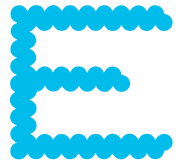
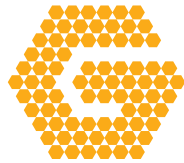
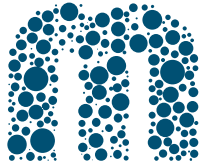


Cisco *live!*

January 28 - February 1, 2019 - Barcelona



INTUITIVE



BRKSEC-2049

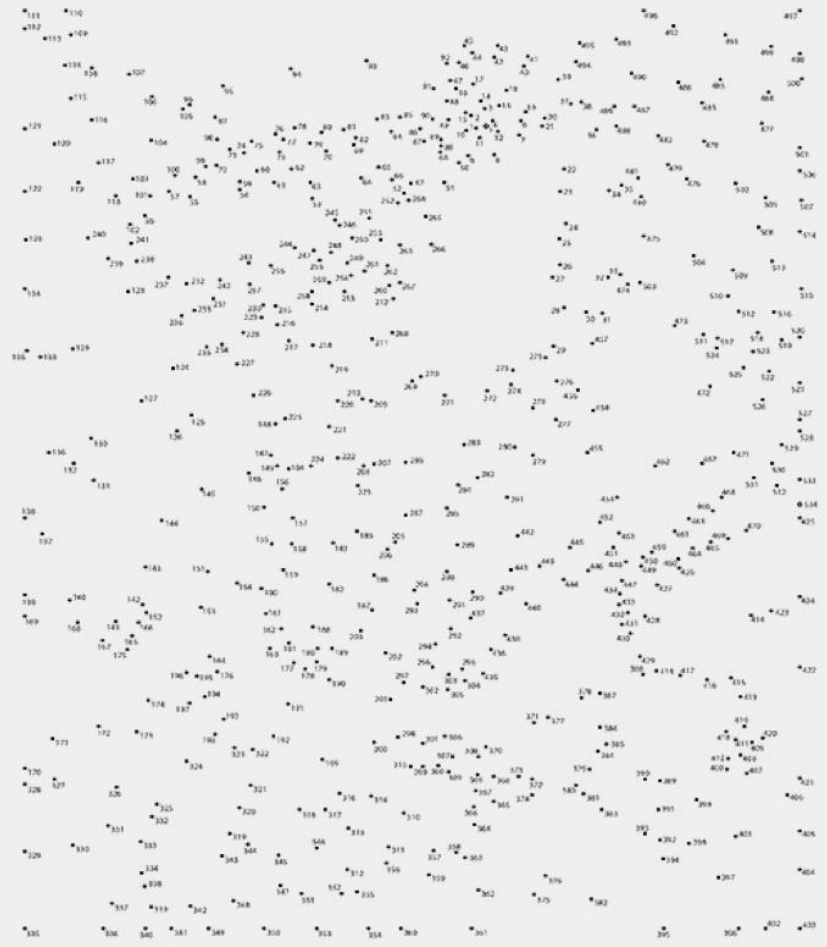
# Tracking Down the Cyber Criminals

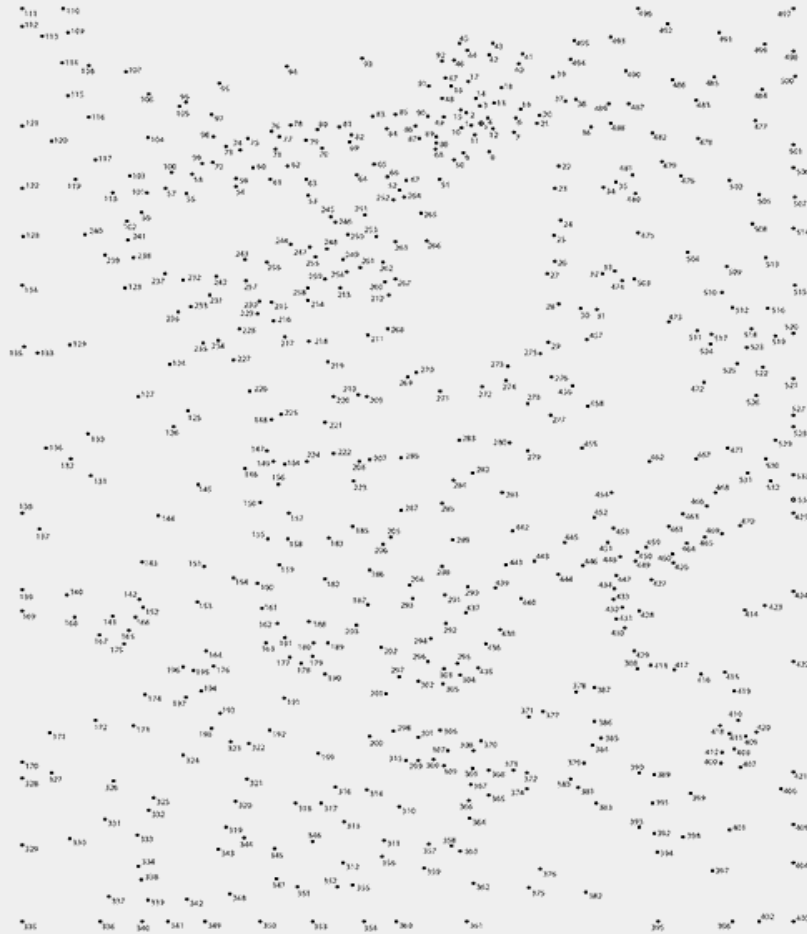
Revealing Malicious Infrastructure with Umbrella

Chris Riviere, CSE - Cloud Security



INTUITIVE





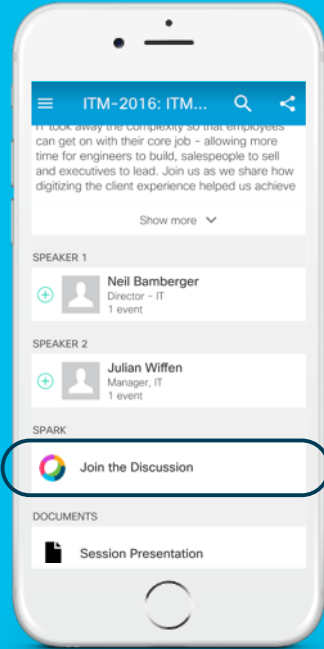
# About Me

- Consulting Systems Engineer
- OPNET, Riverbed, Piston Cloud Computing
- Cycling, Scuba Diving, Traveling
- @rivimont



# Agenda

- What is Cisco Umbrella?
- Making Sense of Big Data
- Real-World Threat Campaigns
- Putting it into Action
- Q&A



[cs.co/ciscolivebot#BRKSEC-2049](https://cs.co/ciscolivebot#BRKSEC-2049)

# Cisco Webex Teams

## Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

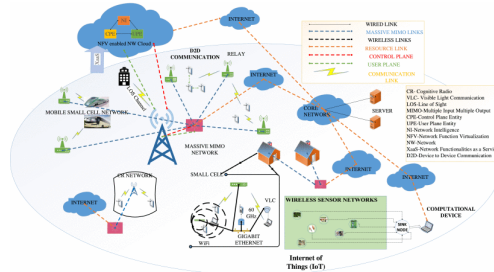
## How

- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space

# DNS is the Critical Lifeline of the Network



Every Possible Device



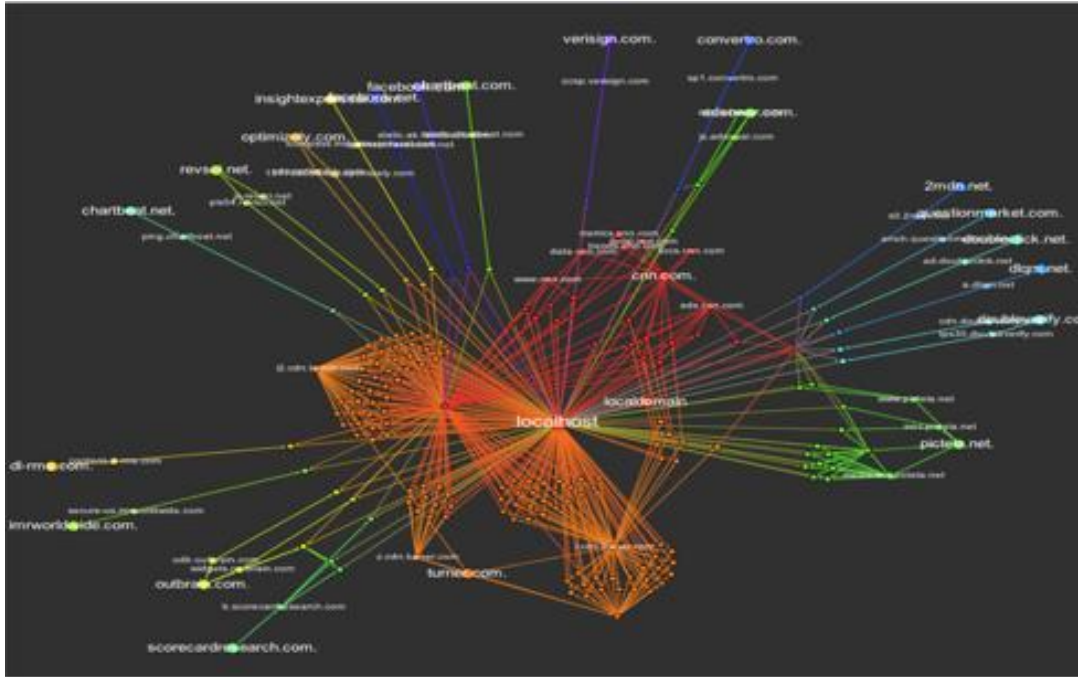
All Network Architectures



All Operating Systems



# What happens when you visit a single site?



68%

of organizations  
don't monitor  
DNS

# Using a Single Global Recursive DNS Service

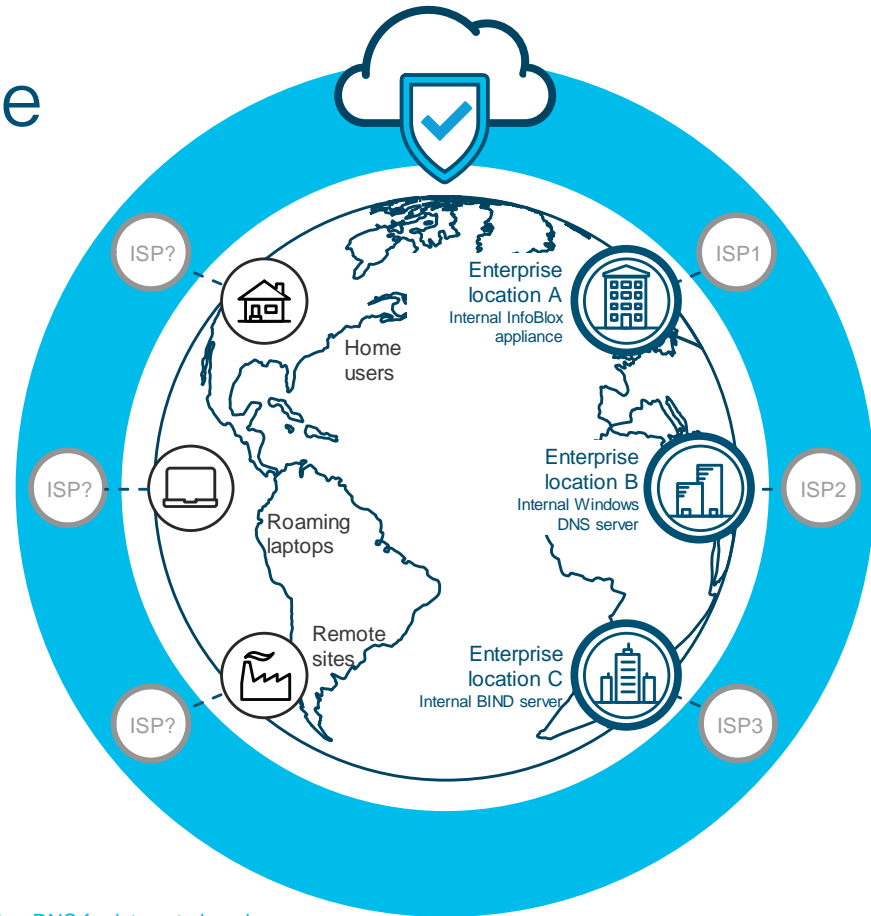
## Benefits

Global internet activity visibility

Network security w/o adding latency

Consistent policy enforcement

Internet-wide cloud app visibility



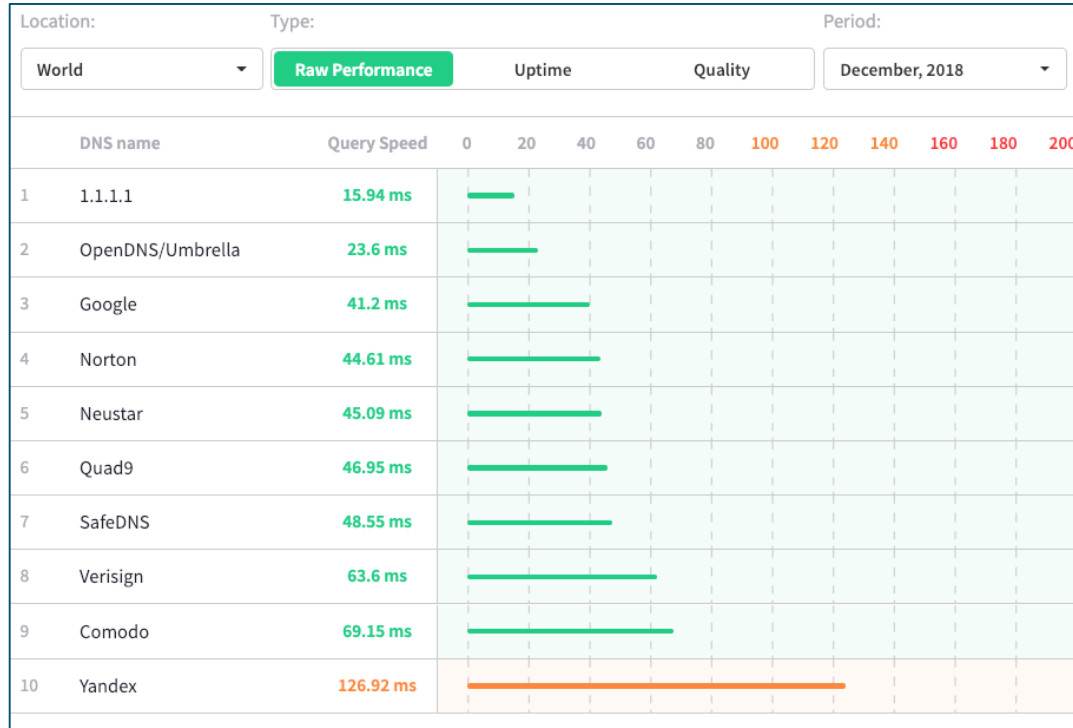
✓ Recursive DNS for internet domains

○ Authoritative DNS for intranet domains

# 3rd Party Validation

[www.dnsperf.com](http://www.dnsperf.com) → Public DNS Resolvers

- 1.1.1.1 isn't doing any blocking or applying policies
- Provide free visibility!



