🔕

CRYPTO
PARTY

31

TU
WIEN

Was bisher geschah…

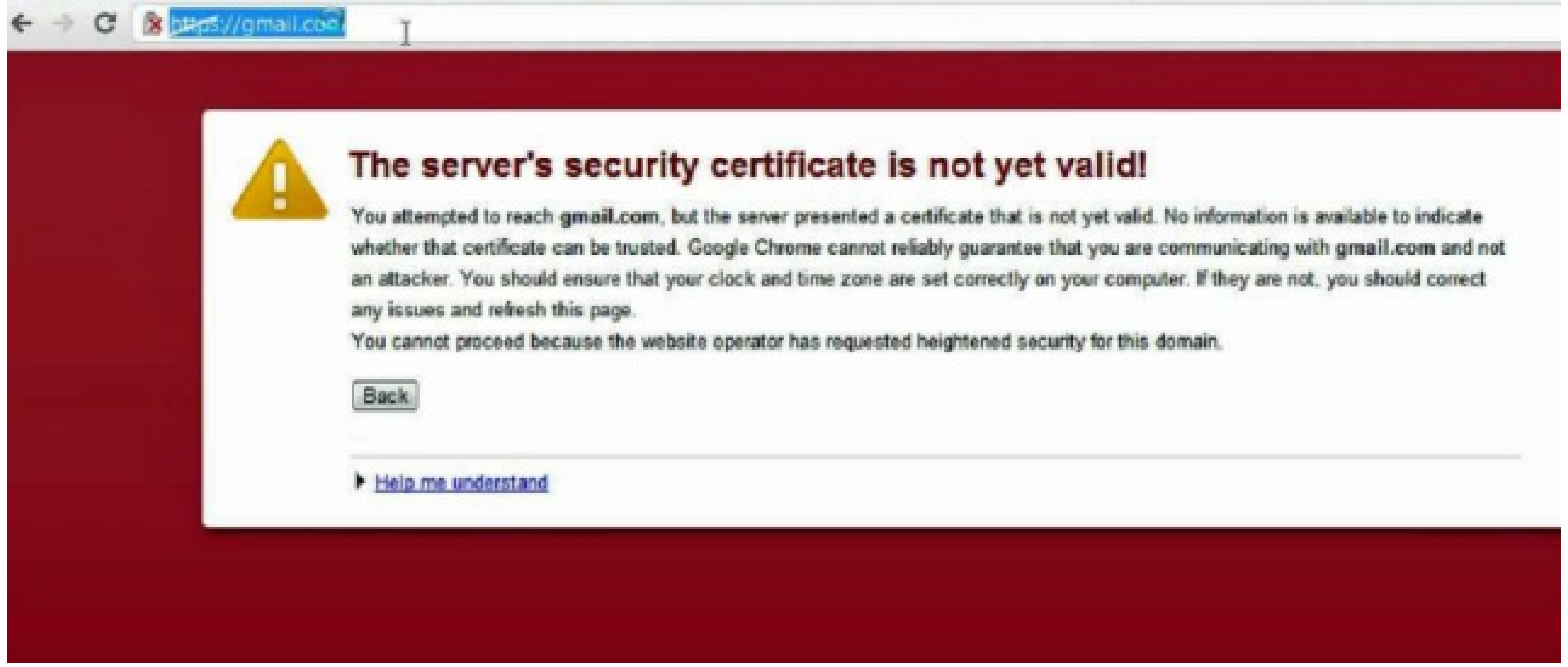
RISK ASSESSMENT / SECURITY & HACKTIVISM

Google warns of unauthorized TLS certificates trusted by almost all OSes [Updated]

Misissued certs known to impersonate several Google domains, may affect others.

by **Dan Goodin** - Mar 24, 2015 8:20pm CET

Share Tweet 77



The server's security certificate is not yet valid!

You attempted to reach **gmail.com**, but the server presented a certificate that is not yet valid. No information is available to indicate whether that certificate can be trusted. Google Chrome cannot reliably guarantee that you are communicating with **gmail.com** and not an attacker. You should ensure that your clock and time zone are set correctly on your computer. If they are not, you should correct any issues and refresh this page.

You cannot proceed because the website operator has requested heightened security for this domain.

In the latest security lapse involving the Internet's widely used encryption system, Google said unauthorized digital certificates have been issued for several of its domains and warned misissued credentials may be impersonating other unnamed sites as well.

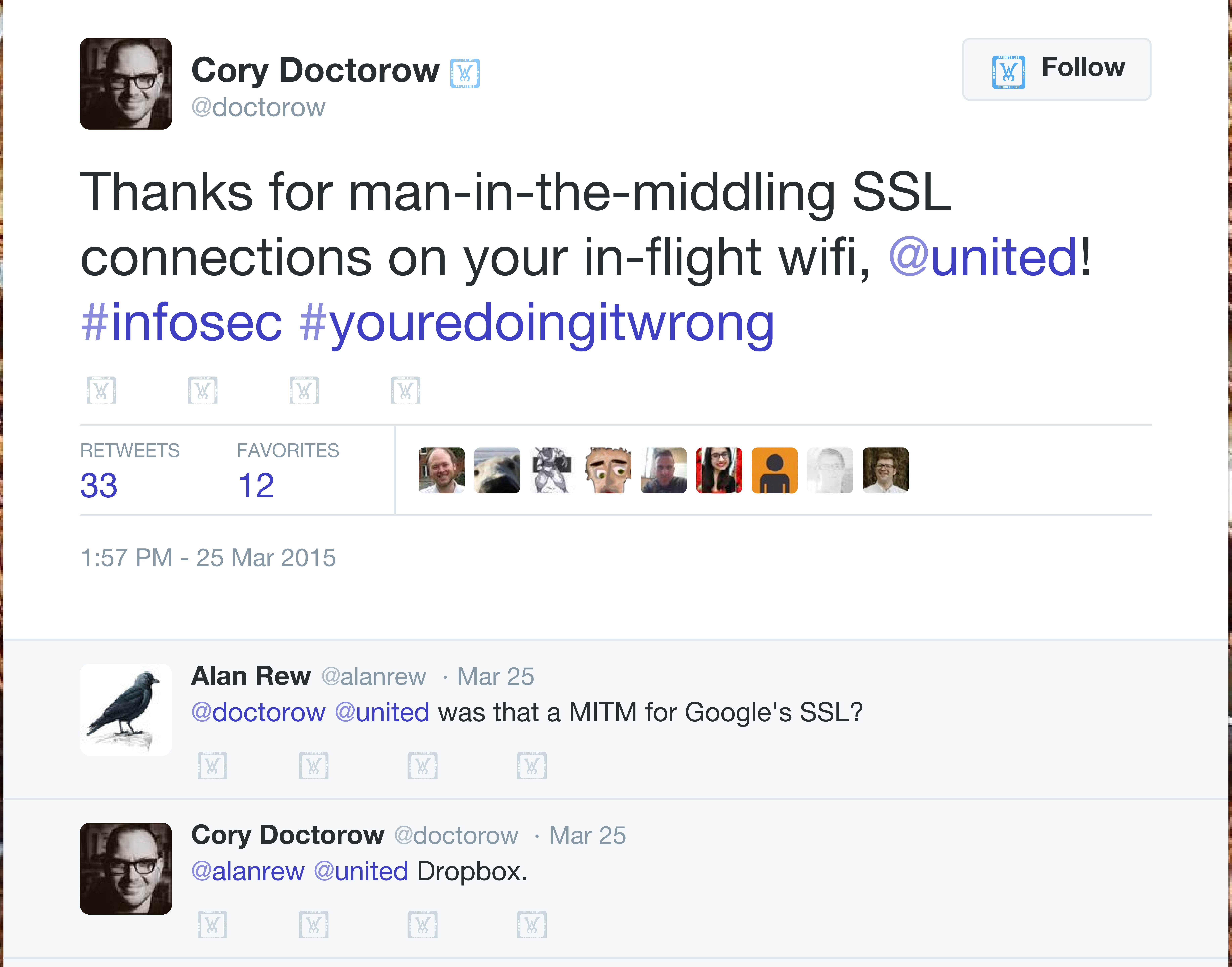
LATEST FEATURE STORY

FEATURE STORY (3 PAGES)

AT&T's plan to watch your Web browsing—and what you can do about it

Want to opt out? It could cost up to $744 extra per year.

WATCH ARS VIDEO



Cory Doctorow @doctorow

Thanks for man-in-the-middling SSL connections on your in-flight wifi, @united! #infosec #youredoingitwrong

RETWEETS 33 FAVORITES 12

1:57 PM - 25 Mar 2015

Alan Rew @alanrew · Mar 25

@doctorow @united was that a MITM for Google's SSL?

Cory Doctorow @doctorow · Mar 25

@alanrew @united Dropbox.

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Superfish SSL Interception Library Found in Several Applications: Researchers

By Eduard Kovacs on February 23, 2015

Share 57 +1 9 Tweet Recommend 215 RSS

The controversial SSL interception library used by the Superfish software installed recently on Lenovo laptops can be found in at least a dozen other applications, researchers have determined.

Lenovo came into the spotlight last week after numerous individuals who acquired new laptops started complaining about ad injections made by a browser add-on from Superfish. It later turned out that the application used a proxy and a self-signed root certificate to intercept HTTPS connections and inject the ads.

Several problems have been identified by security experts. Besides the fact that the adware

Google™ Custom Search

SSL/TLS Sicherheitslücken

FREAKing hell: ALL Windows versions vulnerable to SSL snoop

Relax! We've got a (server-knackering) workaround to sort things out, says Microsoft

6 Mar 2015 at 00:04, Darren Pauli

314 77 62

Security

Related topics

Microsoft, Security , Ssl

Careers
Sign out
OK
Search
Advanced Search
Search Tips
Login
Login Help
Register Now
First
Previous
Next
Last
View 100

NSA Careers

Welcome! Please enter your user name
password to login. If you have not yet re

To view additional job openings, click
enter key words then click on the "Sea

If you do not remember your passwor

https://www.nsa.gov

You have entered a secured site. (31000,88) Data you enter on this site is protected in transit.

Basic Job Search

Keywords:

Posted: Anytime

User Name:

Password:

Select all positions of interest.

Job Postings

1-25 of 176

	Job Title	Job ID	Location
□	General Counsel, National Security Agency	1055972	Fort George G. Meade, MD
□	Attorney	1055851	Fort George G. Meade, MD
□	Cooperative Education Program	1055679	Fort George G. Meade, MD
□	Language Analyst - Chinese (Mandarin)	1055121	Multiple Locations
□	Software Engineer	1052899	Honolulu, HI
□	Software Engineer	1055116	Denver, CO
□	Multimedia Producer	1055158	Fort George G. Meade, MD
□	Research Post-Graduate and Postdoctoral Program (RDGPD)	1054712	Fort George G. Meade, MD

https://www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1

```
This is not the page you think it is!
Yes, it has the right certificate above.
Do you really want a job here?
```

Safari is using an encrypted connection to www.nsa.gov.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.nsa.gov.

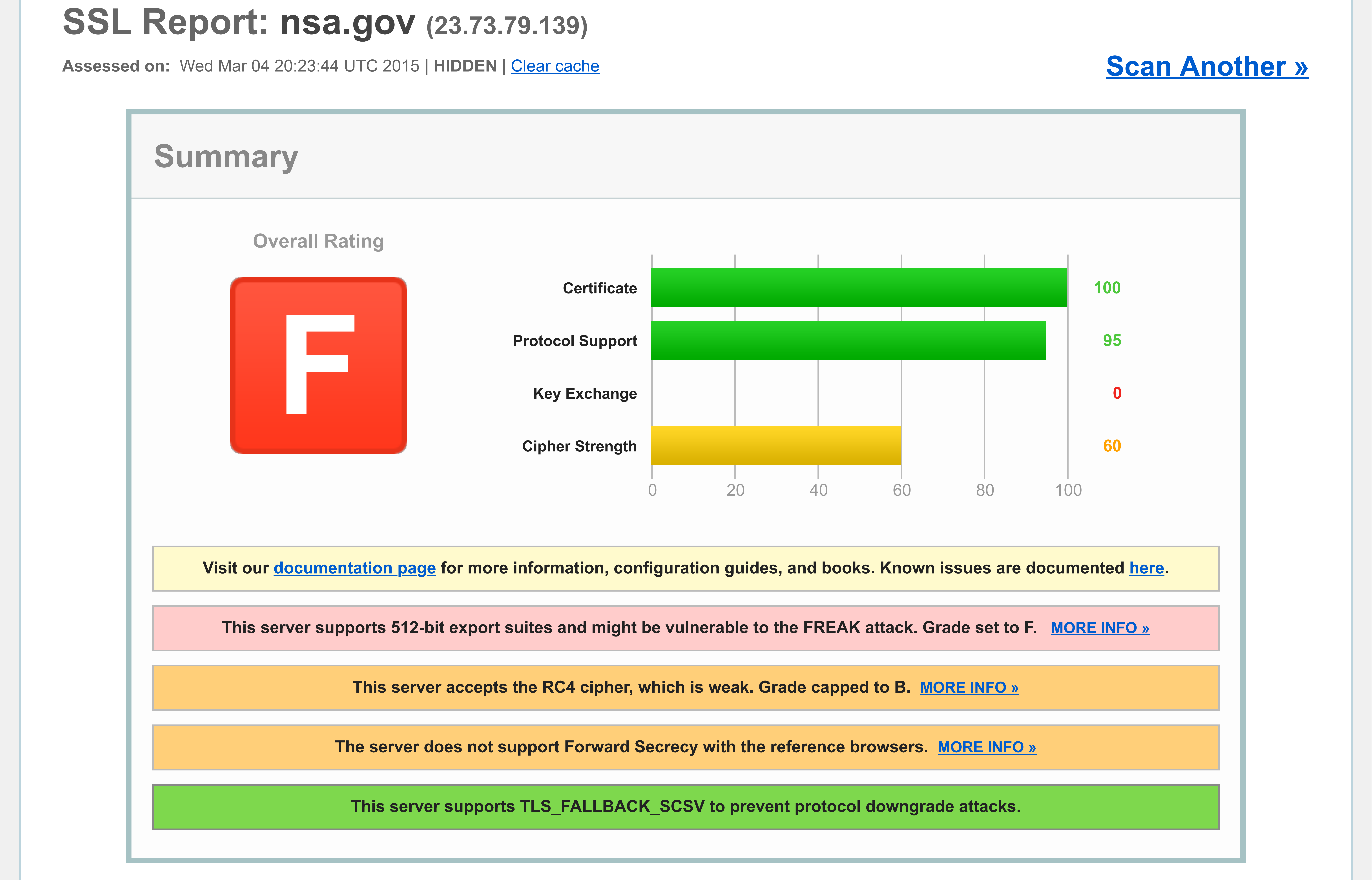
GeoTrust Global CA
↳ GeoTrust SSL CA - G4
↳ www.nsa.gov

