

Der AV-TEST Sicherheitsreport 2015/2016



ÜBER AV-TEST

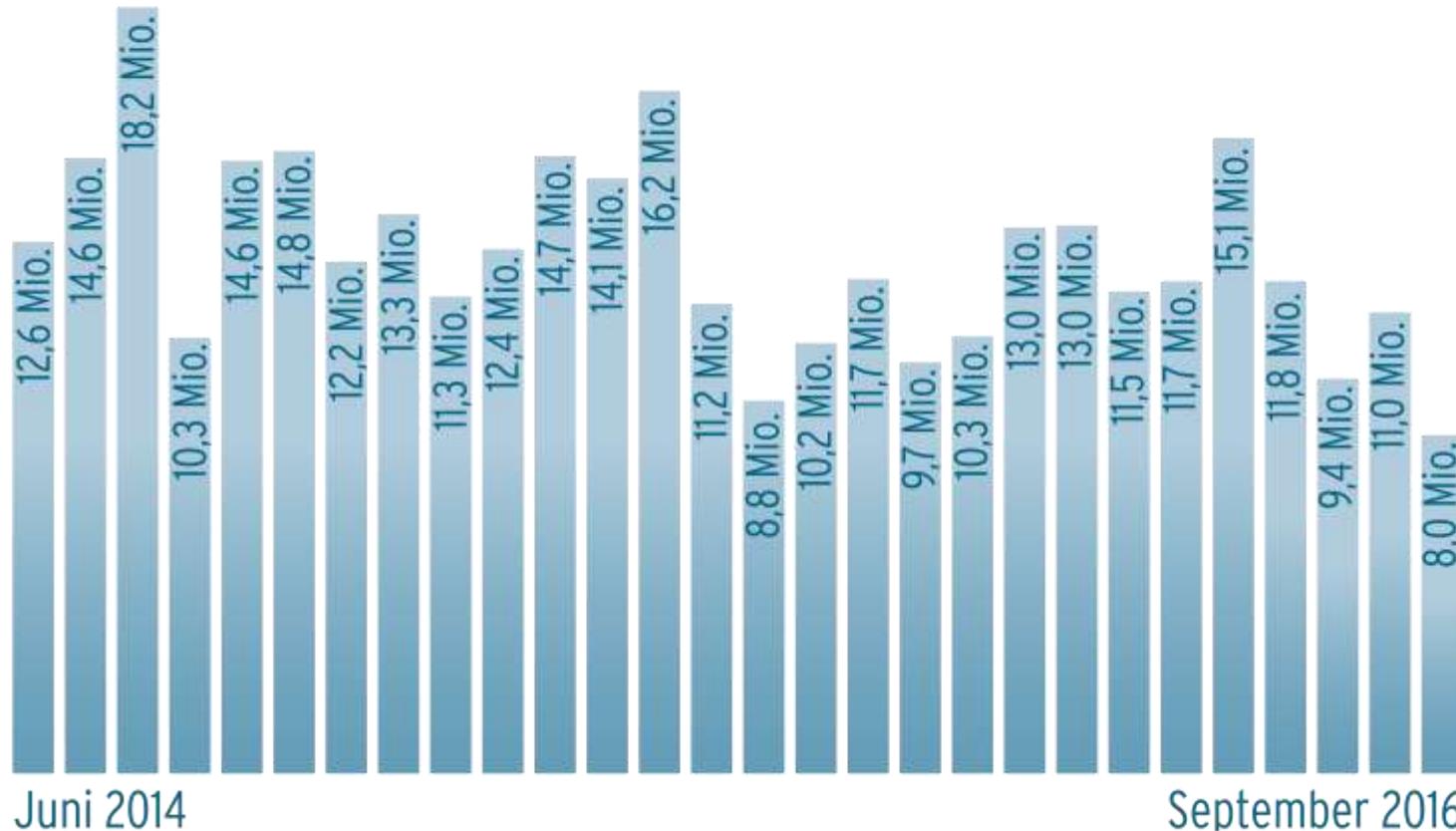
- **Team: über 30 international anerkannte Security-Spezialisten**
- **eine der größten Sammlungen digitaler Schädlinge weltweit**
- **eigene Forschungsabteilung**
- **intensive Zusammenarbeit mit wissenschaftlichen Einrichtungen**
- **selbstentwickelte Analysesysteme**
- **reproduzierbare Testergebnisse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



Gesamtentwicklung von Schadprogrammen in den letzten 10 Jahren



Auftreten neuer Malware insgesamt



Malware-Erkennung nach Betriebssystem

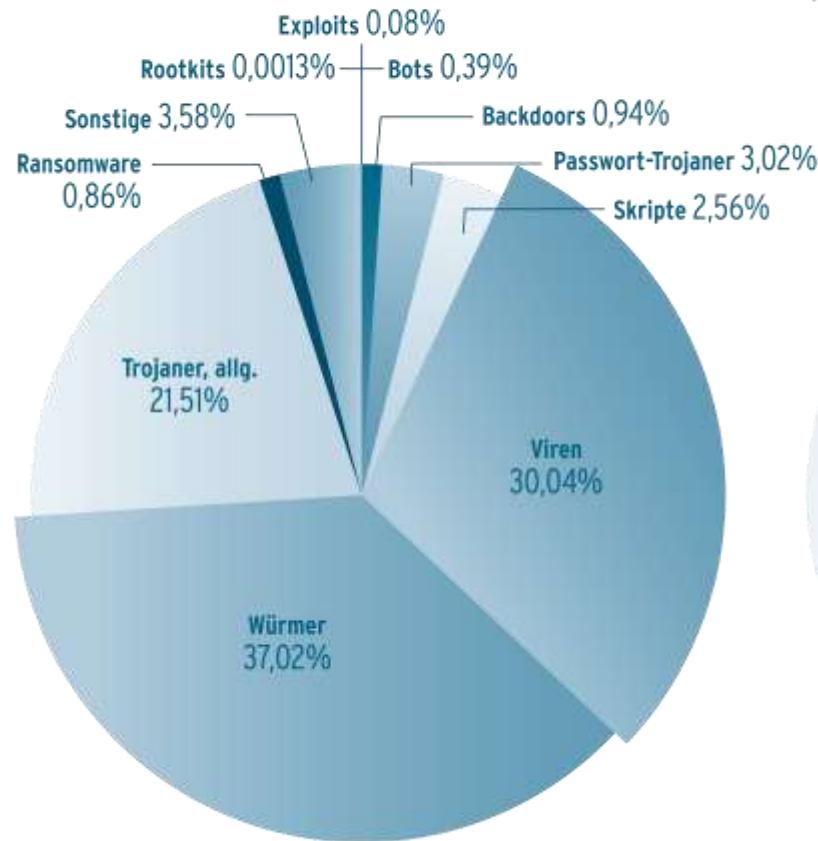


- **Hauptangriffsziel Windows**
- **Android und Skript-Malware holen stark auf**

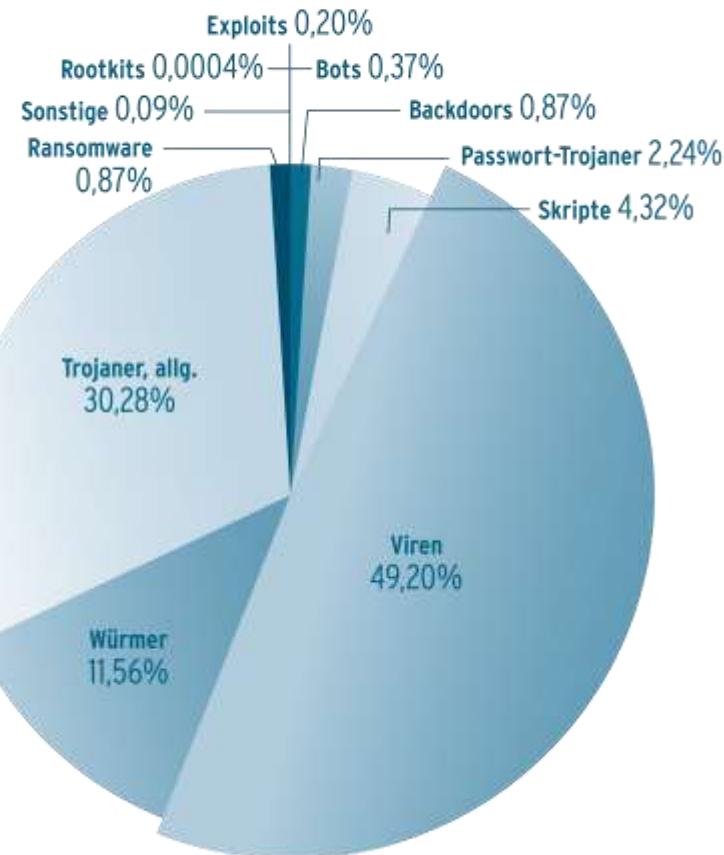
VIREN UNTER WINDOWS AUF DEM VORMARSCH

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> Antwort an: Stefan Friedrich <s.friedrich@t-online.de>

An: [REDACTED]

Sehr geehrte Damen und Herren,

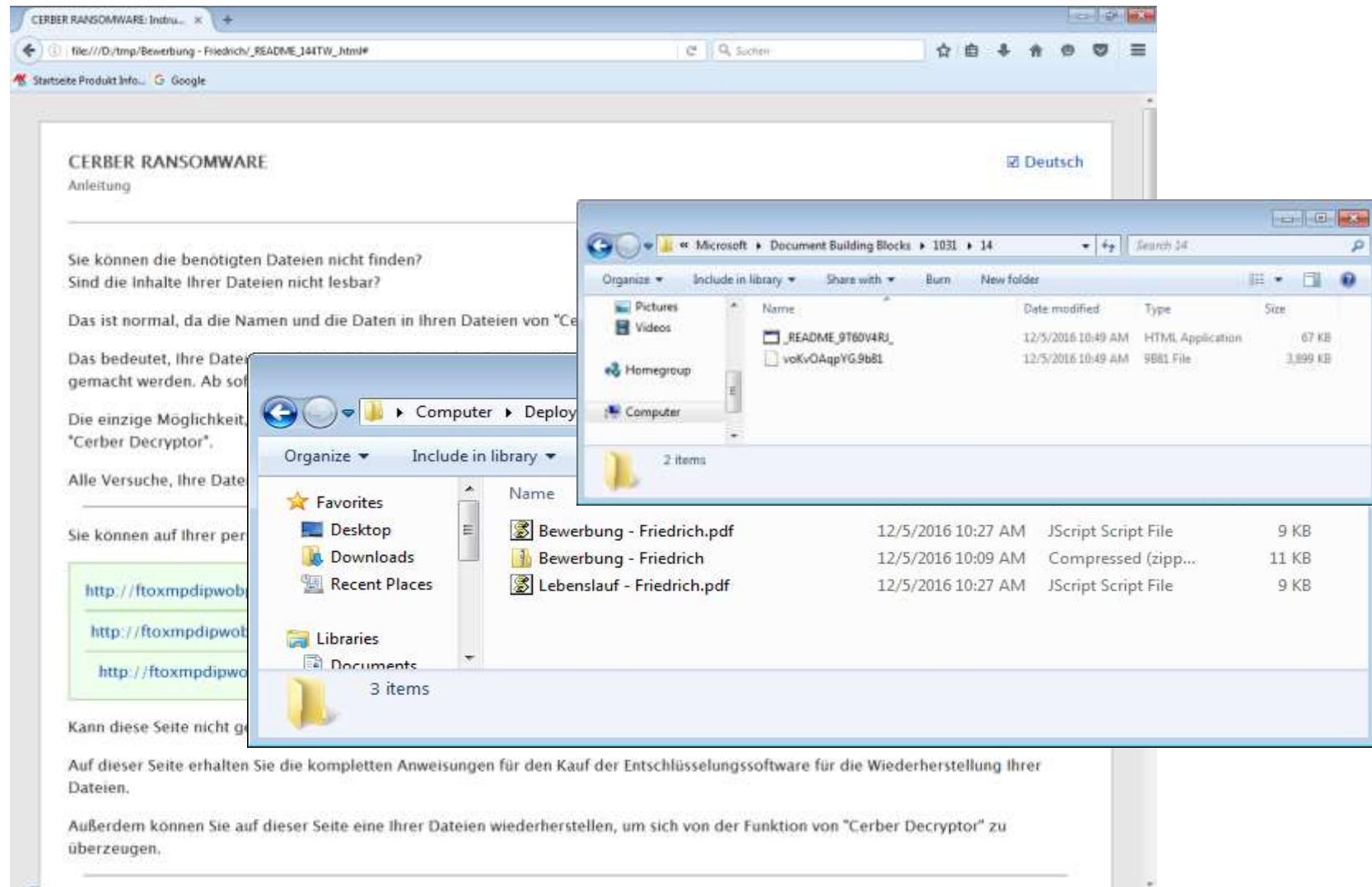
anbei finden Sie meine Bewerbung für Ihre ausgeschriebene Position. Die Stelle entspricht genau meinen Vorstellungen und reizt mich sehr. Da mein Profil und meine bisherigen Erfahrungen gut zu Ihren Anforderungen passen, bin ich davon überzeugt, einen echten Mehrwert leisten zu können. Und das möchte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

