Upgrading your Cyber Threat Intelligence to Track Down Criminal Hosting Infrastructures

Jan 30th, 2018, Bethesda, MD

Dhia Mahjoub, PhD., Head of Security Research
Takeaways

1. Bulletproof hosting providers business model
2. A taxonomy of bulletproof hosting providers
3. BPH behind current malspam campaigns
4. Techniques and signals to track BPH and malware campaigns
Who am I?

* Dhia @DhiaLite
* Principal Engineer and Head of Security Research at Cisco Umbrella
* Background in network security, network traffic analysis
* PhD in graph algorithms applied on sensor networks problems from SMU
* Speaker at Black Hat, Defcon, RSA, Shmoocon, Brucon, Kaspersky SAS, and a few more
Day in the life of a SOC

Internal Feed:
- Security controls
  - Firewall, IDS/IPS
  - Other network security
  - Web security/proxy
  - Endpoint security
    (AV, EDR, VPN, etc.)
- Network Infrastructure
  - Routers/switches
  - Domain controllers
  - Wireless, Access points

External Feed:
- Domain ownership
- Relationships with IPs and ASNs
- Passive DNS
- WHOIS record data
- Co-occurrences
- Reputation scores

Threats

YOU

SIEM

TIP

Threat Intelligence
Types of Threat Intel

**Strategic Intelligence** involves understanding the broader threat landscape to identify the risk to the organization and help influence change in security investments or operations

**Players:** C-level executives, policymakers, high-level positions

**Operational Intelligence** involves identifying the patterns and trends of adversary campaigns that an organization can build into their security awareness

**Players:** Security Operations Center (SOC)

**Tactical Intelligence** includes IOCs and tactics that help drive the security of an organization and enable it to hunt and respond to threats

**Players:** Security Operations Center (SOC)
Know your adversary

Uncovering Criminal Hosting infrastructures
Umbrella Investigate Intel Production Cycle

Feedback
Protected customers, actionable use cases with Investigate

Requirements
Detect and block domains/IPs to protect customers and provide insight and context around domains/IPs

Collection
Retrieve raw DNS, IP, BGP, SSL, whois, hash, crawled web data, etc. at scale

Dissemination
Domains, IPs into block list
Investigate UI and API

Analysis
Threat detection and reputation scores using ML & graph models, human domain expertise

Processing
Caching, indexing, enriching, summarizing data at scale
Threat Landscape
Cybercrime Ecosystem

**Products**
- Malware – RATs, banking trojans, ransomware, etc.
- Brute force tools and account checkers
- Vulnerabilities and Exploits

**Services**
- Bulletproof Hosting
- DDOS services
- Ransomware as a service
- Installs and traffic
- Exploit Kit
- Cash out and exchangers

**Goods**
- Credit card dumps
- Fullz information and PII
- Database dumps
BulletProof Hosting

Cybercrime

Products

Services

Goods

Bulletproof hosting
Bulletproof hosting provider (BPH)

A criminal hosting provider who shields their customers from abuse complaints and take down action.
Spectrum of Hosting Providers

Good

Abused

Bulletproof

Cisco Umbrella
A Taxonomy of BulletProof Hosting

Cybercrime

- Products
- Services
- Goods

Bulletproof hosting

BPH classification

Botnet-based
Ex. ZBOT FF

Host-based
Ex. ALEX
Dedicated, Hybrid, Leased
Bulletproof Hosting business model
Dedicated hoster recipe

Low barrier of entry (Approx <$2K)
1. Register business offshore
2. Register own ASN and lease IP space
3. Setup website(s) or stay underground
4. Drive customers – forums (open, closed), social media
5. Generate revenue through hosting or sending traffic
7. Handle abuse
8. Shut down, move elsewhere, repeat
Dedicated BPH technical features

- Leaf ASN
- Offshore business registration
- Anonymous payment methods
- Small IP range
- Toxic hosted content or outgoing traffic
Leaf (Stub) ASN or leaf ASNs chain

Have only upstream peers, no downstream
Frequent pattern for questionable/bulletproof hosters
Register Business in Offshore Jurisdictions

Belize
Anguilla
British Virgin Islands
Dominica
Panama
United Arab Emirates
Seychelles
Multiple Layers of Resistance

