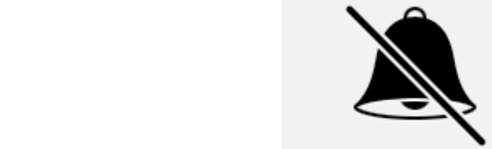
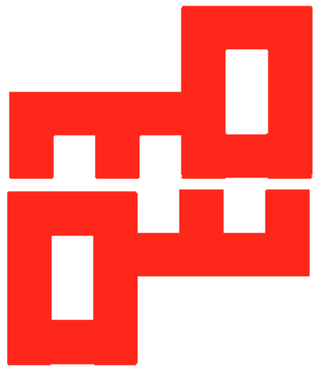



CRYPTO
PARTY



30


fachschaft
informatik

Was bisher geschah…

Facebook

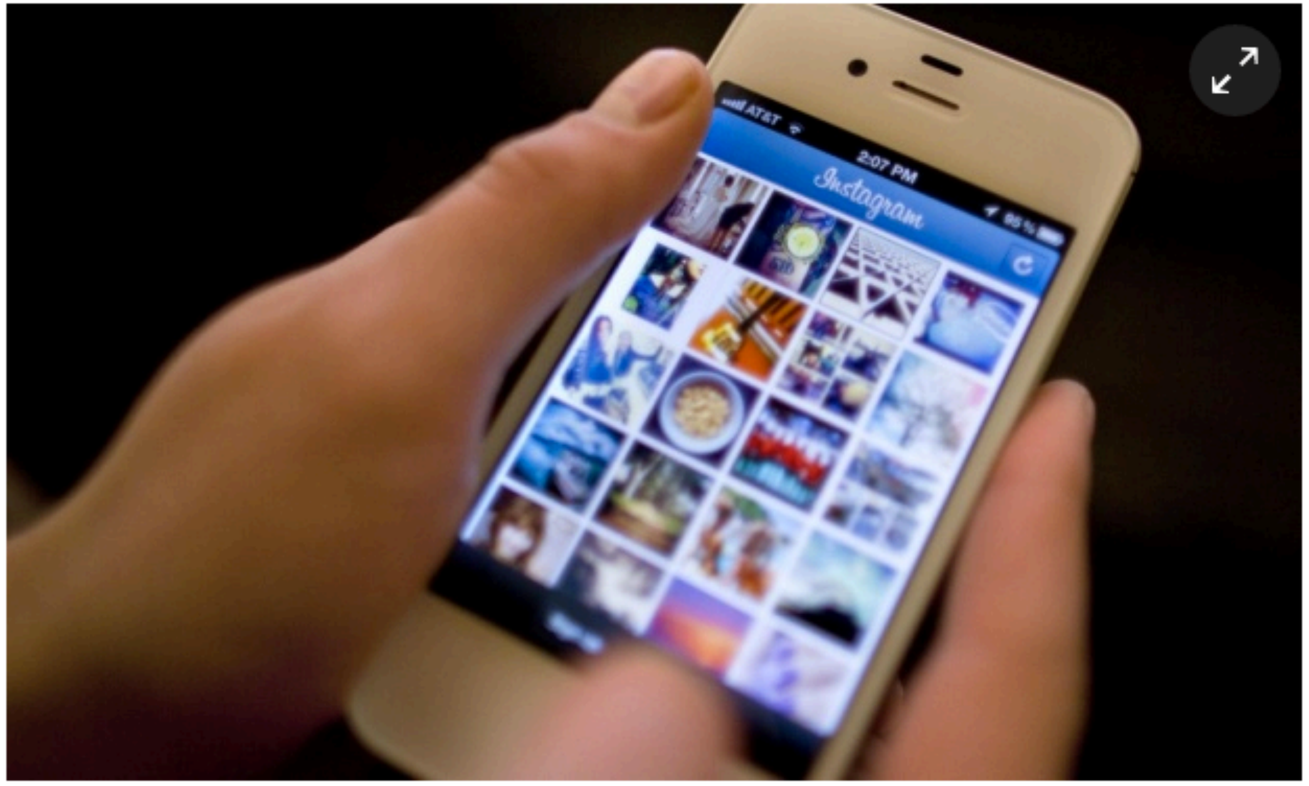
Facebook not hacked: server error takes social network offline

Facebook, Tinder, Instagram and others were unavailable for 40 minutes after an apparent outage at Facebook's HQ cascaded to other networks

Alex Hern and Samuel Gibbs

Tuesday 27 January 2015
07.33 GMT

Comments
132



Facebook
First thoughts

Facebook's outage exposes our digital fragility

Simon Jenkins

Today's Facebook suspension shows how vulnerable digital information is – penetrable by hackers, governments or subject to random failures

Tuesday 27 January 2015
10.57 GMT

Comments
130

'Any electronic device is subject to failure. Any locked door invites trespass.' Photograph: Alamy

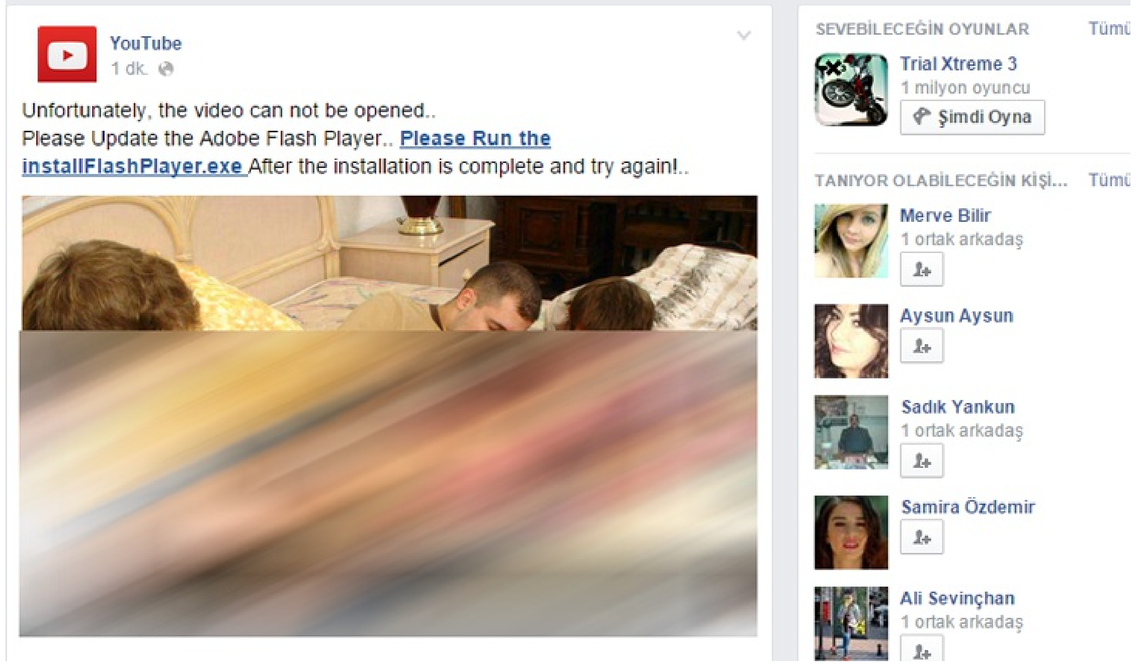
OMG Facebook is down! Down too went Instagram. It was just for an hour this morning, but the tweets screamed "Do I have to talk to someone real?"

In a manner of speaking, yes. Despite the hackers of Lizard Squad claiming credit, it is now clear that an outage at Facebook's HQ was responsible. But the confusion was understandable after Lizard Squad had in recent weeks variously hit Sony executives and Microsoft products. It brought down PlayStation and Xbox platforms over Christmas.

The Hacker News™
Security in a serious way

Malware Poses as Flash Update Infects 110,000 Facebook Users within 2 Days

Friday, January 30, 2015 Wang Wei

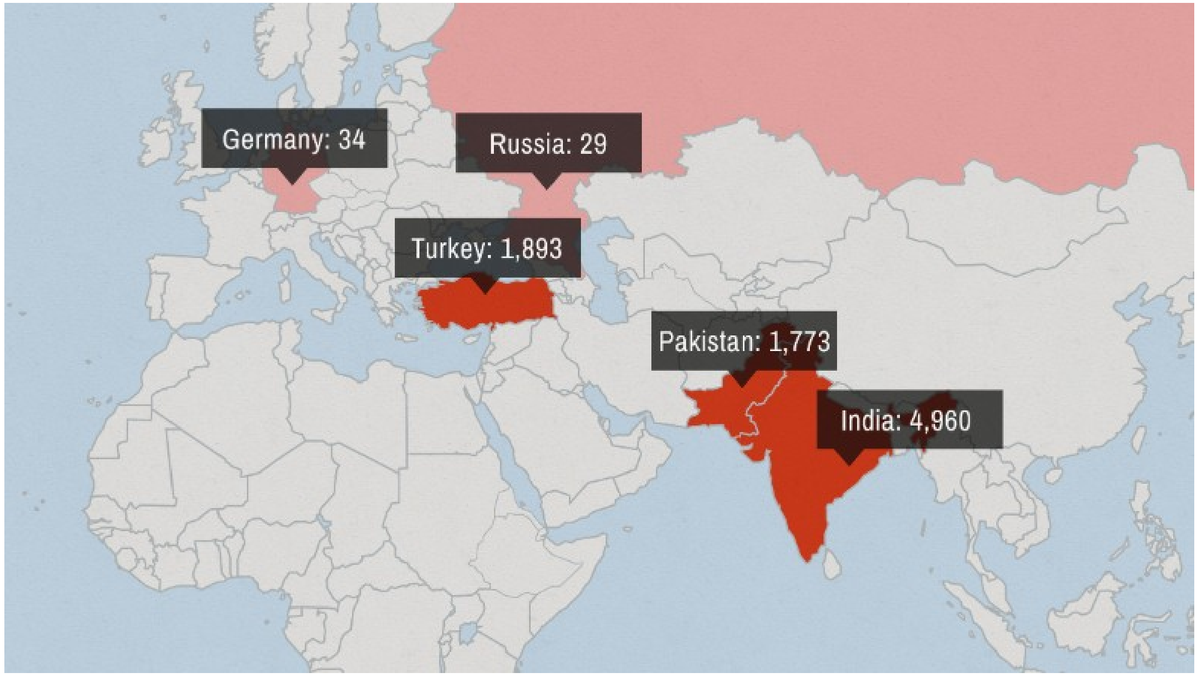


Facebook users just Beware!! Don't click any porn links on Facebook. Foremost reason is that you have thousands of good porn sites out there, but there's an extra good reason right now.

Rogue pornography links on the world's most popular social network have reportedly ***infected over 110,000 Facebook users with a malware Trojan*** in just two days and it is still on the rise, a security researcher

The 3 places where Facebook censors you the most

By Jose Pagliery @Jose_Pagliery



In certain countries, Facebook is faced with a draconian dilemma: censor your posts or the company gets banned.

Most Popular


CBS staffers refute Bill O'Reilly's 'war zone' story


Upgrading from Windows 7 or 8? You'll love Windows 10

America Inc. warns of turbulence ahead

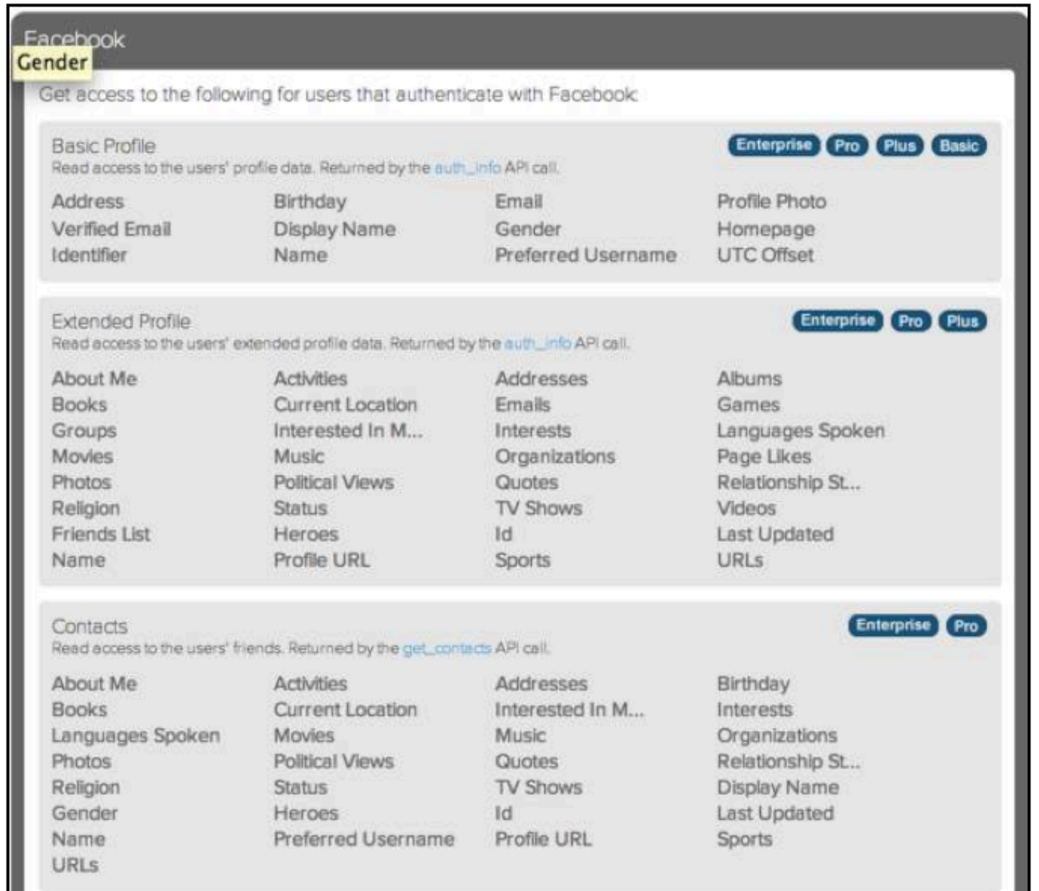
"Pieces of content" blocked by Facebook

India	4,960	United Kingdom	9
Turkey	1,893	Australia	7
Pakistan	1,773	Saudi Arabia	7
Germany	34	Thailand	5
Russia	29	Italy	3
France	22	Kuwait	1
Austria	15	United Arab Emirates	1
Israel	15		

SOURCE: FACEBOOK

What is exposed about you and your friends when you login with Facebook

By Cory Doctorow at 8:00 pm Mon, Jan 27, 2014



Facebook

Gender

Get access to the following for users that authenticate with Facebook:

Basic Profile

Enterprise Pro Plus Basic

Read access to the users' profile data. Returned by the auth_info API call.

