Nach Installation waren nachstehende Software Programme auf dem Rechner

PC regclean
Media encoder
Re-markt
V-Raskahne
Web s security scanner
Any protect
My PC Banking
Sync Folder
New Player
Speed Up My PC
HQ total
Lolli pop
Windows 7 Reiniger

+ 10 weitere Programme

Gefährliches Internet


Anzeige
Google-Anzeigen
Entfernen von Trojaner
Geldanlage Schweiz - 12%
Antivirus 2014 Kostenlos
Telefonanlage der Zukunft
Kostenlose Registrierung
Antivirus Download
Antivirus Vergleich 2014
Norton™ AntiVirus 2014
norton.com
Neueste Norton™ Antivirus Download v. d. offiziellen Website!


Amazon-Angebote zu Spam software Liste
Ähnliche Suchen
Spam Block Software
Software Inventory
Scheduling Software
Spam Filter
Anti Spam Exchange
Email Filter Software
Software Help Desk
Software programs
Management Software
Free Billing Software
Open Source Software
System Software


Heise-Foren: Einloggen | Registrieren
heise online
Software suchen
congstar Allnet Flat S
Die günstige All-Net Flat in bester D-Netz-Qualität - nur 19,99 €*
Kostenloses Girokonto
COMMERZBANK
50 Euro Startguthaben und 50 Euro bei Nichtgefallen.*
Nur bei BASE:
Samsung Galaxy S4 mit BASE all-in. Jetzt mit Online-Vorteil 120 € sparen.
Software Verzeichnis
im Software-Verzeichnis
suchen
Erweiterte Suche
27.943 Programme | 1142 Webdienste | 144 E-Books
Sie beobachten 0 Programme
Alle Systeme
Windows
Apple
Linux
Smartphones
Alle Rubriken
Audio & Video
Foto & Grafik
Freizeit & Hobby
Handy, Fax & Co.
Internet
Browser
Sie sind hier: Download > Neuzugänge > Internet > E-Mail > Spam-Filter
Alle
Neuzugänge
Updates
Top-100
Bestbewertet
Themen-Specials
Kauf-Software
Filtern:
100 Einträge
Software
Webdienste
E-Books
kommerziell
Demo
Shareware
werbefinanziert
kostenlos
Open Source
NOKIA LUMIA
NOKIA LUMIA 925


F-Secure
Schutz des Unersetzlichen
PRODUKTE
Internet Security
Anti-Virus
Anti-Virus for Mac
Mobile Security
Online Backup
Child Safe
KOSTENLOSE TOOLS
Online Scanner
Health Check
Anti-Theft
SUPPORT
Online Support
Knowledge Base
Community
Downloads
Kontakt zum Support
KONTAKT
Folgen Sie uns auf
Facebook
Begleiten Sie uns auf
Twitter
Safe and Savvy Blog
INFORMATIONEN
Impressum
Gesetzliche
Bestimmungen
Datenschutzbestimmungen
Lizenzbestimmungen
ANDERE SITES
F-SECURE FÜR UNTERNEHMEN
Produkte
Referenzen
Partner
F-SECURE FÜR NETZBETREIBER
Werden Sie Partner
SPA
Erfolgsgeschichten
F-SECURE LABS
Labs-Blog
Probe einsenden
Malware-Definitionen
Beta-Programm

Exchange Server Toolbox v5.0

Anti-Spam & -Virus, Backup und Regelsystem für den Exchange Server

Windows Server 2012 Certified

Lizenz kaufen

ab 89,95 €

30 Tage testen

kostenlos

News

20.03.2014
Exchange Server Toolbox V5.0.1 - Volle Unterstützung für Exchange Server 2013 Service Pack 1.

20.03.2014
SEPA-Transfer 8.1.8 - Die Konvertierung von Kto.-Nr./BLZ nach IBAN/BIC ist nun umkehrbar.

14.03.2014
TreeSize Professional V6.0.3 wurde mit diversen kleineren Verbesserungen und Fixes veröffentlicht.

11.03.2014
TreeSize Free V3.0 mit neuem Spalten-Modus und verbesserter Performance wurde veröffentlicht.

28.02.2014
Exchange Server Toolbox

Spam – Ärgernis und Zeitfresser. Spam Blocker helfen!

Spam ist ein alltägliches Ärgernis. Keine Branche bleibt von den unerwünschten E-Mails verschont. Eine **Anti Spam-Lösung** ist aus verschiedenen Gründen anzuraten:

- **Spam kostet Zeit!** Manuelles Aussortieren von Spam-Mails hält Ihre Mitarbeiter effektiv von der Arbeit ab.
- **Spam frisst Speicherplatz!** Backups Ihrer E-Mail-Konten werden durch Spam aufgebläht.
- **Spam ist ein Sicherheitsrisiko!** Spam E-Mails enthalten oft Schadsoftware.

Eine weitere spambedingte Gefahr: Wird eine empfangene E-Mail durch **lokale Spamfilter** fälschlich als Spam eingestuft und lediglich in den Spam-Ordner verschoben, so gilt sie rechtlich dennoch als zugestellt. Beispielsweise darf eine nichtbezahlte Rechnung auch dann angemahnt werden, wenn sie unentdeckt im Spam-Ordner lag.

Wird eine E-Mail jedoch bereits durch den **Server als Spam abgelehnt** (ab Exchange Server 2007 möglich), wird der Empfänger benachrichtigt und kann Ihnen die Nachricht noch einmal auf anderem Wege zustellen. Auch muss eine abgewiesene E-Mail nicht mit der geschäftlichen Korrespondenz archiviert werden – kurz: Ein **guter Spamfilter** ist daher auch aus rechtlicher Sicht eine Notwendigkeit.

Welcher Exchange Spam Filter ist der richtige?

Die Exchange Server Toolbox nutzt den effektiven Spam-Filter **SpamAssassin**. Der aus Unix bekannte **Spam-Blocker** kommt bei namhaften Providern zum Einsatz und wurde von JAM Software nach Windows portiert. SpamAssassin für Exchange kann ohne langwierige Anpassung verwendet werden und lernt im Laufe der Zeit selbsttätig – eine **ideale Anti-Spam-Lösung**.

zurück

Download | Plugins/Add-ons | Support | Impressum

Spamihilator

... entfernt mehr als 98% der Spam-Nachrichten bereits beim Herunterladen Ihrer E-Mails!

Herunterladen **kostenlos!**
Windows (32-Bit oder 64-Bit)

Was ist Spamihilator?

