MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

REPAIRING THE INTERNET WITH RESPONSIBLE DISCLOSURES

Victor Gevers

Chairman GDI.foundation

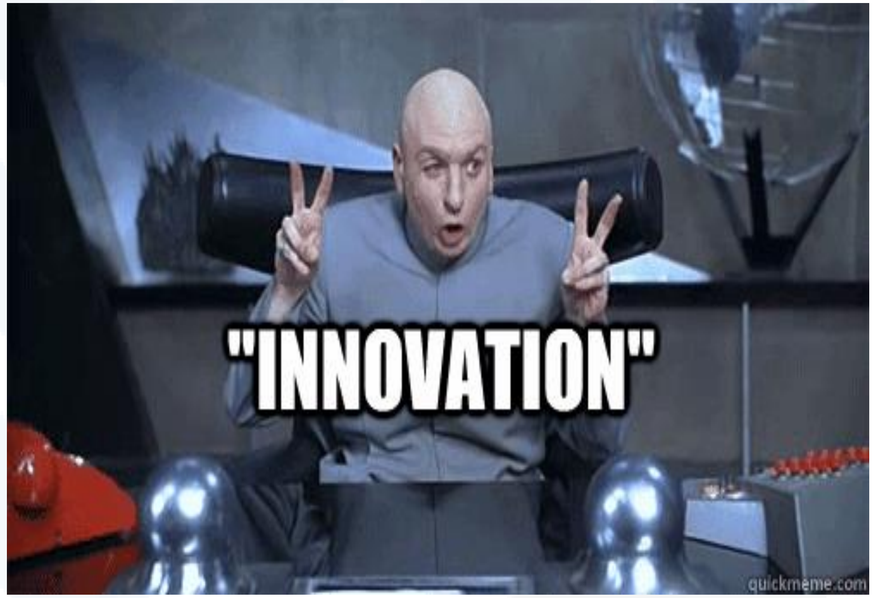
@GDI_fdn

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


THE DUTCH FARMER
Handcrafted in the Green Heart of Holland
100% Traditional Farmhouse Cheese
Milk matured
Old
Matured
Very old
Extra matured
Very very old
Handcrafted the old fashioned way


"INNOVATION"
quickmeme.com


INNOVATION
MANAGER
ONLY BECAUSE...
FULL TIME
MULTI TASKING
NINJA
IS NOT AN ACTUAL
JOB TITLE

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 being 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

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, Janit0r 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 specialized in notifying organizations affected by vulnerabilities, malware, and other cyber threats.

How

GDI Foundation
@GDI_FDN Follows you

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

Tweets | Tweets & replies | Media

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

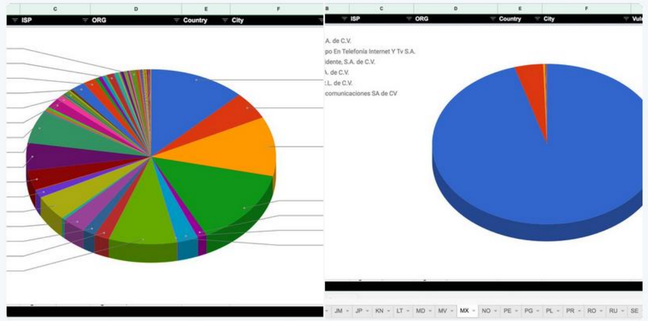
GDI Foundation @GDI_FDN · 10h
We want to express our deep gratitude to all ISPs, involved organizations and volunteers for their contribution to help to address the issue of vulnerable Memcached servers. Thank you so much for your effort. We could not have achieved this level of success without your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

4 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

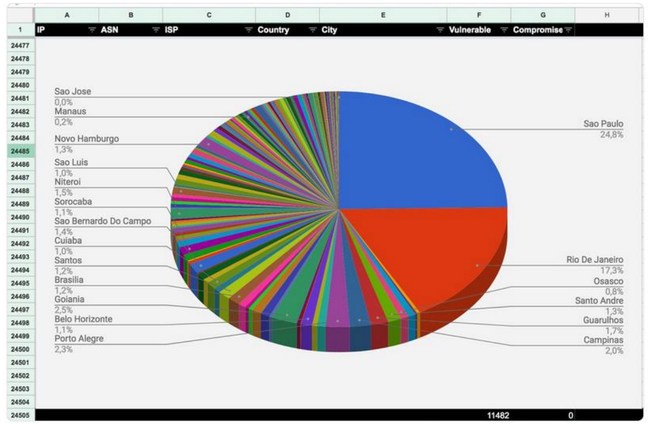
GDI Foundation @GDI_FDN · 2 Sep 2017
There a lot of Arris devices scattered over a lot cities and villages in Mexico. Luckily there are not some many ISP we need to reach out to



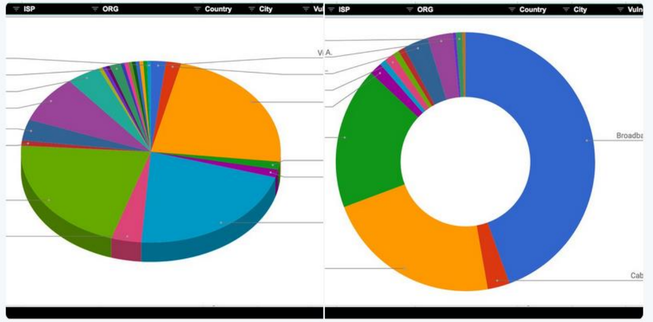
1 3 5

Show this thread

GDI Foundation @GDI_FDN · 2 Sep 2017
We currently helping a few ISP's in Brazil. Most of them started with mitigation after we contacted them. Next up is Mexico.

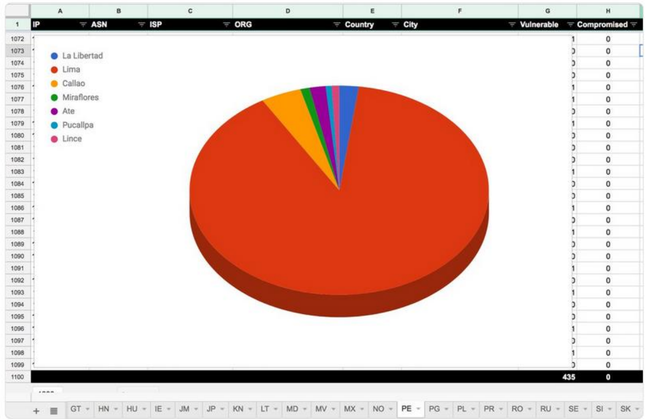


GDI Foundation @GDI_FDN · 3 Sep 2017
In a few more hours the most identified vulnerable Arris devices will be taken care of in Argentina. Next up is Colombia.



2 5

GDI Foundation @GDI_FDN · 3 Sep 2017
This morning we started reporting vulnerable Arris devices in Peru. After this only 2 more countries left and South America will be done.



1 3

InfoSecWorld Conference & Expo 2018

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

Search

FOLLOW BY EMAIL

Email address... Submit

BLOG ARCHIVE

▼ 2017 (30)

► April (1)

► March (10)

► February (6)

▼ January (13)

Foreign fighters' helpers excluded from refugee st...

The UK Brexits 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)

download

https://www.justice.gov/criminal-ccips/page/file/983996/download

1 of 8 — Automatic Zoom

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

A Framework for a Vulnerability Disclosure Program for Online Systems[1]

Version 1.0 (July 2017)

An increasing number of organizations in the public and private sectors are adopting vulnerability disclosure programs to improve their ability to detect security issues on their networks that could lead to the compromise of sensitive data and the disruption of services.[2] Some organizations are informally soliciting vulnerability reports without creating structured vulnerability disclosure programs. Others, however, are creating formalized vulnerability disclosure programs that include published policies describing the manner in which they will accept information about security vulnerabilities and how they may disclose vulnerability reports to affected parties and/or the public. Such policies may also outline authorized methods that may be used to discover vulnerabilities in an organization's information systems, services, and products.

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 of or objectives for vulnerability disclosure programs; different

https://www.eenews.net/assets/2017/08/02/document_ew_01.pdf

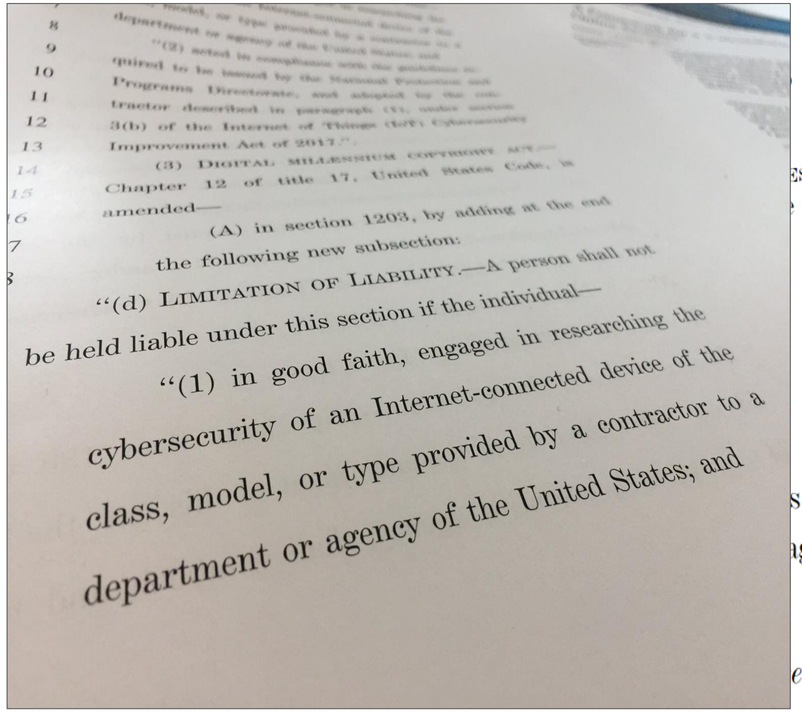
1 of 20 — 150%

115TH CONGRESS
1ST SESSION

S. _____

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

_____



Programs Directorate, and adopted by the con-
tractor described in paragraph (1), under section
3(b) of the Internet of Things (IoT) Cybersecurity
Improvement Act of 2017."

(3) DIGITAL MILLENNIUM COPYRIGHT ACT.—
Chapter 12 of title 17, United States Code, is
amended—

(A) in section 1203, by adding at the end
the following new subsection:

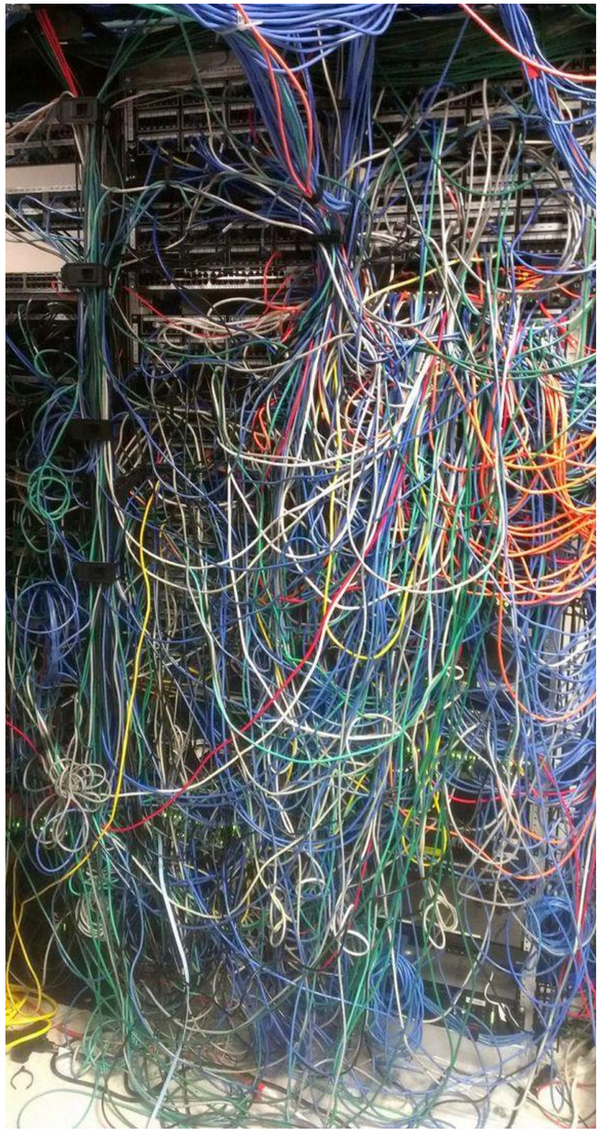
"(d) LIMITATION OF LIABILITY.—A person shall not
be held liable under this section if the individual—

"(1) in good faith, engaged in researching the
cybersecurity of an Internet-connected device of the
class, model, or type provided by a contractor to a
department or agency of the United States; and

es) in-
Com-
s for
agen-
enta-

2 *tives of the United States of America in Congress assembled,*

The Internet landscape (today)



2016

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

Insert Metrics

RESOLVED VULNERABILITIES AFTER REPORTED* IN 2016

TOP 5 SHORTEST TIME TO FIX

COUNTRY	REPORT	AVG FIX TIME
CN	43 (39)	4,9 days
BE	14 (14)	5,3 days
UA	35 (31)	5,3 days
INDIA	15 (14)	7,4 days
NL	136 (114)	8,0 days

TOP 5 LONGEST TIME TO FIX

COUNTRY	REPORT	AVG FIX TIME
RU	16 (11)	18,6 days
GB	75 (57)	14,6 days
FR	23 (17)	14,0 days
JP	34 (23)	12,8 days
US	144 (106)	10,5 days

TOP 5 NOT FIXED

COUNTRY	REPORT	OPEN VULN.
US	144	38
NL	136	22
GB	75	18
JP	34	11
FR	23	6

* Responsible Disclosure (NCSC.NL)
** in parentheses indicates number of resolved reported vulnerability

2017

Screenshot 2017
WSJ report

2018

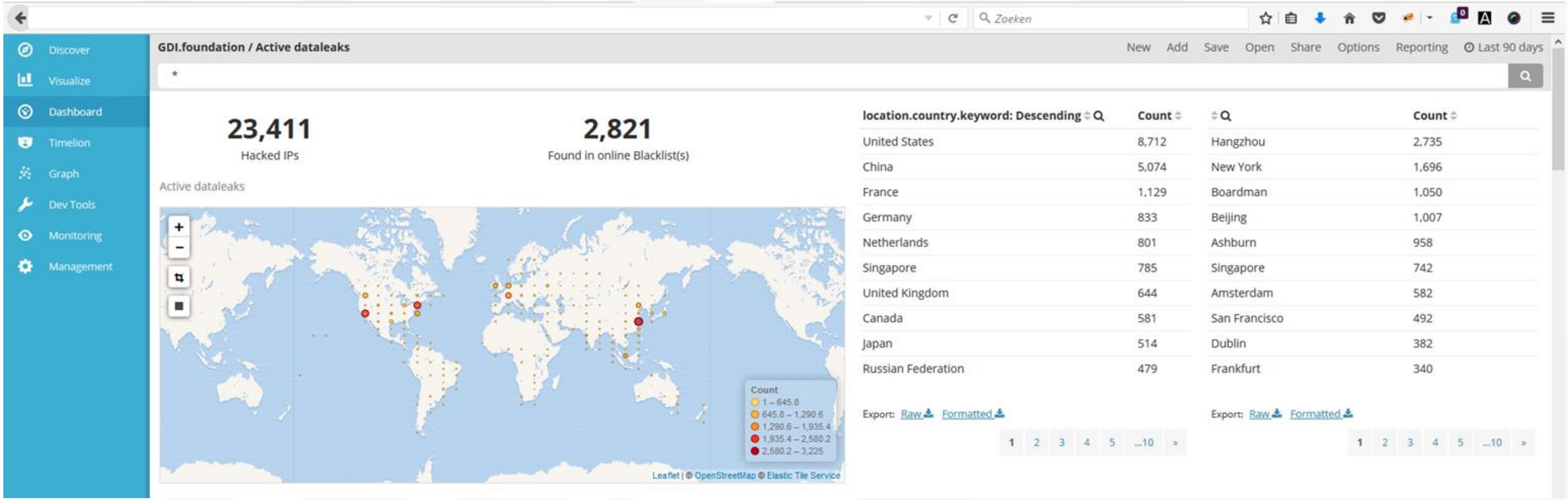
GDI foundation - Overview 2018

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

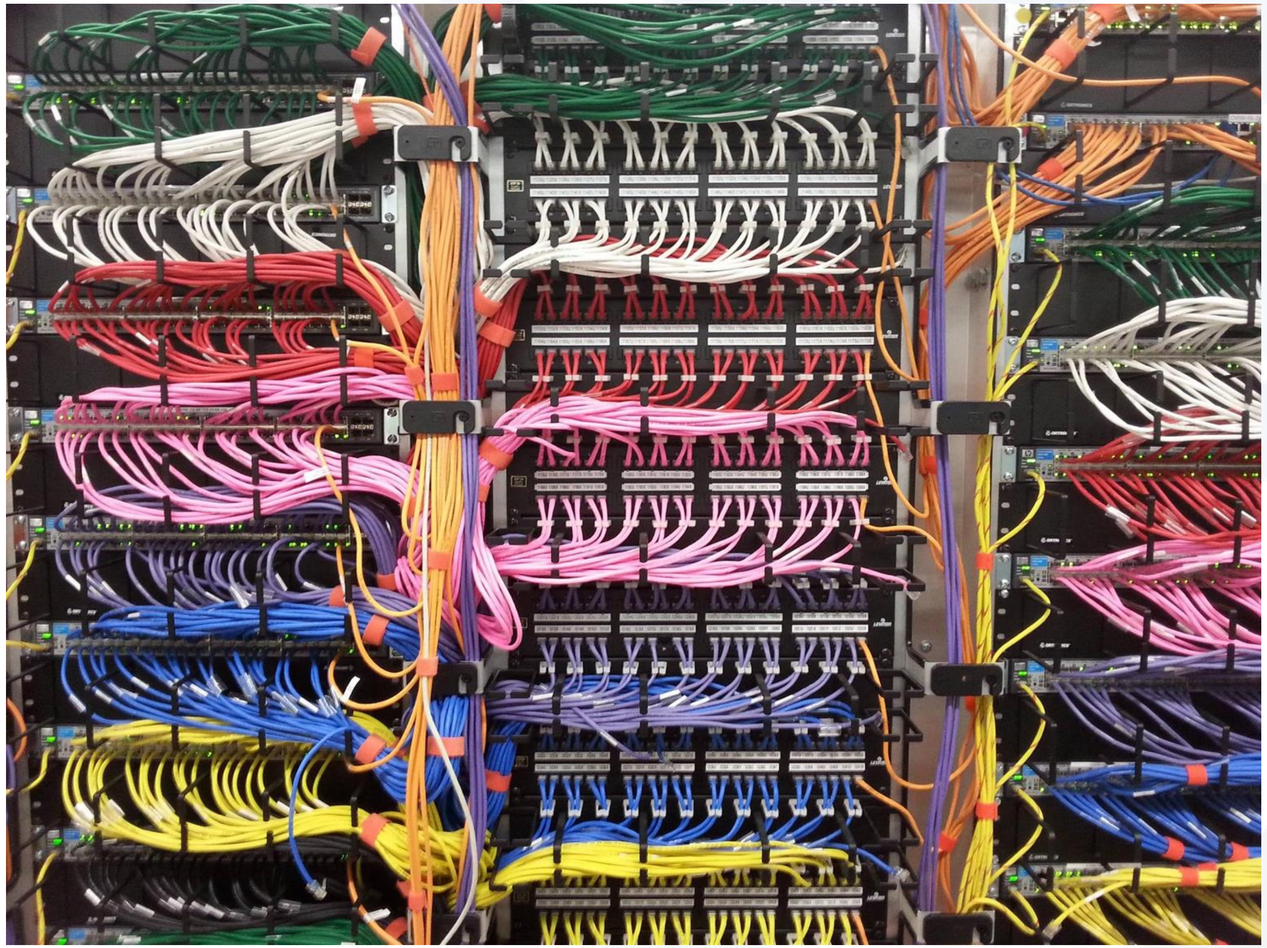
	A	B	C	D	E
1		Found	Comprised	Reported	Fixed
2	AWS S3 [scanner]	536	1	529	109
3	Cassandra	1.432			
4	CouchDB	16.372	1.203	9.032	8.039
5	Elasticsearch	7		7	6
6	Hadoop HDFS	5.778			
7	Jenkins	6.661	27	54	50
8	MongoDB	18	15	18	18
9	Redis	21.382			
10	Vuln: EternalBlue	7.493		14	14
11	Github Scanner				
12	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

