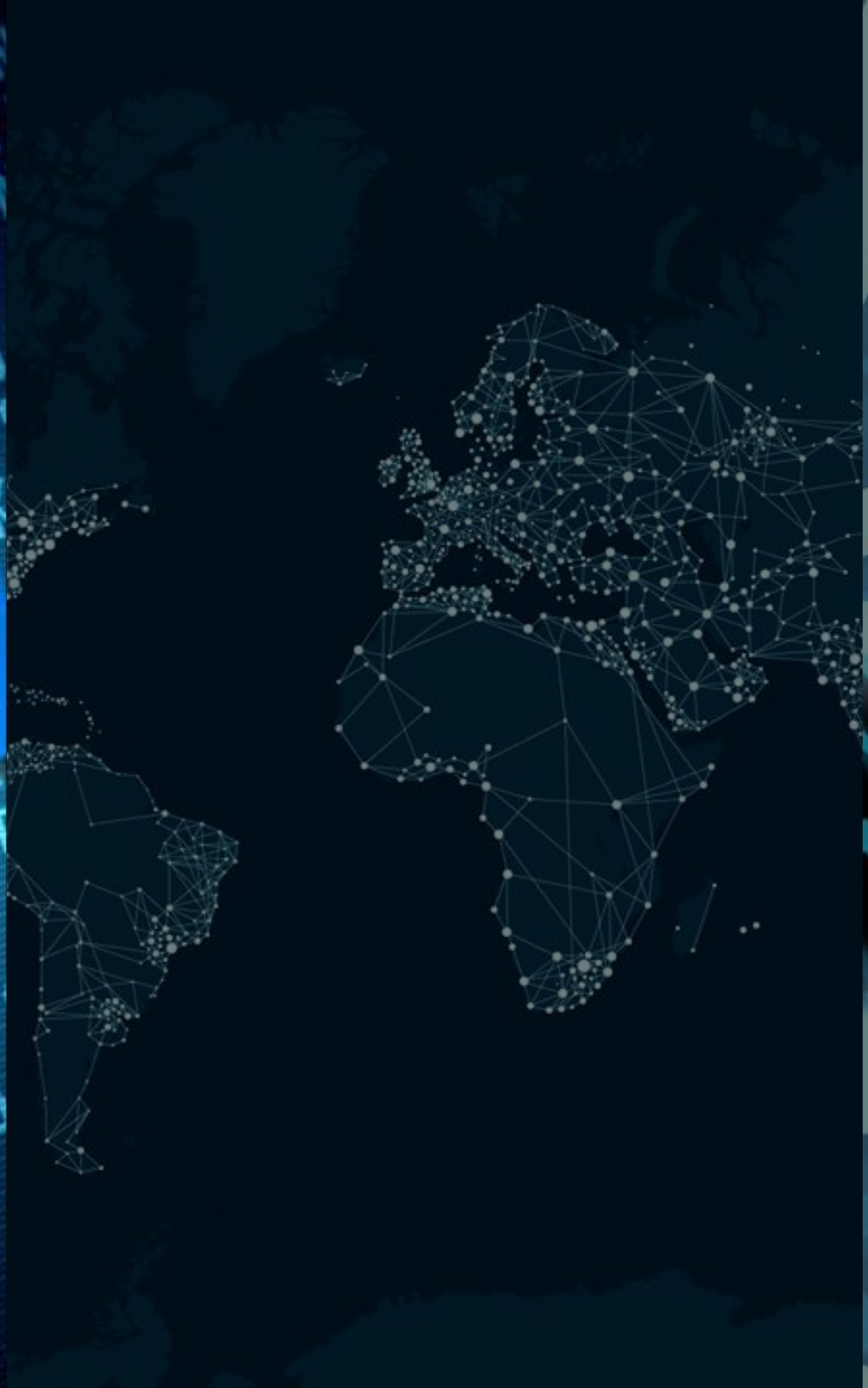
THREAT TRENDS OF 2017

F-Secure

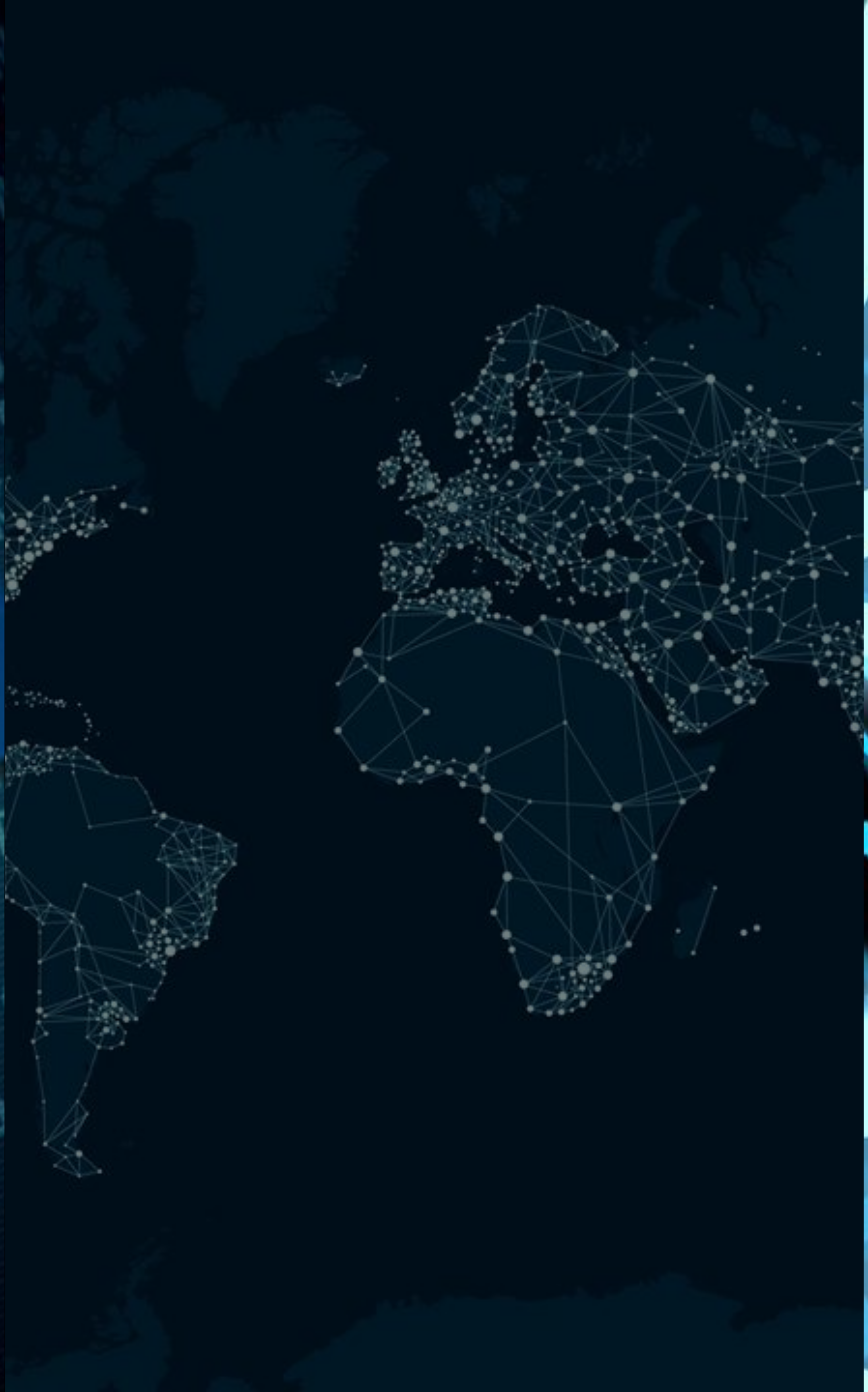
UPDATE
loading
86%

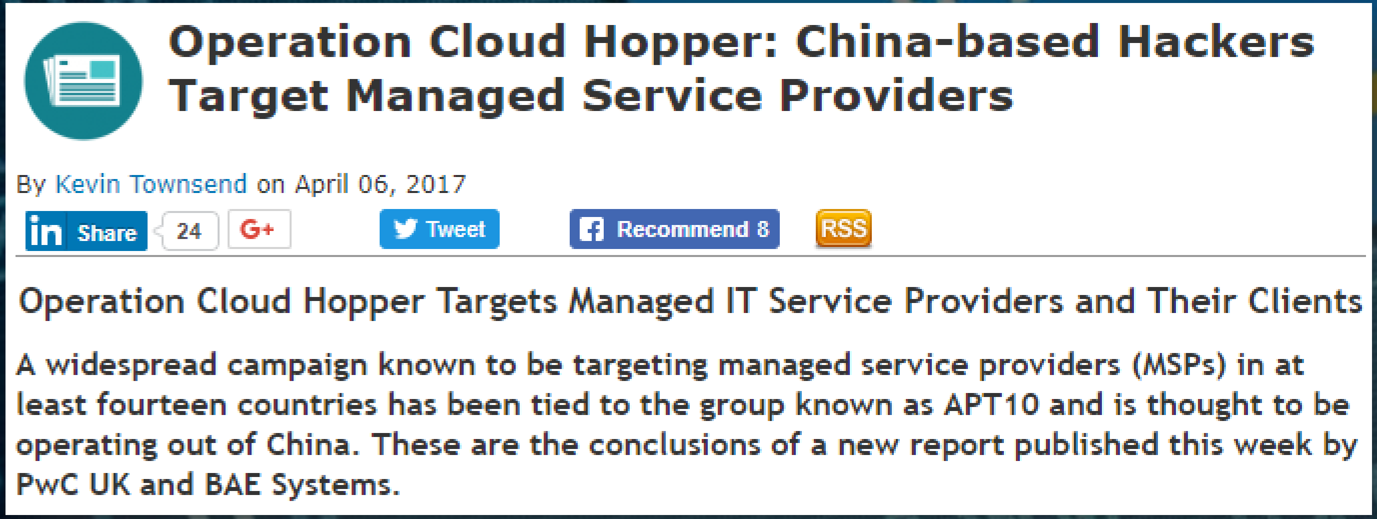
UPDATE
loading
86%



UPDATE
loading
86%

UPDATE
loading
86%





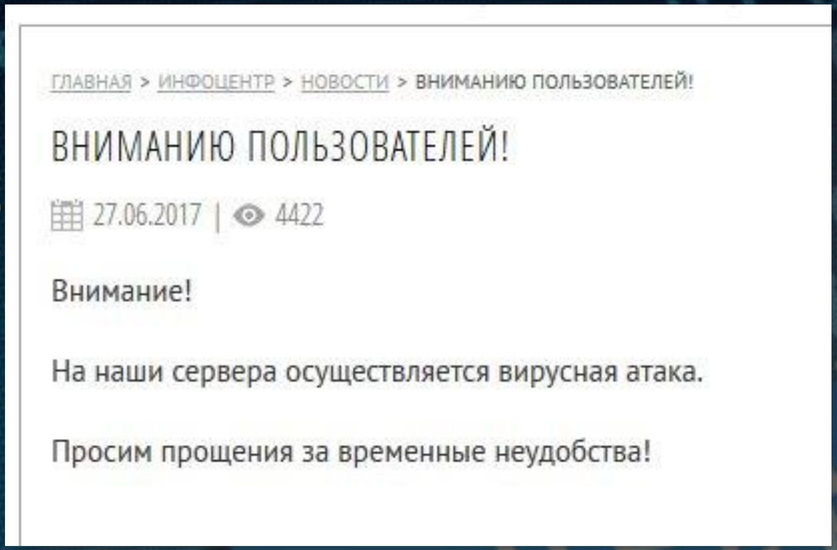
Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

By Kevin Townsend on April 06, 2017

Operation Cloud Hopper Targets Managed IT Service Providers and Their Clients

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.

me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ



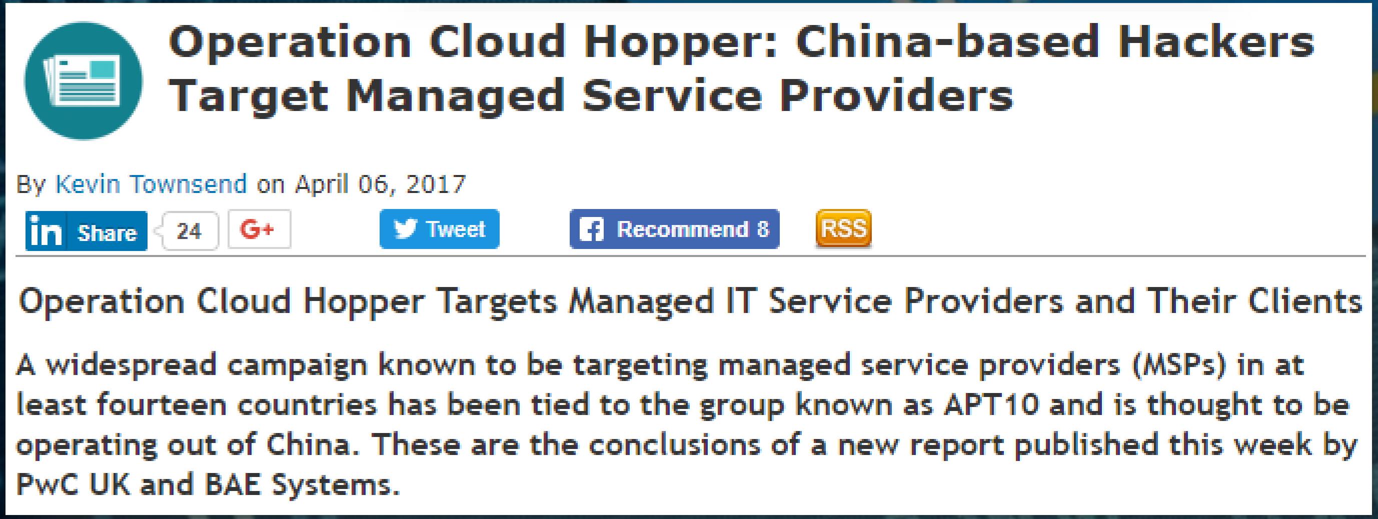
