OLAF PURSCHE
98. ERFA-KREIS TAGUNG

Der AV-TEST Sicherheitsreport 2015/2016

ÜBER AV-TEST

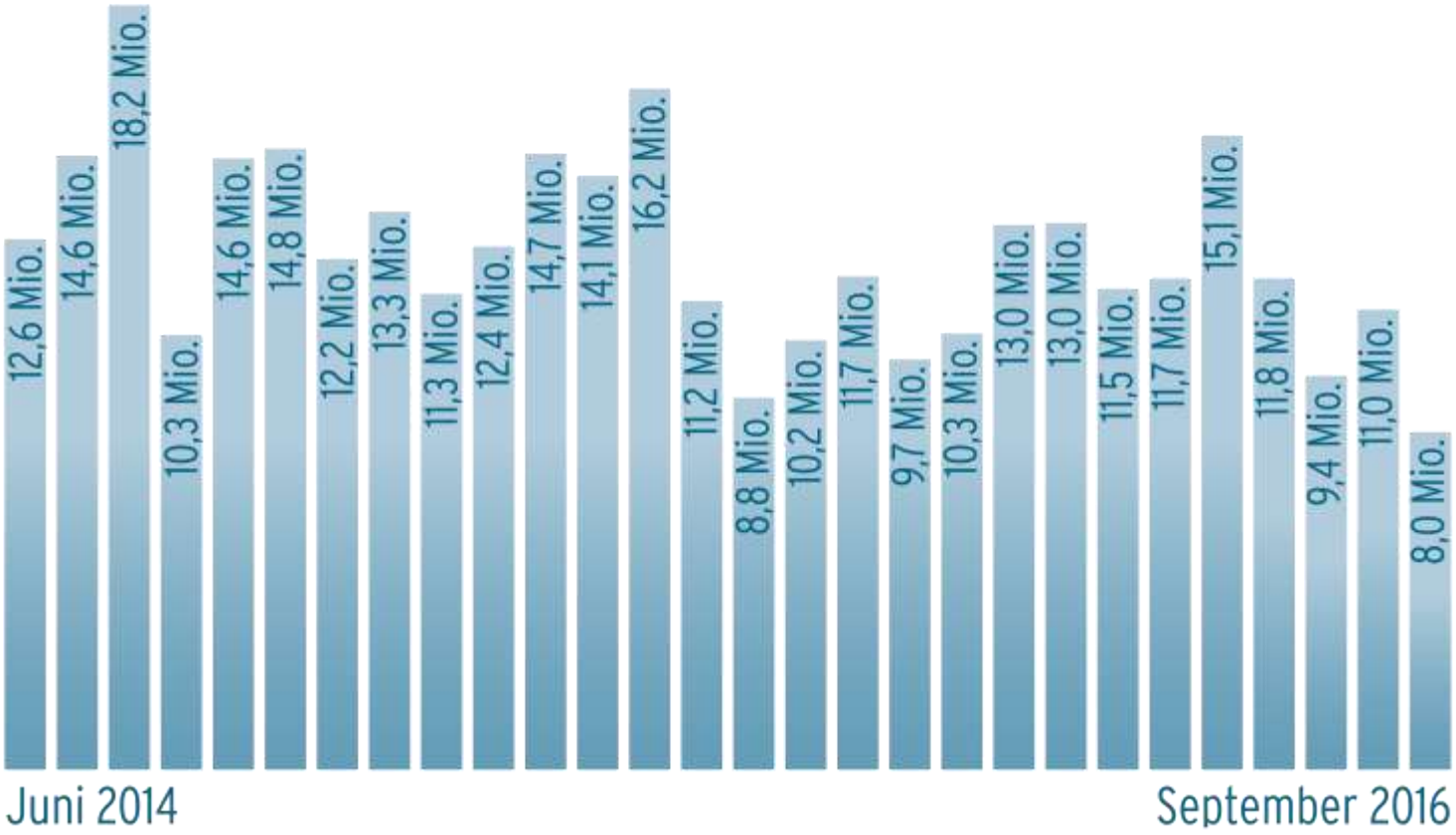
- Team: über 30 international anerkannte Security-Spezialisten
- eine der größten Sammlungen digitaler Schädlinge weltweit
- eigene Forschungsabteilung
- intensive Zusammenarbeit mit wissenschaftlichen Einrichtungen
- selbstentwickelte Analysesysteme
- reproduzierbare Testergebnisse für alle gängigen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

MALWARE-ENTWICKLUNG

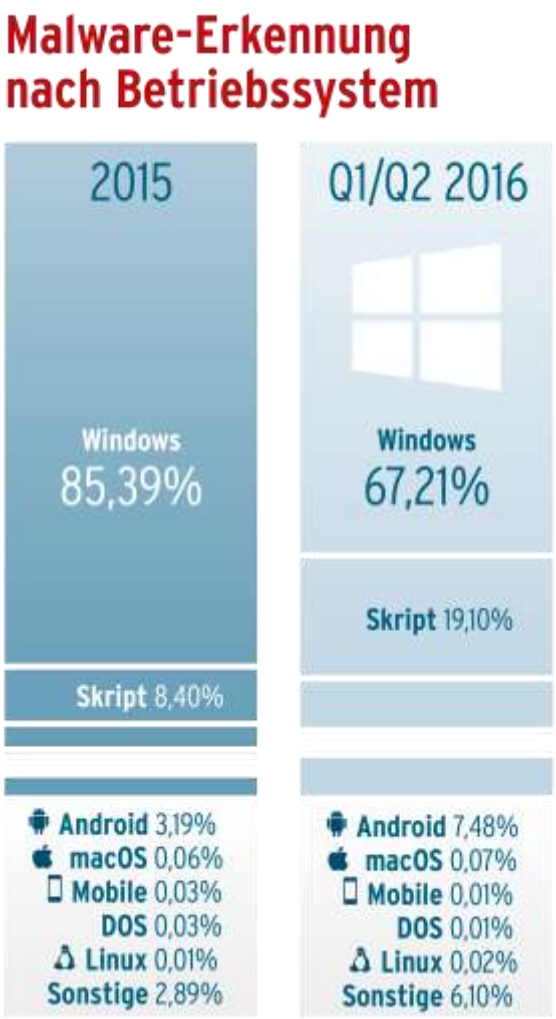
Gesamtentwicklung von Schadprogrammen in den letzten 10 Jahren

5 NEUE SCHÄDLINGE PRO SEKUNDE!

Auftreten neuer Malware insgesamt



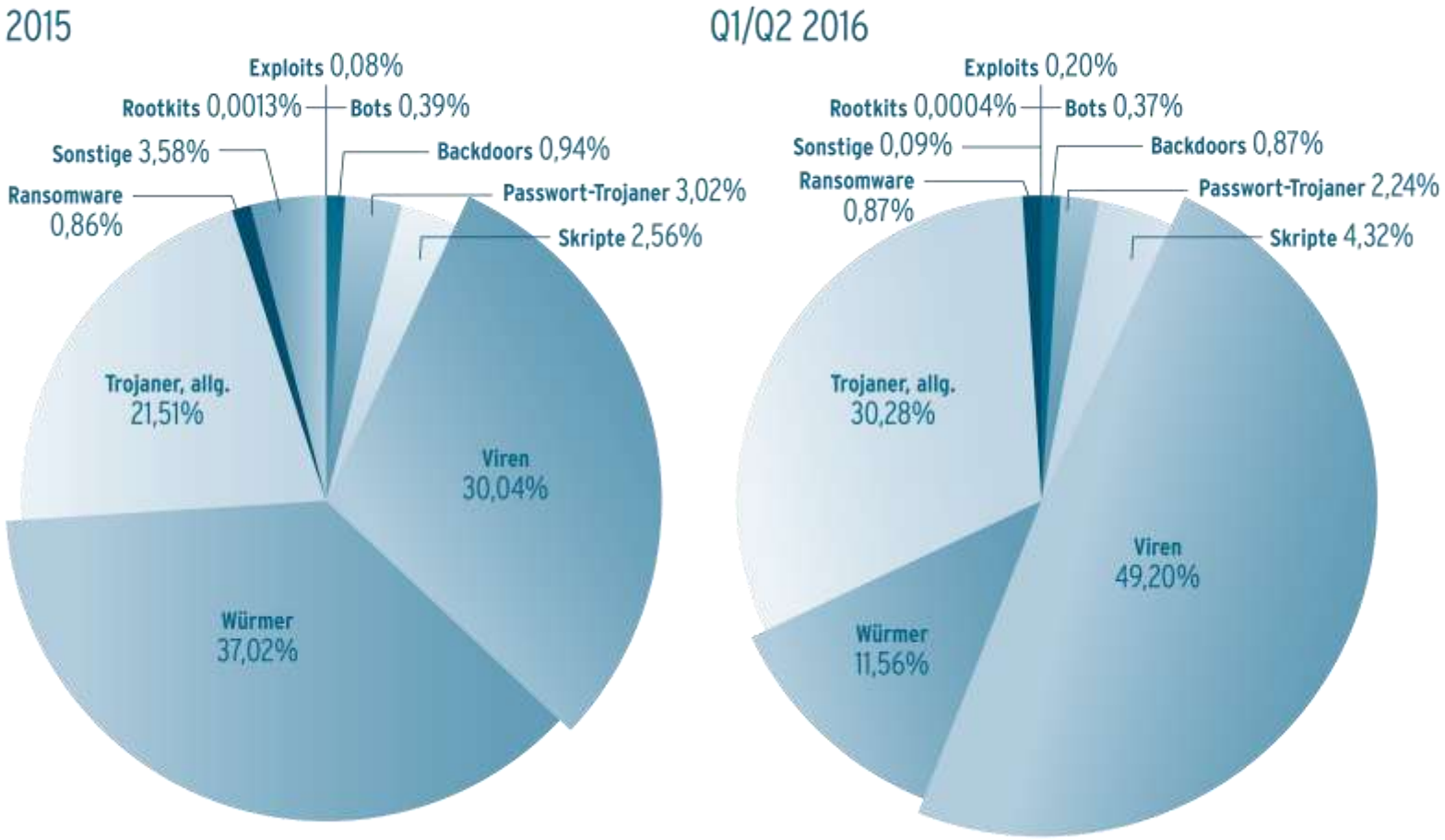
VERTEILUNG VON MALWARE



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

VIREN UNTER WINDOWS AUF DEM VORMARSCH

Malware-Verteilung unter Windows



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,

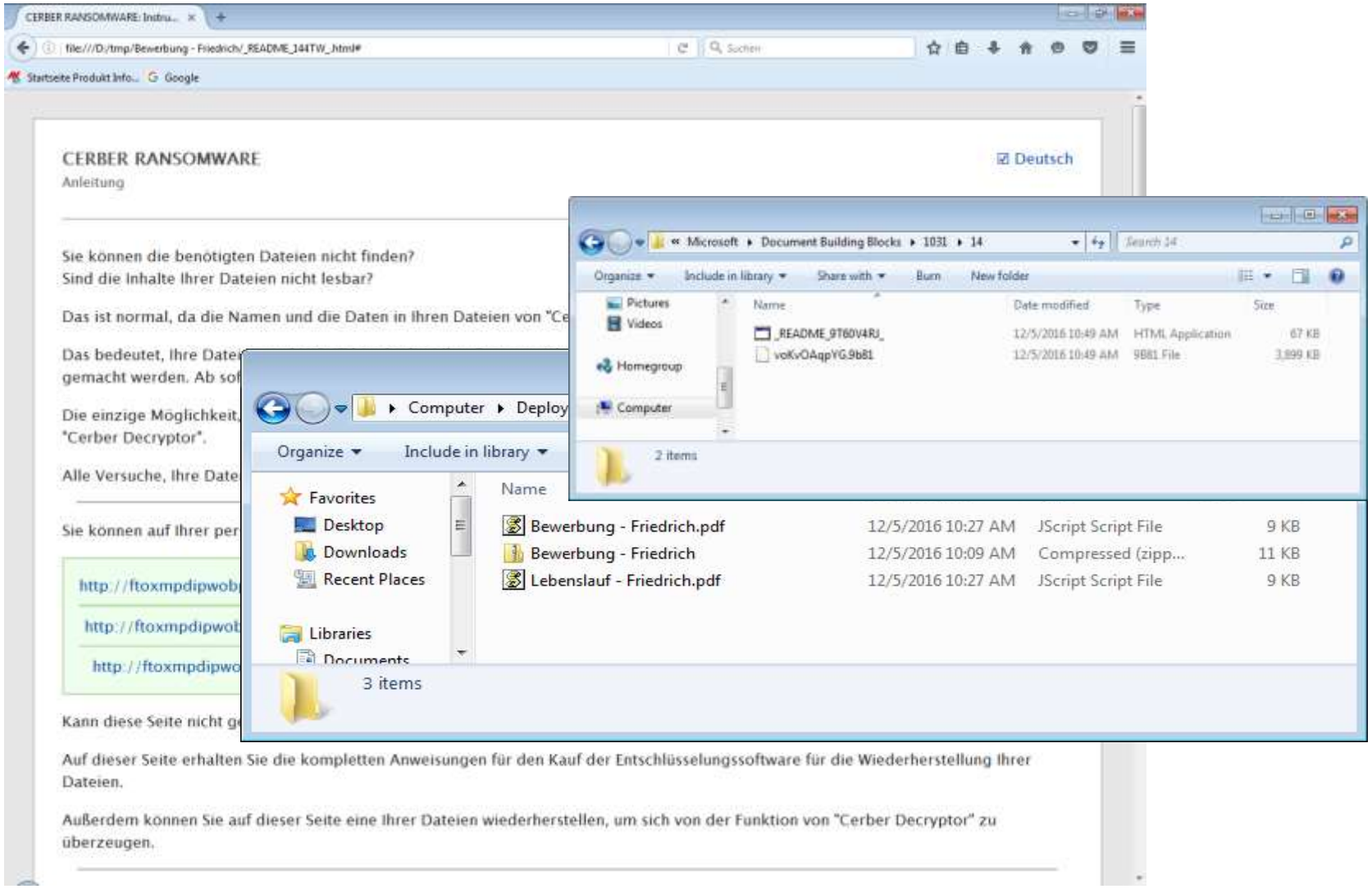
anbei finden Sie meine Bewerbung für Ihre ausgeschriebene Position. Die Stelle entspricht genau meinen Vorstellungen und reizt mich sehr. Da mein Profil und meine bisherigen Erfahrungen gut zu Ihren Anforderungen passen, bin ich davon überzeugt, einen echten Mehrwert leisten zu können. Und das möchte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