Address	Birthday	Email	Profile Photo
Verified Email	Display Name	Gender	Homepage
Identifier	Name	Preferred Username	UTC Offset

Extended Profile

Enterprise Pro Plus

Read access to the users' extended profile data. Returned by the auth_info API call.

About Me	Activities	Addresses	Albums
Books	Current Location	Emails	Games
Groups	Interested In M...	Interests	Languages Spoken
Movies	Music	Organizations	Page Likes
Photos	Political Views	Quotes	Relationship St...
Religion	Status	TV Shows	Videos
Friends List	Heroes	Id	Last Updated
Name	Profile URL	Sports	URLs

Contacts

Enterprise Pro

Read access to the users' friends. Returned by the get_contacts API call.

About Me	Activities	Addresses	Birthday
Books	Current Location	Interested In M...	Interests
Languages Spoken	Movies	Music	Organizations
Photos	Political Views	Quotes	Relationship St...
Religion	Status	TV Shows	Display Name
Gender	Heroes	Id	Last Updated
Name	Preferred Username	Profile URL	Sports
URLs			

Facebook will tag every photo ever taken of you—whether you like it or not

By Taylor Hatmaker Follow on February 07, 2015

Facebook is getting smarter at faces—a *lot* smarter. If you've uploaded photos to the social network recently, you might have noticed an upswing in just how good Facebook is getting at guessing which of your friends appear in that photo from happy hour or a baby shower last weekend.

To test out what Facebook's facial recognition algorithm has been up to lately, I decided to upload a test album of 15 photos. The photos were pictured I had recently taken of my friends, and I hadn't previously shared any of them, to eliminate the possibility that Facebook was cross-referencing the photos with images already stored on its servers.

Of my test set, Facebook identified and automatically tagged faces in eight of the photos, and seven out of eight of the tags were correct. In the one it guessed wrong (a selfie of a friend and I eating corndogs, if you must know), it tagged my face as the with the name of the other person in the picture, so that's at least half right in my book. Notably, two of the images it didn't nail were taken in dark rooms, one was blurry, and one was of a friend who just buzzed her hair and dyed her eyebrows.

Facebook

It's worth noting that I didn't ask Facebook to scan or tag these faces—the process happened automatically as I uploaded the photos from mobile. The tagging produced no delay whatsoever in the process of uploading the photo set to Facebook over Wi-Fi. It only took seconds. The automatic face scanning also prevented me from making a private test album by automatically making my photo set viewable to "people tagged" even though I'd selected the little lock icon and "only me" in the privacy settings menu.

Related News

All the ways you can hide from facial recognition
202
In real life, your face can be used to reveal and track the real you. Here's how to work around that.
January 28, 2014

Your Facebook stalking might be making you depressed
1.2k
Put down your phone and stop looking at your college boyfriend's vacation photos.
By Elizabeth Robinson — February 04, 2015

Creepy masks show what your face looks like to Facebook
2.0k
Art project's 3D masks deconstruct Facebook's facial recognition technology.
By Taylor Hatmaker — November 26, 2014

30. Januar 2015, 13:27 Neue AGB

Ex-Datenschutzbeauftragter meldet sich aus Protest bei Facebook ab

Mit Peter Schaar kann man sich schon anfreunden - nur eben nicht mehr auf Facebook. (Foto: dpa)

Peter Schaar, früherer Bundesdatenschutzbeauftragter,

https://www.facebook.com/help/delete_account

WhatsApp security bug shows private pictures to strangers

i100 BETA NOW TRENDING


1 Remembering when two students snuck into the Oscars


2 This is who would win Oscars if the public decided, not the Academy


3 The secret to making better decisions


4 This man harnesses the power of the sun to make incredible art


5 This Game of Thrones blooper reel is everything we expected and more

Christoph Lederer
@cldrr

Follow

Best way to get rid of @PlentyOfFish: upload nudity pictures :D

Your face MUST be clearly visible in your MAIN IMAGE. All images MUST contain you. Images of cartoons, celebrities, bare torsos and joke pictures will be deleted. Improve the images on your profile to get the most responses!

Set your images to private to only share them with people in a message.
UPLOADING NUDITY WILL GET YOUR ACCOUNT DELETED

23 July 2014 Last updated at 10:30 GMT

Share

New broadband users shun UK porn filters, Ofcom finds

By Joe Miller
Technology Reporter

The vast majority of new broadband customers in the UK are opting out of "child friendly" filters when prompted to install them by service providers.

Related Stories

Bomb explodes at rally in Ukraine

Shopping mall terror threat 'serious'

Oscars 2015: Birdman battles Boyhood

Maldives ex-leader Nasheed arrested

Turkey enters Syria to remove tomb

No hard feelings
The shark attack survivor who sticks up for sharks

Meal mission
Why the UK's homeless are turning to Sikhs for food

Who is 'Oscar', anyway?
All the background to the 2015 Academy Awards ceremony

'Sold out'
The fate of Japanese-Latin Americans during World War Two

Australia's chief censor redacts official website to downplay his role in censorship

By Cory Doctorow at 11:37 pm Thu, Feb 25, 2010

Australian Communications Minister Stephen Conroy -- who has been responsible for pushing through Australia's national Internet censorship program -- has been caught censoring his own website: the script that creates a tag cloud of topics covered on his site had been modified to ignore any references to his censorship initiatives. This means that visitors to his site would not have an easy means of reading the Minister's statements in support of censorship, and anyone who relied on the tag-cloud to understand the Minister's agenda would have no way of knowing he'd been involved in the censorship initiative.

It was revealed today a script within the minister's homepage deliberately removes references to internet filtering from the list.

In the function that creates the list, or "tag cloud", there is a condition that if the words "ISP filtering" appear they should be skipped and not displayed.

The discovery is unlikely to do any favours for Senator Conroy's web filtering policy, which has been criticised for its secrecy.

N E T G E A R

WLAN-Router aus der Ferne angreifbar

Über eine Schwachstelle in zahlreichen WLAN-Routern der Firma Netgear lassen sich Passwörter und Schlüssel auslesen.

Netgears Genie enthält eine Schwachstelle, über die WLAN-Schlüssel und Passwörter ausgelesen werden können. (Bild: Netgear)

Datum: 16.2.2015, 18:03

Autor: Jörg Thoma

Themen: Security, Netzwerk, Passwort, Router, Netgear, Applikationen, PC-Hardware

Teilen: 0 31 53 22

Tools: Drucken

Ein Fehler in der Weboberfläche der Konfigurationssoftware Netgear Genie lässt sich ausnutzen, um Passwörter und WLAN-Schlüssel auszulesen. Netgear Genie ist auf zahlreichen Routern der Serie WNDR installiert und kann auch zur Wartung aus der Ferne genutzt werden. Peter Adkins, der Entdecker der Schwachstelle, hatte Netgear bereits Mitte Januar 2015 informiert.

Adkins hat den Fehler in Netgears WLAN-Routern WNDR3700v4, WNR2200 und WNR2500 nachweisen können. Da die Software aber auch auf weiteren Modellen läuft, könnten auch die Router WNDR3800, WNDRMAC, WPN824N und WNDR4700 betroffen sein. Besitzern der betroffenen Geräte rät Adkins, die Fernwartungsfunktion abzuschalten und im internen Netzwerk den Zugriff nur für vertrauenswürdige Geräte zuzulassen.

WLAN-Wartung aus der Ferne

DNS HIJACK IN D-LINK ROUTERS, NO AUTHENTICATION REQUIRED

Top Stories

'Yes, Your Car Wash Is On Facebook'

February 19, 2015 , 7:47 am

Two-Factor Snafu Opened Door to JPMorgan Breach

December 24, 2014 , 10:00 am

Facebook Malware Poses as Flash Update, Infects 110K Users

January 30, 2015 , 12:34 pm

GHOST glibc Remote Code Execution Vulnerability Affects All Linux Systems

January 27, 2015 , 12:55 pm

Eric Leblond
@Regiteric

Follow

#NetNeutrality is at best in France.
Resolving piratebay.se return 127.0.0.1
when using DNS of Free Telecom.

```
eric@ice-age2:~$ host thepiratebay.se
thepiratebay.se has address 127.0.0.1
thepiratebay.se has IPv6 address ::1
eric@ice-age2:~$ host thepiratebay.se 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

thepiratebay.se has address 104.28.5.42
thepiratebay.se has address 104.28.4.42
thepiratebay.se has IPv6 address 2400:cb00:2048:1::681c:42a
thepiratebay.se has IPv6 address 2400:cb00:2048:1::681c:52a
eric@ice-age2:~$
```

```
eric@ice-age2:~$ host thepiratebay.se
thepiratebay.se has address 127.0.0.1
thepiratebay.se has IPv6 address ::1
eric@ice-age2:~$ host thepiratebay.se 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

thepiratebay.se has address 104.28.5.42
thepiratebay.se has address 104.28.4.42
thepiratebay.se has IPv6 address 2400:cb00:2048:1::681c:42a
thepiratebay.se has IPv6 address 2400:cb00:2048:1::681c:52a
eric@ice-age2:~$
```

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314-5794
(703) 299-3700

FACSIMILE TRANSMISSION COVER PAGE

DATE: 12/14/10

TO: Twitter Attn: Trust & Safety

PHONE:

TO FAX NO.: (415) 222-9958

SENDER: Vivian Ha, Assistant to Tracy McCormick

SENDER'S PHONE NO.: 703 299 3859

SENDER'S FAX NO.: 703 299 3981

NUMBER OF PAGES: 4 *Not Including Cover Page*

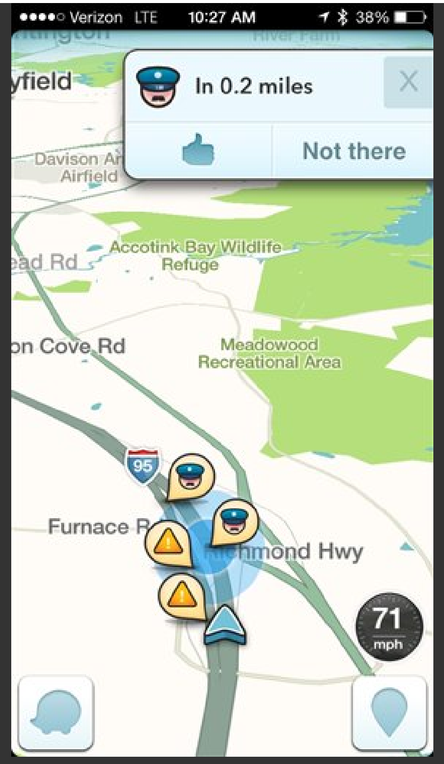
Level of Transmitted Information:

Sheriffs expand concerns about Waze mobile traffic app

Jan. 28, 2015 4:47 PM

By EILEEN SULLIVAN EST

2 photos



This image taken from the the Waze app on an iPhone, in Washington, shows police at the scene on a... Read more


BFMTV
.com
NICOLAS COMTE
SYNDICAT UNITÉ SGP POLICE

HipChat Security Notice and Password Reset

By Craig Davies | 3 weeks ago | 34 Comments

Atlassian's security team has discovered and blocked suspicious activity on the HipChat service that resulted in unauthorized access to names, usernames, email addresses, and encrypted passwords for a very small percentage (<2%) of our users. We have no evidence that any payment information was accessed.

