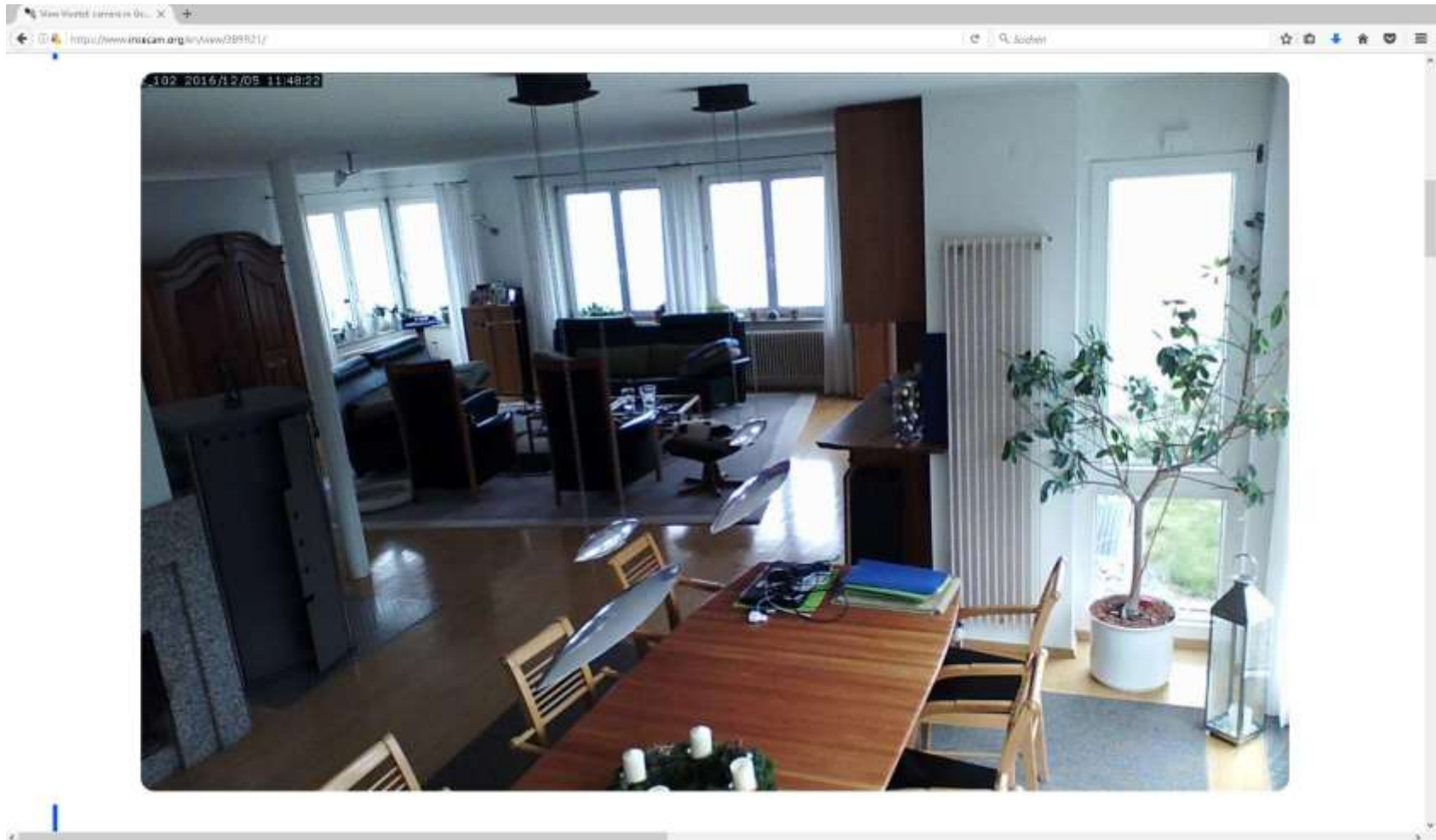
Watch Vivitek camera in Germany, Karlsruhe

