TOMORROW'S NEWS IS TODAY'S INTEL

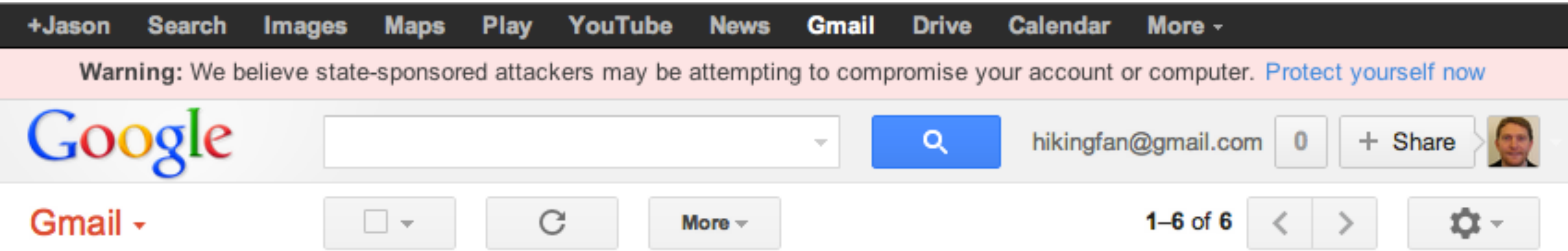
JOURNALISTS AS TARGETS AND COMPROMISE VECTORS

Shane Huntley
@shanehuntley

Morgan Marquis-Boire
@headhntr

Overview

- Why journalists
- The threats we see
- Regional Variation
- What we can do



Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now

Warning: We believe state-sponsored attackers may be to compromise your account or computer.

Protect yourself now.

US Constitution

Amendment I

Congress shall make no law ... abridging the freedom of speech, or of the press;

International Law

Article 19 of the Universal Declaration of Human Rights adopted in 1948 states simply that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers."

Watergate and Deep Throat

“Holding the powerful to account”

Watergate Scandal took down a President

Primary source,
“Deep Throat” secret for 30 years

The second oldest profession

Espionage, Spying and secrets

Who has great contact networks and traditionally poor operational security procedures?

Declassified documents show NSA spying on New York Times journalist Tom Wicker back in the 70’s under Project Minaret

Welcome to Today

Threats and Attacks

"In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google....

...this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a **wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted**."

-- Official Google Blog

The Media Giant

Fake questionnaire from Beijing News Office

Govt malware of .cn origin.

Opened by 10 employees.

Unfortunately, they believed anti-virus would protect them.

The Newspaper

National daily paper

Active compromise

Commercial government-only tools

European vendor

FINFISHER™: GOVERNMENTAL IT INTRUSION AND REMOTE MONITORING SOLUTIONS

GAMMA
INTERNATIONAL UK LIMITED

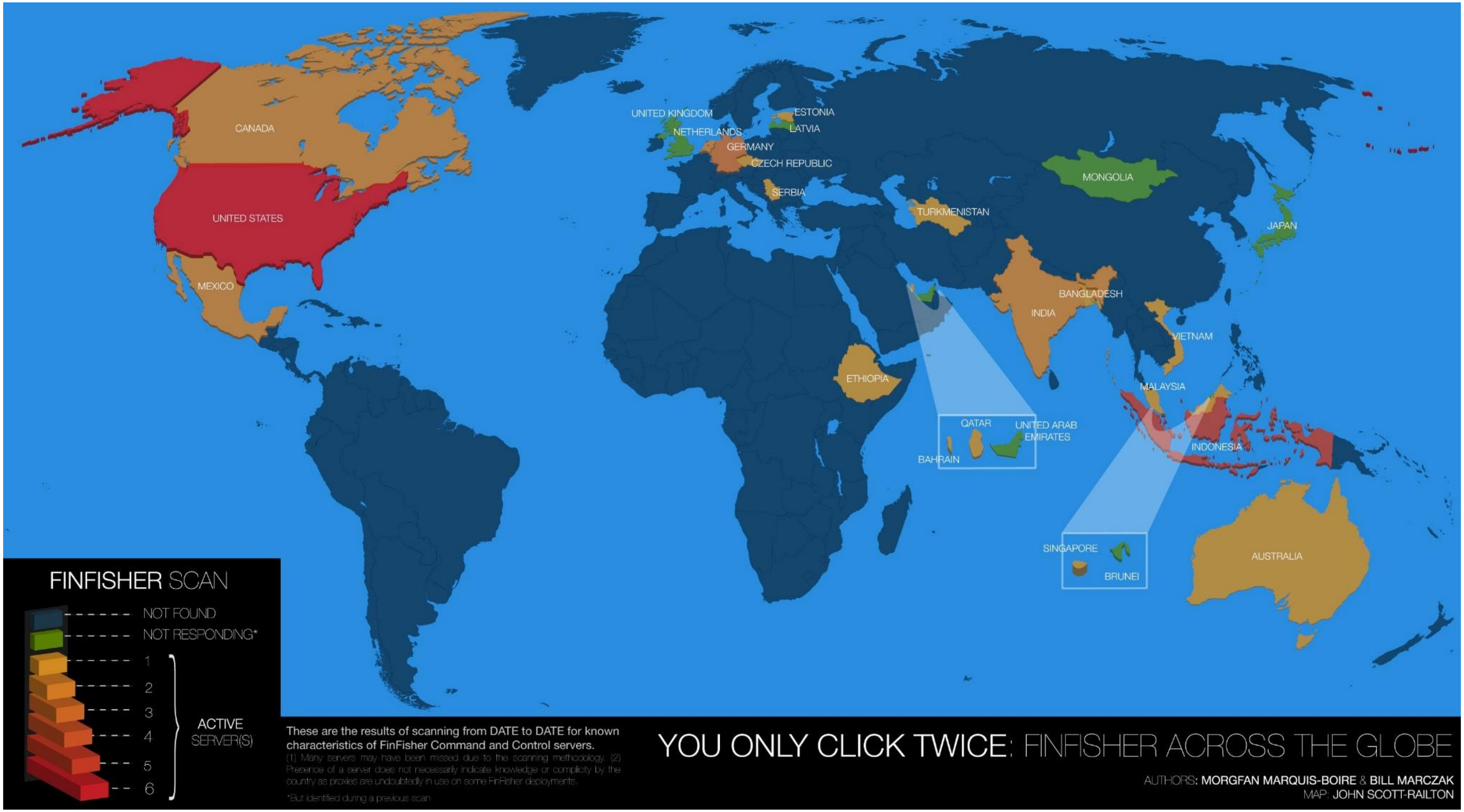
GAMMA INTERNATIONAL
UK LIMITED
Europe • Asia • Middle East • Africa

TO: State Security Investigation Department
Cairo
Egypt

OFFER NO. 0610-FF-GUK-061
DATE Tuesday June 29, 2010
CUSTOMER ID EGY-SSD
PAGE 6 / 12

ITEM #	DESCRIPTION	MODEL	QTY	UNIT PRICE (Euros)	LINE TOTAL (Euros)
A	**Remote Intrusion Solution**				
1	**FinSpy**				
1.1	**FinSpy Software**				
1.1.1	FinSpy Proxy License FinSpy Master License FinSpy Generation License	FSPL FSML FSGL	1	188,549.00	188,549.00
1.1.2	FinSpy Agent License (per client)	FSAGL	2	12,887.00	25,774.00
1.1.3	[illegible]				
				SUBTOTAL	**280,787.00**
				Freight	**6,350.00**
				TOTAL	**287,137.00**

FinFisher Global Proliferation



These are the results of scanning from DATE to DATE for known characteristics of FinFisher Command and Control servers.

(1) Many servers may have been missed due to the scanning methodology. (2) Presence of a server does not necessarily indicate knowledge or complicity by the country as proxies are undoubtedly in use on some FinFisher deployments.

*But identified during a previous scan

YOU ONLY CLICK TWICE: FINFISHER ACROSS THE GLOBE

AUTHORS: MORGFAN MARQUIS-BOIRE & BILL MARCZAK

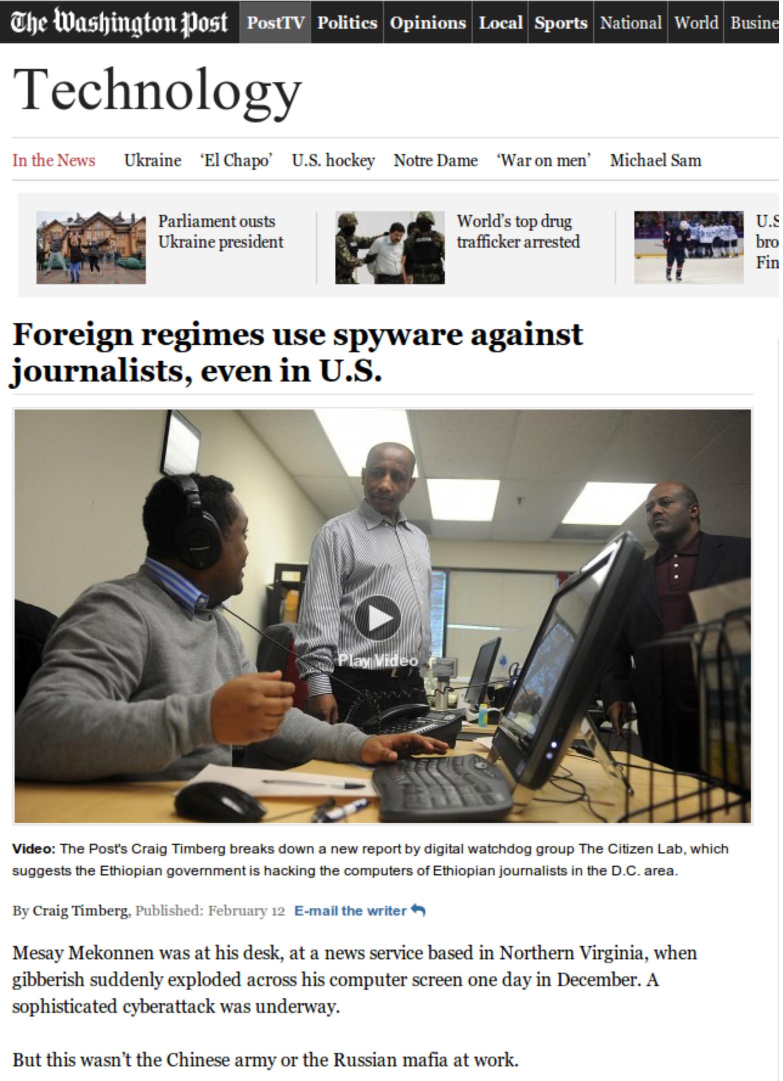
MAP: JOHN SCOTT-RAILTON

Citizen Journalists Targeted

Citizen Journalists Targeted

"Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d embrouilles…

http://freeme.eu5.org/scandale%20(2).doc"



Technology

Foreign regimes use spyware against journalists, even in U.S.

Video: The Post's Craig Timberg breaks down a new report by digital watchdog group The Citizen Lab, which suggests the Ethiopian government is hacking the computers of Ethiopian journalists in the D.C. area.

By Craig Timberg, Published: February 12 E-mail the writer

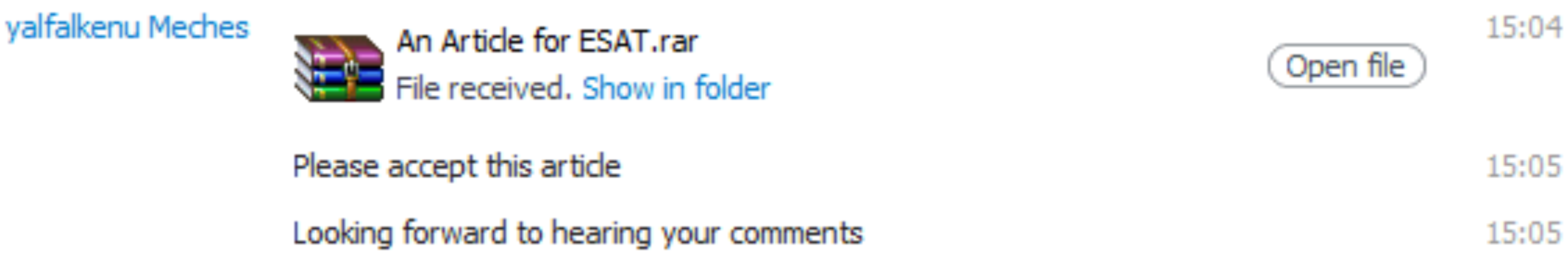
Mesay Mekonnen was at his desk, at a news service based in Northern Virginia, when gibberish suddenly exploded across his computer screen one day in December. A sophisticated cyberattack was underway.

But this wasn't the Chinese army or the Russian mafia at work.