While HipChat passwords are one-way encrypted (hashed and salted), as an added precaution we have triggered a password reset for all affected HipChat user accounts and all Atlassian services that share the same email address. If you have not received communication from us, we do not believe you were affected. However, you can **easily change your password here**. As a reminder, always avoid using simple passwords based on dictionary words and never use the same password on multiple sites or services.

We take our responsibility to protect you and your data very seriously, and we're constantly enhancing the security of our service infrastructure to keep you and your data safe. While recent events with other large services have demonstrated this type of activity is increasing, so too is our vigilance in blocking and addressing it.

If you have any questions or concerns, please contact us at **support@hipchat.com**.

DATENSCHUTZ

Sag mir, was du kaufst, und ich sag dir, wer du bist

Ein Buch hier, eine Jeans dort: Wenn wir mit der Karte zahlen, fallen Metadaten an. Die sollen anonym verwendet werden. Reichen aber, um den Käufer zu identifizieren.

VON EIKE KÜHL

29. Januar 2015 20:14 Uhr

28 Kommentare

Eine Frau zeigt ihre Kreditkarte. | © Wathiq Khuzaie /Getty Images

ARTIKEL Auf einer Seite lesen

QUELLE ZEIT ONLINE, dpa

SCHLAGWORTE Apple | Ebay | Edeka | Facebook | IP-Adresse | Jacob Appelbaum

NEU IM RESSORT

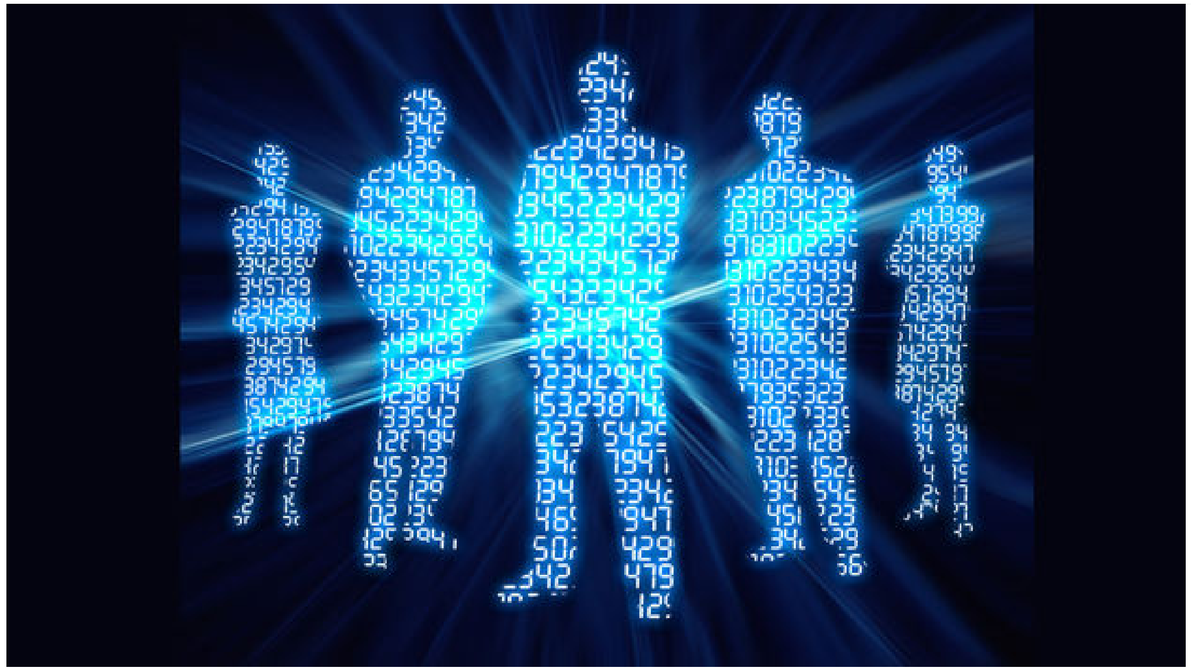
1. **RUNPEE** Die Datenbank der Pinkelpausen
2. **STÖRERHAFTUNG** Gefahrlos offene WLANs bleiben Utopie
3. **MOBILFUNK** Sieben Wege, ein Handy abzuhören
4. **LENOVO** Der Superfish ist weitverbreitet
5. **HITCHBOT** "Die Leute sollten wissen, was das Ding am Straßenrand ist"

NEU AUF ZEIT ONLINE

1. **OSCAR LIVE** Durch die Nacht in Hollywood
2. **UNGARN** Orbán-Partei Fidesz verliert Zweidrittelmehrheit
3. **SEBASTIAN EDATHY** Der Prozess nach dem Skandal
4. **UKRAINE-KONFLIKT** Anti-Maidan-Demonstranten wurden bezahlt
5. **FRANZISKA GIFFEY** Ihr Traum von Neukölln

Anonymisierte Datensätze nicht so sicher wie gedacht

30.01.15, 08:59 Mail an die Redaktion



Verräterische Daten – Foto: Fotolia

FORSCHUNG

Anonymisierte Datensätze nicht so sicher wie gedacht

Aus großen Mengen an anonymisierten Daten lassen sich laut Wissenschaftlern einfach Informationen über einzelne Personen herausfiltern.

FORSCHUNG, MIT, ANONYMITÄT, ANONYMISIERUNG

FEATURED

GRÜNE

SIM-Karten-Hack: "Regierung soll Klagen unterstützen"

EU-Innenminister wollen Internet-Inhalte löschen lassen

von Barbara Wimmer Letztes Update am 29.01.15, 15:21 shroombab Mail an Autor

Vorratsdatenspeicherung und Fluggastdatenspeicherung stehen ganz oben auf der Wunschliste der EU-Innenminister. – Foto: Bild: APA/Techt

RIGA-TREFFEN

EU-Innenminister fordern in Riga Fluggastdaten-

FEATURED

Snoopers' Charter is a step too far in counter terrorism fight

12 JANUARY, 2015 @ 3:48 PM

Liberal Democrat Justice Minister Simon Hughes has warned that introducing a Snoop Charter is a step too far in tackling terrorism.

His comments come after the Conservatives announced plans to introduce a Snooper's C if they are elected to govern following the General Election.

The charter would require internet companies to keep a record of all websites visited by e single member of the public.

9 February 2015 Last updated at 11:20 GMT

Samsung warns customers over Smart TV privacy

Samsung said personal information could be scooped up by the Smart TV

Samsung is warning customers about discussing personal information in front of their smart television set.

Related Stories

France stops Syria-bound 'jihadists'

Deadline looms for Greek reform plan

Birdman, Redmayne, Moore lead Oscars

Jerusalem mayor overpowers attacker

N Korea bans foreigners from race

Dangerous luxury

'Why I regret my years as a suntan addict'

Touch test

The blind breast cancer detectors who find 2mm tumours

All at sea

The boy forced to pilot a rickety boat across the Mediterranean

Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live--did live, from habit that became instinct--in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

Samsung smart TVs don't encrypt the voice data they collect

Samsung TVs at the International CES trade show. Credit: Martyn Williams/IDG News Service

By Lucian Constantin FOLLOW
IDG News Service | February 18, 2015

Samsung does not encrypt voice recordings that are collected and transmitted by its smart TVs to a third party service, even though the company has claimed that it uses encryption to secure consumers' personal information.

A week ago, the revelation that Samsung collects words spoken by consumers when they use the voice recognition feature in their smart TVs enraged privacy

MORE GOOD READS


How to remain (mostly) invisible online


Top malware families turn point-of-sale into point-of-theft

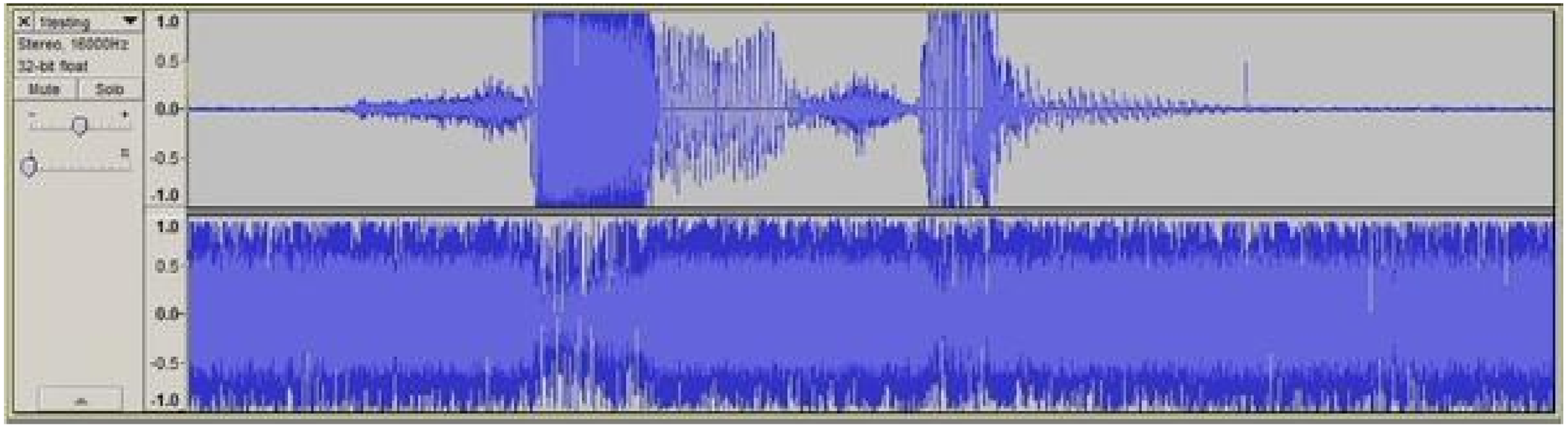

Low and no-cost ways to learn about IT security

on IDG Answers
Why would companies use a "fake" 404 page?

Ken Munro
@TheKenMunroShow

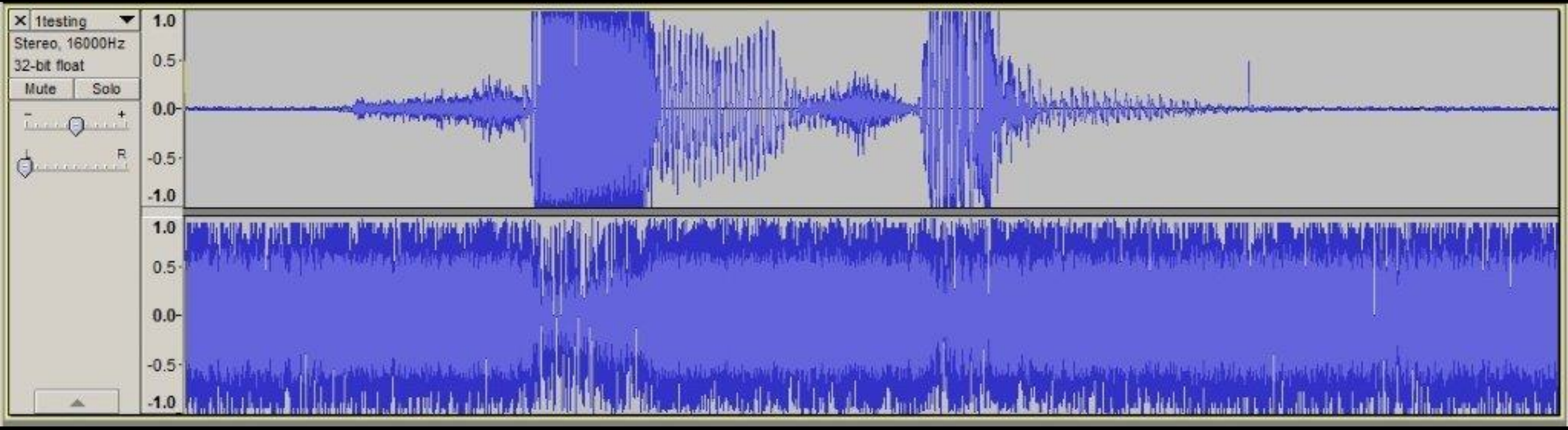
Follow

Sniffing 'Samsung' in @tautology0 's northern accent from the wire from my TV. Not encrypted in transit. Oh dear



RETWEETS
44

FAVORITES
22


1testing
Stereo, 16000Hz
32-bit float
Mute
Solo
1.0
0.5
0.0
-0.5
-1.0

Securing your business, together

HOT SECURITY TOPICS

Suffered a Security Breach?

Mobile Security

SCADA Security

Web application testing

STAR Financial Services Testing

CREST Cyber Essentials Testing

Get Free Security Socks!

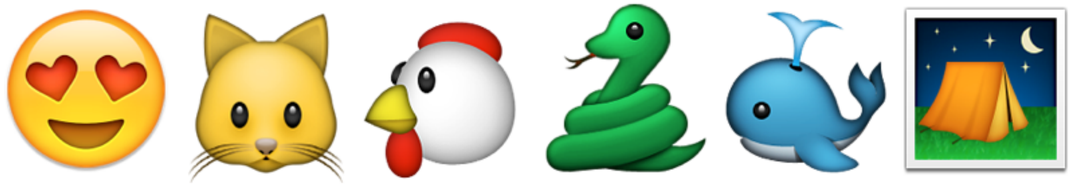
IS YOUR SAMSUNG TV LISTENING TO YOU?

