



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

2015-16: political actors enter people's lives



April 2015 – TV5



April 2015 – TV5 Facebook page

CYBERCALIPHATE

Je suis **IS** IS

CyberCallphate

Je suis **IS**

TV5MONDE ✓
TV Network

Watch Video Like Share

Timeline About Photos TV5MONDE+ More

PEOPLE >

1,706,218 likes

Invite your friends to like this Page

Post

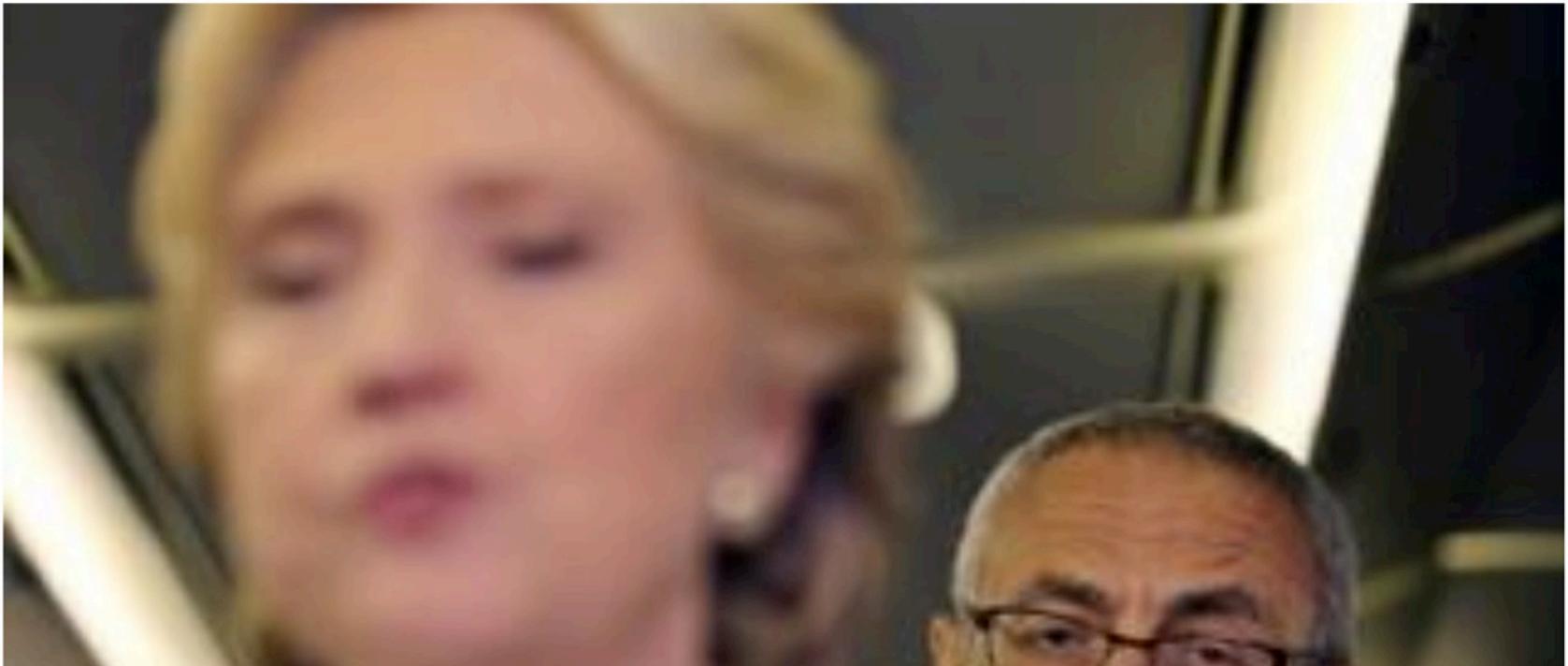
Write something on this Page...

October 2016

18 revelations from Wikileaks' hacked Clinton emails

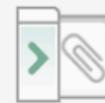
27 October 2016 | US & Canada

f    [Share](#)



2016 – Pawn Storm contacts media

Re leaked emails.eml



From: [Stephan Orphan](#)
To: thesmokinggun@gmail.com
Date: Mon, 27 Jun 2016 16:18:16 -0400
Subject: Re : leaked emails

That's something new. Specially for you. This's the inside for you. This's a part of the big archive that includes Hillary Clinton's staff correspondence. I asked the DCleaks, the Wikileaks sub project, to release a part with a closed access. I can send you a link and a pass. You'll have a couple of days to study themails until it becomes available for public access. But DCleaks asked me not to make any announcements yet. So I ask you not to make links to my blog. Ok?

-----E-mail d'origine-----

De : The Smoking Gun <thesmokinggun@gmail.com>

A: Stephan Orphan <guccifer20@aol.fr>

Envoy le : Lu, 27 Jun 2016 14:46

Sujet : Re: leaked emails

Sure. Are these DNC e-mails exchanged with HRC's staff?

On Mon, Jun 27, 2016 at 3:43 PM, Stephan Orphan <guccifer20@aol.fr> wrote:

Hi there, I can give you an exclusive access to some leaked emails linked Hillary Clinton's staff as I see them. Are you interested?

