Root causes

technical & non-technical

Erik Poll

Radboud University Nijmegen

How vs Why

- How do web applications get hacked?

vs

- Why are applications so vulnerable?
- Why are people hacking them?
- Why are security problems not being fixed?

Web Security

What we have seen:

Technology to build things

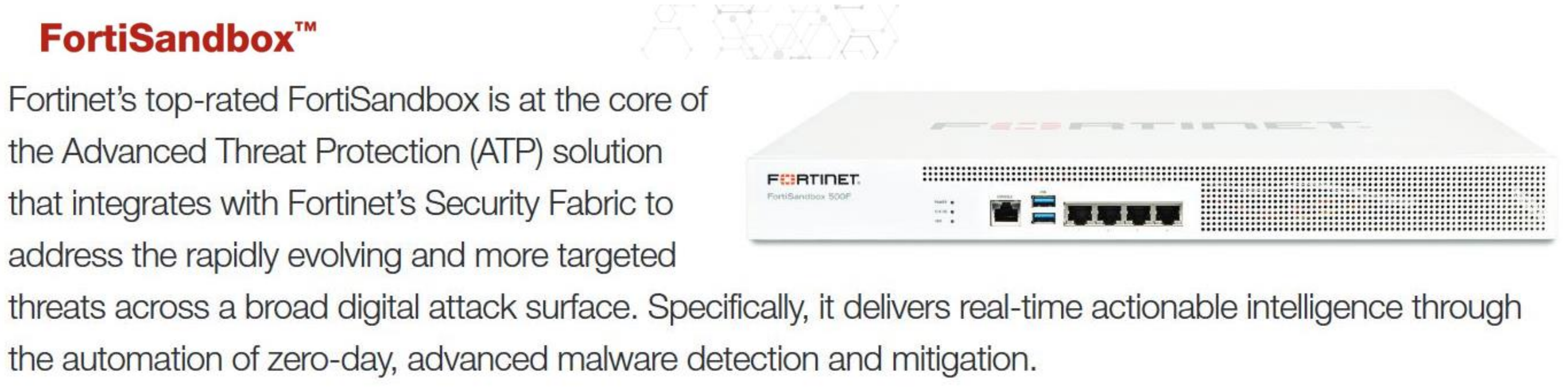
- HTTP, URL, HTML
- How to secure sessions
- What is possible using javascript & the DOM

Ways to attacks this

- Attacks on servers (OS command injection, SQL injection, ..)
- Attacks on the client (reflected XSS, CSRF, ...)
- Attacks on their interaction (injected XSS, CSRF, ...)
- Attacks on sessions (SSL stripping, cookie stealing,...)
- Attacks on privacy
- New attacks today: default passwords, phishing, supply chain attacks

Not just for the typical web applications

Not only web-sites & browser under attack, but web-interfaces that show up in of all sorts of devices (eg routers, firewalls, VPN servers, ...)

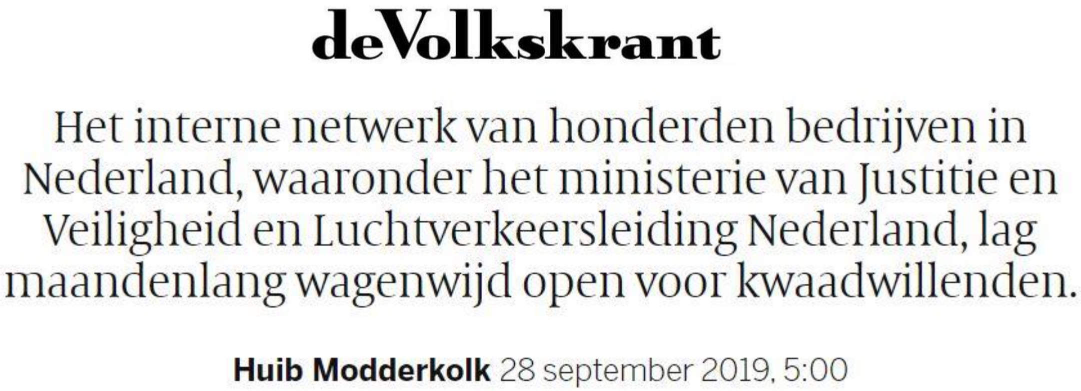


FortiSandbox™

Fortinet's top-rated FortiSandbox is at the core of the Advanced Threat Protection (ATP) solution that integrates with Fortinet's Security Fabric to address the rapidly evolving and more targeted threats across a broad digital attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and mitigation.

CVE-2015-8038 Multiple cross-site scripting (XSS) vulnerabilities in the Graphical User Interface (GUI) in Fortinet FortiManager before 5.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) sharedjobmanager or (2) SOMServiceObjDialog.

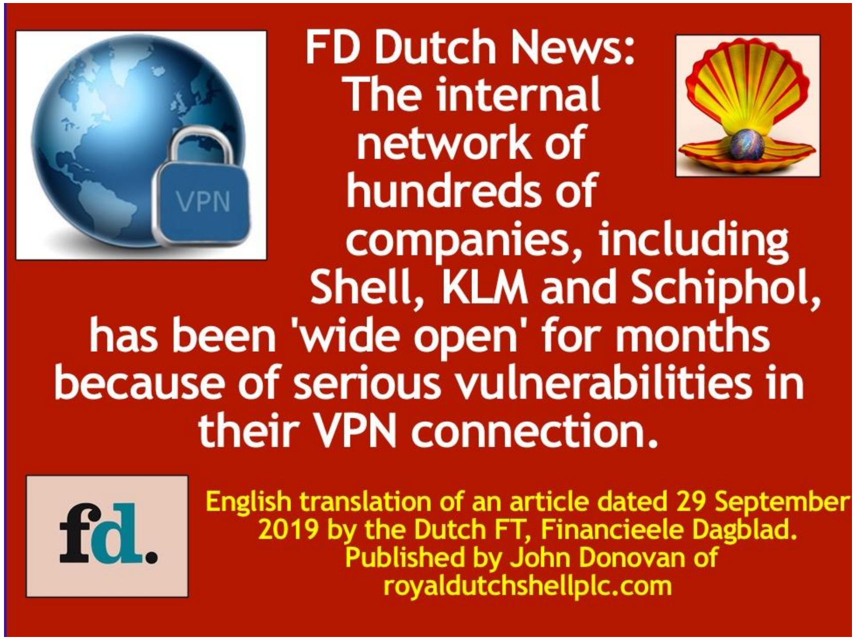
More recent VPN problems



deVolkskrant

Het interne netwerk van honderden bedrijven in Nederland, waaronder het ministerie van Justitie en Veiligheid en Luchtverkeersleiding Nederland, lag maandenlang wagenwijd open voor kwaadwillenden.

Huib Modderkolk 28 september 2019, 5:00



FD Dutch News: The internal network of hundreds of companies, including Shell, KLM and Schiphol, has been 'wide open' for months because of serious vulnerabilities in their VPN connection.

fd.

English translation of an article dated 29 September 2019 by the Dutch FT, Financieele Dagblad. Published by John Donovan of royaldutchshellplc.com

also involved Fortinet VPN

Just fixing bugs and improving technology we’re not going to solve things...

We have to understand

- security requirements
- attackers and their motivations
- underlying root causes, that keep causing new categories of problems

I.e. not just ***how*** attacks works, but also

- ***what*** attackers attack and ***why***
- the recurring ***root causes*** that make attacks possible

Recurring themes

complexity,
languages & formats

Complexity in systems

Root cause of many security problems is **complexity** in the many technologies, languages, features and the *interaction* between them

- eg HTML, javascript, file systems, Operating System (OS), database systems,... SQL, PHP, ...

The virtual world is only possible thanks to abstractions

- web as abstraction layer over the internet
- domain names (URL/URIs) as abstraction over IP addresses
- internet as abstraction over routers, networks, servers, ...
- OS and its file system as abstraction of computer with CPU & disk

that we need to control the complexity.

Unfortunately, these abstractions are *not perfect*, and *bugs in corner cases* or *unforeseen interactions* can create havoc.

(Errors in) handling languages & formats

- Languages & formats need to be interpreted/processed
  - email address needs to be parsed by email client
  - path & filenames have to be parsed & handled by OS
  - HTML, jpg, mpeg,.. need to be displayed by browser
  - javascript and program code need to be executed

  Such interpretation of data is what computing science is all about!
- Bugs in processing inputs causes many security problems

  Attackers supply malicious inputs to exploit these bugs, eg
  - buffer overflows & format string attacks in Hacking in C
  - command injection, path traversal, SQL injection, HTML injection, ...
- Worst case scenario: the malicious input can contains ***code***

  eg machine code in buffer overflow, or javascript in HTML

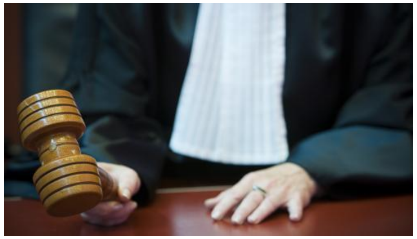
Prevent, but also ***detect*** and ***react***

***Never* be tempted into thinking that prevention makes detection & reaction superfluous.**

Eg. breaking into any house with big windows is trivial;
only detection & reaction really deters burglars.

Detection of digital break-in is harder

- Who noticed a break-in on his computer recently?

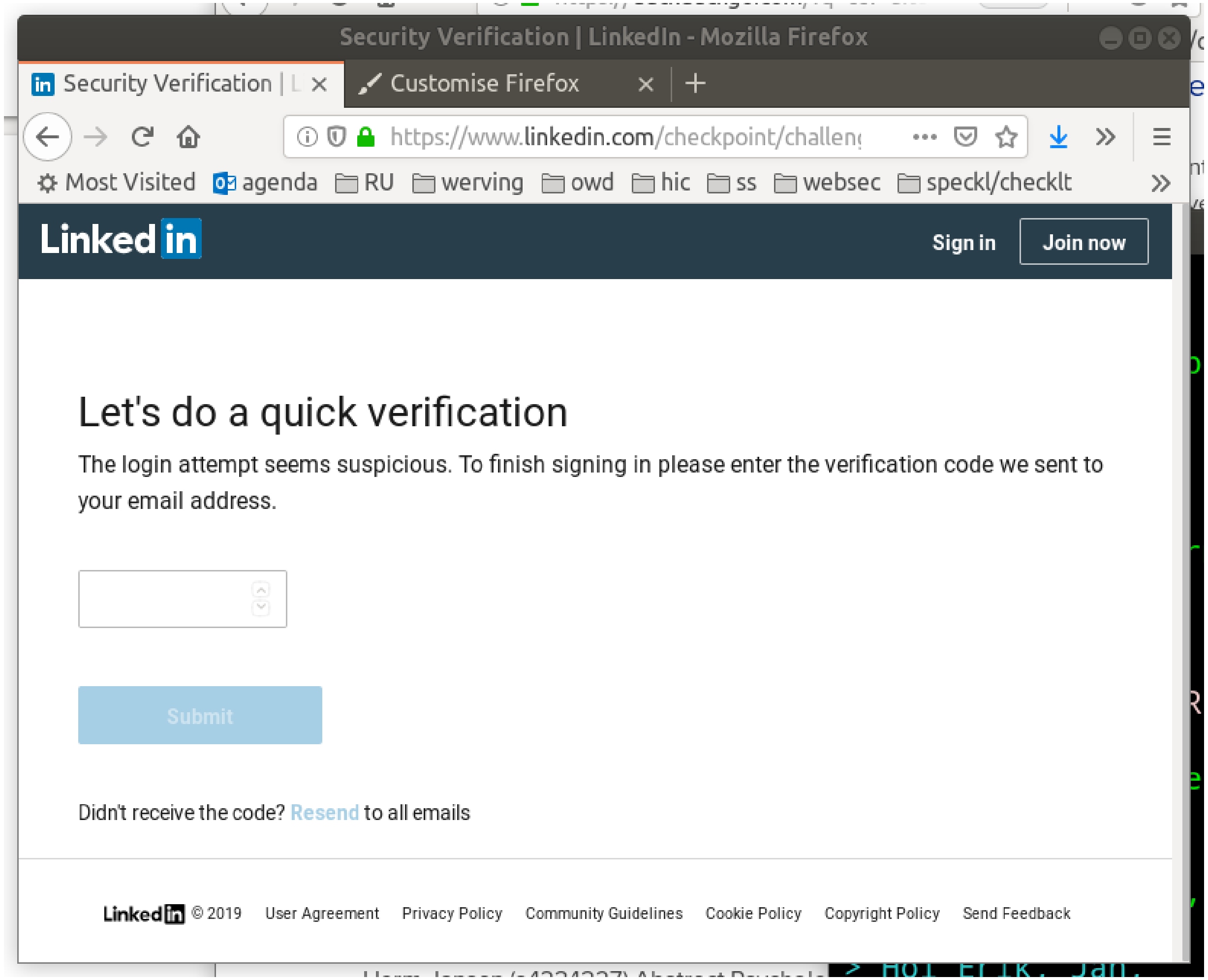


Reaction (incl. prosecution) is even harder

- How to find the person responsible,
  somewhere on the internet?

Trend in cyber security in recent years:
more attention to detection, instead of just prevention

Example detection of suspicious behaviour



Security Verification | LinkedIn - Mozilla Firefox
Security Verification | L
Customise Firefox
https://www.linkedin.com/checkpoint/challen
Most Visited
agenda
RU
werving
owd
hic
ss
websec
speckl/checklt
Linked in
Sign in
Join now

Let's do a quick verification

The login attempt seems suspicious. To finish signing in please enter the verification code we sent to your email address.

Submit

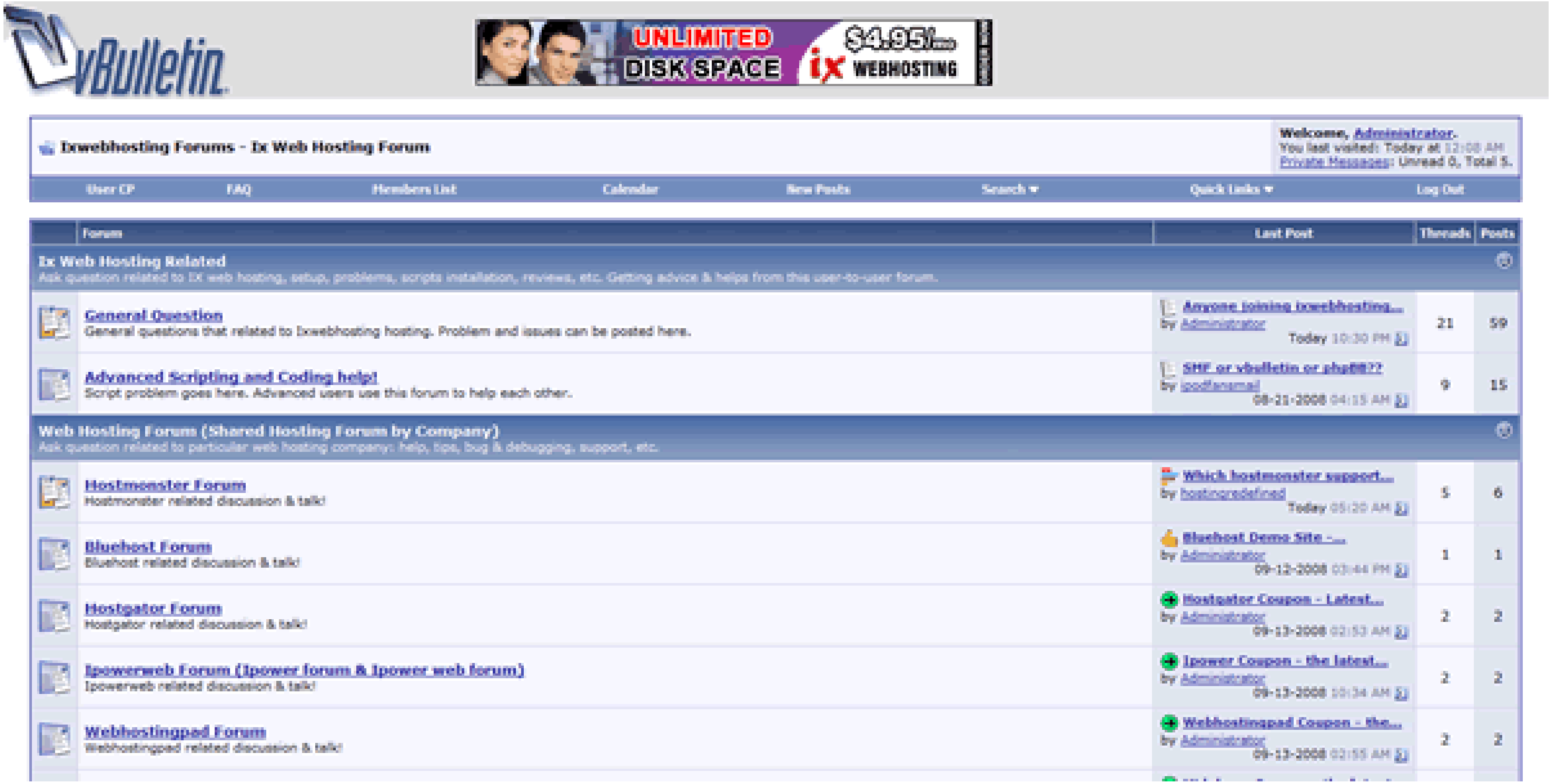
Didn't receive the code? Resend to all emails

Why is

“is this web application secure?”

a meaningless question to ask?