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

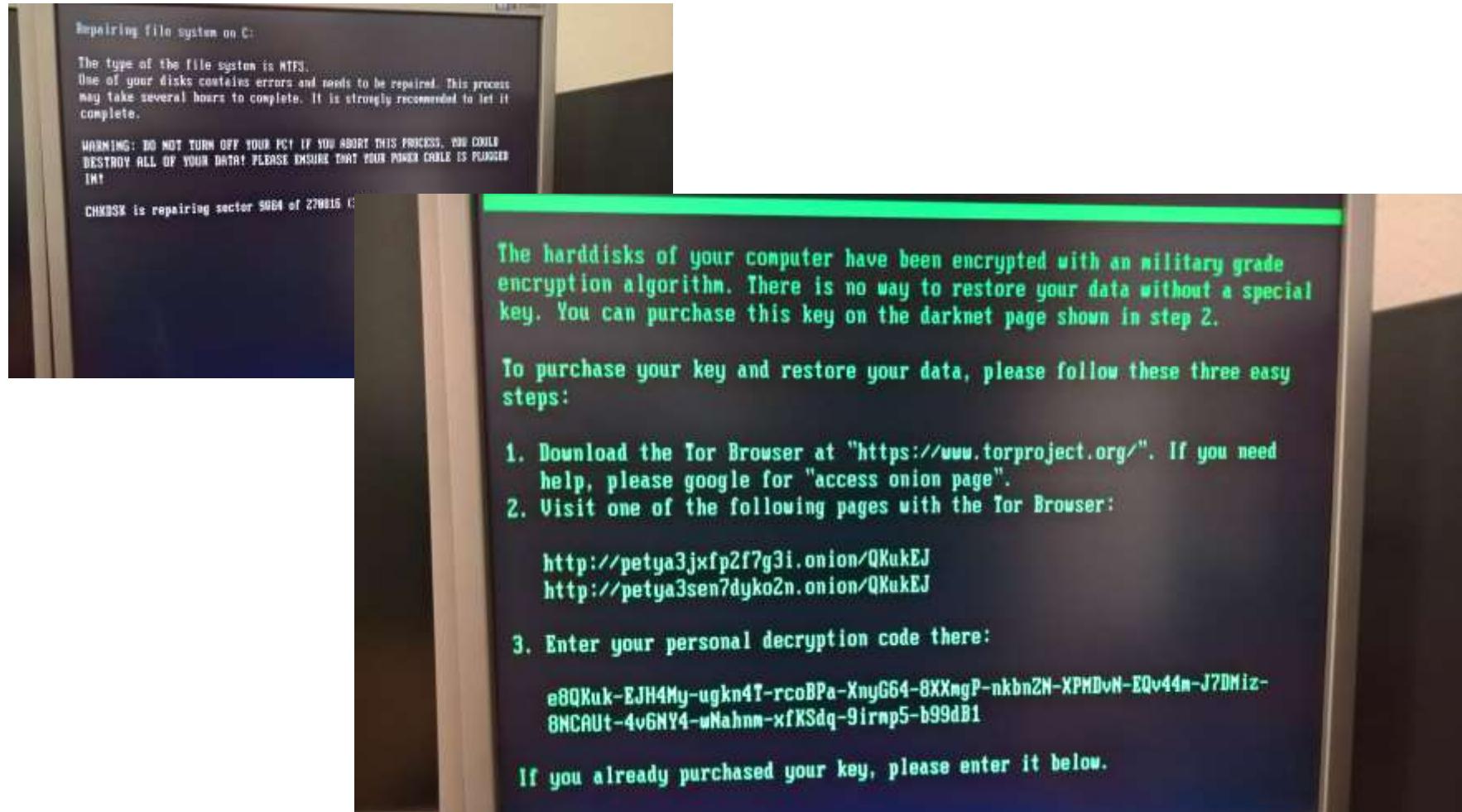
Mit besten Grüßen,

Stefan Friedrich

WINDOWS-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



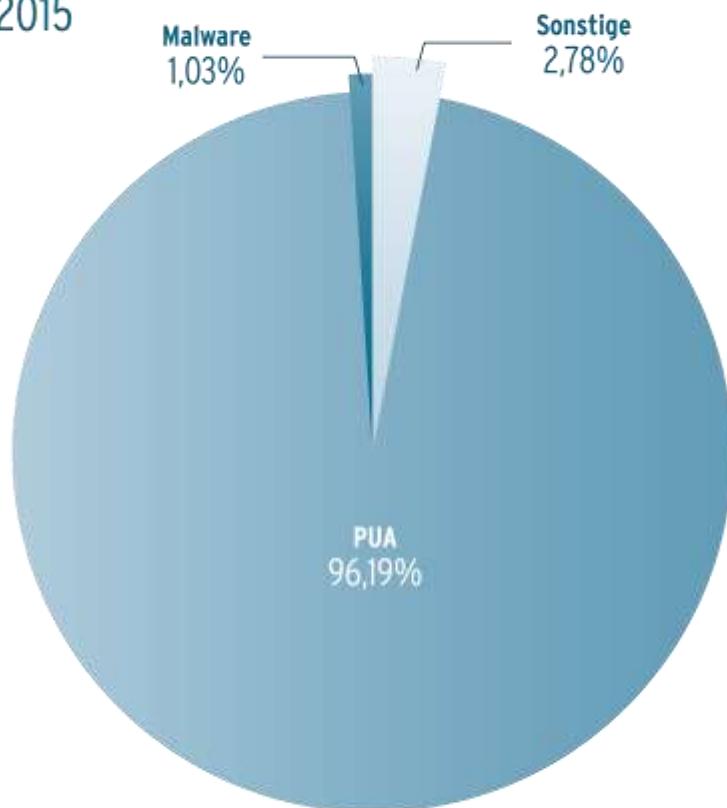
WINDOWS-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



