Towards a secure research environment

Aad van der Klaauw

ITF

January 2016

Current Status

- Breaking and entering (and attempts)
- (NFS) Data and (Tape) Backup's in-house
- Personal Data Protection Act 2016

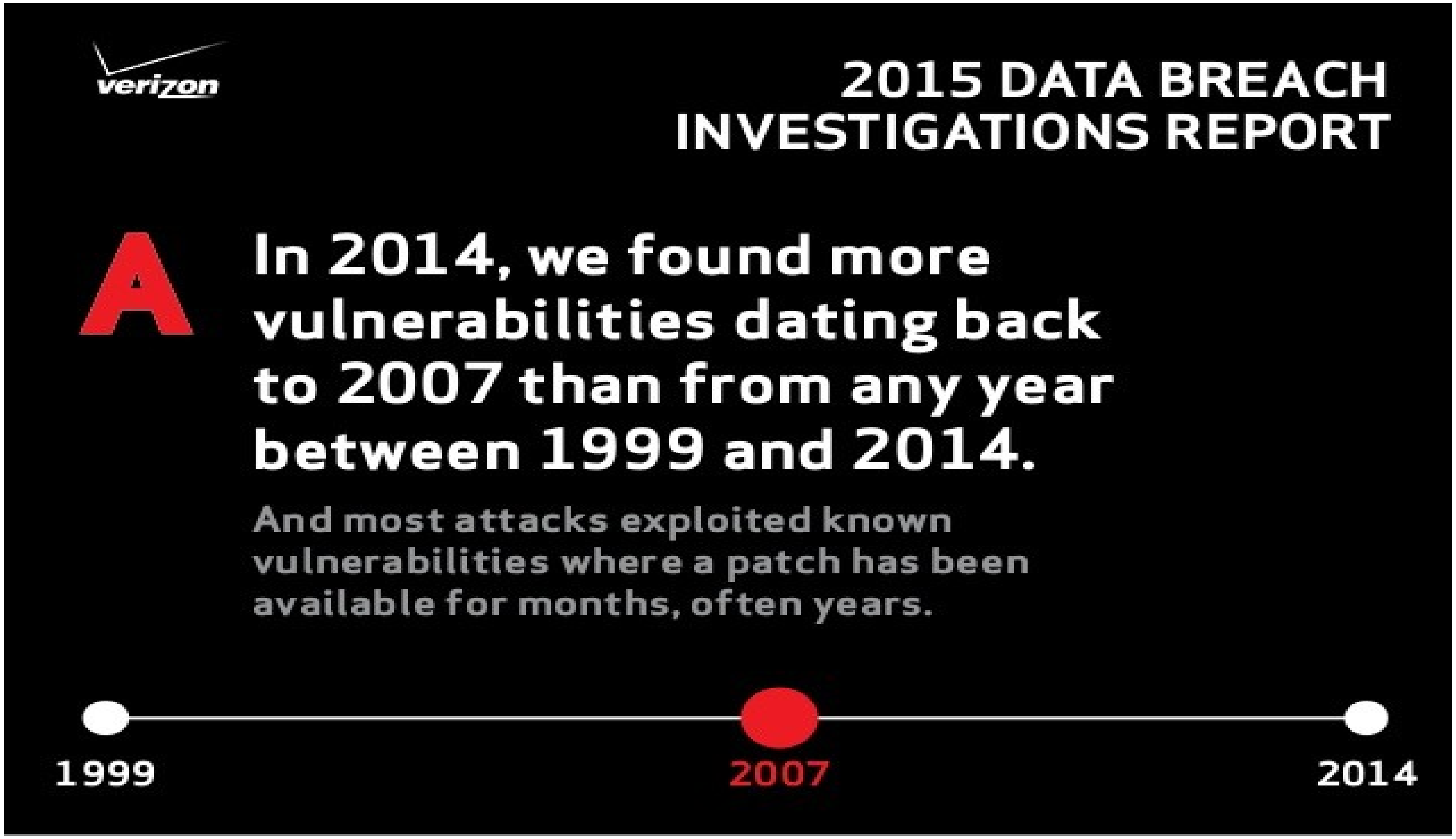
CYBER CRIME
Ctrl
Esc

Personal Data Protection Act 2016
Fine 2nd category > € 120.000,-
or our reputation?

Trend Analysis 2014

- Verizon 2014, worldwide
- SURFnet 2014, NL
- Evidence

Neglect
How about fines in 2016?



verizon

2015 DATA BREACH INVESTIGATIONS REPORT

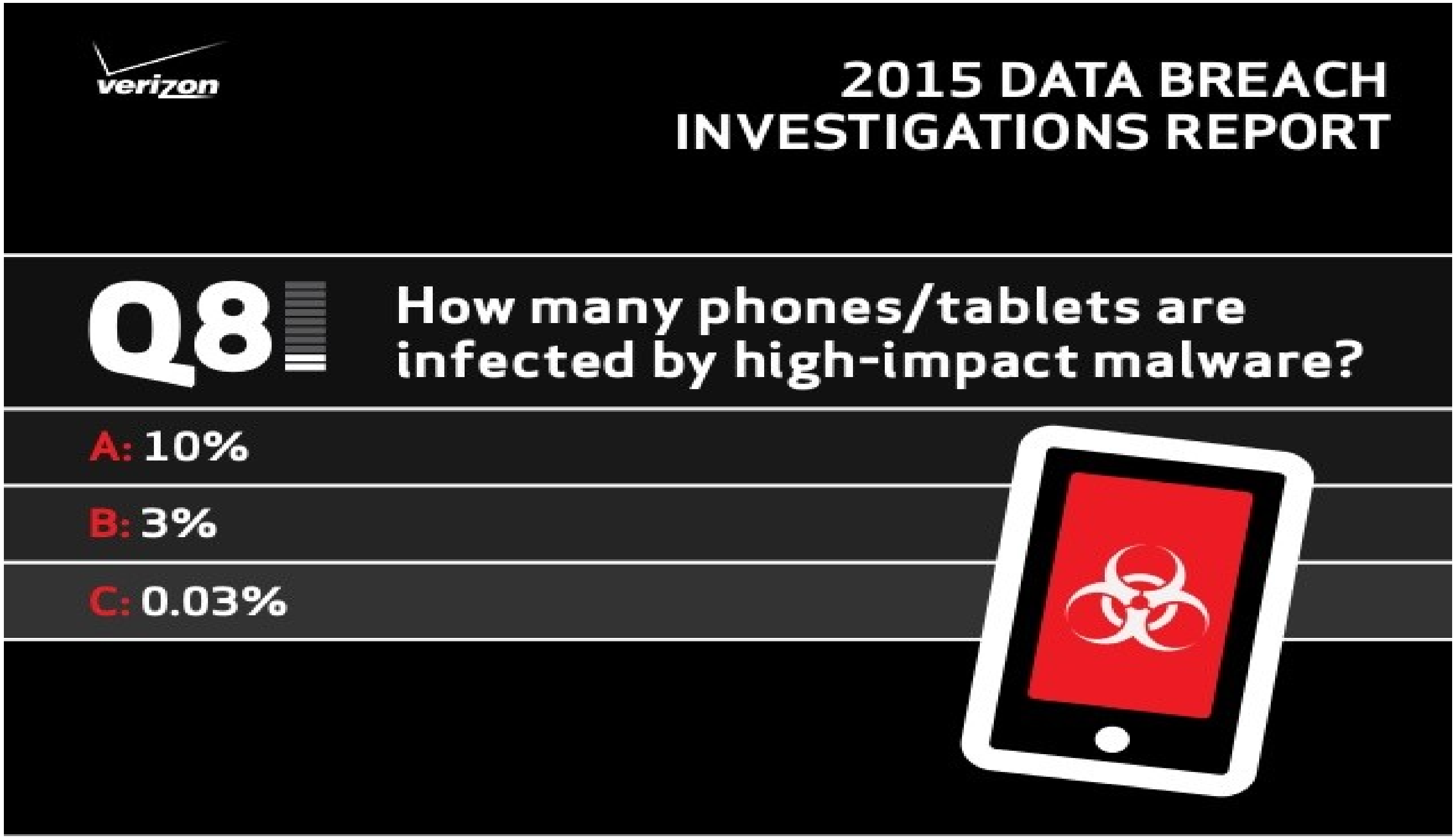
A

In 2014, we found more vulnerabilities dating back to 2007 than from any year between 1999 and 2014.