Security requirements of some web forum?



Ixwebhosting Forums - Ix Web Hosting Forum

Welcome, Administrator.
You last visited: Today at 12:08 AM
Private Messages: Unread 0, Total 5.

Forum	Last Post	Threads	Posts
Ix Web Hosting Related Ask question related to IX web hosting, setup, problems, scripts installation, reviews, etc. Getting advice & helps from this user-to-user forum.			
General Question General questions that related to Ixwebhosting hosting. Problem and issues can be posted here.	Anyone joining ixwebhosting... by Administrator Today 10:30 PM	21	59
Advanced Scripting and Coding help! Script problem goes here. Advanced users use this forum to help each other.	SMF or vbulletin or phpBB?? by ipodfansmal 08-21-2008 04:15 AM	9	15
Web Hosting Forum (Shared Hosting Forum by Company) Ask question related to particular web hosting company: help, tips, bug & debugging, support, etc.			
Hostmonster Forum Hostmonster related discussion & talk!	Which hostmonster support... by hostingredefined Today 05:20 AM	5	6
Bluehost Forum Bluehost related discussion & talk!	Bluehost Demo Site -... by Administrator 09-12-2008 03:44 PM	1	1
Hostgator Forum Hostgator related discussion & talk!	Hostgator Coupon - Latest... by Administrator 09-13-2008 02:53 AM	2	2
Ipowerweb Forum (Ipower forum & Ipower web forum) Ipowerweb related discussion & talk!	Ipower Coupon - the latest... by Administrator 09-13-2008 10:34 AM	2	2
Webhostingpad Forum Webhostingpad related discussion & talk!	Webhostingpad Coupon - the... by Administrator 09-13-2008 02:55 AM	2	2

Security requirements of some web forum

That depends! Is it a forum to discuss

- terrorist plots
- criminal plans
- embarrassing diseases
- how to secure websites
- solutions of homework assignments?

Even if there are no important security requirements for a web forum,
then

- username/passwords might still be valuable,
  as people will reuse these for more valuable sites
- the machine hosting the web forum might be interesting for an attacker to highjack

Saying “... is secure” only meaningful given

1. the security requirements
   for the assets of the system, and
2. an attacker model
   describing capabilities & resources and motives of the attacker

In other words,

1. What does it mean for the system to be secure?
2. Against what & whom is the system meant to be secure?

Leaving these aspects implicit is a common mistake!

What does it mean to be secure?

- What are the **security objectives/requirements**?

  eg. confidentiality, integrity, availability, authentication, authorisation, logging,...
- What are the **assets** we are trying to secure?

  incl. data, services (functionality), but also reputation, and other assets on same machine, ...
- Who are the parties involved? ie. the **stakeholders**

Often attacker goals are often in one-to-one correspondence with security requirements:

an attacker goal is the opposite of a security requirement

Thinking about it from both sides, both from attacker & defender perspective, makes it less likely you overlook things.

Security requirements: CIA

- Confidentiality
  - of traffic
  - of credentials (cookies, uname/passwords, credit card no’s)
  - privacy & anonymity
- Integrity
  - of website
    - eg broken by website defacement
    - but also
  - of user actions and their intent (eg broken by CSRF, XSS,...)
  - of logs
  - ...
- Availability
  - resisting DoS attacks on website as a whole
  - flooding topics with so much data to make it unusable
  - not just availability of the website, but also the machine hosting the website

The attacker

The attacker

Attacker model aka threat model

1. what kind of attackers?
2. what are their capabilities & resources?
3. what is the attack vector used?
4. what is their **motivation**?

Attacker models & attack vectors

- Phishing
- Network eavesdropper
- Malicious website
- Malicious content on a webpage
  - via 3rd party content or via XSS
- Malicious user

- Man-in-the-Middle attacks
  - by network eavesdropper, malicious website, …
- Endpoint attacks
  - eg Man-in-the-Browser attack
    - attacker in (partial or full) control of the browser
    - via XSS, browser plugin, bugs in the browser, …
- Attacker in control of the underlying OS
  - computer compromised by malware

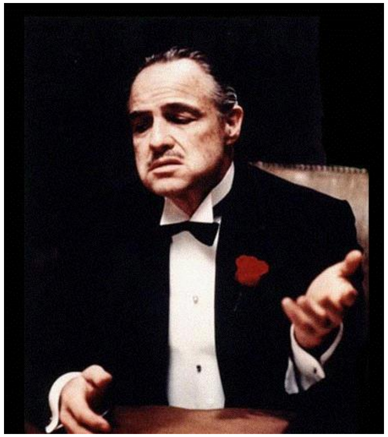
Types of attackers

- hobbyists and script kiddies

  motive: vandalism, fun, kudos (glorie & roem)

- **criminals**

  motive: profit



- hacktivists

- terrorists

- **nation states**

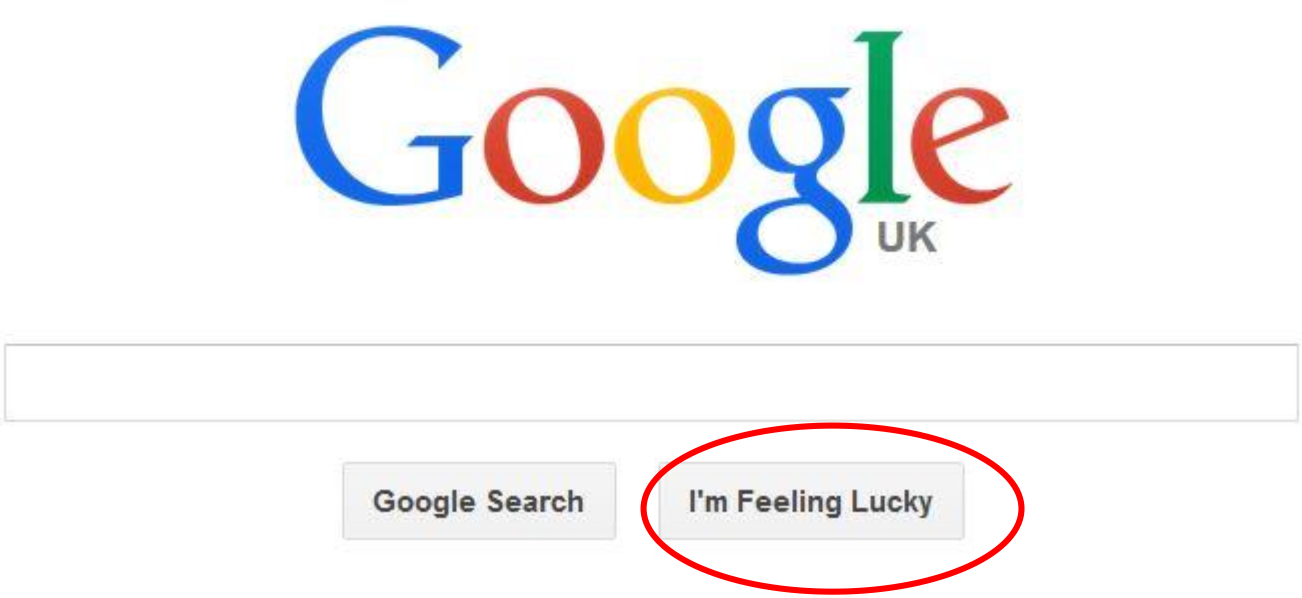
Types of attackers: trackers

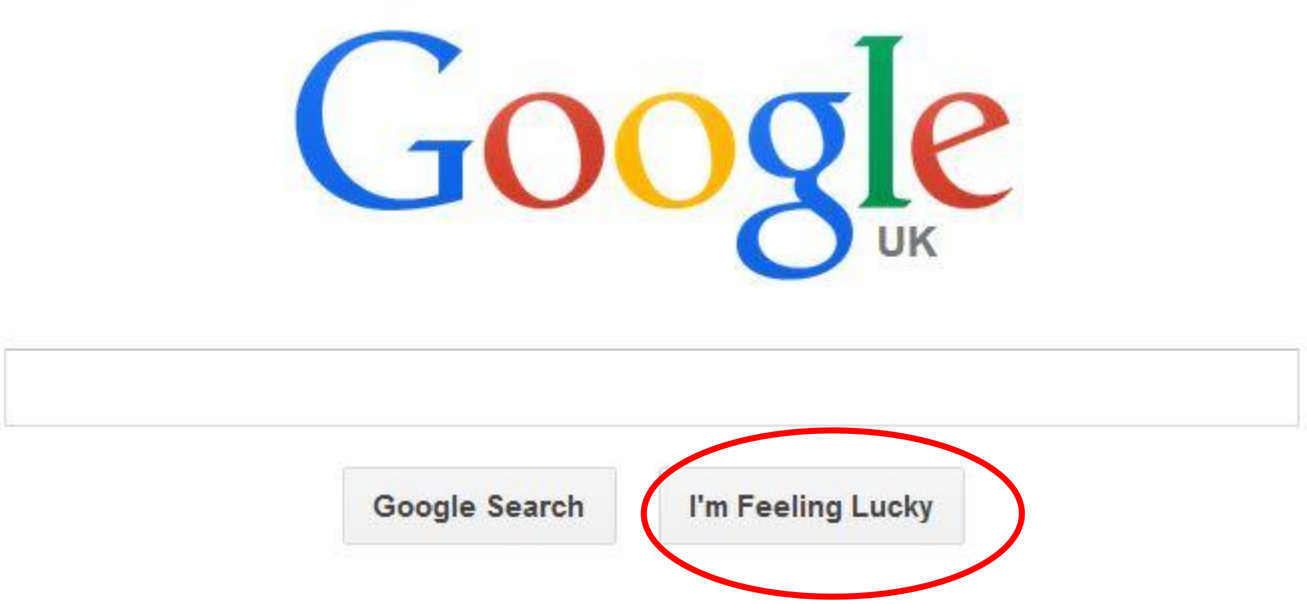
- Business models of Google, Facebook, Microsoft, … all these advertising networks, all providers of ‘free’ apps & online services, are centred around collecting personal information & serving advertisements.

- So strong economic/market forces in favour of facilitating tracking.

- Last week we discussed: ***how** are you being tracked?*
- The more interesting question may be: ***why** are you being tracked?*

Google
UK
Google Search
I'm Feeling Lucky

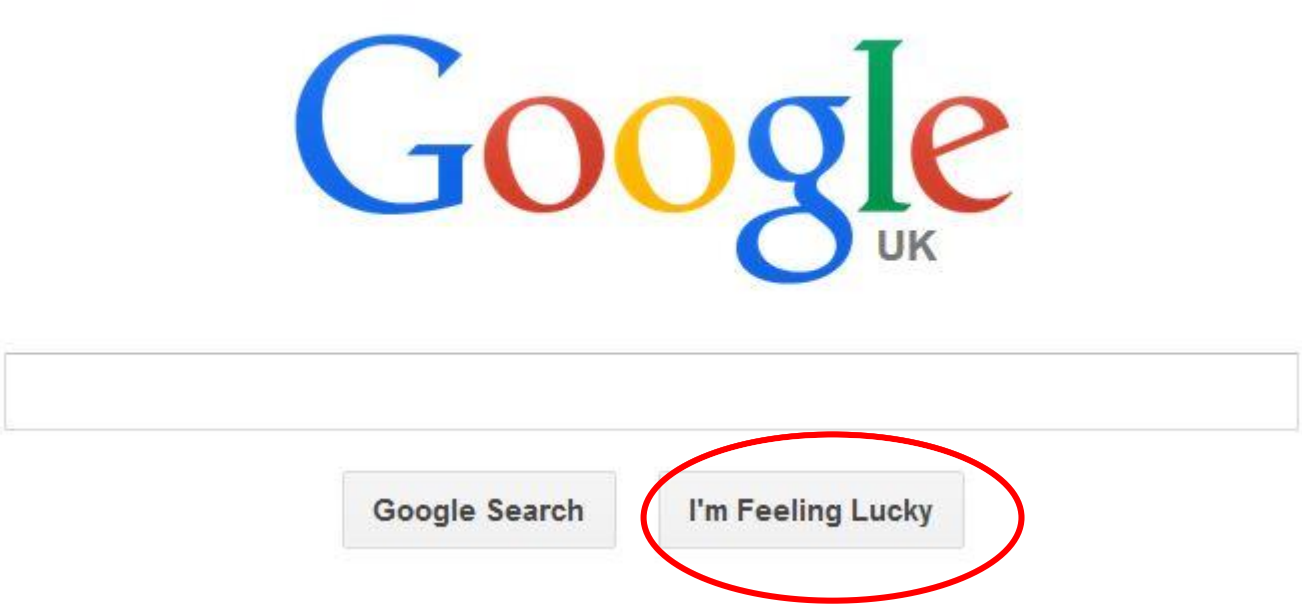

Google
UK
Google Search
I'm Feeling Lucky



I’m feeling lucky

means

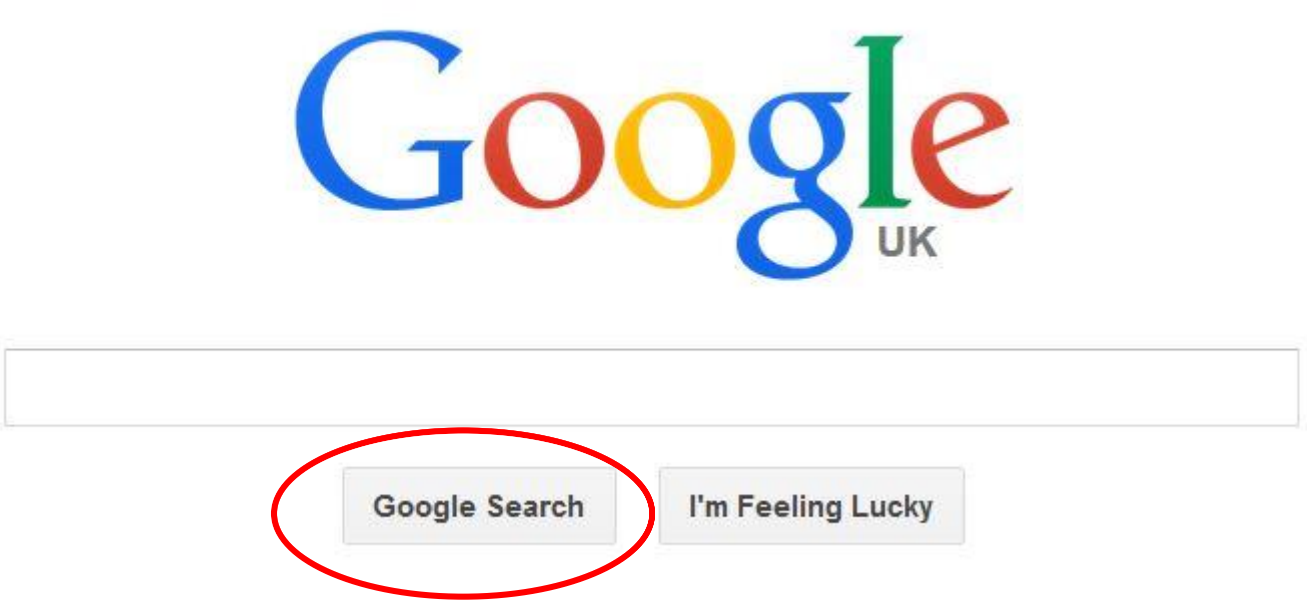
I trust Google to decide what is best for me ?



