cisco Engage

On-line každých 14 dní

Cisco Tech Club Webináře

You make **possible**

cisco Engage

Prečo je Cisco Umbrella efektívna v boji s kyberzločinom nielen v dnešných dňoch

28.4.2020

Peter Mesjar
Technical Solutions Architect
pmesjar@cisco.com

CISCO CERTIFIED CCIE 10 YEARS

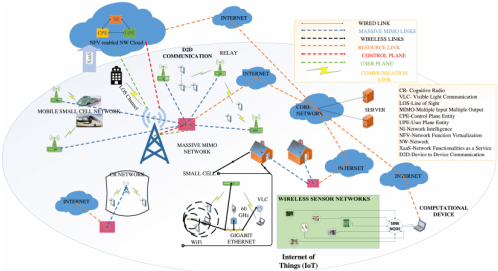
CISSP®

Agenda

- Ako používame DNS
- Ako Umbrella analyzuje DNS dátové toky
- Ako “ne“obchádzať Umbrella

DNS je kritická služba naprieč celou IT infraštruktúrou

Každé zariadenie



Akákoľvek TCP/IP počítačová sieť

Všetky operačné systémy

68% organizácií nemonitoruje DNS

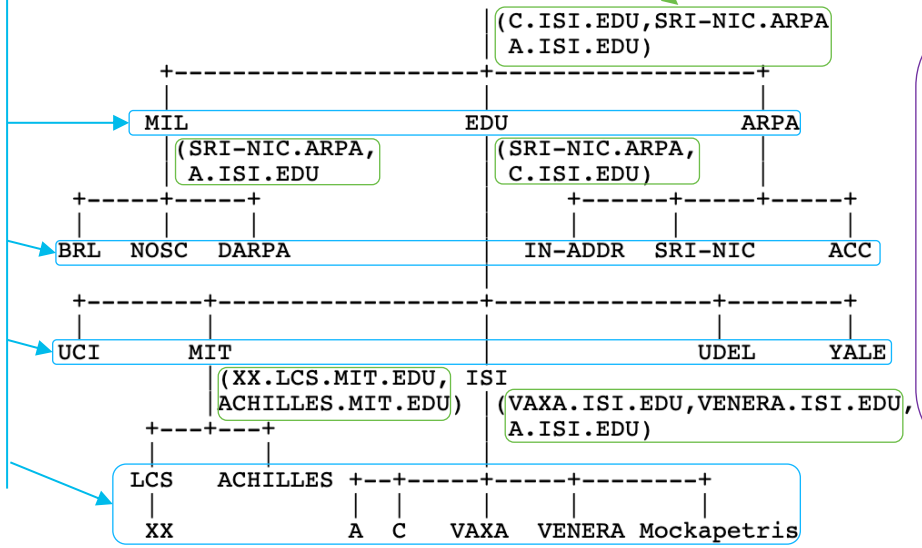
Štruktúra DNS

Tri základné komponenty (RFC 1034):