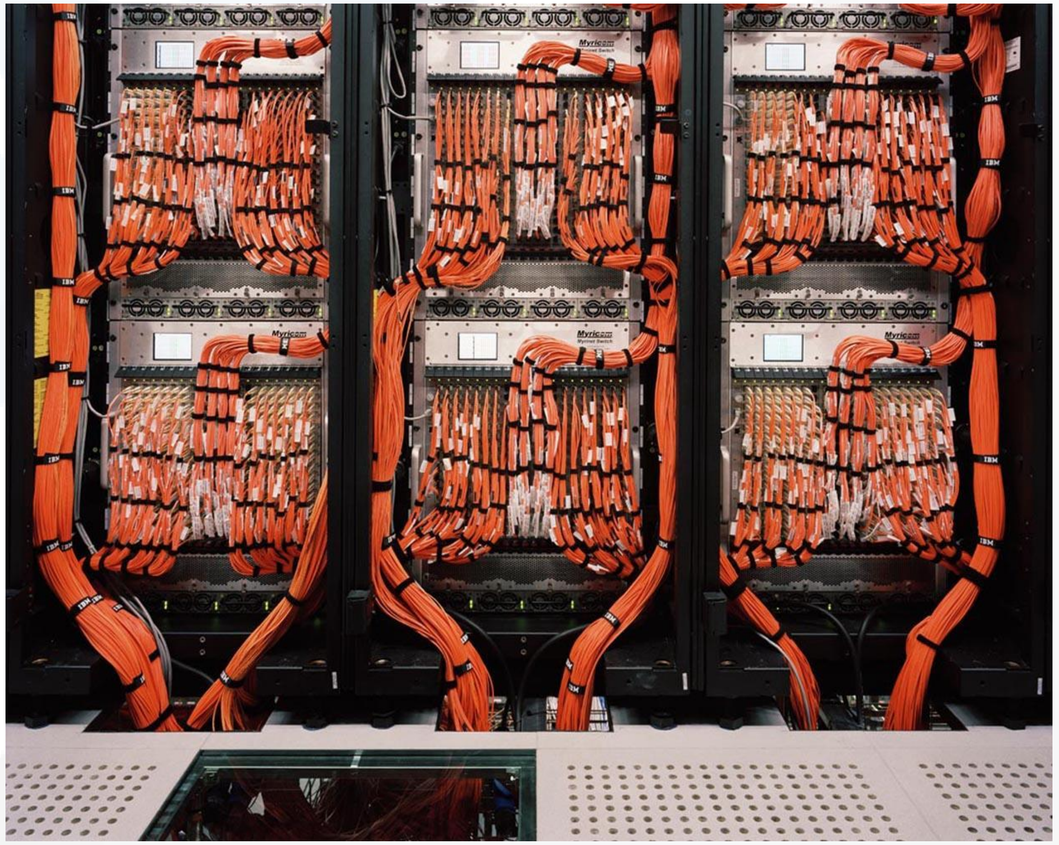
Current Internet Landscape

Data Leaks



Getting the overview





Finding vulnerabilities

- Searching the internet

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category | Search | Search

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 inurl:"index.php?option=com_joomanager"

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=itemslist...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
No information is available for this page.
Learn why

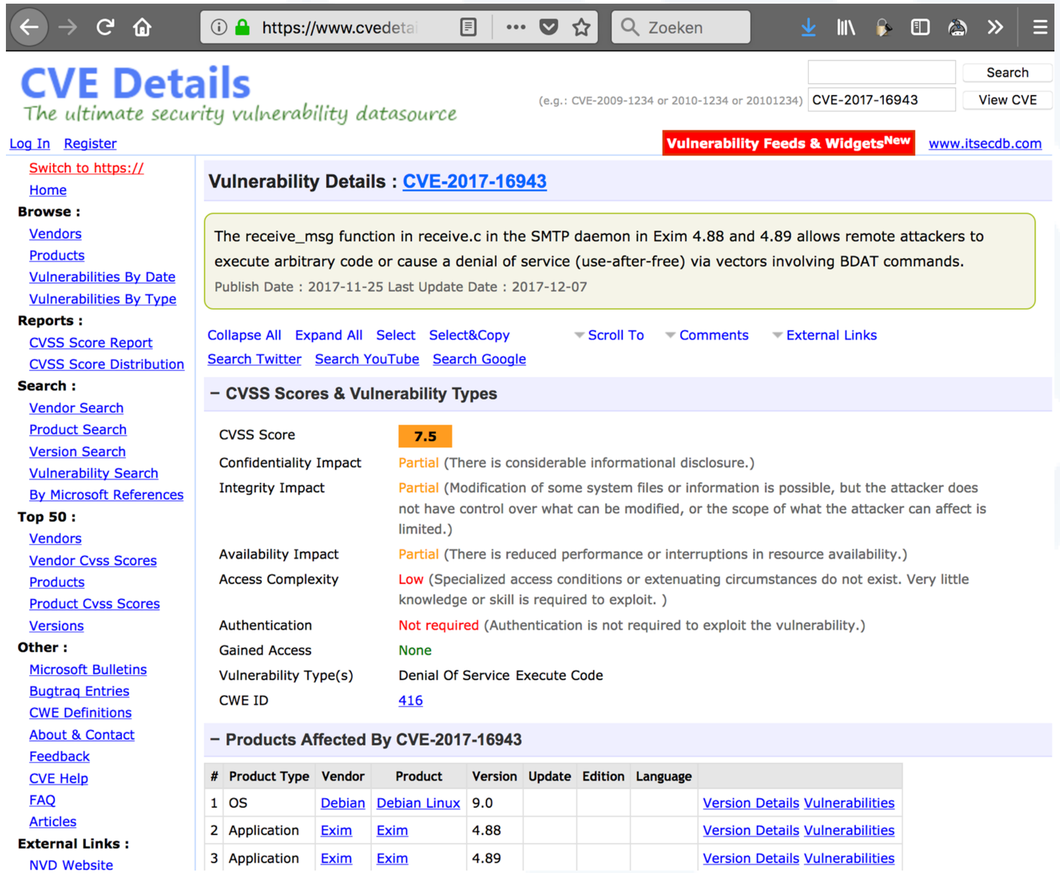
Joomanager Component - Joomla Templates
www.shape5.com/demo/real_estate/index.php?option=com_joomanager&view...
Joomla! - the dynamic portal engine and content management system.

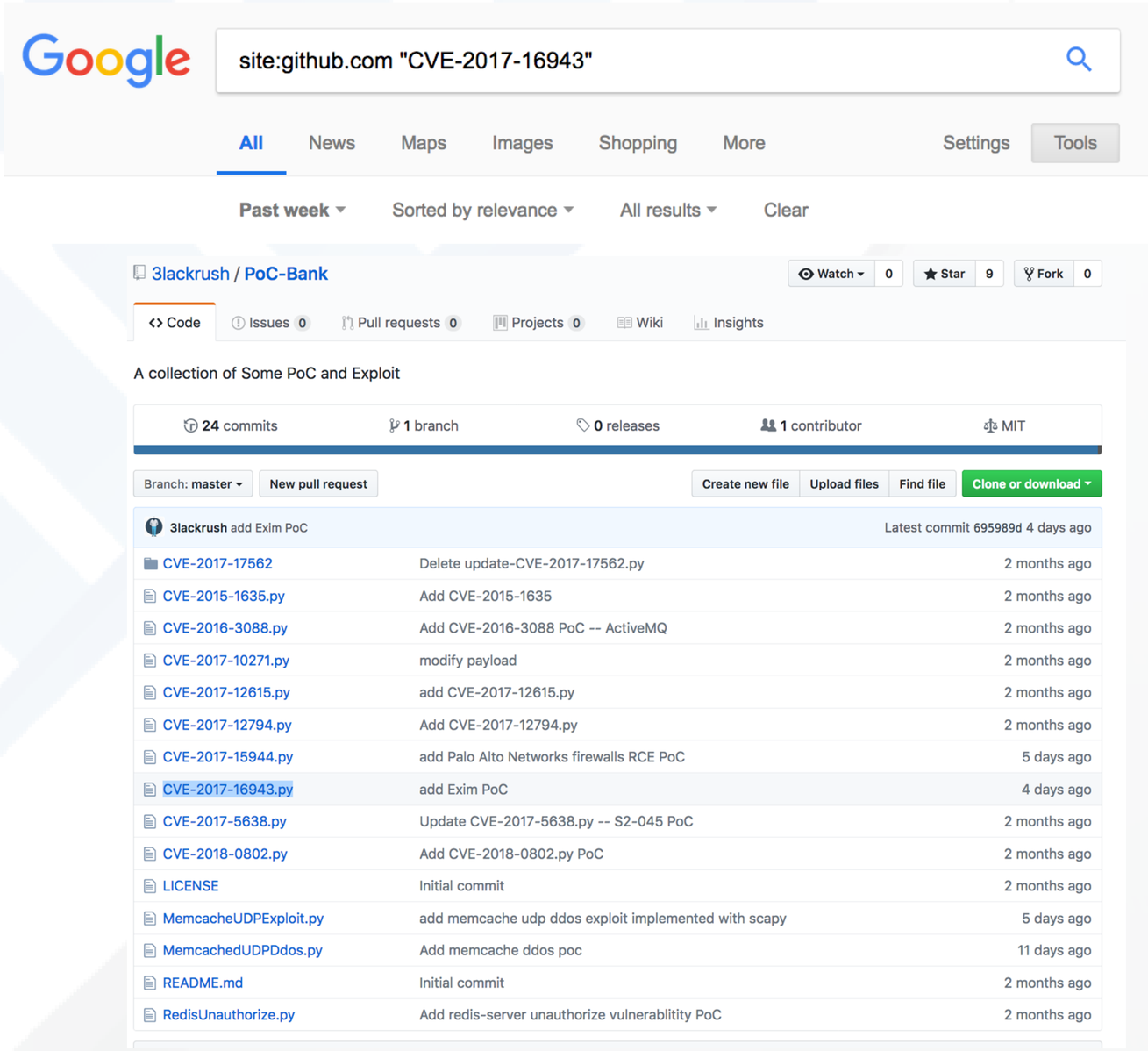
Joomanager Item List - Joomla Templates
www.shape5.com/demo/portfolio/index.php?option=com_joomanager&view...
Joomla! - the dynamic portal engine and content management system.

Rob Marland Listings
www.robmarland.com/index.php?option=com_joomanager&view=items
Home · Listings · Current Listings · Past Sold Listings · For Sellers · Property Evaluation · Marketing

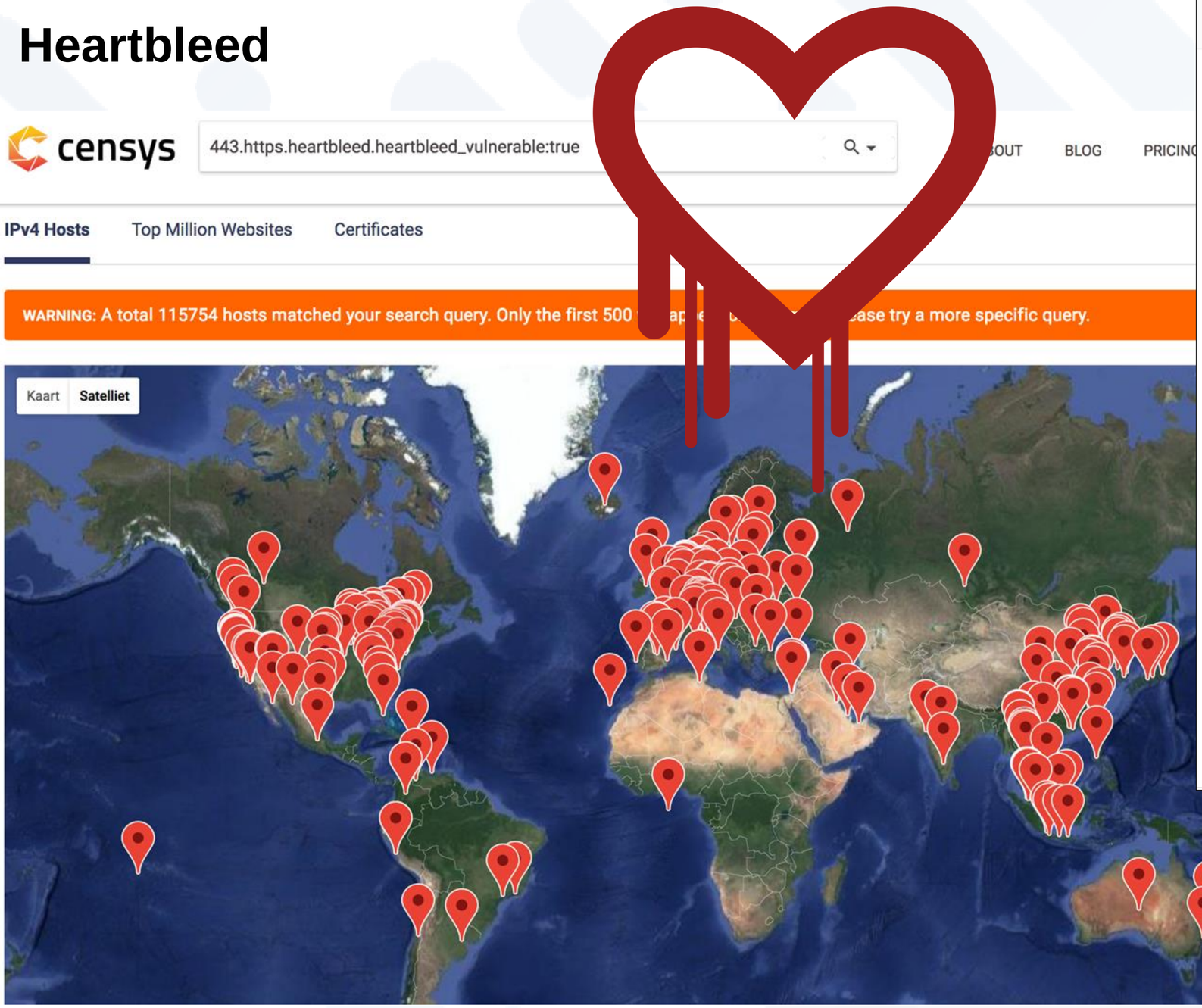
Finding vulnerabilities

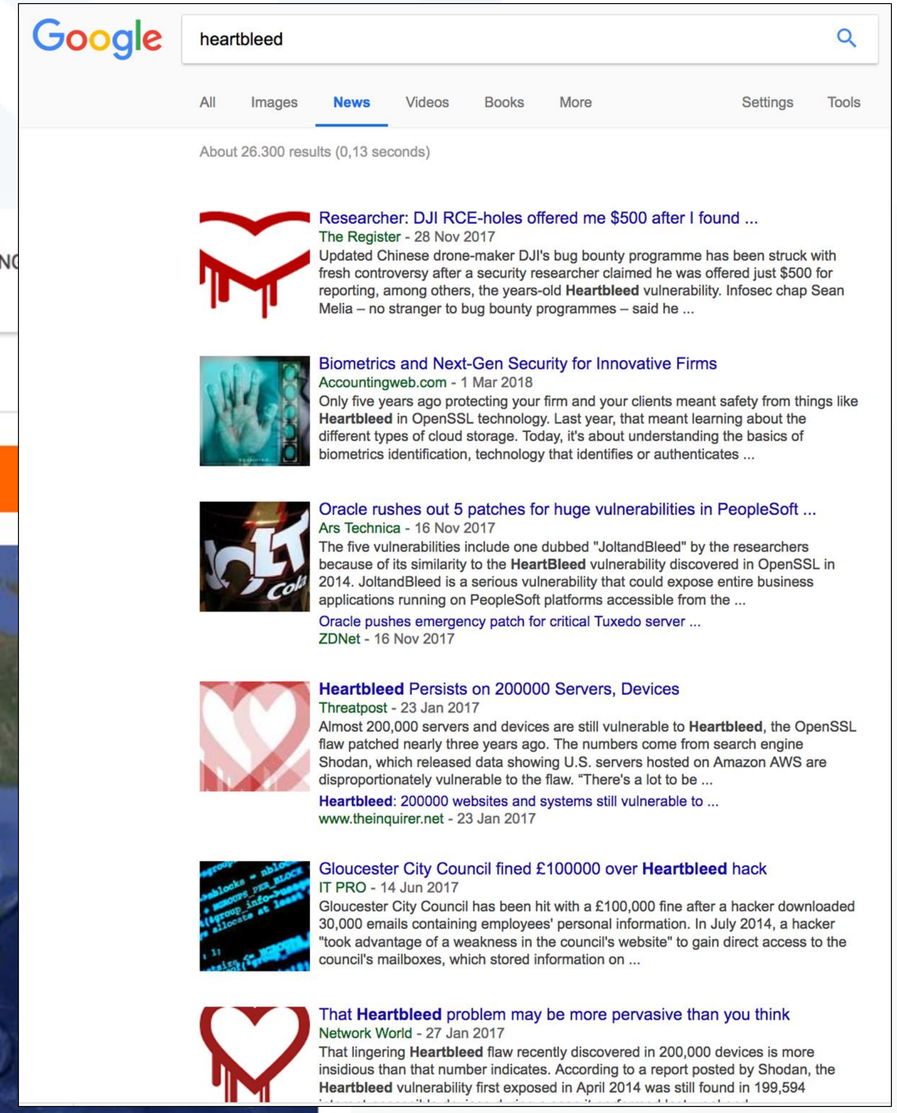
- Searching the internet
- Scraping everything what is public