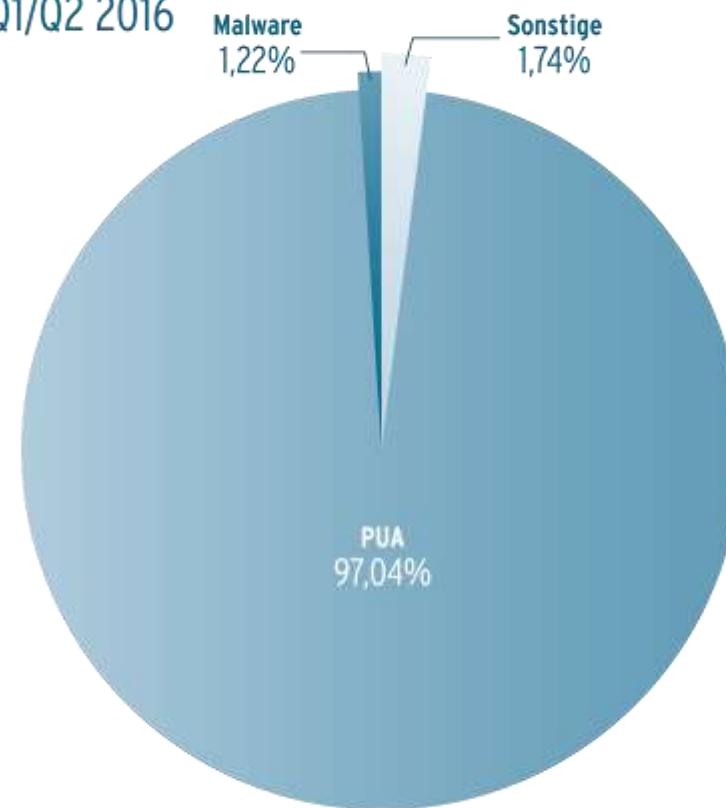
GEFAHRENLAGE FÜR MAC-NUTZER

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

358.881

90.058

Januar 2013

16.514.928

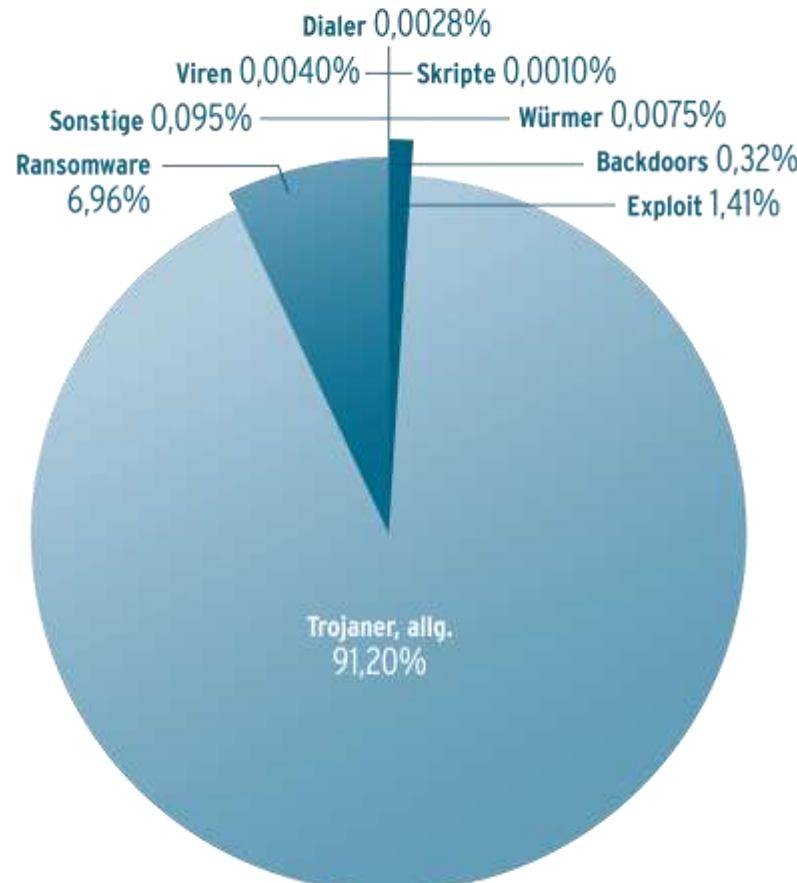
725.738

September 2016

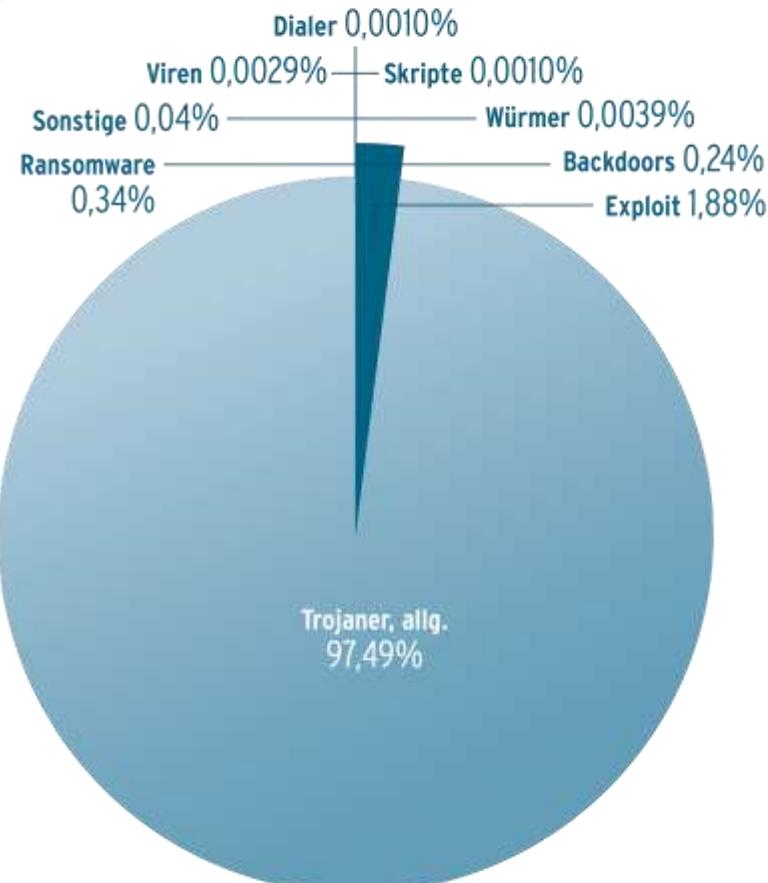
TROJANER-ATTACKEN AUF ANDROID

Malware-Verteilung Android

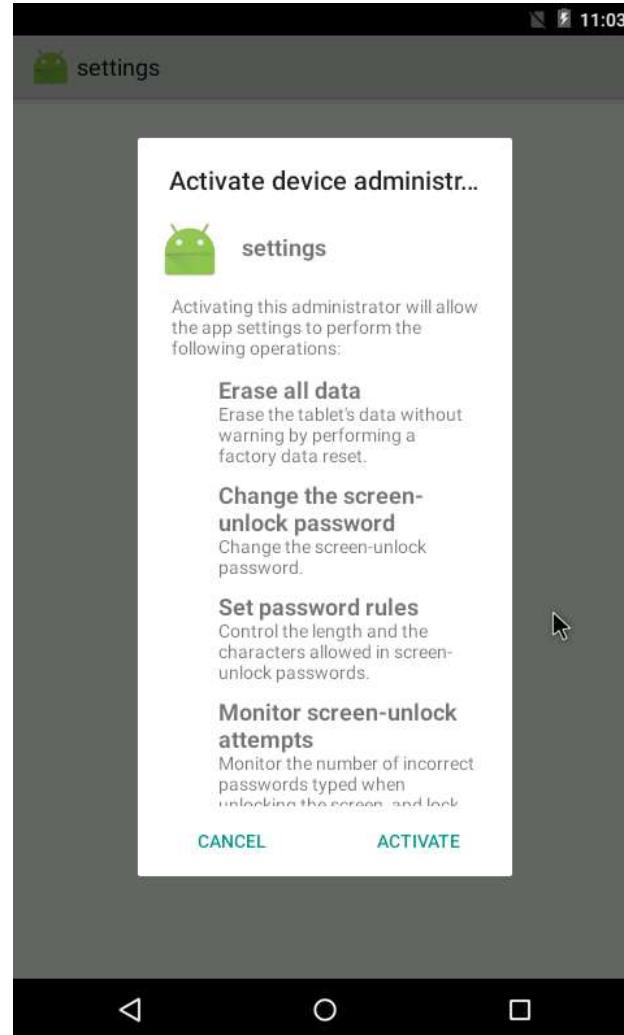
2015



Q1/Q2 2016



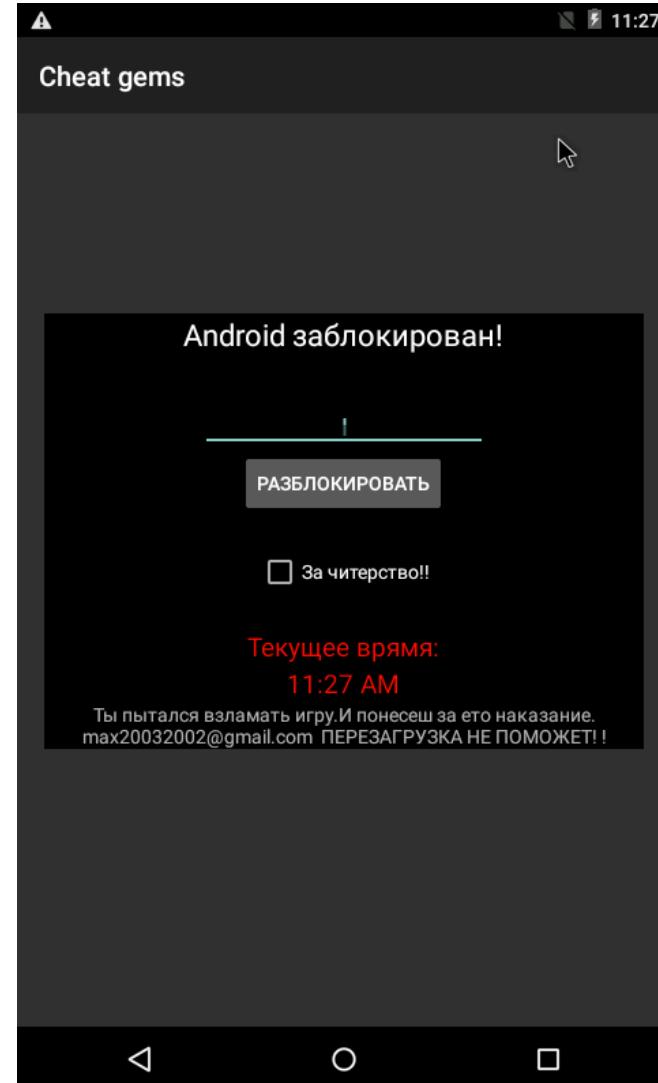
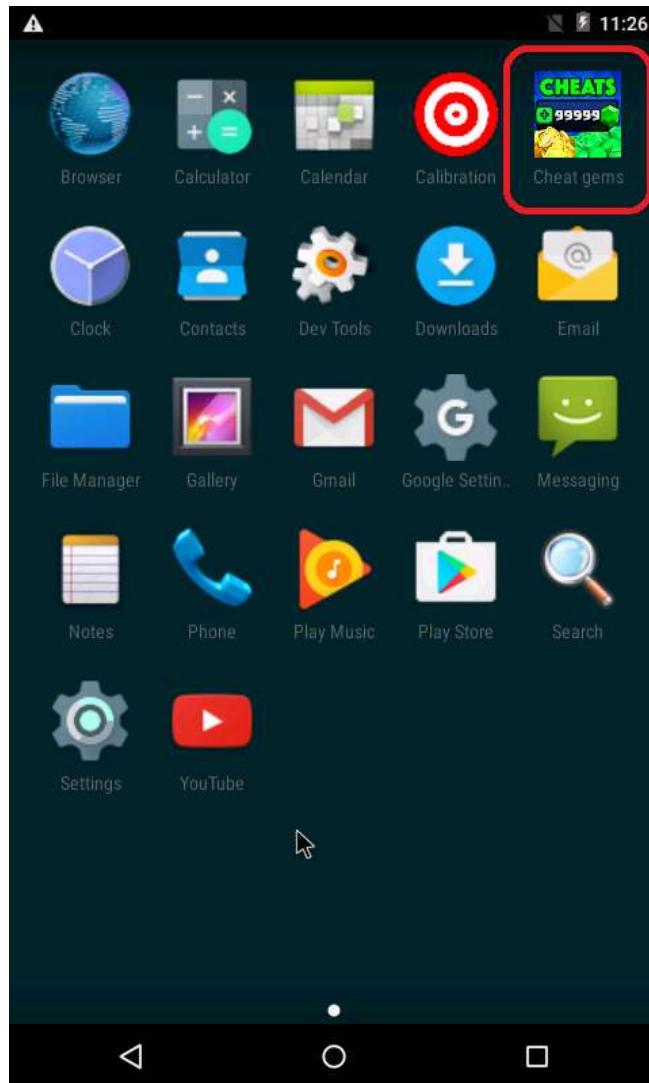
ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER



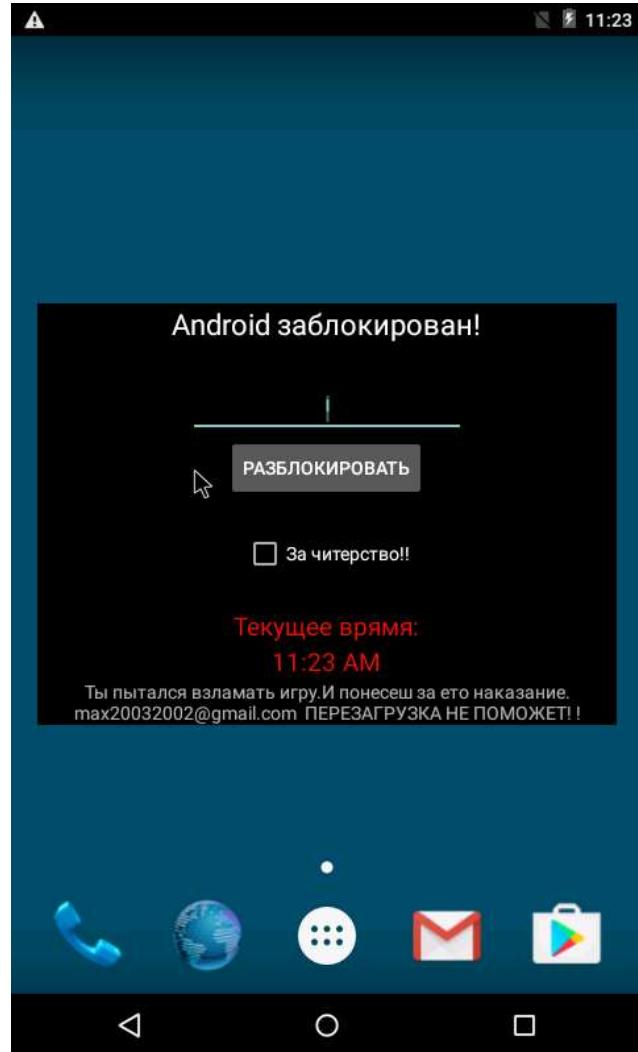
ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER



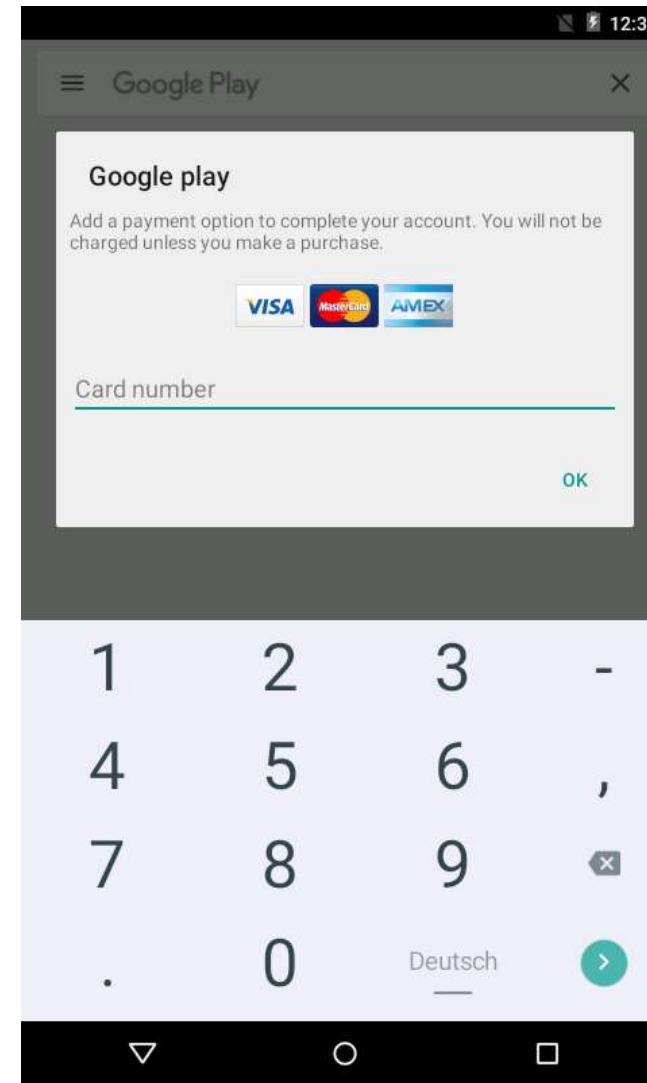
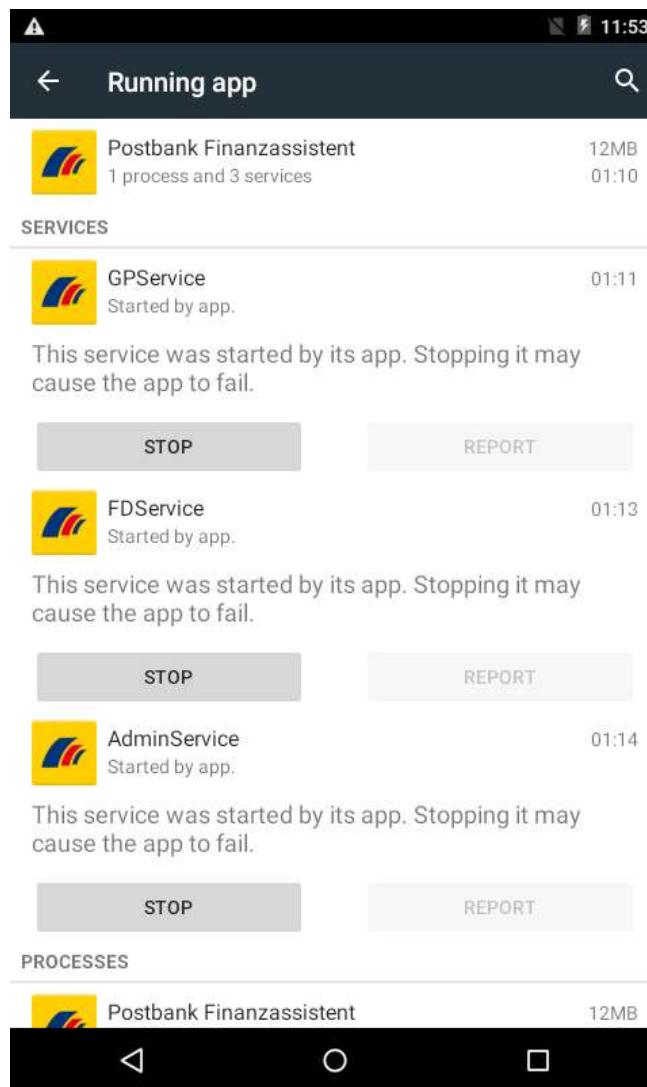
ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER



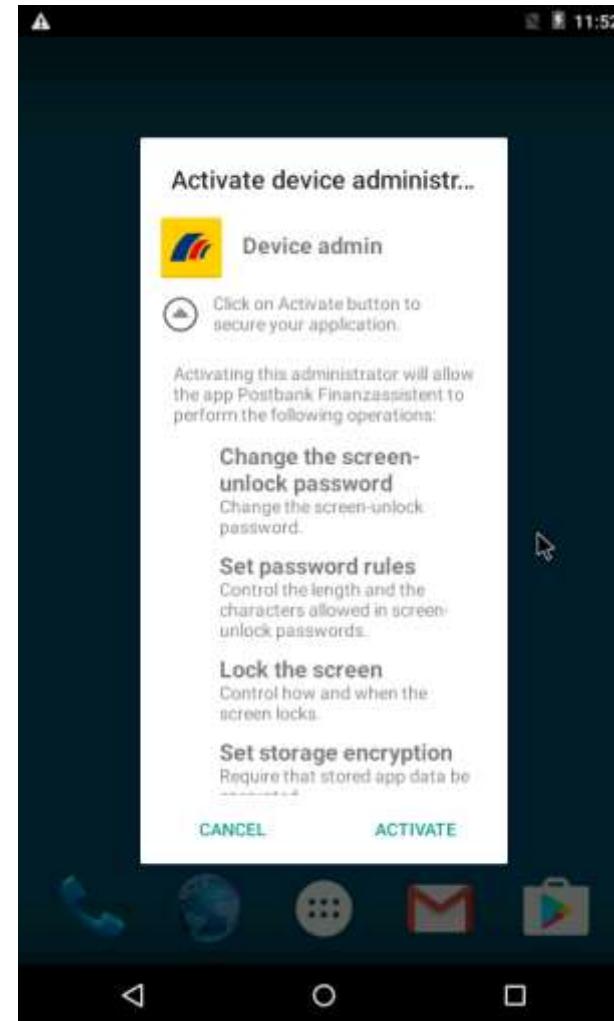
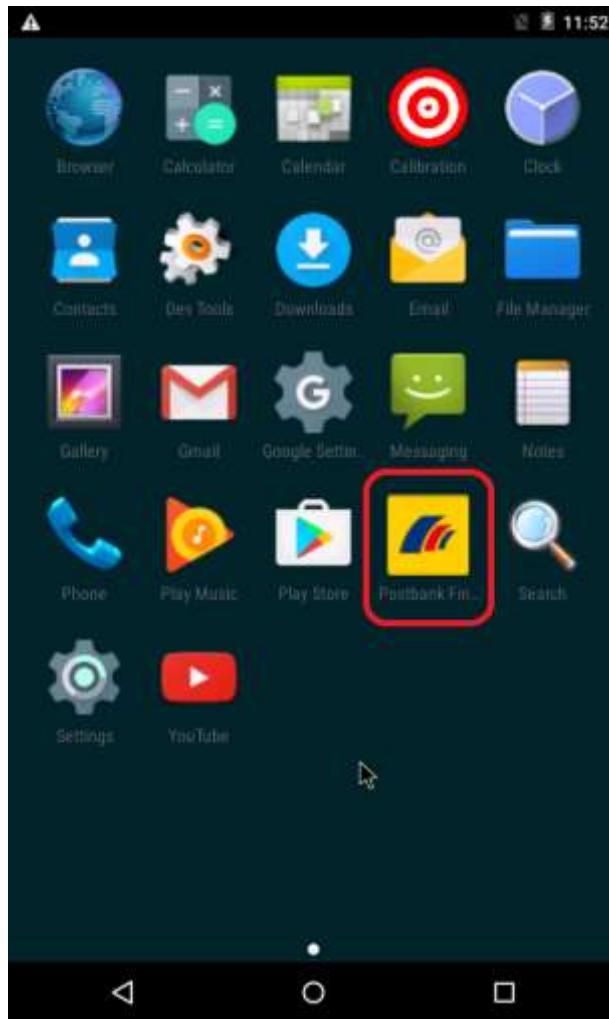
ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER



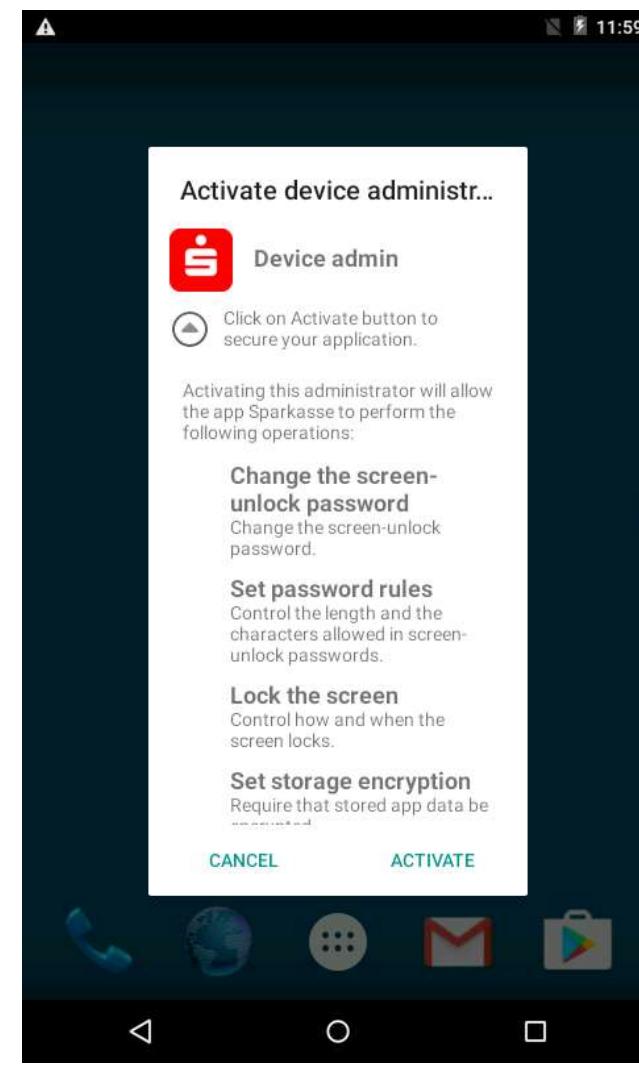
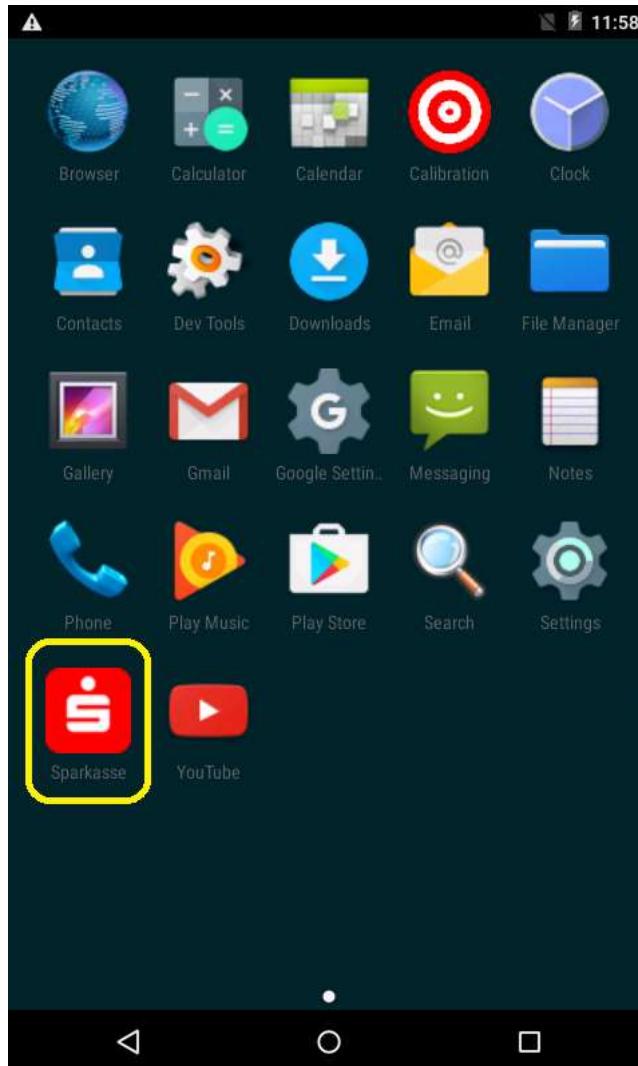
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



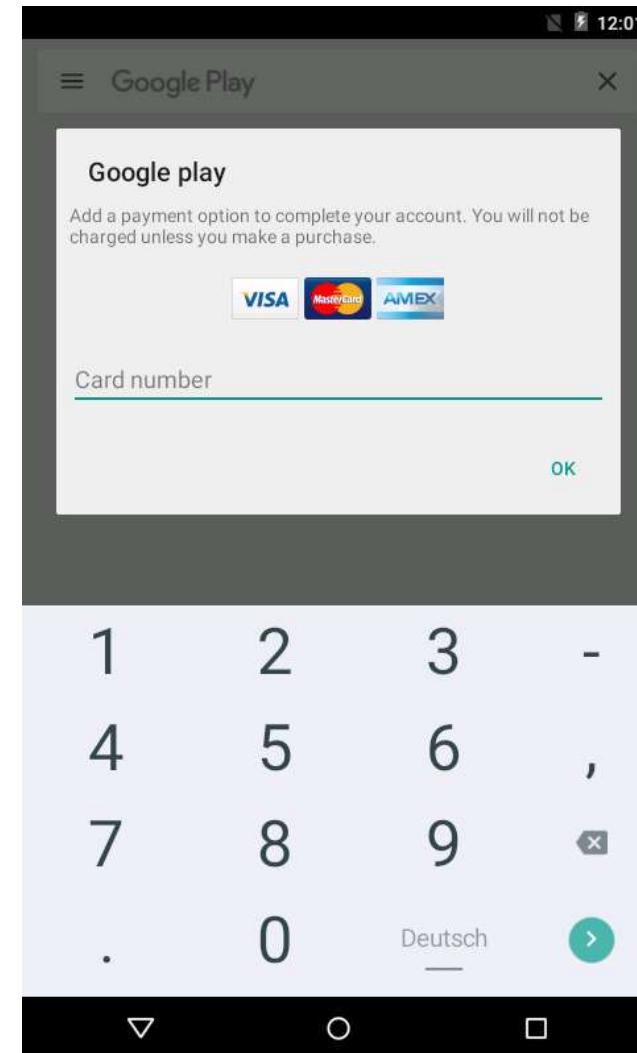
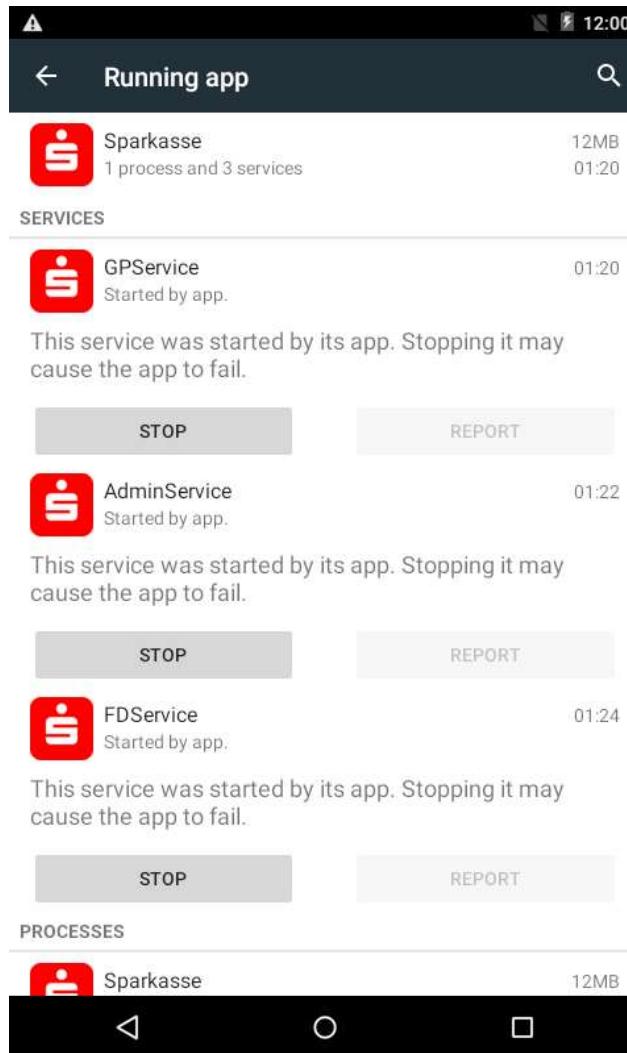
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



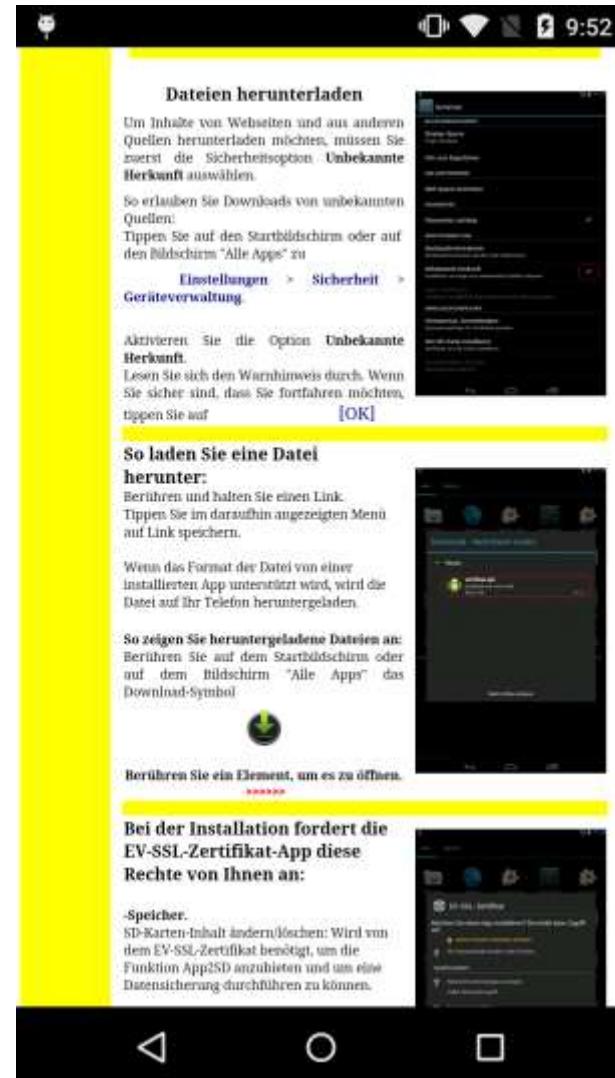
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