Servers
RIPE, ARIN space

Business
Belize, Panama, Seychelles

Operators
Ukraine, Russia
Major BPH operations
ZBot Fast Flux BPH Operation

Actor(s) grow and maintain FF network
*FF service offered in underground forums

Zbot Fast Flux Proxy Network
Aka Fluxxy, Darkcloud

Botnet comprised of 30-40K compromised residential IPs, mainly in UA, RU

40-50 bot IPs provisioned per domain

Criminal customer's site origin IP

Content delivered
Short lifetime: malware, ransomware
Medium lifetime: phishing
Long lifetime: carding, cybercrime forums

Introduced at Black Hat 2014, Botconf 2014, Defcon 2017
Threats delivered by ZBot Fast Flux network
Host-based BPH

- Cybercrime
  - Products
  - Services
  - Goods
  - Bulletproof hosting
    - BPH classification
      - Botnet-based
      - Host-based
        - Dedicated
        - Hybrid
        - Leased
Sample Rogue Hosters

Alex
Maxided
Dataflow.su
Ecatel
Hostsailor
Webzilla
Hostkey
QHoster
Hostzealot

King Servers
Koddos/Amarutu
Abelohost/Elkupi
Deltahost
Dataclub.biz
Blazingfast.io
Altuhost
& many more
“Alex”

Top tier BPH provider

Russian-based with some presence in China

Active for a decade, prominent since 2016

Host-based Fast Flux network

Hybrid model: dedicated ASNs & abused 3rd party cloud hosters

Joint Research with **INTEL 471**
Alex BPH enables a variety of toxic content

- Malware
- Ransomware
- Phishing
- Crimeware forums
- Credit card dump shops
Alex’s Network Infrastructure

- AS9002, UA RETN
  - AS8492, RU OBIT
    - AS206728, RU MEDIALAND
      - AS197569, RU ENERGOMONTAZH
        - ALEXANDER, VOLOSOVYK
        - ALEXANDER, VOLOSOVYK
        - ALEXANDER, VOLOSOVYK
        - AS197812, RU FERAZKO HOLDING
          - AS47920, UA COMTEC
            - AS45017, UA LIRUKFIRST
              - AS47920, UA COMTEC
                - AS8492, RU OBIT
                  - AS9002, UA RETN

- AS43350, NL NFORCE
  - AS39164, NL CHECKTOR

Abused third party cloud and hosting services

- NOT ACTIVE SINCE FEB 2017
- CREATED MARCH 2016
- CREATED MARCH 2016
- CREATED MARCH 2016
- CREATED MAY 2011

Sound vision House
Francis Rachel Street
Victoria, Mahe, Seychelles

AS58001, RU IDEAL-SOLUTION
Malspam campaign: leverages Host-based & hybrid BPH
Path of malspam attack

1. Phishing email sent from delta@performanceair.com

2. Victims click on malicious URLs

   - myhearthstonehomes.org
   - ourrealtyguy.info
   - ourrealtyguy.org
   - ourrealtyguy.us
   - package2china.com

3. Malicious word doc drops Hancitor

4. Hancitor makes C2 call to domains for trojans
   - uneventrendi.com
   - ketofonerof.ru
   - thettertrefbab.ru

5. Trojans (Pony, Evil Pony, Zloader) make C2 call for extra malware or functionality

   - mebelucci.com.ua
   - uneventrendi.com
   - lycasofrep.com
   - rinbetarrab.com

6. Infection on device & positioned for data extraction
Malicious malspam campaign

From Delta Airlines Inc. <delta@performanceair.com>⭐
Subject Your order DELTA64377537 has been approved!
To ⭐

Dear client,

Your order has been processed and your credit card has been charged.
Please download and print your ticket by clicking here.

Please find your order details below.

FLIGHT NUMBER: DT3547138446US
ORDER#: DELTA64377537
CARD NUMBER: 4XXX-XXXX-XXXX-5741
CARD TYPE: VISA
AMOUNT CHARGED: 958.50

For more information regarding your order, contact us by visiting http://www.delta.com.