Heartbleed





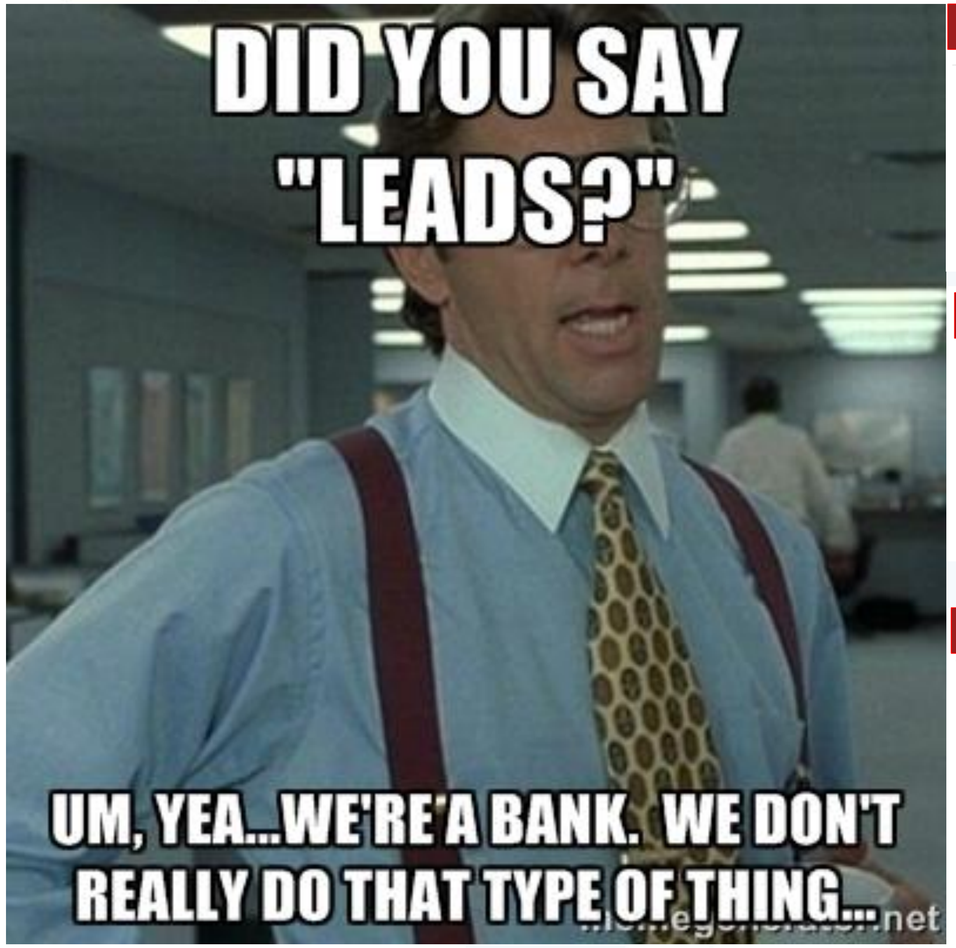
Heartbleed

censys

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

IPv4 Hosts Top Million Websites Certificates Tools Help

Results: 765,854 Time: 207ms



[redacted]

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

[redacted]

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

[redacted]rusnarbank.ru)

Network 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

Devices

Reposify BETA

Discover Overview Pricing

Documentation Help My Account

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

Query Credits Count: **99**

Filter By

Service Port

80
443
49154
7547

Device Type

Router
Firewall
ICS
Modem
Gateway
Website

197.0.140.197 Tunisia BackBone AS 2016-09-

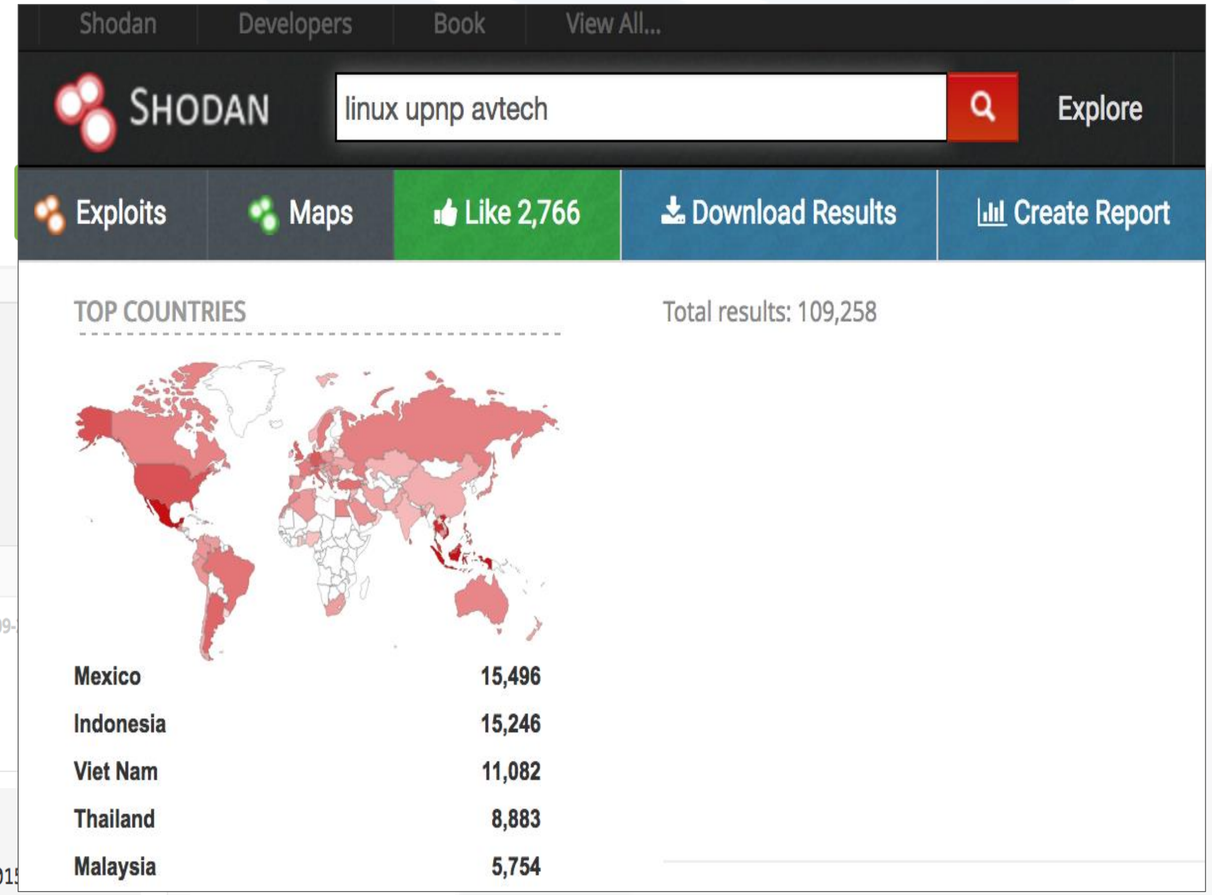
HTTP (80/TCP)

Type Webcam

Name DNVRS-Webs

Response

```
Last-Modified: Fri, 18 Dec 201
9 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
```



InfoSecWorld Conference & Expo 2018

Brickers, Cure, Wipers

The Register®
Biting the hand that feeds IT

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

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 Brickbot, 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.

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
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 the 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

mongoDB®

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

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & A

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
[redacted]
> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"
, "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNc2jyvDRhLyYpkCh323MsMq AND
 CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
> exit
bye
victor@windowlicker:~$ ^C
victor@windowlicker:~$
```

RETWEETS 194 LIKES 124

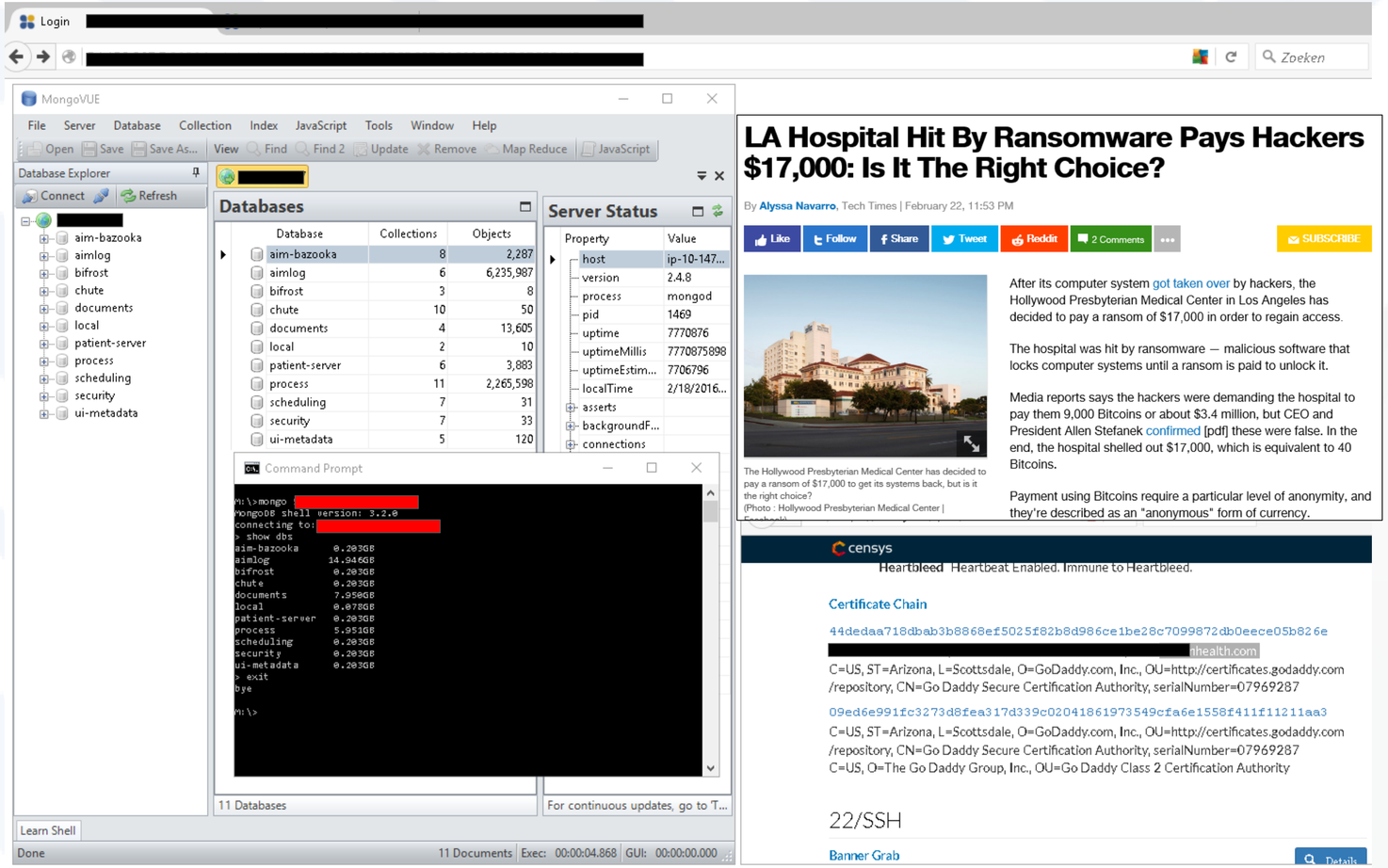
10:52 PM - 27 Dec 2016

pastebin.com/raw/

pastebin.com/raw/ciVmwzHg