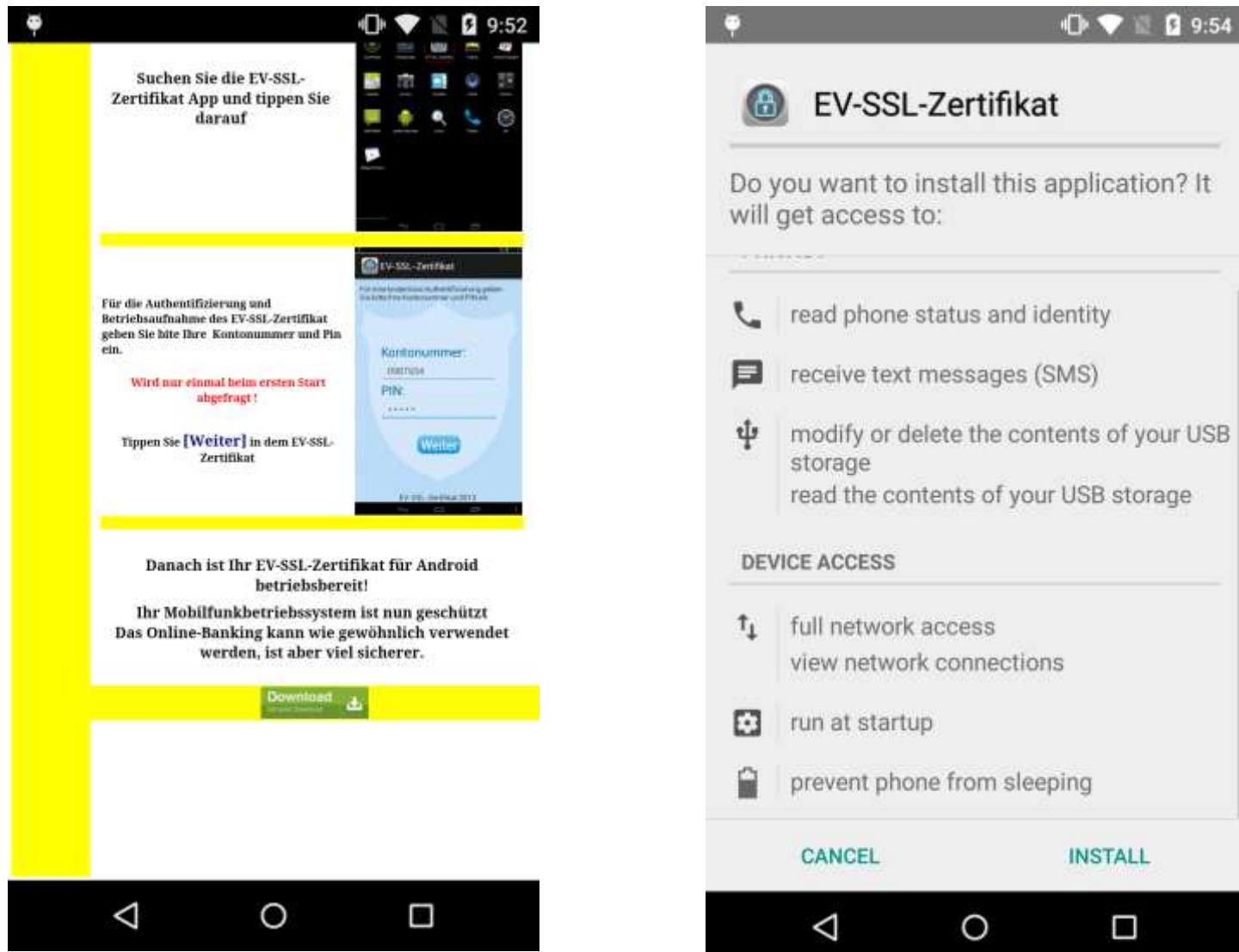
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



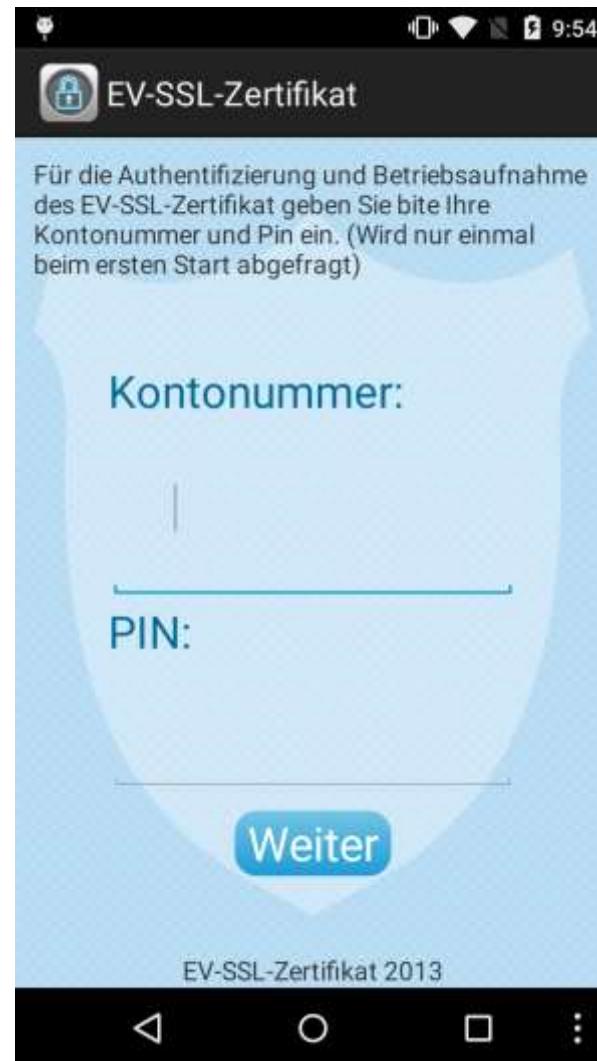
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER

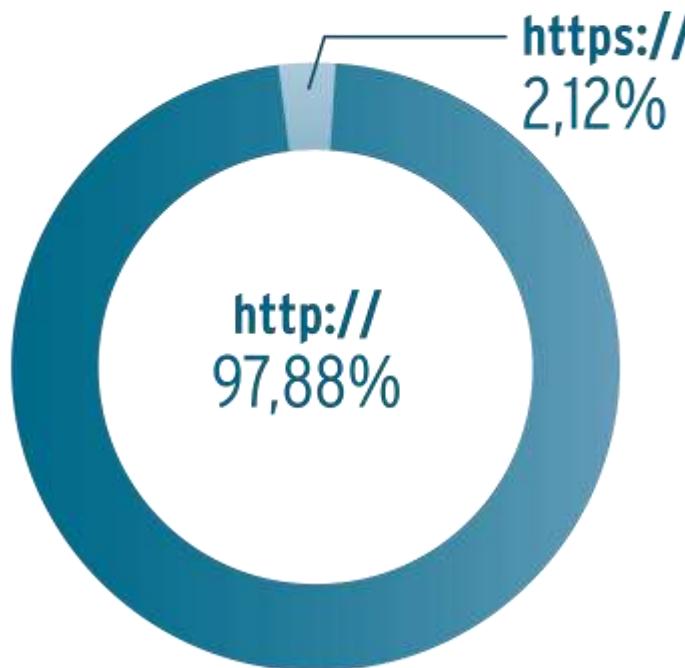


ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER

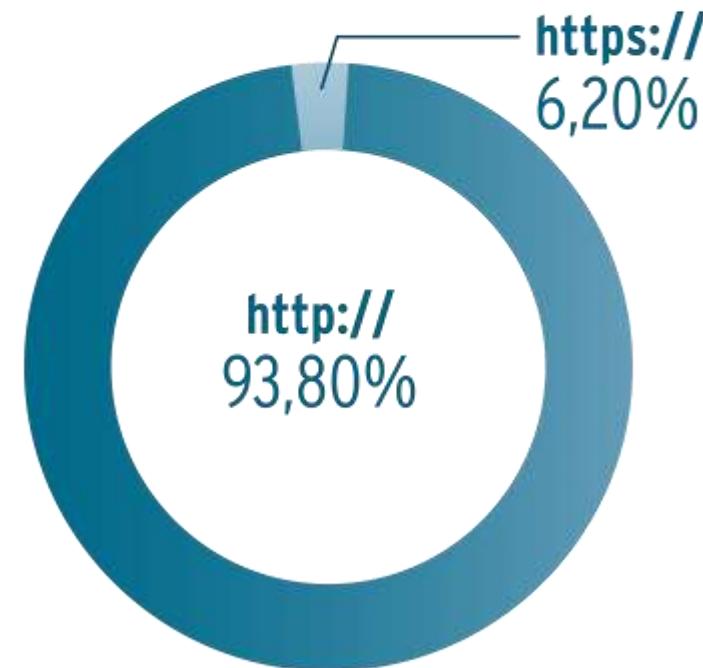


Malware-Verteilung über verschlüsselte und unverschlüsselte Internetseiten

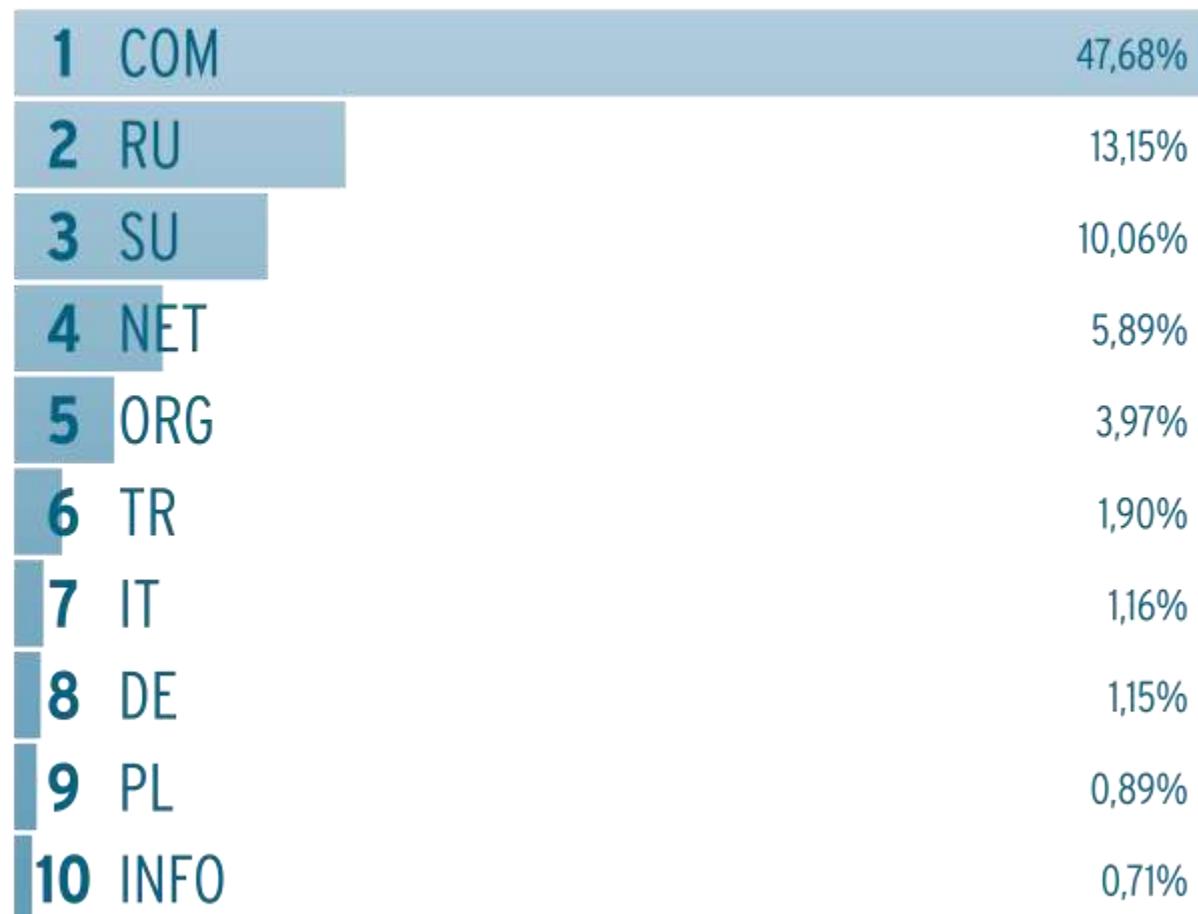
2015



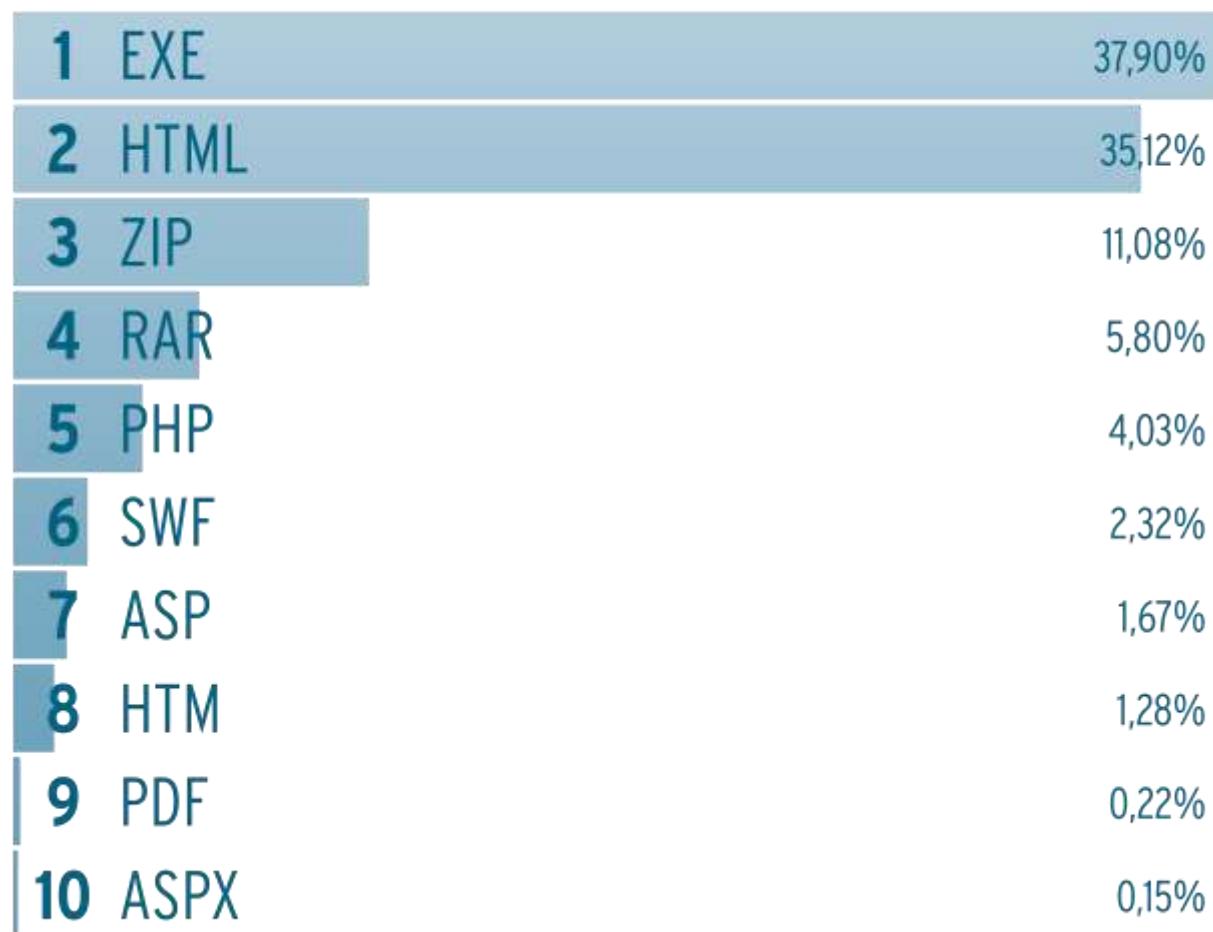
Q1/Q2 2016



TOP 10 Malware-Domains 2015



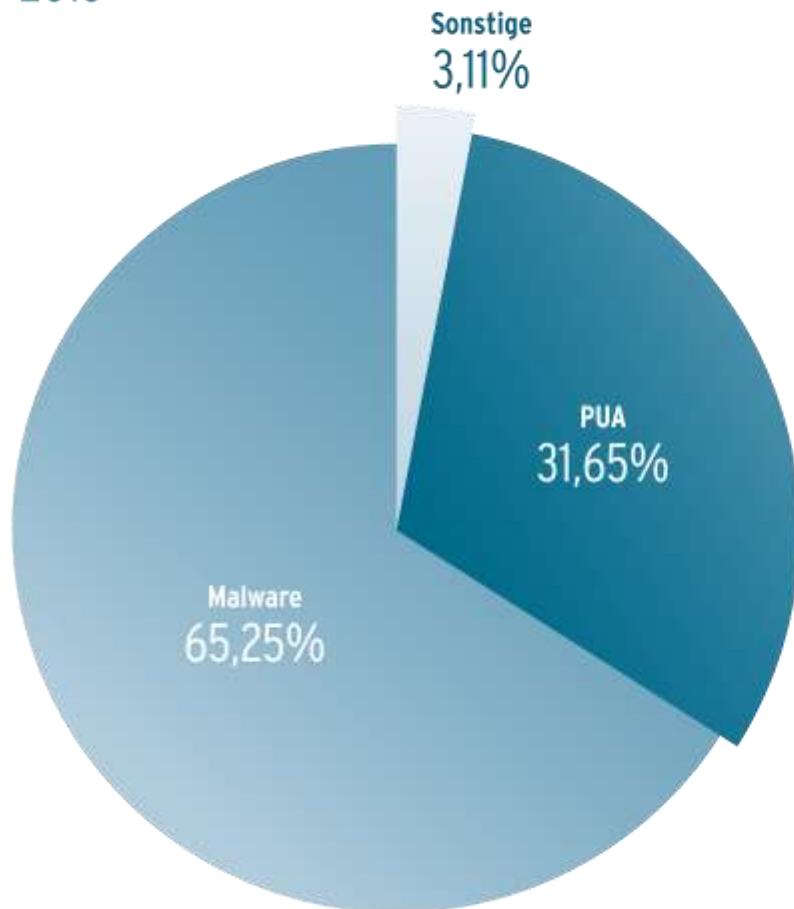
TOP 10 File Extensions Malware 2015



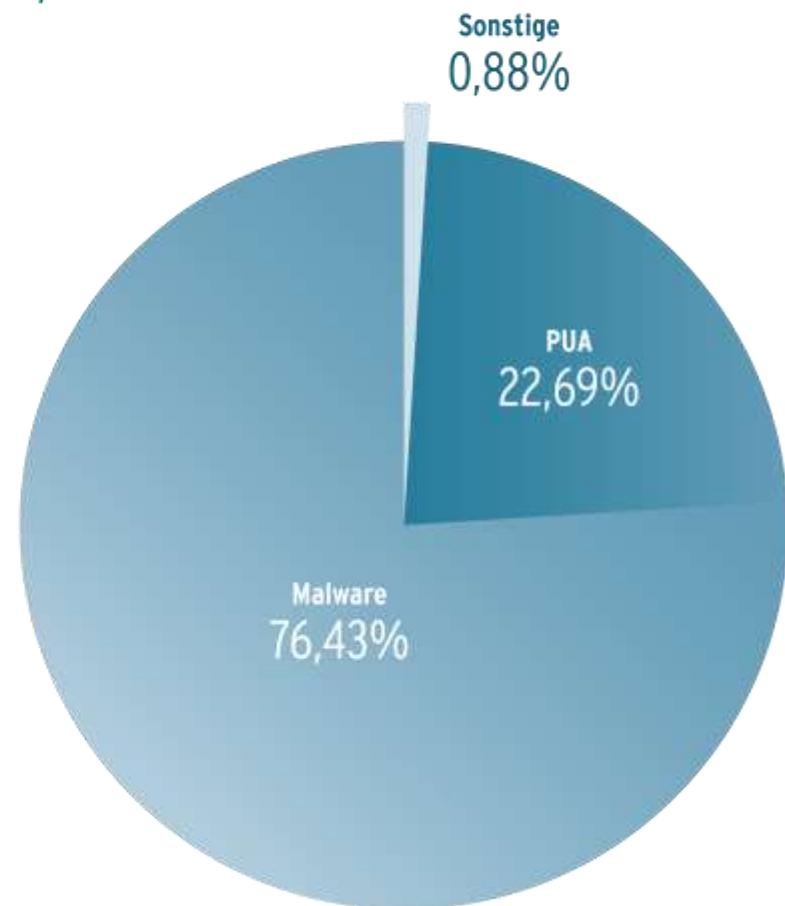
PUA – DIE WACHSENDE GEFAHR

PUA-Erkennung gesamt

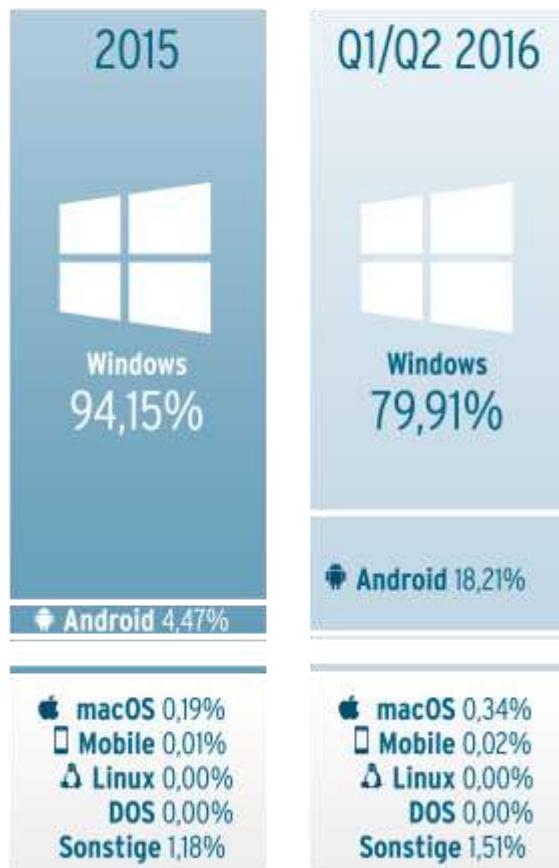
2015



Q1/Q2 2016



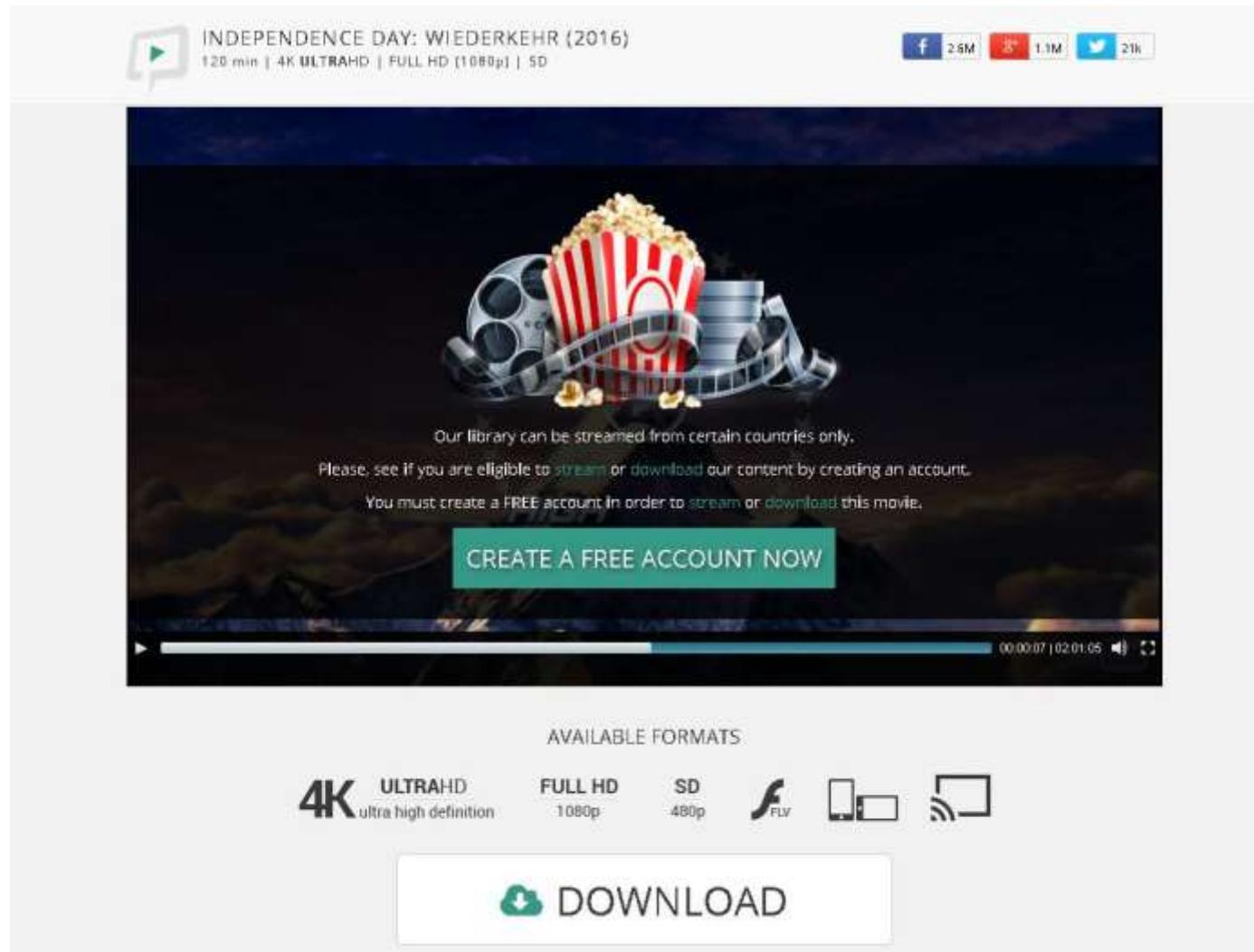
PUA-Erkennung nach Betriebssystem



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

The screenshot shows the MyKino.to website interface. At the top, there is a search bar with the placeholder "Geben Sie Ihr Suchbegriff ein...". Below the search bar, the MyKino.to logo is displayed with the tagline "Filme und Serien kostenlos!". To the right of the logo, there is a message: "Wusstest du schon das MyKino.to auch am iPad verfügbar ist? Einfach www.mykino.to aufrufen, lesezeichen speichern und streams genießen." Below this message, there is a "Genres" section with two columns: "Filme" and "Serien". The "Filme" column includes: ABENTEUER, BIOGRAPHIE, FAMILIE, HORROR, KRIMI, SCI-FI, TRICKFILM, and KRIEG. The "Serien" column includes: ACTION, DRAMA, FANTASY, KOMÖDIE, ROMANTIK, THRILLER, WESTERN, and SPORT. The main content area features the movie "Independence Day: Wiederkehr". The movie poster shows a large alien mothership hovering over Earth. The plot summary is as follows: "20 Jahre ist es her, dass Aliens die Erde attackierten und die Hälfte der Bevölkerung auslöschten. Vor allem der mutige