ВНИМАНИЮ ПОЛЬЗОВАТЕЛЕЙ!

27.06.2017 | 4422

Внимание!

На наши сервера осуществляется вирусная атака.

Просим прощения за временные неудобства!



Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

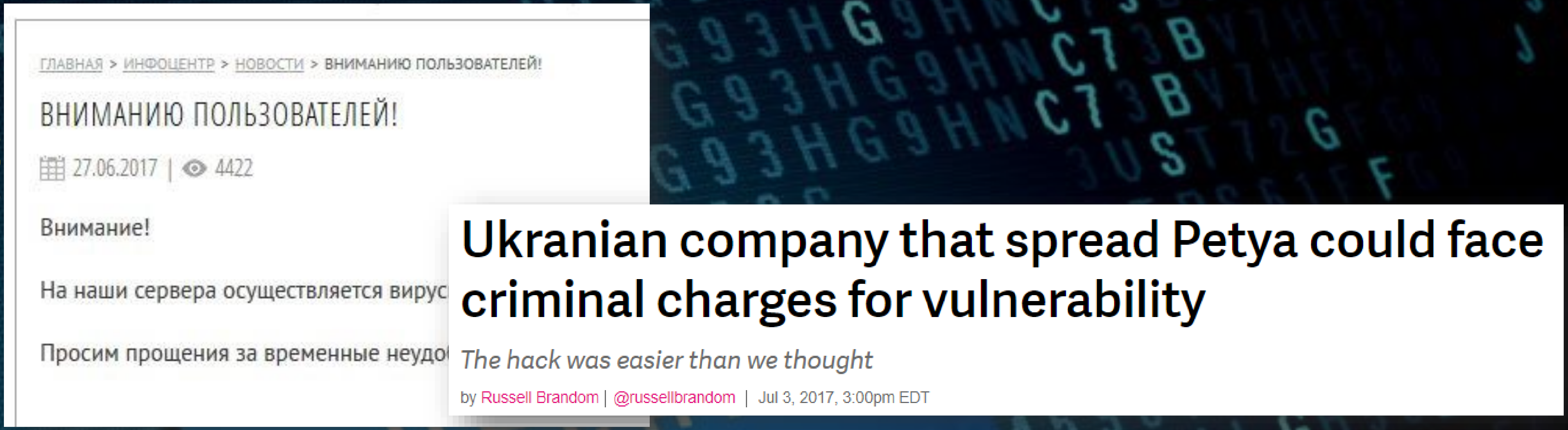
By Kevin Townsend on April 06, 2017

Operation Cloud Hopper Targets Managed IT Service Providers and Their Clients

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.

me doc

МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ



ГЛАВНАЯ > ИНФОЦЕНТР > НОВОСТИ > ВНИМАНИЮ ПОЛЬЗОВАТЕЛЕЙ!

ВНИМАНИЮ ПОЛЬЗОВАТЕЛЕЙ!

27.06.2017 | 4422

Внимание!