Africa - ESAT

"In the space of two hours on 20 December 2013, an attacker made three separate attempts to target two ESAT employees with sophisticated computer spyware"

ESAT - First Attempt



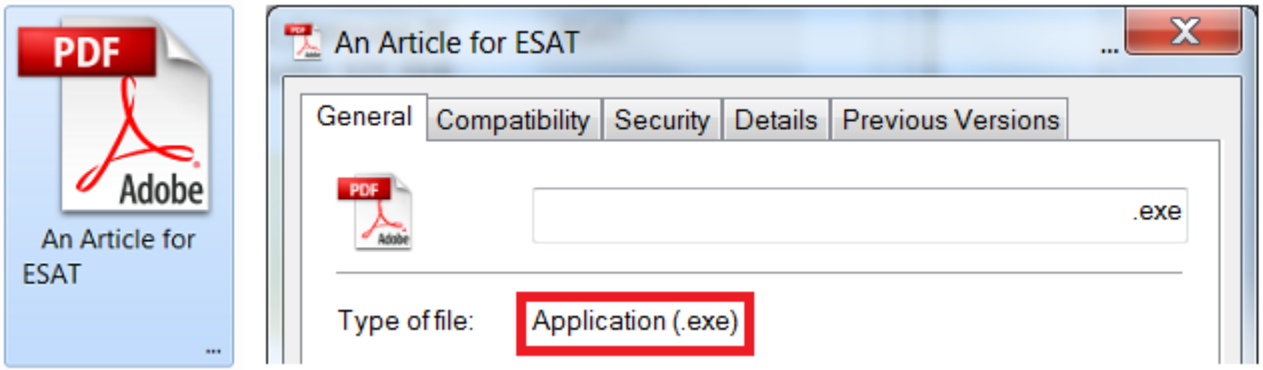
yalfalkenu Meches

An Article for ESAT.rar 15:04

File received. Show in folder

Please accept this article 15:05

Looking forward to hearing your comments 15:05

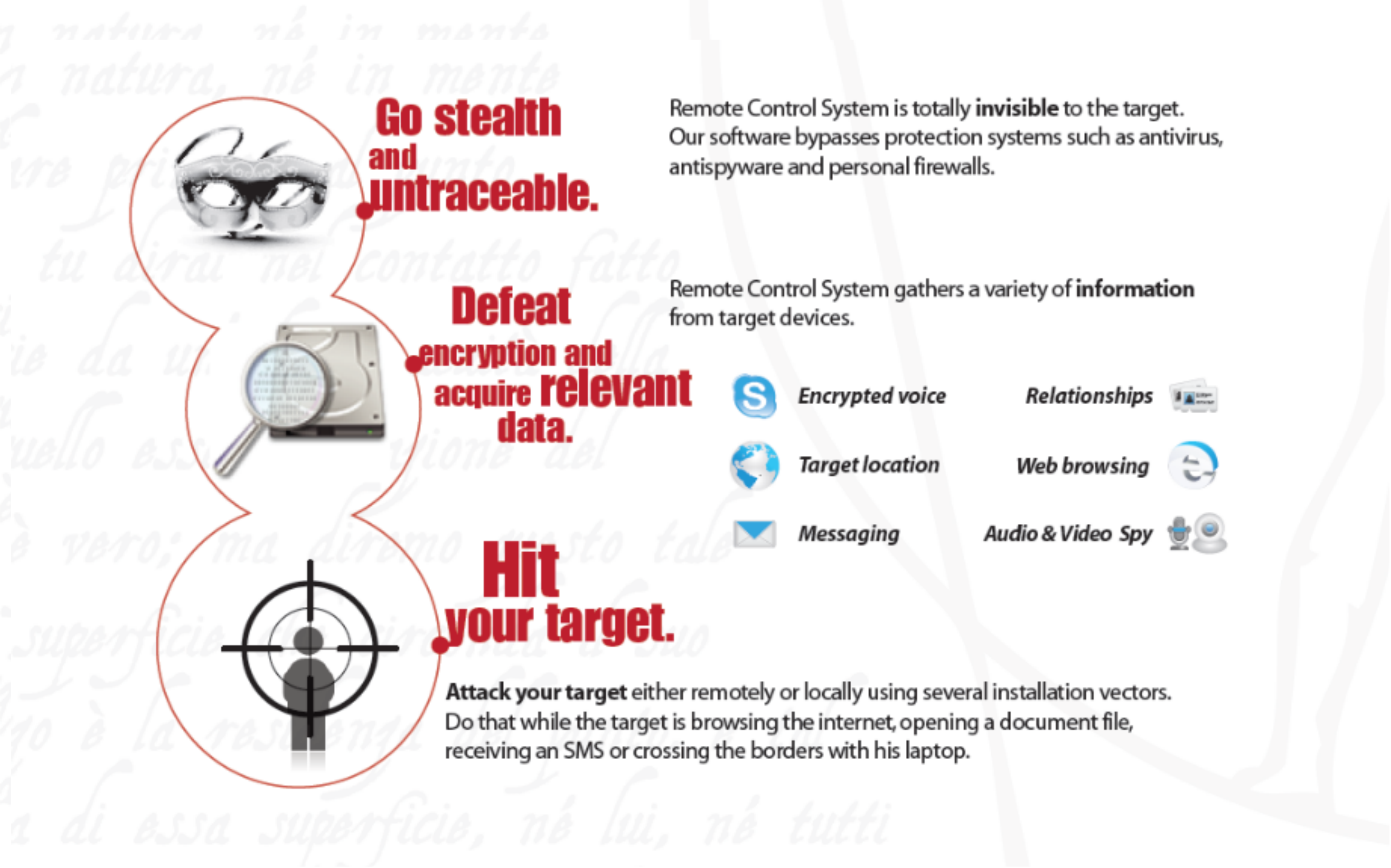


An Article for ESAT

An Article for ESAT

.exe

Type of file: Application (.exe)



Go stealth and untraceable.

Remote Control System is totally **invisible** to the target. Our software bypasses protection systems such as antivirus, antispyware and personal firewalls.

Defeat encryption and acquire relevant data.

Remote Control System gathers a variety of **information** from target devices.

- *Encrypted voice*
- *Target location*
- *Messaging*
- *Relationships*
- *Web browsing*
- *Audio & Video Spy*

Hit your target.

Attack your target either remotely or locally using several installation vectors. Do that while the target is browsing the internet, opening a document file, receiving an SMS or crossing the borders with his laptop.

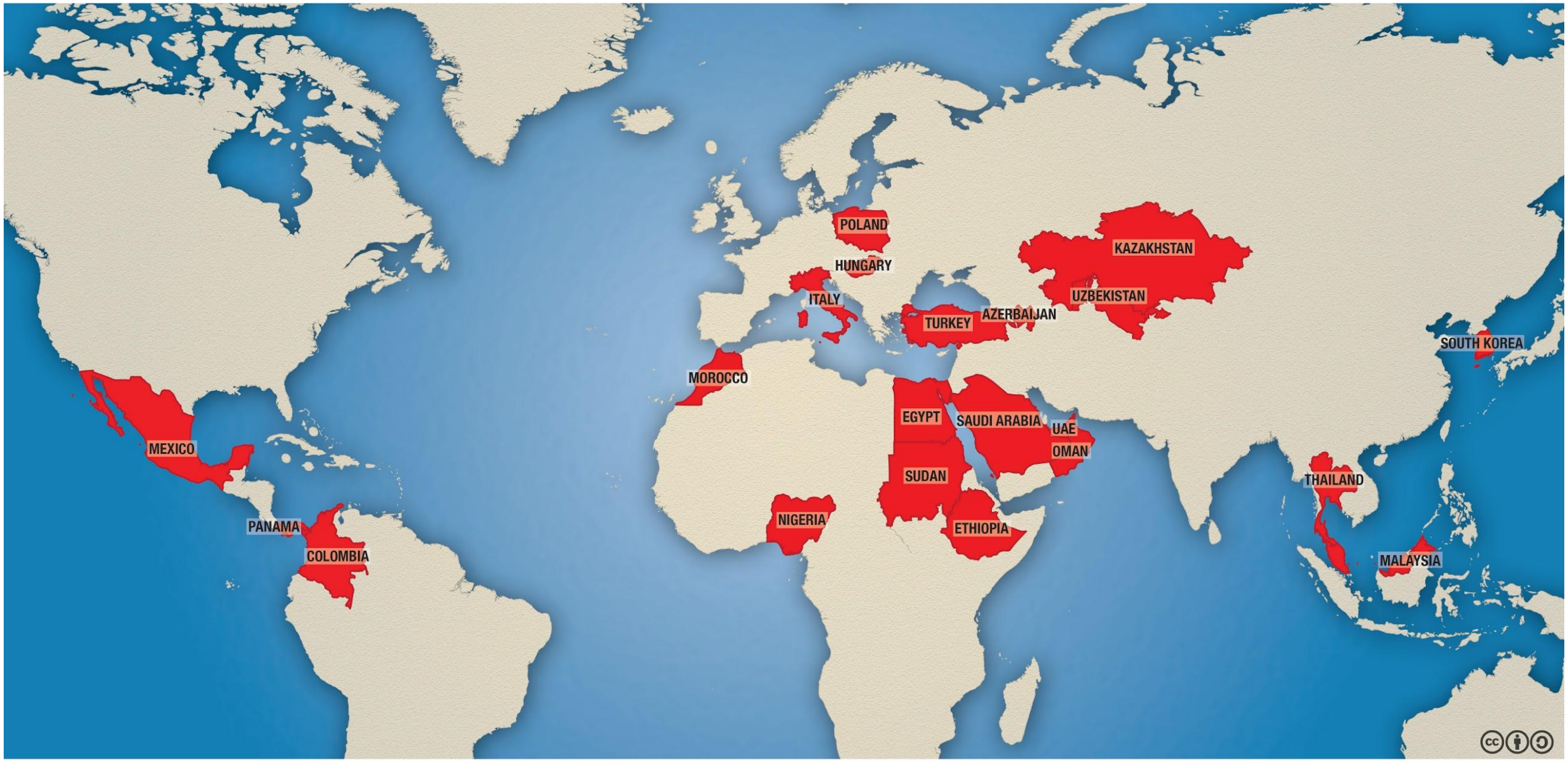
Description of RCS in a 2011 official brochure.[17]

HACKING TEAM RCS

Suspected Government Users Worldwide

Citizen Lab 2014

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire & John Scott-Railton



21 SUSPECTED GOVERNMENT USERS

AMERICAS	EUROPE	MIDDLE EAST	AFRICA	ASIA
Mexico Colombia Panama	Hungary Italy Poland Turkey	**Oman** **Saudi Arabia** **UAE**	**Egypt** **Ethiopia** **Morocco** **Nigeria** **Sudan**	**Azerbaijan** **Kazakhstan** Malaysia Thailand South Korea **Uzbekistan**

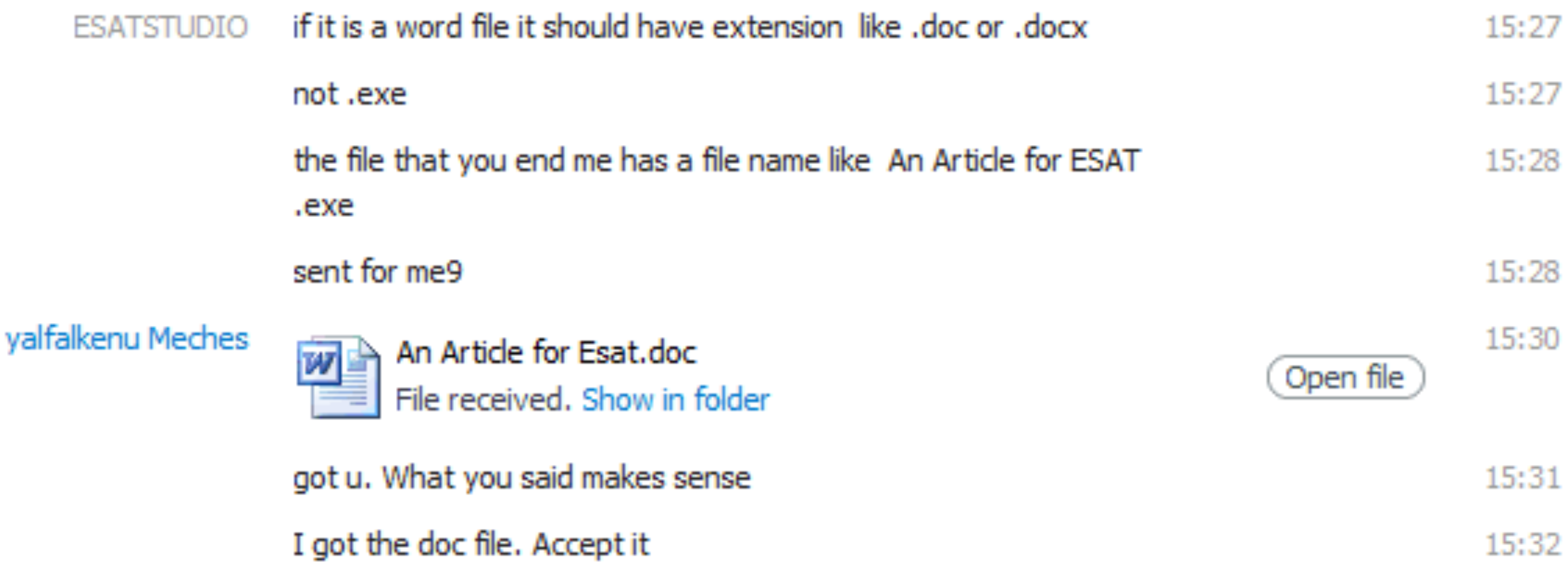
CAUSE FOR CONCERN

52% (**in bold**) fall in the bottom 3rd of a World Bank ranking* of freedom of expression and accountability