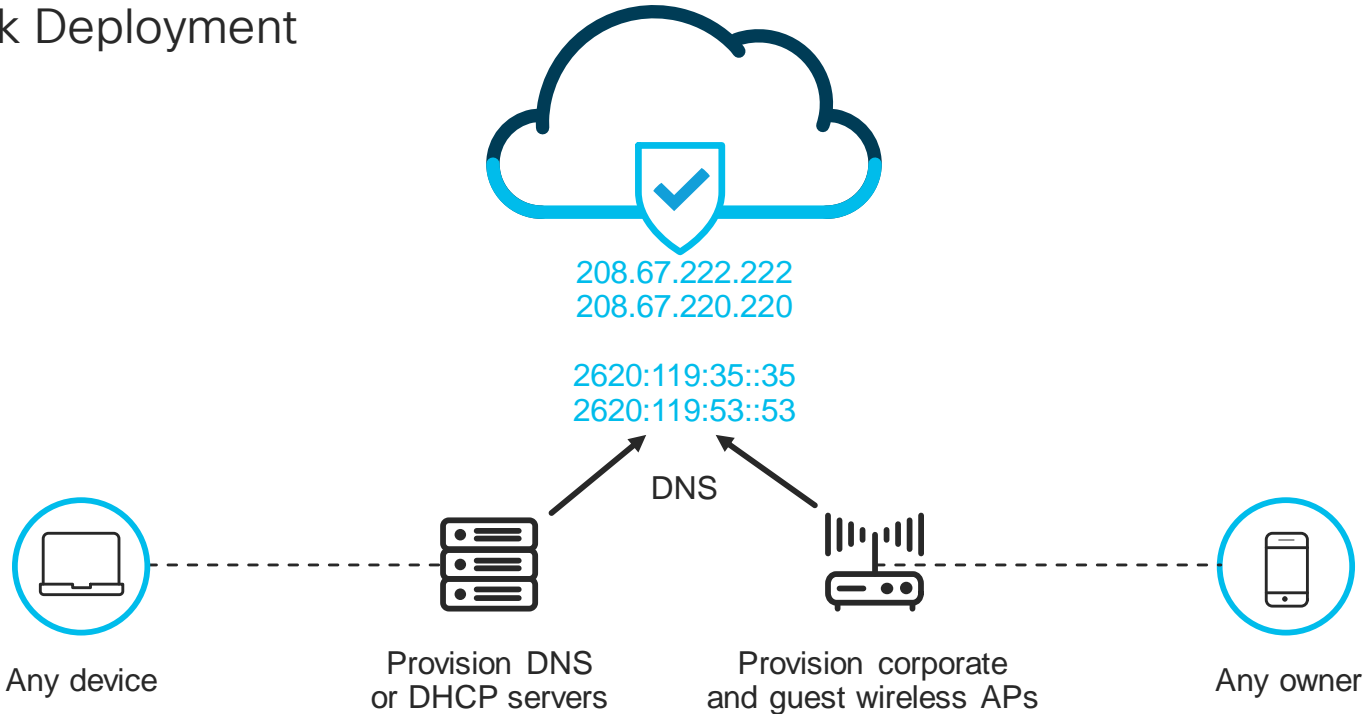
|                 | EUROPE | NORTH AMERICA | OCEANIA |
|-----------------|--------|---------------|---------|
| CLOUDFLARE      | 6.95   | 10.28         | 9.2     |
| GOOGLE          | 9.04   | 10            | 22.78   |
| OPENDNS (CISCO) | 10.9   | 13.48         | 17.43   |
| LEVEL3          | 17.05  | 13.27         | 134.56  |
| CLEANBROWSING   | 17.64  | 22.83         | 19.79   |
| QUAD9           | 18.45  | 16.26         | 22.71   |
| DNS.WATCH       | 21.13  | 129.34        | 308.48  |
| SAFEDNS         | 23.5   | 21.52         | 22.91   |
| NEUSTAR         | 34.99  | 41.09         | 22.98   |
| FREEDNS         | 37.21  | 146.86        | 323.72  |
| YANDEX          | 40.52  | 153.47        | 336.81  |
| COMODO          | 42.14  | 35.79         | 189.77  |
| DYN             | 45.68  | 31.43         | 60.89   |
| VERISIGN        | 77.06  | 35.45         | 168.55  |
| OPENNIC         | 255.09 | 221.61        | 277.91  |

Source: ThousandEyes Global DNS Performance Benchmark Report

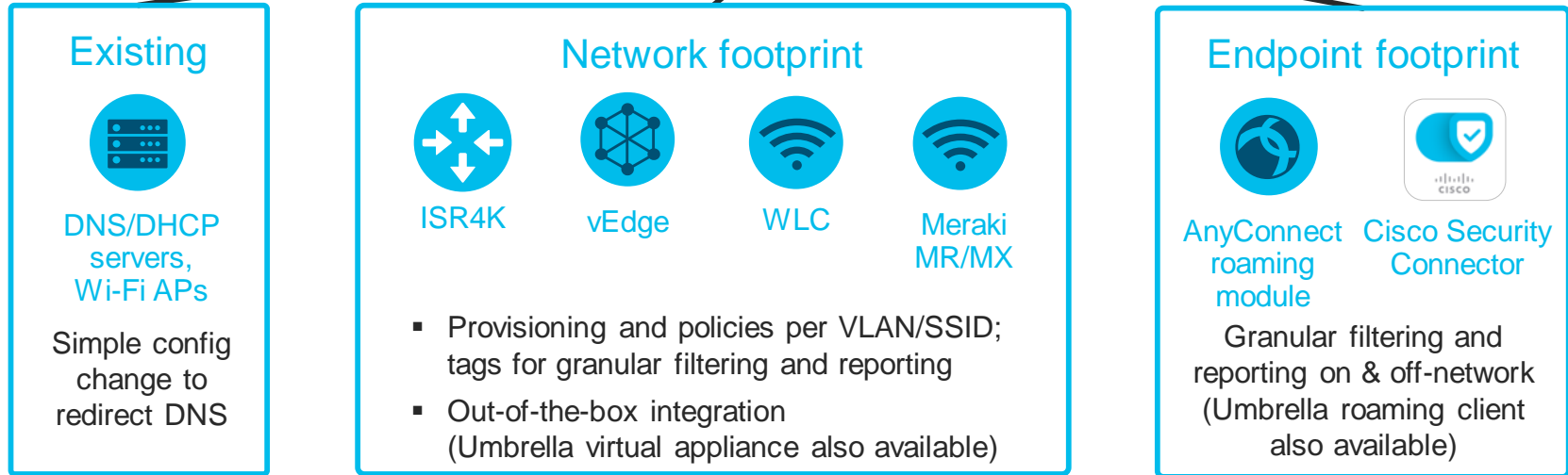
# Simplest Security Deployment on the Planet

Point external DNS traffic to Umbrella

Network Deployment

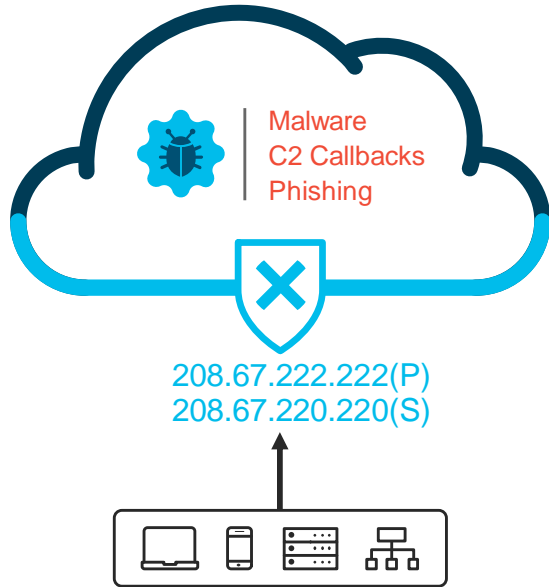


# Enterprise-wide deployment in minutes



# Cisco Umbrella

## Cloud security platform



- Built into the foundation of the internet
- Intelligence to see attacks before launched
- Visibility and protection everywhere
- Enterprise-wide deployment in minutes
- Integrations to amplify existing investments

# Integral Part of Your Security Platform

YOU CURATE & CORRELATE

WE TAKE IMMEDIATE ACTION



logs

SECURITY INCIDENT & EVENT MANAGEMENT



Customer



logs

YOUR SCRIPTS

domains

context on domains, IPs, or ASNs



## UMBRELLA

### Enforcement & Visibility

Network security service that blocks Internet activity attributed to domains. And retain all DNS logs for as long as required



## INVESTIGATE

### Intelligence & Enrichment

Live graph of global DNS requests and contextual data  
Features our passive DNSDB

# Agenda

- What is Cisco Umbrella?
- **Making Sense of Big Data**
- Real-World Threat Campaigns
- Putting it into Action
- Q&A

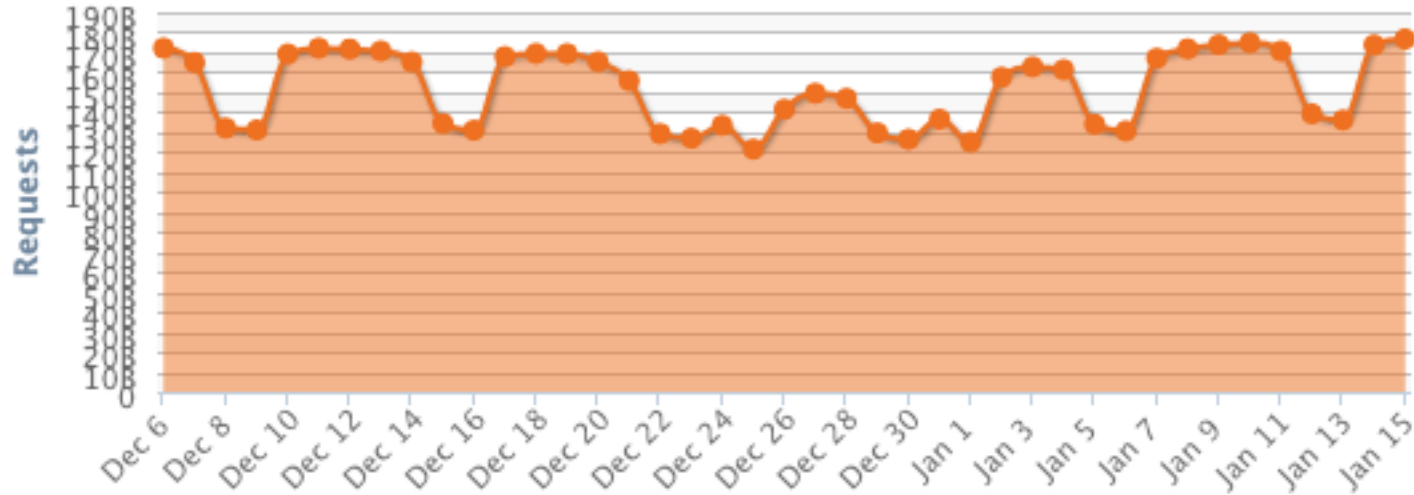


# Global Network System Statistics

# Global Activity

## Total Activity

Number of DNS requests per day in billions



221,034,740,818,032 DNS requests since [July 10, 2006](#).