I’m feeling lucky

means

I trust Google to decide what is best for Google’s shareholders and advertisers?



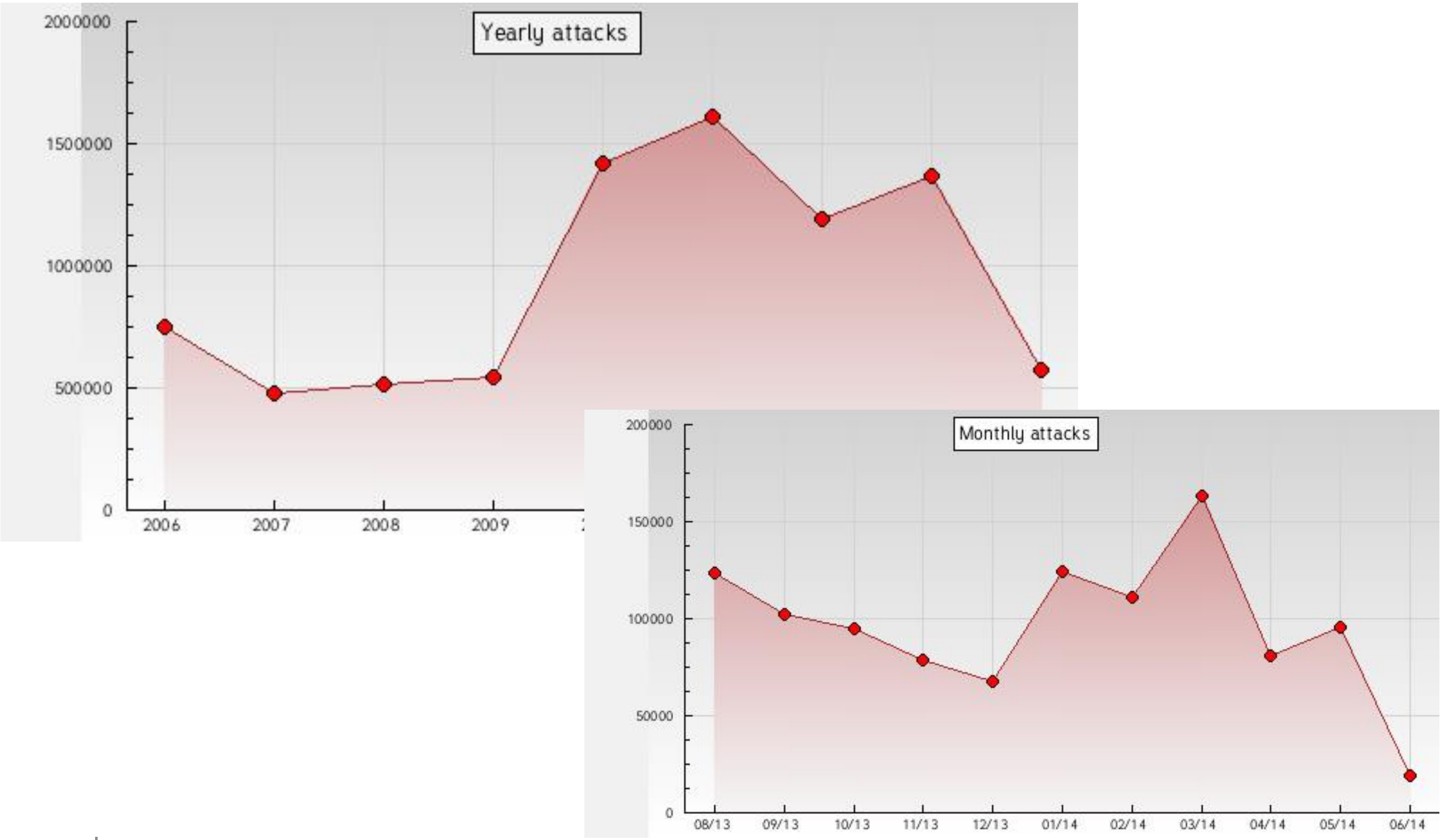
also means

I trust Google to decide what is best for Google’s shareholders and advertisers?

Sample attacks
&
some attack trends

Online vandalism – web site defacement

www.zone-h.org/archive monitors and archives web site defacements typically >100,000 sites per month



Cyber criminals

Central challenge of the *professional* cyber criminal:

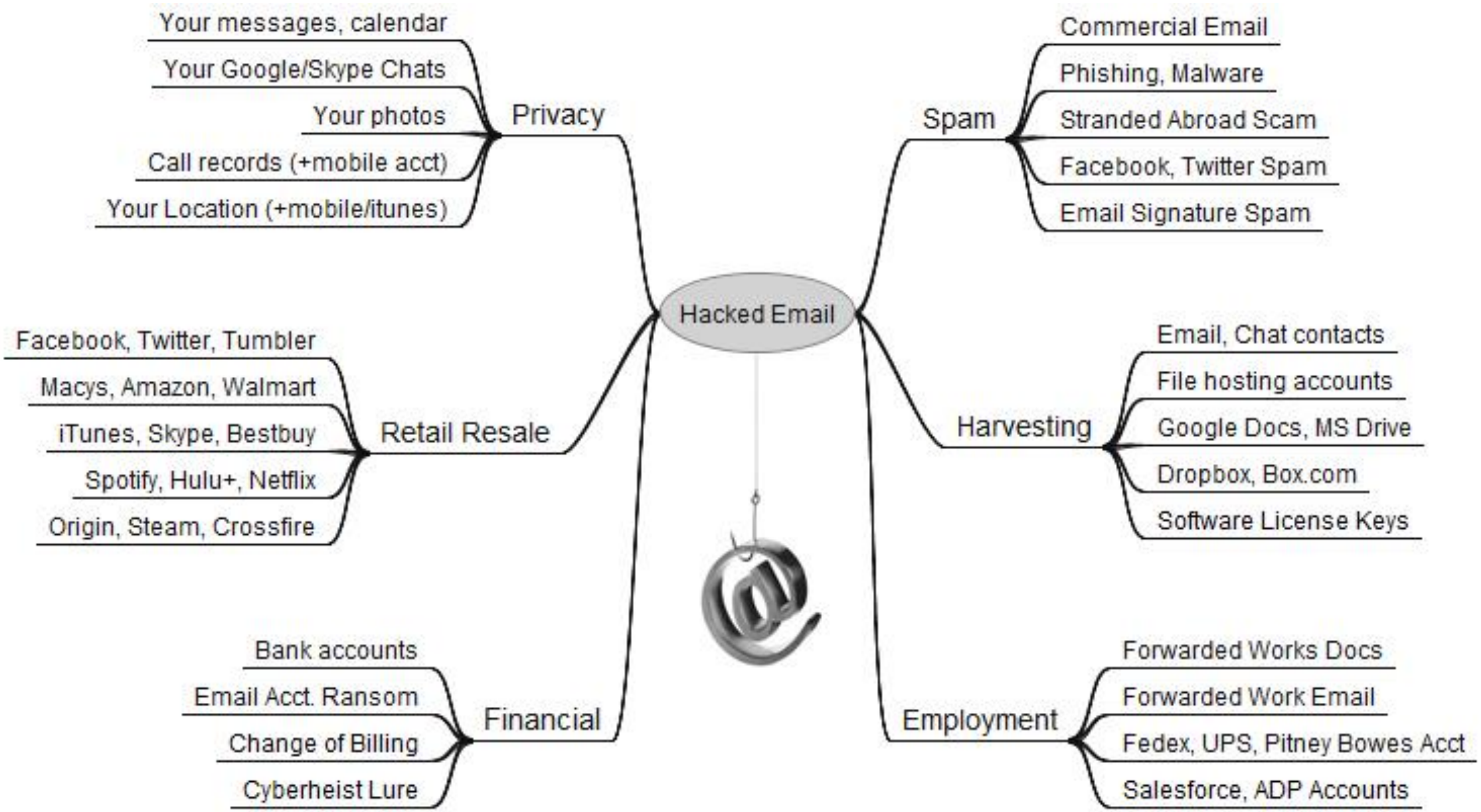
monetisation, ie making some money

What are the best (criminal) ***business models*** *for this?*

Does this business model ***scale****?*

- getting money from the end user (or his bank):
  - by using stolen credit card information, paypal accounts, internet banking, or fake web shops
  - scareware & ransomware
- selling services or data to other non-criminals
  - selling copyrighted material, stolen goods, counterfeit drugs, ...
- selling services or data to other cyber criminals
  - advertising (eg on compromised website)
  - click jacking, like jacking,... to improve ratings and traffic
  - selling DDoS attacks
    - eg to gamers to knock opponents offline

The Value of a Hacked Email Account

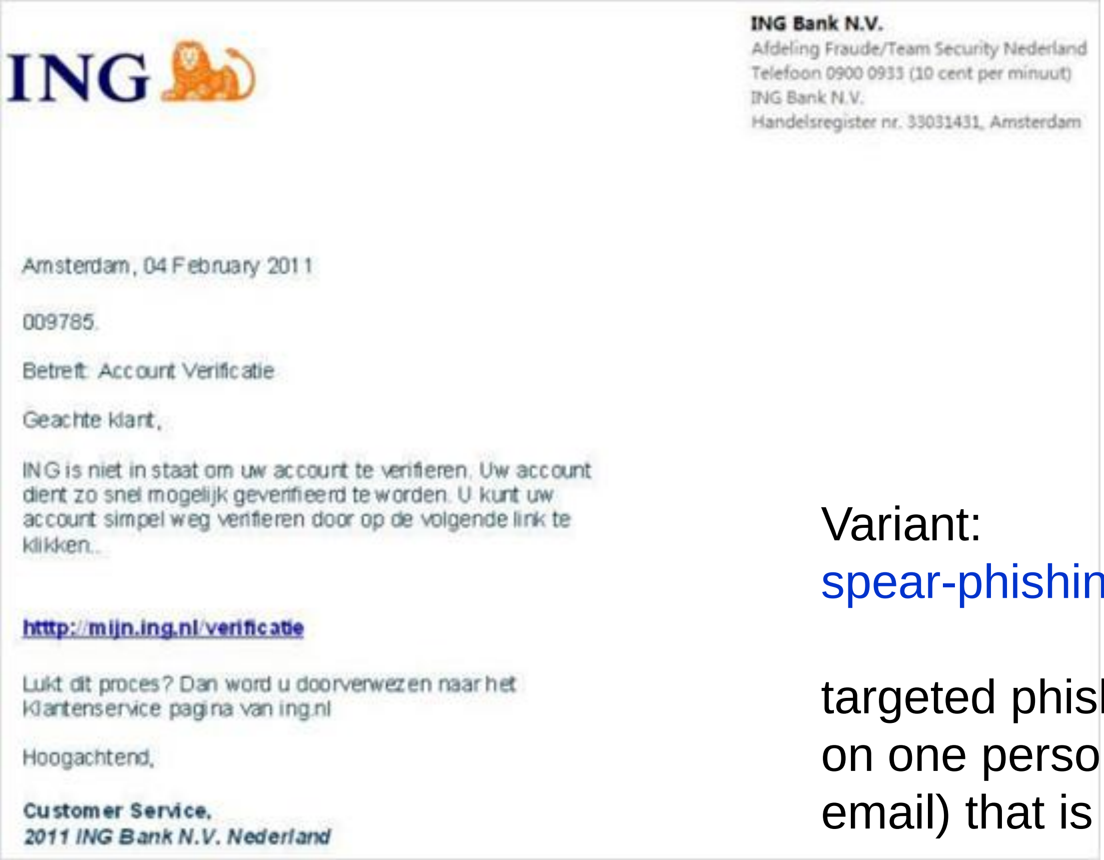


Hacked Email

- Privacy
  - Your messages, calendar
  - Your Google/Skype Chats
  - Your photos
  - Call records (+mobile acct)
  - Your Location (+mobile/itunes)
- Retail Resale
  - Facebook, Twitter, Tumbler
  - Macys, Amazon, Walmart
  - iTunes, Skype, Bestbuy
  - Spotify, Hulu+, Netflix
  - Origin, Steam, Crossfire
- Financial
  - Bank accounts
  - Email Acct. Ransom
  - Change of Billing
  - Cyberheist Lure
- Spam
  - Commercial Email
  - Phishing, Malware
  - Stranded Abroad Scam
  - Facebook, Twitter Spam
  - Email Signature Spam
- Harvesting
  - Email, Chat contacts
  - File hosting accounts
  - Google Docs, MS Drive
  - Dropbox, Box.com
  - Software License Keys
- Employment
  - Forwarded Works Docs
  - Forwarded Work Email
  - Fedex, UPS, Pitney Bowes Acct
  - Salesforce, ADP Accounts

https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Phishing



ING

ING Bank N.V.
Afdeling Fraude/Team Security Nederland
Telefoon 0900 0933 (10 cent per minuut)
ING Bank N.V.
Handelsregister nr. 33031431, Amsterdam

Amsterdam, 04 February 2011

009785.

Betreft Account Verificatie

Geachte klant,

ING is niet in staat om uw account te verifieren. Uw account dient zo snel mogelijk geverifieerd te worden. U kunt uw account simpel weg verifieren door op de volgende link te klikken..

htttp://mijn.ing.nl/verificatie

Lukt dit proces? Dan word u doorverwezen naar het Klantenservice pagina van ing.nl

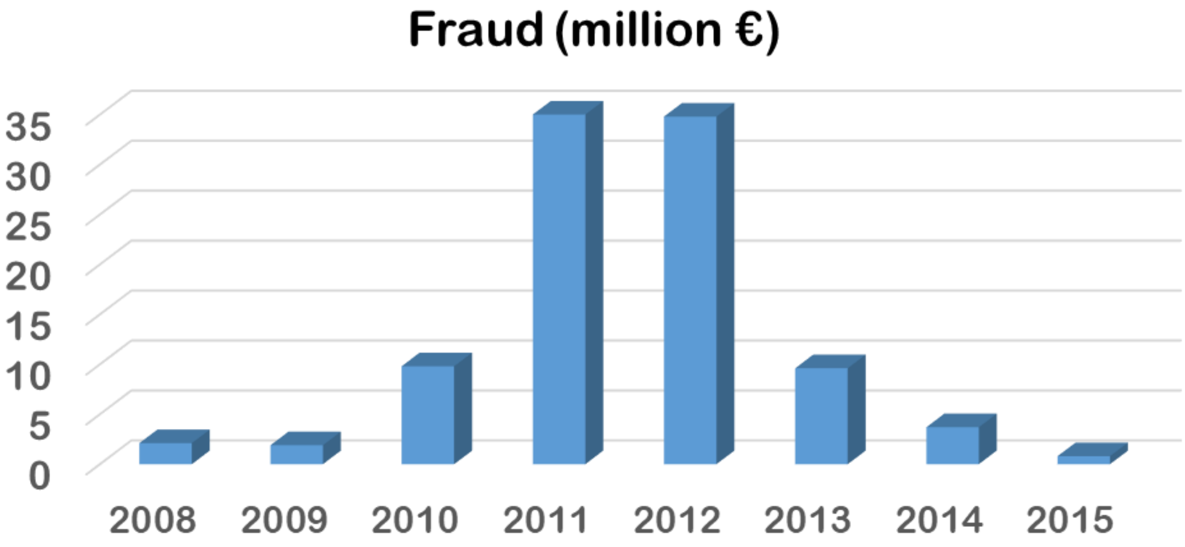
Hoogachtend,

Customer Service,
2011 ING Bank N.V. Nederland

Variant:
spear-phishing aka whaling:

targeted phishing attack
on one person (with personalised email) that is very rich (a whale)