Spamihilator schaltet sich zwischen Ihre E-Mail-Software und das Internet und überprüft jede eingehende E-Mail auf Spam. Überflüssige Werbenachrichten (Spam, Junk) werden herausgefiltert. Die Filterung läuft dabei vollständig im Hintergrund ab. Spamihilator nutzt eine Reihe verschiedener Filter, um eine bestmögliche Erkennungsrate zu erreichen. Das Programm ist konfigurierbar und kann durch Plugins erweitert werden. **Laden Sie Spamihilator noch heute kostenlos herunter!**

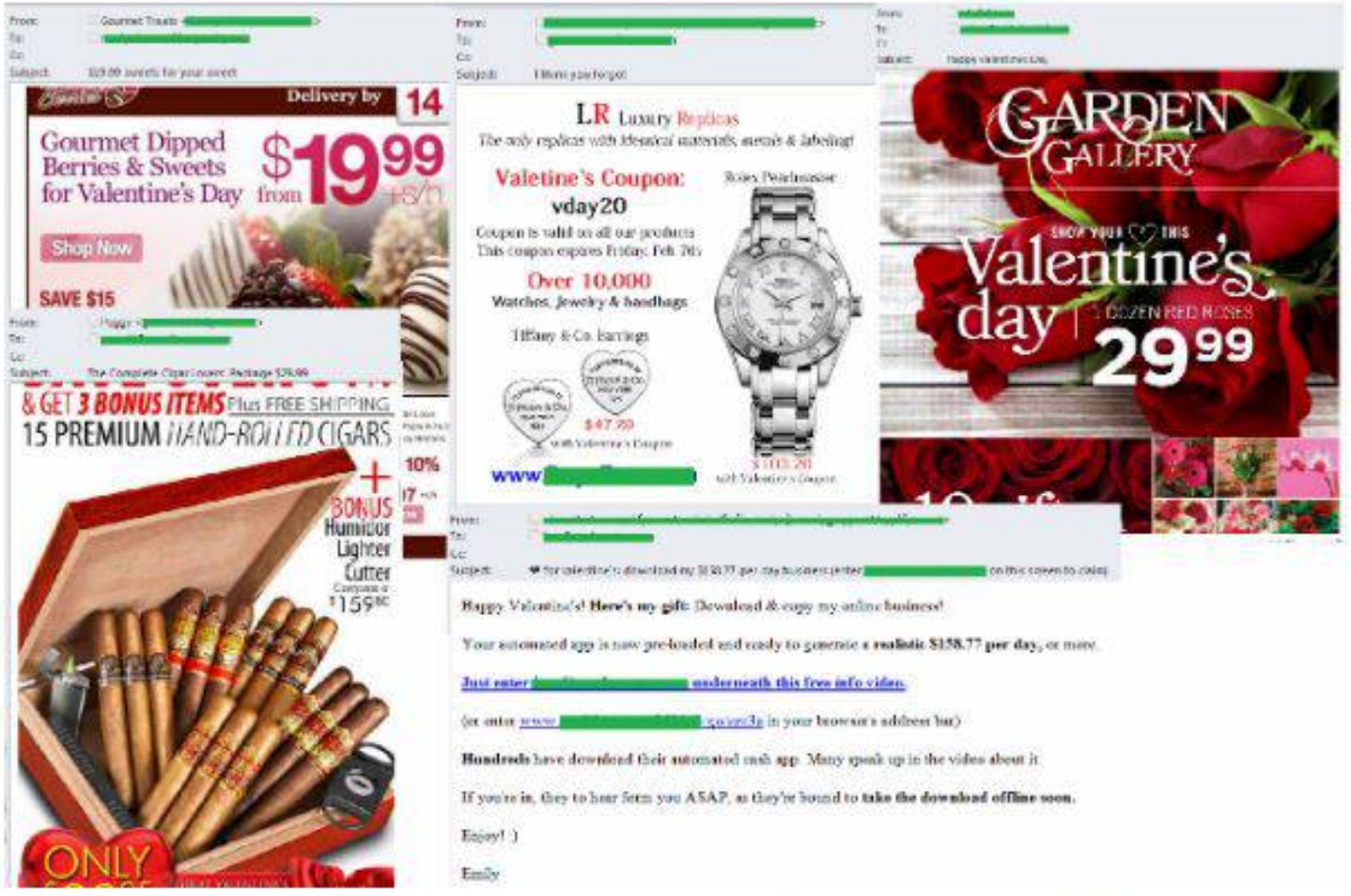
weiterlesen ...

Spam-Erkennung

Ankündigungen

Feiertags-Spam

Im englischsprachigen Spam mit Bezug auf den Valentinstag registrierten wir Versendungen mit Werbung für gefälschte Markenware sowie Angebote über Blumen und erlesenes Naschwerk. Dabei kamen die Werbemails in festtäglicher Aufmachung daher. Zudem entdeckten wir einen betrügerischen Brief mit dem Angebot, eine große Geldsumme mit Hilfe einer speziellen App zu verdienen, die als Valentinsgeschenk versendet wurde.



Wir gehen davon aus, dass die Spammer auch im März verschiedene Feiertage (z.B. den St. Patrick's Day) zum Anlass für ihre unerwünschten Versendungen mit Werbung für alle nur erdenklichen Waren und Dienstleistungen nehmen werden.

Wiederherstellung des Sehvermögens

Im englischsprachigen Internet bewarben die Spammer aktiv Laserbehandlungen der Augen zur Verbesserung der Sehkraft, die sie teilweise mit erheblichen Rabatten oder sogar kostenlos durchzuführen versprachen. Der Inhalt der Mails einer solchen Versendung bestand aus einem Werbe-Flyer mit einem anklickbaren Link-Feld, das einen nach einer Reihe von Redirects auf eine der Spammer-Seiten mit Angeboten für Laser-Augenbehandlungen führte, aber auch für andere Waren und Dienstleistungen. Normalerweise wurde in der Mail der Name der beworbenen Klinik genannt, die der interessierte Anwender, wenn gewünscht, mit Hilfe einer Suchmaschine finden könnte. Um den Empfänger zu überzeugen, fanden sich in einigen Mitteilungen Danksagungen zufriedener Patienten.