Source: <http://system.opendns.com>

# Big Data > Vast Data = Unique Perspective

DNS Requests

160B

Daily Active  
Users

90M

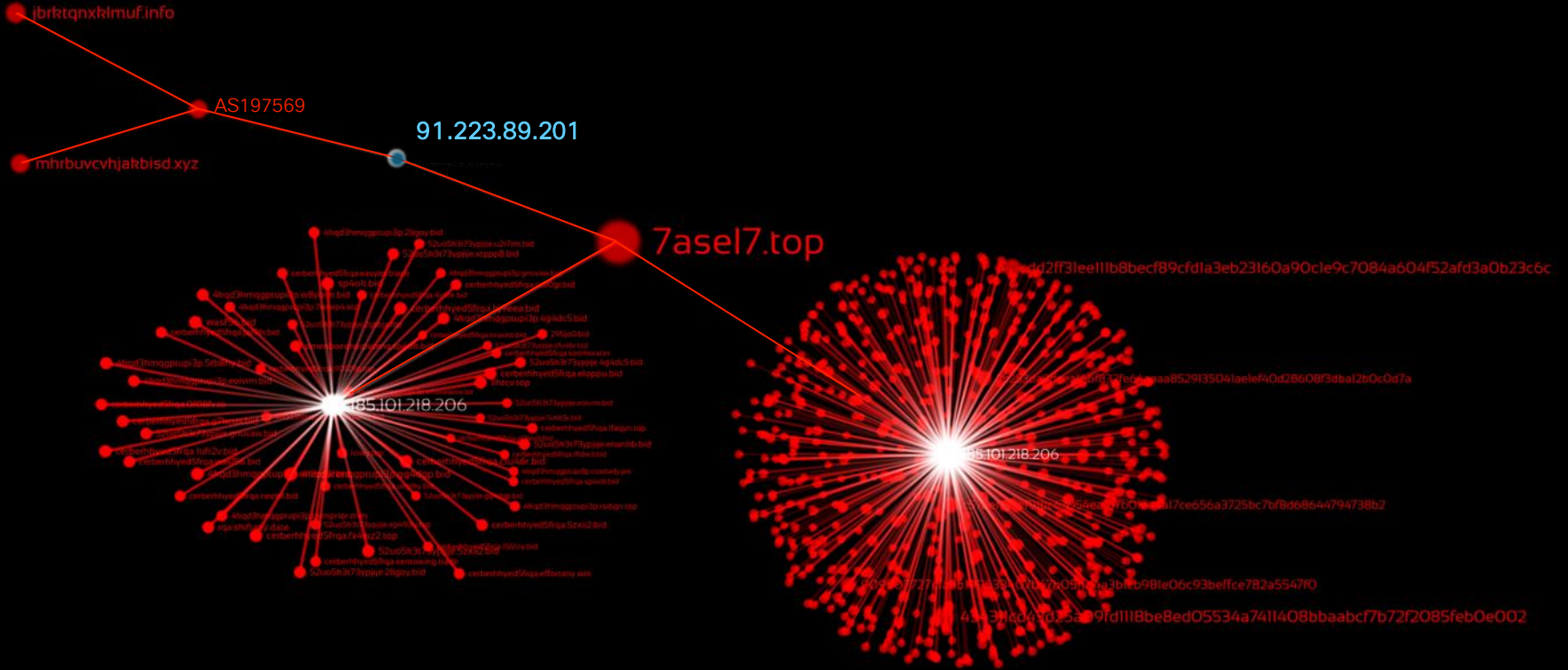
Enterprises

15K

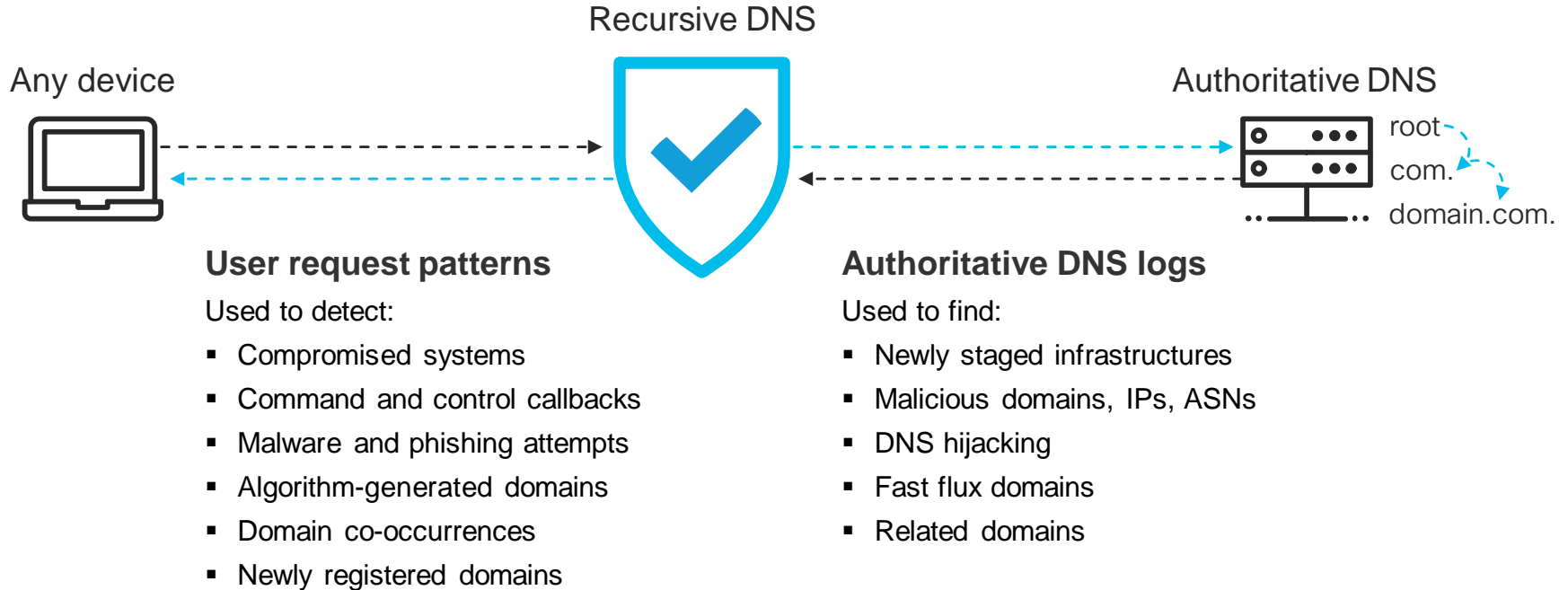
Countries

160+

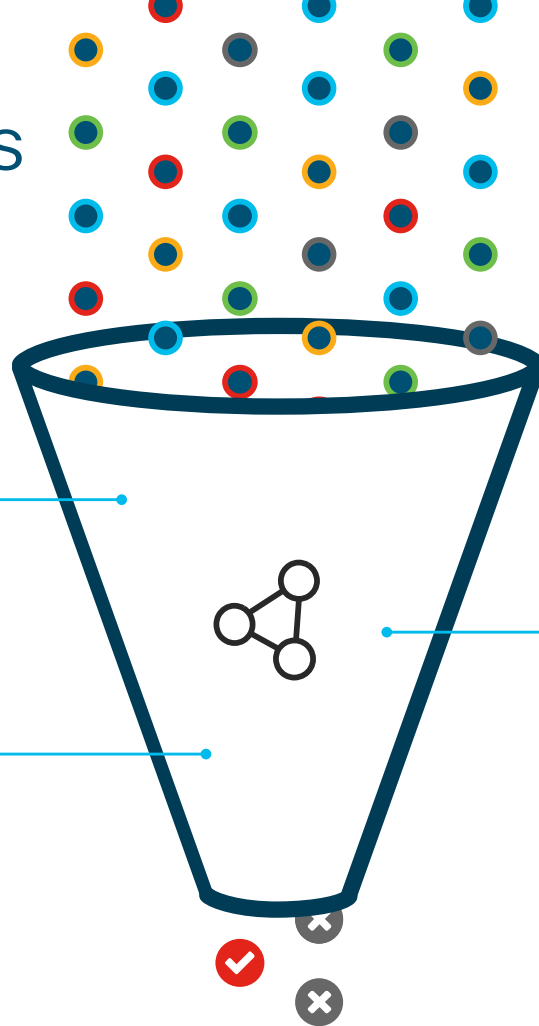
# Our View of the Internet



# Gathering Intelligence at the DNS Layer



# Statistical Models



2M+ live events per second

11B+ historical events

## Guilt by inference

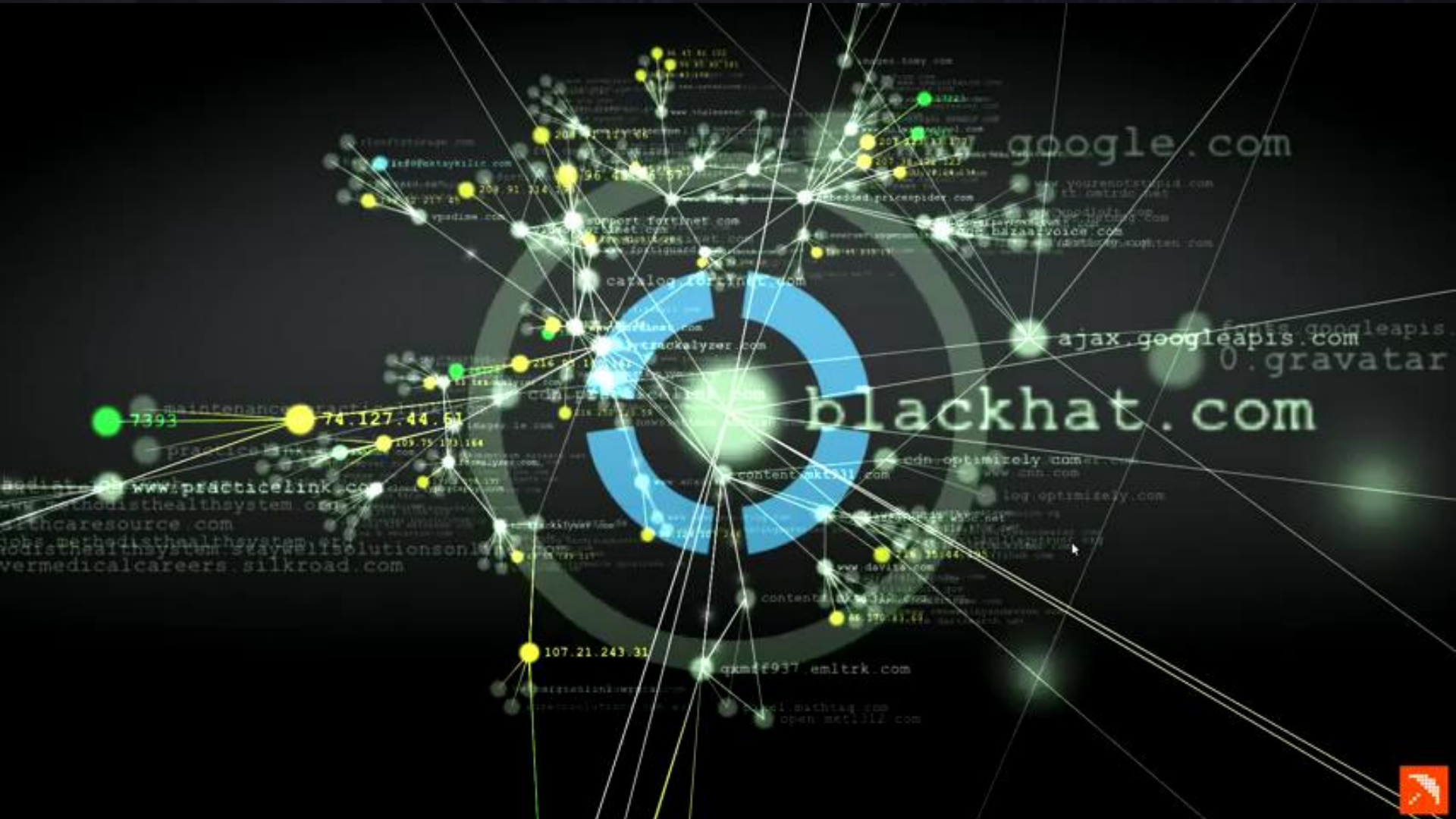
- Co-occurrence model
- Geo-Location model
- Secure Rank model

## Guilt by association

- Predictive IP Space Modeling
- Passive DNS and WHOIS Correlation

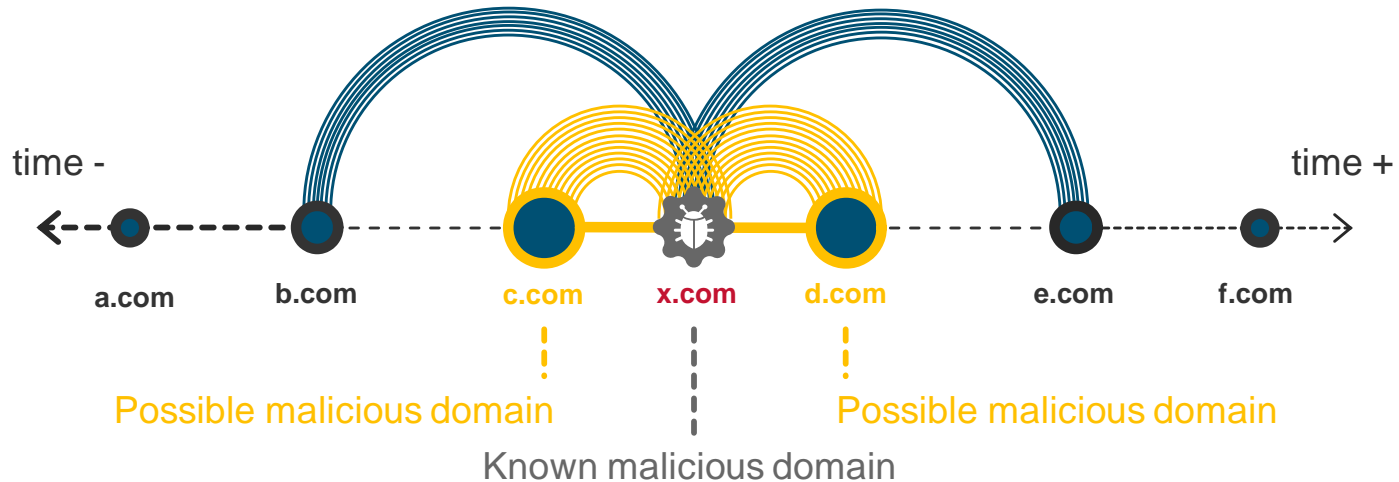
## Patterns of guilt

- Spike Rank model
- Natural Language Processing Rank model
- Live DGA Detection



# Co-occurrence Model

Domains guilty by inference

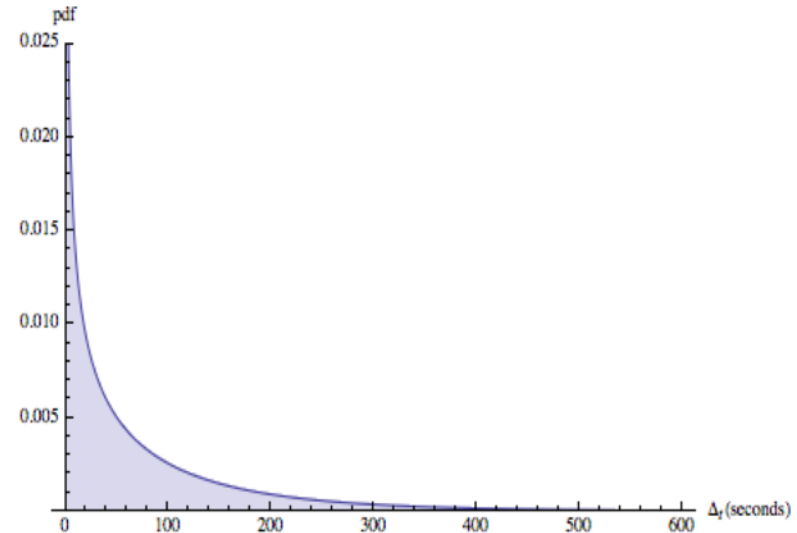


Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe



# The Co-Occurrence Probability Distribution Function

- The histogram of  $|t_i(c) - t_j(c)|$  for all clients and all pairs of malicious domains  $(i,j)$  appears to be gamma distributed.
- This allows to calculate the probability that two malicious domains are related.
- The Co-Occurrence is the sum of this probability for all the possible clients connecting to both domains.
- The model is normalized to take into account “legitimate co-occurrences”
  - (e.g google-analytics).

