Cisco Umbrella

# 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

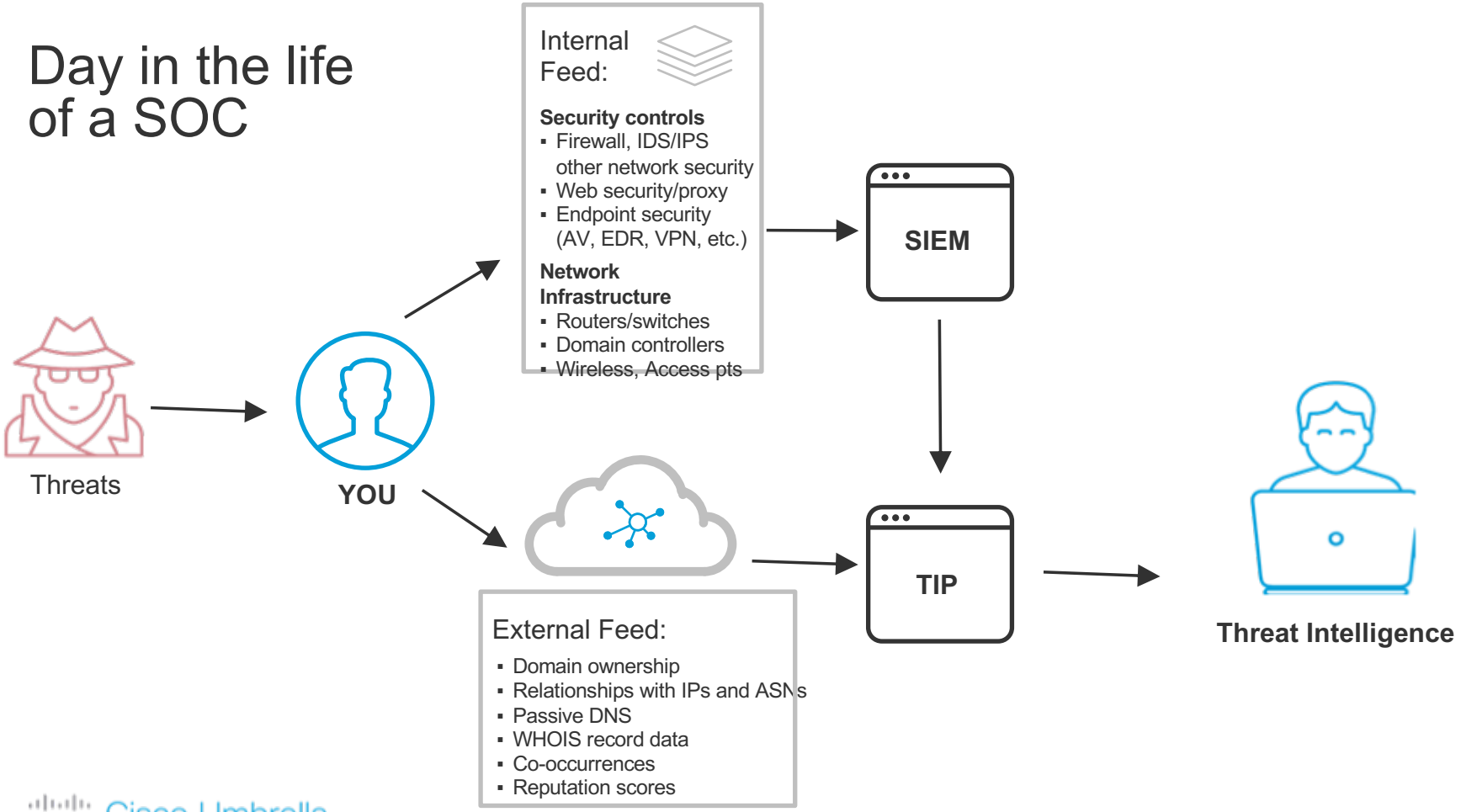
3. BPH behind current malspam campaigns

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



# 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)

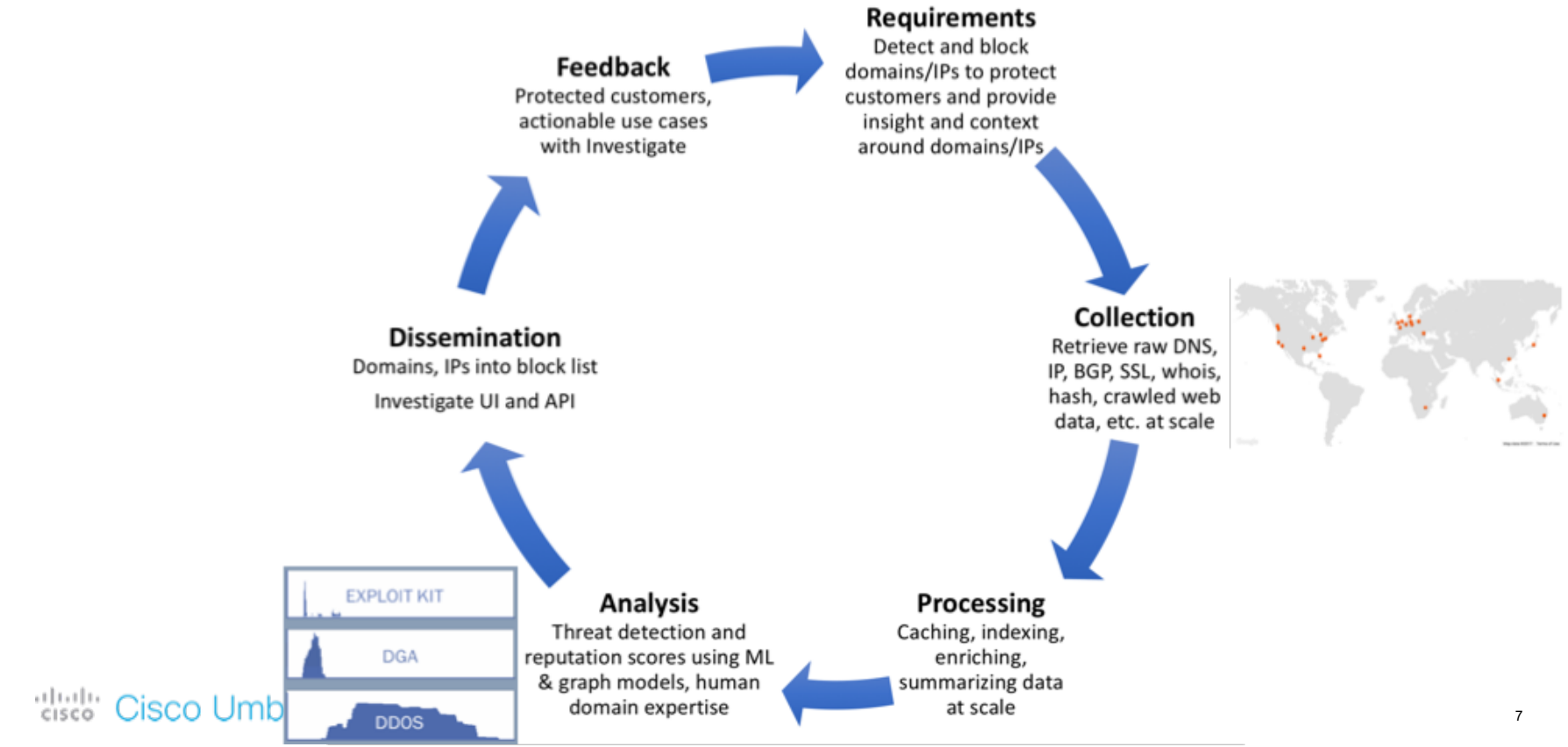
**Tactical Intelligence** includes IOCs and tactics that help drive the security of an organization and enable it to hunt and respond to threats