« Previous / Next

Posted on Monday, February 16th, 2015 by David Lodge.

You may have heard about the recent stuff about whether your Samsung TV is listening to you whilst you watch it. If you haven't here's a quick synopsis:

1. Modern Samsung Smart TVs have a voice command facility
2. The voice command facility is enabled by saying a command phrase (the default is "Hi TV")
3. The terms and conditions state that voice data may be shipped to a third party at any point



Rosyna Keller
@rosyna

Follow

So… you can cause a Samsung Smart TV to repeatedly reboot if you name your iPhone in emoji, turn on hotspot, and TRY join it on the TV!!

RETWEETS 76 FAVORITES 48

4:24 PM - 14 Feb 2015

Rosyna Keller @rosyna · Feb 14
The name of the emoji network will appear blank in the Samsung Smart TV settings, select the blank name. Turning off hotspot will not fix it

1 1

Millions Of 'Connected' BMWs Were Possibly Using Unencrypted Data

Jason Torchinsky

Filed to: BMW 1/30/15 1:45pm

3 ★

BMW sent a press release out today partially titled *BMW Group ConnectedDrive increases data security*. This is technically true, but doesn't quite get at the core issue: data security was

Dieter

Spaar

25

Auto, öffne dich!

Sicherheitslücken bei BMWs ConnectedDrive

Autos mit eingebautem Modem senden Daten an die Hersteller und der ADAC wollte wissen, was da genau übertragen wird. c't vermittelte einen Experten, der im Auftrag des ADAC die Übertragung am Beispiel von BMWs ConnectedDrive untersuchte. Er stieß dabei auf Sicherheitslücken, die sogar das unberechtigte Öffnen der Fahrzeuge ermöglichten.

Links & Extras zum Artikel:

29.01.2015

Oettinger: Autobauer müssen bei Vernetzung Tempo erhöhen

EU-Digitalkommissar Günther Oettinger (CDU) hat an die deutschen Autobauer appelliert, bei den Zukunftsthemen Vernetzung von Fahrzeugen und automatisiertes Fahren aufs Tempo zu drücken. „Wir brauchen eine digitale Aufholjagd – und damit brauchen wir Sie“, sagte der CDU-Politiker am Mittwochabend beim Neujahrsempfang des Verbands der Automobilindustrie (VDA) in Berlin. Im klassischen IT-Sektor hätten die deutsche und europäische Wirtschaft vor allem gegenüber den USA und Südkorea stark an Boden verloren. „Jetzt geht es um die Wirtschaft insgesamt, um Industrie 4.0, Handwerk 4.0, Bankenwelt 4.0, Versicherungen 4.0. (...) Jetzt können wir alles gewinnen – und noch mehr verlieren.“

Oettinger betonte, dass die heimischen Hersteller die Herausforderung gegenüber den IT-Konzernen aber annähmen. Er sehe „mit Freude“, wie die Autobauer das Thema im Prinzip schon erkannt hätten. „Ein junger Mensch steigt in ein Auto nicht mehr ein, weil es tiefer gelegt ist, weil es chromlackiert ist, weil es viel PS hat, weil es mehr Sitze hat, als es eigentlich braucht. Digitale Kommunikation in Perfektion und die digitale Revolution werden Ihren Sektor elementar verändern“, sagte Oettinger vor den Vertretern der deutschen Autobranche.

„Ein junger Mensch steigt in ein Auto nicht mehr ein, weil es tiefer gelegt ist, weil es chromlackiert ist, weil es viel PS

Dabei komme es für die Unternehmen immer mehr darauf an, Angebote der IT-

7-Tage-Übersicht

KURZMELDUNG

Zetsche sieht mögliches iAuto von Apple skeptisch

Aus für VW-Klappdach-Cabrio Eos

Peugeot verlängert Garantie auf Antriebsbatterien

Apple plant E-Auto für 2020 – Klage nährt Spekulationen

Polizei darf Tempo nicht nur durch Hinterherfahren messen

Citroën und Peugeot: Gewinnzone in Sicht

Autoabsatz in Europa steigt wieder an

Rückruf: Mercedes CLS und E-Klasse mit defekter Dichtung

Apple: Pläne für ein eigenes Auto?

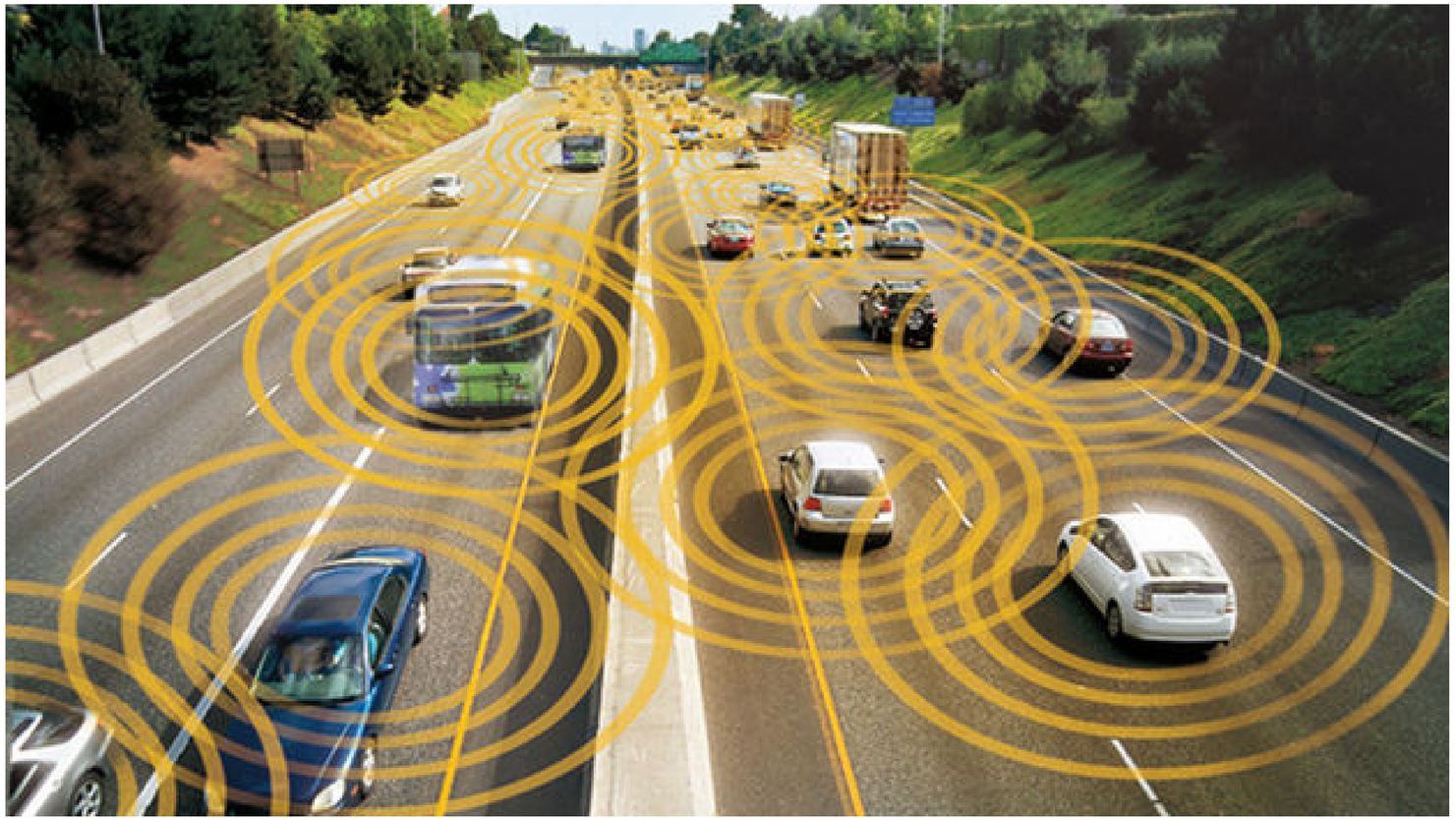
Alle Kurzmeldungen

WEITERE THEMEN

- Bildergalerien
- Erlkönige
- Hybridantrieb
- Elektroautos
- Zweirad
- Klartext
- Messeberichte
- Klassiker

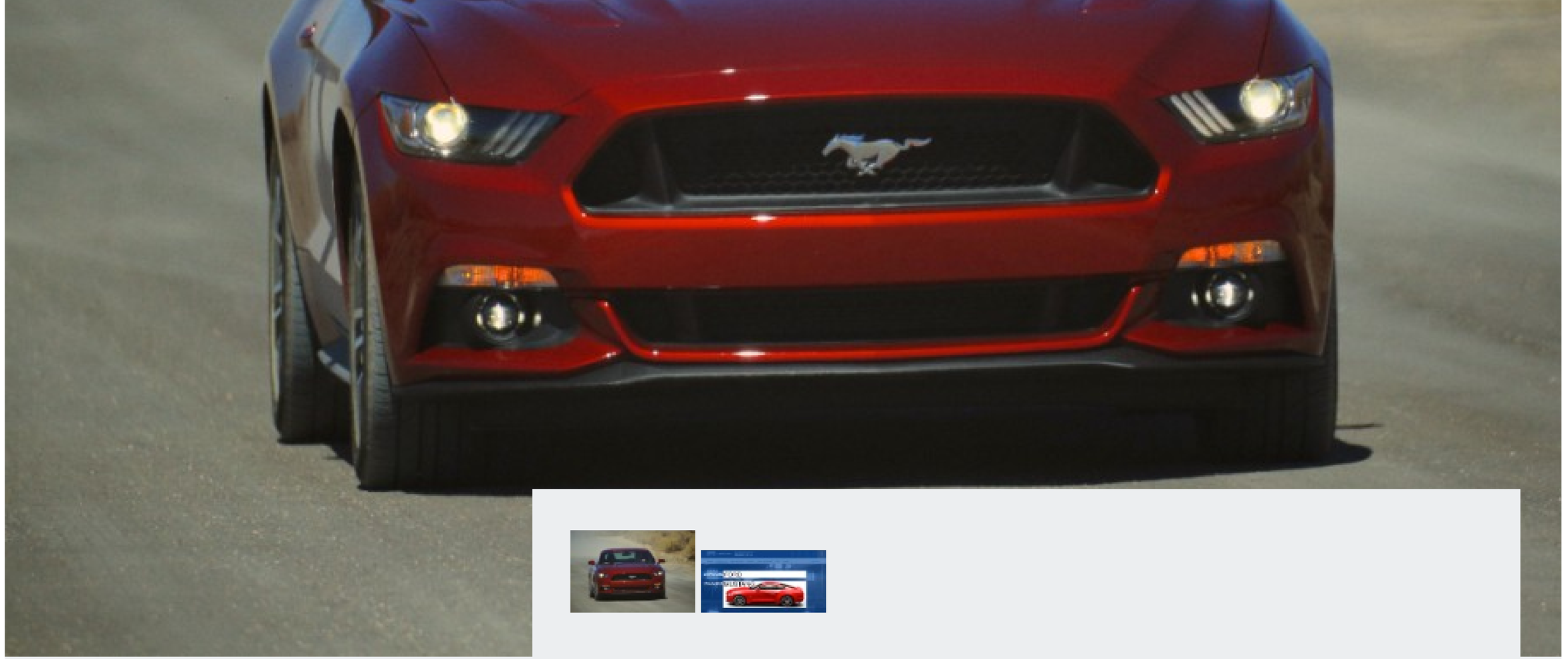
Autohersteller auf Cyberangriffe nicht vorbereitet

10.02.15, 08:58 Mail an die Redaktion



Vernetzte Autos sind für Angriffe anfällig. – Foto: RITA

FEATURED



DOWNLOADS

JAN 23, 2015 I DEARBORN, MICH.

'MUSTANG' MORE POPULAR THAN 'SUPERMAN,' 'BATMAN' ACCORDING TO RESEARCH BY SPLASHDATA

- “Mustang” is the 16th most common password on the Internet according to a recent study by SplashData, besting both “superman” in 21st place and “batman” in 24th
- Mustang is the only car to appear in the top 25 most common Internet passwords
- Adding letters, numbers, acronyms and symbols to your favorite pony car-inspired code for sign-in will help strengthen your password

Download this

Ford Mustang is one of the most popular cars ever built, and now it has the distinct honor of being one of the most common passwords on the Internet, a recent study reveals.

According to SplashData – a company specializing in password management – the word “mustang” was the 16th most common password found on the Internet in 2014, the only car moniker that found its way into the top 25. Not only that,

Happy Birthday!

