



MIS|TI™ PRESENTS

InfoSecWorld
Conference & Expo 2018

REPAIRING THE INTERNET WITH RESPONSIBLE DISCLOSURES

Victor Gevers

Chairman GDI.foundation

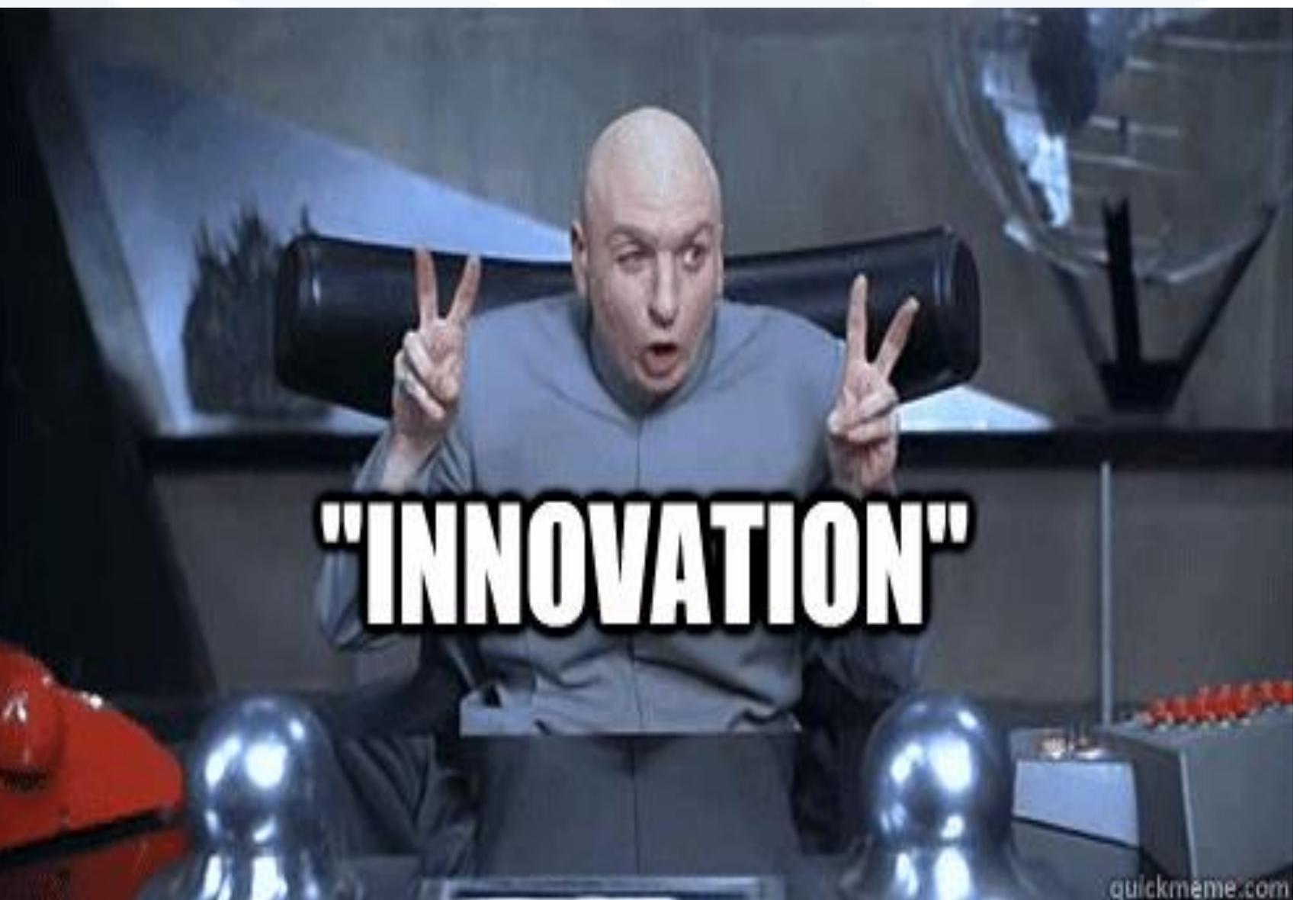
@GDI_fdn

Title Text

- Introduction
- Who we are
- What we do
 - **Finding vulnerabilities**
 - Scanning the internet
 - Scraping everything what is public
 - **Using OSINT**
 - International overview
 - Comparing trusted sources
 - Running in depth scans
 - Digging in public password dumps
 - Learning from source code leaks
 - **Reporting vulnerable items**
 - Responsible Disclosures / CVD
 - Bulk reporting
 - **Success factors**
 - Communication is key
 - Intent / goal and governance
 - Personal touches
 - Translation by locals
 - Keep the (Gov)CERTS informed
 - Keep tracking reported items
 - Publish your findings.



Whois



Who



Vincent Toms

is a cyber security consultant who works for the Dutch Government. In the last 20 years he has gained extensive knowledge in advising & providing assurance in the areas of IT Security, Governance, Risk and Control.

He worked for more than 12 years for the Ministry of Defense as IT auditor and did several postgraduate courses in the field of IT Governance, Risk and Control. The last 5 years he uses his knowledge in advising organization(s) about Cyber Risk and Controls.



Victor Gevers

(also known as 0xDUDE) is a senior security specialist working as innovation manager for the Dutch Government, specialized in network, mobile, and web application security. He performs research on state-of-the-art attack and defense mechanisms, general ethical hacking techniques, protocols.

In his free time he is a vulnerability researcher and hunts down weak security implementations. In several occasions he has been pointed out to be a true responsible disclosure evangelist, practicing the art over 18 years and has made over five thousand responsible disclosures world-wide.



Whoami

```
sh-3.2# whoami  
root  
sh-3.2#
```



Victor Gevers

@0xDUDE

(Ethical) hacker. 5,353 Responsible Disclosures / Coordinated Vulnerability Disclosures since '98. Chairman GDI.foundation & proud member of the GGOH.

Chairman GDI.foundation

GDI.foundation

G.G.O.H. - Guild of the Grumpy Old Hackers



What

Google

GDI.foundation



All Shopping Images Videos News More Settings Tools

All news ▾ Past year ▾ Sorted by date ▾ Hide Duplicates ▾ Clear



[Proof-of-Concept Code for Memcached DDoS Attacks Published ...](#)

BleepingComputer - 7 Mar 2018

For example, Victor Gevers, Chairman of the **GDI Foundation**, has been contacting Memcached server owners for almost two years, advising companies to secure servers and place them behind a firewall. "It's sour to see [DDoS attacks] finally happen after more than two years of warnings. Sometimes you don't want to be ...



[Should Investors Worry About A Stock Exchange Hack?](#)

ValueWalk - 22 Jan 2018

"Actually, 'owning the network' is a breeze," according to Victor Gevers, a security consultant for the **GDI Foundation** who discovered the vulnerability and promotes himself as an "ethical hacker." Hackers often scan for such vulnerabilities because they are easy targets, he said. "Our advice was to block the telnet protocol on ...



[Stock exchange finally fixes telnet router weakness](#)

Naked Security - 22 Jan 2018

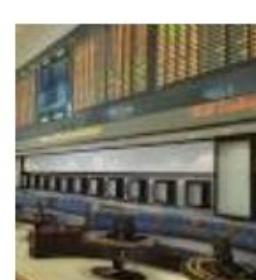
Although it later emerged that only 1,775 of these still worked, one that did was for a Huawei router that belonged to Oman's Muscat Securities Market (MSM), as Dutch **GDI Foundation** researcher Victor Gevers discovered. An enterprise model, this was running a telnet interface accessible with a default password and ...



[Major security flaw found in Oman stock exchange](#)

The Stack - 19 Jan 2018

The IP address of the Huawei-developed router was found amongst a list of 33,000 credentials. Many of these credentials still worked when attempting to access devices over an old telnet protocol. Gevers, who is chairman of Netherlands-based ethical hacking group **GDI Foundation**, had reported these vulnerable devices ...



[A security gaffe left Oman's stock exchange vulnerable to hackers for ...](#)

International Business Times UK - 18 Jan 2018

According to Gevers, who is the founder of the non-profit group **GDI foundation** that hunts vulnerabilities, several attempts to contact Omani authorities by phone and email failed to yield any response. Meanwhile, the exchange remained vulnerable. According to Gevers, if a hacker had stumbled onto the vulnerable router, ...



[Oman's stock exchange was easily hackable for months](#)

ZDNet - 18 Jan 2018

Gevers, chairman of the **GDI Foundation**, a Netherlands-based non-profit group focused on finding security vulnerabilities, spent months reporting each vulnerable device in the list to its owner. Many had already been compromised. It was during his

Google

GDI.foundation



All Shopping Images Videos News More Settings Tools

All news ▾ Past year ▾ Sorted by date ▾ Hide Duplicates ▾ Clear



[Proof-of-Concept Code for Memcached DDoS Attacks Published ...](#)

BleepingComputer - 7 Mar 2018

For example, Victor Gevers, Chairman of the **GDI Foundation**, has been contacting Memcached server owners for almost two years, advising companies to secure servers and place them behind a firewall. "It's sour to see [DDoS attacks] finally happen after more than two years of warnings. Sometimes you don't want to be ...



[Stock exchange finally fixes telnet router weakness](#)

Naked Security - 22 Jan 2018

Although it later emerged that only 1,775 of these still worked, one that did was for a Huawei router that belonged to Oman's Muscat Securities Market (MSM), as Dutch **GDI Foundation** researcher Victor Gevers discovered. An enterprise model, this was running a telnet interface accessible with a default password and ...



[BrickerBot Author Retires Claiming to Have Bricked over 10 Million ...](#)

BleepingComputer - 11 Dec 2017

Fourth, JanitOr advises security researchers to volunteer their free time to organizations such as **GDI Foundation** or the Shadowserver Foundation, which have been working to secure some of these vulnerable devices. Last but not least, he advises that some of us that have too much time and money on our hands to start ...



[Data Pours from Cloud—And 'The Enemy is Us'](#)

Threatpost - 6 Nov 2017

From December 2016 into the first part of 2017, the nonprofit **GDI Foundation** tracked close to 45,000 open MongoDB databases in which hackers dropped database tables or locked out legitimate users to extort a ransom payment. In a separate study by GDI in August, it tracked a second wave of these attacks, resulting in a ...



[Hundreds of Printers Expose Backend Panels and Password Reset ...](#)

BleepingComputer - 5 Oct 2017

"I am planning to reach and notify the orgs with my colleague," Anubhav said. Bleeping Computer also forwarded the list to fellow researcher Victor Gevers. Gevers is the chairman of the **GDI Foundation**, a non-profit that specializes in notifying organizations affected by vulnerabilities, malware, and other cyber threats.



InfoSecWorld
Conference & Expo 2018

How

GDI Foundation
@GDI_FDN Follows you

Tweets 7,914 Following 1,892 Followers 2,954 Likes 4,326

GDI Foundation
@GDI_FDN Follows you

Non-profit organization. Our mission is to defend the free & open Internet by trying to make it safer. We address security issues via Responsible Disclosure.

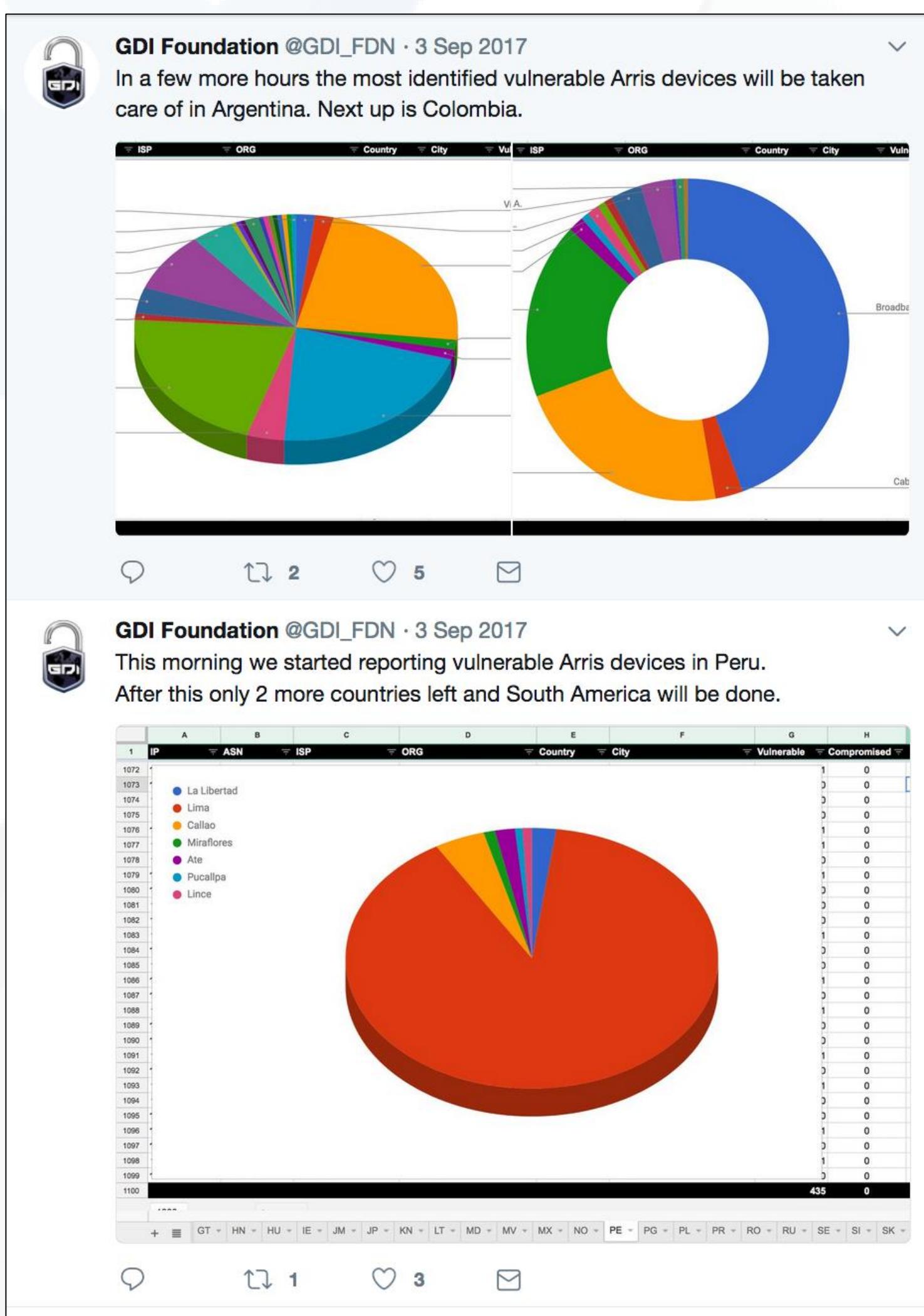
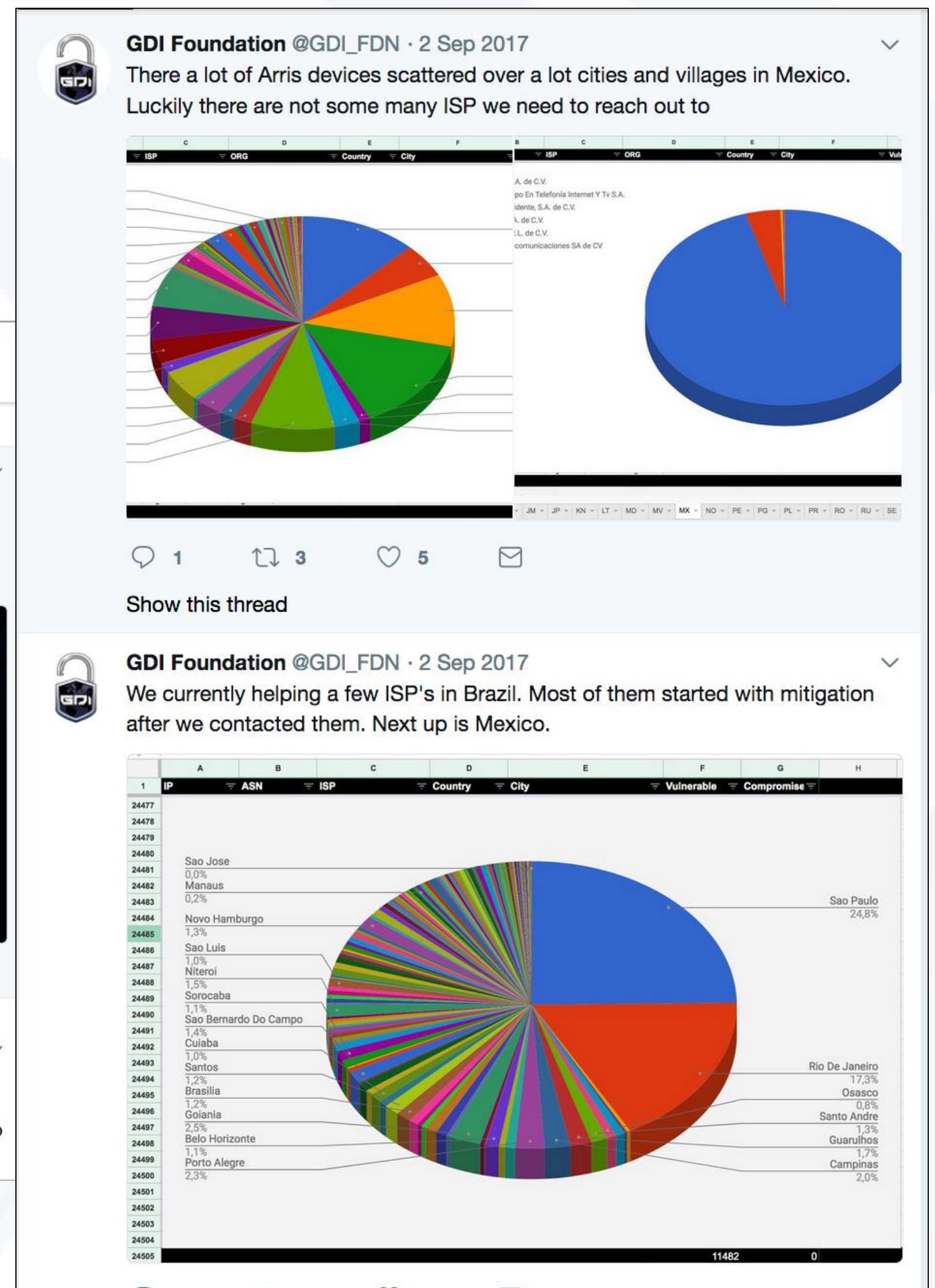
📍 The Hague, The Netherlands
🔗 GDI.foundation
📅 Joined July 2012

GDI Foundation @GDI_FDN · 10h
We want to express our deep gratitude to all ISPs, involved organizations and volunteers for their contribution to help to address the issue of vulnerable Memcached servers. Thank you so much for your effort. We could not have achieved this level of success without your help.



1 3 5 10

↳ GDI Foundation Retweeted
InfoSec World @InfoSec_World · Mar 8
The GDI.foundation helps victims of ransom attacks worldwide. @0xDUDE, chairman & co-founder of @GDI_FDN, will share the experiences and challenges they have faced as a non-profit organization so far at #InfoSecWorld 2018. okt.to /Be6a94



The “law”

ars TECHNICA UK BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS ☰

YOU WIN SOME, YOU LOSE SOME —

Your dynamic IP address is now protected personal data under EU law

CJEU rules that personal IPs can't be stored, unless to thwart cybernetic attacks or similar.

GLYN MOODY - 19/10/2016, 14:24

20

Europe's top court has ruled that dynamic IP addresses can constitute "personal data," just like static IP addresses, affording them some protection under EU law against being collected and stored by websites.

But the Court of Justice of the European Union (CJEU) also said in its judgment on Wednesday that one legitimate reason for a site operator to store them is "to protect itself against cyberattacks."

The case was referred to the CJEU by the German Federal Court of Justice, after an action brought by German Pirate Party politician Patrick Breyer. He asked the courts to grant an injunction to prevent websites that he consults, run by federal German bodies, from collecting and storing his dynamic IP addresses.

EU Law Analysis

Expert insight into EU law developments

WEDNESDAY, 4 JANUARY 2017

IP addresses as personal data - the CJEU's judgment in C-582/14 Breyer



Marcin Kotula, Legal Officer at the European Commission

The views expressed are purely those of the author and may not in any circumstances be regarded as stating an official position of the European Commission

Background

In the *Breyer* case the CJEU was asked by the German Supreme Court (Bundesgerichtshof) if dynamic IP addresses are personal data within the meaning of the [EU Data Protection Directive](#) and to what extent they can be stored and processed to ensure the general operability of websites. [Mr Breyer](#), the applicant in this case, is a German politician and privacy activist. He visited various websites of the German federal institutions. The information about the IP addresses of the visitors (or more precisely of the owners of the devices from which the websites were visited) as well as the information about the name of the accessed web page or file, the terms entered in the search fields, the time of access and the quantity of data transferred is stored in the log files after the visit.

PAGES

[Studying EU Law: A Law Student's Guide \(updated Oct 2016\)](#)

[Follow this blog on Facebook and Twitter](#)

[Using this blog with Barnard & Peers, European Union Law](#)

[Blog contributors](#)

[Would you like to write for this blog?](#)

SEARCH THIS BLOG

FOLLOW BY EMAIL

BLOG ARCHIVE

- ▼ 2017 (30)
 - April (1)
 - March (10)
 - February (6)
 - ▼ January (13)
 - Foreign fighters' helpers excluded from refugee st...