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

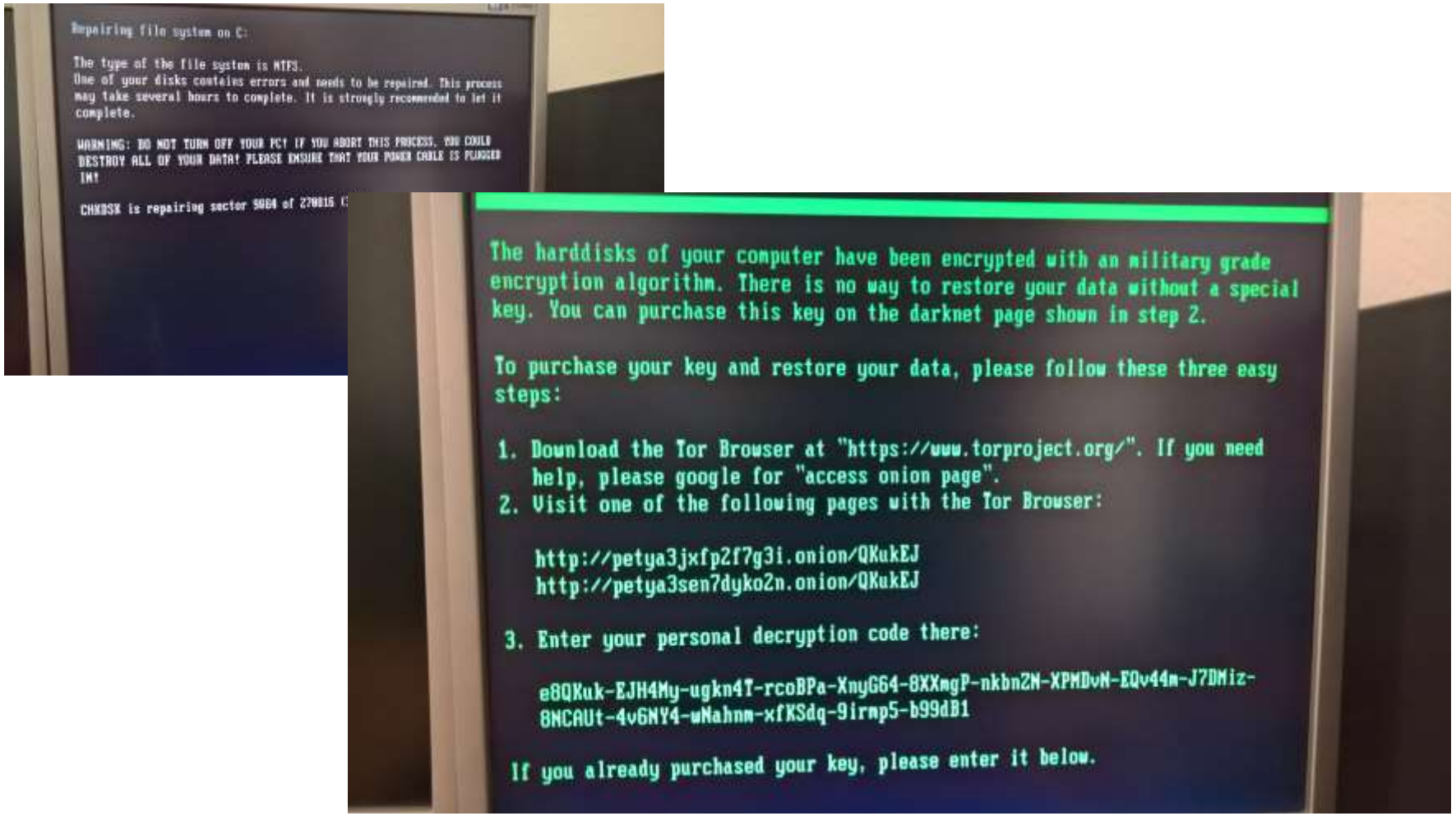
Mit besten Grüßen,

Stefan Friedrich

WINDOWS-MALWARE „HIGHLIGHTS“: BANKING-TROJANER

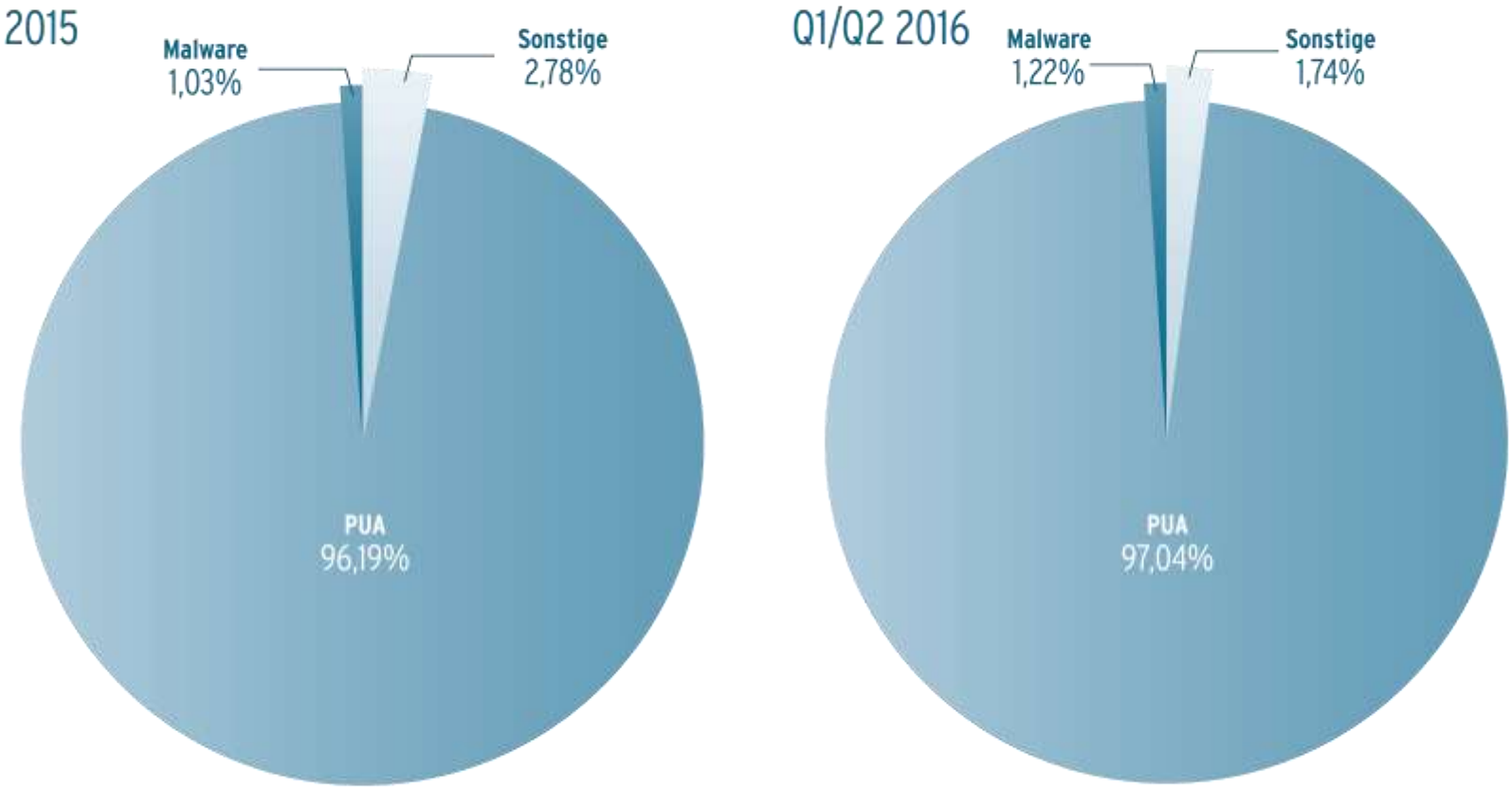


WINDOWS-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



GEFAHRENLAGE FÜR MAC-NUTZER

Schädlinge macOS



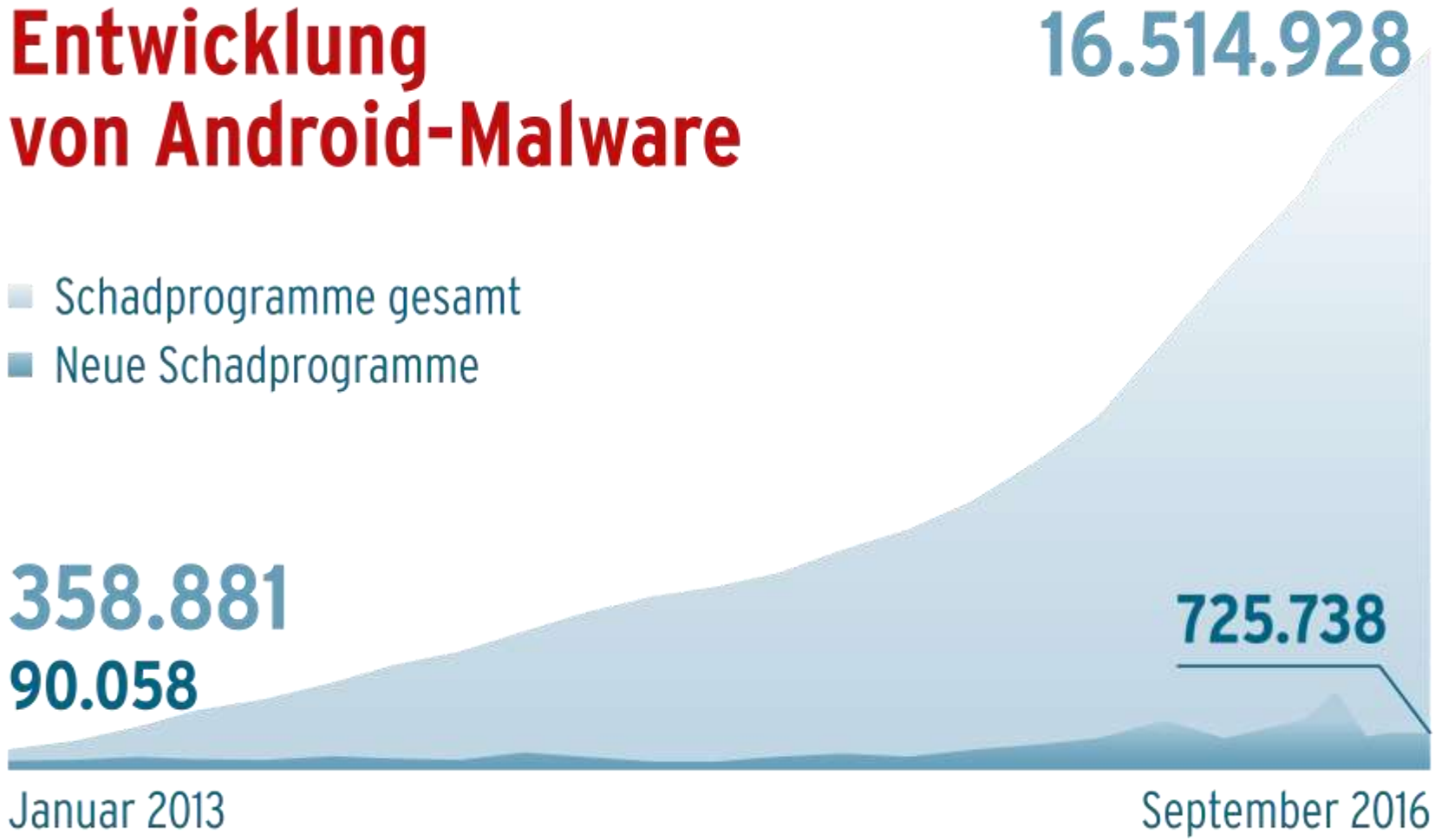
Schädlinge Android versus Mobil

Android 2015
99,18%

Android Q1/Q2 2016
99,87%

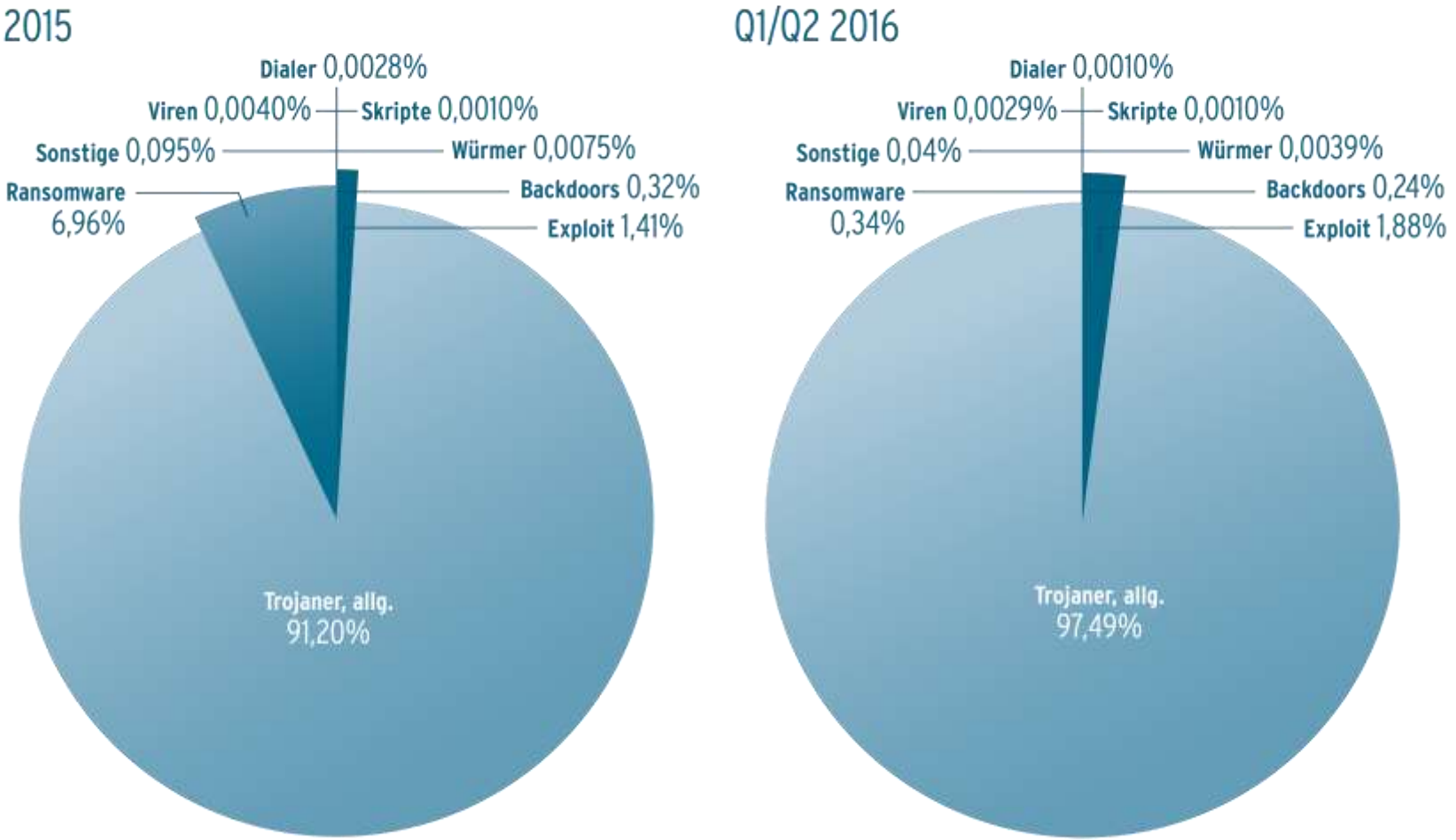
Mobile 2015
0,82%

Mobile Q1/Q2 2016
0,13%

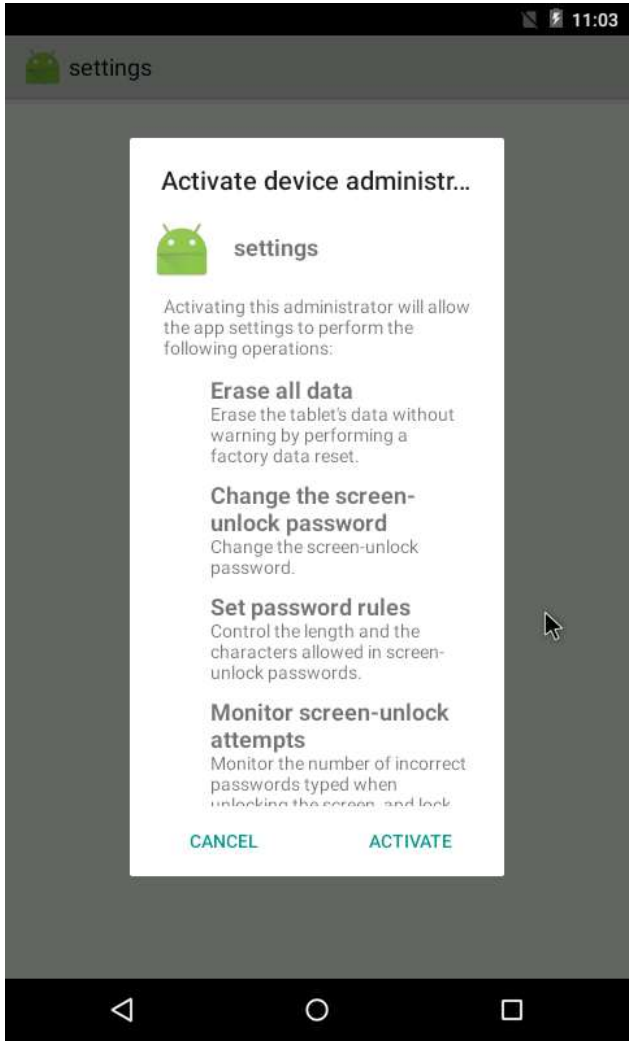

Entwicklung
von Android-Malware
16.514.928
Schadprogramme gesamt
Neue Schadprogramme
358.881
90.058
725.738
Januar 2013
September 2016