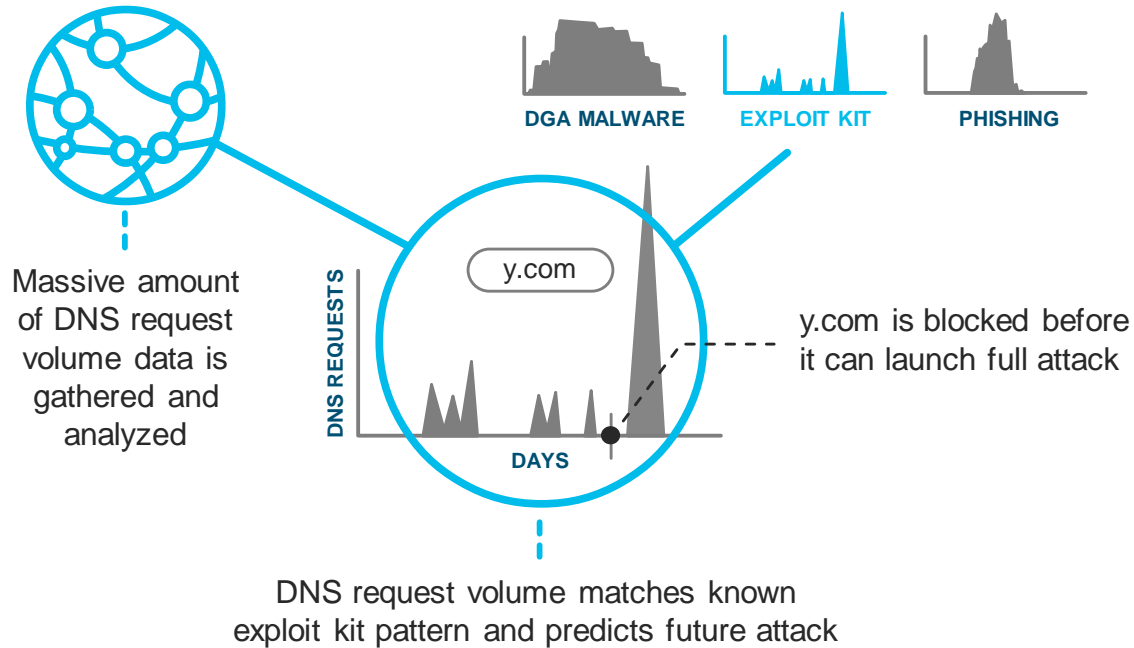


<https://umbrella.cisco.com/blog/2013/07/24/co-occurrences/>

# What do these applications have in common?

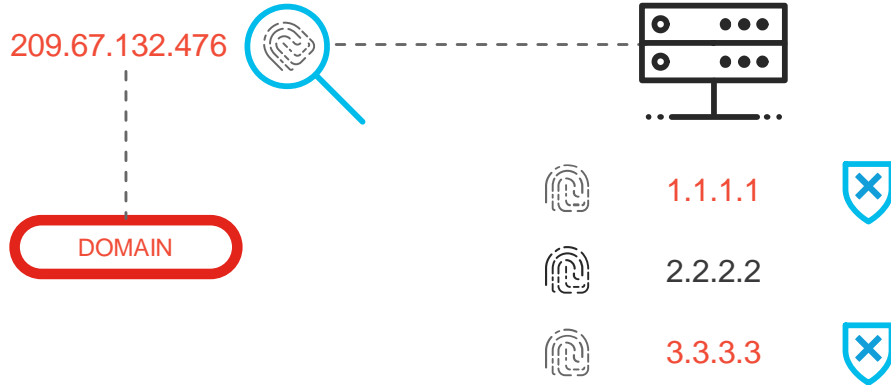


# Spike Rank Model



# Predictive IP Space Monitoring

Guilt by association



Pinpoint suspicious domains, and observe their IP's fingerprint

Identify other IPs (hosted on the same server) that share the same fingerprint

Block those IPs and their malicious domains

# IP Geo-location Analysis

## Host Infrastructure

Location of the server  
IP addresses mapped to domain



Hosted across 28+ countries

## DNS Requesters

Location of the network and off-network device  
IP addresses requesting the domain



Only US-based customers  
requesting a .RU TLD

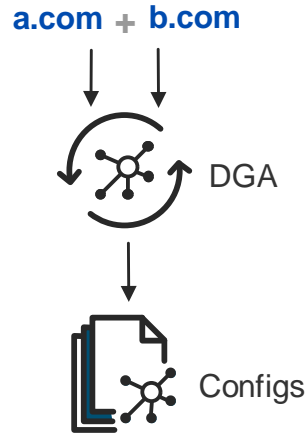
# Live DGA Prediction

## Automated at an unparalleled scale



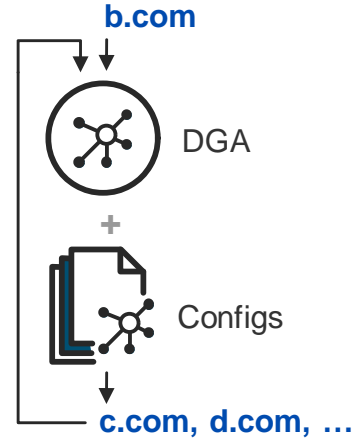
### Live DNS log stream

Identify millions of domains, many used by DGAs and unregistered



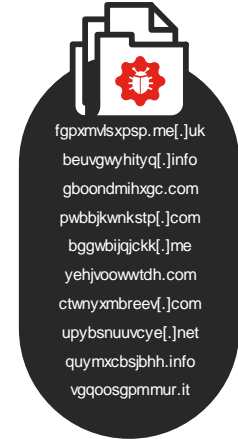
### Automate reverse engineering

Combine C2 domain pairs and known DGA to identify unknown configs



### Predict 100,000s of future domains

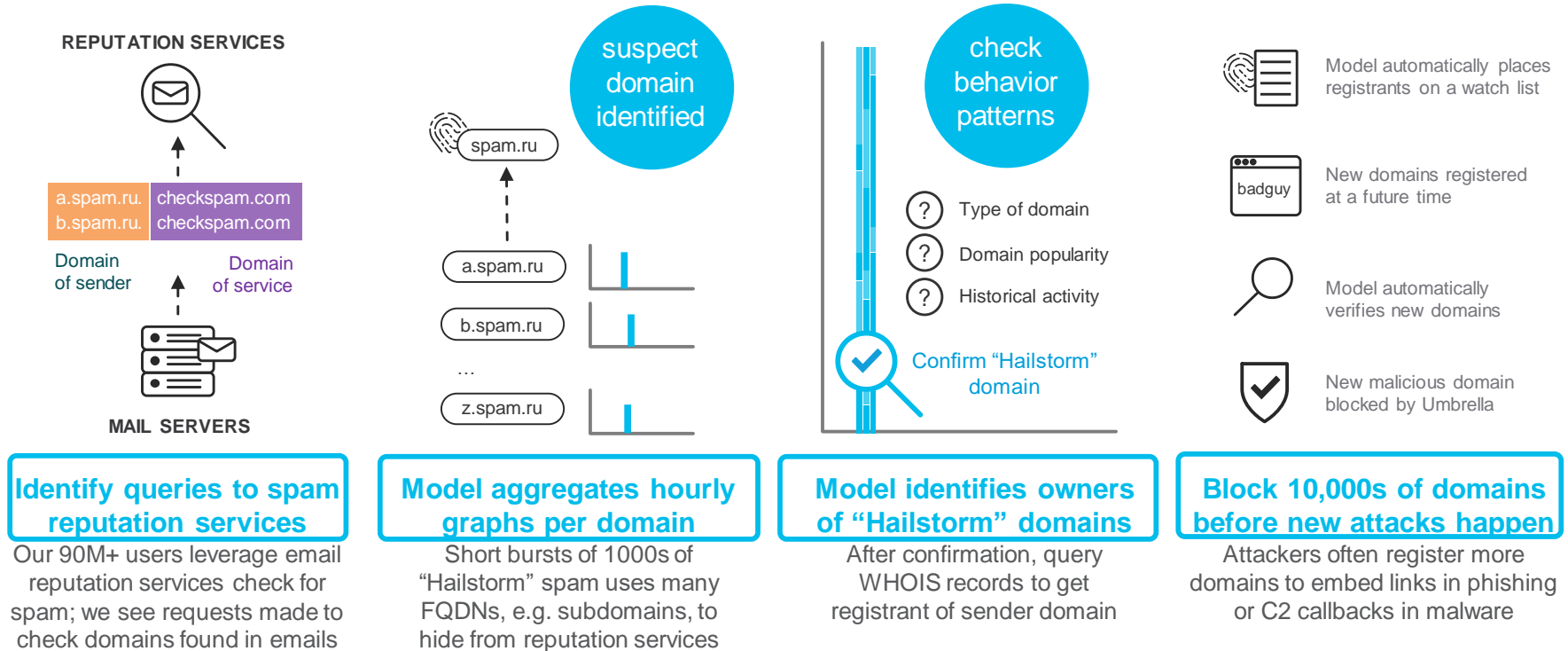
Combine newly-identified configs with DGA to identify C2 domains continuously



### Automate blocking pool of C2 domains

Used by thousands of malicious samples now and in the future

# Sender Rank Model: Predict Domains Related to Spammers



## Identify queries to spam reputation services

Our 90M+ users leverage email reputation services check for spam; we see requests made to check domains found in emails

## Model aggregates hourly graphs per domain

Short bursts of 1000s of "Hailstorm" spam uses many FQDNs, e.g. subdomains, to hide from reputation services

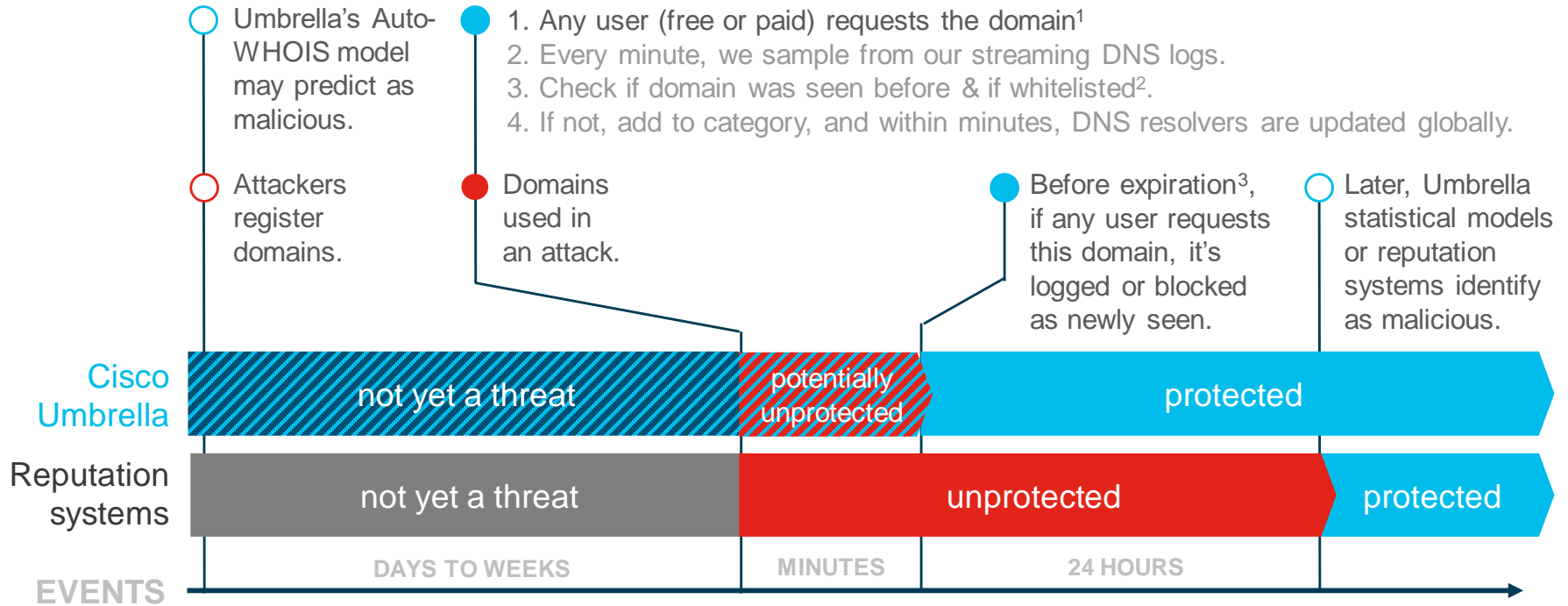
## Model identifies owners of "Hailstorm" domains

After confirmation, query WHOIS records to get registrant of sender domain

## Block 10,000s of domains before new attacks happen

Attackers often register more domains to embed links in phishing or C2 callbacks in malware

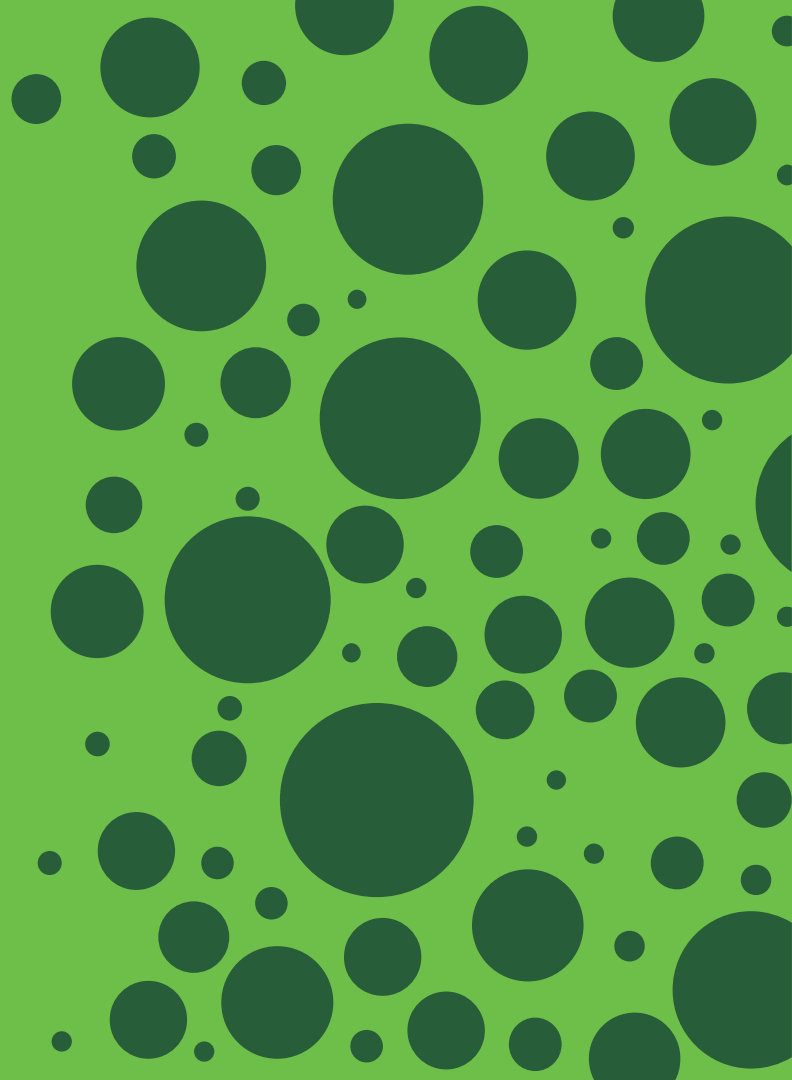
# Newly Seen Domains Category Reduces Risk of the Unknown



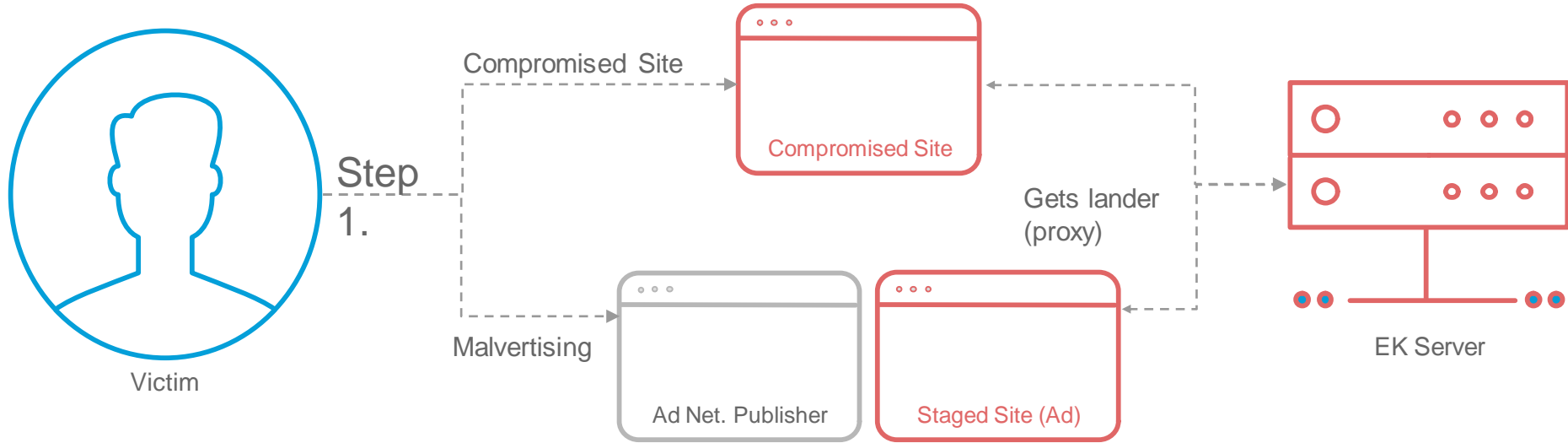
1. May have predictively blocked it already, and likely the first requestor was a free user.
2. E.g. domain generated for CDN service.
3. Usually 24 hours, but modified for best results, as needed.