And most attacks exploited known vulnerabilities where a patch has been available for months, often years.

1999
2007
2014

When, how many?, Or ...



verizon

2015 DATA BREACH INVESTIGATIONS REPORT

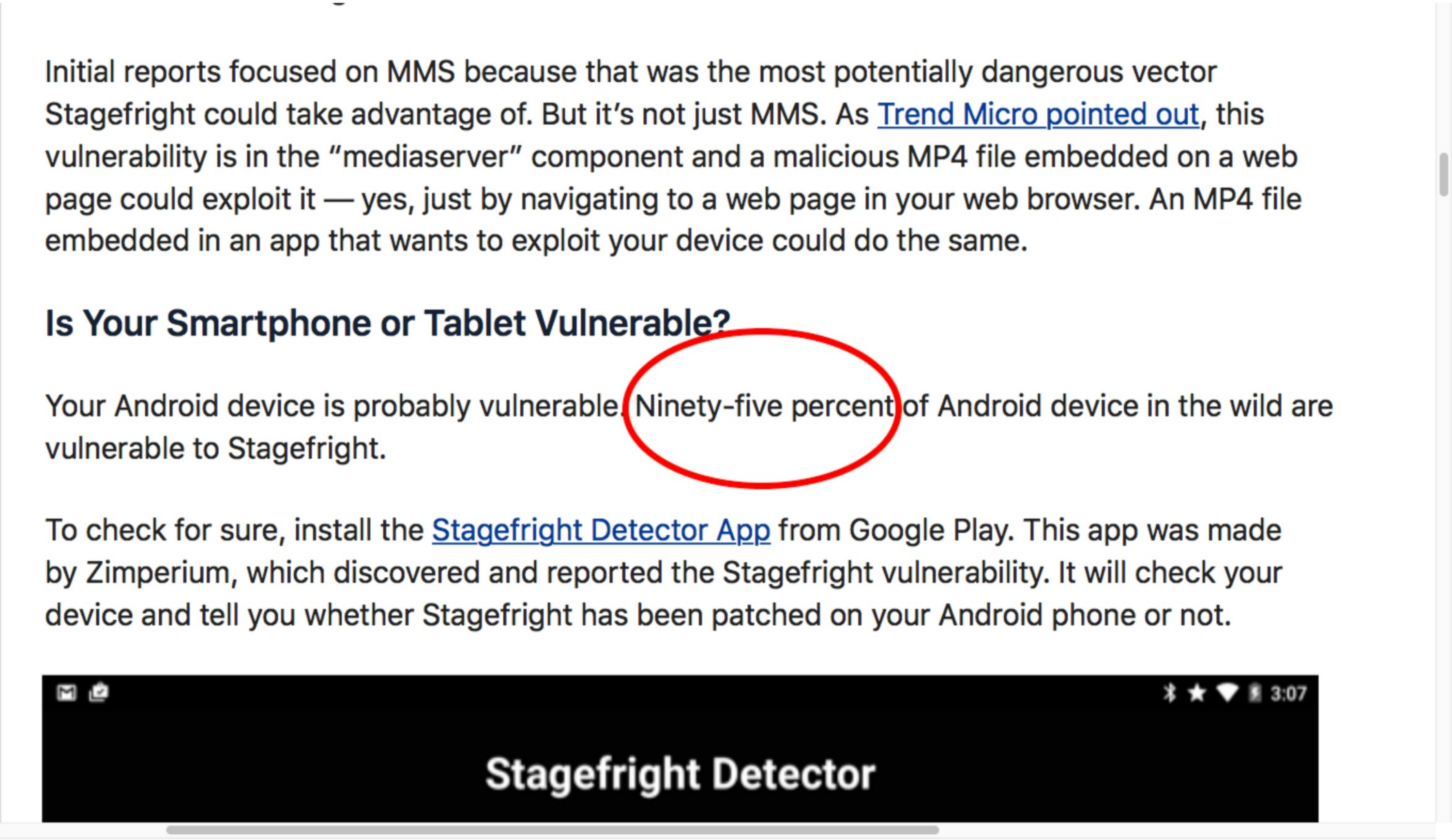
Q8 How many phones/tablets are infected by high-impact malware?

A: 10%

B: 3%

C: 0.03%

What about MyPhone?



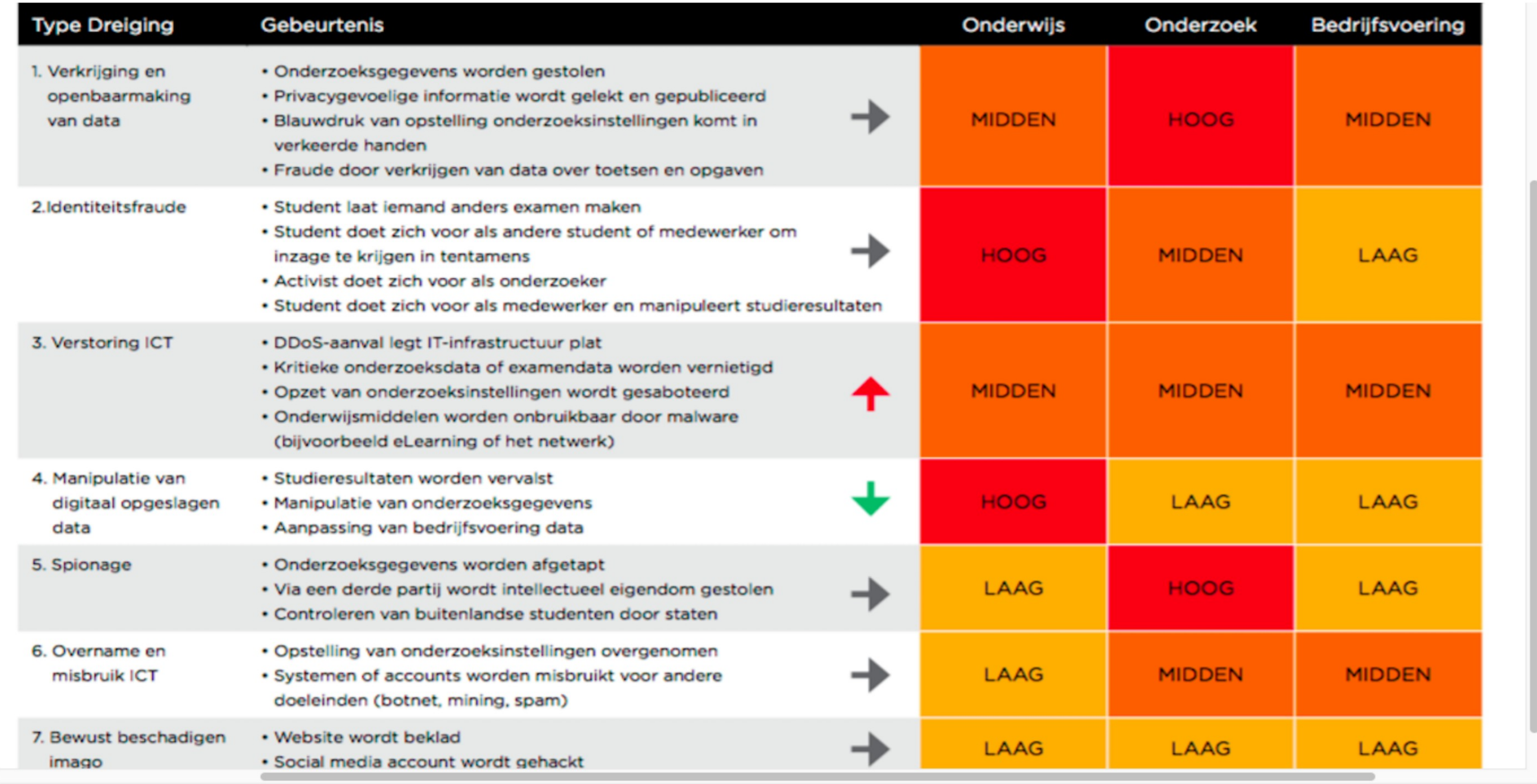
Initial reports focused on MMS because that was the most potentially dangerous vector Stagefright could take advantage of. But it's not just MMS. As Trend Micro pointed out, this vulnerability is in the "mediaserver" component and a malicious MP4 file embedded on a web page could exploit it — yes, just by navigating to a web page in your web browser. An MP4 file embedded in an app that wants to exploit your device could do the same.

Is Your Smartphone or Tablet Vulnerable?