29% are in the bottom 3rd for Rule of Law

*World Bank 2012 WGI

ESAT - Second Attempt



ESATSTUDIO if it is a word file it should have extension like .doc or .docx 15:27

not .exe 15:27

the file that you end me has a file name like An Article for ESAT .exe 15:28

sent for me9 15:28

yalfalkenu Meches An Article for Esat.doc 15:30

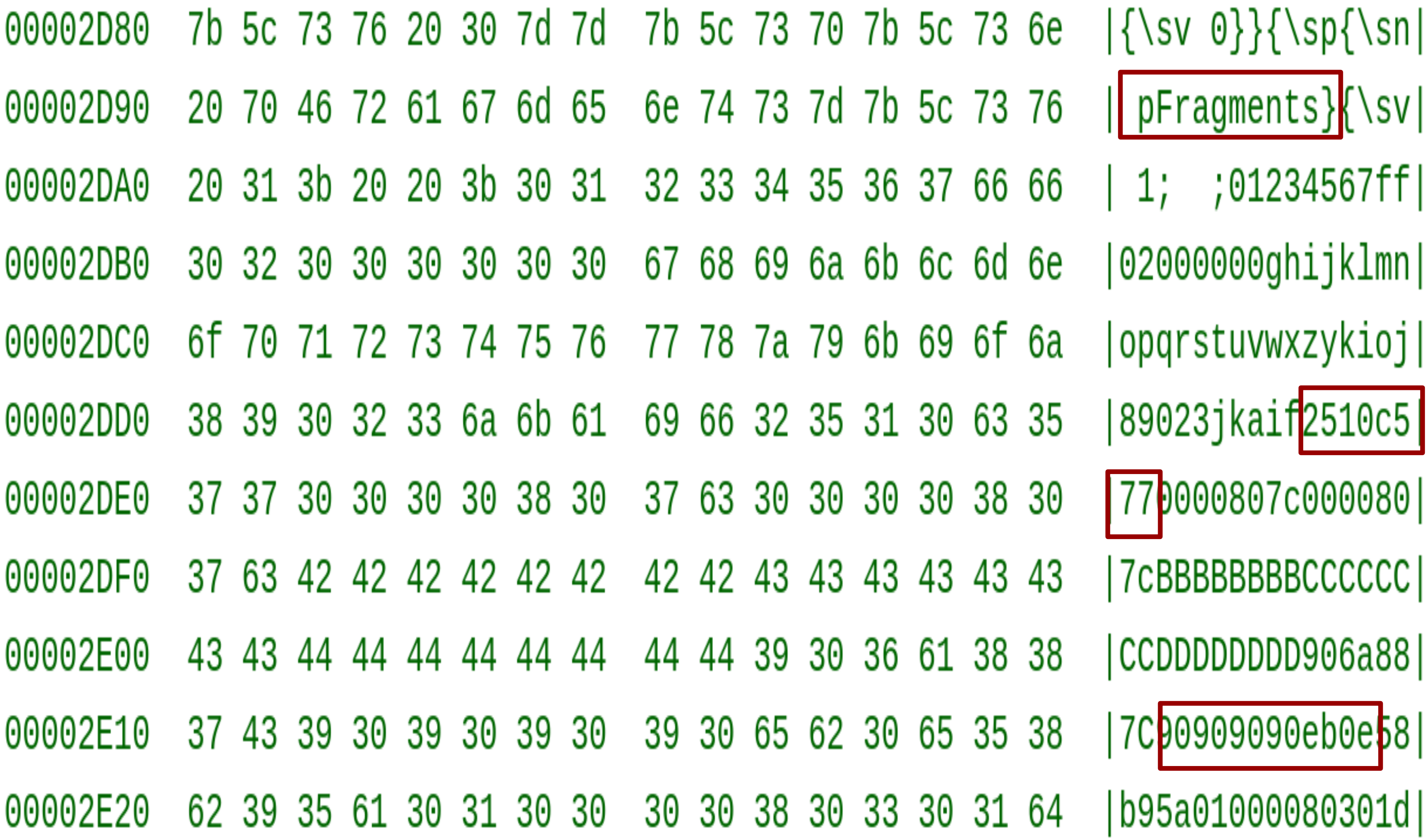
File received. Show in folder

got u. What you said makes sense 15:31

I got the doc file. Accept it 15:32

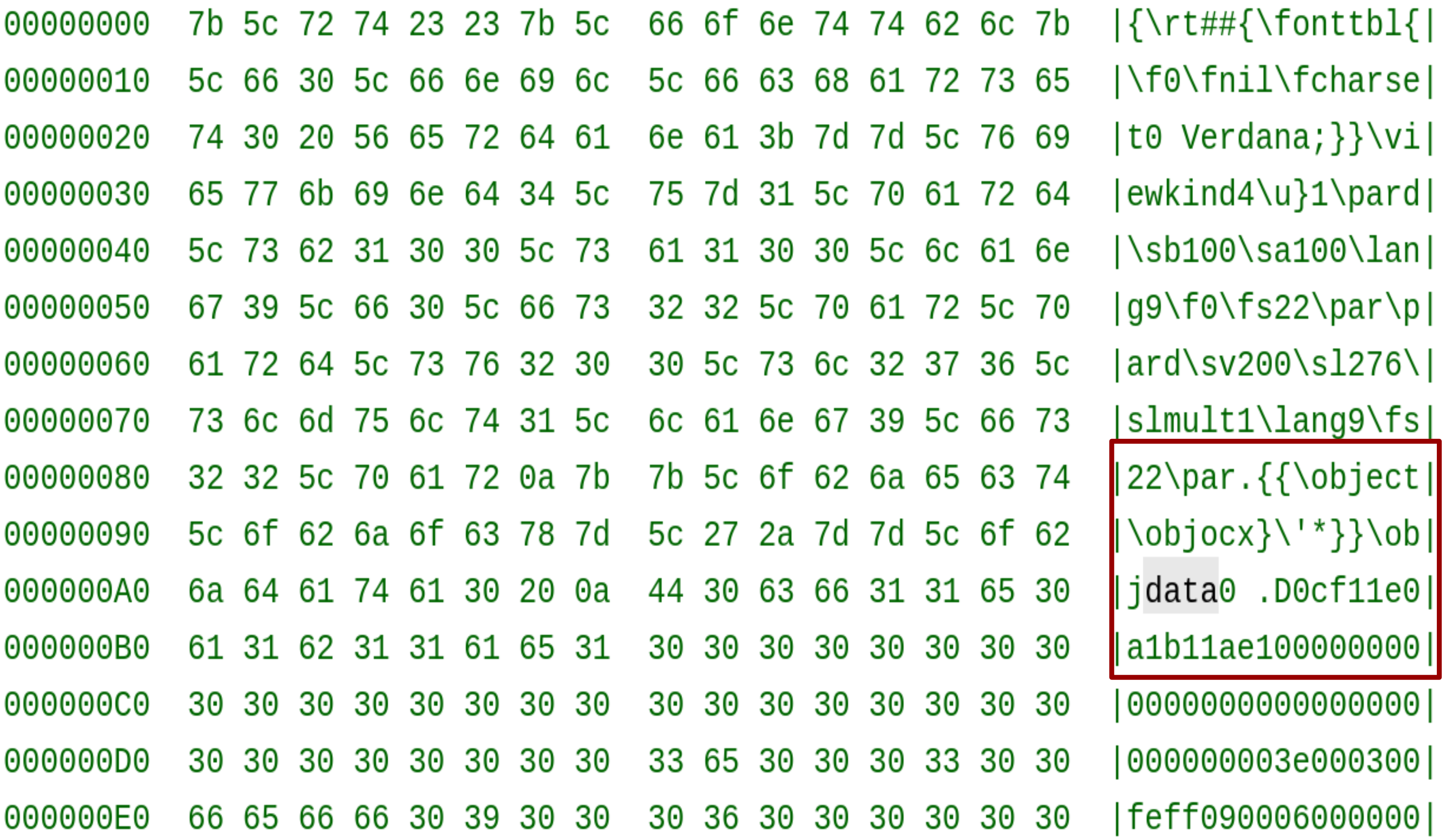
CVE-2012-0158 - Yay RTF!

CVE-2010-3333 PFragments



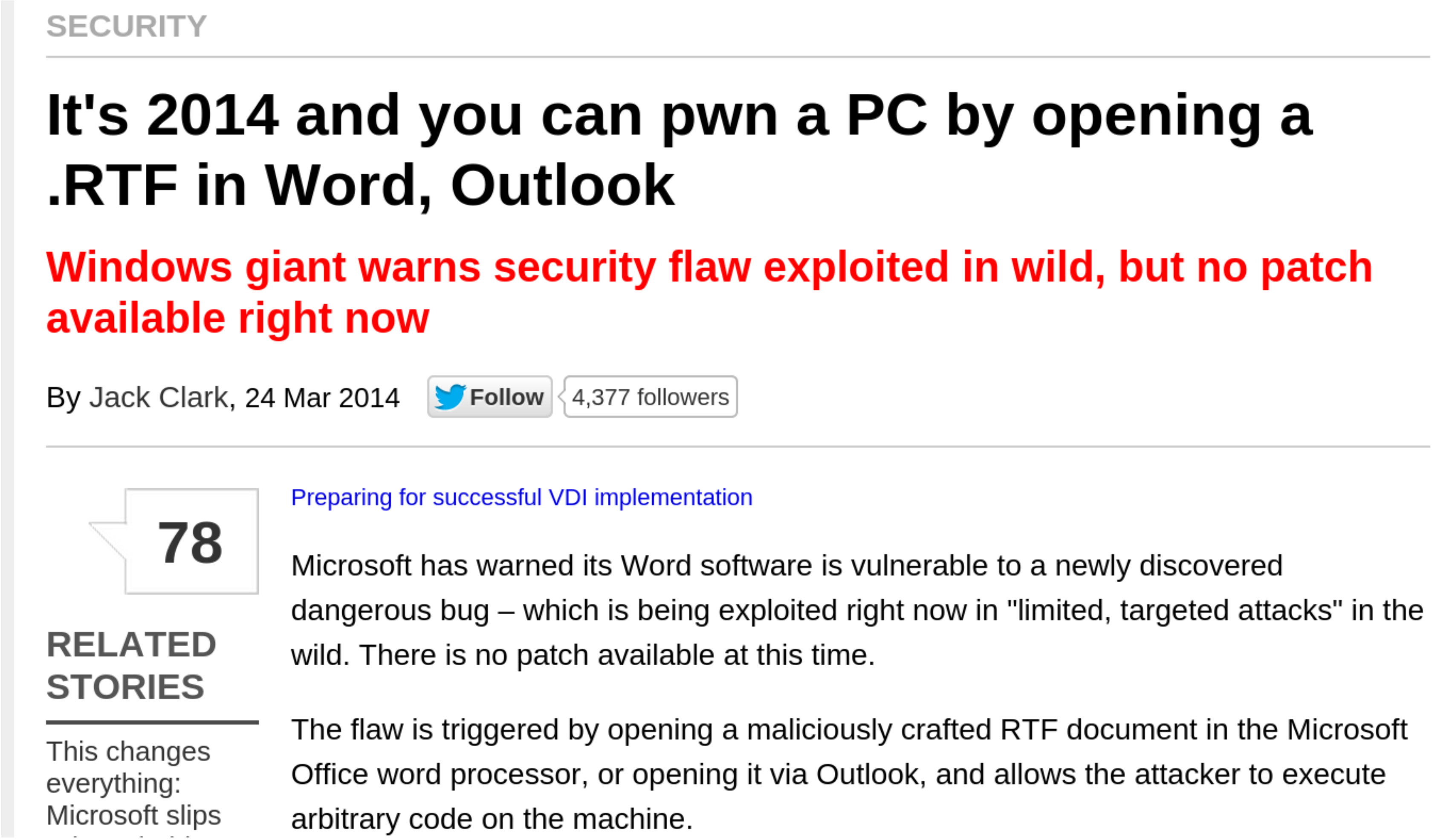
```
00002D80  7b 5c 73 76 20 30 7d 7d  7b 5c 73 70 7b 5c 73 6e  |{\sv 0}}{\sp{\sn|
00002D90  20 70 46 72 61 67 6d 65  6e 74 73 7d 7b 5c 73 76  | pFragments}{\sv|
00002DA0  20 31 3b 20 20 3b 30 31  32 33 34 35 36 37 66 66  | 1;  ;01234567ff|
00002DB0  30 32 30 30 30 30 30 30  67 68 69 6a 6b 6c 6d 6e  |02000000ghijklmn|
00002DC0  6f 70 71 72 73 74 75 76  77 78 7a 79 6b 69 6f 6a  |opqrstuvwxzykioj|
00002DD0  38 39 30 32 33 6a 6b 61  69 66 32 35 31 30 63 35  |89023jkaif2510c5|
00002DE0  37 37 30 30 30 30 38 30  37 63 30 30 30 30 38 30  |770000807c000080|
00002DF0  37 63 42 42 42 42 42 42  42 42 43 43 43 43 43 43  |7cBBBBBBBBCCCCCC|
00002E00  43 43 44 44 44 44 44 44  44 44 39 30 36 61 38 38  |CCDDDDDDDD906a88|
00002E10  37 43 39 30 39 30 39 30  39 30 65 62 30 65 35 38  |7C90909090eb0e58|
00002E20  62 39 35 61 30 31 30 30  30 30 38 30 33 30 31 64  |b95a010000080301d|
```