```
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 Mongodb 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 )
```

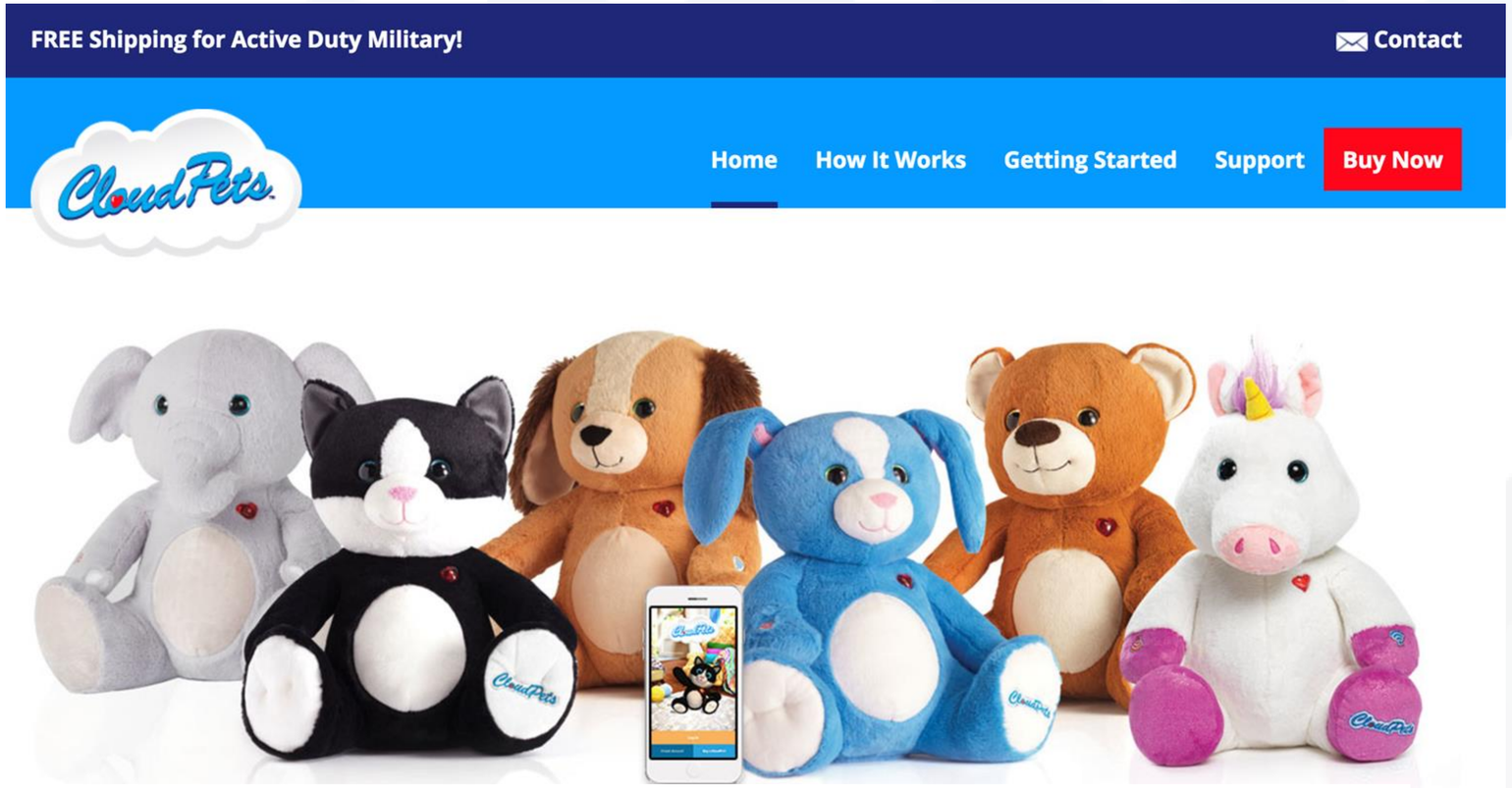
Ransom (Ransack attacks)



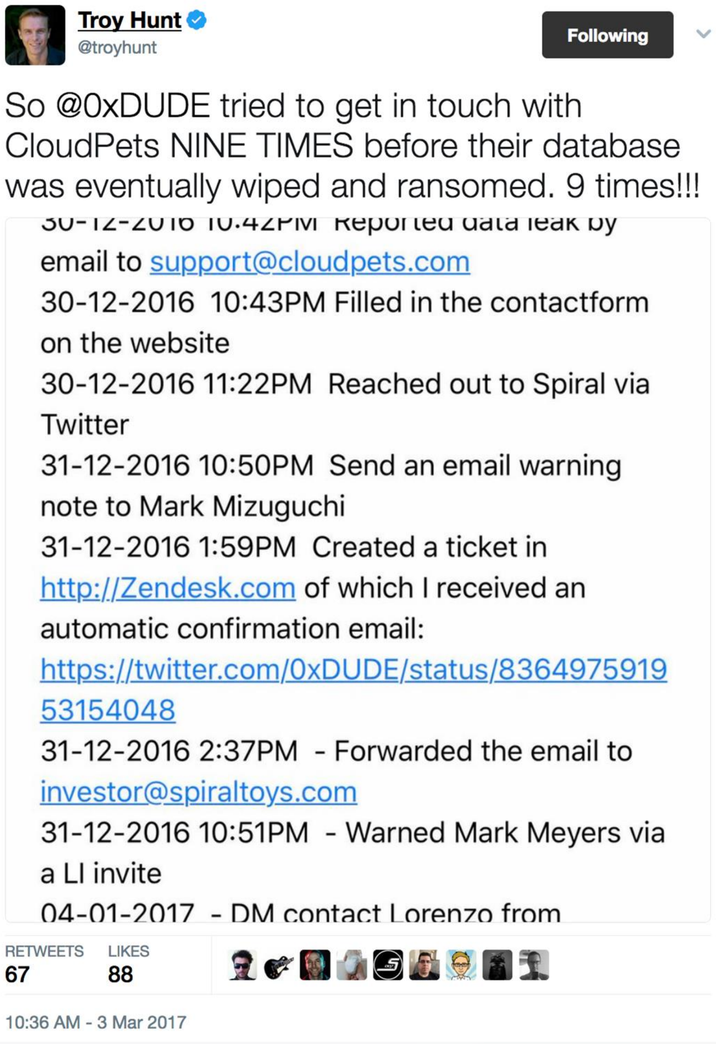
Internet of Toys

The Washington Times | HOME | NEWS | OPINION | SPORTS | MARKET | SUBSCRIBE

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



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 67 LIKES 88

10:36 AM - 3 Mar 2017

Sharing IOCs via Google (Sheets)

MongoDB ransacking

Bestand Bewerken Weergeven Invoegen Opmaak Gegevens Extra Add-ons Help Alle wijzigingen zijn opgeslagen in Drive

Arial 10

04-04-2017

https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransoms-your-data

Last Sighted on	Email Address(Sighted As)	Bitcoin Address	Ransom size	ıber of Transact	Total BTC Recieved	Name of replaced DB	Known Attacker IPs	Victims (OSINT)	Victims (helped)
10-1-2017 14:00:00	bitcoinbaron@protonmail.com	17KdFUA9WJTTwYNp4iRPjLyLDkBfiz2zj6	0.2BTC					18	
								5	
							23	43	
							53	4034	
							3.100	745	
11								18	
16			TC				138		
			TC						
16			BTC					5913	
19			TC				9.112		1
1-1			C				164	2553	
31.01.2017 08:30	m4l1c3@sigaint.org	1B5PMtKhqC97ppNrixfkyT1chQuvDGXXei	0.5BTC					4106	
08-02-2017 20:57		1NHrbhXmSzzCa8VhWqsza82NaUynxs	0.5BTC				64		
14-03-2017	vxware@sigaint.org	1B4kMRmY4yb4XW8hHnYRZT1WWNfnPfPbHR	0.2BTC					5066	
04-04-2017	mongodb@protonmail.ch	15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2	0.1 BTC				212	2368	3
Total				268	23.858734			32640	102

Google 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2

All Images Maps Videos News More Settings Tools

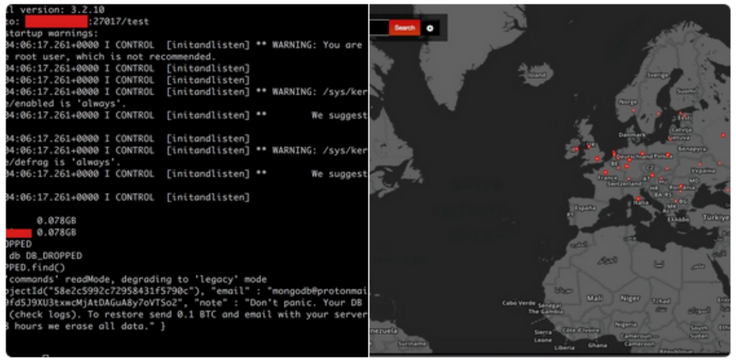
8 results (0.38 seconds)

Bitcoin Address 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2
https://blockchain.info/address/15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2
