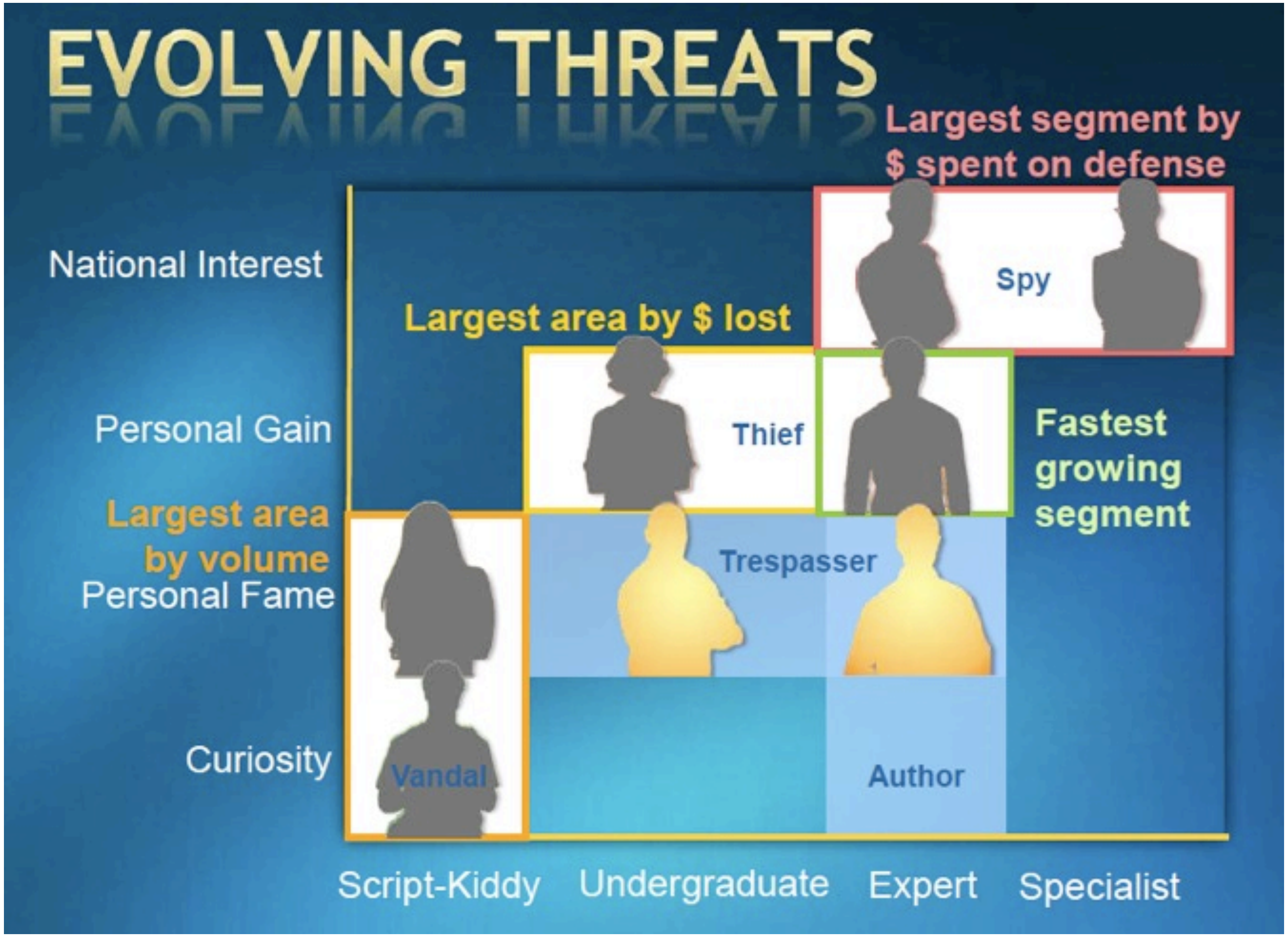
Sécurité Informatique késako ?

Pascal Junod // HEIG-VD

Qui suis-je?

Contexte



EVOLVING THREATS

Largest segment by $ spent on defense

National Interest

Spy

Largest area by $ lost

Personal Gain

Thief

Fastest growing segment

Largest area by volume

Personal Fame

Trespasser

Curiosity

Vandal

Author

Script-Kiddy

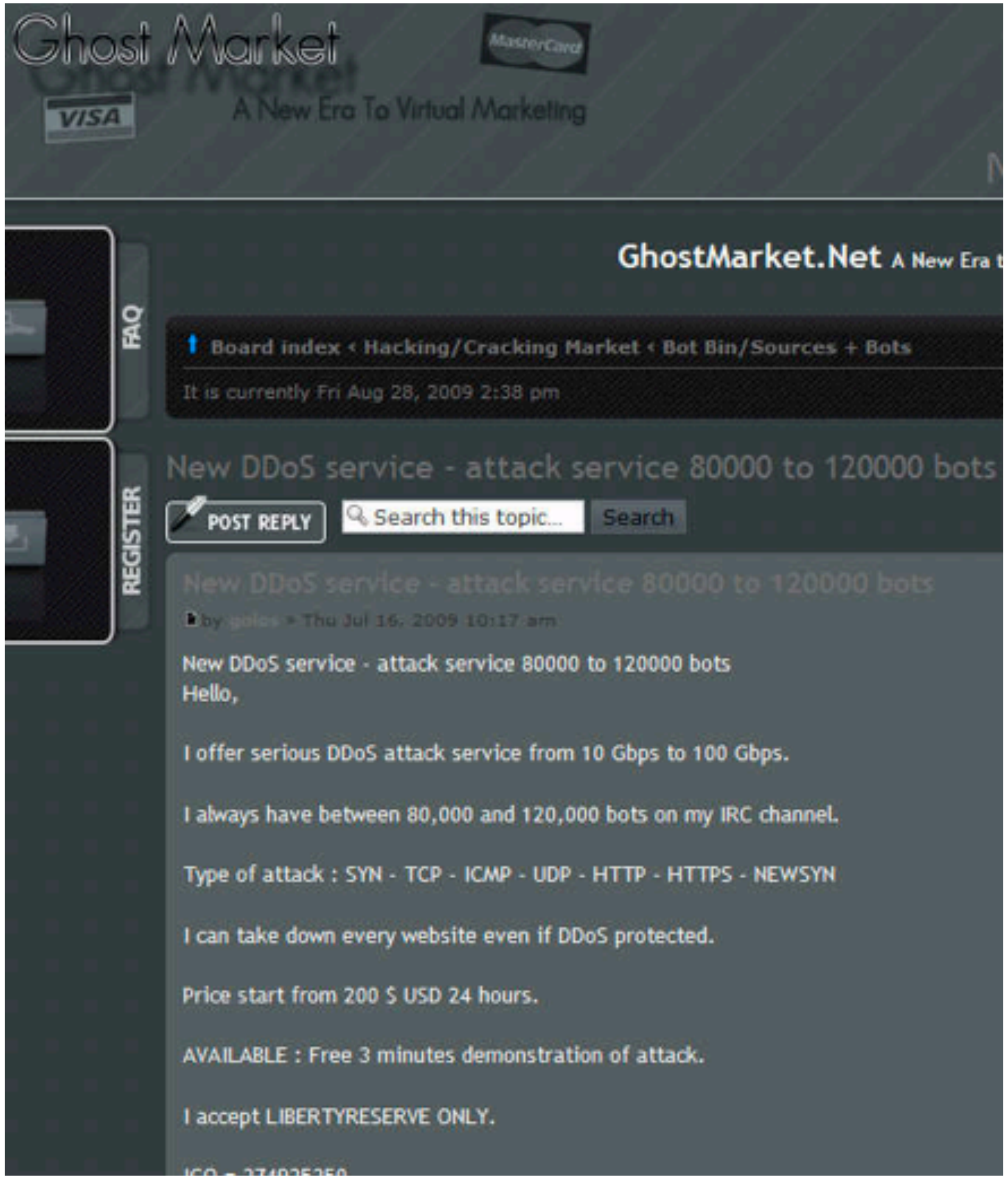
Undergraduate

Expert

Specialist

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	$0.06–$30
2	2	Bank account credentials	19%	17%	$10–$1000
3	9	Email accounts	5%	4%	$0.10–$100
4	3	Email addresses	5%	6%	$0.33/MB–$100/MB
5	12	Proxies	4%	3%	$0.16–$20
6	4	Full identities	4%	6%	$0.70–$60
7	6	Mailers	3%	5%	$2–$40
8	5	Cash out services	3%	5%	8%–50% or flat rate of $200–$2000 per item
9	17	Shell scripts	3%	2%	$2–$20
10	8	Scams	3%	5%	$3–$40/week for hosting, $2–$20 design

Table 1. Goods and services available for sale on underground economy servers
Source: Symantec



GhostMarket.Net A New Era t

Board index ‹ Hacking/Cracking Market ‹ Bot Bin/Sources + Bots

It is currently Fri Aug 28, 2009 2:38 pm

New DDoS service - attack service 80000 to 120000 bots

New DDoS service - attack service 80000 to 120000 bots

by golos » Thu Jul 16, 2009 10:17 am

New DDoS service - attack service 80000 to 120000 bots
Hello,

I offer serious DDoS attack service from 10 Gbps to 100 Gbps.

I always have between 80,000 and 120,000 bots on my IRC channel.

Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN

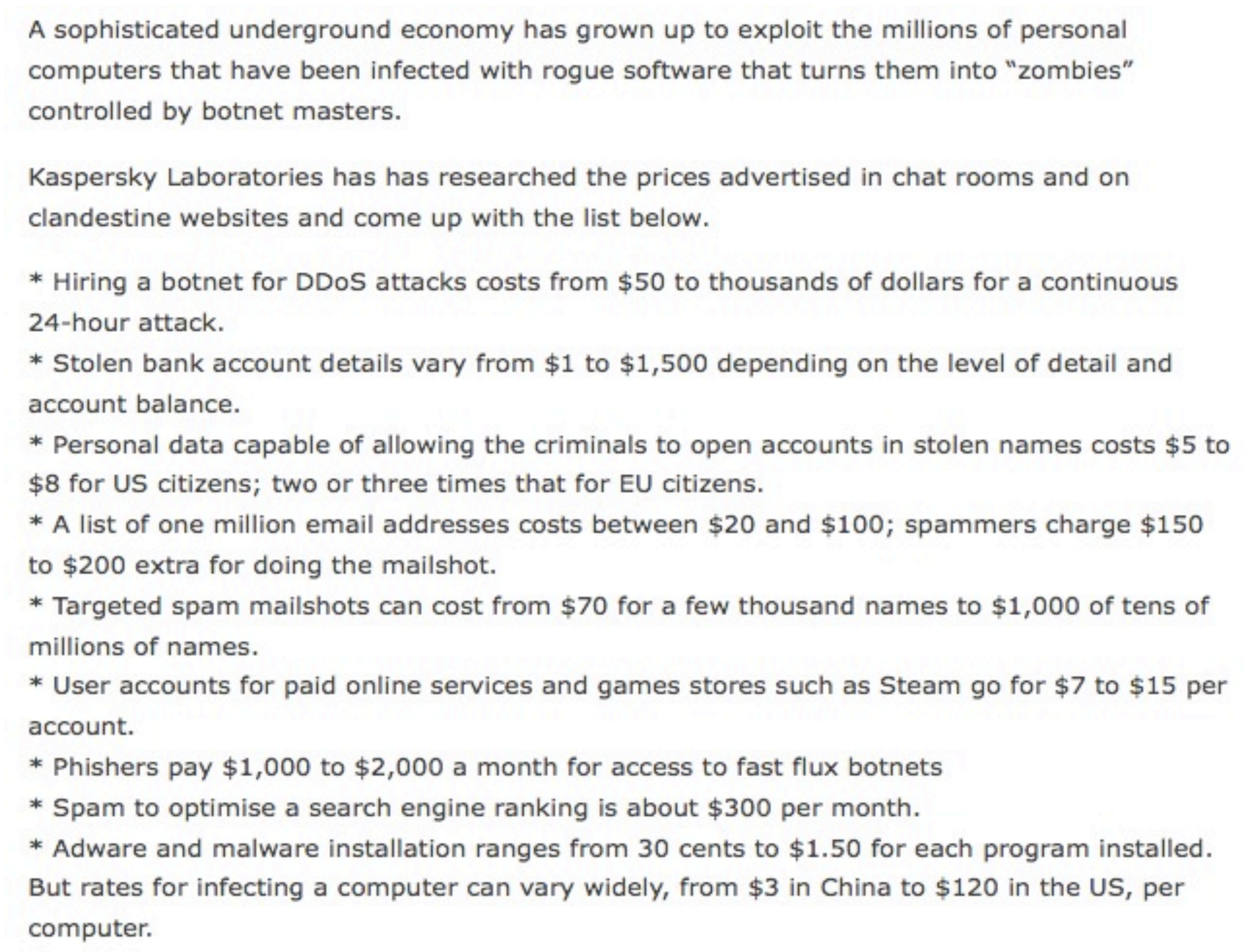
I can take down every website even if DDoS protected.

