HARVESTING BOTNETS FOR UNUSUAL DATA
TOPICS FOR TODAY

• More to a botnet than a virus-infected system

• Typical data types

• Additional data

• Understanding botnets and using their data to do good
WHAT IS A TYPICAL BOTNET?

- Virus Infected Devices
- Traffic
- Loader
- Dropper
- Agent
- Controller (C&C)
- Data Distribution Network
COMMAND AND CONTROL PANELS

Size Matters

Variety

Not Always Offering Data
### Traffic Generation

#### Stats

<table>
<thead>
<tr>
<th>#</th>
<th>Url</th>
<th>Countries</th>
<th>BrowserLanguages</th>
<th>Browsers</th>
<th>ISP</th>
<th>Referrer</th>
<th>Timezone</th>
<th>CaptchaScore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>http://test_redir.html</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td>any</td>
<td>any</td>
<td>any%</td>
</tr>
<tr>
<td></td>
<td>http://test_redir2.html</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td>any</td>
<td>any</td>
<td>any%</td>
</tr>
<tr>
<td></td>
<td>http://test_redir3.html</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td>any</td>
<td>any</td>
<td>any%</td>
</tr>
<tr>
<td></td>
<td>http://test_redir4.html</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td>any</td>
<td>any</td>
<td>any%</td>
</tr>
<tr>
<td></td>
<td>http://test_redir5.html</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td>any</td>
<td>any</td>
<td>any%</td>
</tr>
</tbody>
</table>

#### New Rule

- **Enabled:**
- **Url:** http://
- **GeoIP countries:** any
- **Browsers:**
  - Firefox
  - Internet Explorer
  - Microsoft Edge
  - Opera
  - Safari
  - Google Chrome
  - Other
- **Browser language:** any
- **Filter by ISP:**
- **Referer:** any
- **Timezones:** Any
- **Minimal captcha score:** 0

#### Traffic Statistics

<table>
<thead>
<tr>
<th>ID</th>
<th>Date</th>
<th>Time</th>
<th>IP Address</th>
<th>User-Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>44942</td>
<td>2019-09-25</td>
<td>23:12:33</td>
<td>213.239.206.90</td>
<td>Hetzner Online GmbH</td>
</tr>
<tr>
<td>44943</td>
<td>2019-09-25</td>
<td>23:12:35</td>
<td>213.239.206.90</td>
<td>Hetzner Online GmbH</td>
</tr>
</tbody>
</table>
# Traffic Generation - To Measure Success

## Manage Campaigns

### Period
01.01.2019 - 01.10.2019

### Filter by status
All

### Filter by type
All

### Filter by name

<table>
<thead>
<tr>
<th>ID</th>
<th>CAMPAIGN NAME</th>
<th>CAMPAIGN TYPE</th>
<th>STATUS</th>
<th>ADS / LANDINGS</th>
<th>AVG. CPM</th>
<th>IMPRESSIONS</th>
<th>CLICKS/HITS</th>
<th>CTR</th>
<th>AVG. CPC</th>
<th>SPENT</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>PU_5</td>
<td>Popunder</td>
<td>paused</td>
<td></td>
<td>$1.21</td>
<td>5,164</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>$6.40</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>SK_10</td>
<td>Skimmed</td>
<td>paused</td>
<td></td>
<td>$1.42</td>
<td>35,912</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>$78.31</td>
<td></td>
</tr>
</tbody>
</table>

**Total on this page**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>41,376</th>
<th>0</th>
<th>0.00%</th>
<th>$84.71</th>
</tr>
</thead>
</table>

**Total**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>41,376</th>
<th>0</th>
<th>0.00%</th>
<th>$84.71</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Status</td>
<td>Version</td>
<td>Bot ID</td>
<td>IP Address</td>
<td>Language</td>
<td>Environment</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>---------</td>
<td>--------</td>
<td>------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>b1b39c5</td>
<td>(NO)</td>
<td>8.0.0</td>
<td>RNE-L21 (RNE-L21)</td>
<td>HILTSPMEDAD</td>
<td>com.bbva.bbvacontigo.es.cm.android</td>
<td></td>
</tr>
<tr>
<td>7a0204f</td>
<td>(Orange)</td>
<td>7.1.2</td>
<td>LM.X210 (cv109_lao_com)</td>
<td>PROSPMED</td>
<td>com.google.android.apps.walletnforl-GP</td>
<td></td>
</tr>
<tr>
<td>5504e6e</td>
<td>(NO)</td>
<td>8.0.0</td>
<td>SM-G930F (heroltexx)</td>
<td>PROSPMED</td>
<td>com.google.android.apps.walletnforl-GP com.google.android.apps.walletnforl-GP com.samsung.android.spay - SamsungPay</td>
<td></td>
</tr>
</tbody>
</table>
WHO IS ONLINE NOW?