Apr 6, 2017 - Transactions sent and received from bitcoin address **15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2**.

Victor Gevers on Twitter: "New group: mongodb@protonmail.ch / 623 ...
https://twitter.com/0xdude/status/850090023911391233?lang=en
Apr 6, 2017 - New group: mongodb@protonmail.ch / 623 victims / **15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2** / DB_DROPPED / IP 62.244.25.212 ...

MongoDB ransacking - Google Docs
https://docs.google.com/spreadsheets/d/.../htmlview?sle=true
mongodb@protonmail.ch, 04-04-2017, mongodb@protonmail.ch, **15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2**, 0.1 BTC, 3, 0.3, DB_DROPPED, 62.244.25.212 ...

New group: mongodb@protonmail.ch / 623 victims / 15b9fd5J9XU3txwcMjAtDAGuA8y7oVTSo2 / DB_DROPPED / IP 62.244.25.212 goo.gl /VKKR1c



RETWEETS 4 LIKES 13

10:57 PM - 6 Apr 2017 from Ukraine

IoT Botnets for DDoS attacks

Dyn SM

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

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.

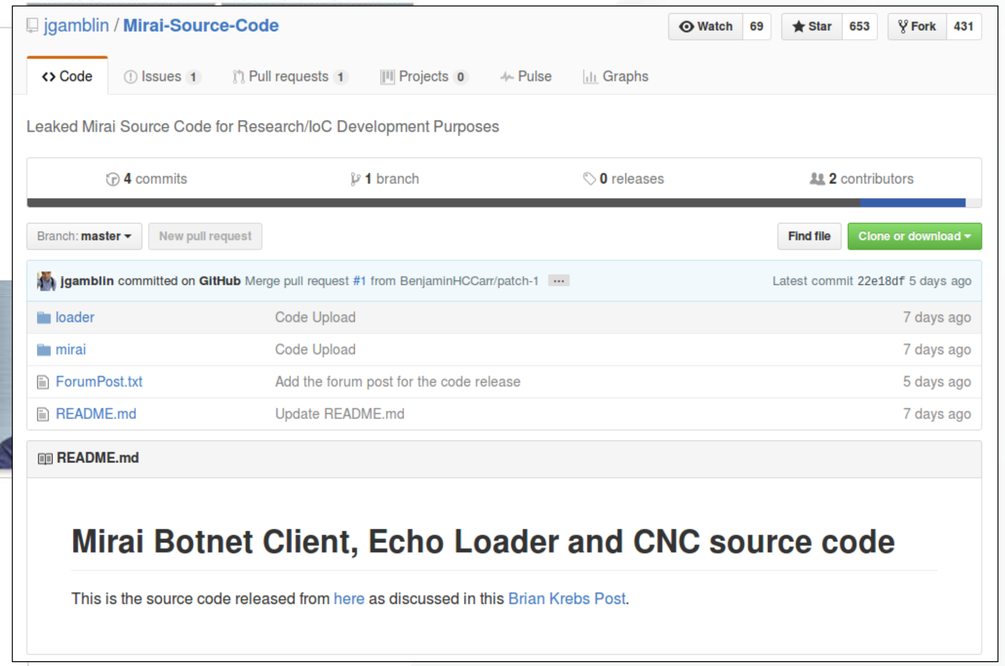
Posts Tagged: Mirai botnet

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.

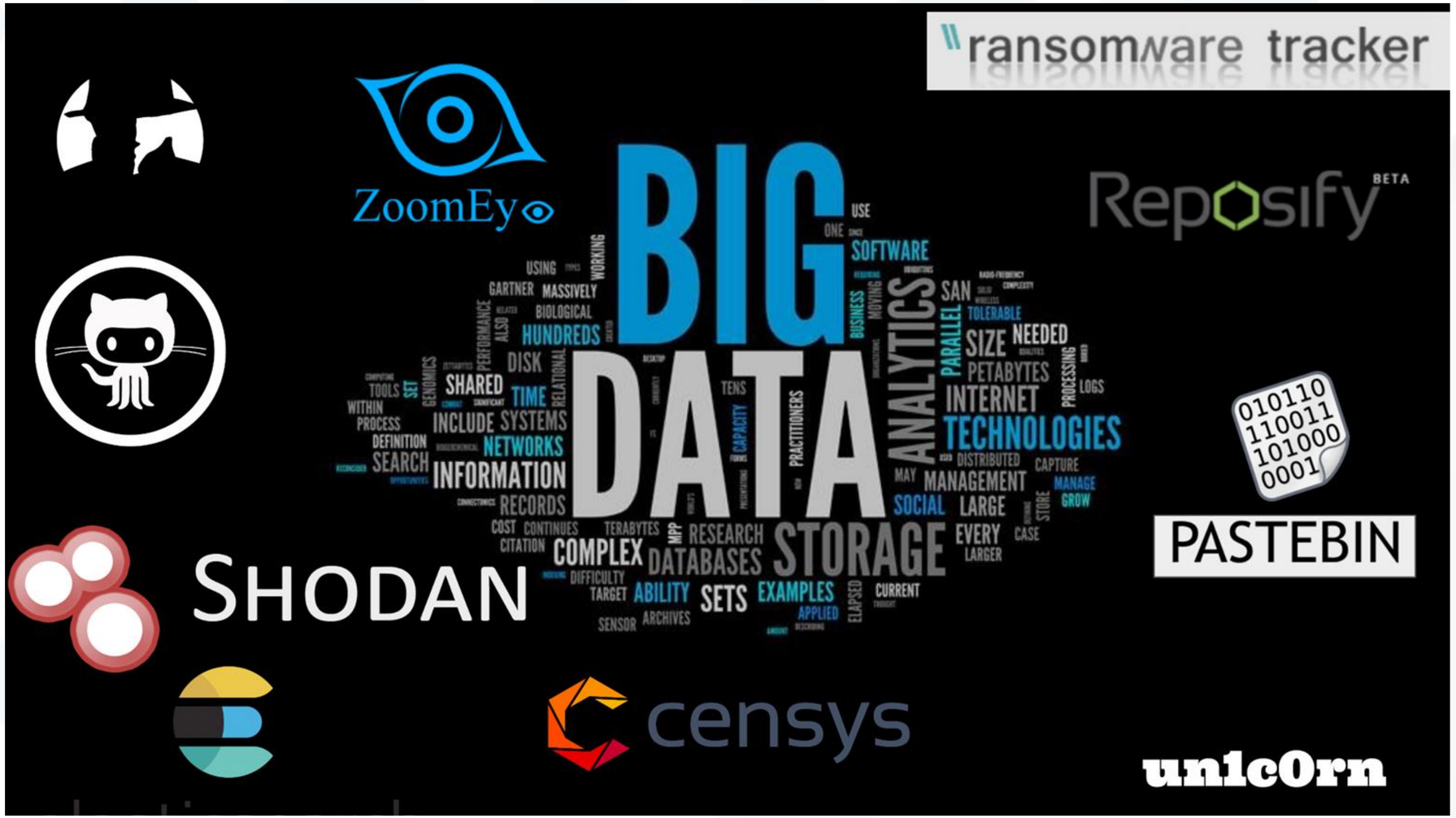
First, a quick recap on Mirai: This blog was taken offline in September following a record 620 Gpbs attack launched by a Mirai botnet. The source code for Mirai was leaked online at the end of September. Since then, the code has been forked several times, resulting in the emergence of several large Mirai-based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



InfoSecWorld
Conference & Expo 2018

Using Open source Intelligence (OSINT)

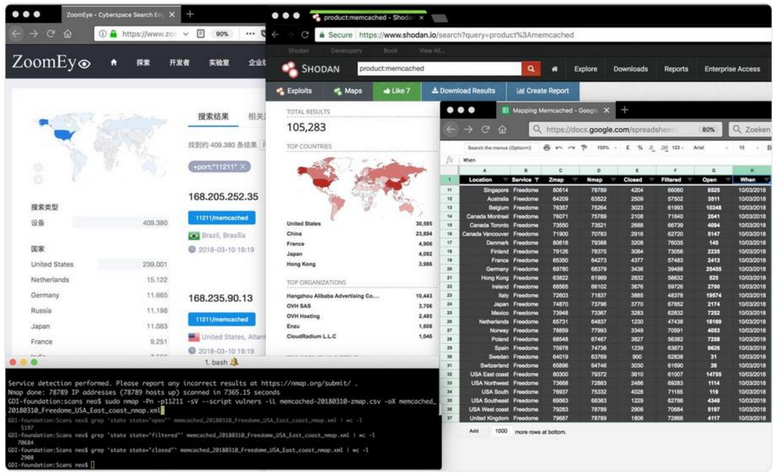
- Trusted and untrusted sources



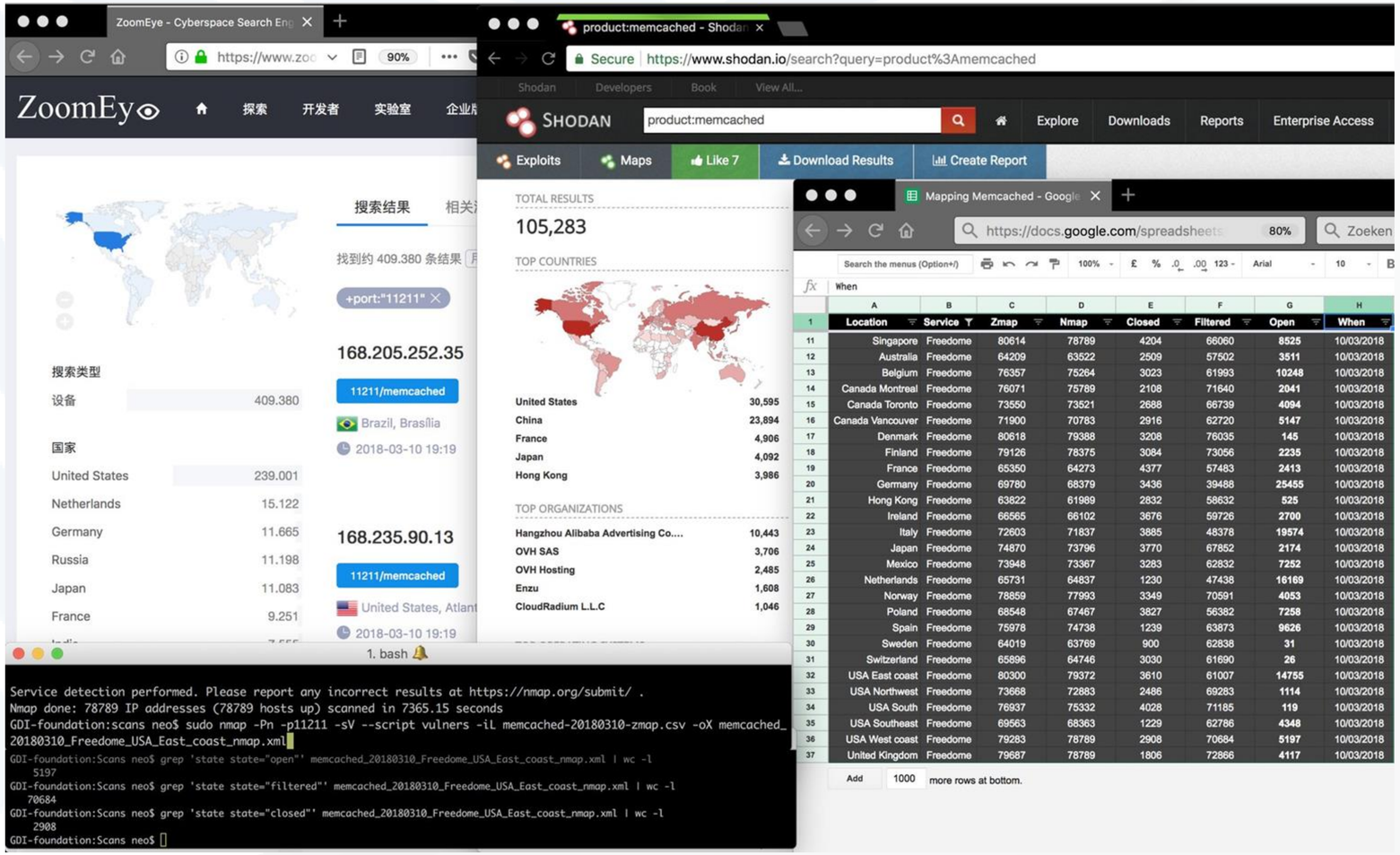
Using Open source Intelligence (OSINT)

- 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