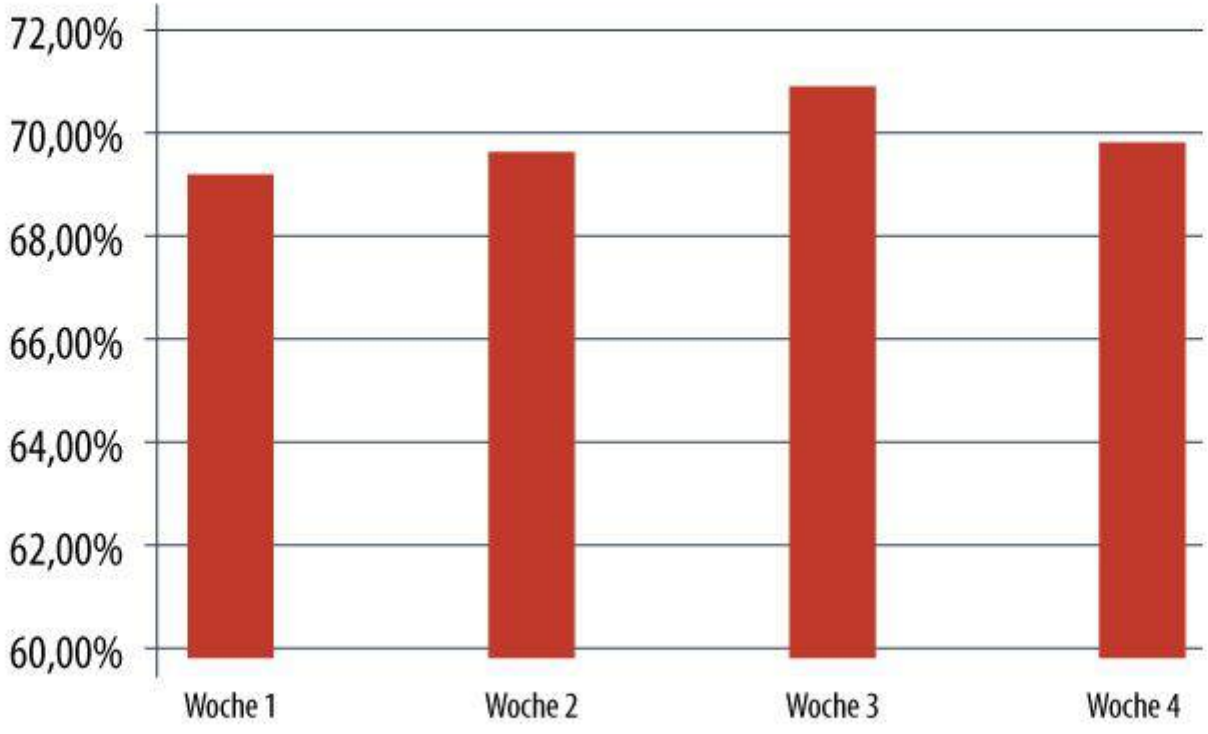
Refill-Patronen

Ein anderes Thema im Spam war die Werbung für Refill-Toner bzw. Tintenpatronen für Drucker und Kopiergeräte. Innerhalb der letzten zwei Jahre hat die Spammenge mit derartigen Angeboten deutlich zugenommen. Solche Mitteilungen registrierten wir in unterschiedlichen Sprachen, doch Art und Aufmachung der Versendungen waren im Großen und Ganzen gleich.

Die Versendungen in englischer, schwedischer und anderen Sprachen enthielten im Wesentlichen nur Angebote für Druckerpatronen. Dabei wurde in der Werbung gleich auf die vorhandenen Druckermodelle und die Preise für das Auffüllen der Patronen hingewiesen. In einigen Mitteilungen wurde die Aufmerksamkeit des Empfängers auf Rabattmarken und kurzfristige Promo-Aktionen gelenkt. Und in einer Versendung rühmte sich ein gewisser Manager aus China, in dessen Namen die Mails verschickt worden waren, der erfolgreichen Teilnahme seines Unternehmens an einer internationalen Fachmesse in Deutschland. Um den Leser von der Echtheit des Schreibens zu überzeugen, war an das Schreiben ein Foto von der Messe angehängt, verbunden mit der Bitte, benötigte Tinte unbedingt bei ihm zu bestellen.

Statistik

Spam-Anteil im E-Mail-Traffic



Spam-Anteil im E-Mail-Traffic

Der Spam-Anteil im E-Mail-Traffic hat sich im Laufe des Monats praktisch nicht verändert, abgesehen von einer geringen Zunahme in der dritten Woche des Monats. Der durchschnittliche Spam-Anteil betrug im Februar 69,9%.

Spam-Herkunftsländer

Im Februar 2014 sah die Liste der Länder, die Spam in die ganze Welt versenden, folgendermaßen aus:

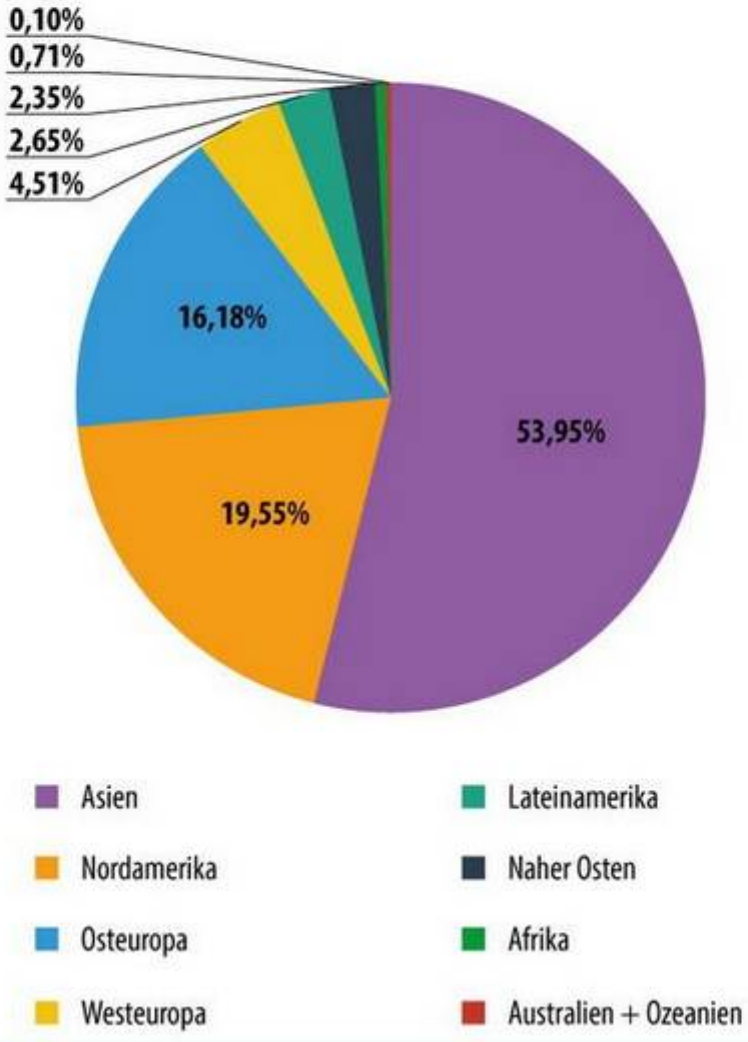
Spam-Herkunftsländer weltweit

Den ersten Platz belegte wieder einmal China (23%). Im Vormonat lag dieses Land auf Position zwei, doch eine Steigerung der versendeten Spam-Menge um 7 Prozentpunkte sicherte China erneut die Führungsposition. Es folgen die USA mit 19,1%. Innerhalb des vergangenen Monats verlor der Spitzenreiter aus dem Januar 2,8 Prozentpunkte und belegt daher nun die zweite Position. Ebenfalls zum Führungstrio gehört Südkorea (12,8%). Der Anteil des aus diesem Land versendeten

Ein Anstieg des Spam-Anteils um 0,5 Prozentpunkte war auch in der Ukraine (2,3%) und in Vietnam (1,8%) zu beobachten. Während das erstgenannte Land allerdings nur eine geringe Veränderung in der Liste bewirkte (die Ukraine stieg von Position 8 auf Platz 7), so legte Vietnam gleich ganze acht Zähler zu und war damit unter den ersten Zehn.

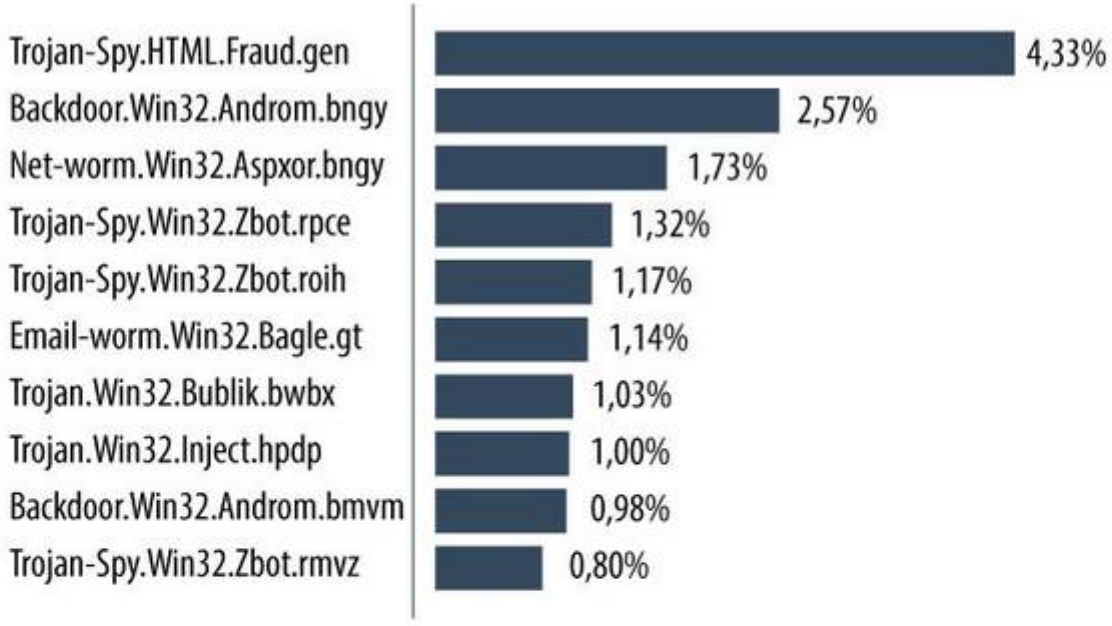
Abgeschlossen werden die TOP 10 nach den Ergebnissen des Monats von Indien, mit einem Wert von 1,6%. Die Werte von Großbritannien und Deutschland sind mit 1,5% und 1,4% respektive nur wenig geringer.

Italien (1%) hingegen rutschte um sieben Positionen ab und ist damit nicht mehr in den TOP 10 vertreten. Der Anteil des versendeten Spams ging hier um mehr als einen Prozentpunkt zurück. Ein Rückgang wurde auch in Spanien (0,8%) und Argentinien (0,7%) registriert. Spanien ist damit nicht mehr unter den ersten 10, obgleich es noch im Vormonat den 6. Platz belegte.



Schädliche Anhänge

Im Februar setzten sich die TOP 10 der via E-Mail verbreiteten Schadprogramme folgendermaßen zusammen:



Den ersten Platz belegt wie schon seit Monaten der Schädling Trojan-Spy.HTML.Fraud.gen. Bei diesem Schadprogramm handelt es sich um eine gefälschte HTML-Seite, die sich via E-Mail getarnt als wichtige Mitteilung von großen Banken, Internet-Shops, Software-Herstellern usw. verbreitet.

Auf den Positionen zwei und neun befinden sich Backdoor.Win32.Androm.bngy und Backdoor.Win32.Androm.bmvm. Die Schädlinge der Familie Andromeda sind Backdoors, die es Cyberkriminellen ermöglichen, einen befallenen Computer verborgen zu steuern. Häufig werden mit solchen Programmen infizierte Computer an ein Botnetz angegliedert.

Platz drei belegt der Netzwurm Asprox. Er infiziert automatisch Websites, lädt und startet andere Software, sammelt wertvolle Informationen auf dem Computer, wie etwa gespeicherte Passwörter, Zugangsdaten zu E-Mail und FTP-Accounts.

Die Ränge vier und fünf besetzen Trojan-Spy.Win32.Zbot.rpce und Trojan-Spy.Win32.Zbot.rpce. Zbot - Trojaner, die auf den Diebstahl von vertraulichen Daten spezialisiert sind. Wir erinnern daran, dass dieser Schädling zudem in der Lage ist, Cryptolocker zu installieren, ein Schadprogramm, das Geld für die Dechiffrierung von Anwenderdaten fordert.