Domain name space + Resource Records

Name Servers

Resolvers -> *Umbrella*

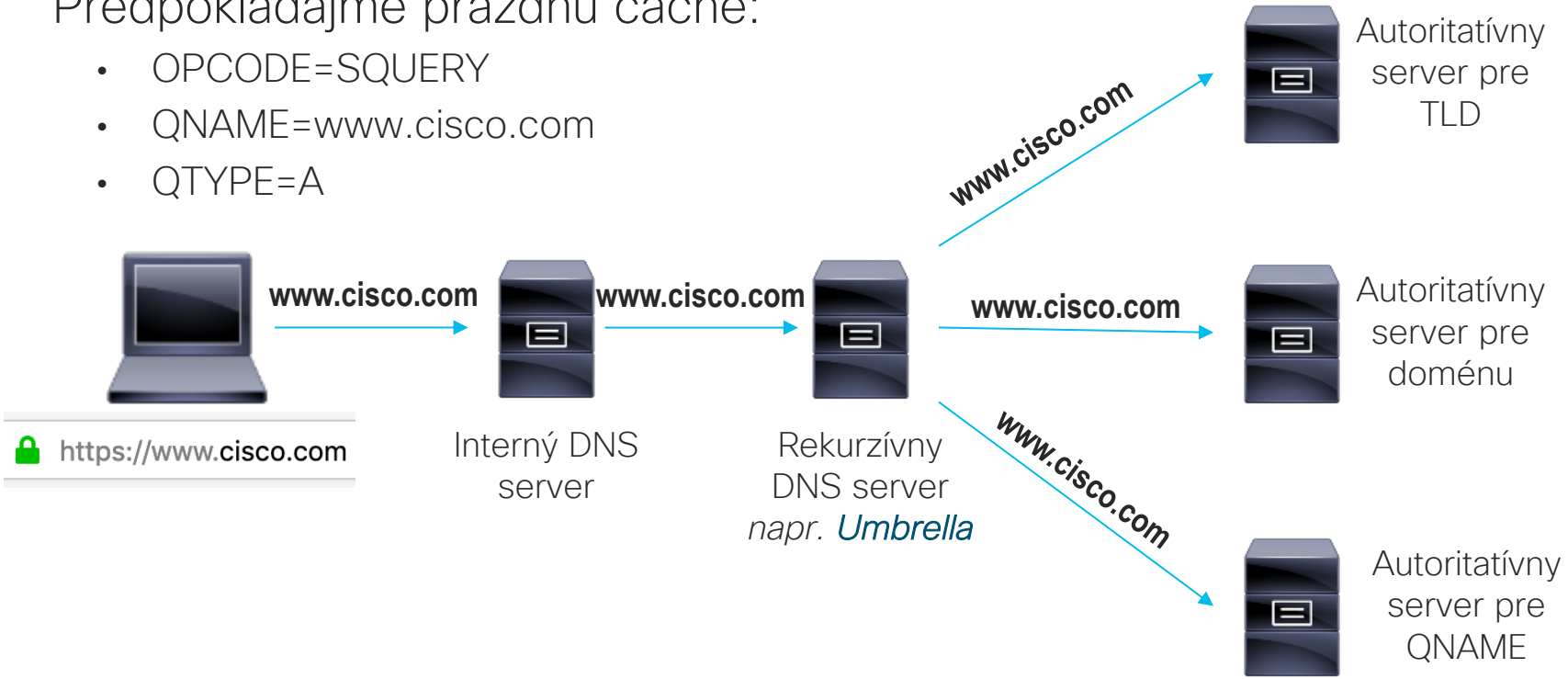


ISI.EDU.	MX	10 VENERA.ISI.EDU
	MX	10 VAXA.ISI.EDU
VENERA.ISI.EDU.	A	128.9.0.32
	A	10.1.0.52
VAXA.ISI.EDU.	A	10.2.0.27
	A	128.9.0.33

Ako typicky používame DNS

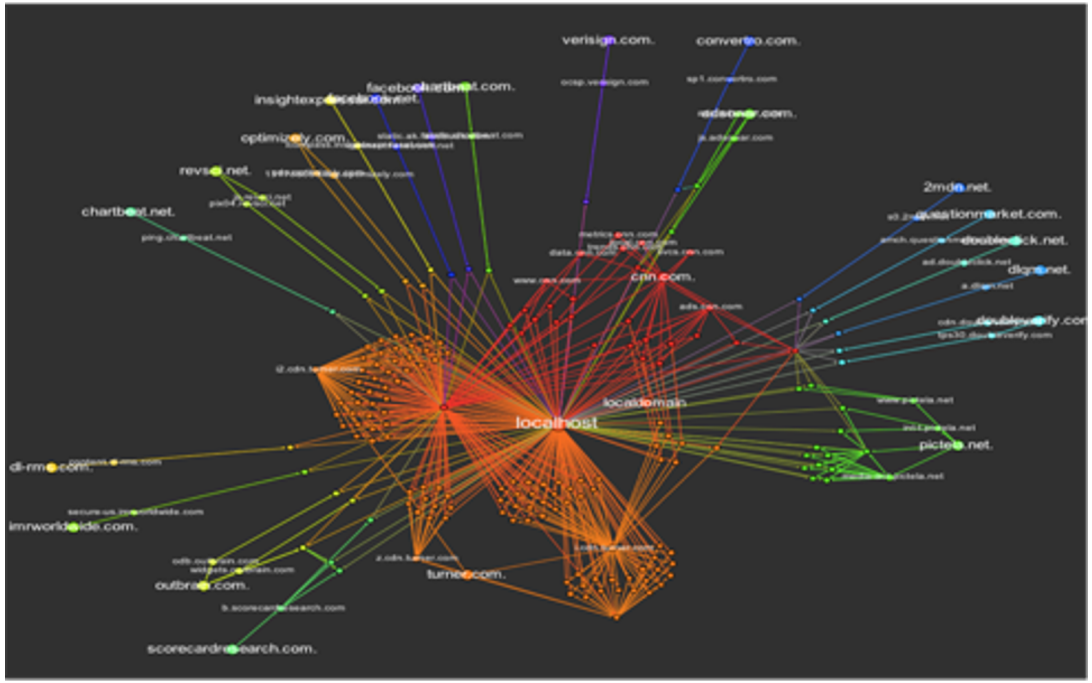
Predpokladajme prázdnu cache:

- OPCODE=SQUERY
- QNAME=www.cisco.com
- QTYPE=A



https://support.umbrella.com/hc/en-us/articles/360032551931-Cisco-Umbrella-DNS-and-QNAME-Minimization

Čo sa deje pri návšteve jednej webovej stránky?