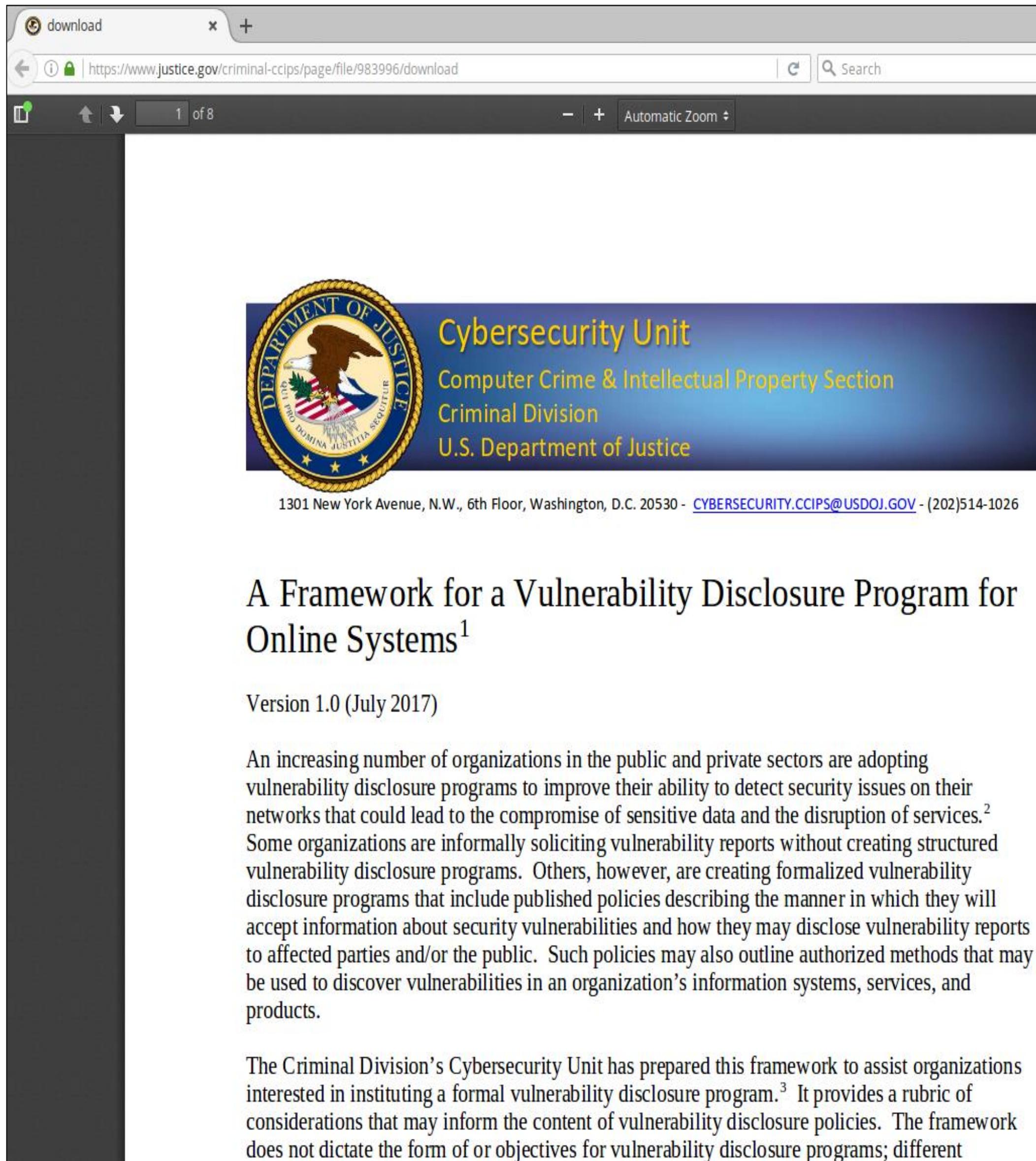
[The UK Brexit Euratom: Legal Framework and Future...](#)

[Brexit and the Safeguard of EU Transnational Right...](#)

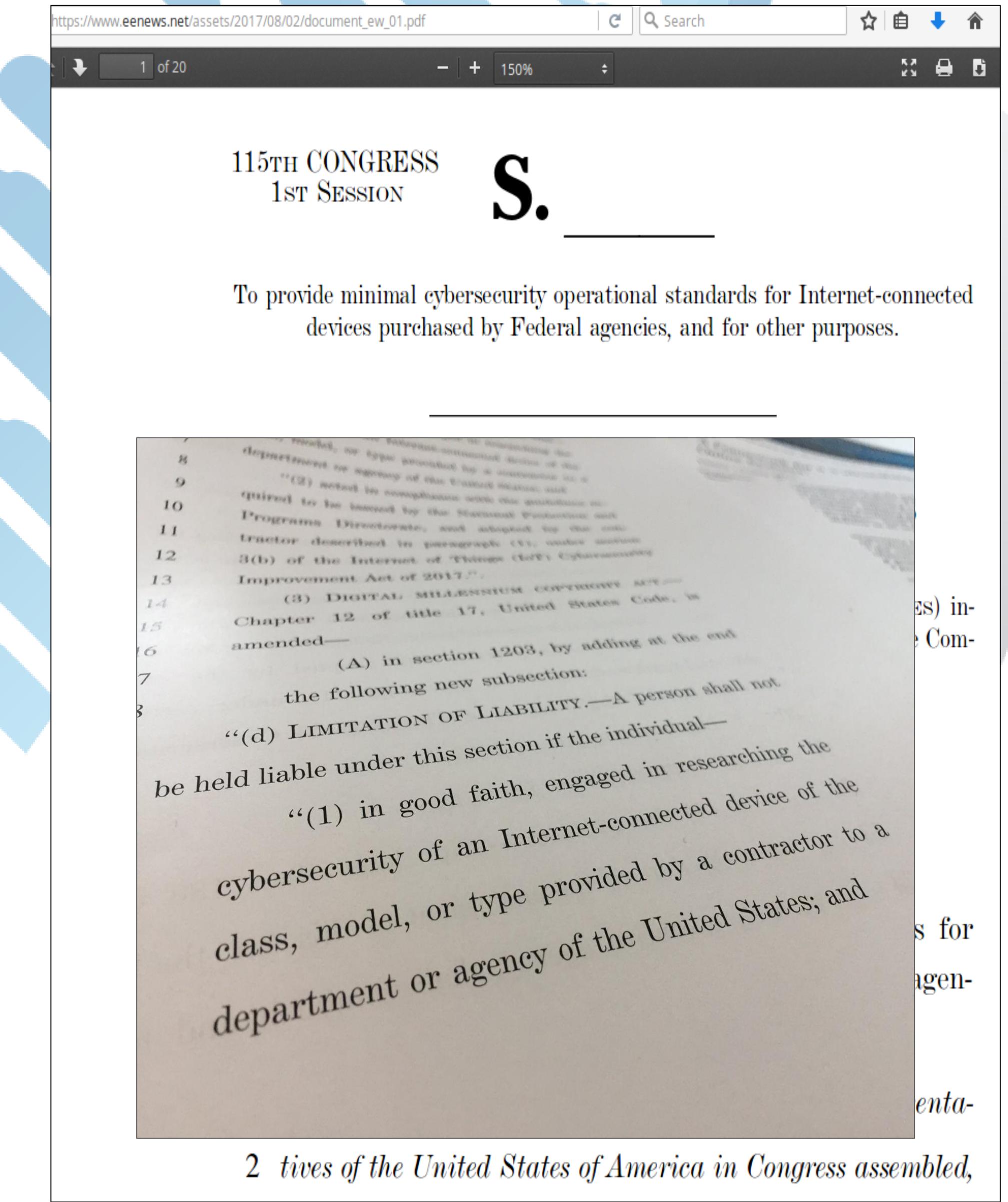
[The judgment in Miller: Representative Democracy S...](#)

[When is Facebook liable for illegal content under ...](#)

Law (making)

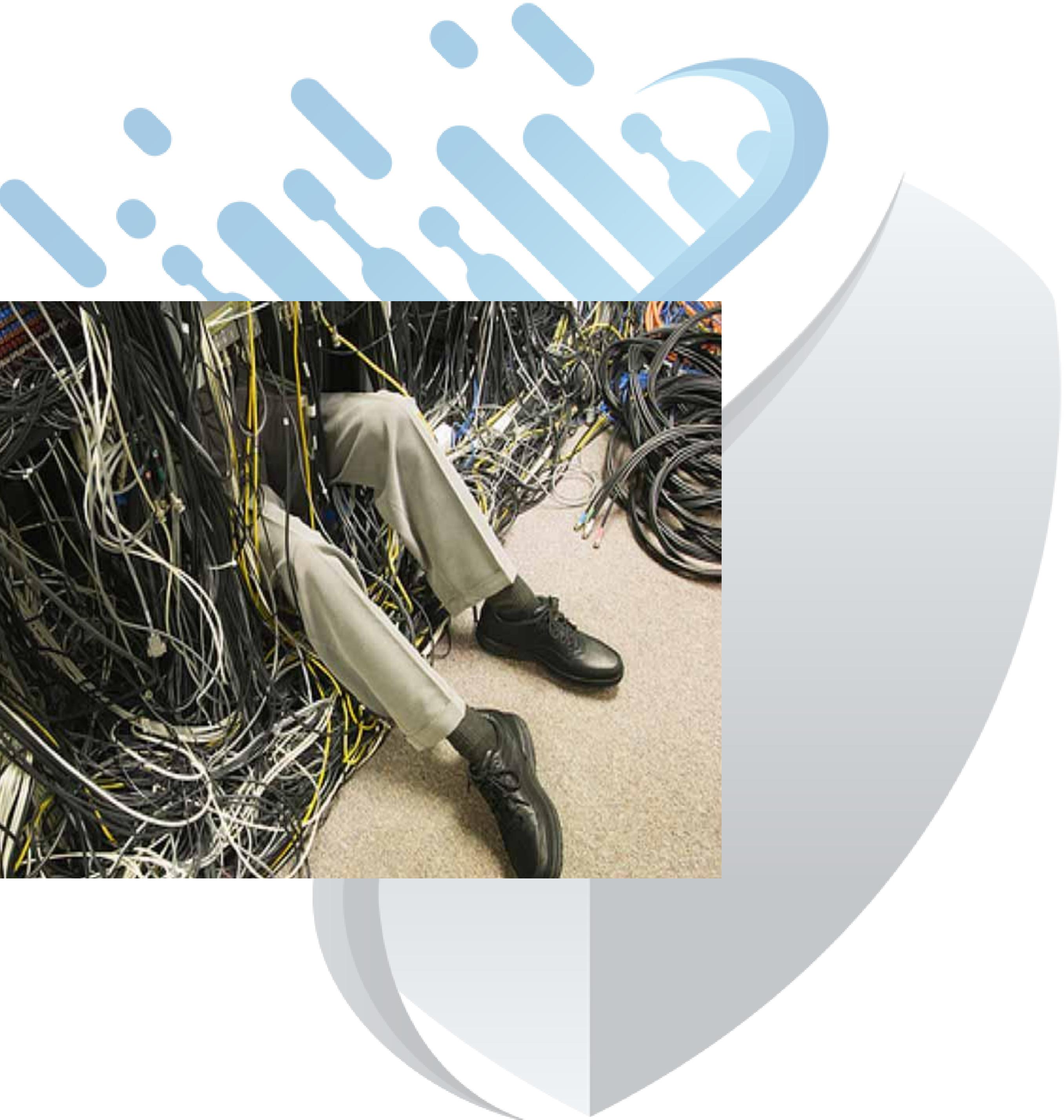
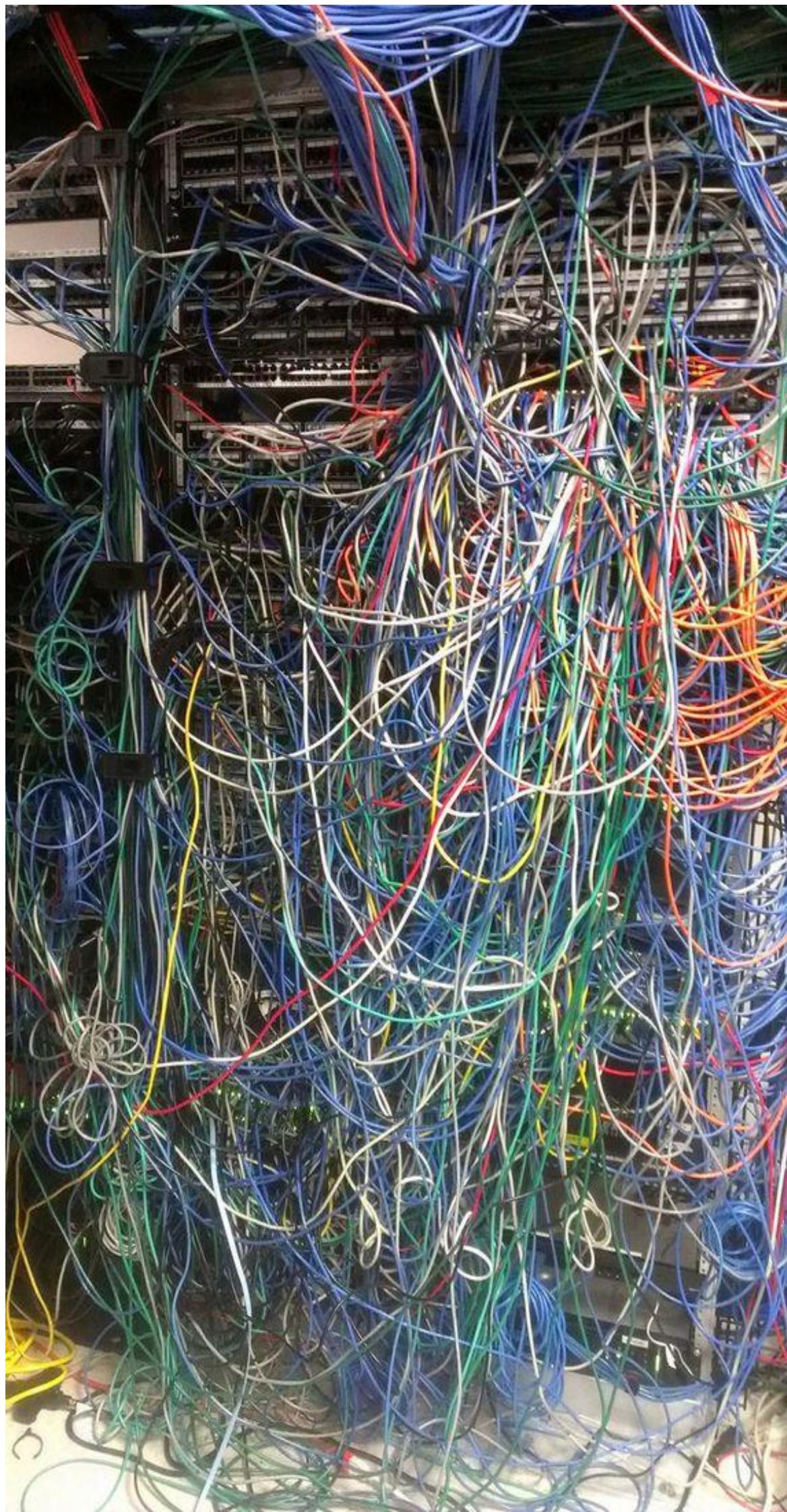


The screenshot shows a web page from the U.S. Department of Justice's Cybersecurity Unit. The header includes the DOJ seal and text: "Cybersecurity Unit", "Computer Crime & Intellectual Property Section", "Criminal Division", and "U.S. Department of Justice". Below the header is an address: "1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026". The main title is "A Framework for a Vulnerability Disclosure Program for Online Systems¹". Below the title is the subtitle "Version 1.0 (July 2017)". The text discusses the increasing number of organizations adopting vulnerability disclosure programs and the need for formalized programs. It also mentions the Criminal Division's Cybersecurity Unit preparing this framework. The footer states: "The Criminal Division's Cybersecurity Unit has prepared this framework to assist organizations interested in instituting a formal vulnerability disclosure program.³ It provides a rubric of considerations that may inform the content of vulnerability disclosure policies. The framework does not dictate the form or objectives for vulnerability disclosure programs; different



The screenshot shows a PDF document from EENews.net. The title reads "115TH CONGRESS 1ST SESSION S. [redacted]". The text describes the bill's purpose: "To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes." The document contains several numbered sections and subsections, some of which are redacted. A large portion of the text is obscured by a large blue rectangular redaction box. At the bottom, there is a note: "2 tives of the United States of America in Congress assembled," followed by a large blue abstract graphic.

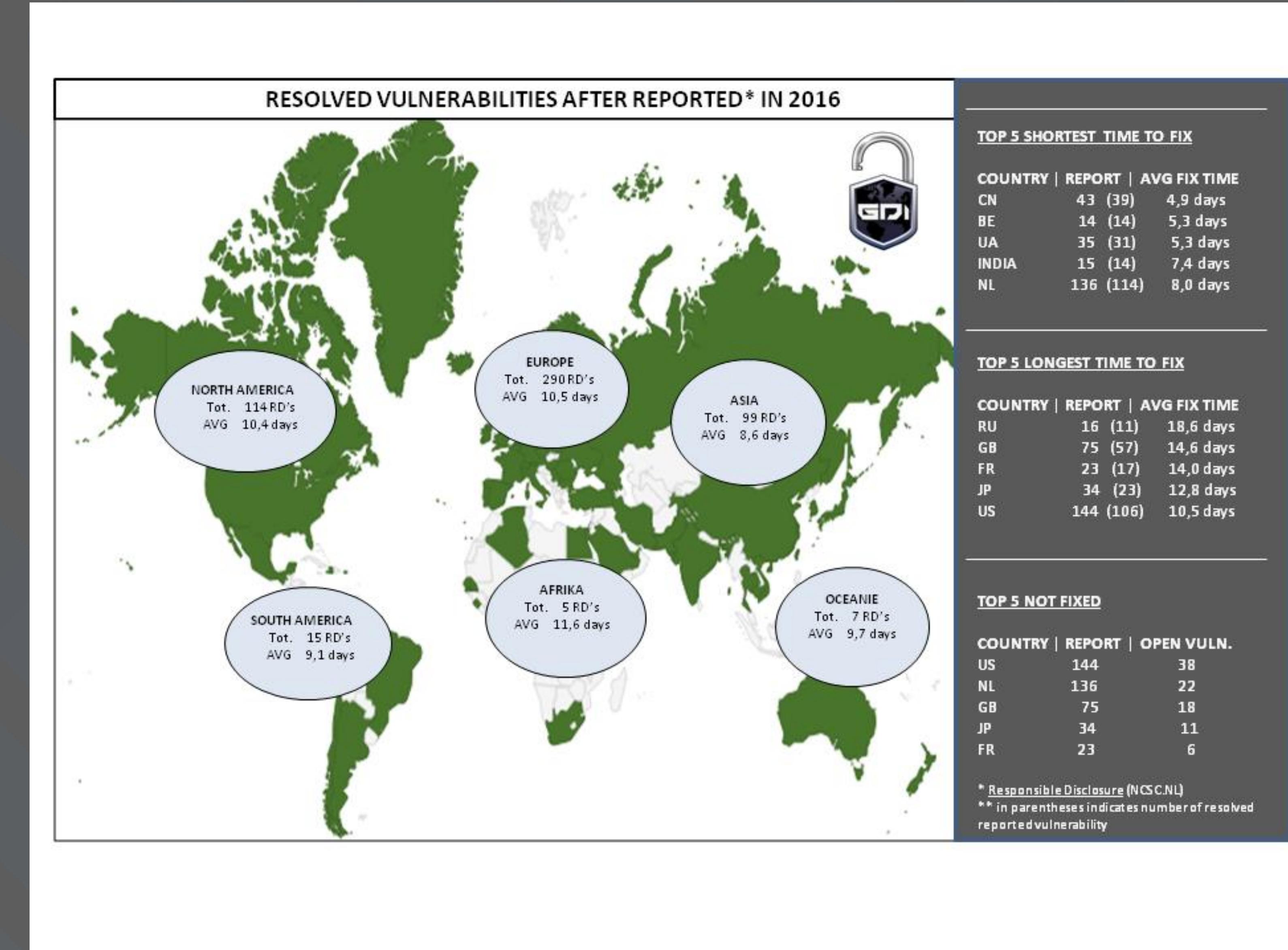
The Internet landscape (today)



2016

Body Level One
Body Level Two
Body Level Three
Body Level Four
Body Level Five

Insert Metrics



2017

Screenshot 2017
WSJ report

2018

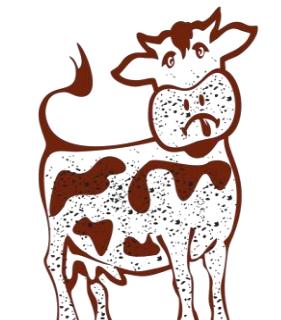
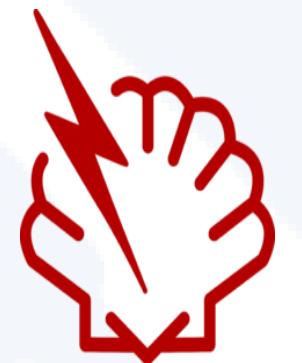
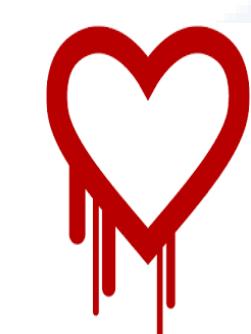
GDI foundation - Overview 2018

File Edit View Insert Format Data Tools Add-ons Help All changes saved in Drive

fx

	A	B	C	D	E
1	Found	Comprised	Reported	Fixed	
2	AWS S3 [scanner]	536	1	529	109
3	Cassandra	1.432			
4	CouchDB	16.372	1.203	9.032	8.039
5	Elasticsearch	7		7	6
6	Hadoop HDFS	5.778			
7	Jenkins	6.661	27	54	50
8	MongoDB	18	15	18	18
9	Redis	21.382			
10	Vuln: EternalBlue	7.493		14	14
11	Github Scanner				
12	Hardware (default creds)	42.401	42.401	6	4
13	Memcached	107.431	19	7.684	6.475
14	DNSmasq	1.266.907			
15	GSoap	187.721			
16	IOT Devices	193.893			
17	Palo Alto RCE CVE-2017-15944	27.392			
18	Exim CVE-2017-16943	6.401.689			
20	PostgreSQL	1	0	1	1
21	RiaK	178			
22	IEC 60870-5-104	569			
23	SIMATIC 30 "Tecnodrone"	2.778			
24	GE-SRTP	20.352			
25	PLC	788		2	2
26	FINS	1.155			
27	ProCroNos	180			
28	HART	121			
29	Red Lion Controls	1.088		1	1
30	Modbus	13.817		1	1
31	DNP3	347			
32	Niageria Fox	49.766			
33	MELSEC-Q	114			
34	BACnet	13.744		1	1
35	EtherNET	28.656			
36	CODESYS	2.154			
37	MQTT	36.554		2	1
38	TR-069	24.745.091		1	1
39		33.204.568	43.668	17.355	14.725