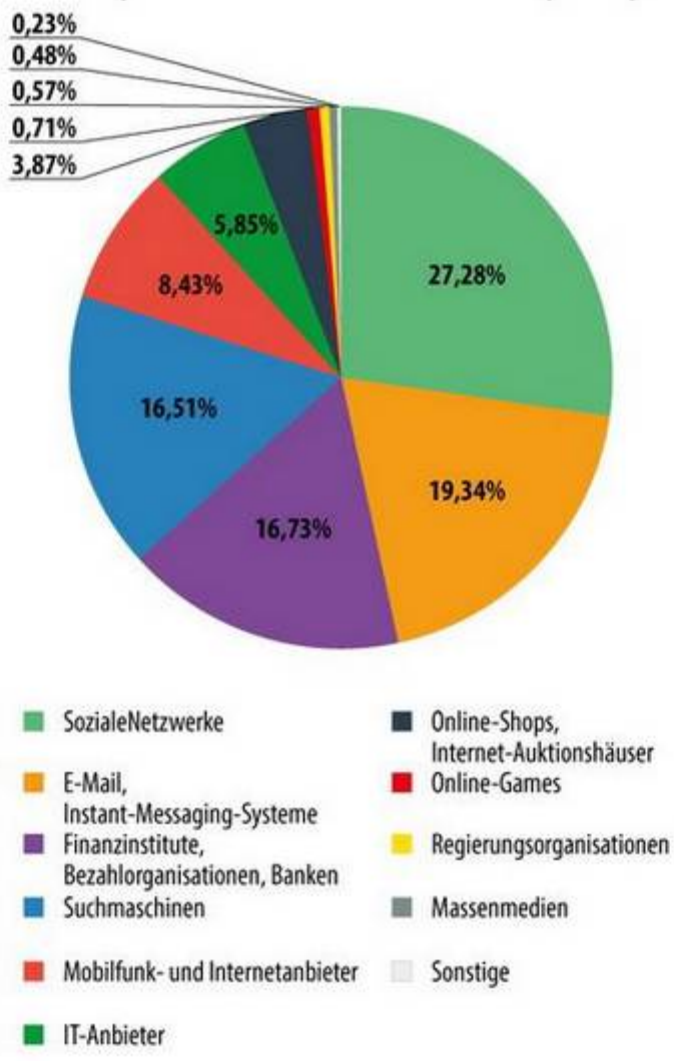
Es folgt Email-Worm.Win32.Bagle.gt, ein E-Mail-Wurm, der sich selbst an alle auf einem infizierten Computer gefundenen E-Mail-Adressen versendet. Zudem ist der Wurm in der Lage, Daten aus dem Internet für den Anwender unbemerkt herunterzuladen. Für den Versand der infizierten Mitteilungen verwendet Email-Worm.Win32.Bagle.gt eine eigene SMTP-Bibliothek.

Position acht belegt Trojan.Win32.Inject.hpdp. Es handelt sich hierbei um einen Spion und Keylogger (Limitless Logger). Das Programm fängt Tastatureingaben, Systeminformationen, Autorisierungsdaten auf verschiedenen Websites, Passwörter von E-Mail-Clients sowie Kennwörter zu Passwortspeichern ab.

Abgeschlossen werden die TOP 10 von Trojan.Win32.Bublik.cbds, einem kleinen Trojan-Downloader, der Trojaner der Familie Zbot lädt und startet.

Phishing

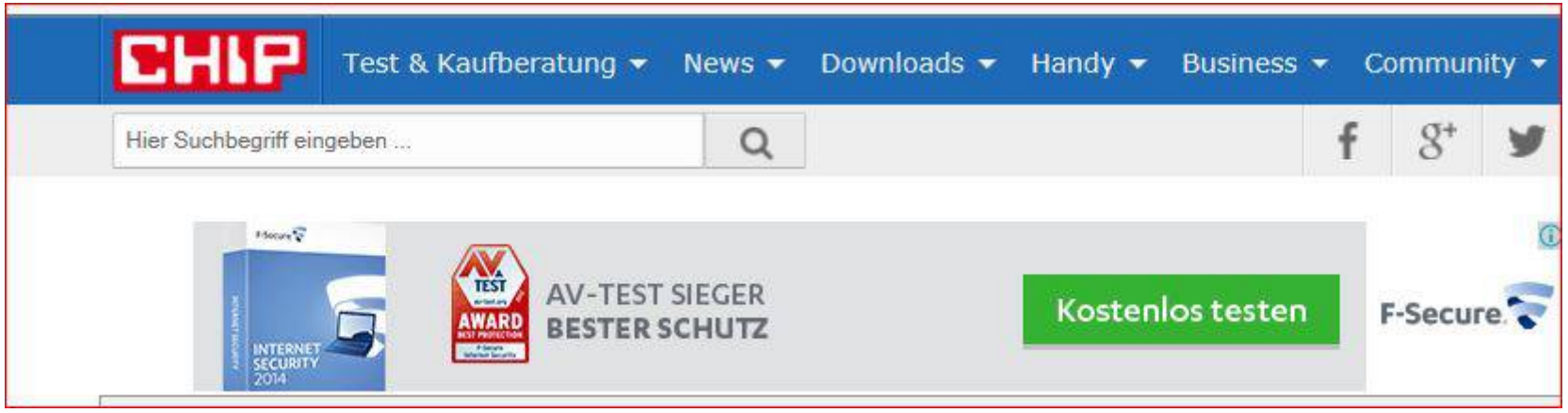
Das Rating der von Phishern angegriffenen Organisationen war im Februar keinen bedeutenden Veränderungen unterworfen.



Top 100 der am häufigsten von Phishern angegriffenen Organisationen nach Kategorien

Das Kategorien-Ranking der von Phishern angegriffenen Organisationen wird auf Grundlage der Alarme der Anti-Phishing-Komponente auf den Computern der Teilnehmer des Kaspersky Security Network (KSN) erstellt. Das Anti-Phishing-Modul erkennt alle Phishing-Links, die Anwender aufrufen, wobei die Links in einer Spam-Mitteilung oder im Internet platziert sein können.