YouTube now defaults to HTML5 <video>

Posted: Tuesday, January 27, 2015

Four years ago, we wrote about YouTube's early support for the HTML5 <video> tag and how it performed compared to Flash. At the time, there were limitations that held it back from becoming our preferred platform for video

Labels
Archive

Warnungen
als Email-Abo
RSS-Feed
ATOM-Feed

Aktuelles
als Email-Abo
RSS-Feed

Spezielles
RSS-Feed
ATOM-Feed

3. Update - "Zero-Day"-Sicherheitslücke in Adobe Flash Player (aktiv ausgenützt) - Patches jetzt verfügbar

2. Februar 2015

Update 05.02.2015
Update 05.02.2015 18:10 UTC+1
Update 06.02.2015

Beschreibung

Wie Adobe in seinem Security Bulletin berichtet (https://helpx.adobe.com/security/products/flash-player/apsa15-02.html), scheint es eine neue, noch ungepatchte Sicherheitslücke im Adobe Flash Player zu geben, die bereits aktiv ausgenützt wird.

Auswirkungen

Durch Ausnutzen dieser Lücke kann ein Angreifer vermutlich vollständige Kontrolle über betroffene Systeme erlangen.
Damit sind alle Daten auf diesen Systemen, sowie alle durch diese erreichbaren (etwa durch Login, VPN etc.) Daten und Systeme gefährdet.

Da das Bestehen einer Lücke nun öffentlich bekannt ist, ist auch anzunehmen, dass sich diverse Akteure nun darauf konzentrieren werden, und entsprechend ist bald mit grossflächigen Kampagnen, die diese Lücke auszunutzen versuchen, zu rechnen.

Betroffene Systeme

Systeme, auf denen folgende Software von Adobe installiert ist:

Kontakt

Email: reports@cert.at
Tel.: +43 1 5056416 78

mehr ...

Warnungen

Sicherheitslücke in TYPO3
19. Februar 2015 | ...

3. Update - "Zero-Day"-Sicherheitslücke in Adobe Flash Player (aktiv ausgenützt) - Patches jetzt verfügbar
2. Februar 2015 | ...

mehr ...

Blog

Superfish - Eine Zusammenfassung
20. Februar 2015 | Die ...

Gemalto hack - lessons learned
20. Februar 2015 | In ...

mehr ...

Jahresbericht 2014

Privates WLAN blockiert: Hotelkette Marriott gibt auf

01.02.15, 18:15 Mail an die Redaktion

Marriott International musste in den USA nun klein beigeben – Foto: Marriott Hotel

ENTSCHEIDUNG

Privates WLAN blockiert: Hotelkette Marriott gibt auf

Marriott hat in den USA seine Pläne endgültig begraben, WLAN-Hotspots von Gästen unterbinden zu wollen. Die Kommunikationsbehörde FCC stellte klar, dass so etwas illegal ist.

FEATURED

LEAK
HTC One M9 Bilder und Spezifikationen durchgesickert

Statistics

- Federal Judicial Caseload Statistics
- Federal Court Management Statistics
- Bankruptcy Statistics
- Judicial Facts and Figures
- Judicial Business Of The U.S. Courts
- Wiretap Reports
  - Wiretap Report 2013
  - Wiretap Report FAQs
  - Wiretap Reports Archive
- Statistical Tables For The Federal Judiciary
- Civil Justice Reform Act Report

Home > Statistics > Wiretap Reports > Wiretap Report 2013

email updates RSS print share FAQs

WIRETAP REPORT 2013

Each *Wiretap Report* uses tables, text, and charts to report information provided by federal and state officials on orders authorizing or approving interceptions of wire, oral, or electronic communications for the calendar year ending December 31.

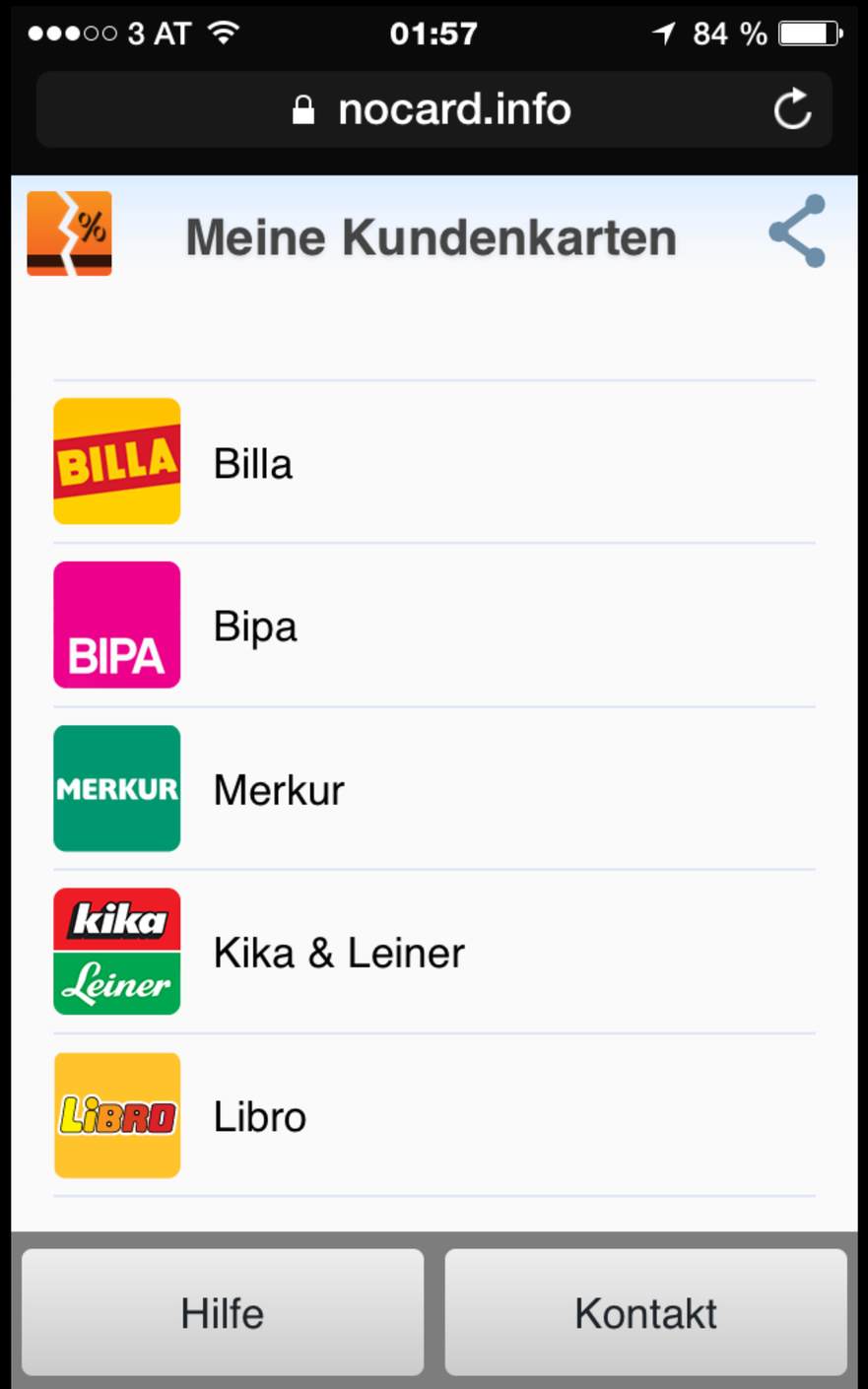
- The reports present data on types of offenses under investigation, nature and locations of intercept devices, costs and durations of intercepts, and intercept extensions granted.
- They do not include names, addresses, or phone numbers of subjects under surveillance.
- Publications dating back to 1997 are available in the archive.
- This report does not include data on interceptions regulated by the Foreign Intelligence Surveillance Act of 1978.

- Wiretap Report FAQs
- Wiretap Report Archive

WIRETAP REPORT 2013 STATISTICAL TABLES

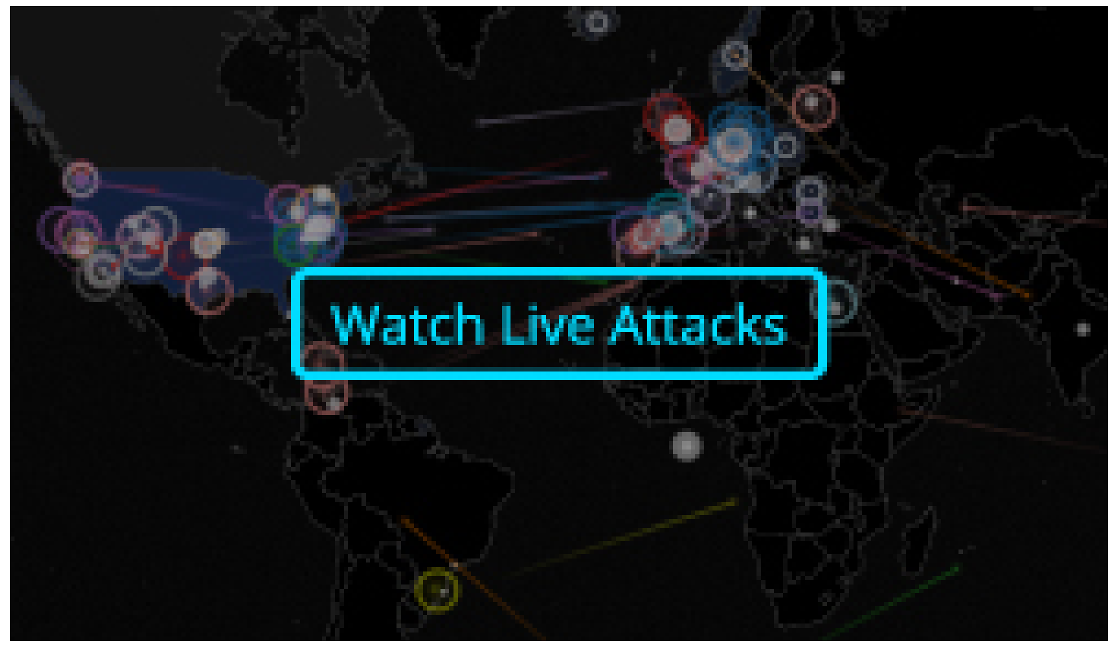
(Statistical tables are in pdf format)

- Table 1 - Jurisdictions with Statutes Authorizing the Interception of Wire, Oral, or Electronic Communications
- Table 2 - Intercept Orders Issued by Judges
- Table 3 - Major Offenses for Which Court-Authorized Intercepts Were Granted
- Table 4 - Summary of Interceptions of Wire, Oral, or Electronic


3 AT
01:57
84 %
nocard.info
Meine Kundenkarten
Billa
Bipa
Merkur
Kika & Leiner
Libro
Hilfe
Kontakt

Posted by: Anthony M. Freed
February 17th, 2015

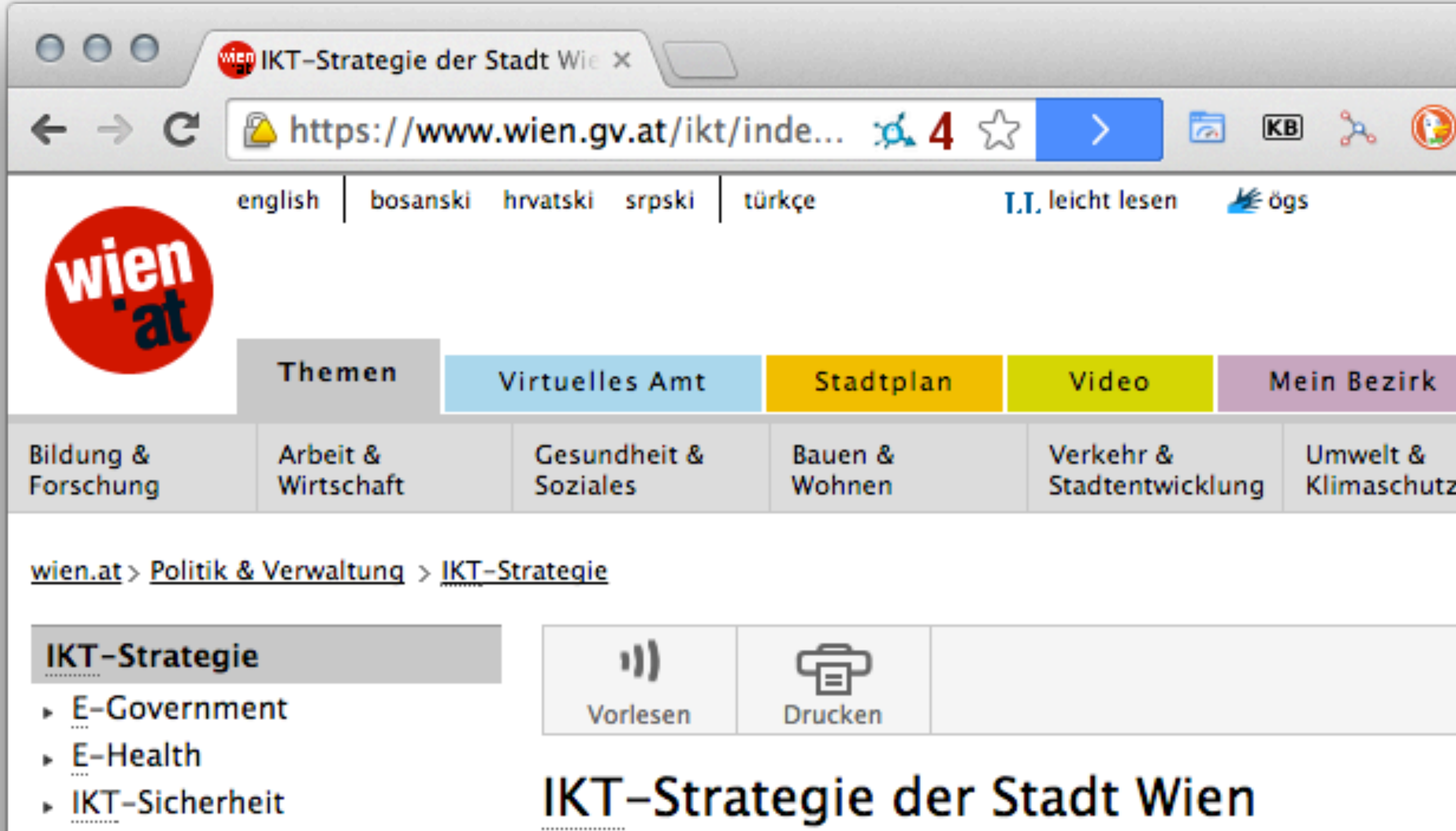
No Version of SSL Meets PCI SSC's Definition of Strong Cryptography