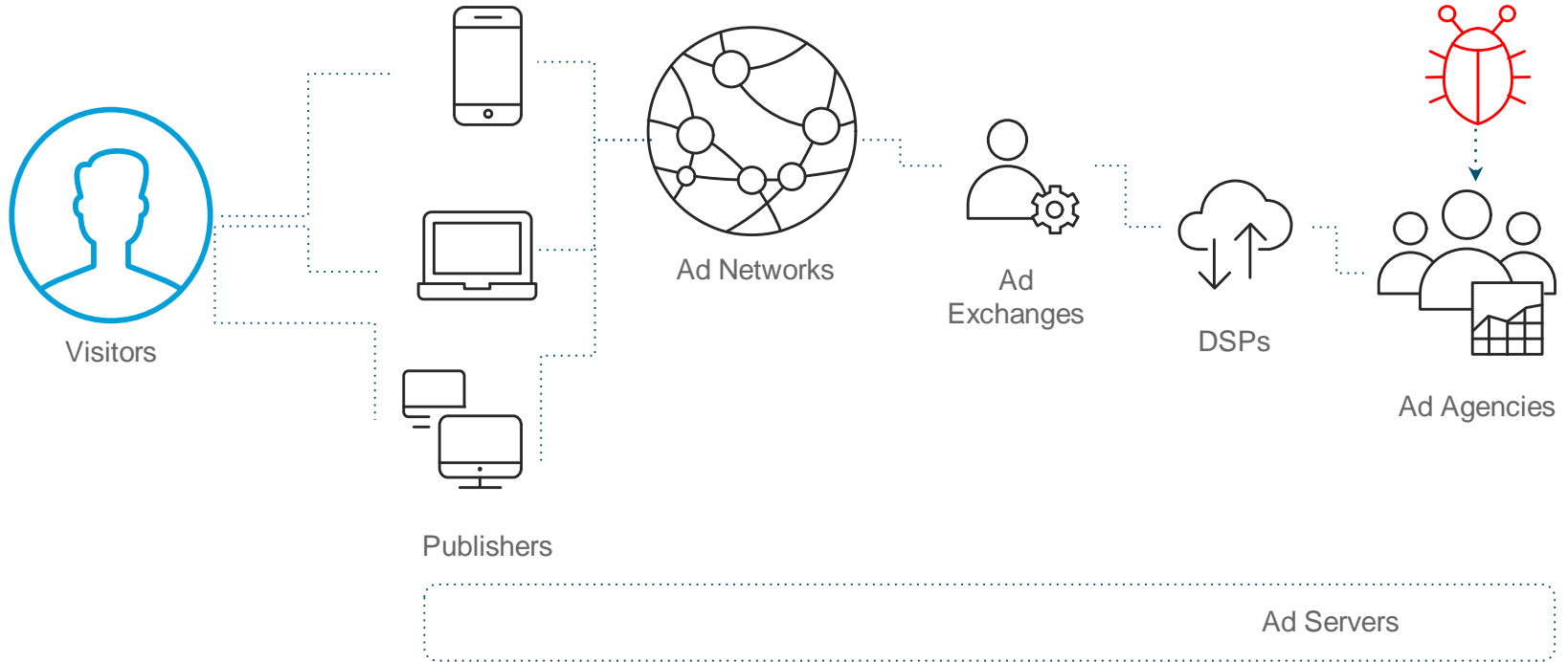
# Investigate Demo



# Exploit Kits



# What is Malvertising?





Your security matters

Google recommends using Chrome, a fast and secure browser. Try it?

[NO, NOT INTERESTED](#)

[YES](#)

# Google

Google Search

I'm Feeling Lucky



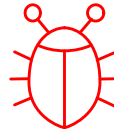
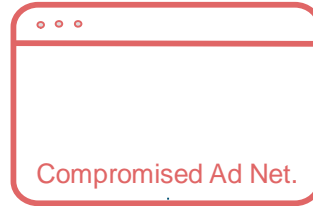
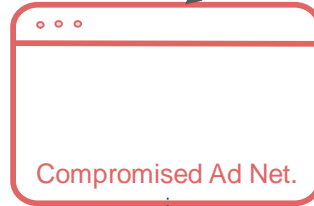
# Ad Campaign Flow



User visits publisher site



Publisher site includes ad network javascript



Examples:

- Tech support scam
- Rig Exploit Kit
- Fake flash/java update

Ad network fingerprints and sends user to malvertisement

Microsoft  
Windows  
Windows  
Activ  
Please Do  
Call Microso  
Get Instant He  
Call On Our T  
Call  
Hello from Seattle. United States

Message from webpage

**\*\* YOUR COMPUTER HAS BEEN BLOCKED \*\***

Error # 268d3

Please call us immediately at: 1844 584 6326  
Do not ignore this critical alert.  
If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen...

- > Facebook Login
- > Credit Card Details
- > Email Account Login
- > Photos stored on this computer

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: 1844 584 6326

6326  
user  
raining  
) 584-6326  
Microsoft  
Site Map © 2016 Microsoft

# Tech Support Scams

upnow2app.contentfreeandsafe4update.bid says:

WARNING! Your Flash Player is out of date. Please install update to continue.

OK

Adobe

Install the latest update

Update now

# Fake Flash and Java Updates

Later

Install

[Affiliates](#) | [EULA](#) | [TOS](#) | [Privacy](#) | [Download Manager](#) | [Uninstall](#) | [Contact](#)

By downloading, you accept our TOS and Privacy Policy.  
This free download is done via download manager which may offer other applications you can decline or uninstall.  
This site and the download manager have no relationship with the author. Any third party products, brands or trademarks listed above are the sole property of their respective owner.



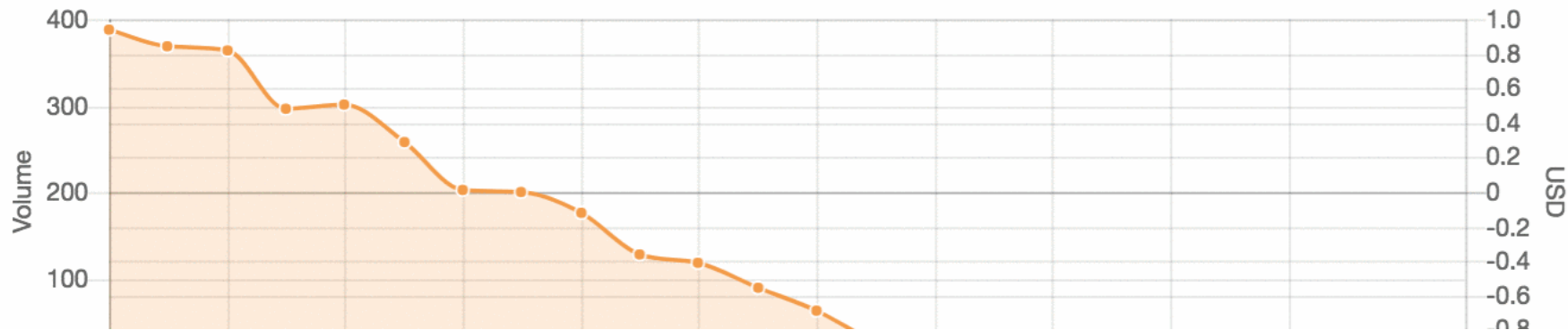
# Dashboard

Today

All Campaigns



|        |               |             |      |         |             |     |
|--------|---------------|-------------|------|---------|-------------|-----|
| Clicks | Unique Clicks | Conversions | Cost | Revenue | Profit/Loss | ROI |
| 2,975  | 10            | 41          | \$0  | \$10.20 | \$10.20     | 0%  |







SEARCH

PATTERN SEARCH

BULK EDIT



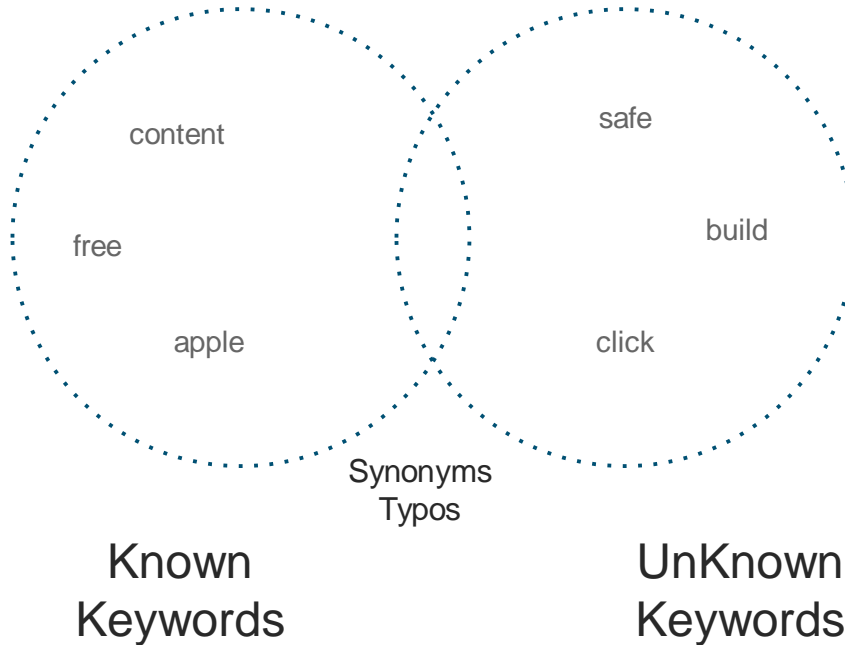
INVESTIGATE

Constrain RegEx search to

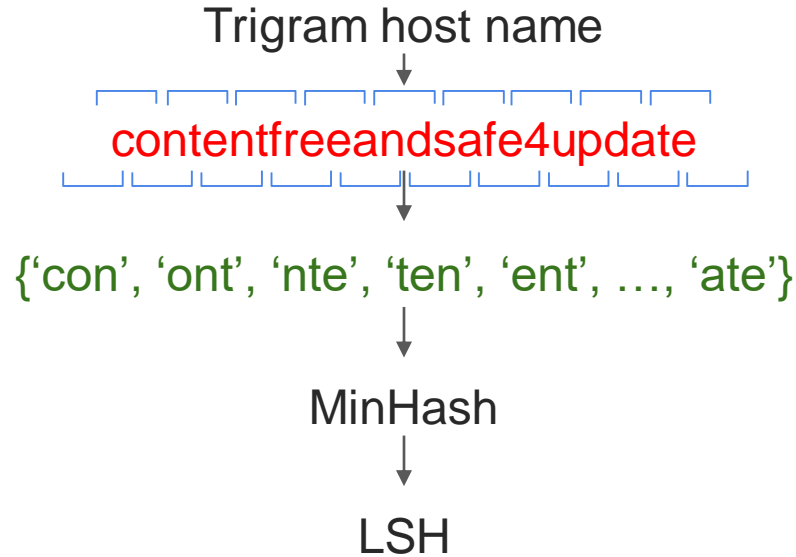
Showing 460 results for **contentfreeandsafe.\***

| Domain Name   | Security Categ... | First Seen                 |
|---|-------------------|----------------------------|
| <a href="#">contentfreeandsafe2updating.stream</a>    | Newly Seen Do...  | December 13, 2017, 3:17pm  |
| <a href="#">contentfreeandsafetoupdating.review</a>   | Newly Seen Do...  | December 13, 2017, 3:09pm  |
| <a href="#">contentfreeandsafe4updating.date</a>      | Newly Seen Do...  | December 13, 2017, 3:00pm  |
| <a href="#">contentfreeandsafeupdatesgreat.win</a>    | Newly Seen Do...  | December 13, 2017, 2:18pm  |
| <a href="#">contentfreeandsafeupdatingnew.win</a>     |                   | December 13, 2017, 11:27am |
| <a href="#">contentfreeandsafetoupgrade.stream</a>    |                   | December 13, 2017, 11:16am |
| <a href="#">contentfreeandsafe4upgrading.download</a> |                   | December 13, 2017, 10:39am |

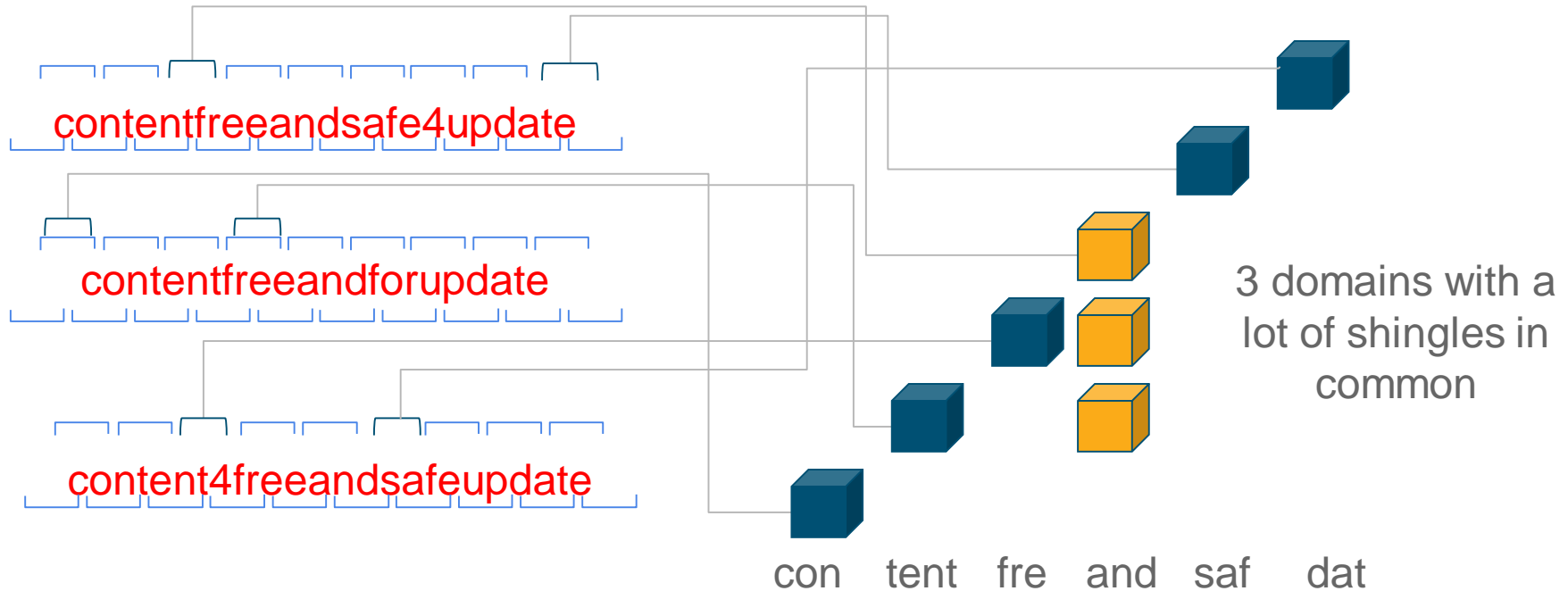
# Consider the Almighty Regex Keywords



# Shingling Fake Flash and Java Update



# Locality Sensitive Hashing Fake Hash



# Fake Flash and Java Update Lexical Clustering

cluster\_1:

goodnewcontentssafe.download  
goodnewfreecontentsload.date  
goodnewfreecontentall.trade

...

cluster\_3:

artificialintelligencesweden.se  
artificialintelligencechip.com  
artificialintelligence.net.cm

...

cluster\_2:

call-microsoftnw-err81711102.win  
call-microsoftnw-err99817109.win  
call-microsoftnw-err81711101.win

...

cluster\_4:

mkto-sj220048.com  
mkto-sj220146.com  
mkto-sj220162.com

...