Internet banking fraud in the Netherlands



by eg
infected computers, fake websites, or by phone

[Source: Betaalvereniging]

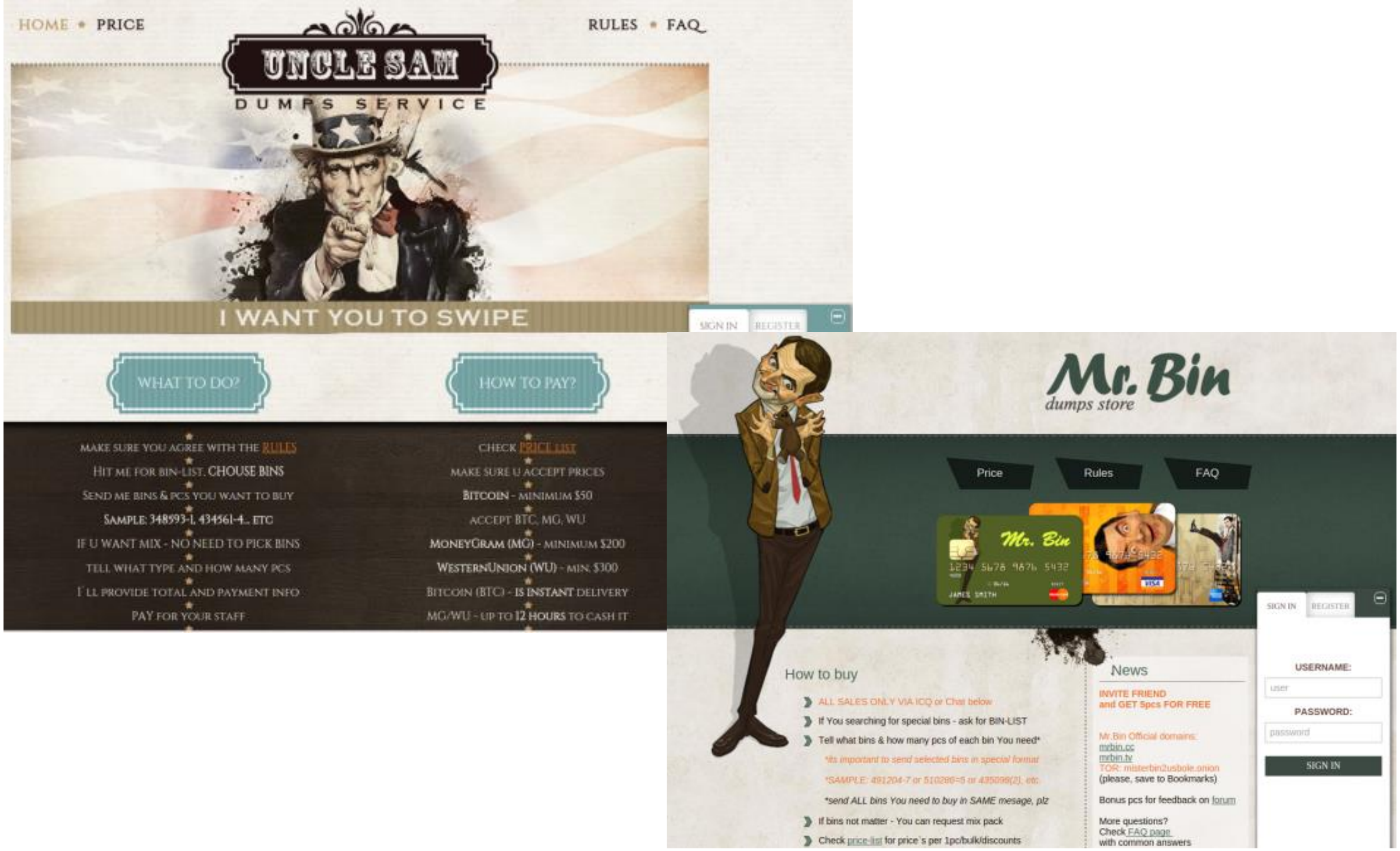
Serious organised crime, not clever teenagers

Improved countermeasures of banks:

- *better detection & reaction of fraud*
- *prevention & detection of money mules*
  Recruiting money mules is bottleneck for the criminal: labour-intensive work
- Also, maybe criminals now prefer to focus on ransomware instead?

Carding sites

for trading dumps of stolen credit cards & magstripe data



MAKE SURE YOU AGREE WITH THE RULES
HIT ME FOR BIN-LIST. CHOUSE BINS
SEND ME BINS & PCS YOU WANT TO BUY
SAMPLE: 348593-1, 434561-4... ETC
IF U WANT MIX - NO NEED TO PICK BINS
TELL WHAT TYPE AND HOW MANY PCS
I`LL PROVIDE TOTAL AND PAYMENT INFO
PAY FOR YOUR STAFF

CHECK PRICE LIST
MAKE SURE U ACCEPT PRICES
BITCOIN - MINIMUM $50
ACCEPT BTC, MG, WU
MONEYGRAM (MG) - MINIMUM $200
WESTERNUNION (WU) - MIN. $300
BITCOIN (BTC) - IS INSTANT DELIVERY
MG/WU - UP TO 12 HOURS TO CASH IT

How to buy

- ALL SALES ONLY VIA ICQ or Chat below
- If You searching for special bins - ask for BIN-LIST
- Tell what bins & how many pcs of each bin You need*

  *its important to send selected bins in special format

  *SAMPLE: 491204-7 or 510280=5 or 435098(2), etc

  *send ALL bins You need to buy in SAME mesage, plz
- If bins not matter - You can request mix pack
- Check price-list for price`s per 1pc/bulk/discounts

News

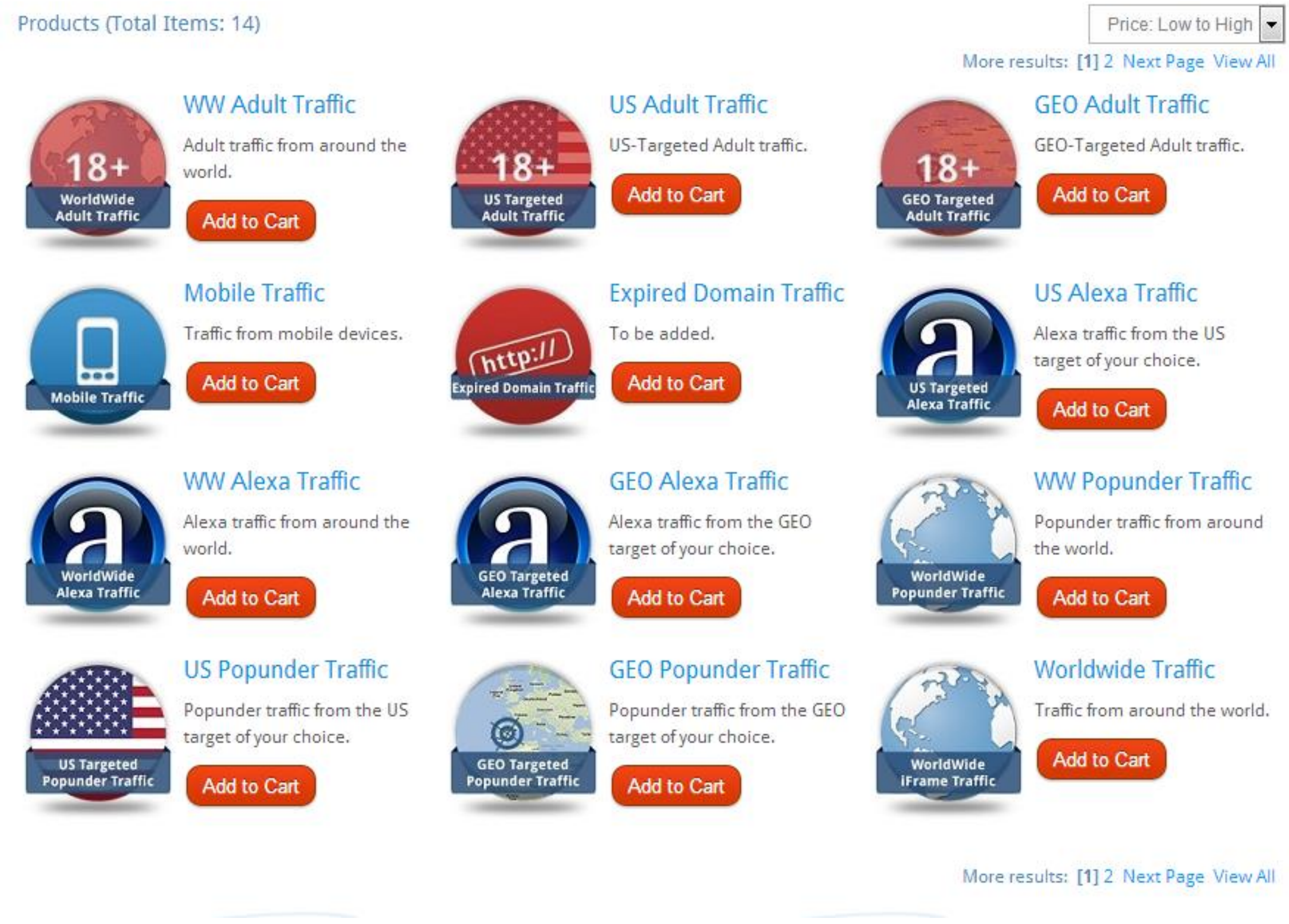
INVITE FRIEND
and GET 5pcs FOR FREE

Mr.Bin Official domains:
mrbin.cc
mrbin.tv
TOR: misterbin2usbole.onion
(please, save to Bookmarks)

Bonus pcs for feedback on forum

More questions?
Check FAQ page
with common answers

Criminal business models: selling traffic or clicks



Products (Total Items: 14)

Price: Low to High

More results: [1] 2 Next Page View All

WW Adult Traffic

Adult traffic from around the world.

US Adult Traffic

US-Targeted Adult traffic.

GEO Adult Traffic

GEO-Targeted Adult traffic.

Mobile Traffic

Traffic from mobile devices.

Expired Domain Traffic

To be added.

US Alexa Traffic

Alexa traffic from the US target of your choice.

WW Alexa Traffic

Alexa traffic from around the world.

GEO Alexa Traffic

Alexa traffic from the GEO target of your choice.

WW Popunder Traffic

Popunder traffic from around the world.

US Popunder Traffic

Popunder traffic from the US target of your choice.

GEO Popunder Traffic

Popunder traffic from the GEO target of your choice.

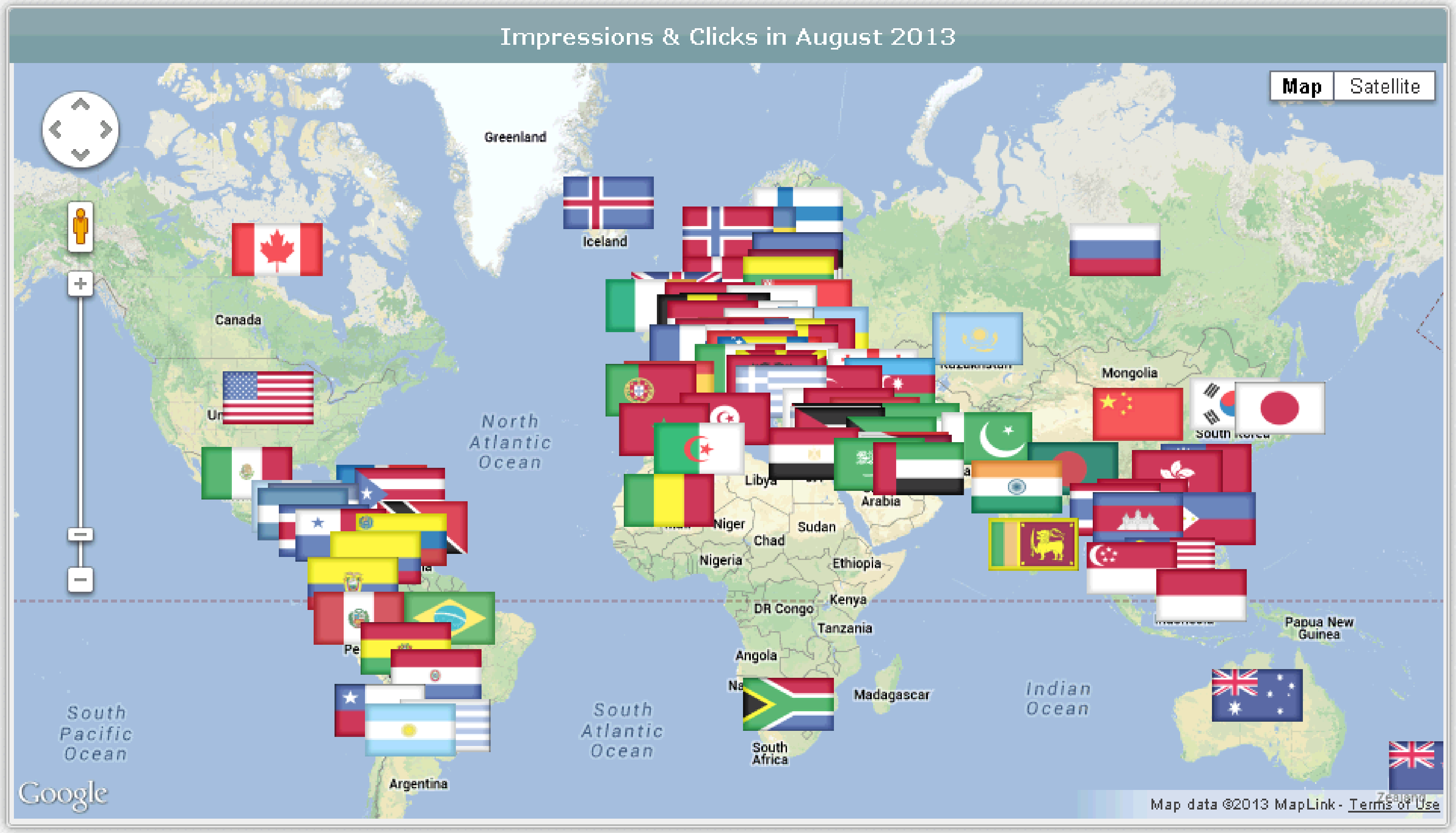
Worldwide Traffic

Traffic from around the world.

