Targeted Attacks Against Civil Society in Asia

Or why you should check the md5 before opening this deck.
Katie Kleemola

Citizen Lab, Munk
School of Global Affairs, University of Toronto

katie@citizenlab.org

HITB GSEC 2015
Civil Society Group face persistent targeted attacks from highly motivated actors.

Vulnerable due to low resources and limited technical literacy.
Study of 10 civil society groups over 4 years

Report: https://targetedthreats.net

Indicators: https://github.com/citizenlab/malware-indicators
Case Studies

Tibetan Diaspora
Hong Kong
Burma
Attacks on Tibetan Diaspora
Dear Tibetan Media,

Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org <http://www.europe-stands-with-tibet.org/>

On behalf of the Working Committee for the “March 10th Rally” in Paris.
Wangpo Tethong

1 attachment: Detailed arrangements.doc 183.3 KB
Dear Tibetan Media,

Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org

On behalf of the Working Committee for the “March 10th Rally” in Paris.
Wangpo Tethong

1 attachment: Detailed arrangements.doc 183.3 KB
Dear Tibetan Media

Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org

On behalf of the Working Committee for the “March 10th Rally” in Paris. 

Wangpo Tethong
Dear Tibetan Media

Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org <hxpg://www.europe-stands-with-tibet.org/>

On behalf of the Working Committee for the “March 10th Rally” in Paris.
Wangpo Tethong
Twenty four months ago Xi Jinping, and 5th generation leaders, inherited extraordinary powers as they took over the helm of the Chinese Communist Party. Alongside these powers they also took on a considerable number of major challenges, prominent among which is China’s occupation of Tibet.

In this powerful new role Xi Jinping was given the opportunity to change four generations of failed Tibet policies by adopting a paradigm shift in the Chinese Communist Party’s approach to Tibet that gives full agency over formulating future policies to the Tibetan people.

However Xi has shown no sign of changing course in Tibet. Instead the Chinese Communist Party can be seen to be continuing down the failed path of previous generations of Chinese leaders, implementing a harsh military crackdowns and unsustainable economic subsidies, which - far from bringing about the stability they seek - serve to exacerbate Tibetan grievances and create widespread resistance right across Tibet.

During the past 24 months we have seen China’s stranglehold occupation in Tibet maintained by Three Pillars of Coercive Control: Military Occupation, Colonial Rule and Fear and Intimidation.

Xi Jinping needs to recognize that Tibetan resistance to China’s failed Tibet policies is not fading away, and the growing strength of international condemnation of China’s leadership is further highlighting the need for change.

Thanks.

Tibet Network,
1310 Fillmore Street,
Suite 401,San Francisco,
CA 94115 United States
Phone:+91 988 225 5516
Xi Jinping's Tibet Challenge
60 Years Of Failed Policies In Tibet
“Sandworm”

- Vulnerabilities in OLE package manager
  - CVE 2014 4114, CVE 2014 6352
  - Original: load remote .inf and “.gif” file
  - Later: from temp folder, no need to worry about firewalls, etc

- Vector: .pps / .ppsx
  - Launches slide deck automatically

- Logic error: no crash or obvious signs to user that they had been compromised
Xi Jinping’s Tibet Challenge
60 Years Of Failed Policies In Tibet
ཐུན་མཐབ་དང་ཐཱིམ་ངོས་

Google

GoogleDocs གི་ Dropbox རུང་ www.ge.tt རུང་

Google docs Dropbox GETT
Detach from Attachments!

Open documents, but don't email them.

Never click on links in attachments sent as email. If you receive an attachment that you do not want or need, delete it immediately. Make sure that any email attachments are free from viruses or other malicious content.

If you open an attachment, read it carefully before executing any actions. If you are unsure whether the attachment is safe, consult with a trusted IT professional or your system administrator.

The way to keep your attachments secure:

1. Never open attachments from unknown sources.
2. Always scan attachments for viruses or other malicious content.
3. Keep your antivirus software updated and running at all times.
4. Use a malware scanner and firewall to protect your system.