Den ersten Platz belegen mit Abstand die sozialen Netzwerke (27,3%), die im Laufe des Monats nur 0,06 Prozentpunkte eingebüßt haben. Der Wert der E-Mail-Dienste


CHIP
Test & Kaufberatung
News
Downloads
Handy
Business
Community
Hier Suchbegriff eingeben ...
INTERNET SECURITY 2014
AV-TEST SIEGER
BESTER SCHUTZ
Kostenlos testen
F-Secure


Werbung
Download Starten
Version: 3.7
OS: Win XP/Vista/7/8
Sprache: Deutsch
BrowserSafeguard

Anzeigen zu: Spam software Liste

SPAM-Filter Gateway
www.weblink.ch/cloud-mx-**spam**-filter.html
Cloud basierter **SPAM**- & Virenfilter Unlimitiert Emailkonten
Exchange Anti-**Spam** - Kein **Spam** im Posteingang
www.jam-**software**.de/exchange/
Sicherer Spamschutz für E-Mails:
Preisgekrönte Anti **Spam**
www.**spam**fighter.com/Filter
100% Kostenlos für Outlook Testversion für Exchange
1.489 Personen folgen SPAMfighter auf Google+

Anti **Spam Software** - Schutz vor **Spam** & Phishing E-Mails
www.f-secure.com/
F-Secure IS 2014 gratis downloaden!
1.437 Personen folgen F-Secure auf Google+

spyware Spyware? - (Empfohlen) entfernen Spyware in 3 Minuten
www.windowstechies.com/spyware
Kostenlos herunterladen.

Antivirus **Software** 2014 - PC-Schutz vor Viren und Malware
www.eset.com/de/antivirus
Jetzt kostenlos für 30 Tage!
6.565 Personen folgen ESET auf Google+

Freeware **Spam**
www.registry-scan.org/
Fix Freeware **Spam** problem. Jetzt herunterladen - 30 sek.

.

1. Fotos und Texte ohne Copyright-Vermerk können frei verwendet werden.

Falsch! Das Urheberecht entsteht automatisch mit Vollendung des Werkes, d.h. mit Betätigen des Auslösers der Kamera bzw. mit Schreiben des Textes. Es sind keinerlei Formalien wie Anmeldung oder Hinterlegung zu erfüllen, wie bspw. im Marken- oder Patentrecht. Allerdings schützt das Urheberrecht nicht alles, sondern grundsätzlich nur solche Werke, die eine gewisse Schöpfungshöhe erreichen. Gemeint ist damit, dass das Werk eine persönliche geistige Schöpfung eines Menschen und nicht etwa einer Maschine ist oder es sich um ein banales Werk handelt. Ob diese Bedingung erfüllt ist, entscheidet das Gesetz gänzlich unabhängig davon, ob Copyright-Vermerk am Werkstück angebracht ist oder nicht. Im Umkehrschluss heißt das: allein das Anbringen eine Copyright-Zeichens an einem Text führt nicht automatisch dazu das dieser Text urheberrechtlich geschützt ist.

Ausnahme: Fotos sind immer geschützt! Egal ob es sich um eine künstlerisch wertvolle Fotografie oder nur ein einfaches Produktfoto handelt, auf die Schöpfungshöhe kommt es bei Bildern nicht an. Daher ist ein Foto auch dann geschützt, wenn kein Copyright-Vermerk angebracht ist.

Ein falscher Klick genügt

Schon mit einem Klick auf die Werbung hat man dann unbemerkt ein Abo abgeschlossen – zumindest wird das von den Betrügern behauptet. Mithilfe des sogenannten WAP-Billing-Protokolls können sie die Kennnummer des Handys auslesen. „Und dann wird einfach über den Telekommunikationsdienstleister des Handynutzers ein Betrag abgebucht, beispielsweise 3 Euro pro Woche oder 30 Euro pro Monat“, weiß Peter Lindackers von der Verbraucherzentrale Nordrhein-Westfalen.

Die fiesen Fallen kann man vermeiden, wenn man das WAP-Billing vom Netzbetreiber sperren lässt (was aber leider nicht alle anbieten). Und wenn man vor dem Download einer App per Internet checkt, ob andere User damit reingefallen sind.

So oder so sollte man die Handy-Rechnung stets genau überprüfen – und ihr im Zweifelsfall widersprechen.

In Gratis-Apps können teure Abo-Fallen lauern

Düsseldorf. Smartphones, internetfähige Handys also, sind sehr praktisch –
und die zahllosen Zusatzprogramme alias „Apps“ erhöhen den Nutzen dieser Geräte gewaltig.

Aber Achtung: Manch kostenlose App führt zu viel Ärger. Bei den Gratis-Apps wird nämlich oft, wie man es schon vom Internet-PC kennt, Werbung eingeblendet.

Klicken Sie niemals auf so ein Werbe-Banner in einer Gratis-App! Dahinter stecken nämlich womöglich Abzocker.