Price start from 200 $ USD 24 hours.

AVAILABLE : Free 3 minutes demonstration of attack.

I accept LIBERTYRESERVE ONLY.

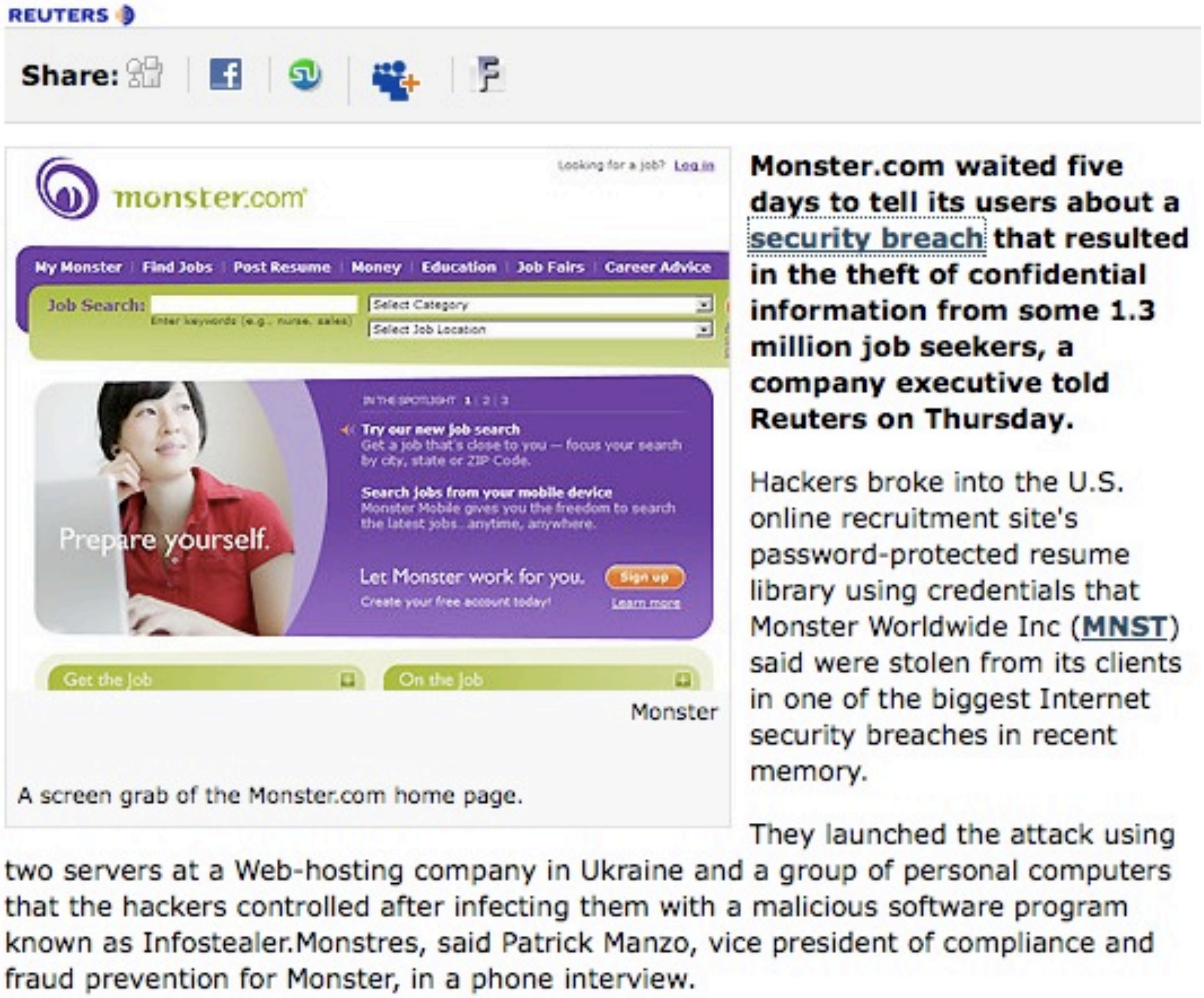
ICQ = 274025250



A sophisticated underground economy has grown up to exploit the millions of personal computers that have been infected with rogue software that turns them into "zombies" controlled by botnet masters.

Kaspersky Laboratories has has researched the prices advertised in chat rooms and on clandestine websites and come up with the list below.

* Hiring a botnet for DDoS attacks costs from $50 to thousands of dollars for a continuous 24-hour attack.
* Stolen bank account details vary from $1 to $1,500 depending on the level of detail and account balance.
* Personal data capable of allowing the criminals to open accounts in stolen names costs $5 to $8 for US citizens; two or three times that for EU citizens.
* A list of one million email addresses costs between $20 and $100; spammers charge $150 to $200 extra for doing the mailshot.
* Targeted spam mailshots can cost from $70 for a few thousand names to $1,000 of tens of millions of names.
* User accounts for paid online services and games stores such as Steam go for $7 to $15 per account.
* Phishers pay $1,000 to $2,000 a month for access to fast flux botnets
* Spam to optimise a search engine ranking is about $300 per month.
* Adware and malware installation ranges from 30 cents to $1.50 for each program installed. But rates for infecting a computer can vary widely, from $3 in China to $120 in the US, per computer.


REUTERS
Share:
monster.com
Looking for a job? Log in
My Monster | Find Jobs | Post Resume | Money | Education | Job Fairs | Career Advice
Job Search:
Enter keywords (e.g., nurse, sales)
Select Category
Select Job Location
IN THE SPOTLIGHT 1 | 2 | 3
Try our new job search
Get a job that's close to you — focus your search by city, state or ZIP Code.
Search jobs from your mobile device
Monster Mobile gives you the freedom to search the latest jobs...anytime, anywhere.
Prepare yourself.
Let Monster work for you.
Sign up
Create your free account today!
Learn more
Get the Job
On the Job

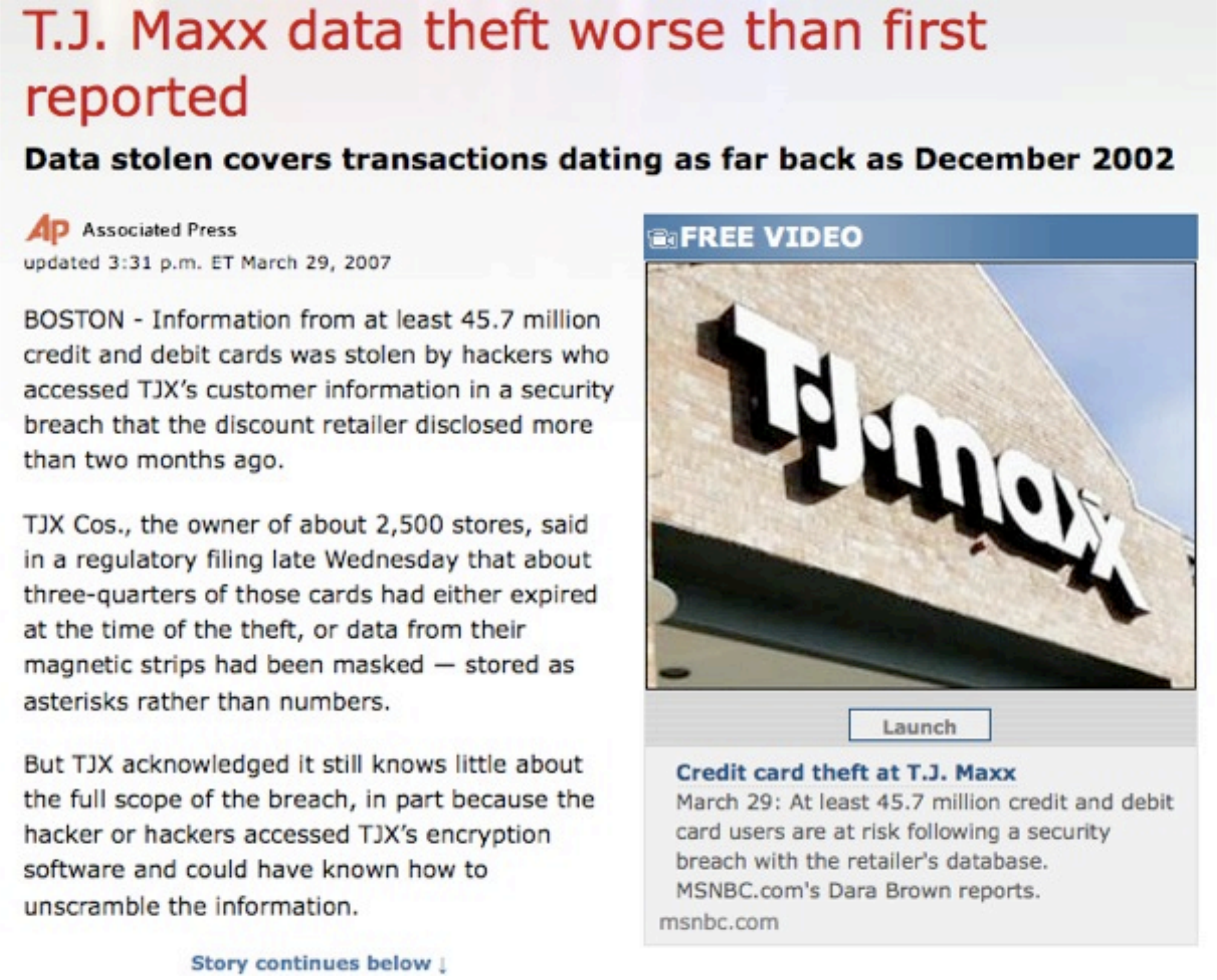
Monster

A screen grab of the Monster.com home page.

Monster.com waited five days to tell its users about a security breach that resulted in the theft of confidential information from some 1.3 million job seekers, a company executive told Reuters on Thursday.

Hackers broke into the U.S. online recruitment site's password-protected resume library using credentials that Monster Worldwide Inc (**MNST**) said were stolen from its clients in one of the biggest Internet security breaches in recent memory.

They launched the attack using two servers at a Web-hosting company in Ukraine and a group of personal computers that the hackers controlled after infecting them with a malicious software program known as Infostealer.Monstres, said Patrick Manzo, vice president of compliance and fraud prevention for Monster, in a phone interview.



T.J. Maxx data theft worse than first reported

Data stolen covers transactions dating as far back as December 2002

AP Associated Press
updated 3:31 p.m. ET March 29, 2007

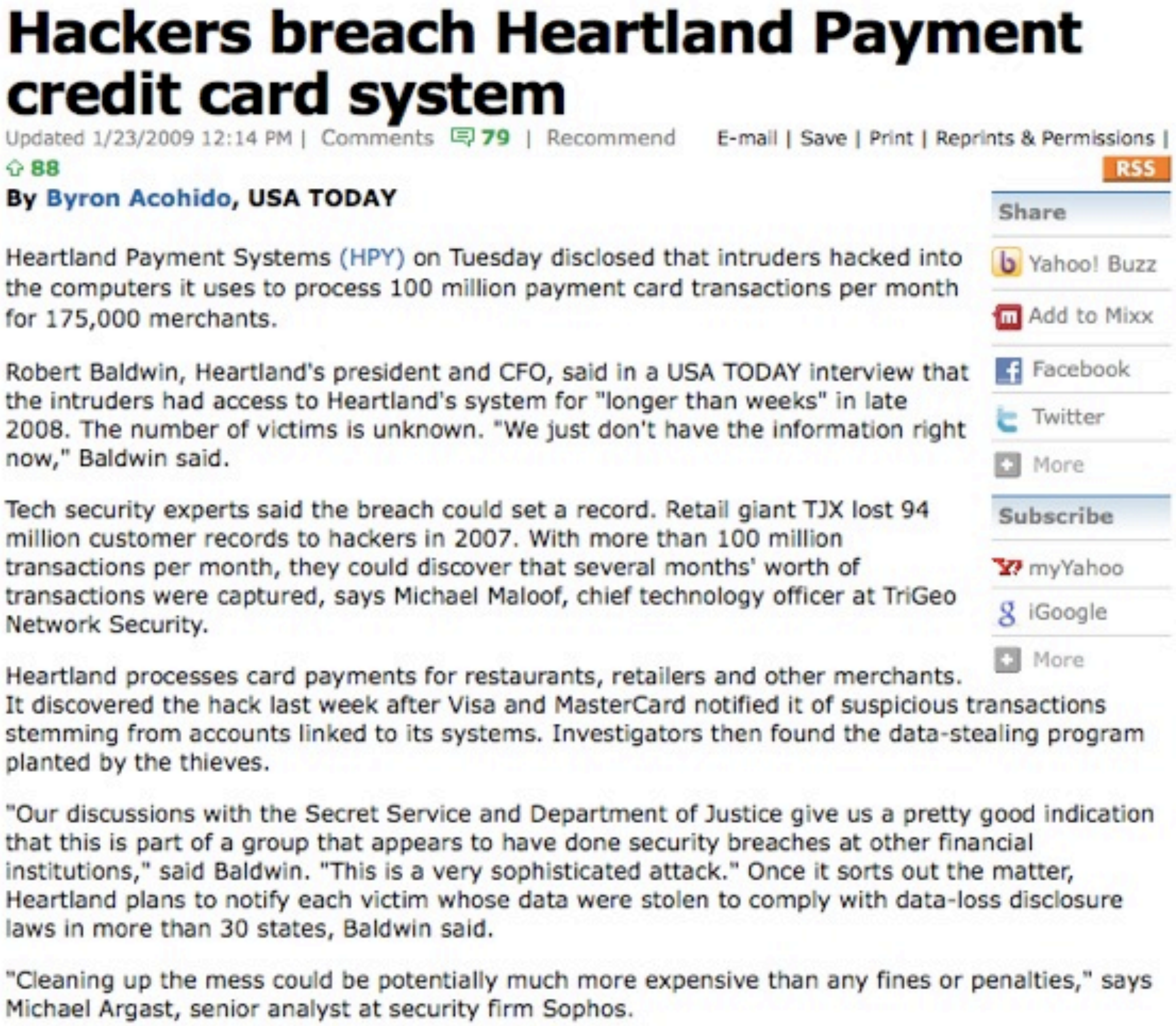
BOSTON - Information from at least 45.7 million credit and debit cards was stolen by hackers who accessed TJX's customer information in a security breach that the discount retailer disclosed more than two months ago.