Your Android device is probably vulnerable. Ninety-five percent of Android device in the wild are vulnerable to Stagefright.

To check for sure, install the Stagefright Detector App from Google Play. This app was made by Zimperium, which discovered and reported the Stagefright vulnerability. It will check your device and tell you whether Stagefright has been patched on your Android phone or not.

SURFnet 2014



Type Dreiging	Gebeurtenis		Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	• Onderzoeksgegevens worden gestolen • Privacygevoelige informatie wordt gelekt en gepubliceerd • Blauwdruk van opstelling onderzoeksinstellingen komt in verkeerde handen • Fraude door verkrijgen van data over toetsen en opgaven	→	MIDDEN	HOOG	MIDDEN
2.Identiteitsfraude	• Student laat iemand anders examen maken • Student doet zich voor als andere student of medewerker om inzage te krijgen in tentamens • Activist doet zich voor als onderzoeker • Student doet zich voor als medewerker en manipuleert studieresultaten	→	HOOG	MIDDEN	LAAG
3. Verstoring ICT	• DDoS-aanval legt IT-infrastructuur plat • Kritieke onderzoeksdata of examendata worden vernietigd • Opzet van onderzoeksinstellingen wordt gesaboteerd • Onderwijsmiddelen worden onbruikbaar door malware (bijvoorbeeld eLearning of het netwerk)	↑	MIDDEN	MIDDEN	MIDDEN
4. Manipulatie van digitaal opgeslagen data	• Studieresultaten worden vervalst • Manipulatie van onderzoeksgegevens • Aanpassing van bedrijfsvoering data	↓	HOOG	LAAG	LAAG
5. Spionage	• Onderzoeksgegevens worden afgetapt • Via een derde partij wordt intellectueel eigendom gestolen • Controleren van buitenlandse studenten door staten	→	LAAG	HOOG	LAAG
6. Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	→	LAAG	MIDDEN	MIDDEN
7. Bewust beschadigen imago	• Website wordt beklad • Social media account wordt gehackt	→	LAAG	LAAG	LAAG

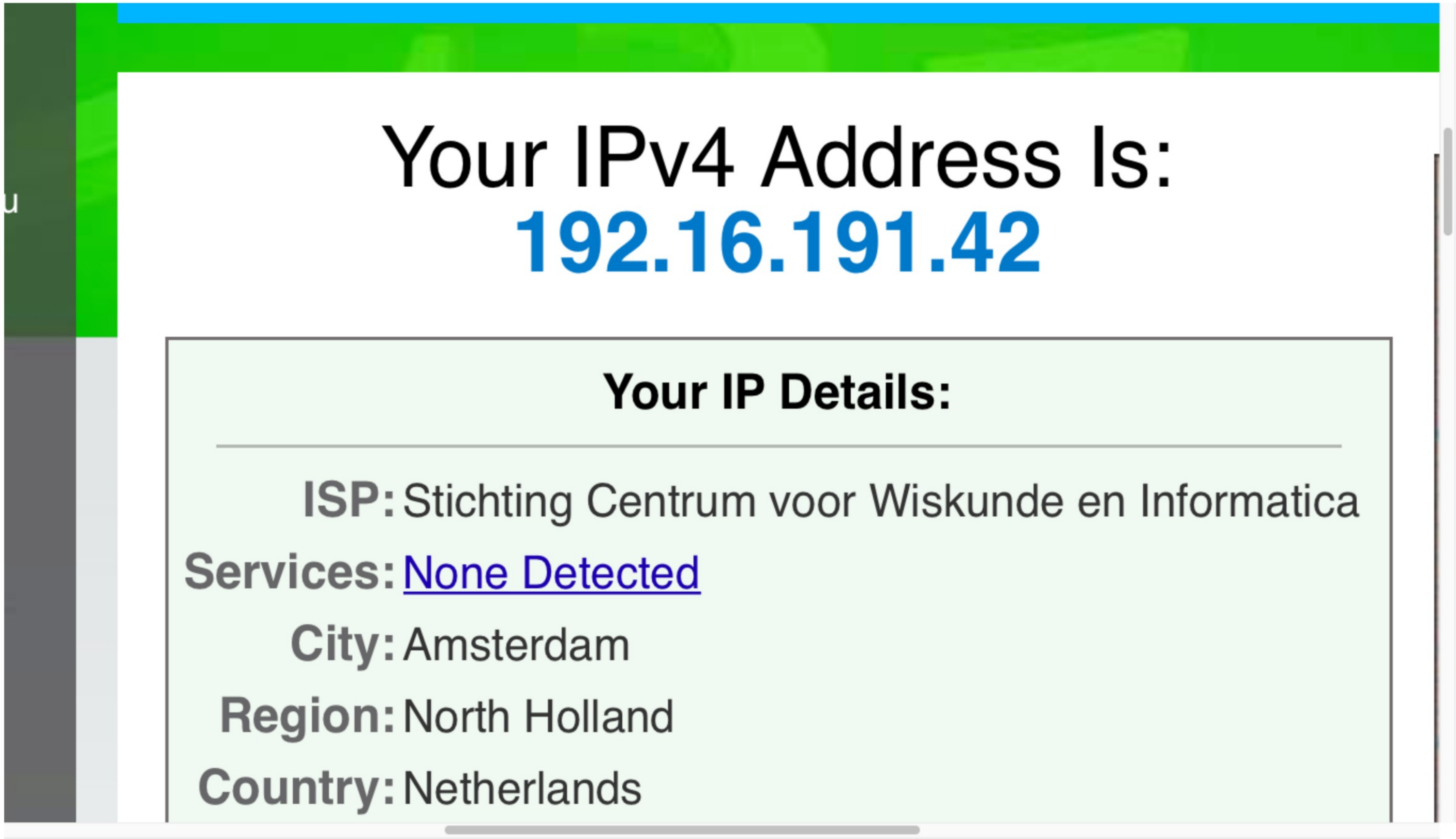
Layered Access to … Data

- **SSH (through), VPN (in), webservers (out)**
- **Private Data, Educational Data, Copyright Data : e-mail, homepages, outside (facebook, dropbox, google etc.)**
- **signing, encrypt (PGP, PDF), archiving (PDF/A-1a)**