Info!

Image: TrickBot
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Out URL</th>
<th>Type</th>
<th>Bank</th>
<th>Bank Hash</th>
<th>Size</th>
<th>CRC</th>
<th>Add Time</th>
<th>InPrivate</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>wcmfd_token.abt</td>
<td>wcmfd</td>
<td>wcmfd</td>
<td>Token2.0</td>
<td>wcmfd</td>
<td>fe4a0f9a8f0a36e64608c75a21dea9</td>
<td>46kb</td>
<td>93130a7</td>
<td>16-May-2018 16:10:55</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>gmail.abt</td>
<td></td>
<td>gmail.com</td>
<td>Info</td>
<td>gmail.com</td>
<td>f74d396b44a6309eae4e3e8f7e73c</td>
<td>1kb</td>
<td>ac86cc0d</td>
<td>16-Jul-2017 16:26:42</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>onepass_regions.abt</td>
<td></td>
<td>onepass.regions.com</td>
<td>Token2.0</td>
<td>onepass.regions.com</td>
<td>e4f3952270a62b227e60b12a4c3751e1a9</td>
<td>2kb</td>
<td>e9f6209</td>
<td>02-Mar-2018 11:30:04</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>citiCard.abt</td>
<td></td>
<td>citibank</td>
<td>Info</td>
<td>citibank</td>
<td>f18d6f9964a2c4e436c0873e3c2c9d0</td>
<td>1kb</td>
<td>6066cd7</td>
<td>24-Oct-2017 11:46:19</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>intelix_capitolinebank.abt</td>
<td></td>
<td>intelix.capitolinebank.com</td>
<td>Token2.0</td>
<td>intelix.capitolinebank.com</td>
<td>e1993c2686c775a4f7e82f716c4d36</td>
<td>2kb</td>
<td>13f96cbb</td>
<td>16-May-2018 16:52:23</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>cashanalyzer.abt</td>
<td></td>
<td><a href="https://www.cashanalyzer.com/">https://www.cashanalyzer.com/</a></td>
<td>Token2.0</td>
<td>cashanalyzer.com</td>
<td>da3bcb48a443930ab997e4448c767f1c7</td>
<td>1kb</td>
<td>81397da</td>
<td>02-Mar-2018 11:20:38</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>union.abt</td>
<td></td>
<td>sso.unionbank.com</td>
<td>Token2.0</td>
<td>unionbank.com</td>
<td>d8b80525d4d0f6f0c5b25d45f435</td>
<td>1kb</td>
<td>25636c30</td>
<td>02-Mar-2018 11:31:08</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>treasury_pncbank.abt</td>
<td></td>
<td><a href="http://www.treasury.pncbank.com">www.treasury.pncbank.com</a></td>
<td>Token2.0</td>
<td>treasury_pncbank.com</td>
<td>ca244a6e8e697a6d446c2b6a96089</td>
<td>1kb</td>
<td>8223488b</td>
<td>16-Jul-2017 16:31:46</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>synxous_bussines.abt</td>
<td></td>
<td>businessbankingcenter.synxous.com</td>
<td>Token2.0</td>
<td>businessbankingcenter.synxous.com</td>
<td>c0977e4a017b44ad758b4cbe18f6eae</td>
<td>1kb</td>
<td>866cad8</td>
<td>16-May-2018 16:36:46</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>live.abt</td>
<td></td>
<td>live.com</td>
<td>Info</td>
<td>live.com</td>
<td>bd5f934cc356d068f5e8b23b5b5d9</td>
<td>1kb</td>
<td>9299618</td>
<td>16-Jul-2017 16:28:52</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Royal_Bank.abt</td>
<td></td>
<td>www6.rbc.com</td>
<td>Token2.0</td>
<td>www6.rbc.com</td>
<td>0b6e08ba3529d16005f1a3e529d5444</td>
<td>1kb</td>
<td>b3574ec3</td>
<td>02-Mar-2018 11:30:18</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>tdbank_answers.abt</td>
<td></td>
<td>tdbank_answers</td>
<td>Info</td>
<td>tdbank_answers</td>
<td>0b6d8396d5d5a1875682bf3272d943b</td>
<td>20kb</td>
<td>64bd4e96</td>
<td>26-Sep-2017 06:48:59</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>amazon.abt</td>
<td></td>
<td>amazon.com</td>
<td>Info</td>
<td>amazon.com</td>
<td>a2620f2818d3f0466a56cb8b5f879f6e</td>
<td>1kb</td>
<td>b7439218</td>
<td>06-Sep-2017 13:39:03</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>singlepoint_usbank.abt</td>
<td></td>
<td><a href="https://singlepoint.usbank.com/cs/70_bankingtoken">https://singlepoint.usbank.com/cs/70_bankingtoken</a> /stubber</td>
<td>Token2.0</td>
<td>singlepoint.usbank.com</td>
<td>b96f83eb238938b9e2eb55f5903</td>
<td>1kb</td>
<td>4c7a0de0</td>
<td>02-Mar-2018 11:30:28</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>adp.abt</td>
<td></td>
<td>adp.com</td>
<td>Info</td>
<td>adp.com</td>
<td>5924157e3c9b54f64ca47fd9b30e74026463</td>
<td>30kb</td>
<td>cb1d56c6</td>
<td>06-Jul-2017 11:24:42</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
CONSTANTLY ADDING NEW FEATURES
Image: Vidar Botnet
PAY-TO-PLAY MODEL