More results: [1] 2 Next Page View All

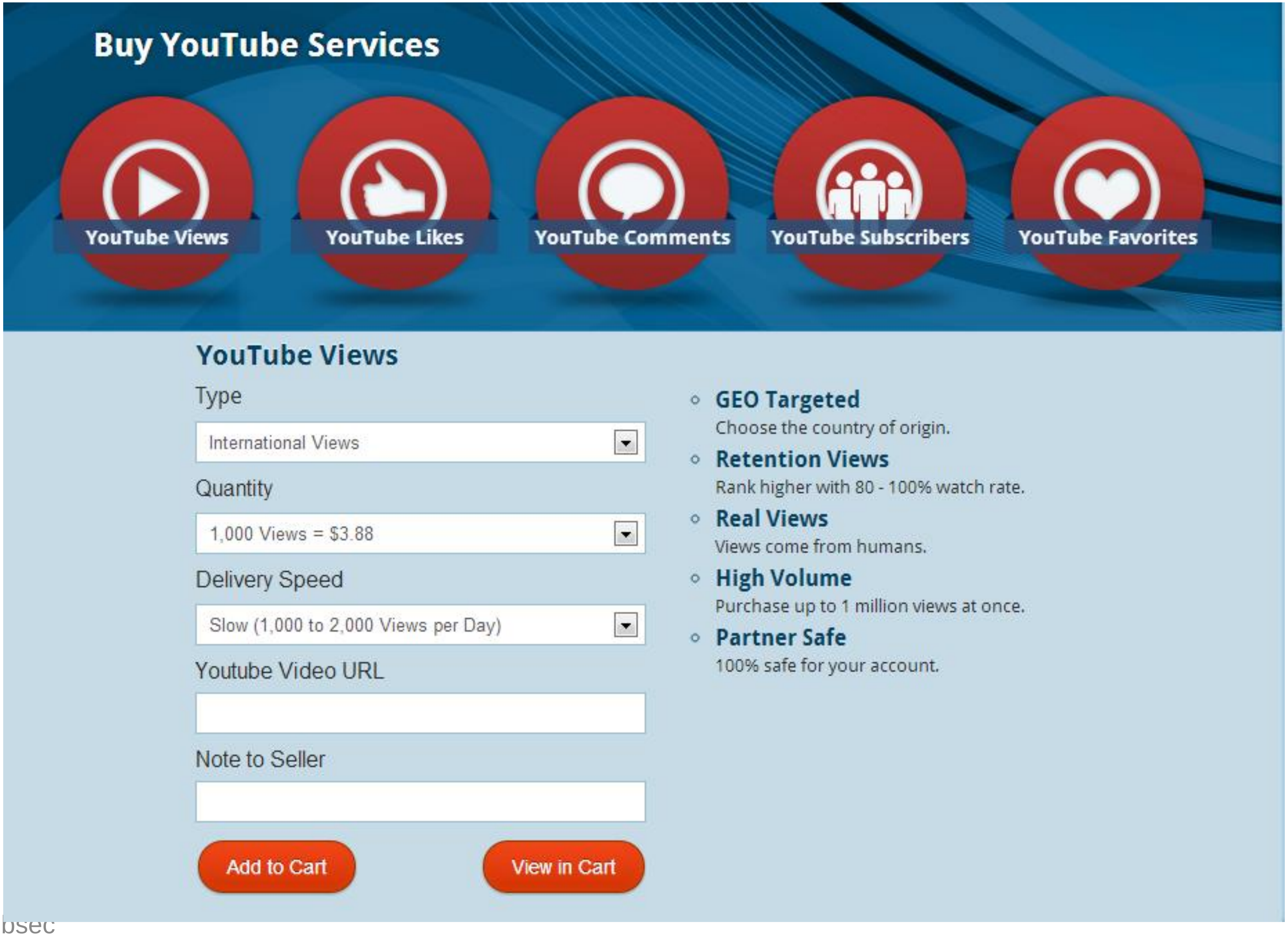
18+
WorldWide Adult Traffic
18+
US Targeted Adult Traffic
18+
GEO Targeted Adult Traffic
Mobile Traffic
http://
Expired Domain Traffic
a
US Targeted Alexa Traffic
a
WorldWide Alexa Traffic
a
GEO Targeted Alexa Traffic
WorldWide Popunder Traffic
US Targeted Popunder Traffic
GEO Targeted Popunder Traffic
WorldWide iFrame Traffic
Add to Cart

Criminal business models: selling traffic or clicks



Impressions & Clicks in August 2013

Criminal business models: YouTube views



YouTube Views

Type: International Views

Quantity: 1,000 Views = $3.88

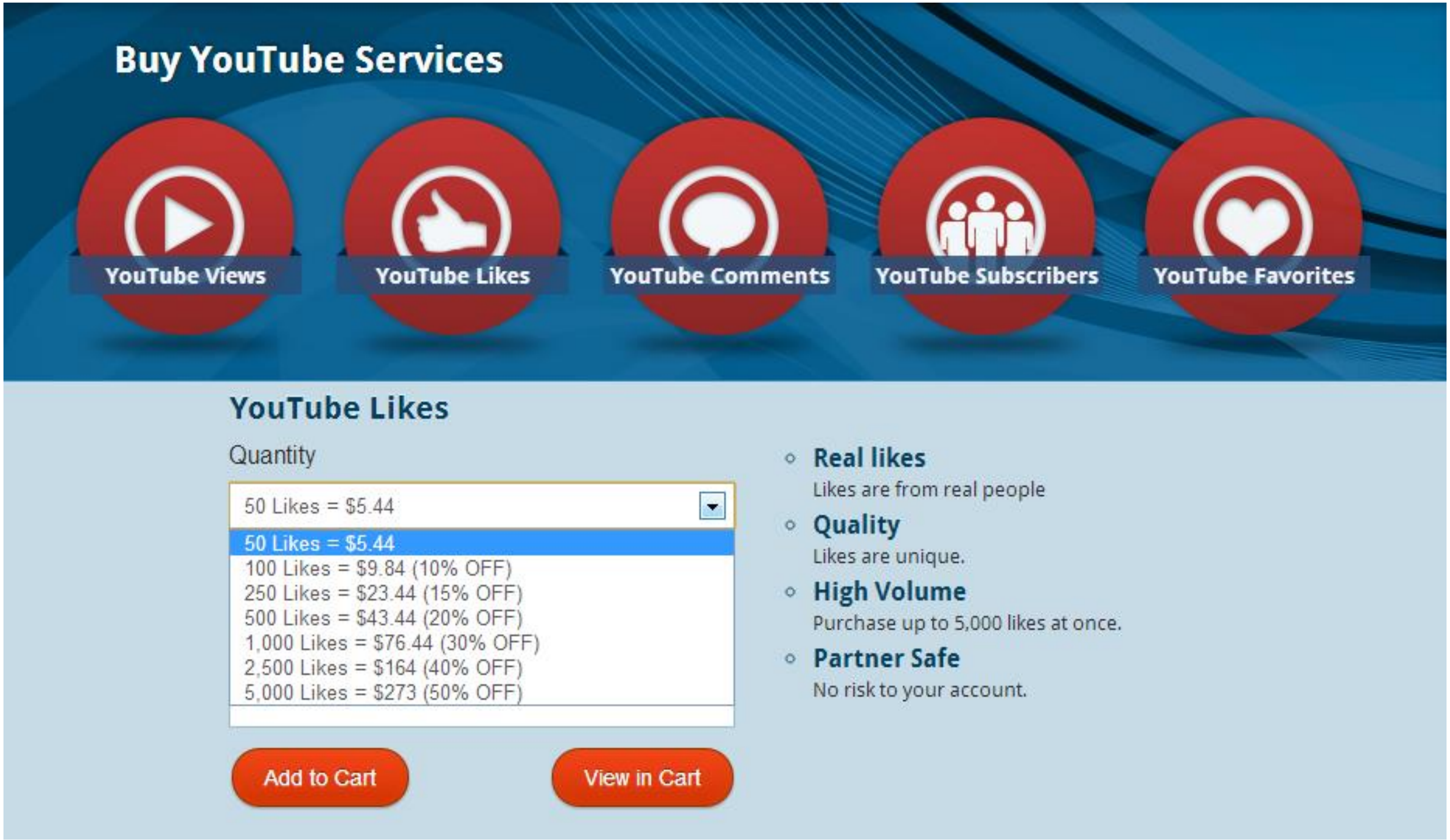
Delivery Speed: Slow (1,000 to 2,000 Views per Day)

Youtube Video URL:

Note to Seller:

- **GEO Targeted**
  Choose the country of origin.
- **Retention Views**
  Rank higher with 80 - 100% watch rate.
- **Real Views**
  Views come from humans.
- **High Volume**
  Purchase up to 1 million views at once.
- **Partner Safe**
  100% safe for your account.

Criminal business models: YouTube likes



Buy YouTube Services

YouTube Likes

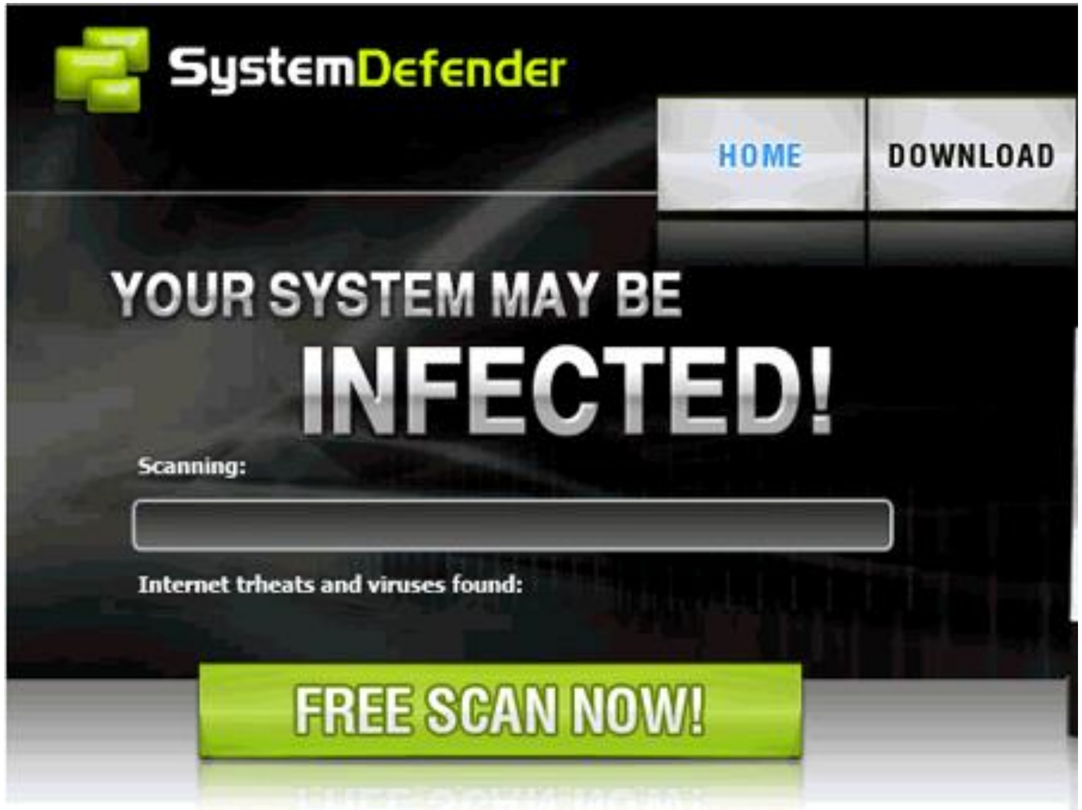
Quantity

50 Likes = $5.44

- 50 Likes = $5.44
- 100 Likes = $9.84 (10% OFF)
- 250 Likes = $23.44 (15% OFF)
- 500 Likes = $43.44 (20% OFF)
- 1,000 Likes = $76.44 (30% OFF)
- 2,500 Likes = $164 (40% OFF)
- 5,000 Likes = $273 (50% OFF)

- **Real likes**
  Likes are from real people
- **Quality**
  Likes are unique.
- **High Volume**
  Purchase up to 5,000 likes at once.
- **Partner Safe**
  No risk to your account.

Scareware



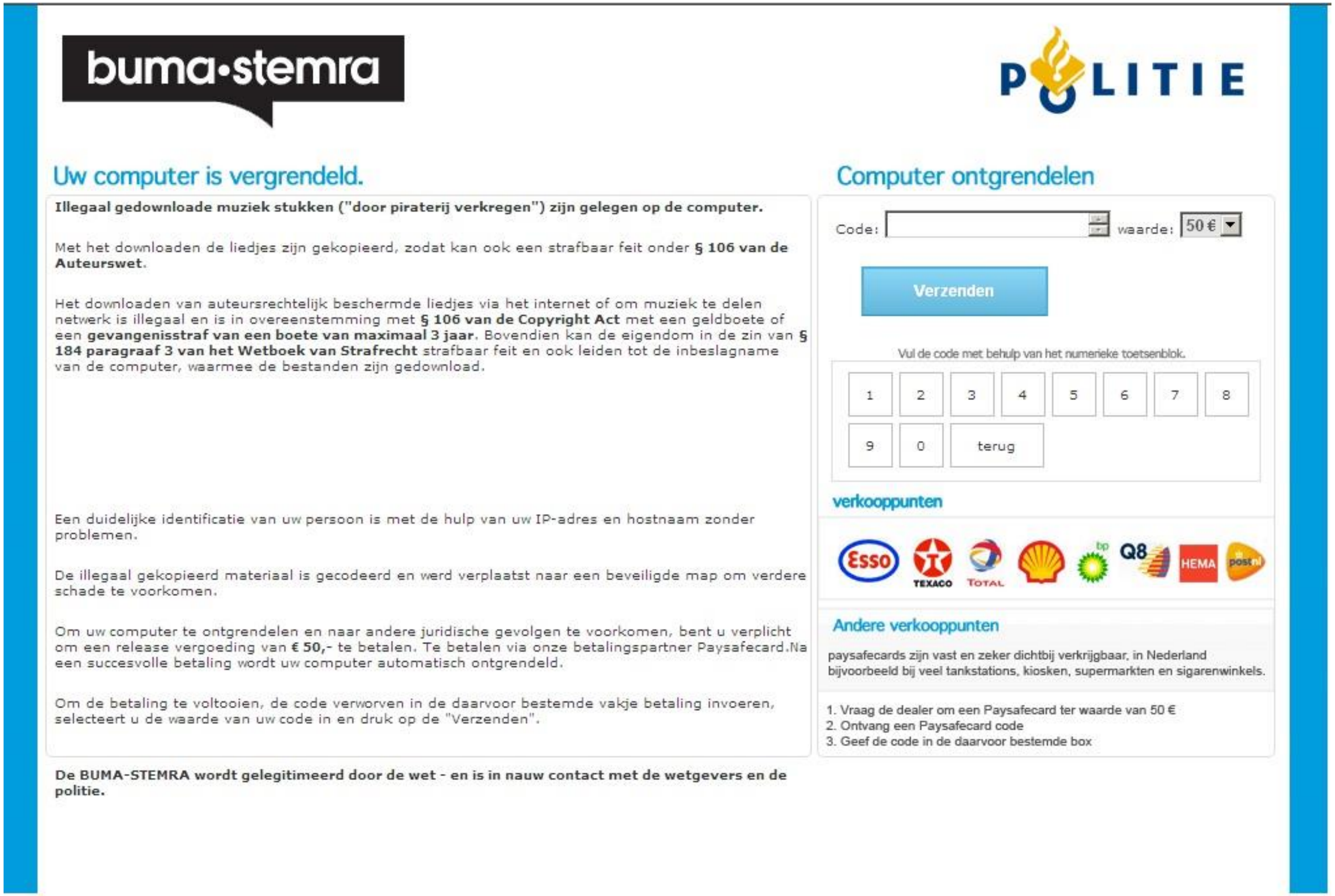
YOUR SYSTEM MAY BE INFECTED!

Scanning:

Internet trheats and viruses found:

of course, the “free scan” will install malware

Ransomware



Uw computer is vergrendeld.

Illegaal gedownloade muziek stukken ("door piraterij verkregen") zijn gelegen op de computer.

Met het downloaden de liedjes zijn gekopieerd, zodat kan ook een strafbaar feit onder **§ 106 van de Auteurswet**.

Het downloaden van auteursrechtelijk beschermde liedjes via het internet of om muziek te delen netwerk is illegaal en is in overeenstemming met **§ 106 van de Copyright Act** met een geldboete of een **gevangenisstraf van een boete van maximaal 3 jaar**. Bovendien kan de eigendom in de zin van **§ 184 paragraaf 3 van het Wetboek van Strafrecht** strafbaar feit en ook leiden tot de inbeslagname van de computer, waarmee de bestanden zijn gedownload.

Een duidelijke identificatie van uw persoon is met de hulp van uw IP-adres en hostnaam zonder problemen.

De illegaal gekopieerd materiaal is gecodeerd en werd verplaatst naar een beveiligde map om verdere schade te voorkomen.

Om uw computer te ontgrendelen en naar andere juridische gevolgen te voorkomen, bent u verplicht om een release vergoeding van **€ 50,-** te betalen. Te betalen via onze betalingspartner Paysafecard.Na een succesvolle betaling wordt uw computer automatisch ontgrendeld.

Om de betaling te voltooien, de code verworven in de daarvoor bestemde vakje betaling invoeren, selecteert u de waarde van uw code in en druk op de "Verzenden".

De BUMA-STEMRA wordt gelegitimeerd door de wet - en is in nauw contact met de wetgevers en de politie.

Computer ontgrendelen

Code: waarde: 50 €

Vul de code met behulp van het numerieke toetsenblok.