Re leaked emails.eml

Delivered-To: thesmokinggun@gmail.com

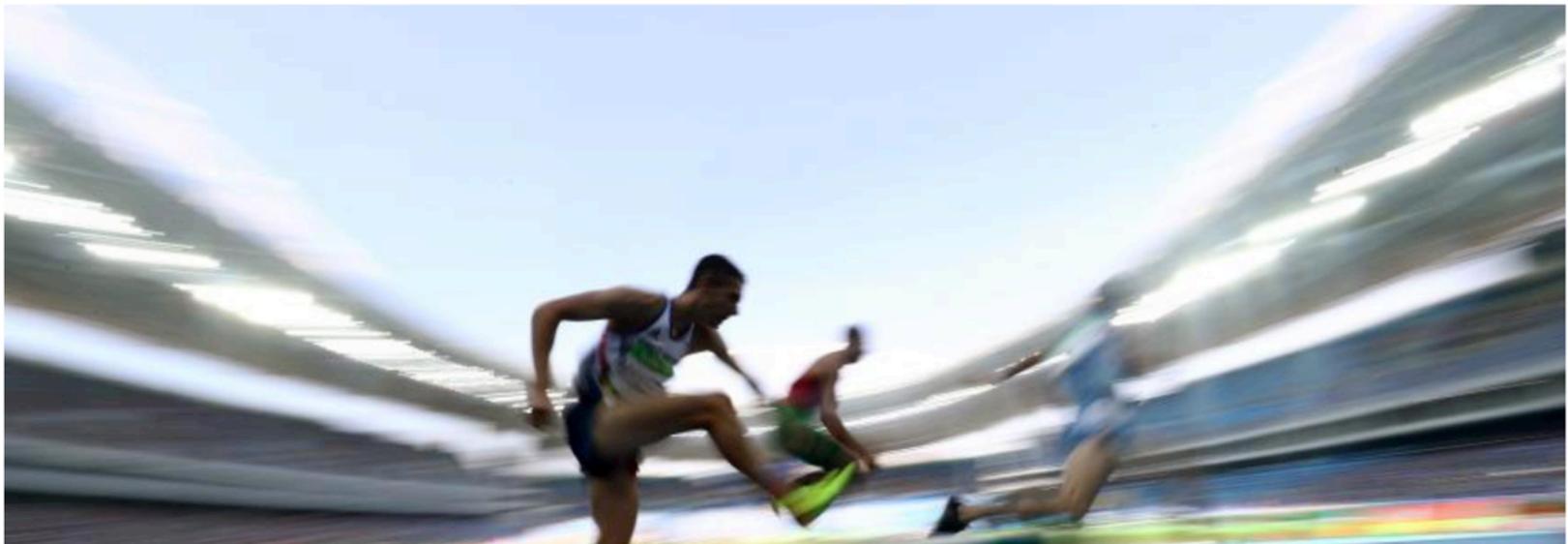
December 2016

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

The image shows a web browser window with a single tab titled "NetScaler Gateway". The address bar displays the URL "https://kasapp.de/vpn/index.html". The page content features a dark blue background with a white logo on the left that reads "Konrad Adenauer Stiftung". On the right side, there is a login form titled "Please log on" with three input fields labeled "User name", "Password", and "OTP". Below these fields is a prominent blue "Log On" button. The browser's search bar is visible in the top right corner.