TJX Cos., the owner of about 2,500 stores, said in a regulatory filing late Wednesday that about three-quarters of those cards had either expired at the time of the theft, or data from their magnetic strips had been masked — stored as asterisks rather than numbers.

But TJX acknowledged it still knows little about the full scope of the breach, in part because the hacker or hackers accessed TJX's encryption software and could have known how to unscramble the information.

Credit card theft at T.J. Maxx
March 29: At least 45.7 million credit and debit card users are at risk following a security breach with the retailer's database. MSNBC.com's Dara Brown reports.
msnbc.com

Story continues below ↓



Hackers breach Heartland Payment credit card system

Updated 1/23/2009 12:14 PM | Comments 79 | Recommend 88

E-mail | Save | Print | Reprints & Permissions | RSS

By Byron Acohido, USA TODAY

Heartland Payment Systems (HPY) on Tuesday disclosed that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants.

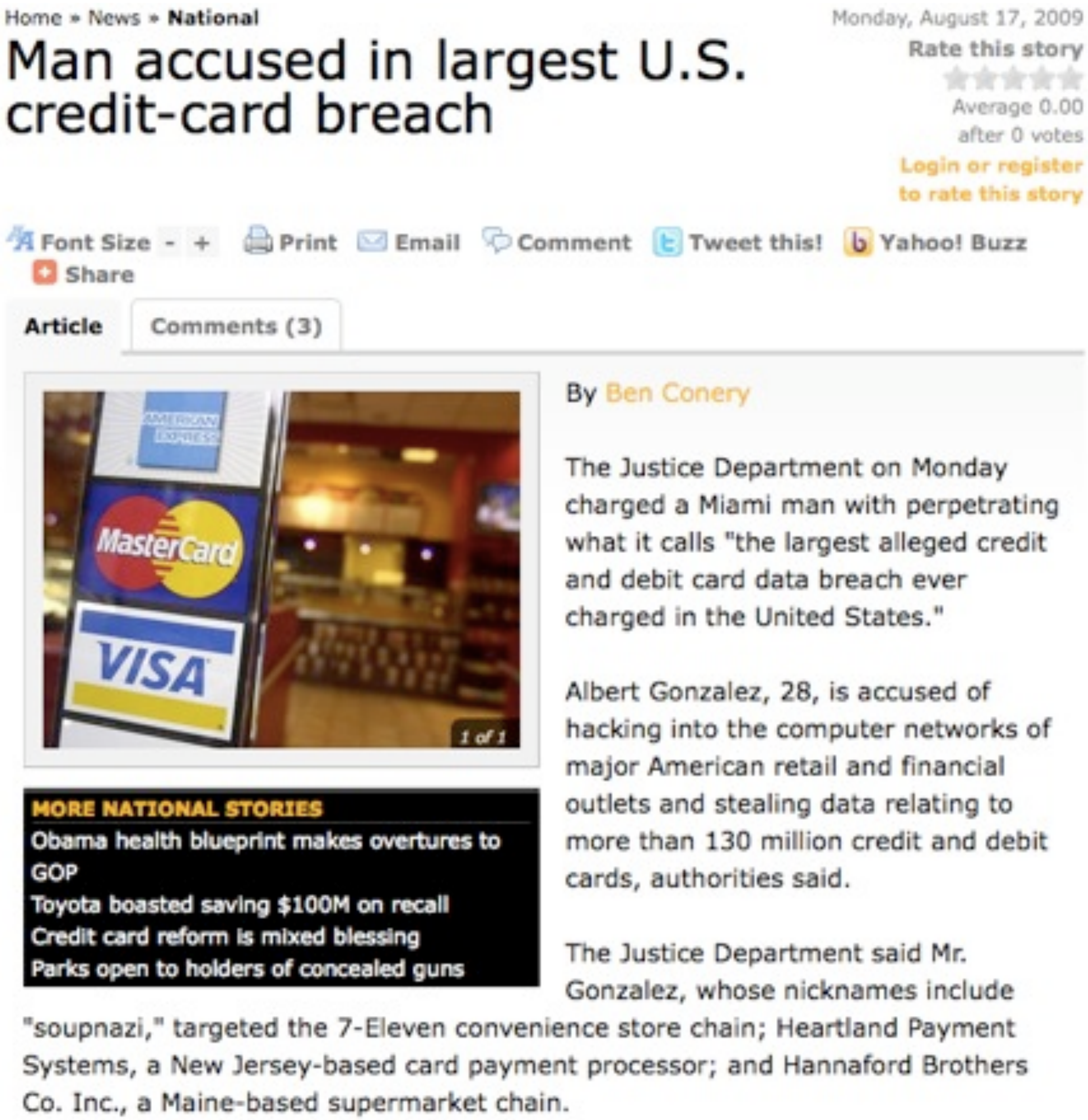
Robert Baldwin, Heartland's president and CFO, said in a USA TODAY interview that the intruders had access to Heartland's system for "longer than weeks" in late 2008. The number of victims is unknown. "We just don't have the information right now," Baldwin said.

Tech security experts said the breach could set a record. Retail giant TJX lost 94 million customer records to hackers in 2007. With more than 100 million transactions per month, they could discover that several months' worth of transactions were captured, says Michael Maloof, chief technology officer at TriGeo Network Security.

Heartland processes card payments for restaurants, retailers and other merchants. It discovered the hack last week after Visa and MasterCard notified it of suspicious transactions stemming from accounts linked to its systems. Investigators then found the data-stealing program planted by the thieves.

"Our discussions with the Secret Service and Department of Justice give us a pretty good indication that this is part of a group that appears to have done security breaches at other financial institutions," said Baldwin. "This is a very sophisticated attack." Once it sorts out the matter, Heartland plans to notify each victim whose data were stolen to comply with data-loss disclosure laws in more than 30 states, Baldwin said.

"Cleaning up the mess could be potentially much more expensive than any fines or penalties," says Michael Argast, senior analyst at security firm Sophos.



Home » News » **National**

Monday, August 17, 2009

Man accused in largest U.S. credit-card breach

Rate this story

☆☆☆☆☆

Average 0.00
after 0 votes

Login or register to rate this story

By Ben Conery

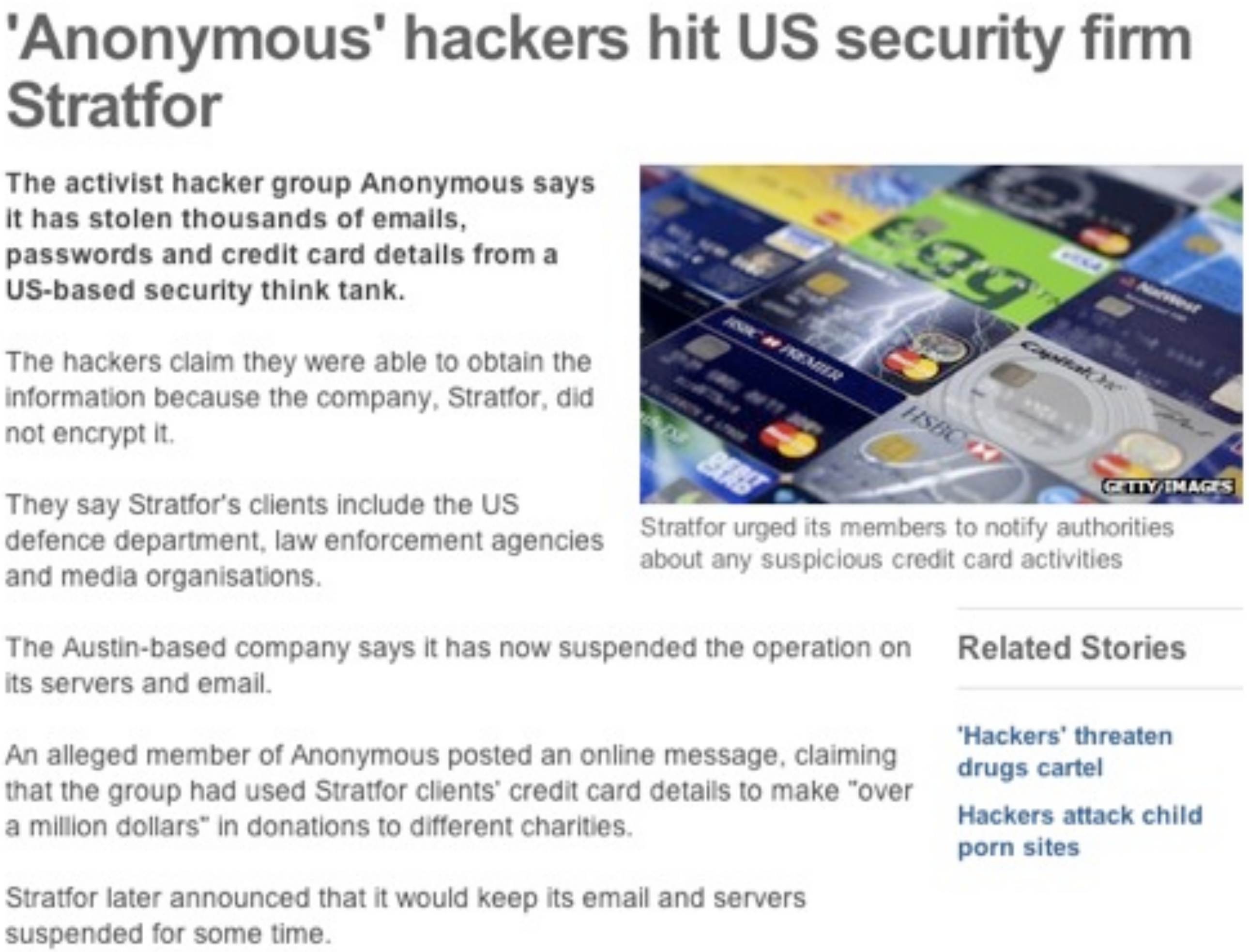
The Justice Department on Monday charged a Miami man with perpetrating what it calls "the largest alleged credit and debit card data breach ever charged in the United States."

Albert Gonzalez, 28, is accused of hacking into the computer networks of major American retail and financial outlets and stealing data relating to more than 130 million credit and debit cards, authorities said.

The Justice Department said Mr. Gonzalez, whose nicknames include "soupnazi," targeted the 7-Eleven convenience store chain; Heartland Payment Systems, a New Jersey-based card payment processor; and Hannaford Brothers Co. Inc., a Maine-based supermarket chain.

MORE NATIONAL STORIES

Obama health blueprint makes overtures to GOP
Toyota boasted saving $100M on recall
Credit card reform is mixed blessing
Parks open to holders of concealed guns



'Anonymous' hackers hit US security firm Stratfor

The activist hacker group Anonymous says it has stolen thousands of emails, passwords and credit card details from a US-based security think tank.

The hackers claim they were able to obtain the information because the company, Stratfor, did not encrypt it.

They say Stratfor's clients include the US defence department, law enforcement agencies and media organisations.

Stratfor urged its members to notify authorities about any suspicious credit card activities

The Austin-based company says it has now suspended the operation on its servers and email.