Watch Vivitek camera in Germany, Karlsruhe





## BEISPIEL IP-KAMERAS: INSECAM




# BEISPIEL IP-KAMERAS: INSECAM



View World's cameras in 3D... JC


https://www.insecam.org/en/view/389521/

Search



**Make Your Photos Amazing**  
Apply Makeup To Your Portraits! Get New Version 15 now. Go to [portraitprofessional.com](http://portraitprofessional.com)

Country: Germany. You can see other [online cameras](#) in Germany.  
Country code: DE  
Region: Bayern  
City: Nuremberg. [View CCTV online](#) in Nuremberg.  
Latitude: 49.447780  
Longitude: 11.080330  
ZIP: 90455  
Timezone: +01:00  
Manufacturer: Vivotek



NOTE: The coordinates are very approximative and have accuracy in hundreds of miles

# BEISPIEL IP-KAMERAS: SHODAN

The screenshot displays the Shodan website interface. At the top, there's a navigation bar with the Shodan logo, a search bar, and links for 'Explore', 'Enterprise Access', and 'Contact Us'. Below this, a large 'Explore' heading is followed by the tagline 'Discover the Internet Using search queries shared by other users.' The main content area is divided into three columns: 'Featured Categories', 'Top Voted', and 'Recently Shared'. The 'Featured Categories' column lists 'Industrial Control Systems', 'Databases', and 'Video Games'. The 'Top Voted' column shows a list of search results, including 'Webcam' (8,099 votes), 'Cams' (2,968 votes), 'Netcam' (1,704 votes), 'dreambox' (852 votes), and 'default password' (607 votes). The 'Recently Shared' column shows a list of shared search results, including 'ASSP Proxy' and 'NB1600 LTE/4G Router'. A QR code is visible in the bottom right corner of the screenshot.

# BEISPIEL IP-KAMERAS: SHODAN



Shodan search results for "linux vncip:ntech".

**TOP COUNTRIES**

Country	Count
Indonesia	37,486
Mexico	30,282
United States	17,070
Thailand	6,388
Malaysia	5,752

**TOP SERVICES**

Service	Count
HTTP	37,476
Webcam	16,371
HTTP (80)	13,111
HTTP (8080)	12,782
Quota	6,888

**TOP ORGANIZATIONS**

Organization	Count
Netcom	16,386
PT Telkom Indonesia	12,679
De Net	5,340
Vietnam Posts and Telecommunications (VPT)	4,242
TOT	3,587

**TOP OPERATING SYSTEMS**

OS	Count
Linux 2.6.x	1,387
Linux 3.x	128
Linux 5.0.2.6	2

**TOP PRODUCTS**

Product	Count
Avant 4000i network camera	106,145

**Sample Search Results:**

**1. Login**  
 192.168.1.100  
 2017-12-10 10:00:00  
 Server: Linux/2.6.32-042-pae  
 Connection: Close  
 Last-Modified: Mon, 11 Jan 2016 11:38:42 GMT  
 Content-Type: text/html  
 ETag: W/"16273-180652123"  
 Content-Length: 16273