International Mobile Equipment Identity (IMEI) is a unique number assigned to every mobile phone. IMEI is used by mobile operators and manufacturers to identify their devices. It is also used by law enforcement agencies to trace stolen or lost phones.
[We are] trying to equip people with a different mindset, so that they are changing their behaviours...so they...run through a mental filter before doing something
Dear Sir/Madam,

I have shared the Biography of H.H. THE 14TH DALAI LAMA via Google Drive.

Kindly download it.

H.H. THE 14TH DALAI LAMA.pps <https://docs.google.com/file/d/087vLM3esIIq-YUdfZ3YxUUI1Qk/edit?usp=drive_web>

With Warm Regard,

Tibet News Group
Contact Address: 1228, 17th Street NW, New Delhi
E-mail: tibetnews2015@gmail.com
“[Technology is] this funny thing where it’s a life line, and then it’s...maybe your ticket to jail”

- Tibetan Activist
“Threat Actors”

• How to identify connections between different campaigns?
  – Malware families
    • Source code may be publicly available, RAT may be sold
      – Typically in Asia, we see “home grown” RATs vs repurposed crimeware (Syria), or commercial malware (FinFisher/Hacking Team)
  – Command and control infrastructure
  – Contextual information
PlugX

• Been under active use /development since at least 2012
  – Originally contained debug messages, pdb paths and “THIS IS A DEMO VERSION!”
  – AlienVault report identified the creator based on evidence like the pdb path
    • Disappeared for a bit after the report
    • Resurfaced with the identified indicators scrubbed
PlugX

• Uses DLL side loading (WinSxS vs KnownDLLs)
  – Signed legitimate executable
    • So a signed executable is running and added as a service
  – Malicious DLL
  – Encrypted binary containing payload
    • Payload is only ever decrypted in memory to hinder detection and analysis
• Typical features: key logger, screenshots, enumerating files, etc
• Configure multiple C2s
• Use alternate DNS to avoid detection through organization’s logs
• Multiple communications protocols: TCP, UDP, P2P
Favorite target for side loading? AV Vendors!
Hong Kong
Hong Kong

- Spring 2015: Same PlugX malware embedded into two different malicious PowerPoint slideshows
  - One sent to a Tibetan group (shown earlier) repurposing slides from an ITN presentation
  - Another sent to individuals related to pro-democratic political parties featuring Occupy Central related lure
Extent of overlap?

- The same threat actor?
- Commonalities across attacks indicate at least some form of resource sharing between attackers
- Our focus is NGOs but we’ve seen overlap with well documented attacks against industry and government
  - Mandiant’s APT1, and others
Attacks in Burma
Political and Economic Context

• Burma is undergoing political and economic transformation

• Country is rich in natural resources (e.g., oil, gas, minerals, timber, etc)

• Heavy investment from China in commercial development

• NGOs are concerned over environmental and human rights impact of development
From: redacted

Subject: Japanese firms apply to operate in SEZs Permit.

Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip
<https://drive.google.com/file/d/0B-FCGiKuUvEQX3Y4RmlyAD4NQo/edit?usp=drive_web>
Japanese firms apply to operate in SEZs

Among the international insurance firms that have representative offices in Myanmar, only Japanese firms have applied to operate in special economic zones, according to the supervisory board of Myanmar Insurance.

Sixteen foreign insurance firms have opened representative offices in Myanmar, but they have not begun operations since regulations have not yet been fully disclosed.

“We will give them permits to begin operating as soon after the principles are issued,” said Dr Maung Maung Thein, the chairperson of the supervisory board.

Only those who meet the criteria will be given the green light. The insurance firms will first be permitted to operate in Myanmar’s three SEZs: Thilawa, Kyaukphyu and Dawei.
Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip
<https://drive.google.com/file/d/0B-FCGiKuUvEQX3Y4RmlyaD4N00/edit?usp=drive_web>

- Permit/Permit.jpg.Ink (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
    - mcutil.dll (Embedded)
From: [redacted]

Subject: Japanese firms apply to operate in SEZs Permit.

Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip

<https://drive.google.com/file/d/0B-FCGiKuU6EQX3Y4Rmlyx14N00/edit?usp=drive_web>

- Permit/Permit.jpg-lnk (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
      - mcutil.dll (Embedded)

PlugX!
Surprise!

From [redacted]
Subject: Japanese firms apply to operate in SEZs Permit.

Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip
<https://drive.google.com/file/d/0B-FCgiKuUvEQX3Y4RnlMyA414N00/edit?usp=drive_web>

- Permit/Permit.jpg.lnk (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
      - mcutil.dll (Embedded)

PlugX!
Surprise!

From: [Redacted]

Subject: Japanese firms apply to operate in SEZs Permit.

Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip
<https://drive.google.com/file/d/0B-FCGiKuUvEQX3Y4RmIyA4D4N00/edit?usp=drive_web>

- Permit/Permit.jpg, lnk (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
      - mcutil.dll (Embedded)

PlugX!
Connections with other campaigns?

• Malware using related C2 signed using same revoked certificate as in attacks against Tibetan organizations
  – PlugX, EvilGrab
• Large volume of attacks in Burma around the same time using the same malware families
uh oh...

“oh dear lord everyone is owned”
Attack identified after “globally recognized organization in the oil and gas industry” visited the URL containing the malicious code.
Index of /mmpdd/sites/default/files/field

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBMAPP.exe</td>
<td>08-Jul-2015 01:29</td>
<td>32K</td>
<td></td>
</tr>
<tr>
<td>fIBMAPP.exe</td>
<td>15-Jul-2015 23:33</td>
<td>241K</td>
<td></td>
</tr>
<tr>
<td>fields.exe</td>
<td>07-Jul-2015 23:50</td>
<td>320K</td>
<td></td>
</tr>
<tr>
<td>image/</td>
<td>06-Feb-2013 09:31</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apache/2.2.15 (CentOS) Server at www.moi.gov.mm Port 80

image source: https://asert.arbornetworks.com/defending-the-white-elephant/
Preliminary discussions about the election, invitations.

PlugX
Same McAfee executable!
From: office <hinthin1asd23@gmail.com>
Date: Sun, Aug 16, 2015 at 7:47 PM
Subject: Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms
Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms
Related Readings

• Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites [https://citizenlab.org/2015/10/targeted-attacks-ngo-burma](https://citizenlab.org/2015/10/targeted-attacks-ngo-burma)


• Communities @ Risk [https://targetedthreats.net](https://targetedthreats.net)

• Indicators: [https://github.com/citizenlab/malware-indicators](https://github.com/citizenlab/malware-indicators)
Targeted Attacks
Deep Analysis:
Case Study in Hong Kong

VXRL
HITB GSEC Singapore 2015
Disclaimer

*** No national secrets ^_^: ***
Case Study about APT against Hong Kong

- Observation
- Against people in the political movement
- Against Voting Website
Observation

We analysed around 40 samples and incidents from the past 18 months against NGOs/Democrats/University sites and obtain the following observation

Who are they?

We never know as I just know they know Chinese characters and didn’t capture any last mile of traffic, we are not talented as mandiant, could guess which dept from a particular string like this: 1j2b3c (Please refer to APT1 report) :)

Where are they?

Most of them put their C2 and VPS in Hong Kong in 2nd/3rd of Internet Service Providers.
Observation

**Their favorite payload**
They do like RATs always: JRAT, PoisonIvy, ….etc, but as I said I can’t see they use TeamViewer, this link is for “their” reference to consider other RATs :)


**Single Server Serves Different Purposes**

Sometimes, we have found those servers, could be C2, serve different purpose. For example, It could serve a phishing site or malware download and C2 together against a single target. It looks the operator didn’t care about the secrecy of command and control server.
Observation Against Democrats/Human Rights/NGOs/Media

There are many ways to attack and we simply classify them into various level based on sophistication and expertise. The percentage stands for the proportion.

Level 0: Web Defacement and Phishing Site (20%)

Level 1: Putting an executable or/and hidden frame and link in the compromised site (10%)

Level 2: Sending phishing mails from Google GMail/Yahoo GMail/Dropbox/Whatsapp (20%)

Level 3: Sending malicious attachment with exploits (commonly in MS Office and PDF) with RAT as payload including PoisonIvy and Java RAT as well as VNC (35%)
Observation Against Democrats/Human Rights/NGOs/Media

Level 4: Sending more “advanced” exploitation with “customised” encryption with use of XOR. It is not common in Hong Kong case but Taiwan (5%)

Level 5: Make a malicious mobile application or software for espionage purpose. (5%)

Level 6: DDoS attack against a site for important political events (5%)
In coming 10 minutes

We will illustrate attacks in levels 5 and 6 so that you could get to know more about the techniques and their revolution as well as their “commitment” :-) 

All attacks are happened during Occupying Central, called Umbrella Movement, in Hong Kong.
Case Study #1: Fake Mobile Application

It spoofs CodeForHK organisation to send out a SMS message to people who could download an application to coordinate OccupyCentral movement.

Credit and appreciation to CodeForHK fellows and Matthew for this analysis, it is good to work with them for the analysis.
Story begins

Check out this Android app designed by CODE4HK for the coordination of OCCUPYCENTRAL!
http://is.gd/
1. Hacking QQ

When it boots it copies assets/qq.xml to the location "/sdcard/.qq/temp.apk". It attempts to hijack victim’s application.
2. Capture Outgoing Call

It hooks into any outgoing calls

<receiver android:name="com.v1.PhoneReceiver" android:priority="2147483647">
  <intent-filter>
    <action android:name="android.intent.action.PHONE_STATE"/>
    <action android:name="android.intent.action.NEW_OUTGOING_CALL"/>
  </intent-filter>
</receiver>

And seems to record them

And stores them at "/data/data/com.v1/XXXXXX.amr"
invoke-virtual {v0}, Landroid/media/MediaRecorder;->release()V

sput-object v6, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;

sput-boolean v5, Lcom/v1/StreamService;->e:Z

:cond_5
sget-boolean v0, Lcom/v1/StreamService;->e:Z

if-nez v0, :cond_2

new-instance v0, Landroid/media/MediaRecorder;

invoke-direct {v0}, Landroid/media/MediaRecorder;-><init>()V

sput-object v0, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;

invoke-virtual {v0, v2}, Landroid/media/MediaRecorder;->setAudioSource(I)V

sget-object v0, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;

invoke-virtual {v0, v2}, Landroid/media/MediaRecorder;->setOutputFormat(I)V

sget-object v0, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;

invoke-virtual {v0, v2}, Landroid/media/MediaRecorder;->setAudioEncoder(I)V

new-instance v0, Ljava/lang/StringBuilder;

cst-string v1, "in_"

invoke-direct {v0, v1}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V

sget-object v1, Lcom/v1/PhoneReceiver;->c:Ljava/lang/String;

invoke-virtual {v0, v1}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
move-result-object v0
new-instance v1, Ljava/io/File;

const-string v2, "/data/data/com.v1/.record/"
invoke-direct {v1, v2}, Ljava/io/File;-><init>(Ljava/lang/String;)V
invoke-virtual {v1}, Ljava/io/File;->mkdirs()Z

sget-object v1, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;
new-instance v2, Ljava/lang/StringBuilder;
const-string v3, "/data/data/com.v1/.record/"
invoke-direct {v2, v3}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V
invoke-virtual {v2, v0}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v0

const-string v2, ".amr"
invoke-virtual {v0, v2}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
move-result-object v0
invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
3. Using Baidu as Geolocation
Other Findings

- Virustotal shows this IP address is used as malware service before in Nov 2013
  - URL: https://www.virustotal.com/en/ip-address/61.36.11.75/information/
- 221.226.58.202 is hardcoded in StreamService
- 101.55.121.36 is suspected to be the C2 server
- Both can be accessed by RDP As of 2014-09-17, it's a Windows 2003 server in simplified Chinese
- Look at the com.google.xrat.protocol stuff, it seems to be able to grab call history, contacts db, SMS history and files on the phone
No more?

<table>
<thead>
<tr>
<th></th>
<th>Resolve</th>
<th>First</th>
<th>Last</th>
<th>Source</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wotlj.click</td>
<td>2015-07-26 00:00:00</td>
<td>2015-07-26 00:00:00</td>
<td>virustotal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exunf.click</td>
<td>2015-07-26 00:00:00</td>
<td>2015-07-26 00:00:00</td>
<td>virustotal</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.dyh.lsgwu61.cn">www.dyh.lsgwu61.cn</a></td>
<td>2015-07-12 05:33:02</td>
<td>2015-07-12 05:33:02</td>
<td>riskiq</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hanguob0008.sjx88.cn</td>
<td>2015-02-26 17:18:00</td>
<td>2015-02-26 17:18:00</td>
<td>mnemonic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hanguob0007.sjx88.cn</td>
<td>2015-02-26 17:17:47</td>
<td>2015-02-26 17:17:47</td>
<td>mnemonic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hanguob0012.sjx88.cn</td>
<td>2015-02-26 17:17:40</td>
<td>2015-02-26 17:17:40</td>
<td>mnemonic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hanguob0007.sjx88.cn</td>
<td>2015-02-26 00:00:00</td>
<td>2015-02-26 00:00:00</td>
<td>virustotal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hanguob0012.sjx88.cn</td>
<td>2015-02-26 00:00:00</td>
<td>2015-02-26 00:00:00</td>
<td>virustotal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hanguob0008.sjx88.cn</td>
<td>2015-02-26 00:00:00</td>
<td>2015-02-26 00:00:00</td>
<td>virustotal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>code4hk.vicp.cc</td>
<td>2014-09-17 00:00:00</td>
<td>2014-09-17 07:36:38</td>
<td>virustotal, kaspersky</td>
<td></td>
</tr>
<tr>
<td>Resolve</td>
<td>First</td>
<td>Last</td>
<td>Source</td>
<td>Tags</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------</td>
<td>---------------</td>
<td>--------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>sywybb.cn</td>
<td>2015-07-29 07:07:42</td>
<td>2015-07-29 07:07:45</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>qjinlkh.click</td>
<td>2015-07-28 17:34:30</td>
<td>2015-07-29 06:57:17</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>apvff.click</td>
<td>2015-07-29 06:38:34</td>
<td>2015-07-29 06:38:34</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>jrkwi.cn</td>
<td>2015-07-29 05:35:52</td>
<td>2015-07-29 05:35:52</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gzfvdq.click</td>
<td>2015-07-29 05:17:27</td>
<td>2015-07-29 05:17:27</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>jhgkc.cn</td>
<td>2015-07-29 05:17:06</td>
<td>2015-07-29 05:17:06</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gowu888.cn</td>
<td>2015-07-28 00:02:06</td>
<td>2015-07-28 00:02:06</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resolve</td>
<td>First</td>
<td>Last</td>
<td>Source</td>
<td>Tags</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>kbvvs.baidu.com.ktvof.cn</td>
<td>2015-10-04 09:02:23</td>
<td>2015-10-04 09:02:23</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.fpz9r.ivhmnclick">www.fpz9r.ivhmnclick</a></td>
<td>2015-08-27 00:00:00</td>
<td>2015-08-27 14:33:06</td>
<td>mnemonic, virustotal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.r3ljl.ookect.click">www.r3ljl.ookect.click</a></td>
<td>2015-08-26 00:00:00</td>
<td>2015-08-26 22:38:10</td>
<td>mnemonic, virustotal, kaspersky</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ivhmnclick</td>
<td>2015-07-29 09:58:36</td>
<td>2015-07-29 09:58:36</td>
<td>riskiq</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ATTRIBUTES