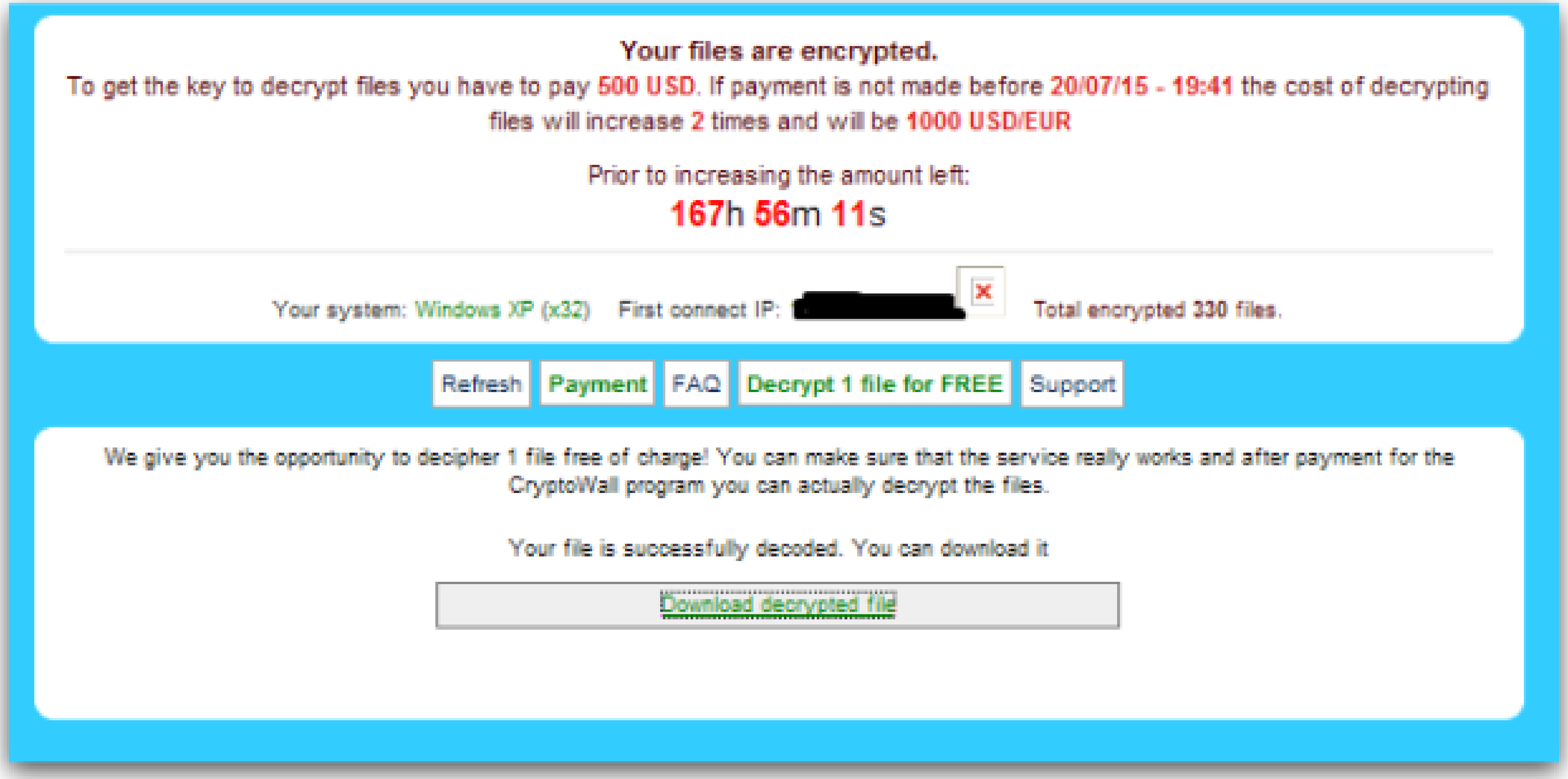
verkooppunten

Andere verkooppunten

paysafecards zijn vast en zeker dichtbij verkrijgbaar, in Nederland bijvoorbeeld bij veel tankstations, kiosken, supermarkten en sigarenwinkels.

1. Vraag de dealer om een Paysafecard ter waarde van 50 €
2. Ontvang een Paysafecard code
3. Geef de code in de daarvoor bestemde box

Ransomware: CryptoWall [2015]



Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 20/07/15 - 19:41 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR

Prior to increasing the amount left:

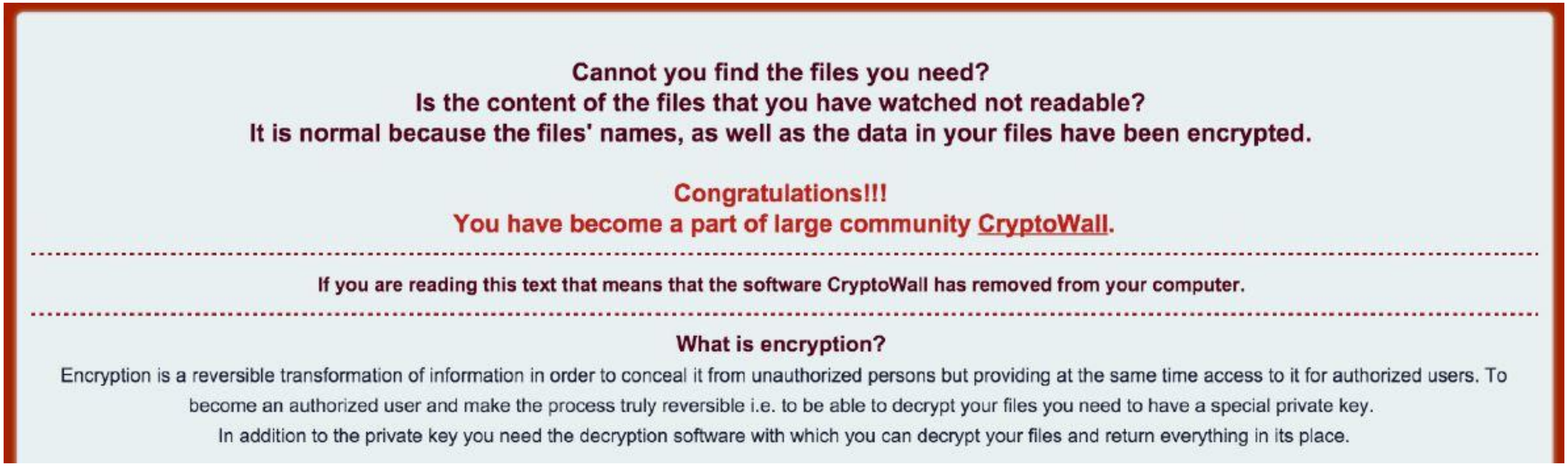
167h 56m 11s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 330 files.

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

Your file is successfully decoded. You can download it

Ransomware: CryptoWall



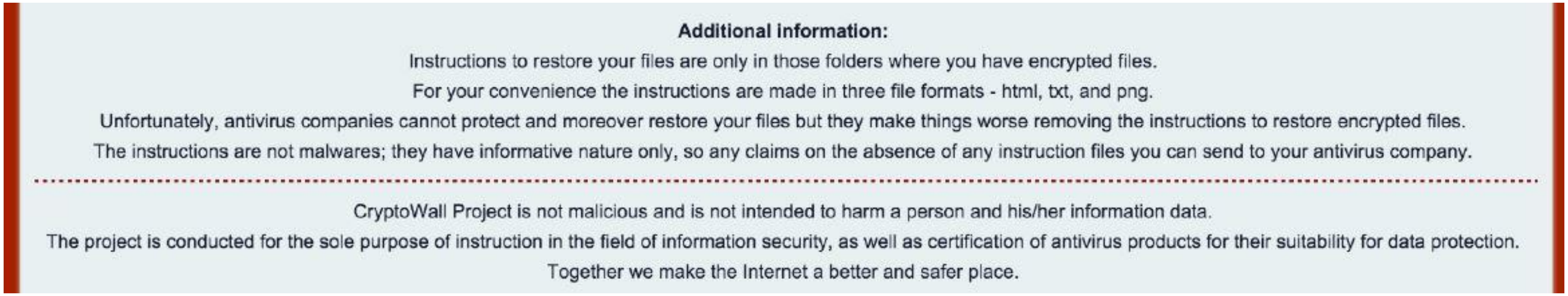
Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?

Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.



Additional information:

Instructions to restore your files are only in those folders where you have encrypted files.
For your convenience the instructions are made in three file formats - html, txt, and png.
Unfortunately, antivirus companies cannot protect and moreover restore your files but they make things worse removing the instructions to restore encrypted files.
The instructions are not malwares; they have informative nature only, so any claims on the absence of any instruction files you can send to your antivirus company.

CryptoWall Project is not malicious and is not intended to harm a person and his/her information data.
The project is conducted for the sole purpose of instruction in the field of information security, as well as certification of antivirus products for their suitability for data protection.
Together we make the Internet a better and safer place.

Ransomware

- Rapidly taken off since 2015
- *Why?*

  Why is it a better business model than attacking internet banking?:

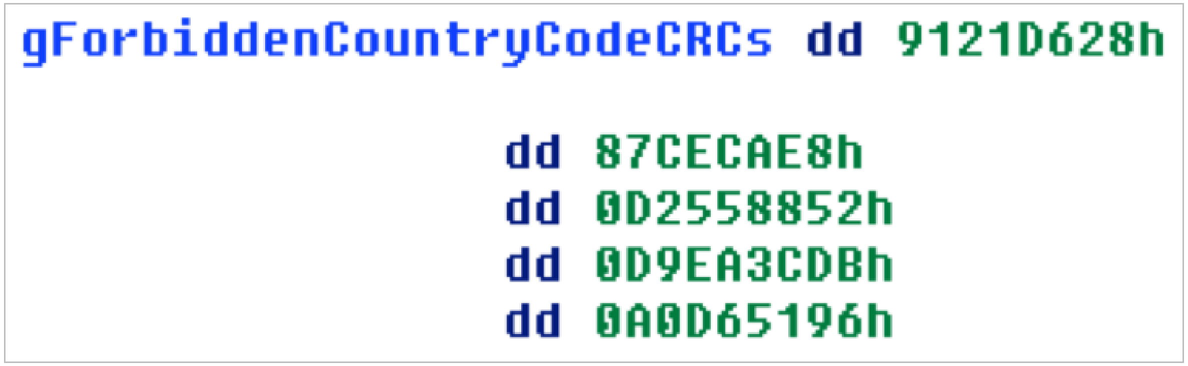
  Easier: easier to scale, with less effort

  - No need to recruit money mules
  - No hassle getting money out of the traceable banking system
  - Does not depend on particular bank, country, …
  - Eg Cryptowall3 collected +/- 300 Meuro in 2015
- *Do criminals give back the data after you pay?*

  What is the best business model for attackers here?

  - It’s in the criminals interests to release data after payment,
    - so that more people pay up, for a *trustworthy* criminal practice
- Scary thing: this business model can be applied to anything
  - eg your phone, your car, hospital, online shop, …

code snippet from CryptoWall ransomware



```
gForbiddenCountryCodeCRCs dd 9121D628h

                dd 87CECAE8h
                dd 0D2558852h
                dd 0D9EA3CDBh
                dd 0A0D65196h
```

CryptoWall

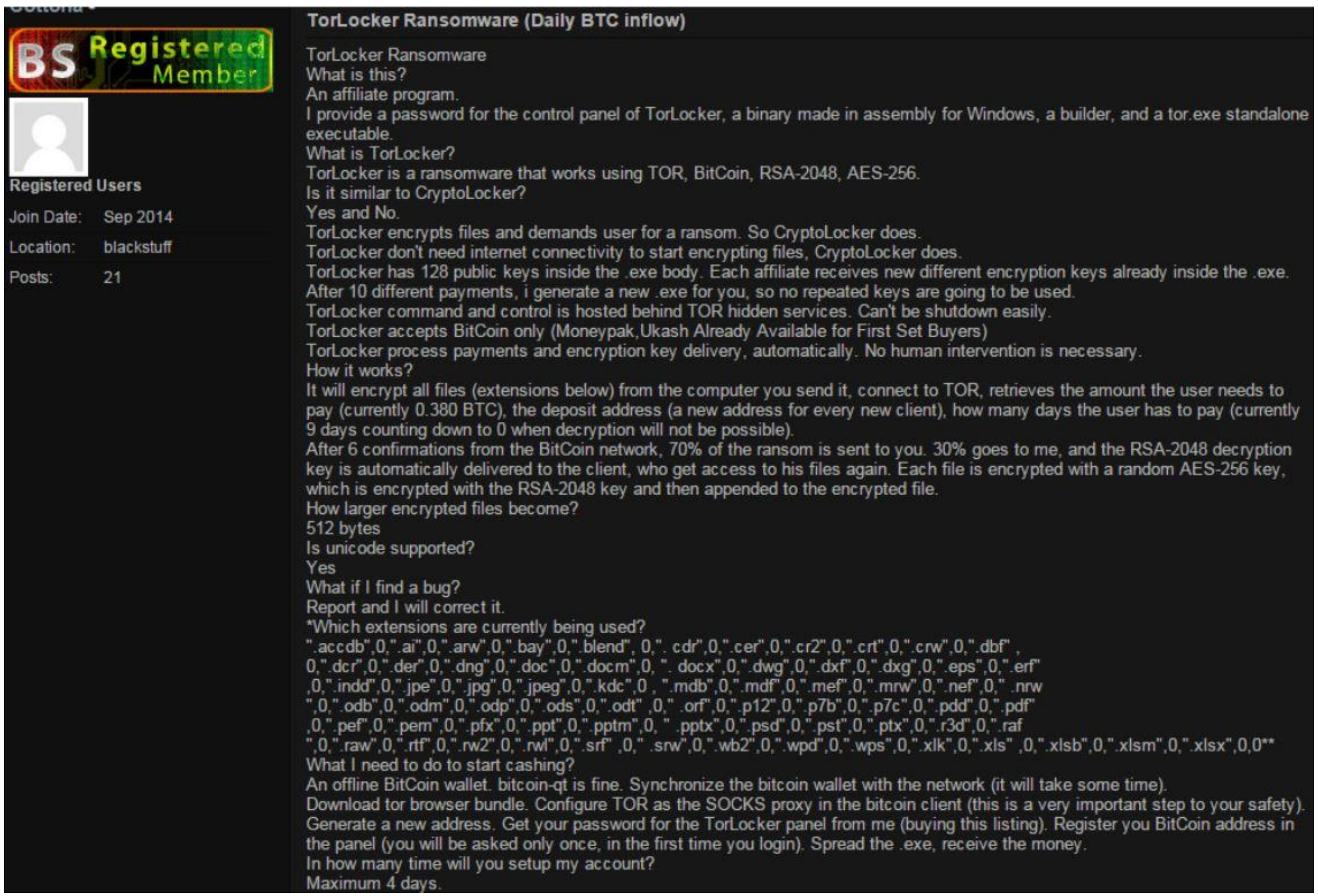
Exempted countries: Russia, Bellorussia, Kazachstan, Ukraine

- later also Armenia and Iran

Why?