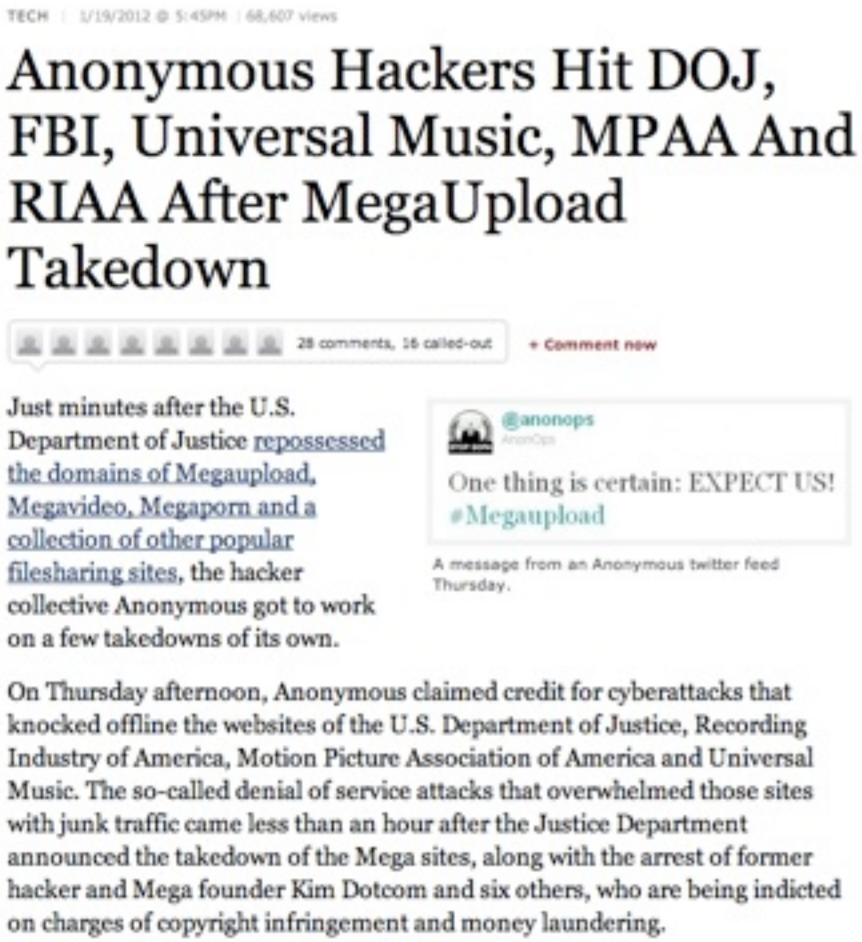
An alleged member of Anonymous posted an online message, claiming that the group had used Stratfor clients' credit card details to make "over a million dollars" in donations to different charities.

Stratfor later announced that it would keep its email and servers suspended for some time.

Related Stories

'Hackers' threaten drugs cartel

Hackers attack child porn sites



TECH | 1/19/2012 @ 5:45PM | 68,607 views

Anonymous Hackers Hit DOJ, FBI, Universal Music, MPAA And RIAA After MegaUpload Takedown

28 comments, 16 called-out + Comment now

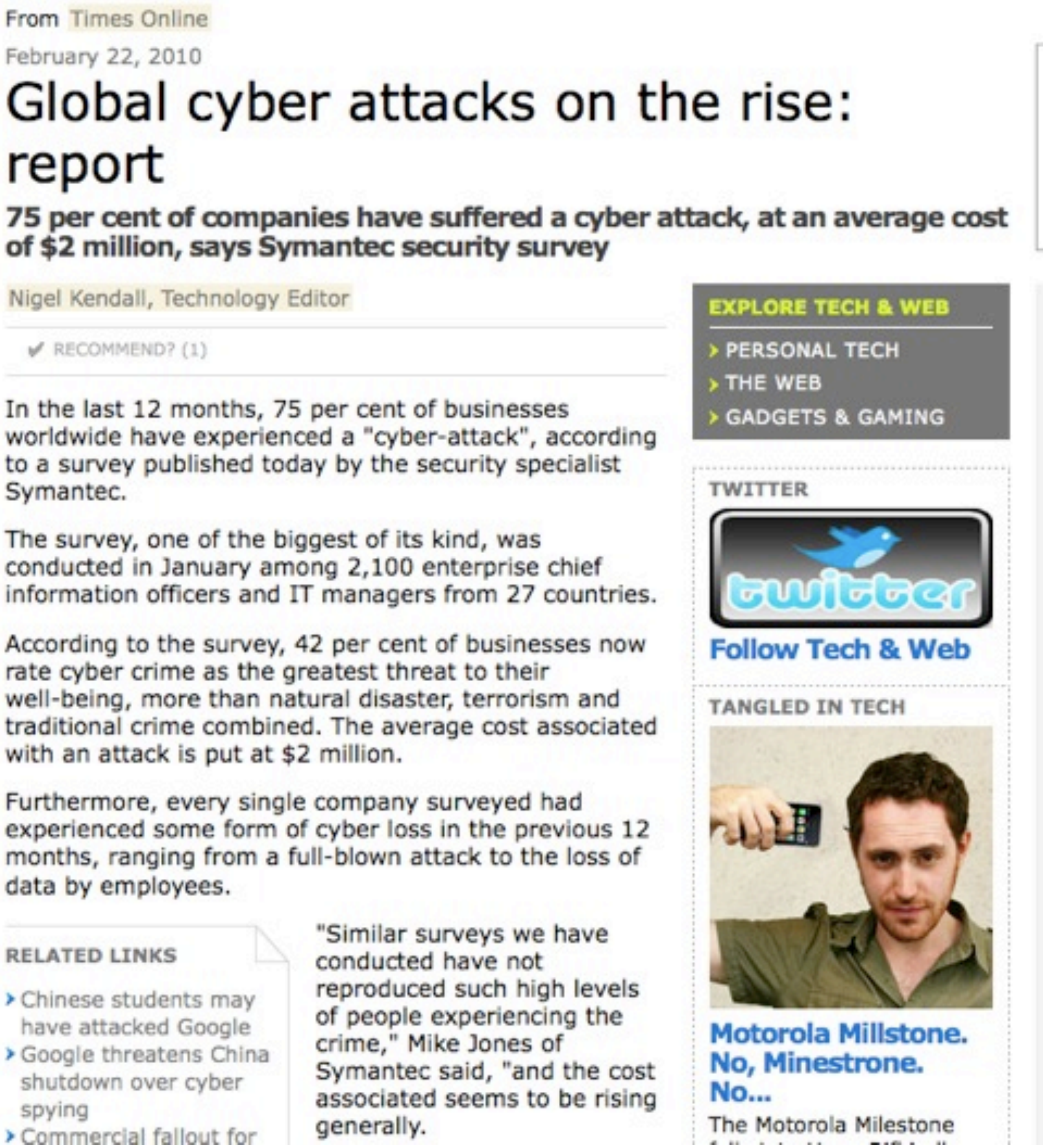
Just minutes after the U.S. Department of Justice repossessed the domains of Megaupload, Megavideo, Megaporn and a collection of other popular filesharing sites, the hacker collective Anonymous got to work on a few takedowns of its own.

@anonops
AnonOps

One thing is certain: EXPECT US! #Megaupload

A message from an Anonymous twitter feed Thursday.

On Thursday afternoon, Anonymous claimed credit for cyberattacks that knocked offline the websites of the U.S. Department of Justice, Recording Industry of America, Motion Picture Association of America and Universal Music. The so-called denial of service attacks that overwhelmed those sites with junk traffic came less than an hour after the Justice Department announced the takedown of the Mega sites, along with the arrest of former hacker and Mega founder Kim Dotcom and six others, who are being indicted on charges of copyright infringement and money laundering.



From Times Online

February 22, 2010

Global cyber attacks on the rise: report

75 per cent of companies have suffered a cyber attack, at an average cost of $2 million, says Symantec security survey

Nigel Kendall, Technology Editor

✔ RECOMMEND? (1)

In the last 12 months, 75 per cent of businesses worldwide have experienced a "cyber-attack", according to a survey published today by the security specialist Symantec.

The survey, one of the biggest of its kind, was conducted in January among 2,100 enterprise chief information officers and IT managers from 27 countries.

According to the survey, 42 per cent of businesses now rate cyber crime as the greatest threat to their well-being, more than natural disaster, terrorism and traditional crime combined. The average cost associated with an attack is put at $2 million.

Furthermore, every single company surveyed had experienced some form of cyber loss in the previous 12 months, ranging from a full-blown attack to the loss of data by employees.

"Similar surveys we have conducted have not reproduced such high levels of people experiencing the crime," Mike Jones of Symantec said, "and the cost associated seems to be rising generally.

RELATED LINKS

- Chinese students may have attacked Google
- Google threatens China shutdown over cyber spying
- Commercial fallout for

EXPLORE TECH & WEB

- › PERSONAL TECH
- › THE WEB
- › GADGETS & GAMING

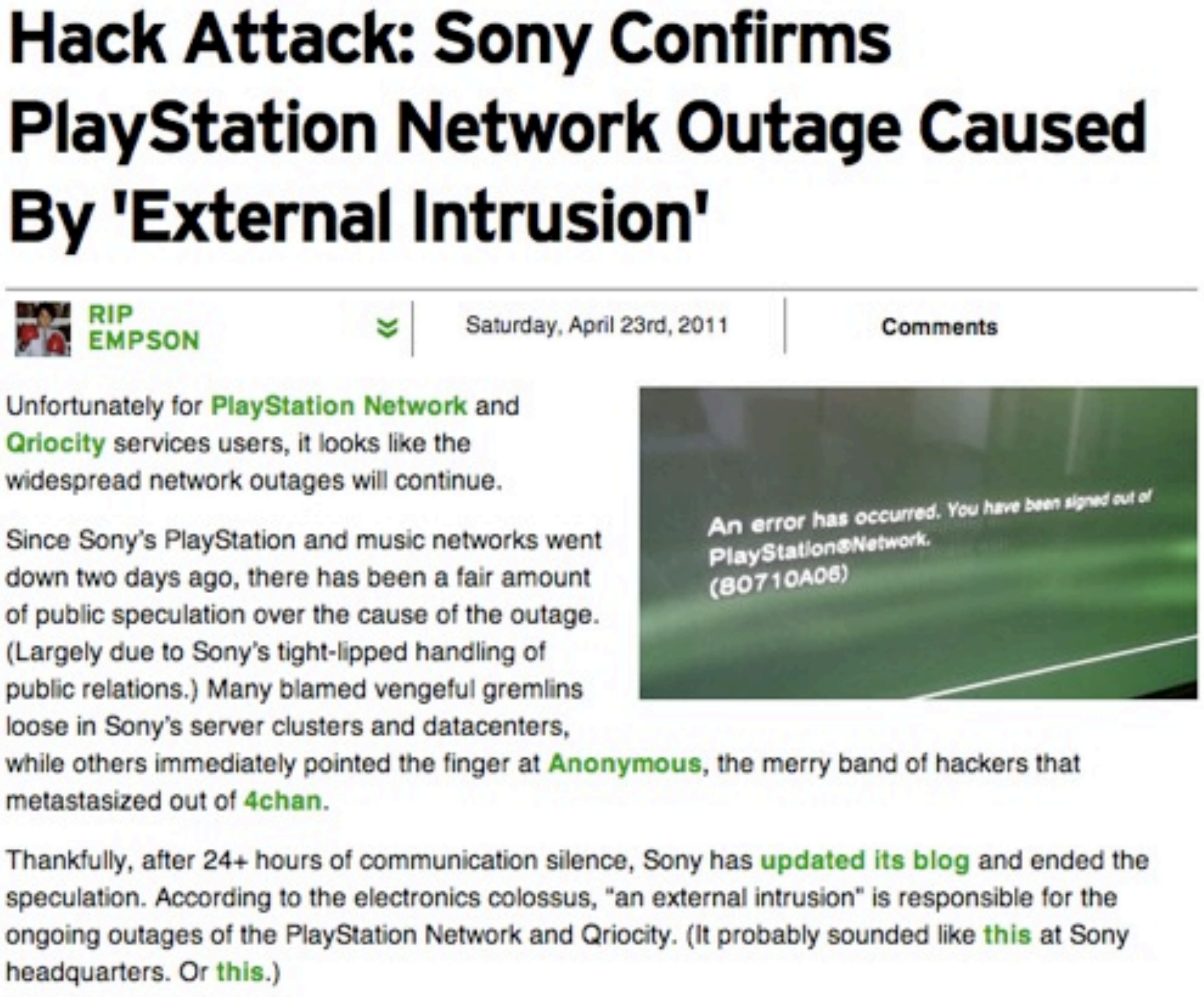
TWITTER

Follow Tech & Web

TANGLED IN TECH

Motorola Millstone. No, Minestrone. No...