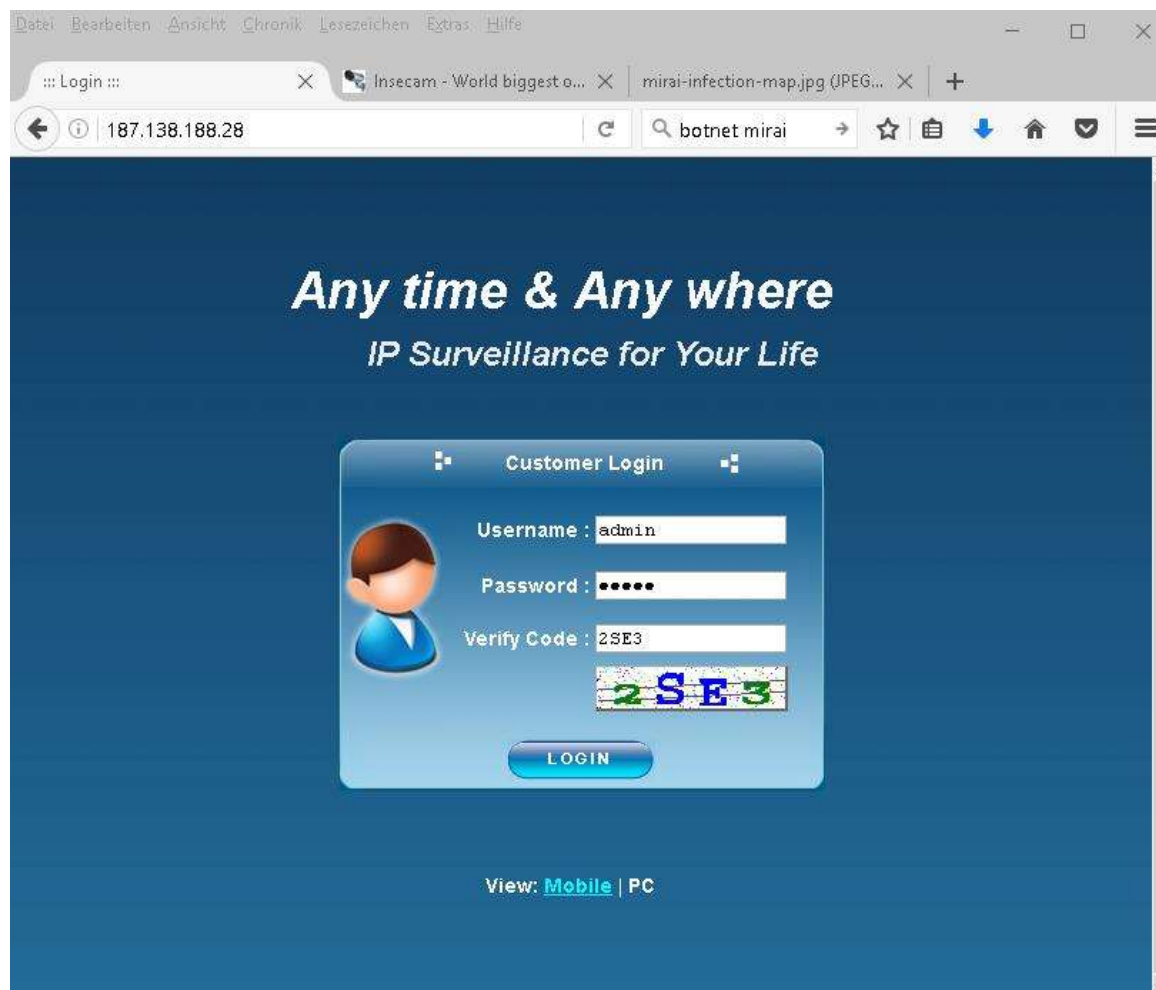
**2. Login**  
 192.168.1.100  
 2017-12-10 10:00:00  
 Server: Linux/2.6.32-042-pae  
 Connection: Close  
 Last-Modified: Thu, 21 Jan 2016 07:18:50 GMT  
 Content-Type: text/html  
 ETag: W/"16273-180652123"  
 Content-Length: 16273

**3. Login**  
 192.168.1.100  
 2017-12-10 10:00:00  
 Server: Linux/2.6.32-042-pae  
 Connection: Close  
 Last-Modified: Fri, 10 Aug 2016 05:57:42 GMT  
 Content-Type: text/html  
 ETag: W/"16273-180652123"  
 Content-Length: 16273