Current Internet Landscape



DIRTY COW



InfoSecWorld
Conference & Expo 2018

Data Leaks



GDI.foundation / Active dataleaks

New Add Save Open Share Options Reporting Last 90 days

Hacked IPs: 23,411

Found in online Blacklist(s): 2,821

Active dataleaks:

location.country.keyword: Descending	Count	Count	
United States	8,712	Hangzhou	2,735
China	5,074	New York	1,696
France	1,129	Boardman	1,050
Germany	833	Beijing	1,007
Netherlands	801	Ashburn	958
Singapore	785	Singapore	742
United Kingdom	644	Amsterdam	582
Canada	581	San Francisco	492
Japan	514	Dublin	382
Russian Federation	479	Frankfurt	340

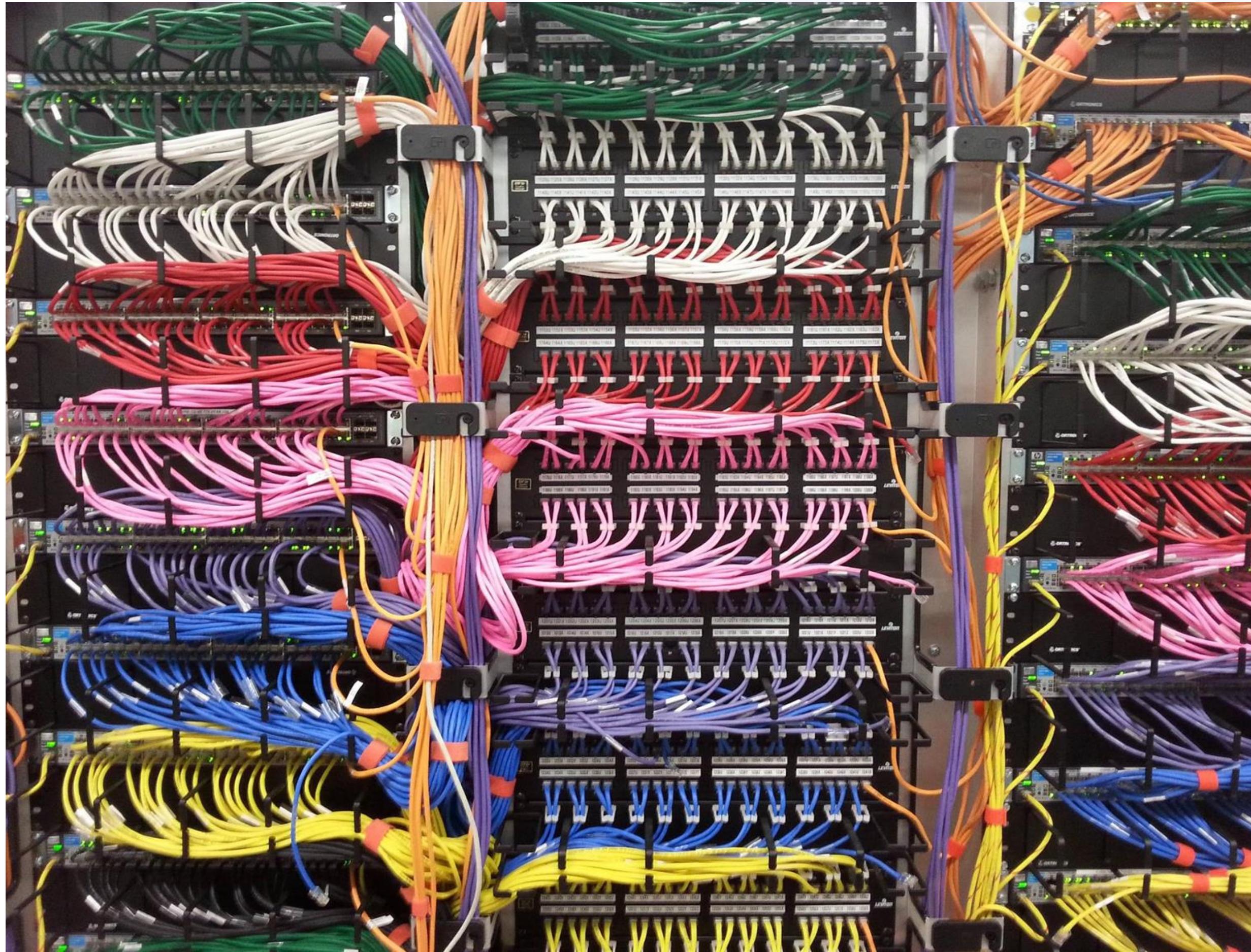
Export: Raw Formatted

Export: Raw Formatted

1 2 3 4 5 ...10 >

1 2 3 4 5 ...10 >

Getting the overview



Finding vulnerabilities

■ Searching the internet

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

Date	Title	Category
2018-03-12	ext:pem "PRIVATE KEY" -site:facebook.com -example -test*	Files Containing Juicy Info
2018-03-12	inurl:control/camerainfo	Various Online Devices
2018-03-12	"IBM Security AppScan Report" ext:pdf	Network or Vulnerability Data
2018-03-12	inurl:"/etc/fail2ban/" + ext:conf	Files Containing Juicy Info
2018-03-07	intext:"Powered by ViewVC" intitle:"ViewVC Repository Listing"	Sensitive Directories
2018-03-07	inurl:cloud_main.asp	Various Online Devices
2018-03-07	inurl:"server-status" "Server Version: Apache/" "Server Built: " "Server uptime:" "Total accesses" "CPU.....	Web Server Detection
2018-03-07	"database_password" filetype:yml "config/parameters.yml"	Files Containing Passwords
2018-03-07	inurl::5601/app/kibana	Various Online Devices
2018-03-05	Joomla! com_joomanager - Arbitrary File Download	Vulnerable Servers

Google

All Maps Videos News Shopping More Settings Tools

About 3.490 results (0,22 seconds)

Rental Properties - Cornerstone Property Solutions
[www.cpsnorthfl.com/index.php?option=com_joomanager&view=itemlist...32... ▾](http://www.cpsnorthfl.com/index.php?option=com_joomanager&view=itemlist...32...)
Association, Property, & Condominium Management in Gainesville, FL.

planteis - Clube Desportivo 1º de Agosto
[1agosto.com/.../index.php?option=com_joomanager...task... - Translate this page](http://1agosto.com/.../index.php?option=com_joomanager...task...)
No information is available for this page.
Learn why

Joomanager Component - Joomla Templates
[www.shape5.com/demo/real_estate/index.php?option=com_joomanager&view... ▾](http://www.shape5.com/demo/real_estate/index.php?option=com_joomanager&view...)
Joomla! - the dynamic portal engine and content management system.

Joomanager Item List - Joomla Templates
[www.shape5.com/demo/portfolio/index.php?option=com_joomanager&view... ▾](http://www.shape5.com/demo/portfolio/index.php?option=com_joomanager&view...)
Joomla! - the dynamic portal engine and content management system.

Rob Marland Listings
[www.robmarland.com/index.php?option=com_joomanager&view=items ▾](http://www.robmarland.com/index.php?option=com_joomanager&view=items)
Home · Listings · Current Listings · Past Sold Listings · For Sellers · Property Evaluation · Marketing

Finding vulnerabilities

- Searching the internet
- Scraping everything what is public

<https://www.cvedetails.com/cve/CVE-2017-16943>

CVE Details

The ultimate security vulnerability datasource

Log In Register

Switch to https://

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :

- NVD Website

Vulnerability Details : CVE-2017-16943

The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands.

Publish Date : 2017-11-25 Last Update Date : 2017-12-07

CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Execute Code
CWE ID	416

Products Affected By CVE-2017-16943

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Debian	Debian Linux	9.0				Version Details Vulnerabilities
2	Application	Exim	Exim	4.88				Version Details Vulnerabilities
3	Application	Exim	Exim	4.89				Version Details Vulnerabilities

Google

site:github.com "CVE-2017-16943"

All News Maps Images Shopping More Settings Tools

Past week ▾ Sorted by relevance ▾ All results ▾ Clear

Blackrush / PoC-Bank

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights

A collection of Some PoC and Exploit

24 commits 1 branch 0 releases 1 contributor MIT

Branch: master New pull request Create new file Upload files Find file Clone or download

Blackrush add Exim PoC Latest commit 695989d 4 days ago

CVE-2017-17562 Delete update-CVE-2017-17562.py 2 months ago

CVE-2015-1635.py Add CVE-2015-1635 2 months ago

CVE-2016-3088.py Add CVE-2016-3088 PoC -- ActiveMQ 2 months ago

CVE-2017-10271.py modify payload 2 months ago

CVE-2017-12615.py add CVE-2017-12615.py 2 months ago

CVE-2017-12794.py Add CVE-2017-12794.py 2 months ago

CVE-2017-15944.py add Palo Alto Networks firewalls RCE PoC 5 days ago

CVE-2017-16943.py add Exim PoC 4 days ago

CVE-2017-5638.py Update CVE-2017-5638.py -- S2-045 PoC 2 months ago

CVE-2018-0802.py Add CVE-2018-0802.py PoC 2 months ago

LICENSE Initial commit 2 months ago

MemcacheUDPExploit.py add memcache udp ddos exploit implemented with scapy 5 days ago

MemcachedUDPDdos.py Add memcache ddos poc 11 days ago

README.md Initial commit 2 months ago

RedisUnauthorize.py Add redis-server unauthorize vulnerability PoC 2 months ago

Heartbleed



443.https.heartbleed.heartbleed_vulnerable:true

IPv4 Hosts Top Million Websites Certificates

WARNING: A total 115754 hosts matched your search query. Only the first 500 are displayed. Please try a more specific query.



Google

heartbleed

All Images News Videos Books More Settings Tools

About 26.300 results (0,13 seconds)



Researcher: DJI RCE-holes offered me \$500 after I found ...

The Register - 28 Nov 2017

Updated Chinese drone-maker DJI's bug bounty programme has been struck with fresh controversy after a security researcher claimed he was offered just \$500 for reporting, among others, the years-old **Heartbleed** vulnerability. Infosec chap Sean Melia – no stranger to bug bounty programmes – said he ...



Biometrics and Next-Gen Security for Innovative Firms

Accountingweb.com - 1 Mar 2018

Only five years ago protecting your firm and your clients meant safety from things like **Heartbleed** in OpenSSL technology. Last year, that meant learning about the different types of cloud storage. Today, it's about understanding the basics of biometrics identification, technology that identifies or authenticates ...



Oracle rushes out 5 patches for huge vulnerabilities in PeopleSoft ...

Ars Technica - 16 Nov 2017

The five vulnerabilities include one dubbed "JoltandBleed" by the researchers because of its similarity to the **HeartBleed** vulnerability discovered in OpenSSL in 2014. JoltandBleed is a serious vulnerability that could expose entire business applications running on PeopleSoft platforms accessible from the ...

Oracle pushes emergency patch for critical Tuxedo server ...
ZDNet - 16 Nov 2017



Heartbleed Persists on 200000 Servers, Devices

Threatpost - 23 Jan 2017

Almost 200,000 servers and devices are still vulnerable to **Heartbleed**, the OpenSSL flaw patched nearly three years ago. The numbers come from search engine Shodan, which released data showing U.S. servers hosted on Amazon AWS are disproportionately vulnerable to the flaw. "There's a lot to be ...

Heartbleed: 200000 websites and systems still vulnerable to ...
www.theinquirer.net - 23 Jan 2017



Gloucester City Council fined £100000 over **Heartbleed** hack

IT PRO - 14 Jun 2017

Gloucester City Council has been hit with a £100,000 fine after a hacker downloaded 30,000 emails containing employees' personal information. In July 2014, a hacker "took advantage of a weakness in the council's website" to gain direct access to the council's mailboxes, which stored information on ...



That **Heartbleed** problem may be more pervasive than you think

Network World - 27 Jan 2017

That lingering **Heartbleed** flaw recently discovered in 200,000 devices is more insidious than that number indicates. According to a report posted by Shodan, the **Heartbleed** vulnerability first exposed in April 2014 was still found in 199,594



InfoSecWorld
Conference & Expo 2018

Heartbleed

censys 443.https.heartbleed.heartbleed_vulnerable:true "bank"

IPv4 Hosts Top Million Websites Certificates Tools Help

Results: 765,854 Time: 207ms

DID YOU SAY "LEADS?"

UM, YEA...WE'RE A BANK. WE DON'T REALLY DO THAT TYPE OF THING...net

BNZ-NZ – Bank of New Zealand NZ-based networks (NZ)
Routing via AS11164, AS4637, AS9901, AS4768, AS17472
Protocols 443/HTTPS
Tags https, heartbleed

ATTICA-BANK – Attica Bank S.A (GR)
Routing via AS7018, AS1299, AS12713, AS6799, AS41579
Protocols 443/HTTPS
Tags https, heartbleed

BELSVYAZ-AS – PJSC Rostelecom (RU)
Routing 82.151.96.0/19 via AS6939, AS12389, AS44237, AS29456
Protocols 80/HTTP, 23/TELNET, 993/IMAPS, 995/POP3S, 25/SMTP, 110/POP3, 143/IMAP, 53/DNS, 443/HTTPS
Tags http, pop3s, smtp, heartbleed, imaps, pop3, https, dhe-export, rsa-export, imap

rusnarbank.ru)



InfoSecWorld
Conference & Expo 2018

Devices



Discover Overview Pricing

Documentation Help My Account ▾

Found about **13,193** results (0.13 seconds).

Query Credits Count: **99**

Filter By

197.0.140.197

Tunisia BackBone AS

2016-09-

HTTP (80/TCP)

Service Port

80

443

49154

7547

Type Webcam

Response

Last-Modified: Fri, 18 Dec 2011 09 GMT
Server: DNVRS-Webs
Keep-Alive: timeout=60, max=99
ETag: "0-848-1e0"
Content-Length: 480
Content-Type: text/html
Connection: keep-alive
Date: Sat, 24 Sep 2016 03:23:29 GMT

Name DNVRS-Webs

Device Type

Router

Firewall

ICS

Modem

Gateway

Website

SHODAN

linux upnp avtech

Explore

Exploits Maps Like 2,766 Download Results Create Report

TOP COUNTRIES

Total results: 109,258

Country	Results
Mexico	15,496
Indonesia	15,246
Viet Nam	11,082
Thailand	8,883
Malaysia	5,754

Brickers, Cure, Wipers

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES Q

Twitter Facebook Google+ LinkedIn

Security

Forget Mirai – Brickerbot malware will kill your crap IoT devices

Rogue code aims to create permanent DoS

8 Apr 2017 at 09:32, Iain Thomson



A new form of attack code has come to town and it uses techniques similar to Mirai to permanently scramble Internet of Things devices.

On March 20 researchers at security shop Radware spotted the malware, dubbed Brickerbot, cropping up in honeypots it sets up across the web to lure interesting samples. In the space of four days, one honeypot logged 1,895 infection attempts by Brickerbot, with the majority of attacks coming from Argentina, and a second logged 333 attempts – untraceable as they came from a Tor node.

"The Bricker Bot attack used Telnet brute force – the same exploit vector used by Mirai – to breach a victim's devices," Radware's advisory states.

"Bricker does not try to download a binary, so Radware does not have a complete list of credentials that were used for the brute force attempt, but were able to record that the first attempted username/password pair was consistently 'root'/vizxv."

The malware targets Linux-based IoT devices running the BusyBox toolkit, and seems to have a particular affinity for Ubiquiti network devices, which have their own security issues. Once inside the operating system, the code starts to scramble the onboard memory using rm -rf /* and disabling TCP timestamps, as well as limiting the max number of kernel threads to one.

```
1 fdisk -l
2 busybox cat /dev/urandom >/dev/mtdblock0 &
3 busybox cat /dev/urandom >/dev/sda &
4 busybox cat /dev/urandom >/dev/mtdblock10 &
5 busybox cat /dev/urandom >/dev/mmc0 &
6 busybox cat /dev/urandom >/dev/sdb &
7 busybox cat /dev/urandom >/dev/ram0 &
8 fdisk -C 1 -H 1 -S 1 /dev/mtd0
```

BrickerBot the work of a vigilante?

All in all, BrickerBot isn't like anything we've seen before in the landscape of IoT malware. Most IoT malware strains try to hoard devices in massive botnets that are then used as proxies to relay malicious traffic or to launch DDoS attacks. Both of these are lucrative businesses for any cyber-criminal talented enough to hijack large numbers of IoT equipment.

BrickerBot's destructive capabilities are something new, which don't benefit anyone. Not BrickerBot's author, and certainly not the device owner, who'll have to reinstall firmware, or even worse, buy a new device.

BrickerBot could also be the work of an Internet vigilante that wants to destroy insecure IoT devices. A similar malware strain first appeared in October 2015.

Called Linux.Wifatch, this IoT malware strain took over insecure routers and then executed commands that improved the device's security. The creators of this malware open-sourced the code on GitLab, also explaining the reasons why they created the malware to begin with, claiming they had no bad intentions.

BrickerBot is bent on destroying IoT devices

The same cannot be said for BrickerBot's author, who clearly is intent on wiping as much of unsecured IoT devices as he can.

"Wow. That's pretty nasty," said Cybereason security researcher Amit Serper after Bleeping Computer showed him Radware's security alert. "They're just bricking it for the sake of bricking it. [They're] deliberately destroying the device."

"It's someone who wanted to clean up the mess in a harsh way," said Victor Gevers, chairman of the GDI.foundation, a security expert that tracked the destructive ransom attacks against MongoDB servers that took place at the start of the year.

"Very effective and in some point very risky because attacking devices without knowing their exact duty could be dangerous," Gevers added. "Imagine you disable a security camera of an embassy. Is that an act of aggression towards a country?"

BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices

By Catalin Cimpanu

December 11, 2017 07:35 PM 1



The author of the BrickerBot malware has announced his retirement in an email to Bleeping Computer, also claiming to have bricked over 10 million devices since he started the "Internet Chemotherapy" project in November 2016.

Databases



Andreas Nilsson
January 06, 2017

Category: Company

Recently, there have been reports of malicious attacks on unsecured instances of MongoDB running openly on the internet. The attacker erased the database and demanded a ransom be paid before restoring it.

If you believe your database was attacked, see these [suggested steps](#).

These attacks are preventable with the extensive security protections built into MongoDB. You need to use these features correctly, and our security documentation will help you do so. Here are pointers to the relevant documentation and other useful resources:

- Security is addressed in detail in our [Security Manual](#). We also recently expanded our [online training on security](#) as part of the MongoDB University curriculum.
- Follow the steps in our [Security Checklist](#). It discusses enforcing authentication, enabling access control, limiting network exposure, and other important best practices.
- The most popular installer for MongoDB (RPM) limits network access to localhost by default. Use this configuration too if you're installing via another means.
- [MongoDB Cloud Manager](#) and [MongoDB Ops Manager](#) provide continuous backup with point in time recovery, and users can enable alerts in Cloud Manager to detect if their deployment is internet exposed (see Figure 1 below).

BBC NEWS

Sign in | News | Sport | Weather | Shop | Earth | Travel

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts | Technology

Web databases hit in ransom attacks

6 January 2017 | Technology

Share



Gigabytes of medical data was deleted from one vulnerable database

Thousands of web-based databases have been deleted by cyberthieves seeking a ransom to restore the data.

Gigabytes of medical, payroll and other data held in MongoDB databases have been taken by attackers, say security researchers.

The systems were vulnerable to attack because their administrators accidentally left them easily accessible via the internet.

Attackers are seeking small amounts of bitcoins as payment to restore data.

The alarm about hackers targeting the vulnerable databases was raised by Victor Gevers - an ethical hacker who currently works for the Dutch government.

 Victor Gevers
@0xDUDE

Open MongoDB = Money 4 bad ppl.

SEND 0.2 BTC TO THIS ADDRESS AND CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !

```
victor@windowlicker:~$ mongo --host [REDACTED]
MongoDB shell version v3.4.1
connecting to: mongodb://[REDACTED]
MongoDB server version: 2.2.0
WARNING: shell and server versions do not match
> show dbs
WARNING          0.203GB

> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harakir1@sigaint.org",
  "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNc2jyvDRhLyvpkCh323MsMq AND CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
> exit
bye
victor@windowlicker:~$ ^C
victor@windowlicker:~$
```

RETWEETS LIKES
194 124

10:52 PM - 27 Dec 2016

pastebin.com/raw/ciVmzwHg

selling Kraken DB Ransomware Kit c# source code

Kit source price: 500USD in bitcoins
we also sell compiled binary ready to work for 100usd total for both

This shit is very fast Multi-Threaded can handle 1000+ ips per second and way more if you got powerful 10GBs port
CPU load is very low, RAM is important if you have big ip list.

what you'll get :
* kraken Mongodbs ransomware source code
* kraken Elastic Search ransomware source code
* 100,000 ip list with mongodb open
* 30,000 ip:port list with Elastic Search open
* mass mongodb & Elastic Search scanner to scan the whole internet ip range for open dbs

Email: kraken0@india.com
jabber: kraken0@exploit.im (for fast communication)

Ransom (Ransack attacks)

The screenshot shows a MongoDB interface with several windows:

- MongoVUE**: A database management tool with a "Database Explorer" sidebar listing databases like aim-bazooka, aimlog, bifrost, chute, documents, local, patient-server, process, scheduling, security, and ui-metadata. The "Databases" and "Server Status" panes are open.
- Command Prompt**: A terminal window showing the command `mongo` being run, connecting to a MongoDB shell version 3.2.0, and listing all databases and their sizes.
- News Article**: A news article titled "LA Hospital Hit By Ransomware Pays Hackers \$17,000: Is It The Right Choice?" by Alyssa Navarro from Tech Times. It discusses the Hollywood Presbyterian Medical Center's ransomware attack and its decision to pay \$17,000.
- Censys**: A security tool showing a certificate chain for a domain, listing issuers like Go Daddy Secure Certification Authority and The Go Daddy Group, Inc.
- 22/SSH**: A banner grab from port 22 showing the text "Heartbleed Heartbeat Enabled. Immune to Heartbleed."

Internet of Toys

The Washington Times

HOME NEWS ▾ OPINION ▾ SPORTS ▾ MARKET ▾ SUBSCRIBE



Kids toy CloudPets target of major data breach; millions of audio messages compromised: Report

FREE Shipping for Active Duty Military!