Make sure you don’t become priority of your local police force

Ransomware-as-a-service



Registered Users

Join Date: Sep 2014

Location: blackstuff

Posts: 21

TorLocker Ransomware (Daily BTC inflow)

TorLocker Ransomware
What is this?
An affiliate program.
I provide a password for the control panel of TorLocker, a binary made in assembly for Windows, a builder, and a tor.exe standalone executable.
What is TorLocker?
TorLocker is a ransomware that works using TOR, BitCoin, RSA-2048, AES-256.
Is it similar to CryptoLocker?
Yes and No.
TorLocker encrypts files and demands user for a ransom. So CryptoLocker does.
TorLocker don't need internet connectivity to start encrypting files, CryptoLocker does.
TorLocker has 128 public keys inside the .exe body. Each affiliate receives new different encryption keys already inside the .exe.
After 10 different payments, i generate a new .exe for you, so no repeated keys are going to be used.
TorLocker command and control is hosted behind TOR hidden services. Can't be shutdown easily.
TorLocker accepts BitCoin only (Moneypak,Ukash Already Available for First Set Buyers)
TorLocker process payments and encryption key delivery, automatically. No human intervention is necessary.
How it works?
It will encrypt all files (extensions below) from the computer you send it, connect to TOR, retrieves the amount the user needs to pay (currently 0.380 BTC), the deposit address (a new address for every new client), how many days the user has to pay (currently 9 days counting down to 0 when decryption will not be possible).
After 6 confirmations from the BitCoin network, 70% of the ransom is sent to you. 30% goes to me, and the RSA-2048 decryption key is automatically delivered to the client, who get access to his files again. Each file is encrypted with a random AES-256 key, which is encrypted with the RSA-2048 key and then appended to the encrypted file.
How larger encrypted files become?
512 bytes
Is unicode supported?
Yes
What if I find a bug?
Report and I will correct it.
*Which extensions are currently being used?
".accdb",0,".ai",0,".arw",0,".bay",0,".blend", 0,". cdr",0,".cer",0,".cr2",0,".crt",0,".crw",0,".dbf" ,
0,".dcr",0,".der",0,".dng",0,".doc",0,".docm",0, ". docx",0,".dwg",0,".dxf",0,".dxg",0,".eps",0,".erf"
,0,".indd",0,".jpe",0,".jpg",0,".jpeg",0,".kdc",0 , ".mdb",0,".mdf",0,".mef",0,".mrw",0,".nef",0," .nrw
",0,".odb",0,".odm",0,".odp",0,".ods",0,".odt" ,0," .orf",0,".p12",0,".p7b",0,".p7c",0,".pdd",0,".pdf"
,0,".pef",0,".pem",0,".pfx",0,".ppt",0,".pptm",0, " .pptx",0,".psd",0,".pst",0,".ptx",0,".r3d",0,".raf
",0,".raw",0,".rtf",0,".rw2",0,".rwl",0,".srf" ,0," .srw",0,".wb2",0,".wpd",0,".wps",0,".xlk",0,".xls" ,0,".xlsb",0,".xlsm",0,".xlsx",0,0**
What I need to do to start cashing?
An offline BitCoin wallet. bitcoin-qt is fine. Synchronize the bitcoin wallet with the network (it will take some time).
Download tor browser bundle. Configure TOR as the SOCKS proxy in the bitcoin client (this is a very important step to your safety).
Generate a new address. Get your password for the TorLocker panel from me (buying this listing). Register you BitCoin address in the panel (you will be asked only once, in the first time you login). Spread the .exe, receive the money.
In how many time will you setup my account?
Maximum 4 days.

70% of the ransom is sent to you. 30% goes to me,

Cyber crime as a service

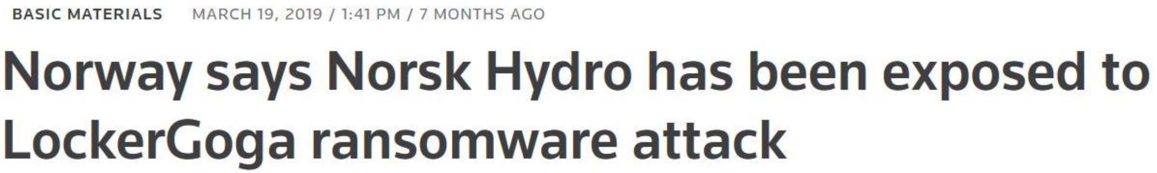
Cyber criminals collaborate by selling all sort of services to each other

- providing malware, or toolkits for creating malware
- franchise models to exploit malware
- selling or renting botnets
  - for spamming, (D)DoS attacks, stealing information, infecting other accounts and machines, ...
- buying and selling of traffic (visits or clicks)
  - to distribute malware
  - to inject ads or generate clicks
    - increasing market for SEO (Search Engine Optimisation)
- buying and selling information
  - credit card numbers, username/passwords, email addresses for spamming, ...
- ...

The central issue: monetisation

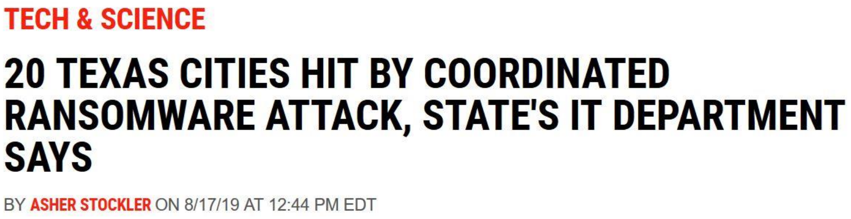
Trend: more targeted & sophisticated ransomware

- Ransomware is becoming more targeted & sophisticated
  - instead of attacking thousands of people & asking for a few hundred euros: attack major organisation, intrude to really corrupt all their backups, and then ask for thousands of euros



BASIC MATERIALS MARCH 19, 2019 / 1:41 PM / 7 MONTHS AGO

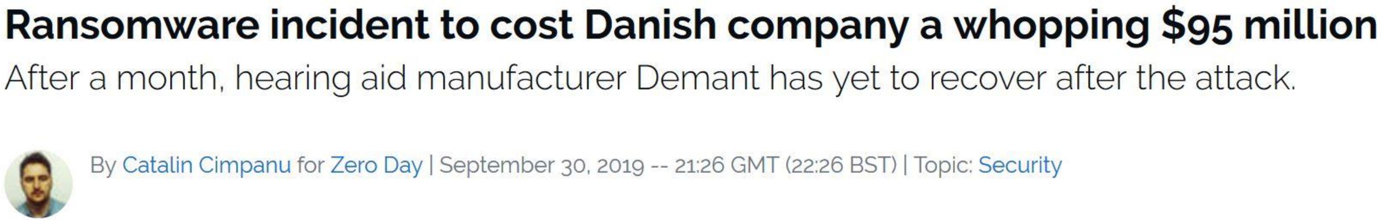
Norway says Norsk Hydro has been exposed to LockerGoga ransomware attack



TECH & SCIENCE

20 TEXAS CITIES HIT BY COORDINATED RANSOMWARE ATTACK, STATE'S IT DEPARTMENT SAYS

BY ASHER STOCKLER ON 8/17/19 AT 12:44 PM EDT



Ransomware incident to cost Danish company a whopping $95 million

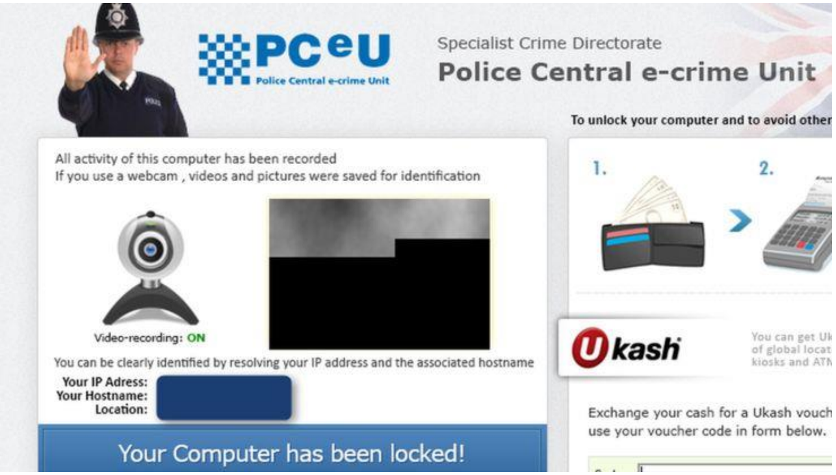
After a month, hearing aid manufacturer Demant has yet to recover after the attack.

By Catalin Cimpanu for Zero Day | September 30, 2019 -- 21:26 GMT (22:26 BST) | Topic: Security

Earlier ransomware example

UK student Zain Qaiser spread malware made by Russian associates in 2013-2014

- Malware spread via ads on porn websites
- Actual malware that encrypted files, not just scareware
- Profits estimated 700,000 – 4,000,000 £
- Student convicted in April 2019



PCeU Police Central e-crime Unit

Specialist Crime Directorate

Police Central e-crime Unit

To unlock your computer and to avoid other

All activity of this computer has been recorded
If you use a webcam , videos and pictures were saved for identification

Video-recording: ON

You can be clearly identified by resolving your IP address and the associated hostname

Your IP Adress:
Your Hostname:
Location:
[redacted]

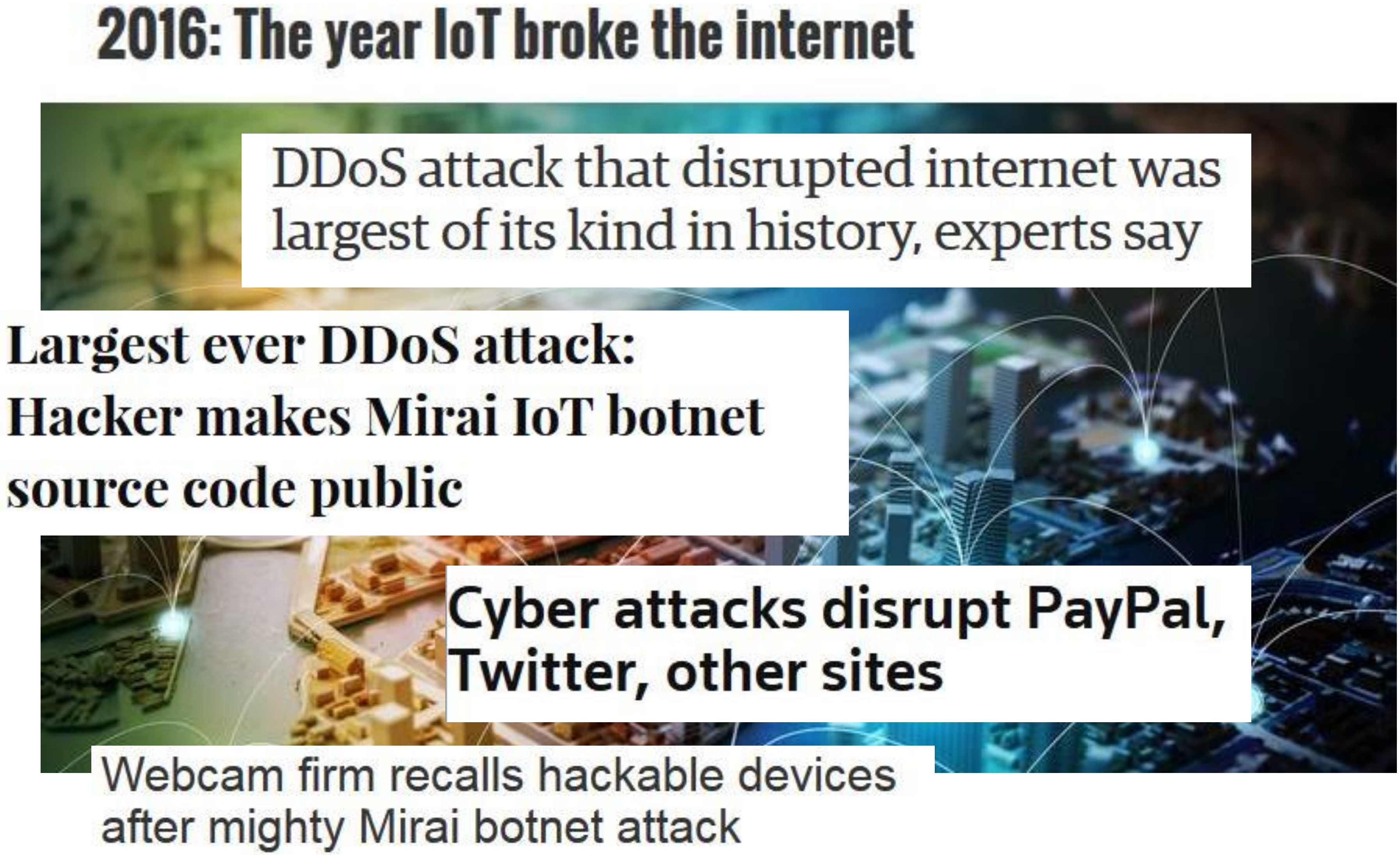
Your Computer has been locked!

You can get Uk
of global locat
kiosks and ATM

Exchange your cash for a Ukash vouch
use your voucher code in form below.

- https://www.bbc.com/news/uk-47800378
- Darknet diaries podcast https://darknetdiaries.com/episode/44/

DDoS



2016: The year IoT broke the internet

DDoS attack that disrupted internet was largest of its kind in history, experts say

Largest ever DDoS attack: Hacker makes Mirai IoT botnet source code public

Cyber attacks disrupt PayPal, Twitter, other sites

Webcam firm recalls hackable devices after mighty Mirai botnet attack

Mirai botnet [2016]

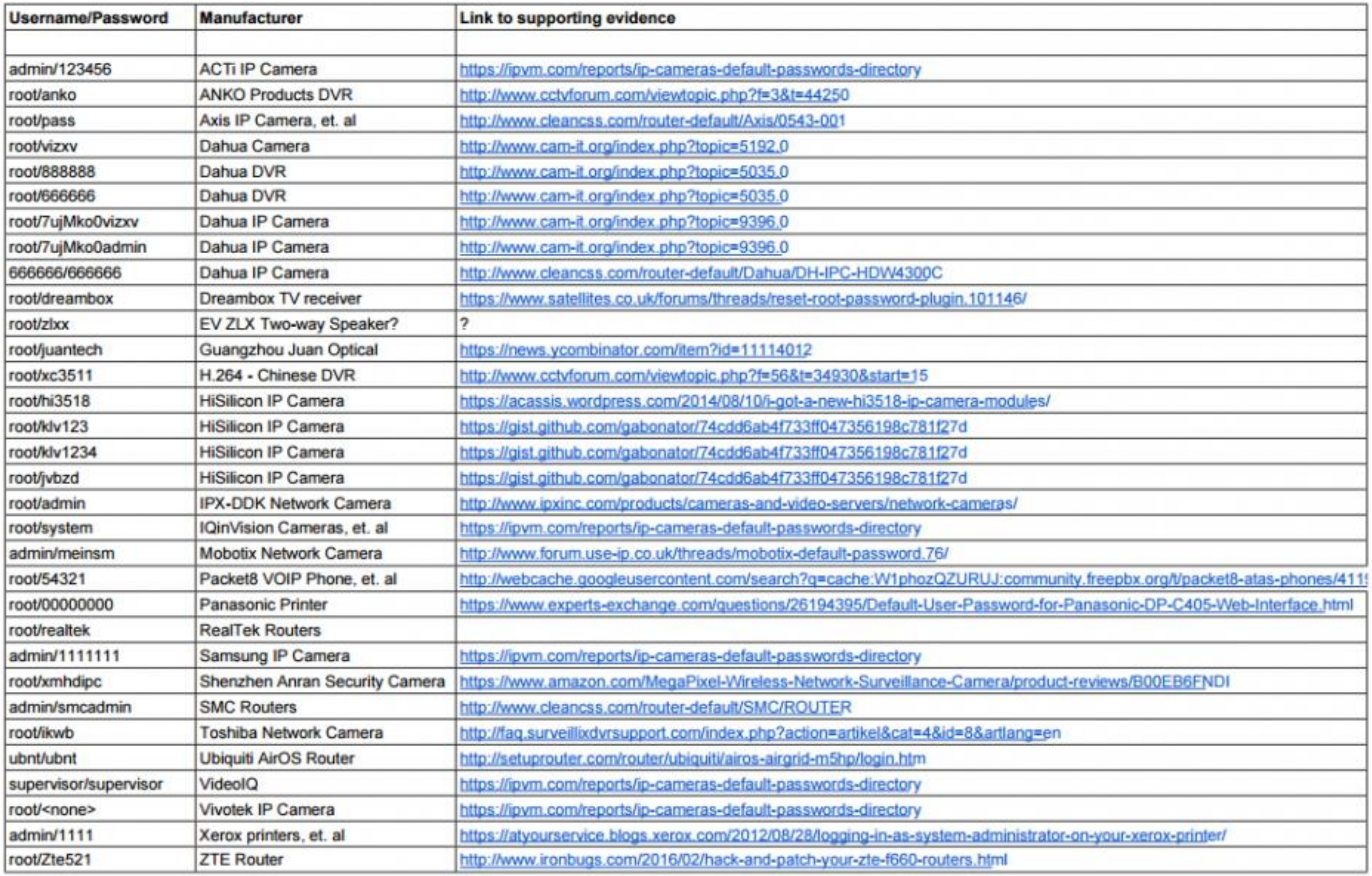
- First botnet comprises of Internet-of-Things (IoT) devices
  - eg webcams, cameras, printers,routers, hard-disk recorders, …
- One of the biggest DDoS attacks ever seen: 620Gbps