The Motorola Milestone



Hack Attack: Sony Confirms PlayStation Network Outage Caused By 'External Intrusion'

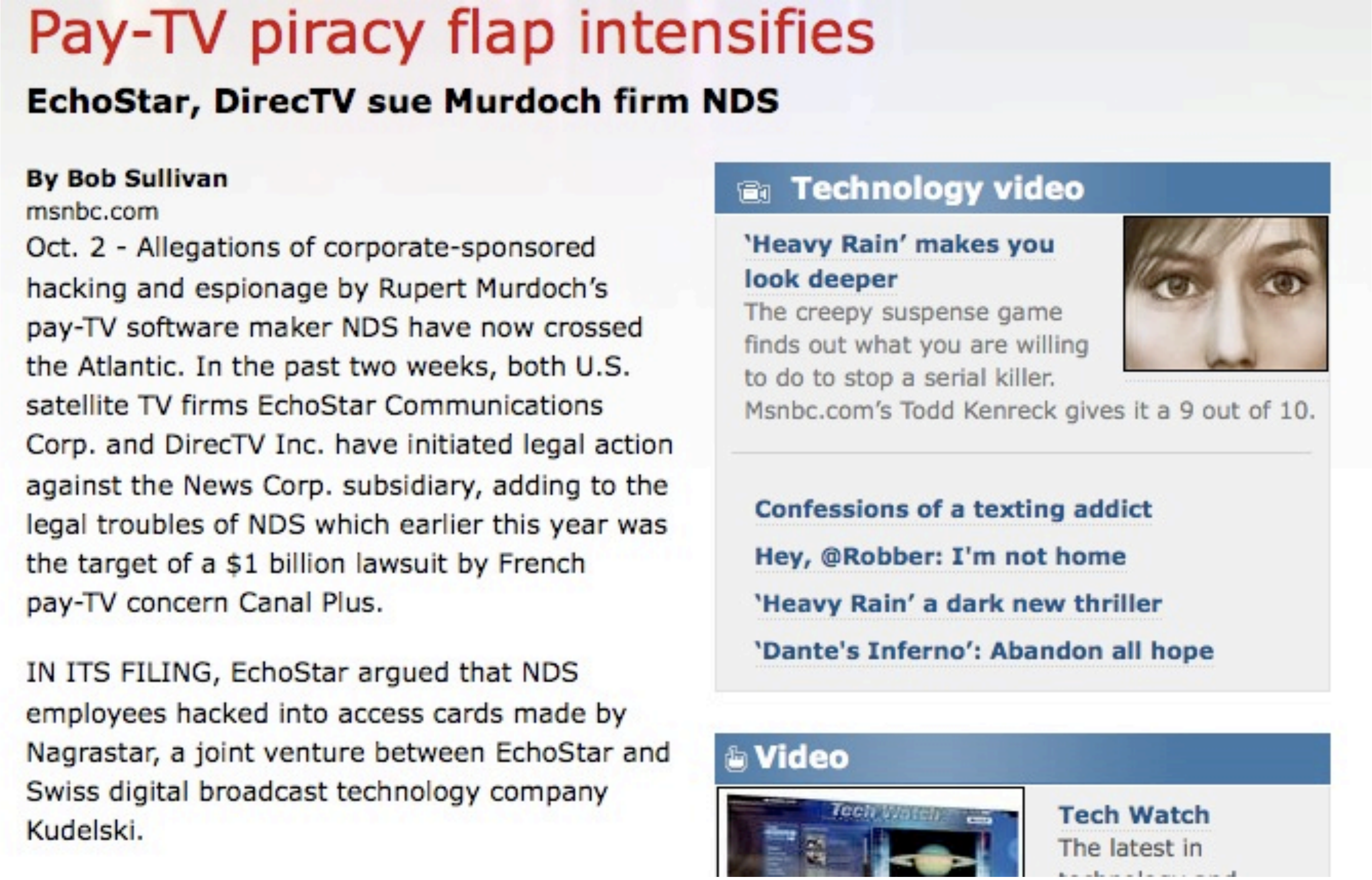
RIP EMPSON | Saturday, April 23rd, 2011 | Comments

An error has occurred. You have been signed out of PlayStation®Network.
(80710A06)

Unfortunately for PlayStation Network and Qriocity services users, it looks like the widespread network outages will continue.

Since Sony's PlayStation and music networks went down two days ago, there has been a fair amount of public speculation over the cause of the outage. (Largely due to Sony's tight-lipped handling of public relations.) Many blamed vengeful gremlins loose in Sony's server clusters and datacenters, while others immediately pointed the finger at Anonymous, the merry band of hackers that metastasized out of 4chan.

Thankfully, after 24+ hours of communication silence, Sony has updated its blog and ended the speculation. According to the electronics colossus, "an external intrusion" is responsible for the ongoing outages of the PlayStation Network and Qriocity. (It probably sounded like this at Sony headquarters. Or this.)



Pay-TV piracy flap intensifies

EchoStar, DirecTV sue Murdoch firm NDS

By Bob Sullivan
msnbc.com

Oct. 2 - Allegations of corporate-sponsored hacking and espionage by Rupert Murdoch's pay-TV software maker NDS have now crossed the Atlantic. In the past two weeks, both U.S. satellite TV firms EchoStar Communications Corp. and DirecTV Inc. have initiated legal action against the News Corp. subsidiary, adding to the legal troubles of NDS which earlier this year was the target of a $1 billion lawsuit by French pay-TV concern Canal Plus.

IN ITS FILING, EchoStar argued that NDS employees hacked into access cards made by Nagrastar, a joint venture between EchoStar and Swiss digital broadcast technology company Kudelski.

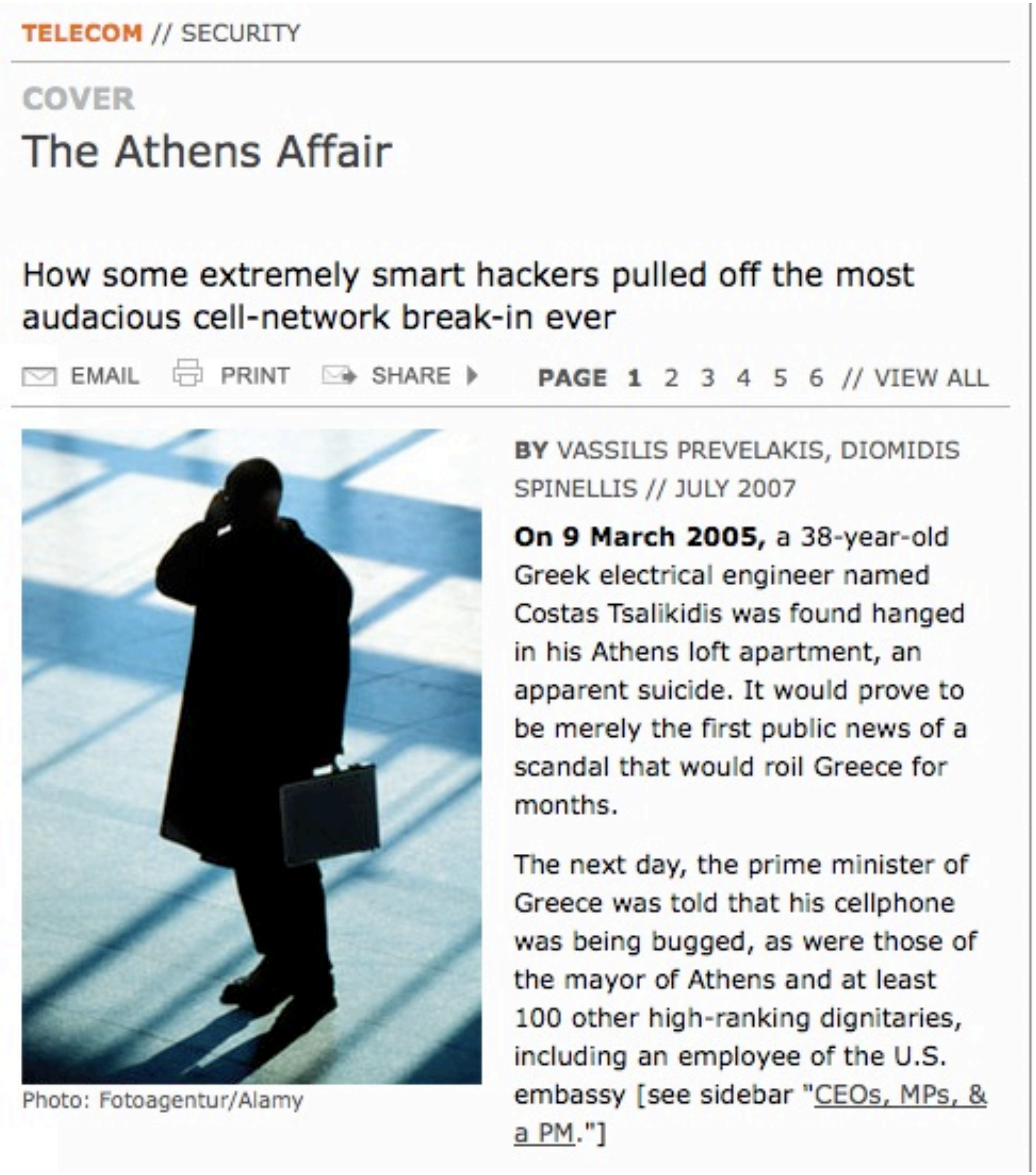
Technology video

'Heavy Rain' makes you look deeper
The creepy suspense game finds out what you are willing to do to stop a serial killer. Msnbc.com's Todd Kenreck gives it a 9 out of 10.

Confessions of a texting addict
Hey, @Robber: I'm not home
'Heavy Rain' a dark new thriller
'Dante's Inferno': Abandon all hope

Video

Tech Watch
The latest in



TELECOM // SECURITY

COVER

The Athens Affair

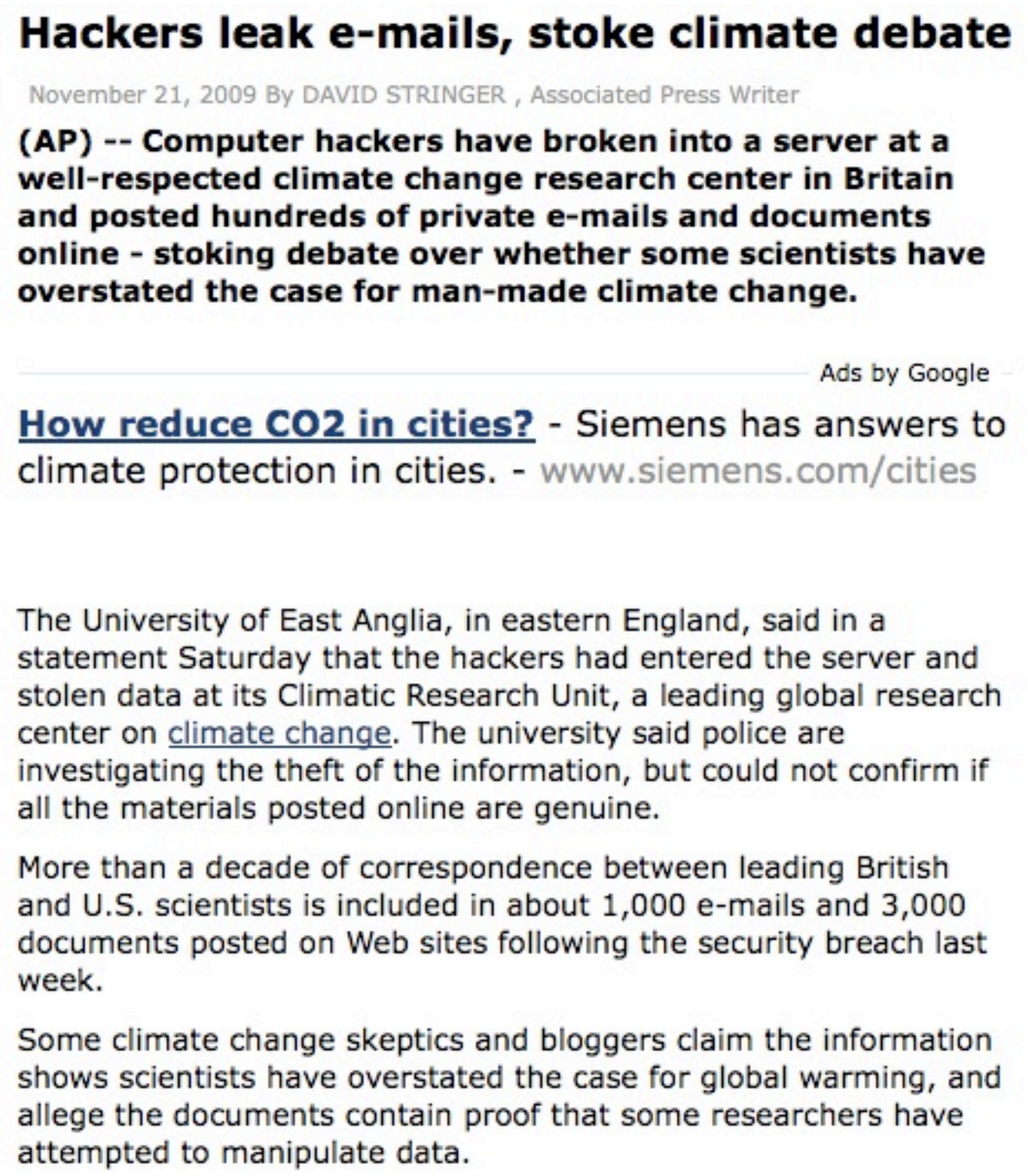
How some extremely smart hackers pulled off the most audacious cell-network break-in ever

BY VASSILIS PREVELAKIS, DIOMIDIS SPINELLIS // JULY 2007

On 9 March 2005, a 38-year-old Greek electrical engineer named Costas Tsalikidis was found hanged in his Athens loft apartment, an apparent suicide. It would prove to be merely the first public news of a scandal that would roil Greece for months.