Contact

CloudPets

Home How It Works Getting Started Support Buy Now

It's likely the attack against the CloudPets data was random and targeted exposed MongoDB instances instead. Spiral Toys said the database in question belong to a contracted third party that was performing a migration on behalf of the company. Spiral Toys said this was a temporary scenario, and as a result, it never received a ransom demand. The company also denied knowing about the breach until Feb. 22.



Troy Hunt @troyhunt

Following

So @0xDUDE tried to get in touch with CloudPets NINE TIMES before their database was eventually wiped and ransomed. 9 times!!!

30-12-2016 10:42PM Reported data leak by email to support@cloudpets.com
30-12-2016 10:43PM Filled in the contactform on the website
30-12-2016 11:22PM Reached out to Spiral via Twitter
31-12-2016 10:50PM Send an email warning note to Mark Mizuguchi
31-12-2016 1:59PM Created a ticket in <http://Zendesk.com> of which I received an automatic confirmation email:
<https://twitter.com/0xDUDE/status/836497591953154048>
31-12-2016 2:37PM - Forwarded the email to investor@spiraltoys.com
31-12-2016 10:51PM - Warned Mark Meyers via a LI invite
04-01-2017 - DM contact Lorenzo from

RETWEETS LIKES
67 88



10:36 AM - 3 Mar 2017

Sharing LOCs via Google (Sheets)

MongoDB ransacking										
Alle wijzigingen zijn opgeslagen in Drive										
	Bestand	Bewerken	Weergeven	Invoegen	Opmaak	Gegevens	Extra	Add-ons	Help	
					\$ % .0 .00	Arial	10	B	<i>I</i>	<u>S</u>
fx	04-04-2017		B	C	D	E	F	G	H	I
1	https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransom-your-data									
2	Last Sighted on	Email Address(Sighted As)	Bitcoin Address	Ransom size	Total Number of Transactions	BTC Received	Name of replaced DB	Known Attacker IPs	Victims (OSINT)	Victims (helped)
57	10-1-2017 14:00:00	bitcoinbaron@protonmail.com	17KdFUA9WJTTwYNp4iRPjLyLDkBfz2zj6	0.2BTC			REDACTED			18
58	<p>Google search results for Bitcoin Address 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02. The search bar shows the address. Results include links to blockchain.info and Twitter posts from Victor Gevers.</p>									
59	<p>New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 goo.gl/VKKR1c</p> <p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
60	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
61	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
62	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
63	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
64	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
65	11									
66										
67	11									
68										
69	16									
70										
71										
72	16									
73	19									
74										
75	1-1									
76										
77	31.01.2017 08:30	m4l1c3@sigaint.org	1B5PMtKhqC97ppNrixflyT1chQuvDGXXei	0.5BTC						
78	08-02-2017 20:57		1NHrbhXmSzzCa8VhWqsza82NaUynxs	0.5BTC						
79										
80	14-03-2017	vxware@sigaint.org	1B4kMRmY4yb4XW8hHnYRZT1WWNfnPfPbHR	0.2BTC						
81										
82	04-04-2017	mongodb@protonmail.ch	15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02	0.1 BTC						
83										
84	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<p>Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTS02 / DB_DROPPED / IP 62.244.25.212 ..."</p>									
	<img alt="Screenshot of a tweet from Victor Gevers (@0xdude) about the MongoDB ransom									

IoT Botnets for DDoS attacks



FEATURE

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Mirai took advantage of insecure IoT devices in a simple but clever way. It scanned big blocks of the internet for open Telnet ports, then attempted to log in default passwords. In this way, it was able to amass a botnet army.



By **Josh Fruhlinger**
CSO | MAR 9, 2018 3:00 AM PT

KrebsOnSecurity

In-depth security news and investigation



01 Source Code for IoT Botnet ‘Mirai’ Released

OCT 16

The source code that powers the “Internet of Things” (IoT) botnet responsible for launching the [historically large distributed denial-of-service \(DDoS\) attack](#) against KrebsOnSecurity last month has been publicly released, virtually guaranteeing that the Internet will soon be flooded with attacks from many new botnets powered by insecure routers, IP cameras, digital video recorders and other easily hackable devices.

KrebsOnSecurity

In-depth security news and investigation

Posts Tagged: Mirai botnet

4 Did the Mirai Botnet Really Take Liberia Offline?

NOV 16

KrebsOnSecurity received many a missive over the past 24 hours from readers who wanted to know why I’d not written about widespread media reports that [Mirai](#) — a malware strain made from hacked “Internet of Things” (IoT) devices such as poorly secured routers and IP cameras — was used to knock the entire country of [Liberia](#) offline. The trouble is, as far as I can tell no such nationwide outage actually occurred.

First, a quick recap on Mirai: This blog was taken offline in September following a [record 620 Gbps attack](#) launched by a Mirai botnet. The source code for Mirai was leaked online at the end of September. Since then, the code has been forked several times, resulting in the emergence of several large Mirai-based botnets. In late October, many of the Internet’s top destinations went offline for the better part of a

jgamblin / Mirai-Source-Code

Code Issues Pull requests Projects Pulse Graphs

Leaked Mirai Source Code for Research/IoC Development Purposes

4 commits 1 branch 0 releases 2 contributors

Branch: master New pull request Find file Clone or download

jgamblin committed on GitHub Merge pull request #1 from BenjaminHCCarr/patch-1 ... Latest commit 22e18df 5 days ago

loader Code Upload 7 days ago

mirai Code Upload 7 days ago

ForumPost.txt Add the forum post for the code release 5 days ago

README.md Update README.md 7 days ago

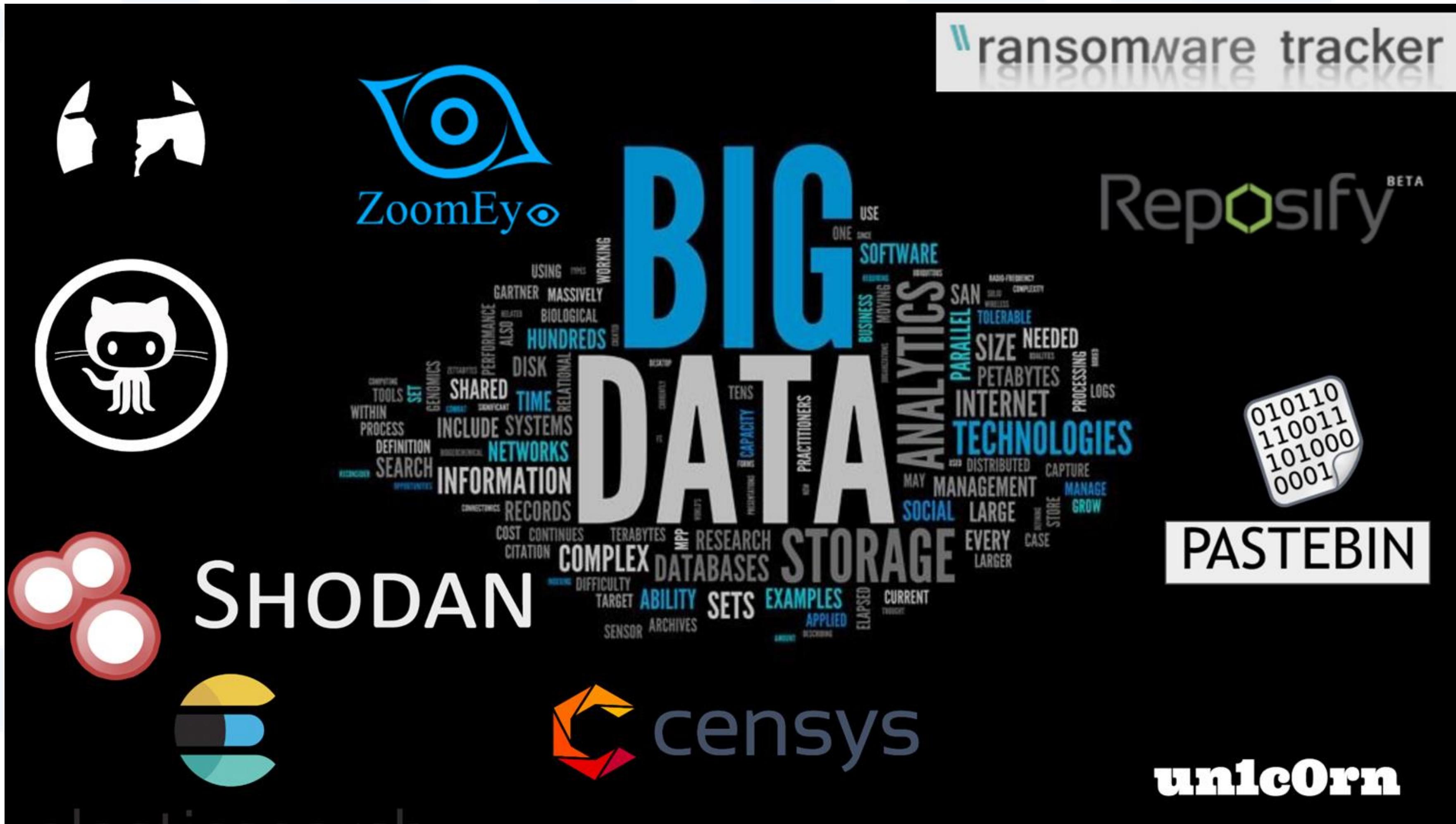
README.md

Mirai Botnet Client, Echo Loader and CNC source code

This is the source code released from [here](#) as discussed in this [Brian Krebs Post](#).

Using Open source Intelligence (OSINT)

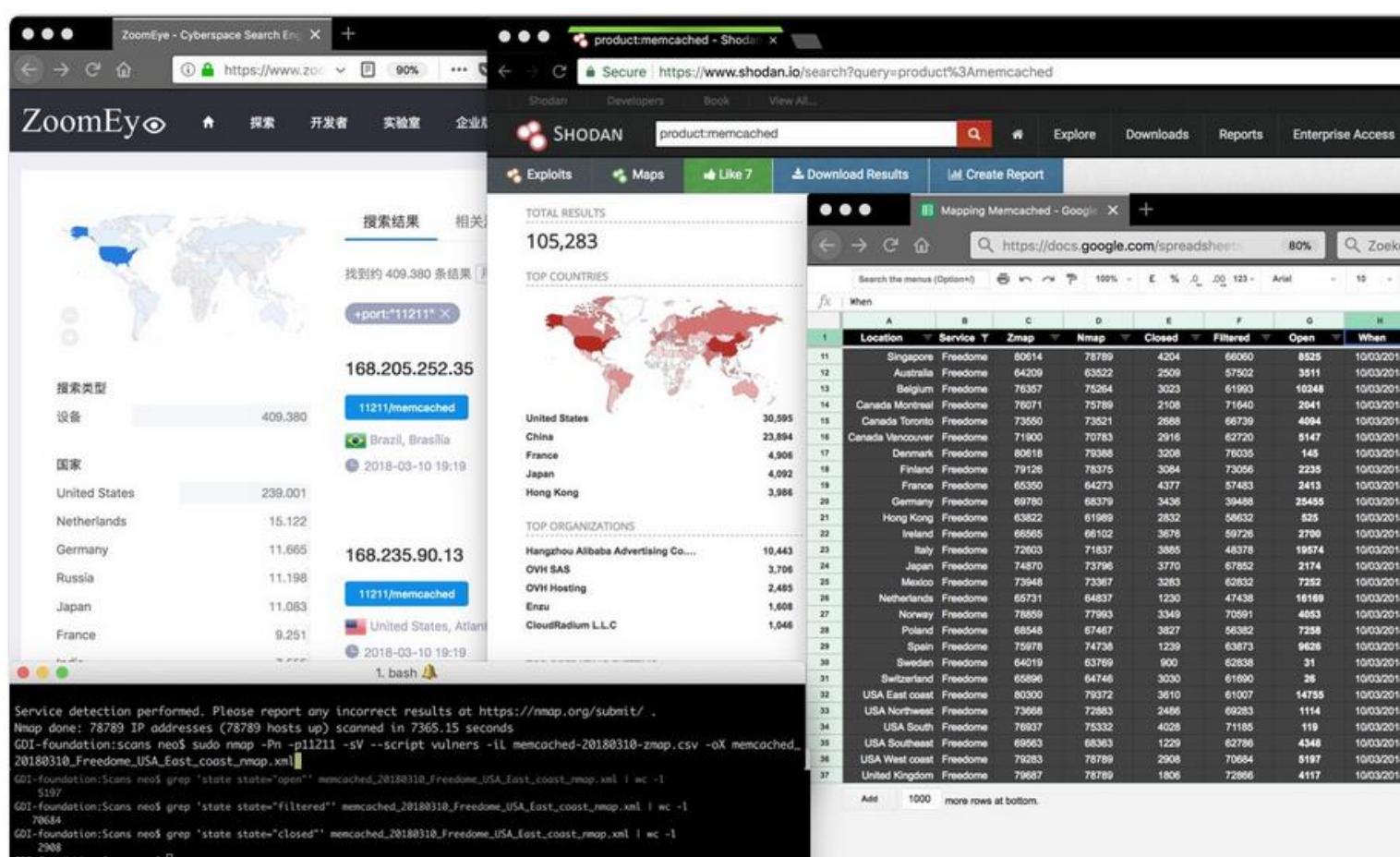
- Trusted and untrusted sources



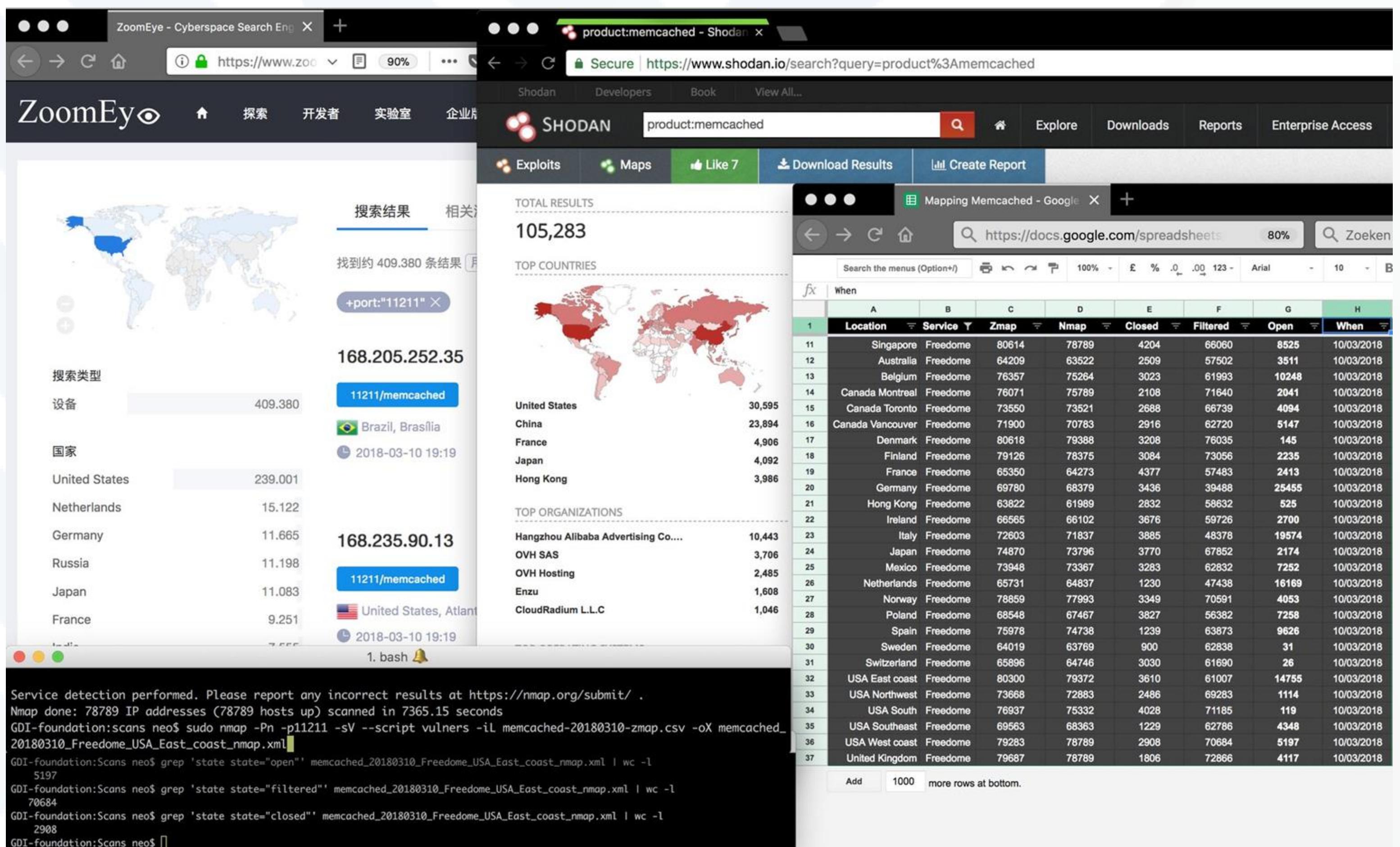
Using Open source Intelligence (OSINT)

- Trusted and untrusted sources
 - Comparing trusted sources

Exploring and comparing great OSINT sources like Shodan [US] vs ZoomEye [China] vs the DIY ZMap/NMap scans via 27 different geolocation (with Freedome VPN) to explore ISP filtering on Memcached traffic. The numbers speak volumes. Cloud service providers seem to block the most 1/2



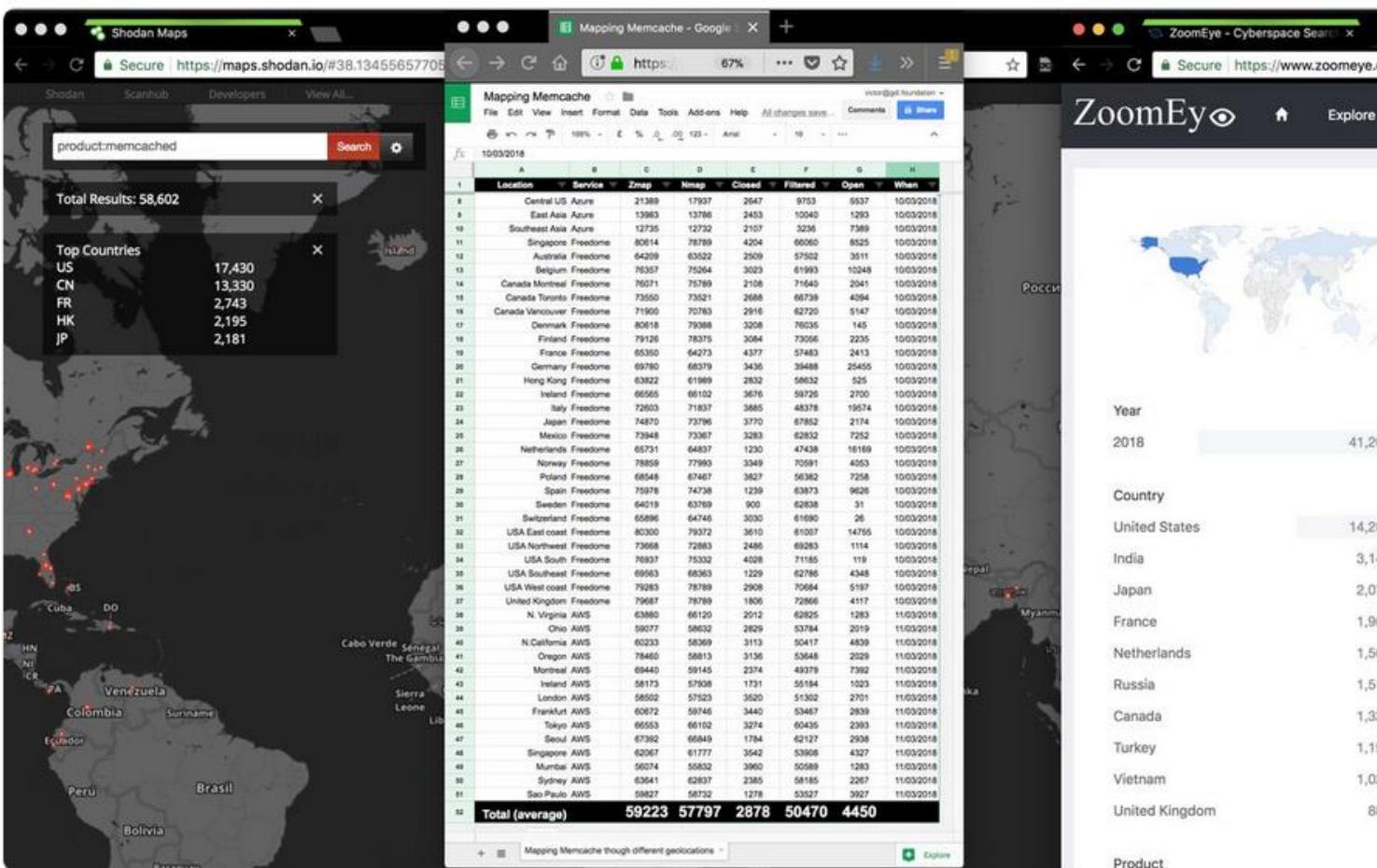
10:56 PM - 10 Mar 2018 from Amsterdam, The Netherlands