CVE-2012-0158 ListViewCtrl.2



```
00000000  7b 5c 72 74 23 23 7b 5c  66 6f 6e 74 74 62 6c 7b  |{\rt##{\fonttbl{|
00000010  5c 66 30 5c 66 6e 69 6c  5c 66 63 68 61 72 73 65  |\f0\fnil\fcharse|
00000020  74 30 20 56 65 72 64 61  6e 61 3b 7d 7d 5c 76 69  |t0 Verdana;}}\vi|
00000030  65 77 6b 69 6e 64 34 5c  75 7d 31 5c 70 61 72 64  |ewkind4\u}1\pard|
00000040  5c 73 62 31 30 30 5c 73  61 31 30 30 5c 6c 61 6e  |\sb100\sa100\lan|
00000050  67 39 5c 66 30 5c 66 73  32 32 5c 70 61 72 5c 70  |g9\f0\fs22\par\p|
00000060  61 72 64 5c 73 76 32 30  30 5c 73 6c 32 37 36 5c  |ard\sv200\sl276\|
00000070  73 6c 6d 75 6c 74 31 5c  6c 61 6e 67 39 5c 66 73  |slmult1\lang9\fs|
00000080  32 32 5c 70 61 72 0a 7b  7b 5c 6f 62 6a 65 63 74  |22\par.{{\object|
00000090  5c 6f 62 6a 6f 63 78 7d  5c 27 2a 7d 7d 5c 6f 62  |\objocx}\'*}}\ob|
000000A0  6a 64 61 74 61 30 20 0a  44 30 63 66 31 31 65 30  |jdata0 .D0cf11e0|
000000B0  61 31 62 31 31 61 65 31  30 30 30 30 30 30 30 30  |a1b11ae100000000|
000000C0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
000000D0  30 30 30 30 30 30 30 30  33 65 30 30 30 33 30 30  |000000003e000300|
000000E0  66 65 66 66 30 39 30 30  30 36 30 30 30 30 30 30  |feff090006000000|
```

New this week: CVE-2014-1761



SECURITY

It's 2014 and you can pwn a PC by opening a .RTF in Word, Outlook

Windows giant warns security flaw exploited in wild, but no patch available right now

By Jack Clark, 24 Mar 2014

Preparing for successful VDI implementation

Microsoft has warned its Word software is vulnerable to a newly discovered dangerous bug – which is being exploited right now in "limited, targeted attacks" in the wild. There is no patch available at this time.

The flaw is triggered by opening a maliciously crafted RTF document in the Microsoft Office word processor, or opening it via Outlook, and allows the attacker to execute arbitrary code on the machine.

RELATED STORIES

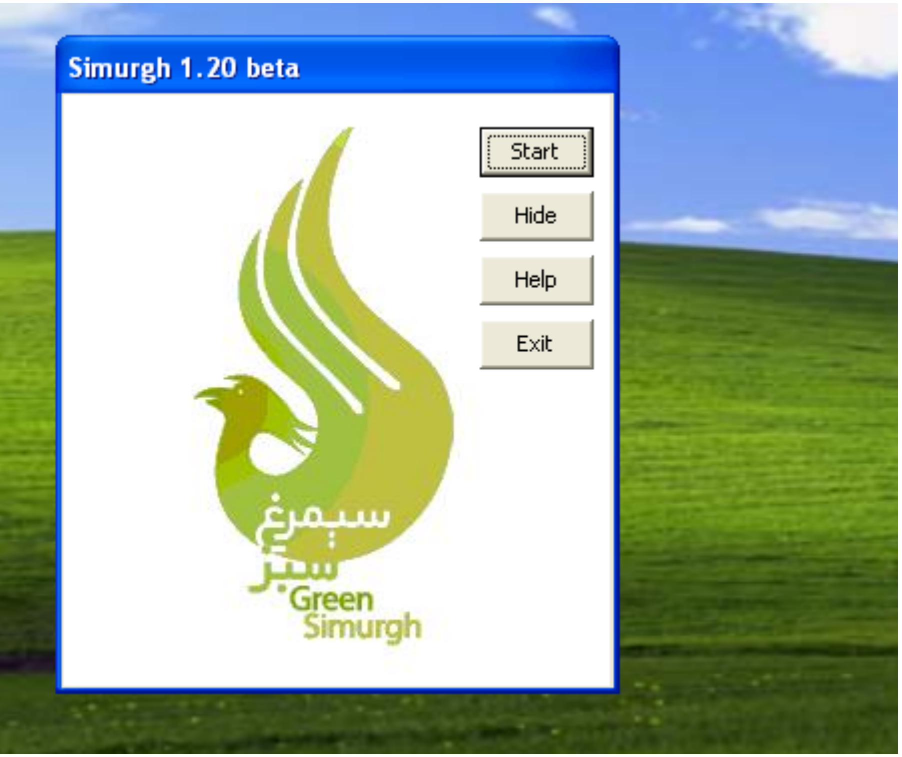
This changes everything: Microsoft slips

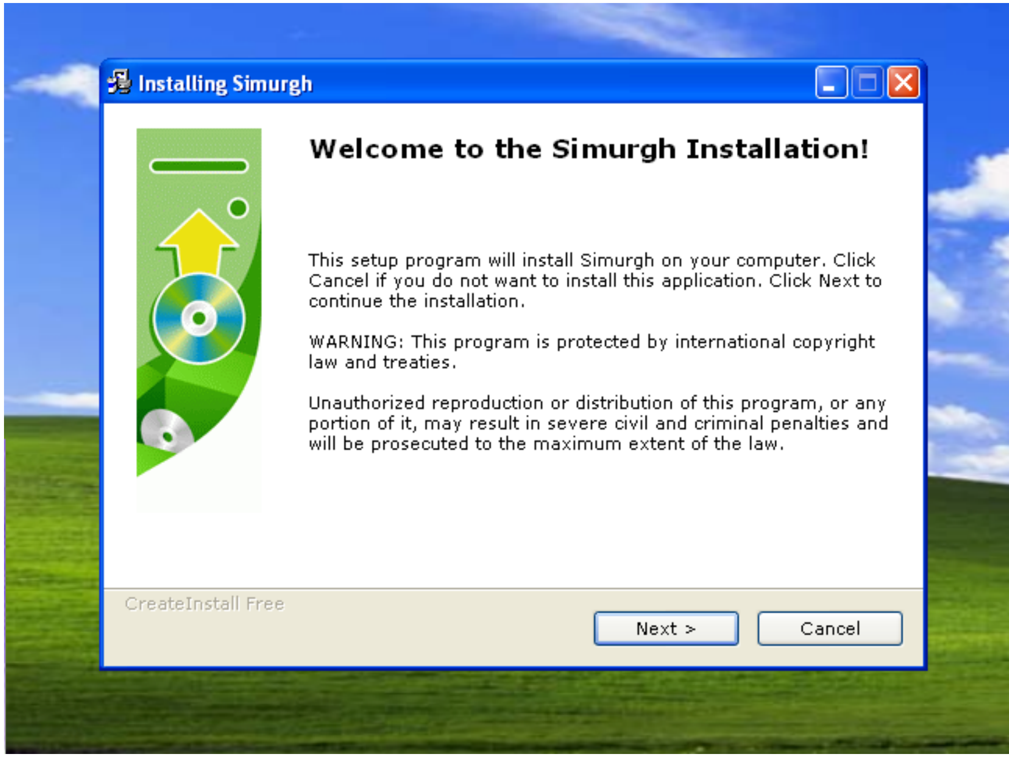
http://www.theregister.co.uk/2014/03/24/microsoft_rtf_vuln/

Exploits today

- Only if they have to
- Old ones work
- The 0 days are out there...
- ... and they are for sale.

Backdoored Circumvention Tools - Simurgh





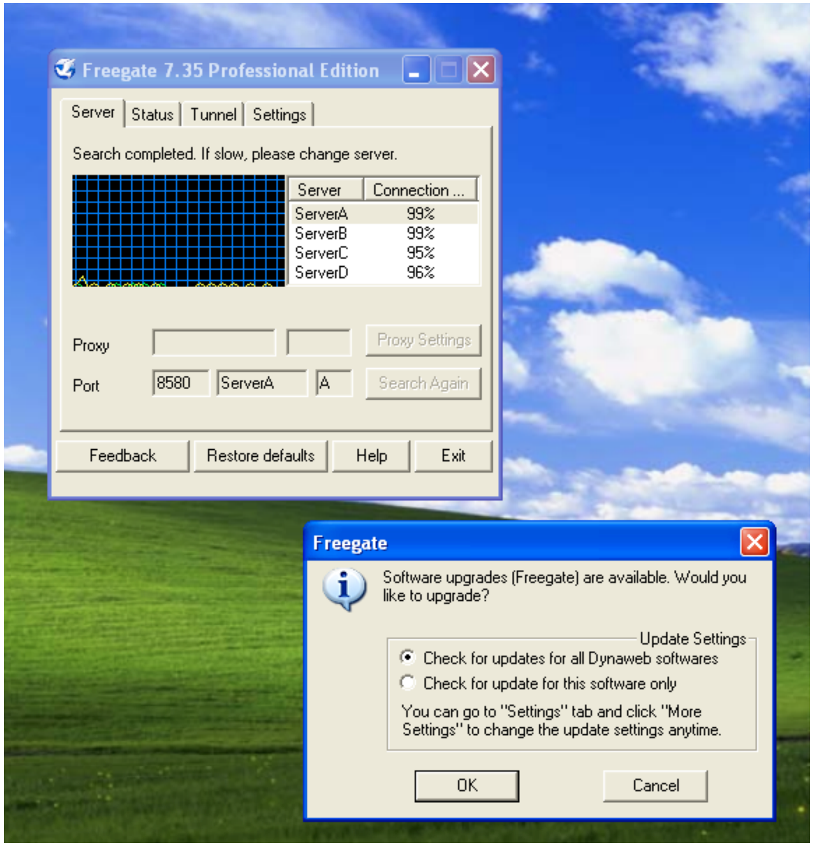
Welcome to the Simurgh Installation!

This setup program will install Simurgh on your computer. Click Cancel if you do not want to install this application. Click Next to continue the installation.

WARNING: This program is protected by international copyright law and treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties and will be prosecuted to the maximum extent of the law.

Backdoored Circumvention Tools - FreeGate



Freegate 7.35 Professional Edition

Search completed. If slow, please change server.

Server	Connection ...
ServerA	99%
ServerB	99%
ServerC	95%
ServerD	96%

Proxy:

Port: 8580 ServerA A

Freegate

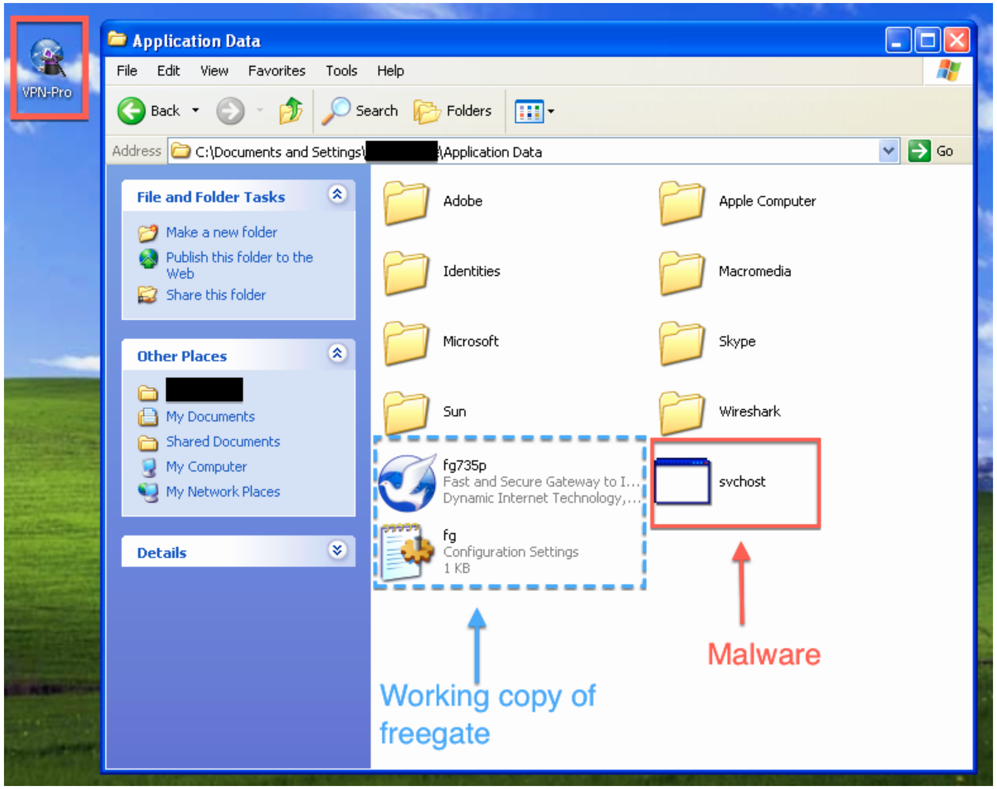
Software upgrades (Freegate) are available. Would you like to upgrade?

Update Settings

● Check for updates for all Dynaweb softwares

○ Check for update for this software only

You can go to "Settings" tab and click "More Settings" to change the update settings anytime.