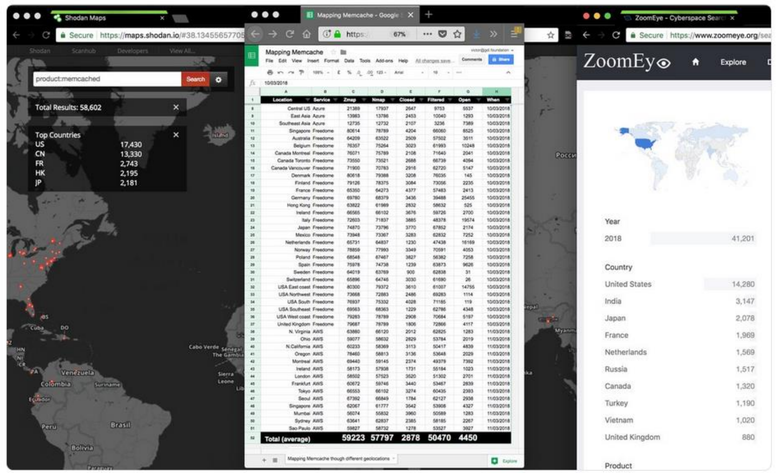
10:56 PM - 10 Mar 2018 from Amsterdam, The Netherlands



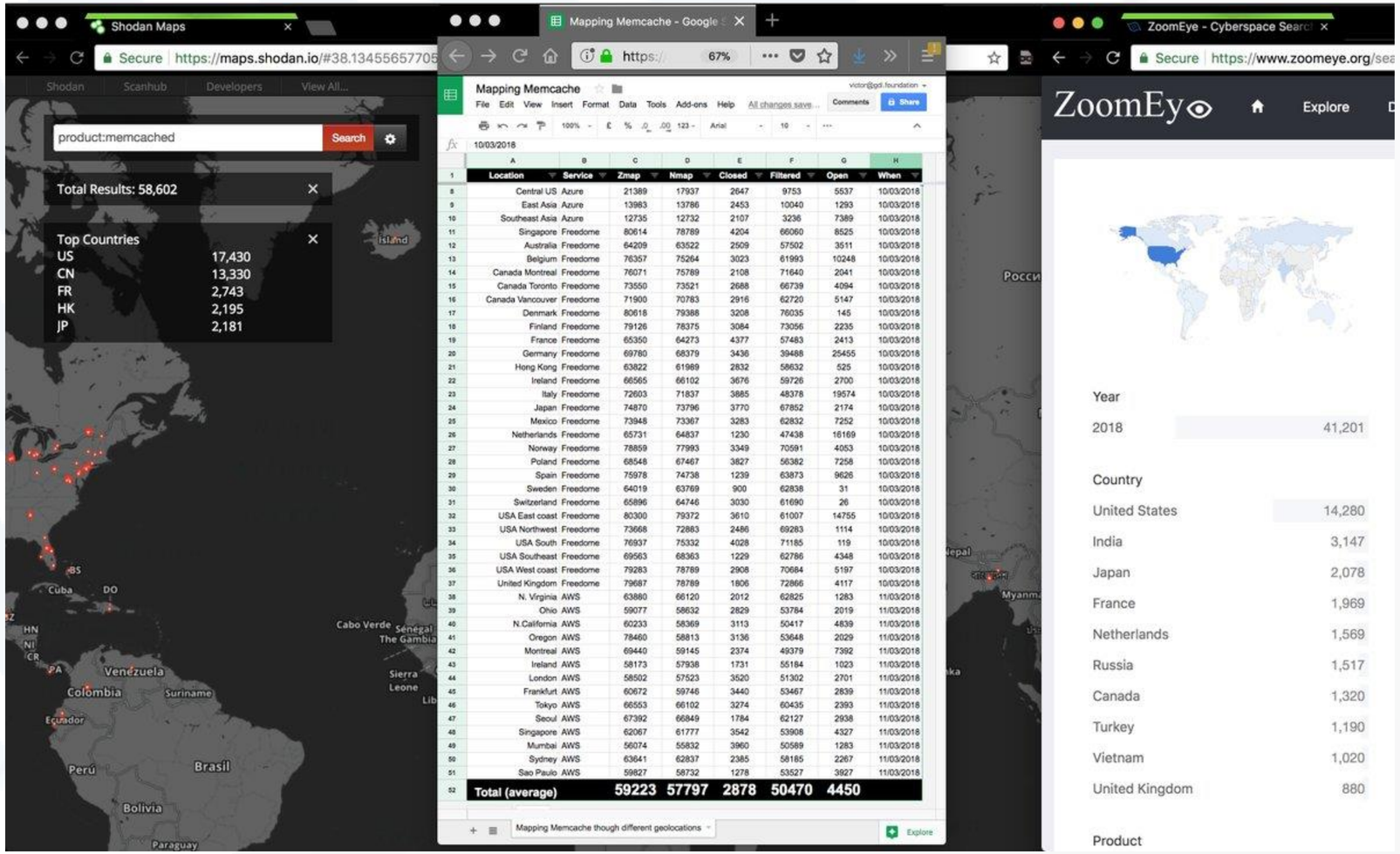
Using Open source Intelligence (OSINT)

- 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



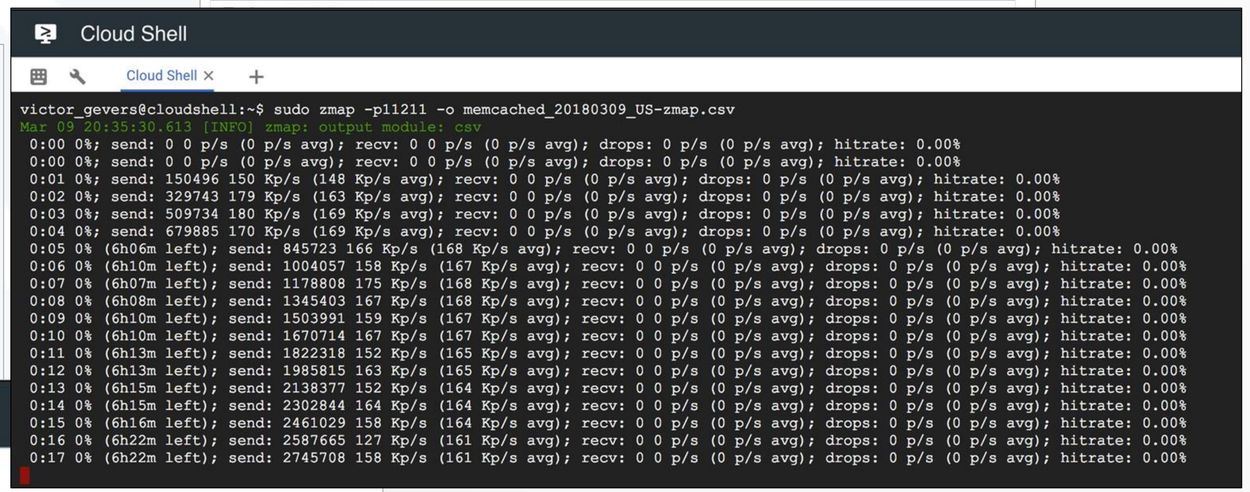
2:10 PM - 11 Mar 2018 from Amsterdam, The Netherlands



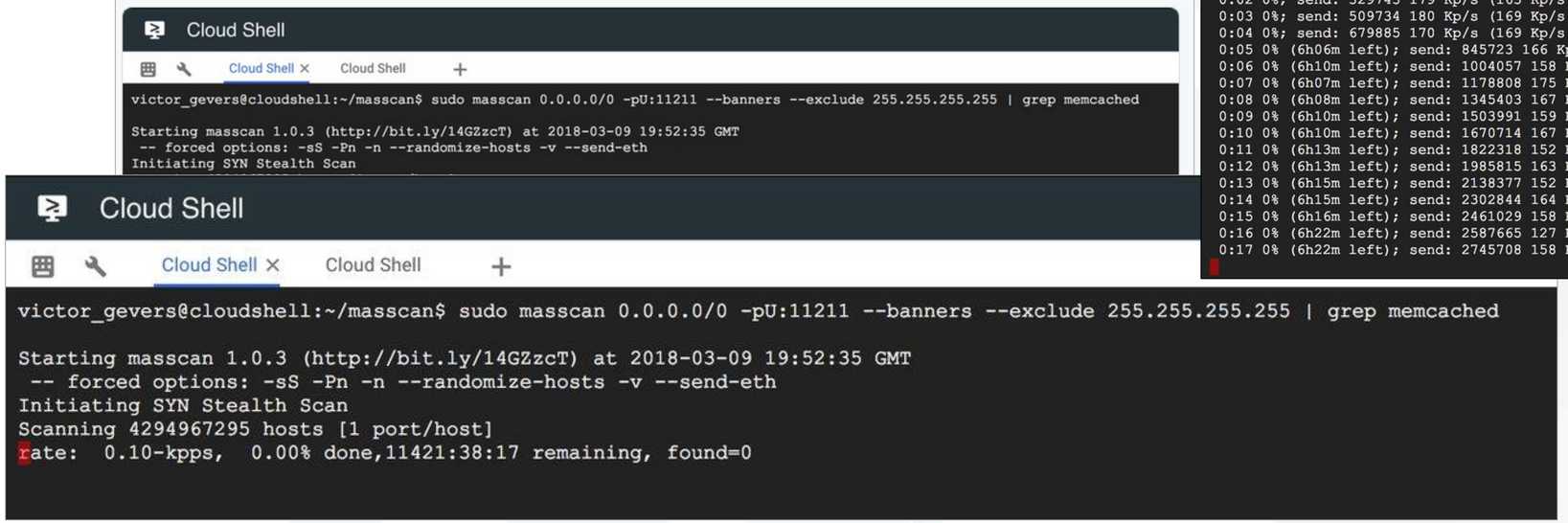
Using Open source Intelligence (OSINT)

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

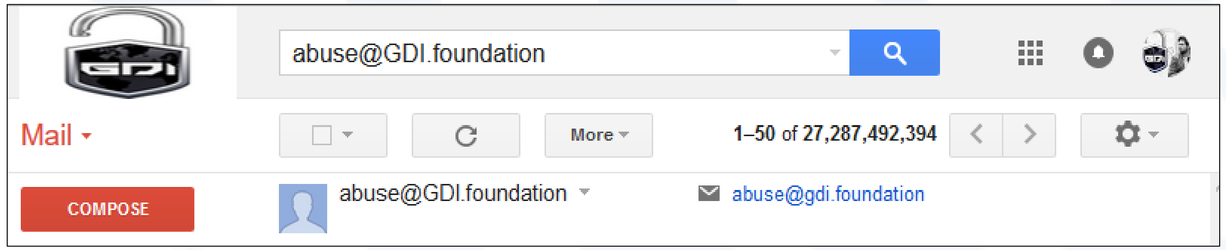
ZMap scanning from a Google Cloud Shell kind of works. It will take 6 hours just to scan for one port.



And running Massscan 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 :-)



Using Open source Intelligence (OSINT)



MongoDB ✓
@MongoDB

Follow

Check out Victor using Stitch and #MongoDBAtlas to build awesome tools at no cost in the cloud. Really cool job! Security scanning always important! 🔒

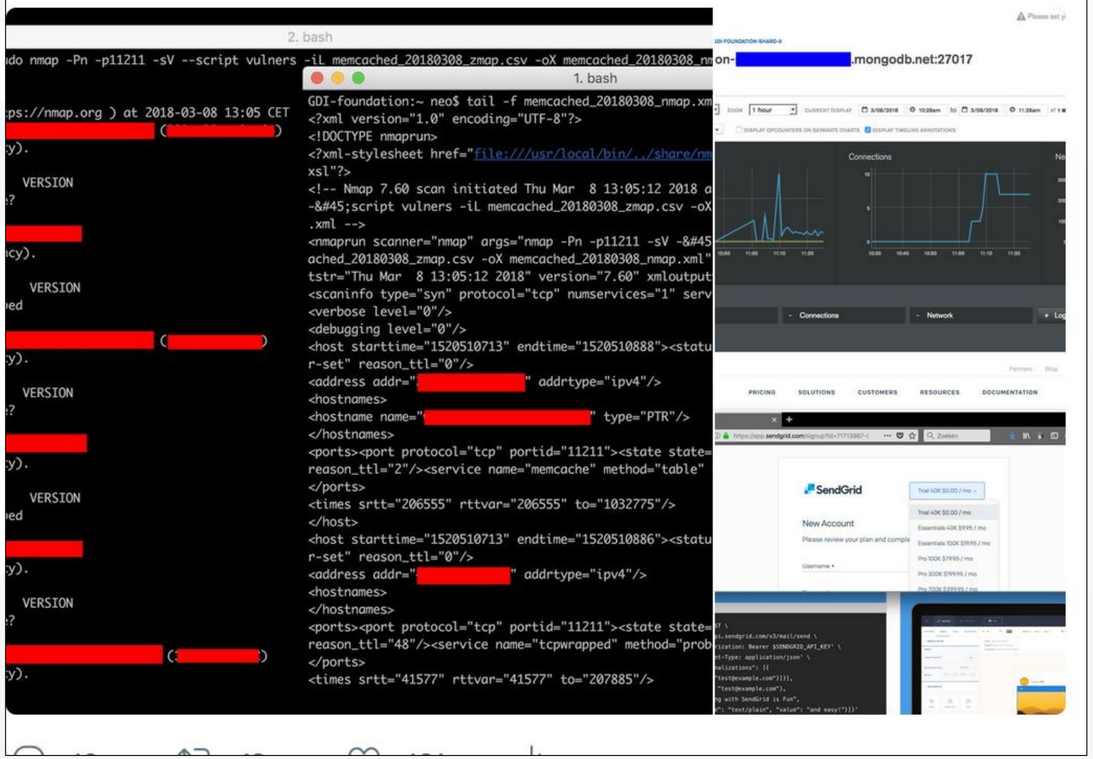
> **Victor Gevers** @0xDUDE
> Scanning & reporting vulnerable Memcached servers costs:
> Running ZMap scan for port 11211- $0
> Running Nmap scan on discovered hosts - $0
> Storing scans on MongoDB Atlas M0 cluster - $0…

Show this thread

7:05 PM - 8 Mar 2018

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



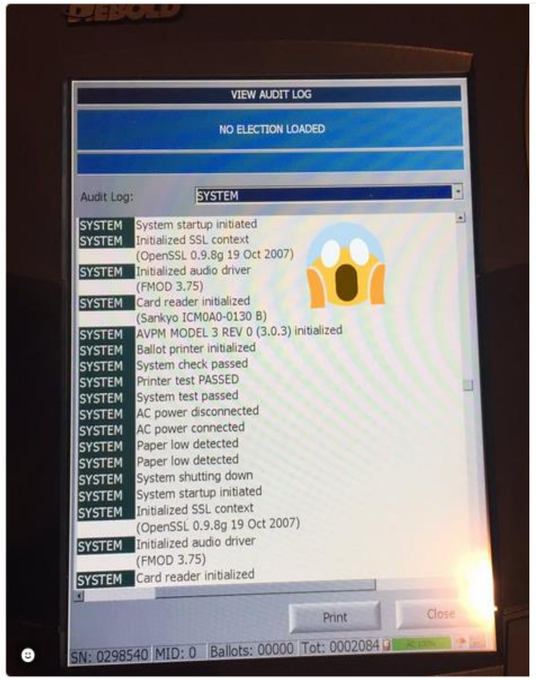
Digging in public password dumps

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 😟

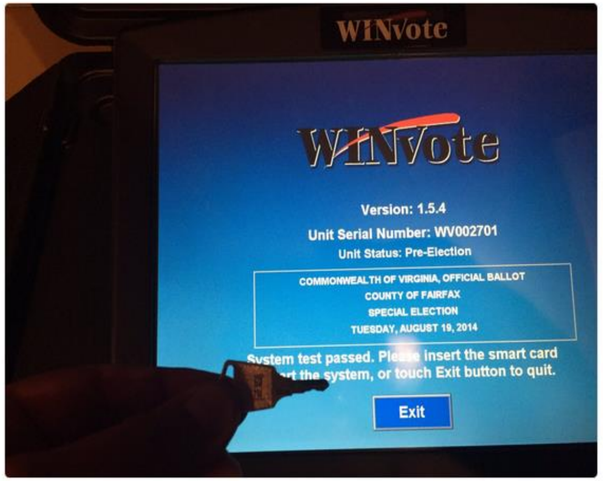


8:39 PM - 28 Jul 2017

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.

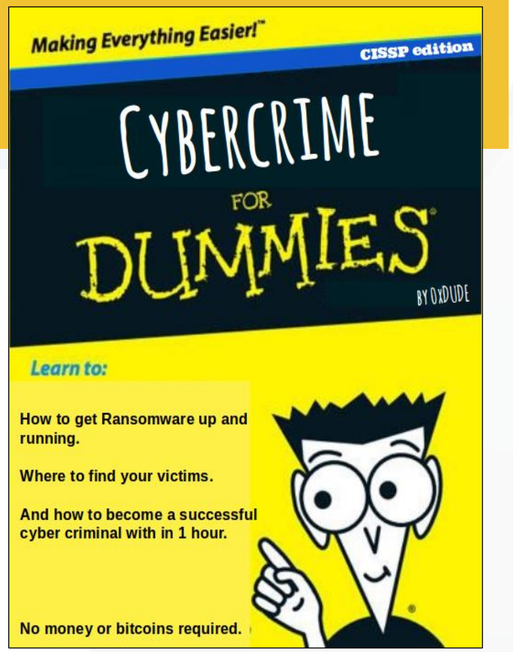
Dummies

Certified Cyber Criminal Professional

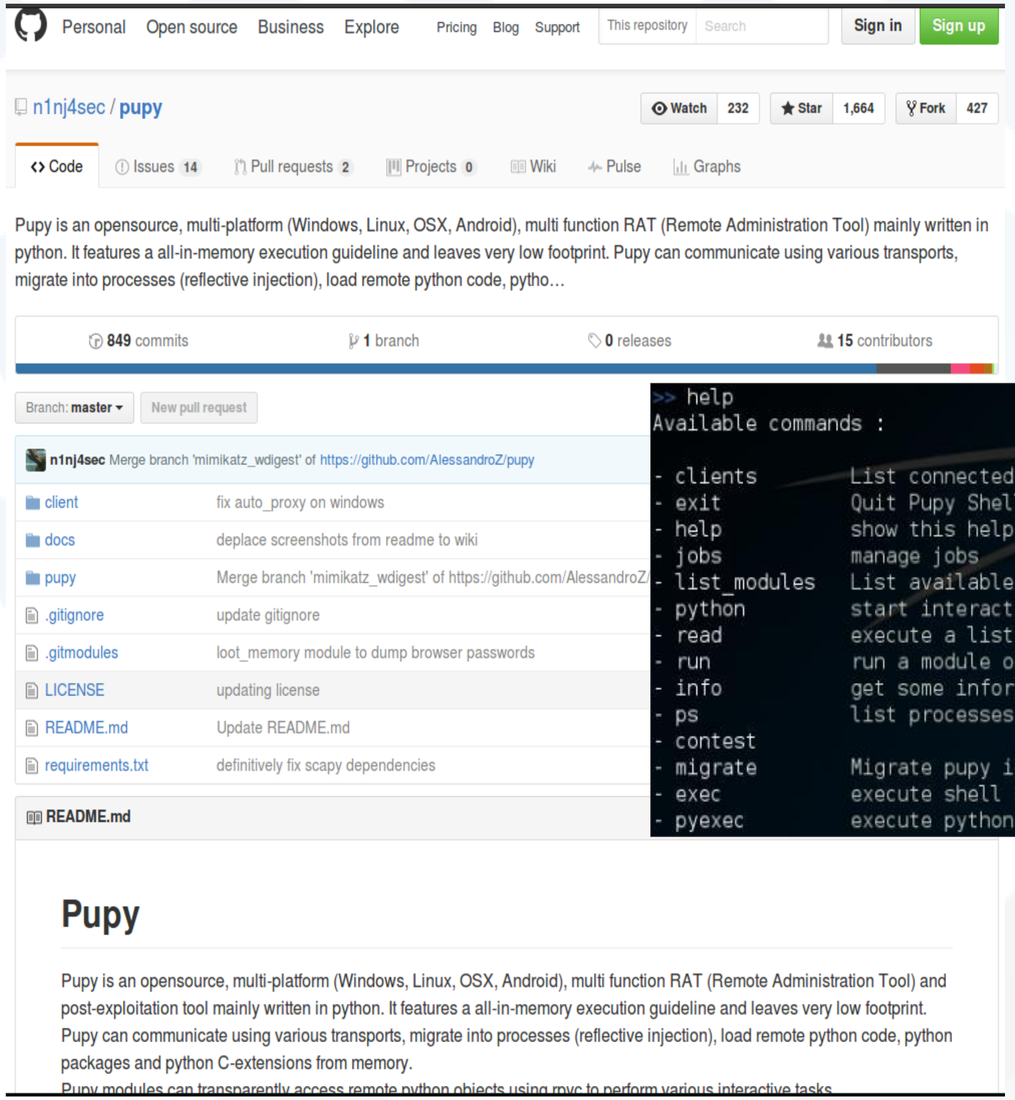
Your name after this presentation

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.

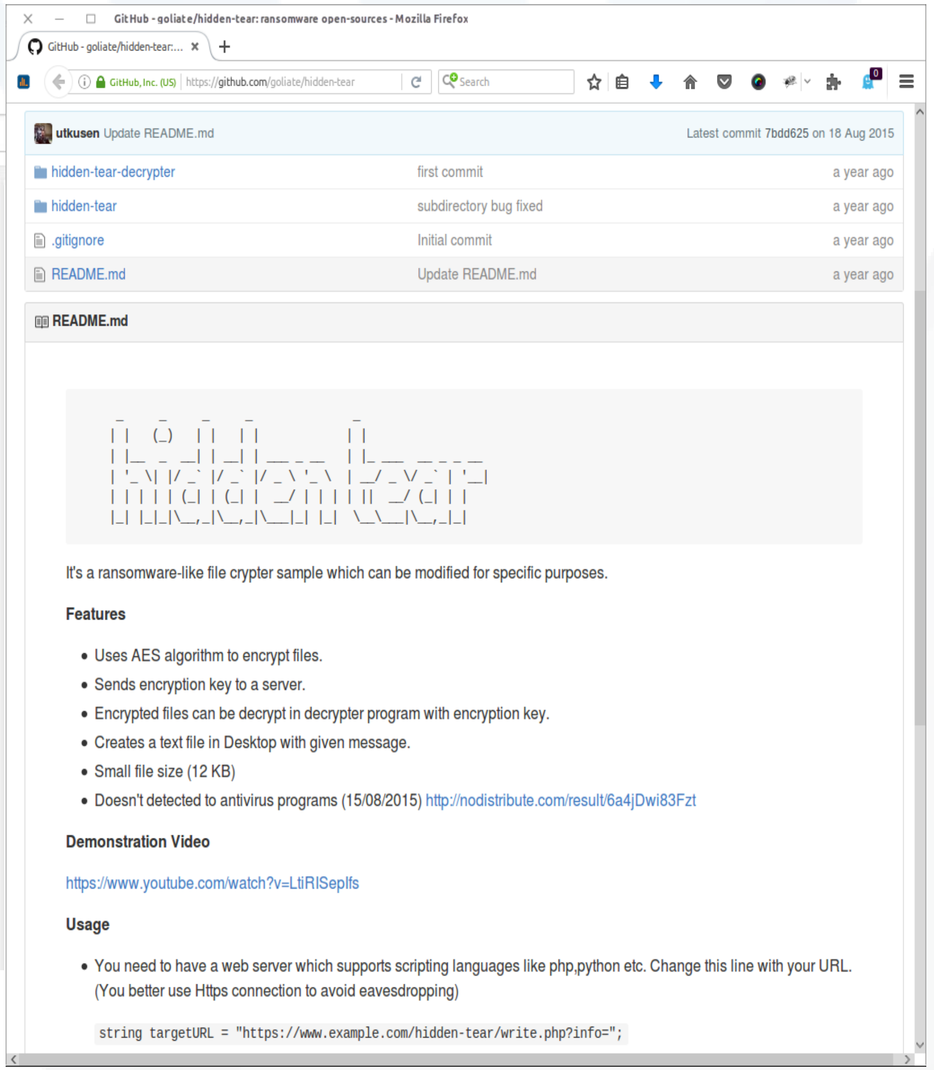


Dirty RAT

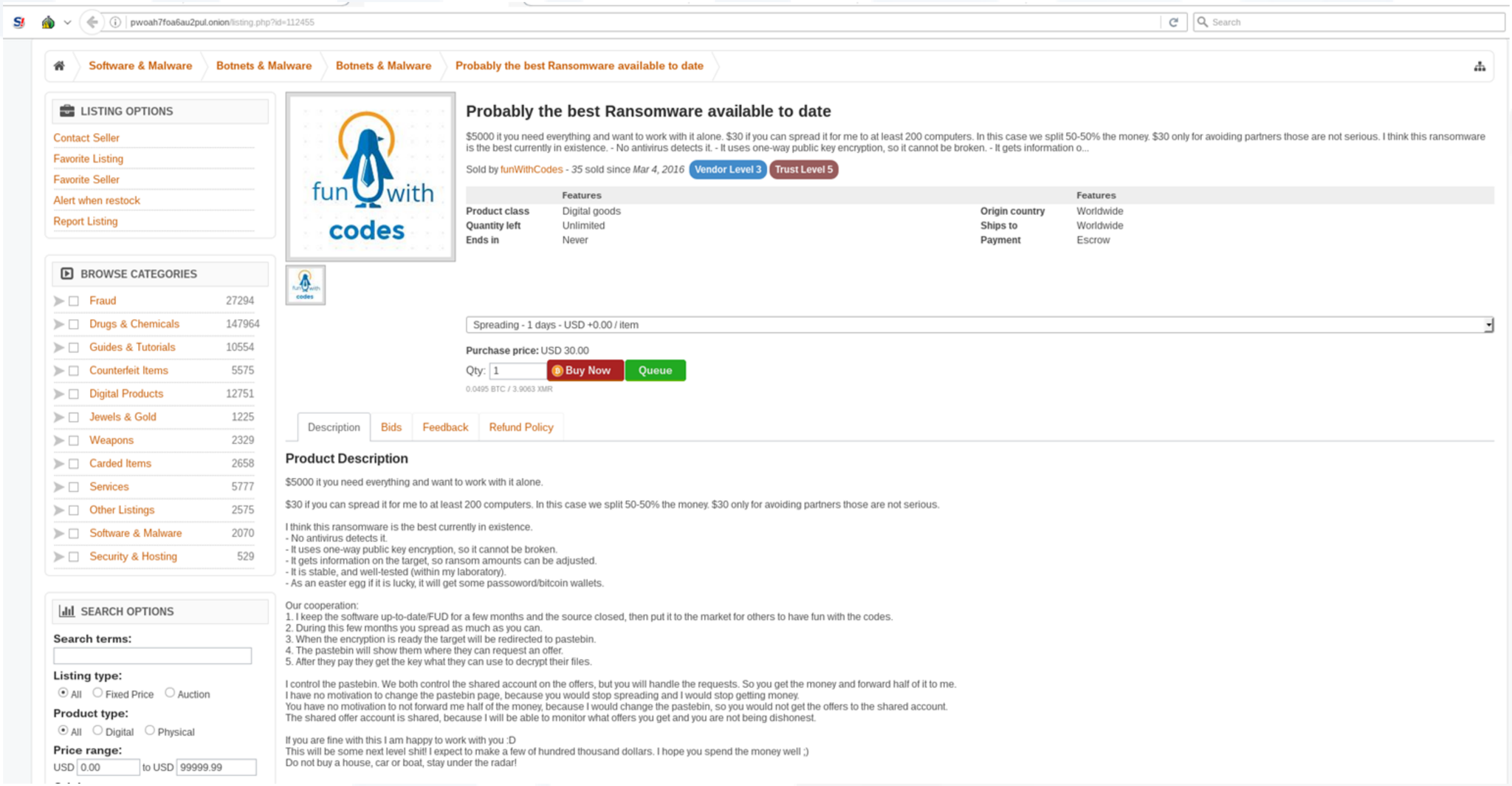