Access

- For research
- As a game
- For criminal profit
- As state afair

CWI SSL VPN

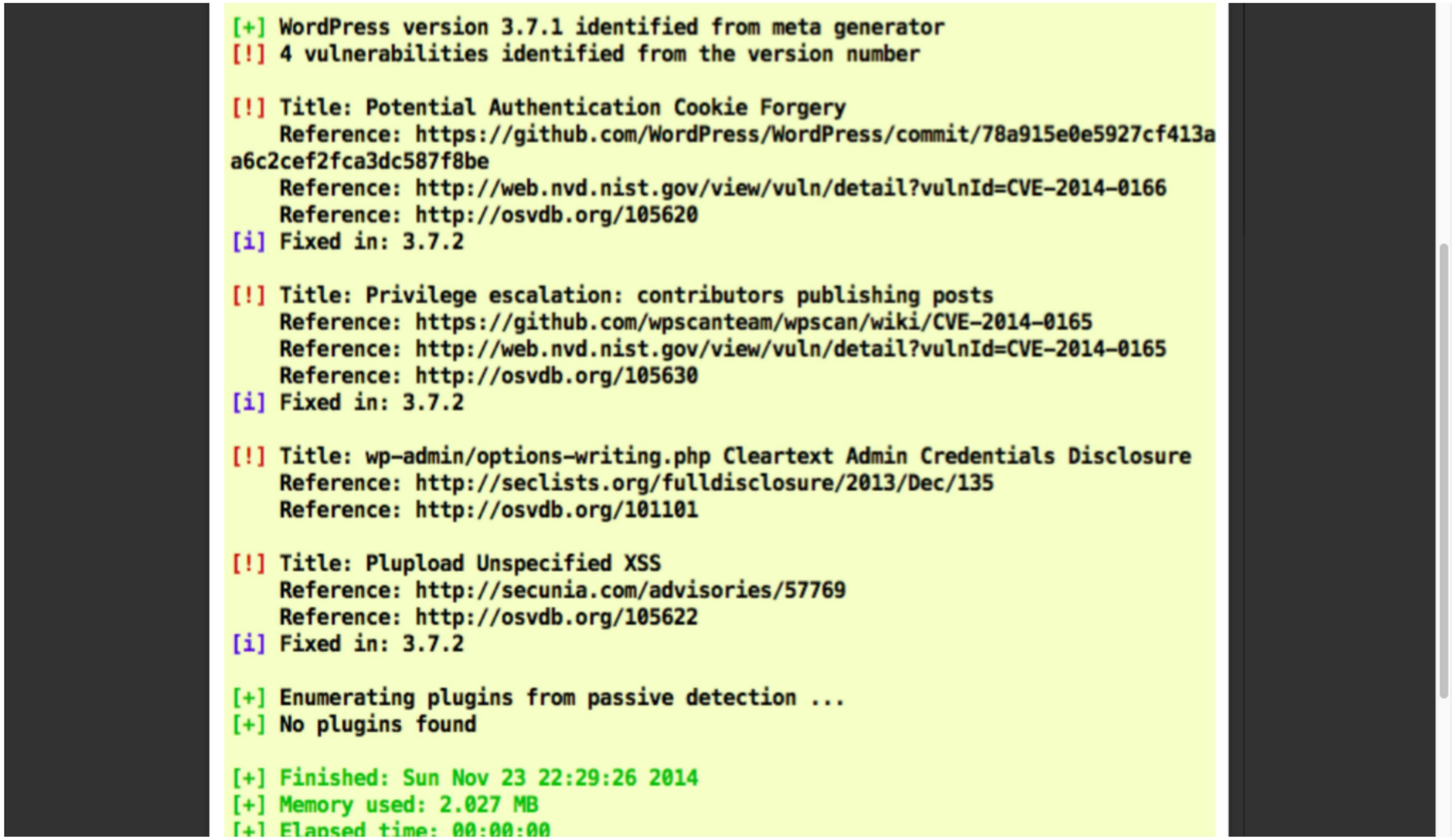


Your IPv4 Address Is:
192.16.191.42

Your IP Details:

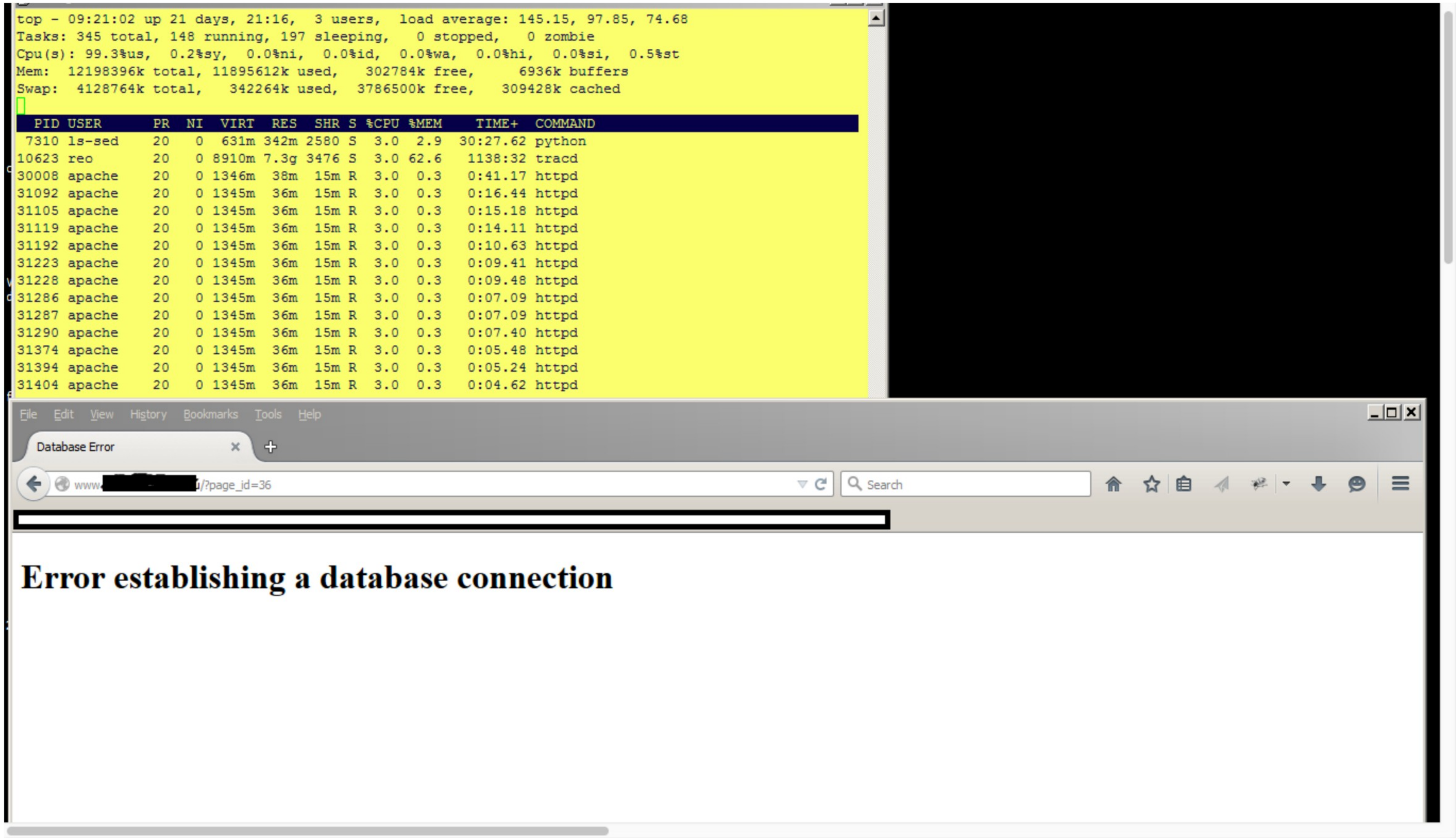
ISP:	Stichting Centrum voor Wiskunde en Informatica
Services:	None Detected
City:	Amsterdam
Region:	North Holland
Country:	Netherlands

CWI webhosting



```
[+] WordPress version 3.7.1 identified from meta generator
[!] 4 vulnerabilities identified from the version number

[!] Title: Potential Authentication Cookie Forgery
    Reference: https://github.com/WordPress/WordPress/commit/78a915e0e5927cf413a
a6c2cef2fca3dc587f8be
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0166
    Reference: http://osvdb.org/105620
[i] Fixed in: 3.7.2

[!] Title: Privilege escalation: contributors publishing posts
    Reference: https://github.com/wpscanteam/wpscan/wiki/CVE-2014-0165
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0165
    Reference: http://osvdb.org/105630
[i] Fixed in: 3.7.2

[!] Title: wp-admin/options-writing.php Cleartext Admin Credentials Disclosure
    Reference: http://seclists.org/fulldisclosure/2013/Dec/135
    Reference: http://osvdb.org/101101

[!] Title: Plupload Unspecified XSS
    Reference: http://secunia.com/advisories/57769
    Reference: http://osvdb.org/105622
[i] Fixed in: 3.7.2

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Finished: Sun Nov 23 22:29:26 2014
[+] Memory used: 2.027 MB
[+] Elapsed time: 00:00:00
```

CWI webhosting



```
top - 09:21:02 up 21 days, 21:16,  3 users,  load average: 145.15, 97.85, 74.68
Tasks: 345 total, 148 running, 197 sleeping,   0 stopped,   0 zombie
Cpu(s): 99.3%us,  0.2%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.5%st
Mem:  12198396k total, 11895612k used,   302784k free,     6936k buffers
Swap:  4128764k total,   342264k used,  3786500k free,   309428k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 7310 ls-sed    20   0  631m 342m 2580 S  3.0  2.9  30:27.62 python
10623 reo       20   0 8910m 7.3g 3476 S  3.0 62.6   1138:32 tracd
30008 apache    20   0 1346m  38m  15m R  3.0  0.3   0:41.17 httpd
31092 apache    20   0 1345m  36m  15m R  3.0  0.3   0:16.44 httpd
31105 apache    20   0 1345m  36m  15m R  3.0  0.3   0:15.18 httpd
31119 apache    20   0 1345m  36m  15m R  3.0  0.3   0:14.11 httpd
31192 apache    20   0 1345m  36m  15m R  3.0  0.3   0:10.63 httpd
31223 apache    20   0 1345m  36m  15m R  3.0  0.3   0:09.41 httpd
31228 apache    20   0 1345m  36m  15m R  3.0  0.3   0:09.48 httpd
31286 apache    20   0 1345m  36m  15m R  3.0  0.3   0:07.09 httpd
31287 apache    20   0 1345m  36m  15m R  3.0  0.3   0:07.09 httpd
31290 apache    20   0 1345m  36m  15m R  3.0  0.3   0:07.40 httpd
31374 apache    20   0 1345m  36m  15m R  3.0  0.3   0:05.48 httpd
31394 apache    20   0 1345m  36m  15m R  3.0  0.3   0:05.24 httpd
31404 apache    20   0 1345m  36m  15m R  3.0  0.3   0:04.62 httpd
```