TROJANER-ATTACKEN AUF ANDROID

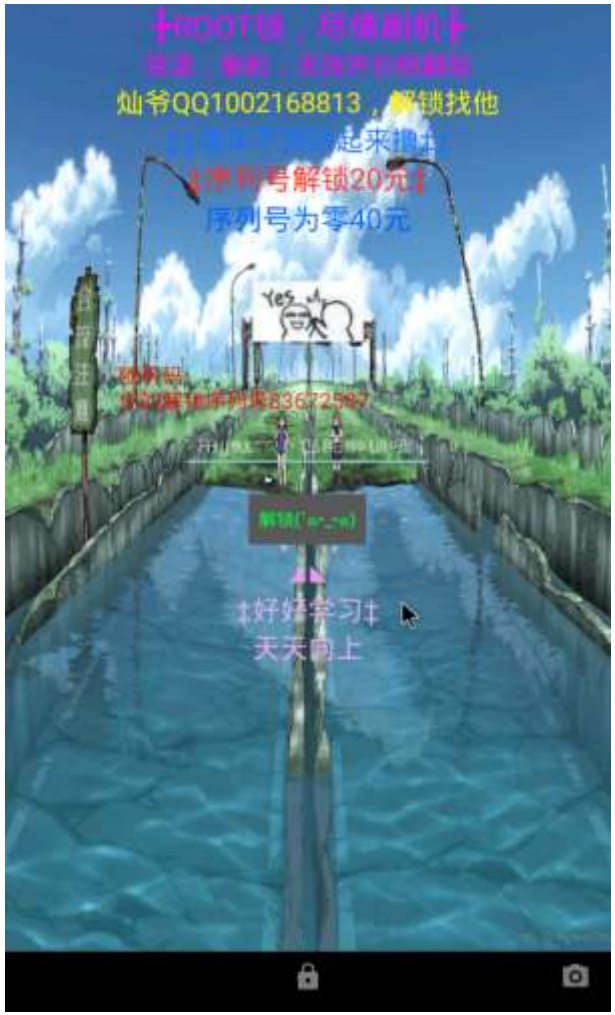
Malware-Verteilung Android



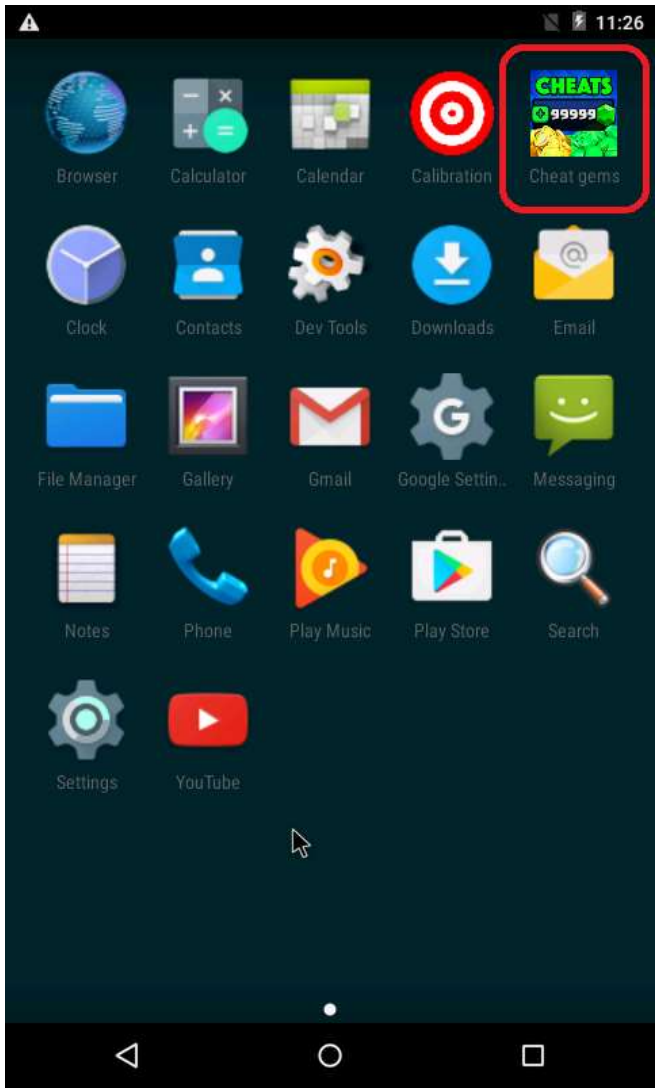
ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER

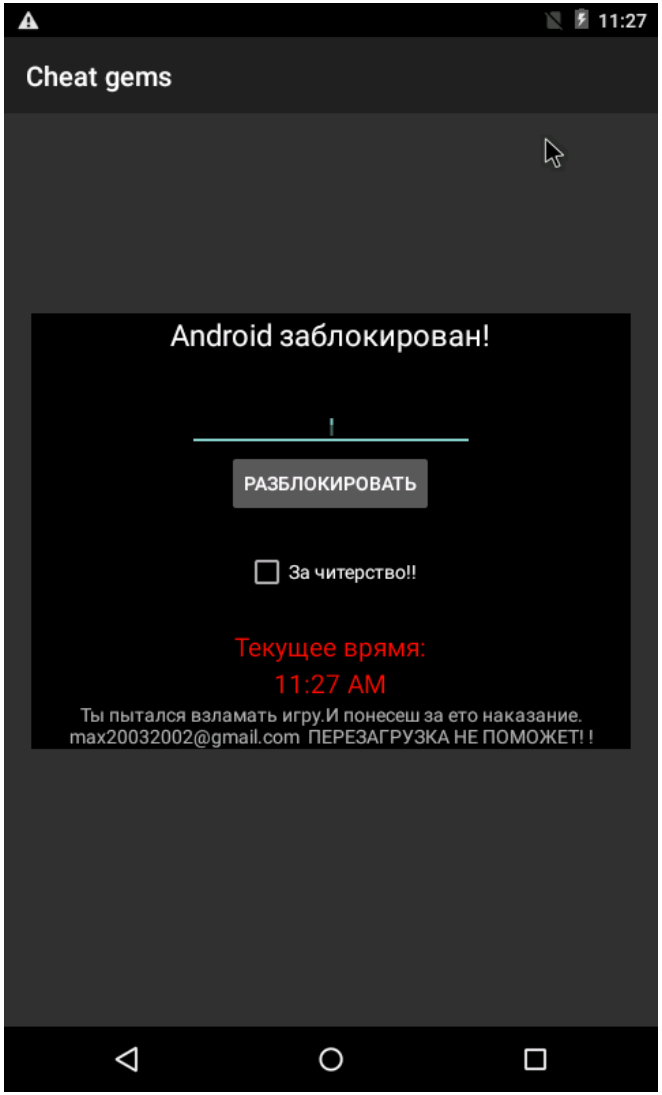


ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER

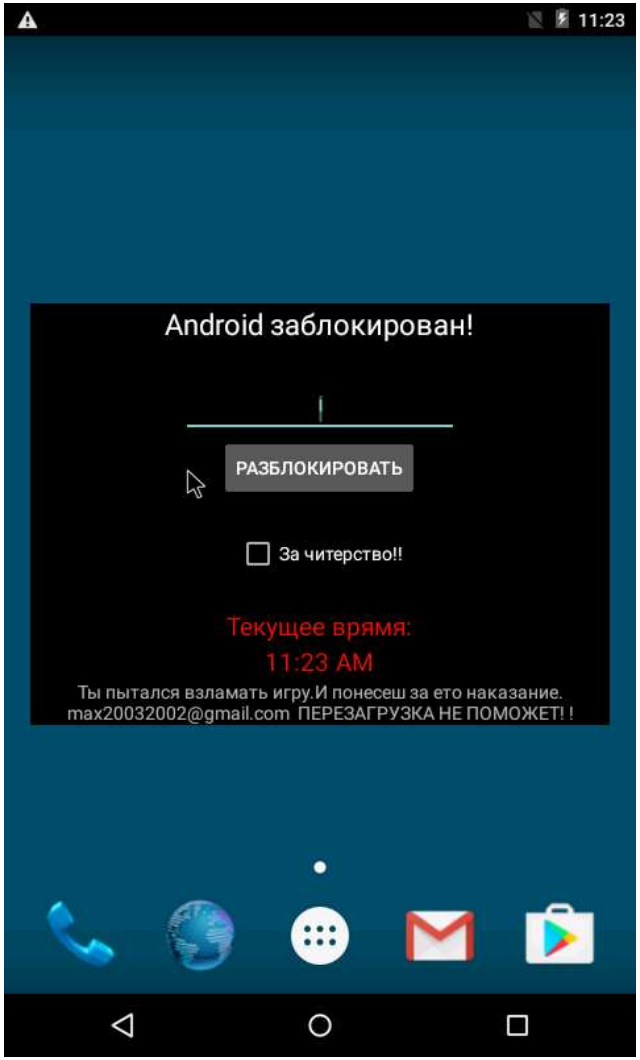


ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER

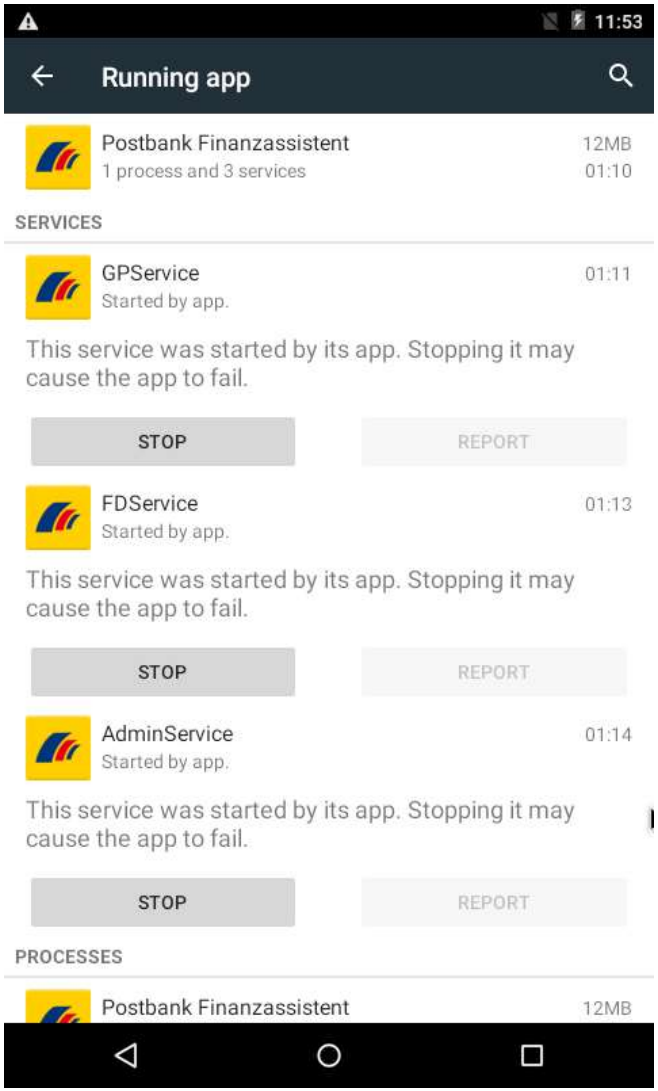


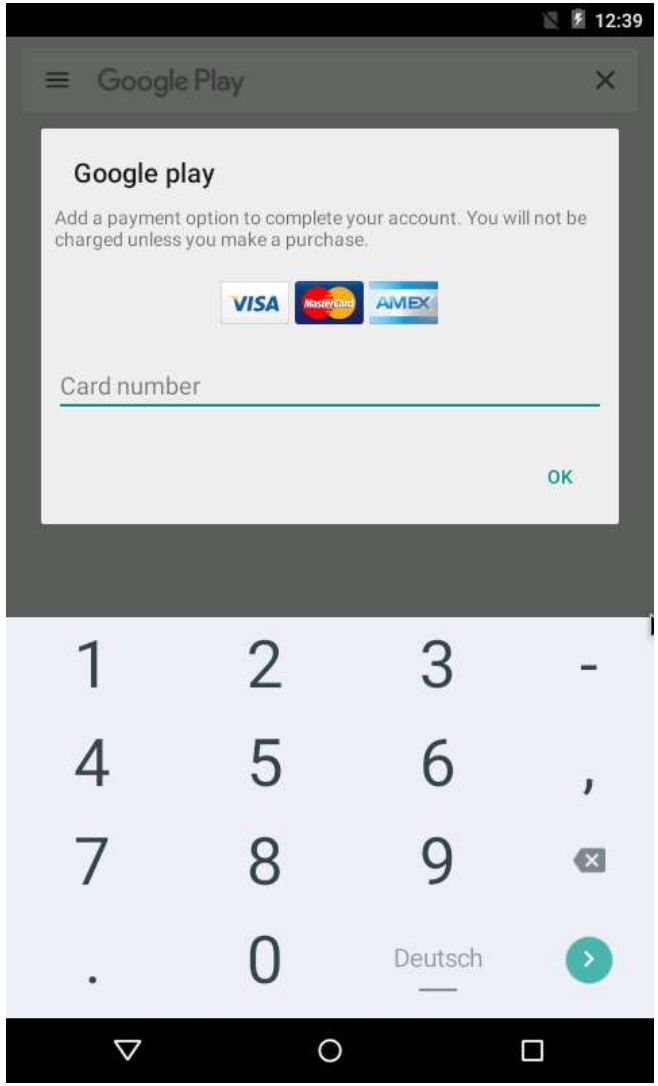


ANDROID-MALWARE „HIGHLIGHTS“: CRYPTOLOGGER

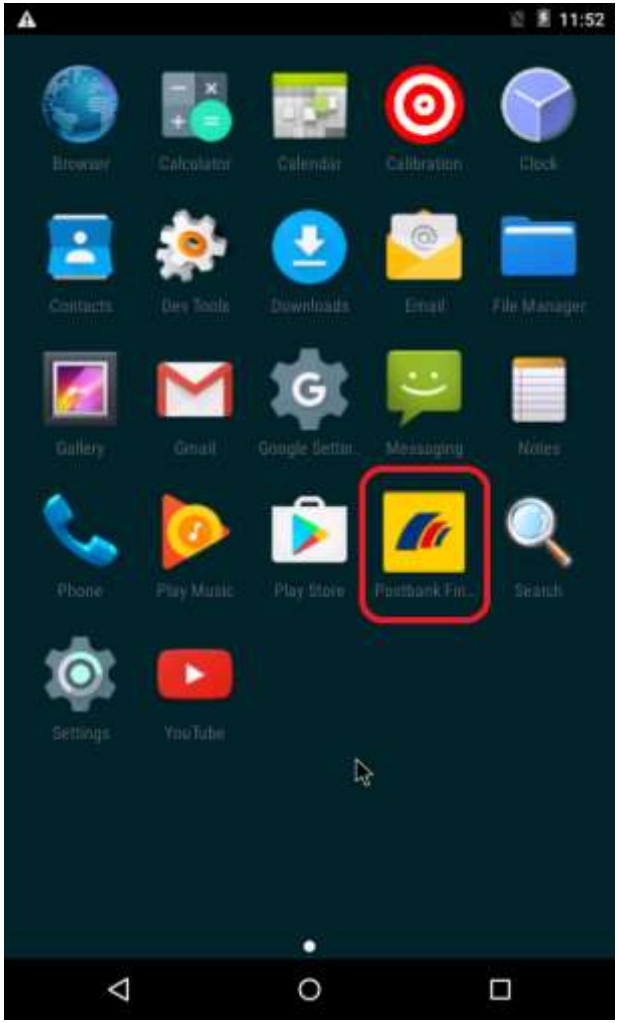


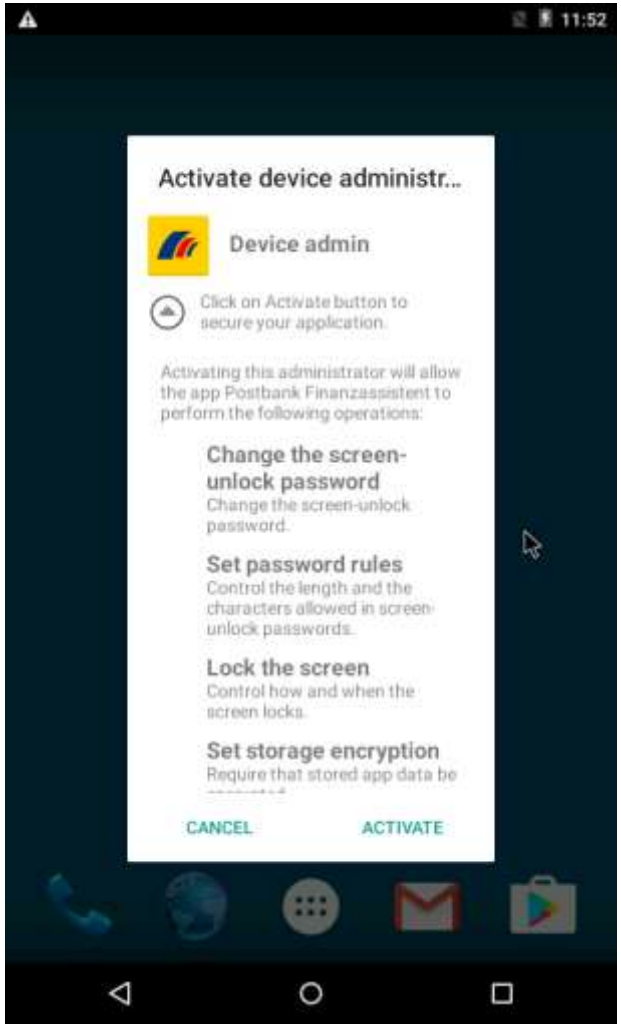
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



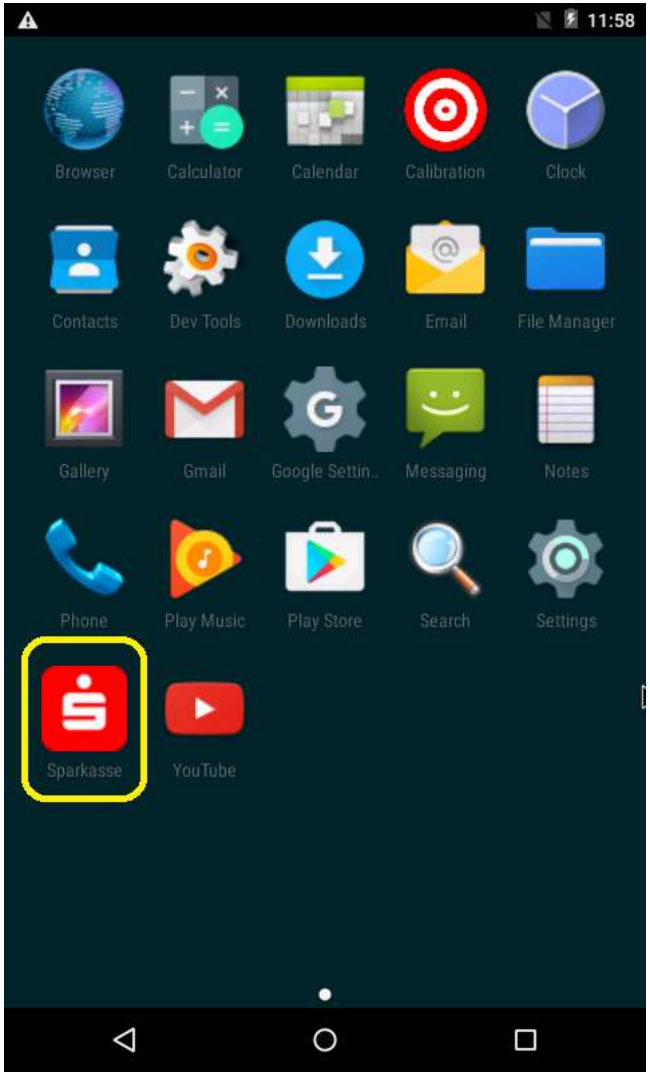


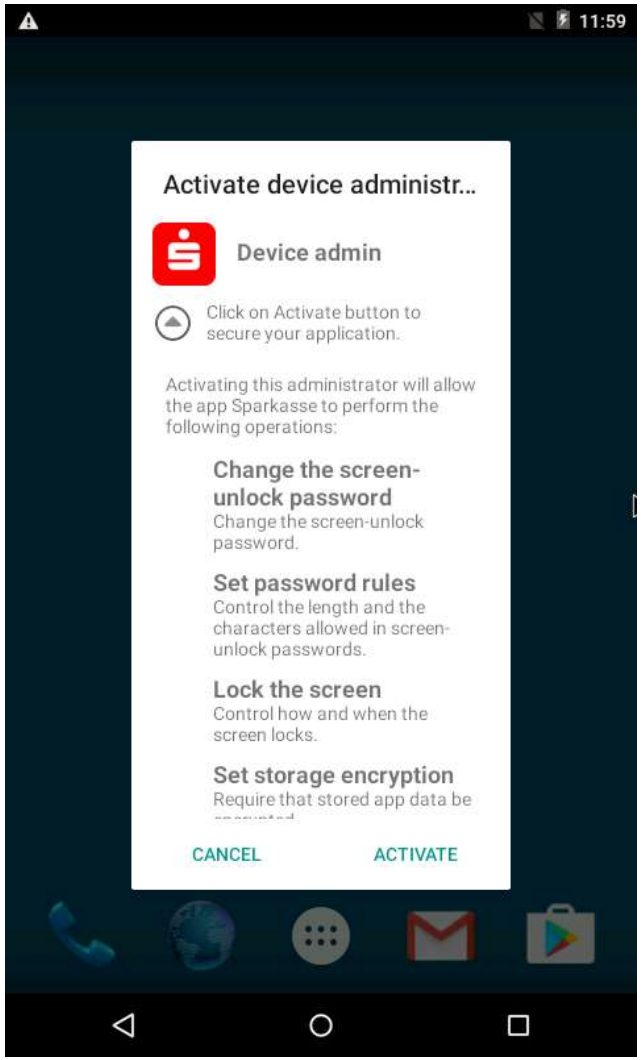
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



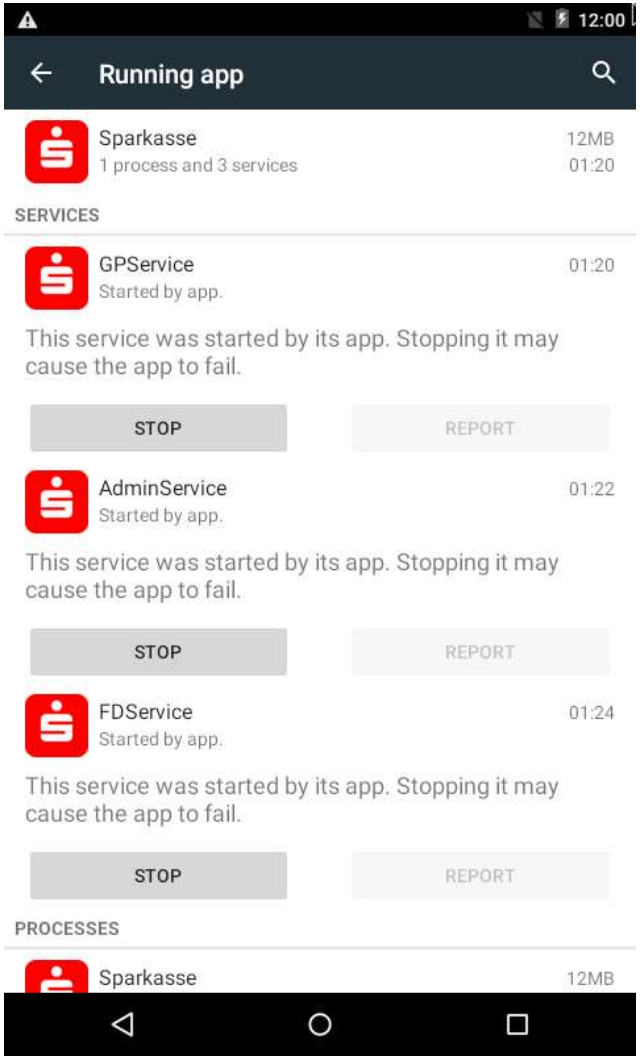


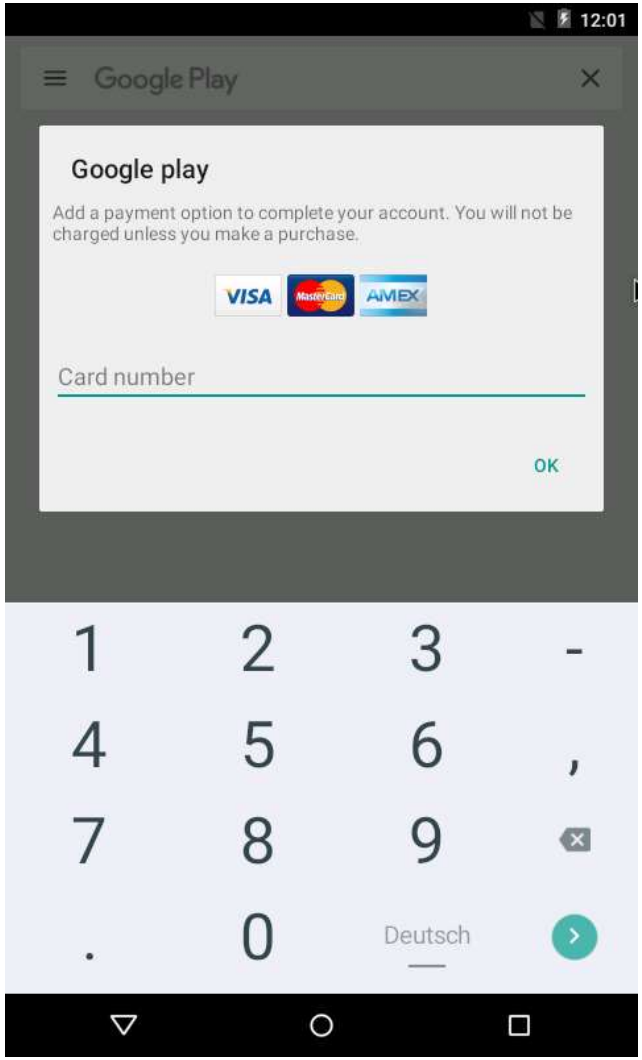
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