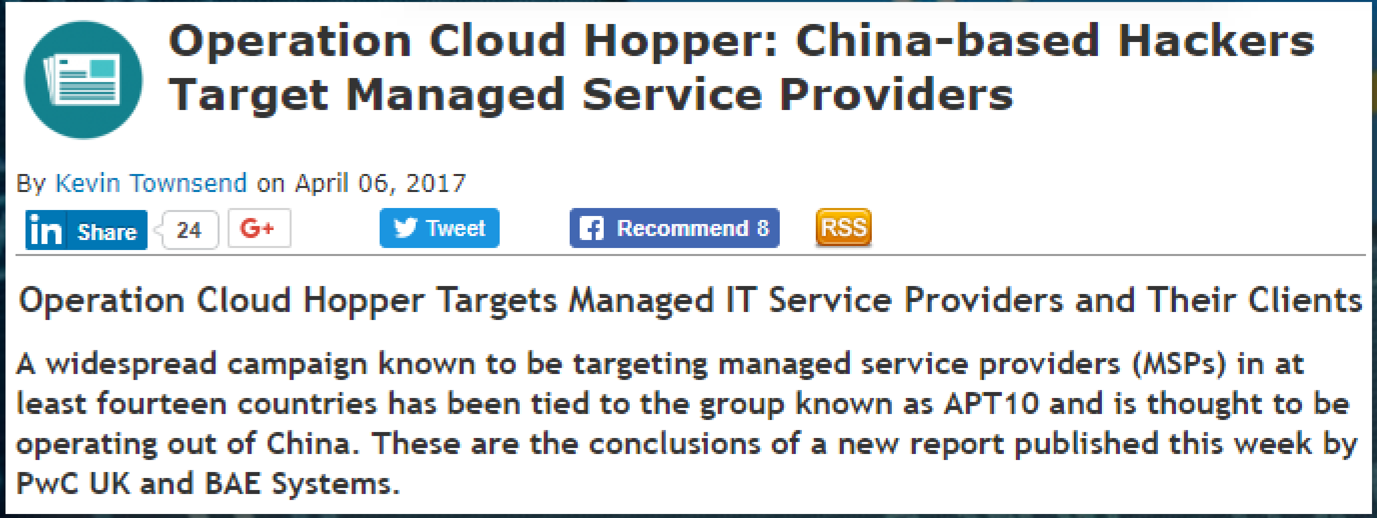
На наши сервера осуществляется вирус

Просим прощения за временные неудо

Ukranian company that spread Petya could face criminal charges for vulnerability

The hack was easier than we thought

by Russell Brandom | @russellbrandom | Jul 3, 2017, 3:00pm EDT



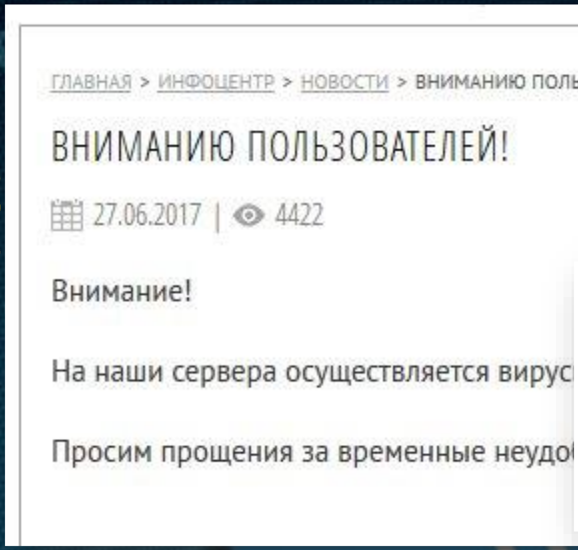
Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

By Kevin Townsend on April 06, 2017

Operation Cloud Hopper Targets Managed IT Service Providers and Their Clients

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.

me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ



ГЛАВНАЯ > ИНФОЦЕНТР > НОВОСТИ > ВНИМАНИЮ ПОЛЬЗОВАТЕЛЕЙ!

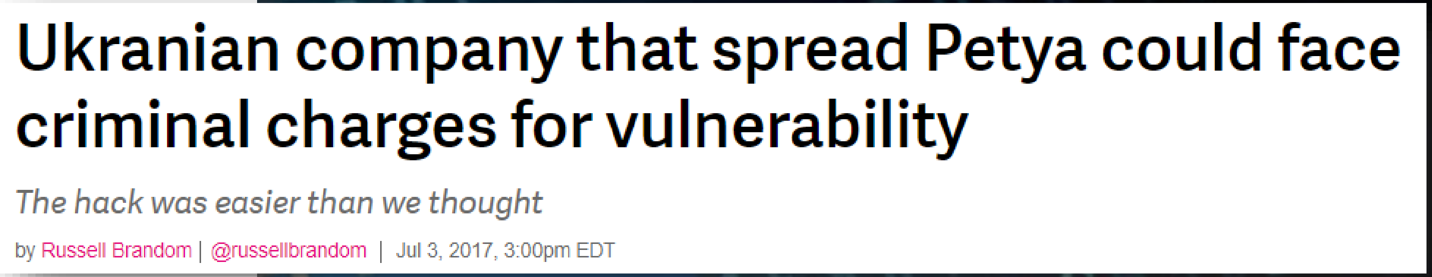
ВНИМАНИЮ ПОЛЬЗОВАТЕЛЕЙ!

27.06.2017 | 4422

Внимание!