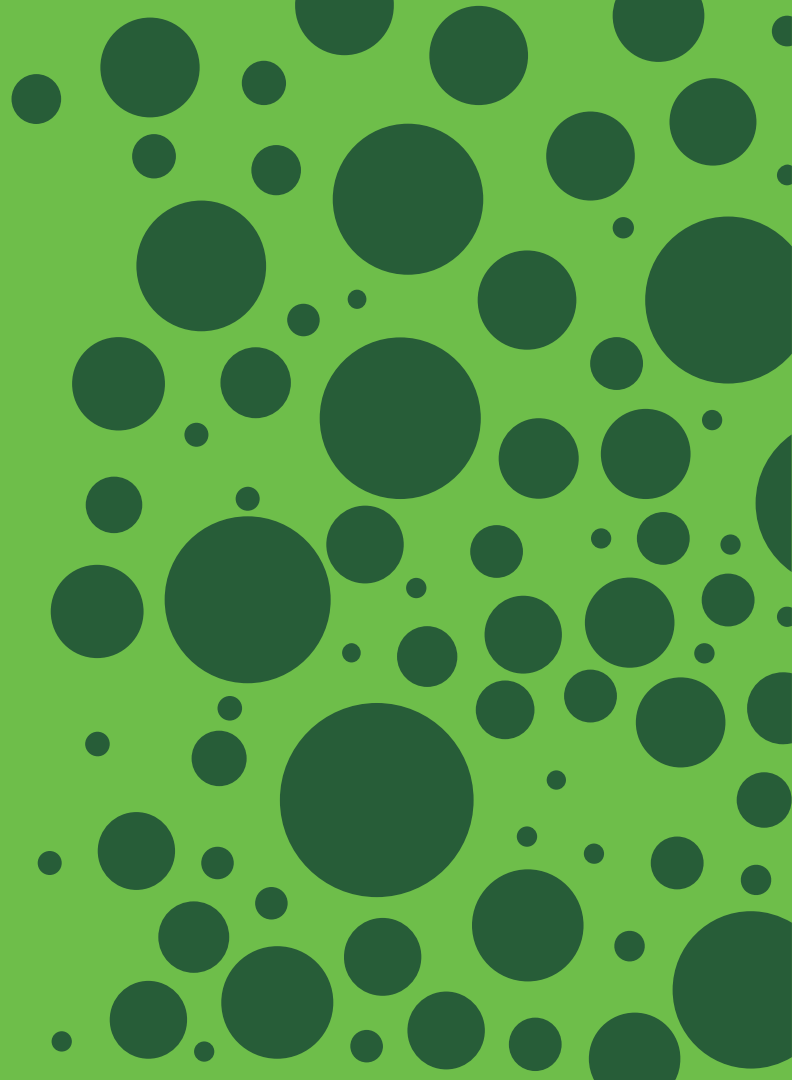
# Simple Flask App Dashboard

| Cluster ID   | Preview   | Type   |
|--------------|---|--|
| 1513796401_0 | 2goodcalling118121234567890.tk<br>2goodcalling1181212345.tk | Fake Update<br>Tech Support Scam<br>Suspicious |

Skip

```
30
31     for j, domain in enumerate(entry['domains']):
32         entry['domains'][j] = {'domain': domain, 'timestamp': entry['ti
33
34     entry.pop('timestamps')
35
36     for i, idx in enumerate(date_changes):
37         n = date_changes[i+1] if i < len(date_changes) - 1 else None
38         r[idx:n] = sorted(r[idx:n], key=lambda x: x['c_num'])
39
40 @app.route("/clusters/attribution", methods=['POST'])
41 def attribution():
42     if not request.json:
43         return "Error!"
44     resp = {}
45     for cluster_id in request.json:
46         attr = request.json[cluster_id]
47         ret = add_attribution(cluster_id, attr)
48         resp[cluster_id] = ret
49
50     if ret == 'success' and BLOCKING:
51         domains = m.get_cluster_domains(cluster_id)['domains']
52         block_description = "Domain showed similarities to {0} malverti
53         print "Blocking domains: {0}".format(", ".join(domains))
54         block(domains, block_description=block_description)
55
56     return jsonify(resp)
57
58 @app.route("/clusters/attribution/<string:cluster_id>")
59 def get_attribution(cluster_id):
60     return jsonify(m.get_attribution(cluster_id))
61
62 @app.route("/clusters/uncategorized")
63 def get_uncategorized():
64     r = [entry for entry in m.get_uncategorized()]
65
66     if not r or len(r) == 1:
67         return jsonify(results=r)
68 --
```

# Malvertising Demo



# Result = Unrivalled Efficacy

**3M+**  
daily new  
domain names

Identify  
**60K+**  
daily malicious  
destinations

Enforce  
**7M+**  
malicious destinations  
while resolving DNS



# Agenda

- What is Cisco Umbrella?
- Making Sense of Big Data
- **Real-World Threat Campaigns**
- Putting it into Action
- Q&A

# 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



- 2 Victims click on malicious URLs



- 3 Malicious word doc drops Hancitor



- 6 Infection on device and positioned for data extraction



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

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



- 4 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 [here](#).

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

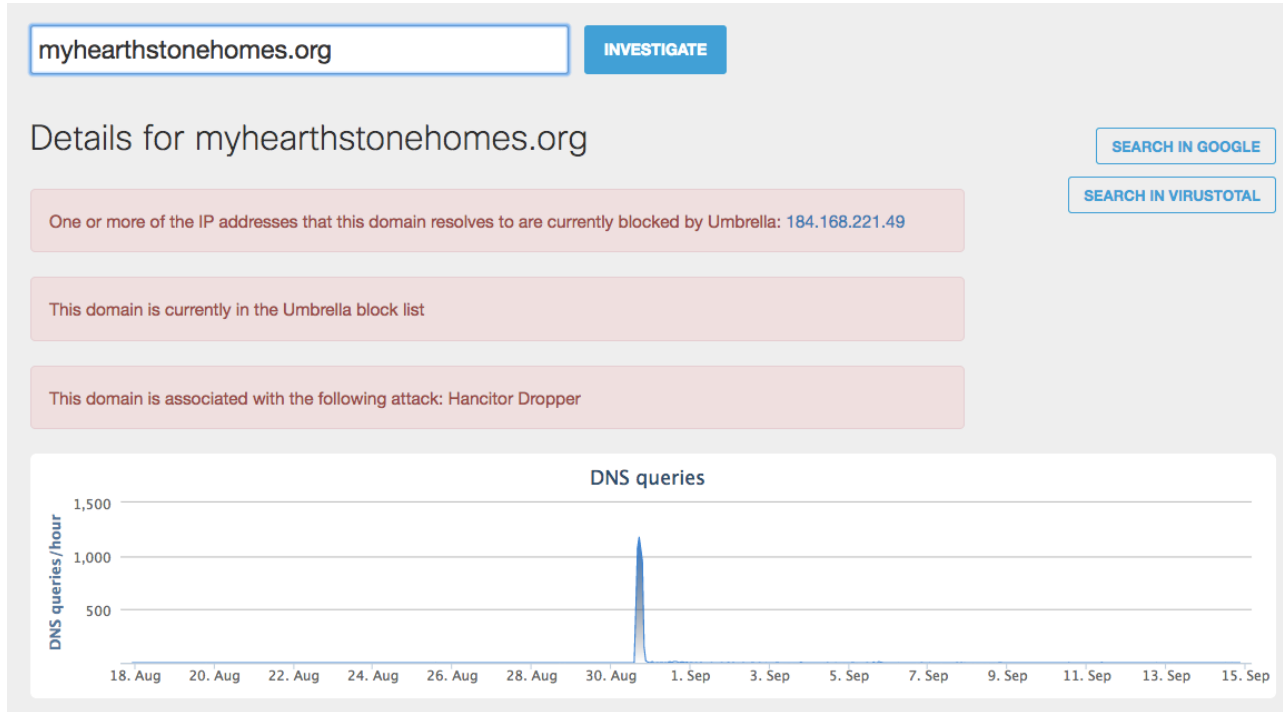
↑  
Maldoc  
URL

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

Thank you for flying with us  
Delta Airlines

[http://myhearthstonehomes\[.\]org/i.php?d=](http://myhearthstonehomes[.]org/i.php?d=)

# August 30: Peak of malicious redirect



# Insight into the IP network

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

[agentsellingtips.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

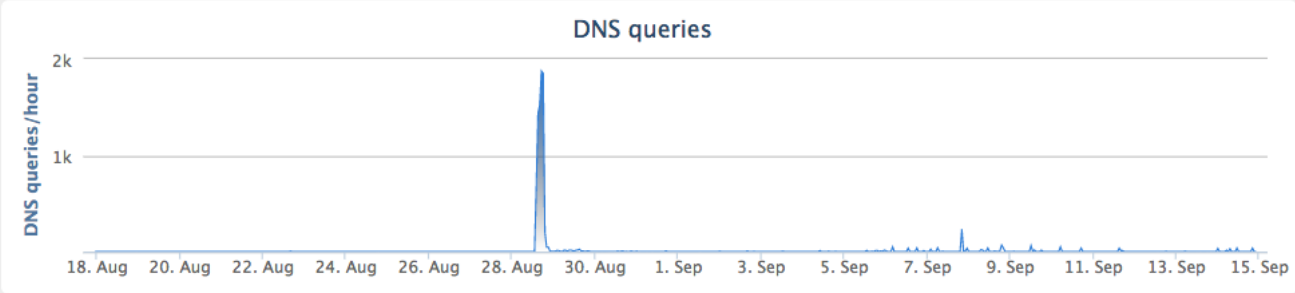
[BACK TO TOP](#)

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**



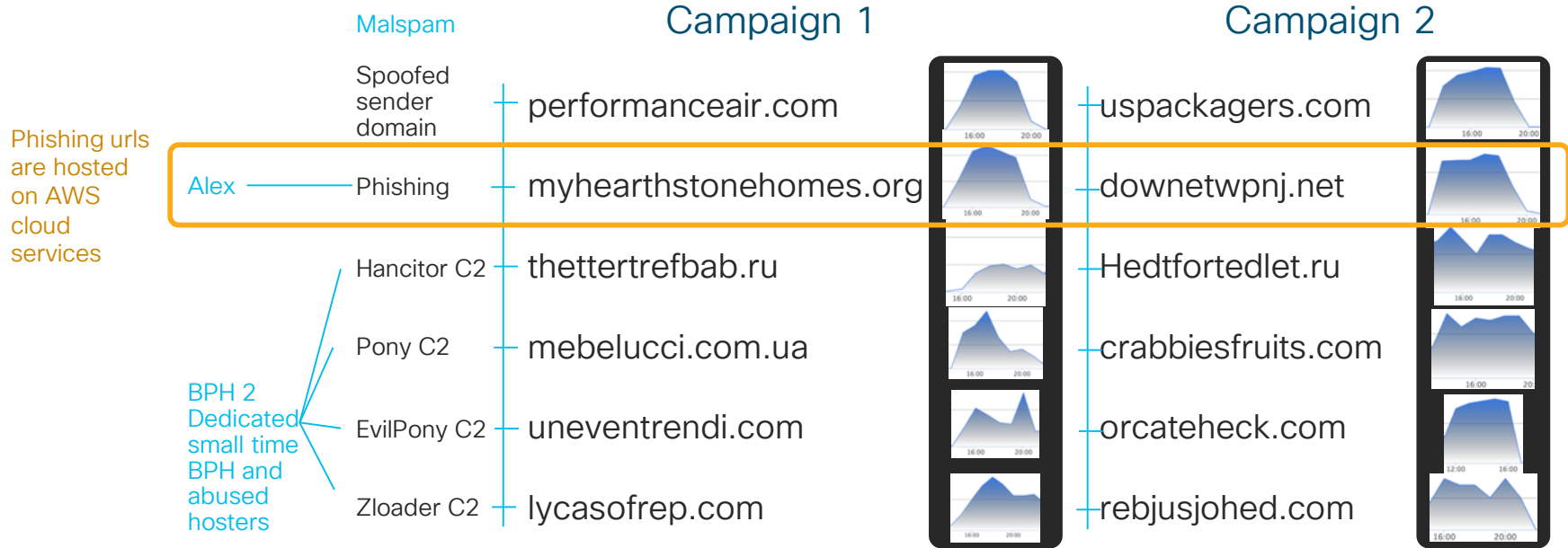
# Insight into 'heymamaradio.com' malicious IP hosting