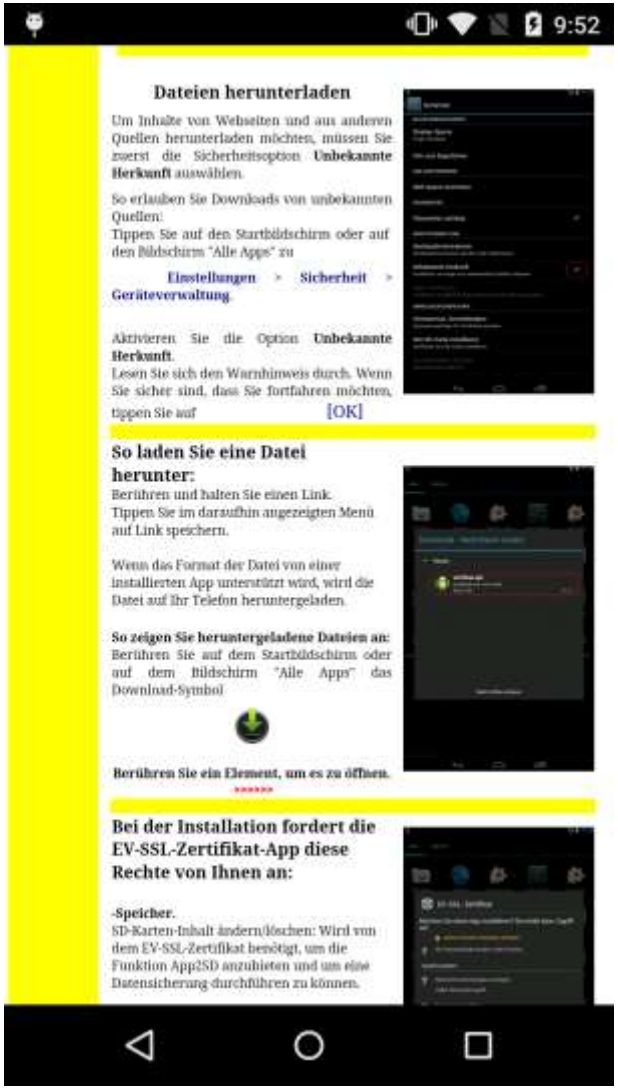


ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER

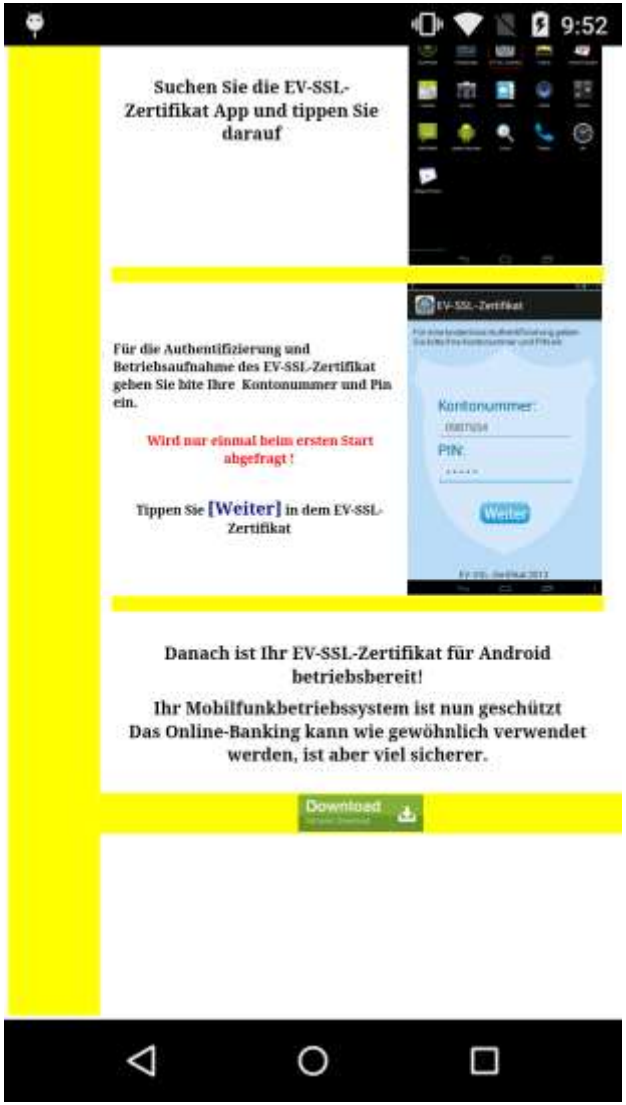


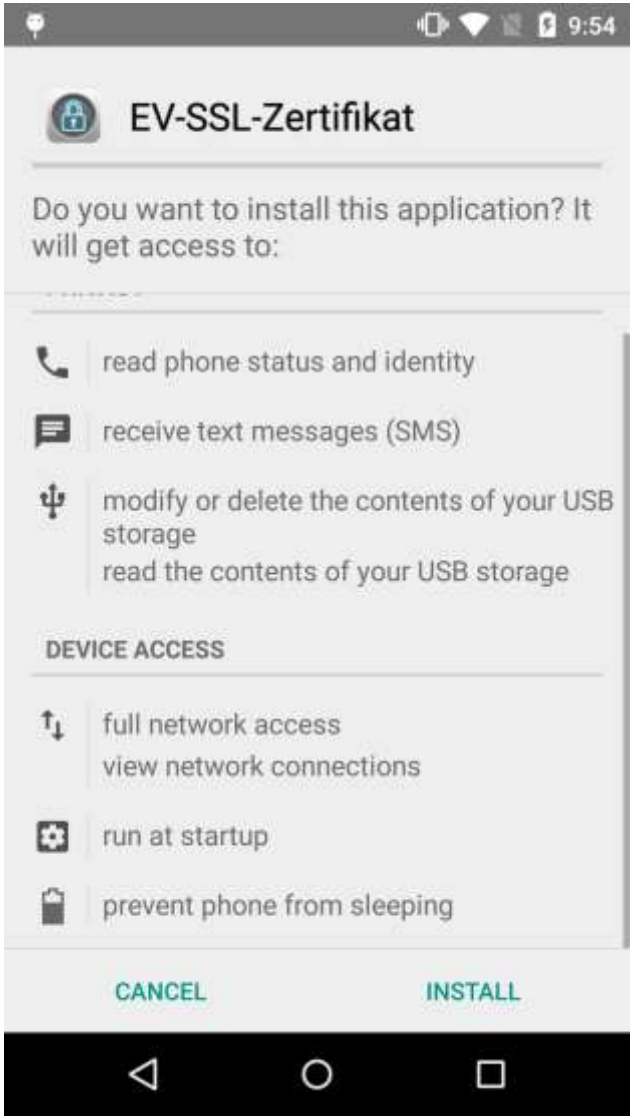


ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER



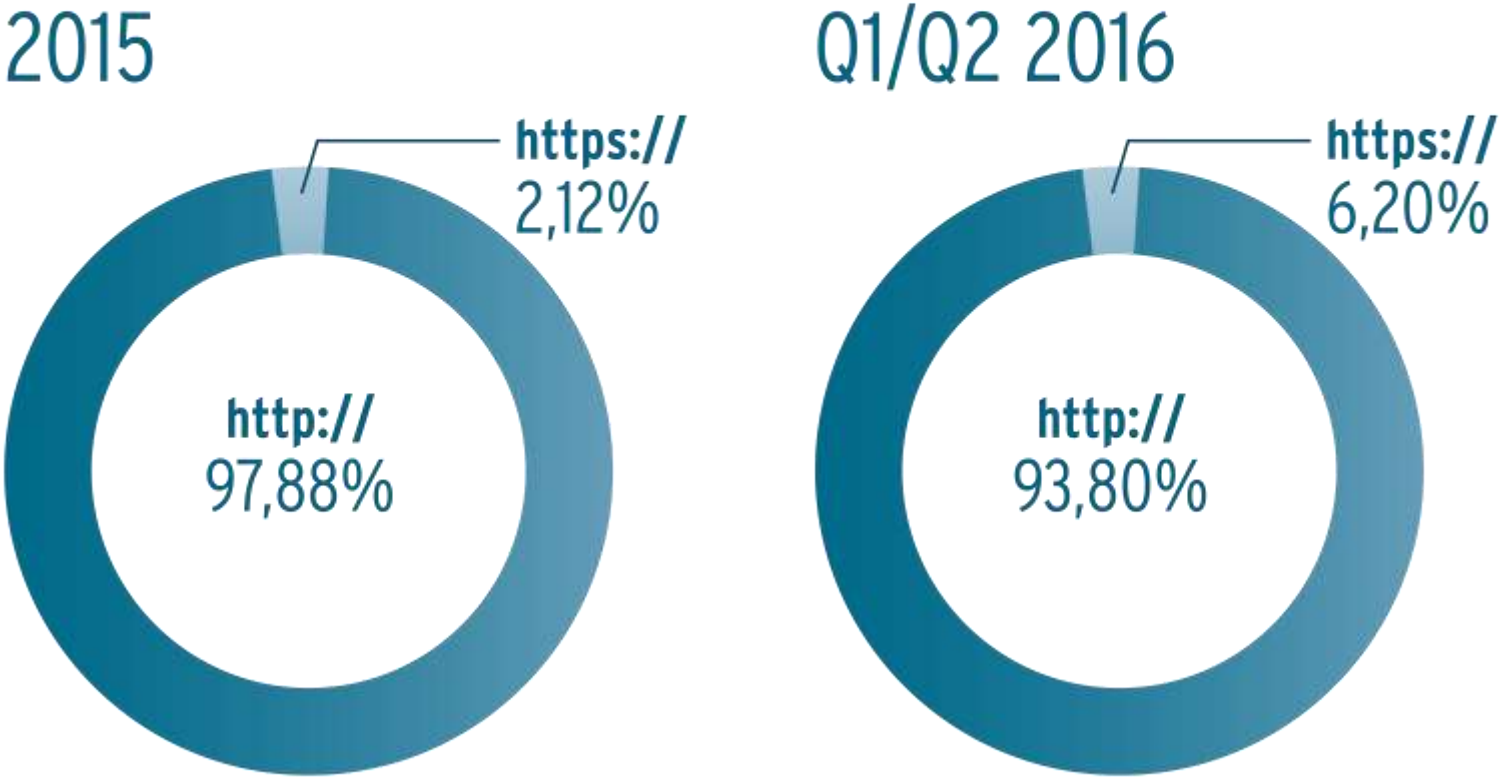
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER





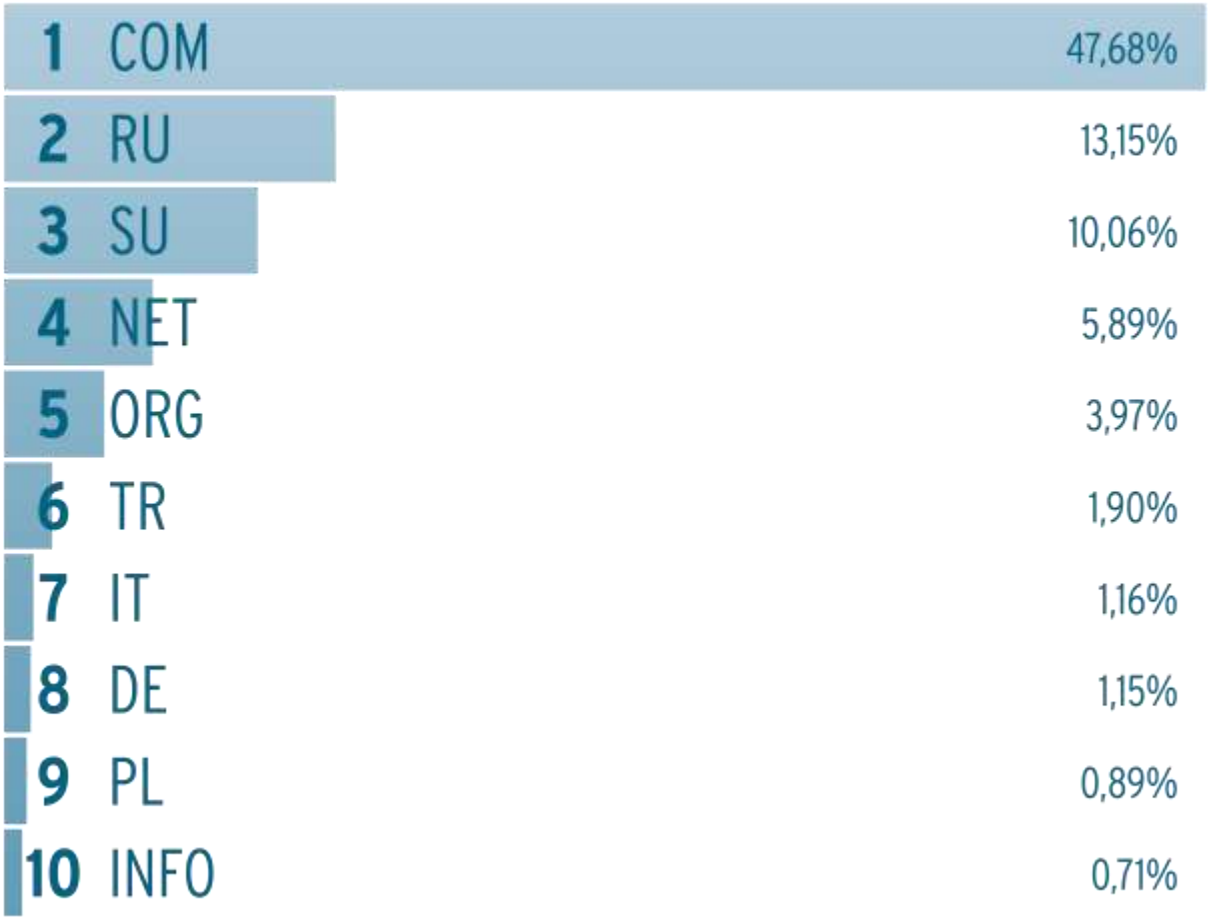
ANDROID-MALWARE „HIGHLIGHTS“: BANKING-TROJANER

Malware-Verteilung über verschlüsselte und unverschlüsselte Internetseiten

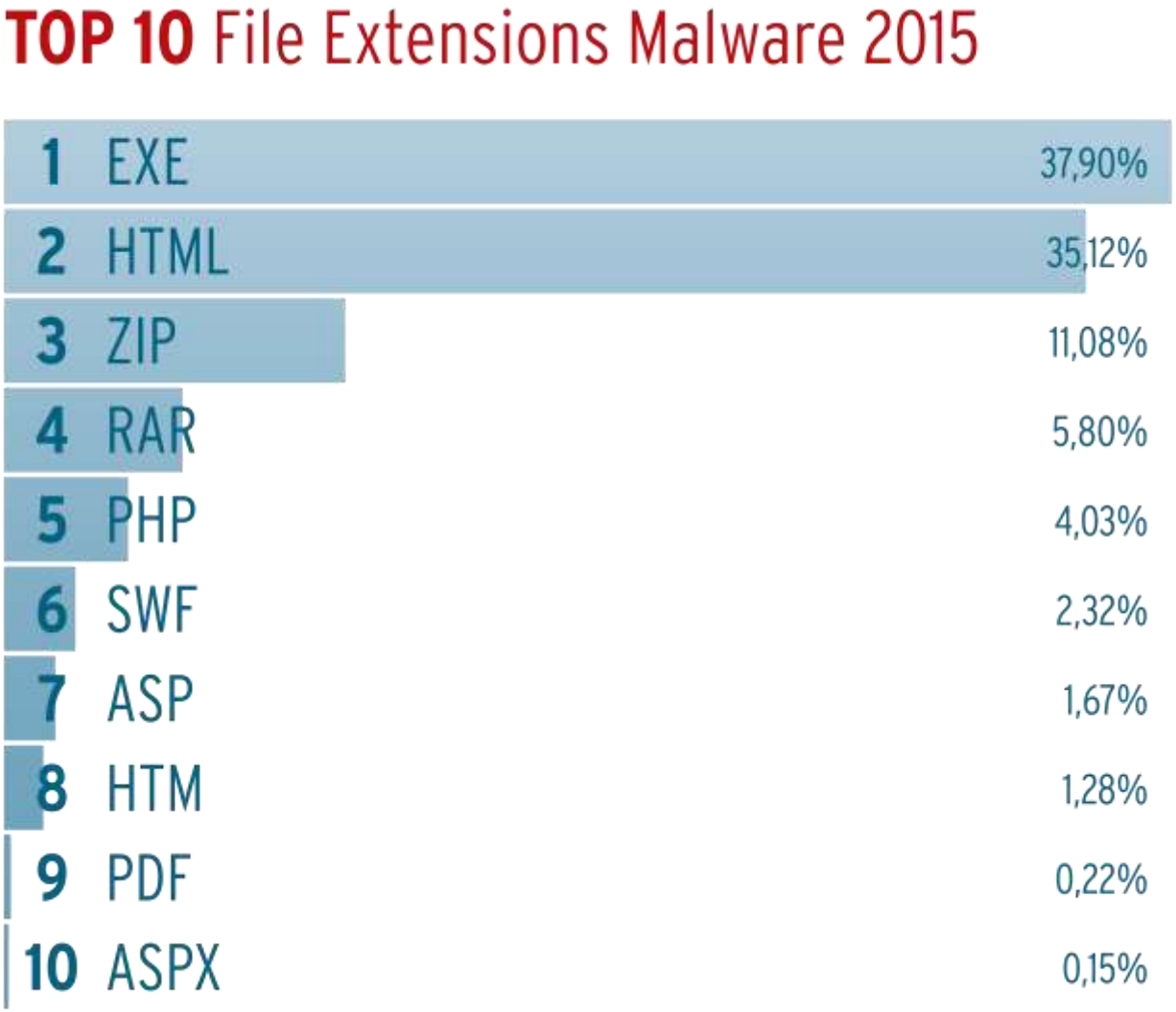


MALWARE-ÜBERTRAGUNG DURCH WEBSITES

TOP 10 Malware-Domains 2015

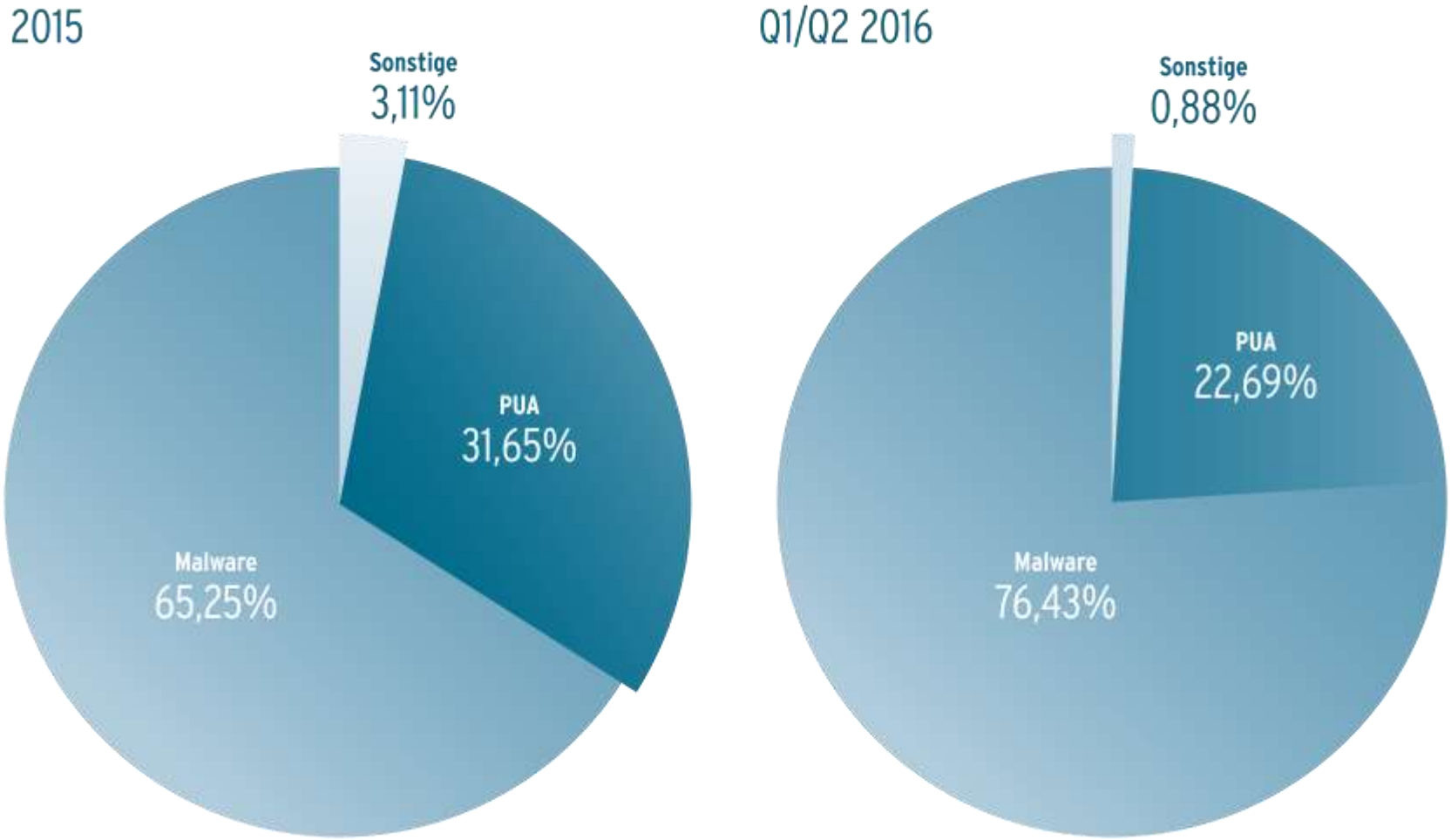


ZUR MALWARE-ÜBERTRAGUNG GENUTZTE FORMATE

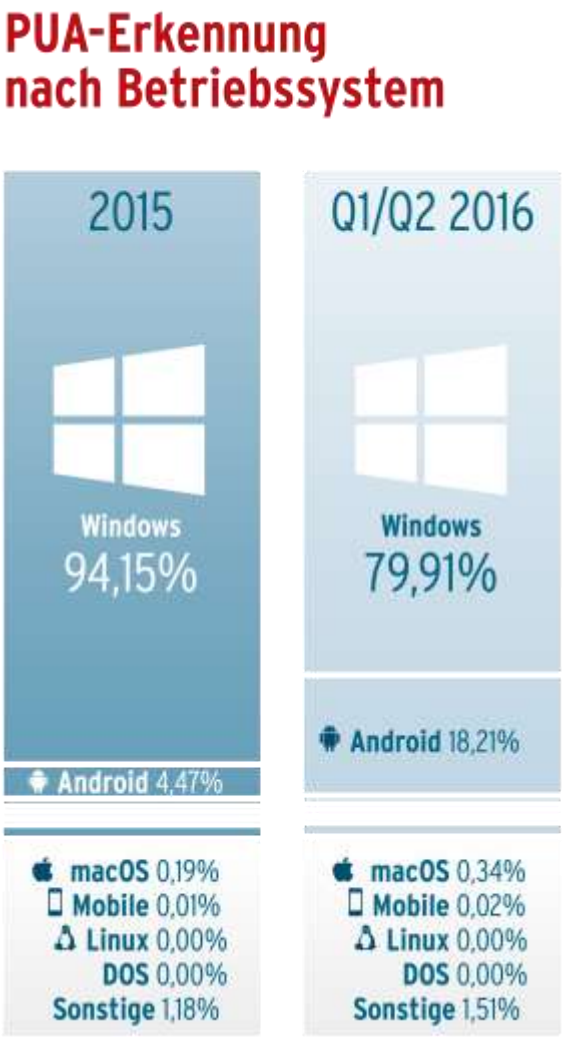


PUA – DIE WACHSENDE GEFAHR

PUA-Erkennung gesamt



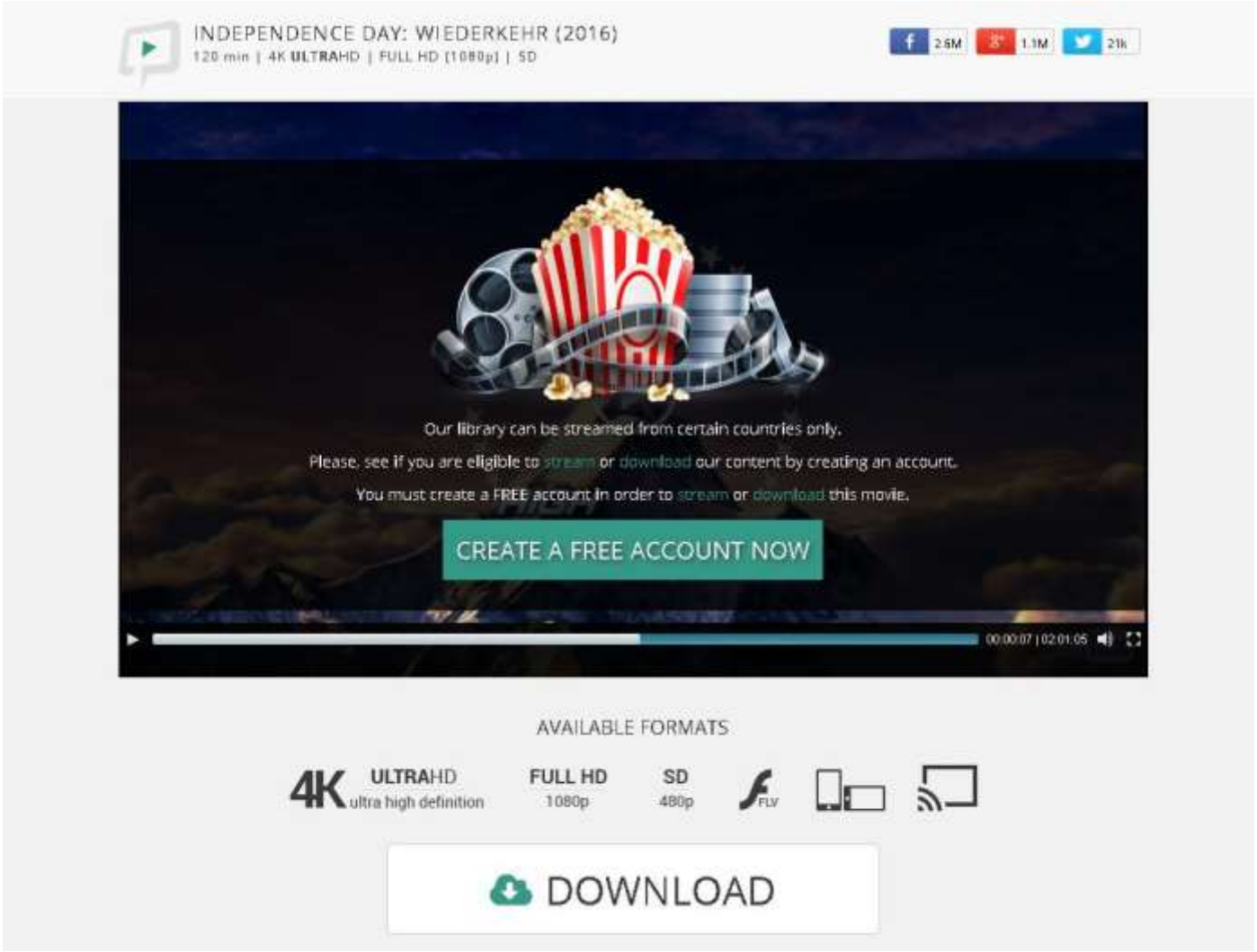
PUA – DIE WACHSENDE GEFAHR



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

PUA – DIE WACHSENDE GEFAHR

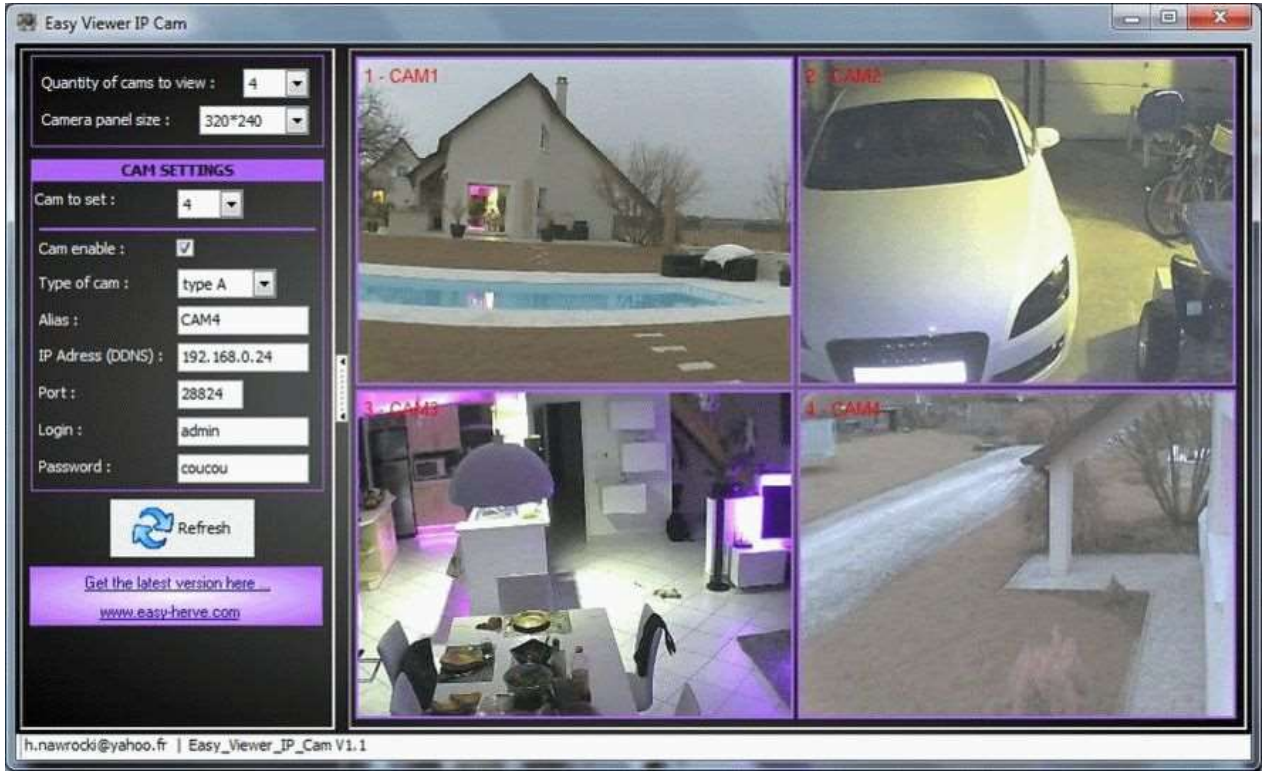
PUA – DIE WACHSENDE GEFAHR



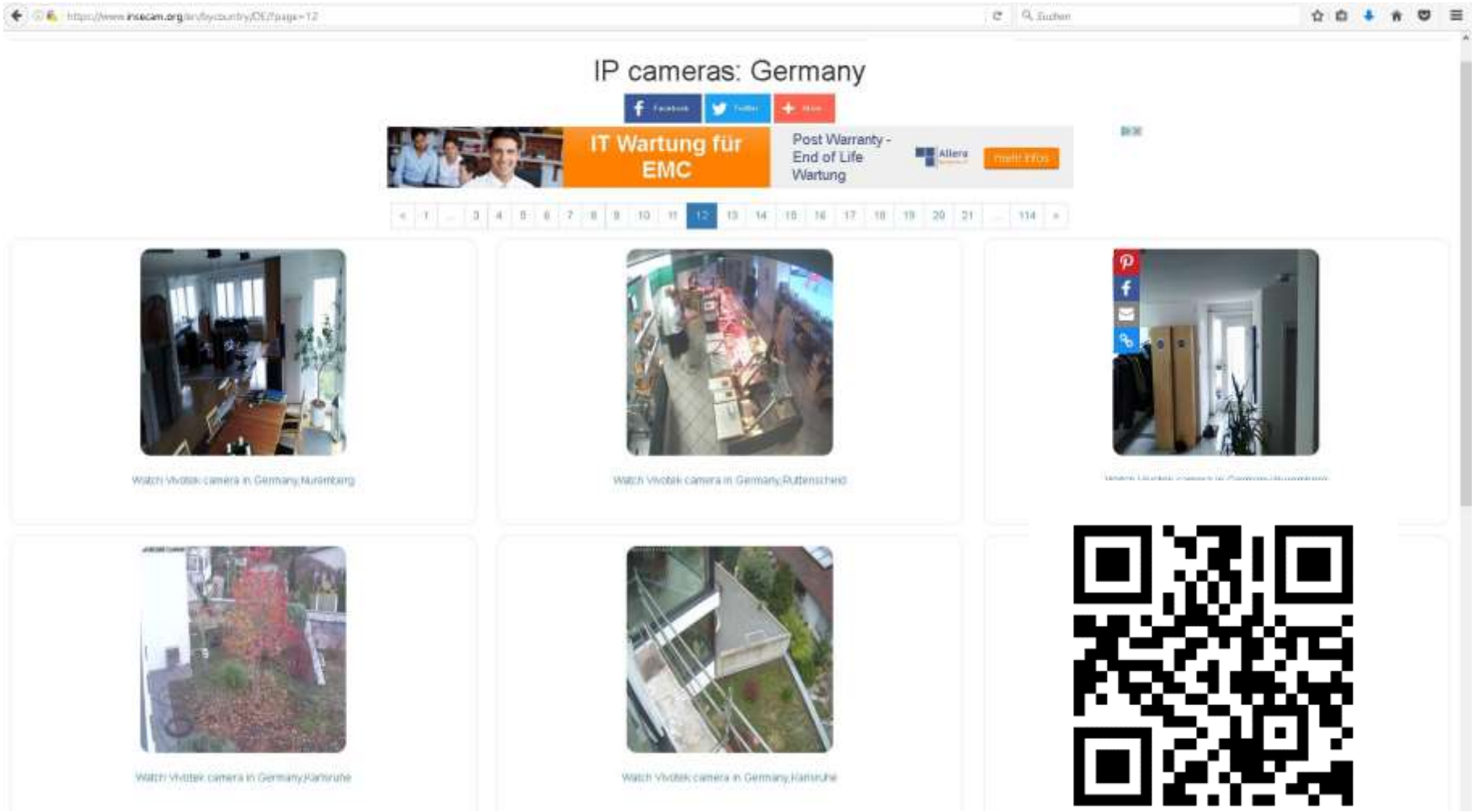
INTERNET DER DINGE: ALLES SMART, ODER NICHT?