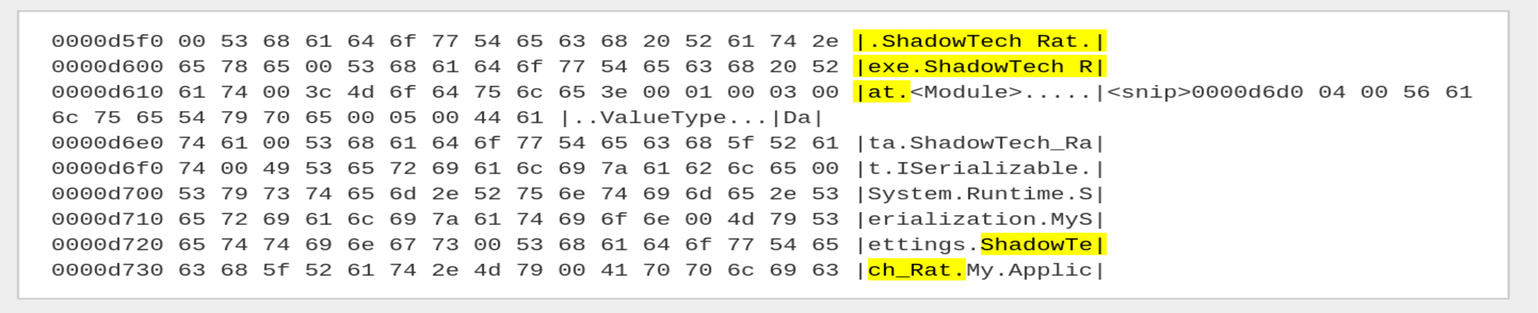
Address: C:\Documents and Settings\[redacted]\Application Data

[redacted]

fg735p
Fast and Secure Gateway to I...
Dynamic Internet Technology,...

fg
Configuration Settings
1 KB

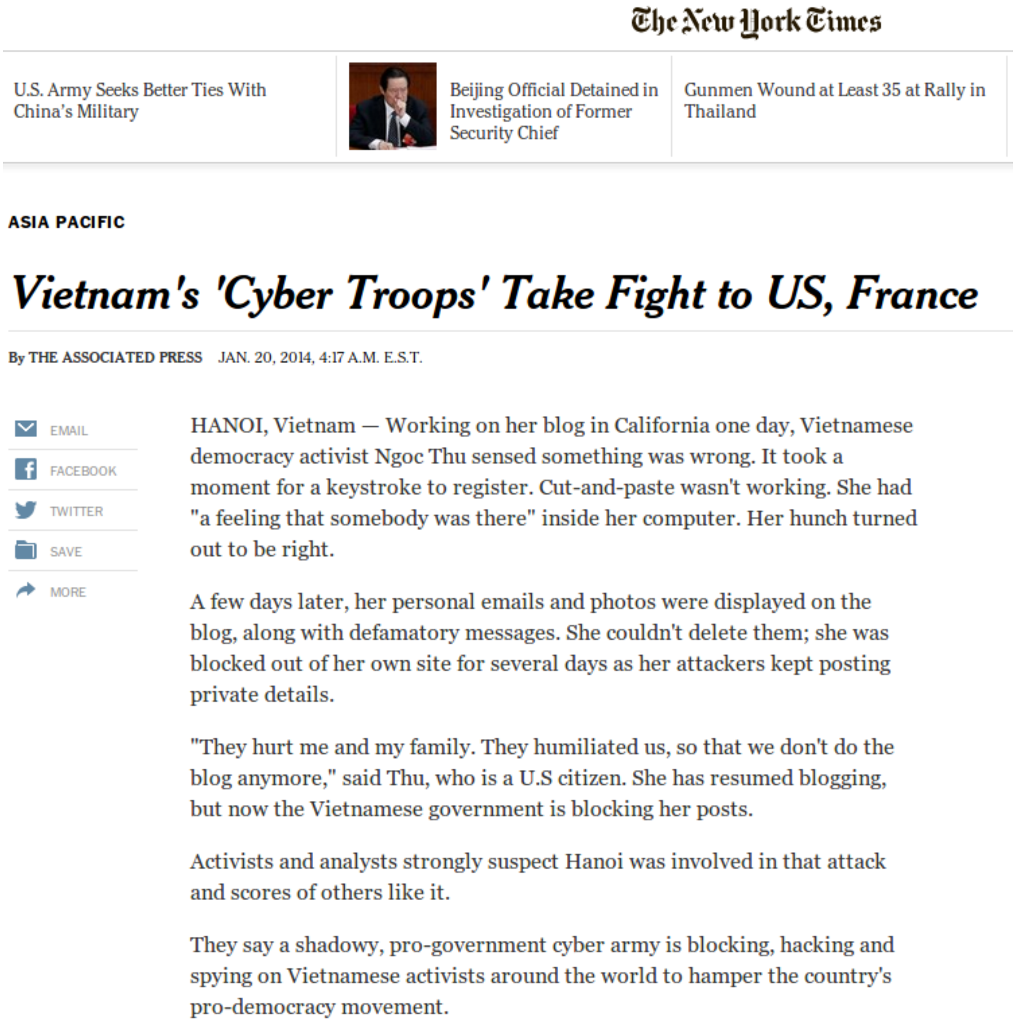
svchost



```
0000d5f0 00 53 68 61 64 6f 77 54 65 63 68 20 52 61 74 2e |.ShadowTech Rat.|
0000d600 65 78 65 00 53 68 61 64 6f 77 54 65 63 68 20 52 |exe.ShadowTech R|
0000d610 61 74 00 3c 4d 6f 64 75 6c 65 3e 00 01 00 03 00 |at.<Module>.....|<snip>0000d6d0 04 00 56 61
6c 75 65 54 79 70 65 00 05 00 44 61 |..ValueType...|Da|
0000d6e0 74 61 00 53 68 61 64 6f 77 54 65 63 68 5f 52 61 |ta.ShadowTech_Ra|
0000d6f0 74 00 49 53 65 72 69 61 6c 69 7a 61 62 6c 65 00 |t.ISerializable.|
0000d700 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 53 |System.Runtime.S|
0000d710 65 72 69 61 6c 69 7a 61 74 69 6f 6e 00 4d 79 53 |erialization.MyS|
0000d720 65 74 74 69 6e 67 73 00 53 68 61 64 6f 77 54 65 |ettings.ShadowTe|
0000d730 63 68 5f 52 61 74 2e 4d 79 00 41 70 70 6c 69 63 |ch_Rat.My.Applic|
```

Backdoored Circumvention Tools - Tor

hash: bd970e0d63cd3abeb10ab2b0b82f33065be7f4b440564a24c6e19724f643a133



The New York Times

U.S. Army Seeks Better Ties With China's Military

Beijing Official Detained in Investigation of Former Security Chief

Gunmen Wound at Least 35 at Rally in Thailand

ASIA PACIFIC

Vietnam's 'Cyber Troops' Take Fight to US, France

By THE ASSOCIATED PRESS JAN. 20, 2014, 4:17 A.M. E.S.T.

HANOI, Vietnam — Working on her blog in California one day, Vietnamese democracy activist Ngoc Thu sensed something was wrong. It took a moment for a keystroke to register. Cut-and-paste wasn't working. She had "a feeling that somebody was there" inside her computer. Her hunch turned out to be right.

A few days later, her personal emails and photos were displayed on the blog, along with defamatory messages. She couldn't delete them; she was blocked out of her own site for several days as her attackers kept posting private details.

"They hurt me and my family. They humiliated us, so that we don't do the blog anymore," said Thu, who is a U.S citizen. She has resumed blogging, but now the Vietnamese government is blocking her posts.

Activists and analysts strongly suspect Hanoi was involved in that attack and scores of others like it.

They say a shadowy, pro-government cyber army is blocking, hacking and spying on Vietnamese activists around the world to hamper the country's pro-democracy movement.

Ngoc Thu ran the largest political blog outside of Vietnam. Hacked in Jan 2013, personal information of website owner posted. Site shut down.

Vietnamese mathematician in France. Hacked in May, 2013.

EFF bloggers targeted in December 2013.

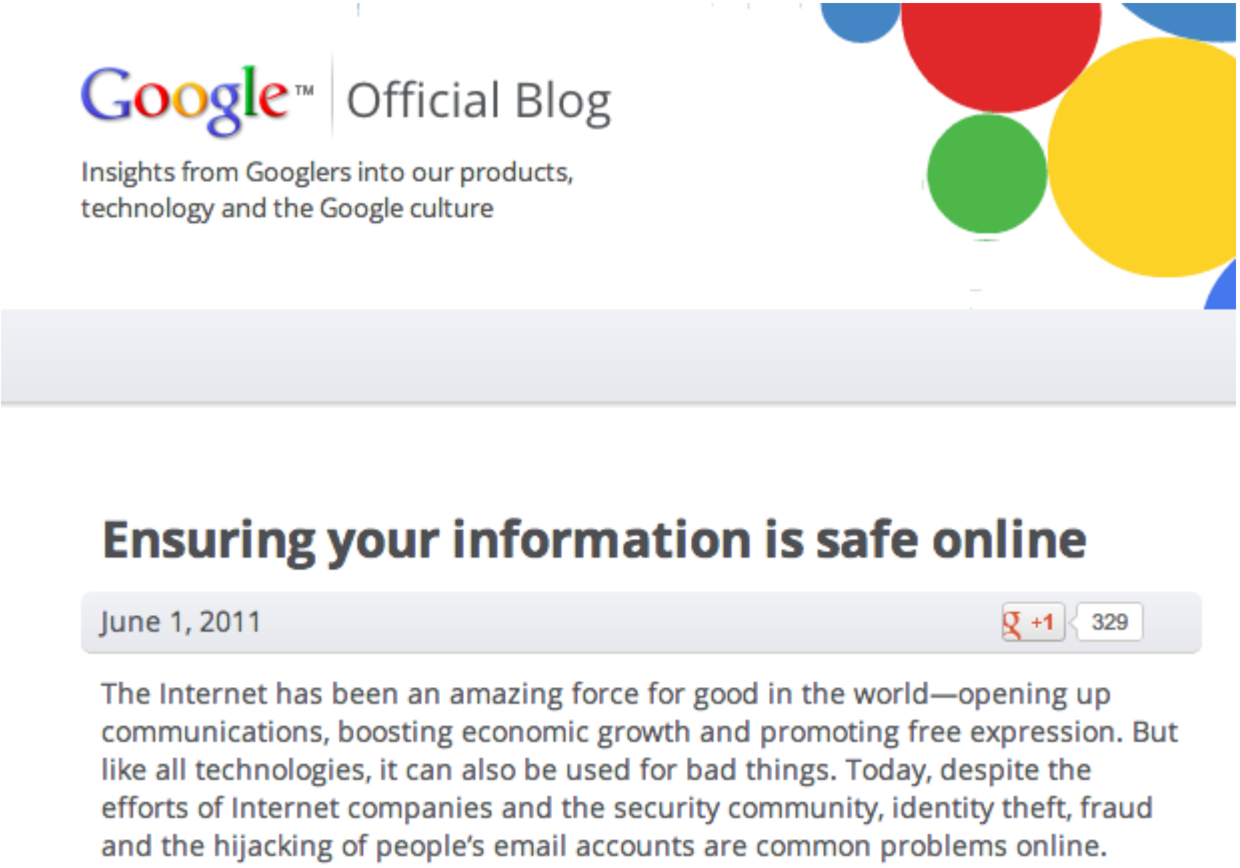
Associated Press reporter targeted in December 2013.

This article appeared Jan 20th, 2014.