## IP Addresses

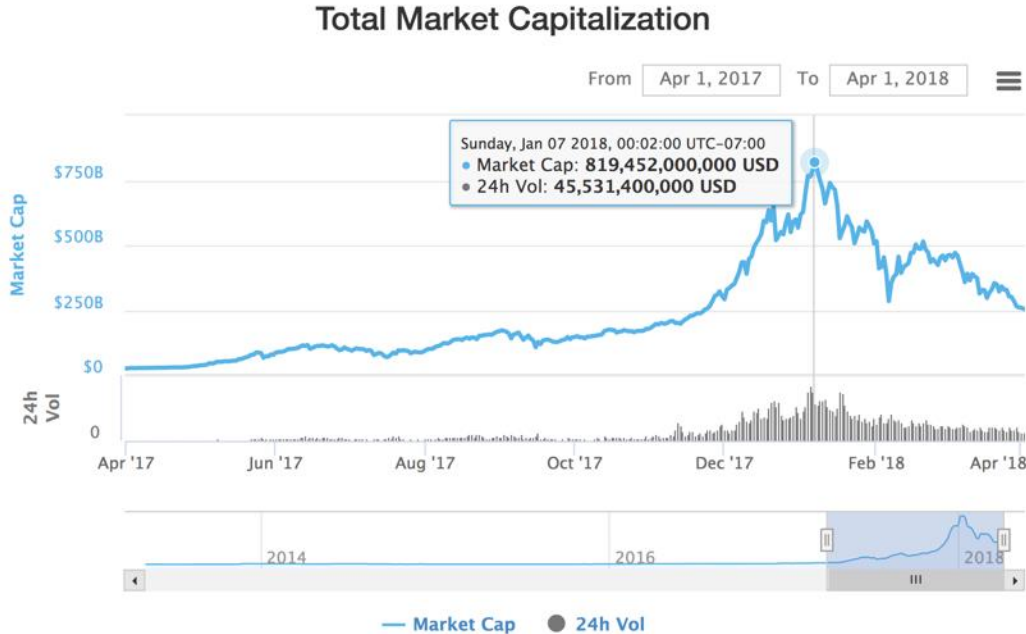
| First seen | Last seen | IPs  |
|------------|-----------|--|
| 9/5/17     | 9/5/17    | 185.180.231.238 (TTL: 600) 47.91.75.193 (TTL: 600) 54.87.201.155 (TTL: 600)                          |
| 9/4/17     | 9/4/17    | 185.180.231.238 (TTL: 600) 52.14.244.225 (TTL: 600) 54.84.39.209 (TTL: 600) 54.87.201.155 (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)   |

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



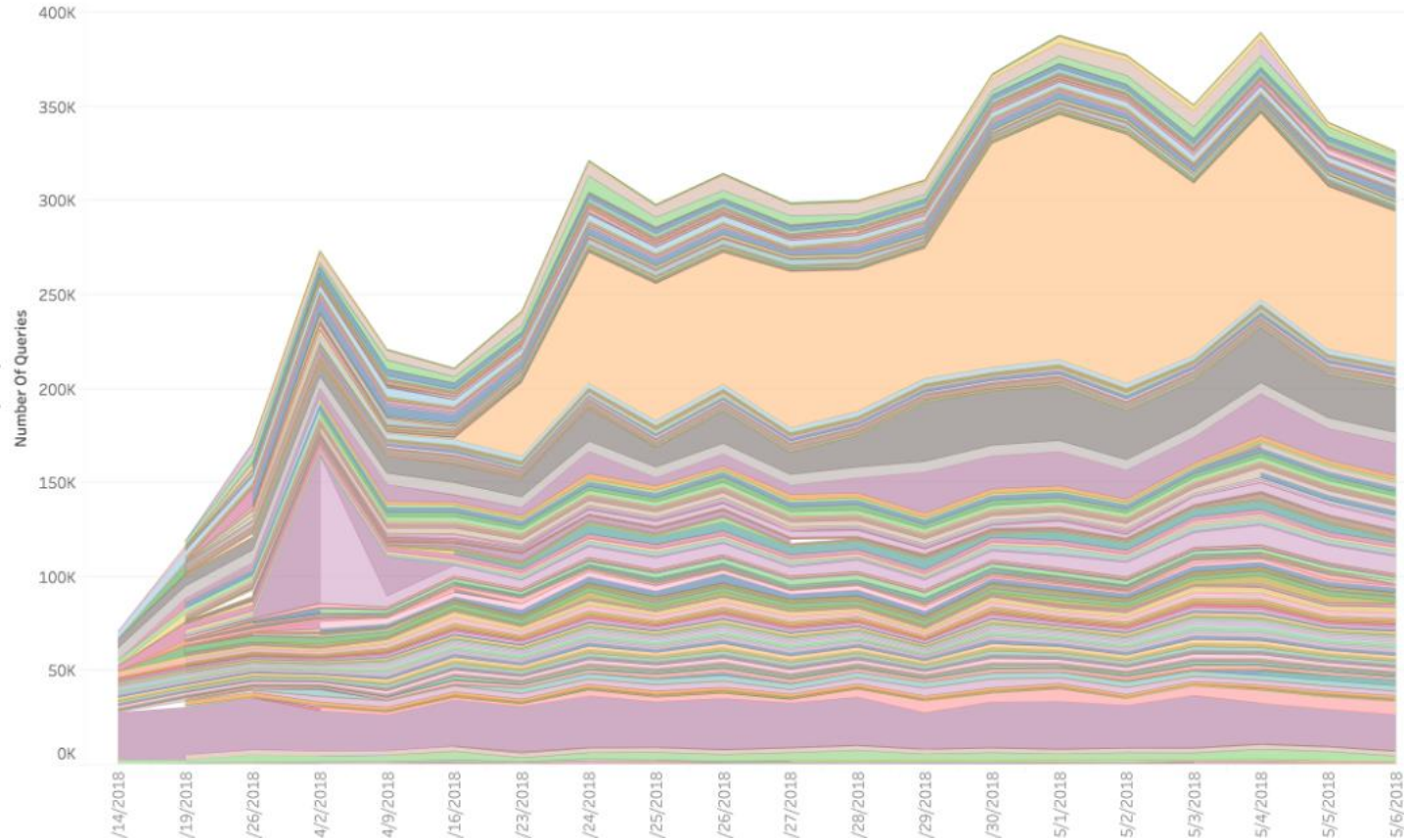
# Cryptocurrency's Meteoric Rise



- In less than one year we saw the crypto market cap go from 26B to north of 835B
- The crypto market is going mainstream, but it is still in the wild west stage
- Under regulated, highly volatile, and full of malicious actors looking to score it big and stay anonymous

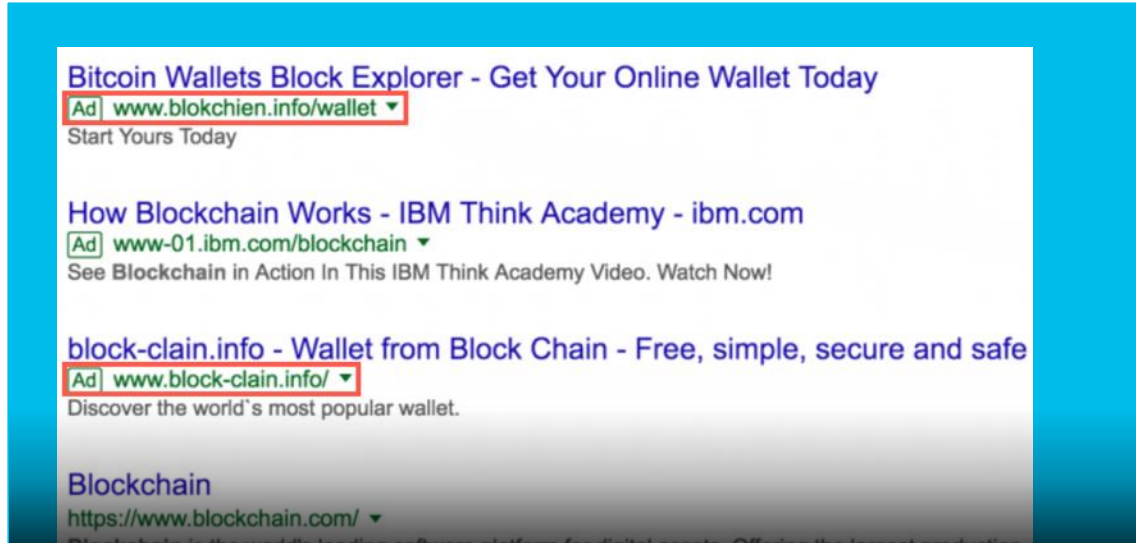
Source: [coinmarketcap.com](https://coinmarketcap.com)

# Cryptomining Volume Across Resolvers

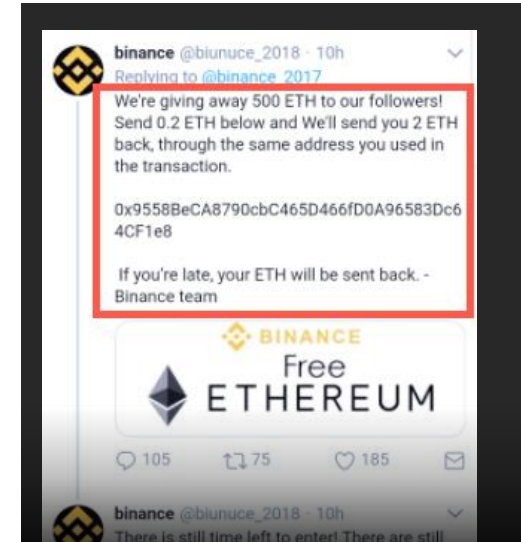


# Crypto Phishing and Scams

Crypto exchange phishing sites are on the rise and they are using advertisements on search engines to lure people into giving up their credentials



A screenshot of search engine results for Bitcoin wallets. The results are listed on a white background with a blue header. The first result is titled "Bitcoin Wallets Block Explorer - Get Your Online Wallet Today" and includes an advertisement link for "www.blokchien.info/wallet" which is highlighted with a red box. The second result is titled "How Blockchain Works - IBM Think Academy - ibm.com" and includes an advertisement link for "www-01.ibm.com/blockchain" highlighted with a green box. The third result is titled "block-clain.info - Wallet from Block Chain - Free, simple, secure and safe" and includes an advertisement link for "www.block-clain.info/" highlighted with a red box. The fourth result is titled "Blockchain" and includes a link for "https://www.blockchain.com/" highlighted with a green box.



A screenshot of a tweet from the account "binance @binuuce\_2018" replying to "@binance\_2017". The tweet text, enclosed in a red box, reads: "We're giving away 500 ETH to our followers! Send 0.2 ETH below and We'll send you 2 ETH back, through the same address you used in the transaction." Below the text is a hexadecimal address: "0x9558BeCA8790cbC465D466fD0A96583Dc64CF1e8". The tweet also includes the text "If you're late, your ETH will be sent back. - Binance team" and a "BINANCE Free ETHEREUM" graphic. The tweet has 105 replies, 75 retweets, and 185 likes.

We're giving away ETH!  
Just send me 0.2 ETH and  
I'll send you back 2 ETH.  
Send me your crypto to the  
address below...

# Crypto Phishing

www.bivnance.com = www.binance.com Right?

The screenshot shows a browser window with the URL <http://www.bivnance.com>. The page layout is a dark-themed header with the Binance logo and navigation links. Below the header, there are promotional banners for macOS, BINANCE VIETNAM, DEXATHON, and QLC. At the bottom, there is a market data section with a table of trading pairs.

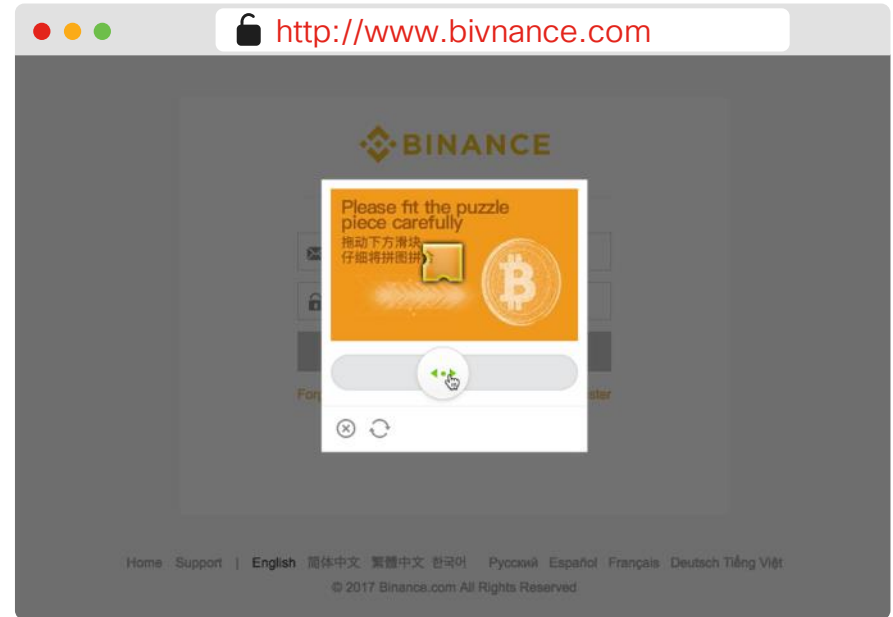
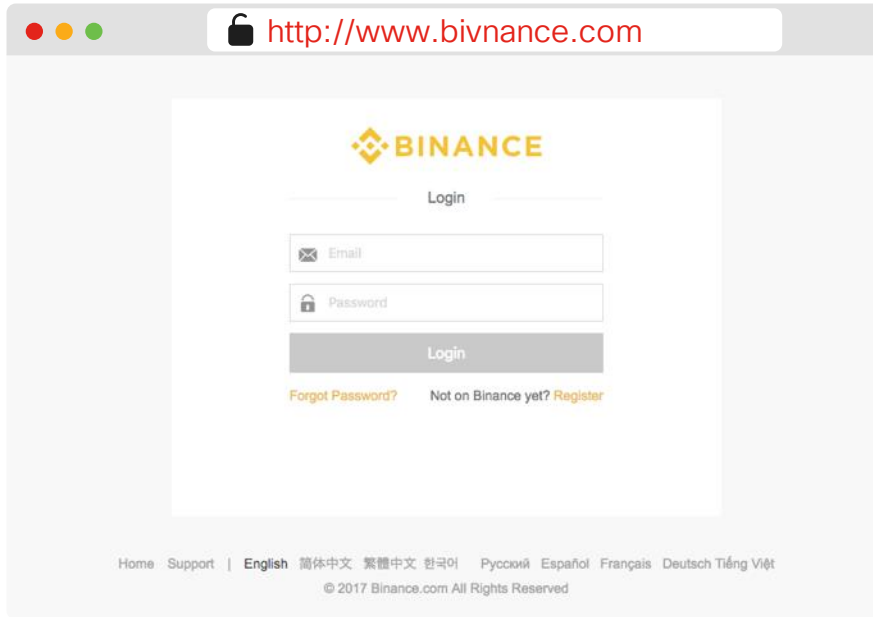
| Pair    | Last Price         | 24h Change | 24h High  | 24h Low   | 24h Volume ↓  |
|---------|--------------------|------------|-----------|-----------|---------------|
| TRX/BTC | 0.0000489 / \$0.03 | -5.63%     | 0.0000496 | 0.0000436 | 8,926.0532962 |

The screenshot shows a browser window with the URL <https://www.binance.com>. The page layout is identical to the phishing site, but the URL is secure (https) and the data values in the market table are different.

| Pair    | Last Price         | 24h Change | 24h High  | 24h Low   | 24h Volume ↓   |
|---------|--------------------|------------|-----------|-----------|----------------|
| TRX/BTC | 0.0000467 / \$0.03 | -5.47%     | 0.0000497 | 0.0000436 | 8,960.64975453 |

# Crypto Phishing

www.bivnance.com login looks legitimate **Right?**





# Crypto Phishing

What do we know about  
www.bivnance.com?