NetScaler Gateway

https://kasapp.de/vpn/index.html

Search

Konrad Adenauer Stiftung

Please log on

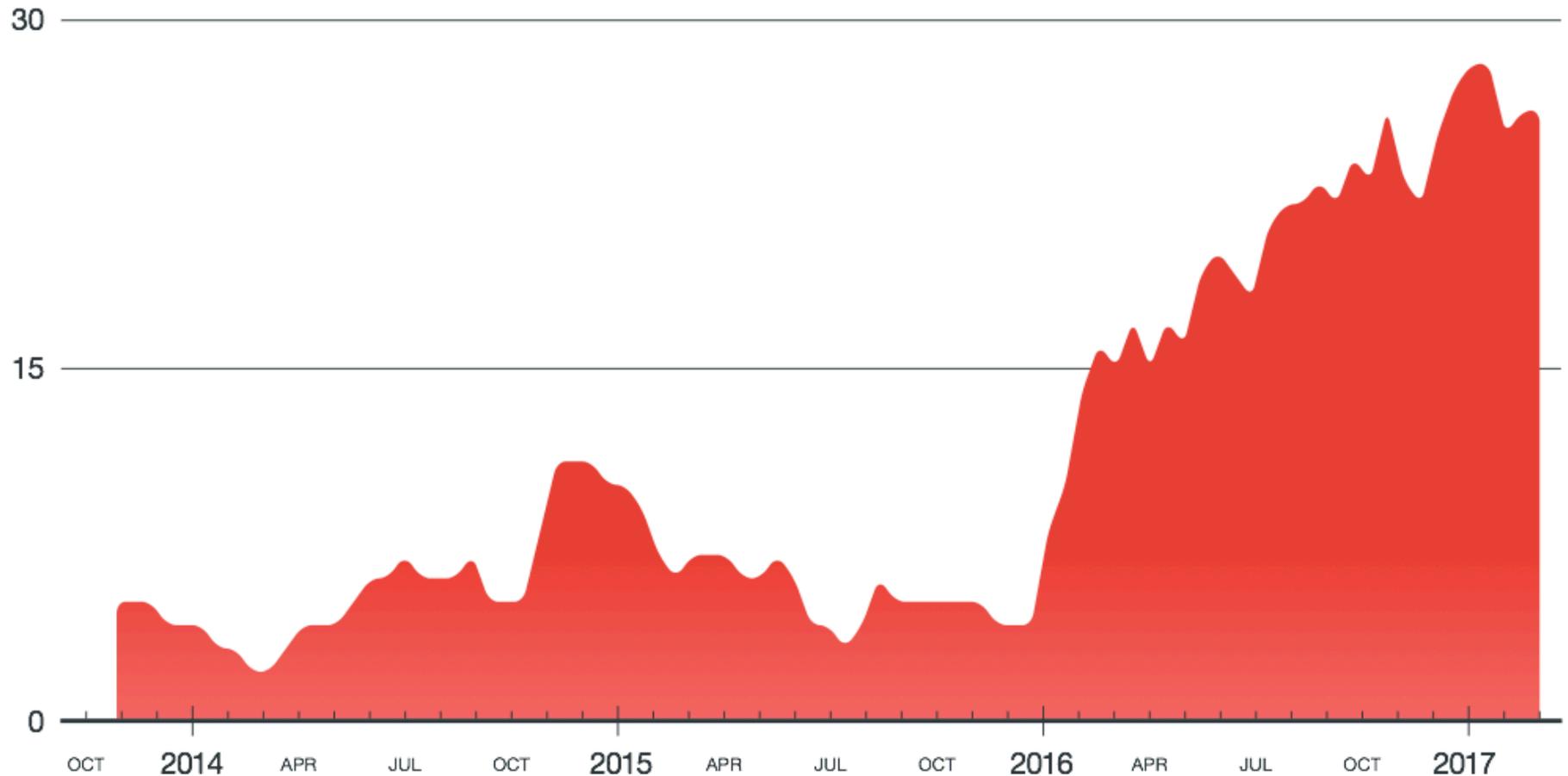
User name

Password

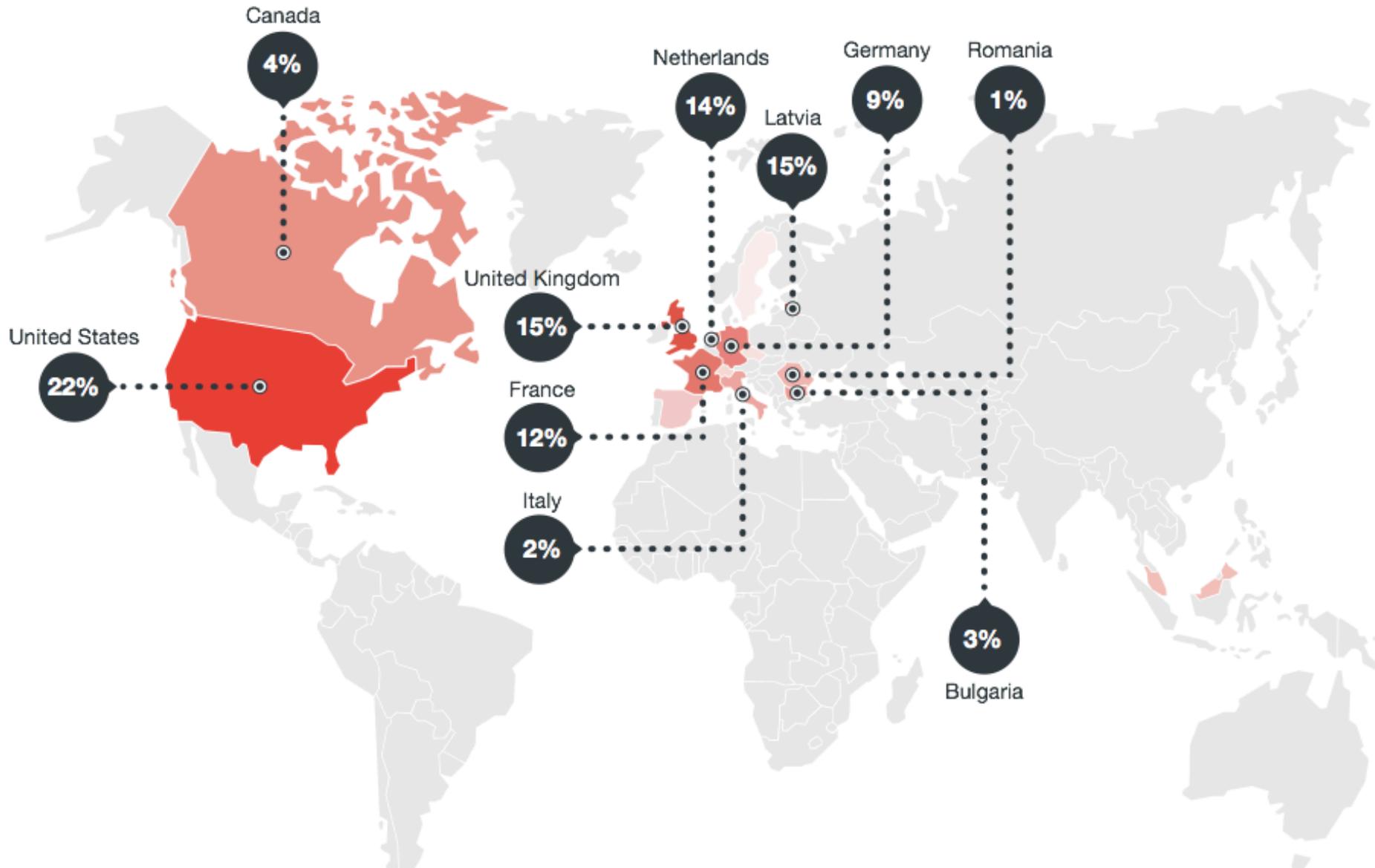
OTP

Log On

Growth of 2nd stage C&C Pawn Storm



facilitators – location of C&C servers



fake news collector – likely Pawn Storm

The screenshot shows the website **VBROSAM.NET** with a search bar and navigation links. The main content area is titled "Недоверенные новостные публикации" (Unreliable news publications) and lists four articles, each with a red "FAKE" stamp and a "Жалоб:" (Complaints) count:

- Article 1:** "Жалоб: 26". Source: BBC NEWS. Title: "Trump Russia dossier key claim 'verified'". Description: "О публикации американской редакции британской службы новостей «Би-Би-Си» «Основное подозрение «российского досье на Д. Трампа» подтвердилось»". Date: 31.03.2017 12:48.
- Article 2:** "Жалоб: 1". Source: OSCE. Title: "Как ОБСЕ осталась без представителя по вопросам свободы СМИ". Description: "О публикации на сайте «Дойче Велле» о Представителе ОБСЕ по вопросам свободы СМИ". Date: 15.03.2017 17:34.
- Article 3:** "Жалоб: 65". Source: NSZC. Title: "Magyar szélsőjobb orosz zsidókat...". Description: "Об инсинуациях на тему подготовки Россией «пятой колонны» в Венгрии с целью дестабилизации ЕС". Date: 10.03.2017 19:30.
- Article 4:** "Жалоб: 47". Source: CNN politics. Title: "Graham, McCain want to hold Sessions-Russia report...". Description: "Об инсинуациях на тему служебной деятельности Посла России в США". Date: 02.03.2017 21:53.

At the bottom, there is a "Рейтинг недоверенных статей" (Unreliable article rating) section with filters for "Все" (All), "За день" (For the day), and "За неделю" (For the week). The current counts are 0 publications from "The New York Times" and 115 total. A "Пожаловаться" (Report) button is also visible.

Two Years of Pawn Storm

Examining an Increasingly Relevant Threat

Feike Hacquebord

Forward-Looking Threat Research (FTR) Team

TM paper

A TrendLabs Report



Operation C-Major: Information Theft Campaign Targets Military Personnel in India

TrendLabs Security Intelligence Blog

David Sancho and Feike Hacquebord
Forward-Looking Threat Research (FTR) Team
March 2016

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?