Thank you for flying with us
Delta Airlines

Reference hazmalware.wordpress.com
Spoofed email used in mailspam attack
Path of malspam attack

1. Phishing email sent from delta@performanceair.com

2. Victims click on malicious URLs

   myhearthstonehomes.org
   ourrealtyguy.info
   ourrealtyguy.org
   ourrealtyguy.us
   package2china.com
August 30: Peak of malicious redirect
Duration: 7 hour period

Attack took place between 14:00-21:00 UTC
Insight into the IP network

**myhearthstonehomes.org**

**IP Addresses**

<table>
<thead>
<tr>
<th>First seen</th>
<th>Last seen</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/14/17</td>
<td>9/14/17</td>
<td>184.168.221.49 (TTL: )</td>
</tr>
<tr>
<td>8/31/17</td>
<td>9/13/17</td>
<td>184.168.221.49 (TTL: 600)</td>
</tr>
<tr>
<td><strong>8/30/17</strong></td>
<td><strong>8/30/17</strong></td>
<td><strong>52.14.244.225 (TTL: 600)</strong></td>
</tr>
</tbody>
</table>
Details for 52.14.244.225

Hosting 0 malicious domains for 1 week

This IP is currently in the Umbrella block list as malware

Security Categories: Malware

Threat Types: Bulletproof Hosting

<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>Network Owner Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>52.14.0.0/16</td>
<td>AS 16509</td>
<td>AMAZON-02 - Amazon.com, Inc., US 86400</td>
</tr>
</tbody>
</table>
Known domains hosted by 52.14.244.225

agentssellingtips.info antoineandmuse.com apriadiana.com brookestonehousevalue.info centralflhousevalue.info

**heymamaradio.com** imap.antoineandmuse.com imap.centralflhousevalue.info imap.vetstuff.com myoutdoorchild.com

rexahunter.com susannahope.com thechristianblog.com verumpharmaceuticals.com whymovenow.info writerbloggers.com

greathomesellingtips.info newwestorangehomes.info package2china.com realestatetrueth.info vetstuff.com

wgopodcastbooking.com writerblogger.com www.agentssellingtips.info zasbiopharmaceuticals.com zasproperties.com

zasbiopharm.com zashealthsystems.com zasholdings.com zashealth.com lovelyflrealestate.com ourrealtyguy.org


myhearthstonehomes.info myhearthstonehomes.net myhearthstonehomes.org ourrealtyguy.info ourrealtyguy.net

ourrealtyguy.us www.myhearthstonehomes.info www.ourrealtyguy.org
This domain is associated with the following attack: Hancitor Dropper

This domain has a suspicious prefix score

This domain has a suspicious RIP score

Classifier prediction: suspicious

Umbrella risk score: 93

DNS queries
Insight into ‘heymamaradio.com’ malicious IP hosting

<table>
<thead>
<tr>
<th>First seen</th>
<th>Last seen</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/5/17</td>
<td>9/5/17</td>
<td><strong>185.180.231.238</strong> (TTL: 600) <strong>47.91.75.193</strong> (TTL: 600) <strong>54.87.201.155</strong> (TTL: 600)</td>
</tr>
<tr>
<td>9/4/17</td>
<td>9/4/17</td>
<td><strong>185.180.231.238</strong> (TTL: 600) <strong>52.14.244.225</strong> (TTL: 600) <strong>54.84.39.209</strong> (TTL: 600) <strong>54.87.201.155</strong> (TTL: 600)</td>
</tr>
<tr>
<td>8/31/17</td>
<td>9/3/17</td>
<td><strong>52.14.244.225</strong> (TTL: 600) <strong>54.84.39.209</strong> (TTL: 600)</td>
</tr>
<tr>
<td>8/30/17</td>
<td>8/30/17</td>
<td><strong>52.14.244.225</strong> (TTL: 600)</td>
</tr>
<tr>
<td>8/29/17</td>
<td>8/29/17</td>
<td><strong>185.197.72.17</strong> (TTL: 600) <strong>47.74.150.46</strong> (TTL: 600)</td>
</tr>
</tbody>
</table>
WHOIS information of myhearthstonehomes.org

- **Registrar Name**: GoDaddy.com, LLC
- **IANA ID**: 146
- **Creation Date**: November 16, 2015
- **Last Updated**: August 30, 2017
- **Expiration Date**: November 16, 2018

**Email Address**: john@liveingarnetvalley.net
- **Associated Domains**: 17 Total - 7 malicious
- **Email Type**: Administrative, Registrant, Technical
- **Last Observed**: Current

**Nameserver** list includes:
- ns70.domaincontrol.com
- ns69.domaincontrol.com
- **Associated Domains**: Greater than 500 Total
- **Last Observed**: Current
## Domains Associated with john@liveingarnetvalley.net