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Seen</td>
<td>2014-09-17 00:00:00</td>
</tr>
<tr>
<td>Last Seen</td>
<td>2015-10-10 15:54:09</td>
</tr>
<tr>
<td>Resolutions</td>
<td>134</td>
</tr>
<tr>
<td>Network</td>
<td>101.55.120.0/23</td>
</tr>
<tr>
<td>ASN</td>
<td>4766 (KIXS-AS-KR Korea Telecom)</td>
</tr>
<tr>
<td>Country</td>
<td>KR</td>
</tr>
</tbody>
</table>

### Heatmap

<table>
<thead>
<tr>
<th>Source</th>
<th>Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>virustotal</td>
<td>5b1430f955c0089dca797c3250edb71f18969c3321b5eac2139b7e42ae818cac</td>
</tr>
</tbody>
</table>
Level 1?!

Detailed analysis from VirusTotal:
https://www.virustotal.com/en/file/5b1430f955c0089dca797c3250edeb71f18969c3321b5eac2139b7e42ae818cac/analysis/1434349022/

Observation

- Hook over WH_KEYBOARD_LL with SetWindowsHook method
- Sending back the data to 101.55.121.36:1604
Case Study #2: DDoS attack against Popvote

A voting site held by The University of Hong Kong is under DDoS attack.

You could get more background information from the following presentation slide:

https://www.hkupop.hku.hk/chinese/resources/workshops/20140925/PopVote_Seminar_22sept2014_Jazz.pdf
<table>
<thead>
<tr>
<th>Date</th>
<th>Attack Event</th>
<th>Outcome</th>
<th>POP’s Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>14&lt;sup&gt;th&lt;/sup&gt;</td>
<td>DDoS on DNS service provider CloudFlare</td>
<td>CloudFlare added service rate limit to the domain name (popvote.hk)</td>
<td>Add Amazon Route 53 as another DNS service provider</td>
</tr>
<tr>
<td>15&lt;sup&gt;th&lt;/sup&gt; - 16&lt;sup&gt;th&lt;/sup&gt;</td>
<td>More than 100 billion DNS requests sent to Amazon</td>
<td>Amazon stopped providing Route 53 (DNS) and CloudFront (CDN) services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDomain under attack with the peak traffic at 10Gbps</td>
<td>Stop providing protection service by UDomain</td>
<td>Turn on protection service by CloudFlare (with limited service rate)</td>
</tr>
<tr>
<td>Day</td>
<td>Description</td>
<td>Action</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>17th</td>
<td>DNS and NTP Reflected DDoS attacks with the peak traffic of 150Gbps.</td>
<td>Report the incidents to the Police</td>
<td></td>
</tr>
<tr>
<td>18th</td>
<td>(Ongoing DDoS attacks)</td>
<td>Announce to extend voting period and prepare to use paper ballots.</td>
<td></td>
</tr>
<tr>
<td>19th</td>
<td></td>
<td>Enroll CloudFlare’s Project Galileo and get 4 dedicated name servers by CloudFlare</td>
<td></td>
</tr>
<tr>
<td>20th</td>
<td>300Gbps DDoS attack taking place before the voting:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 3 DNS Reflection and NTP reflection attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 4 attacks including 100 million SYN packets recorded per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 7 DNS flood with 128 Gbps DNS requests received without amplification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Large amount of random and non-existent sub-domain requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20th</td>
<td>Top level domain, .hk, under attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mitigate by CloudFlare: Transfer zone files to some DNS service providers, use Anycast to absorb bandwidth consumption attack and hard code DNS responses with major recursors, including Google Public DNS, OpenDNS and HK IPS.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Whitelist existent sub-domains at Google Public DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update Android application to minimize the dependence on cloud hosting, and monitor the system around the clock by the Incident Response Team</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Can you handle this kind of attack in your hometown? :)

Compared with ransom in DDOS case, they will leave their contact, QQ number and phone number to the victim to pay the money, there is no way to pay off the attack from Popvote.