На наши сервера осуществляется вирус

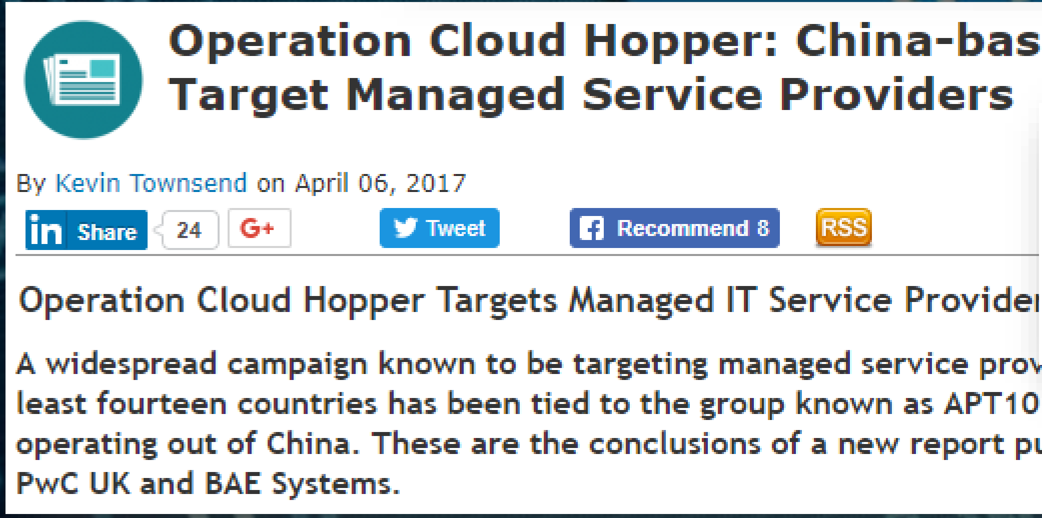
Просим прощения за временные неудо



Ukranian company that spread Petya could face criminal charges for vulnerability

The hack was easier than we thought

by Russell Brandom | @russellbrandom | Jul 3, 2017, 3:00pm EDT

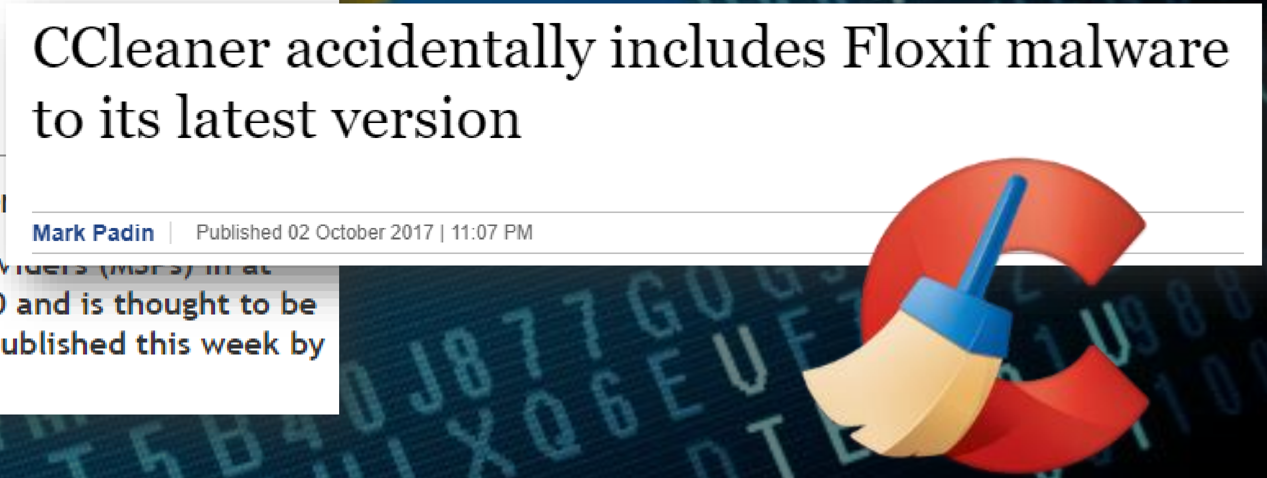


Operation Cloud Hopper: China-based Hackers Target Managed Service Providers

By Kevin Townsend on April 06, 2017

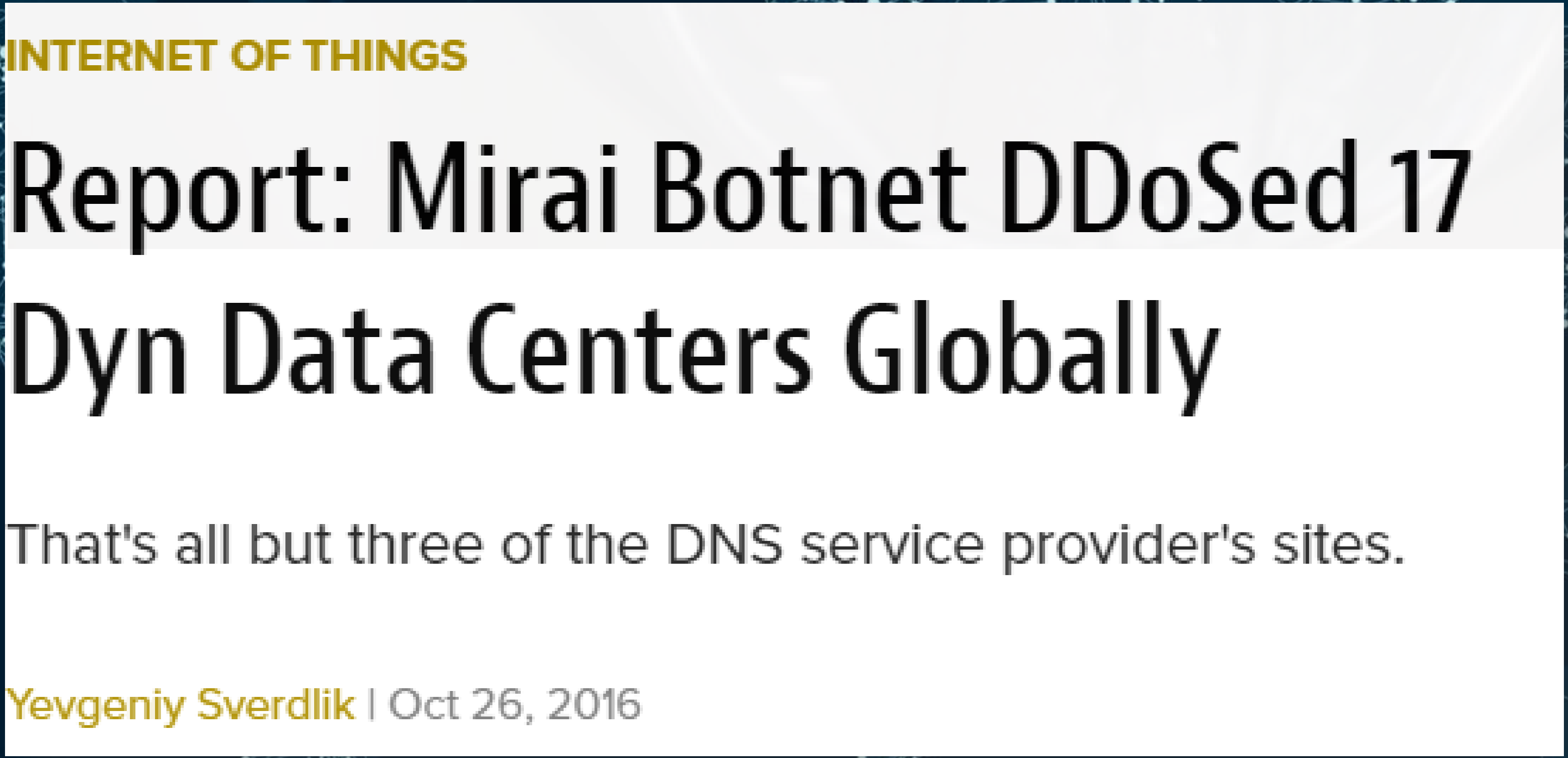
Operation Cloud Hopper Targets Managed IT Service Provider

A widespread campaign known to be targeting managed service providers (MSPs) in at least fourteen countries has been tied to the group known as APT10 and is thought to be operating out of China. These are the conclusions of a new report published this week by PwC UK and BAE Systems.



CCleaner accidentally includes Floxif malware to its latest version

Mark Padin | Published 02 October 2017 | 11:07 PM

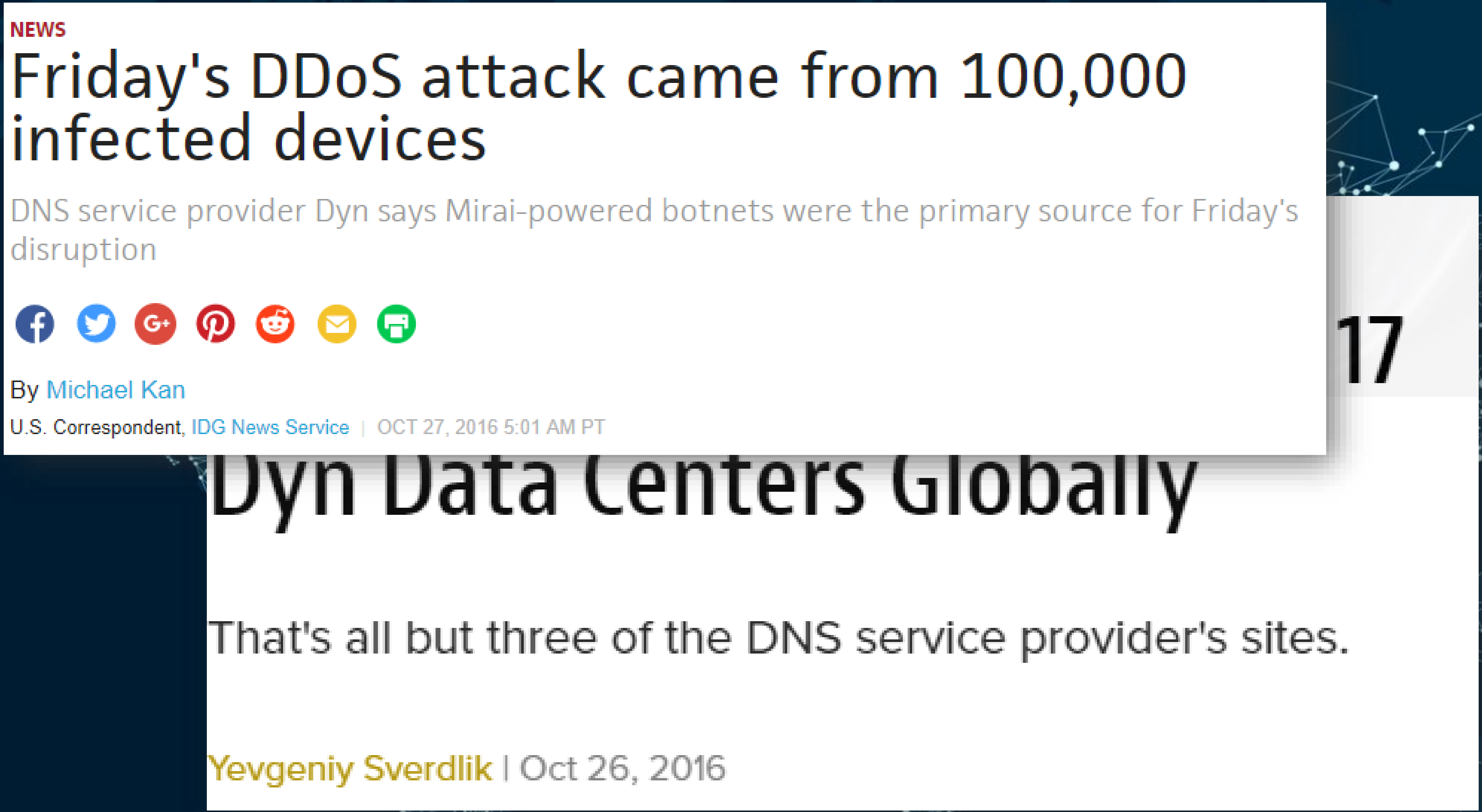


INTERNET OF THINGS

Report: Mirai Botnet DDoSed 17 Dyn Data Centers Globally

That's all but three of the DNS service provider's sites.

Yevgeniy Sverdlik | Oct 26, 2016



NEWS

Friday's DDoS attack came from 100,000 infected devices

DNS service provider Dyn says Mirai-powered botnets were the primary source for Friday's disruption

By Michael Kan

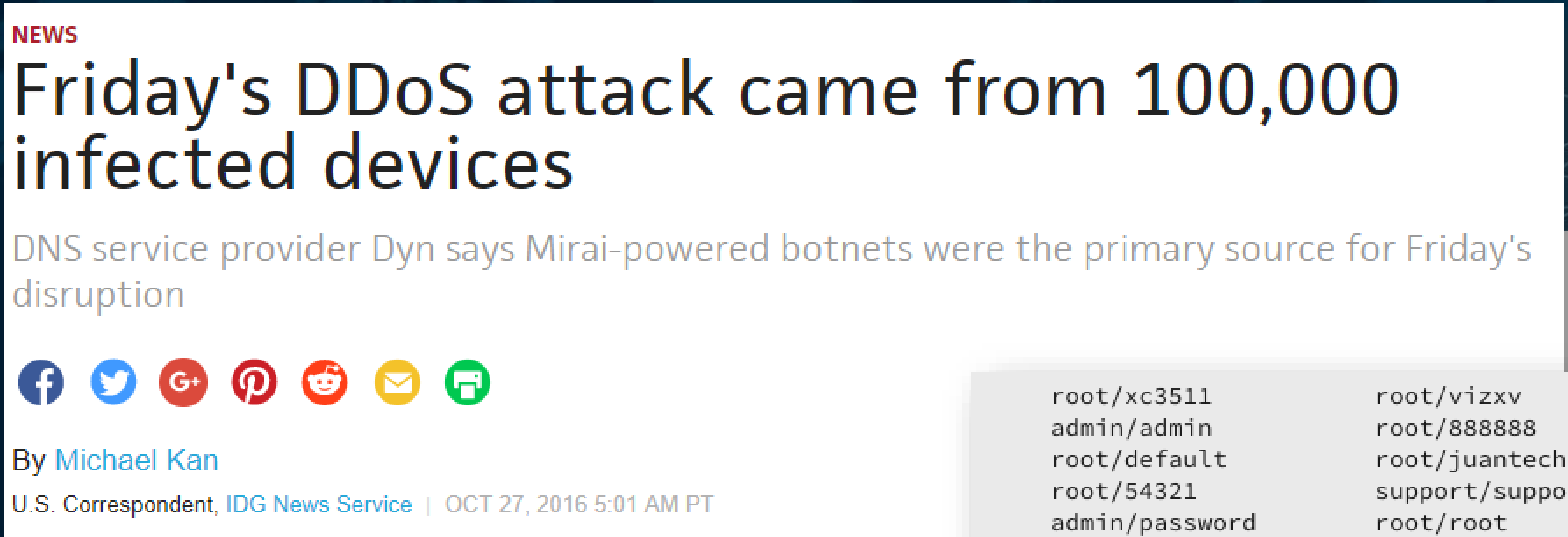
U.S. Correspondent, IDG News Service | OCT 27, 2016 5:01 AM PT

17

Dyn Data Centers Globally

That's all but three of the DNS service provider's sites.