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

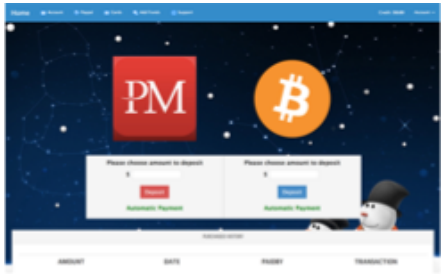
# Know your adversary

## Uncovering Criminal Hosting infrastructures

# Umbrella Investigate Intel Production Cycle



# Threat Landscape

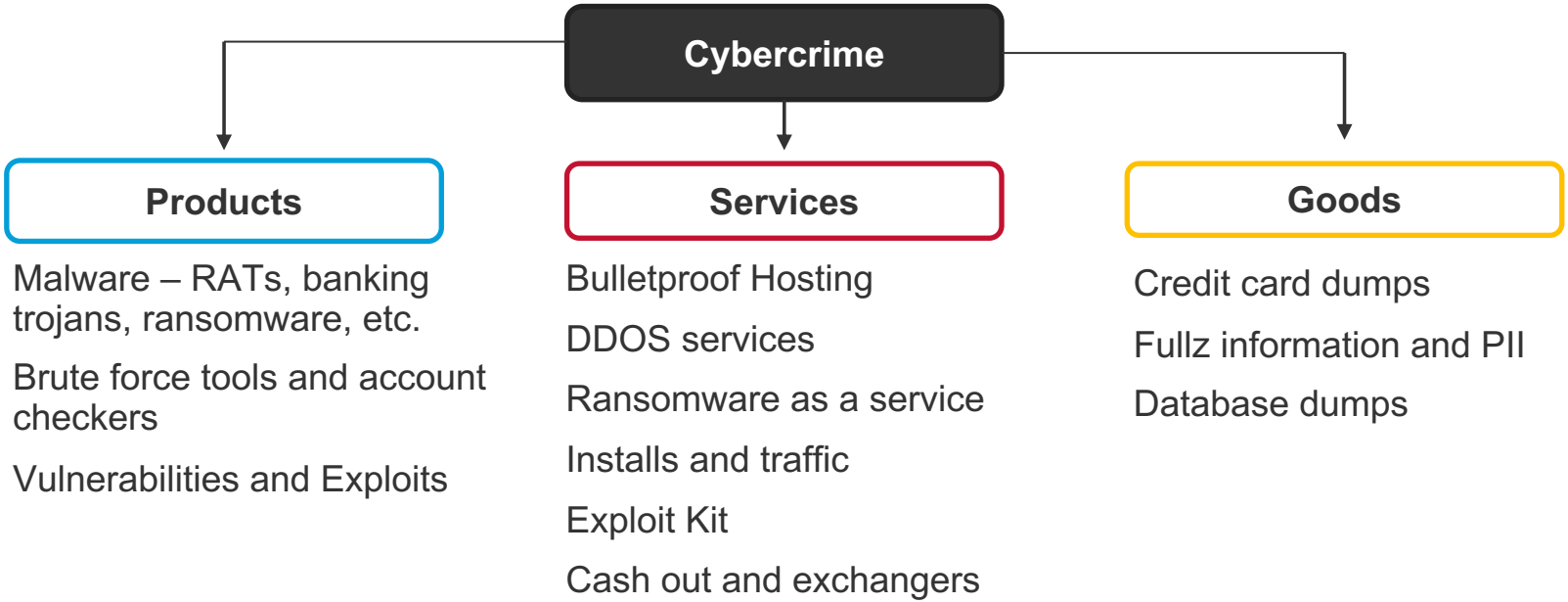





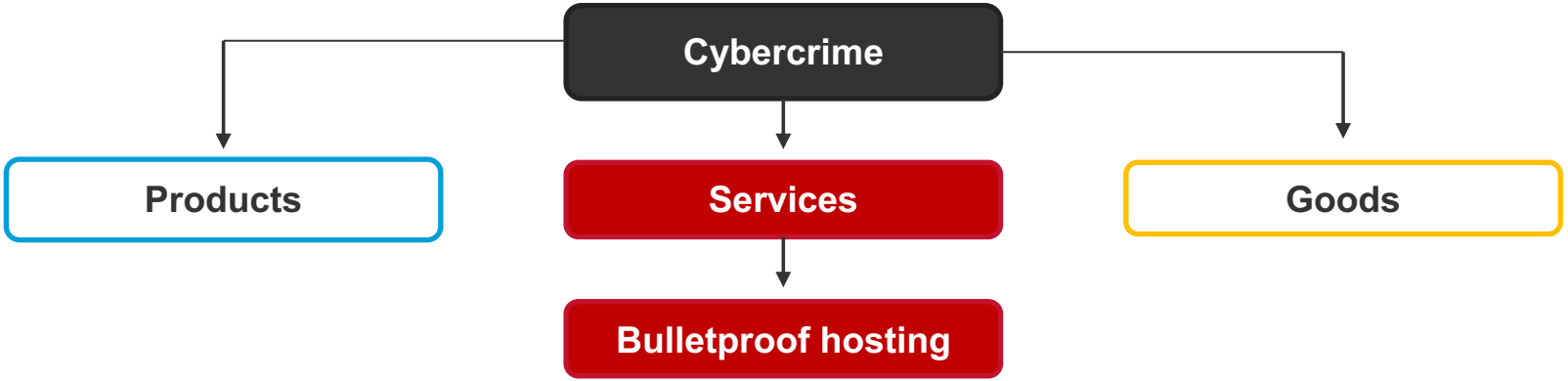



Cisco Umbrella

# Cybercrime Ecosystem



# BulletProof Hosting



# Bulletproof hosting provider (BPH)

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

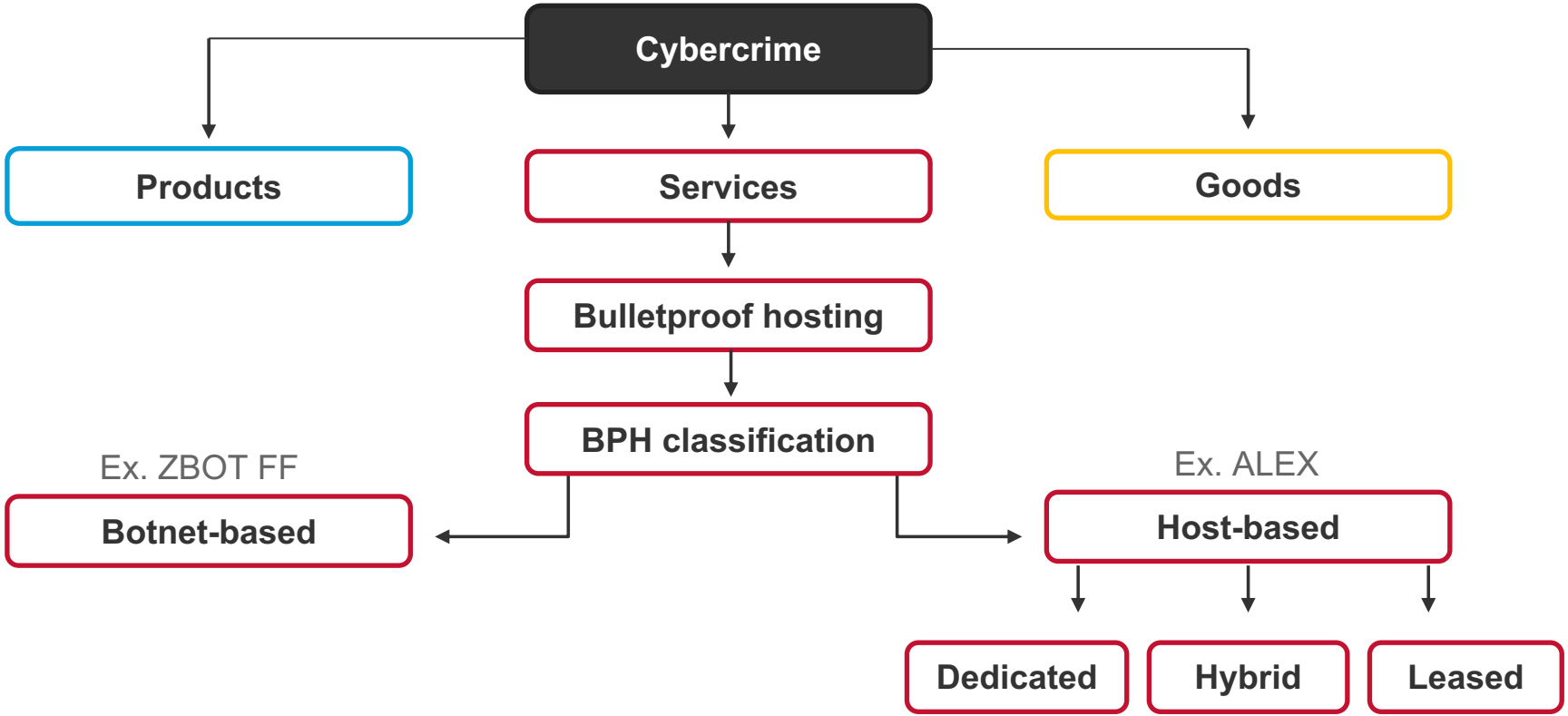
# Spectrum of Hosting Providers


Good

Abused