- Used to DDoS the website of cyber security researcher Brian Krebs
- Brian Krebs then did research to expose the people behind it

  https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author

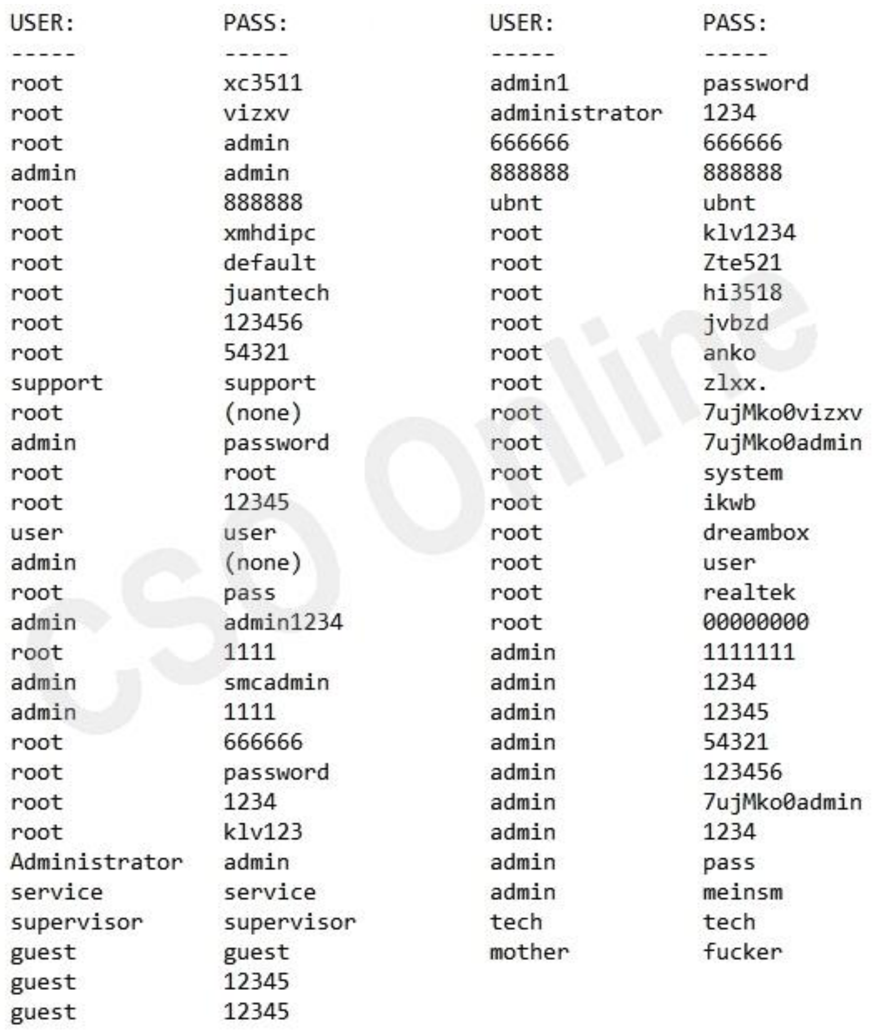
- Botnet authors arrested, pleaded guilty & convicted Sept 2018

Root cause: default passwords exploited by Mirai



Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Root cause: default passwords exploited by Mirai



```
USER:          PASS:               USER:          PASS:
-----          -----               -----          -----
root           xc3511              admin1         password
root           vizxv               administrator  1234
root           admin               666666         666666
admin          admin               888888         888888
root           888888              ubnt           ubnt
root           xmhdipc             root           klv1234
root           default             root           Zte521
root           juantech            root           hi3518
root           123456              root           jvbzd
root           54321               root           anko
support        support             root           zlxx.
root           (none)              root           7ujMko0vizxv
admin          password            root           7ujMko0admin
root           root                root           system
root           12345               root           ikwb
user           user                root           dreambox
admin          (none)              root           user
root           pass                root           realtek
admin          admin1234           root           00000000
root           1111                admin          1111111
admin          smcadmin            admin          1234
admin          1111                admin          12345
root           666666              admin          54321
root           password            admin          123456
root           1234                admin          7ujMko0admin
root           klv123              admin          1234
Administrator  admin               admin          pass
service        service             admin          meinsm
supervisor     supervisor          tech           tech
guest          guest               mother         fucker
guest          12345
guest          12345
```

Root cause of IoT problems: **economics**

- *Why are these IoT devices so insecure?*
  - There is no incentive for manufacturers to provide more secure webcams, routers, hard-disk recorders, …
  - In fact, there is an economic disincentive:
    - Manufacturers who pay attention to secure will be more expensive, late to get to market, an will go bust
- Moreover:
  - *If your webcam is part of a botnet, is there an incentive for you to fix it? or take it offline?*
  - *If your webcam is part of a botnet, is there an incentive for your ISP to warn you? Or to put you in quarantine?*

- Security problems are often an externality for parties responsible of causing it & parties capable of fixing it

Older botnet example: Carna botnet [2012]

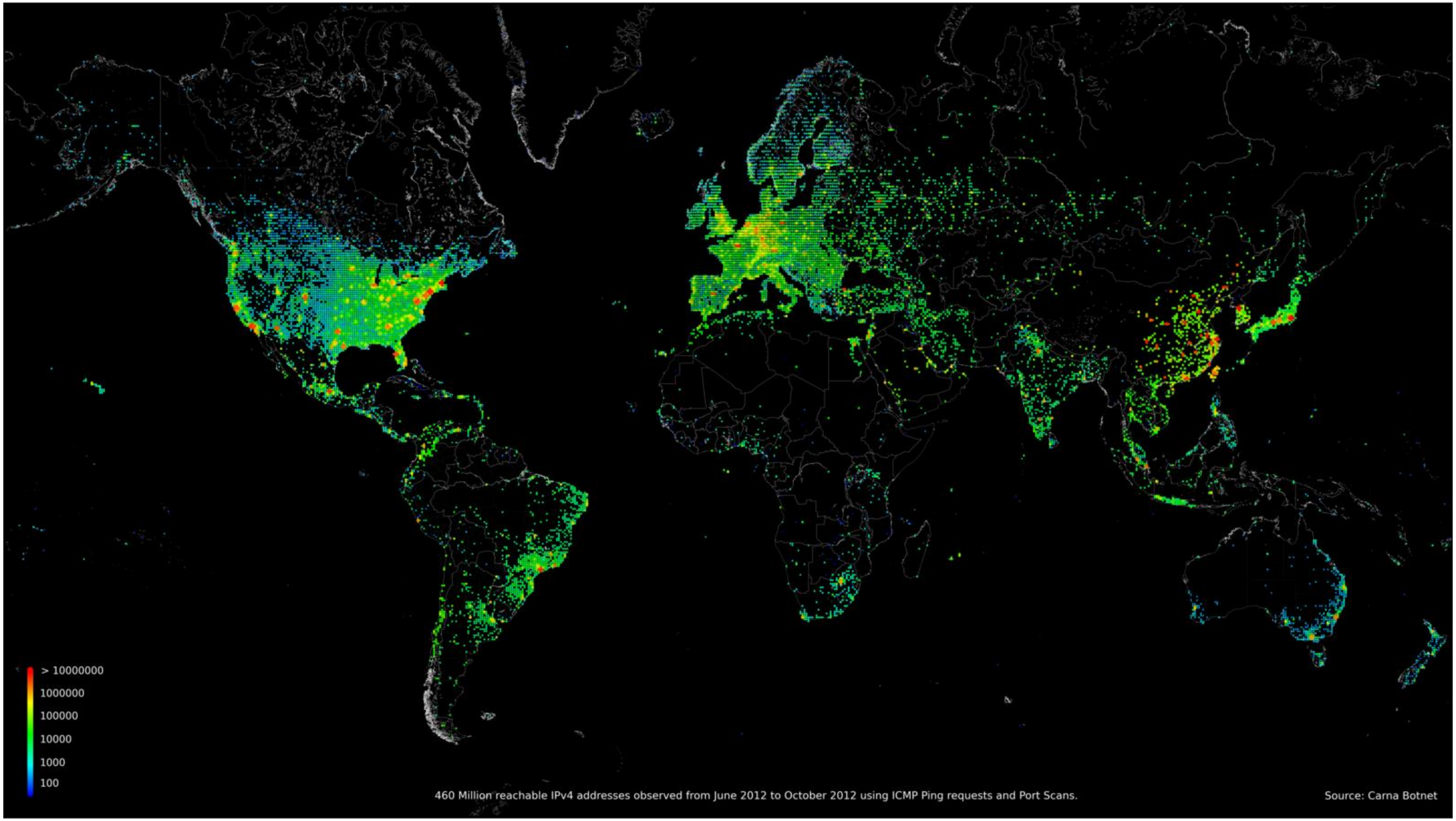
- Large collection of Linux-based embedded systems hacked by
  - using **`telnet`** and classic username/password combinations: **`root/root`** and **`admin/admin`**
  - simply trying random IP addresses
  - Each infected machine was given a range of IP addresses to try
  - Over 400K devices infected

- The entire botnet was then used to scan all IP addresses, to measure internet usage

- Details at http://internetcensus2012.bitbucket.org

- Darknet diaries Podcast about this: https://darknetdiaries.com/episode/13

Carna botnet measuring internet usage



460 Million reachable IPv4 addresses observed from June 2012 to October 2012 using ICMP Ping requests and Port Scans.

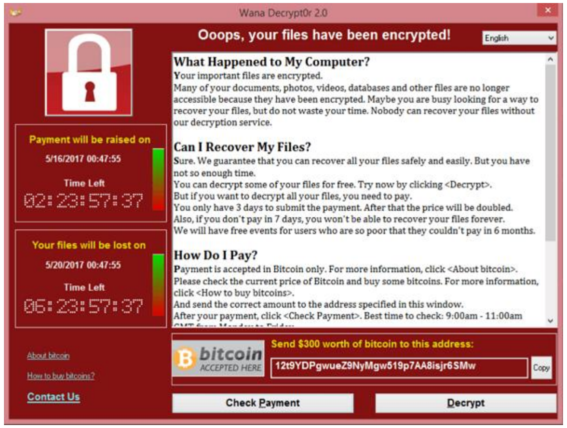
Source: Carna Botnet

WannaCry [March 2017]

- Used NSA malware EternalBlue leaked by Shadow Brokers hacker group
- Killed by registering non-existent domain name that malware checked for
- Caused shutdowns at UK hospitals, Nissan & Renault factories, Telefonica telco, FedEx, German railway, …
- Tied to the Lazarus group, associated with North Korea
- Poorly executed and little money made: only 150 K$

https://bitinfocharts.com/bitcoin/wallet/WannaCry-wallet

- Damage orders of magnitude bigger:
  - 90 M£ & 19,000 cancelled medical appoint for UK hospitals
  - Total damage estimated > 4- billion $



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

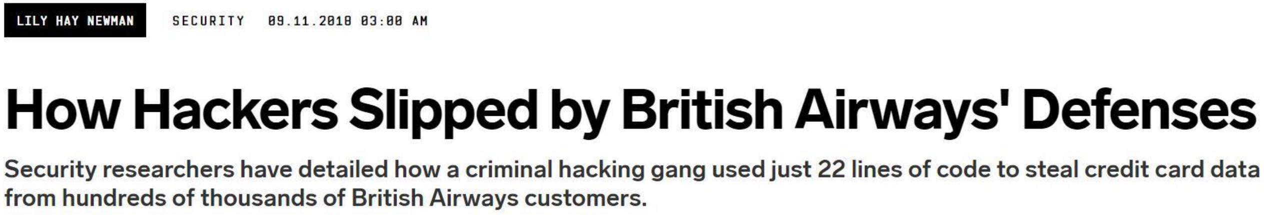
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

NotPetya [June 2017]

- Used NSA exploits EternalBlue & EternalRomance for initial infection
- Used Mimikatz to harvest credentials and spread
- Attack initially spread via Ukrainian accountancy software
  - example of a supply chain attack
- Masquerading as ransomware, but its only aim is sabotage
- Caused shutdowns at Maersk shipping, Merck pharmaceuticals, …
- Estimated damage 10 billion $
- Good write-up in Wired magazine

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

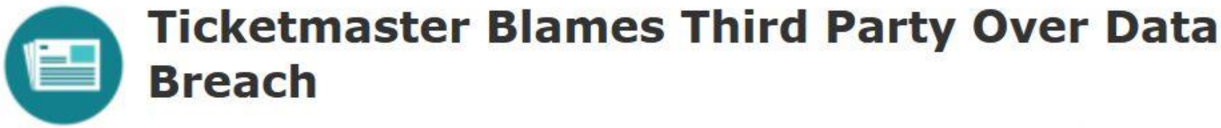
Supply chain attacks [2018-2019]



LILY HAY NEWMAN SECURITY 09.11.2018 03:00 AM

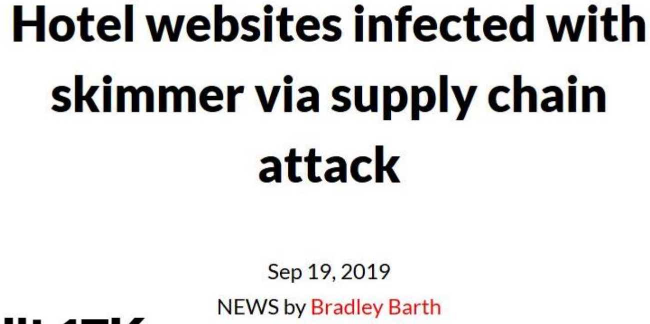
How Hackers Slipped by British Airways' Defenses

Security researchers have detailed how a criminal hacking gang used just 22 lines of code to steal credit card data from hundreds of thousands of British Airways customers.



Ticketmaster Blames Third Party Over Data Breach

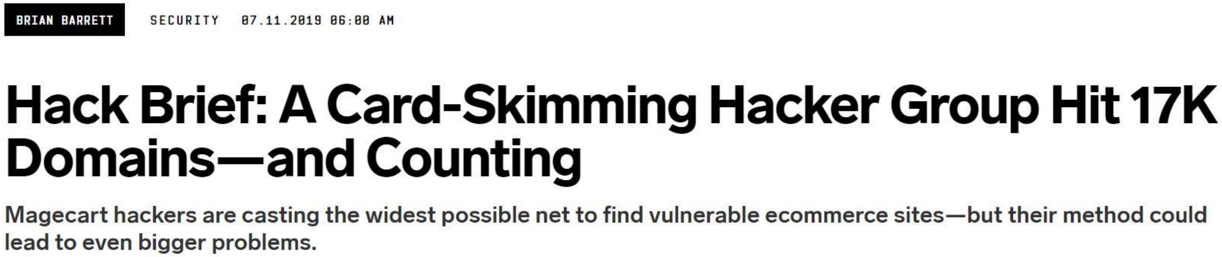
By Kevin Townsend on June 28, 2018



Hotel websites infected with skimmer via supply chain attack

Sep 19, 2019

NEWS by Bradley Barth



BRIAN BARRETT SECURITY 07.11.2019 06:00 AM

Hack Brief: A Card-Skimming Hacker Group Hit 17K Domains—and Counting

Magecart hackers are casting the widest possible net to find vulnerable ecommerce sites—but their method could lead to even bigger problems.

https://www.wired.com/story/magecart-amazon-cloud-hacks/

Supply chain attacks

- Attack vector that is increasingly popular in recent years:
  corrupt 3rd party library with malicious code
  - for websites: via 3rd party javascript
  - eg ‘javascript that scrapes webpage for forms to enter credit card data
- One of in the ways that a criminal group, Magecart, did this
  1. Look for misconfigured S3 buckets in Amazon cloud that are world-readable & writeable
  2. Add malicious code to any *.js files in that bucket
  3. Sit back & wait for any credit cards to be reported
- Countermeasure: Subresource Integrity (SRI)
  HTML source of webpage includes a hash of external resource and browser checks the hash after loading it (and before using it)

https://www.riskiq.com/blog/category/magecart

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity