How politically motivated actors attack

Feike Hacquebord
Forward Looking Threat Research, Trend Micro
First Technical Colloquium
Amsterdam, April 26 2017
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 Facebook page
18 revelations from Wikileaks' hacked Clinton emails

27 October 2016 | US & Canada
2016 – Pawn Storm contacts media

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>
Envoyé 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?
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

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

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

Please log on

User name
Password
OTP

Log On
Growth of 2\textsuperscript{nd} stage C&C Pawn Storm
facilitators – location of C&C servers

- United States: 22%
- Canada: 4%
- United Kingdom: 15%
- France: 12%
- Italy: 2%
- Netherlands: 14%
- Latvia: 14%
- Germany: 9%
- Romania: 1%
- Bulgaria: 3%
fake news collector – likely Pawn Storm
Two Years of Pawn Storm
Examining an Increasingly Relevant Threat

Feike Hacquebord
Forward-Looking Threat Research (FTR) Team
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
"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

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
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
This program cannot be run in DOS mode.

.reloc
taskkill.exe
213.136.83.136
webserver246.com

1System.Resources.ResourceReader,mscorlib,Version=2.0.0.0,Culture=neutral,PublicKeyToken=
System.Resources.RuntimeResourceSet
PADPADP
1System.Resources.ResourceReader,mscorlib,Version=2.0.0.0,Culture=neutral,PublicKeyToken=
System.Resources.RuntimeResourceSet
PADPADP
v2.0.50727
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 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
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

Copyright 2014 Trend Micro Inc.
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>
To i@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
Question

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

Google Defender would like to:

- View and manage your mail
- View and manage the files in your Google Drive

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.

Deny  Allow
Hello

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
OAuth abuse against Yahoo users
Pawn Storm creates a rogue application and signs it up for OAuth with a webmail provider

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

The target receives a fraudulent email with a link to the OAuth request page of the rogue app

The request page will prompt the target to allow or authorize OAuth for the rogue app

If OAuth is authorized for the rogue app, Pawn Storm has access to the target’s email account

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.mail.mil.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

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 malicious, sets open windows property to

  webmail.academl.com
Target clicks link in OWA e-mail
Simple JavaScript

Simple non-malicious javascript

Source of: http://tolonews.com/
OWA “closed” ➔ phishing
other targets with tab nabbing

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