Anatomy of an Attack

And How to Stay Ahead with Cisco and Splunk

Victor Pichs & Jan Dembowski

September 2018

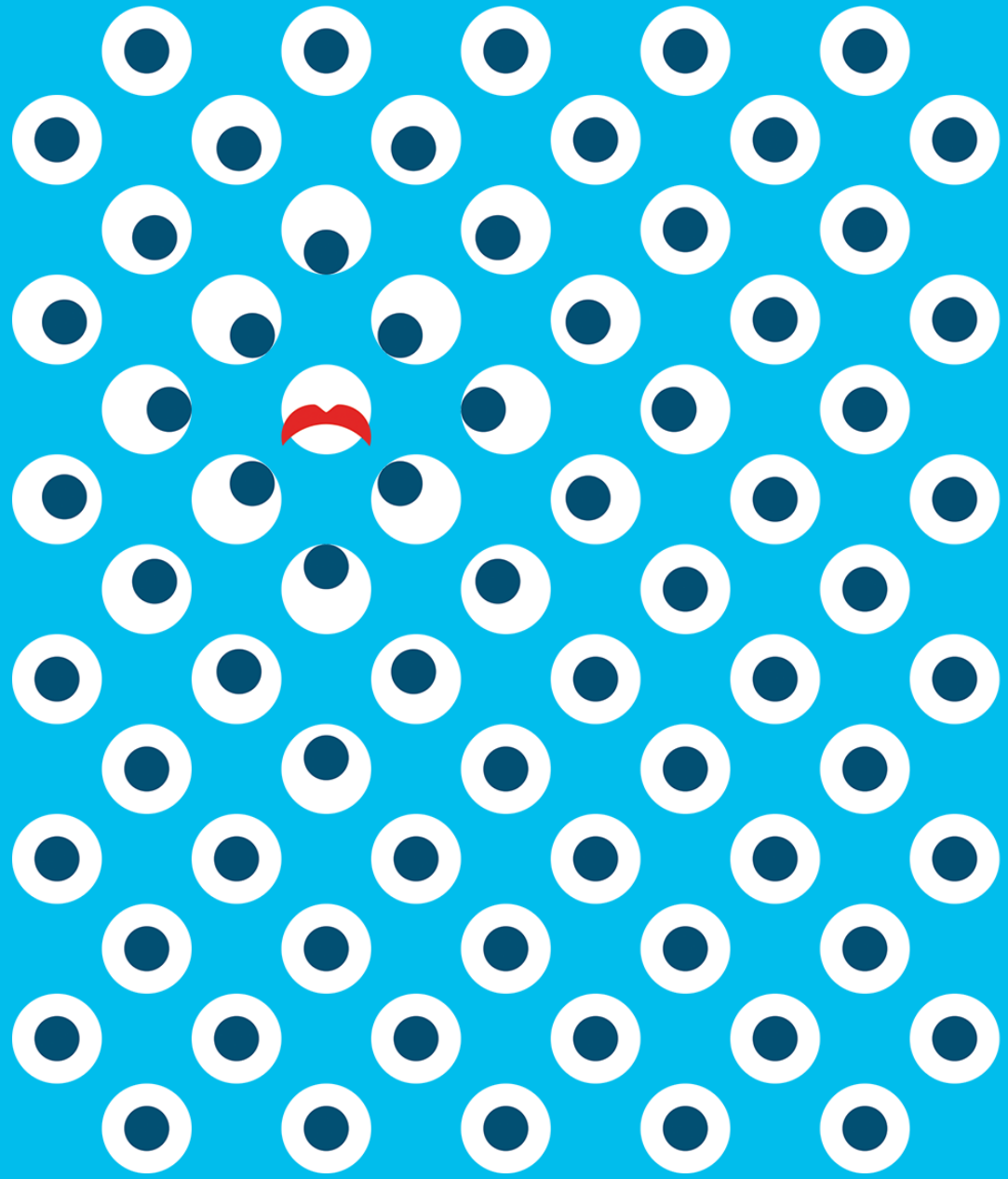
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

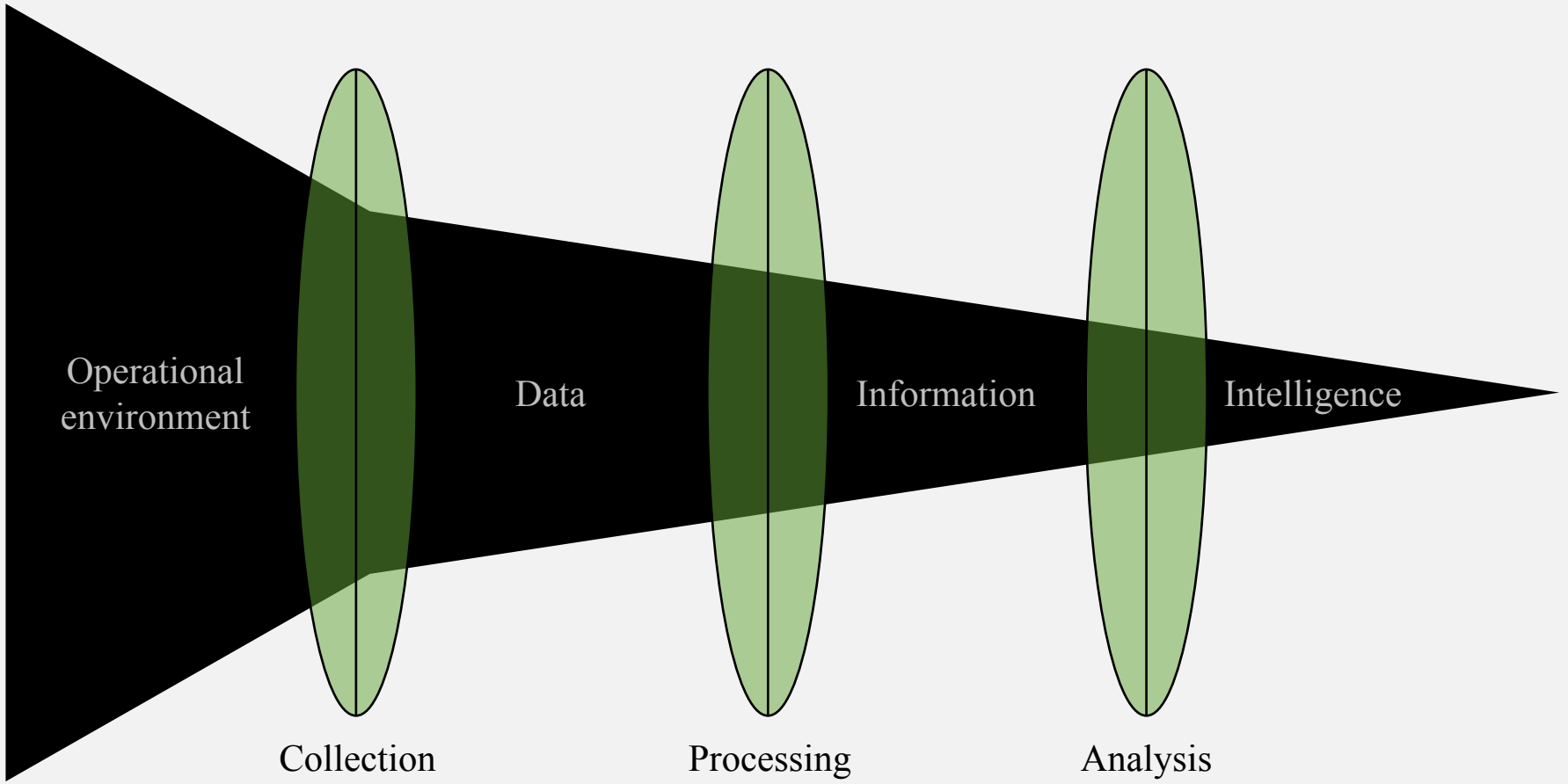
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Raw data does not equal threat intelligence



Relationship Of Data, Information, and Intelligence



Source: Joint Intelligence/Joint Publication 2.0 (Joint Chiefs of Staff)

Umbrella's view of the internet

125B
requests per day

90M
daily active users

16K
enterprise customers

160+
countries worldwide

Know Your Enemy

Cybercrime – Products, Services, and Goods

Products

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

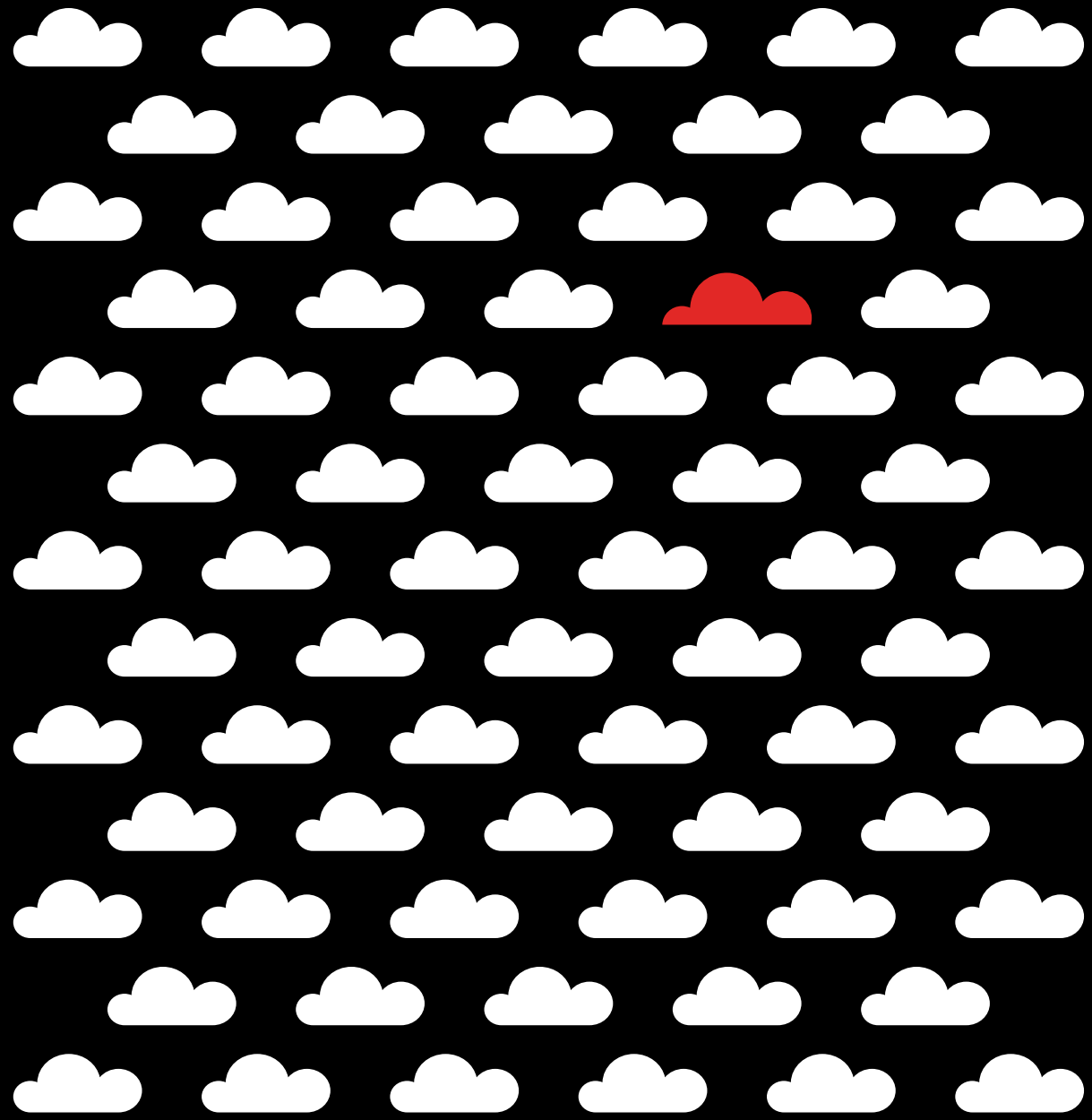
Services

- Bullet Proof 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

Malspam Campaign: Host-based & Hybrid BPH



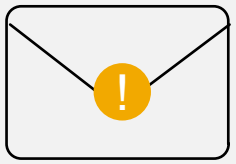
Alex BPH harvests a variety of toxic content

- Malware
- Ransomware
- Phishing
- Crimeware forums
- Credit card dump shops

Path Of Malspam Attack

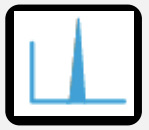
Phishing

1. Phishing email sent from delta@performanceair.com

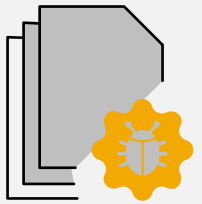


- Victims click on malicious URLs

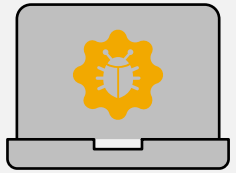
myhearthstonehomes.org
ourrealtyguy.info
ourrealtyguy.org
ourrealtyguy.us
package2china.com



- Malicious word doc drops Hancitor



- Infection on device and positioned for data extraction



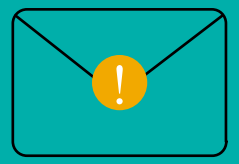
- Trojans (Pony, Evil Pony, Zloader) make C2 call for extra malware or functionality

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

- Hancitor makes C2 call to domains for trojans

uneventrendi.com
ketofonerof.ru
thettertrefbab.ru

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 [redacted]

[redacted]

Maldoc URL

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

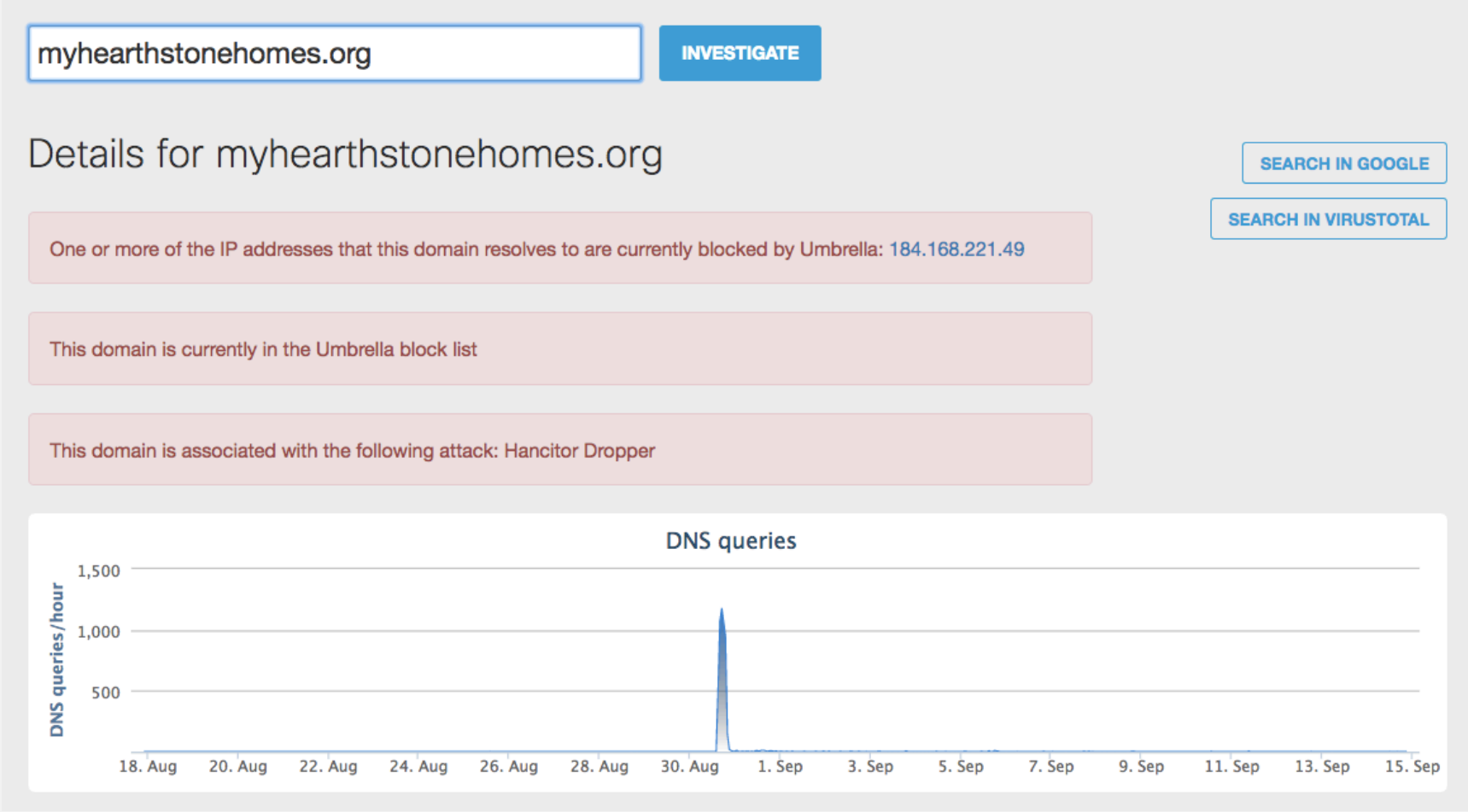
Thank you for flying with us
Delta Airlines

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

Reference: hazmalware.wordpress.com

splunk> .conf18

August 30: Peak of Malicious Redirect



Insight into the IP Network

myhearthstonehomes.org

INVESTIGATE

IP Addresses

First seen	Last seen	IPs
9/14/17	9/14/17	184.168.221.49 (TTL:)
8/31/17	9/13/17	184.168.221.49 (TTL: 600)
8/30/17	8/30/17	52.14.244.225 (TTL: 600)

Details for 52.14.244.225

Hosting 0 malicious domains for 1 week

This IP is currently in the Umbrella block list as malware

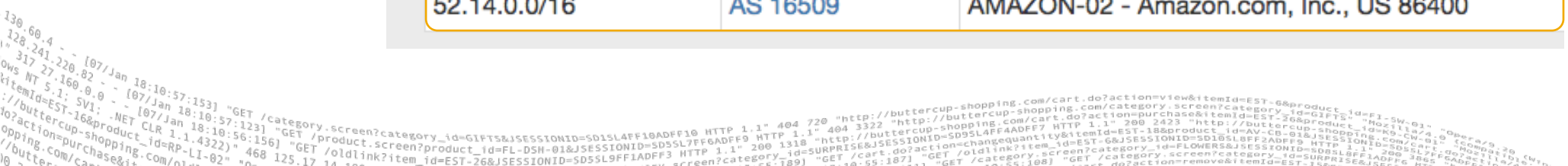
Security Categories: Malware

Threat Types: Bulletproof Hosting

An AWS IP abused by Alex' BPH and offered to criminal customers to host malspam attack domains

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

splunk> .conf18

heymamaradio.com

INVESTIGATE

BACK TO TOP

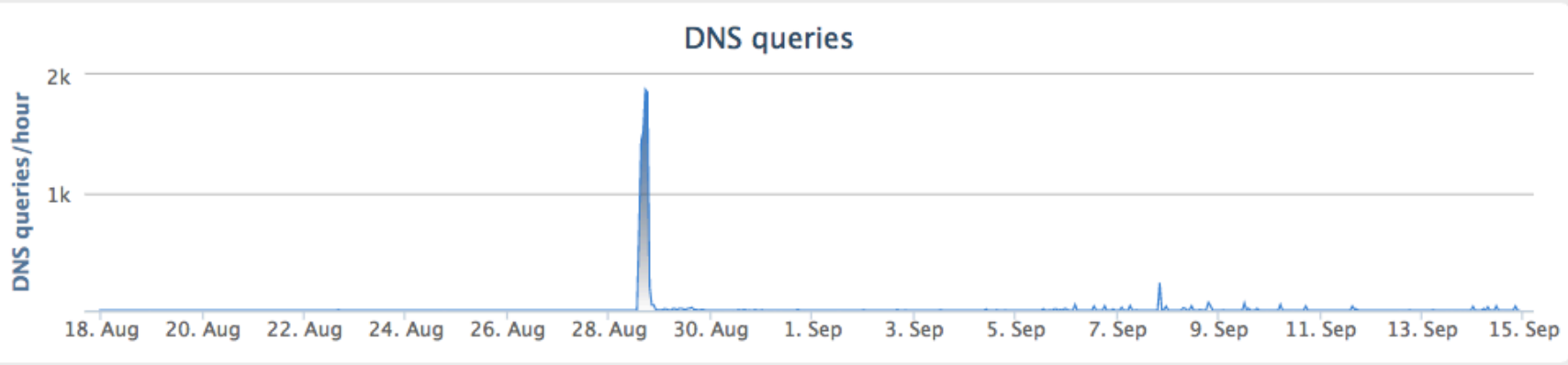
This domain is associated with the following attack: Hancitor Dropper

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)

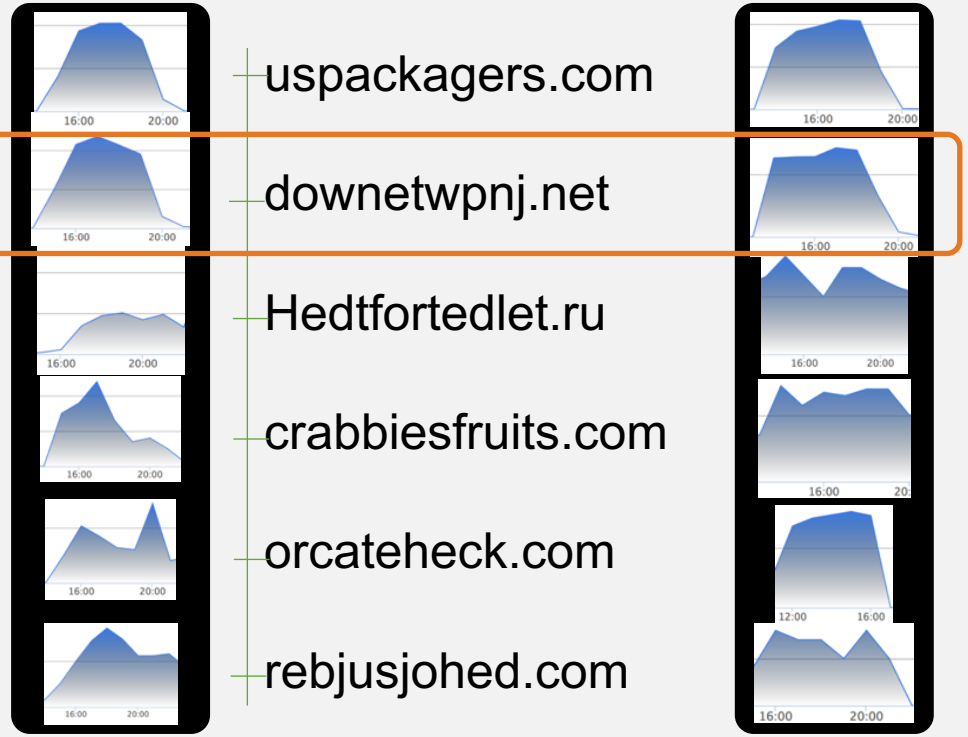
Domain is a compromised domain used for malspam attacks. IPs in green are the legitimate registrar’s initial hosting IPs. IPs in red are all criminal hosting IPs offered by the bulletproof hosting provider. IPs in purple (subset of the red set) are AWS IPs and are part of the criminal hosting IP space operated by the BPH provider. The BPH provider abuses AWS IPs and offers them as hosting space to his criminal customers.

Overarching Patterns Across a Dozen Malspam Campaigns

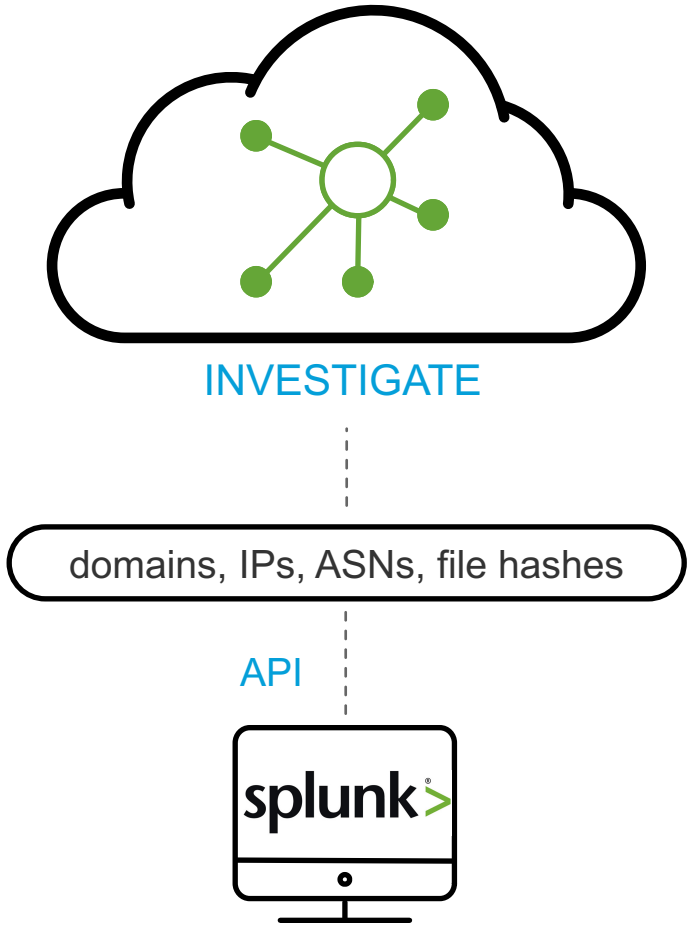
Phishing urls are hosted on AWS cloud services

BPH 2 Dedicated small time BPH and abused hosters

Malspam	Campaign 1	Campaign 2
Spoofed sender domain	performanceair.com	uspackagers.com
Alex — Phishing	myhearthstonehomes.org	downetwpnj.net
Hancitor C2	thettertrefbab.ru	Hedtfortedlet.ru
Pony C2	mebelucci.com.ua	crabbiesfruits.com
EvilPony C2	uneventrendi.com	orcateheck.com
Zloader C2	lycasofrep.com	rebjusjohed.com



Splunk Add-on for Cisco Umbrella Investigate



Automatically enrich security alerts inside Splunk, allowing analysts to discover the connections between the domains, IPs, and file hashes in an attacker's infrastructure.

Key Benefits of Investigate Add-on

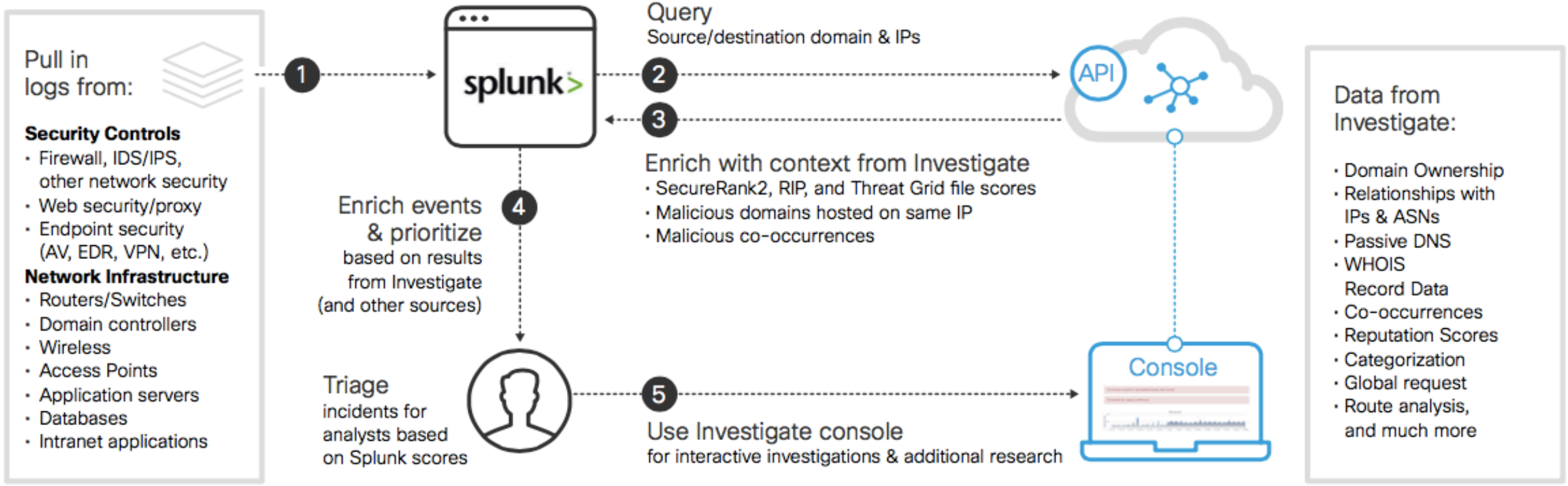
Complete view of an attack

Better prioritize incident response

Uncover missing connections

Speed up investigations

How it Works



Q&A

Thank You

Don't forget to rate this session in the .conf18 mobile app