**4. 403 Forbidden**  
 192.168.1.100  
 2017-12-10 10:00:00  
 Server: Linux/2.6.32-042-pae  
 Connection: Close  
 Last-Modified: Thu, 21 Jan 2016 07:18:50 GMT  
 Content-Type: text/html  
 ETag: W/"16273-180652123"  
 Content-Length: 16273

**5. Login**  
 192.168.1.100  
 2017-12-10 10:00:00  
 Server: Linux/2.6.32-042-pae  
 Connection: Close  
 Last-Modified: Fri, 10 Aug 2016 05:57:42 GMT  
 Content-Type: text/html  
 ETag: W/"16273-180652123"  
 Content-Length: 16273

# BEISPIEL IP-KAMERAS: SHODAN



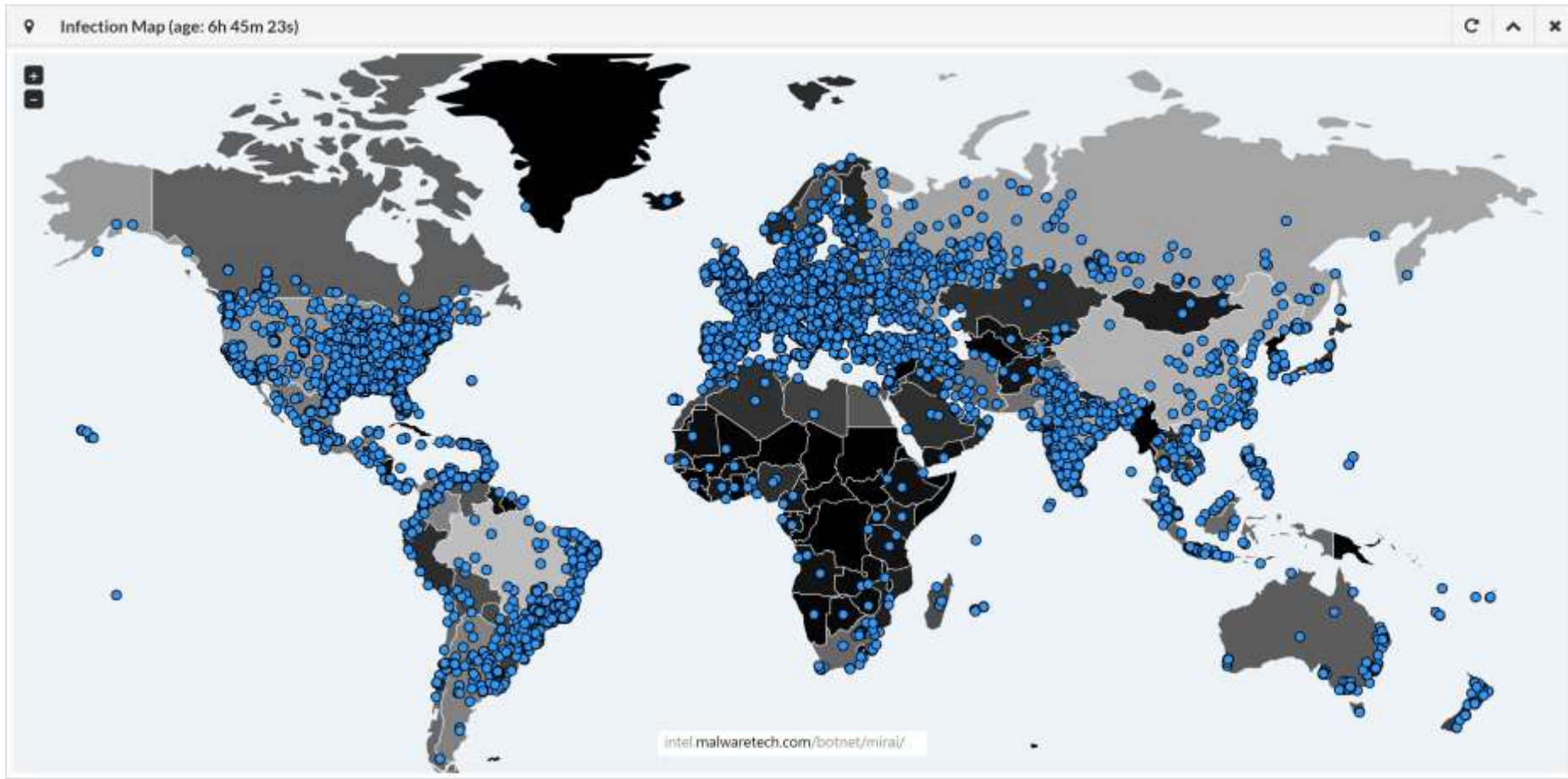


## BEISPIEL IP-KAMERAS: SHODAN





# GAR NICHT SMART: IOT-BOTNETZE WIE MIRAI



## ZERTIFIZIERTE IT-SICHERHEIT?



# ZERTIFIZIERTE SICHERHEIT „MADE IN GERMANY“



# ALLE ERGEBNISSE GRATIS BEI AV-TEST ONLINE

**AV-TEST**  
The Independent IT-Security Institute

Deutsch English Français Español

Initial News **Tests** Award Testverfahren Statistiken Publikationen Presse Kontakt

Anwendungsbereich eingrenzen

MOBILE GERÄTE ANDROID PRIVATANWENDER WINDOWS PRIVATANWENDER MAC OS UNTERNEHMEN WINDOWS CLIENT

Einzelnen Hersteller betrachten

## Die besten Antivirus Programme für Windows Client Unternehmensanwender

Getestete Betriebssysteme in Ihrer Auswahl: [Windows 10](#) | [Windows 8](#) | [Windows 7](#) | [Windows XP](#)

Windows 10 Klicken Sie auf das Logo, um die Testreihe anzuzeigen.