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Security Categories</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>myhearthstonehomes.info</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>myhearthstonehomes.net</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>myhearthstonehomes.org</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>ourrealtyguy.info</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>ourrealtyguy.net</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>ourrealtyguy.net</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>ourrealtyguy.org</td>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>ourrealtyguy.us</td>
<td>Malware</td>
<td></td>
</tr>
</tbody>
</table>
Details for ourrealtyguy.info

This domain is currently in the Umbrella block list

This domain is associated with the following attack: Locky Ransomware

DNS queries

1,500
1,000
500

DNS queries/hour

Related domains tied to the same malspam campaign

<table>
<thead>
<tr>
<th>Domain</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.delta.com">www.delta.com</a></td>
<td>18</td>
</tr>
<tr>
<td>a1.verisigndns.com</td>
<td>14</td>
</tr>
<tr>
<td>a3.verisigndns.com</td>
<td>10</td>
</tr>
<tr>
<td>a.dnspod.com</td>
<td>10</td>
</tr>
<tr>
<td>a2.verisigndns.com</td>
<td>10</td>
</tr>
<tr>
<td>b.dnspod.com</td>
<td>9</td>
</tr>
<tr>
<td>c.dnspod.com</td>
<td>9</td>
</tr>
<tr>
<td>mx00.1and1.com</td>
<td>4</td>
</tr>
<tr>
<td>mx01.1and1.com</td>
<td>4</td>
</tr>
<tr>
<td>myhearthstonehomes.net</td>
<td>4</td>
</tr>
<tr>
<td>ourrealtyguy.net</td>
<td>4</td>
</tr>
<tr>
<td>ourrealtyguy.org</td>
<td>3</td>
</tr>
</tbody>
</table>
Malspam internet infrastructure uncovered by Investigate

1. performanceair.com
   Stage 1

2. www.ourrealtguy.org
   Domains on same IP

3. 52.14.244.225
   IP / ALEX

4. heymamaradio.com
   Mal. domains on same IP

5. 47.74.150.46
   Changing IP hosting / ALEX

6. john@liveingarnetvalley.net
   WHOIS

7. myhearthstonehomes.org
   Starting domain

8. myhearthstonehomes.net
   Domains reg. to same email

9. 100c3ee0008...
   File hash

10. uneventrendi.com
    Network connection

11. 217.197.116.46
    Hosted on small time BPH or rogue hosters
TTPs across a dozen malspam campaigns

**Campaign 1**
- performanceair.com
- myhearthstonehomes.org
- thettertrefbab.ru
- mebelucci.com.ua
- uneventrendi.com
- lycasofrep.com

**Campaign 2**
- uspackagers.com
- downetwpnj.net
- Hedtfortedlet.ru
- crabbiesfruits.com
- orcateheck.com
- rebjusjohed.com
Our other related work

- Virus Bulletin 2017
- Defcon 2017 [https://www.youtube.com/watch?v=AbJCOVLQbjs](https://www.youtube.com/watch?v=AbJCOVLQbjs)
- Black Hat 2017
- Usenix Enigma 2017 [https://www.youtube.com/watch?v=ep2gHQgjYTt&t=818s](https://www.youtube.com/watch?v=ep2gHQgjYTt&t=818s)
- Black Hat 2016 [https://www.youtube.com/watch?v=m9yqnwuqSk](https://www.youtube.com/watch?v=m9yqnwuqSk)
- RSA 2016 [https://www.rsaconference.com/events/us16/agenda/sessions/2336/using-large-scale-data-to-provide-attacker](https://www.rsaconference.com/events/us16/agenda/sessions/2336/using-large-scale-data-to-provide-attacker)
- BruCon 2015 [https://www.youtube.com/watch?v=8edBgoHXwng](https://www.youtube.com/watch?v=8edBgoHXwng)
- Botconf 2014
- Virus Bulletin 201 [https://www.virusbtn.com/conference/vb2014/abstracts/Mahjoub.xml](https://www.virusbtn.com/conference/vb2014/abstracts/Mahjoub.xml)
- Black Hat 2014 [https://www.youtube.com/watch?v=UG4ZUaWDXs](https://www.youtube.com/watch?v=UG4ZUaWDXs)
Thank you

Dhia Mahjoub, dmahjoub@cisco.com, @DhiaLite

Acknowledgements

Atheana Altayyar
Austin McBride
Sarah Brown