Bulletproof

# A Taxonomy of BulletProof Hosting



# 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

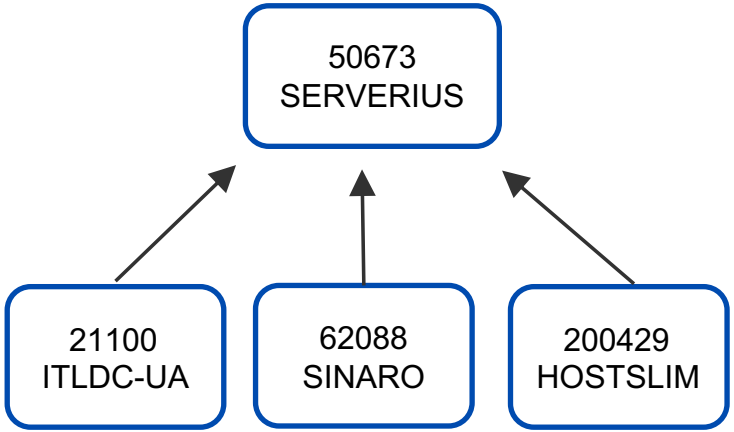
Anonymous payment methods

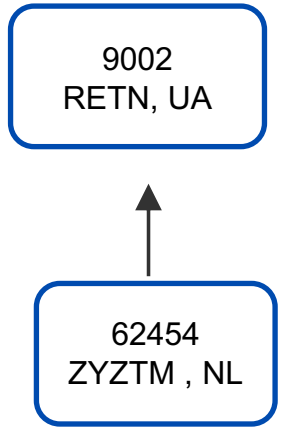
Small IP range

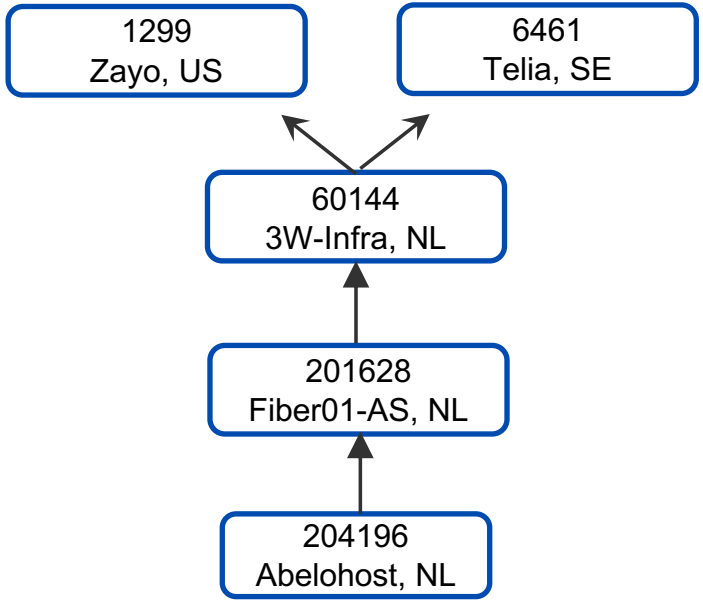
Toxic hosted content or outgoing traffic

# Leaf (Stub) ASN or leaf ASNs chain

Have only upstream peers, no downstream
Frequent pattern for questionable/bulletproof hosters

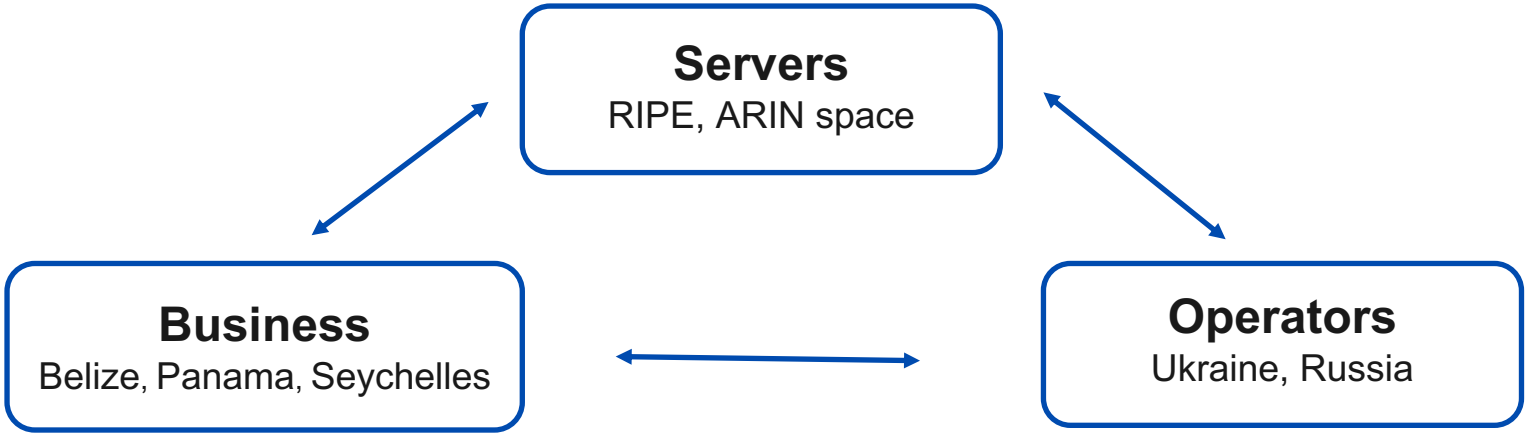


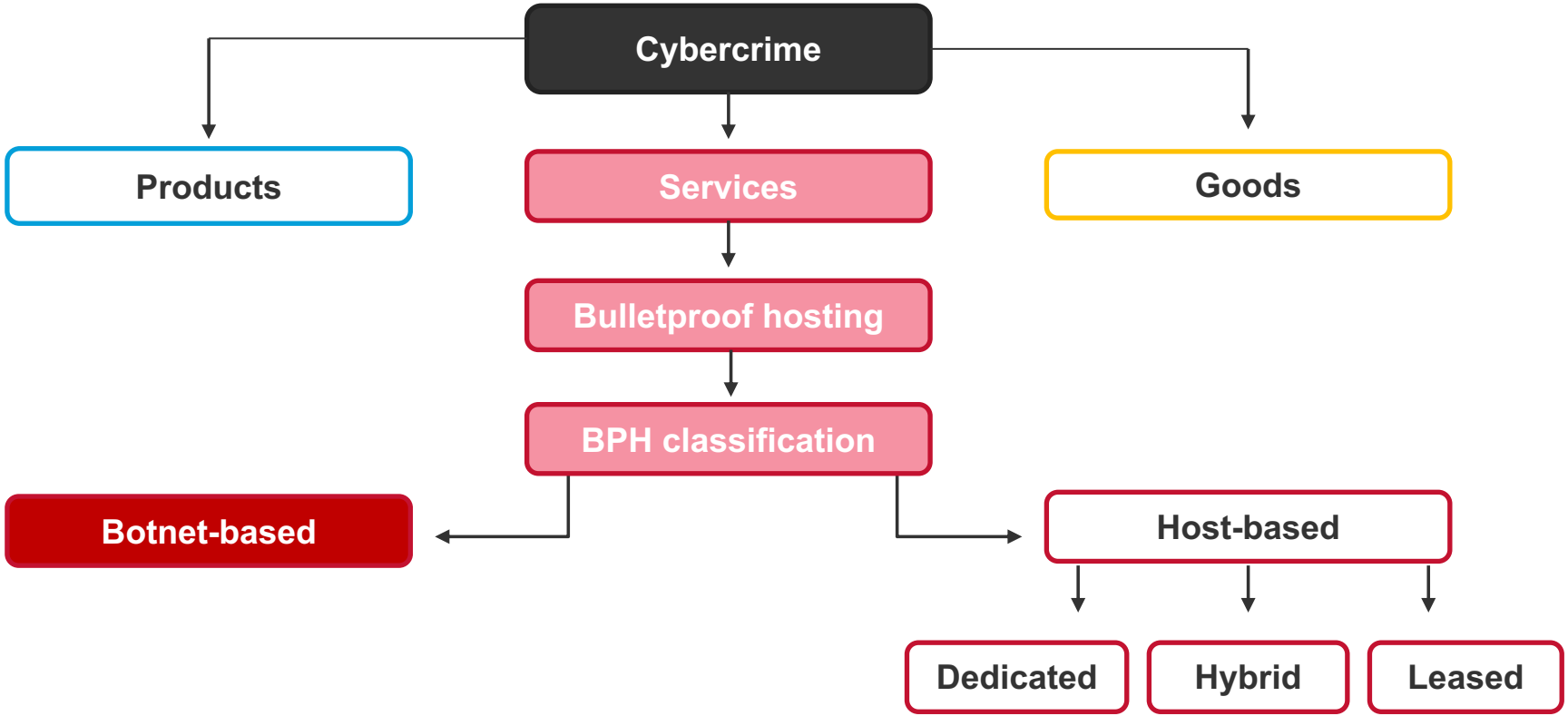
# Register Business in Offshore Jurisdictions