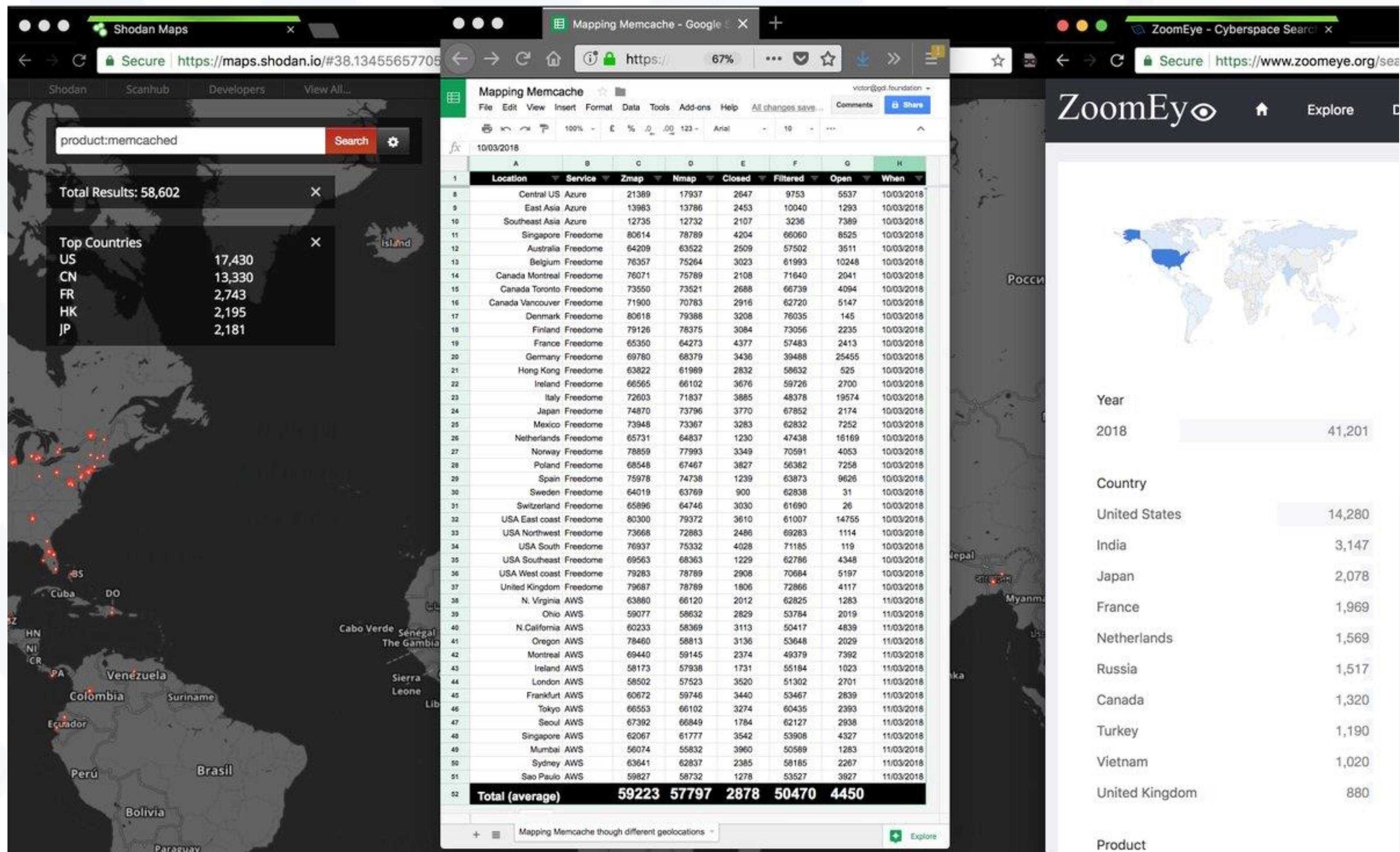
Using Open source Intelligence (OSINT)

- Trusted and untrusted sources
- Comparing trusted sources

After 24 hours of scanning for Memcached servers using 2 cloud service [Azure & AWS] and a VPN [Freedome] provider divided over 50 different geolocations to compare the results [goo.gl/yZzbZg] and see which one produces the most accurate insight. The answer is @shodanhq



2:10 PM - 11 Mar 2018 from Amsterdam, The Netherlands



Using Open source Intelligence (OSINT)

- Trusted and untrusted sources
- Comparing trusted sources
- Running in depth scans

And running Masscan on a Google Cloud shell has the same performance "challenge". Free shells are nice but a little bit more network speed would be more pleasant :-)

```
Cloud Shell
Cloud Shell x Cloud Shell +
victor_gevers@cloudshell:~/masscan$ sudo masscan 0.0.0.0/0 -pU:11211 --banners --exclude 255.255.255.255 | grep memcached
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-03-09 19:52:35 GMT
-- forced options: -ss -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
```

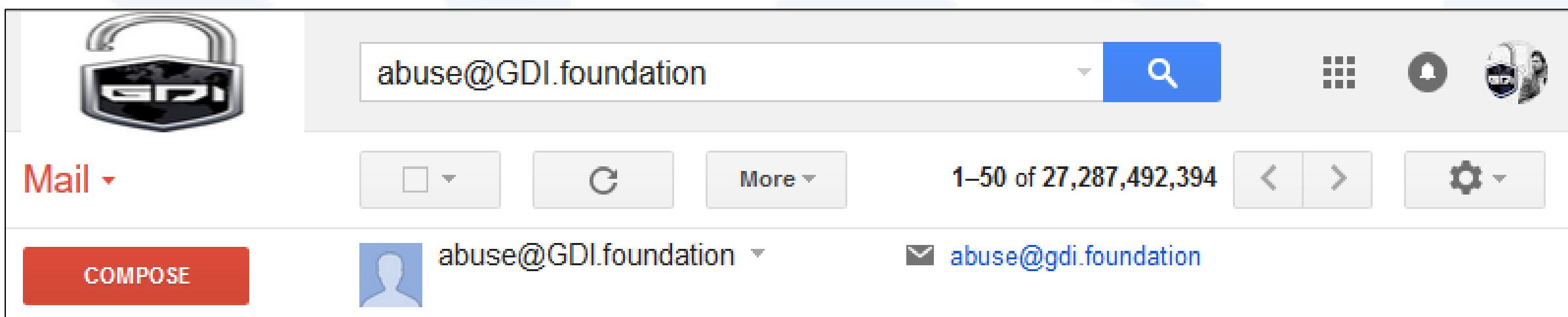
```
Cloud Shell
Cloud Shell x Cloud Shell +
victor_gevers@cloudshell:~/masscan$ sudo masscan 0.0.0.0/0 -pU:11211 --banners --exclude 255.255.255.255 | grep memcached
```

```
victor_gevers@cloudshell:~/masscan$ sudo masscan 0.0.0.0/0 -pU:11211 --banners --exclude 255.255.255.255 | grep memcached
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-03-09 19:52:35 GMT
-- forced options: -ss -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 4294967295 hosts [1 port/host]
rate: 0.10-kpps, 0.00% done, 11421:38:17 remaining, found=0
```

ZMap scanning from a Google Cloud Shell kind of works. It will take 6 hours just to scan for one port.

```
Cloud Shell
Cloud Shell x
victor_gevers@cloudshell:~$ sudo zmap -p11211 -o memcached_20180309_US-zmap.csv
Mar 09 20:35:30.613 [INFO] zmap: output module: csv
0:00 0%; send: 0 0 p/s (0 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:00 0%; send: 0 0 p/s (0 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:01 0%; send: 150496 150 Kp/s (148 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:02 0%; send: 329743 179 Kp/s (163 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:03 0%; send: 509734 180 Kp/s (169 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:04 0%; send: 679885 170 Kp/s (169 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:05 0% (6h06m left); send: 845723 166 Kp/s (168 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:06 0% (6h10m left); send: 1004057 158 Kp/s (167 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:07 0% (6h07m left); send: 1178808 175 Kp/s (168 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:08 0% (6h08m left); send: 1345403 167 Kp/s (168 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:09 0% (6h10m left); send: 1503991 159 Kp/s (167 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:10 0% (6h10m left); send: 1670714 167 Kp/s (167 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:11 0% (6h13m left); send: 1822318 152 Kp/s (165 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:12 0% (6h13m left); send: 1985815 163 Kp/s (165 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:13 0% (6h15m left); send: 2138377 152 Kp/s (164 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:14 0% (6h15m left); send: 2302844 164 Kp/s (164 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:15 0% (6h16m left); send: 2461029 158 Kp/s (164 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:16 0% (6h22m left); send: 2587665 127 Kp/s (161 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:17 0% (6h22m left); send: 2745708 158 Kp/s (161 Kp/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
```

Using Open source Intelligence (OSINT)



A screenshot of a Twitter post from the official MongoDB account (@MongoDB). The post reads: "Check out Victor using Stitch and #MongoDBAtlas to build awesome tools at no cost in the cloud. Really cool job! Security scanning always important! 🔒". Below the post is a screenshot of a tweet from Victor Gevers (@0xDUDE) about scanning vulnerable Memcached servers.

Victor Gevers @0xDUDE · Mar 8

Scanning & reporting vulnerable Memcached servers costs:

Running ZMap scan for port 11211 - \$0

Running Nmap scan on discovered hosts - \$0

Storing scans on MongoDB Atlas M0 cluster - \$0

Building a dashboard with MongoDB Stitch - \$0

Sending security reports with SendGrid Trial - \$0

A composite screenshot showing the process of performing OSINT. It includes:

- A terminal window displaying ZMap and Nmap scan results for Memcached servers, with several IP addresses redacted.
- A MongoDB Stitch dashboard showing network traffic over time.
- A SendGrid trial interface showing pricing options and a preview of an email message.

Digging in public password dumps

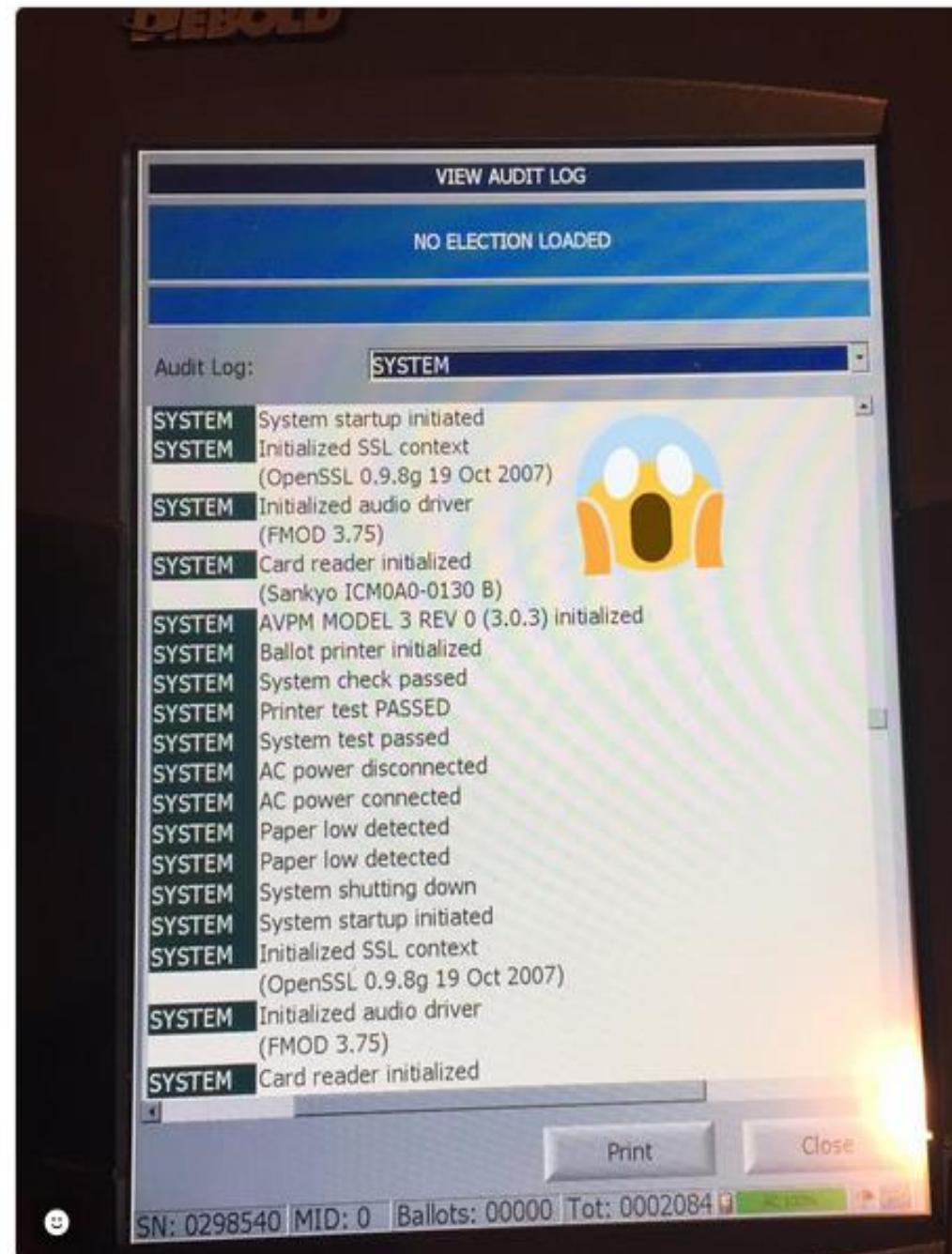
Hardware



Victor Gevers
@0xDUDE

Replying to @0xDUDE @defcon

This voting machine has a vulnerable OpenSSL (CVE-2011-4109) which allows remote attackers execute stuff. These machines are a scary 😰



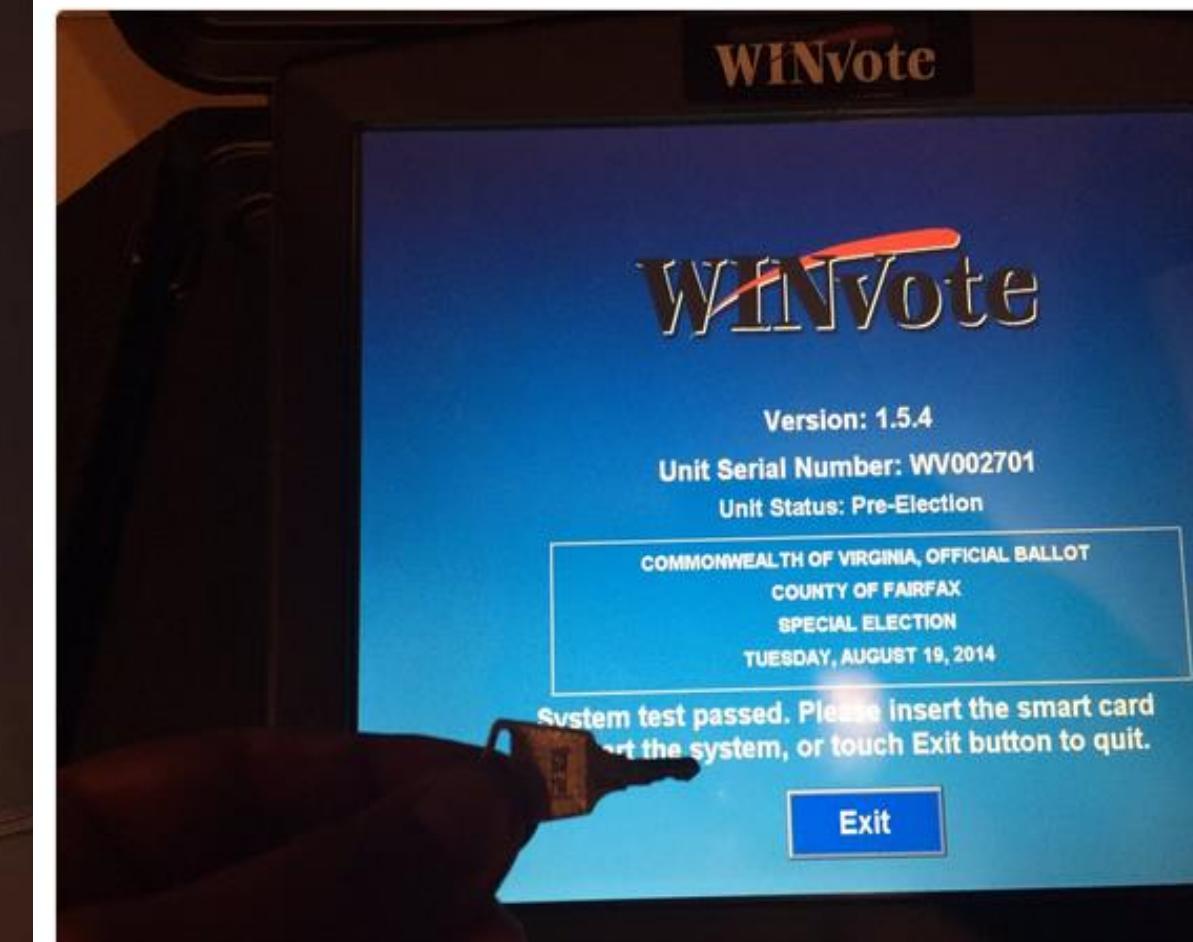
8:39 PM - 28 Jul 2017

685 Retweets 649 Likes

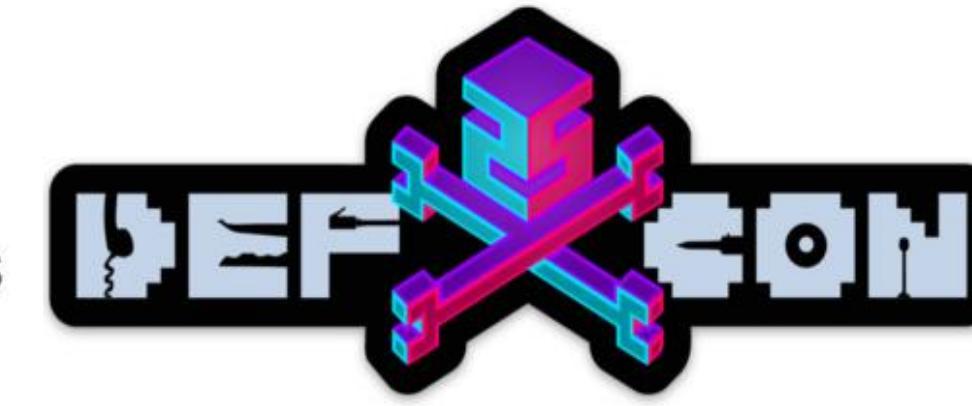


Victor Gevers
@0xDUDE

The "security" of these WINvote machines is so bad. Running WinXP, autorun enabled and hard-coded WEP wifi password.



8:19 PM - 28 Jul 2017 from Paradise, NV



NBC NEWS

SECTIONS ▾

TECH > TECH NEWS

GADGETS INTERNET SECURITY INNOVATION MOBILE

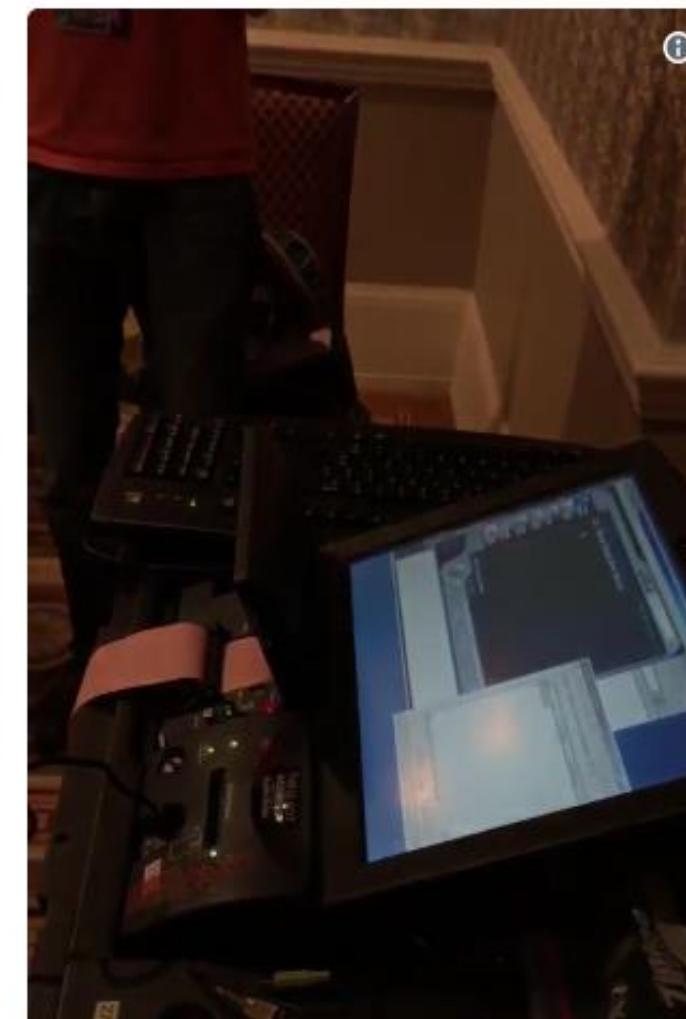
TECH JUL 31 2017, 1:28 PM ET

Hackers Were Able to Breach — and Then Rick-Roll — a Voting Machine

by ALYSSA NEWCOMB

"Never gonna give you up, never gonna let you down," Rick Astley sings in his 1987 hit. But the voting machine the song was blaring from at the Def Con security conference in Las Vegas sure did.

Hackers were able to successfully "Rick-Roll" a WinVote voting machine at the Def Con cyber security conference this weekend. Video of the hack, which was shared on Twitter, provides a stunning reminder of how nothing is ever truly safe from hackers.