The next day, the prime minister of Greece was told that his cellphone was being bugged, as were those of the mayor of Athens and at least 100 other high-ranking dignitaries, including an employee of the U.S. embassy [see sidebar "CEOs, MPs, & a PM."]

Photo: Fotoagentur/Alamy



Hackers leak e-mails, stoke climate debate

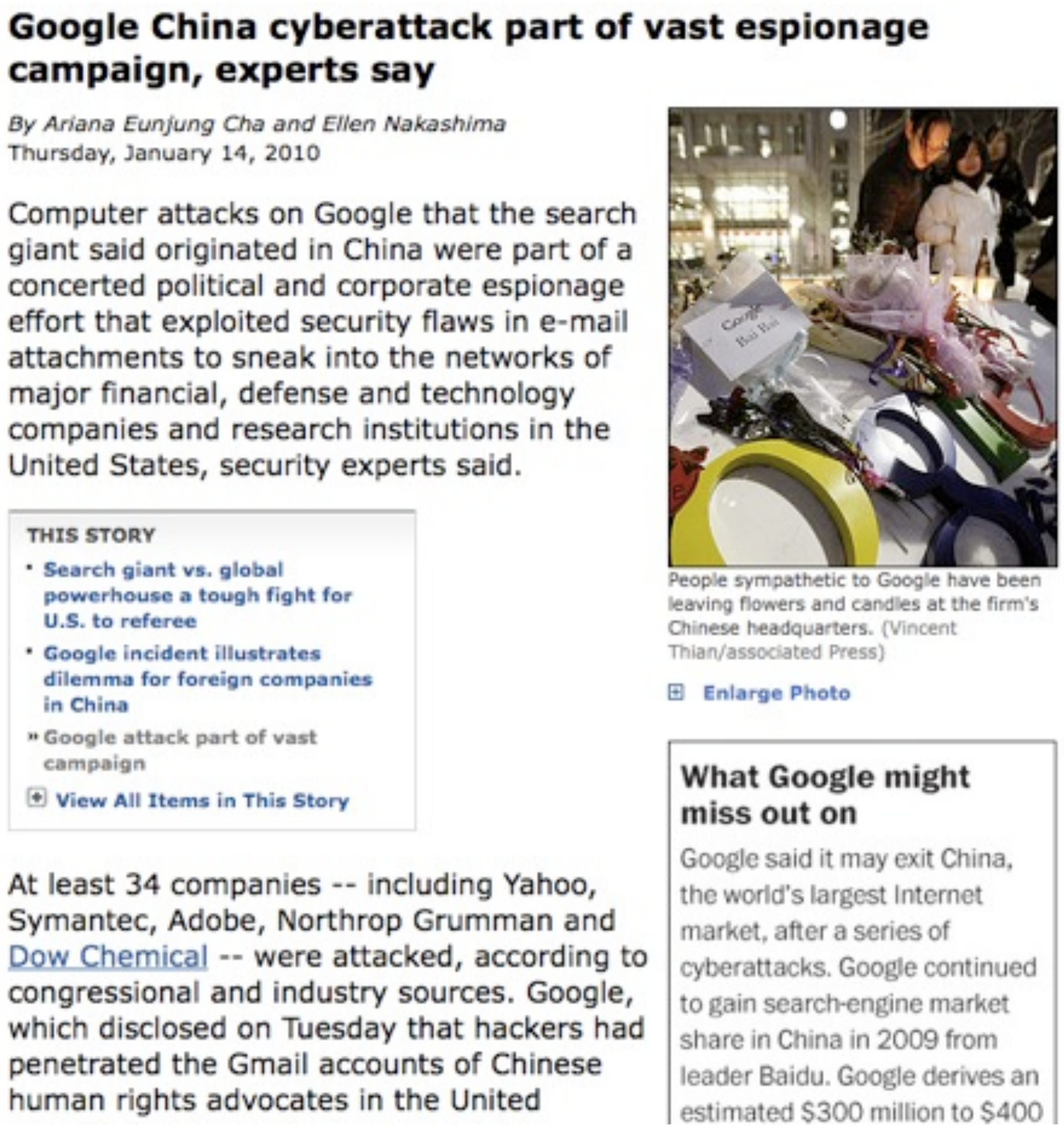
November 21, 2009 By DAVID STRINGER , Associated Press Writer

(AP) -- Computer hackers have broken into a server at a well-respected climate change research center in Britain and posted hundreds of private e-mails and documents online - stoking debate over whether some scientists have overstated the case for man-made climate change.

The University of East Anglia, in eastern England, said in a statement Saturday that the hackers had entered the server and stolen data at its Climatic Research Unit, a leading global research center on climate change. The university said police are investigating the theft of the information, but could not confirm if all the materials posted online are genuine.

More than a decade of correspondence between leading British and U.S. scientists is included in about 1,000 e-mails and 3,000 documents posted on Web sites following the security breach last week.

Some climate change skeptics and bloggers claim the information shows scientists have overstated the case for global warming, and allege the documents contain proof that some researchers have attempted to manipulate data.



Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima
Thursday, January 14, 2010

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

THIS STORY

- **Search giant vs. global powerhouse a tough fight for U.S. to referee**
- **Google incident illustrates dilemma for foreign companies in China**
- » Google attack part of vast campaign

⊞ **View All Items in This Story**

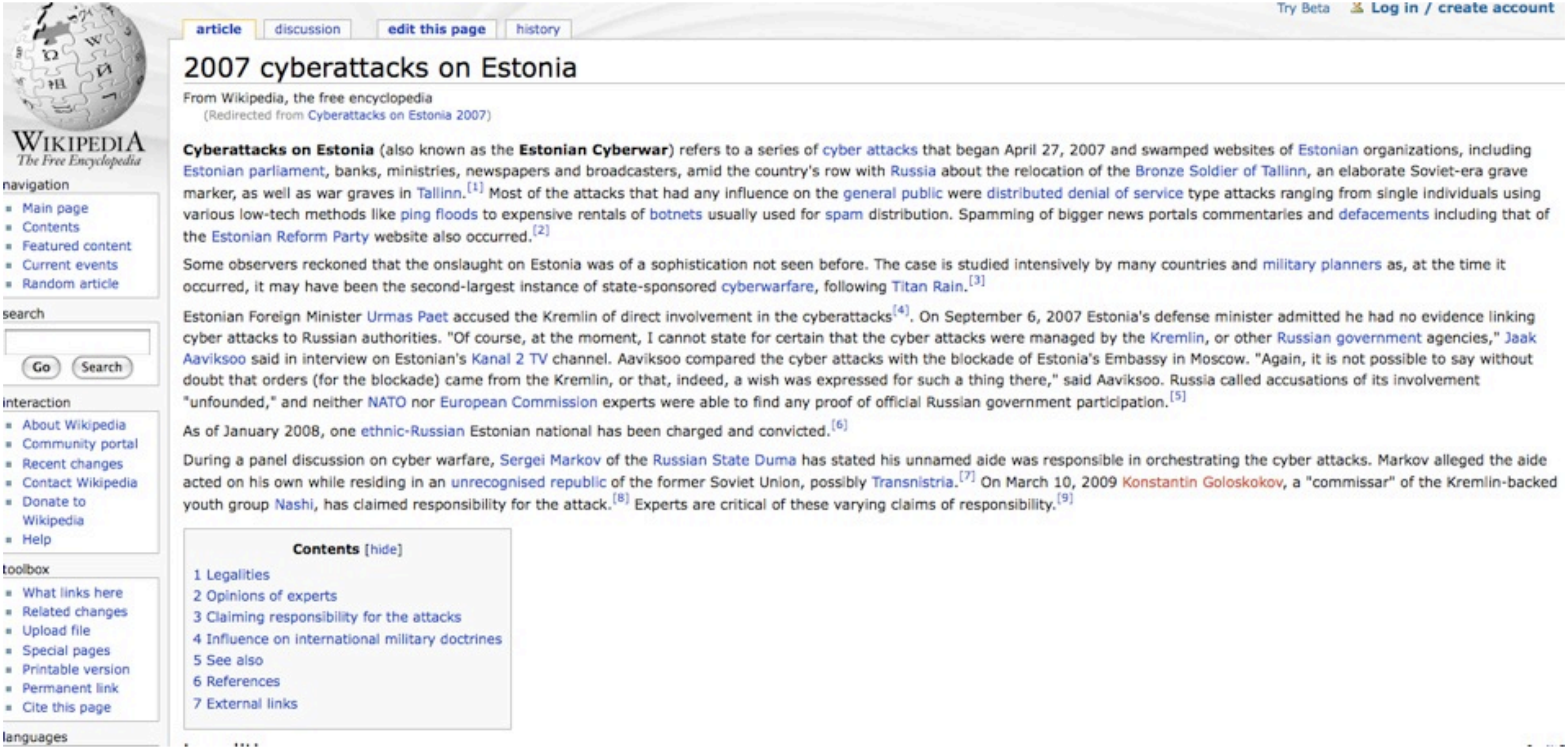
At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail accounts of Chinese human rights advocates in the United

People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

⊞ **Enlarge Photo**

What Google might miss out on

Google said it may exit China, the world's largest Internet market, after a series of cyberattacks. Google continued to gain search-engine market share in China in 2009 from leader Baidu. Google derives an estimated $300 million to $400



2007 cyberattacks on Estonia

From Wikipedia, the free encyclopedia
(Redirected from Cyberattacks on Estonia 2007)

Cyberattacks on Estonia (also known as the **Estonian Cyberwar**) refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's row with Russia about the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn.[1] Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred.[2]

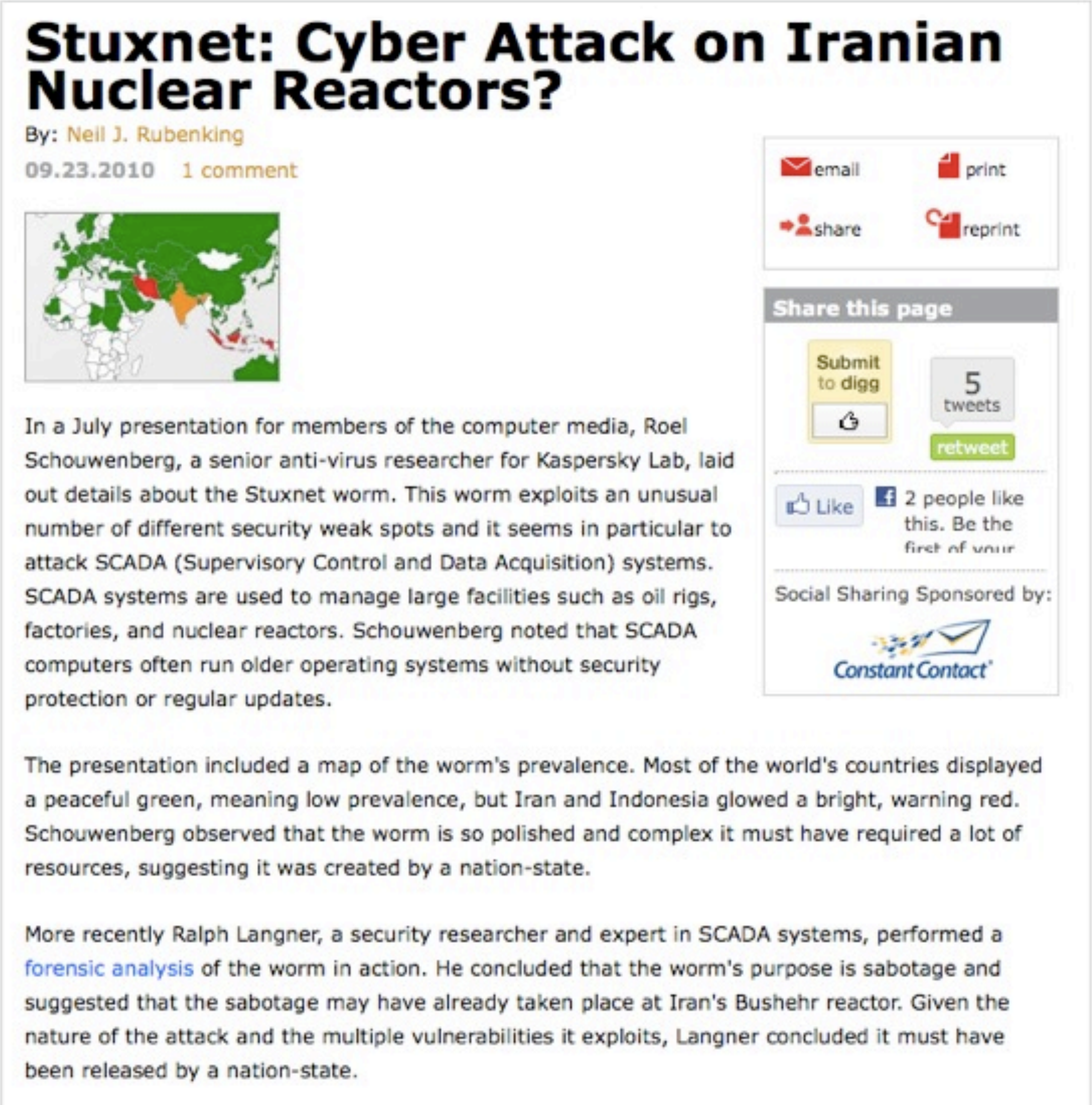
Some observers reckoned that the onslaught on Estonia was of a sophistication not seen before. The case is studied intensively by many countries and military planners as, at the time it occurred, it may have been the second-largest instance of state-sponsored cyberwarfare, following Titan Rain.[3]

Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyberattacks[4]. On September 6, 2007 Estonia's defense minister admitted he had no evidence linking cyber attacks to Russian authorities. "Of course, at the moment, I cannot state for certain that the cyber attacks were managed by the Kremlin, or other Russian government agencies," Jaak Aaviksoo said in interview on Estonian's Kanal 2 TV channel. Aaviksoo compared the cyber attacks with the blockade of Estonia's Embassy in Moscow. "Again, it is not possible to say without doubt that orders (for the blockade) came from the Kremlin, or that, indeed, a wish was expressed for such a thing there," said Aaviksoo. Russia called accusations of its involvement "unfounded," and neither NATO nor European Commission experts were able to find any proof of official Russian government participation.[5]

As of January 2008, one ethnic-Russian Estonian national has been charged and convicted.[6]

During a panel discussion on cyber warfare, Sergei Markov of the Russian State Duma has stated his unnamed aide was responsible in orchestrating the cyber attacks. Markov alleged the aide acted on his own while residing in an unrecognised republic of the former Soviet Union, possibly Transnistria.[7] On March 10, 2009 Konstantin Goloskokov, a "commissar" of the Kremlin-backed youth group Nashi, has claimed responsibility for the attack.[8] Experts are critical of these varying claims of responsibility.[9]

Contents [hide]



Stuxnet: Cyber Attack on Iranian Nuclear Reactors?