www.[redacted]/?page_id=36

Error establishing a database connection

Hacking firewalls as a challenge

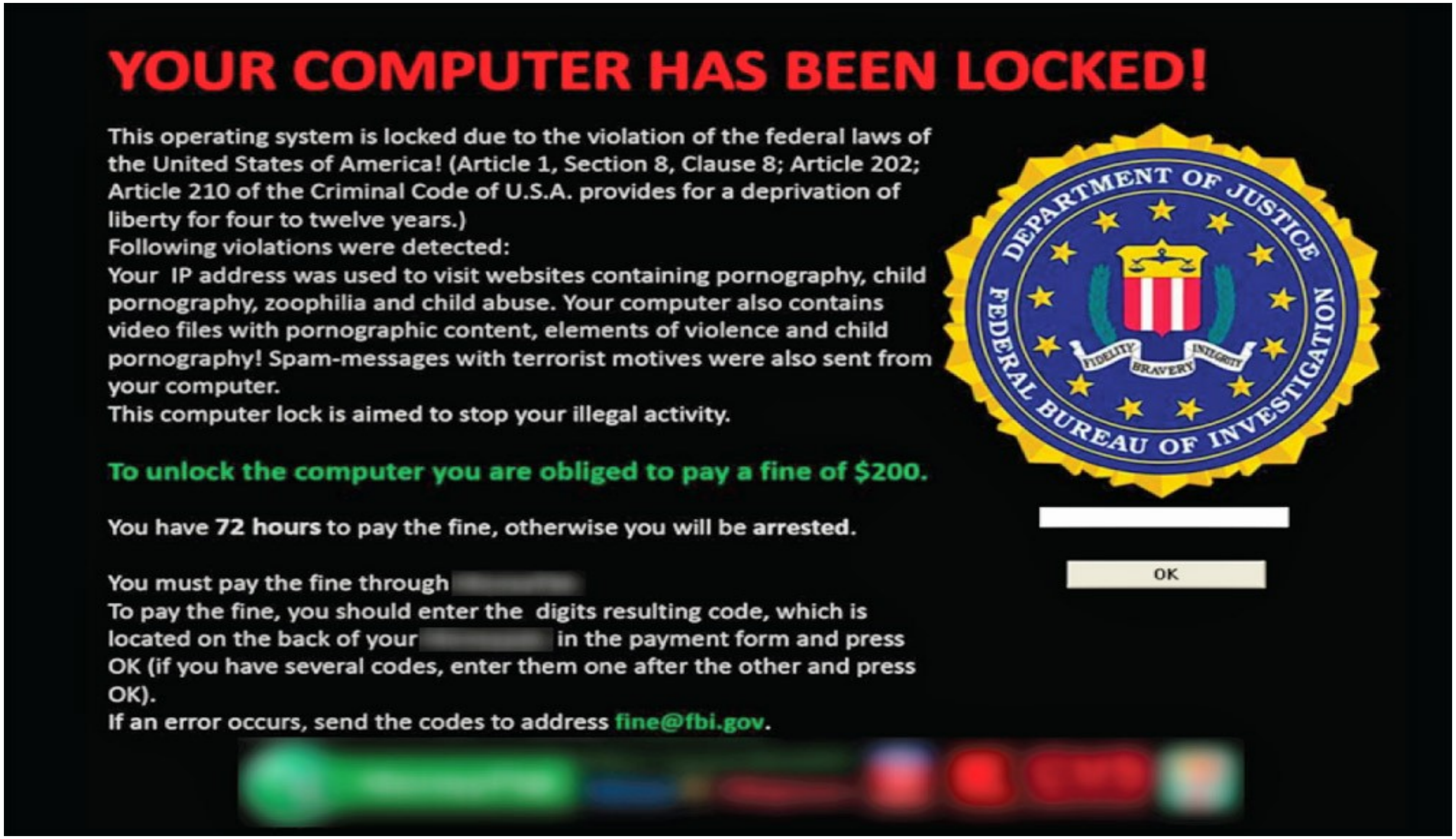
BREAKING BRICKS AND PLUMBING PIPES

Cisco ASA:

A SUPER MARIO ADVENTURE

ALEC STUART-MUIRK

E-mail, phishing, encrypting data



YOUR COMPUTER HAS BEEN LOCKED!

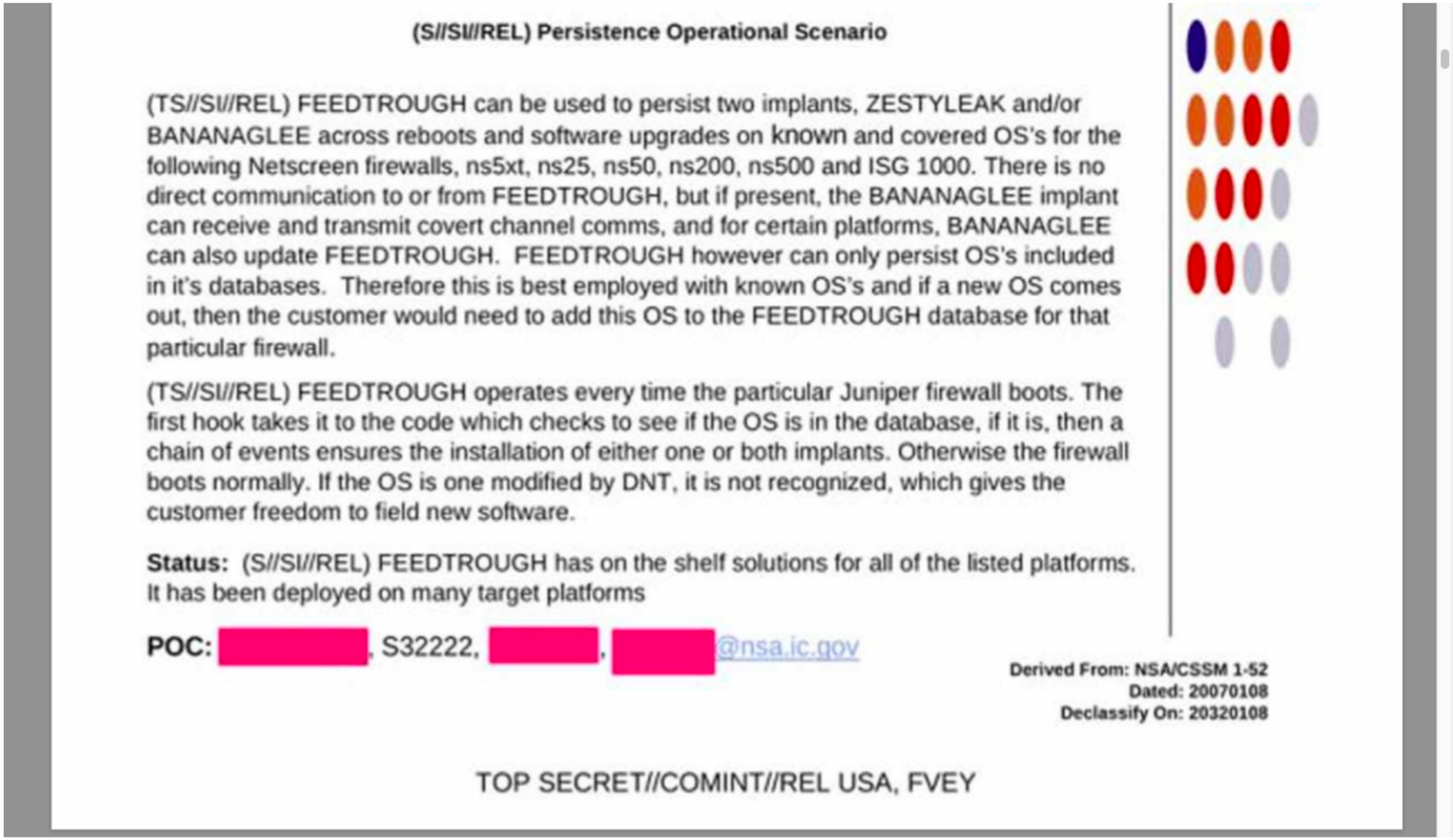
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Access as a backdoor, by design



(S//SI//REL) Persistence Operational Scenario

(TS//SI//REL) FEEDTROUGH can be used to persist two implants, ZESTYLEAK and/or BANANAGLEE across reboots and software upgrades on known and covered OS's for the following Netscreen firewalls, ns5xt, ns25, ns50, ns200, ns500 and ISG 1000. There is no direct communication to or from FEEDTROUGH, but if present, the BANANAGLEE implant can receive and transmit covert channel comms, and for certain platforms, BANANAGLEE can also update FEEDTROUGH. FEEDTROUGH however can only persist OS's included in it's databases. Therefore this is best employed with known OS's and if a new OS comes out, then the customer would need to add this OS to the FEEDTROUGH database for that particular firewall.