Phishing

The scariest lame threat

Phishing Journalist Accounts - June 2011



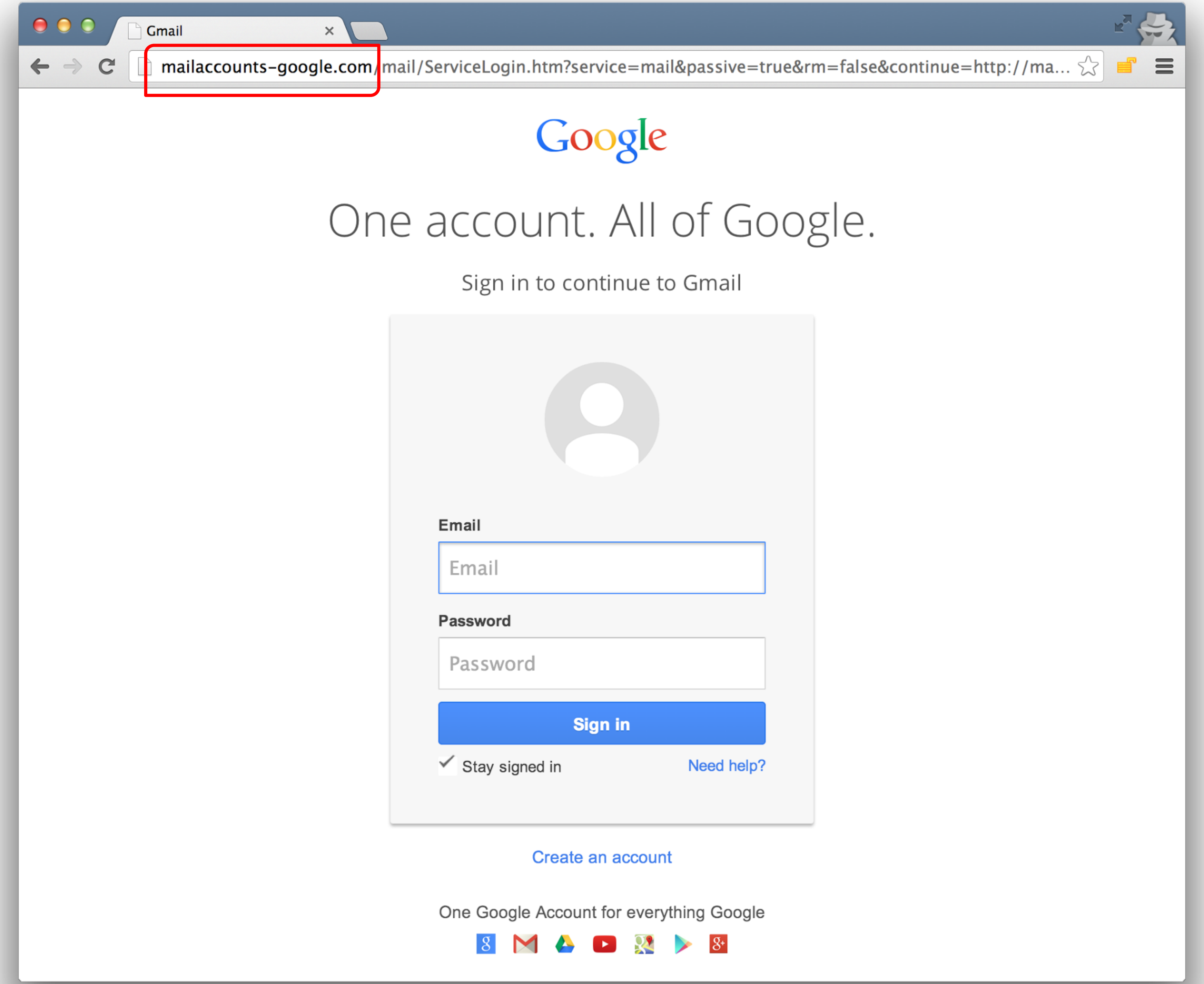
Google™ | Official Blog

Insights from Googlers into our products, technology and the Google culture

Ensuring your information is safe online

June 1, 2011

The Internet has been an amazing force for good in the world—opening up communications, boosting economic growth and promoting free expression. But like all technologies, it can also be used for bad things. Today, despite the efforts of Internet companies and the security community, identity theft, fraud and the hijacking of people's email accounts are common problems online.

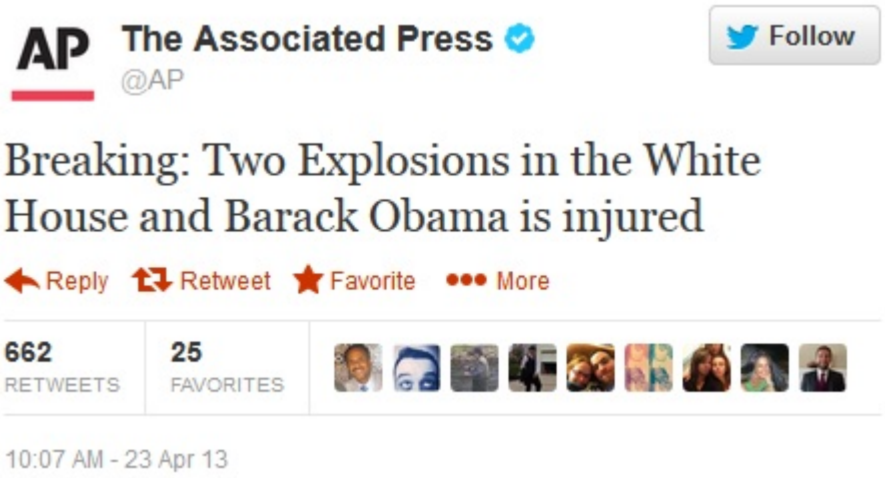


mailaccounts-google.com/mail/ServiceLogin.htm?service=mail&passive=true&rm=false&continue=http://ma…

One account. All of Google.

Sign in to continue to Gmail

One Google Account for everything Google



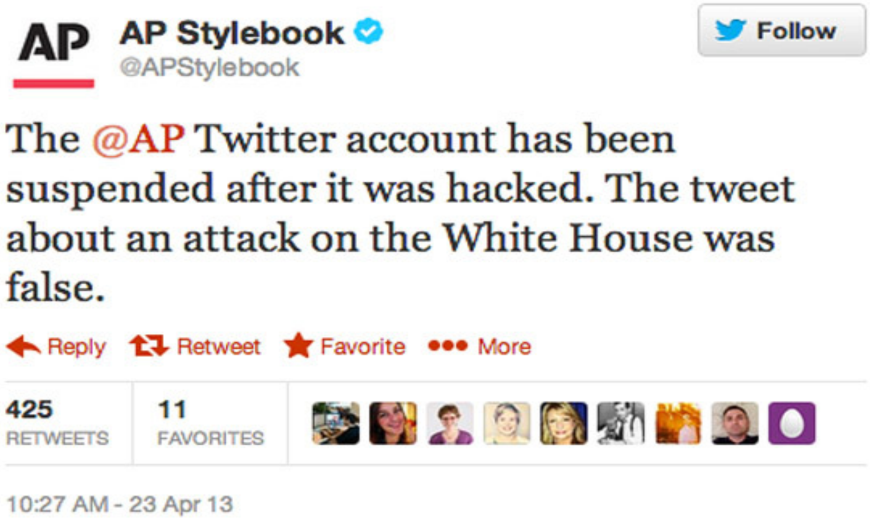
The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

662 RETWEETS

25 FAVORITES

10:07 AM - 23 Apr 13



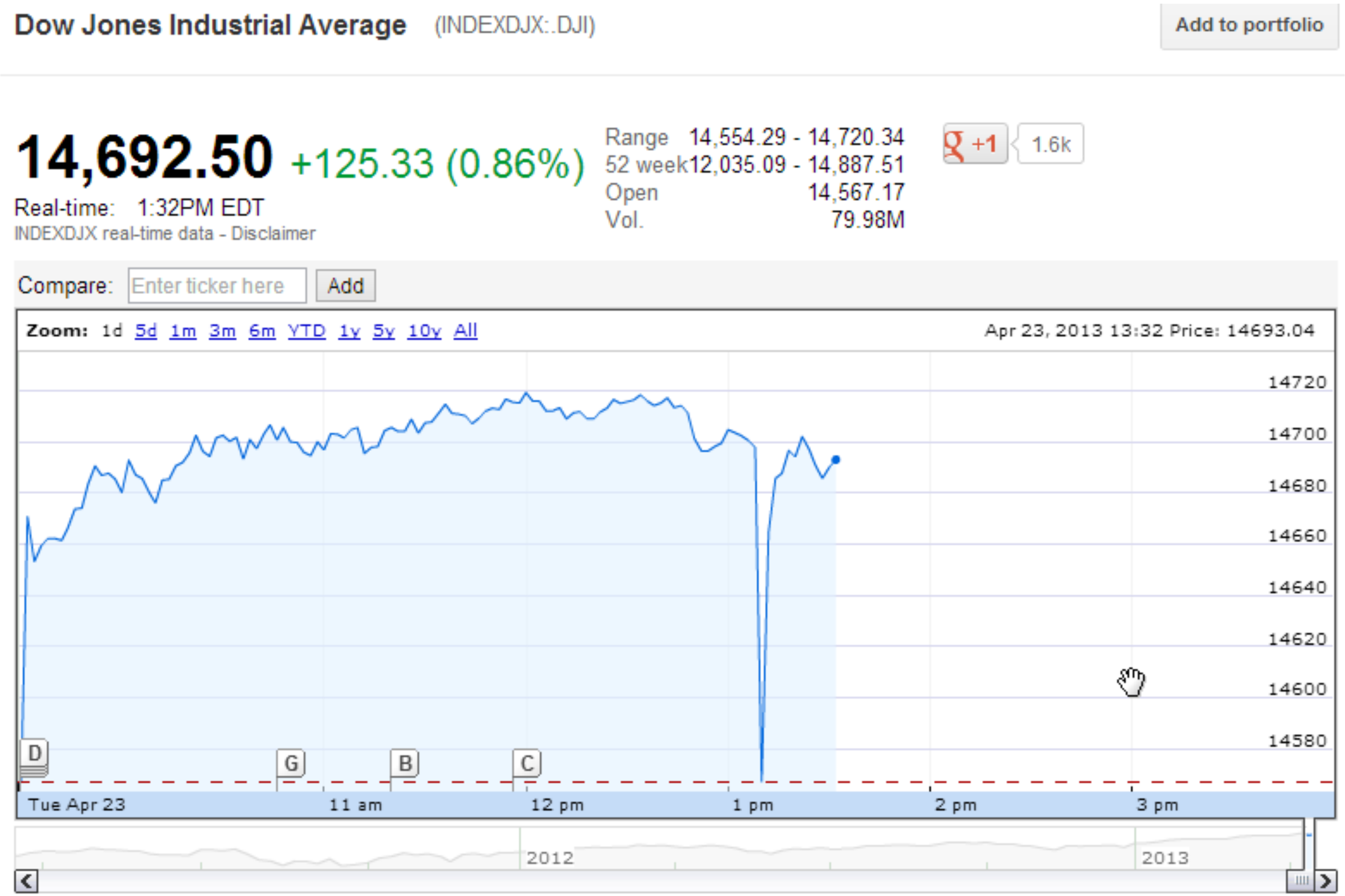
AP Stylebook
@APStylebook

The @AP Twitter account has been suspended after it was hacked. The tweet about an attack on the White House was false.

425 RETWEETS

11 FAVORITES

10:27 AM - 23 Apr 13



Dow Jones Industrial Average (INDEXDJX:.DJI)

14,692.50 +125.33 (0.86%)

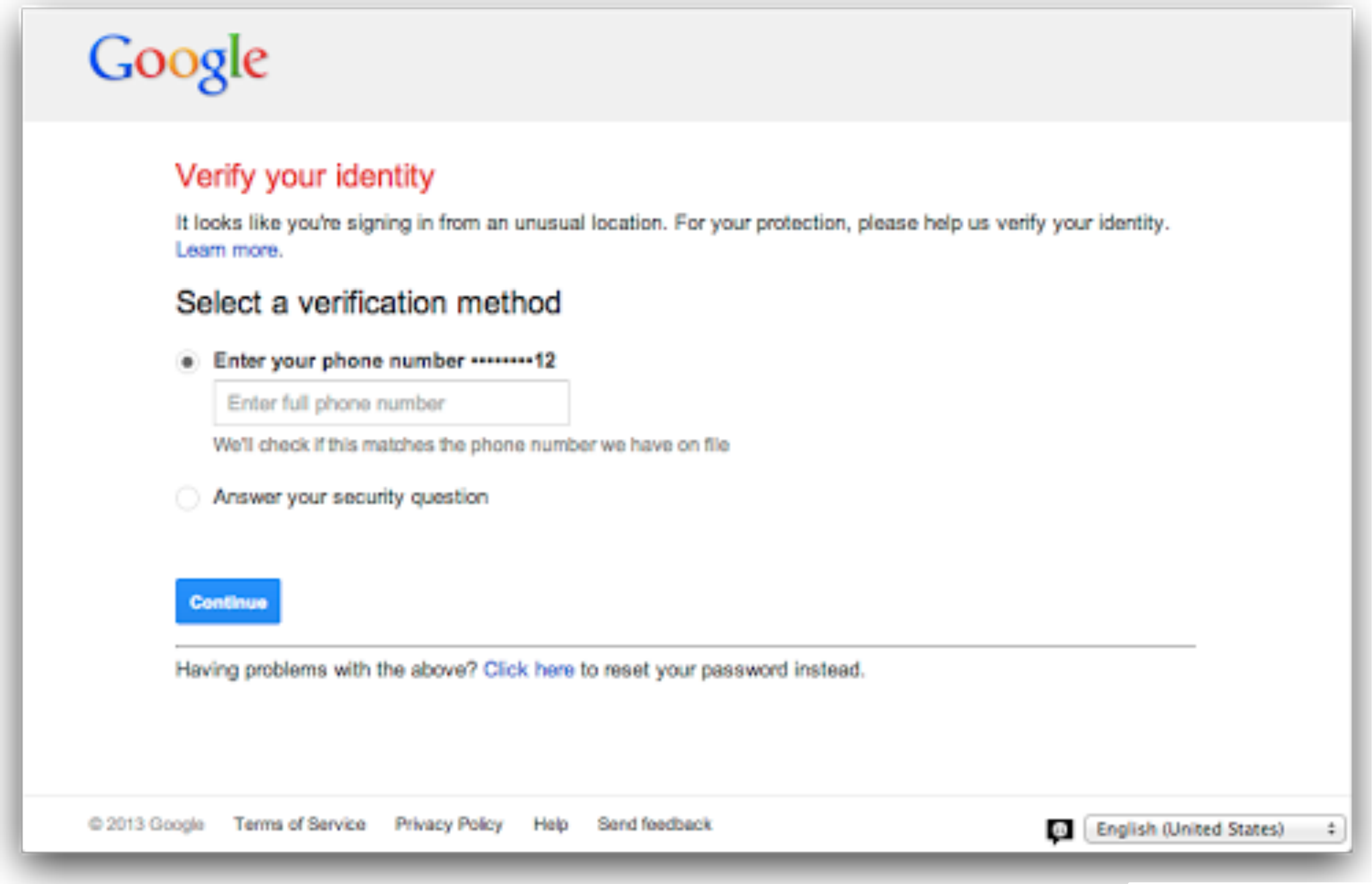
Real-time: 1:32PM EDT

INDEXDJX real-time data - Disclaimer

Range	14,554.29 - 14,720.34
52 week	12,035.09 - 14,887.51
Open	14,567.17
Vol.	79.98M

Apr 23, 2013 13:32 Price: 14693.04

Reducing hijacking



Google

Verify your identity

It looks like you're signing in from an unusual location. For your protection, please help us verify your identity. Learn more.