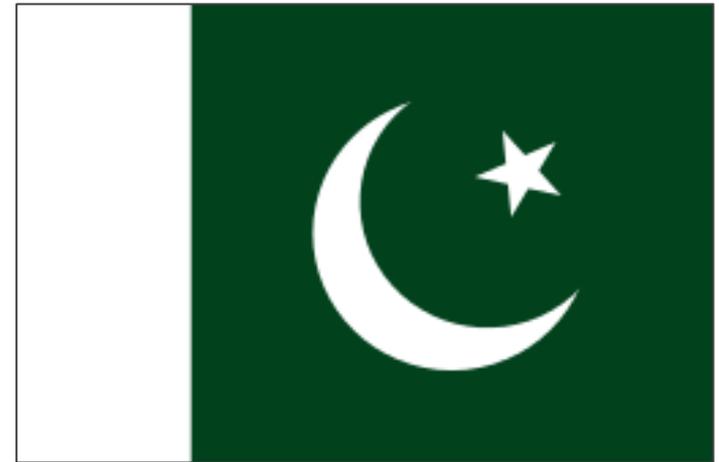
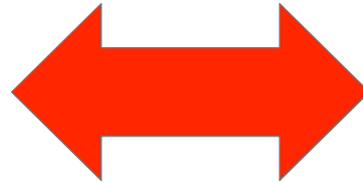
CVE-2016-3298: Microsoft Put Another IE Zero-day Used in A

FastPOS Updates in Time for t Season

Business Email Compr



Summary of C-Major



C-Major characteristics

many campaigns

malware usually poorly detected

heavily focused on military targets

C-Major characteristics

social engineering pretty good

some use of n days... but limited

use of social media like Facebook

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

1st stage malware – very basic

no encryption

hardcoded C&C IP

hardcoded backup C&C domain

campaigns use different TCP ports

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

Refresh

1st stage malware – very basic

actor is **VERY** sloppy with the C&C
backup domain

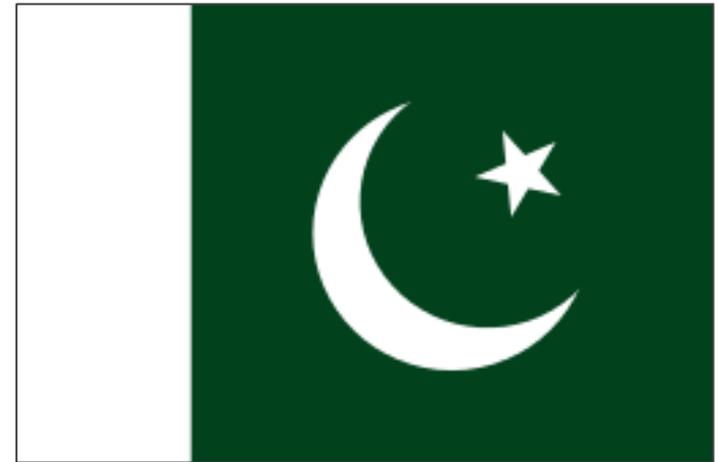
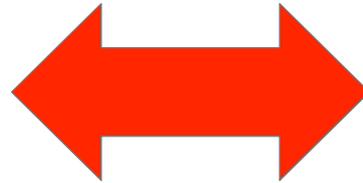
usually not registered

sometimes an existing domain....

Biggest target



is C-Major more than



Pakistani targets





Iran

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**



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

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

CD

JO

MU

RW

SC

TR

BH

EG

MM

MV

SA

SD

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?

our investigation started with this e-mail

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

• **defence minister** <mod@minister.com>

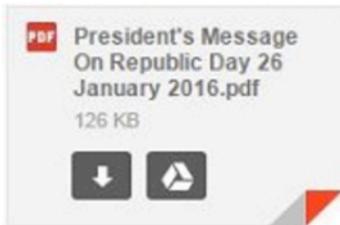
Jan 26 at 8:20 PM ★

To [redacted]@yahoo.com

Dear all,

All heads of wings are requested 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

Question

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

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?

Lessons to learn

better malware

0days

credential phishing

disruptive campaigns (TV5)

influencing public opinion

influencing events

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]

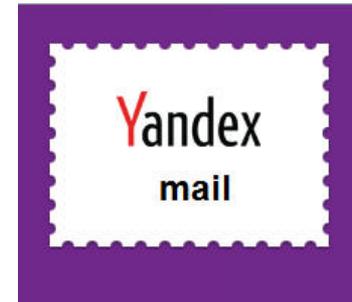
Pawn Storm is also an eager student

The image shows a browser window with the Yahoo! login page. The browser's address bar displays the URL: `login.yahoo.com/?src=ym&intl=us&lang=en&done=https://mail.yahoo.com`. The page features the Yahoo! logo in the top left corner. The main content area is a sign-in form with the following elements:

- The Yahoo! logo at the top of the form.
- The text "Sign in" centered below the logo.
- An input field with the placeholder text "Enter your email".
- A blue "Next" button below the input field.
- A checked checkbox labeled "Stay signed in" and a link "Trouble signing in?" to its right.
- A yellow warning box at the bottom containing:
 - The text "Updated December 2016" in red.
 - An information icon followed by the text "Account security issue".
 - A link "More information about the account security issue." in blue.
 - A link "Our notice to potentially affected users" in blue.

Pawn Storm credential phishing

Pawn Storm does LOTS of targeted phishing



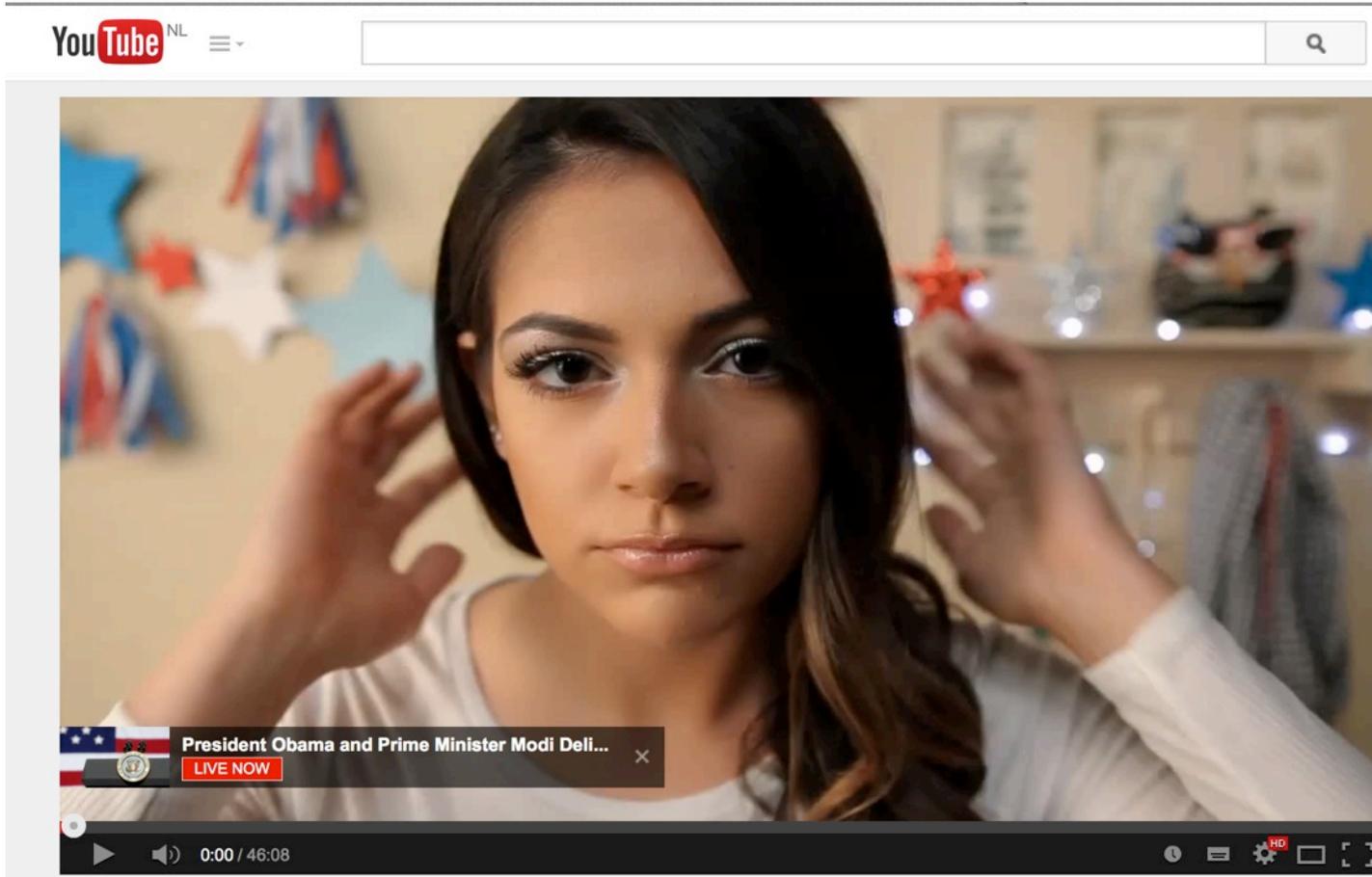
why is credential phishing a big deal?