Yevgeniy Sverdlik | Oct 26, 2016



NEWS

Friday's DDoS attack came from 100,000 infected devices

DNS service provider Dyn says Mirai-powered botnets were the primary source for Friday's disruption

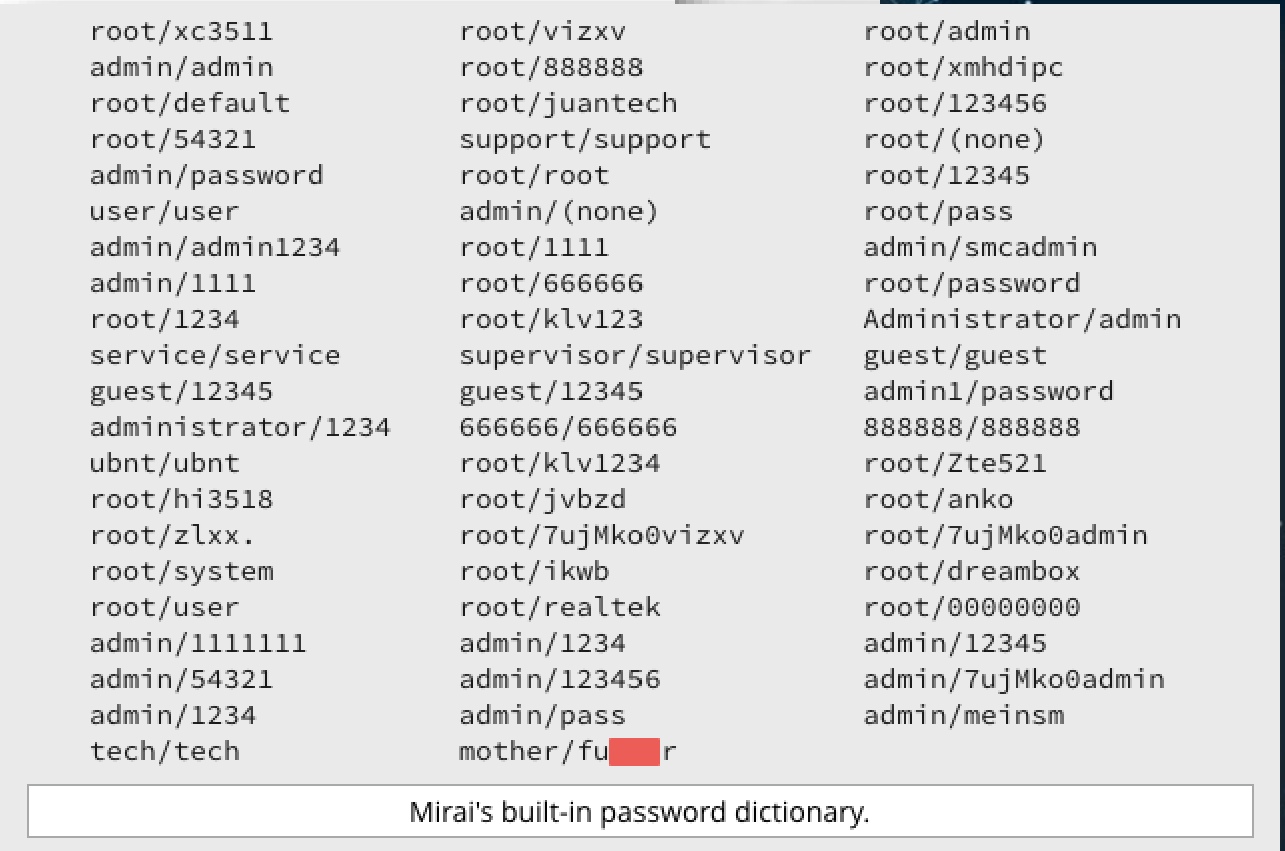
By Michael Kan

U.S. Correspondent, IDG News Service | OCT 27, 2016 5:01 AM PT

Dyn Data Center

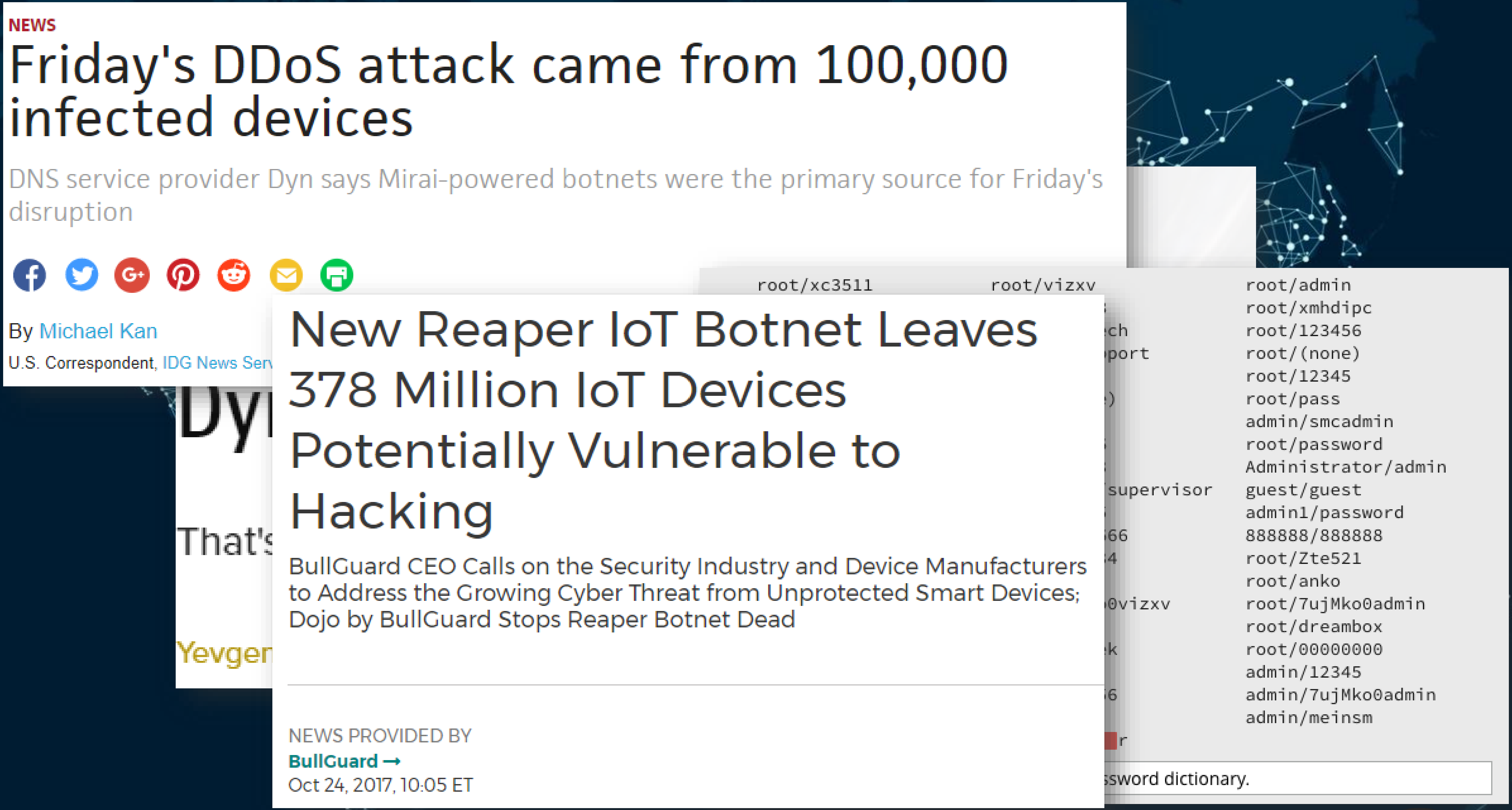
That's all but three of the DN

Yevgeniy Sverdlik | Oct 26, 2016



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

Mirai's built-in password dictionary.