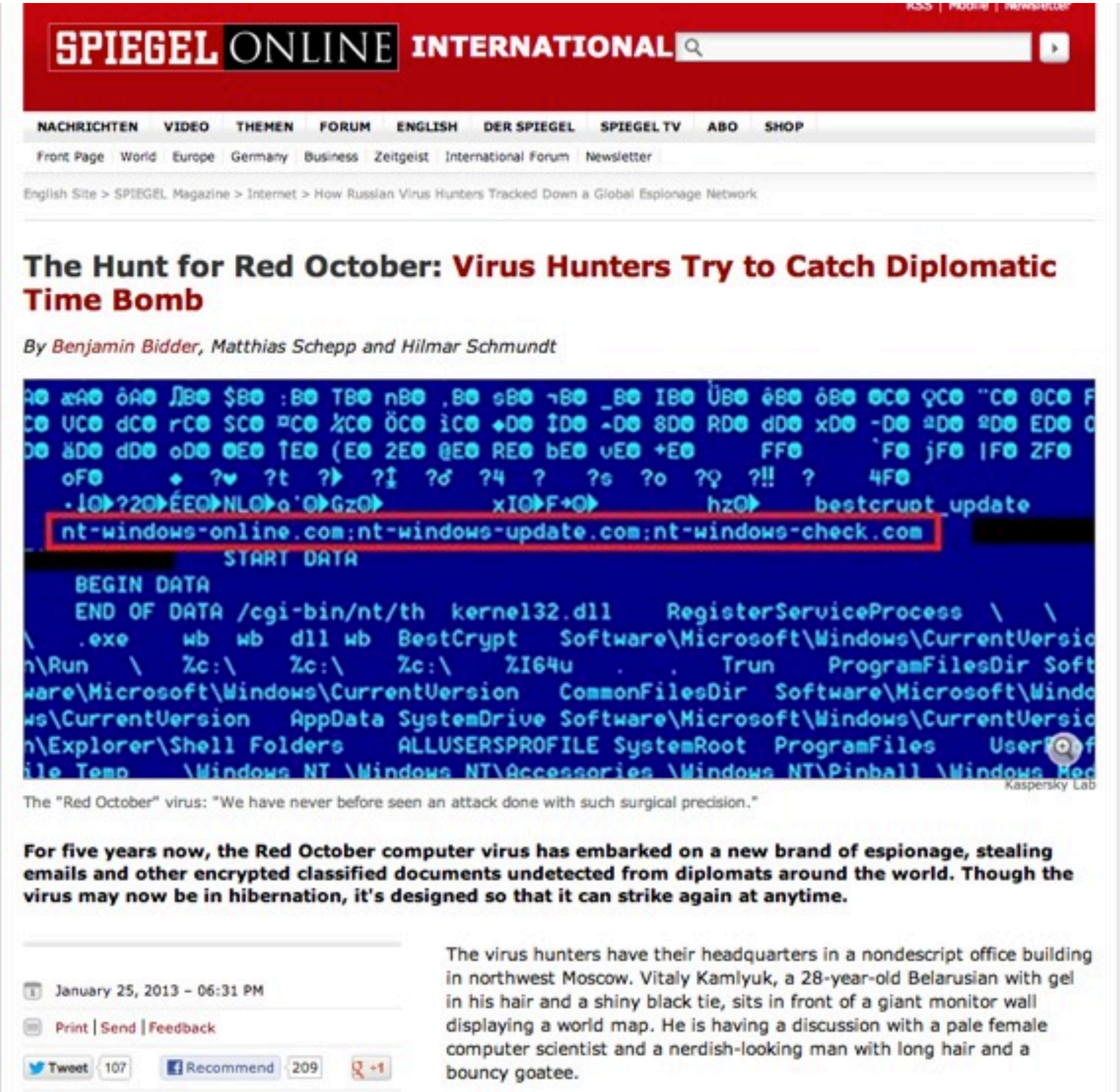
By: Neil J. Rubenking

09.23.2010 1 comment

In a July presentation for members of the computer media, Roel Schouwenberg, a senior anti-virus researcher for Kaspersky Lab, laid out details about the Stuxnet worm. This worm exploits an unusual number of different security weak spots and it seems in particular to attack SCADA (Supervisory Control and Data Acquisition) systems. SCADA systems are used to manage large facilities such as oil rigs, factories, and nuclear reactors. Schouwenberg noted that SCADA computers often run older operating systems without security protection or regular updates.

The presentation included a map of the worm's prevalence. Most of the world's countries displayed a peaceful green, meaning low prevalence, but Iran and Indonesia glowed a bright, warning red. Schouwenberg observed that the worm is so polished and complex it must have required a lot of resources, suggesting it was created by a nation-state.

More recently Ralph Langner, a security researcher and expert in SCADA systems, performed a forensic analysis of the worm in action. He concluded that the worm's purpose is sabotage and suggested that the sabotage may have already taken place at Iran's Bushehr reactor. Given the nature of the attack and the multiple vulnerabilities it exploits, Langner concluded it must have been released by a nation-state.



RSS | Mobile | Newsletter
SPIEGEL ONLINE INTERNATIONAL
NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP
Front Page | World | Europe | Germany | Business | Zeitgeist | International Forum | Newsletter

English Site > SPIEGEL Magazine > Internet > How Russian Virus Hunters Tracked Down a Global Espionage Network

The Hunt for Red October: Virus Hunters Try to Catch Diplomatic Time Bomb

By Benjamin Bidder, Matthias Schepp and Hilmar Schmundt

```
A0 æA0 ôA0 ЉB0 $B0 :B0 TB0 nB0 .B0 sB0 ¬B0 _B0 IB0 ÜB0 êB0 ôB0 0C0 ♀C0 "C0 0C0 F
C0 UC0 dC0 rC0 SC0 ¤C0 ½C0 ÖC0 ìC0 •D0 ↕D0 -D0 8D0 RD0 dD0 xD0 -D0 ªD0 ºD0 ED0 C
D0 ăD0 dD0 oD0 0E0 ↑E0 (E0 2E0 @E0 RE0 bE0 vE0 +E0     FF0     `F0 jF0 |F0 ZF0
  oF0     ◆  ?♥  ?t  ?▶  ?↨  ?♂  ?4  ?   ?s  ?o  ?♀  ?‼  ?    4F0
   ·↓O▶?2O▶ÉEO▶NLO▶a'O▶GzO▶         xIO▶F+O▶         hzO▶    bestcrupt update
  nt-windows-online.com;nt-windows-update.com;nt-windows-check.com     [redacted]
[redacted]        START DATA
   BEGIN DATA
   END OF DATA /cgi-bin/nt/th  kernel32.dll    RegisterServiceProcess  \   \
\   .exe    wb  wb  dll wb  BestCrypt   Software\Microsoft\Windows\CurrentVersio
n\Run   \   %c:\    %c:\    %c:\    %I64u   .   .   Trun    ProgramFilesDir Soft
ware\Microsoft\Windows\CurrentVersion   CommonFilesDir  Software\Microsoft\Windo
ws\CurrentVersion   AppData SystemDrive Software\Microsoft\Windows\CurrentVersio
n\Explorer\Shell Folders    ALLUSERSPROFILE SystemRoot  ProgramFiles    UserProf
ile Temp    \Windows NT \Windows NT\Accessories \Windows NT\Pinball \Windows Med
```

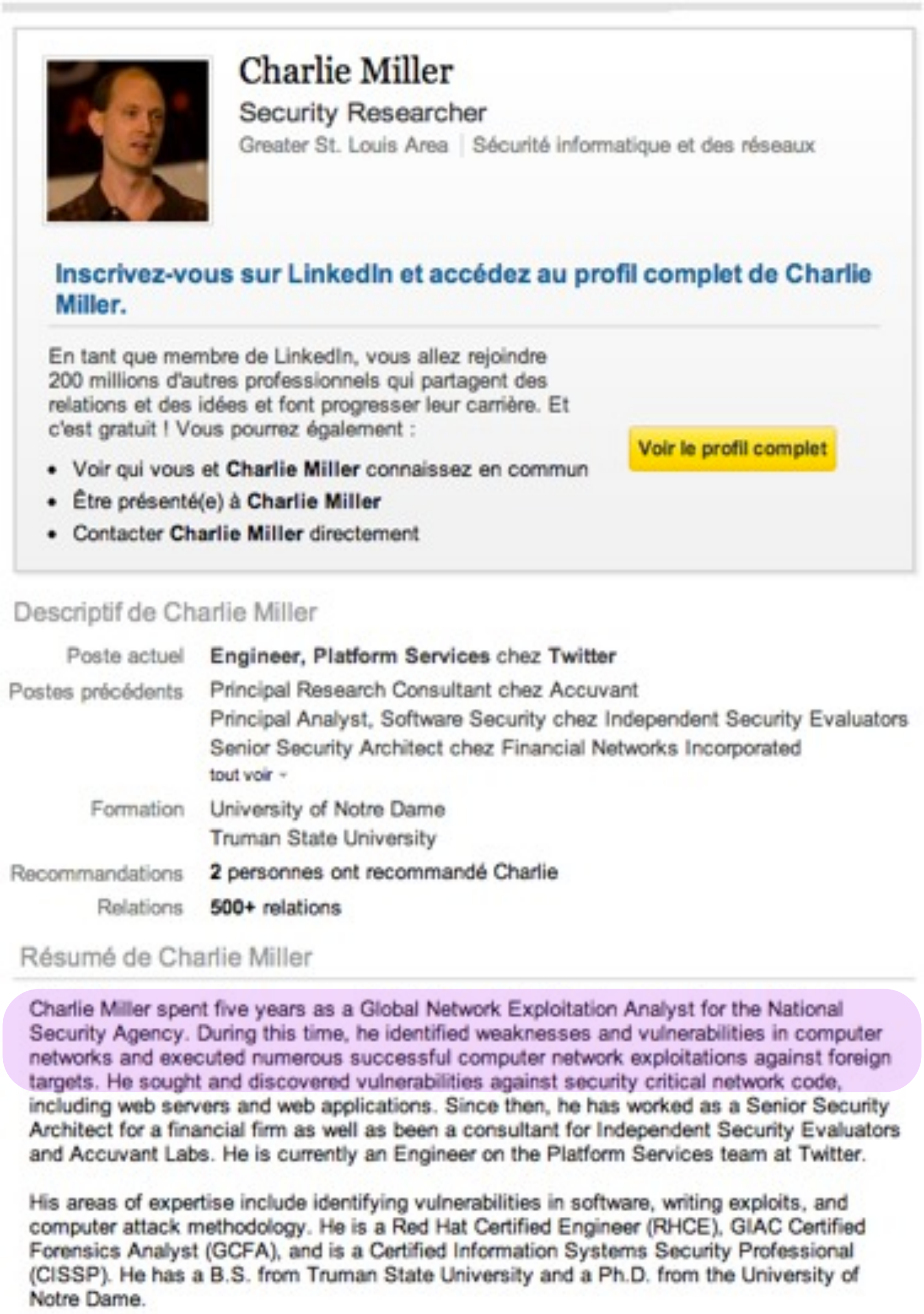
Kaspersky Lab

The "Red October" virus: "We have never before seen an attack done with such surgical precision."

For five years now, the Red October computer virus has embarked on a new brand of espionage, stealing emails and other encrypted classified documents undetected from diplomats around the world. Though the virus may now be in hibernation, it's designed so that it can strike again at anytime.