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

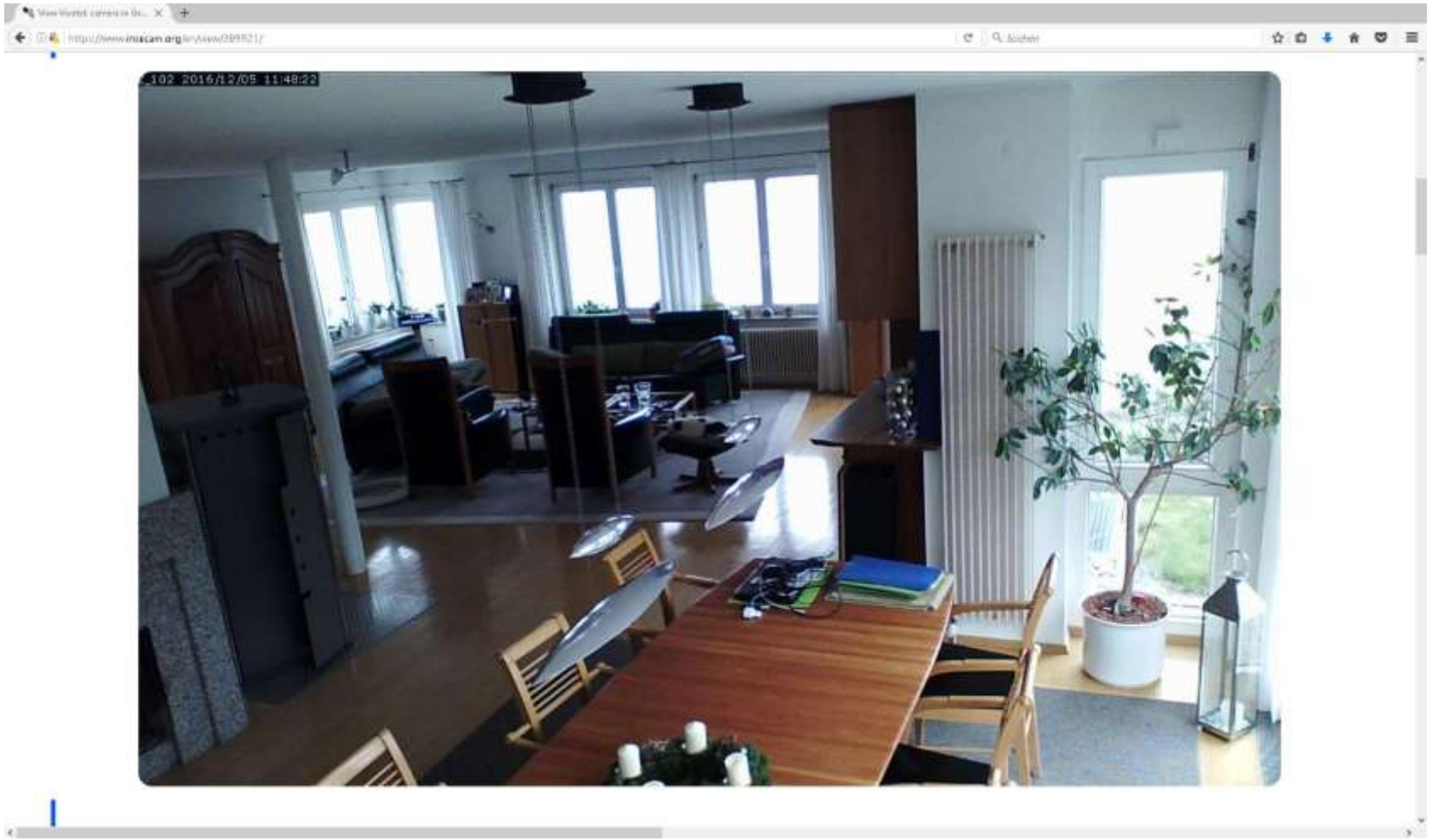
BEISPIEL IP-KAMERAS: SORGEN FÜR SICHERHEIT



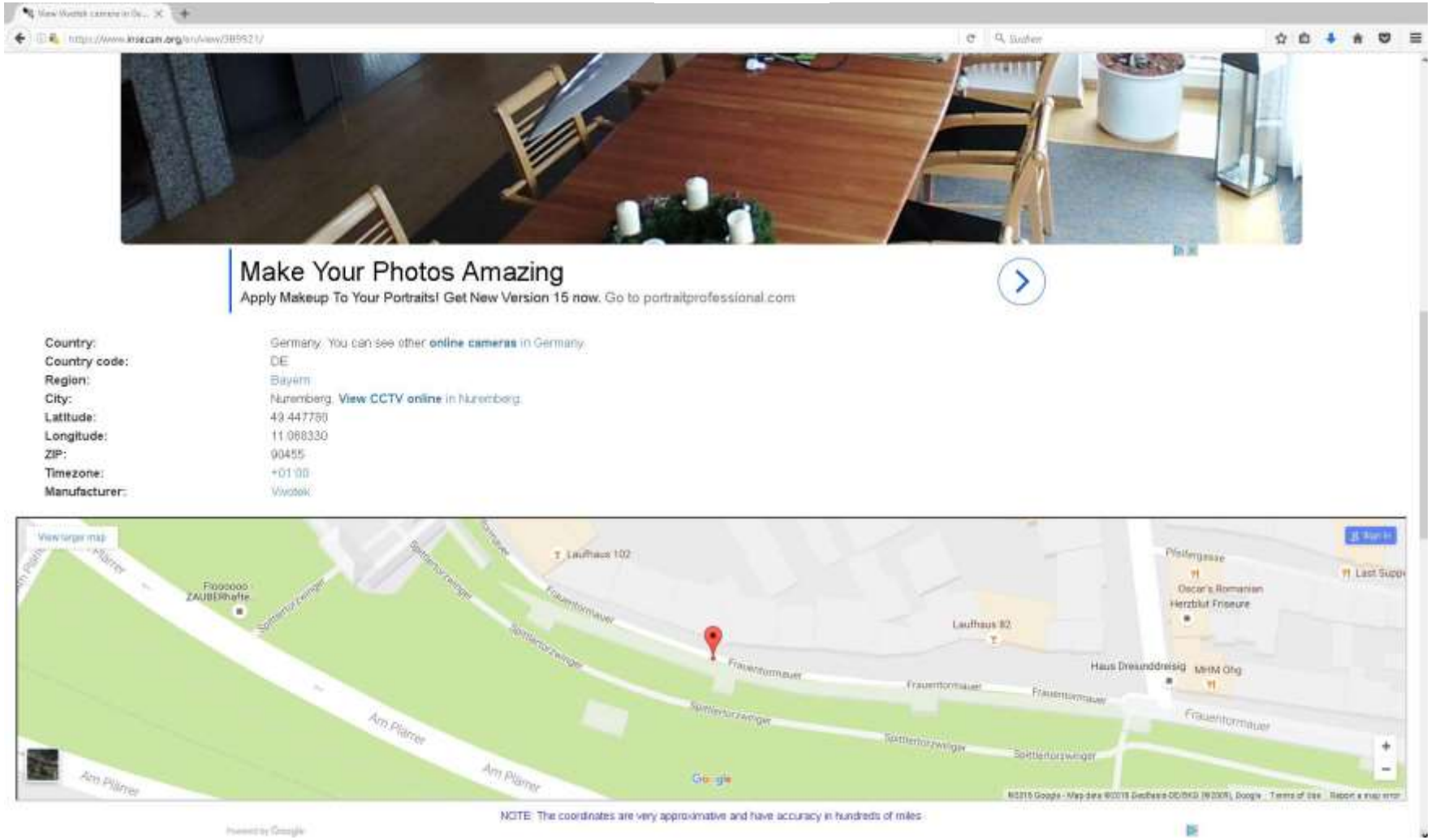
BEISPIEL IP-KAMERAS: INSECAM



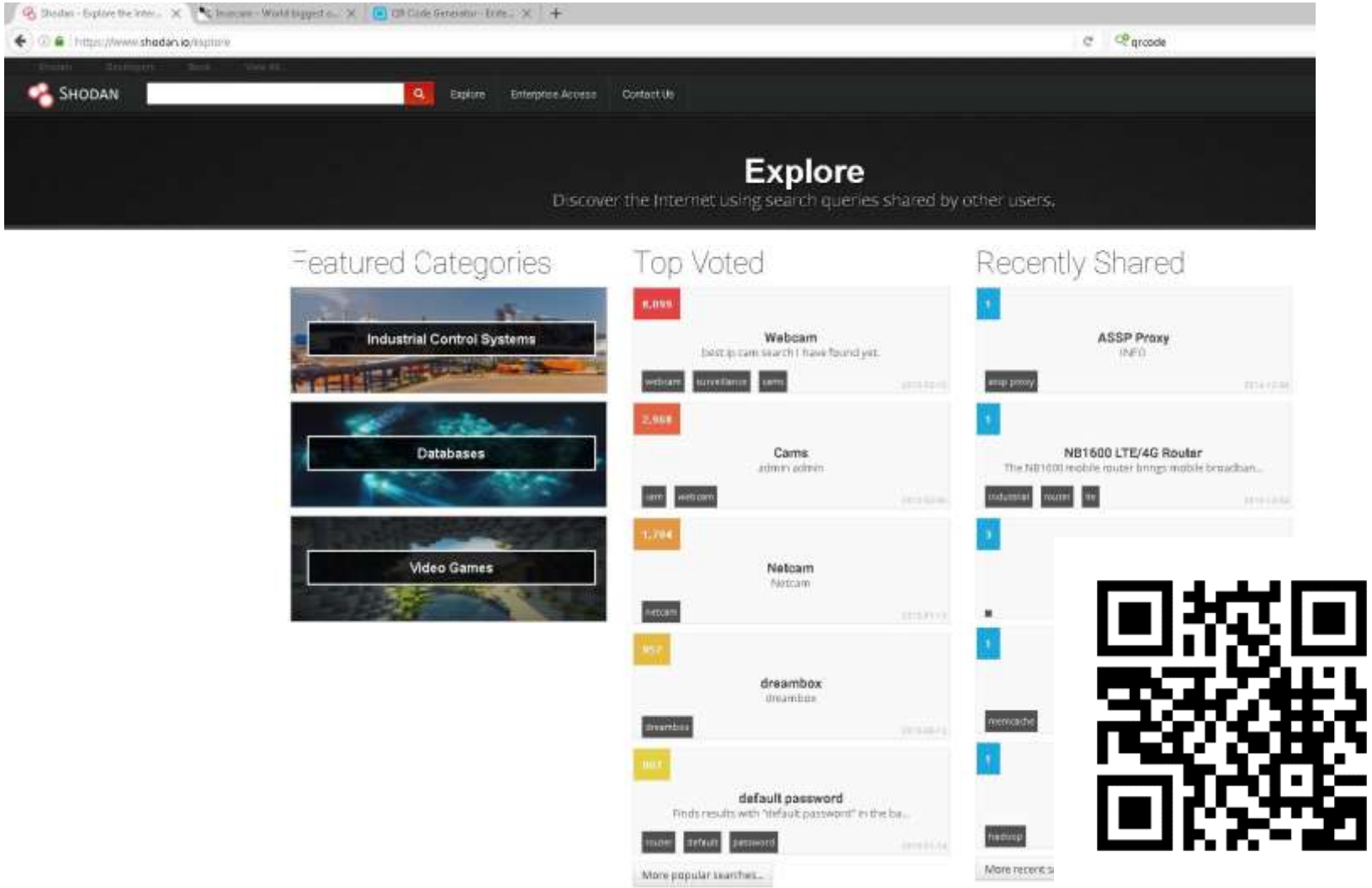
BEISPIEL IP-KAMERAS: INSECAM



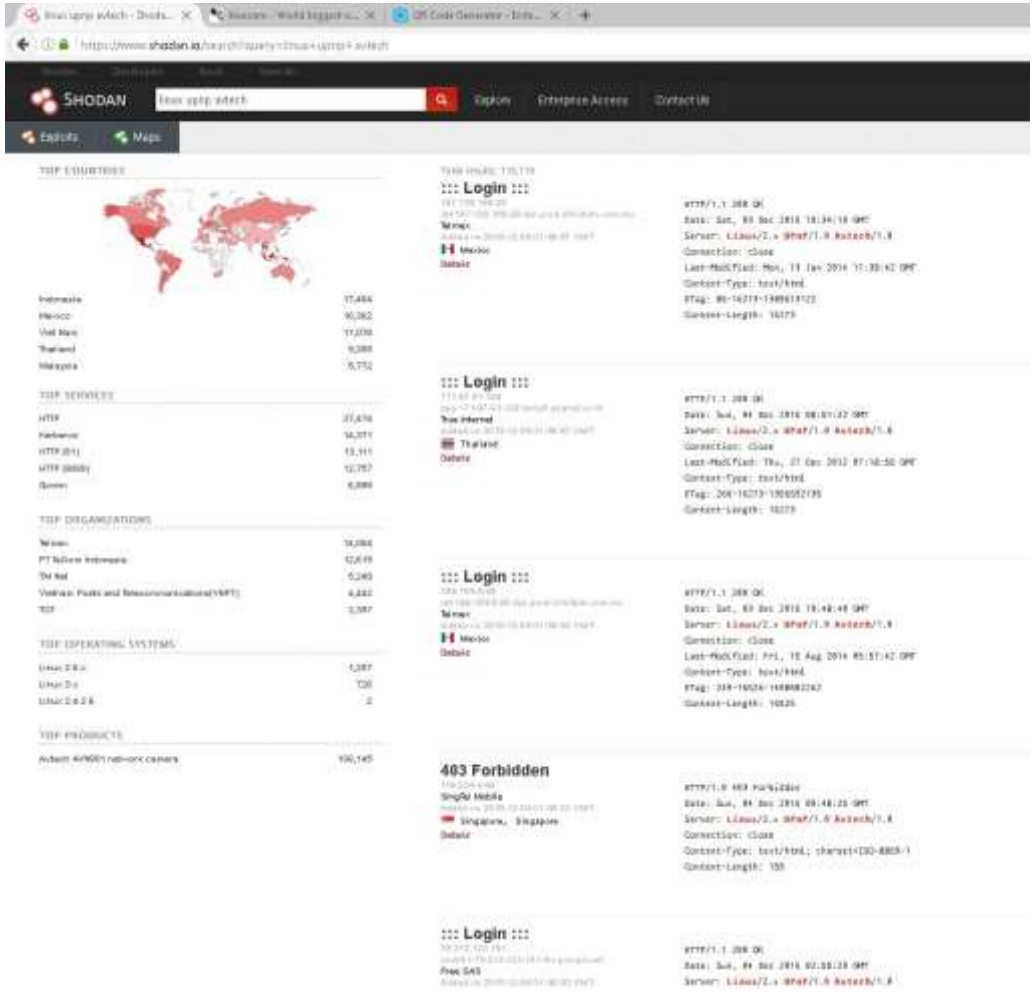
BEISPIEL IP-KAMERAS: INSECAM



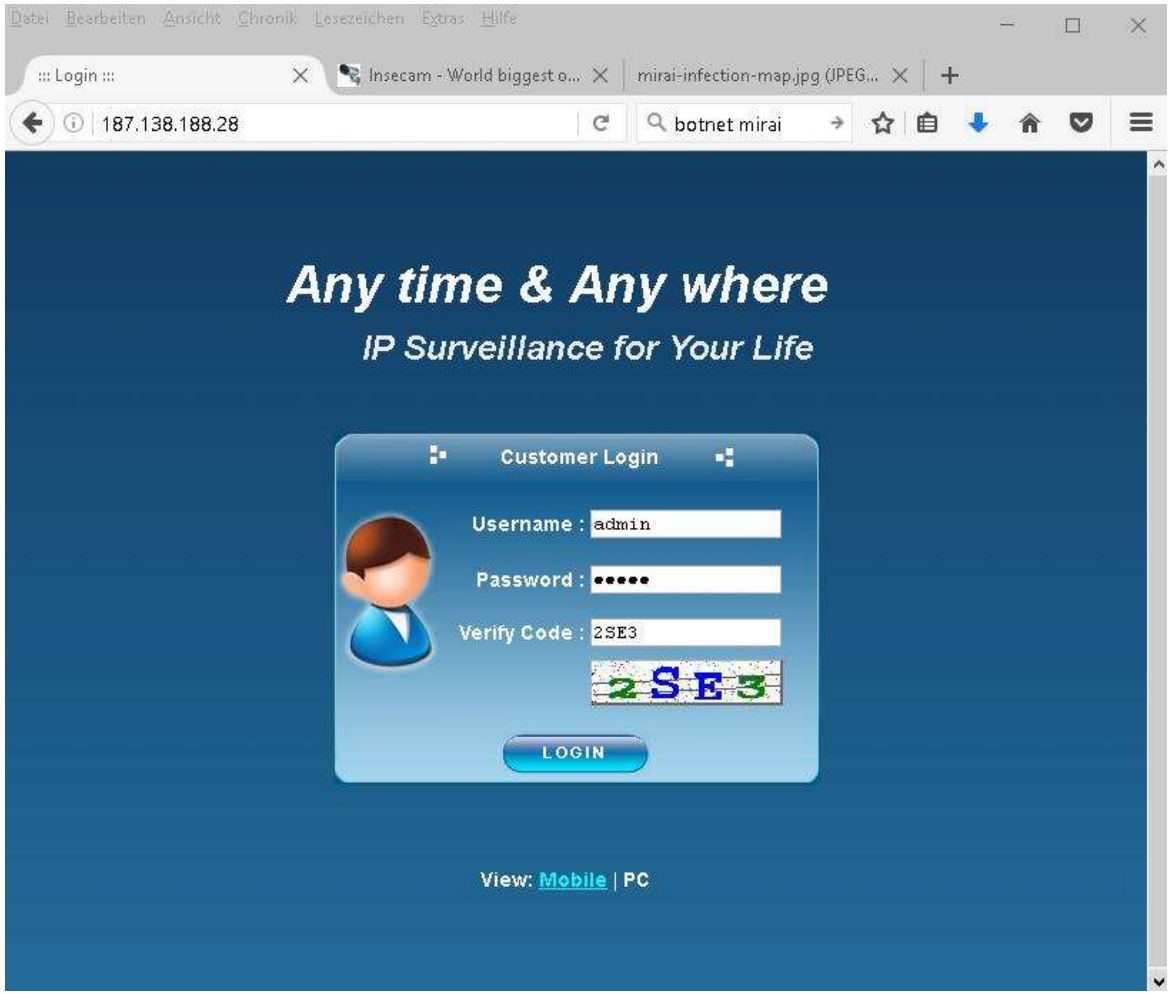
BEISPIEL IP-KAMERAS: SHODAN



BEISPIEL IP-KAMERAS: SHODAN

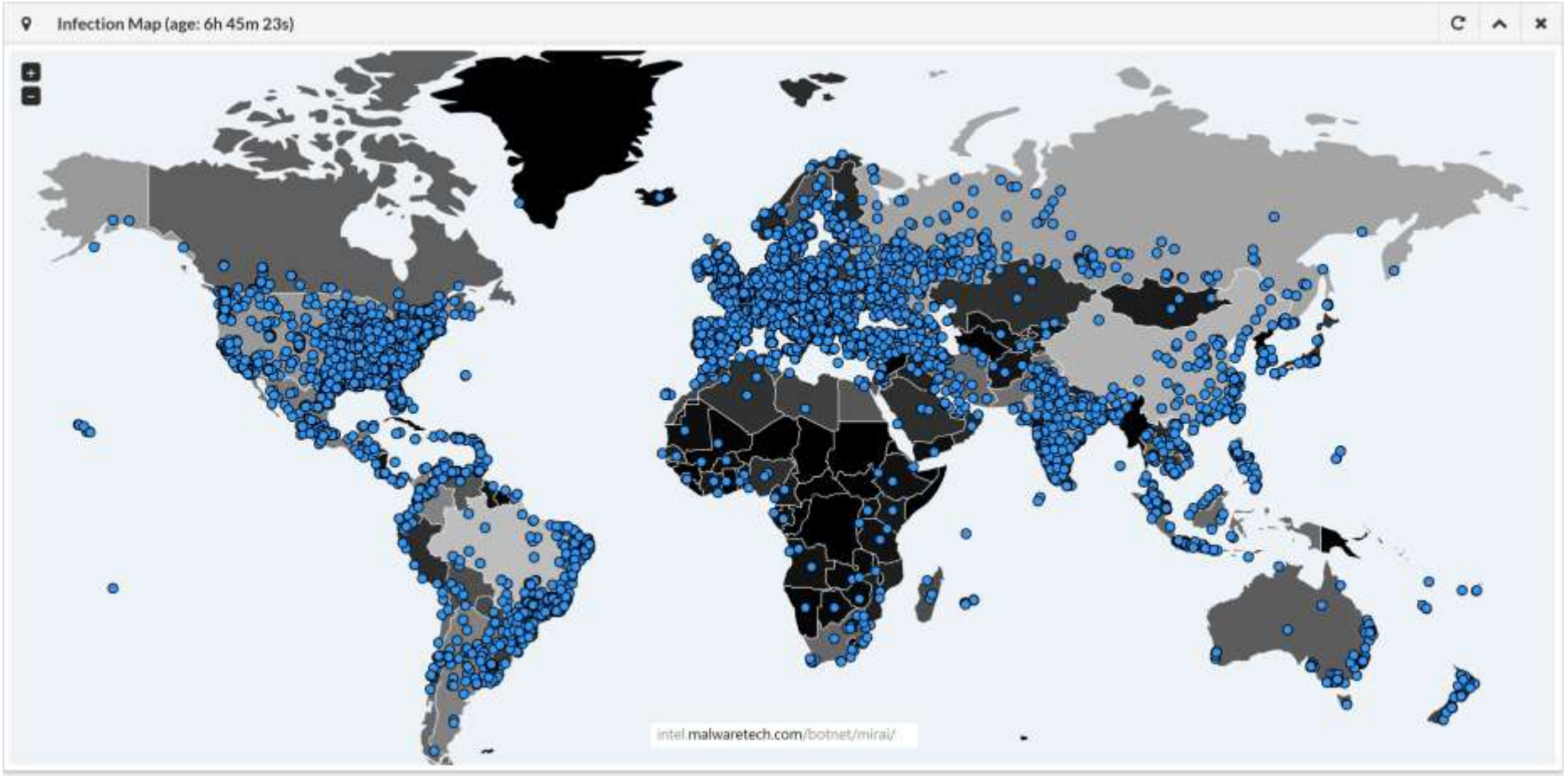


BEISPIEL IP-KAMERAS: SHODAN

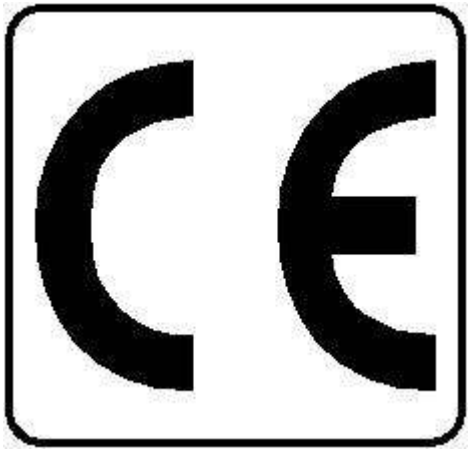


BEISPIEL IP-KAMERAS: SHODAN

GAR NICHT SMART: IOT-BOTNETZE WIE MIRAI

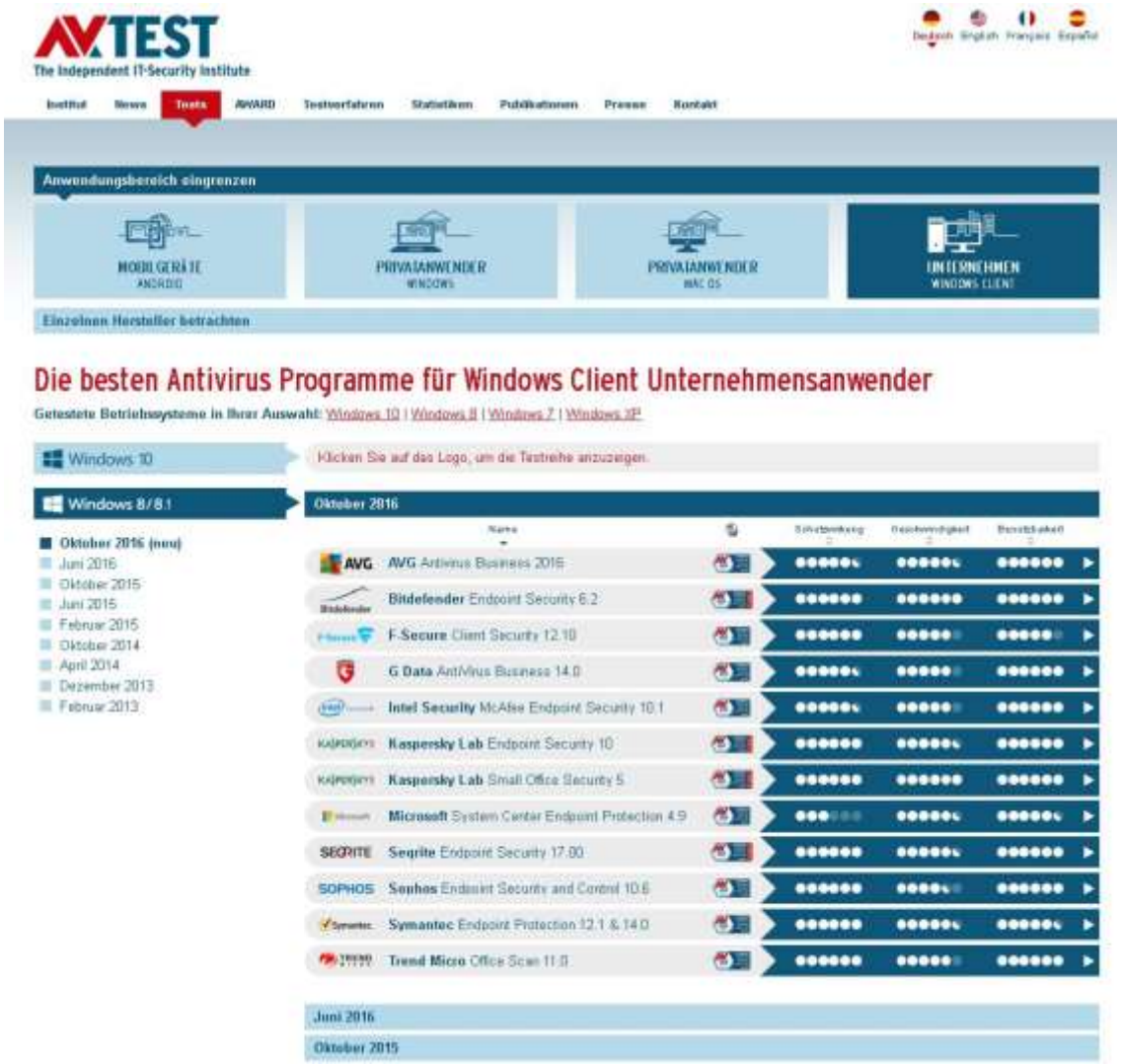


ZERTIFIZIERTE IT-SICHERHEIT?



ZERTIFIZIERTE SICHERHEIT „MADE IN GERMANY“

ALLE ERGEBNISSE GRATIS BEI AV-TEST ONLINE



@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?