NEWS

Friday's DDoS attack came from 100,000 infected devices

DNS service provider Dyn says Mirai-powered botnets were the primary source for Friday's disruption

By Michael Kan

U.S. Correspondent, IDG News Serv

Dy

That's

Yevgen

New Reaper IoT Botnet Leaves 378 Million IoT Devices Potentially Vulnerable to Hacking

BullGuard CEO Calls on the Security Industry and Device Manufacturers to Address the Growing Cyber Threat from Unprotected Smart Devices; Dojo by BullGuard Stops Reaper Botnet Dead

NEWS PROVIDED BY

BullGuard →

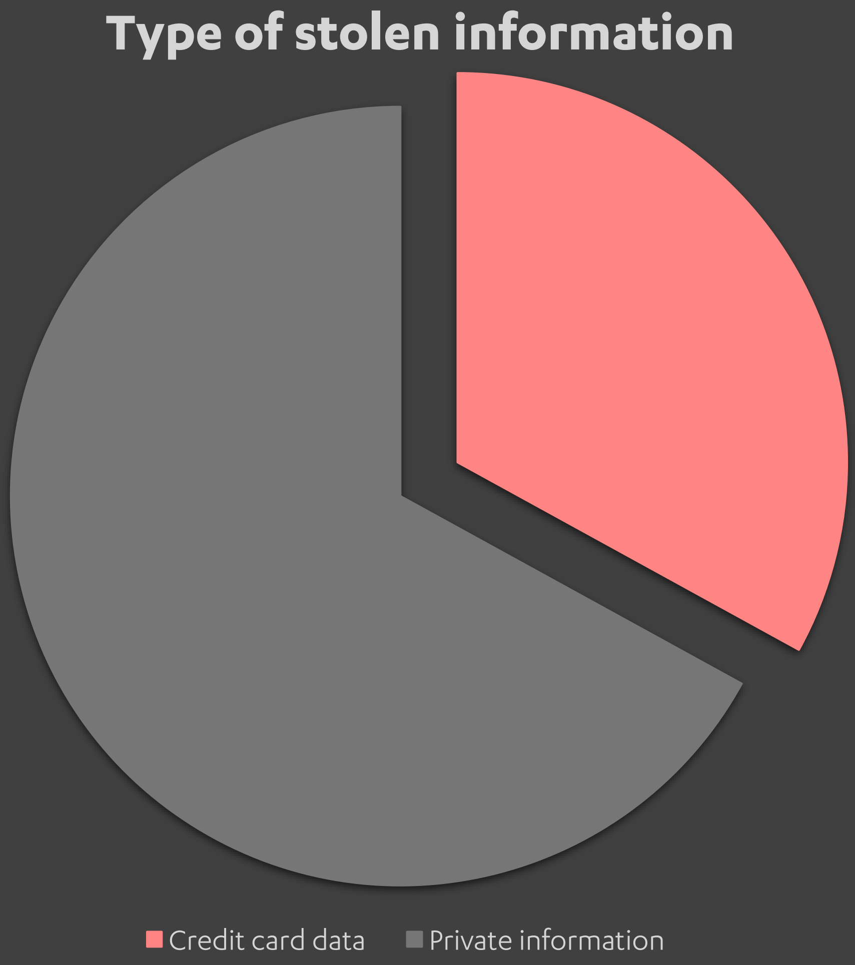
Oct 24, 2017, 10:05 ET

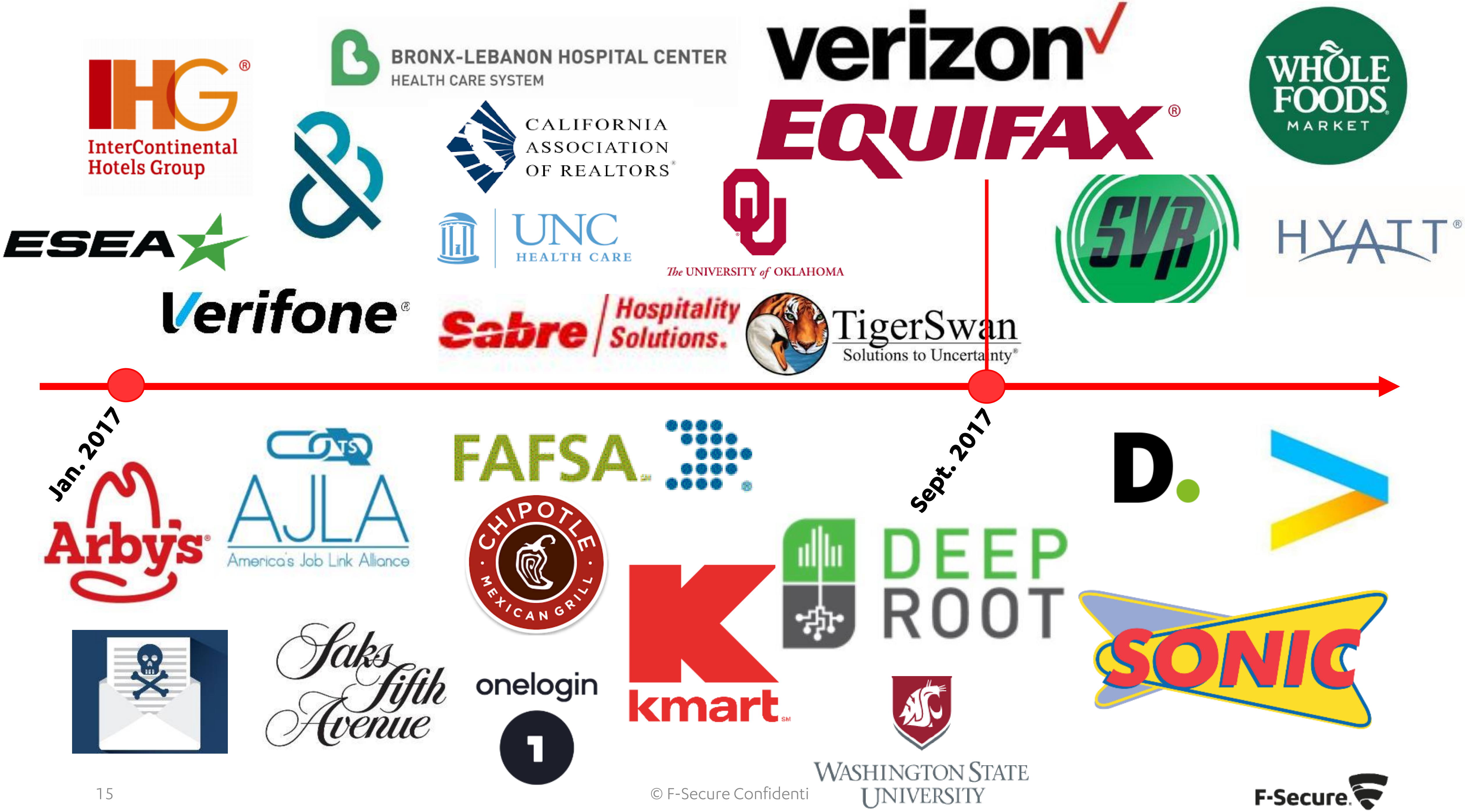
```
root/xc3511        root/vizxv          root/admin
                                       root/xmhdipc
                   ch                  root/123456
                   port                root/(none)
                                       root/12345
                   )                   root/pass
                                       admin/smcadmin
                                       root/password
                                       Administrator/admin
                   supervisor          guest/guest
                                       admin1/password
                   66                  888888/888888
                   4                   root/Zte521
                                       root/anko
                   0vizxv              root/7ujMko0admin
                                       root/dreambox
                   k                   root/00000000
                                       admin/12345
                   6                   admin/7ujMko0admin
                                       admin/meinsm
                   r
```

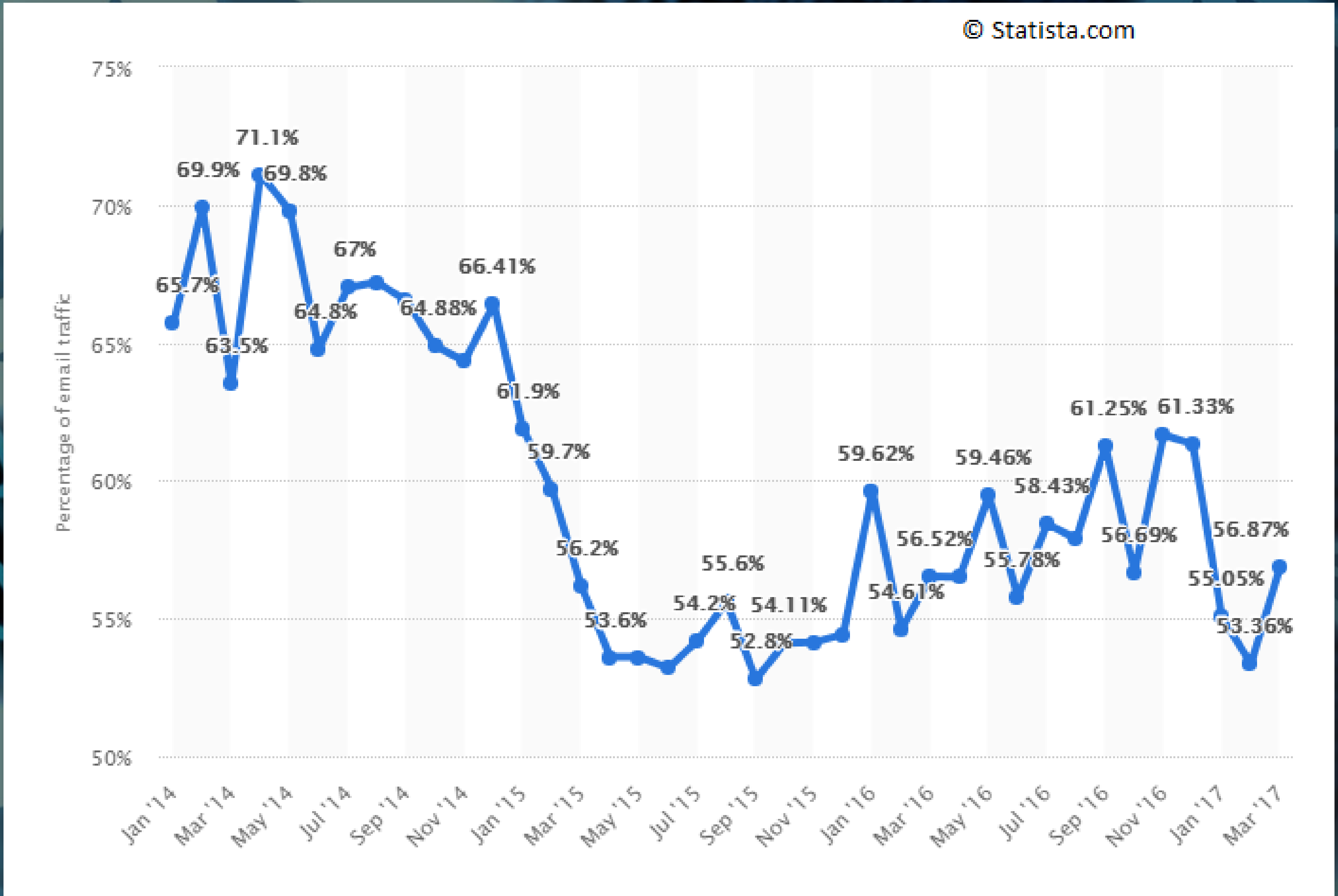
ssword dictionary.