Minion des Pilots Steven Hiller und des Satellitentechnikers David Levinson verhinderten, dass die außerirdischen BSG besiegt werden – tragischerweise kam Hiller dann 2000 ums Leben, als er einen Alien-Hybrid-Fighter testete. Und 2016 wird er umso mehr vermisst, als sich die Warnings des Ex-Präsidenten Whitmore bewahrheitet und die außerirdischen einen neuen, noch verhängnisvollen Angriff starten! Die Menschheit, die in bis dato nie gekannter Eingänglichkeit mit Alien-Technologie ausgerüstetes Verteidigungssystem schützt, steht vor ihrer größten Herausforderung. Die Hoffnungen richten auf den jungen Kampfpiloten Jake und Dylan, den Sohn des verstorbenen Steven Hiller...". Below the plot summary, there are two buttons: "Download" and "Jetzt Anschauen". Below these buttons, there is a section for "Anbieter Auswahl für: Independence Day: Wiederkehr". It lists several streaming platforms: StreamCloud, Nowvideo.ch, Shared.sx, Flashtv, HD-Stream, Mirror: #1, Mirror: #2, Mirror: #3, Mirror: #4, Mirror: #5, Mirror: #6, Mirror: #7, Mirror: #8, Mirror: #9, and Mirror: #10. Each platform has a "PLAY NOW" button. Below this section, there are sharing options: Share, Senden, Tweet, Google+, Pinterest, and Email. At the bottom of the main content area, there is a section titled "Empfohlene Einträge für 'Independence Day: Wiederkehr'" showing thumbnail images of other movie posters.

PUA – DIE WACHSENDE GEFAHR



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

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](#)

00:00:07 | 02:01:05

AVAILABLE FORMATS

4K ULTRAHD
ultra high definition

FULL HD
1080p

SD
480p

 FLV



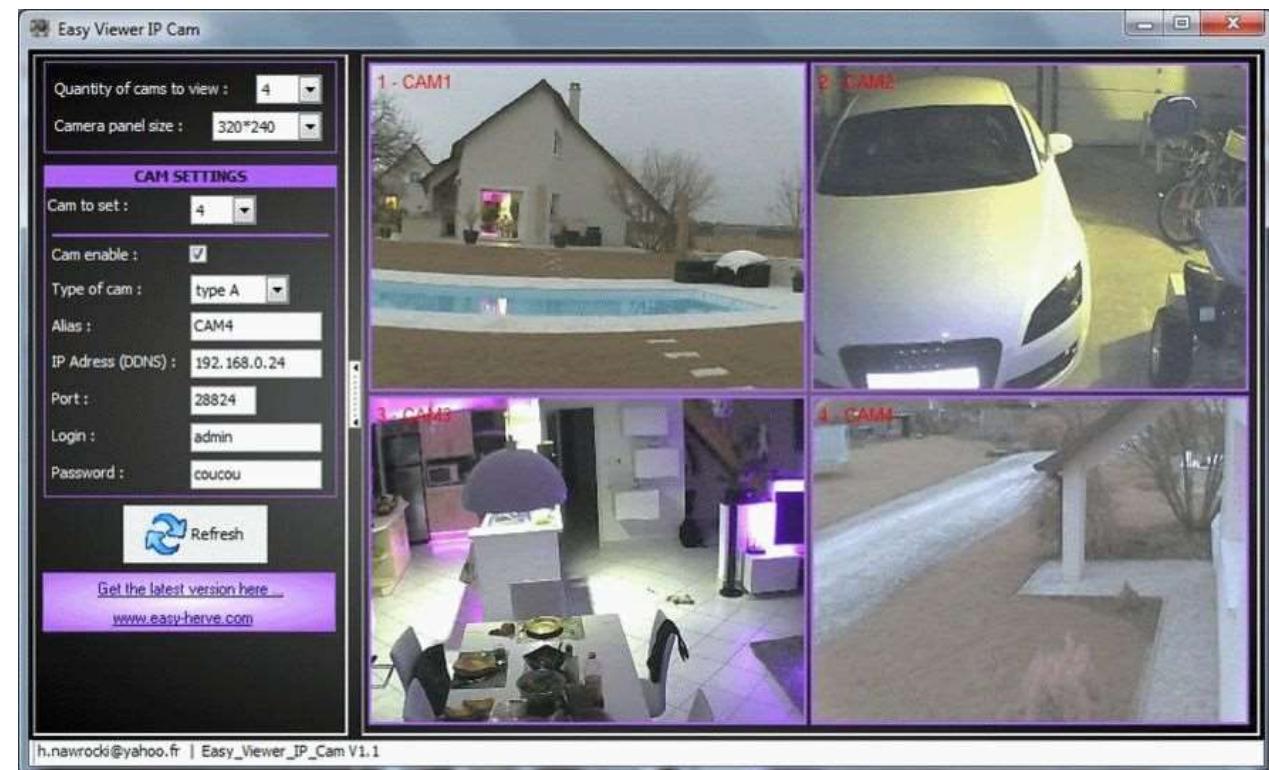
 DOWNLOAD

INTERNET DER DINGE: ALLES SMART, ODER NICHT?