InfoSecWorld
Conference & Expo 2018

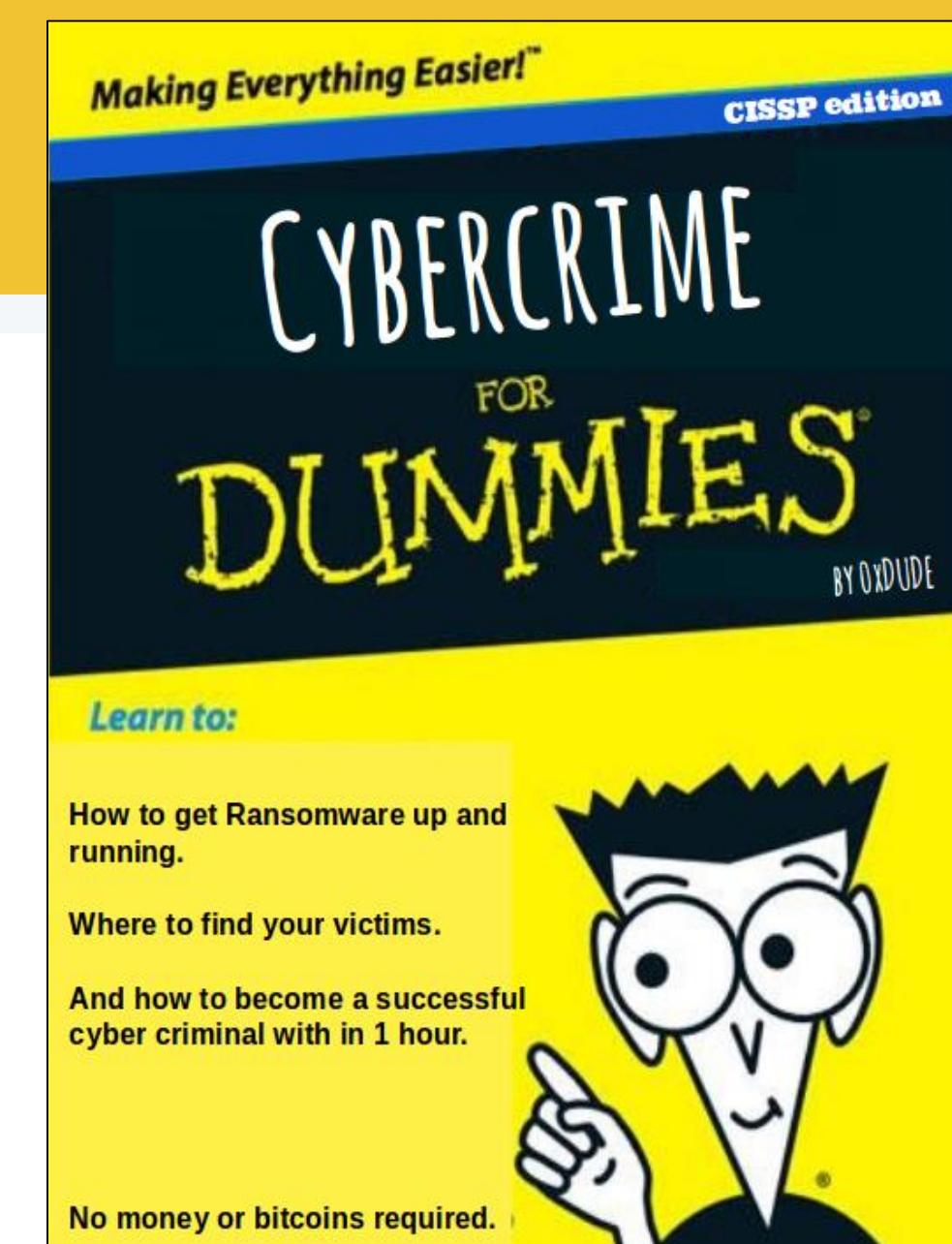
Dummies

Certified Cyber Criminal Professional

Your name after this presentation

The individual named above meets all of the certification requirements set forth by the CCCB Board of White Collar Criminals, which include the professional experience prerequisites, adoption of the CCCP Code of Cyber Criminals, and successful performance on the required competency examination.

This individual is hereby awarded the Certified Cyber Criminal Professional credential and is entitled to all the rights and privileges of poorly secured systems and ignorant users of the internet.



InfoSecWorld
Conference & Expo 2018

Dirty RAT

The screenshot shows the GitHub repository page for 'n1nj4sec / pupy'. The repository has 849 commits, 1 branch, 0 releases, and 15 contributors. A terminal window displays the available commands for Pupy:

```
>> help
Available commands :

- clients      List connected clients
- exit         Quit Pupy Shell
- help          show this help
- jobs          manage jobs
- list_modules List available modules with a brief description
- python        start interacting with the server local python interpreter (for debugging)
- read          execute a list of commands from a file
- run           run a module on one or multiple clients
- info          get some informations about one or multiple clients
- ps            list processes
- contest
- migrate
- exec
- pyexec
```

Pupy

Pupy is an opensource, multi-platform (Windows, Linux, OSX, Android), multi function RAT (Remote Administration Tool) and post-exploitation tool mainly written in python. It features a all-in-memory execution guideline and leaves very low footprint. Pupy can communicate using various transports, migrate into processes (reflective injection), load remote python code, python packages and python C-extensions from memory.

Pupy modules can transparently access remote python objects using rnc to perform various interactive tasks

GitHub - goliate/hidden-tear: ransomware open-sources - Mozilla Firefox

GitHub - goliate/hidden-tear: ransomware open-sources - Mozilla Firefox

utkusen Update README.md Latest commit 7bdd625 on 18 Aug 2015

hidden-tear-decrypter first commit a year ago

hidden-tear subdirectory bug fixed a year ago

.gitignore Initial commit a year ago

README.md Update README.md a year ago

README.md

[REDACTED]

It's a ransomware-like file crypter sample which can be modified for specific purposes.

Features

- Uses AES algorithm to encrypt files.
- Sends encryption key to a server.
- Encrypted files can be decrypted in decrypter program with encryption key.
- Creates a text file in Desktop with given message.
- Small file size (12 KB)
- Doesn't detect by antivirus programs (15/08/2015) <http://nodistribute.com/result/6a4jDwi83Fzt>

Demonstration Video

<https://www.youtube.com/watch?v=LtiRISepIfs>

Usage

- You need to have a web server which supports scripting languages like php, python etc. Change this line with your URL. (You better use Https connection to avoid eavesdropping)

```
string targetURL = "https://www.example.com/hidden-tear/write.php?info=";
```

Ransomware as a Service

S! pwoah7foa6au2pu.onion/listing.php?id=112455 Search

Software & Malware > Botnets & Malware > Botnets & Malware > Probably the best Ransomware available to date

LISTING OPTIONS

Contact Seller
Favorite Listing
Favorite Seller
Alert when restock
Report Listing

BROWSE CATEGORIES

- Fraud 27294
- Drugs & Chemicals 147964
- Guides & Tutorials 10554
- Counterfeit Items 5575
- Digital Products 12751
- Jewels & Gold 1225
- Weapons 2329
- Carded Items 2658
- Services 5777
- Other Listings 2575
- Software & Malware 2070
- Security & Hosting 529

SEARCH OPTIONS

Search terms:

Listing type:
 All Fixed Price Auction

Product type:
 All Digital Physical

Price range:
USD to USD

Probably the best Ransomware available to date

\$5000 if you need everything and want to work with it alone. \$30 if you can spread it for me to at least 200 computers. In this case we split 50-50% the money. \$30 only for avoiding partners those are not serious. I think this ransomware is the best currently in existence. - No antivirus detects it. - It uses one-way public key encryption, so it cannot be broken. - It gets information on the target, so ransom amounts can be adjusted. - It is stable, and well-tested (within my laboratory). - As an easter egg if it is lucky, it will get some password/bitcoin wallets.

Sold by **funWithCodes** - 35 sold since Mar 4, 2016 Vendor Level 3 Trust Level 5

Features	Features
Product class	Digital goods
Quantity left	Unlimited
Ends in	Never
Origin country	Worldwide
Ships to	Worldwide
Payment	Escrow

Spreading - 1 days - USD +0.00 / item

Purchase price: USD 30.00

Qty:

0.0495 BTC / 3.9063 XMR

Description Bids Feedback Refund Policy

Product Description

\$5000 if you need everything and want to work with it alone.
\$30 if you can spread it for me to at least 200 computers. In this case we split 50-50% the money. \$30 only for avoiding partners those are not serious.

I think this ransomware is the best currently in existence.
- No antivirus detects it.
- It uses one-way public key encryption, so it cannot be broken.
- It gets information on the target, so ransom amounts can be adjusted.
- It is stable, and well-tested (within my laboratory).
- As an easter egg if it is lucky, it will get some password/bitcoin wallets.

Our cooperation:
1. I keep the software up-to-date/FUD for a few months and the source closed, then put it to the market for others to have fun with the codes.
2. During this few months you spread as much as you can.
3. When the encryption is ready the target will be redirected to pastebin.
4. The pastebin will show them where they can request an offer.
5. After they pay they get the key what they can use to decrypt their files.

I control the pastebin. We both control the shared account on the offers, but you will handle the requests. So you get the money and forward half of it to me.
I have no motivation to change the pastebin page, because you would stop spreading and I would stop getting money.
You have no motivation to not forward me half of the money, because I would change the pastebin, so you would not get the offers to the shared account.
The shared offer account is shared, because I will be able to monitor what offers you get and you are not being dishonest.

If you are fine with this I am happy to work with you :D
This will be some next level shit! I expect to make a few of hundred thousand dollars. I hope you spend the money well :)
Do not buy a house, car or boat, stay under the radar!

Catalogues with open Windows machines

AlphaBay Market

Logged in as blaNL
Balance: BTC 0.0000 / XMR 0.0000
Autoshop Logout

USD 605.67 CAD 801.77 EUR 540.62 AUD 791.01 GBP 466.07

HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK FORUMS API SUPPORT

Software & Malware Other Other Bulk VNC Servers - Ideal for spreading/infecting w...

BULK VNC SERVERS - IDEAL FOR SPREADING/INFECTION WITH BOTNET/RANSOMWARE ETC

Selling bulk VNC servers, minimum order 100 pcs =50\$. For those of you who never dealt with these before, they are remote servers like RDP's, approx 70% of them belong to different types of companies, ranging from small corner shops/ depots to multinational companies (insurers , supermarkets , online retailers etc). For 50\$ you get access to 100 random pc's easily accessible using VNC vie...

Sold by dillinger9112 - 11 sold since Dec 6, 2015 Vendor Level 2 Trust Level 5

Features

Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Description

100 servers - 1 days - USD +50.00 / item

Purchase price: USD 0.01

Qty: 1 **Buy Now** **Buy Now** Queue

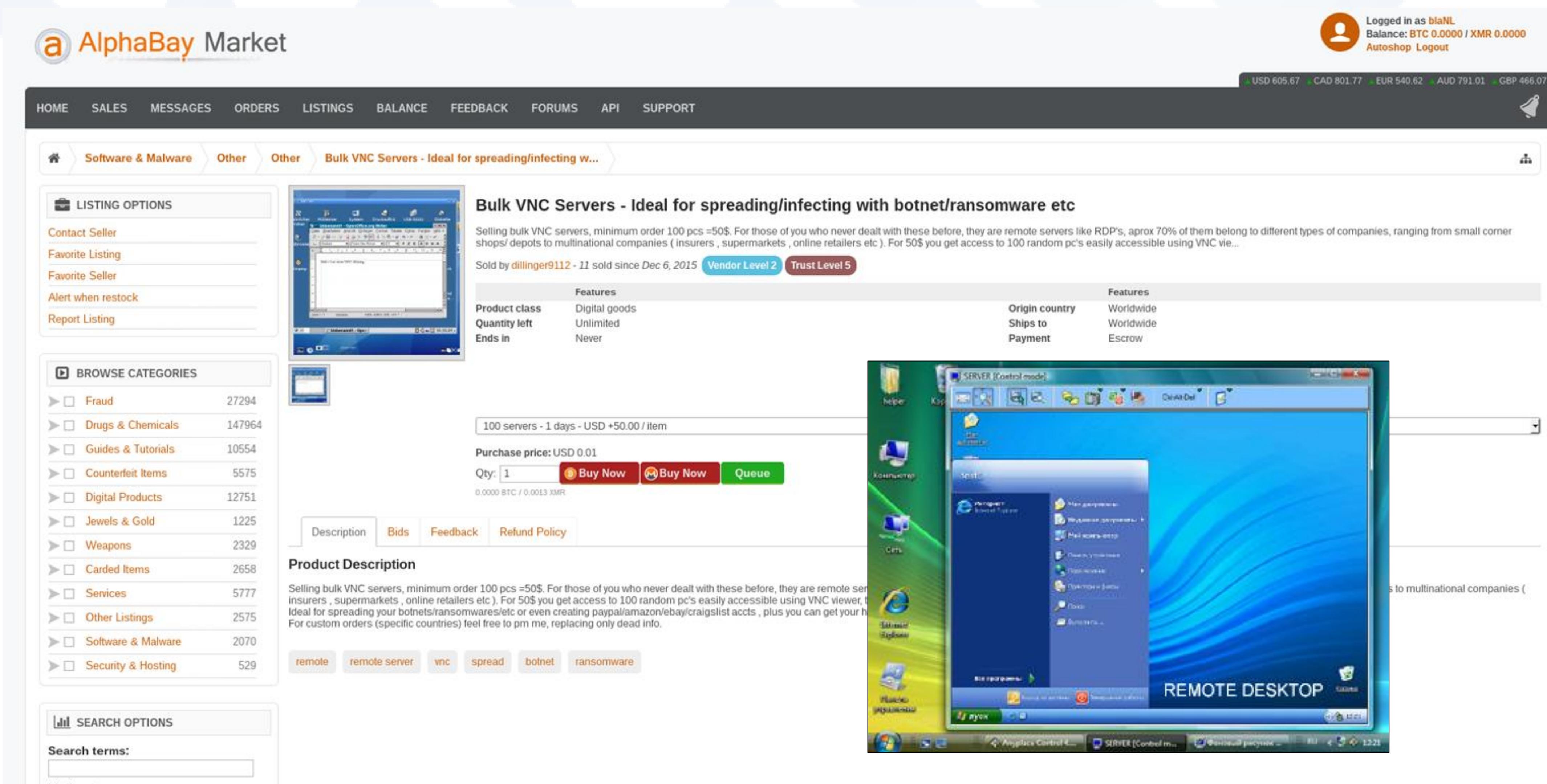
0.0000 BTC / 0.0013 XMR

BROWSE CATEGORIES

- Fraud 27294
- Drugs & Chemicals 147964
- Guides & Tutorials 10554
- Counterfeit Items 5575
- Digital Products 12751
- Jewels & Gold 1225
- Weapons 2329
- Carded Items 2658
- Services 5777
- Other Listings 2575
- Software & Malware 2070
- Security & Hosting 529

SEARCH OPTIONS

Search terms:



Open for your convenience

RealVNC | The original and best for remote access across desktop and mobile - Mozilla Firefox

RealVNC | The original and b... x +

https://www.realvnc.com

REALVNC

FEATURES DOWNLOAD PRICING NEWS SUPPORT ABOUT US

Access your computers remotely.
Anytime. Anywhere.

VNC® is ideal for simple and secure remote working, customer helpdesk, IT support, systems maintenance, classroom learning, training, collaboration and more. Across desktop and mobile.

BUY VNC NOW

Or download to start a free trial

VNC shares your computer screens with you wherever you are, whatever desktop or mobile device you're in front of, and lets you take control.

Learn more

has_screenshot:true - Shodan Search - Mozilla Firefox

has_screenshot:true - Shoda... x +

https://www.shodan.io/search?query=has_screenshot%3Atrue

Shodan Developers Book View All...

SHODAN has_screenshot:true

Exploits Maps Images Share Search Download Results Create Report

TOP COUNTRIES

Total results: 1,068,942

100.43.227.127

100-43-227-127.static-ip.telepacific.net
TelePacific Communications
Added on 2016-10-04 15:48:12 GMT
United States, Costa Mesa
Details

COUNTRY	RESULTS
United States	326,330
China	171,264
Germany	44,813
Brazil	44,037
United Kingdom	31,196

I weep for humanity

World of VNC

The image shows a screenshot of the World of VNC website on the left and a VNC viewer interface on the right.

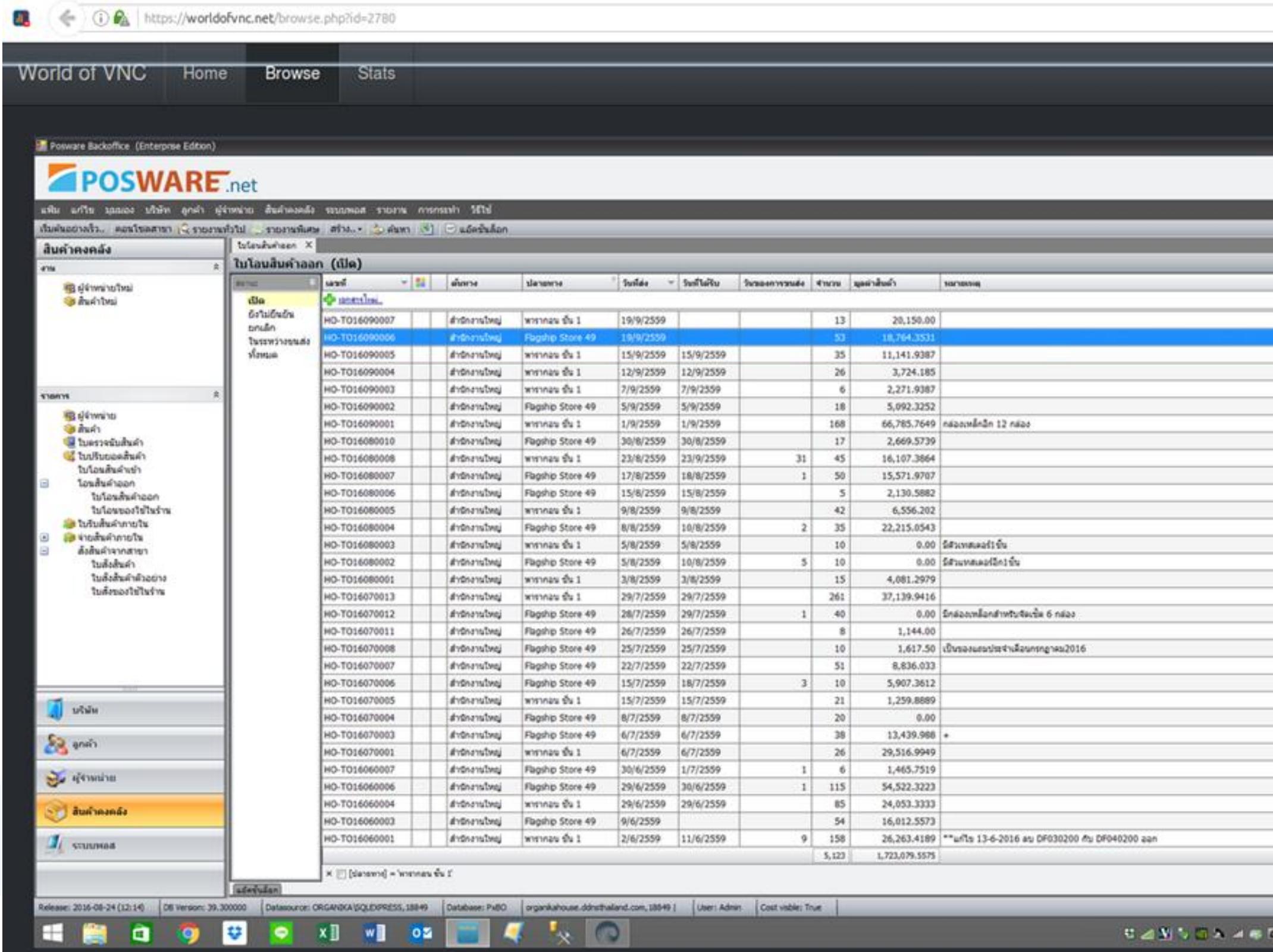
World of VNC Website:

- Header:** "World of VNC" logo, navigation bar with "Home", "Browse", "Stats", and social sharing buttons ("Like", "Share", "Follow @worldofvnc").
- Main Content:** "Welcome to the World of VNC" heading, text about scanning for unprotected VNC servers, and a green button labeled "Browse screenshots".
- Donate Section:** Text about donations, PayPal and Bitcoin payment buttons.
- Social Links:** Twitter and Facebook buttons.
- What is VNC? Section:** Text explaining VNC as a graphical desktop sharing system.
- Why this website? Section:** Text about the process of scanning the internet for VNC servers without passwords.

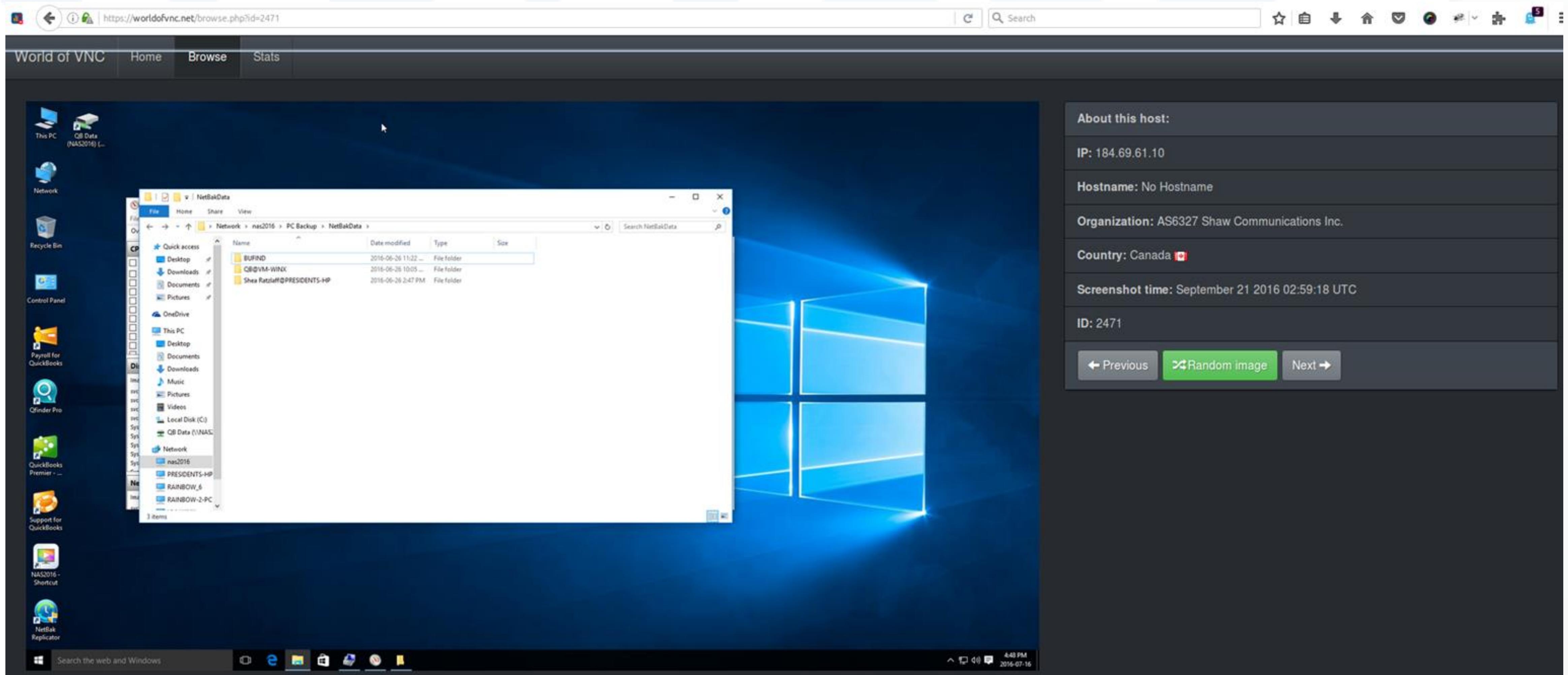
VNC Viewer Interface:

- Title Bar:** "VNC Viewer: New Connection" with "REAL VNC" logo.
- Input Fields:** "VNC Server:" dropdown set to "192.168.1.1:1" and "Encryption: Let VNC Server choose".
- Buttons:** "About...", "Options...", "Connect", and "Close".
- Thumbnail Preview:** A screenshot of a construction site with heavy machinery under a cloudy sky.
- Details Panel:** "About this host:" section showing IP: 66.112.190.79, Hostname: No Hostname, Organization: AS36817 MCSNet, Country: Canada, Screenshot time: September 20 2016 19:47:42 UTC, ID: 2758, and a "Tweet" button.
- Navigation:** "Previous", "Random image", and "Next" buttons.