```
>> help
Available commands :

- 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        Migrate pupy into another process using reflective DLL injection
- exec           execute shell commands on a remote system
- pyexec         execute python code on a remote system
```

...



Ransomware as a Service



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...

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:

Bulk VNC Servers - Ideal for spreading/infecting with botnet/ransomware etc

Selling bulk VNC servers, minimum order 100 pcs =50$. For those of you who never dealt with these before, they are remote servers like RDP's, aprox 70% of them belong to different types of companies, ranging from small corner shops/ depots to multinational companies (insurers , supermarkets , online retailers etc). For 50$ 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		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

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

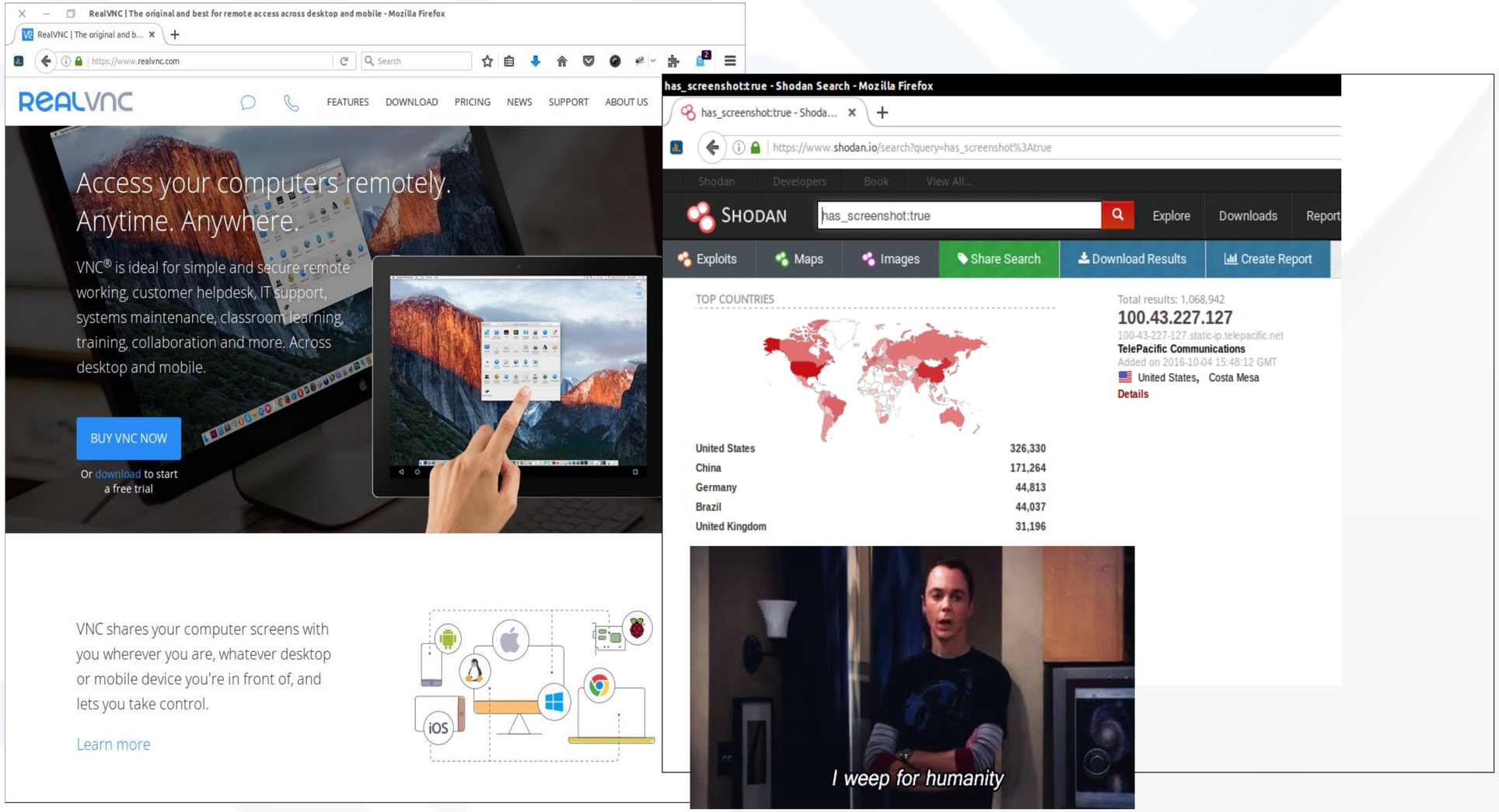
Description Bids Feedback Refund Policy

Product Description

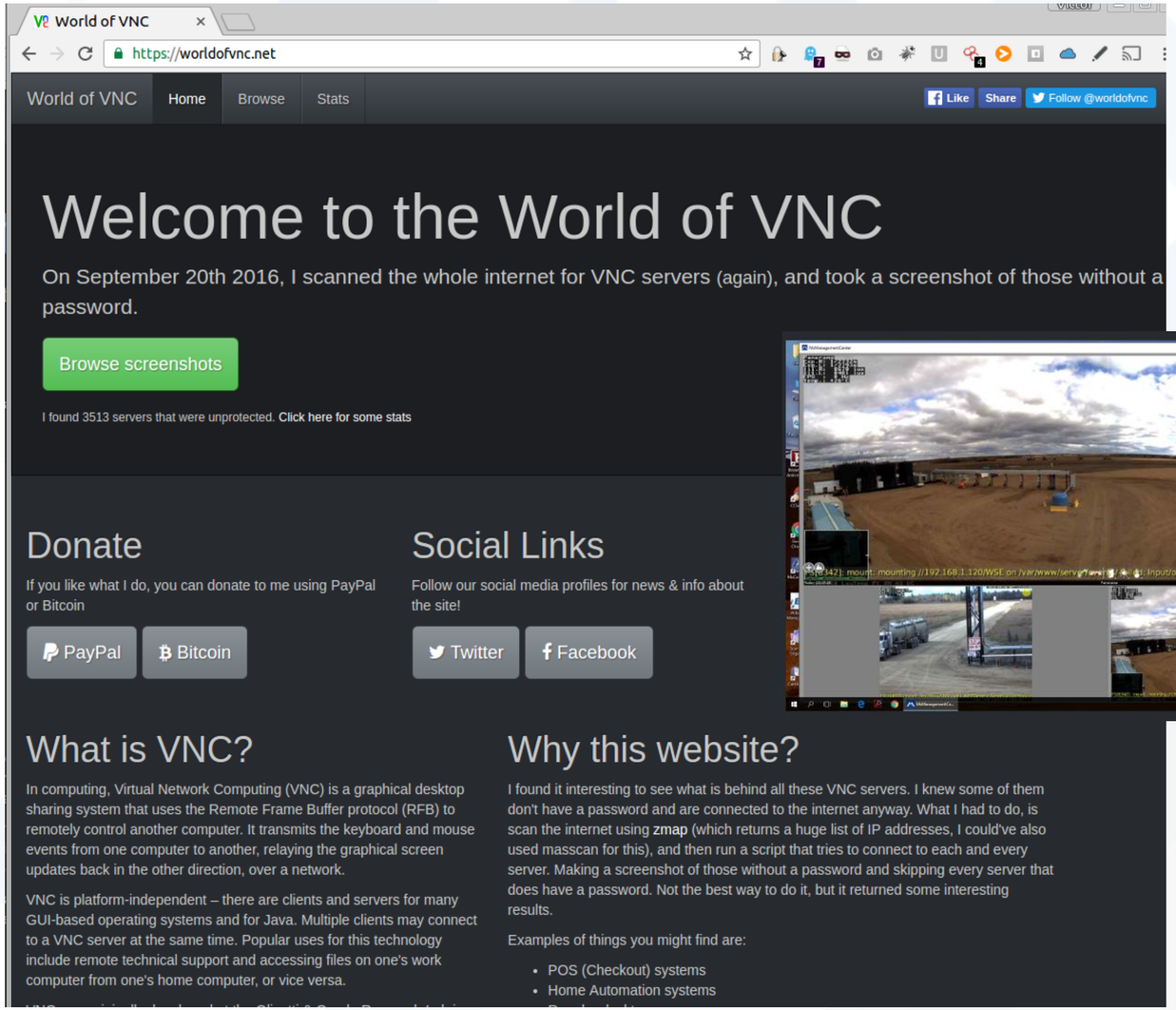
Selling bulk VNC servers, minimum order 100 pcs =50$. For those of you who never dealt with these before, they are remote ser... to multinational companies (insurers , supermarkets , online retailers etc). For 50$ you get access to 100 random pc's easily accessible using VNC viewer, t... Ideal for spreading your botnets/ransomwares/etc or even creating paypal/amazon/ebay/craigslist accts , plus you can get your h... For custom orders (specific countries) feel free to pm me, replacing only dead info.

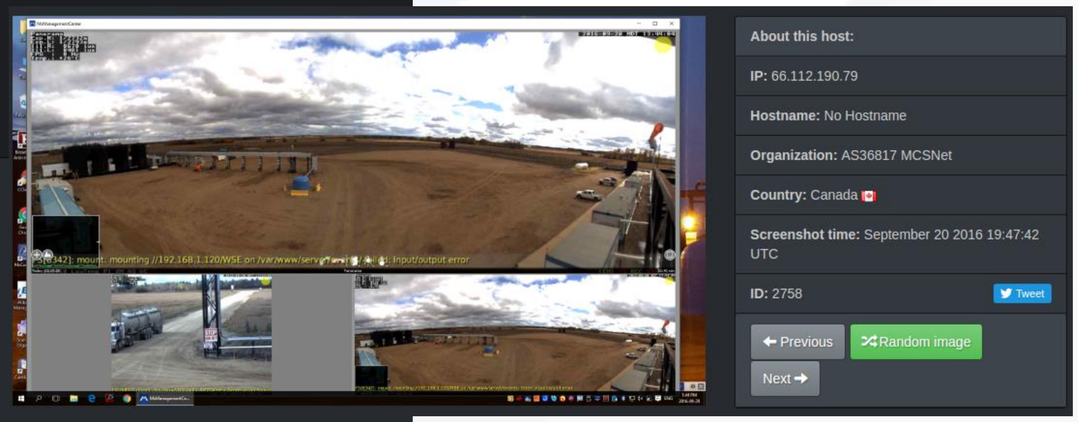
remote remote server vnc spread botnet ransomware

Open for your convenience

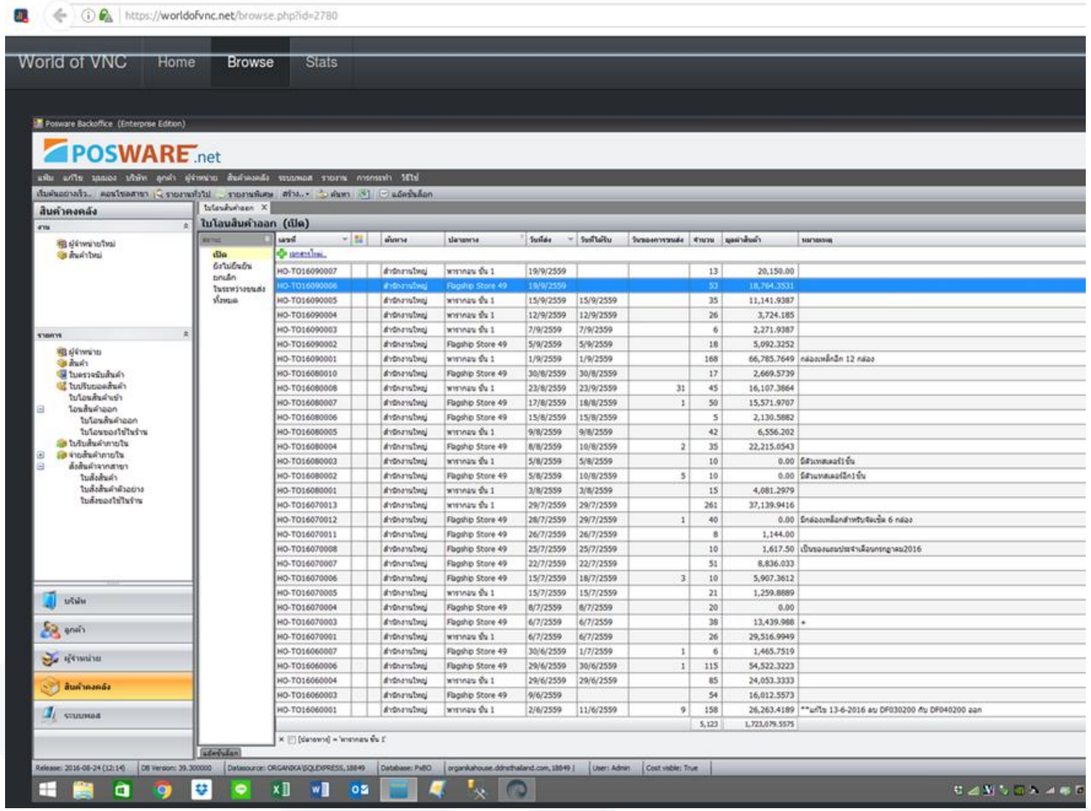


World of VNC

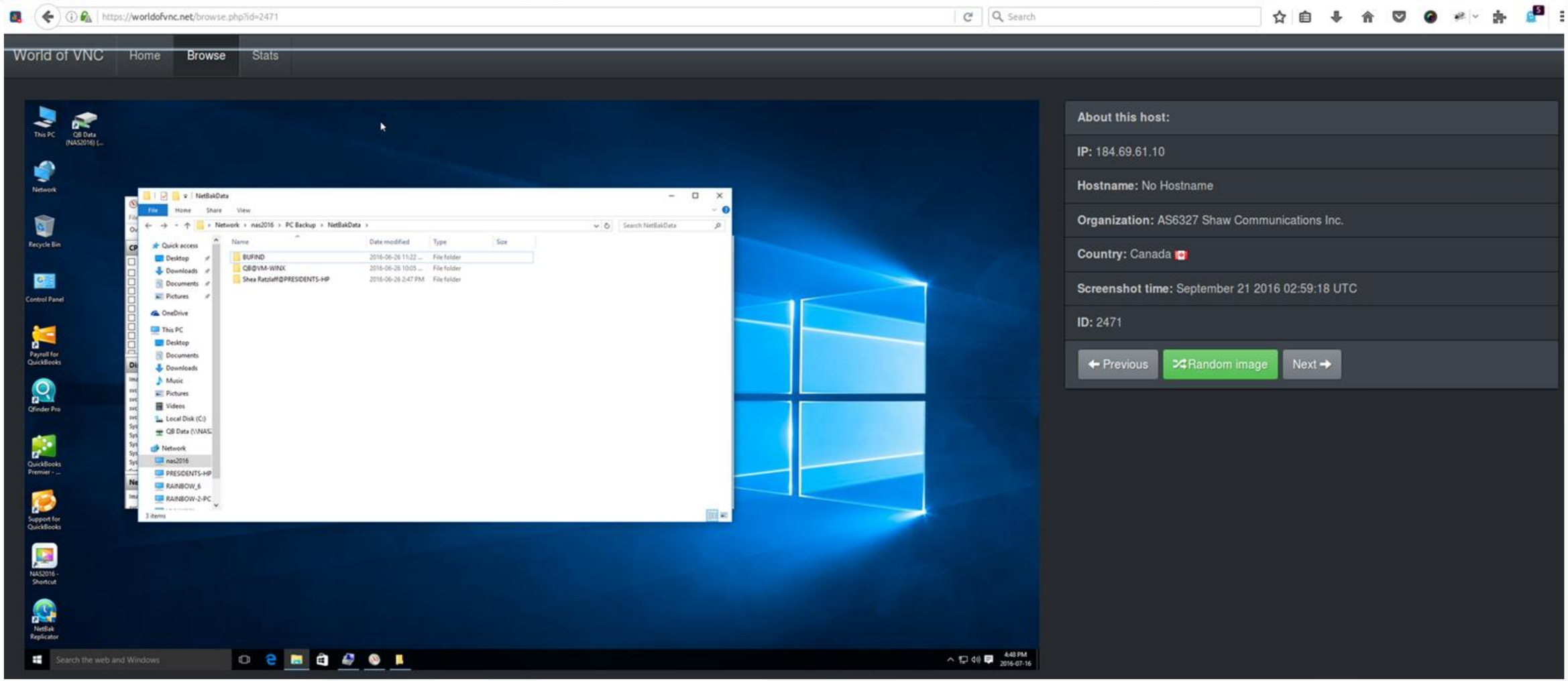




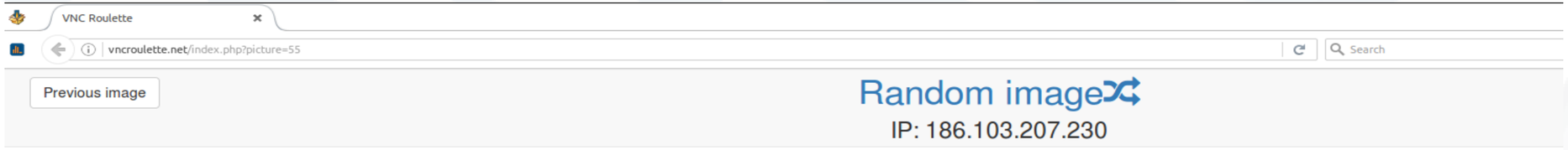
Point of Sale systems

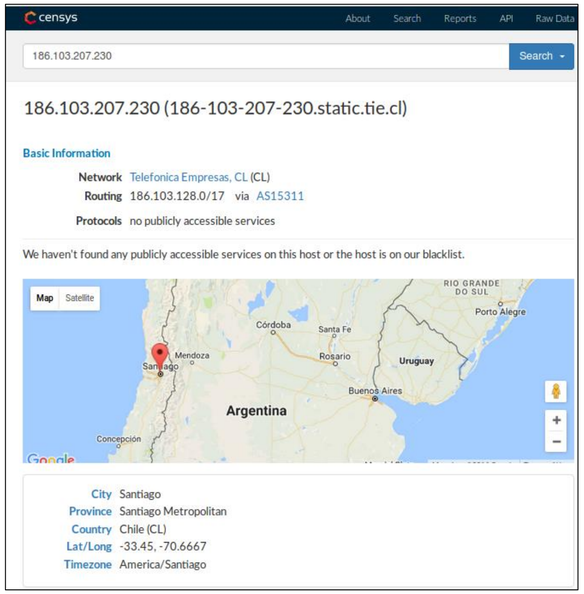


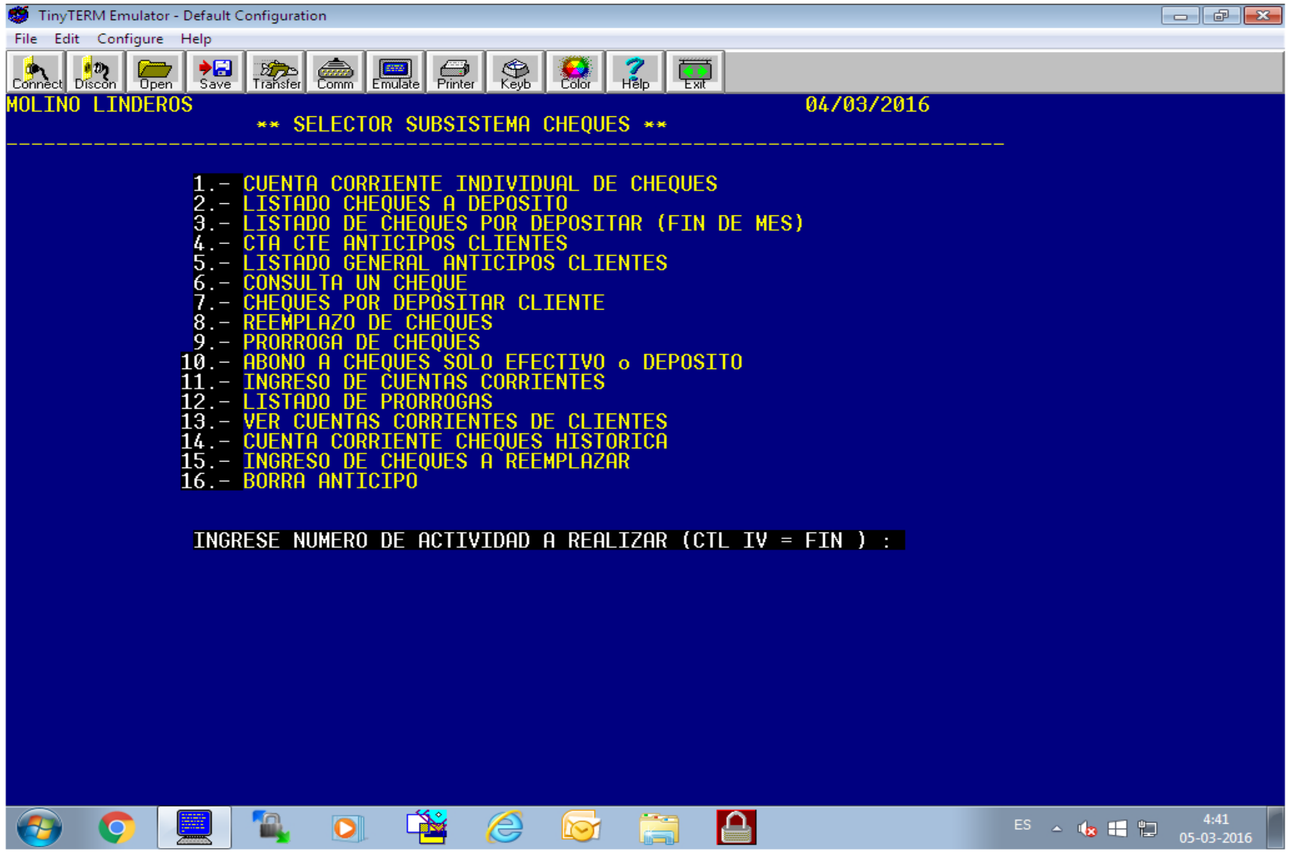
Windows 10



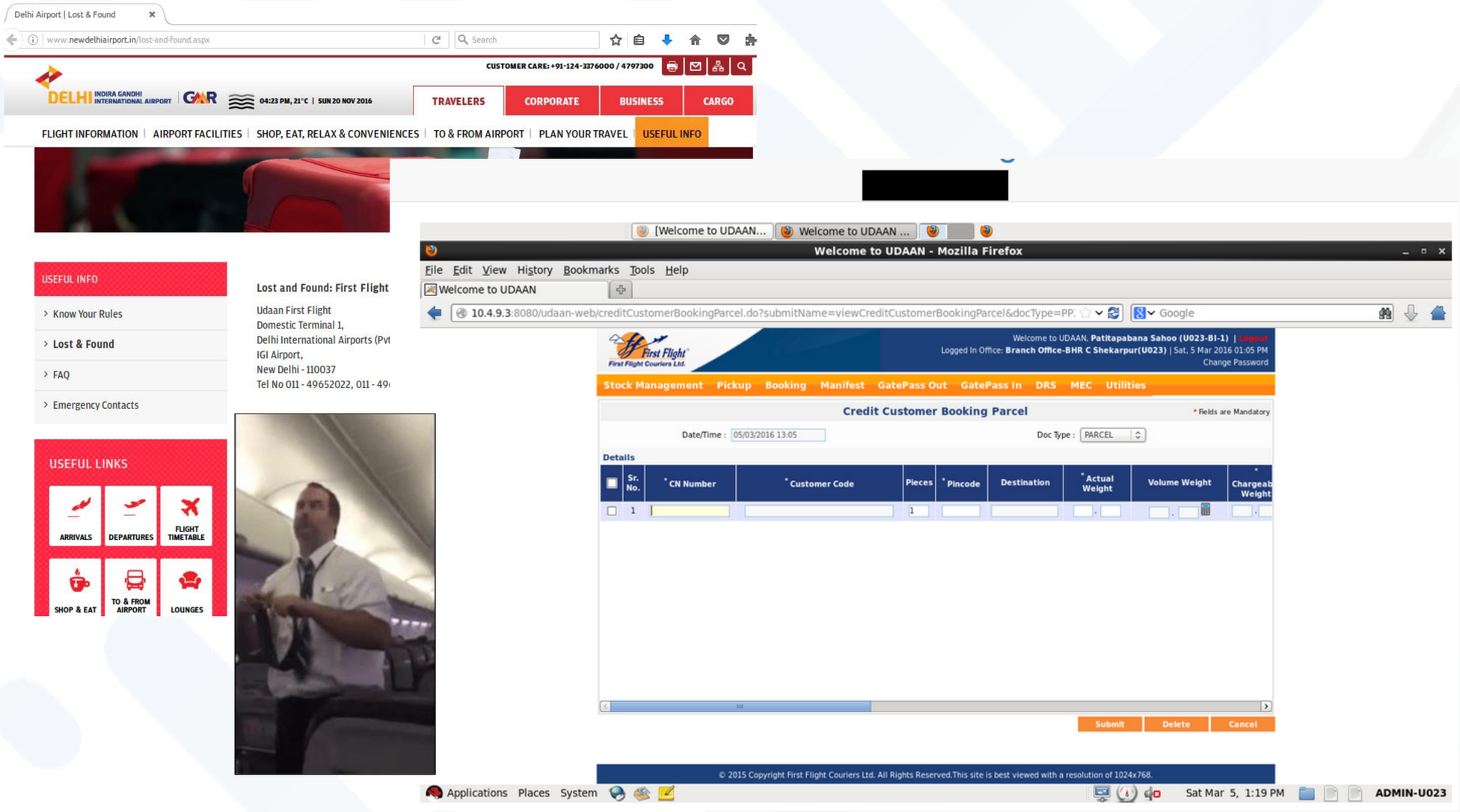
Banking systems







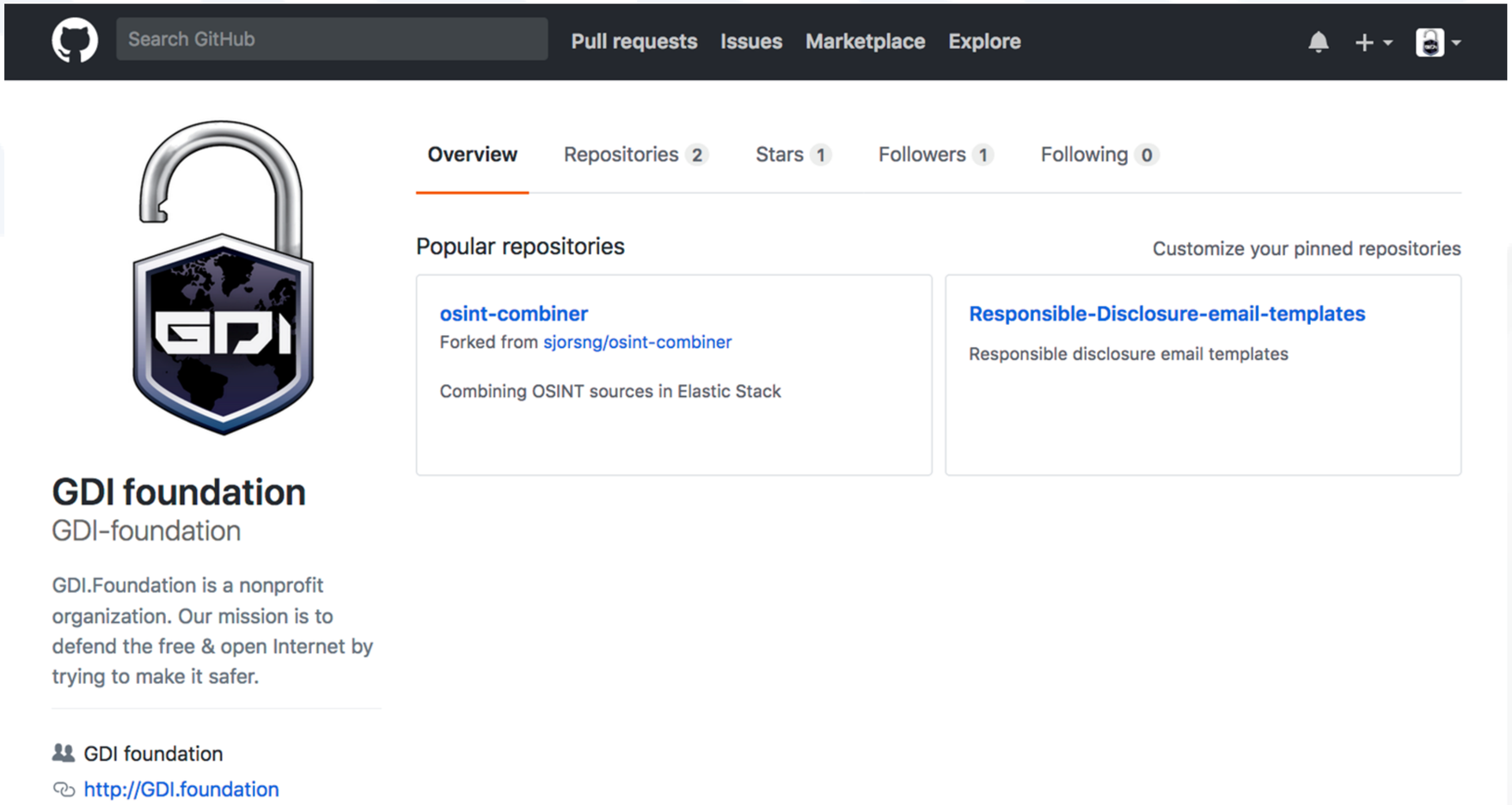
Airports




InfoSecWorld
Conference & Expo 2018

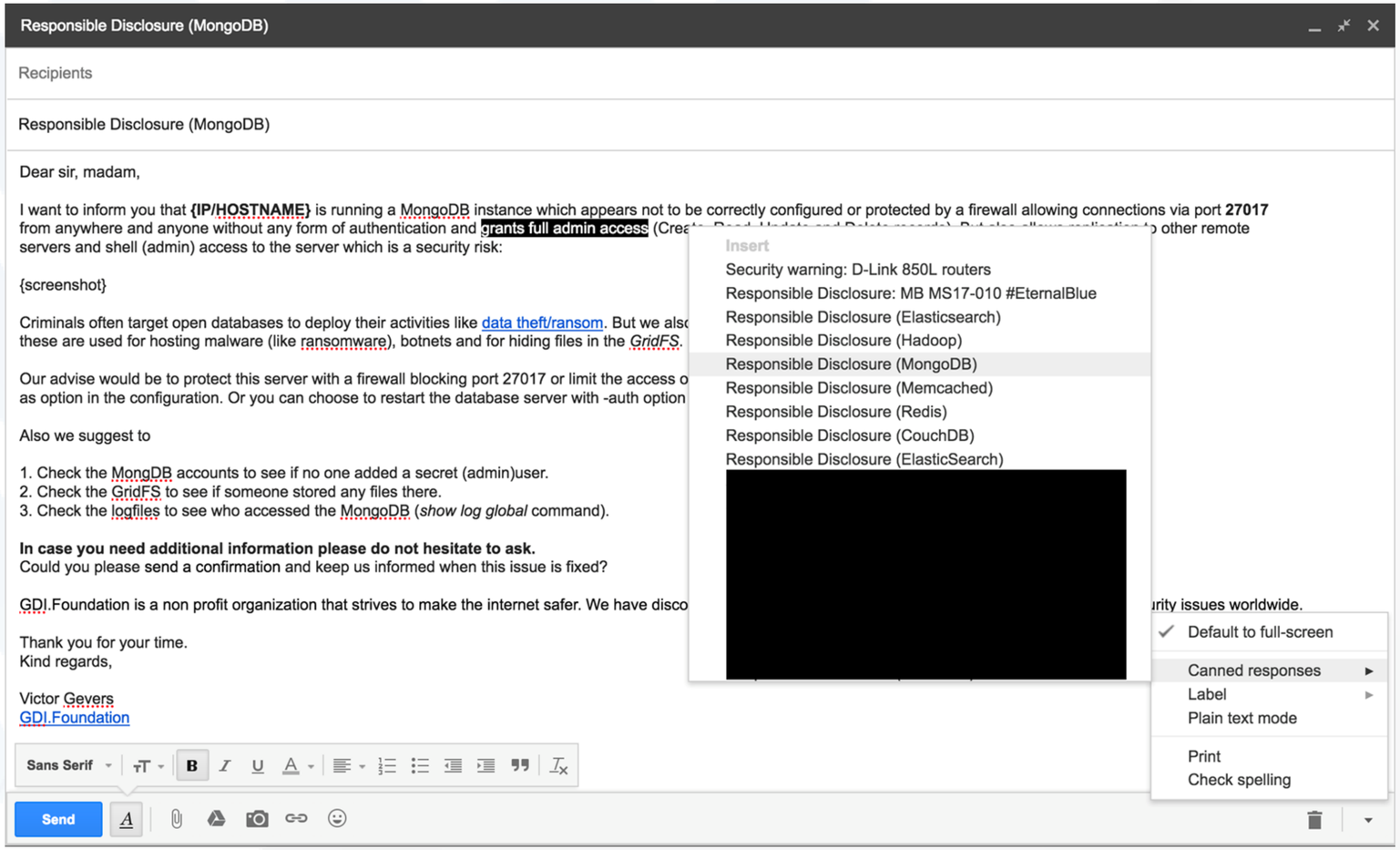
Success factors

- Communication is key



Success factors

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



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/BRA42k8T
- 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/admins/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 database _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 for or let a firewall block port 5984 to untrusted IPs.

Contact

Victor Gevers: victor@gdi.foundation / @0xDUDE
Niall Merrigan: niall@gdi.foundation / @nmerrigan
Matt Bromley: mbromley@gdi.foundation / @mbromleyDFIR
Dylan Katz: dylan@gdi.foundation / @Plazmaz1
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 System on port 50070.

The default web interface settings are

Security is off.
Safemode is off.

Block Pool ID:

Summary

Security is off.