- often starting point attack
- unexpected attack angles
- risky features that enable social engineering

why is credential phishing a big deal?

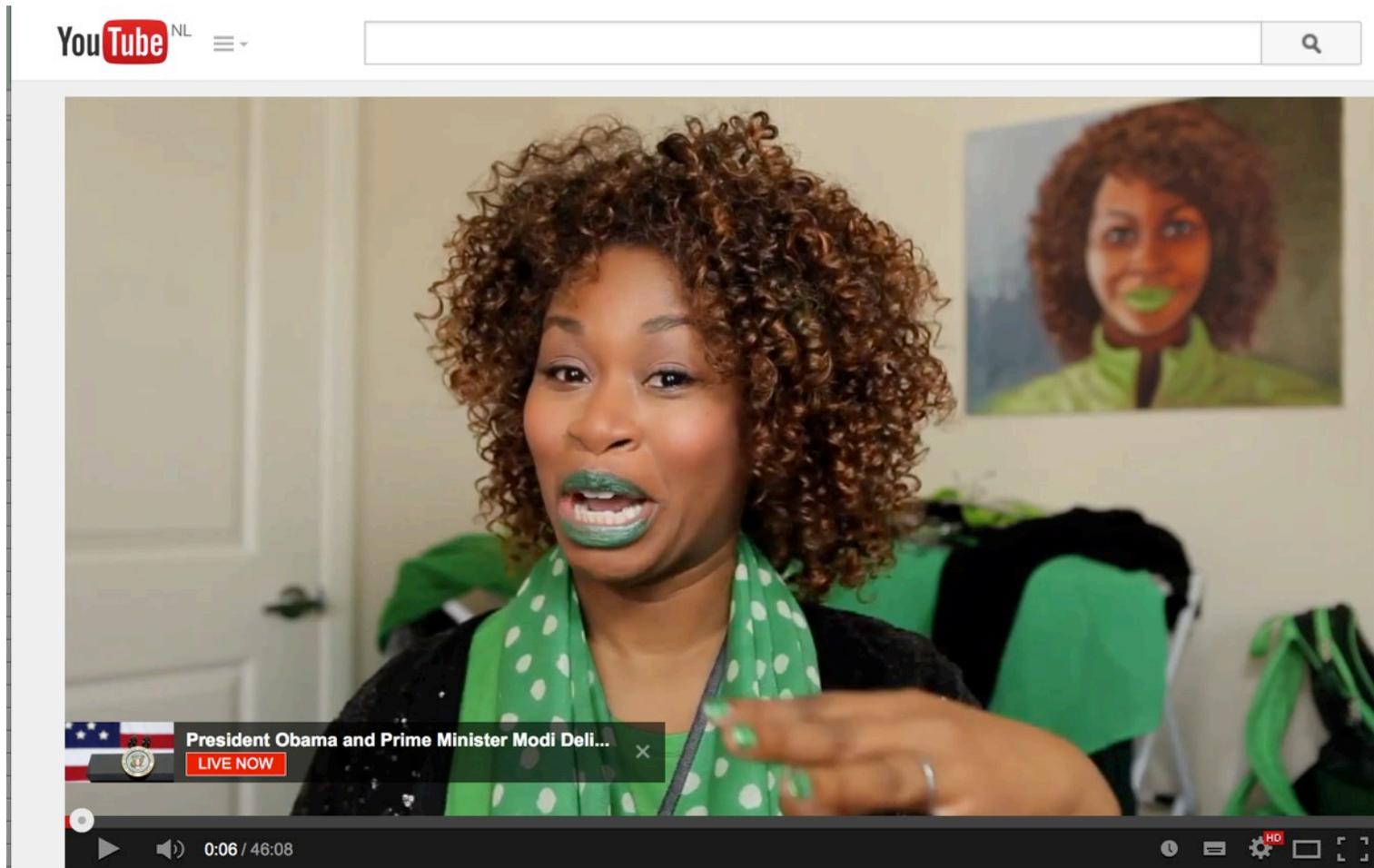
unexpected attack angles

Bethany got Gmail phishing Jan 26 2015



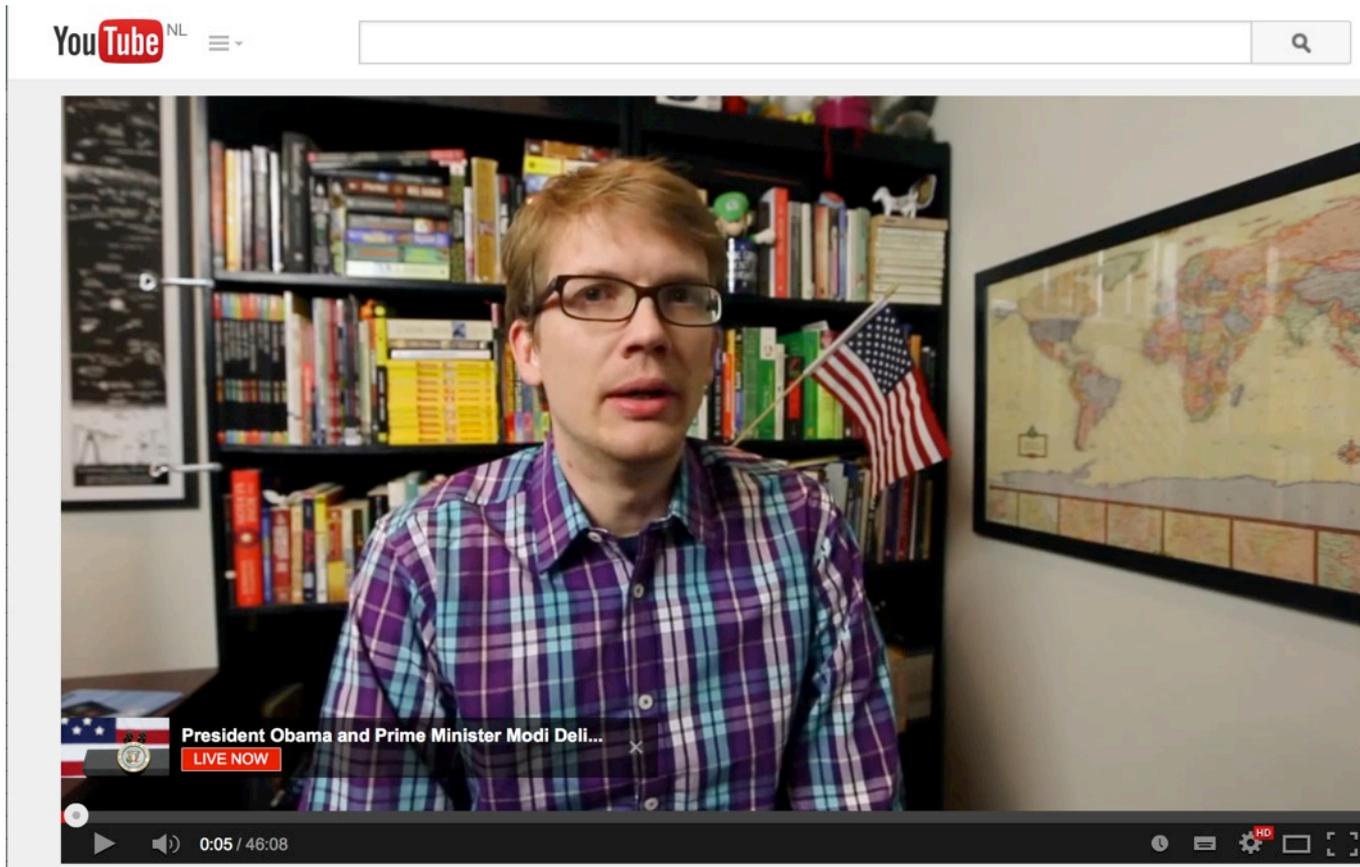
SHE DID **NOT** CLICK ON THE PHISHING LINK

GloZell got Gmail phishing Jan 26 2015



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

Hank got Gmail phishing Jan 26 2015



**HE CLICKED ON THE PHISHING LINK
SURE, JUST TO FIND OUT WHAT IS GOING ON**

high profile target: the White House

The YouTube Interview with President Obama



YouTube



BETHANY MOTA

HANK GREEN

GLOZELL GREEN

JANUARY 22, 2015 5PM EST

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

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

journalists – targeted all the time



CLICKED ON YAHOO PHISHING LINK ON DEC 2014

NYT targeted

corporate e-mail NYT outsourced to Gmail

Dec 23 2014: 40 employees attacked

Dec 30 2014: 16 employees attacked

OAuth abuse

Your account is in danger Inbox x



 **Google** <no-reply.accounts.google@wpereview.org>
to  

Aug 19 



Hi

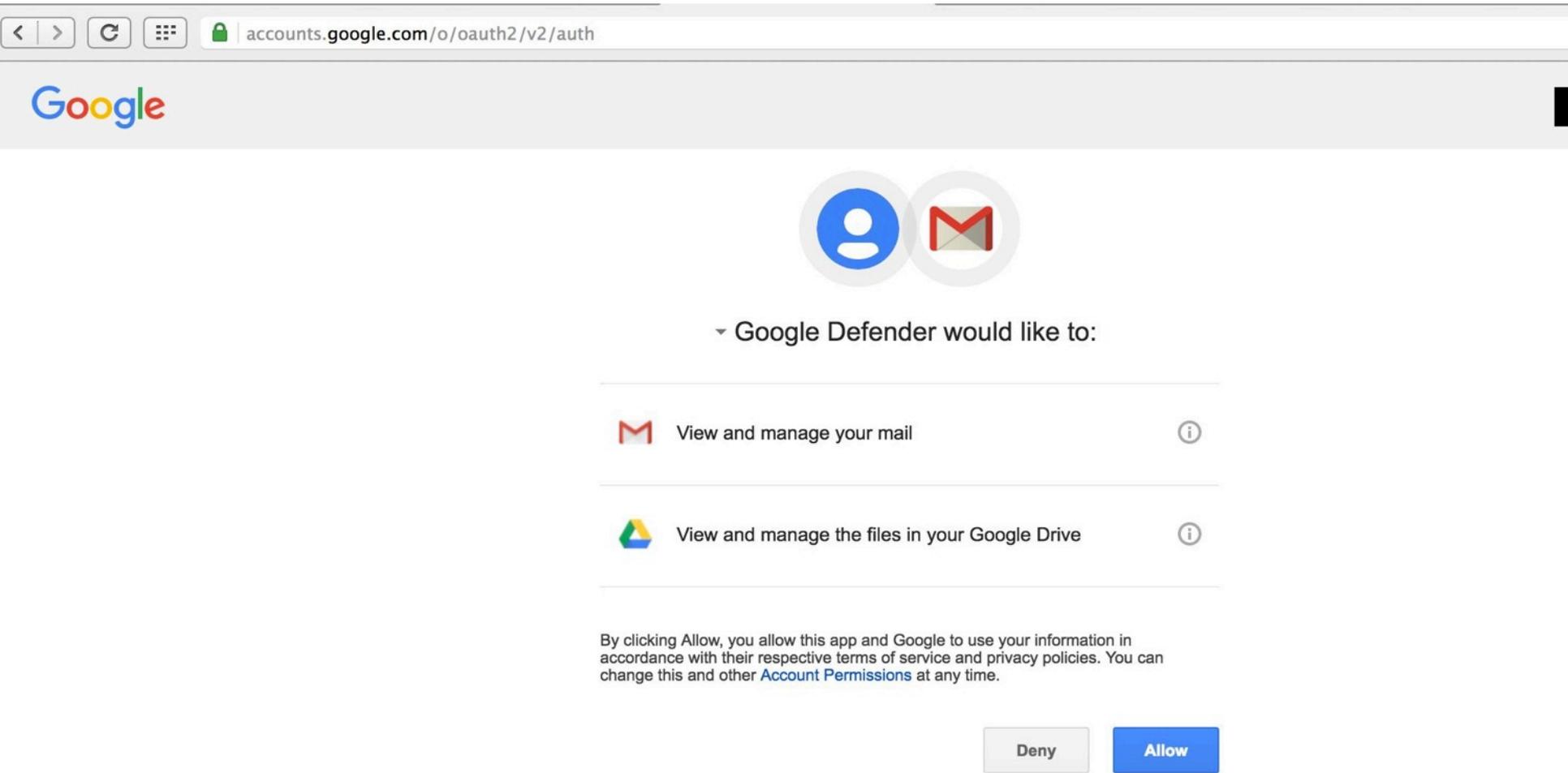
Our security system detected several unexpected sign-in attempts on your account. To improve your account safety use our new official application "Google Defender".

[Install Google Defender](#)



Best, The Mail Team

OAuth abuse



The screenshot shows a web browser window with the address bar containing `accounts.google.com/o/oauth2/v2/auth`. The Google logo is visible in the top left. The main content area displays two circular icons: a blue person icon and a red envelope icon. Below these icons, the text reads "Google Defender would like to:". There are two permission items listed, each with a horizontal line above it and an information icon (i) on the right:

- View and manage your mail (with a red envelope icon)
- View and manage the files in your Google Drive (with a multi-colored triangle icon)

At the bottom, there is a paragraph of text: "By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other [Account Permissions](#) at any time." Below this text are two buttons: a grey "Deny" button and a blue "Allow" button.

OAuth abuse against Yahoo users

McAfee Email Protection

Yahoo <service@mail.yahoo.com>
To c [redacted]@yahoo.com

Dec 6 at [redacted] ★

YAHOO!

Hello [redacted]
Try our new security service for FREE.

Cloud-based email security that is never outdated
McAfee Email Protection and Continuity blocks
advanced phishing, spam, malware, viruses, zero-
hour threats, malicious email attachments, graymail,
denial-of-service, and inappropriate content before it
reaches your mail.

Features:

- Filter outbound email automatically to protect you and your recipients.
- Ensure 24/7 email access, even during email server outages.
- Apply technology advances automatically, saving time and money.
- Access customer support around the clock.

[Try McAfee Email Protection](#)

Thanks for taking these additional steps to keep your account safe.

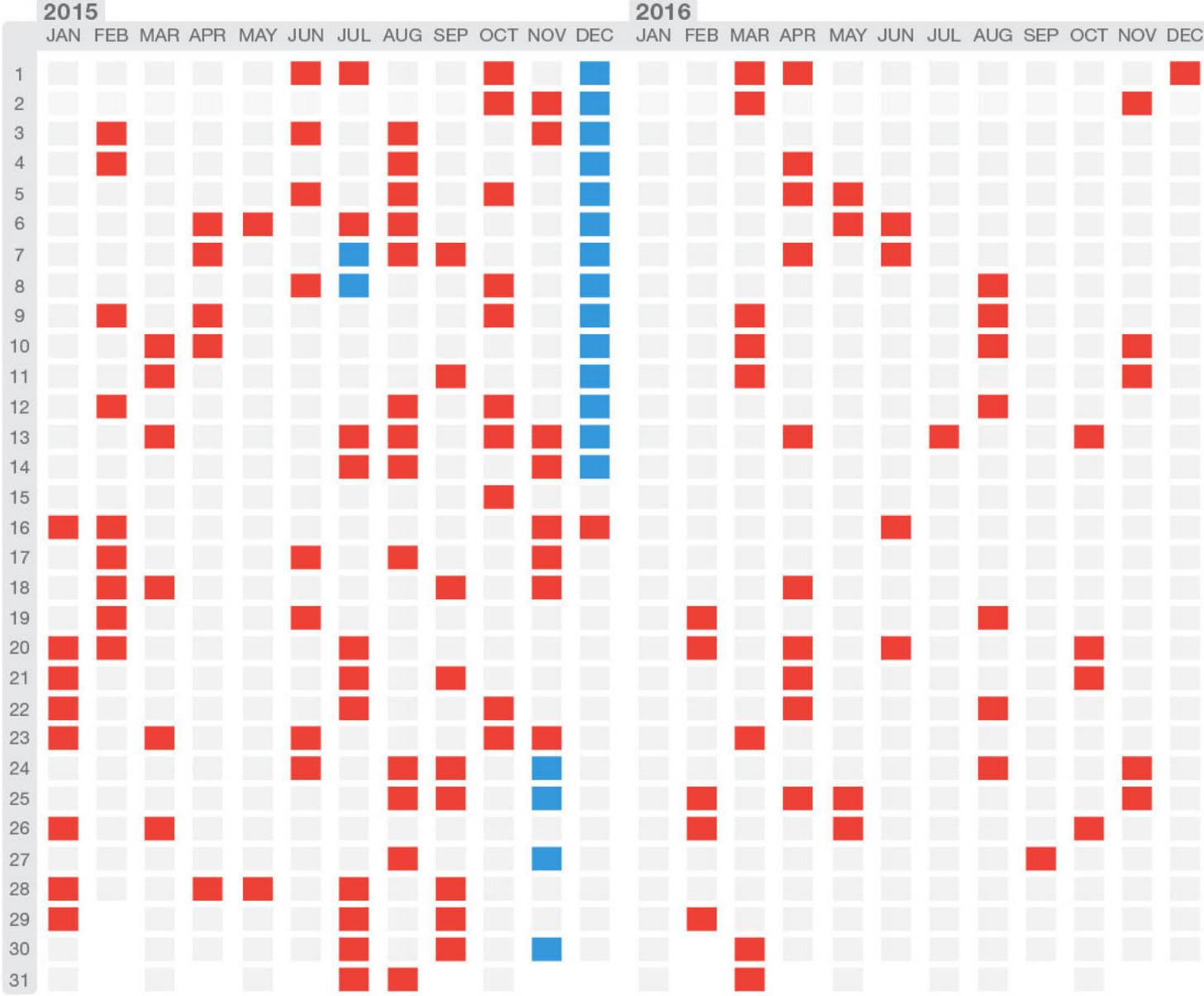
Yahoo

Replies sent to this email cannot be answered.

OAuth abuse against Yahoo users

The screenshot shows a web browser window with the URL `https://api.login.yahoo.com/oauth2/request_auth?client_id=dj0yJmk9eUd5czRSNmVDYTZ...`. The page features the Yahoo logo in the top left and a user profile icon with the name "Help" in the top right. The main content area displays a greeting "Hi, [redacted]" followed by the text "By agreeing, you'll allow McAfee to access:". Below this, a horizontal line separates the header from a list of permissions. The first permission is "Yahoo Mail" with a mail icon and "Full access" below it. At the bottom of the list is a downward arrow. Two buttons are positioned below the list: a blue "Agree" button and a white "Not now" button with a blue border. At the very bottom of the screen, there is a link: "I agree to the Yahoo [Additional terms of service](#)".

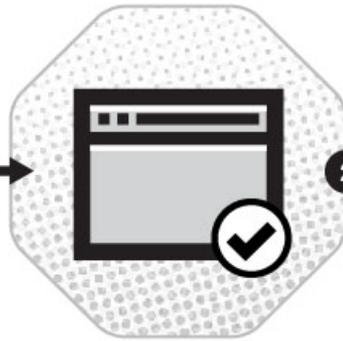
OAuth abuse against Yahoo users





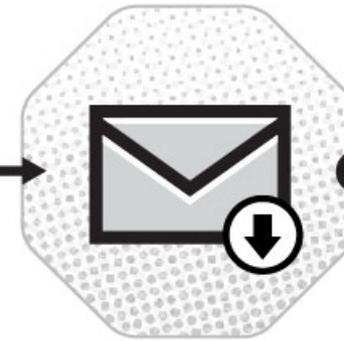
1

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



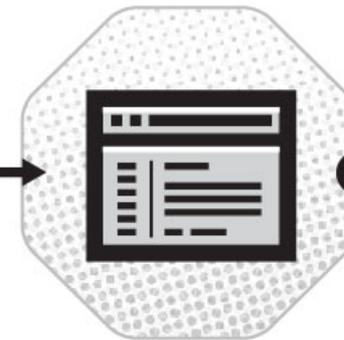
4

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 target's email account



6

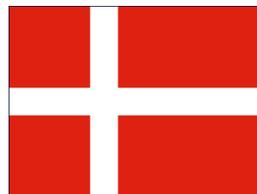
Even if the target changes the password to the email account, the rogue app still has OAuth access—the token needs to be revoked

phishing – more advanced

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

phishing – NATO armed forces

webmail-mil.dk



webmail.exercito.pt



web.mailmil.lv



webmail-mil.gr



targeted phishing by Pawn Storm

the list of phishing domain is endless

and will continue to grow

root cause

too many webmail servers

too many webmail servers of critical organizations online...

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 \(Senior Threat Researcher\)](#)



31



427



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



ELITE TRAINING. TRUSTED PROTECTION.



ABOUT US

ASSESS

TRAIN

PROTECT

FACILITIES

NEWSROOM

CAREERS

PROSHOP

YOUR TRUSTED PARTNER IN GLOBAL SECURITY

BEST-IN-CLASS OPERATIONAL EXCELLENCE

PROVEN SECURITY FOR A CHANGING WORLD
AWARD WINNING GOVERNANCE STRUCTURE

ABOVE ALL.

→ LEARN MORE

WE SPECIALIZE IN

CRITICAL INFRASTRUCTURE
PROTECTION

MARITIME SECURITY

SECURITY TECHNOLOGY

TRAIN WITH US

ACTIVE SHOOTER RESPONSE TABLE TOP
→ RECAP AND PHOTOS

53 RANGES TO TRAIN ON IN MOYOCK
→ EXPAND YOUR SKILL SET TODAY

3 TRAINING
FACILITIES ACROSS
THE UNITED STATES



Academi – phishing site



Microsoft®
Outlook Web App

Security ([show explanation](#))

This is a public or shared computer
 This is a private computer

Use the light version of Outlook Web App

User name:

Password:

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

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 malicious, sets open windows property to

webmail.academl.com

Target clicks link in OWA e-mail

The screenshot shows a web browser window with the URL www.tolonews.com. The page features the TOLONews logo, a navigation menu with categories like News, Photos, Video, and Blogs & Opinion, and a main content area with a featured article and a 'Top Stories' section. A video player for 'Nightly News' is also visible.

News Photos Video Blogs & Opinion Arts & Culture Programmes Watch TOLONews People

Afghanistan World Business Sports Elections 2014

Cabinet Appointment Process Underway

Monday, 20 October 2014

A member of the committee charged with overseeing new ministerial appointments on Monday said that

Top Stories

- Government Should Prioritize Environmental Issues**
French Ambassador to Kabul Jean-Michel Marlaud emphasized on the support of his country for making...
- Guarantors To Face Legal Action If Bank Suspects Don't Show For Court**
The Attorney General's office has cautioned that the guarantors of individuals being called to cou...
- Parliament To Vote On BSA, SOFA Next Week**
Next week the Afghan Parliament will decide whether or not to completely reject or

Nightly News

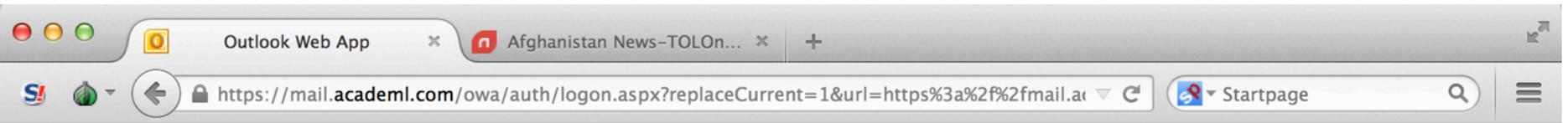
TOLONews 6 pm Ne...

0:00 / 23:12

eglb NEWS

LIVE

OWA “closed” → phishing



Microsoft®
Outlook Web App

Security ([show explanation](#))

This is a public or shared computer
 This is a private computer

Use the light version of Outlook Web App

User name:

Password:

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

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