(TS//SI//REL) FEEDTROUGH operates every time the particular Juniper firewall boots. The first hook takes it to the code which checks to see if the OS is in the database, if it is, then a chain of events ensures the installation of either one or both implants. Otherwise the firewall boots normally. If the OS is one modified by DNT, it is not recognized, which gives the customer freedom to field new software.

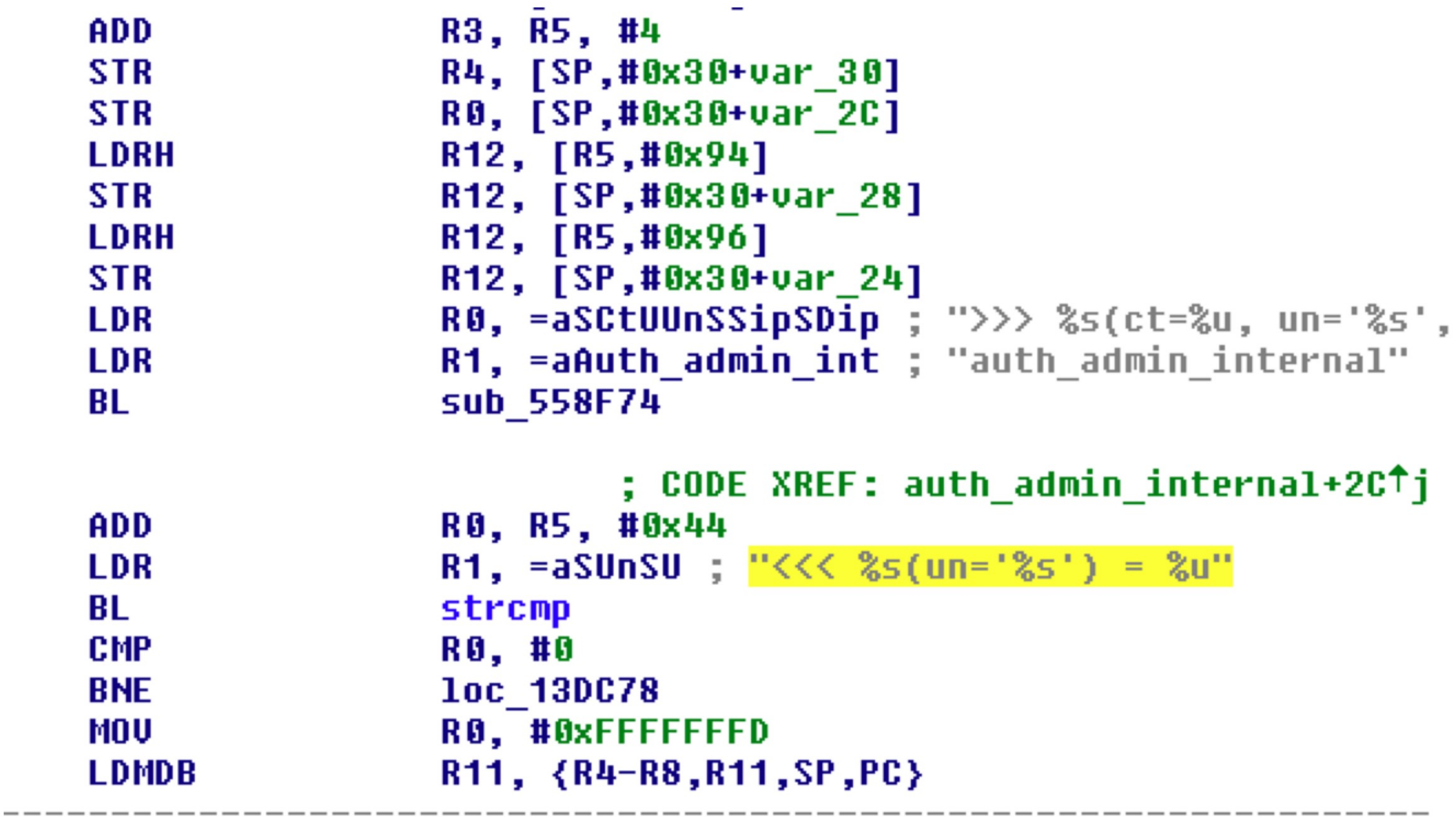
Status: (S//SI//REL) FEEDTROUGH has on the shelf solutions for all of the listed platforms. It has been deployed on many target platforms

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL USA, FVEY

Access as a backdoor, by design II



```
ADD              R3, R5, #4
STR              R4, [SP,#0x30+var_30]
STR              R0, [SP,#0x30+var_2C]
LDRH             R12, [R5,#0x94]
STR              R12, [SP,#0x30+var_28]
LDRH             R12, [R5,#0x96]
STR              R12, [SP,#0x30+var_24]
LDR              R0, =aSCtUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
LDR              R1, =aAuth_admin_int ; "auth_admin_internal"
BL               sub_558F74

                         ; CODE XREF: auth_admin_internal+2C↑j
ADD              R0, R5, #0x44
LDR              R1, =aSUnSU ; "<<< %s(un='%s') = %u"
BL               strcmp
CMP              R0, #0
BNE              loc_13DC78
MOV              R0, #0xFFFFFFFD
LDMDB            R11, {R4-R8,R11,SP,PC}
```