Point of Sale systems



Windows 10



Banking systems

VNC Roulette vncroulette.net/index.php?picture=55

Previous image Random image X IP: 186.103.207.230

censys About Search Reports API Raw Data 186.103.207.230 (186-103-207-230.static.tie.cl)

Basic Information Network Telefónica Empresas, CL (CL) Routing 186.103.128.0/17 via AS15311 Protocols no publicly accessible services We haven't found any publicly accessible services on this host or the host is on our blacklist.

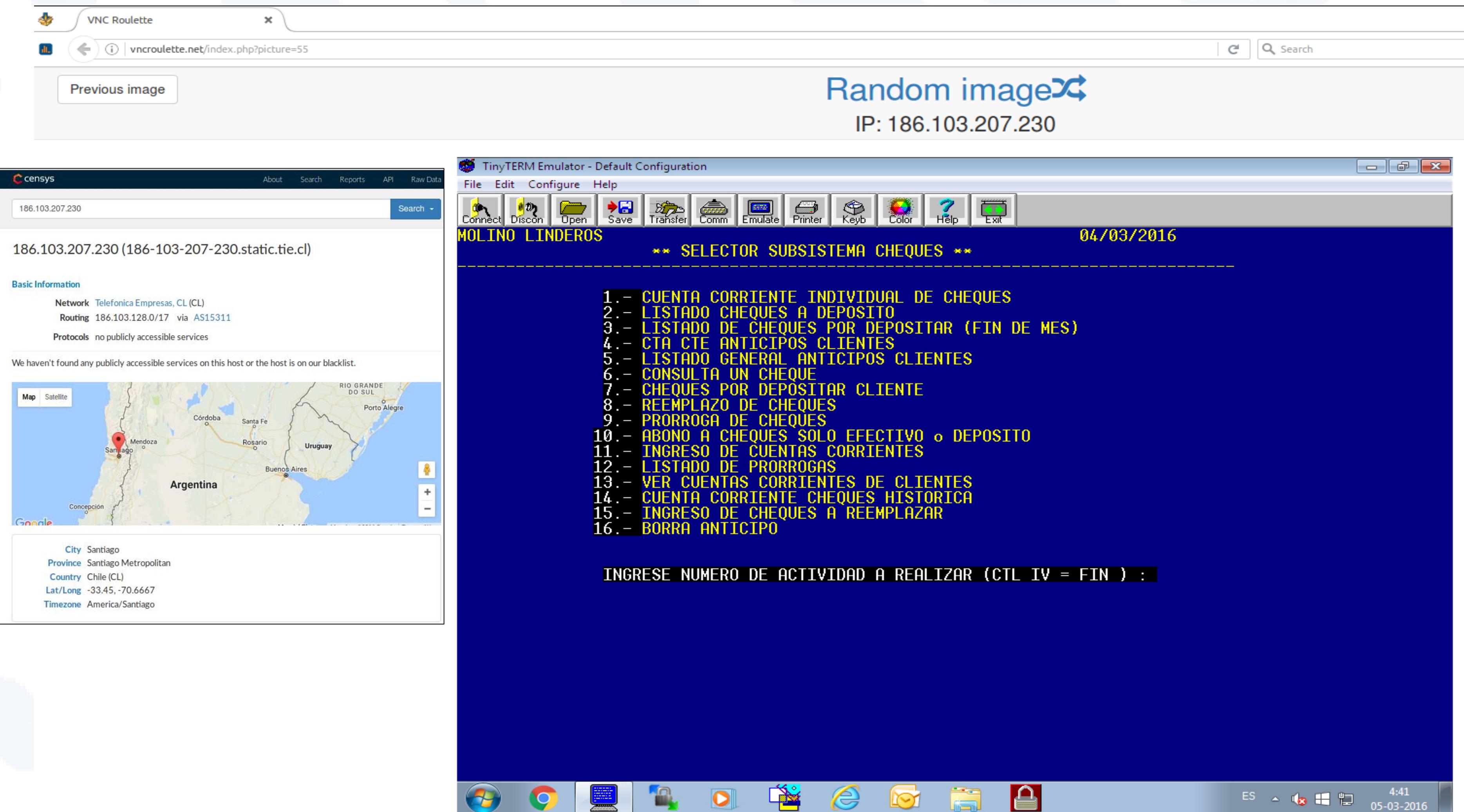
Map Satellite Google City Santiago Province Santiago Metropolitan Country Chile (CL) Lat/Long -33.45, -70.6667 Timezone America/Santiago

TinyTERM Emulator - Default Configuration File Edit Configure Help Connect Discn Open Save Transfer Comm Emulate Printer Keyb Color Help Exit MOLINO LINDEROS 04/03/2016 ** SELECTOR SUBSISTEMA CHEQUES **

1.- CUENTA CORRIENTE INDIVIDUAL DE CHEQUES
2.- LISTADO CHEQUES A DEPOSITO
3.- LISTADO DE CHEQUES POR DEPOSITAR (FIN DE MES)
4.- CTA CTE ANTICIPOS CLIENTES
5.- LISTADO GENERAL ANTICIPOS CLIENTES
6.- CONSULTA UN CHEQUE
7.- CHEQUES POR DEPOSITAR CLIENTE
8.- REEMPLAZO DE CHEQUES
9.- PRORROGA DE CHEQUES
10.- ABONO A CHEQUES SOLO EFECTIVO o DEPOSITO
11.- INGRESO DE CUENTAS CORRIENTES
12.- LISTADO DE PRORROGAS
13.- VER CUENTAS CORRIENTES DE CLIENTES
14.- CUENTA CORRIENTE CHEQUES HISTORICA
15.- INGRESO DE CHEQUES A REEMPLAZAR
16.- BORRA ANTICIPO

INGRESE NUMERO DE ACTIVIDAD A REALIZAR (CTL IV = FIN) :

4:41 ES 05-03-2016



Airports

Delhi Airport | Lost & Found

CUSTOMER CARE: +91-124-3376000 / 4797300

DELHI INDIRA GANDHI INTERNATIONAL AIRPORT | GAR 04:23 PM, 21°C | SUN 20 NOV 2016

TRAVELERS CORPORATE BUSINESS CARGO

FLIGHT INFORMATION | AIRPORT FACILITIES | SHOP, EAT, RELAX & CONVENiences | TO & FROM AIRPORT | PLAN YOUR TRAVEL | USEFUL INFO

USEFUL INFO

Lost and Found: First Flight

Udaan First Flight
Domestic Terminal 1,
Delhi International Airports (Pvt
IGI Airport,
New Delhi - 110037
Tel No 011 - 49652022, 011 - 491

ARRIVALS DEPARTURES FLIGHT TIMETABLE

SHOP & EAT TO & FROM AIRPORT LOUNGES

[Welcome to UDAAN... Welcome to UDAAN ...] Welcome to UDAAN - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Welcome to UDAAN

10.4.9.3:8080/udaan-web/creditCustomerBookingParcel.do?submitName=viewCreditCustomerBookingParcel&docType=PP. Google

Welcome to UDAAN, Patitapabana Sahoo (U023-BI-1) | Logout

Logged In Office: Branch Office-BHR C Shekarpur(U023) | Sat, 5 Mar 2016 01:05 PM

Change Password

Stock Management Pickup Booking Manifest GatePass Out GatePass In DRS MEC Utilities

Credit Customer Booking Parcel * Fields are Mandatory

Date/Time : 05/03/2016 13:05 Doc Type : PARCEL

	Sr. No.	* CN Number	* Customer Code	Pieces	* Pincode	Destination	* Actual Weight	Volume Weight	Chargeable Weight
	1			1					

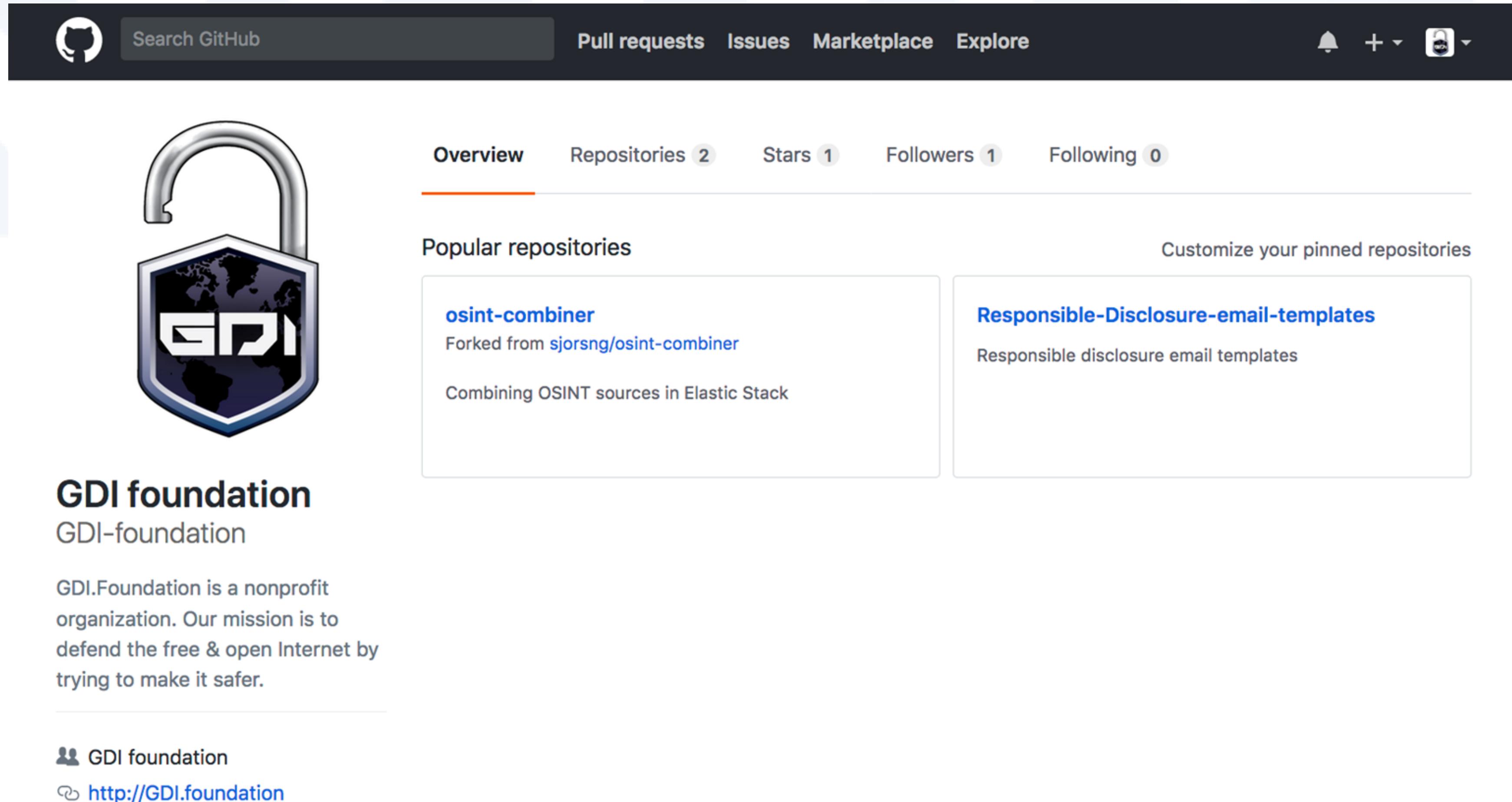
Submit Delete Cancel

© 2015 Copyright First Flight Couriers Ltd. All Rights Reserved. This site is best viewed with a resolution of 1024x768.

Applications Places System Sat Mar 5, 1:19 PM ADMIN-U023

Success factors

- Communication is key



The screenshot shows a GitHub profile page for the organization "GDI foundation". The top navigation bar includes links for Pull requests, Issues, Marketplace, and Explore. Below the navigation, there are tabs for Overview, Repositories (2), Stars (1), Followers (1), and Following (0). The "Overview" tab is selected. On the left, there is a large logo featuring an open padlock with a globe inside it, and the text "GDI foundation" and "GDI-foundation". A bio section states: "GDI.Foundation is a nonprofit organization. Our mission is to defend the free & open Internet by trying to make it safer." At the bottom, there are links to the organization's profile and website.

Search GitHub

Pull requests Issues Marketplace Explore

Overview Repositories 2 Stars 1 Followers 1 Following 0

Popular repositories

osint-combiner Forked from sjorsng/osint-combiner Combining OSINT sources in Elastic Stack

Customize your pinned repositories

Responsible-Disclosure-email-templates Responsible disclosure email templates

GDI foundation
GDI-foundation

GDI.Foundation is a nonprofit organization. Our mission is to defend the free & open Internet by trying to make it safer.

• GDI foundation
http://GDI.foundation

Success factors

- Communication is key
 - Intent / goal and governance
 - Personal touches
 - Translation by locals

The screenshot shows a web-based email editor interface with the following content:

Responsible Disclosure (MongoDB)

Recipients

Responsible Disclosure (MongoDB)

Dear sir, madam,

I want to inform you that {IP/HOSTNAME} is running a MongoDB instance which appears not to be correctly configured or protected by a firewall allowing connections via port 27017 from anywhere and anyone without any form of authentication and grants full admin access (Create Database and Delete Database, Create User and Drop User, Insert, Update, and Delete documents) to other remote servers and shell (admin) access to the server which is a security risk:

{screenshot}

Criminals often target open databases to deploy their activities like [data theft/ransom](#). But we also these are used for hosting malware (like [ransomware](#)), botnets and for hiding files in the [GridFS](#).

Our advise would be to protect this server with a firewall blocking port 27017 or limit the access o as option in the configuration. Or you can choose to restart the database server with -auth option

Also we suggest to

1. Check the MongoDB accounts to see if no one added a secret (admin)user.
2. Check the GridFS to see if someone stored any files there.
3. Check the logfiles to see who accessed the MongoDB ([show log global command](#)).

In case you need additional information please do not hesitate to ask.
Could you please send a confirmation and keep us informed when this issue is fixed?

GDI.Foundation is a non profit organization that strives to make the internet safer. We have disco

Thank you for your time.
Kind regards,

Victor Gevers
[GDI.Foundation](#)

Sans Serif | **B** *I* A | | | | | | |

Send | | | | | | | |

The right side of the interface features a sidebar with the following options:

- Insert
- Security warning: D-Link 850L routers
- Responsible Disclosure: MB MS17-010 #EternalBlue
- Responsible Disclosure (Elasticsearch)
- Responsible Disclosure (Hadoop)
- Responsible Disclosure (MongoDB)
- Responsible Disclosure (Memcached)
- Responsible Disclosure (Redis)
- Responsible Disclosure (CouchDB)
- Responsible Disclosure (ElasticSearch)

At the bottom right of the sidebar, there is a dropdown menu with the following items:

- Default to full-screen
- Canned responses
- Label
- Plain text mode
- Print
- Check spelling

Success factors

- Communication is key
 - Intent / goal and governance
 - Personal touches
 - Translation by locals
- Keep the (Gov)CERTS informed

 **CouchDB generic security warning**

Apache CouchDB is open source database and has a document-oriented NoSQL database architecture written in Erlang. It uses JSON to store data, JavaScript as query language using MapReduce, and HTTP for an API. As of Jan 18th, there are 3,690 internet facing implementations worldwide used as a general purpose database.

Observation
The first actor expanded their reach from 0 to ... "infections" within a time span of .. hours. At this rate and possible copycat behaviour we estimated a full destruction of any internet-facing CouchDB within a week.

Indications of Compromise

- Public tracker
- IP Blacklist: <http://pastebin.com/raw/BRA42kBT>
- Links:

Advisory
Please make sure you create frequently backups of data that you need to restore quickly.

1. set up TLS (HAProxy preferred)
2. set an admin password (`curl -X PUT host:5984/_config/admin/username -d "password here"`)
3. create per application users (<http://docs.couchdb.org/en/2.0.0/intro/security.html#creating-a-new-user>)
4. set per-application _security settings so that only per-app users can r/w databases (<http://docs.couchdb.org/en/2.0.0/api/database/security.html#put-db-security>)
5. review CouchDB security docs (<http://docs.couchdb.org/en/2.0.0/intro/security.html>)
6. Apply network filtering or let a firewall block port 5984 to untrusted IPs.

Contact
Victor Gevers: [@theDUDE](mailto:victor@gdi.foundation)
Natali Mergen: [@nemergen](mailto:natali@gdi.foundation)
Matt Bromiley: [@mattbromileyDFIR](mailto:mattbromiley@gdi.foundation)
Dylan Katz: [@Platz1](mailto:dylan@gdi.foundation)
CouchDB Security Team: security@couchdb.apache.org

CouchDB generic security... 26 jan. 2017

 **HDFS generic security warning**

The Hadoop Distributed File System (HDFS) is designed to reliably store very large files across machines in a large cluster, referred to as a Hadoop cluster. This cluster can be controlled from the Hadoop framework, which is mostly written Java, with some native code in C and command line utilities written as shell scripts. The Hadoop ecosystem is known for its extensive user interfaces that, by default, allows unauthenticated access. This warning focuses on all the internet-facing Hadoop Distributed File Systems on port 50070.

Block Pool ID: [Input field]

Summary

Security is off.
Safe mode is off.

As of this warning, there are 5,307 internet facing implementations worldwide.

The default installation for HDFS Admin binds to the IP address 0.0.0.0 and allows any unauthenticated user to perform super user functions to a Hadoop cluster. These functions can be performed via a web browser, and do not prevent an attacker from destructive actions. This may include destroying data nodes, data volumes, or snapshots with TBs of data in seconds.

Source: https://hadoop.apache.org/docs/current/hadoop-project-dist/hadoop-hdfs/HdfsPermissionsGuide.html#The_Web_Server

Hadoop generic security w... 24 jan. 2017

 **elasticsearch generic security warning**

Elasticsearch is a search engine based on Lucene. It provides a distributed, multi-thread-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java and is released as open source license.

There are 16,280 internet facing implementations that are doing jobs such as data collection and log parsing (with Logstash) that could be used for network monitoring and other NOC/SOC activities such as analytics in combination with the visualization platform called Kibana. These three products are designed to be used as an integrated solution, referred to as the "Elastic stack" which are a popular alternative for Splunk which used by for example military security operation centers worldwide.

The default installation for Elasticsearch binds to localhost, however allows any unauthenticated user to send arbitrary requests to your Elasticsearch cluster as a super user. Destroying an entire Elasticsearch takes merely seconds and can be done by command line or web browser.

Observation
The first actor expanded their reach from 321 to 708 "infections" within a time span of 8 hours. At this rate and possible copycat behaviour we estimated a full destruction of any internet-facing Elasticsearch within two to three weeks.

Indications of Compromise

- Public tracker: <https://go.gd/fy5qf>
- IP Blacklist: <http://pastebin.com/raw/ESEYyFy>
- Links: <https://www.elastic.co/blog/understanding-elasticsearch-security>

Advisory
Please make sure you create frequently backups of data that you need to restore quickly.

1. Apply network filtering or let a firewall block port 9200 to untrusted IPs.
2. Add a free IAM control and network segmentation with an [OpenVPN solution](#).
3. Implement a reverse proxy
4. Purchase the additional Elastic security product named [Shield](#).

And please follow the [security advice](#) from Elastic and read this about securing [Elasticsearch and Kibana](#).

Please consult Elastic for any security related questions because they already helped customers concerning this issue.

Elasticsearch warning 15 jan. 2017

 **Redis generic security warning**

Elasticsearch is a search engine based on Lucene. It provides a distributed, multi-thread-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java and is released as open source license.

There are 16,280 internet facing implementations that are doing jobs such as data collection and log parsing (with Logstash) that could be used for network monitoring and other NOC/SOC activities such as analytics in combination with the visualization platform called Kibana. These three products are designed to be used as an integrated solution, referred to as the "Elastic stack" which are a popular alternative for Splunk which used by for example military security operation centers worldwide.

The default installation for Elasticsearch binds to localhost, however allows any unauthenticated user to send arbitrary requests to your Elasticsearch cluster as a super user. Destroying an entire Elasticsearch takes merely seconds and can be done by command line or web browser.

Observation
The first actor expanded their reach from 321 to 708 "infections" within a time span of 8 hours. At this rate and possible copycat behaviour we estimated a full destruction of any internet-facing Elasticsearch within two to three weeks.

