Let the Crowd Fight Crime:
enabling users to stay safe in cyberspace

Dr. Dominik Herrmann

University of Hamburg

Berlin, August 28, 2015

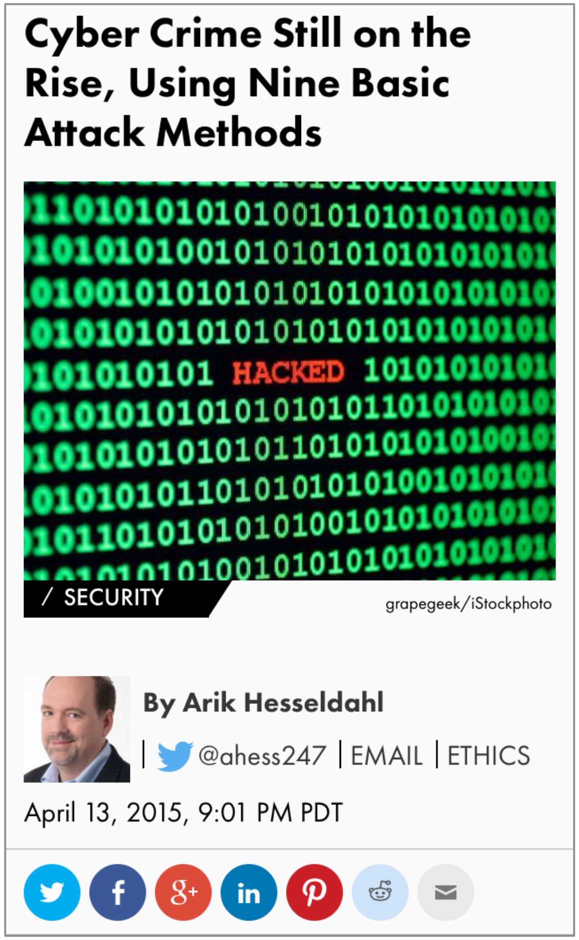
International Summer Academy 2015 organized by Studentenforum im Tönissteiner Kreis e.V.

Postdoctoral researcher @ University of Hamburg (DE)
working on security, privacy, online tracking, forensics

Junior Fellow of German Informatics Society (GI)

Cyber crime is on the rise!

Or merely a hype spurred by fear mongering?



Cyber Crime Still on the Rise, Using Nine Basic Attack Methods

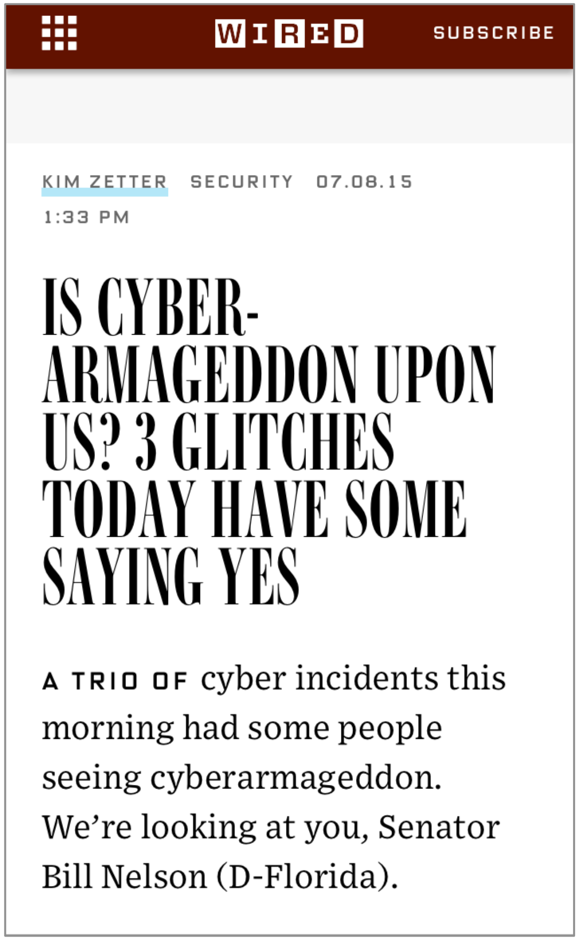
/ SECURITY

grapegeek/iStockphoto

By Arik Hesseldahl

| @ahess247 | EMAIL | ETHICS

April 13, 2015, 9:01 PM PDT

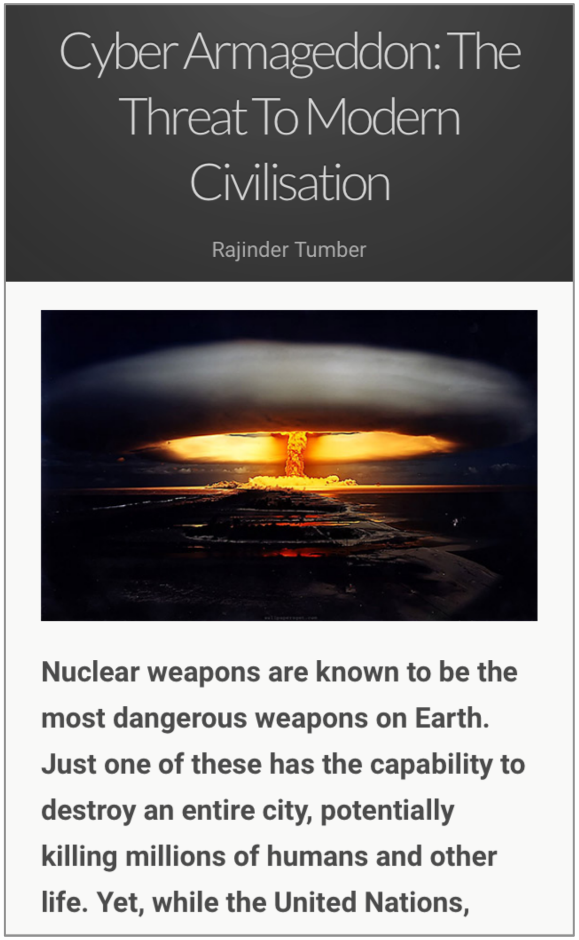


WIRED SUBSCRIBE

KIM ZETTER SECURITY 07.08.15 1:33 PM

IS CYBER-ARMAGEDDON UPON US? 3 GLITCHES TODAY HAVE SOME SAYING YES

A TRIO OF cyber incidents this morning had some people seeing cyberarmageddon. We're looking at you, Senator Bill Nelson (D-Florida).



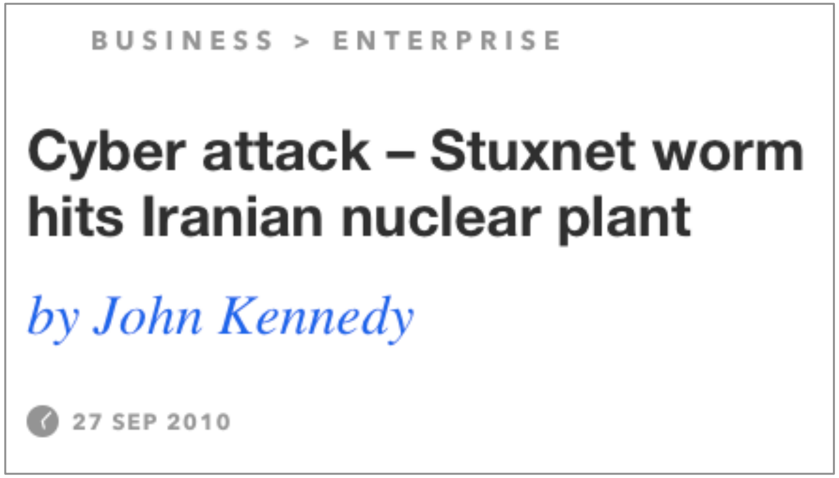
Cyber Armageddon: The Threat To Modern Civilisation

Rajinder Tumber

Nuclear weapons are known to be the most dangerous weapons on Earth. Just one of these has the capability to destroy an entire city, potentially killing millions of humans and other life. Yet, while the United Nations,

Future critical infrastructures and cyber-physical systems at risk.

… as well as most organizations with an online presence.

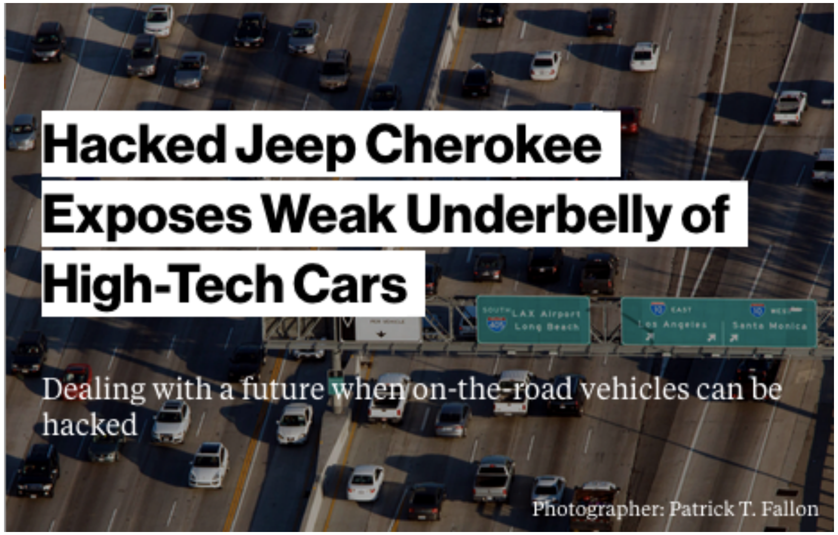


BUSINESS > ENTERPRISE

Cyber attack – Stuxnet worm hits Iranian nuclear plant

by John Kennedy

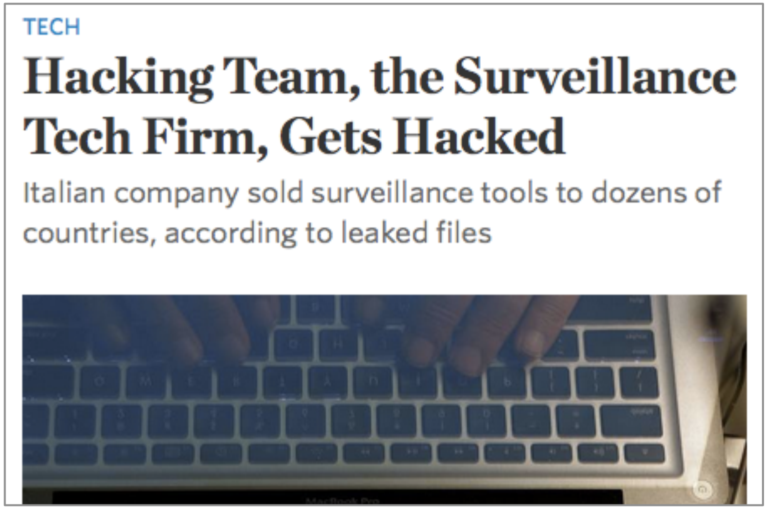
27 SEP 2010



Hacked Jeep Cherokee Exposes Weak Underbelly of High-Tech Cars

Dealing with a future when on-the-road vehicles can be hacked

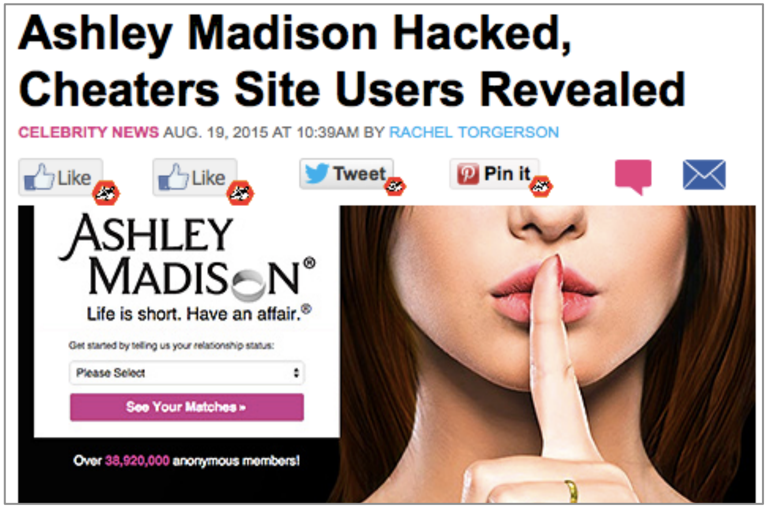
Photographer: Patrick T. Fallon



TECH

Hacking Team, the Surveillance Tech Firm, Gets Hacked

Italian company sold surveillance tools to dozens of countries, according to leaked files



Ashley Madison Hacked, Cheaters Site Users Revealed

CELEBRITY NEWS AUG. 19, 2015 AT 10:39AM BY RACHEL TORGERSON

Like
Like
Tweet
Pin it
ASHLEY MADISON®
Life is short. Have an affair.®
Get started by telling us your relationship status:
Please Select
See Your Matches »
Over 38,920,000 anonymous members!

This workshop focuses on cyber crime targeting citizens and end users.

How are we as citizens affected by cyber crime?

How can academia, industry and policy makers empower citizens to better proctect themselves?

→ We have to educate them!

Other cybercrime topics

- e-commerce fraud
- state-level surveillance
- cyber warfare
- industrial espionage
- media and software piracy
- drug trafficking

For common Internet Crime Schemes see http://www.ic3.gov/crimeschemes.aspx

Many citizens have already become victims of cyber crime.

Have you?

What are common types of cyber crime?

How to fight cybercrime?

Current situation

Today's security measures
do not prevent cybercrime

we fail to track down
criminals on the Internet

Response of policy makers?

> The Australian Security Intelligence Organization (ASIO) is pushing for laws that would make telecommunications companies **retain their customers' web-browsing data …** as well as forcing web users to decrypt encrypted messages.

http://rt.com/news/australia-nsa-snowden-surveillance-510 – http://arstechnica.com/tech-policy/2014/03/after-snowden-australias-cops-worry-about-people-using-crypto

How to fight cybercrime?

Current situation

Today’s security measures
do not prevent cybercrime

we fail to track down
criminals on the Internet

Response of policy makers – is dangerous and futile anyway.

multi-stage attacks
using stepping stones

Tor

http://rt.com/news/australia-nsa-snowden-surveillance-510 – http://arstechnica.com/tech-policy/2014/03/after-snowden-australias-cops-worry-about-people-using-crypto

How to fight cybercrime?

Current situation

Today's security measures
do not prevent cybercrime

we fail to track down
criminals on the Internet

Proposition

We should not rely on
law enforcement to protect us
from professional cyber criminals

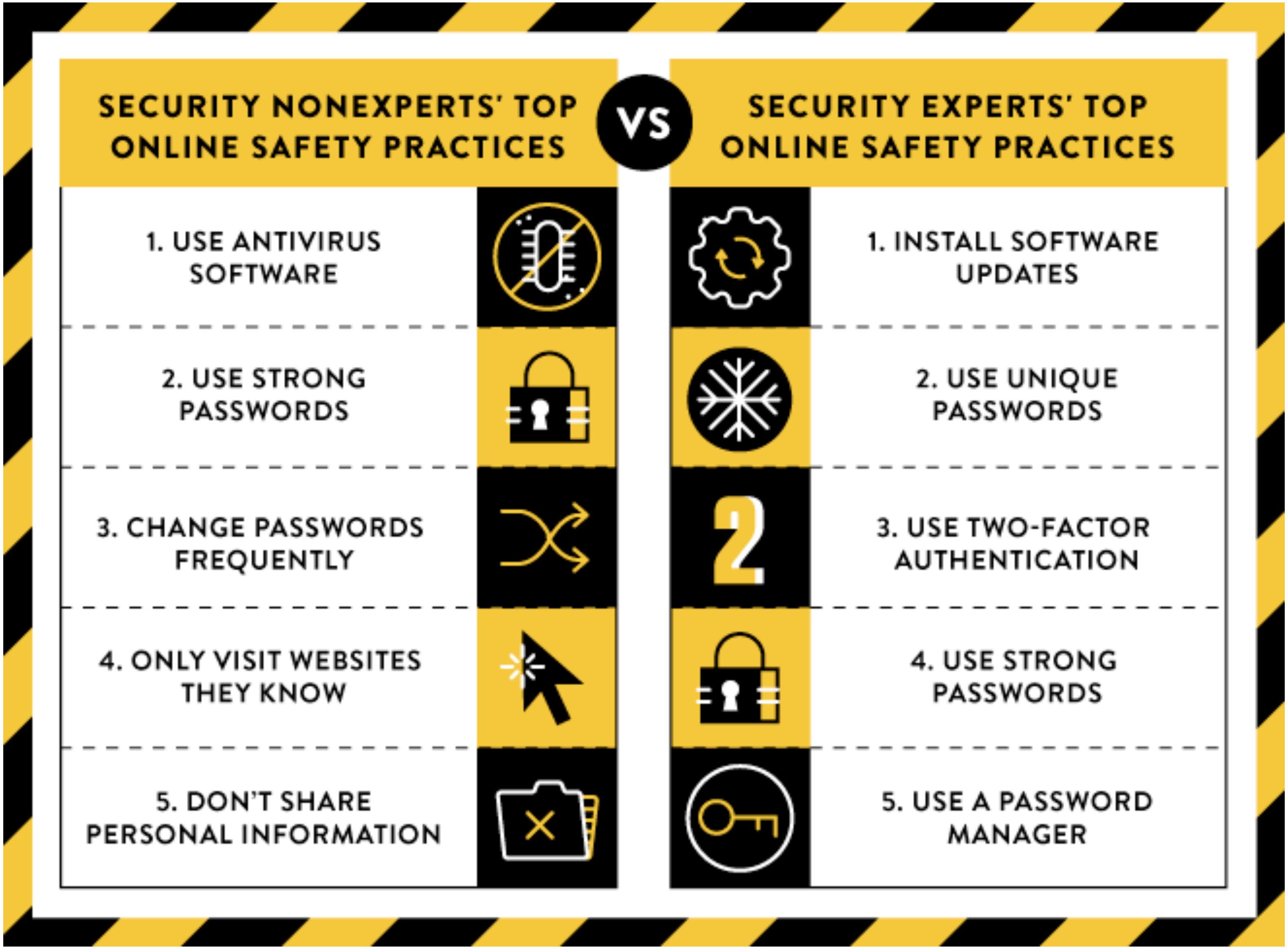
We should try to prevent
crimes from happening
in the very first place

Consequence

We will have to become
more professional ourselves

invest in awareness & better
usability of security solutions

How do professionals stay safe online?