 Investigate

SEARCH PATTERN SEARCH

bivnance.com

INVESTIGATE

## WHOIS Record Data

Registrar Name **Center of Ukrainian Internet Names (UKRNames)** IANAID: 1436

Created: February, 16, 2018

Updated: February, 16, 2018

Email Address

**black13@unseen.is**

Associated Domains

15 Total - 4 malicious

IPs

**195.123.225.64 (TTL: 3600)**

# Crypto Phishing

Domains Associated with black13@unseen.is

| Domain Name  | Security Categories | Content Categories | Last Observed |
|--|---------------------|--------------------|---------------|
| <a href="http://myethxwallet.com">myethxwallet.com</a>         | Phishing            |                    | Current       |
| <a href="http://myethxrwallet.com">myethxrwallet.com</a>       | Phishing            |                    | Current       |
| <a href="http://mynotherwallet.com">mynotherwallet.com</a>     | Phishing            |                    | Current       |
| <a href="http://nnyettiervwailet.com">nnyettiervwailet.com</a> | Phishing            |                    | Current       |

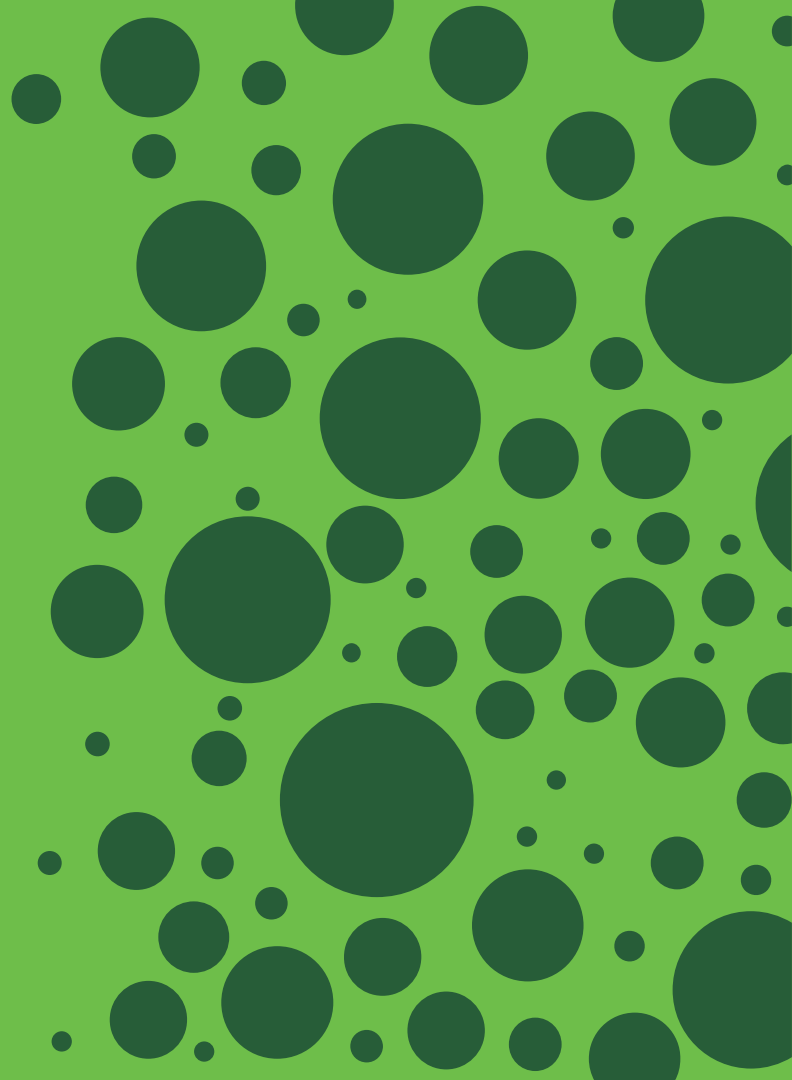
Known domains hosted by 195.123.225.64

[bitinance.com](http://bitinance.com) [bivnance.com](http://bivnance.com) [www.bilinance.com](http://www.bilinance.com) [www.btnance.com](http://www.btnance.com) [biginance.com](http://biginance.com)  
[blinance.com](http://blinance.com) [www.bilinance.com](http://www.bilinance.com) [www.bivnance.com](http://www.bivnance.com) [mail.bwnance.com](http://mail.bwnance.com)  
[resource.blimace.com](http://resource.blimace.com) [www.bilrnance.com](http://www.bilrnance.com) [bvnance.com](http://bvnance.com) [www.blimance.com](http://www.blimance.com)  
[www.bwnance.com](http://www.bwnance.com) [bilinance.com](http://bilinance.com) [www.bornance.com](http://www.bornance.com) [www.bvnance.com](http://www.bvnance.com)  
[mail.bilrnance.com](http://mail.bilrnance.com) [bwnance.com](http://bwnance.com) [mail.bvnance.com](http://mail.bvnance.com) [ww.bivnance.com](http://ww.bivnance.com) [bilrnance.com](http://bilrnance.com)  
[www.blimace.com](http://www.blimace.com) [bornance.com](http://bornance.com) [btnance.com](http://btnance.com) [bilinamce.com](http://bilinamce.com) [mail.btnance.com](http://mail.btnance.com)  
[blimace.com](http://blimace.com) [resource.bilimance.com](http://resource.bilimance.com) [resource.blimance.com](http://resource.blimance.com) [bimanec.com](http://bimanec.com)  
[blnanco.com](http://blnanco.com) [blnancie.com](http://blnancie.com) [www.binanceit.com](http://www.binanceit.com)

What else is  
**black13@unseen.is**  
after?

Maybe all of your  
ERC20 tokens...

Demo



# Agenda

- What is Cisco Umbrella?
- Making Sense of Big Data
- Real-World Threat Campaigns
- **Putting it into Action**
- Q&A

# Rich API Integration with In-house Systems

YOU CURATE & CORRELATE

WE TAKE IMMEDIATE ACTION



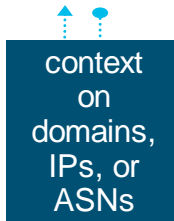
logs



logs



domains



## UMBRELLA

### Enforcement & Visibility

Network security service that blocks Internet activity attributed to domains. And retain all DNS logs for as long as required

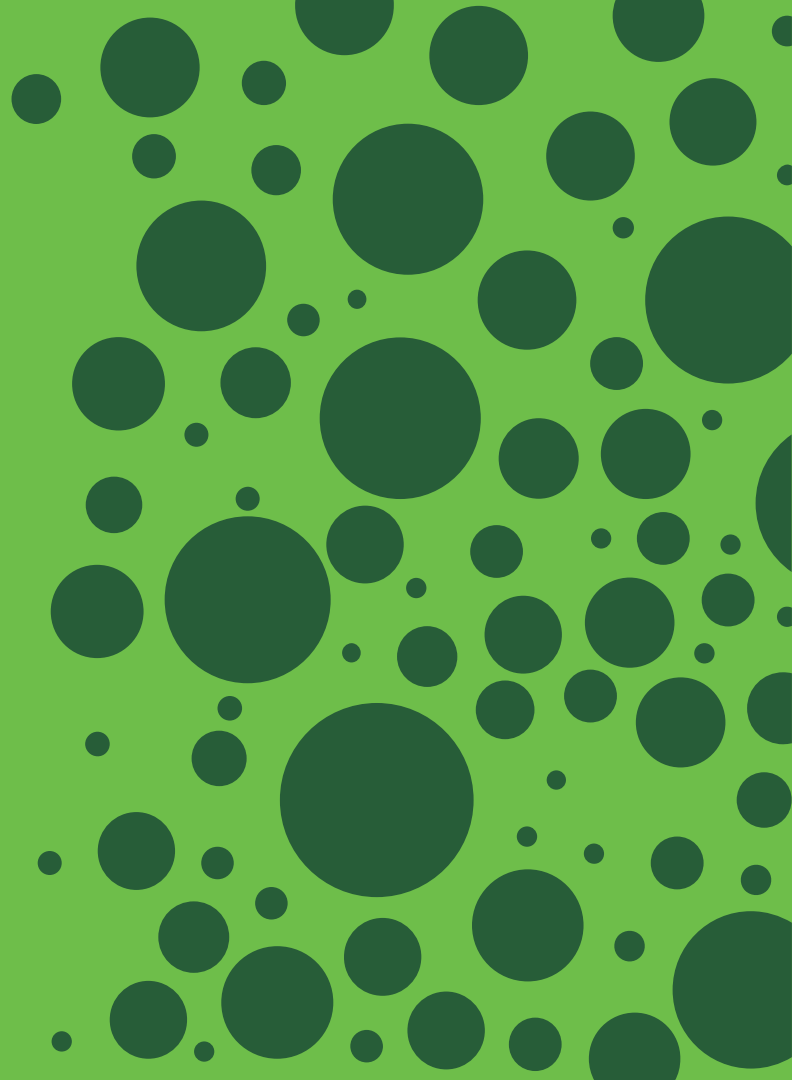


## INVESTIGATE

### Intelligence & Enrichment

Live graph of global DNS requests and contextual data  
Features our passive DNSDB

Demo



# Capture The Flag – Advanced Threats

- Become a Better Defender by gaining hands-on experience with:
  - Real-world attack techniques
  - Threat investigation strategies
- Walk-In Game in **THE HUB** (Monday to Friday)
- Solve Challenges to Win Prizes
- Search for LTRSEC-2016 in the Sessions Catalogue in the Cisco Live App

#CiscoSecurityCTF #CTF

# Resources

- Umbrella Blog – Researchers posting research: <https://umbrella.cisco.com/blog>
- Talos Intelligence Blog – <http://blog.talosintelligence.com>
- OpenGraphiti – Free 3D graphic tool: <http://www.opengraphiti.com>
- OpenGraphiti Miner Github: <https://github.com/opendns/og-miner>
  - You need an Investigate API key
- Umbrella Free Account: <http://signup.umbrella.com> You need to get your Cisco team to convert that to include Investigate with API access



# Easiest Proof Of Value

Go Try Umbrella

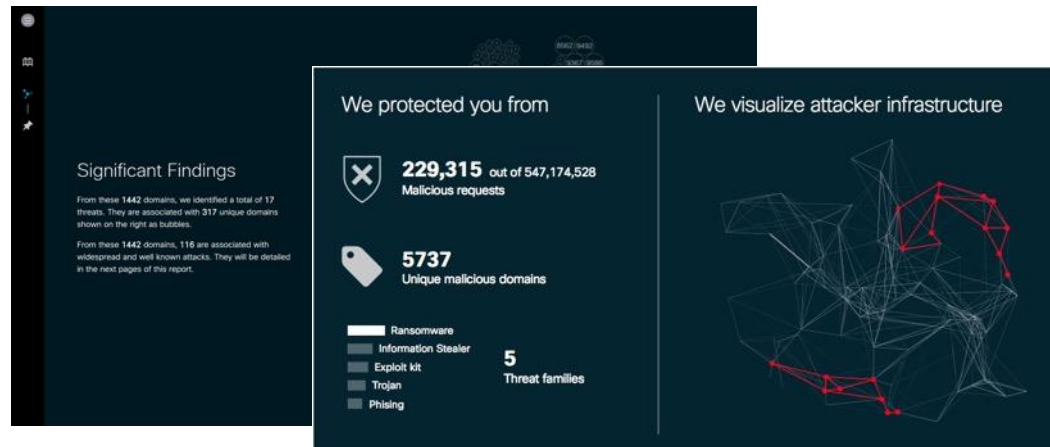
Start protecting in minutes

1 Sign up

2 Point Your DNS

3 Done

Cisco *live!*



1 How effective is this solution?

2 How does it compare (or add) to my current security stack

3 Does it deliver great time-to-value?

# Actions

If there is one action you can take away with you today is to go online and subscribe to a **FREE** 14 day trial with Cisco Umbrella using the following link:

<https://signup.umbrella.com>

# Agenda

- What is Cisco Umbrella?
- Making Sense of Big Data
- Real-World Threat Campaigns
- Putting it into Action
- Q&A

# Hey malicious infrastructure, we see you.

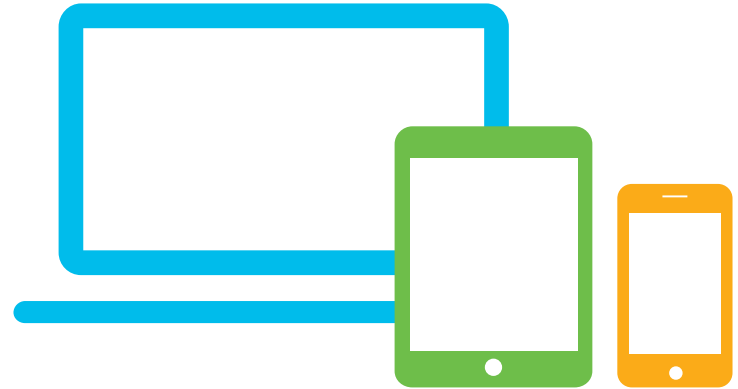
Introducing your first line of defense against threats – network security that stops attacks before they start.



# Complete your online session survey

- Please complete your Online Session Survey after each session
- Complete 4 Session Surveys & the Overall Conference Survey (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Events Mobile App or the Communication Stations


Don't forget: Cisco Live sessions will be available for viewing on demand after the event at [cislive.cisco.com](https://cislive.cisco.com)



# Continue Your Education




Demos in the Cisco Showcase



Walk-in self-paced labs



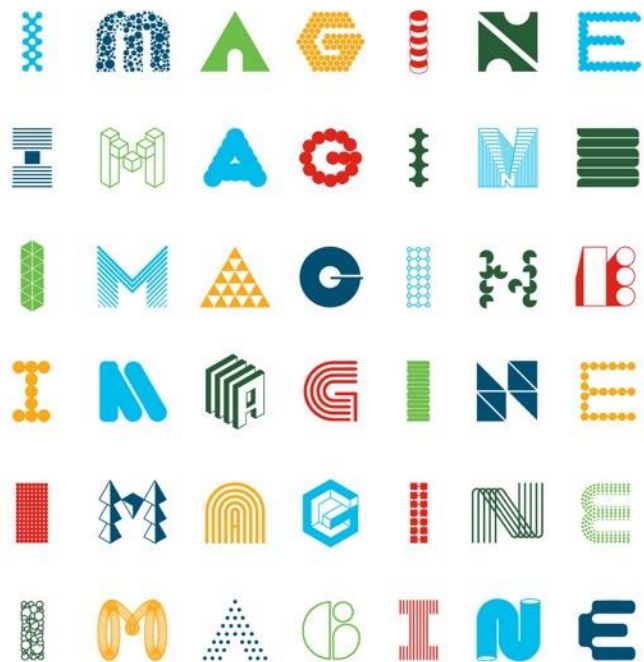
Meet the engineer 1:1 meetings



Related sessions



Thank you



INTUITIVE

# Actions

If there is one action you can take away with you today is to go online and subscribe to a **FREE** 14 day trial with Cisco Umbrella using the following link:

<https://signup.umbrella.com>





INTUITIVE