Windows 8/8.1

**Oktober 2016 (neu)**

- Jun 2016
- Oktober 2015
- Jun 2015
- Februar 2015
- Oktober 2014
- April 2014
- Dezember 2013
- Februar 2013

Name	Selbstbewertung	Unabhängigkeit	Benutzerfreundlichkeit
<b>AVG</b> AVG Antivirus Business 2016	★★★★★	★★★★★	★★★★★
<b>Bitdefender</b> Bitdefender Endpoint Security 6.2	★★★★★	★★★★★	★★★★★
<b>F-Secure</b> F-Secure Client Security 12.10	★★★★★	★★★★★	★★★★★
<b>G Data</b> G Data AntiVirus Business 14.0	★★★★★	★★★★★	★★★★★
<b>Intel Security</b> McAfee Endpoint Security 10.1	★★★★★	★★★★★	★★★★★
<b>Kaspersky Lab</b> Kaspersky Lab Endpoint Security 10	★★★★★	★★★★★	★★★★★
<b>Kaspersky Lab</b> Kaspersky Lab Small Office Security 5	★★★★★	★★★★★	★★★★★
<b>Microsoft</b> Microsoft System Center Endpoint Protection 4.9	★★★★★	★★★★★	★★★★★
<b>Segrate</b> Segrate Endpoint Security 17.00	★★★★★	★★★★★	★★★★★
<b>Sophos</b> Sophos Endpoint Security and Control 10.6	★★★★★	★★★★★	★★★★★
<b>Symantec</b> Symantec Endpoint Protection 12.1 & 14.0	★★★★★	★★★★★	★★★★★
<b>Trend Micro</b> Trend Micro Office Scan 11.0	★★★★★	★★★★★	★★★★★

Jun 2016  
Oktober 2015





@avtestorg (English) & @avtestde (German)



Folgen Sie uns auf [facebook.com/avtestorg](https://facebook.com/avtestorg)

Aktuelle Testergebnisse auf <https://www.av-test.org>

Vielen Dank für Ihre Aufmerksamkeit!





# HABEN SIE FRAGEN?