www.nsa.gov
Issued by: GeoTrust SSL CA - G4
Expires: Monday 8 February 2016 22 h 14 min 42 s Central European Standard Time
This certificate is valid

https
www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1
Reader
Certificate
▶ Trust
▶ Details
?
Hide Certificate
OK

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

TLS_RSA_WITH_AES_256_CBC_SHA (`0x35`)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (`0xa`)	112
TLS_RSA_WITH_AES_128_CBC_SHA (`0x2f`)	128
TLS_RSA_WITH_IDEA_CBC_SHA (`0x7`)	128
TLS_RSA_WITH_RC4_128_SHA (`0x5`) **WEAK**	128
TLS_RSA_WITH_RC4_128_MD5 (`0x4`) **WEAK**	128
TLS_RSA_WITH_DES_CBC_SHA (`0x9`) **WEAK**	56
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (`0x8`) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (`0x6`) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (`0x3`) **INSECURE**	40



SSL Report: nsa.gov (23.73.79.139)

Assessed on: Wed Mar 04 20:23:44 UTC 2015 | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

F

Certificate 100

Protocol Support 95

Key Exchange 0

Cipher Strength 60

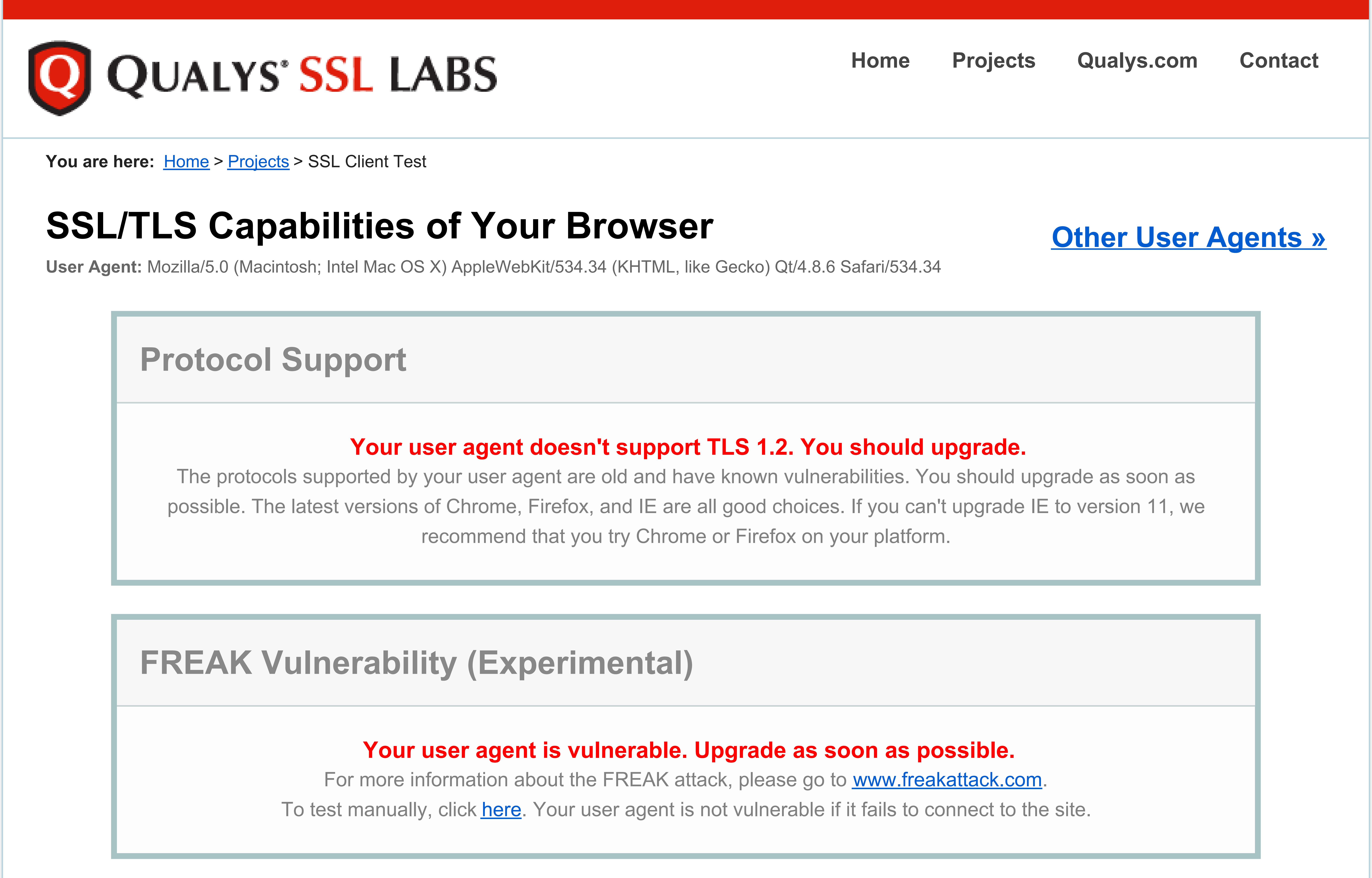
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.



QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHTML, like Gecko) Qt/4.8.6 Safari/534.34

Protocol Support

Your user agent doesn't support TLS 1.2. You should upgrade.

The protocols supported by your user agent are old and have known vulnerabilities. You should upgrade as soon as possible. The latest versions of Chrome, Firefox, and IE are all good choices. If you can't upgrade IE to version 11, we recommend that you try Chrome or Firefox on your platform.

FREAK Vulnerability (Experimental)

Your user agent is vulnerable. Upgrade as soon as possible.

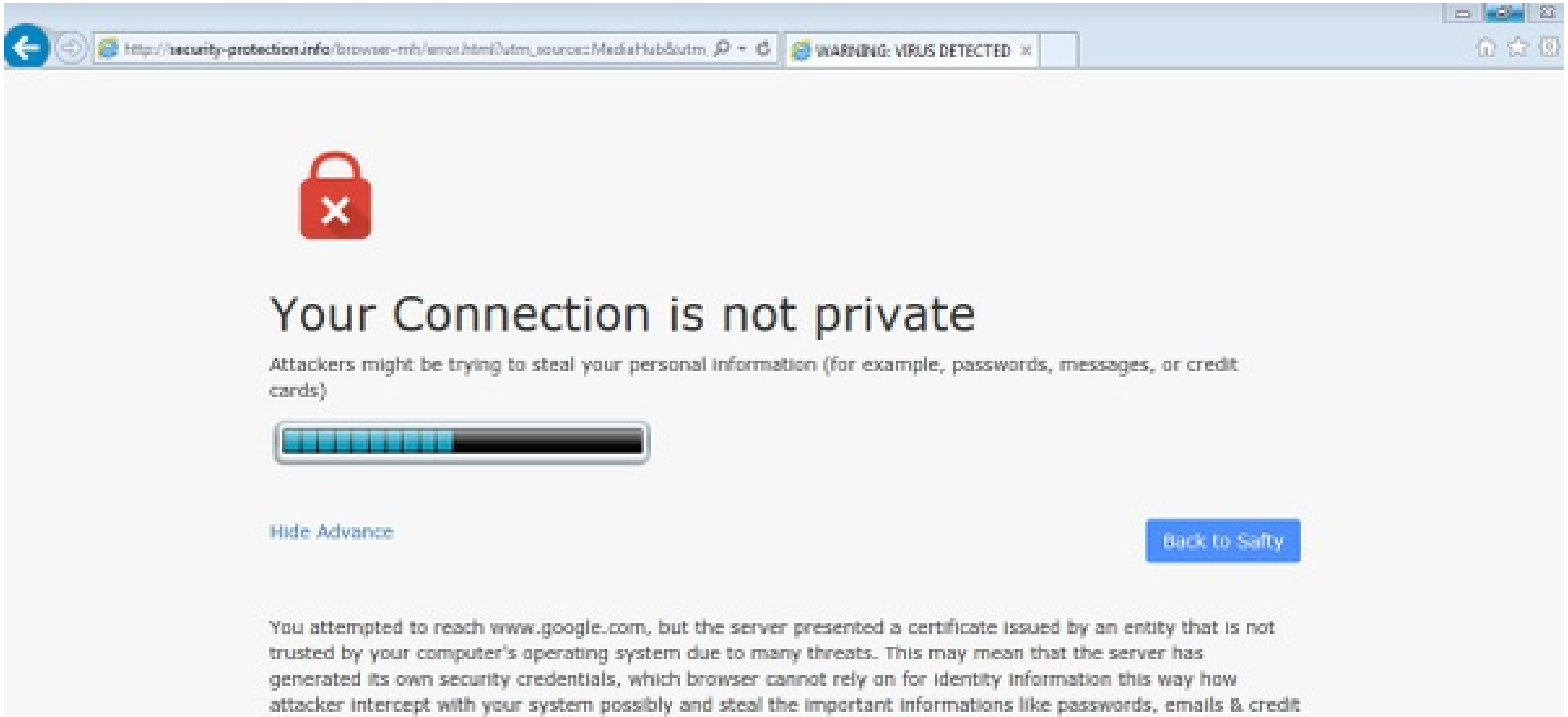
For more information about the FREAK attack, please go to www.freakattack.com.