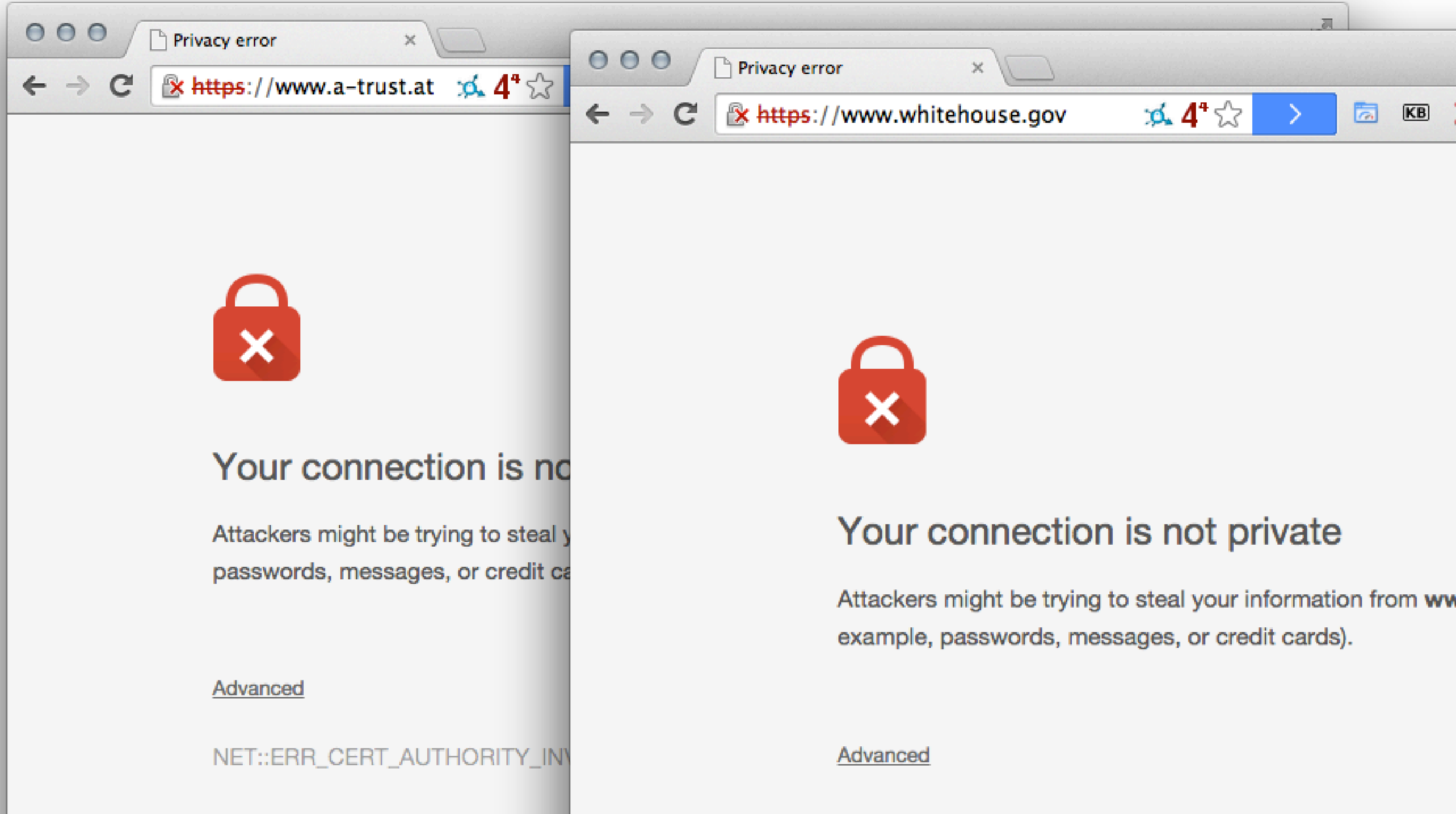


Popular Breaking Featured

Automated


start [CryptoParty Austria]
https://cryptoparty.at
CryptoParty Austria
Zuletzt angesehen: • start


IKT-Strategie der Stadt Wie
https://www.wien.gv.at/ikt/inde...
4
KB
english
bosanski
hrvatski
srpski
türkçe
leicht lesen
ögs
wien.at
Themen
Virtuelles Amt
Stadtplan
Video
Mein Bezirk
Bildung & Forschung
Arbeit & Wirtschaft
Gesundheit & Soziales
Bauen & Wohnen
Verkehr & Stadtentwicklung
Umwelt & Klimaschutz
wien.at > Politik & Verwaltung > IKT-Strategie
IKT-Strategie
E-Government
E-Health
IKT-Sicherheit
Vorlesen
Drucken
IKT-Strategie der Stadt Wien


Privacy error
https://www.a-trust.at
Your connection is nc
Attackers might be trying to steal y
passwords, messages, or credit ca
Advanced
NET::ERR_CERT_AUTHORITY_IN
Privacy error
https://www.whitehouse.gov
KB
Your connection is not private
Attackers might be trying to steal your information from ww
example, passwords, messages, or credit cards).
Advanced

Chrome warnt vor unverschlüsselten Webseiten

01.02.15, 11:12 Mail an die Redaktion

Chrome könnte künftig unverschlüsselte Kommunikation entlarven – Foto: AP/Mark Lennihan

BROWSER
Chrome warnt vor unverschlüsselten Webseiten
KOMMENTARE (3)
MEHR ZUM

Während Politiker das Ende verschlüsselter Kommunikation fordern, experimentiert Google bei Chrome mit einem Feature, das jegliche unverschlüsselte Webseite enttarnt.

GOOGLE, CHROME, VERSCHLÜSSELUNG

In der Testversion von Googles Browser Chrome kann ein neues Feature aktiviert werden, das in der URL-Zeile anzeigt,

FEATURED

LEAK
HTC One M9 Bilder und Spezifikationen durchgesickert

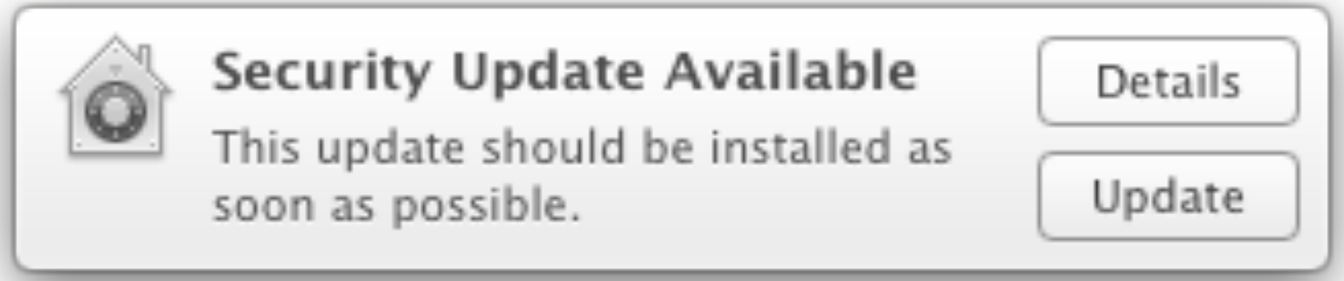
Österreichisches Parlament

www.parlament.gv.at

DEUTSCH | ENGLISH | OTHER LANGUAGES | LETZTES UPDATE: 19.02.2015; 16:24

REPUBLIK ÖSTERREICH
Parlament

PARLAMENT AKTIV | PARLAMENT ERKLÄRT | WER IST WER | GEBÄUDE UND FÜHRUNG


Security Update Available
This update should be installed as soon as possible.
Details
Update


FROM ACADEMY-AWARD® NOMINATED DIRECTOR
LAURA POITRAS
AND EXECUTIVE PRODUCER
STEVEN SODERBERGH
CITIZENFOUR
CITIZENFOURFILM.COM
10_24_14

GPG Key-Signing

Zertifikate

TLS

HTTPS

Client Hello: cryptoparty.at

ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384

Server Hello: cryptoparty.at

ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384


Certificate
Standard


Certificate
Root

Client Done:

Change Cipher Spec

Server Done:

Change Cipher Spec

ECDHE-RSA-AES256-GCM-SHA384

Client:

http/1.1 GET
cryptoparty.at

PKI

Public Key Infrastructure

Zertifizierungsstelle/CA

Zertifizierungsstelle/CA

Comodo
Symantec
Go Daddy
Globalsign
Digicert
Verisign

Zertifizierungsstelle/CA

Intermediate CA

StartCom Class 1 Primary Intermediate Server CA

Zertifizierungsstelle/CA

Intermediate CA

Leaf: cryptoparty.at

Zertifizierungsstelle/CA

Intermediate CA

Leaf: cryptoparty.at

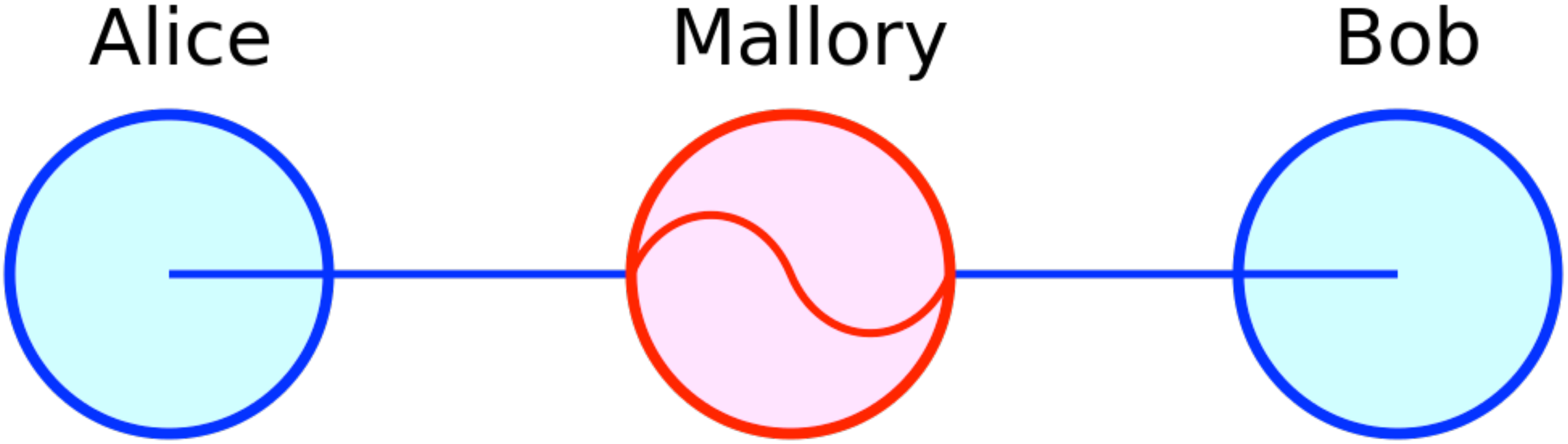

Certificate
Root

XRamp Global Certification Authority	certificate	01 Jan 2035 06:37:19
WellsSecure Public Root Certificate Authority	certificate	14 Dec 2022 01:07:54
VRK Gov. Root CA	certificate	18 Dec 2023 14:51:08
Visa Information Delivery Root CA	certificate	29 Jun 2025 19:42:42
Visa eCommerce Root	certificate	24 Jun 2022 02:16:12
VeriSign Universal Root Certification Authority	certificate	02 Dec 2037 00:59:59
VeriSign Class 4 Public Primary Certification Authority - G3	certificate	17 Jul 2036 01:59:59
VeriSign Class 3 Public Primary Certification Authority - G5	certificate	17 Jul 2036 01:59:59
VeriSign Class 3 Public Primary Certification Authority - G4	certificate	19 Jan 2038 00:59:59
VeriSign Class 3 Public Primary Certification Authority - G3	certificate	17 Jul 2036 01:59:59
VeriSign Class 2 Public Primary Certification Authority - G3	certificate	17 Jul 2036 01:59:59
VeriSign Class 1 Public Primary Certification Authority - G3	certificate	17 Jul 2036 01:59:59
VAS Latvijas Pasts SSI(RCA)	certificate	13 Sep 2024 11:27:57
UTN-USERFirst-Object	certificate	09 Jul 2019 20:40:36
UTN-USERFirst-Network Applications	certificate	09 Jul 2019 20:57:49
UTN-USERFirst-Hardware	certificate	09 Jul 2019 20:19:22
UTN-USERFirst-Client Authentication and Email	certificate	09 Jul 2019 19:36:58
UTN - DATACorp SGC	certificate	24 Jun 2019 21:06:30
UCA Root	certificate	31 Dec 2029 01:00:00
UCA Global Root	certificate	31 Dec 2037 01:00:00
TWCA Root Certification Authority	certificate	31 Dec 2030 16:59:59
TWCA Global Root CA	certificate	31 Dec 2030 16:59:59
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	certificate	22 Mar 2015 11:27:17
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	certificate	16 Sep 2015 12:07:57
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	certificate	22 Dec 2017 19:37:19
TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3	certificate	21 Aug 2017 13:37:07
Trustis FPS Root CA	certificate	21 Jan 2024 12:36:54