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

http://googleonlinesecurity.blogspot.de/2015/07/new-research-comparing-how-security.html

THREAT 1: Malware

Experts have preached countermeasures for years.

- **updates** your software
- do not click on **suspicious links**
- do not visit **unknown websites**
- **antivirus** and **firewalls**

Why are they not effective?

countermeasures ineffective

ignorant users

lazy users

Components of malware

Distribution USB sticks, email, web browser, malicious apps

Infection

- (0-day) exploits
- insecure configuration
- ignorance and laziness of users

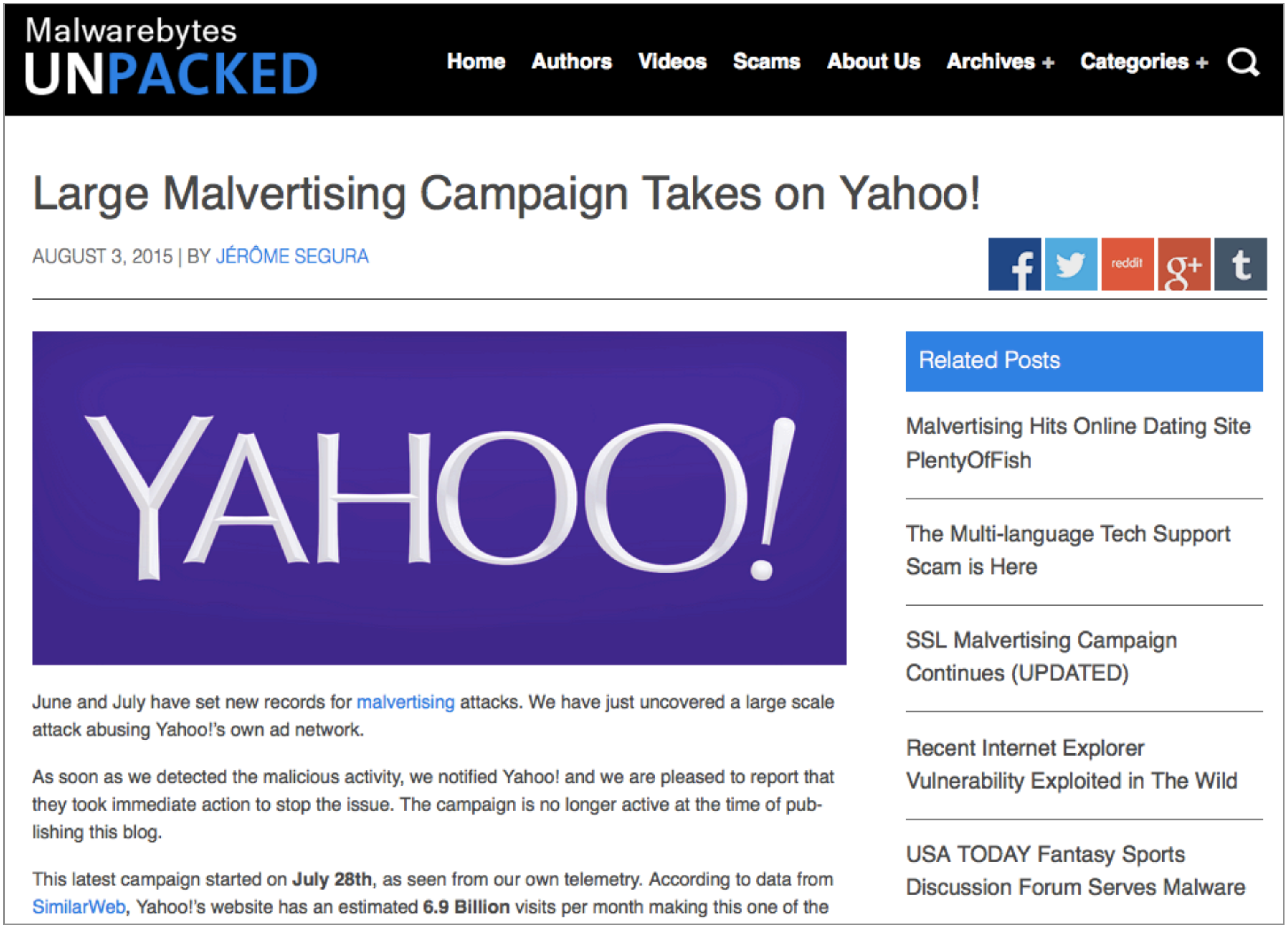
Payload

- send spam or participate in denial-of-service attack
- key logger stealing passwords and credit card numbers
- display advertisements

Best Practice 1: Visit only trustworthy sites.

… to avoid “drive-by downloads”.

Best Practice 1: Visit only trustworthy sites – but that does not protect you.



Large Malvertising Campaign Takes on Yahoo!

AUGUST 3, 2015 | BY JÉRÔME SEGURA

June and July have set new records for malvertising attacks. We have just uncovered a large scale attack abusing Yahoo!'s own ad network.

As soon as we detected the malicious activity, we notified Yahoo! and we are pleased to report that they took immediate action to stop the issue. The campaign is no longer active at the time of publishing this blog.

This latest campaign started on **July 28th**, as seen from our own telemetry. According to data from SimilarWeb, Yahoo!'s website has an estimated **6.9 Billion** visits per month making this one of the

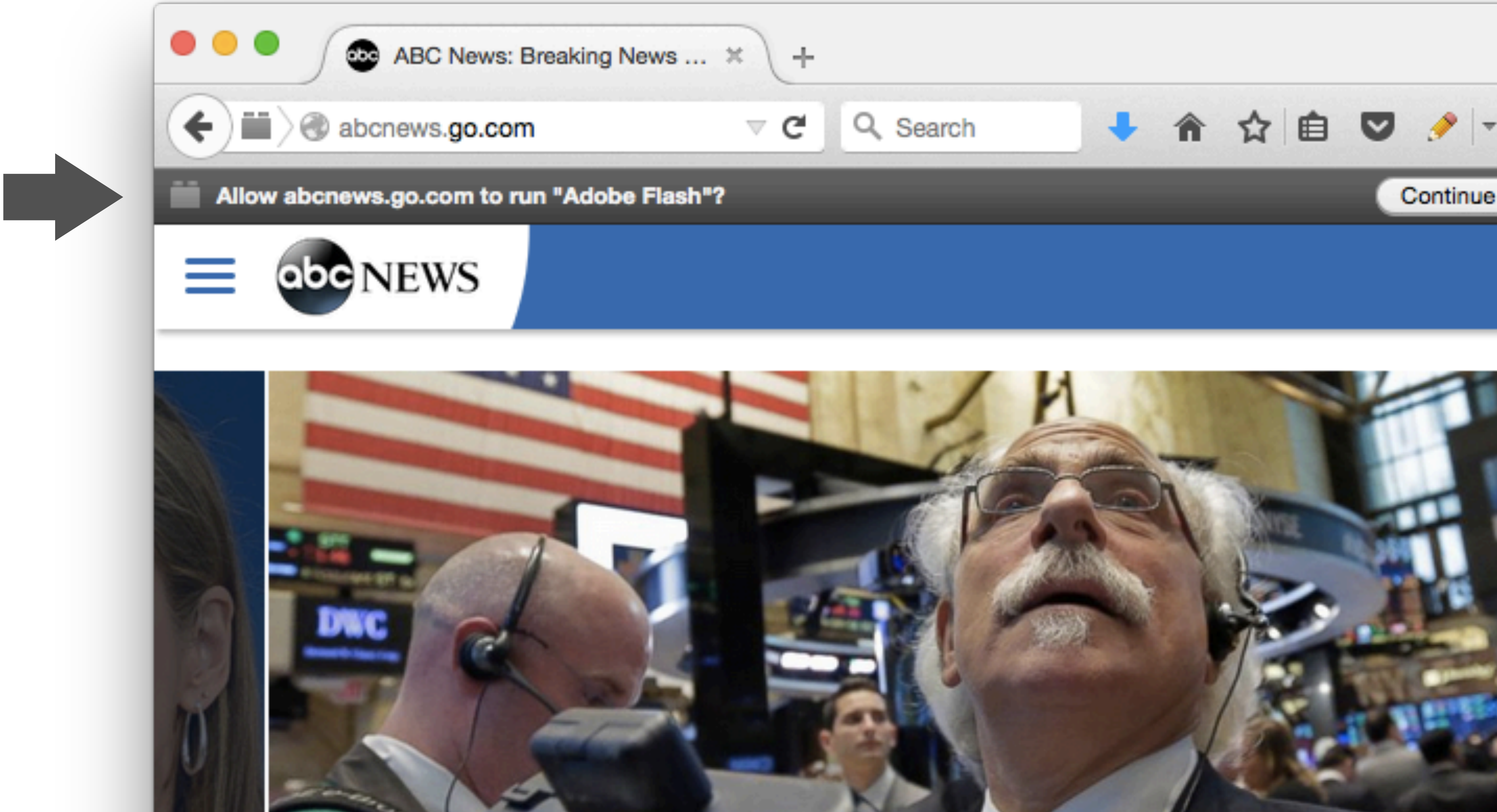
Related Posts

- Malvertising Hits Online Dating Site PlentyOfFish
- The Multi-language Tech Support Scam is Here
- SSL Malvertising Campaign Continues (UPDATED)
- Recent Internet Explorer Vulnerability Exploited in The Wild
- USA TODAY Fantasy Sports Discussion Forum Serves Malware

https://blog.malwarebytes.org/malvertising-2/2015/08/large-malvertising-campaign-takes-on-yahoo/

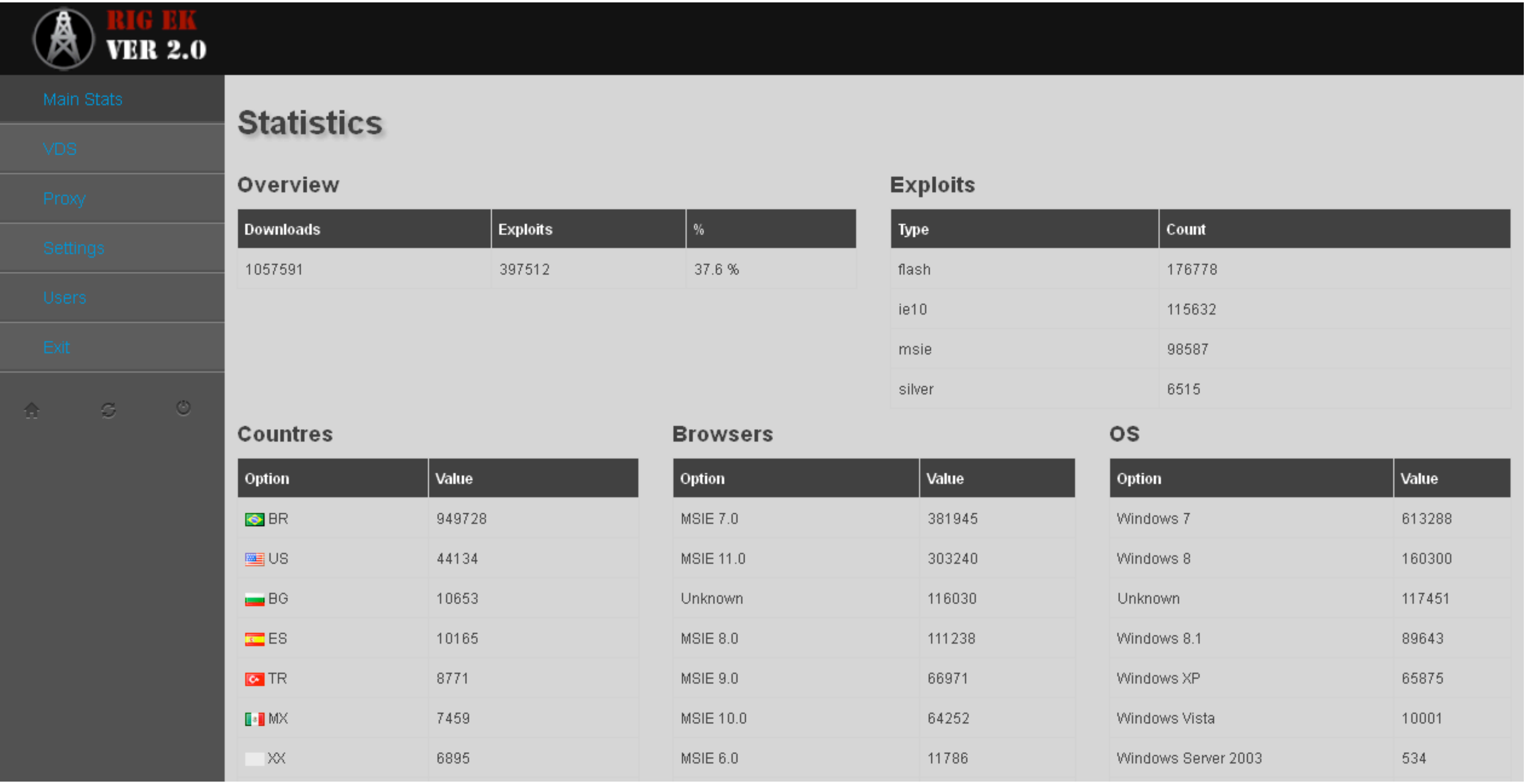
Best Practice 2: Disabling automatic execution of Flash & Java – is effectice.

(but you should also disable JavaScript)
(and create a dedicated user account for surfing)



ABC News: Breaking News ...
abcnews.go.com
Search
Allow abcnews.go.com to run "Adobe Flash"?
Continue
abc NEWS

Recent trend: with “exploit kits” malware is offered as a service.



Statistics

Overview

Downloads	Exploits	%
1057591	397512	37.6 %

Exploits

Type	Count
flash	176778
ie10	115632
msie	98587
silver	6515

Countres

Option	Value
BR	949728
US	44134
BG	10653
ES	10165
TR	8771
MX	7459
XX	6895

Browsers

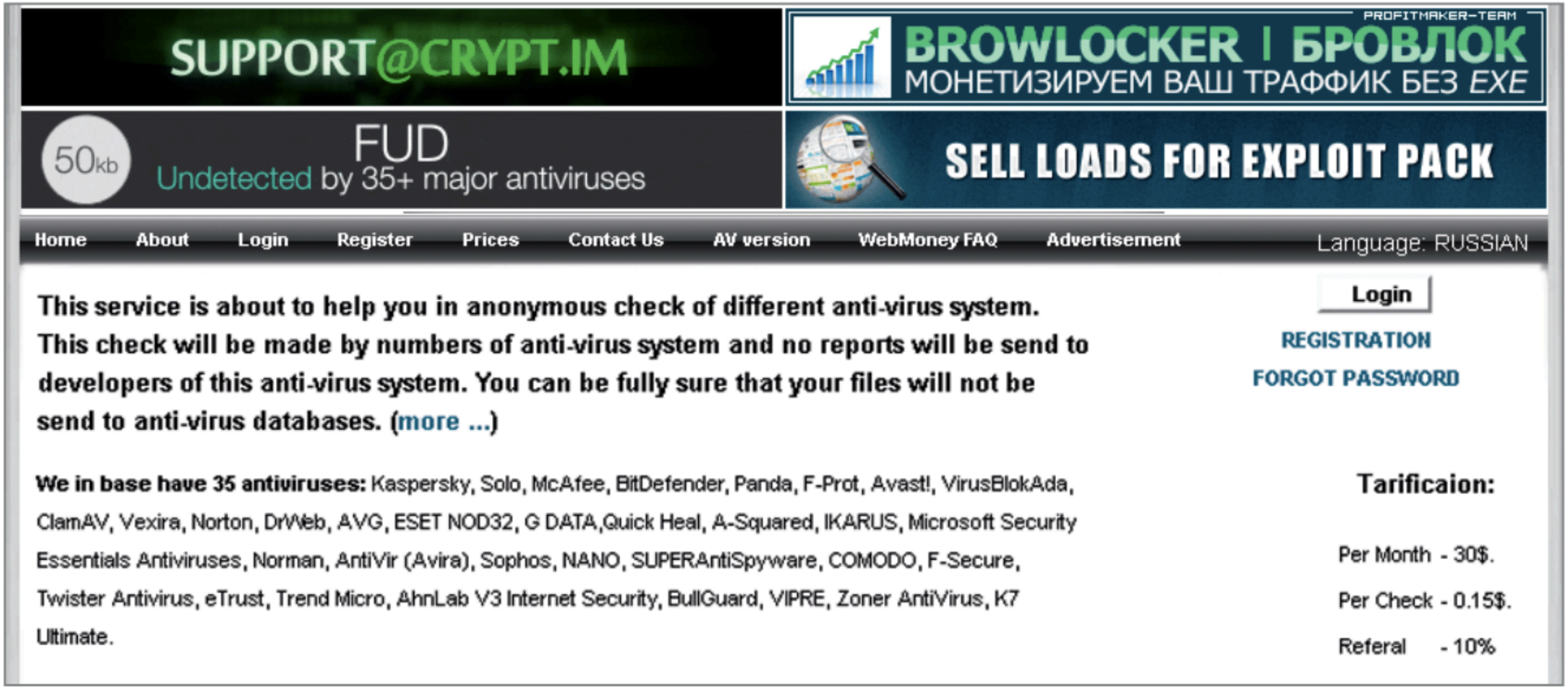
Option	Value
MSIE 7.0	381945
MSIE 11.0	303240
Unknown	116030
MSIE 8.0	111238
MSIE 9.0	66971
MSIE 10.0	64252
MSIE 6.0	11786

OS

Option	Value
Windows 7	613288
Windows 8	160300
Unknown	117451
Windows 8.1	89643
Windows XP	65875
Windows Vista	10001
Windows Server 2003	534

https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Exploit-Kit-Source-Code-Leak---The-End-or-Just-the-Beginning-of-RIG-/
c’t 2015(18) p. 80

Recent trend: with “exploit kits” malware is offered as a service.