To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

Jérôme Segura
@jeromesegura

Follow

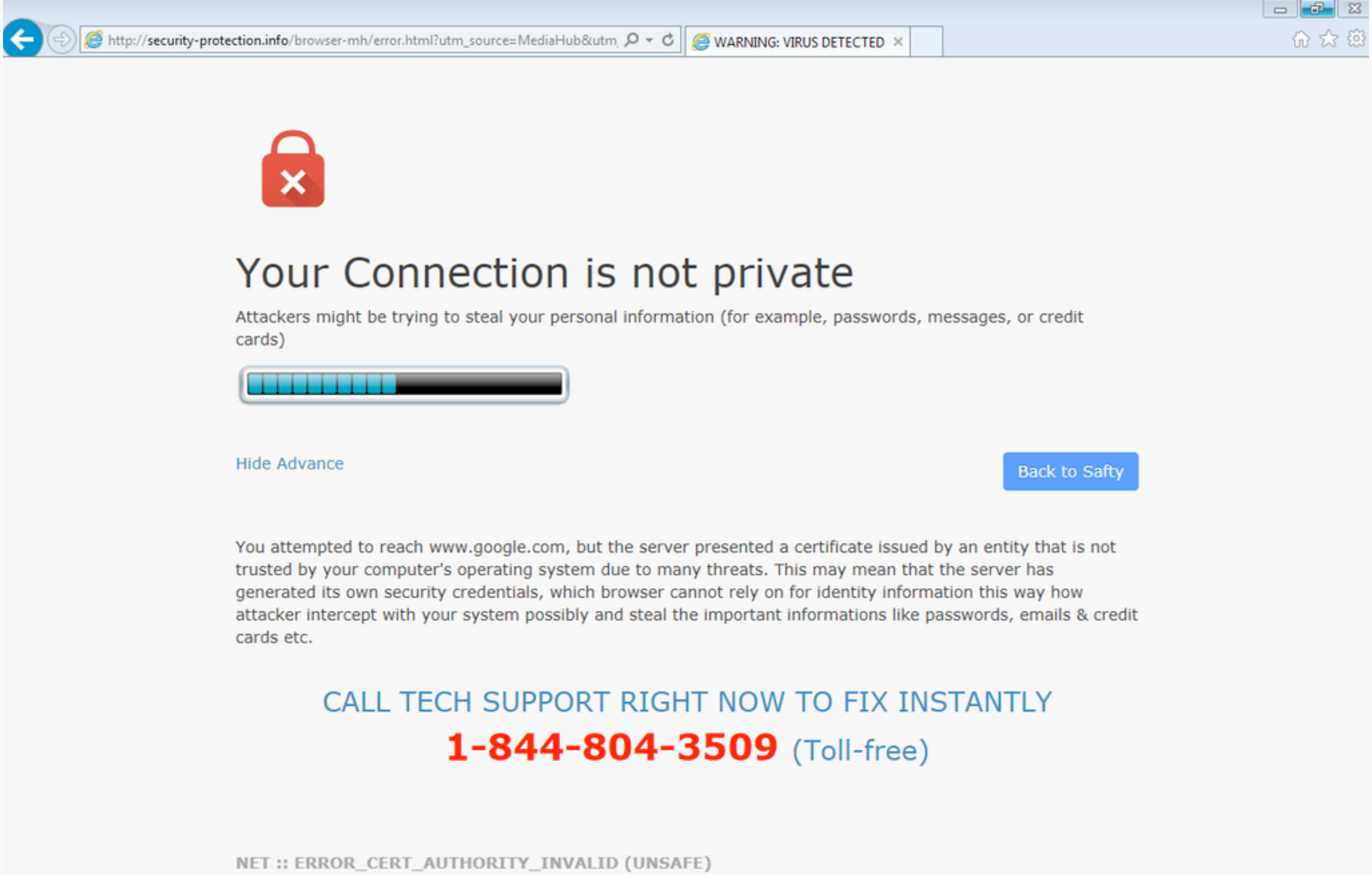
Invalid SSL certificate trick used as scare tactic #TechSupportScams


http://security-protection.info/browser-mh/error.html?utm_source=MediaHub&utm
WARNING: VIRUS DETECTED
Hide Advance
Back to Safty

Your Connection is not private

Attackers might be trying to steal your personal information (for example, passwords, messages, or credit cards)

You attempted to reach www.google.com, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system due to many threats. This may mean that the server has generated its own security credentials, which browser cannot rely on for identity information this way how attacker intercept with your system possibly and steal the important informations like passwords, emails & credit


http://security-protection.info/browser-mh/error.html?utm_source=MediaHub&utm_
WARNING: VIRUS DETECTED
Hide Advance
Back to Safty

Your Connection is not private

Attackers might be trying to steal your personal information (for example, passwords, messages, or credit cards)

You attempted to reach www.google.com, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system due to many threats. This may mean that the server has generated its own security credentials, which browser cannot rely on for identity information this way how attacker intercept with your system possibly and steal the important informations like passwords, emails & credit cards etc.

CALL TECH SUPPORT RIGHT NOW TO FIX INSTANTLY

1-844-804-3509 (Toll-free)

NET :: ERROR_CERT_AUTHORITY_INVALID (UNSAFE)

Phishing attack ahead

Attackers on **security-protection.info** might try to trick you to steal your information (for example, passwords, messages, or credit cards).

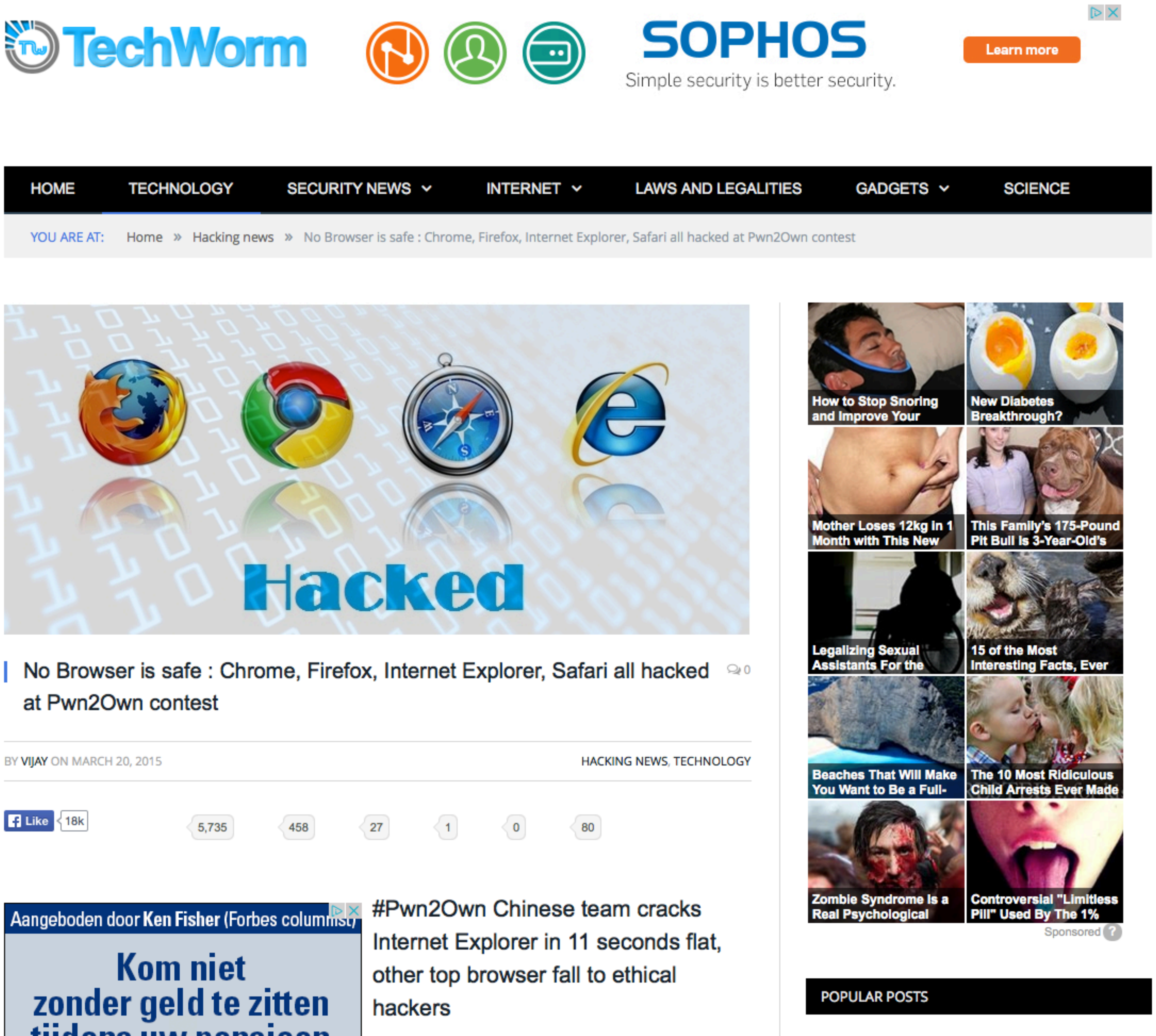
Details
Back to safety

Xtube porn website spreads malware, after being compromised by hackers

Graham Cluley | March 26, 2015 10:12 am | Filed under: **Adobe Flash**, **Malware**, **Vulnerability** | 3

Share 23 68 6
22 3 1

The popular Xtube hardcore porn website, visited by approximately 25 million people every month, has been compromised by hackers and is spreading malware onto visiting computers



No Browser is safe : Chrome, Firefox, Internet Explorer, Safari all hacked at Pwn2Own contest

0

BY VIJAY ON MARCH 20, 2015

HACKING NEWS, TECHNOLOGY

Like 18k 5,735 458 27 1 0 80

#Pwn2Own Chinese team cracks Internet Explorer in 11 seconds flat, other top browser fall to ethical hackers by the database.

8.5 SSL Usage Issues

Consider the following issues when using SSL:

- SSL use enables secure communication with other Oracle products, such as Oracle Internet Directory.
- Because SSL supports both authentication and encryption, the client/server connection is somewhat slower than the standard Oracle Net TCP/IP transport (using native encryption).
- Each SSL authentication mode requires configuration settings.
- Multi-threaded clients currently cannot use SSL.

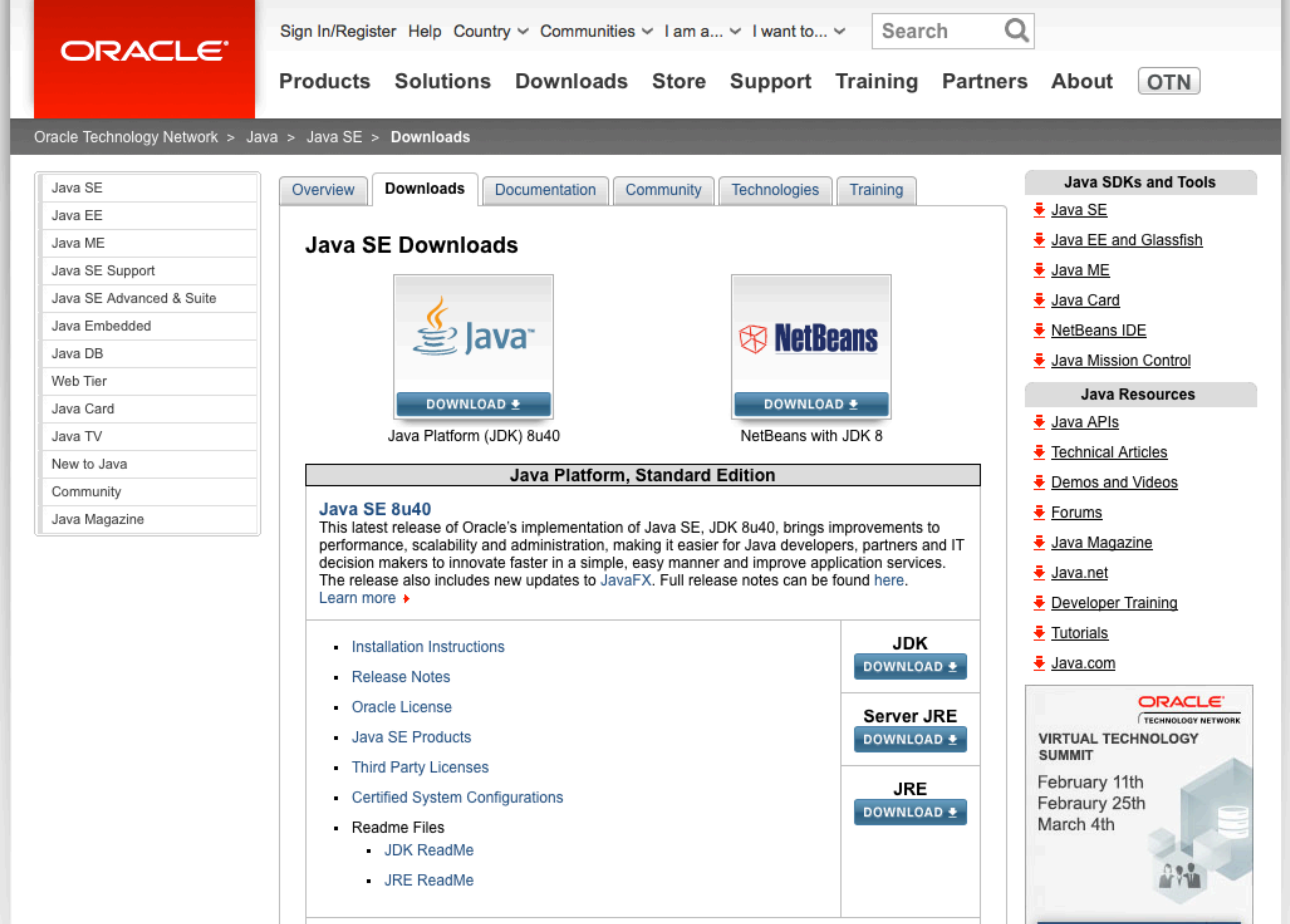
> **Note:**
>
> - U.S. government regulations prohibit double encryption. Accordingly, if you configure Oracle Advanced Security to use SSL encryption and another encryption method concurrently, then the connection fails. You also cannot configure SSL authentication concurrently with non-SSL authentication.
> - If you configure SSL encryption, you must disable non-SSL encryption. To disable such encryption, refer to "Disabling Oracle Advanced Security Authentication".

Each SSL authentication mode requires configuration settings.

Multi-threaded clients currently cannot use SSL.

Note:

- U.S. government regulations prohibit double encryption. Accordingly, if you configure Oracle Advanced Security to use SSL encryption and another encryption method concurrently, then the connection fails. You also cannot configure SSL authentication concurrently with non-SSL authentication.
- If you configure SSL encryption, you must disable non-SSL encryption. To disable such encryption, refer to "Disabling Oracle Advanced Security Authentication".