Indications of Compromise

- Public tracker: <https://go.gd/fy5qf>
- IP Blacklist: <http://pastebin.com/raw/ESEYyFy>
- Links: <https://www.elastic.co/blog/understanding-elasticsearch-security>

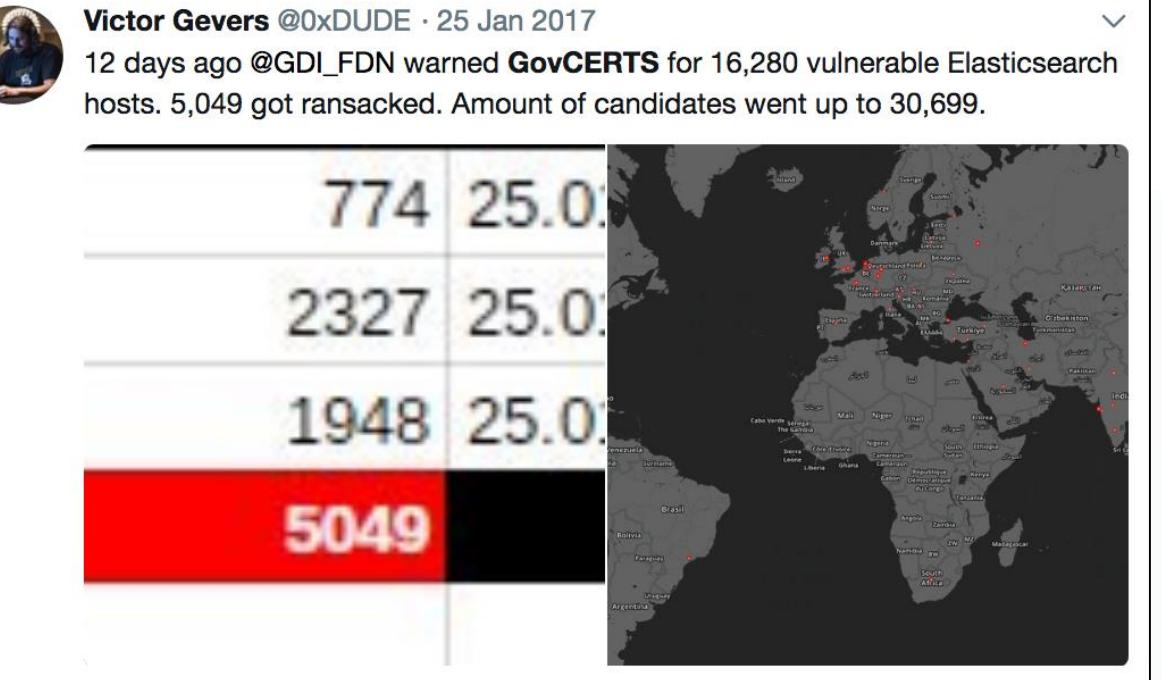
Advisory
Please make sure you create frequently backups of data that you need to restore quickly.

1. Apply network filtering or let a firewall block port 9200 to untrusted IPs.
2. Add a free IAM control and network segmentation with an [OpenVPN solution](#).
3. Implement a reverse proxy
4. Purchase the additional Elastic security product named [Shield](#).

And please follow the [security advice](#) from Elastic and read this about securing [Elasticsearch and Kibana](#).

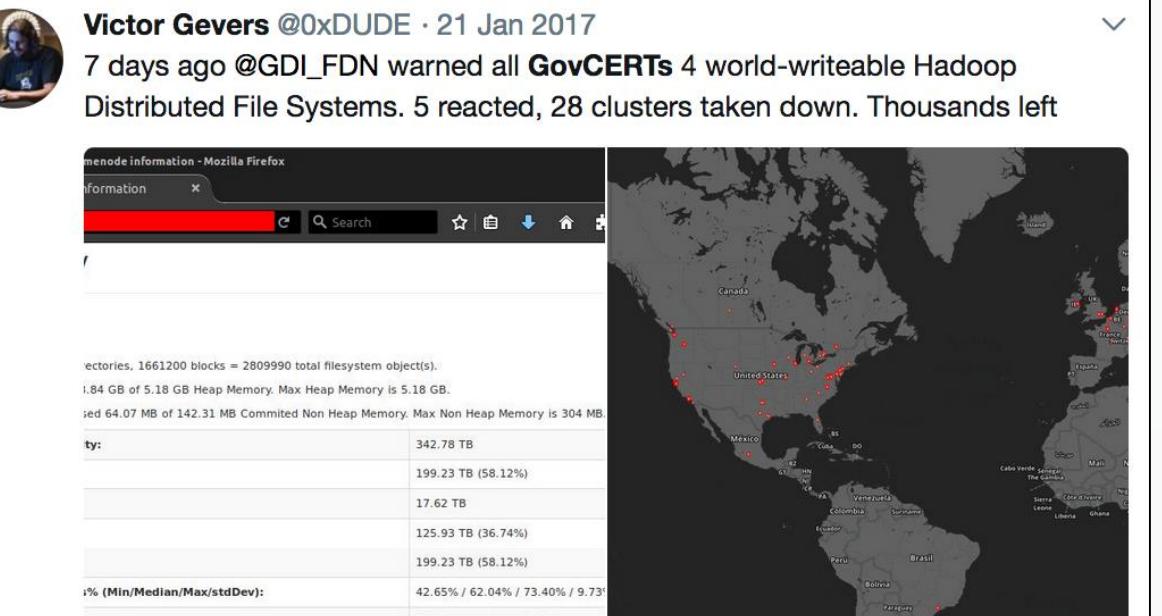
Please consult Elastic for any security related questions because they already helped customers concerning this issue.

Redis generic security wa... 14 jan. 2017


Victor Gevers @0xDUDE · 25 Jan 2017
12 days ago @GDI_FDN warned GovCERTS for 16,280 vulnerable Elasticsearch hosts. 5,049 got ransacked. Amount of candidates went up to 30,699.

774	25.0%
2327	25.0%
1948	25.0%
5049	

2 21 19


Victor Gevers @0xDUDE · 21 Jan 2017
7 days ago @GDI_FDN warned all GovCERTs 4 world-writeable Hadoop Distributed File Systems. 5 reacted, 28 clusters taken down. Thousands left

node information - Mozilla Firefox

ty:	342.78 TB
	199.23 TB (58.12%)
	17.62 TB
	125.93 TB (36.74%)
	199.23 TB (58.12%)
% (Min/Median/Max/stdDev):	42.65% / 62.04% / 73.97%
8 (Decommissioned: 0)	

1.84 GB of 5.18 GB Heap Memory. Max Heap Memory is 5.18 GB.
used 64.07 MB of 142.31 MB Committed Non Heap Memory. Max Non Heap Memory is 304 MB

map

Success factors

- Communication is key
 - Intent / goal and governance
 - Personal touches
 - Translation by locals
 - Keep the (Gov)CERTS informed
 - Keep tracking reported items

Success factors

- Communication is key
 - Intent / goal and governance
 - Personal touches
 - Translation by locals
- Keep the (Gov)CERTS informed
- Keep tracking reported items
- Publish your findings.



GDI Foundation @GDI_FDN · 17h

We want to express our deep gratitude to all ISPs, involved organizations and volunteers for their contribution to help to address the issue of vulnerable Memcached servers. Thank you so much for your effort. We could not have achieved this level of success without your help.

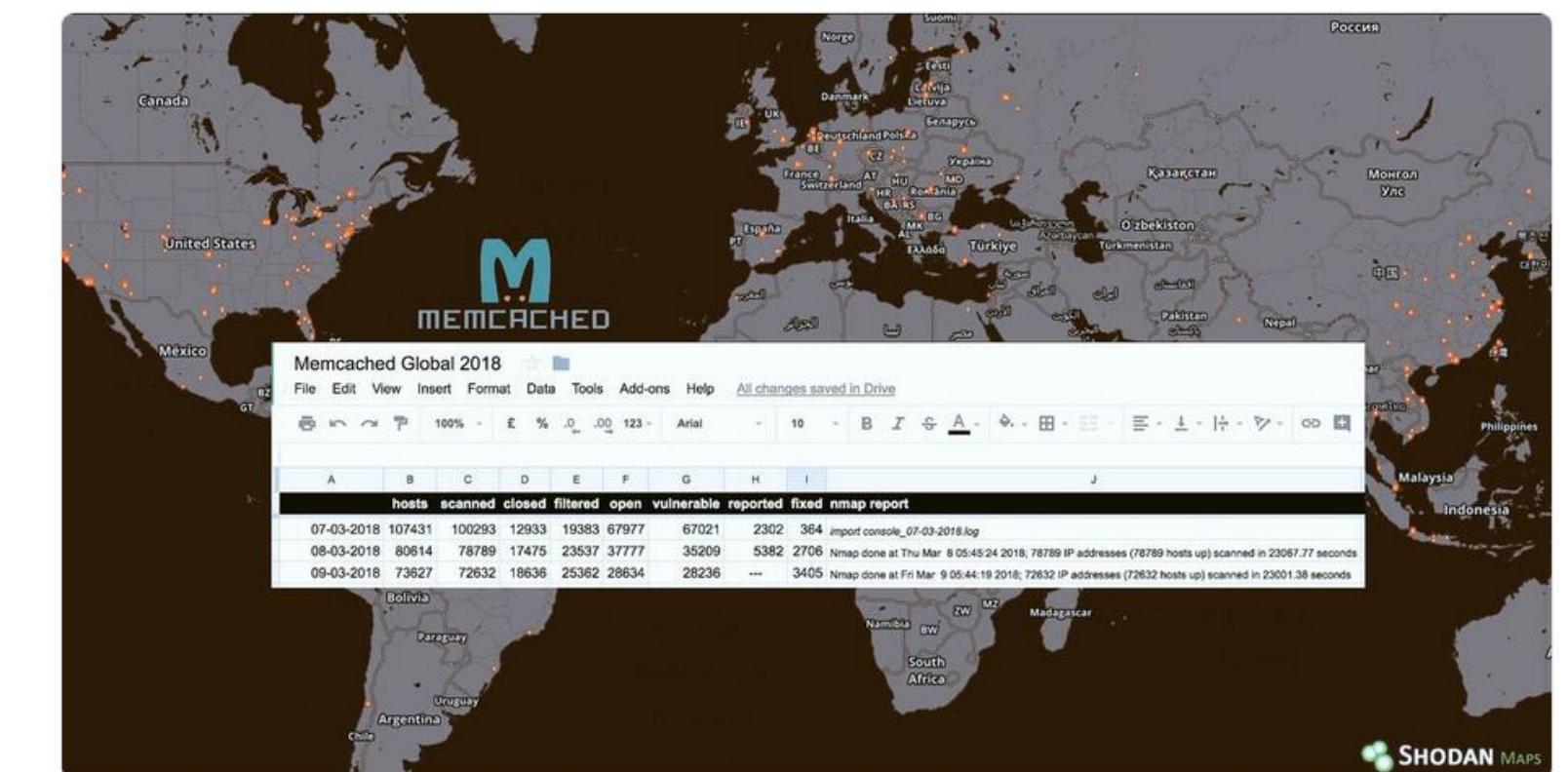


Victor Gevers
@0xDUDE

Mopping-up Memcached
Fri Mar 9 11:00 CET
Hosts in Shodan: 104,936
Hosts found with ZMap: 736,27
Nmap scan: 72,632 hosts were up

- Closed: 18,636
- Filtered: 23,537
- Open: 25,362
- Vuln: 28,236

Reported 7,684 servers in the last 48 hours. 6,475 were fixed. Still 28,236 to go



11:02 AM - 9 Mar 2018 from The Netherlands

Reporting vulnerable items

■ Responsible Disclosures / CVD

❖ THE SEVEN VIRTUES OF BUSHIDO ❖						
義 礼 勇 誉 仁 真 忠						
GI Integrity	REI Respect	YU Heroic Courage	MEIYO Honor	JIN Compassion	MAKOTO Honesty and Sincerity	CHU Duty and Loyalty
Be acutely honest throughout your dealings with all people. Believe in justice, not from other people, but from yourself. To the true warrior, all points of view are deeply considered regarding honesty, justice and integrity.	True warriors have no reason to be cruel. They do not need to prove their strength. Warriors are courteous even to their enemies. Warriors are not only respected for their strength in battle, but also by their dealings with others.	Hiding like a turtle in a shell is not living at all. A true warrior must have heroic courage. It is absolutely risky. It is living life completely, fully, and wonderfully.	Warriors have only one judge of honor and character, and this is themselves. Decisions they make and how these decisions are carried out is a reflection of whom they truly are.	Through intense training and hard work the true warrior becomes quick and strong. They are not as most people. They develop a power that must be used for good. They have compassion. They help their fellow man at every opportunity.	When warriors say that they will perform an action, it is as good as done. Nothing will stop them from completing what they say they will do. They do not have to "give their word." They do not have to "promise."	Warriors are responsible for everything that they have done and everything that they have said, and all of the consequences that follow. They are immensely loyal to all of those in their care.
<input type="checkbox"/> Warriors make a full commitment to their decisions.	<input type="checkbox"/> The true strength of a warrior becomes apparent during difficult times.	<input type="checkbox"/> Heroic courage is not blind. It is intelligent and strong.	<input type="checkbox"/> You cannot hide from yourself.	<input type="checkbox"/> If an opportunity does not arise, they go out of their way to find one.	<input type="checkbox"/> Speaking and doing are the same action.	<input type="checkbox"/> To everyone that they are responsible for, they remain fiercely true.

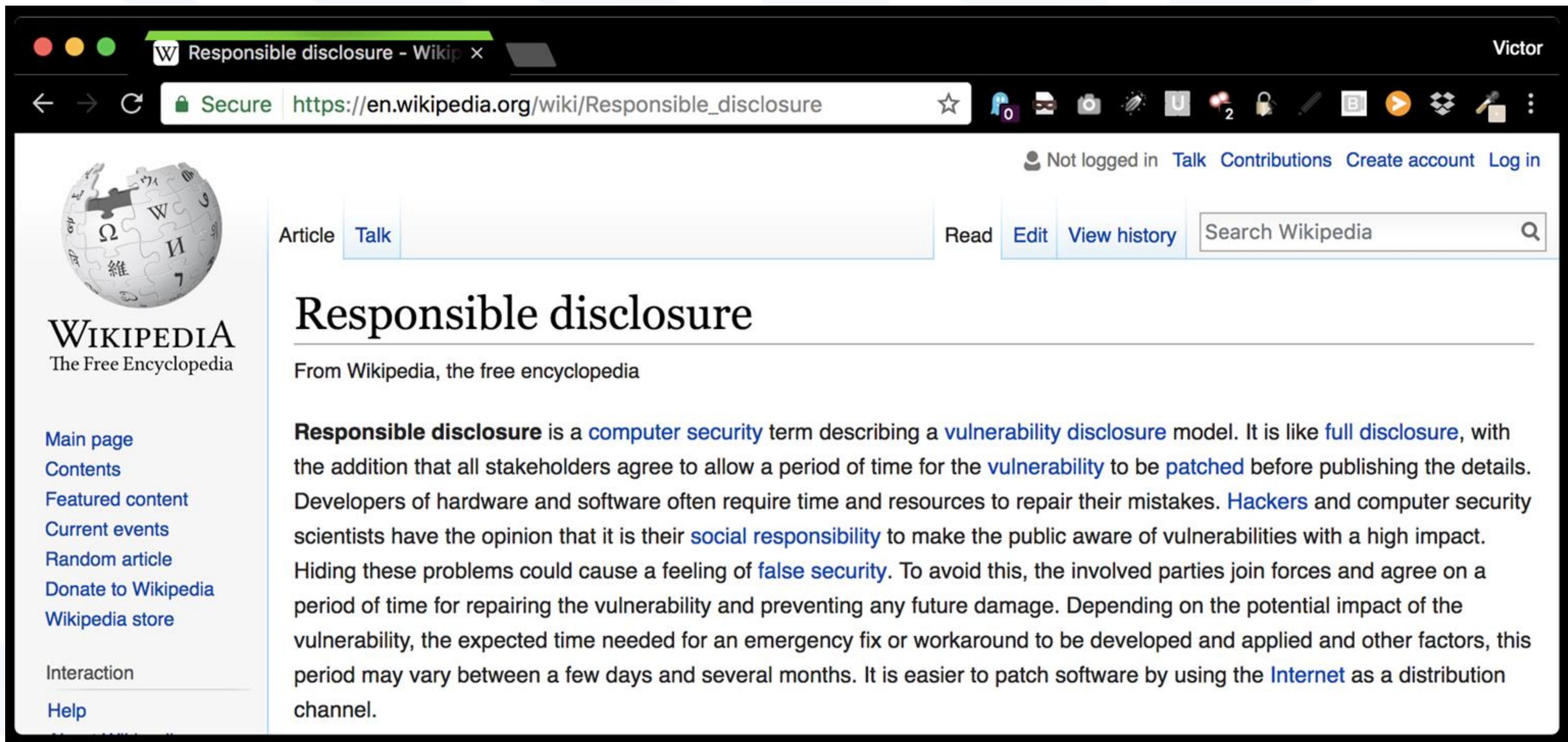


National Cyber Security Centre
Ministry of Security and Justice

» Policy for arriving at a practice
for Responsible Disclosure »

Reporting vulnerable items

■ Responsible Disclosures / CVD



The screenshot shows a web browser displaying the Wikipedia article titled "Responsible disclosure". The page header includes the Wikipedia logo, the title "Responsible disclosure", and navigation links for "Article", "Talk", "Read", "Edit", "View history", and "Search Wikipedia". The main content area begins with the heading "Responsible disclosure" and a summary line: "From Wikipedia, the free encyclopedia". Below this, the text defines responsible disclosure as a computer security term, explaining its purpose, the role of stakeholders, and the potential impact on developers and the public. It also discusses the concept of social responsibility and the prevention of false security.

Responsible disclosure is a [computer security](#) term describing a vulnerability disclosure model. It is like [full disclosure](#), with the addition that all stakeholders agree to allow a period of time for the [vulnerability](#) to be [patched](#) before publishing the details. Developers of hardware and software often require time and resources to repair their mistakes. [Hackers](#) and computer security scientists have the opinion that it is their [social responsibility](#) to make the public aware of vulnerabilities with a high impact. Hiding these problems could cause a feeling of [false security](#). To avoid this, the involved parties join forces and agree on a period of time for repairing the vulnerability and preventing any future damage. Depending on the potential impact of the vulnerability, the expected time needed for an emergency fix or workaround to be developed and applied and other factors, this period may vary between a few days and several months. It is easier to patch software by using the [Internet](#) as a distribution channel.

Reporting vulnerable items

■ Responsible Disclosures / CVD



[Home](#) > [Store](#) > [Standards catalogue](#) > [Browse by ICS](#) > [35](#) > [35.030](#) > ISO/IEC 29147:2014

ISO/IEC 29147:2014

Preview

Information technology -- Security techniques -- Vulnerability disclosure

A screenshot of the ISO Online Browsing Platform (OBP). The top navigation bar includes the ISO logo, the text "Online Browsing Platform (OBP)", and a search bar with the query "ISO/IEC 30111:2013(en)". Below the navigation is a product card for "ISO/IEC 30111:2013(en)" titled "Information technology – Security techniques – Vulnerability handling processes". At the bottom of the card is a "Table of contents" button.

Reporting vulnerable items

- Responsible Disclosures / CVD
- Bulk reporting



The screenshot shows the SendGrid website with a 'New Account' form. The 'Trial 40K \$0.00 / mo' plan is selected. To the right, a developer terminal window runs a curl command to send an email via the API, and a mobile device screen shows the SendGrid mobile app interface.

```
curl --request POST \
--url https://api.sendgrid.com/v3/mail/send \
--header 'Authorization: Bearer $SENDGRID_API_KEY' \
--header 'Content-Type: application/json' \
--data '{"personalizations": [{"to": [{"email": "test@example.com"}]}, {"from": {"email": "test@example.com"}, "subject": "Sending with SendGrid is Fun", "content": [{"type": "text/plain", "value": "and easy!"}]}]}
```


Social targeted ransomware

Warning Message!!

We are sorry to say that your computer and **your files have been encrypted**,
but wait, don't worry. There is a way that you can restore your computer and all of your files

0 years, 6 days, 00 hours, 45 min and 58 sec

Time remain when your files will lost forever!

Your personal unique ID: **[0e72bfe849c71dec4a867fe60c78ffa5](#)**

Please send at least **1.0 Bitcoin** to address **[1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3](#)**

[Click to check your Balance](#)

Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address
[1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3](#). When we will get the money, we will
immediately give you your private decryption key. Payment should be confirmed in about
2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we
will decrypt your files for free.

<https://3hnuhudu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5>

What we did?

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world ([Encryption-Wikipedia](#)). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.

Why we do that?

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more than half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2015**. The sad part of this war is that all the parts keep fighting but eventually the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. ([Syria War in Wikipedia](#))

Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people.
We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

How to buy Bitcoins?

If you aren't familiar with Bitcoin and don't know what it is, please visit the official Bitcoin website (<https://bitcoin.org/en/getting-started>), follow the steps and you'll get your Bitcoins. To understand more you can check also on the FAQ page (<https://bitcoin.org/en/faq>). Please check this website (<https://coinatmradar.com/>) where you can find Bitcoin ATM all over the world.



Title Text

Body Level One
Body Level Two
Body Level Three
Body Level Four
Body Level Five



Freebees

amazon Try Prime Kindle Store ▾

Departments ▾ Your Amazon.com Today's Deals Gift Cards & Registry Sell Help EN Hello. S Account

Buy a Kindle Kindle eBooks Kindle Unlimited Prime Reading Advanced Search Best Sellers & More Kindle Book Deals Free Reading Apps Kindle Singles Newsstand

Books > Computers & Technology > Networking & Cloud Computing

Look inside ↴

HELPFUL HACKERS
How the Dutch do Responsible Disclosure



Chris van 't Hof

TEK TOE

Kindle Edition
by [Chris van 't Hof](#) (Author)
Be the first to review this item

▶ See all formats and editions

Kindle eBook
\$7.78

Read with Our [Free App](#)

'Hospital leaks patient records', 'banking app unsafe' – it seems that discovering a flaw is not necessarily cyber security. He or she immediately well-coordinated approach allows

▼ [Read more](#)

Length: 247 pages ▾
Age Level: 12 - 18

Helpfull Hackers: How the Dutch do Responsible Disclosure

Kindle Edition
by [Chris van 't Hof](#) (Author)
Be the first to review this item

▶ See all formats and editions

Kindle eBook
\$7.78

Read with Our [Free App](#)

'Hospital leaks patient records', 'banking app unsafe' – it seems that discovering a flaw is not necessarily cyber security. He or she immediately well-coordinated approach allows

▼ [Read more](#)

Length: 247 pages ▾
Age Level: 12 - 18

Victor Gevers
@0xDUDE

You can get the ePub version of the book #helpfulhackers here for free:
helpfulhackers.nl

Mikko Hypponen @mikko
Interesting book on how Dutch government & companies work with hackers. Thanks for the copy, @Cvthof!

5:34 PM - 21 Jun 2017 from Serris, France

24 Retweets 34 Likes

1 24 34

Summer Kindle Monthly Deals
Up to 80% off 1,000+ Kindle books [Browse now](#)



MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU
PLEASE FILL OUT YOUR EVALUATIONS!

Victor Gevers
Chairman GDI.foundation
@GDI_fdn