BREACHES IN 2017

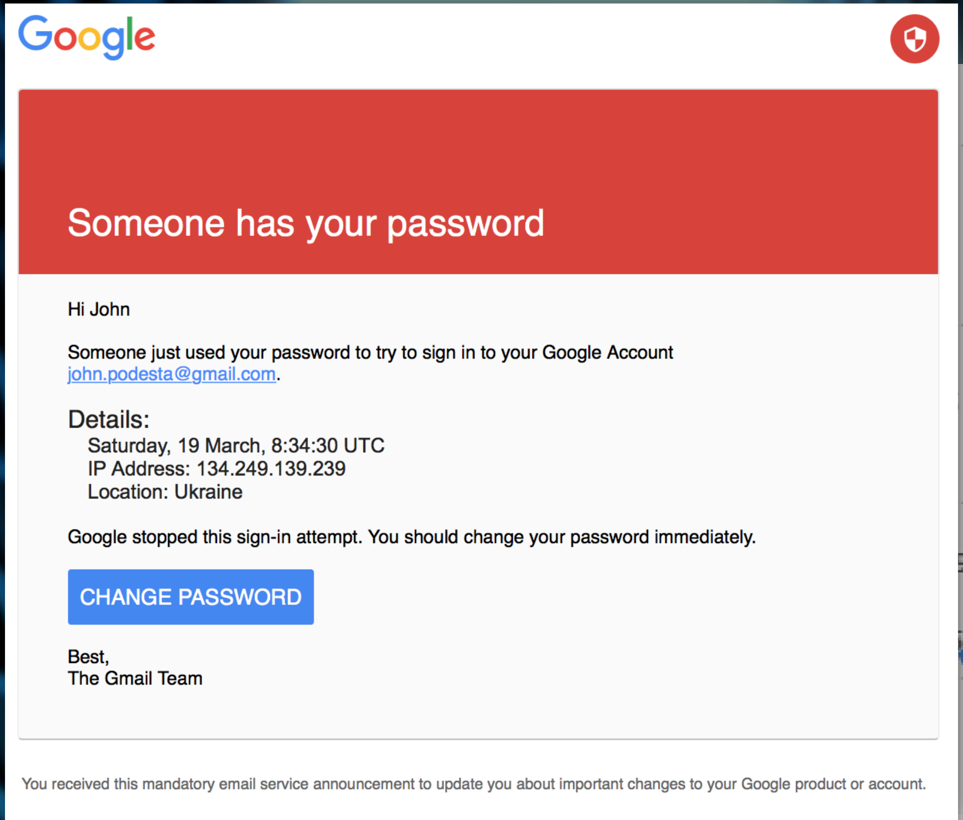
- DBs and systems in public Internet
- PoS malware scraping credit card data
- Private information leaks primarily (90%):
  - Misconfigurations (e.g. poor passwords)
  - Security patches not installed
- Just US statistics: GDPR




IHG InterContinental Hotels Group
BRONX-LEBANON HOSPITAL CENTER HEALTH CARE SYSTEM
verizon
EQUIFAX
WHOLE FOODS MARKET
CALIFORNIA ASSOCIATION OF REALTORS
ESEA
UNC HEALTH CARE
The UNIVERSITY of OKLAHOMA
SVR
HYATT
Verifone
Sabre Hospitality Solutions.
TigerSwan Solutions to Uncertainty
Jan. 2017
Sept. 2017
Arby's
AJLA America's Job Link Alliance
FAFSA
CHIPOTLE MEXICAN GRILL
D.
DEEP ROOT
SONIC
Saks Fifth Avenue
onelogin
kmart
WASHINGTON STATE UNIVERSITY



© Statista.com



Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:

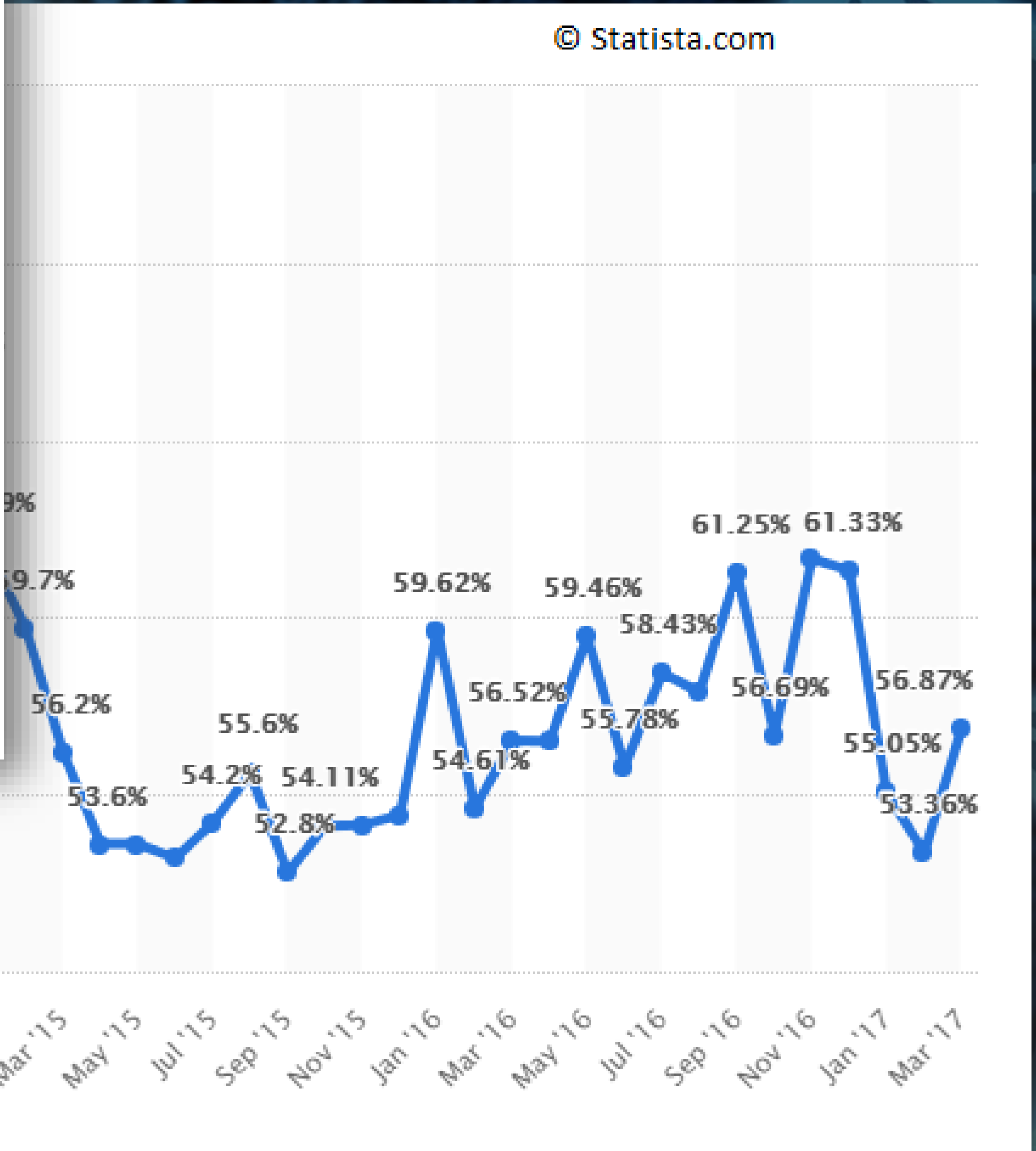
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