# Multiple Layers of Resistance



# Major BPH operations

# Botnet-based BPH



# ZBot Fast Flux BPH Operation

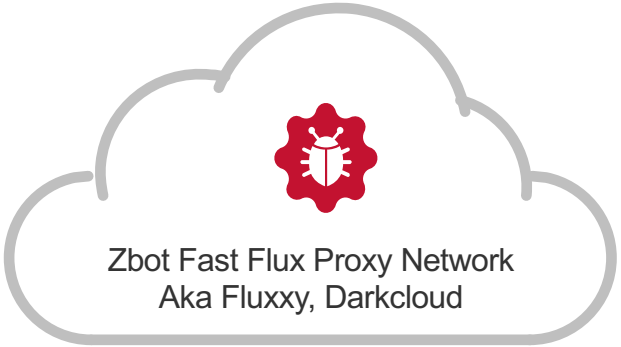
Introduced at Black Hat 2014,
Botconf 2014, Defcon 2017

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

Victim

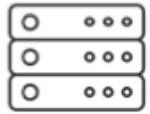
Crimeware consumer

Researcher




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

40-50 bot IPs
provisioned per domain

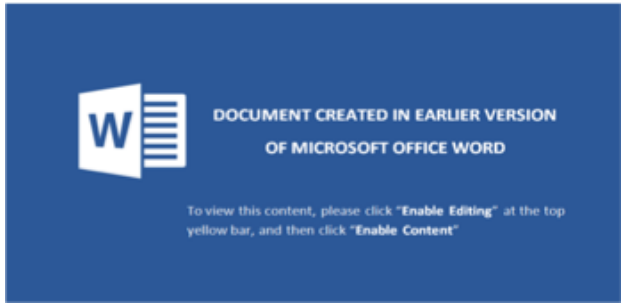


Criminal customer's
site origin IP

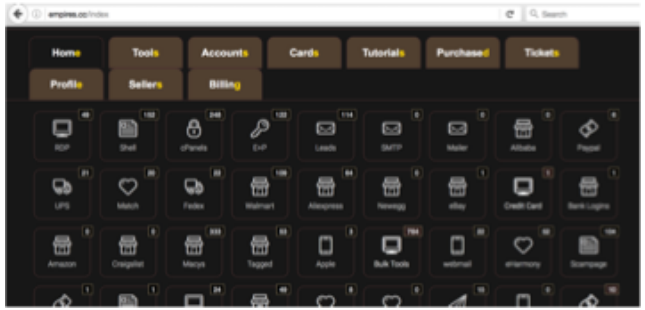
Content delivered
Short lifetime: malware, ransomware
Medium lifetime: phishing
Long lifetime: carding, cybercrime forums

Cisco Umbrella

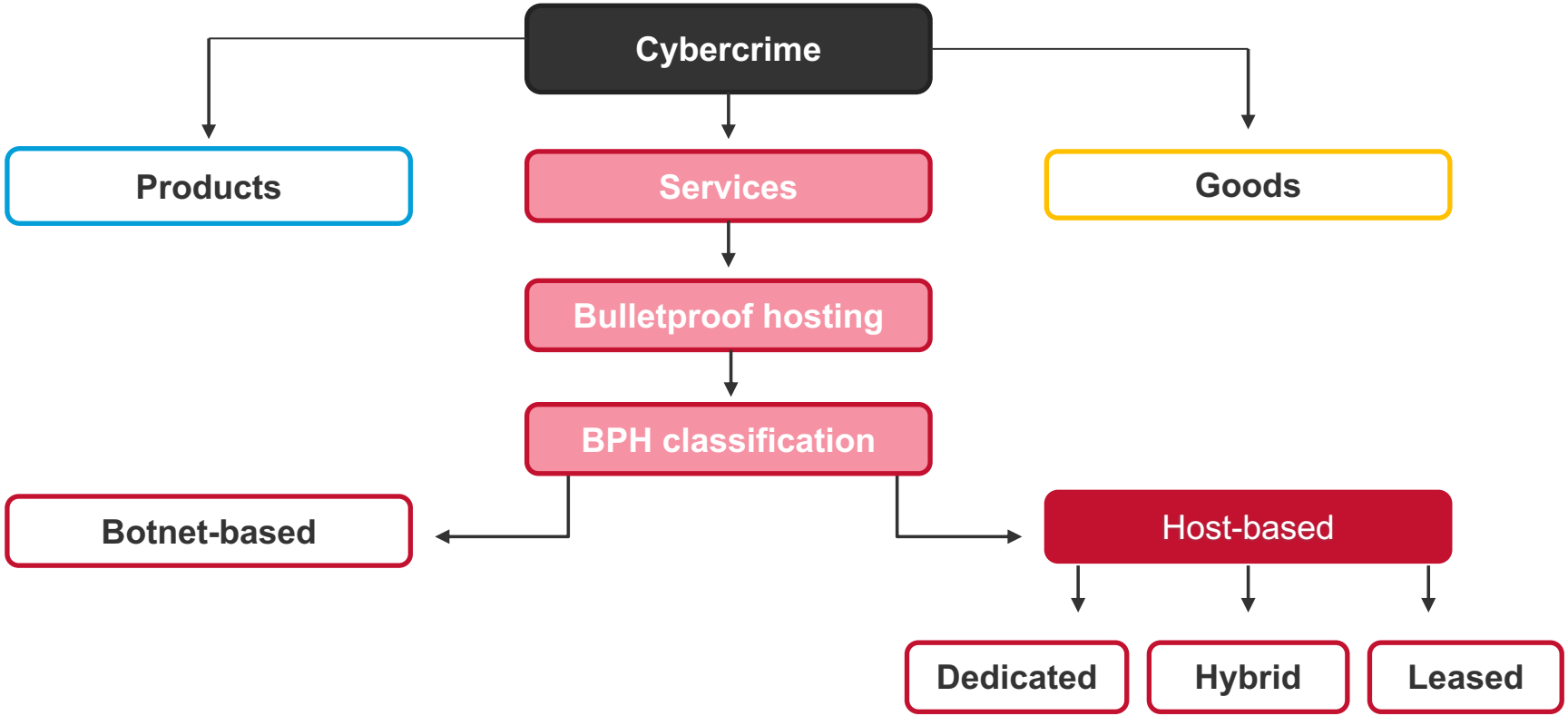
# Threats delivered by ZBot Fast Flux network