This service is about to help you in anonymous check of different anti-virus system. This check will be made by numbers of anti-virus system and no reports will be send to developers of this anti-virus system. You can be fully sure that your files will not be send to anti-virus databases. (more ...)

We in base have 35 antiviruses: Kaspersky, Solo, McAfee, BitDefender, Panda, F-Prot, Avast!, VirusBlokAda, ClamAV, Vexira, Norton, DrWeb, AVG, ESET NOD32, G DATA,Quick Heal, A-Squared, IKARUS, Microsoft Security Essentials Antiviruses, Norman, AntiVir (Avira), Sophos, NANO, SUPERAntiSpyware, COMODO, F-Secure, Twister Antivirus, eTrust, Trend Micro, AhnLab V3 Internet Security, BullGuard, VIPRE, Zoner AntiVirus, K7 Ultimate.

Tarificaion:

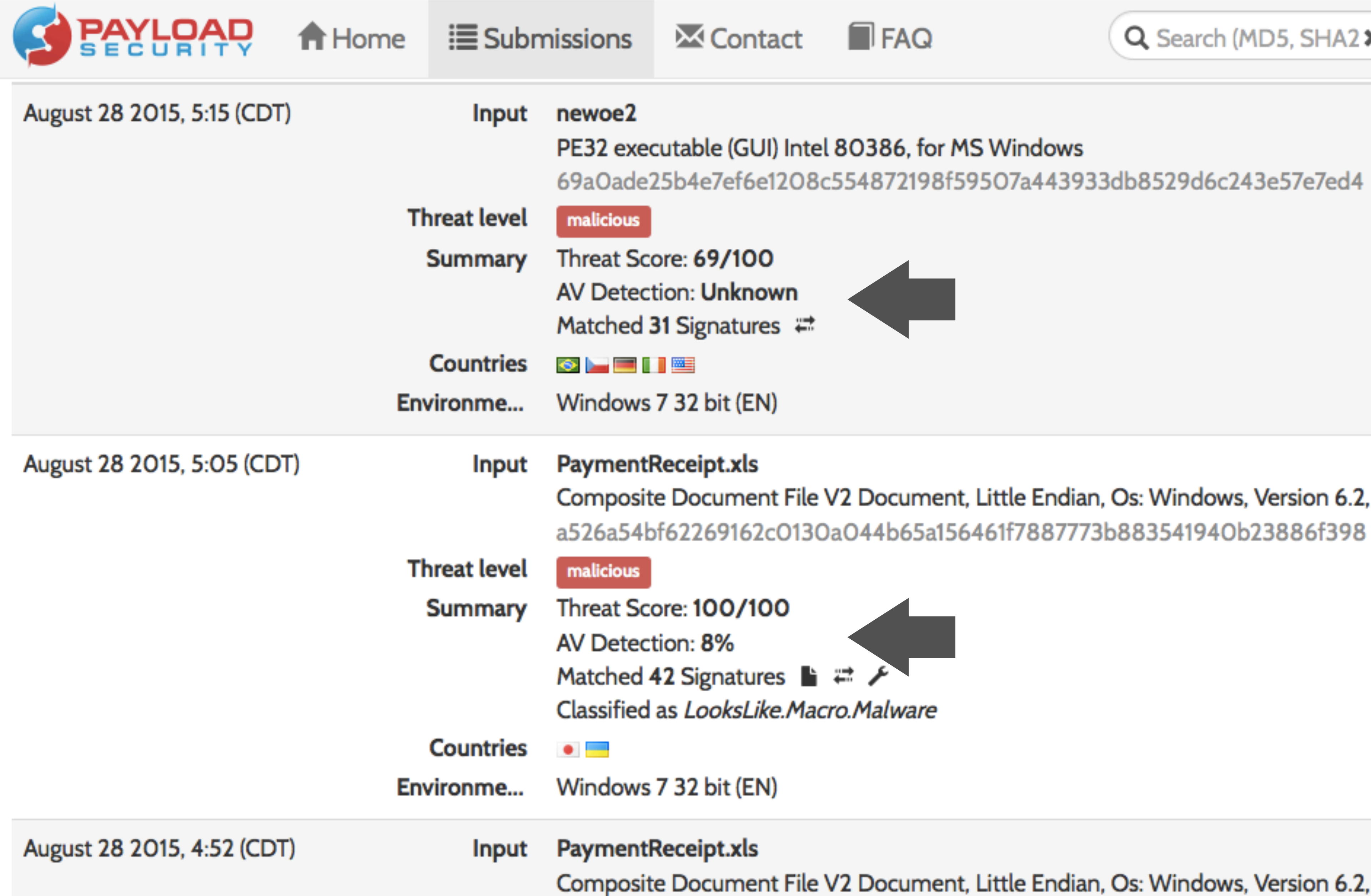
Per Month - 30$.

Per Check - 0.15$.

Referal - 10%

https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Exploit-Kit-Source-Code-Leak---The-End-or-Just-the-Beginning-of-RIG-/
c‘t 2015(18) p. 80

The utility of antivirus software becomes questionable.



August 28 2015, 5:15 (CDT)

Input: **newoe2**
PE32 executable (GUI) Intel 80386, for MS Windows
69a0ade25b4e7ef6e1208c554872198f59507a443933db8529d6c243e57e7ed4

Threat level: malicious

Summary: Threat Score: **69/100**
AV Detection: **Unknown**
Matched **31** Signatures

Countries: 🇧🇷 🇨🇿 🇩🇪 🇮🇹 🇺🇸

Environme...: Windows 7 32 bit (EN)

August 28 2015, 5:05 (CDT)

Input: **PaymentReceipt.xls**
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2,
a526a54bf62269162c0130a044b65a156461f7887773b883541940b23886f398

Threat level: malicious

Summary: Threat Score: **100/100**
AV Detection: **8%**
Matched **42** Signatures
Classified as *LooksLike.Macro.Malware*

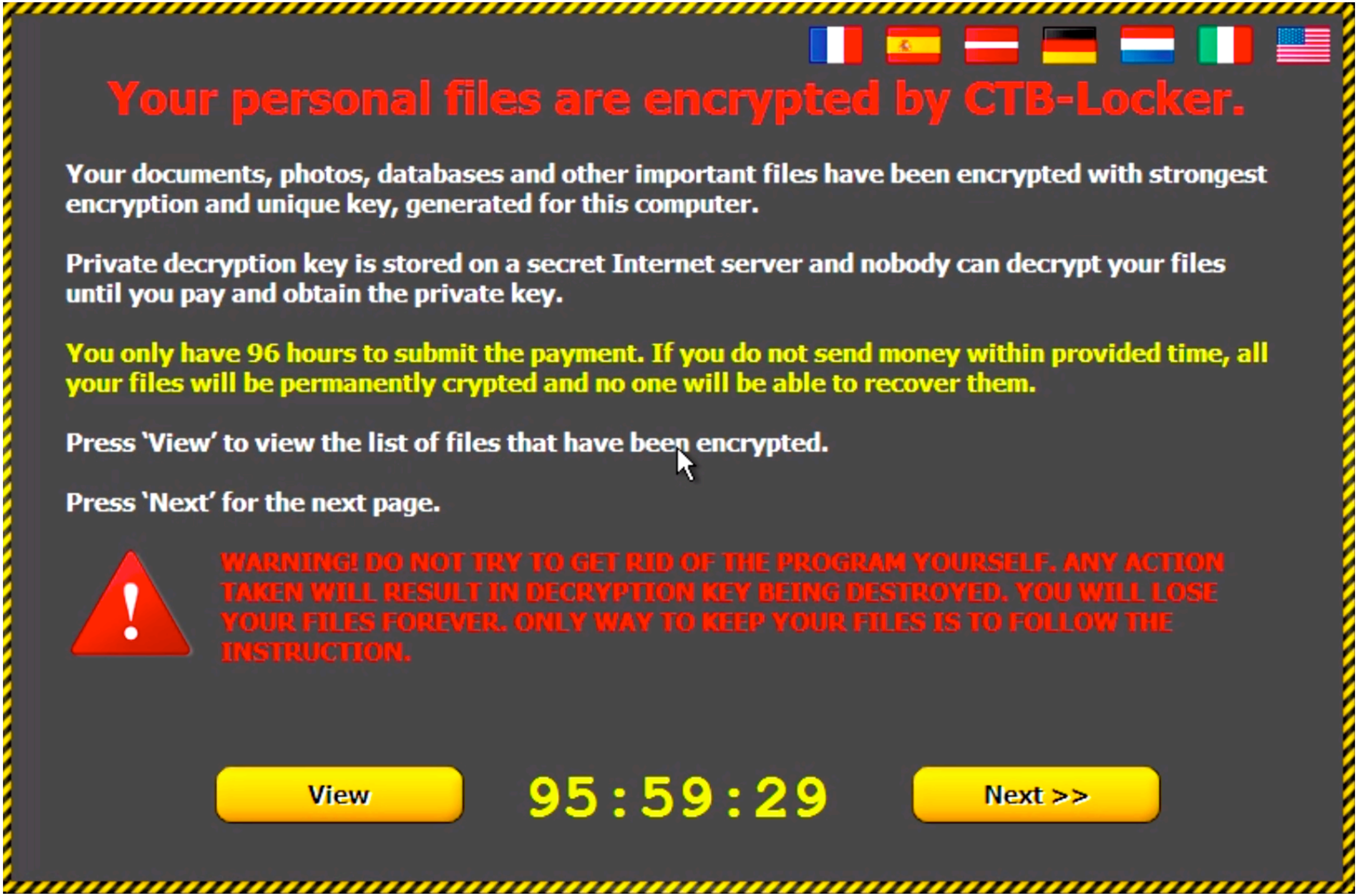
Countries: 🇯🇵 🇺🇦

Environme...: Windows 7 32 bit (EN)

August 28 2015, 4:52 (CDT)

Input: **PaymentReceipt.xls**
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2,

Recent trend: Ransomware



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

https://blogs.cisco.com/wp-content/uploads/CTB-Locker.png

Why is the Ransomware scheme so effective?

… because many users fail to back up their data.
[we discussed various online and offline solutions during the workshop]

Dropbox

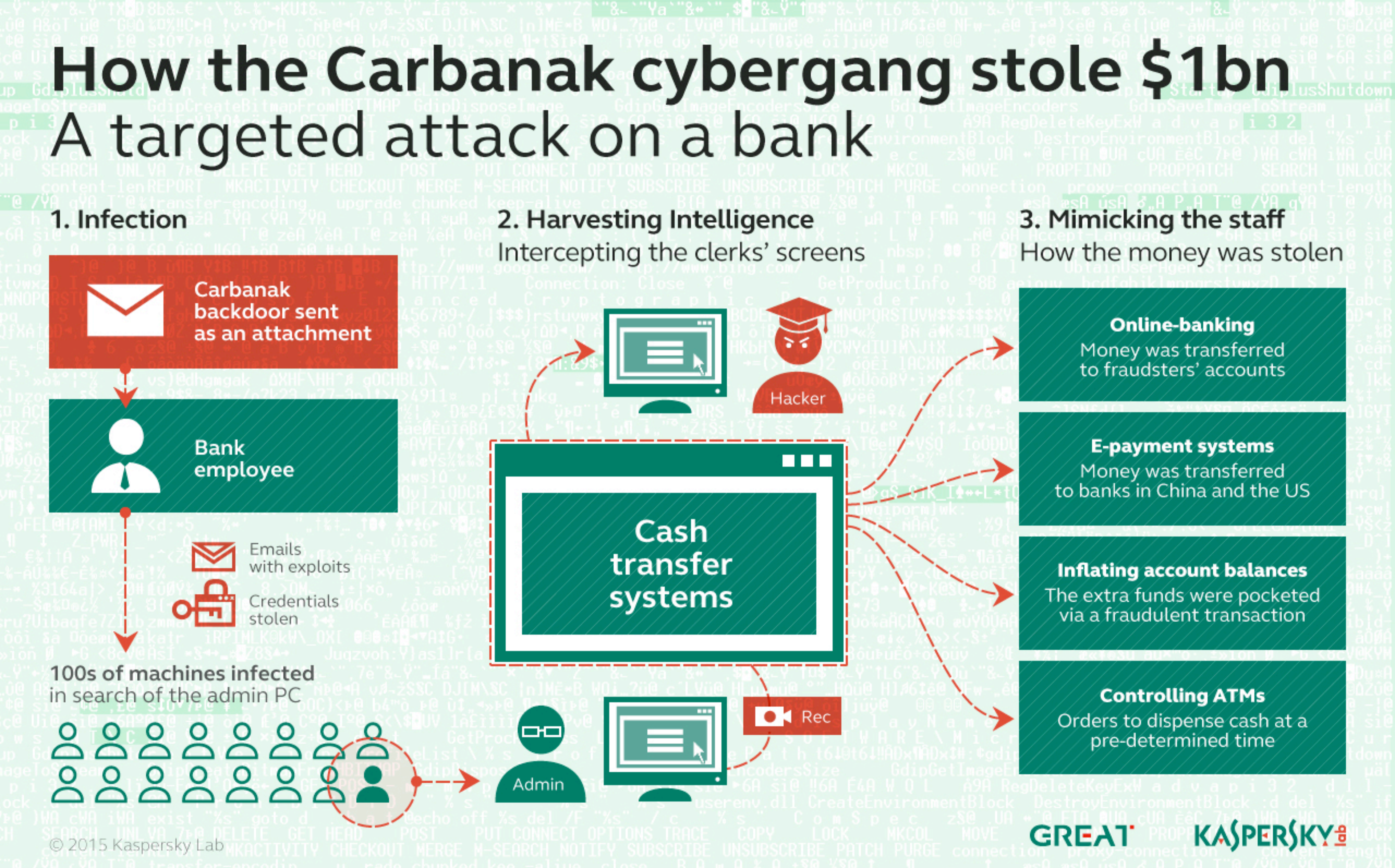
+

boxcryptor

https://upload.wikimedia.org/wikipedia/commons/4/42/Portable_Hard_Disk_1TB_Western_Digital.jpg

Spear Phishing: targeting invididual users to infiltrate organizations.

Protecting against targeted attacks is difficult – even for professionals.



How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected
in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

Cash transfer systems

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

Protecting against targeted attacks is difficult – even for professionals.

How the Carbanak cybergang stole $1bn
A targeted attack on a bank
1. Infection
2. Harvesting Intelligence
Intercepting the clerks' screens
3. Mimicking the staff
How the money was stolen
100s of machines infected
in search of the admin PC
Admin
Rec
Controlling ATMs
Orders to dispense cash at a pre-determined time
© 2015 Kaspersky Lab
GREAT
KASPERSKY lab

Root cause:

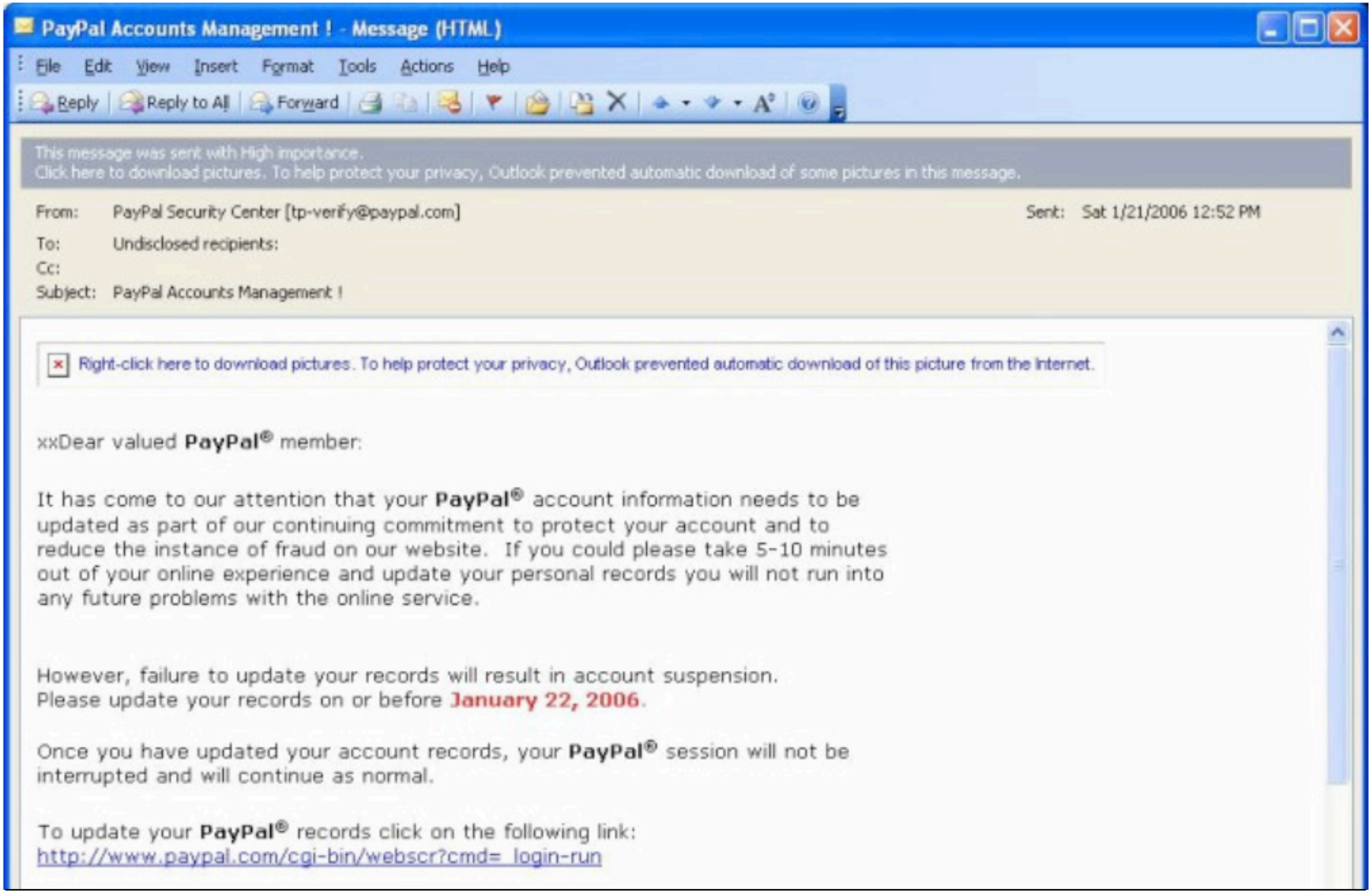
Identities of persons and machines
can be spoofed on the Internet.