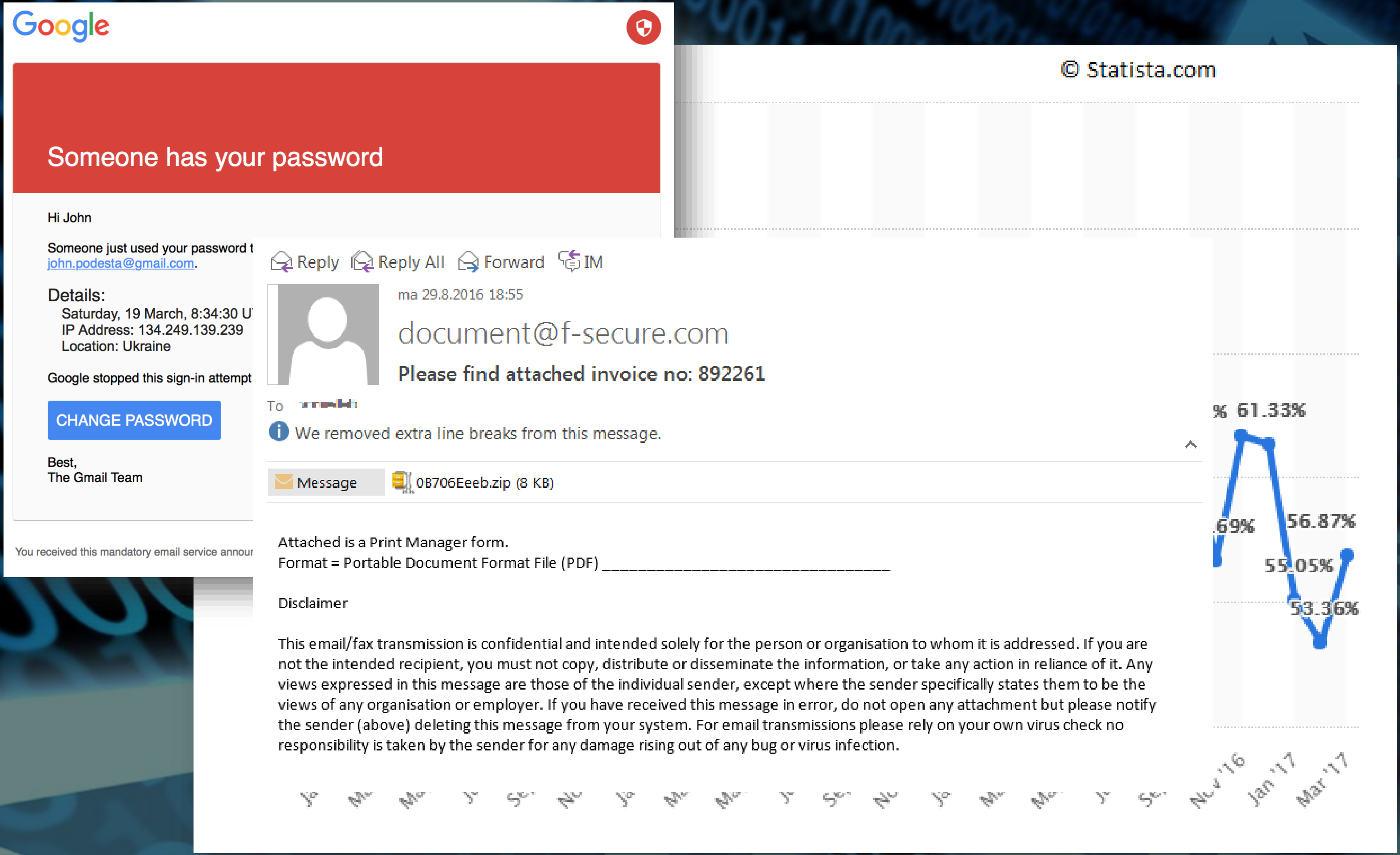
CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.



© Statista.com



Google

Someone has your password

Hi John

Someone just used your password t
john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 U
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service annour

ma 29.8.2016 18:55

document@f-secure.com

Please find attached invoice no: 892261

To [redacted]

We removed extra line breaks from this message.

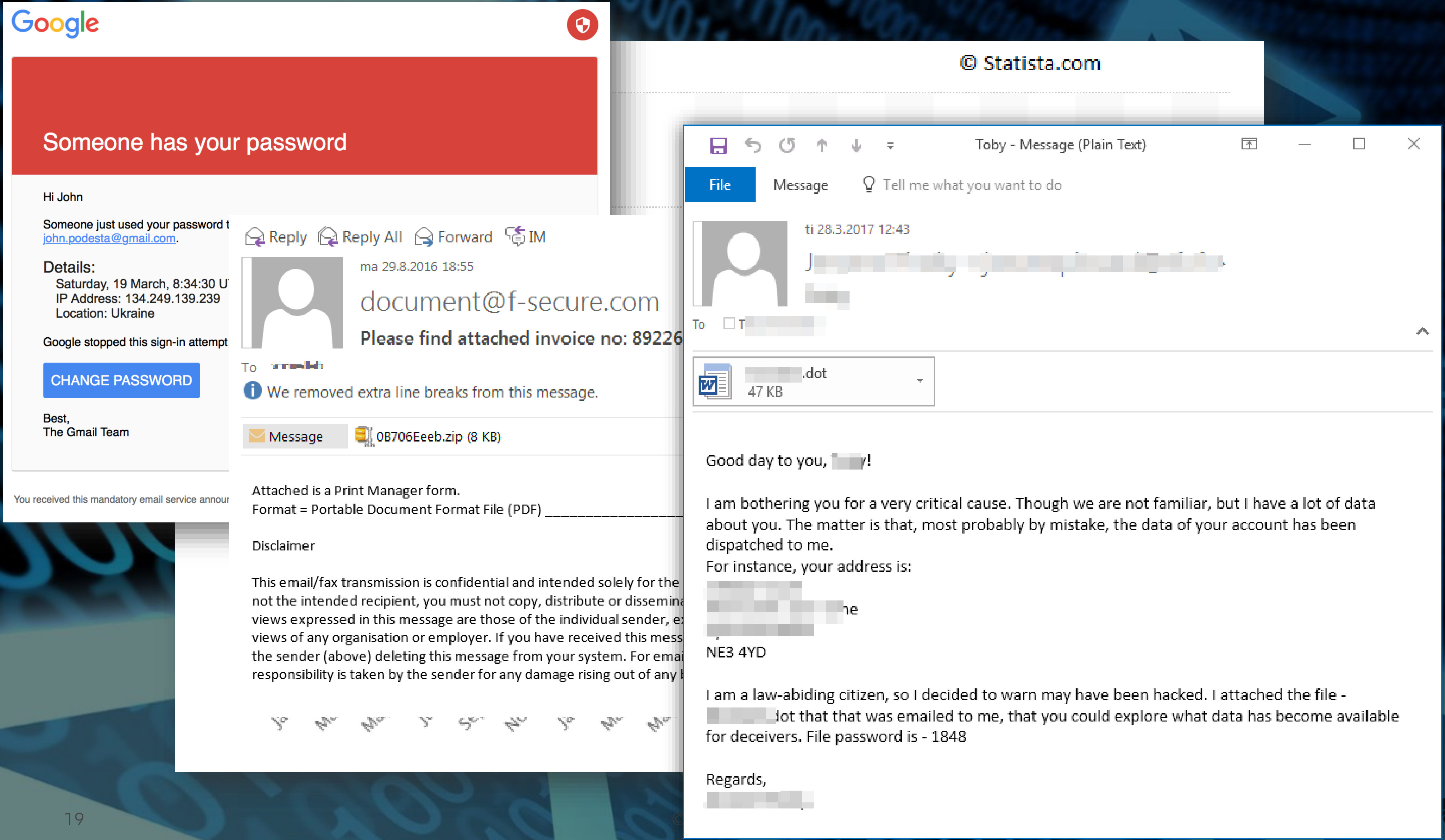
0B706Eeeb.zip (8 KB)

Attached is a Print Manager form.
Format = Portable Document Format File (PDF) ___________________________________

Disclaimer

This email/fax transmission is confidential and intended solely for the person or organisation to whom it is addressed. If you are not the intended recipient, you must not copy, distribute or disseminate the information, or take any action in reliance of it. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of any organisation or employer. If you have received this message in error, do not open any attachment but please notify the sender (above) deleting this message from your system. For email transmissions please rely on your own virus check no responsibility is taken by the sender for any damage rising out of any bug or virus infection.

© Statista.com



Google

Someone has your password

Hi John

Someone just used your password t
john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 U
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service annour

© Statista.com

ma 29.8.2016 18:55

document@f-secure.com

Please find attached invoice no: 89226

To [redacted]

We removed extra line breaks from this message.

0B706Eeeb.zip (8 KB)

Attached is a Print Manager form.
Format = Portable Document Format File (PDF) ___________________

Disclaimer

This email/fax transmission is confidential and intended solely for the
not the intended recipient, you must not copy, distribute or dissemina
views expressed in this message are those of the individual sender, e
views of any organisation or employer. If you have received this mess
the sender (above) deleting this message from your system. For emai
responsibility is taken by the sender for any damage rising out of any

Ja Ma Ma Ju Se No Ja Ma Ma

ti 28.3.2017 12:43

[redacted]

To [redacted]

[redacted].dot
47 KB

Good day to you, [redacted]!

I am bothering you for a very critical cause. Though we are not familiar, but I have a lot of data about you. The matter is that, most probably by mistake, the data of your account has been dispatched to me.
For instance, your address is:
[redacted]
NE3 4YD

I am a law-abiding citizen, so I decided to warn may have been hacked. I attached the file - [redacted]dot that that was emailed to me, that you could explore what data has become available for deceivers. File password is - 1848

Regards,
[redacted]

INTERNET IS NOT FIT FOR NON-SECURED SERVICES

F-Secure.