Fazit

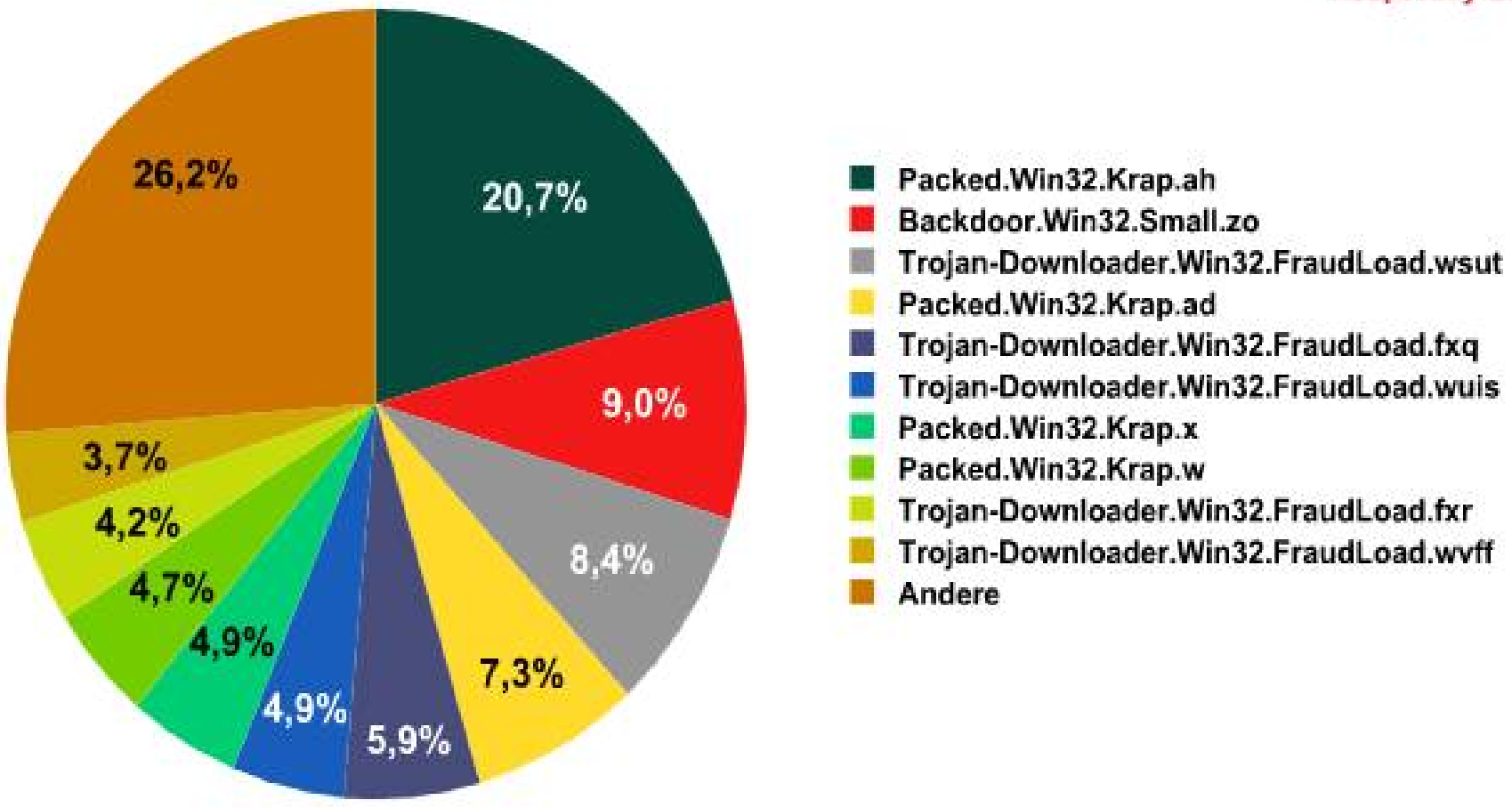
Der Spam-Anteil im weltweiten E-Mail-Traffic stieg im Februar um 4,2 Prozentpunkte und betrug dàmit 69,9%. Der Anstieg dieses Wertes gegenüber dem Januar hängt unter anderem mit der Flaute in den ersten Tagen des Jahres zusammen.

Im Februar wurden den Nutzern im Runet Festtagsangebote über Waren und Dienstleistungen zum Valentinstag gesendet. Und in den 'nigerianischen' Mails versuchten die Betrüger, die Wachsamkeit der User zu untergraben, indem sie die realen Ereignisse in der Ukraine ansprachen und sich als Touristen ausgaben, die dort mittel- und hilflos gestrandet waren.

Unter den Schreiben mit schädlichen Anhängen gab es sowohl Standard-Benachrichtigungen von bekannten sozialen Netzwerken als auch Mitteilungen zum Thema 'Bekanntschaften im Netz', deren Anteil im Zusammenhang mit dem Valentinstag im letzten Monat erhöht war.

Das Rating der von Phishern angegriffenen Organisationen wurde auch im Februar wieder von den sozialen Netzwerken angeführt. Position zwei behaupten die E-Mail-Dienste, und auf dem dritten Rang positionierten sich die Finanz- und Bezahlorganisationen, deren Wert um 1,1 Prozentpunkte zulegte.

Kaspersky Lab



Die Miniprogramme auf internetfähigen Mobilgeräten, kurz Apps genannt, sind gefährliche Daten-Verräter. Seit den jüngsten Enthüllungen von Edward Snowden dürfte das jedem klar sein.

Apps, die im App Store ähnlich beschrieben sind, sollten sich auch ähnlich verhalten. Ist das nicht der Fall, so ist die aus dem Rahmen fallende App verdächtig “, erklärt Zeller die Kernidee.

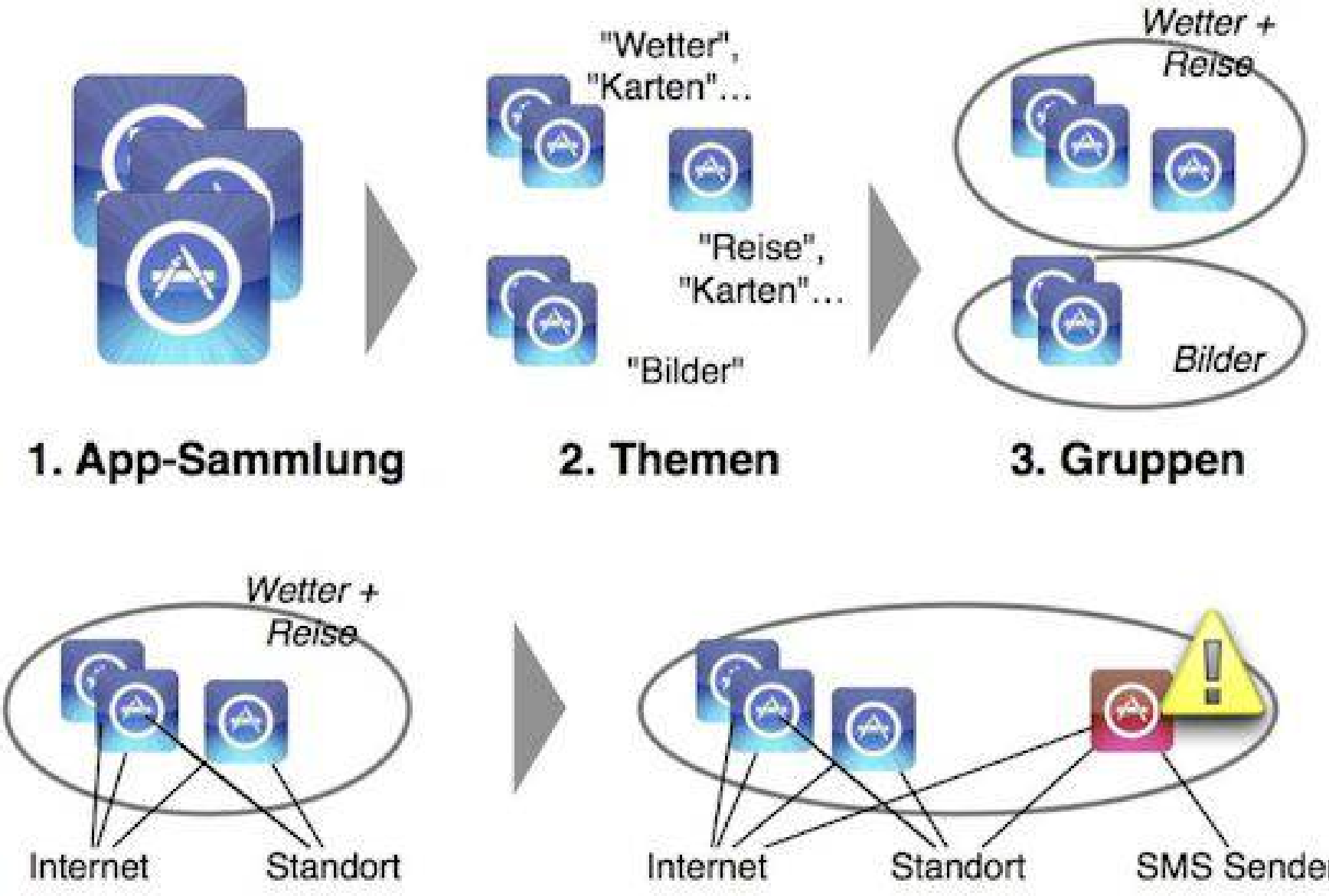
Lernen aus der Masse: Neuartige App-Angriffe durch Android-Apps in Google Play schneller erkennen

Die Miniprogramme auf internetfähigen Mobilgeräten, kurz Apps genannt, sind gefährliche Daten-Verräter. Seit den jüngsten Enthüllungen von Edward Snowden dürfte das jedem klar sein. Um diese Spione in der Hosentasche zu enttarnen, haben Saarbrücker Informatiker die Miniprogramme jetzt massenweise automatisch getestet. Sie haben dafür das tatsächliche Verhalten mit der veröffentlichten Funktionsbeschreibung der jeweiligen App verglichen. Ihr Verfahren konnten die Saarbrücker Forscher an über 22.000 Apps der Plattform „Google Play“ testen. Beim US-amerikanischen Suchmaschinenkonzern stößt das neuartige Verfahren auf großes Interesse.

”

Woher weiß ich, dass eine neu installierte App genau das auf meinem Smartphone tut?“, fragt Andreas Zeller, Professor für Softwaretechnik an der Universität des Saarlandes. Bisher habe man solche „bösartigen“ Apps entlarvt, indem man sie mit bereits bekannten Angriffsmustern verglich. „Was aber, wenn der Angriff brandneu ist?“, so Zeller.

Seine Forschergruppe beantwortet all diese Fragen mit Hilfe ihres neuartigen Verfahrens. „Apps, die im App Store ähnlich beschrieben sind, sollten sich auch ähnlich verhalten. Ist das nicht der Fall, so ist die aus dem Rahmen fallende App verdächtig “, erklärt Zeller die Kernidee.


"Wetter",
"Karten"…
"Reise",
"Karten"…
"Bilder"
Wetter +
Reise
Bilder
1. App-Sammlung
2. Themen
3. Gruppen
Wetter +
Reise
Internet
Standort
Internet
Standort
SMS Senden
4. Genutzte Dienste
5. Abweichler

Die an seinem Lehrstuhl entwickelte Software namens „Chabada” analysiert für jede App den Text, der ihre Funktionen beschreibt. Methoden der Sprachverarbeitung fassen Apps zusammen, deren Beschreibung ähnliche Themen enthält: Die Gruppe „Reise“ enthält dann alle Apps, die sich im weitesten Sinne mit Reise-Themen beschäftigen. Mittels Programmanalyse bestimmt Chabada, auf welche Android-Dienste die Apps zugreifen. Reise-Apps etwa fragen gewöhnlich die aktuelle Position ab, um dann aus dem Internet Karten nachzuladen. Eine Reise-App, die heimlich Textnachrichten versendet, macht sich so sofort verdächtig.

Auf diese Weise untersuchten die Forscher **22.521 Apps.** Mit einem eigens entwickelten Skript hatten sie im Frühling und Winter des vergangenen Jahres regelmäßig die jeweils **150 beliebtesten Apps aus den 30 Kategorien von Google Play heruntergeladen.** Diese analysierte Chabada. **Die 160 eindeutigsten Abweichler untersuchten die** Saarbrücker Informatiker genauer und stellten fest, dass Chabada **56 Prozent** der vorhandenen **Spione-Apps erkannt** hatte, ohne vorab deren Verhaltensmuster zu kennen.

Den neuartigen Ansatz dürfen die Saarbrücker Informatiker nun Ende Mai auf der renommierten International Conference on Software Engineering vorstellen. Diese wird im indischen Hyderabad stattfinden. Der Softwarekonzern Google hat Professor Zeller und seine Forscher bereits eingeladen, um Chabada auf den gesamten Google Play Store loszulassen.

Ansprechpartner:

Professor Andreas Zeller
Lehrstuhl für Softwaretechnik
Universität des Saarlandes
E-Mail: zeller@cs.uni-saarland.de
Tel.: +49 681 302 70791

SpyPhone

Mit der App "SpyPhone" nehmen Sie heimlich Videos mit dem Smartphone auf. Den Bildschirm, der normalerweise den aufgezeichneten Film zeigt, wird durch die App abgedunkelt oder mit einer vorgetäuschten Webseite (etwa einem Browser) verdeckt. Doch die App macht noch mehr: Mit ihr versetzen sich Hacker in die Lage, die über das Smartphone geführten Gespräche und ausgetauschten Nachrichten nachzuverfolgen.

Darauf haben es die Diebe abgesehen

Kreditkartendaten, Kennwörter für Online-Dienste, Adressbuch-Kontakte GPS-Koordinaten, Listen besuchter Internetseiten: Solche Daten sind für Kriminelle und aggressive Werbefirmen bares Geld wert. PC-Nutzer verhindern mit Internet-Schutzpaketen den Diebstahl ihrer privaten Informationen, aber wer per Smartphone oder Tablet online geht, bleibt in der Regel komplett ungeschützt. Und das, obwohl auch auf den meisten dieser Geräte persönliche Daten gespeichert sind.

Vorsicht vor diesen Android-Apps

Schutz vor Schädlingen

Die größte Gefahr für Android-Nutzer sind verseuchte Apps bei [Google Play] und anderen Stores: Im Test von AV Comparatives kamen mehr als 18.000 infizierte Apps zum Einsatz und alle getesteten Schutz-Apps mussten in der Lage sein, die zu erkennen und zu blockieren.


Vorsicht Diebe –
schützen Sie Ihr Weihnachtsgeld!
Berliner Polizei vor Ort
an mobilen Infoständen:

Ende