Probleme

GeoTrust True Credentials CA 2	certificate	21 Jun 2020 06:00:00
DoD Intermediate CA-2	certificate	07 May 2018 15:44:51
DoD Intermediate CA-1	certificate	04 Feb 2018 15:36:43
DOD EMAIL CA-30	certificate	08 Sep 2017 18:03:08
DOD EMAIL CA-29	certificate	08 Sep 2017 18:02:14
DOD EMAIL CA-28	certificate	08 Sep 2017 18:01:19
DOD EMAIL CA-27	certificate	08 Sep 2017 18:00:18
DOD EMAIL CA-26	certificate	14 Jan 2016 18:39:27
DOD EMAIL CA-25	certificate	14 Jan 2016 18:36:32
DOD EMAIL CA-24	certificate	25 Jan 2015 21:26:15
DOD EMAIL CA-23	certificate	25 Jan 2015 17:43:25
DOD EMAIL CA-22	certificate	25 Jan 2015 21:25:07
DOD EMAIL CA-21	certificate	25 Jan 2015 17:41:13
DOD EMAIL CA-20	certificate	23 Apr 2014 22:08:56
DOD EMAIL CA-19	certificate	23 Apr 2014 22:03:06
DOD CA-30	certificate	08 Sep 2017 17:59:24
DOD CA-29	certificate	08 Sep 2017 17:58:26
DOD CA-28	certificate	08 Sep 2017 17:57:01
DOD CA-27	certificate	08 Sep 2017 17:50:25
DOD CA-26	certificate	14 Jan 2016 18:38:05
DOD CA-25	certificate	14 Jan 2016 18:33:12
DOD CA-24	certificate	25 Jan 2015 21:23:11
DOD CA-23	certificate	25 Jan 2015 17:38:45
DOD CA-22	certificate	25 Jan 2015 21:18:59
DOD CA-21	certificate	25 Jan 2015 17:35:03
DOD CA-20	certificate	23 Apr 2014 22:05:37

Monster-in-the-Middle Attacke


Alice
Mallory
Bob

SUPERFISH

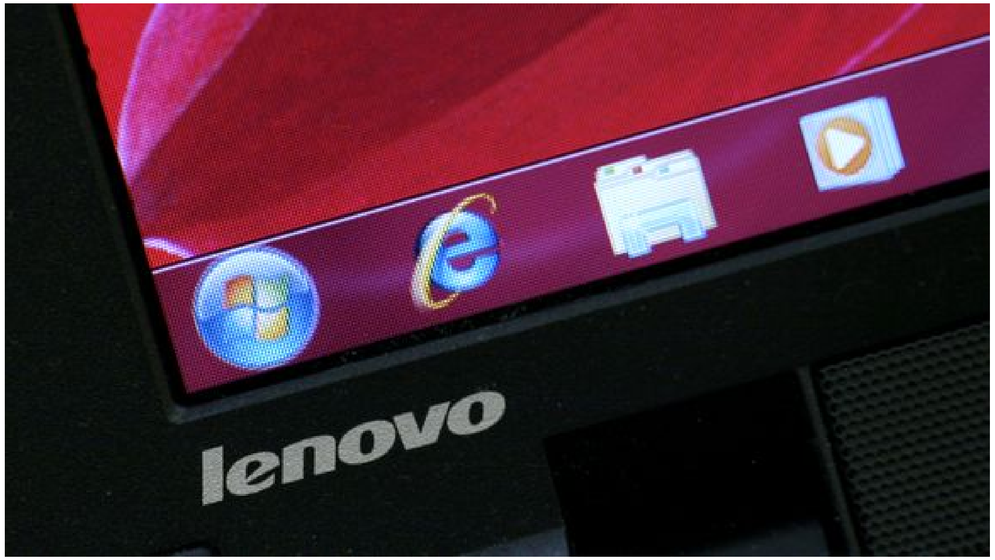
Lenovo steckt gefährliche Adware in seine Laptops

Eine auf Lenovo-Laptops vorinstallierte Software namens Superfish blendet nicht nur ungefragt Werbebanner ein. Sie gefährdet auch die Sicherheit von HTTPS-Verbindungen.

VON HANNO BÖCK

19. Februar 2015 11:51 Uhr

72 Kommentare



Lenovo-Notebook (Archivbild) | © REUTERS/Bobby Yip

Verschiedene aktuelle Laptops des Herstellers Lenovo werden mit einer

ARTIKEL Auf einer Seite lesen

QUELLE ZEIT ONLINE

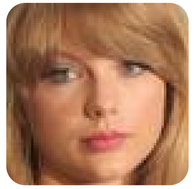
SCHLAGWORTE Lenovo | Windows | Verschlüsselung | Online-Werbung | Firefox | Linux

NEU IM RESSORT

1. VIDEOS YouTube buhlt um Kleinkinder
2. RUNPEE Die Datenbank der Pinkelpausen
3. STÖRERHAFTUNG Gefahrlos offene WLANs bleiben Utopie
4. MOBILFUNK Sieben Wege, ein Handy abzuhören
5. LENOVO Der Superfish ist weitverbreitet

NEU AUF ZEIT ONLINE

1. EUROKRISE Drei verdrängte Wahrheiten über den Griechenland-Deal
2. GRIECHEN-HILFSPROGRAMM Union droht mit Aufständchen
3. SEBASTIAN EDATHY Ein mittlerer, vierstelliger Ausweg
4. DEUTSCHE BAHN Streik der Lokführer abgewendet
5. GESELLSCHAFTSKRITIK Mensch Mama!



InfoSec Taylor Swift
@SwiftOnSecurity

Follow

"Superfish" is malware pre-installed by Lenovo that shows ads, sends your browsing to an ad company and intercepts encrypted bank websites.

RETWEETS 1,227

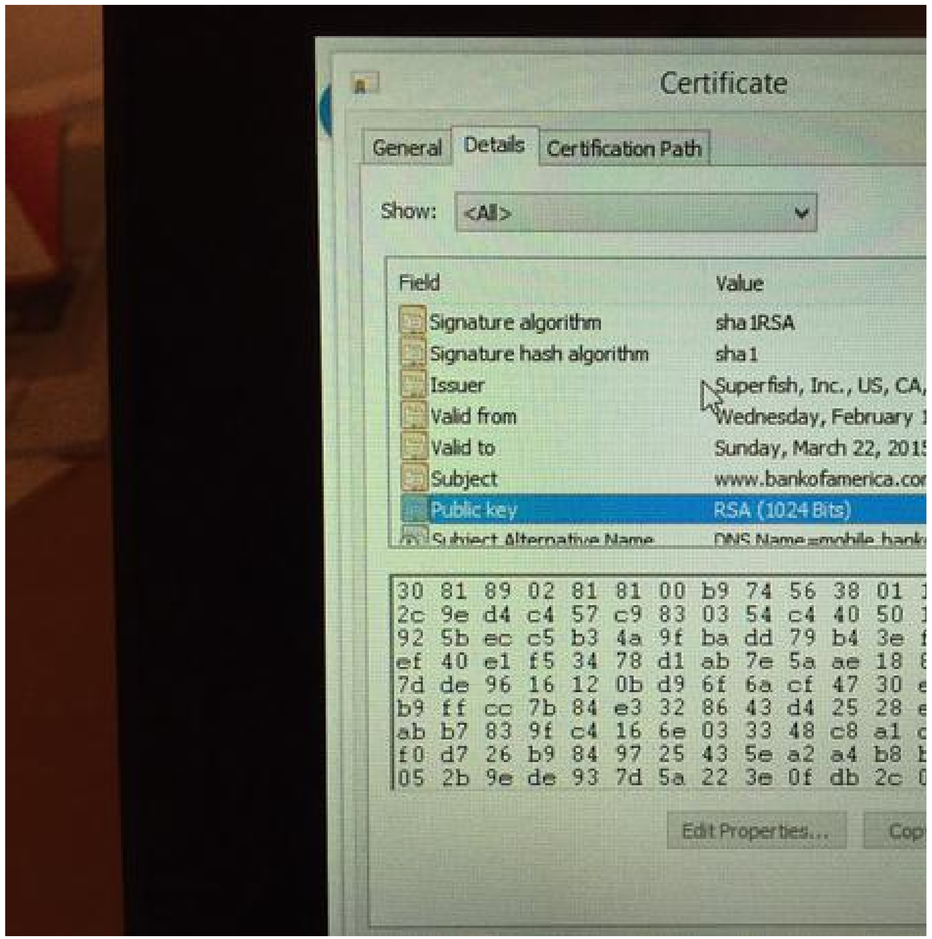
FAVORITES 298

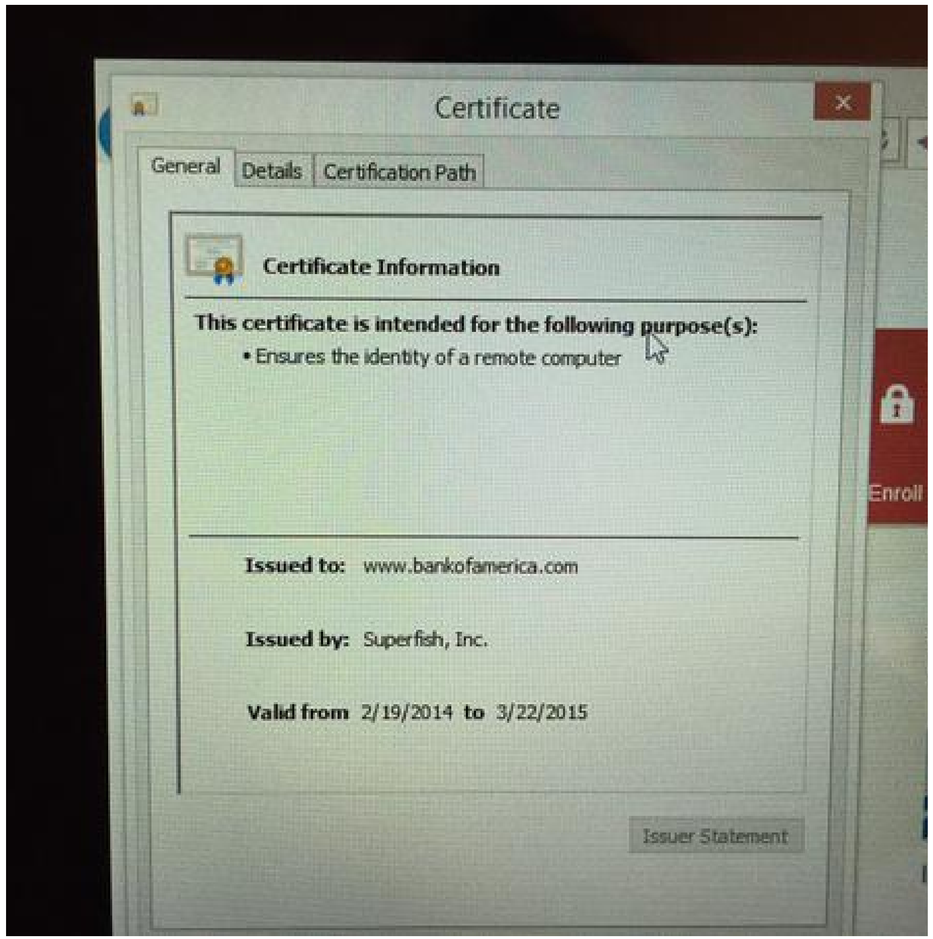
11:25 PM - 18 Feb 2015

Chris Palmer
@fugueish

Follow

#superfish






Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
Issued to: www.bankofamerica.com
Issued by: Superfish, Inc.
Valid from 2/19/2014 to 3/22/2015
Bank of Ameri
Enroll
Bankir
BankAmeric
Rewards™

certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	USERTrust		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
Cybertrust Public SureServer SV...	Baltimore CyberTrust Root	9/8/2020	<All>	<None>		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati...	DigiCert		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Superfish, Inc.	Superfish, Inc.	5/7/2034	<All>	<None>		
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticati...	thawte		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...	USERTrust		
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...	VeriSign		