Image: Genesis.Market
STANDARD “VALUABLE” BOTNET DATA

- **Logins** (including secret questions, cookies and browser fingerprints)
  - Financial Institutions (i.e. Chase, PayPal)
  - Shopping Sites (i.e. Amazon, Ebay)
  - Social Media (i.e. Facebook)
  - Reward Programs (i.e. hotels, airlines)
  - Corporate
  - Gambling Sites

- **Financial Data**
  - Credit Cards
  - Bank Information
STANDARD “VALUABLE” BOTNET DATA (CONT’D)

• PII
  • SSN
  • IDs
  • Taxes
  • Paychecks

Other Data
  • Gift Cards
  • Software License Keys
  • Coupons
  • Screenshots
  • Files
BANKING - MORE THAN CREDENTIALS

Name: Alison
DOB: 19___-03-15
Address: 111 __________________ , Worsley , M2___
Address (Provided by Google Maps):
Telephone: 0778___ (Carrier: Vodafone)
Email: __________________@hotmail.co.uk
Driving no:
NI no: ________________
MMN: ________________
Passport: https://i.imgur.com/________.jpg
BANKING - MORE THAN CREDENTIALS

---

VBV/MC

3 LETTERS: I / I / I
CC EXP: 02/20
CW: ■
DOB: 15/03/19
POSTCODE: M28 1AH
PASSWORD: ■■■■

Log Origins

IP: 82.132.■.■
Useragent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1
Sent From: (Mobile) http://-----------------------------_free/
BANKING - MORE THAN CREDENTIALS

------------------------ FraudFox Settings ------------------------

OS: iOS 12.1.4
Browser Infos: Safari 12
Platform: 32 Bit
Browser Lang: en-GB
TimeZone: GMT+0000 (GMT)
Flash: null
Cookies: true
Screen Size: 375x667
User Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1

------------------------ FraudFox Profile ------------------------

Instructions:
- Open FraudFox, select "open Text Profile"
- Copy / paste following code into txt box that appears.
- Then Manually select correct Flash version.
- Start FF Browser as normal.

---- BEGIN FRAUDFOX PROFILE-----
Vendor: 
Version: 1.0
Hash: 8ef72d40d4e5eac38b2dc427
USE OF BOTNET DATA - ADDITIONAL INFORMATION

- Botnet data mostly correct (if end-user does not make any typos)
- Botnet data is well documented (who, where, when, etc.)
- Botnet data is well illustrated (screen captures)
- Hackers research nodes and leave insightful comments
MAPPING CREDENTIALS

• Data dumps are not very descriptive

• Credentials can be mapped to botnet data
  • Username match
  • Password match

• Dates
  • Account creation dates
  • Password change dates
• Device Types (Desktop/Mobile)

• Mobile devices tend to change IP addresses

• Tracking movement

• Where the initial infection occurred?