CWI related Cybercrime source NCSC 2014

1997: xx

2003: xx,xx

2004: xx,xx

2007: xx,xx,xx

2009: xx

2010: xx,xx,xx

2011: xx,xx

2012: xx

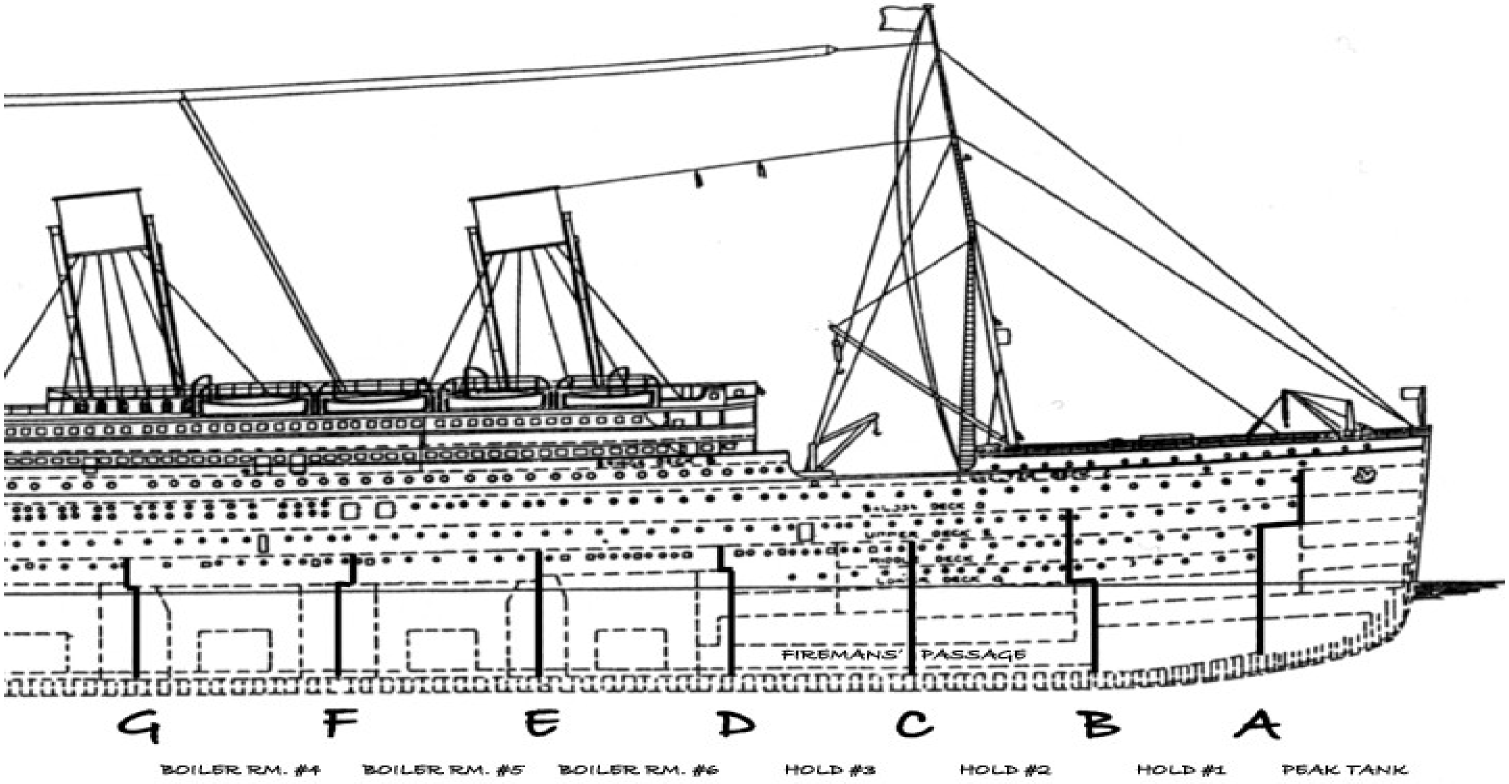
2013: xx,xx,xx

2014: xx,xx,xx,xx,xx,xx

What (if any) changes?

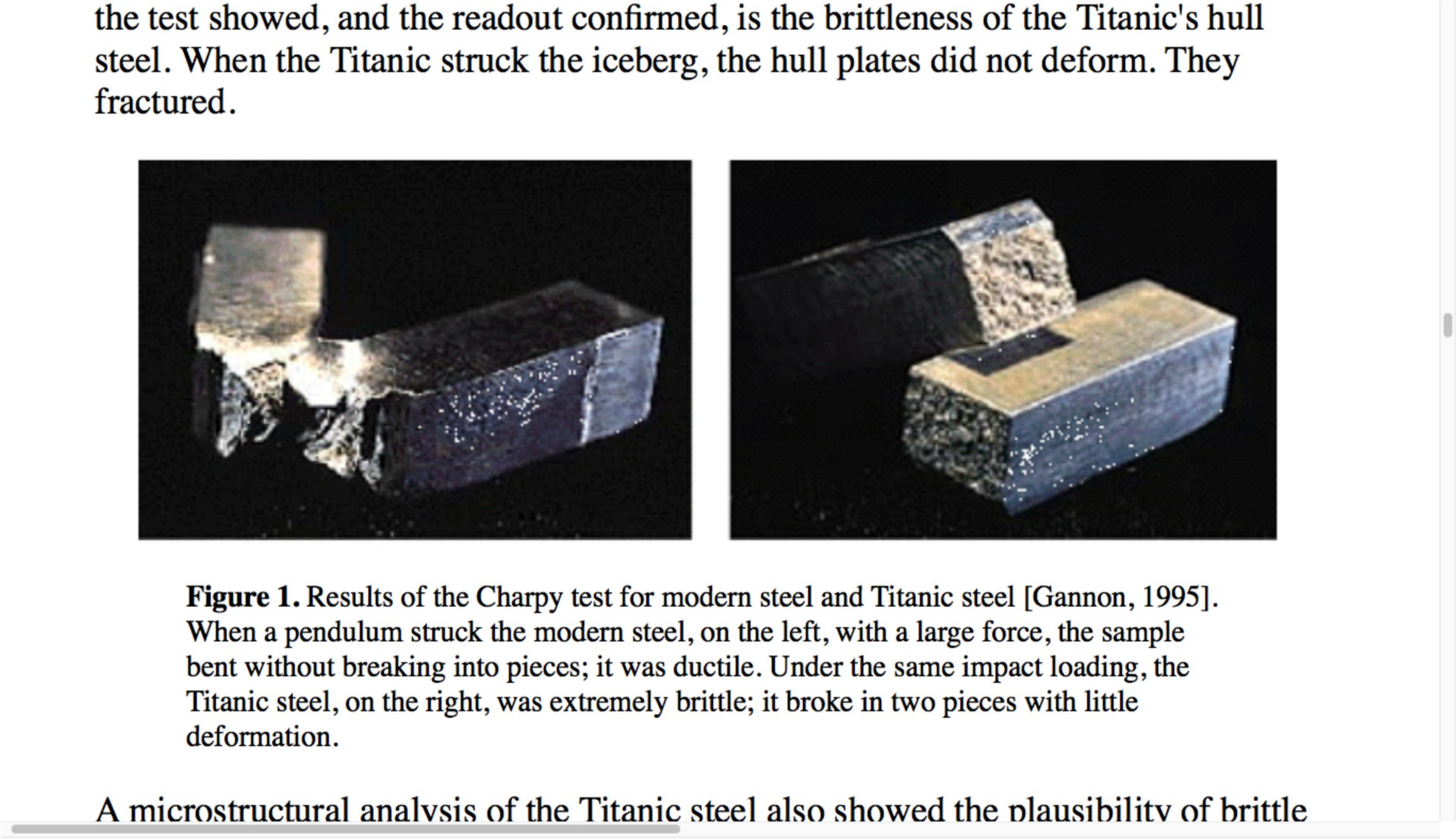
- Security model(s): corporate, organic?
- Risc, Containment, Diversity?
- Defend against espionage?

Design Flaw



Bulkheads & Compartments in the Bow Section

Titanic's implementation flaw

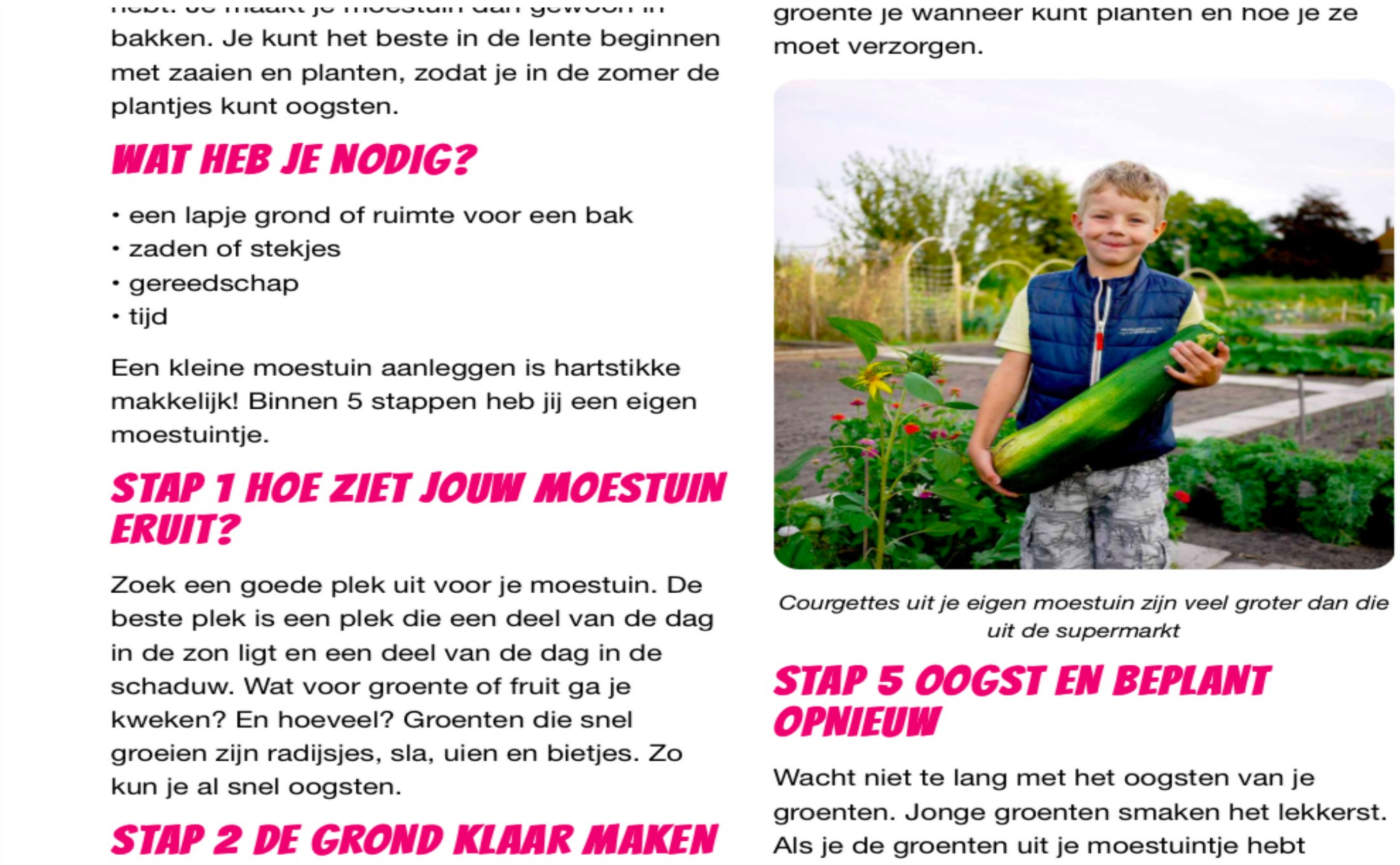


the test showed, and the readout confirmed, is the brittleness of the Titanic's hull steel. When the Titanic struck the iceberg, the hull plates did not deform. They fractured.