Java SE Downloads

Java Platform (JDK) 8u40

NetBeans with JDK 8

Java Platform, Standard Edition

Java SE 8u40

This latest release of Oracle's implementation of Java SE, JDK 8u40, brings improvements to performance, scalability and administration, making it easier for Java developers, partners and IT decision makers to innovate faster in a simple, easy manner and improve application services. The release also includes new updates to JavaFX. Full release notes can be found here.

Learn more

- Installation Instructions
- Release Notes
- Oracle License
- Java SE Products
- Third Party Licenses
- Certified System Configurations
- Readme Files
  - JDK ReadMe
  - JRE ReadMe

We know where you’ve been: Ars acquires 4.6M license plate scans from the cops

One citizen demands: "Do you know why Oakland is spying on me and my wife?"

by **Cyrus Farivar** - Mar 24, 2015 2:00pm CET

Share Tweet 183

LATEST FEATURE STORY

FEATURE STORY (3 PAGES)

AT&T’s plan to watch your Web browsing—and what you can do about it

Want to opt out? It could cost up to $744 extra per year.

WATCH ARS VIDEO

Foto: APA/dpa/Julian Stratenschulte

BND schnappt sich Kabel am DE-CIX (Symbolfoto)

MASSIVE VORWÜRFE

BND überwacht Hauptnetzknoten DE-CIX ohne Kontrolle

Letztes Update am 27.03.2015, 13:37

Bei einer Anhörung vor dem deutschen NSA-Untersuchungsausschuss erhebt der Manager des Frankfurter Knotenpunktes DE-CIX schwere Vorwürfe gegen den Bundesnachrichtendienst.

~~https~~://suchen.upc.at/suchen?q1=nsa
KB
4
85
0
4
4

Your connection is not private

Attackers might be trying to steal your information from **suchen.upc.at** (for example, passwords, messages, or credit cards).

Advanced
Back to safety

NET::ERR_CERT_AUTHORITY_INVALID

ANDROID-SCHADSOFTWARE

Vermeintlich ausgeschaltetes Smartphone hört mit

Eine neuartige Schadsoftware für Android-Geräte wurde entdeckt. Sie gaukelt ein abgeschaltetes Smartphone vor und kann es so unbemerkt als Abhörwerkzeug missbrauchen.

Android-Schadsoftware macht Smartphone zum Spionagewerkzeug. (Bild: Tobias Költzsch/Golem.de)

Datum:	20.2.2015, 10:05
Autor:	Ingo Pakalski
Themen:	Android, Malware, Smartphone, Virus, AVG, Security, Mobil
Teilen:	0 52 47 14
Tools:	Drucken

Bisher galt es eher als Filmstoff, jetzt ist es Realität: Das Smartphone ist abgeschaltet, kann aber weiterhin zum Ausspionieren benutzt werden. Möglich macht das eine Android-Schadsoftware, die dem Nutzer lediglich vorgaukelt, das Smartphone sei abgeschaltet, berichten die Sicherheitsspezialisten von AVG. Die Schadsoftware klinkt sich in den Android-Ausschaltprozess ein und verwendet dann einen eigenen Abschaltvorgang.

Fingierter Abschaltprozess

Der fingierte Abschaltvorgang sieht vom Aussehen her wie der normale Abschaltprozess aus. Auch die Animation zum Herunterfahren des Smartphones wird übernommen. Damit soll der Nutzer eines befallenen Geräts nicht

Security

Security firm finds preinstalled malware on Xiaomi Mi 4 smartphone

Above: Xiaomi's Mi 4 smartphone
Image Credit: Xiaomi

March 7, 2015 3:00 PM
Ruth Reader

921 0 431 436 73 501

Update: On Sunday March 8, Xiaomi contacted VentureBeat with a statement in response to the Bluebox report. Then on March 9, Bluebox told VentureBeat that the device may have been counterfeit and provided

Trending Research

Mobile App Analytics: What winning mobile developers use

Whitepapers

The DevOps Mindset: Real-World Insights From Tech Leaders

Should I Outsource Infrastructure?

Pitching Cloud to the Business

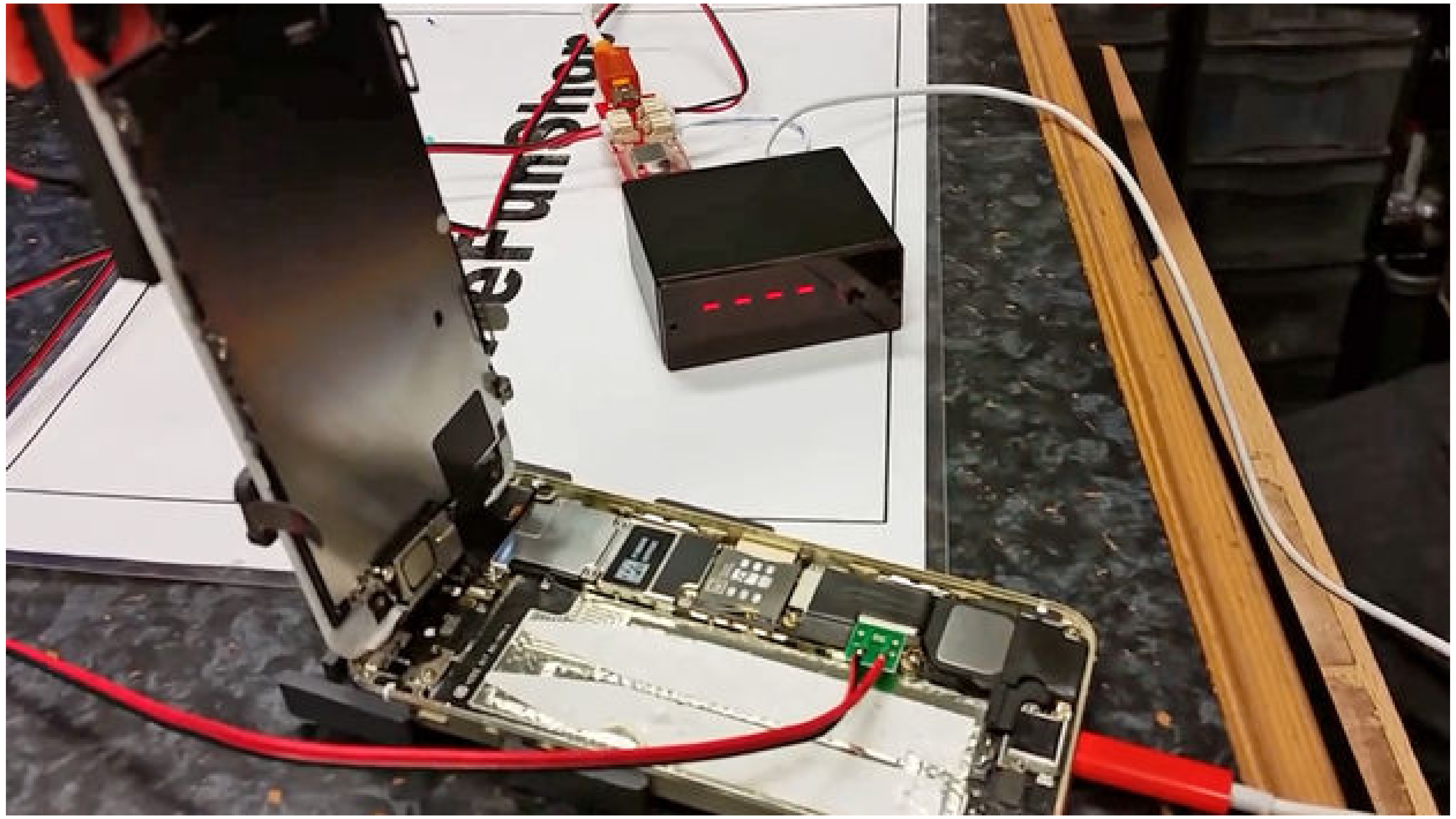
View More

futurezone
TECHNOLOGY NEWS

SICHERHEITSLÜCKE

IP-Box entsperrt iPhones auf brutale Art

20.03.15, 10:47 Mail an die Redaktion



Die IP-Box im Einsatz an einem geöffneten iPhone – Foto: Screenshot

SICHERHEITSLÜCKE

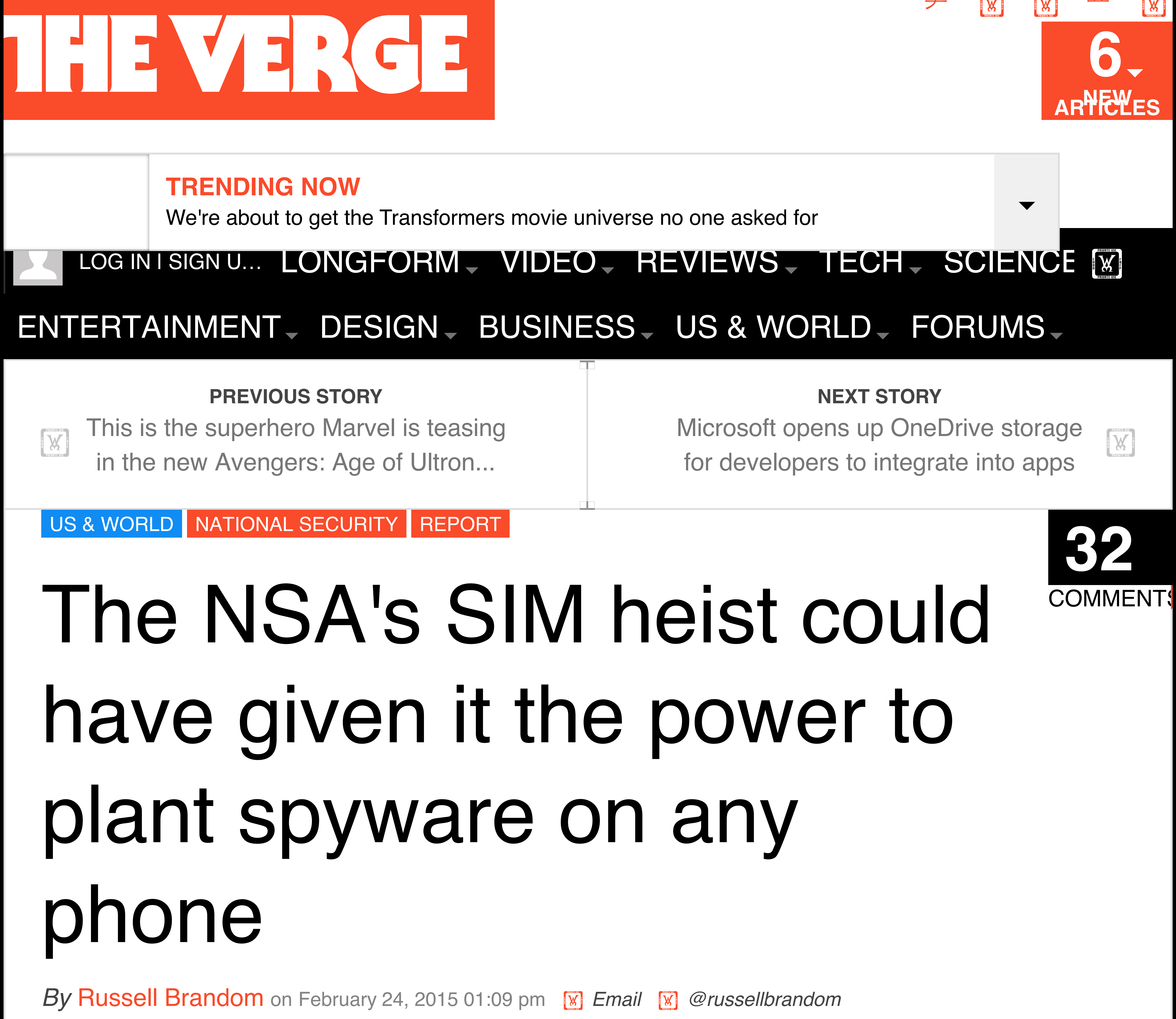
IP-Box entsperrt iPhones auf

Das Hacker-Werkzeug IP-Box probiert alle vierstelligen PIN-Codes für iPhones durch und verhindert, dass Fehlversuche vom Smartphone registriert werden.

FEATURED

GRILLEN

7 Apps für den perfekten Start



PREVIOUS STORY
This is the superhero Marvel is teasing in the new Avengers: Age of Ultron...

NEXT STORY
Microsoft opens up OneDrive storage for developers to integrate into apps

US & WORLD NATIONAL SECURITY REPORT

32 COMMENTS

The NSA's SIM heist could have given it the power to plant spyware on any phone

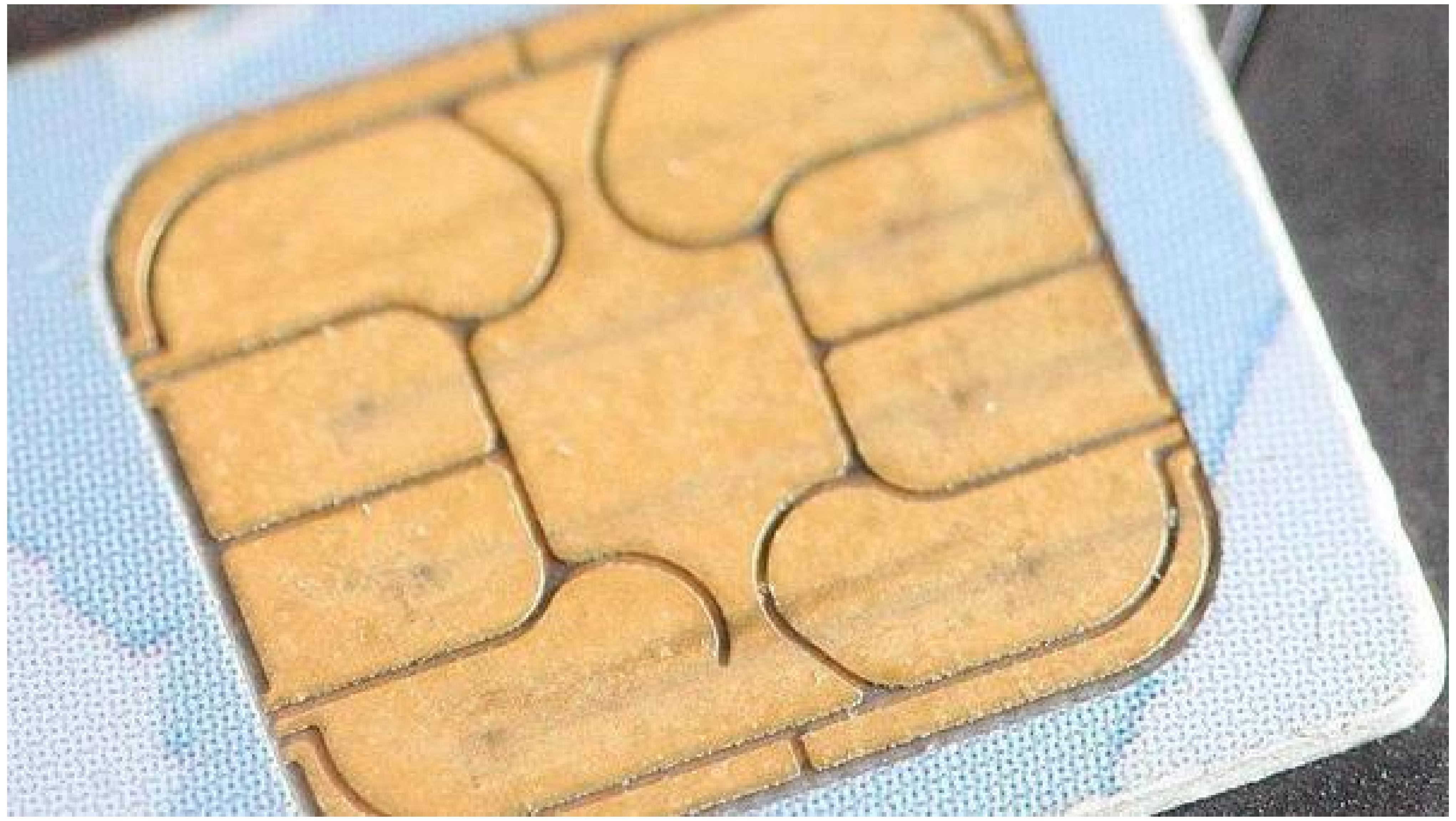
By Russell Brandom on February 24, 2015 01:09 pm Email @russellbrandom

28.02.2015 14:40

« Vorige | Nächste »

Telekom will umprogrammierbare SIM-Karte in vernetzten Geräten

vorlesen / MP3-Download



Aktuelle SiM-Karten sind fest auf eine Telefonnummer und einen Mobilfunk-Anbieter eingestellt. Das soll sich ändern. (Bild: dpa, Bernd Thissen)

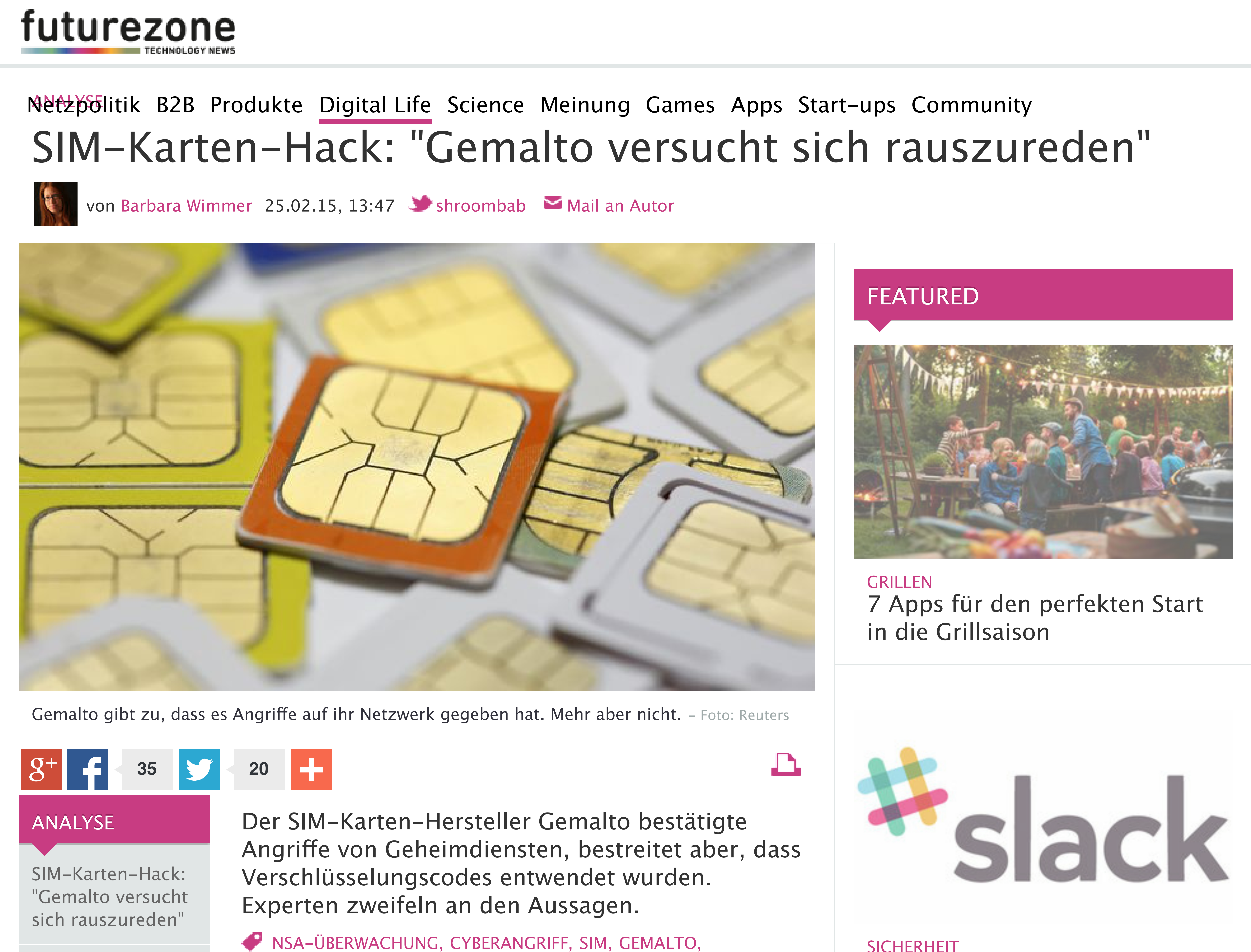
Top-News

Britische Safari-Nutzer können Google wegen Cookie-Betrug verklagen

Die Last eintöniger geistiger Tätigkeit bekämpfen - zum Tode des Informatik-Pioniers Friedrich L. Bauer

Facebook: Internet per HALE UAV und Künstliche Intelligenz fürs Netz

Gefährliches Gedächtnis der Grafikkarte



futurezone
TECHNOLOGY NEWS

Netzpolitik B2B Produkte Digital Life Science Meinung Games Apps Start-ups Community

ANALYSE

SIM-Karten-Hack: "Gemalto versucht sich rauszureden"

von Barbara Wimmer 25.02.15, 13:47 shroombab Mail an Autor

Gemalto gibt zu, dass es Angriffe auf ihr Netzwerk gegeben hat. Mehr aber nicht. – Foto: Reuters

g+ f 35 20 +

ANALYSE

SIM-Karten-Hack: "Gemalto versucht sich rauszureden"

Der SIM-Karten-Hersteller Gemalto bestätigte Angriffe von Geheimdiensten, bestreitet aber, dass Verschlüsselungscodes entwendet wurden. Experten zweifeln an den Aussagen.

NSA-ÜBERWACHUNG, CYBERANGRIFF, SIM, GEMALTO,

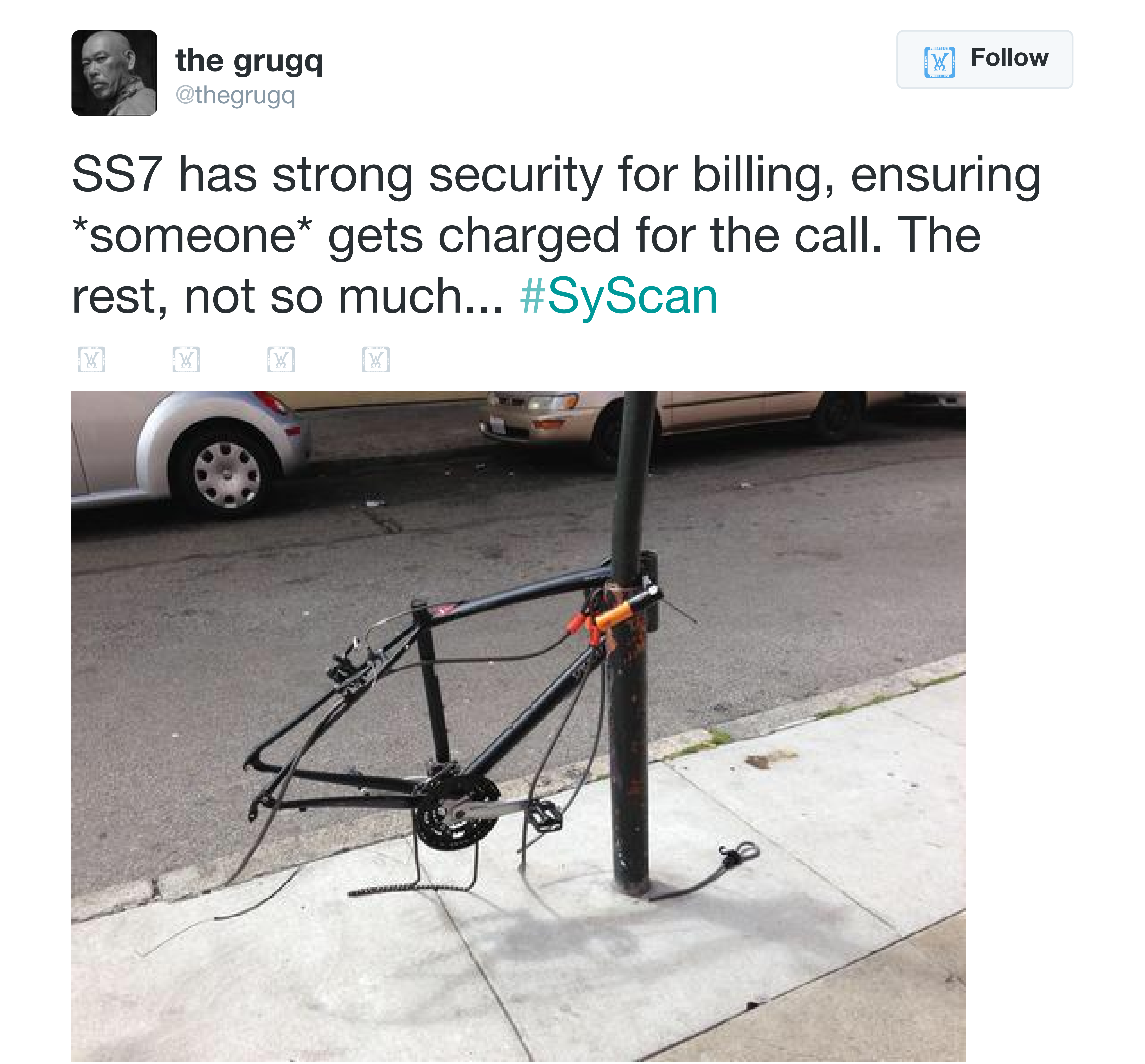
FEATURED

GRILLEN

7 Apps für den perfekten Start in die Grillsaison

slack

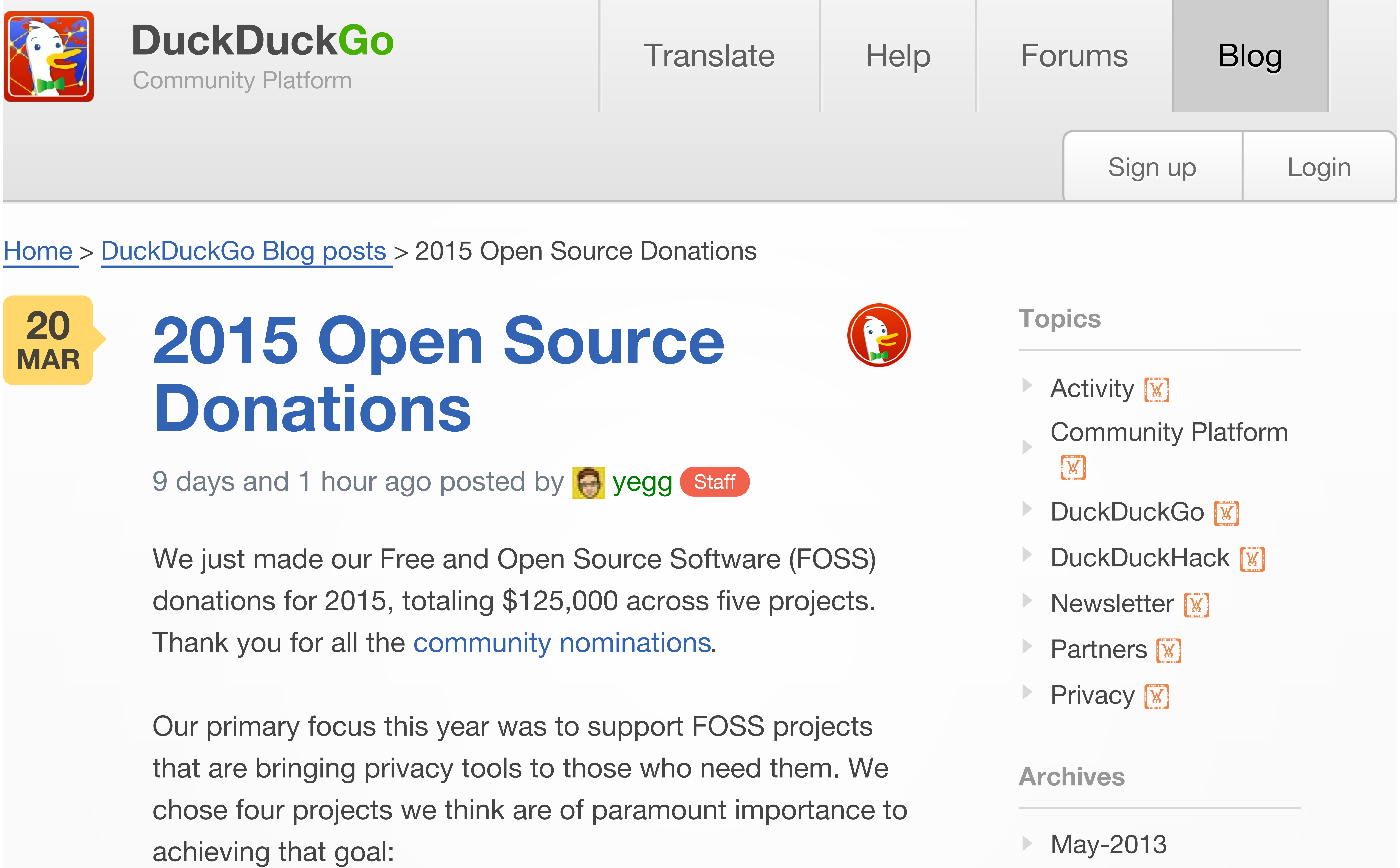
SICHERHEIT



the grugq
@thegrugq

SS7 has strong security for billing, ensuring *someone* gets charged for the call. The rest, not so much... #SyScan

+



Home > DuckDuckGo Blog posts > 2015 Open Source Donations

20 MAR

2015 Open Source Donations

9 days and 1 hour ago posted by yegg Staff

We just made our Free and Open Source Software (FOSS) donations for 2015, totaling $125,000 across five projects. Thank you for all the community nominations.

Our primary focus this year was to support FOSS projects that are bringing privacy tools to those who need them. We chose four projects we think are of paramount importance to achieving that goal:

Girl Develop It
GDI
don't be shy, develop it.

SD
SECUREDROP

Tails
TheAmnesicIncognitoLiveSystem

BETA

GPG TOOLS

MUST READ *Samsung Galaxy S6 or HTC One M9: Which Android flagship did you pre-order today?*

Topic: *Security*

Follow via:

NCC Group to audit OpenSSL for security holes

Summary: *With the support of the Linux Foundation's Core Infrastructure Initiative, the NCC Group will be auditing OpenSSL's source code for problems.*

By Steven J. Vaughan-Nichols for Linux and Open Source | March 7, 2015 -- 21:02 GMT (21:02 GMT)

Follow @sjvn

Get the ZDNet Announce UK newsletter now

Comments 5 | Share on Facebook 42 | Share 163 | more +

OpenSSL, arguably the world's most important Web security library with its support for Secure Sockets Layer (*SSL) and* Transport Layer Security (*TLS*) in such popular Web servers as Apache and Nginx, has had real trouble. First, there was HeartBleed and more recently there is FREAK. It's been one serious security problem after another. Now, the NCC Group, a well-regarded security company, will be auditing OpenSSL's code to catch errors before they appear in the wild.

Recommended

VMware sued for failure to comply with Linux license | ZDNet

Privacy Policy | Calendar | Site Map | Contacts | Wiki | Blog SUBSCRIBE JOIN THE IAB

Like 32k

SEARCH

ABOUT GUIDELINES & BEST PRACTICES MOBILE PUBLIC POLICY RESEARCH EVENTS & TRAINING MEMBERS C TIFICA

Home » IABlog

Search IABlog

SEARCH

Recent Entries

IAB at Mobile World Congress: Bringing Mobile Advertising and Technology Together

Adopting Encryption: The Need for HTTPS

IAB Releases Mobile Programmatic Playbook

How Marketers Can Make Data and Technology Work Better Together

Unleashing Mobile Native's Potential in 2015

About this Entry

This page contains a single

| Subscribe to IABlog

Adopting Encryption: The Need for HTTPS

By Brendan Riordan-Butterworth on March 25, 2015 2:00 PM | Permalink | Comments

It’s time to talk about security.

In fact, last year was the time to talk about security. From The New York Times to Google, the call went out for websites to encrypt communications with their users, protecting the integrity and privacy of information exchanged in both directions. Even the U.S. government heard this call, and is working to require HTTPS delivery of all publicly accessible Federal websites and web services.

This year, the advertising industry needs to finish catching up. Many ad systems are already supporting HTTPS - a survey of our membership late last year showed nearly 80% of member ad delivery systems supported HTTPS. That’s a good start, but doesn’t reflect the interconnectedness of the industry. A publisher moving to HTTPS delivery needs every tag on page, whether included directly or indirectly, to support HTTPS. That means that in addition to their ad server, the agency ad server, beacons from any data partners, scripts from verification and brand safety tools, and any other system required by the supply chain also needs to support HTTPS.

Let’s break that down a bit more - once a website decides to support HTTPS, they need to make sure that their primary ad server supports encryption. That ad server will sometimes need to include tags from brand safety, audience and viewability measurement, and other tools - all of which also need to support encryption. The publisher’s ad server will often direct to one of several agency ad servers, each of which will also need to serve over HTTPS. Each agency ad server also may include a variety of beacons or tags

KRIMINAL PRÄVENTION   POLIZEI

https:// s = Sicher

Der sicherste Weg ins Internet führt über eine sichere Verbindung. Wesentliche Voraussetzung ist dabei, dass die Daten verschlüsselt übermittelt werden. Die Übertragung ist nur dann sicher, wenn die Internetadresse in der Browserleiste mit „https://„ beginnt.

- Geben Sie vertrauliche und persönliche Daten, z.B. beim Online Banking oder beim Einkaufen im Internet, ausschließlich über verschlüsselte Seiten bekannt

- Sie erkennen diese an "https://" am Beginn der Internetadresse

Information vermittelt Wissen und Wissen schützt

- Die Spezialisten der Kriminalprävention stehen Ihnen gerne mit unabhängiger und kompetenter Beratung zur Verfügung.

- Für eine individuelle Beratung wenden Sie sich an ihr Landeskriminalamt / Assistenzbereich Kriminalprävention. Tel. 059 133

- Ein Besuch auf unserer Homepage unter www.bmi.gv.at lohnt sich auf jeden Fall. Sie erhalten neben Informationen über die verschiedenen Bereiche der Kriminalprävention auch wichtige Kontaktadressen

KRIMINAL PRÄVENTION   POLIZEI

NOTRUFNUMMERN

Feuerwehr	122
Polizei	133
Rettung	144
Euro-Notruf	112

POLIZEI Servicekarte einfach abnehmen und einstecken

Impressum: Bundeskriminalamt, Büro 1.6
Kriminalprävention und Opferhilfe
Adresse: Schlickplatz 6, 1090 Wien
Telefon: 01-24836-85452
www.bmi.gv.at/praevention

INTERNETKRIMINALITÄT

SO GEHEN SIE
AUF NUMMER SICHER
✆059 133

www.bmi.gv.at/praevention ✆059 133

https://www.bmi.gv.at/praevention
KB
0

This webpage is not available

Hide details
Reload

https://polizei.at
Details

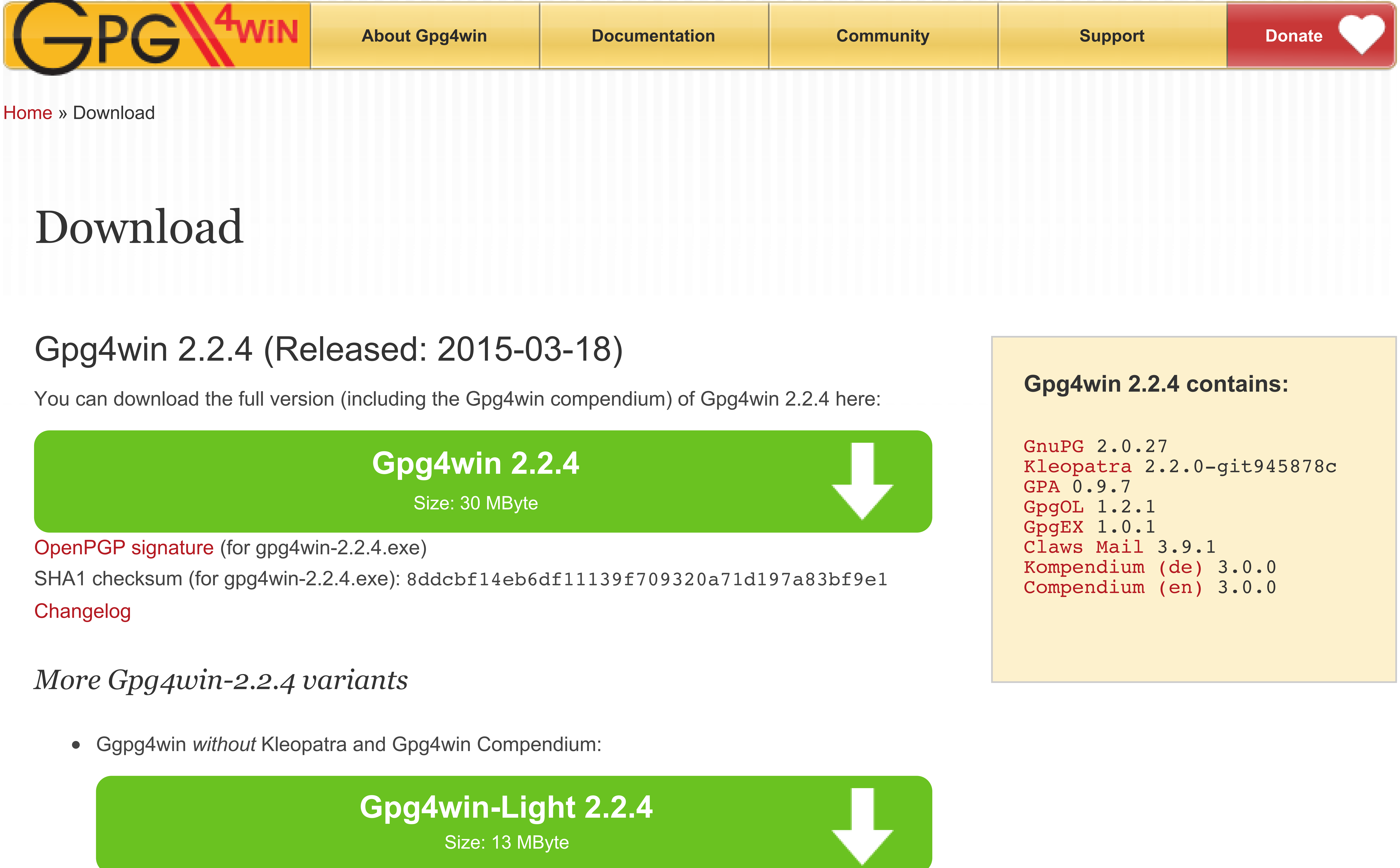
This webpage is not available

https://www.polizei.gv.at
KB
0
2
U
Hide details
Reload

This webpage is not available

Chromium could not load the webpage because **www.polizei.gv.at** took too long to respond. The website may be down, or you may be experiencing issues with your Internet connection.

Check your Internet connection



Home » Download

Download

Gpg4win 2.2.4 (Released: 2015-03-18)

You can download the full version (including the Gpg4win compendium) of Gpg4win 2.2.4 here:

Gpg4win 2.2.4

Size: 30 MByte

OpenPGP signature (for gpg4win-2.2.4.exe)

SHA1 checksum (for gpg4win-2.2.4.exe): `8ddcbf14eb6df11139f709320a71d197a83bf9e1`

Changelog

More Gpg4win-2.2.4 variants

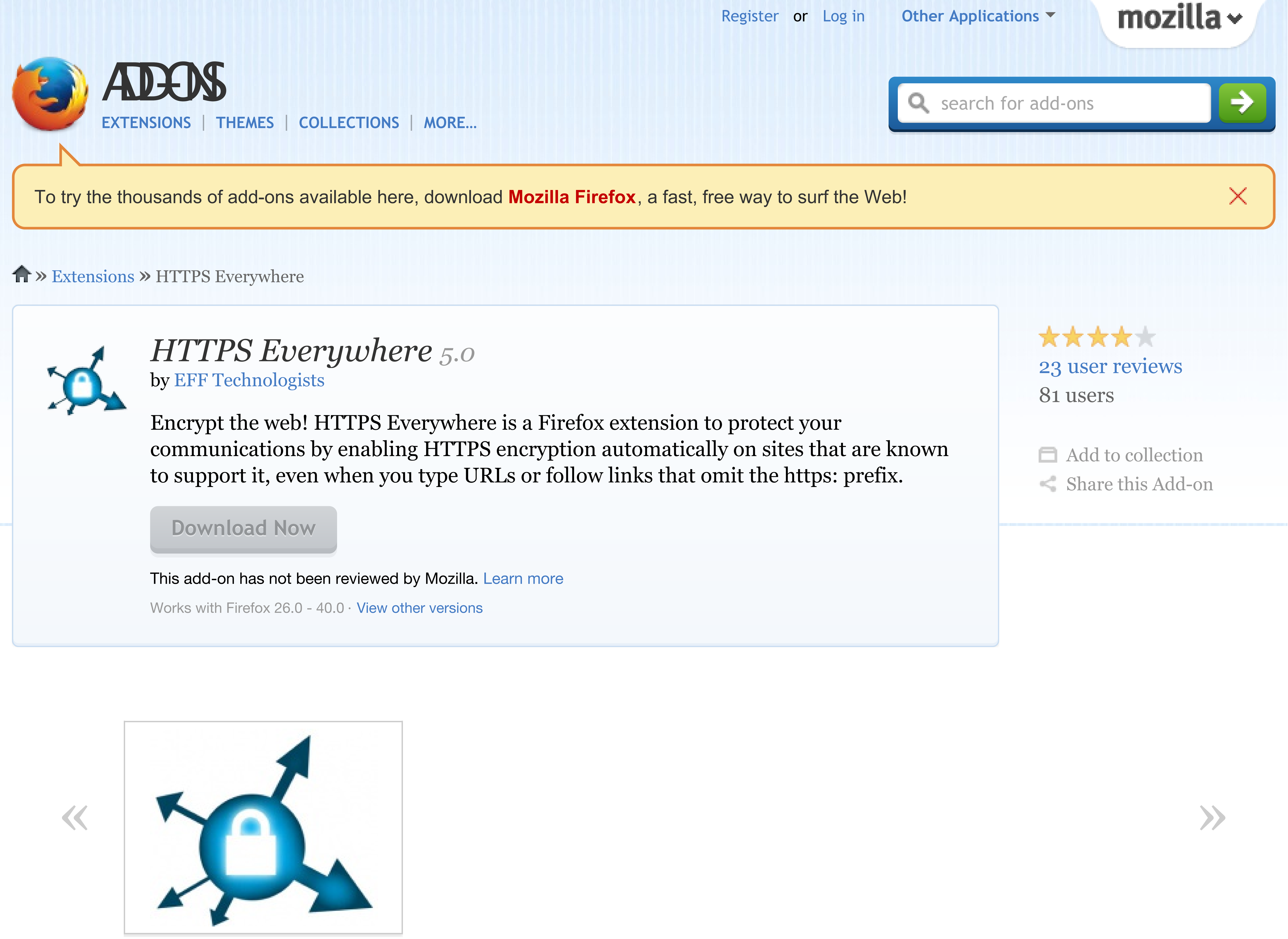
- Ggpg4win *without* Kleopatra and Gpg4win Compendium:

Gpg4win-Light 2.2.4

Size: 13 MByte

Gpg4win 2.2.4 contains:

```
GnuPG 2.0.27
Kleopatra 2.2.0-git945878c
GPA 0.9.7
GpgOL 1.2.1
GpgEX 1.0.1
Claws Mail 3.9.1
Kompendium (de) 3.0.0
Compendium (en) 3.0.0
```



To try the thousands of add-ons available here, download **Mozilla Firefox**, a fast, free way to surf the Web!

» Extensions » HTTPS Everywhere

HTTPS Everywhere 5.0
by EFF Technologists

Encrypt the web! HTTPS Everywhere is a Firefox extension to protect your communications by enabling HTTPS encryption automatically on sites that are known to support it, even when you type URLs or follow links that omit the https: prefix.

This add-on has not been reviewed by Mozilla. Learn more

Works with Firefox 26.0 - 40.0 · View other versions

★★★★☆
23 user reviews
81 users

HTTPS Everywhere

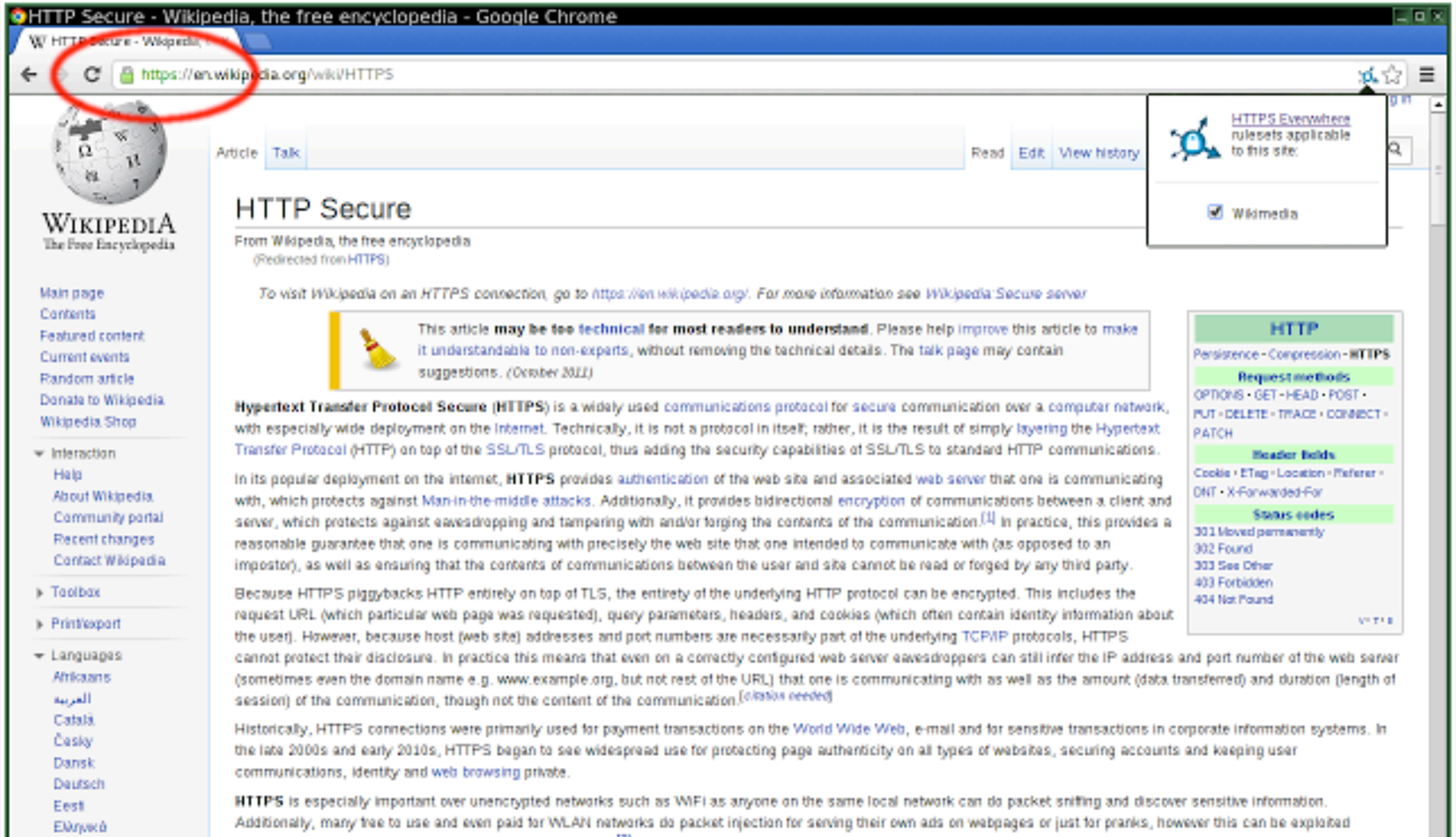
from www.eff.org

★★★★★ (1532) | Social & Communication | 816,371 users

ADDED TO CHROME

OVERVIEW | REVIEWS | SUPPORT | RELATED

g+1 1.6k



HTTP Secure

From Wikipedia, the free encyclopedia

(Redirected from HTTPS)

To visit Wikipedia on an HTTPS connection, go to https://en.wikipedia.org/. For more information see Wikipedia:Secure server

This article **may be too technical for most readers to understand**. Please help improve this article to make it understandable to non-experts, without removing the technical details. The talk page may contain suggestions. *(October 2011)*

Hypertext Transfer Protocol Secure (**HTTPS**) is a widely used communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

In its popular deployment on the internet, **HTTPS** provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication.[1] In practice, this provides a reasonable guarantee that one is communicating with precisely the web site that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

Because HTTPS piggybacks HTTP entirely on top of TLS, the entirety of the underlying HTTP protocol can be encrypted. This includes the request URL (which particular web page was requested), query parameters, headers, and cookies (which often contain identity information about the user). However, because host (web site) addresses and port numbers are necessarily part of the underlying TCP/IP protocols, HTTPS cannot protect their disclosure. In practice this means that even on a correctly configured web server eavesdroppers can still infer the IP address and port number of the web server (sometimes even the domain name e.g. www.example.org, but not rest of the URL) that one is communicating with as well as the amount (data transferred) and duration (length of session) of the communication, though not the content of the communication.[citation needed]

Historically, HTTPS connections were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems. In the late 2000s and early 2010s, HTTPS began to see widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.

HTTPS is especially important over unencrypted networks such as WIFI as anyone on the same local network can do packet sniffing and discover sensitive information. Additionally, many free to use and even paid for WLAN networks do packet injection for serving their own ads on webpages or just for pranks, however this can be exploited

HTTP

Persistence · Compression · **HTTPS**

Request methods

OPTIONS · GET · HEAD · POST · PUT · DELETE · TRACE · CONNECT · PATCH

Header fields

Cookie · ETag · Location · Referer · DNT · X-Forwarded-For

Status codes

301 Moved permanently
302 Found
303 See Other
403 Forbidden
404 Not Found

v · t · e

Encrypt the Web! Automatically use HTTPS security on many sites.

This is an port of the popular HTTPS Everywhere extension for Firefox, created by EFF and the Tor Project. It automatically switches thousands of sites from insecure "http" to secure "https". It will protect you against many forms of surveillance and account hijacking, and some forms of censorship.

Source code and bug tracker are available at https://github.com/efforg/https-everywhere. **Please do not submit bug reports in the reviews!** (I can't respond to them there.)

Changelog:

Website

Report Abuse

Version: 2015.3.23

Updated: March 24, 2015

Tor
HOME
ARCHIVES
ABOUT TOR
DONATE

Tor Browser 4.0.5 is released

Posted March 23rd, 2015 by gk in tbb, tbb-4.0, tor browser, tor browser bundle

A new release for the stable Tor Browser is available from the Tor Browser Project page and also from our distribution directory.

Tor Browser 4.0.5 is based on Firefox ESR 31.5.3, which features important security updates to Firefox. Additionally, it contains updates to Tor and NoScript.