General | Details | Certification Path

Show: <All>

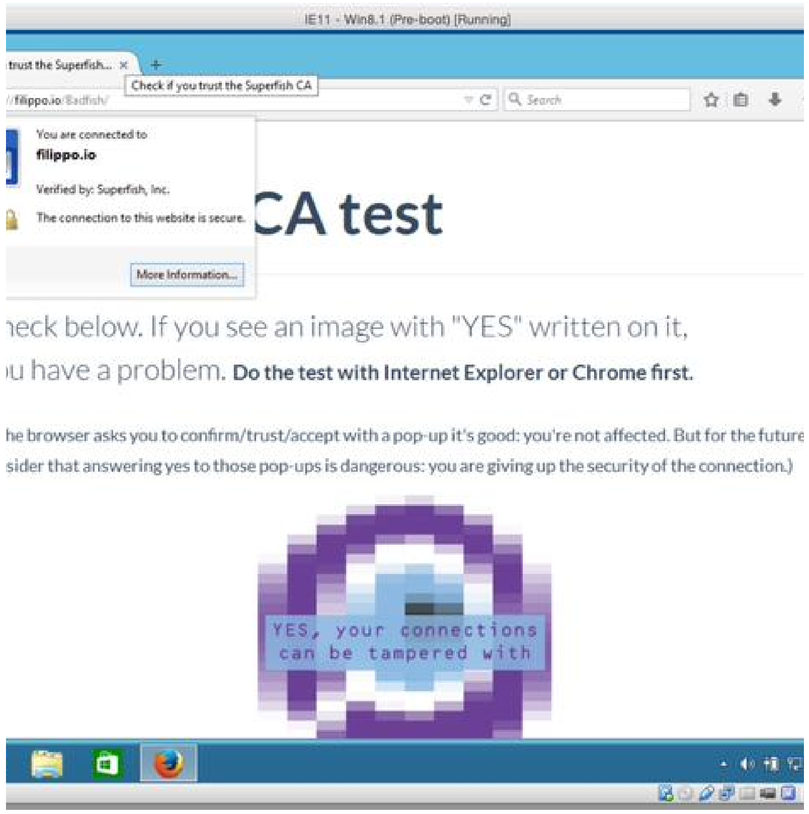
Field	Value
Valid to	Sunday, May 7, 2034 8:25:26 ...
Subject	Superfish, Inc., US, CA, SF, S...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=CA, Path Lengt...
Subject Key Identifier	fb 98 b3 53 7f 14 44 2e e8 ee ...
Authority Key Identifier	KeyID=fb 98 b3 53 7f 14 44 2...
Thumbprint algorithm	sha1
Thumbprint	c8 64 48 48 69 d4 1d 2b 0d 32

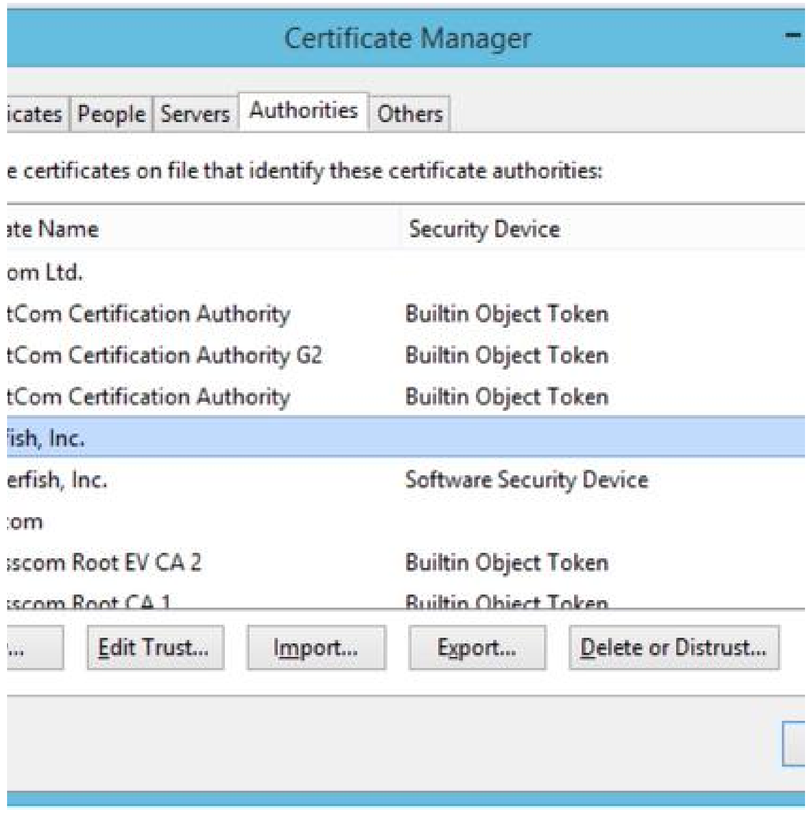
```
30 81 89 02 81 81 00 e8 f3 4a 18 76 5f 19
3f b1 cf 58 e9 7f 43 07 09 95 80 35 c5 0f
fe 71 31 27 81 99 12 26 20 a5 df 8f 6a fc
42 55 39 ee 09 38 89 d9 e0 36 c4 ac 01 82
5b d5 39 e6 f9 8f 07 88 df fe ee f6 a1 14
ce a9 74 45 d8 fd f0 17 57 2a 82 e1 7a 2e
12 93 5a ac 8a d7 15 63 d1 b7 9b 55 80 0f
58 bc 1c 49 ed 20 62 dd b6 4c a5 3a eb 1c
3d a0 ff 7a 71 a6 d3 10 78 33 ae 4b c2 1c
```

Filippo Valsorda
@FiloSottile

Follow

Confirmed: if Firefox is installed when the Superfish installer runs, the cert gets added to the the FF store.

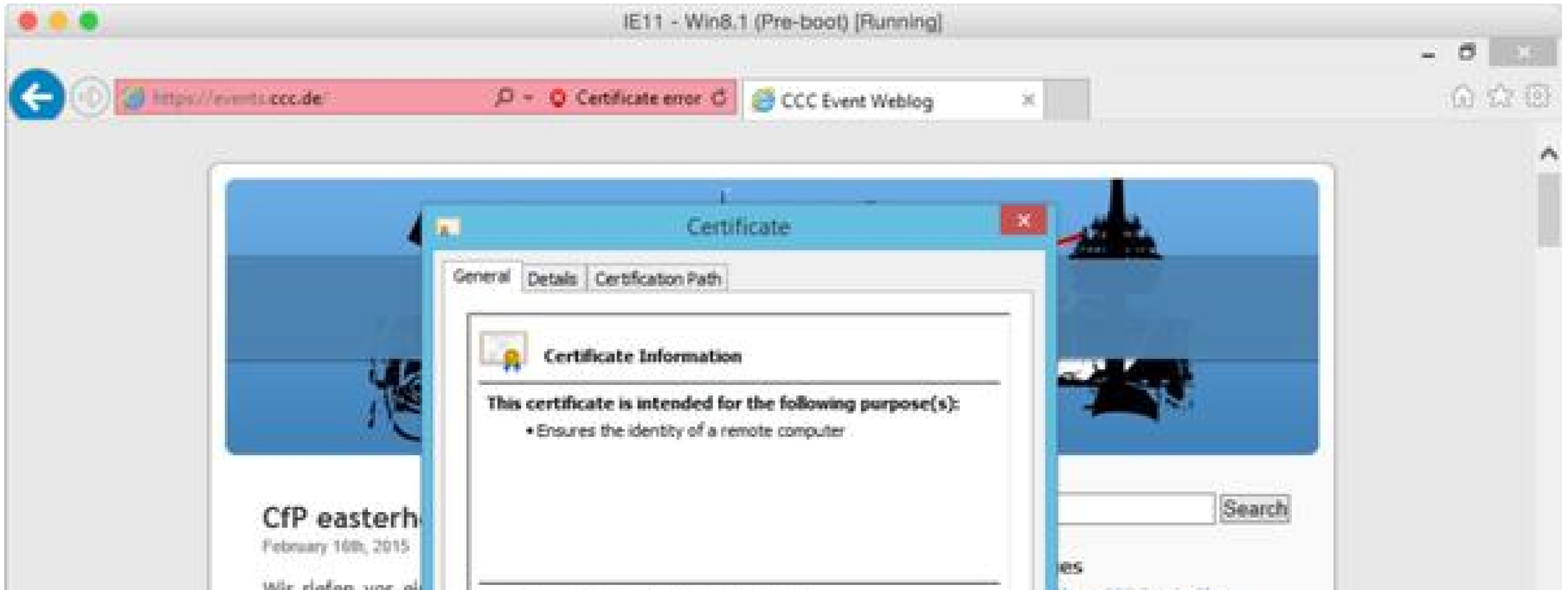




Filippo Valsorda
@FiloSottile

Follow

Cute. When the Superfish client detects a bad cert, it'll create one with a bad name to cause a warn in the browser



Filippo Valsorda, 20 Feb 2015

KOMODIA/SUPERFISH SSL VALIDATION IS BROKEN

If you are on the ball already and just want the new vulnerability, scroll to the "client side SSL verification" section. tl;dr The Komodia/Superfish proxy can be made to allow self-signed certificates without warnings.

Recap

Check for bad certs from Komodia / Superfish

This tool checks if you are affected by a malicious certificate installed by the software Superfish or other software using the same technology (Komodia). See below for a detailed explanation.

Superfish		Keep My Family Secure	
Kurupira		Staffcop	
Qustodio/Windows		Qustodio/OS X	
Easy hide IP		Lavasoft AdAdware WebCompanion	
Sendori / PureLeads			
Komodia generic		Man-in-the-Middle generic	This test didn't seem to work reliably, for testing it's here

Check for bad certs from Komodia / Superfish

This tool checks if you are affected by a malicious certificate installed by the software Superfish or other software using the same technology (Komodia). See below for a detailed explanation.

Superfish	✗	Keep My Family Secure	✗
Kurupira	✗	Staffcop	✗
Qustodio/Windows	✗	Qustodio/OS X	✗
Easy hide IP	✗	Lavasoft AdAdware WebCompanion	✗
Sendori / PureLeads	✗		
Komodia generic	✗	Man-in-the-Middle generic	This test didn't seem to work reliably, for testing it's here

Author | Topic: PrivDog 3.0.0.96 is now released. (Read 2759 times)

Shane
Product Group Manager
Administrator
Comodo's Hero

STAFF
COMODO

PrivDog 3.0.0.96 is now released.
« **on:** December 30, 2014, 03:50:08 PM »

PRIVDOG

Comodo-Adware hebelt HTTPS-Sicherheit aus

Die Adware Privdog hebelt ähnlich wie Superfish den Schutz von HTTPS komplett aus. Pikant daran: Privdog wurde von Comodo verbreitet, einer der größten Zertifizierungsstellen für TLS-Zertifikate.

Comodo hat offenbar eine Software verbreitet, die ähnlich wie Superfish eine riesige Sicherheitslücke in die HTTPS-Verschlüsselung reißt. Privdog heißt das Programm, das offiziell dem Zweck dient, Werbung auf Webseiten durch "vertrauenswürdige Werbung" zu ersetzen. Das soll dem Schutz der Privatsphäre des Anwenders dienen.

Ähnlich wie die Software Superfish, die in den letzten Tagen Schlagzeilen machte und auf Lenovo-Laptops vorinstalliert war, greift Privdog in den TLS-Datenstrom eines Nutzers ein, um auch verschlüsselte HTTPS-Webseiten manipulieren zu können. Dafür wird ein Root-Zertifikat im Betriebssystem installiert. Allerdings wird dies anders implementiert als bei Superfish.

"Ihre Privatsphäre wird angegriffen" warnt Privdog – dabei gefährdet es selbst die Privatsphäre. (Bild: Screenshot / Webseite)

Datum: 23.2.2015, 10:59

Autor: Hanno Böck

Themen: SSL, Man-in-the-Middle, Sicherheitslücke, Superfish, Verschlüsselung, Lenovo, Technologie, Applikationen, Internet, Security

Teilen: 1 10 41 14

Tools: Drucken

Stellenmarkt

SCADA Software Data Engineer (m/w) Wind Power