www.thefuturesagency.com, update: January 20, 2015

BEISPIEL IP-KAMERAS: SORGEN FÜR SICHERHEIT



BEISPIEL IP-KAMERAS: INSECAM

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

IP cameras: Germany

IT Wartung für EMC Post Warranty - End of Life Wartung Alters CreditRisk

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

Watch Vivotek camera in Germany Nürnberg

Watch Vivotek camera in Germany Ruteshörd

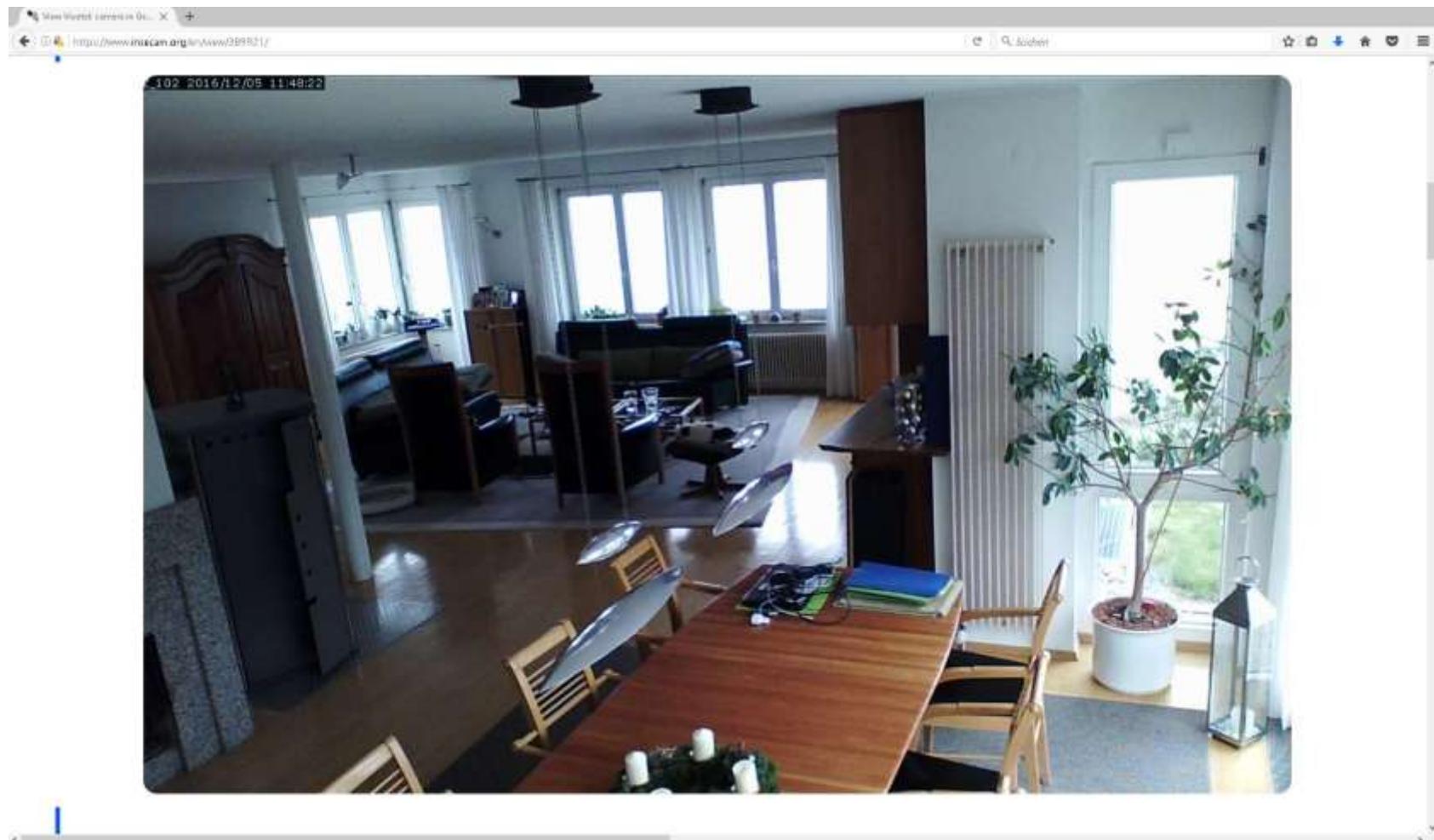
Watch Vivotek camera in Germany Kassel

Watch Vivotek camera in Germany Karlsruhe

Watch Vivotek camera in Germany Kärrtorp

QR code

BEISPIEL IP-KAMERAS: INSECAM



BEISPIEL IP-KAMERAS: INSECAM



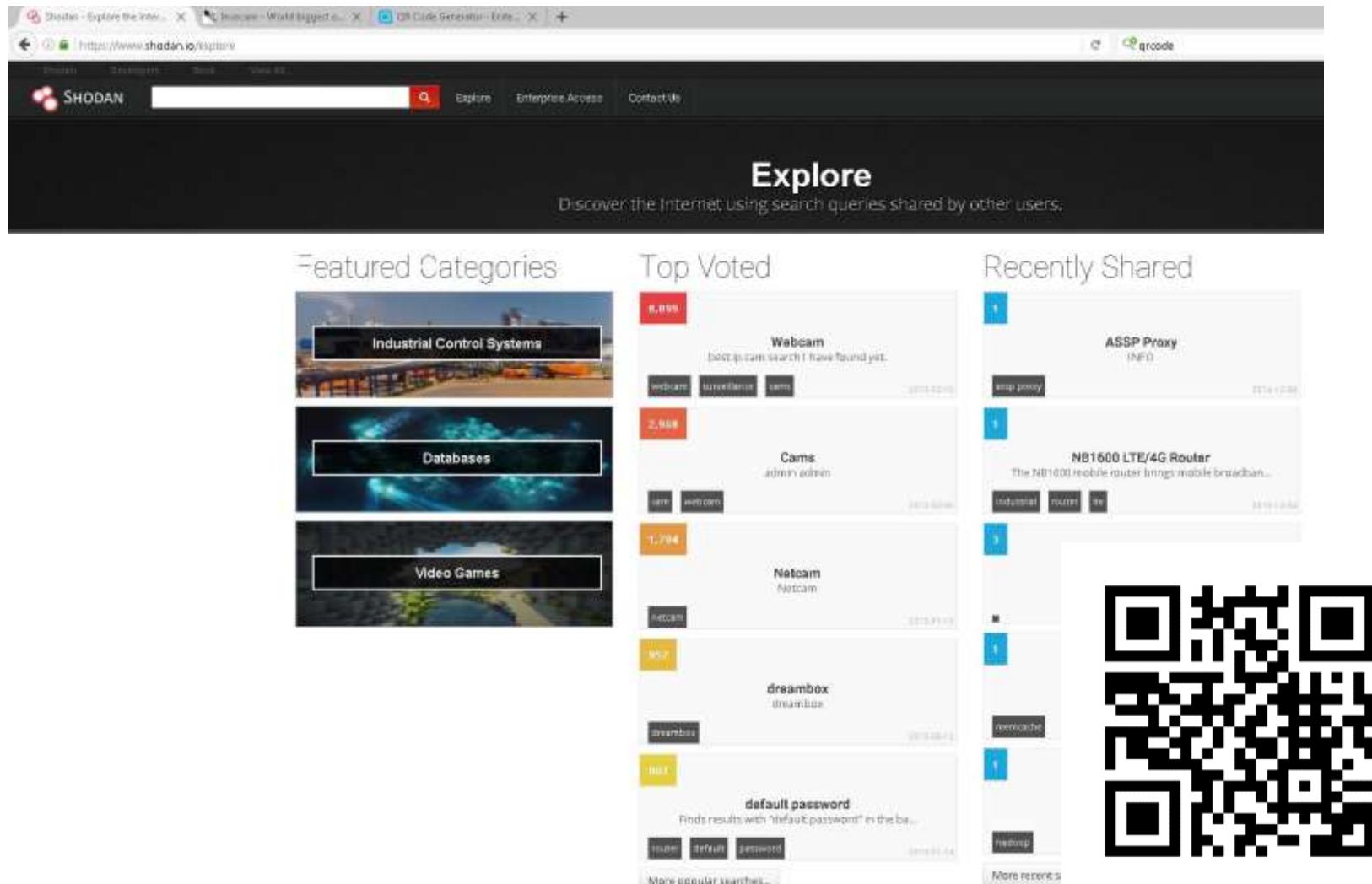
Make Your Photos Amazing
Apply Makeup To Your Portraits! Get New Version 15 now. Go to portraitprofessional.com

Country: Germany. You can see other [online cameras](#) in Germany.
Country code: DE
Region: Bayern
City: Nürnberg. [View CCTV online](#) in Nürnberg.
Latitude: 49.447750
Longitude: 11.088330
ZIP: 90455
Timezone: +01:00
Manufacturer: Vivtek



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

BEISPIEL IP-KAMERAS: SHODAN



The screenshot shows the Shodan Explore page. The main header reads "Explore" with the sub-instruction "Discover the Internet using search queries shared by other users." Below this, there are three main sections: "Featured Categories" (Industrial Control Systems, Databases, Video Games), "Top Voted" (Webcam, Cams, Netcam, dreambox, default password), and "Recently Shared" (ASSP Proxy, NB1600 LTE/4G Router, memcached, haproxy). A QR code is visible on the right side of the page.

Explore
Discover the Internet using search queries shared by other users.

Featured Categories

- Industrial Control Systems
- Databases
- Video Games

Top Voted

- Webcam
- Cams
- Netcam
- dreambox
- default password

Recently Shared

- ASSP Proxy
- NB1600 LTE/4G Router
- memcached
- haproxy

QR Code

BEISPIEL IP-KAMERAS: SHODAN



Intelligent Watch - Dash... X Home - World Map... X QR Code Generator - Dash... X

https://www.shodan.io/search?query=ipcamera+camera+ip+http

SHODAN

Search... Region Enterprise Access Contact Us

Edit Map

TOP COUNTRIES

Country	Count
Indonesia	17,484
Malaysia	10,382
United States	10,038
Thailand	9,388
Malaysia	6,772

TOP SERVICES

Service	Count
HTTP	21,478
Network	14,371
HTTP/2.0	13,115
HTTP (SSL)	12,792
None	6,089

TOP DESTINATIONS

Region	Count
Indonesia	34,084
PT Natura Indonesia	12,619
TM Net	6,249
Verizon - Posts and Telecommunications (VPT)	4,822
PTT	3,397

TOP OPERATING SYSTEMS

OS	Count
Linux	1,287
Ubuntu	128
Ubuntu 6.0.6	2

TOP PRODUCTS

Product	Count
Ascentek AHD/TVI network cameras	106,145

403 Forbidden

Last-Modified: Sun, 01 Dec 2013 08:03:00 GMT

Content-Type: text/html; charset=ISO-8859-1

Content-Length: 105

HTTP/1.0 403 Forbidden

Date: Sun, 01 Dec 2013 08:48:23 GMT

Server: Linux/2.6.38#47.9.1#Debian/7.0

Connection: close

Last-Modified: Mon, 11 Jan 2010 17:39:42 GMT

Content-Type: text/html

etag: 81-16271-1499611523

Content-Length: 14173

HTTP/1.1 200 OK

Date: Sun, 01 Dec 2013 08:03:00 GMT

Server: Linux/2.6.38#47.9.1#Debian/7.0

Connection: close

Last-Modified: Thu, 21 Dec 2012 07:18:38 GMT

Content-Type: text/html

etag: 204-16273-1395521235

Content-Length: 10373

HTTP/1.1 200 OK

Date: Sun, 01 Dec 2013 08:48:23 GMT

Server: Linux/2.6.38#47.9.1#Debian/7.0

Connection: close

Last-Modified: Fri, 10 Aug 2012 05:31:42 GMT

Content-Type: text/html

etag: 219-16273-1148882237

Content-Length: 1025

HTTP/1.1 200 OK

Date: Sun, 01 Dec 2013 08:48:23 GMT

Server: Linux/2.6.38#47.9.1#Debian/7.0

Connection: close

Last-Modified: Mon, 11 Jan 2010 17:39:42 GMT

Content-Type: text/html; charset=ISO-8859-1

Content-Length: 105

HTTP/1.1 200 OK

Date: Sun, 01 Dec 2013 08:48:23 GMT

Server: Linux/2.6.38#47.9.1#Debian/7.0

Connection: close

Last-Modified: Mon, 11 Jan 2010 17:39:42 GMT

Content-Type: text/html; charset=ISO-8859-1

Content-Length: 105

BEISPIEL IP-KAMERAS: SHODAN



Any time & Any where
IP Surveillance for Your Life

Customer Login

Username :

Password :

Verify Code :

2 S E 3

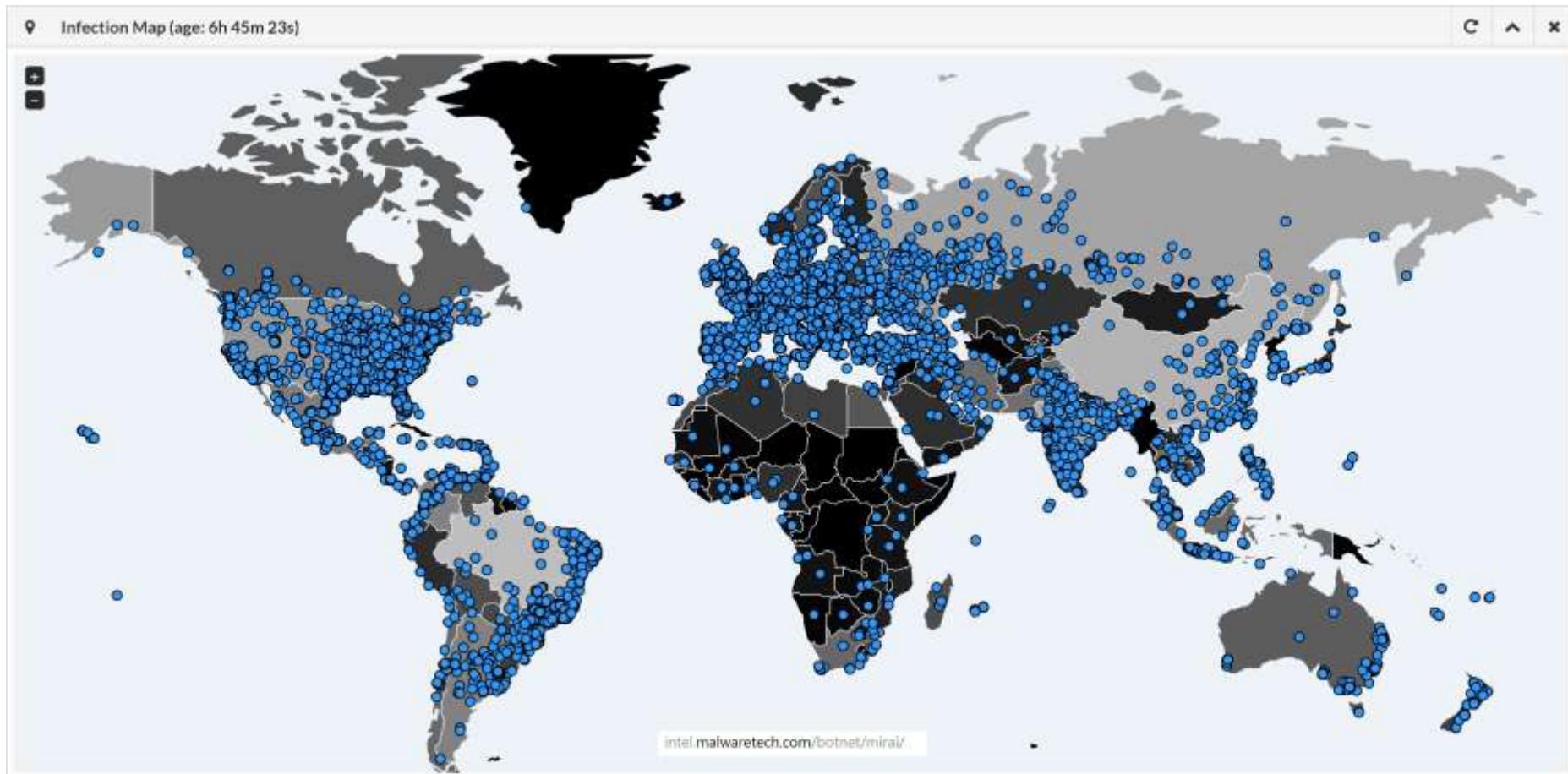
LOGIN

View: [Mobile](#) | [PC](#)

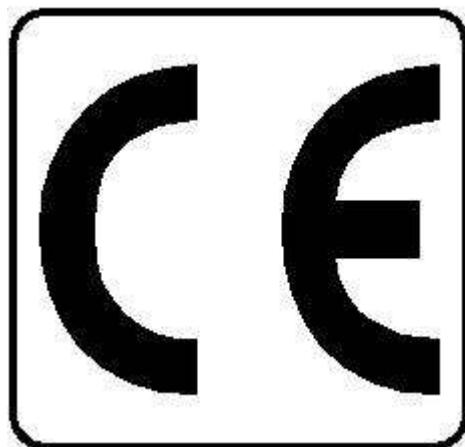
BEISPIEL IP-KAMERAS: SHODAN



GAR NICHT SMART: IOT-BOTNETZE WIE MIRAI



ZERTIFIZIERTE IT-SICHERHEIT?



ZERTIFIZIERTE SICHERHEIT „MADE IN GERMANY“

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany



ALLE ERGEBNISSE GRATIS BEI AV-TEST ONLINE

The screenshot shows the AV-TEST website interface. At the top, there are language links for Deutsch, English, Français, and Español. Below the header, there are navigation links for Institut, News, Tools (which is highlighted in red), Award, Testberichten, Statistiken, Publikationen, Presse, and Kontakt. The main content area is titled "Anwendungsbereich eingrenzen" and shows four categories: MOBIL GERÄT (ANDROID), PRIVATANWENDER (WINDOWS), PRIVATANWENDER (MAC OS), and UNTERNEHMEN (WINDOWS CLIENT). Below this, a sub-section titled "Einzelnen Hersteller betrachten" is shown. The main title of the page is "Die besten Antivirus Programme für Windows Client Unternehmensanwender". A note below the title says "Getestete Betriebssysteme in Ihrer Auswahl: Windows 10 | Windows 11 | Windows 7 | Windows XP". The main content area displays a table of antivirus products for Windows 10, with a sidebar for Windows 8/8.1. The table includes columns for Name, Scanvollständigkeit, Detektionsfähigkeit, and Benutzersicht. The products listed are AVG, Bitdefender Endpoint Security 6.2, F-Secure Client Security 12.0, G Data AntiVirus Business 14.0, Intel Security McAfee Endpoint Security 10.1, Kaspersky Lab Endpoint Security 10, Kaspersky Lab Small Office Security 5, Microsoft System Center Endpoint Protection 4.9, Segurite Endpoint Security 17.00, Sophos Endpoint Security and Control 10.6, Symantec Endpoint Protection 12.1 & 14.0, and Trend Micro Office Scan 11.0. The table is sorted by scan completeness. Below the table, there are links for "Juni 2016" and "Oktober 2015".





@avtestorg (English) & @avtestde (German)



Folgen Sie uns auf facebook.com/avtestorg

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

Vielen Dank für Ihre Aufmerksamkeit!



HABEN SIE FRAGEN?