Note to Tor Browser alpha users: There won't be a corresponding alpha release based on Firefox ESR 31.5.3 this time as we are currently in the midst of preparing releases based on ESR 31.6.0. Alpha users that can't wait another week are strongly recommended to use the Tor Browser 4.0.5 meanwhile.

Here is the changelog since 4.0.4:

- All Platforms
  - Update Firefox to 31.5.3esr
  - Update Tor 0.2.5.11
  - Update NoScript to 2.6.9.19

›› gk's blog

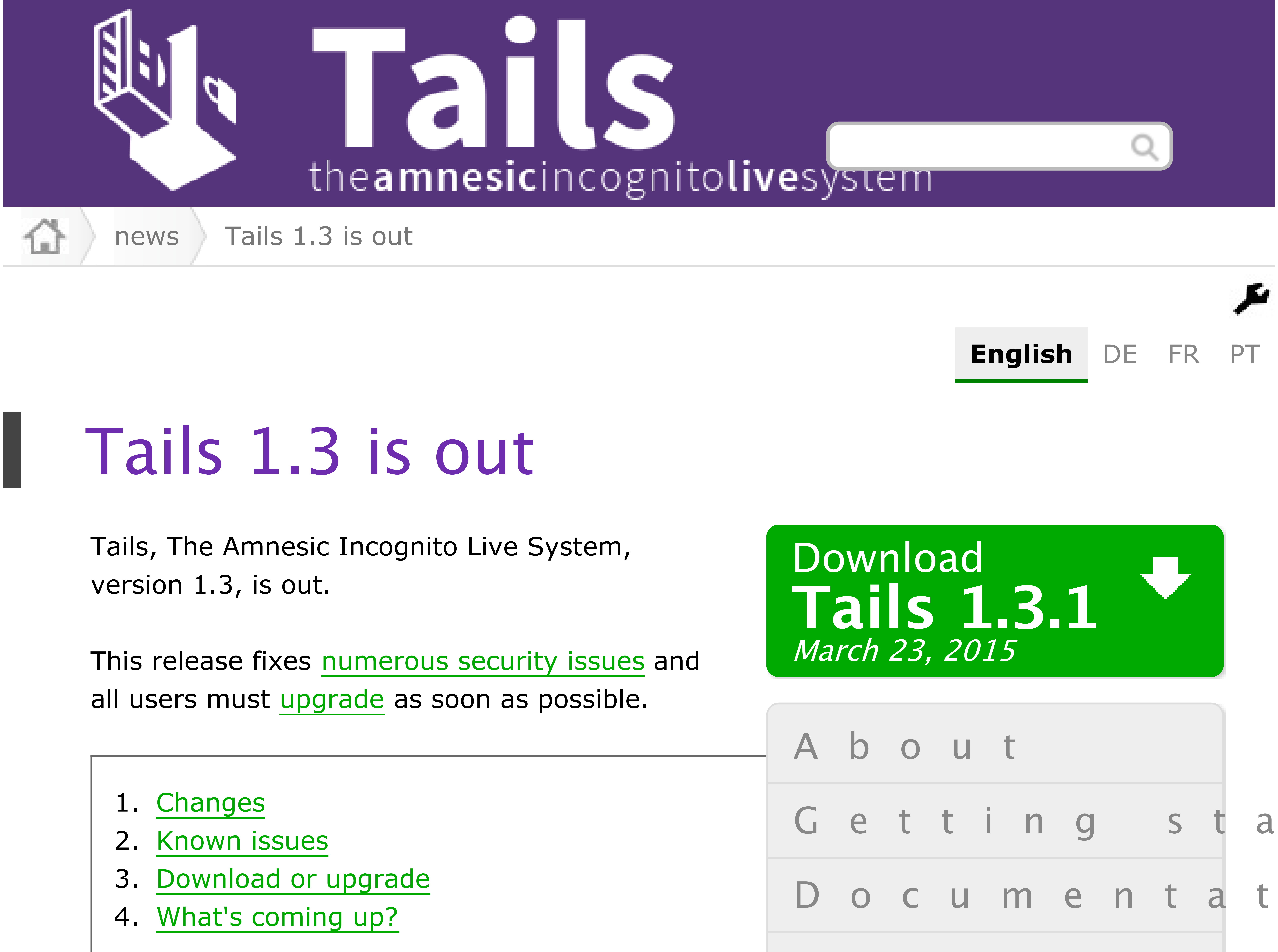
Upcoming events

- Many Tor people at PETS in Philadelphia
  (95 days on Jun 30)

full calendar

Recent blog posts

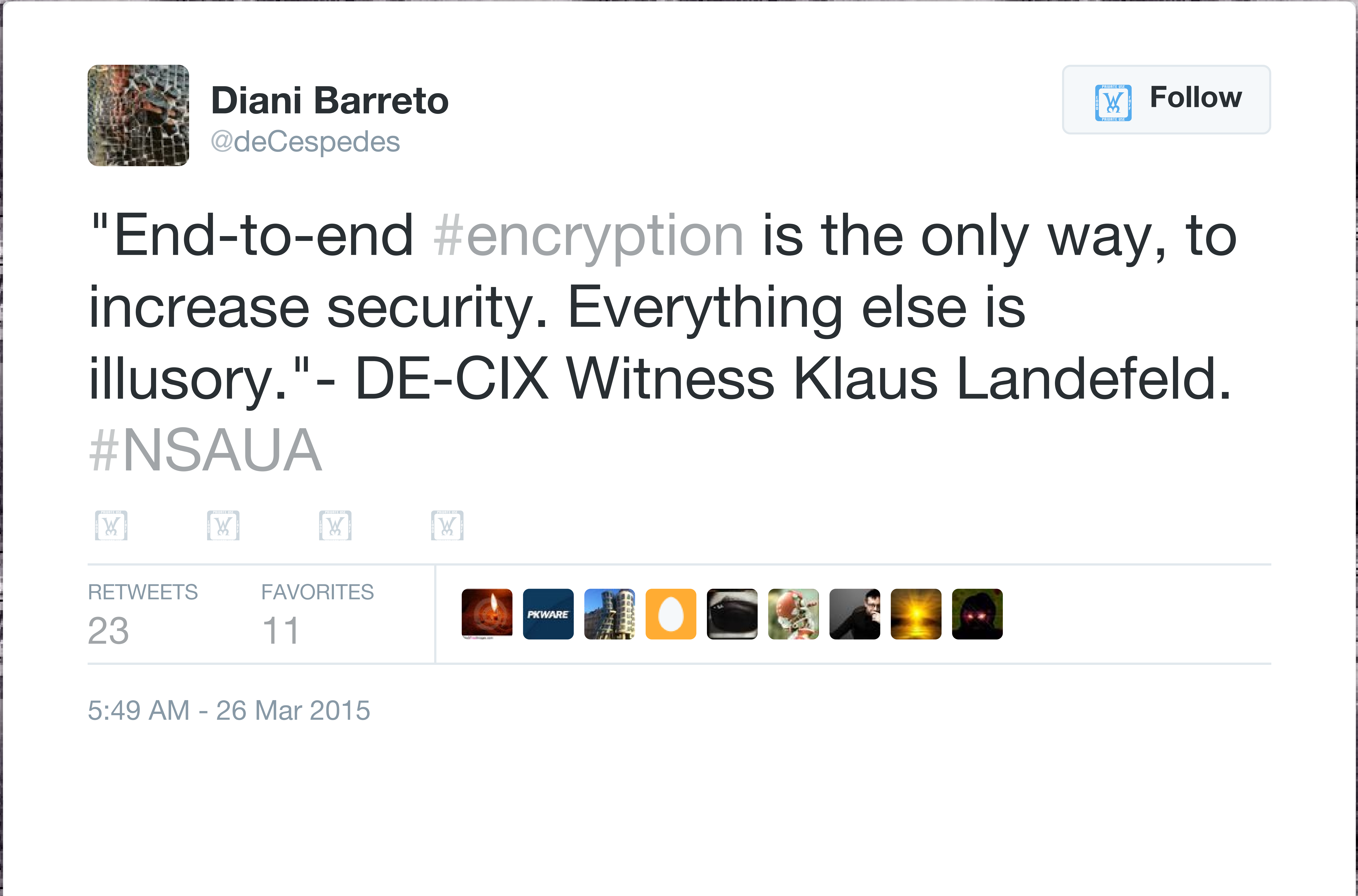
- Tor Weekly News — March 25th, 2015
- Tor 0.2.4.26 and 0.2.5.11 are released
- Tor Browser 4.0.5 is released
- Tor 0.2.6.5-rc is released



Tails 1.3 is out

Tails, The Amnesic Incognito Live System, version 1.3, is out.

This release fixes numerous security issues and all users must upgrade as soon as possible.



Diani Barreto
@deCespedes

Follow

"End-to-end #encryption is the only way, to increase security. Everything else is illusory."- DE-CIX Witness Klaus Landefeld. #NSAUA

RETWEETS
23

FAVORITES
11

5:49 AM - 26 Mar 2015

Mobiltelephone
GSM Netze
Security

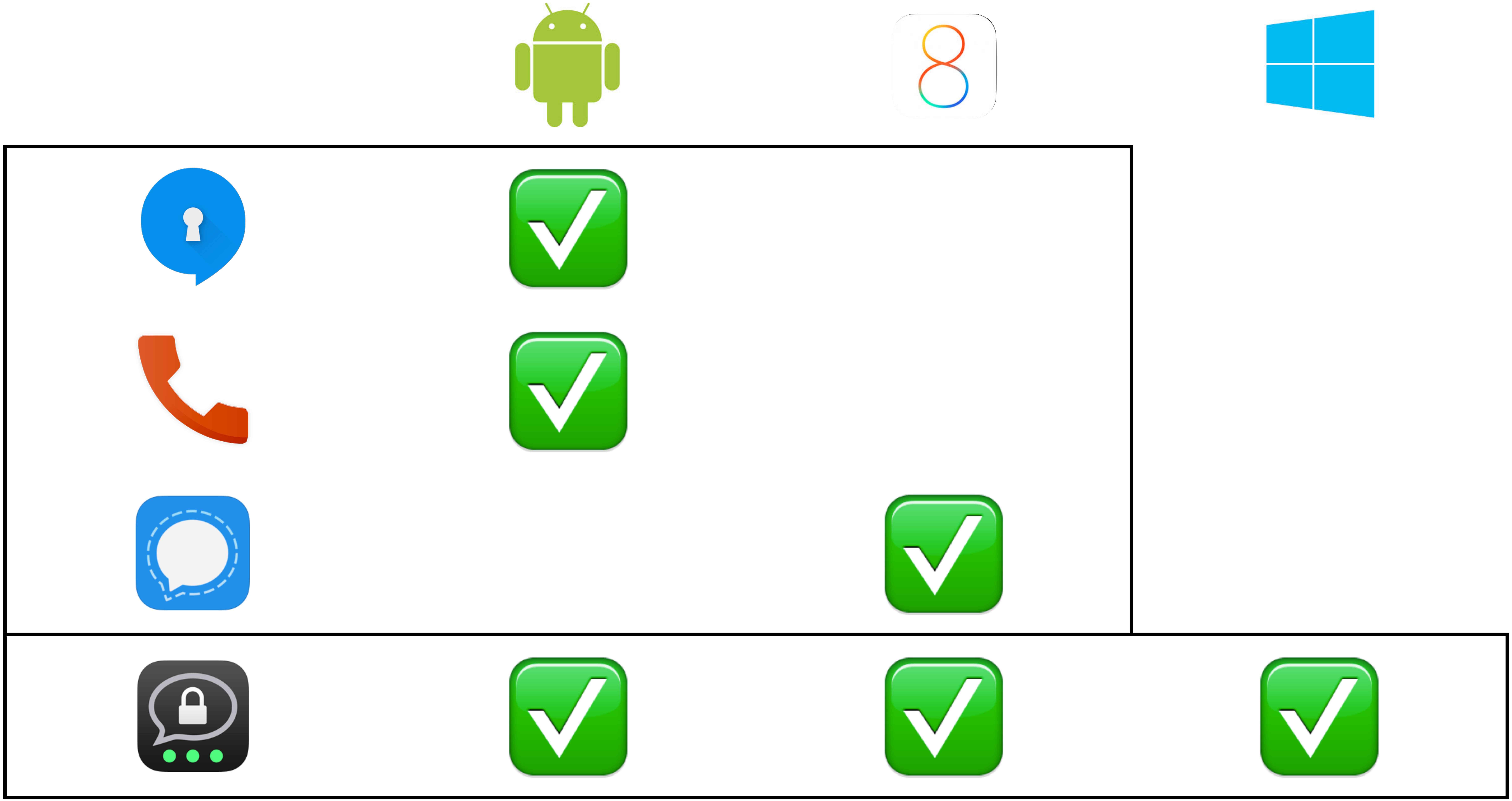
Verfügbarkeit

Threema

Signal

TextSecure

RedPhone



Optional:

GPG Key-Signing

Usorted

Android: Snoop Snitch?