There *is* an effective, yet laborious defense against (spear) phishing.

Permanent vigilance.

Determine the real sender of mails.
Determine owner and location of involved servers.

Worked example 1: PayPal Phishing


PayPal Accounts Management ! - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward

This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: PayPal Security Center [tp-verify@paypal.com]
Sent: Sat 1/21/2006 12:52 PM
To: Undisclosed recipients:
Cc:
Subject: PayPal Accounts Management !

Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

xxDear valued **PayPal**® member:

It has come to our attention that your **PayPal**® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.
Please update your records on or before **January 22, 2006**.

Once you have updated your account records, your **PayPal**® session will not be interrupted and will continue as normal.

To update your **PayPal**® records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

derived from https://www.hvfcu.org/system/files/14/original/howtotellifaphish.pdf

Worked example 1: analyse the email headers (to: paul@company.com)

```
Return-path: <tp-verify@paypal.com
Received: from mta01 (mta01.company.com [10.10.4.5])
 by mss.company.com (iPlanet Messaging Server 5.2 HotFix 2.04 (built Feb 8 2005))
 with ESMTP id <0ITG00I5U@ms-mss-02.rdc-xxx.company.com> for paul@company.com; Sat, 21 Jan 2006
 12:52:01 -0500 (EST)
Received: from mx02.company.com (mx02.company.com [192.168.10.129])
 by mta01.company.com (iPlanet Messaging Server 5.2 HotFix 2.04 (built Feb 8 2005))
 with ESMTP id <0ITG00KX9ETXO2@ms-mta-01.rdc.company.com> for paul@company.com (ORCPT
 me@company.com); Sat, 21 Jan 2006 12:49:18 -0500 (EST)
Received: from vms0xxpub.verizon.net ([206.46.252.xxx])
 by mx02.company.com with ESMTP; Sat, 21 Jan 2006 12:51:48 -0500
Received: from syzygylist ([85.186.221.yy])
 by vms01.paypal.net (Sun Java System Messaging Server 6.2-4.02 (built Sep 9 2005))
 with ESMTPA id <0ITG00BEKEXM88E0@vms046.mailsrvcs.net>; Sat, 21 Jan 2006 11:51:47 -0600 (CST)
Date: Sat, 21 Jan 2006 19:51:48 +0200
From: PayPal Security Center <tp-verify@paypal.com>
Subject: PayPal Accounts Management !
To: Undisclosed recipients: ;
Reply-to: no.reply@paypal.com
Message-id: <0ITG00KX9ETXO2@vms046.mailsrvcs.net>
MIME-version: 1.0
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
Content-type: text/html; charset=Windows-1251
Content-transfer-encoding: 8BIT
X-Priority: 1
X-MSMail-priority: High
Original-recipient: rfc822;paul@company.com
```

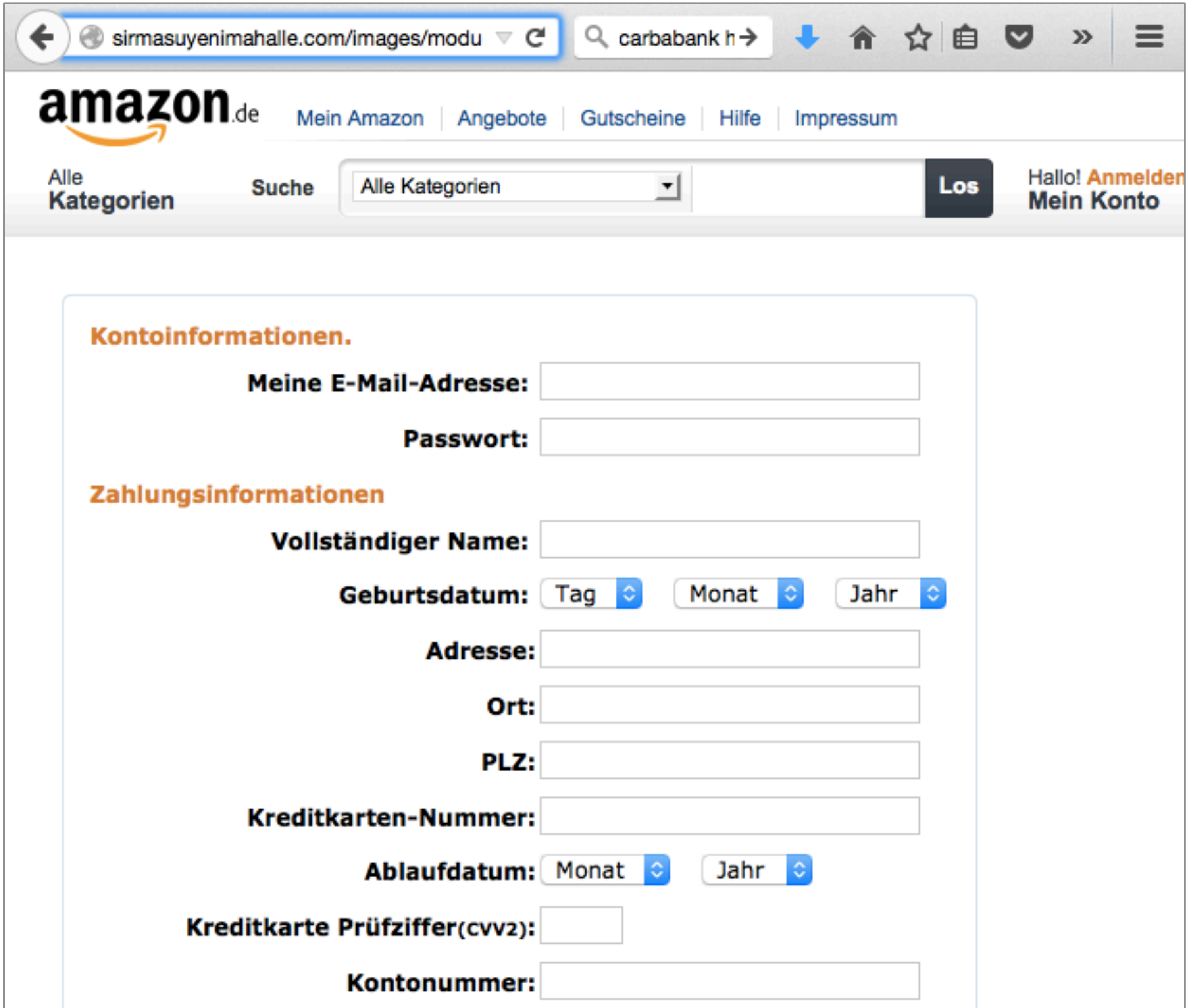
Worked example 1: analyse the email headers (to: paul@company.com)

```
Return-path: <tp-verify@paypal.com
Received: from mta01 (mta01.company.com [10.10.4.5]
 by mss.company.com (iPlanet Messaging Server 5.2 H
 with ESMTP id <0ITG00I5U@ms-mss-02.rdc-xxx.company
2006
 12:52:01 -0500 (EST)
Received: from mx02.company.com (mx02.company.com [
 by mta01.company.com (iPlanet Messaging Server 5.2
 with ESMTP id <0ITG00KX9ETXO2@ms-mta-01.rdc.compan
 me@company.com); Sat, 21 Jan 2006 12:49:18 -0500 (
Received: from vms0xxpub.verizon.net ([206.46.252.x
 by mx02.company.com with ESMTP; Sat, 21 Jan 2006 1
Received: from syzygylist ([85.186.221.yy])
 by vms01.paypal.net (Sun Java System Messaging Ser
 with ESMTPA id <0ITG00BEKEXM88E0@vms046.mailsrvcs.
```

Compare this to an authentic email from PayPal (to: mymail@exomail.to)

```
  Received: from server.exomail.to ([127.0.0.1])
    by localhost (amavisd-new, port 10024)
    with ESMTP id j08NJ4 for <mymail@exomail.to>;
    Wed, 15 Jul 2015 17:22:08 +0200 (CEST)
  Received: from mx2.slc.paypal.com ([173.0.84.226])
    (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/
    (No client certificate requested)
    by server.exomail.to (Postfix) with ESMTPS
    for <mymail@exomail.to>;
    Wed, 15 Jul 2015 17:22:07 +0200 (CEST)
```

Worked example 2: query whois service



Kontoinformationen.

Meine E-Mail-Adresse:

Passwort:

Zahlungsinformationen

Vollständiger Name:

Geburtsdatum: Tag Monat Jahr

Adresse:

Ort:

PLZ:

Kreditkarten-Nummer:

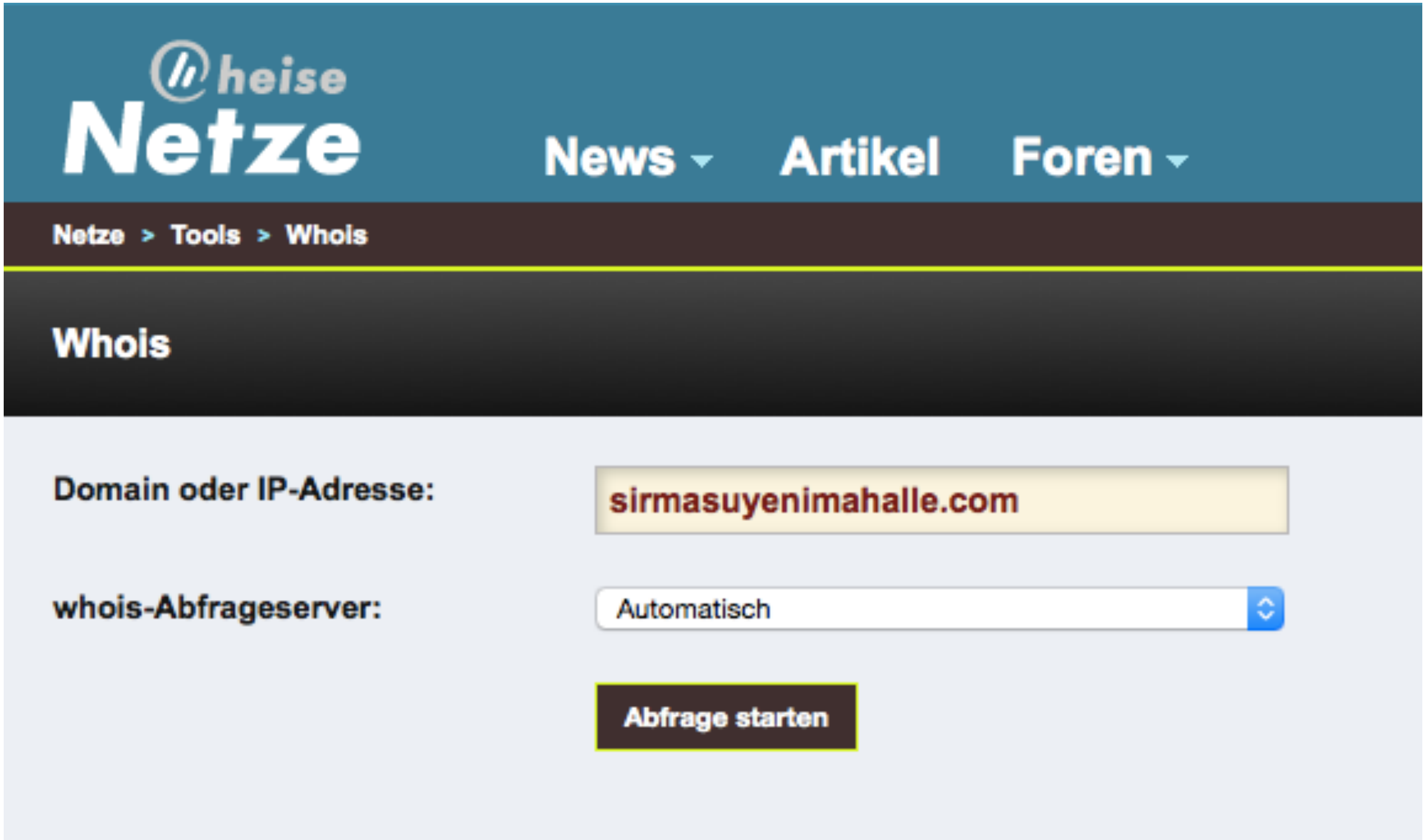
Ablaufdatum: Monat Jahr

Kreditkarte Prüfziffer(cvv2):

Kontonummer:

Worked example 2: query whois service for the domain

e.g. http://www.heise.de/netze/tools/whois/

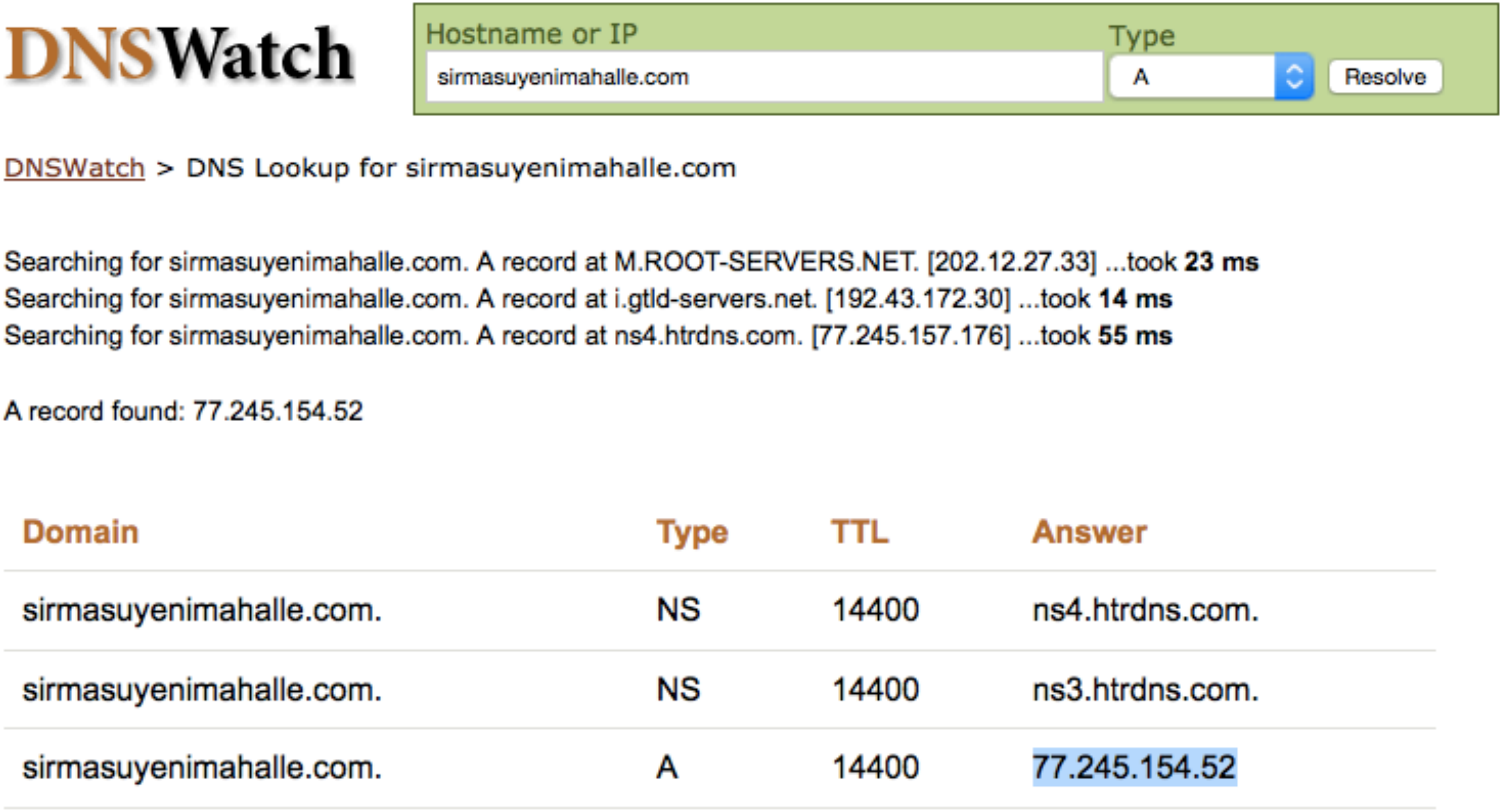


Domain oder IP-Adresse: sirmasuyenimahalle.com

whois-Abfrageserver: Automatisch

Worked example 2: determine IP address

e.g. https://www.dnswatch.info



Hostname or IP: sirmasuyenimahalle.com

Type: A

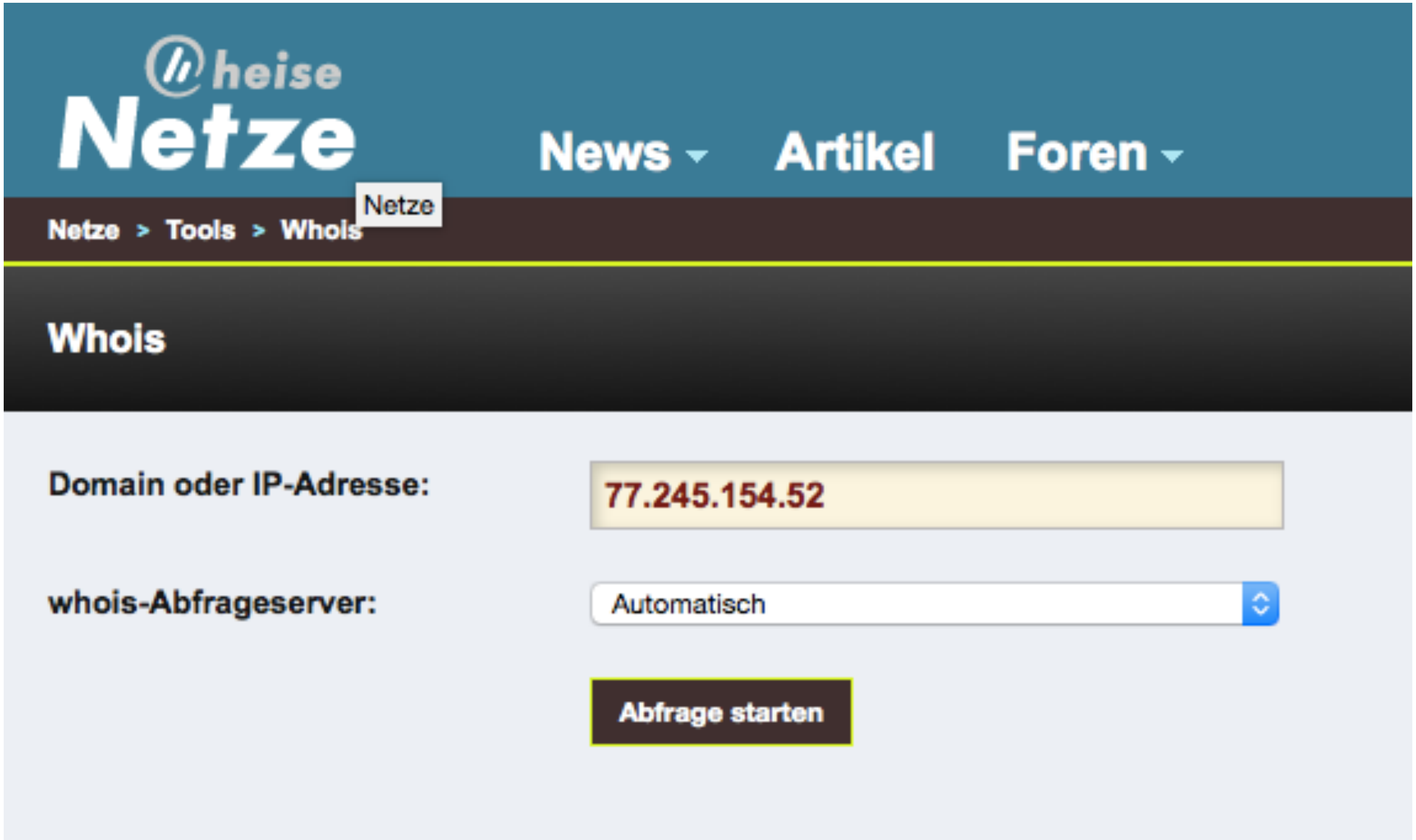
DNSWatch > DNS Lookup for sirmasuyenimahalle.com

```
Searching for sirmasuyenimahalle.com. A record at M.ROOT-SERVERS.NET. [202.12.27.33] ...took 23 ms
Searching for sirmasuyenimahalle.com. A record at i.gtld-servers.net. [192.43.172.30] ...took 14 ms
Searching for sirmasuyenimahalle.com. A record at ns4.htrdns.com. [77.245.157.176] ...took 55 ms

A record found: 77.245.154.52
```

Domain	Type	TTL	Answer
sirmasuyenimahalle.com.	NS	14400	ns4.htrdns.com.
sirmasuyenimahalle.com.	NS	14400	ns3.htrdns.com.
sirmasuyenimahalle.com.	A	14400	77.245.154.52

Worked example 2: query whois service for the IP address



Domain oder IP-Adresse: 77.245.154.52

whois-Abfrageserver: Automatisch

The crowd is effective: requesting take-down works most of the time.

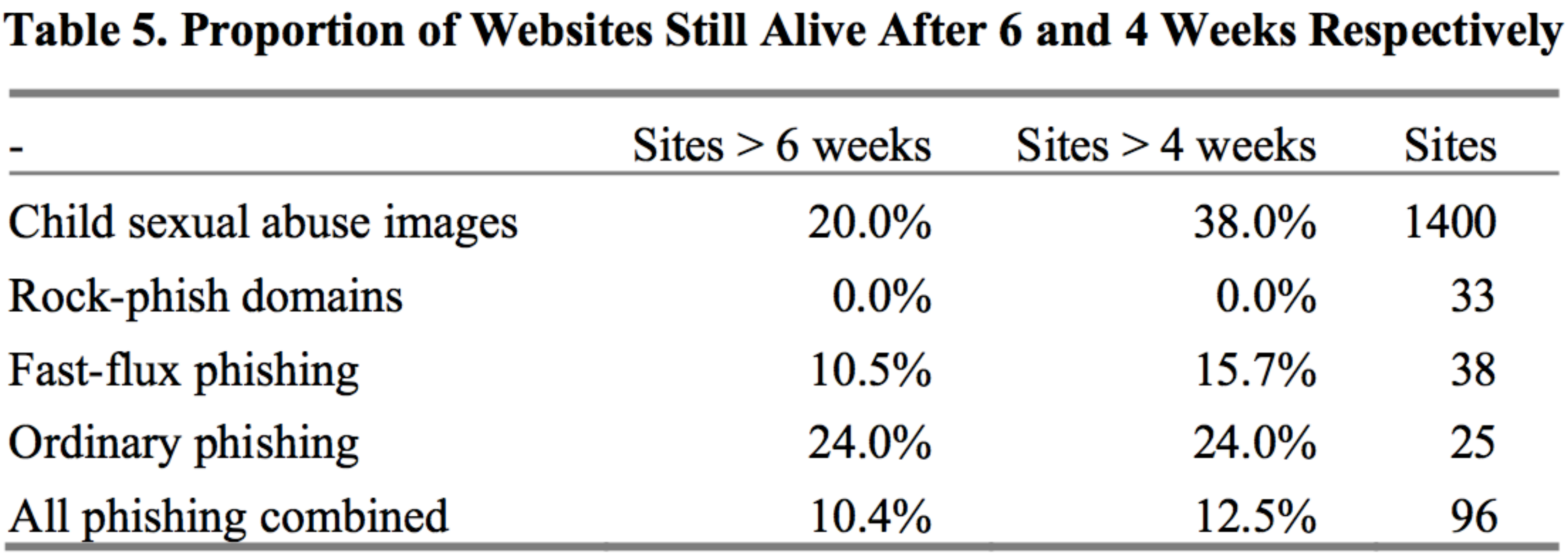


Table 5. Proportion of Websites Still Alive After 6 and 4 Weeks Respectively

-	Sites > 6 weeks	Sites > 4 weeks	Sites
Child sexual abuse images	20.0%	38.0%	1400
Rock-phish domains	0.0%	0.0%	33
Fast-flux phishing	10.5%	15.7%	38
Ordinary phishing	24.0%	24.0%	25
All phishing combined	10.4%	12.5%	96

Who decides what to take down?

Moore, Tyler, and Richard Clayton. "The impact of incentives on notice and take-down." *Managing Information Risk and the Economics of Security*. Springer US, 2009. 199-223.

Let’s call it in with the authorities.

Aug 12, 2015: I received spam.

Unsubscribe link:
http://some-site.com/
nomore.php?MailID=3148655

Let’s call it in with the authorities.

Aug 12, 2015: I received spam.

Unsubscribe link:
http://some-site.com/
nomore.php?MailID=3148655

Leaks personal data of all recipients (>3 million addresses).

Determined that data protection officer in *Schwerin* is in charge.

Aug 12, 2015: Notified DPO by mail.

Aug 26, 2015: Ack. of receipt

Web site is still online today (Aug 31, 2015)…

INTERMEDIATE SUMMARY AND DISCUSSION

What needs to change
so that citizens can fight (report)
cyber crime more effectively?

THREAT 2: Passwords

Weakness 1: Weak passwords

How do you generate
your passwords?

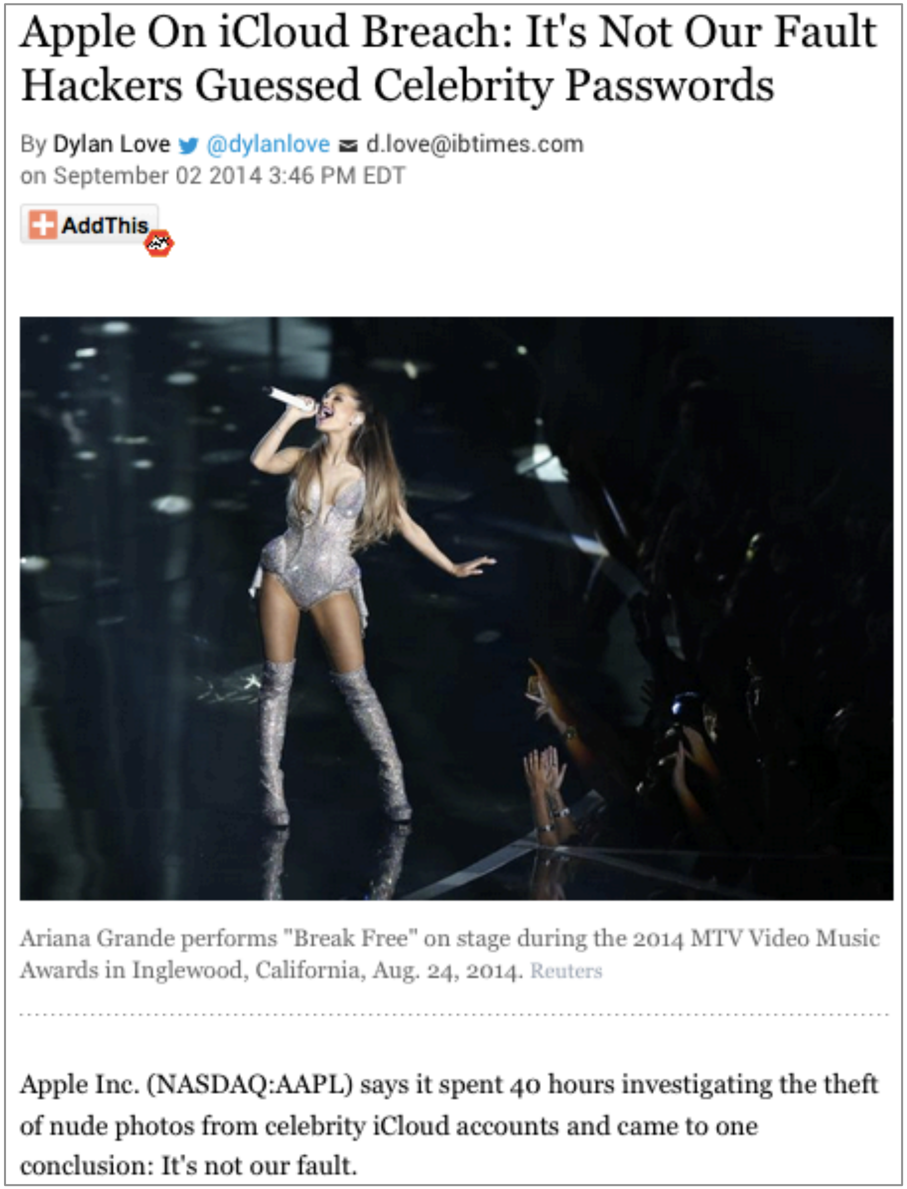
Most popular passwords (comparing rank in 2014 with 2013)

1.	123456	
2.	password	
3.	12345	▲ 17
4.	12345678	▼ 1
5.	qwerty	▼ 1
6.	123456789	
7.	1234	▲ 9
8.	baseball	new
9.	dragon	new
10.	football	new
11.	1234567	▼ 4
12.	monkey	▲ 5
13.	letmein	▲ 1
14.	abc123	▼ 9
15.	111111	▼ 8
16.	mustang	new
17.	access	new
18.	shadow	
19.	master	new
20.	michael	new
21.	superman	new
22.	696969	new
23.	123123	▼ 12
24.	batman	new
25.	trustno1	▼ 1

http://splashdata.com/press/worst-passwords-of-2014.htm

What happens if password rules are enforced?

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein



Apple On iCloud Breach: It's Not Our Fault Hackers Guessed Celebrity Passwords

By Dylan Love @dylanlove d.love@ibtimes.com
on September 02 2014 3:46 PM EDT

Ariana Grande performs "Break Free" on stage during the 2014 MTV Video Music Awards in Inglewood, California, Aug. 24, 2014. Reuters

Apple Inc. (NASDAQ:AAPL) says it spent 40 hours investigating the theft of nude photos from celebrity iCloud accounts and came to one conclusion: It's not our fault.

http://www.ibtimes.com/apple-icloud-breach-its-not-our-fault-hackers-guessed-celebrity-passwords-1676268

What happens if password rules are enforced?

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein

1. Password1
2. Princess1
3. P@ssw0rd
4. Passw0rd
5. Michael1
6. Blink182
7. !QAZ2wsx
8. Charlie1
9. Anthony1
10. 1qaz!QAZ
11. Brandon1
12. Jordan23
13. 1qaz@WSX

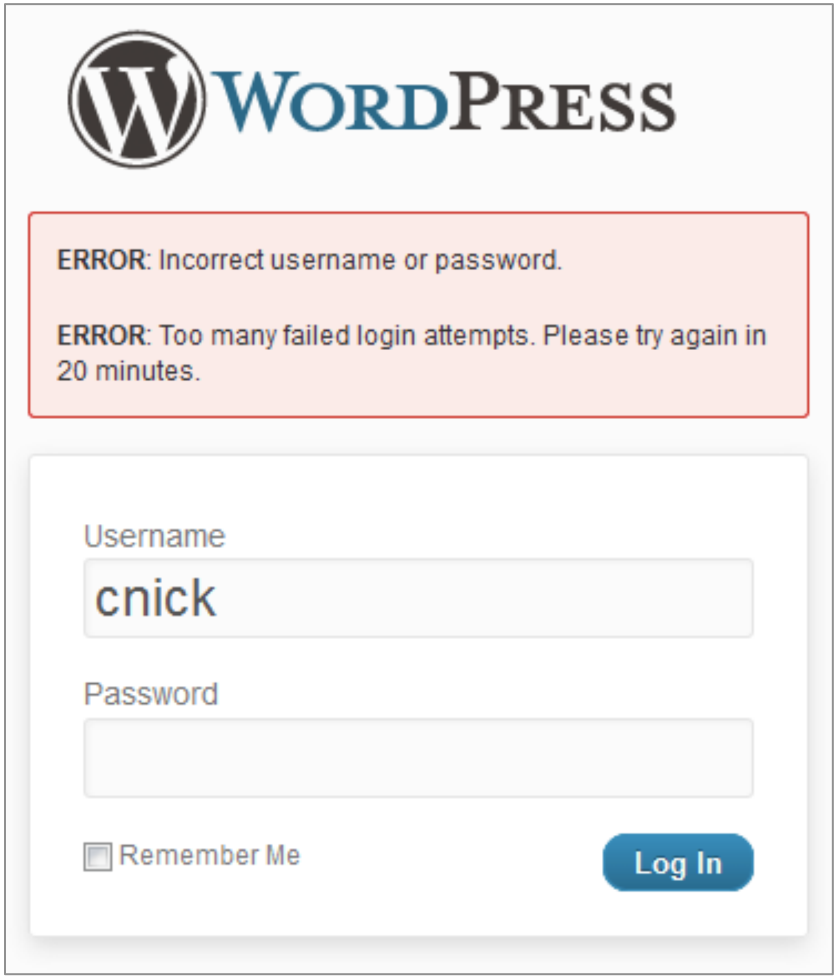
http://www.ibtimes.com/apple-icloud-breach-its-not-our-fault-hackers-guessed-celebrity-passwords-1676268

How popular are popular passwords?

		2014	2011
1.	123456	< 1%	8.5%
2.	password		
3.	12345		
4.	12345678		
5.	qwerty		
6.	123456789		
7.	1234		
8.	baseball		
9.	dragon		
10.	football	1.6%	
11.	1234567		
12.	monkey		
13.	letmein		

http://arstechnica.com/?p=600667

Many users underestimate the security of a password.



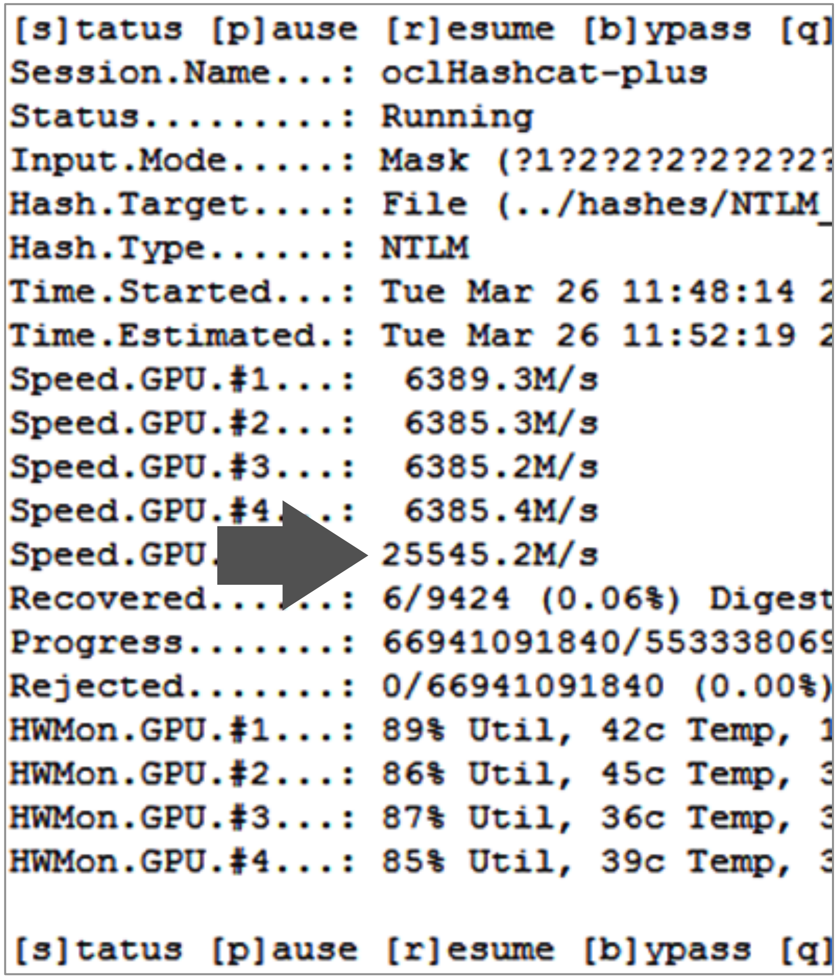
ERROR: Incorrect username or password.

ERROR: Too many failed login attempts. Please try again in 20 minutes.

Username: cnick

Password:

Online authentication
1000 guesses/sec



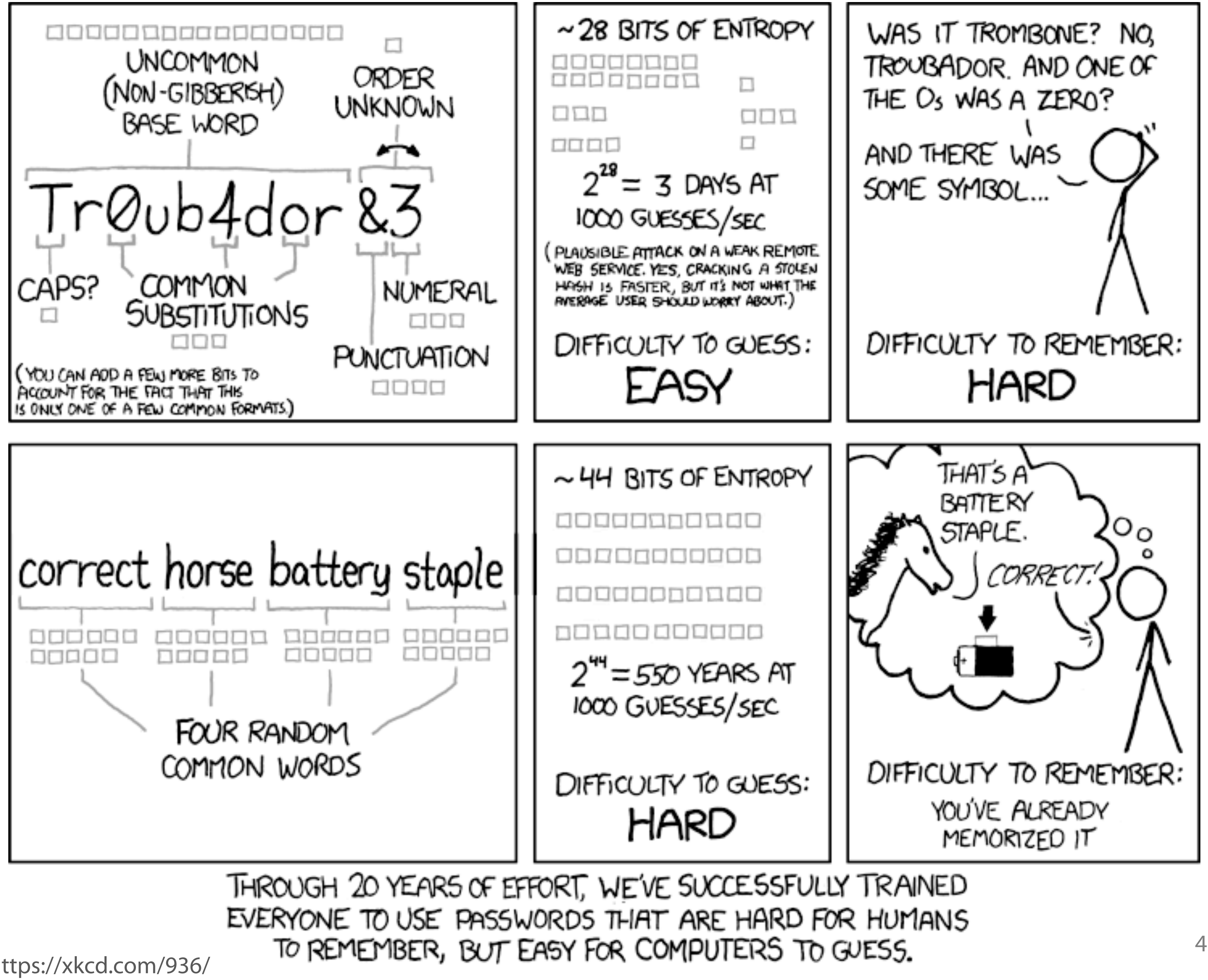
```
[s]tatus [p]ause [r]esume [b]ypass [q]
Session.Name...: oclHashcat-plus
Status.........: Running
Input.Mode.....: Mask (?1?2?2?2?2?2?2?
Hash.Target....: File (../hashes/NTLM_
Hash.Type......: NTLM
Time.Started...: Tue Mar 26 11:48:14 2
Time.Estimated.: Tue Mar 26 11:52:19 2
Speed.GPU.#1...:  6389.3M/s
Speed.GPU.#2...:  6385.3M/s
Speed.GPU.#3...:  6385.2M/s
Speed.GPU.#4...:  6385.4M/s
Speed.GPU.       25545.2M/s
Recovered......: 6/9424 (0.06%) Digest
Progress.......: 66941091840/553338069
Rejected.......: 0/66941091840 (0.00%)
HWMon.GPU.#1...: 89% Util, 42c Temp, 1
HWMon.GPU.#2...: 86% Util, 45c Temp, 3
HWMon.GPU.#3...: 87% Util, 36c Temp, 3
HWMon.GPU.#4...: 85% Util, 39c Temp, 3

[s]tatus [p]ause [r]esume [b]ypass [q]
```

Offline cracking
25 billion guesses/sec

Everyone can create a strong password.

https://xkcd.com/936/

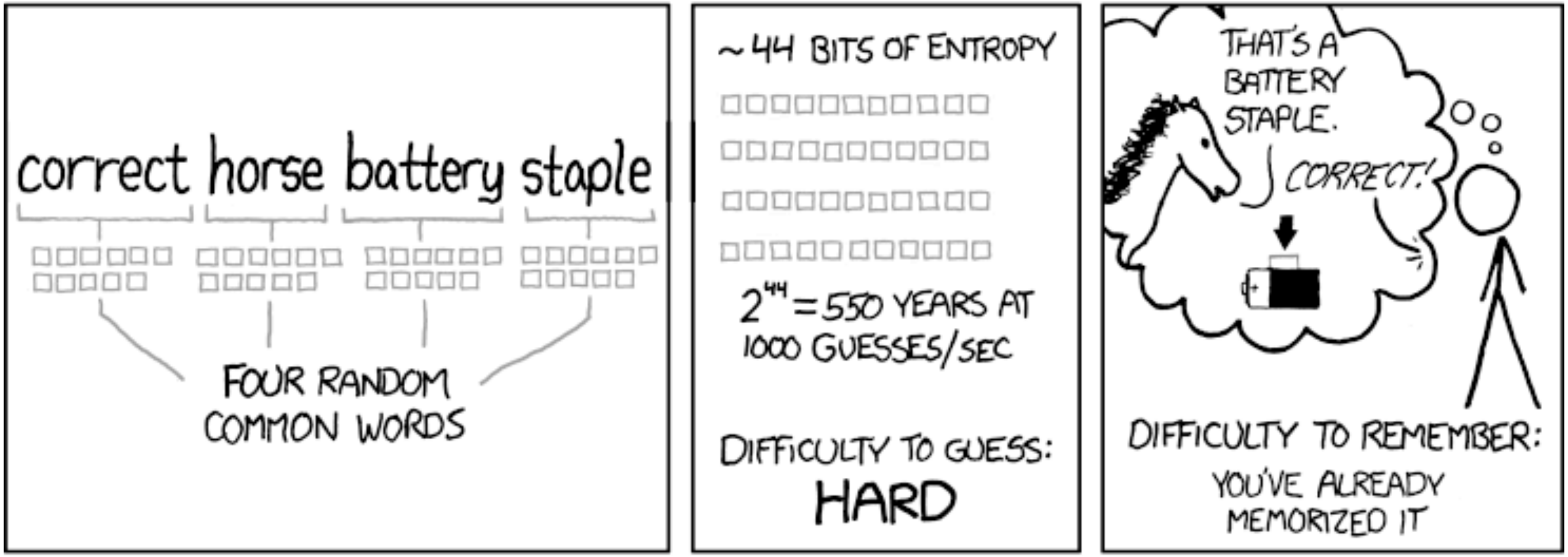

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

https://xkcd.com/936/

Now, it's your turn.

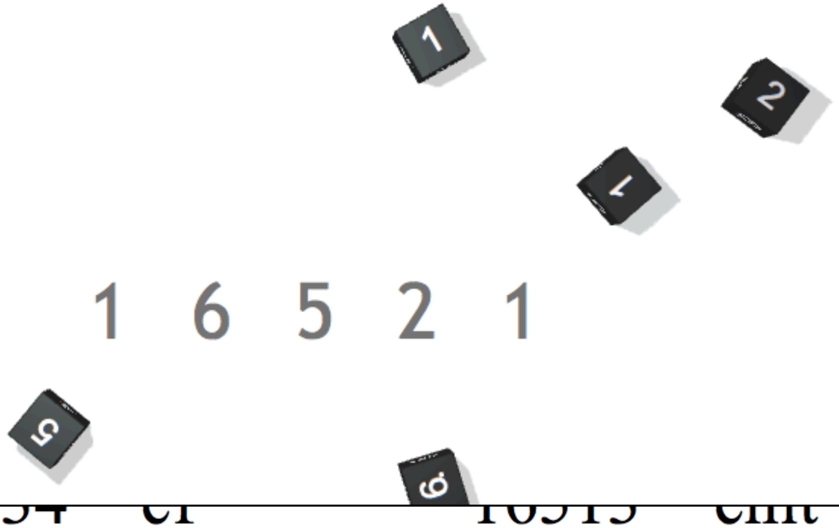
Come up with 3 passwords that contain 5 common (short) English words each.

What is the problem with this approach?


correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

https://xkcd.com/936/

Best Practice 1: Create strong *and* memorizable passwords



Word 1: choke

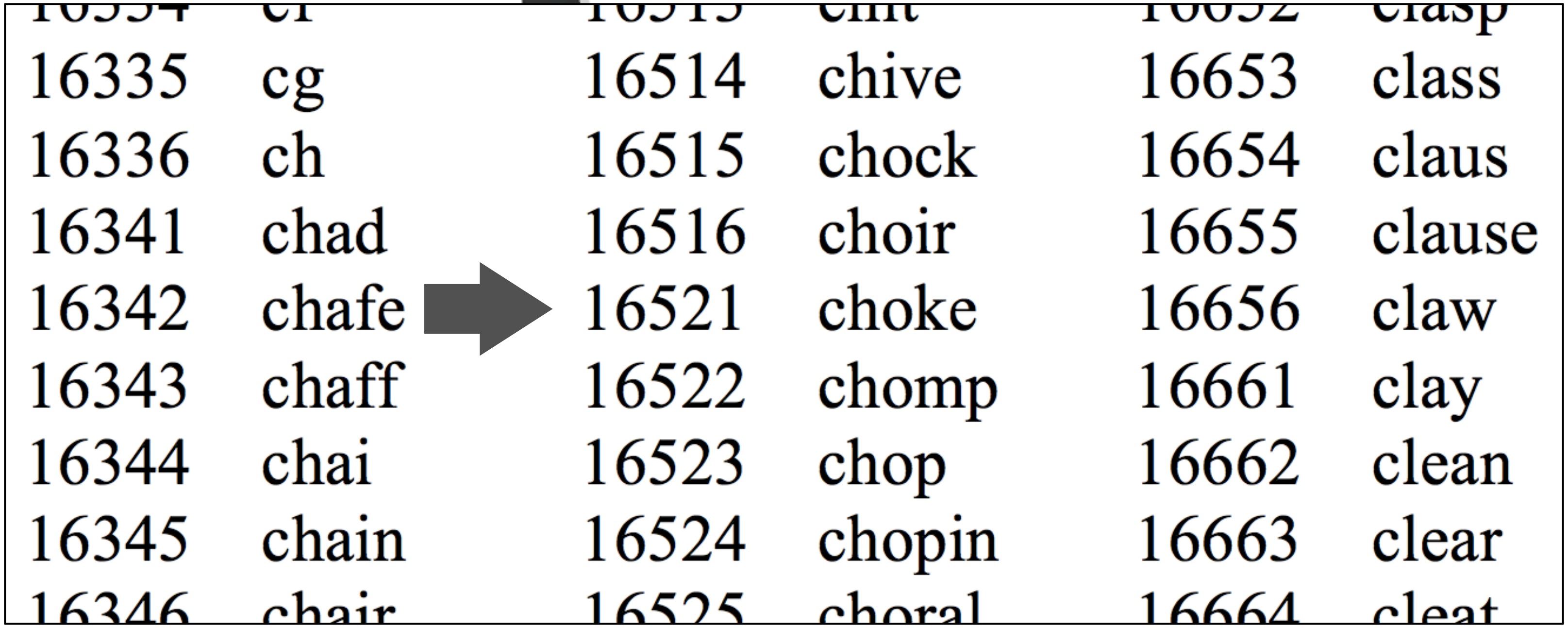
Word 2: goat

Word 3: adam

Word 4: above

Word 5: urban

Word 6: poem



16334	cf	16513	chit	16652	clasp
16335	cg	16514	chive	16653	class
16336	ch	16515	chock	16654	claus
16341	chad	16516	choir	16655	clause
16342	chafe	16521	choke	16656	claw
16343	chaff	16522	chomp	16661	clay
16344	chai	16523	chop	16662	clean
16345	chain	16524	chopin	16663	clear
16346	chair	16525	choral	16664	cleat

http://a.teall.info/dice/ – http://www.rubin.ch/pgp/diceware.html

This approach is called Diceware.

Word 1: choke

Word 2: goat

Word 3: adam

Word 4: above

Word 5: urban

Word 6: poem

“choke goat adam above urban poem”

Resulting security level?

If adversary does not know about Diceware…

6 words
avg. length: 4.2
5 spaces

Number of lowercase passwords to try: $> 26^{(4.2 \bullet 6 + 5)} = 2.81 \bullet 10^{42}$ 141 bit

But what if the adversary knows you use Diceware…

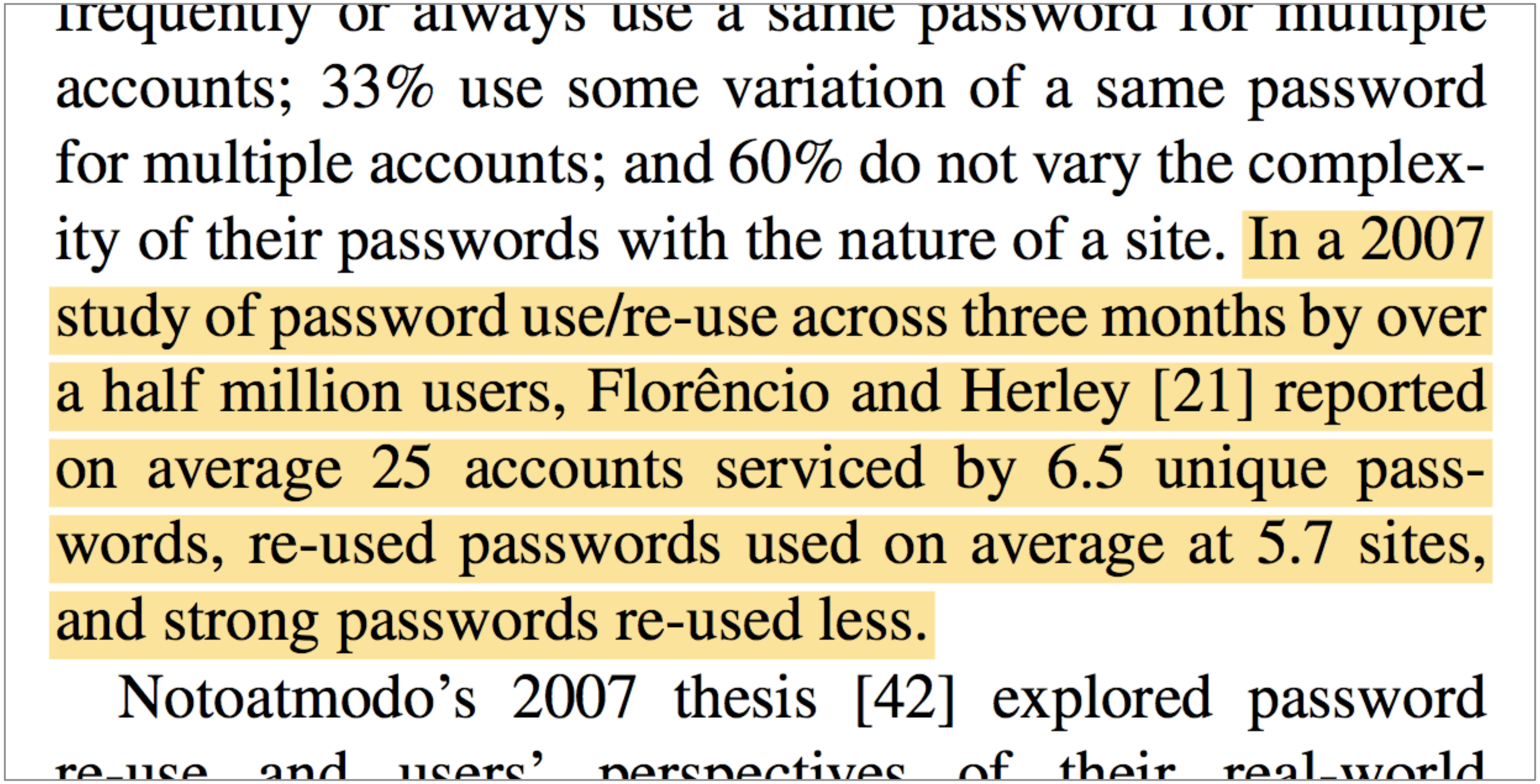
Number of words in Diceware list: $6^5 = 7776$

Number of Diceware passwords: $7776^6 = 2.21 \bullet 10^{23}$ 77 bit

Try that yourself (later)

Make up some passwords and check whether they have been leaked already.

Weakness 2: Using passwords on multiple sites.



frequently or always use a same password for multiple accounts; 33% use some variation of a same password for multiple accounts; and 60% do not vary the complexity of their passwords with the nature of a site. In a 2007 study of password use/re-use across three months by over a half million users, Florêncio and Herley [21] reported on average 25 accounts serviced by 6.5 unique passwords, re-used passwords used on average at 5.7 sites, and strong passwords re-used less.

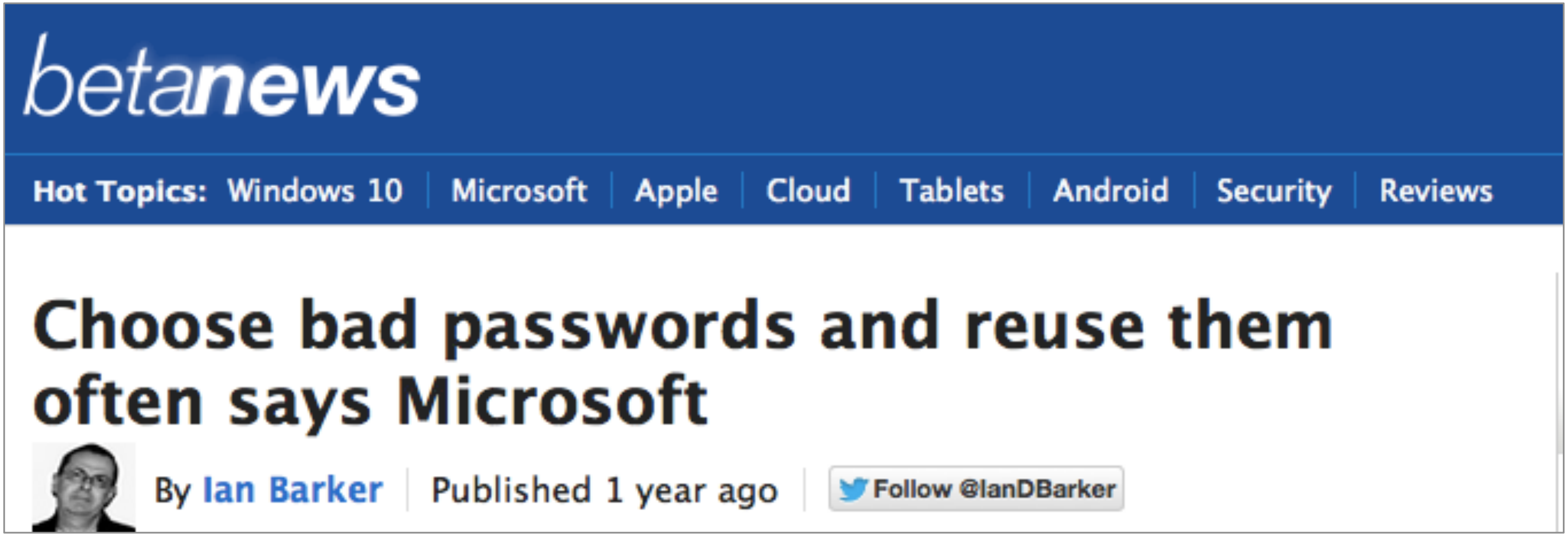
Notoatmodo's 2007 thesis [42] explored password re-use and users' perspectives of their real-world

Why is re-use bad?

D. Florencio and C. Herley. A Large-Scale Study of Web Password Habits. Proc. WWW, 2007.

Best Practice 2: Always use random, strong, and unique passwords!

… has been questioned by recent research.



betanews

Hot Topics: Windows 10 | Microsoft | Apple | Cloud | Tablets | Android | Security | Reviews

Choose bad passwords and reuse them often says Microsoft

By Ian Barker | Published 1 year ago | Follow @IanDBarker

Florêncio, Dinei, Cormac Herley, and Paul C. Van Oorschot. "Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts." Proc. USENIX Security. 2014.

http://research.microsoft.com/pubs/217510/passwordPortfolios.pdf

Best Practice 3: Use a password manager.

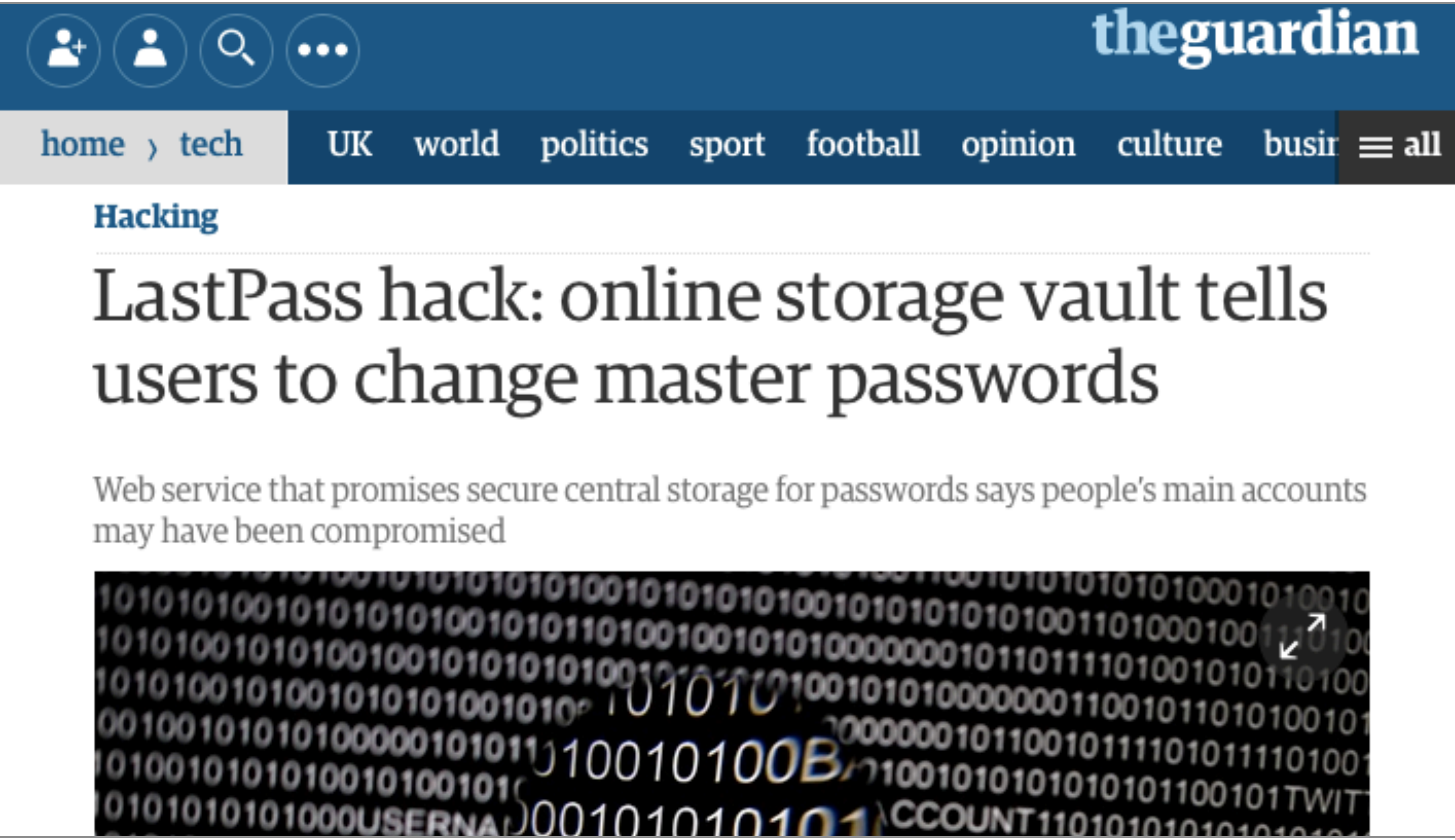
Allows you to choose a unique and random password for every website.

Secure your password store with a strong master password.

Limitations?

- cannot prevent copy & pasted passwords being stolen by malware.
- compromise of master password has severe consequences
- cloud-based introduce additional risks, while local-only software loses portability.

Beware of insecure commercial implementations!

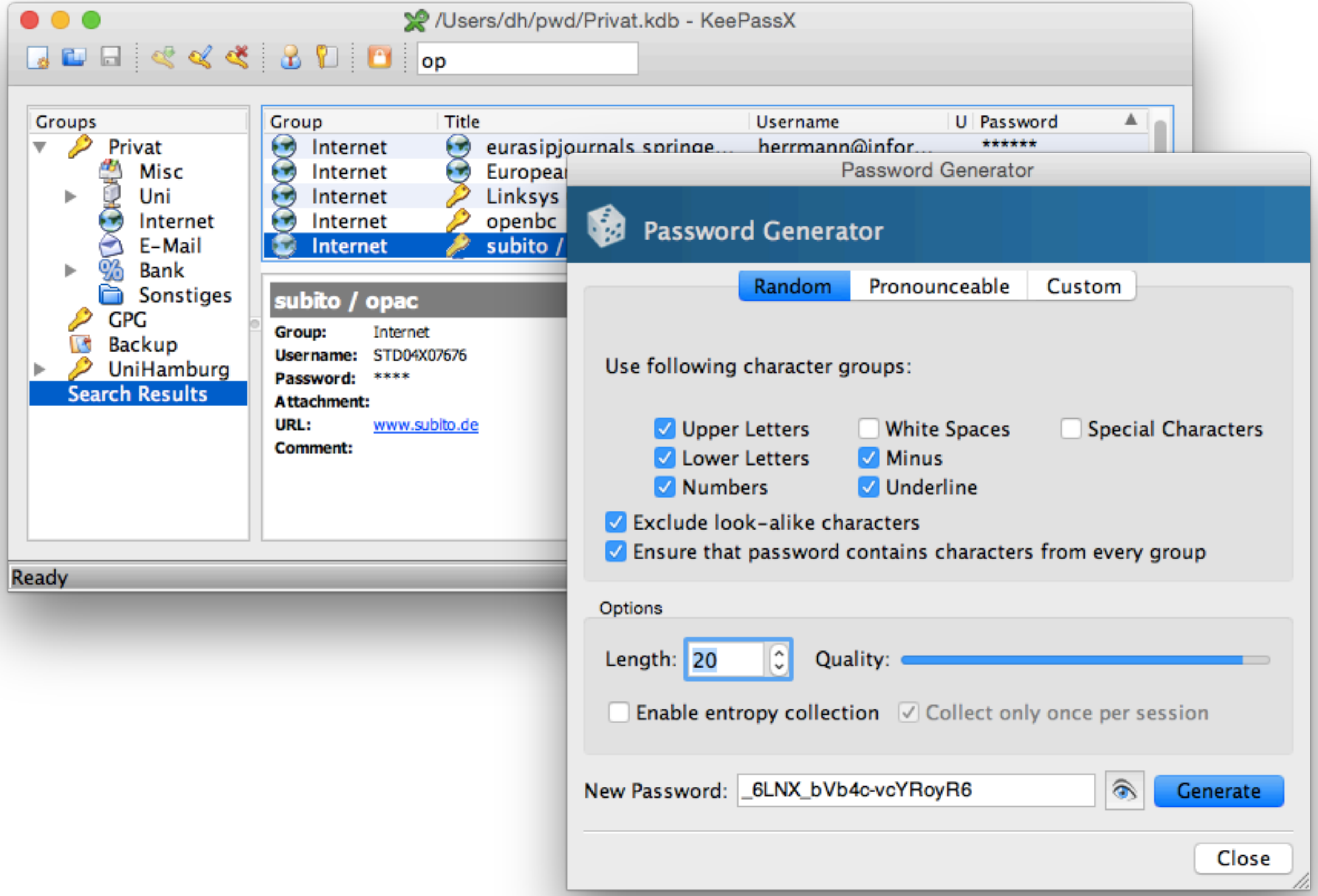


Hacking

LastPass hack: online storage vault tells users to change master passwords

Web service that promises secure central storage for passwords says people's main accounts may have been compromised

Rule of thumb: stick to well-tested open source software. (like KeePassX)



/Users/dh/pwd/Privat.kdb - KeePassX

op

Groups
- Privat
  - Misc
  - Uni
  - Internet
  - E-Mail
  - Bank
  - Sonstiges
- GPG
- Backup
- UniHamburg
- Search Results

Group	Title	Username	U	Password
Internet	eurasipjournals.springe...	herrmann@infor...		******
Internet	Europea			
Internet	Linksys			
Internet	openbc			
Internet	subito /			

subito / opac

Group: Internet
Username: STD04X07676
Password: ****
Attachment:
URL: www.subito.de
Comment:

Ready

Password Generator

Password Generator

Random | Pronounceable | Custom

Use following character groups:

☑ Upper Letters ☐ White Spaces ☐ Special Characters
☑ Lower Letters ☑ Minus
☑ Numbers ☑ Underline
☑ Exclude look-alike characters
☑ Ensure that password contains characters from every group

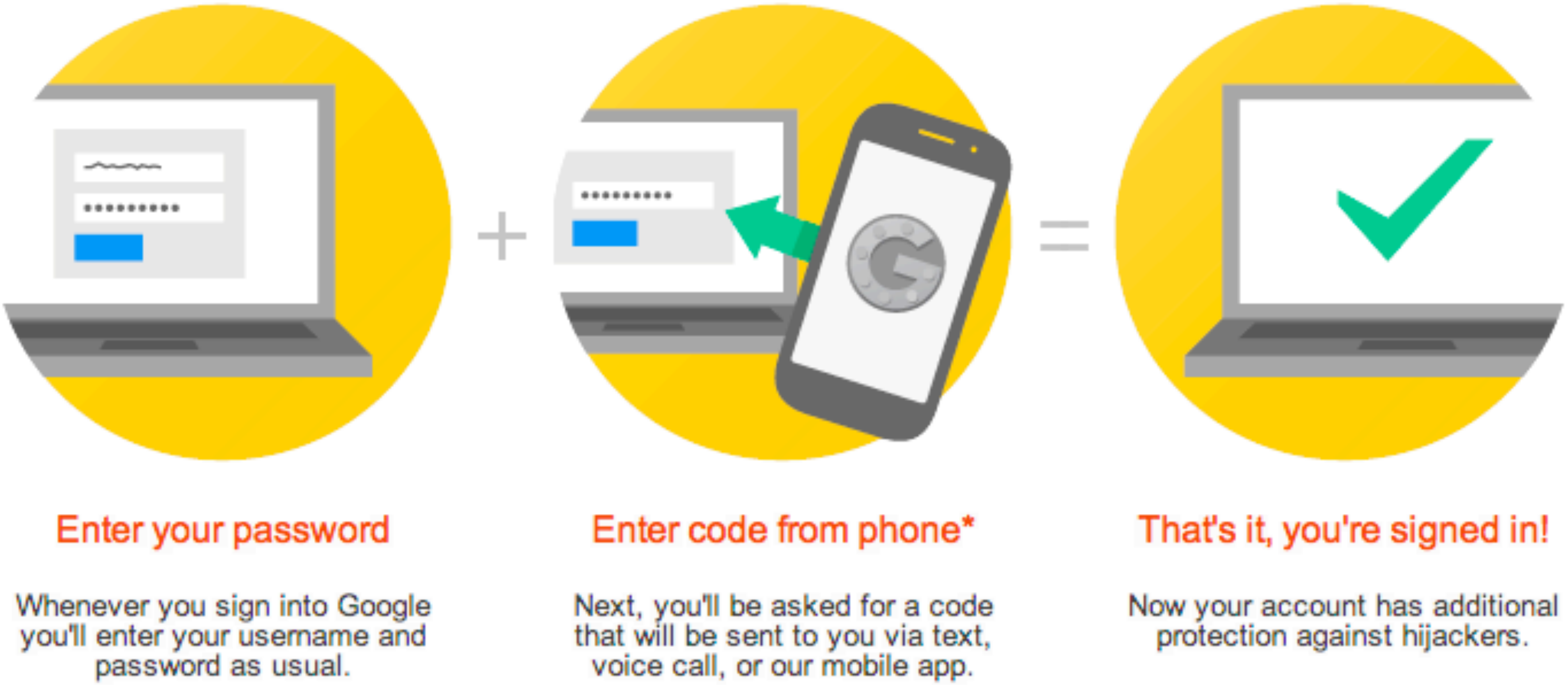
Options

Length: 20 Quality:

☐ Enable entropy collection ☑ Collect only once per session

New Password: _6LNX_bVb4c-vcYRoyR6

Best Practice 4: Use two-factor authentication.



Enter your password

Whenever you sign into Google you'll enter your username and password as usual.

Enter code from phone*

Next, you'll be asked for a code that will be sent to you via text, voice call, or our mobile app.

That's it, you're signed in!

Now your account has additional protection against hijackers.

Something you **know**

Something you **are**

Something you **have**

https://paul.reviews/content/images/2014/Sep/two-factor-authentication-02.png

Problem 1: Industry has little incentive to create secure software.

Why? **Externality effects**

Secure software more expensive than insecure software & patching it later.

Lock-in effects

Incentives? Hold vendors liable for insecure software.

https://www.schneier.com/essays/archives/2007/01/information_security_1.html

Problem 2: Users make poor security choices.

Humans are not good at

determining **likelihood** and **impact** of risks

making **trade-offs** between comfort and security

immediate gratification

hyperbolic discounting

> *"There are apps that collect personal data on fitness, nutrition and habits. Can you imagine to use the feature to forward the collected data to your health insurance company?"*

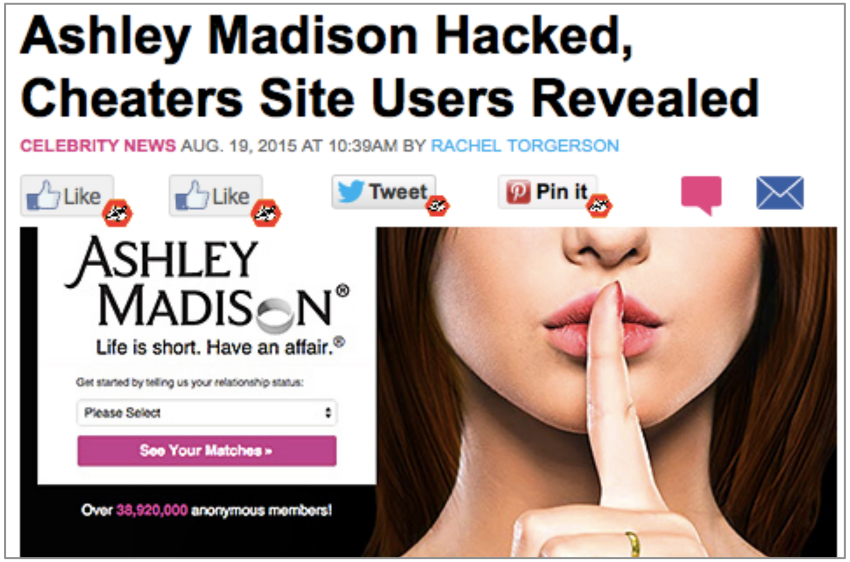
36 % of respondents answered with "yes"

A. Acquisti (2004): Privacy in Electronic Commerce and the Economics of Immediate Gratification
http://www.bitkom.org/de/presse/8477_82168.aspx

INTERMEDIATE SUMMARY AND DISCUSSION

How and when should we train users
to make reasonable security decisions?

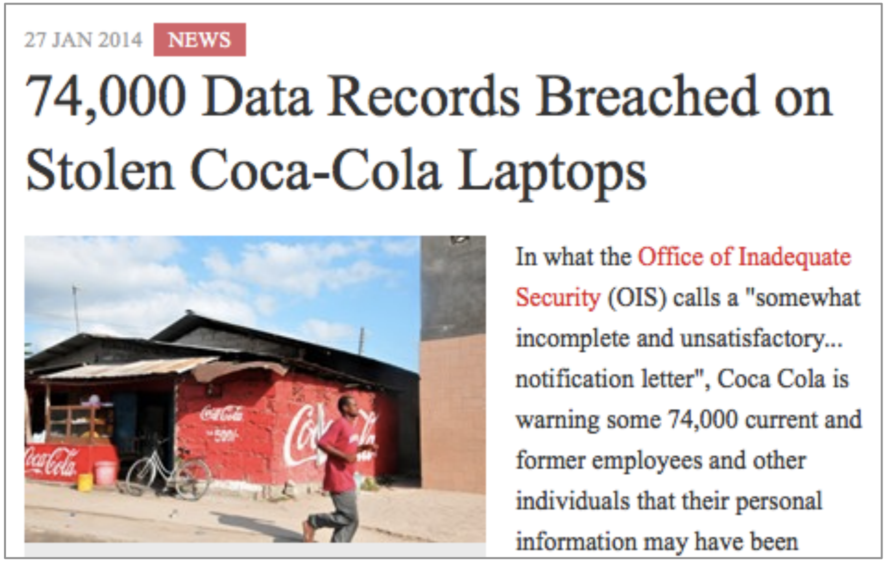
THREAT 3: Disclosure of private information



Ashley Madison Hacked, Cheaters Site Users Revealed

CELEBRITY NEWS AUG. 19, 2015 AT 10:39AM BY RACHEL TORGERSON

Like
Like
Tweet
Pin it
ASHLEY MADISON®
Life is short. Have an affair.®
Get started by telling us your relationship status:
Please Select
See Your Matches »
Over 38,920,000 anonymous members!



27 JAN 2014 NEWS

74,000 Data Records Breached on Stolen Coca-Cola Laptops

In what the Office of Inadequate Security (OIS) calls a "somewhat incomplete and unsatisfactory... notification letter", Coca Cola is warning some 74,000 current and former employees and other individuals that their personal information may have been

Best Practice: Use encryption

Turn on **full disk encryption**

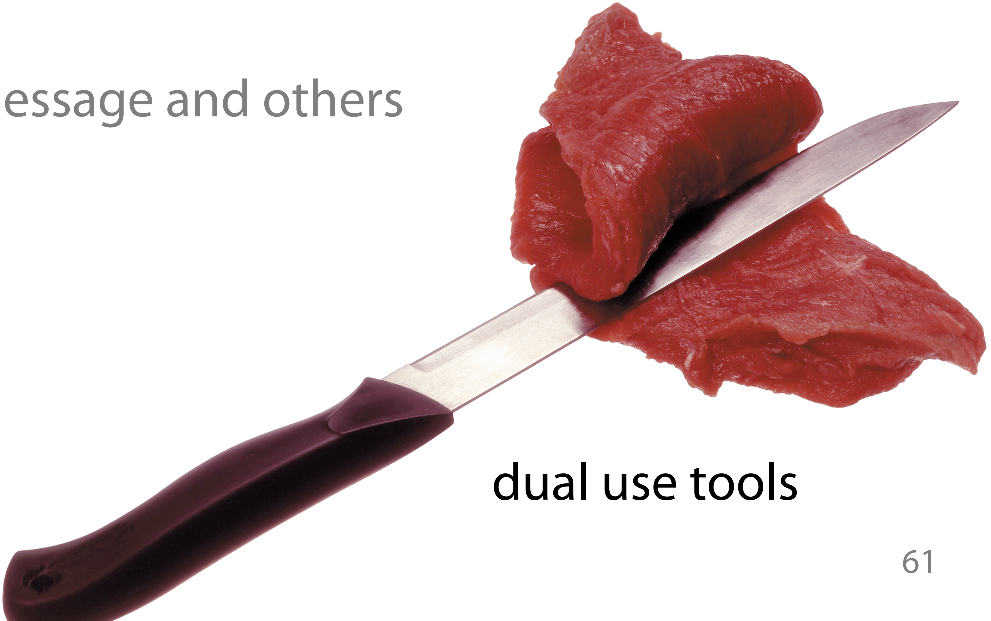
- Microsoft BitLocker, Apple FileVault, VeraCrypt, (TrueCrypt)
- EncFS- or dm-crypt-based (Linux)

Use **encrypted cloud storage**

- Boxcryptor (commercial, but OpenSource)

Messaging solutions that provide **end-to-end encryption**

- PGP, OTR, Threema, TextSecure
- problematic: WhatsApp, Apple iMessage and others

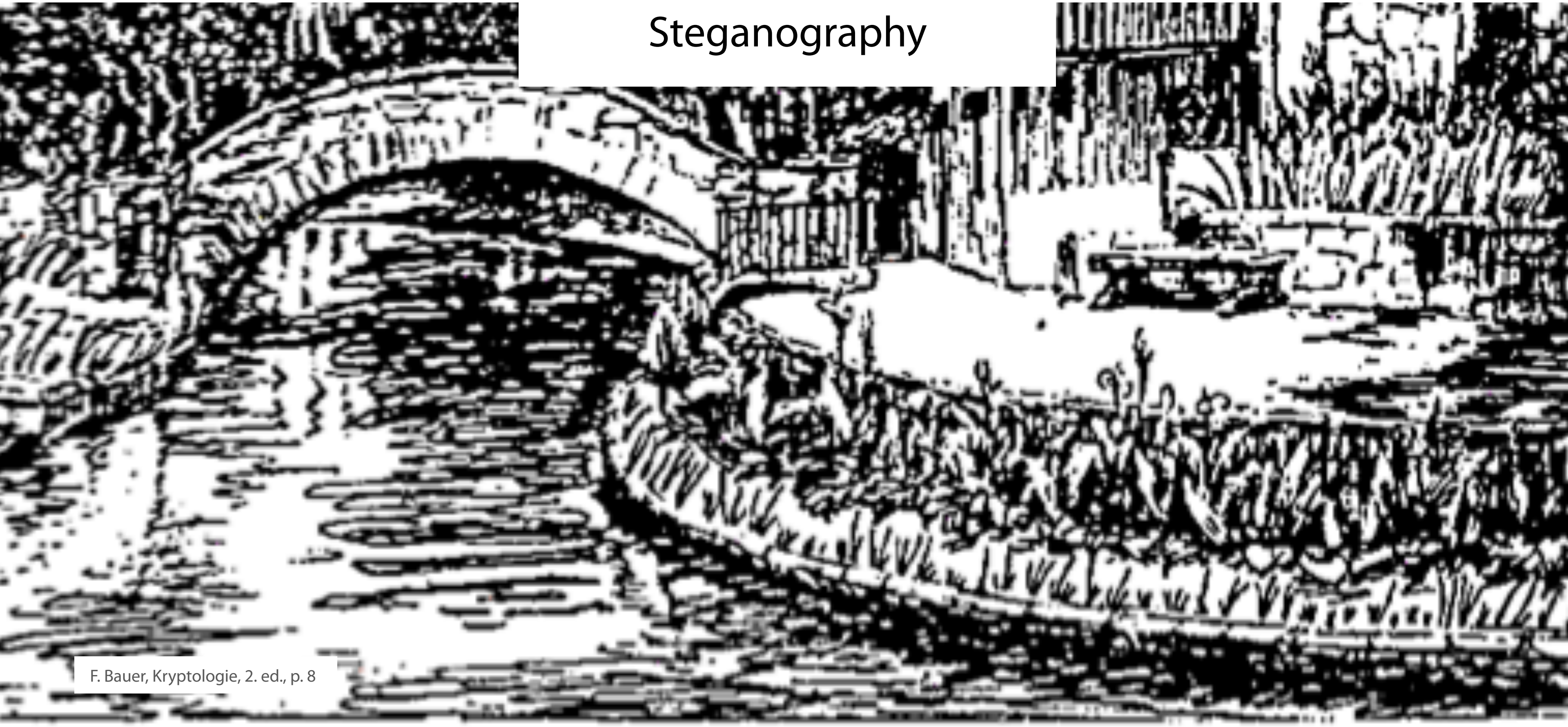


dual use tools

Policy makers want to weaken encryption – which is dangerous and futile.

Law enforcement demands to be able to **decrypt all encrypted** communication (“golden key”).

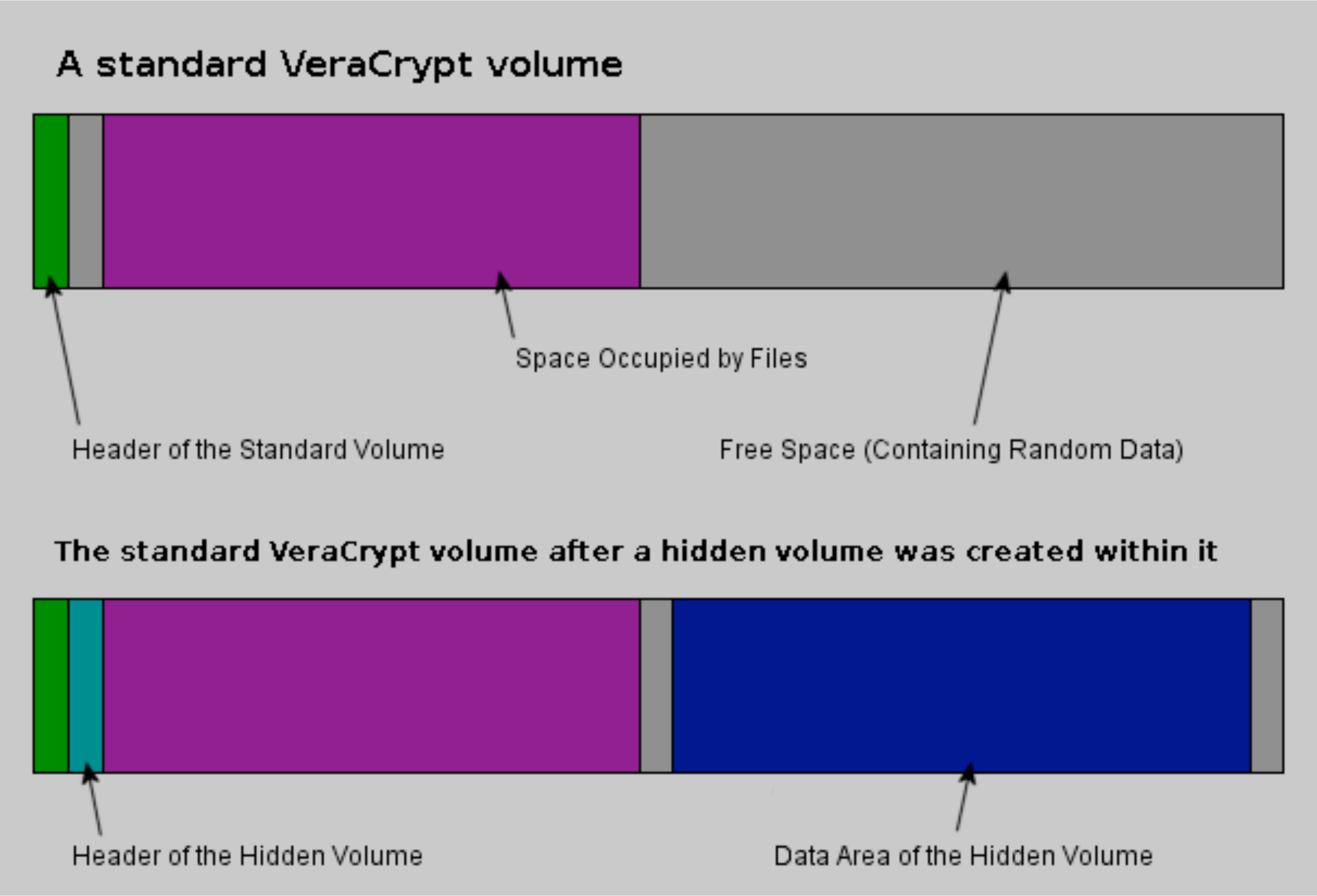
Some have even proposed to **forbid** non-decryptable communication.



Steganography

F. Bauer, Kryptologie, 2. ed., p. 8

Policy makers want to weaken encryption – which is dangerous and futile.


A standard VeraCrypt volume
Space Occupied by Files
Header of the Standard Volume
Free Space (Containing Random Data)
The standard VeraCrypt volume after a hidden volume was created within it
Header of the Hidden Volume
Data Area of the Hidden Volume

http://rt.com/news/australia-nsa-snowden-surveillance-510 – http://arstechnica.com/tech-policy/2014/03/after-snowden-australias-cops-worry-about-people-using-crypto
https://veracrypt.codeplex.com/wikipage?title=Hidden%20Volume, but see also https://defuse.ca/truecrypt-plausible-deniability-useless-by-game-theory.htm

Fear spurs irrational decisions (cf. economic failure of airport security).

https://upload.wikimedia.org/wikipedia/commons/5/53/Security_in_Manchester_aeroport.jpg

TAKE-AWAY MESSAGES

1 We cannot expect law enforcement to be able to fight cyber crime effectively. The **crowd must engage**!

2 There *are* effective countermeasures that **can be applied by anyone**, some often cited ones are impractical.

3 We have to consider **psychological and economical** aspects of security in order to avoid irrational decisions.

Let the Crowd Fight Crime:

enabling users to stay safe in cyberspace

Dr. Dominik Herrmann

dh@exomail.to

Slides are available at
http://dhgo.to/isa2015slides