January 25, 2013 – 06:31 PM

The virus hunters have their headquarters in a nondescript office building in northwest Moscow. Vitaly Kamlyuk, a 28-year-old Belarusian with gel in his hair and a shiny black tie, sits in front of a giant monitor wall displaying a world map. He is having a discussion with a pale female computer scientist and a nerdish-looking man with long hair and a bouncy goatee.



Charlie Miller

Security Researcher

Greater St. Louis Area | Sécurité informatique et des réseaux

Inscrivez-vous sur LinkedIn et accédez au profil complet de Charlie Miller.

En tant que membre de LinkedIn, vous allez rejoindre 200 millions d'autres professionnels qui partagent des relations et des idées et font progresser leur carrière. Et c'est gratuit ! Vous pourrez également :

- Voir qui vous et **Charlie Miller** connaissez en commun
- Être présenté(e) à **Charlie Miller**
- Contacter **Charlie Miller** directement

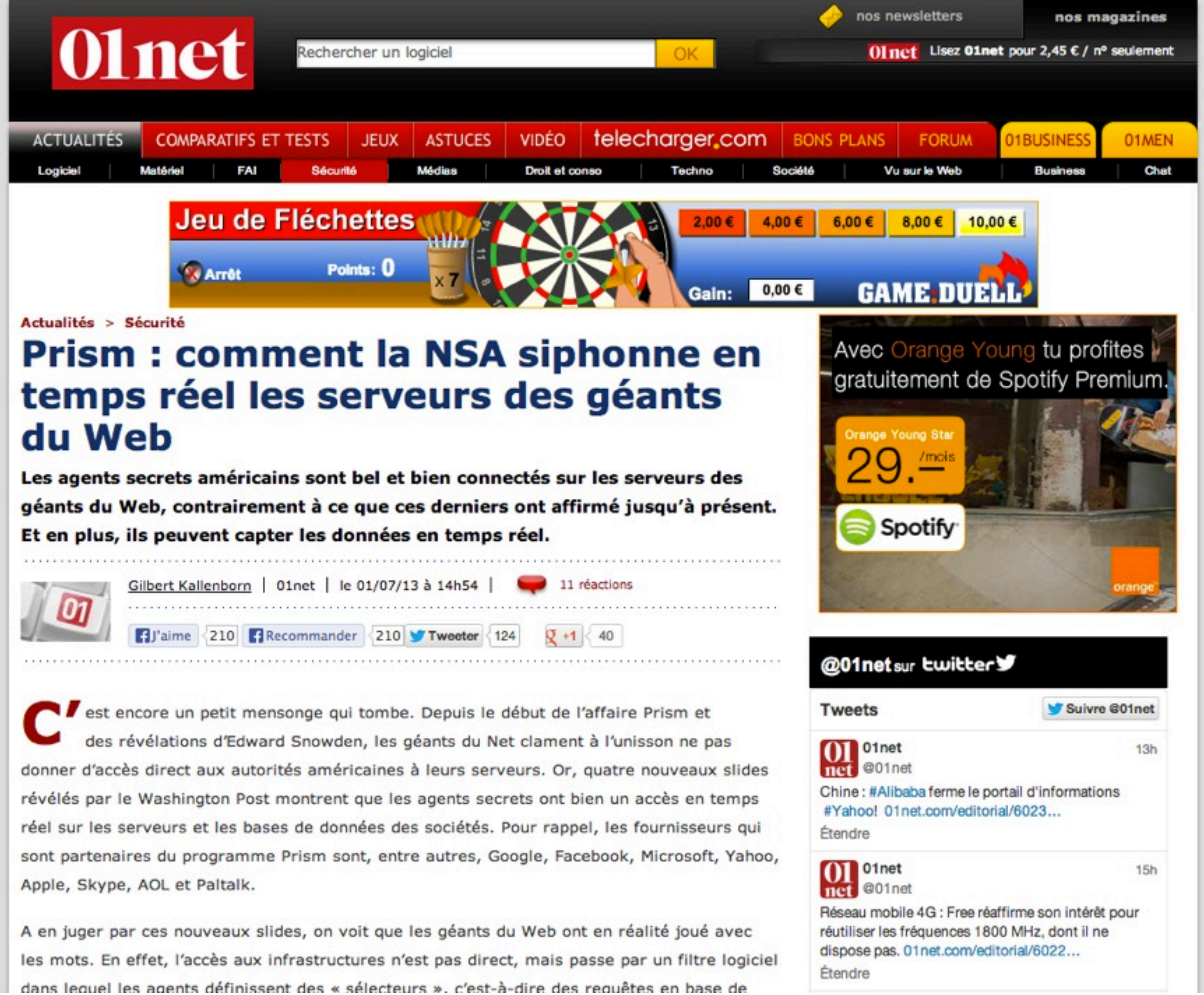
Descriptif de Charlie Miller

Poste actuel	**Engineer, Platform Services** chez **Twitter**
Postes précédents	Principal Research Consultant chez Accuvant Principal Analyst, Software Security chez Independent Security Evaluators Senior Security Architect chez Financial Networks Incorporated tout voir
Formation	University of Notre Dame Truman State University
Recommandations	**2** personnes ont recommandé Charlie
Relations	**500+** relations

Résumé de Charlie Miller

Charlie Miller spent five years as a Global Network Exploitation Analyst for the National Security Agency. During this time, he identified weaknesses and vulnerabilities in computer networks and executed numerous successful computer network exploitations against foreign targets. He sought and discovered vulnerabilities against security critical network code, including web servers and web applications. Since then, he has worked as a Senior Security Architect for a financial firm as well as been a consultant for Independent Security Evaluators and Accuvant Labs. He is currently an Engineer on the Platform Services team at Twitter.

His areas of expertise include identifying vulnerabilities in software, writing exploits, and computer attack methodology. He is a Red Hat Certified Engineer (RHCE), GIAC Certified Forensics Analyst (GCFA), and is a Certified Information Systems Security Professional (CISSP). He has a B.S. from Truman State University and a Ph.D. from the University of Notre Dame.



Prism : comment la NSA siphonne en temps réel les serveurs des géants du Web

Les agents secrets américains sont bel et bien connectés sur les serveurs des géants du Web, contrairement à ce que ces derniers ont affirmé jusqu'à présent. Et en plus, ils peuvent capter les données en temps réel.

Gilbert Kallenborn | 01net | le 01/07/13 à 14h54 | 11 réactions

J'aime 210 Recommander 210 Tweeter 124 +1 40

C'est encore un petit mensonge qui tombe. Depuis le début de l'affaire Prism et des révélations d'Edward Snowden, les géants du Net clament à l'unisson ne pas donner d'accès direct aux autorités américaines à leurs serveurs. Or, quatre nouveaux slides révélés par le Washington Post montrent que les agents secrets ont bien un accès en temps réel sur les serveurs et les bases de données des sociétés. Pour rappel, les fournisseurs qui sont partenaires du programme Prism sont, entre autres, Google, Facebook, Microsoft, Yahoo, Apple, Skype, AOL et Paltalk.

A en juger par ces nouveaux slides, on voit que les géants du Web ont en réalité joué avec les mots. En effet, l'accès aux infrastructures n'est pas direct, mais passe par un filtre logiciel dans lequel les agents définissent des « sélecteurs », c'est-à-dire des requêtes en base de

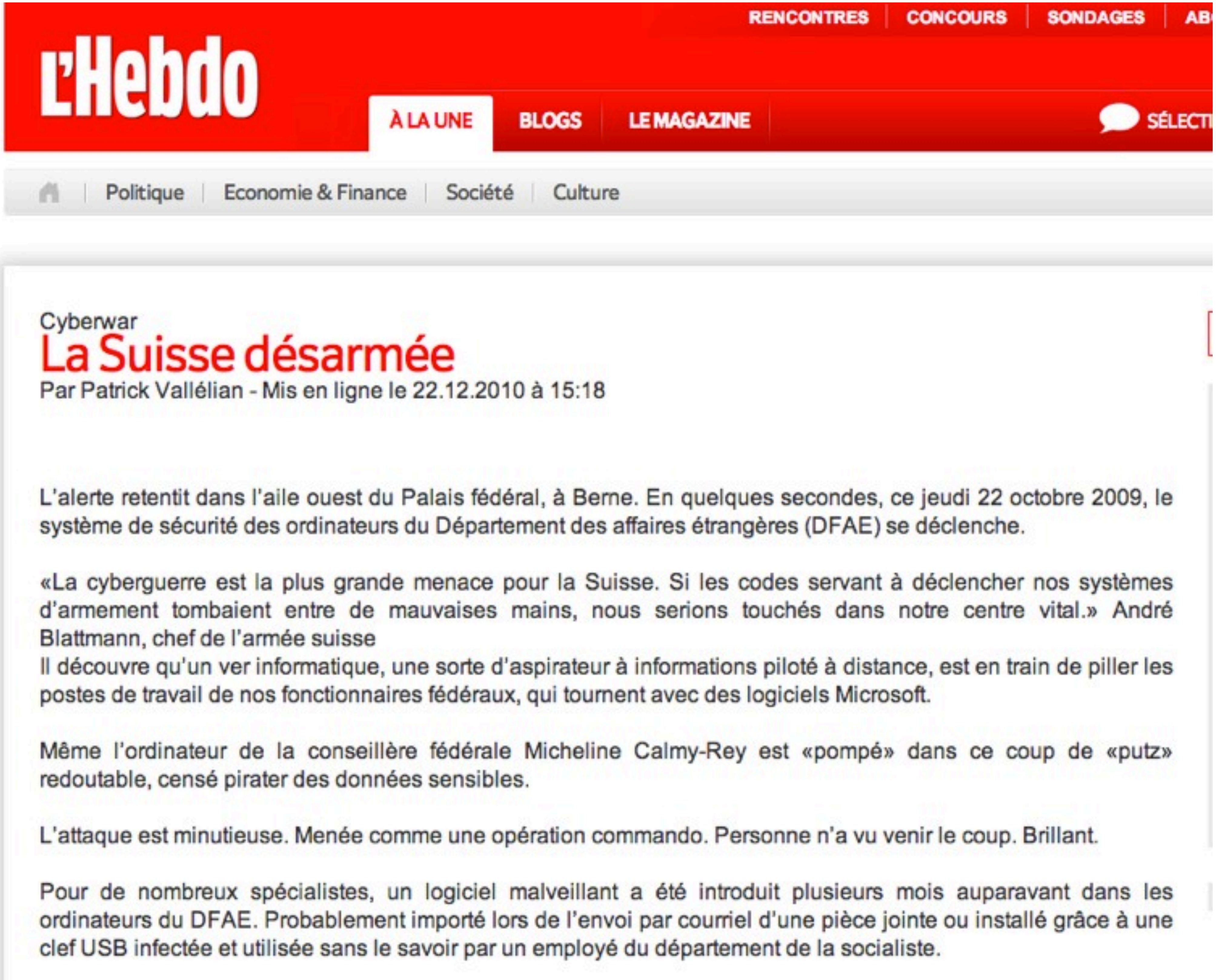
@01net sur twitter

Tweets Suivre @01net

01net @01net 13h
Chine : #Alibaba ferme le portail d'informations #Yahoo! 01net.com/editorial/6023...
Étendre

01net @01net 15h
Réseau mobile 4G : Free réaffirme son intérêt pour réutiliser les fréquences 1800 MHz, dont il ne dispose pas. 01net.com/editorial/6022...
Étendre

Et en Suisse?



Cyberwar

La Suisse désarmée

Par Patrick Vallélian - Mis en ligne le 22.12.2010 à 15:18

L'alerte retentit dans l'aile ouest du Palais fédéral, à Berne. En quelques secondes, ce jeudi 22 octobre 2009, le système de sécurité des ordinateurs du Département des affaires étrangères (DFAE) se déclenche.

«La cyberguerre est la plus grande menace pour la Suisse. Si les codes servant à déclencher nos systèmes d'armement tombaient entre de mauvaises mains, nous serions touchés dans notre centre vital.» André Blattmann, chef de l'armée suisse
Il découvre qu'un ver informatique, une sorte d'aspirateur à informations piloté à distance, est en train de piller les postes de travail de nos fonctionnaires fédéraux, qui tournent avec des logiciels Microsoft.

Même l'ordinateur de la conseillère fédérale Micheline Calmy-Rey est «pompé» dans ce coup de «putz» redoutable, censé pirater des données sensibles.

L'attaque est minutieuse. Menée comme une opération commando. Personne n'a vu venir le coup. Brillant.

Pour de nombreux spécialistes, un logiciel malveillant a été introduit plusieurs mois auparavant dans les ordinateurs du DFAE. Probablement importé lors de l'envoi par courriel d'une pièce jointe ou installé grâce à une clef USB infectée et utilisée sans le savoir par un employé du département de la socialiste.

Acteurs

- EPFL - ETHZ
- Haute écoles spécialisées
- Etat
- Industrie

Et en tant que citoyen lambda?

Hygiène de base

- Mots de passe uniques et solides
- Mises à jours
- Anti-virus / pare-feu
- Backups
- Quelle information va où?

Discussion / Questions