Safemode 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

Elasticsearch generic security warning

Elasticsearch is a search engine based on Lucene. It provides a distributed, multitenant-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 a three weeks.

Indications of Compromise

- Public tracker: https://goo.gl/iVqfs
- IP Blacklist: http://pastebin.com/raw/ESEYfVFy
- Links: https://www.elastic.co/blog/found-elasticsearch-security

Advisory

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

1. Apply network filtering for 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, multitenant-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 a three weeks.

Indications of Compromise

- Public tracker: https://goo.gl/iVqfs
- IP Blacklist: http://pastebin.com/raw/ESEYfVFy
- Links: https://www.elastic.co/blog/found-elasticsearch-security

Advisory

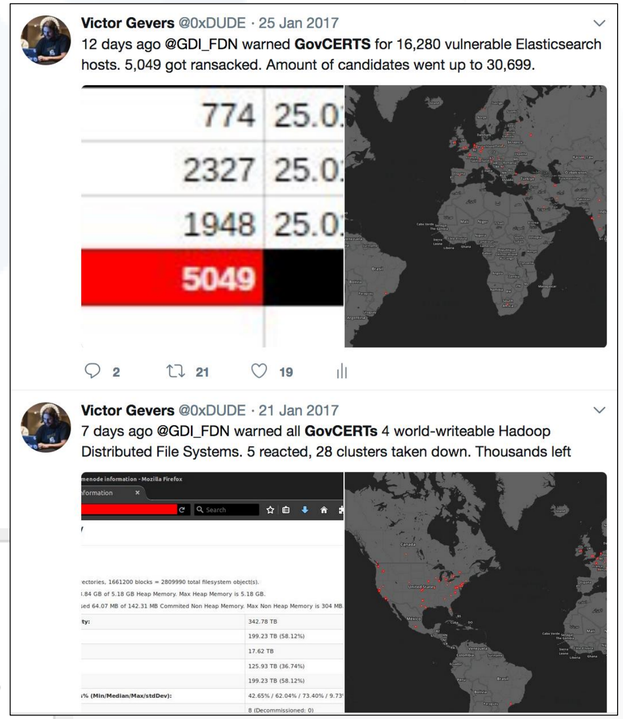
Please make sure you create frequently backups of data that you need to restore quickly.

1. Apply network filtering for 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



Success factors

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

state
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up
up

state
open
open
open
open
open
open
open
filtered
filtered
open
open
filtered
open
filtered
closed
open
open
filtered
open
filtered
filtered
closed
filtered
filtered
filtered
closed
filtered
filtered
filtered

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.

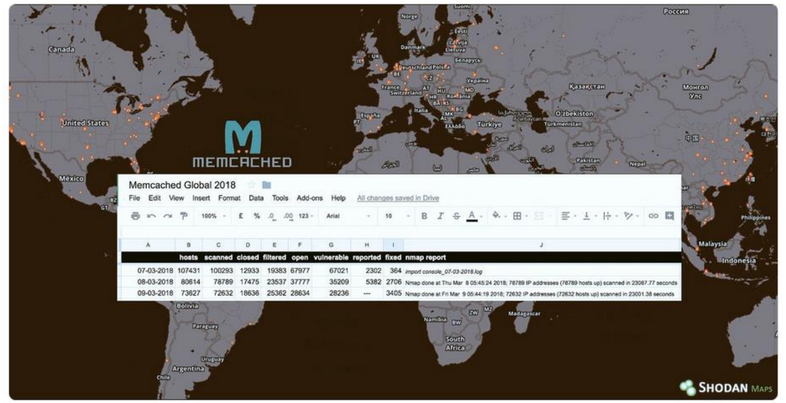
GDI Foundation @GDI_FDN · 17h

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



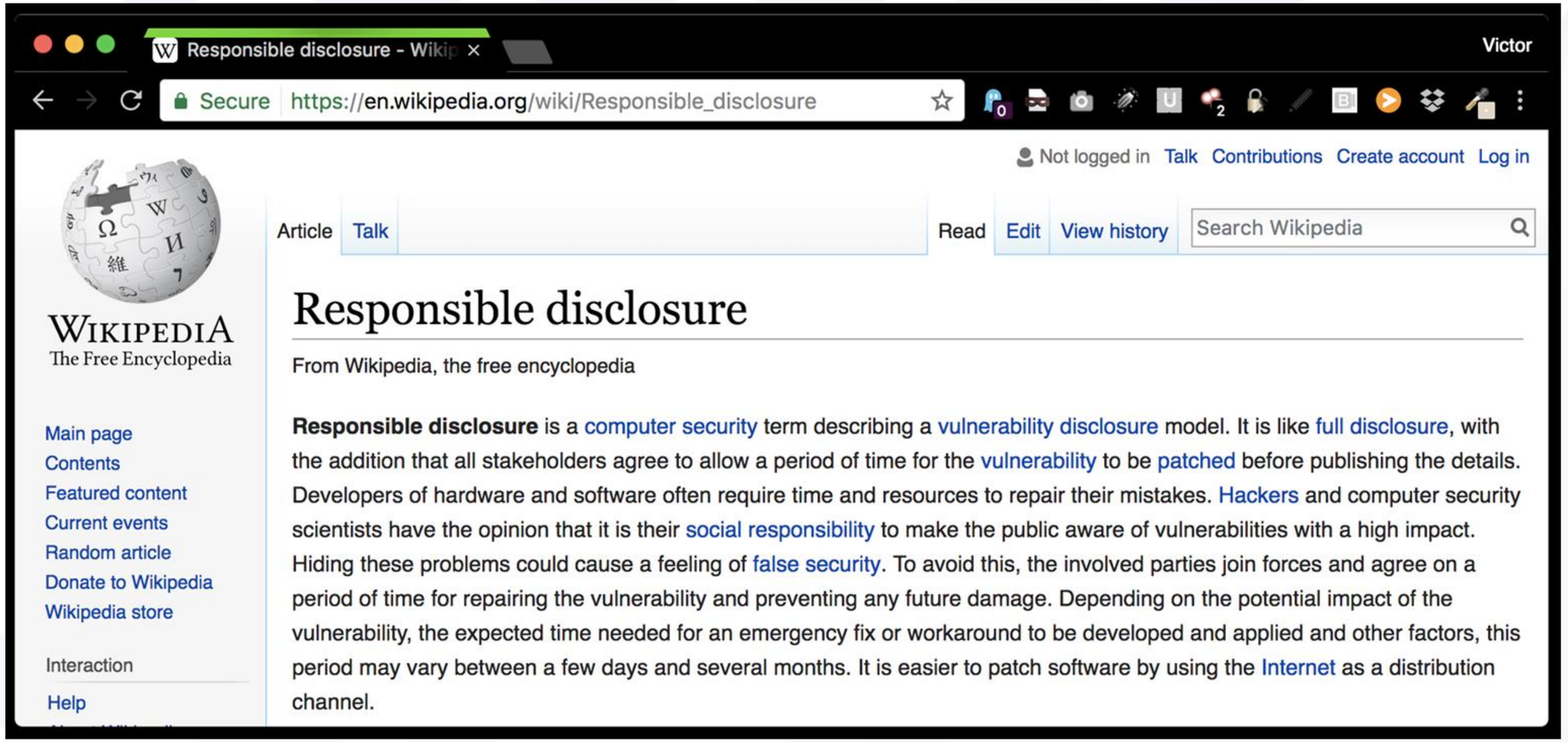
11:02 AM - 9 Mar 2018 from The Netherlands

Reporting vulnerable items

- Responsible Disclosures / CVD

Reporting vulnerable items

- Responsible Disclosures / CVD

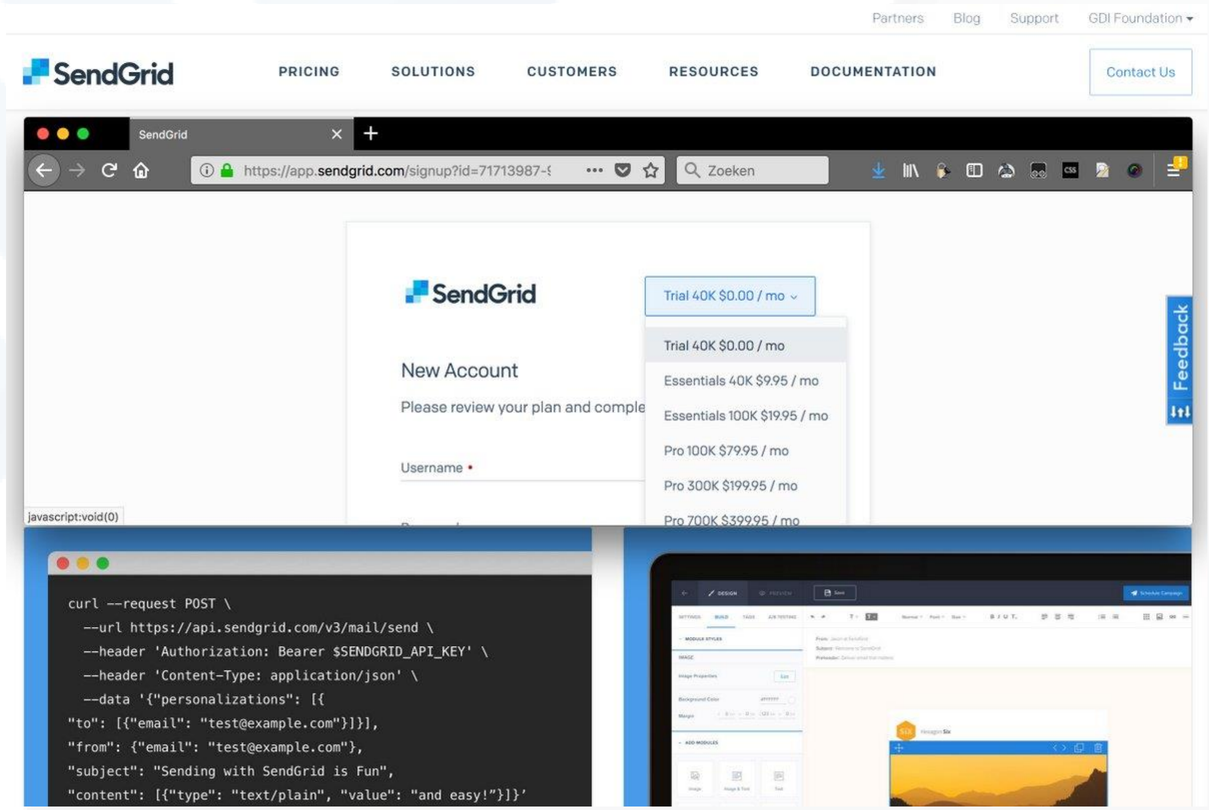


Reporting vulnerable items

- Responsible Disclosures / CVD

Reporting vulnerable items

- Responsible Disclosures / CVD
- Bulk reporting




InfoSecWorld
Conference & Expo 2018

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 **1LEiPgvh6$9VEXWV2dZTytSRd7e9B1bWt3**. 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://3hnuhydu4pd247qb.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 the 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 we 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 is it, 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.

Full list of encrypted files

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
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
READ ON ANY DEVICE
› Get free Kindle app
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 t
discovers a flaw is not necessaril
cyber security. He or she immedi
well-coordinated approach allows
Read more
Length: 247 pages
Age Level: 12 - 18
Summer Kindle Monthly Deals
Up to 80% off 1,000+ Kindle books
› Browse now
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

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Victor Gevers

Chairman GDI.foundation

@GDI_fdn