• Corporate Asset Exploitation
Do you ever wonder what is happening on a victim’s machine at the moment when it is infected with a virus?
CATEGORY 2: EVERYTHING IS OK BECAUSE MY AV SAID SO
We'd love your feedback.

How likely is it that you would recommend AdwCleaner to a friend or colleague?

Not at all likely | Extremely likely
--- | ---
0 | 10
CATEGORY 4: TRY UNINSTALLING RANDOM SOFTWARE BECAUSE ALL VIRUSES COME WITH UNINSTALL...
CATEGORY 5: INSTALL MORE VIRUSES
CATEGORY 6: REALIZE THAT YOU ARE NOT THE FIRST VIRUS ON THIS DEVICE AND LEAVE IT ALONE
All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail fastrecovery@cock.li

Write this ID in the title of your message 44A559FC

In case of no answer in 24 hours write us to these e-mails: fastrecovery@cock.li

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and they should not contain valuable information (database backups, wave files, etc.).
Сайт Киллер [2.0] by zlodey ^_^
ENCRYPTED BY GANDCRAB 5.0.4

DEAR mdaemon,

YOUR FILES ARE UNDER STRONG PROTECTION BY OUR SOFTWARE. IN ORDER TO RESTORE IT YOU MUST BUY DECRYPTOR

For further steps read WGWBFL-DECRYPT.txt that is located in every encrypted folder.

8:21 AM 2/13/2019
## PATIENT ZERO

### Image: L0rdix Botnet

<table>
<thead>
<tr>
<th>No</th>
<th>HWID</th>
<th>Ip</th>
<th>OS</th>
<th>Profiles</th>
<th>Code</th>
<th>Country</th>
<th>Last response</th>
<th>Install date</th>
<th>Status</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td></td>
<td>162.158.18.209</td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
<td>2019-01-12 21:55</td>
<td>2019-01-12 21:45</td>
<td>Dead</td>
<td>show</td>
</tr>
</tbody>
</table>
SANDBOXING - BOTNETS

- Think carefully on how you present yourself to the bad guys

<table>
<thead>
<tr>
<th>ClientID</th>
<th>Country</th>
<th>IP/Domain/User</th>
<th>IP Owner Organisation</th>
<th>Group</th>
<th>ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESEARCH-2_W617601.DC94D60422B4C234EC334CC1C94CCF35</td>
<td>US</td>
<td>IP: 149.13.95.6 Domain: User:</td>
<td>AS17330 FireEye, Inc.</td>
<td>jim497</td>
<td>Cogent Communications</td>
</tr>
<tr>
<td>RESEARCH-3_W617601.78FA3EB9600514C018CB511848C3D9B</td>
<td>US</td>
<td>IP: 149.13.95.6 Domain: User:</td>
<td>AS17330 FireEye, Inc.</td>
<td>jim497</td>
<td>Cogent Communications</td>
</tr>
<tr>
<td>VICTIM-PC_W617601.7B5879A870830A97CB1AB00D68EC541C</td>
<td>US</td>
<td>IP: 149.13.95.6 Domain: User:</td>
<td>AS17330 FireEye, Inc.</td>
<td>del225</td>
<td>Cogent Communications</td>
</tr>
</tbody>
</table>

Image: Emotet Botnet
• Don’t connect it to your network

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix : ork.selabs.fireeye.com
Description ........................ : Intel(R) PRO/1000 MT Network Connection
Physical Address .................. : C2-81-2F-D1-BE-70
DHCP Enabled ...................... : Yes
Autoconfiguration Enabled ........ : Yes
Link-local IPv6 Address .......... : fe80::1da9:653e:9be1:2af$b%11(Preferred)
IPv4 Address ..................... : 10.100.9.126(Preferred)
Subnet Mask ........................ : 255.255.252.0
Lease Obtained ................... : Thursday, May 23, 2019 2:43:24 PM
Default Gateway .................. : 10.100.11.254
DHCP Server ...................... : 10.100.8.1
DHCPv6 IAID ...................... : 236368158
DHCPv6 Client DUID .............. : 00-01-00-01-1D-A5-BD-00-16-B1-1E-E9-C2-43
DNS Servers ...................... : 10.100.1.1
NetBIOS over Tcpip ............... : Enabled
```

Image: Emotet Botnet
• Make sure that your Sandbox was not “born yesterday”

• Put some user history and applications in your Sandbox

• Look for consistent behavior patterns
THANK YOU