Select a verification method

● Enter your phone number ••••••••12

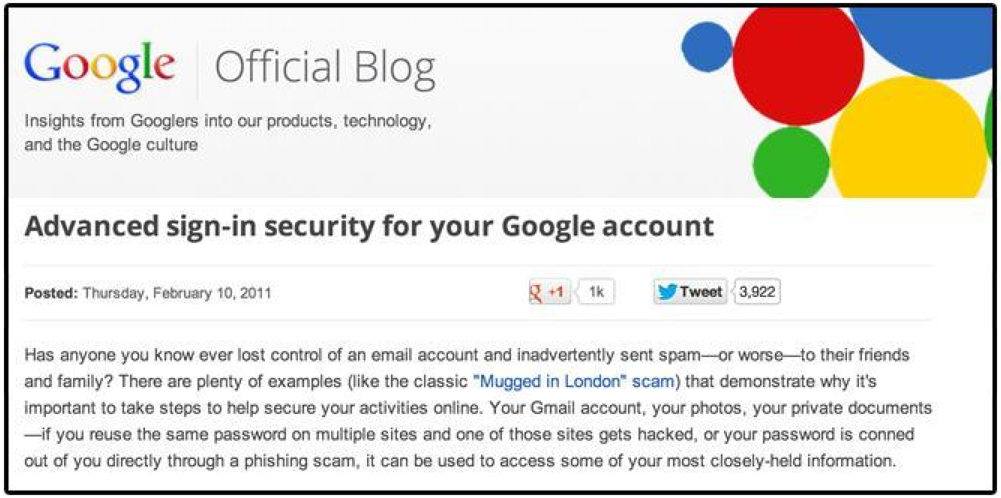
Enter full phone number

We'll check if this matches the phone number we have on file

○ Answer your security question

Continue

Having problems with the above? Click here to reset your password instead.



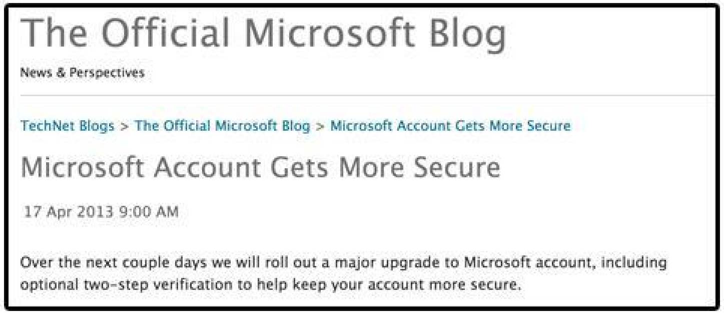
Google | Official Blog

Insights from Googlers into our products, technology,
and the Google culture

Advanced sign-in security for your Google account

Posted: Thursday, February 10, 2011

Has anyone you know ever lost control of an email account and inadvertently sent spam—or worse—to their friends and family? There are plenty of examples (like the classic "Mugged in London" scam) that demonstrate why it's important to take steps to help secure your activities online. Your Gmail account, your photos, your private documents—if you reuse the same password on multiple sites and one of those sites gets hacked, or your password is conned out of you directly through a phishing scam, it can be used to access some of your most closely-held information.



The Official Microsoft Blog

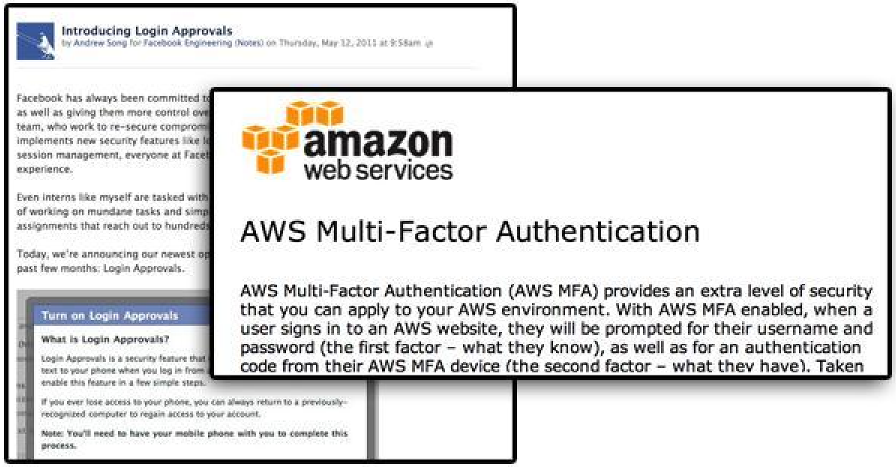
News & Perspectives

TechNet Blogs > The Official Microsoft Blog > Microsoft Account Gets More Secure

Microsoft Account Gets More Secure

17 Apr 2013 9:00 AM

Over the next couple days we will roll out a major upgrade to Microsoft account, including optional two-step verification to help keep your account more secure.



Introducing Login Approvals
by Andrew Song for Facebook Engineering (Notes) on Thursday, May 12, 2011 at 9:58am

Facebook has always been committed t
as well as giving them more control ove
team, who work to re-secure comprom
implements new security features like l
session management, everyone at Faceb
experience.

Even interns like myself are tasked with
of working on mundane tasks and simp
assignments that reach out to hundreds

Today, we're announcing our newest op
past few months: Login Approvals.

Turn on Login Approvals

What is Login Approvals?

Login Approvals is a security feature that
text to your phone when you log in from
enable this feature in a few simple steps.

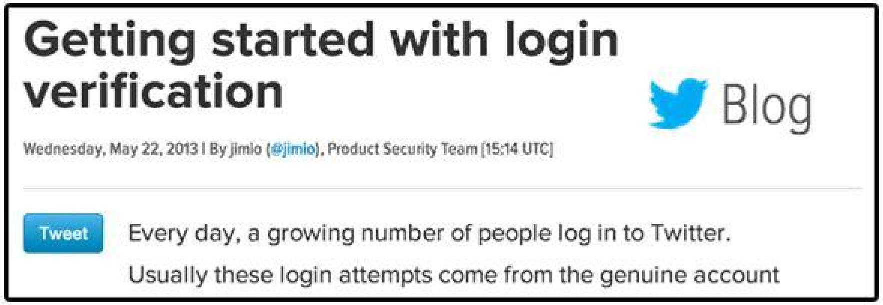
If you ever lose access to your phone, you can always return to a previously-recognized computer to regain access to your account.

Note: You'll need to have your mobile phone with you to complete this process.

amazon web services

AWS Multi-Factor Authentication

AWS Multi-Factor Authentication (AWS MFA) provides an extra level of security that you can apply to your AWS environment. With AWS MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password (the first factor – what they know), as well as for an authentication code from their AWS MFA device (the second factor – what they have). Taken



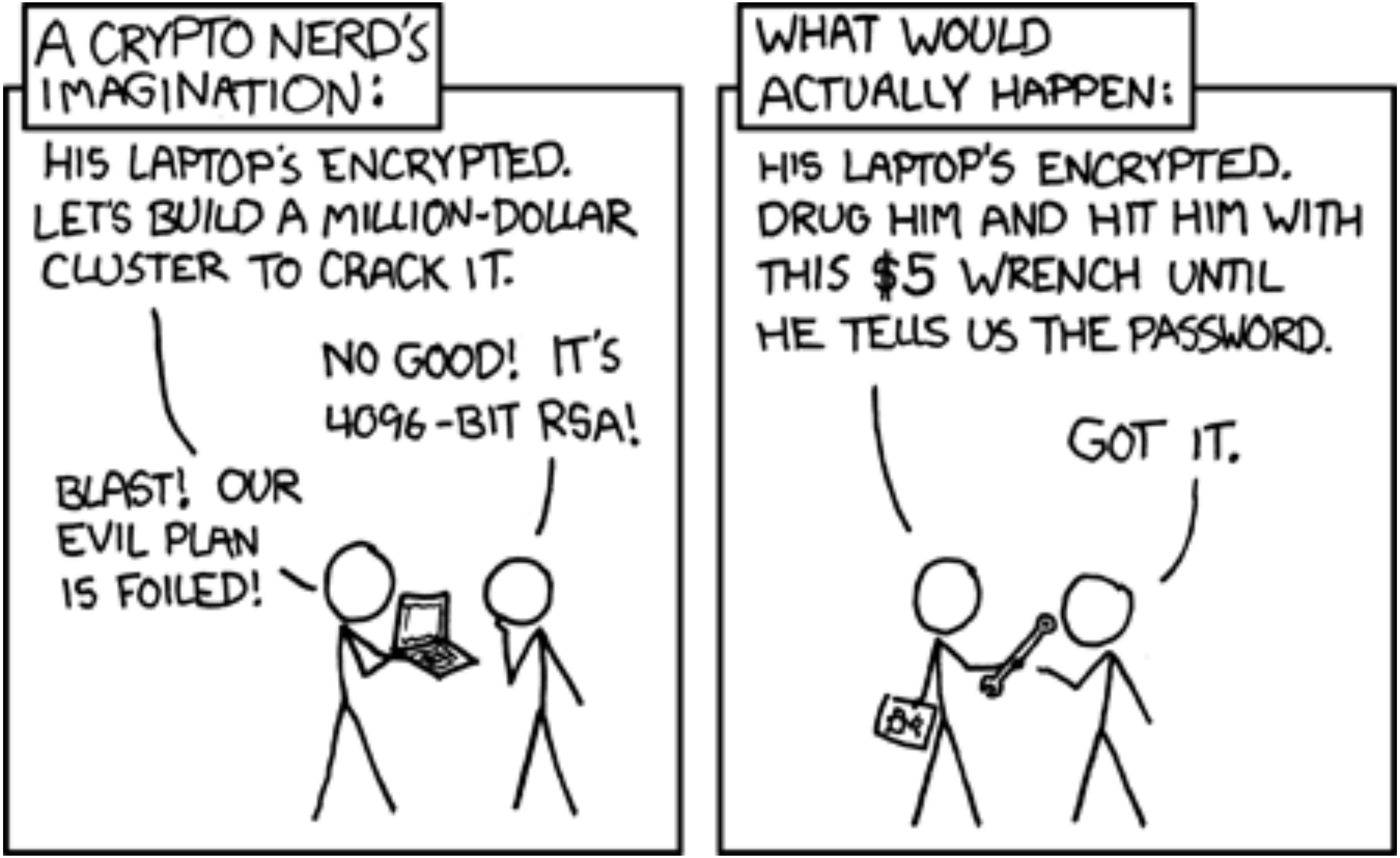
Getting started with login verification

Blog

Wednesday, May 22, 2013 | By jimio (@jimio), Product Security Team [15:14 UTC]

Every day, a growing number of people log in to Twitter.
Usually these login attempts come from the genuine account

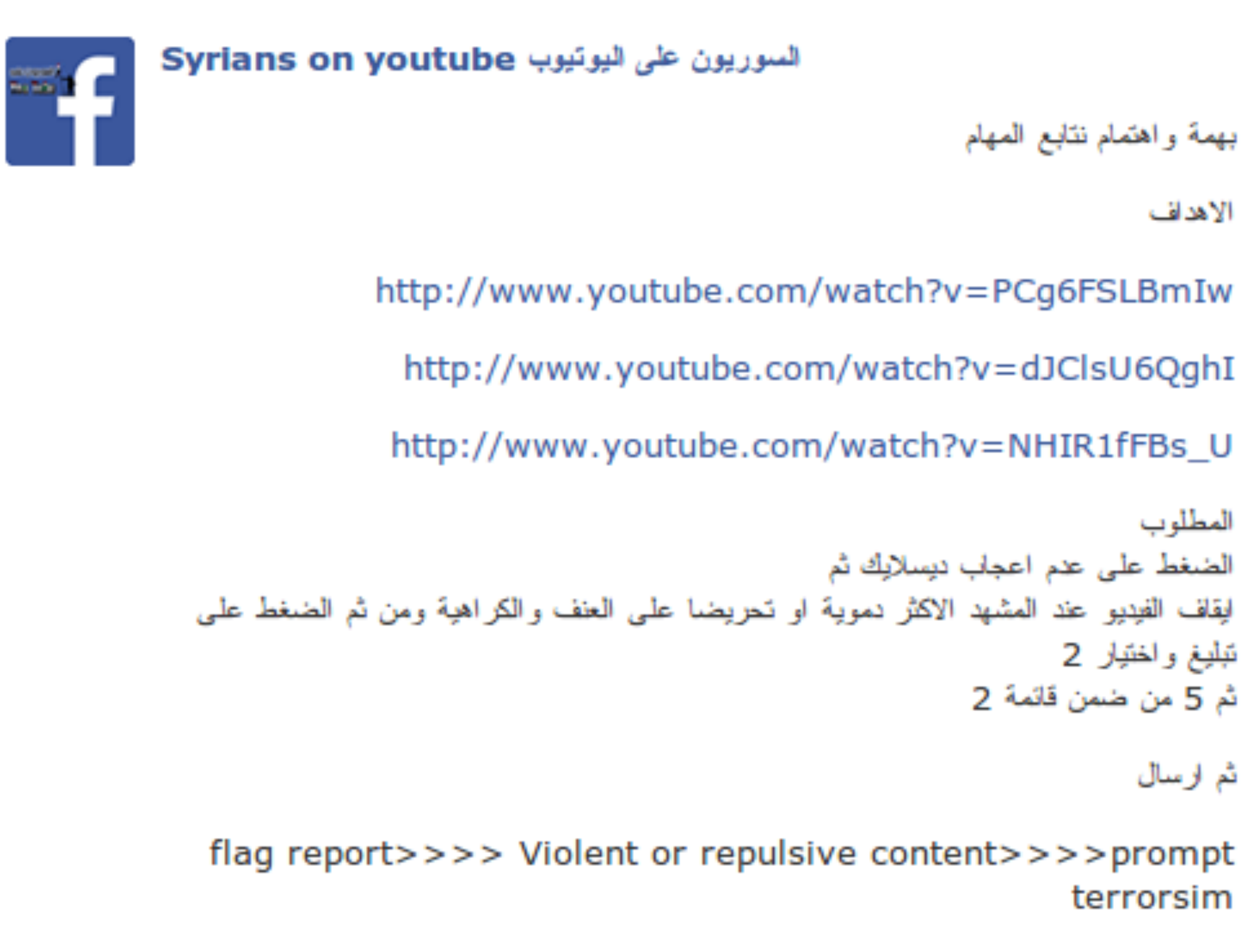
backspace


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

The Revolution

- Will be televised on Youtube

Syrian Targeting of Citizen Media



Syrians on youtube السوريون على اليوتيوب

بهمة و اهتمام نتابع المهام

الاهداف

http://www.youtube.com/watch?v=PCg6FSLBmIw

http://www.youtube.com/watch?v=dJClsU6QghI

http://www.youtube.com/watch?v=NHIR1fFBs_U

المطلوب
الضغط على عدم اعجاب ديسلايك ثم
إيقاف الفيديو عند المشهد الاكثر دموية او تحريضا على العنف و الكراهية ومن ثم الضغط على
تبليغ و اختيار 2
ثم 5 من ضمن قائمة 2