Figure 1. Results of the Charpy test for modern steel and Titanic steel [Gannon, 1995]. When a pendulum struck the modern steel, on the left, with a large force, the sample bent without breaking into pieces; it was ductile. Under the same impact loading, the Titanic steel, on the right, was extremely brittle; it broke in two pieces with little deformation.

A microstructural analysis of the Titanic steel also showed the plausibility of brittle

CWI Research Results ...



hebt. Je maakt je moestuin dan gewoon in bakken. Je kunt het beste in de lente beginnen met zaaien en planten, zodat je in de zomer de plantjes kunt oogsten.

WAT HEB JE NODIG?

- een lapje grond of ruimte voor een bak
- zaden of stekjes
- gereedschap
- tijd

Een kleine moestuin aanleggen is hartstikke makkelijk! Binnen 5 stappen heb jij een eigen moestuintje.

STAP 1 HOE ZIET JOUW MOESTUIN ERUIT?

Zoek een goede plek uit voor je moestuin. De beste plek is een plek die een deel van de dag in de zon ligt en een deel van de dag in de schaduw. Wat voor groente of fruit ga je kweken? En hoeveel? Groenten die snel groeien zijn radijsjes, sla, uien en bietjes. Zo kun je al snel oogsten.

STAP 2 DE GROND KLAAR MAKEN

groente je wanneer kunt planten en hoe je ze moet verzorgen.

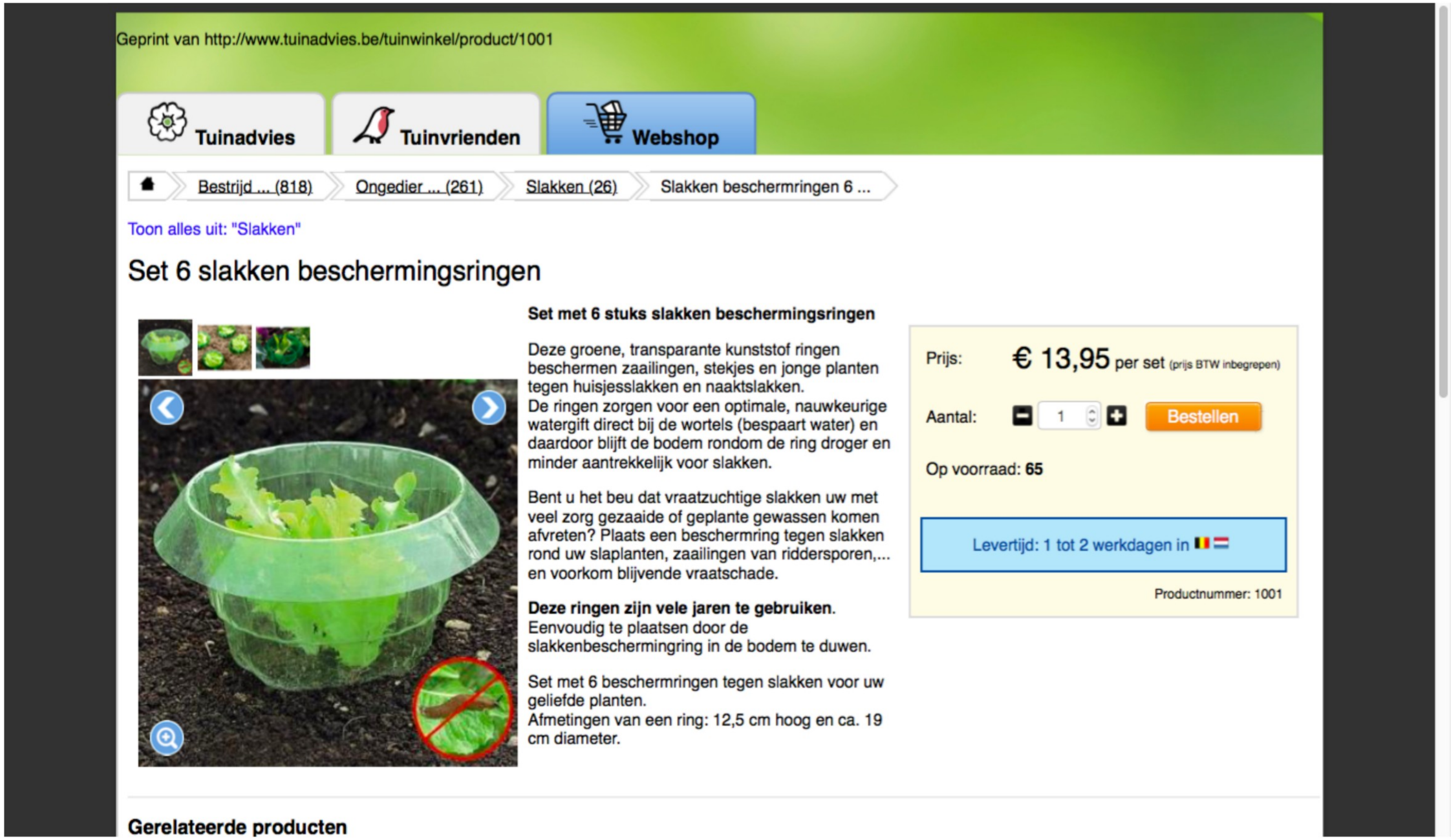
Courgettes uit je eigen moestuin zijn veel groter dan die uit de supermarkt

STAP 5 OOGST EN BEPLANT OPNIEUW

Wacht niet te lang met het oogsten van je groenten. Jonge groenten smaken het lekkerst. Als je de groenten uit je moestuintje hebt

CWI Research Workspace ? ...

Containment, Diversity



Geprint van http://www.tuinadvies.be/tuinwinkel/product/1001

Bestrijd ... (818) › Ongedier ... (261) › Slakken (26) › Slakken beschermringen 6 ...

Toon alles uit: "Slakken"

Set 6 slakken beschermingsringen

Set met 6 stuks slakken beschermingsringen

Deze groene, transparante kunststof ringen beschermen zaailingen, stekjes en jonge planten tegen huisjesslakken en naaktslakken.
De ringen zorgen voor een optimale, nauwkeurige watergift direct bij de wortels (bespaart water) en daardoor blijft de bodem rondom de ring droger en minder aantrekkelijk voor slakken.

Bent u het beu dat vraatzuchtige slakken uw met veel zorg gezaaide of geplante gewassen komen afvreten? Plaats een beschermring tegen slakken rond uw slaplanten, zaailingen van riddersporen,... en voorkom blijvende vraatschade.

Deze ringen zijn vele jaren te gebruiken.
Eenvoudig te plaatsen door de slakkenbeschermingring in de bodem te duwen.

Set met 6 beschermringen tegen slakken voor uw geliefde planten.
Afmetingen van een ring: 12,5 cm hoog en ca. 19 cm diameter.

Prijs: € 13,95 per set (prijs BTW inbegrepen)

Aantal: 1 Bestellen

Op voorraad: **65**

Levertijd: 1 tot 2 werkdagen in 🇧🇪 🇳🇱

Productnummer: 1001

Gerelateerde producten

What (if any) changes?

- **Security model(s): corporate, organic?**
- **Risc, Containment, Diversity?**
- **Defend against espionage?**