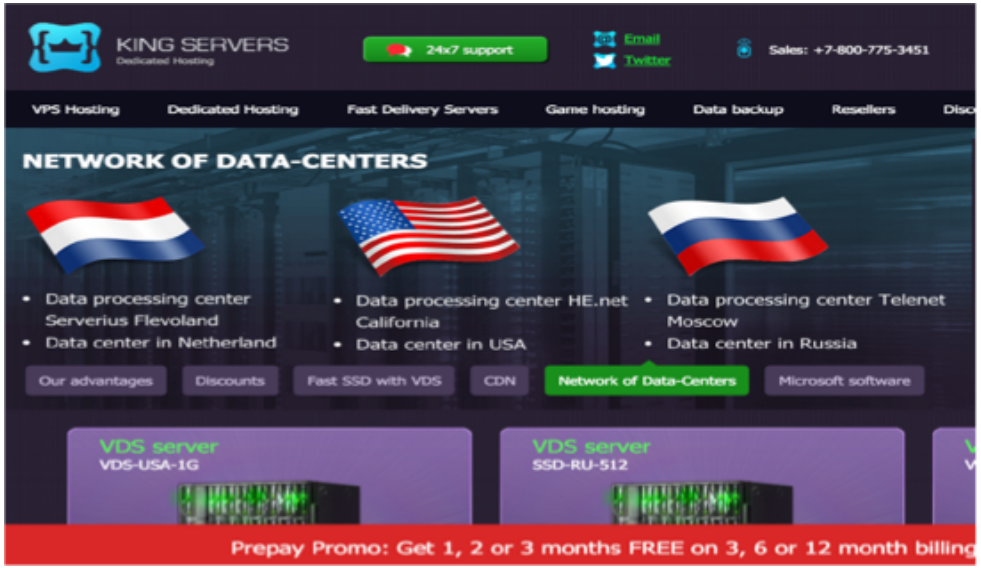





# Host-based BPH



# 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

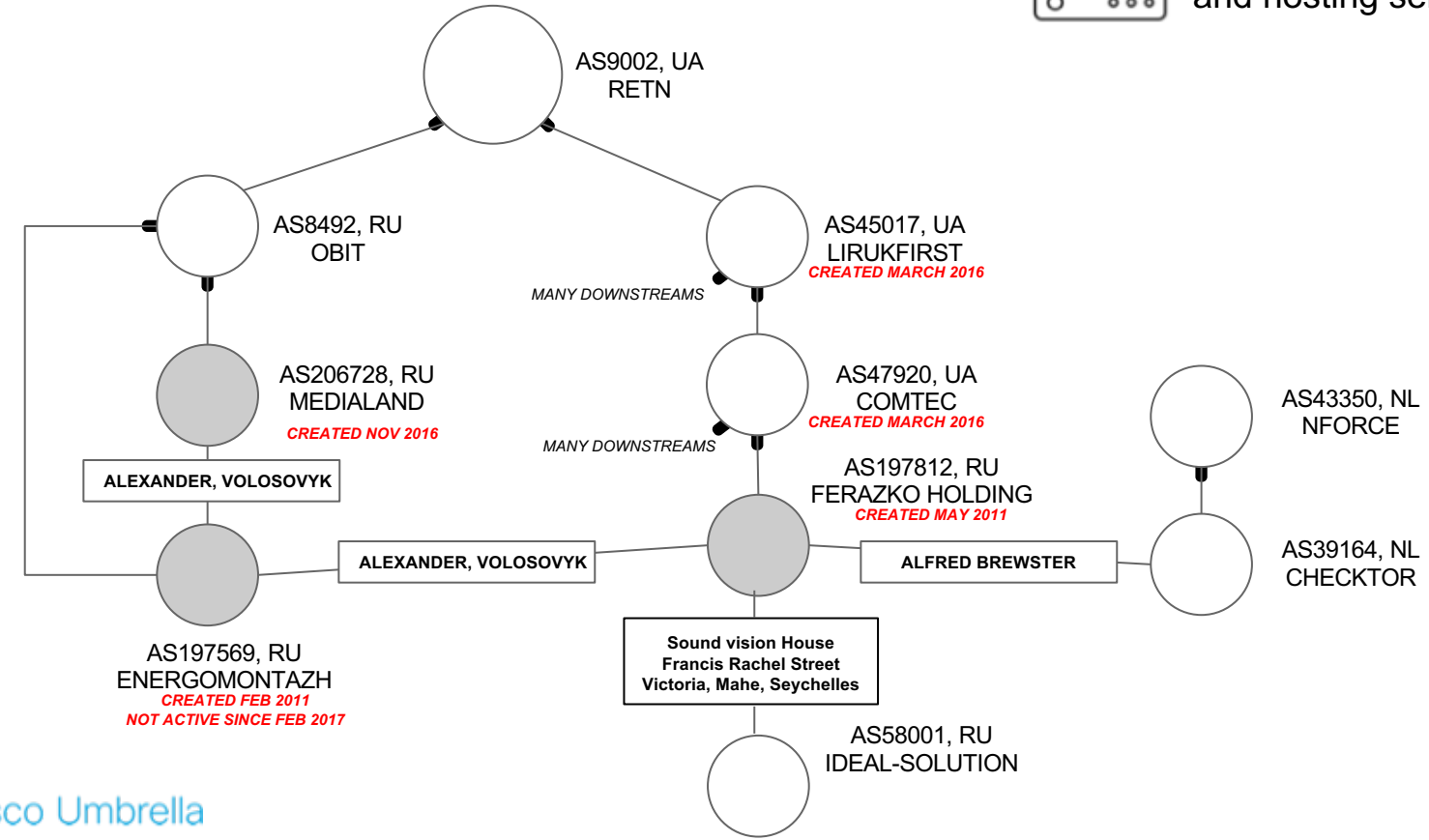
Phishing

Crimeware forums

Credit card dump shops

# Alex's Network Infrastructure

Abused third party cloud and hosting services



# 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

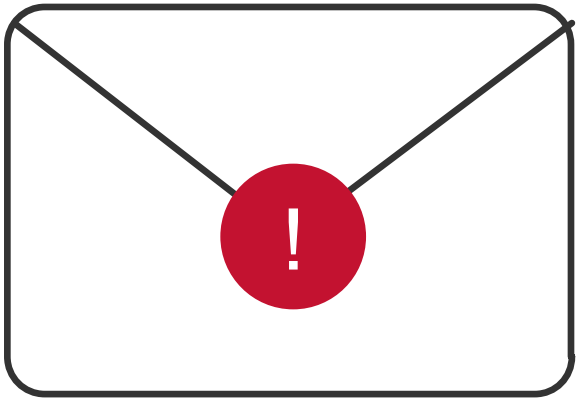
5 **Trojans (Pony, Evil Pony, Zloader) make C2 call for extra malware or functionality**

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

6 **Infection on device & positioned for data extraction**

Cisco Umbrella

# Malicious malspam campaign



From Delta Airlines Inc. <delta@performanceair.com>
Subject **Your order DELTA64377537 has been approved!** 1:08 PM
To [redacted]

Dear client,

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

Please find your order details below.

FLIGHT NUMBER : DT3547138446US
ORDER# : DELTA64377537
DATE : Wed, 30 Aug 2017 13:08:26 -0400
CARD NUMBER : 4XXX-XXXX-XXXX-5741
CARD TYPE : VISA
AMOUNT CHARGED : 958.50

MALDOC URL

hxxp://myhearthstonehomes[.]org/i.php?d=

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

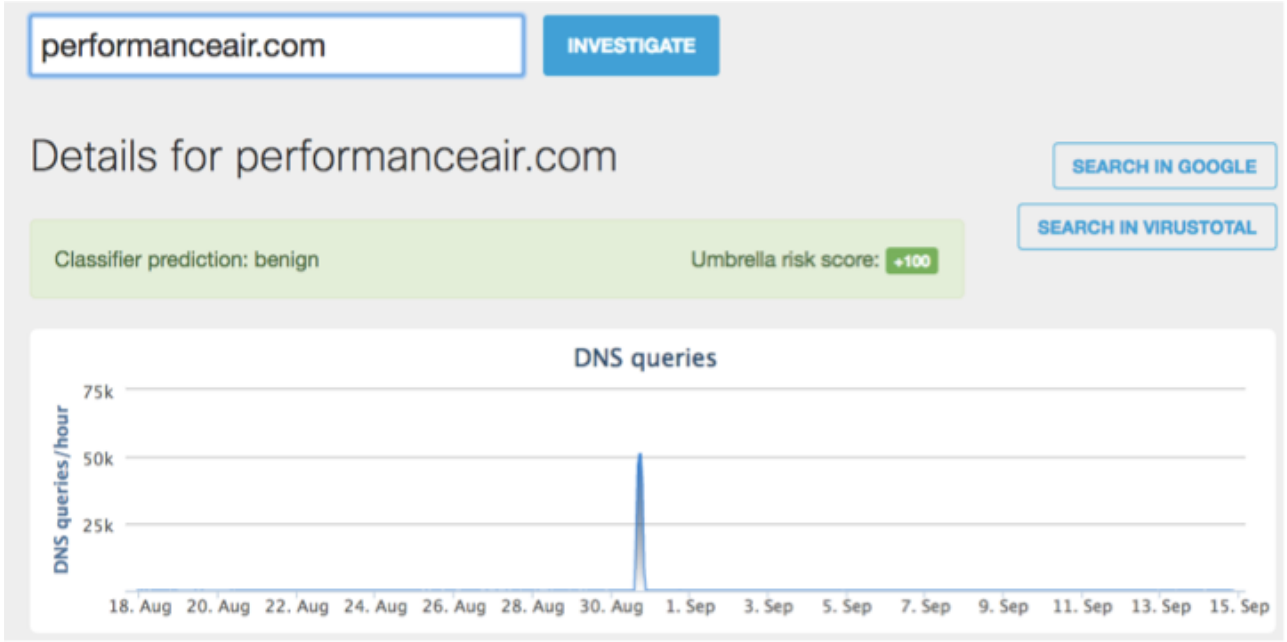
Thank you for flying with us
Delta Airlines