ثم ارسال

flag report>>>> Violent or repulsive content>>>>prompt terrorsim

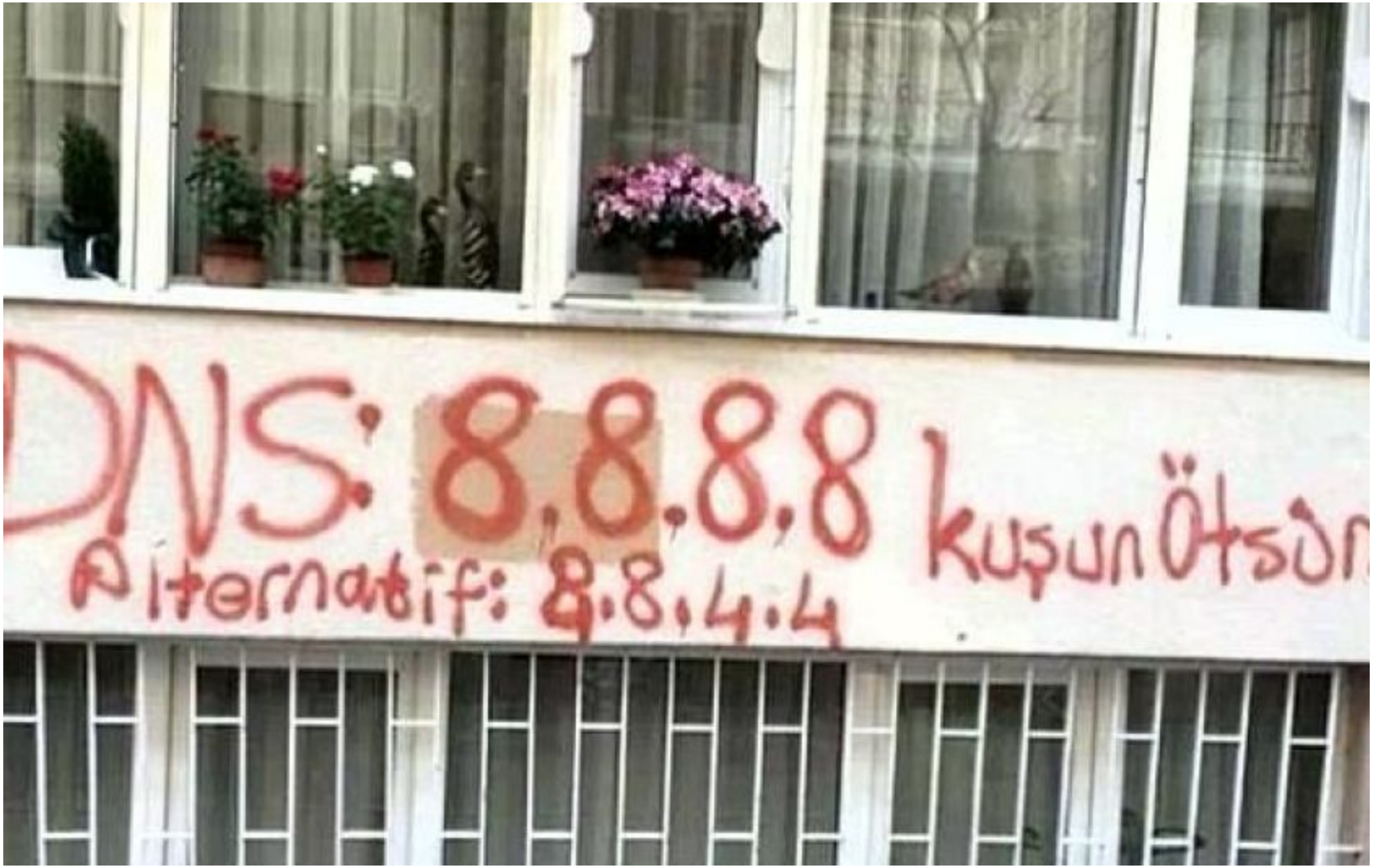
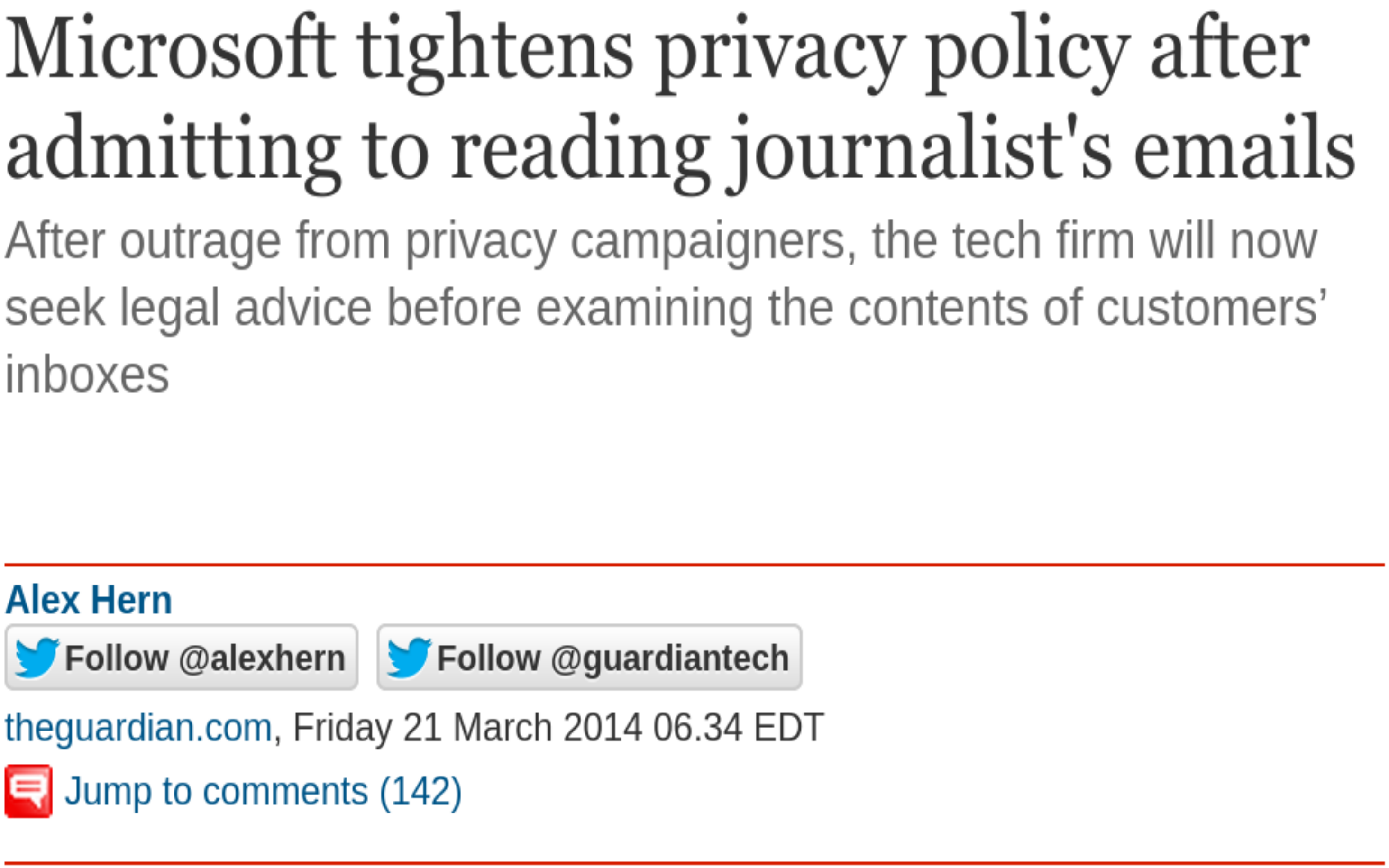


Image Credit: Twitter



Microsoft tightens privacy policy after admitting to reading journalist's emails

After outrage from privacy campaigners, the tech firm will now seek legal advice before examining the contents of customers' inboxes

Alex Hern

Follow @alexhern Follow @guardiantech

theguardian.com, Friday 21 March 2014 06.34 EDT

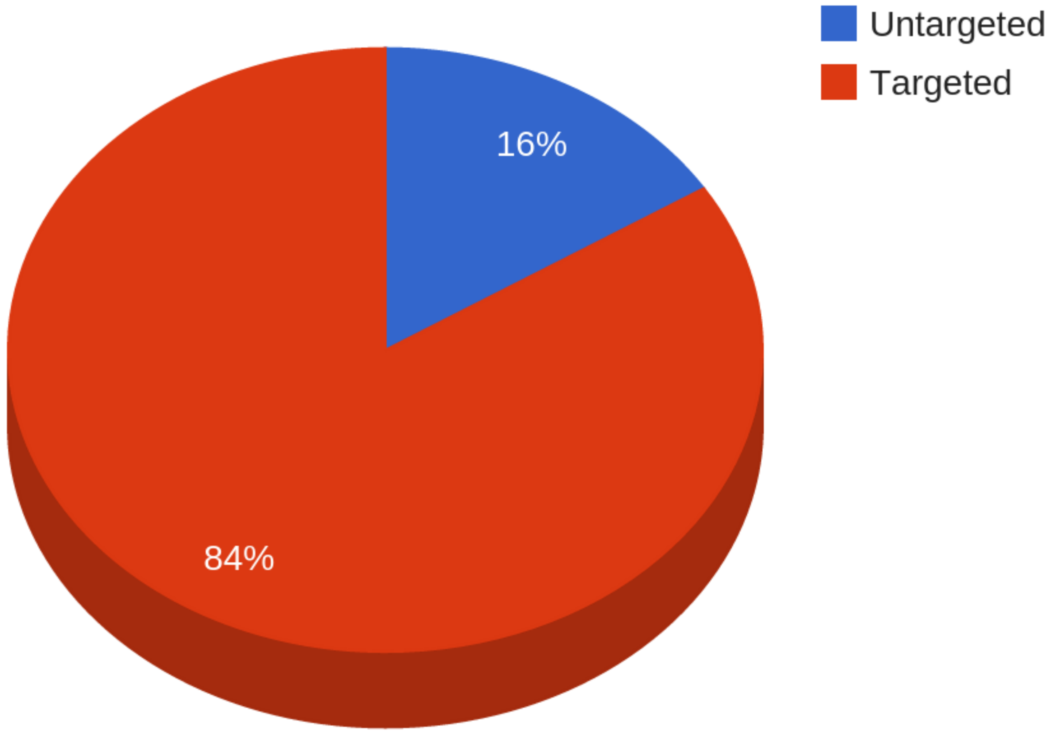
Jump to comments (142)

Regional flavor

RANK*	NEWS SITE
1	nytimes.com
2	indiatimes.com
3	wsj.com
4	usatoday.com
5	washingtonpost.com
6	latimes.com
7	examiner.com
8	smh.com.au
9	sfgate.com
10	chron.com
11	thehindu.com
12	nypost.com
13	hindustantimes.com
14	eenadu.net
15	chicagotribune.com
16	hollywoodreporter.com
17	indianexpress.com
18	theglobeandmail.com
19	theage.com.au
20	manoramonline.com
21	amarujala.com
22	washingtontimes.com
23	thestar.com
24	dnaindia.com
25	nj.com

Top 25 New Sites

Targeted by State Sponsored Groups



*From Alexa Top 25 New as of 03/23/2014 by @ashk4n

Hide yo sources, Hide yo docs
They be hacking everyone out here

How we fix this

- Journalists: Security integral to your job

- Security Industry: We can do better...

- Governments: well...