Reference hazmalware.wordpress.com

# performanceair.com

Spoofed email used in mailspam attack



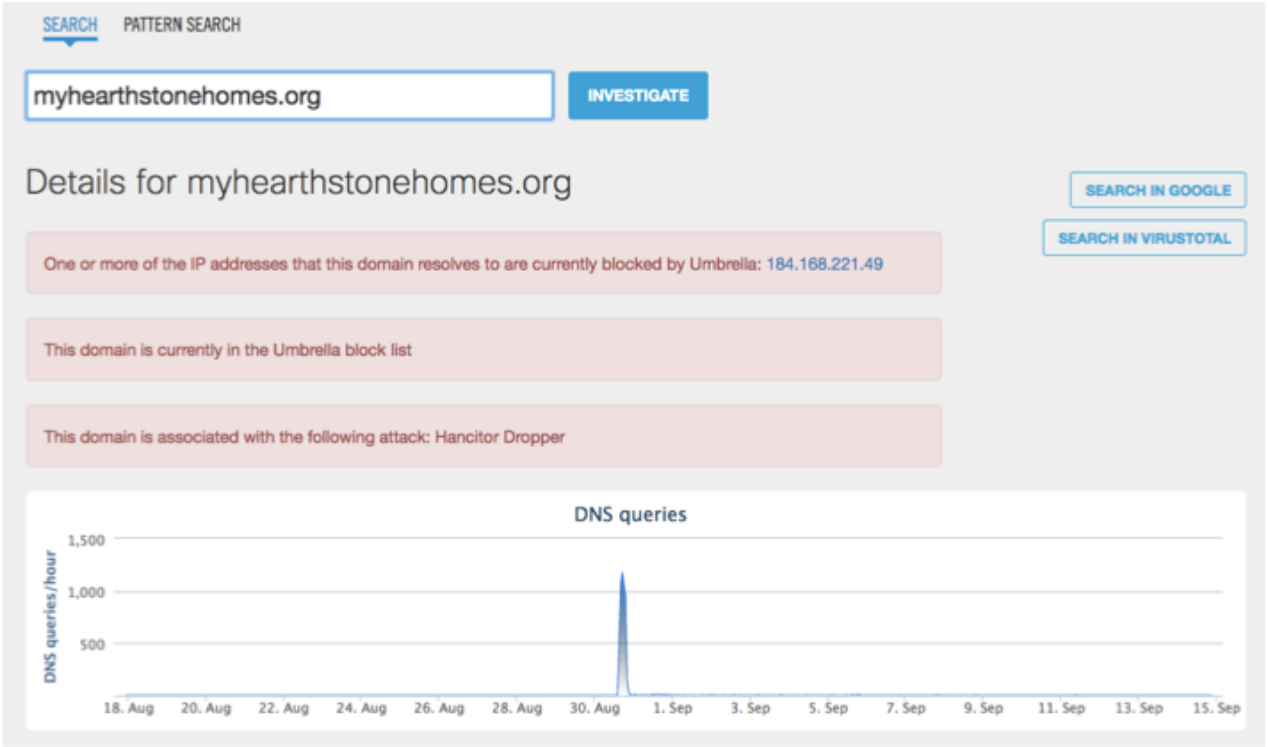
# Path of malspam attack

1. **Phishing email sent from delta@performanceair.com**

2. **Victims click on malicious URLs**

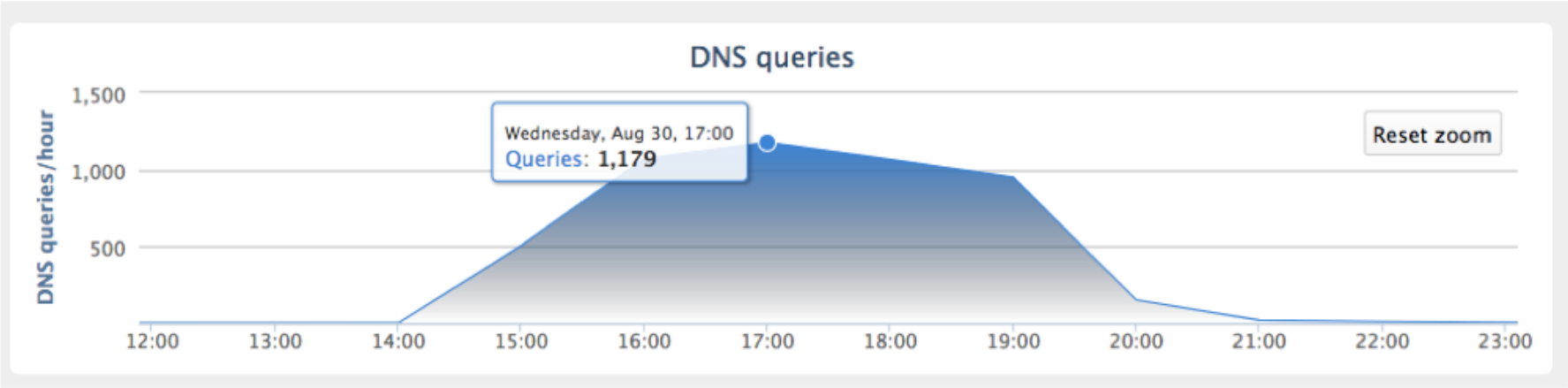
myhearthstonehomes.org
ourrealtyguy.info
ourrealtyguy.org
ourrealtyguy.us
package2china.com

# August 30: Peak of malicious redirect

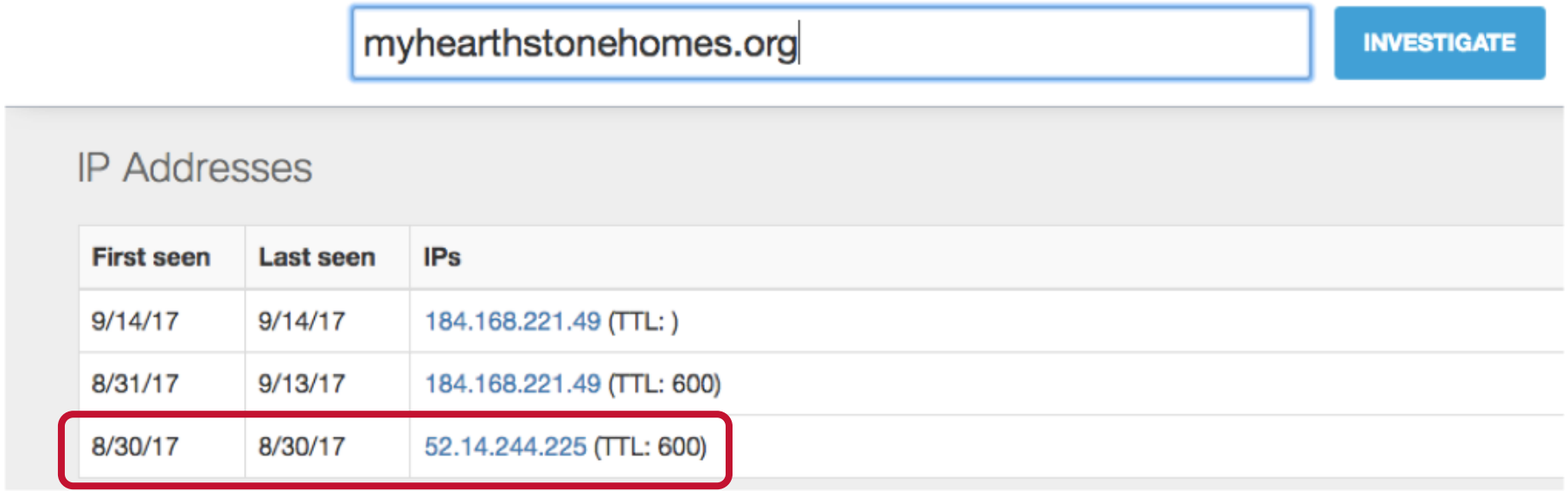


# Duration: 7 hour period

Attack took place between 14:00-21:00 UTC



# Insight into the IP network



# 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

## AS

| Prefix | ASN | Network Owner Description |
|---|---|---|
| 52.14.0.0/16 | AS 16509 | AMAZON-02 - Amazon.com, Inc., US 86400 |

# Known malicious domains on the same IP

## Known domains hosted by 52.14.244.225

agentssellingtips.info antoineandmuse.com apadriana.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
www.heymamaradio.com www.zashealth.com zaspharma.com zassys.com accuratewindermerehousevalue.info
greathomesellingtips.info newwestorangehomes.info package2china.com realestatetruth.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
protectorsuperhero.com www.lovelyflrealestate.com www.realestatetruth.info www.zasholdings.com www.zasproperties.com
myhearthstonehomes.info myhearthstonehomes.net myhearthstonehomes.org ourrealtyguy.info ourrealtyguy.net
ourrealtyguy.us www.myhearthstonehomes.info www.ourrealtyguy.org

heymamaradio.com

INVESTIGATE

BACK TO TOP

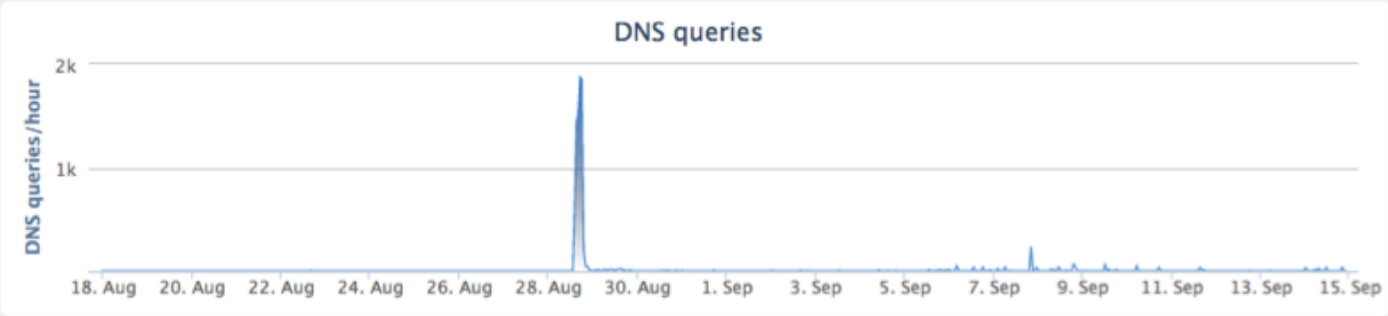
This domain is associated with the following attack: Hancitor Dropper

This domain has a suspicious prefix score

This domain has a suspicious RIP score

Classifier prediction: suspicious

Umbrella risk score: -83



# Insight into ‘heymamaradio.com’ malicious IP hosting

## IP Addresses

| First seen | Last seen | IPs |
|---|---|---|
| 9/5/17 | 9/5/17 | 185.180.231.238 (TTL: 600) 47.91.75.193 (TTL: 600) 54.87.201.155 (TTL: 600) |
| 9/4/17 | 9/4/17 | 185.180.231.238 (TTL: 600) 52.14.244.225 (TTL: 600) 54.84.39.209 (TTL: 600) 54.87.201.155 (TTL: 600) |
| 8/31/17 | 9/3/17 | 52.14.244.225 (TTL: 600) 54.84.39.209 (TTL: 600) |
| 8/30/17 | 8/30/17 | 52.14.244.225 (TTL: 600) |
| 8/29/17 | 8/29/17 | 185.197.72.17 (TTL: 600) 47.74.150.46 (TTL: 600) |

# WHOIS information of myhearthstronehomes.org

myhearthstonehomes.org INVESTIGATE BACK TO TOP

## WHOIS Record Data

**Registrar Name:** GoDaddy.com, LLC **IANAID:** 146 Last retrieved August 31, 2017 GET LATEST

**Created:** November 16, 2015 **Updated:** August 30, 2017 **Expires:** November 16, 2018

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

| Nameserver | Associated Domains | Last Observed |
|---|---|---|
| ns70.domaincontrol.com | Greater than 500 Total | Current |
| ns69.domaincontrol.com | Greater than 500 Total | Current |

Show past data **Showing 2 of 4 Results**

Show more WHOIS data

# Domains Associated with john@liveingarnetvalley.net

| Domain Name | Security Categories | Conte |
|---|---|---|
| myhearthstonehomes.info | Malware | |
| myhearthstonehomes.net | Malware | |
| myhearthstonehomes.org | Malware | |
| ourrealtyguy.info | Malware | |
| ourrealtyguy.net | Malware | |
| ourrealtyguy.org | Malware | |
| ourrealtyguy.us | Malware | |

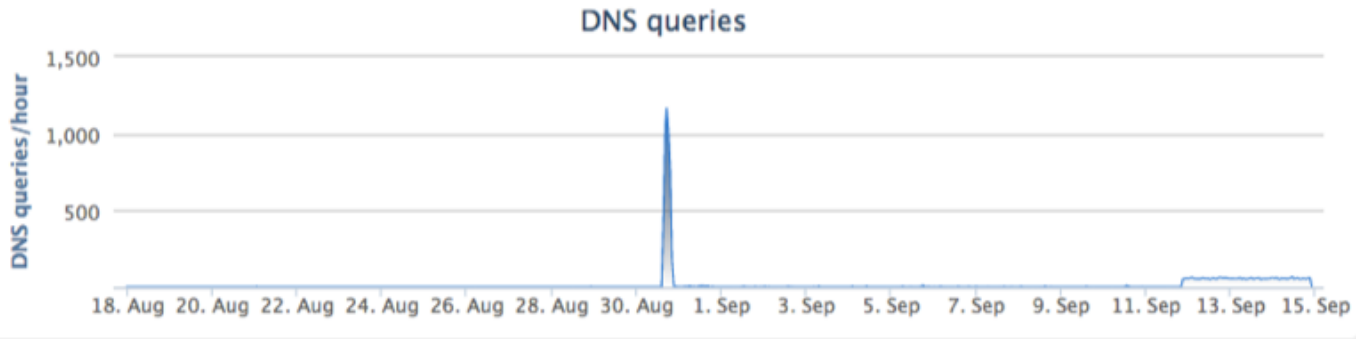
# Details for ourrealtyguy.info

This domain is currently in the Umbrella block list

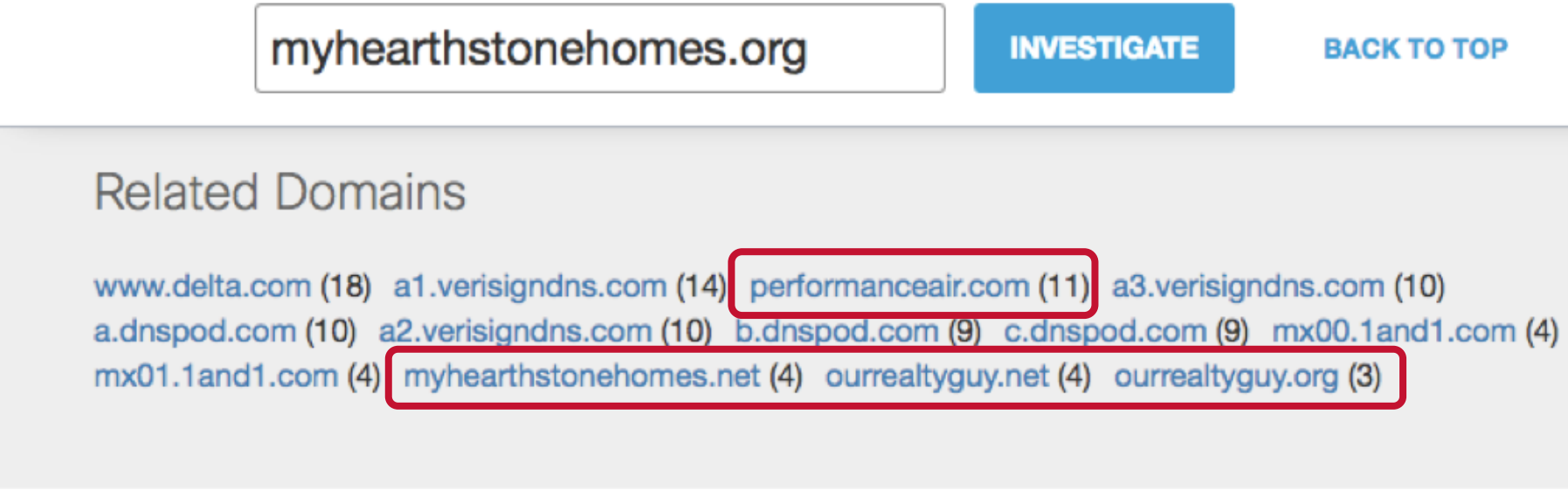
This domain is associated with the following attack: Locky Ransomware

SEARCH IN GOOGLE

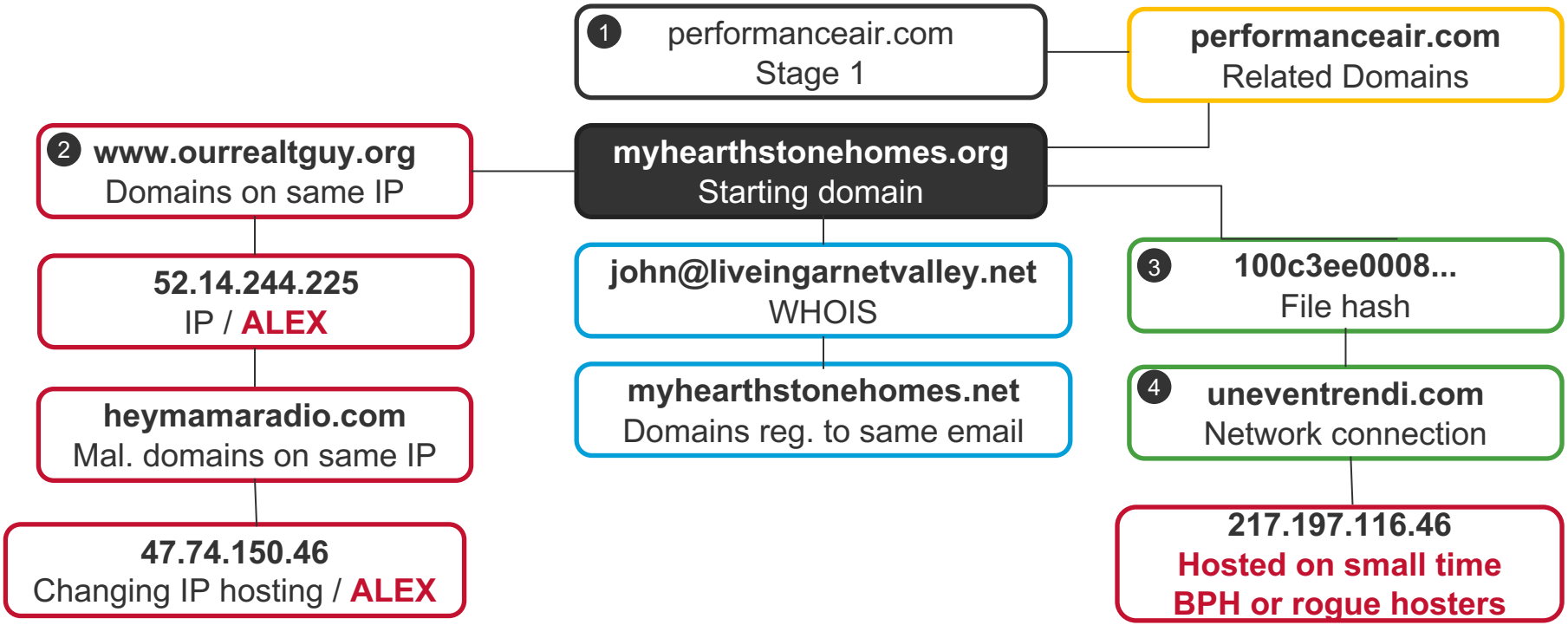
SEARCH IN VIRUSTOTAL



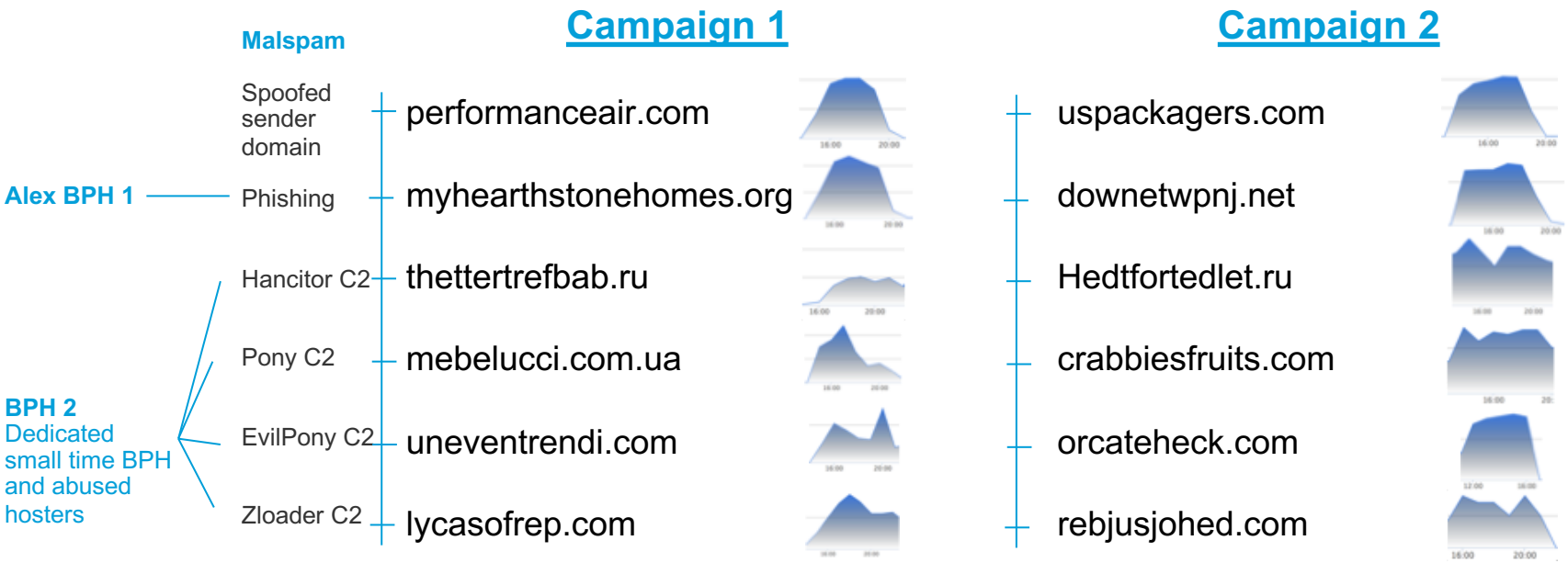
# Related domains tied to the same malspam campaign



# Malspam internet infrastructure uncovered by Investigate



# TTPs across a dozen malspam campaigns



# Our other related work

- Virus Bulletin 2017
- Defcon 2017 https://www.youtube.com/watch?v=AbJCOVLQbjs
- Black Hat 2017
- Usenix Enigma 2017 https://www.youtube.com/watch?v=ep2gHQgjYTs&t=818s
- Black Hat 2016 https://www.youtube.com/watch?v=m9yqnwuqdSk
- RSA 2016 https://www.rsaconference.com/events/us16/agenda/sessions/2336/using-large-scale-data-to-provide-attacker
- BruCon 2015 https://www.youtube.com/watch?v=8edBgoHXnwg
- Botconf 2014
- Virus Bulletin 201 https://www.virusbtn.com/conference/vb2014/abstracts/Mahjoub.xml
- Black Hat 2014 https://www.youtube.com/watch?v=UG4ZUaWDXSs

# Thank you

Dhia Mahjoub, dmahjoub@cisco.com, @DhiaLite

**Acknowledgements**

Atheana Altayyar
Austin McBride
Sarah Brown