CNN[.]COM:

26 Domains
39 Hosts
171 Objects
557 Connections

Umbrella: A Single Global Recursive DNS Service

Benefits

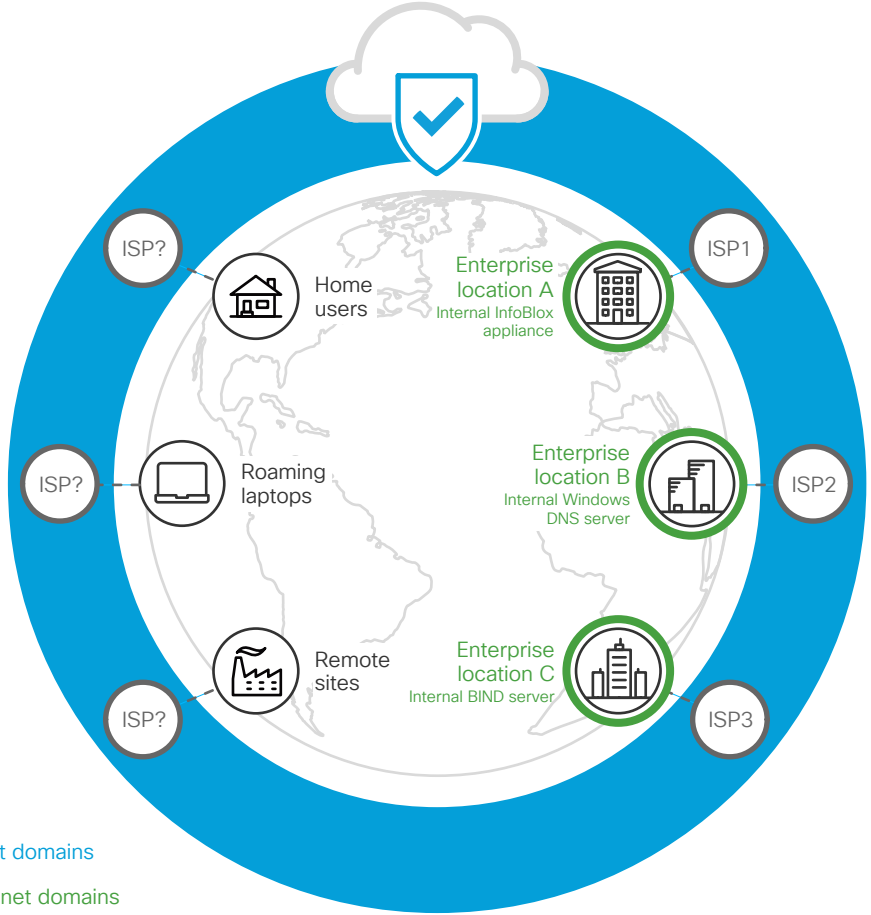
Global internet activity visibility

Network security w/o adding latency

Anycast high availability

Consistent policy enforcement

Internet-wide cloud app visibility



Recursive DNS for internet domains

Authoritative DNS for intranet domains

Umbrella's View of the Internet

200B
requests per day

100M
daily active users

18K
enterprise customers

190+
countries worldwide

https://umbrella.cisco.com/why-umbrella/global-network-and-traffic

Agenda

- Ako používame DNS
- Ako Umbrella analyzuje DNS dátové toky
- Ako “ne“obchádzať Umbrella

Anatómia útoku z pohľadu DNS

Before (pre-compromise)

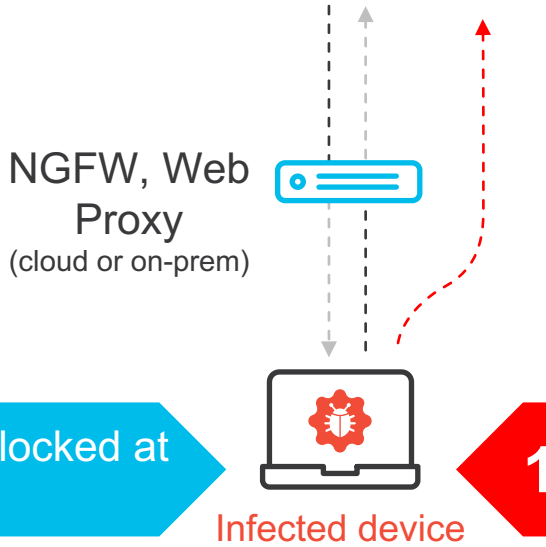
- Reconnaissance and infrastructure setup
- Domain registration, IP, ASN intelligence
- Monitor adaption based on results

During (compromise)

- Patient zero hit

After (post-compromise)

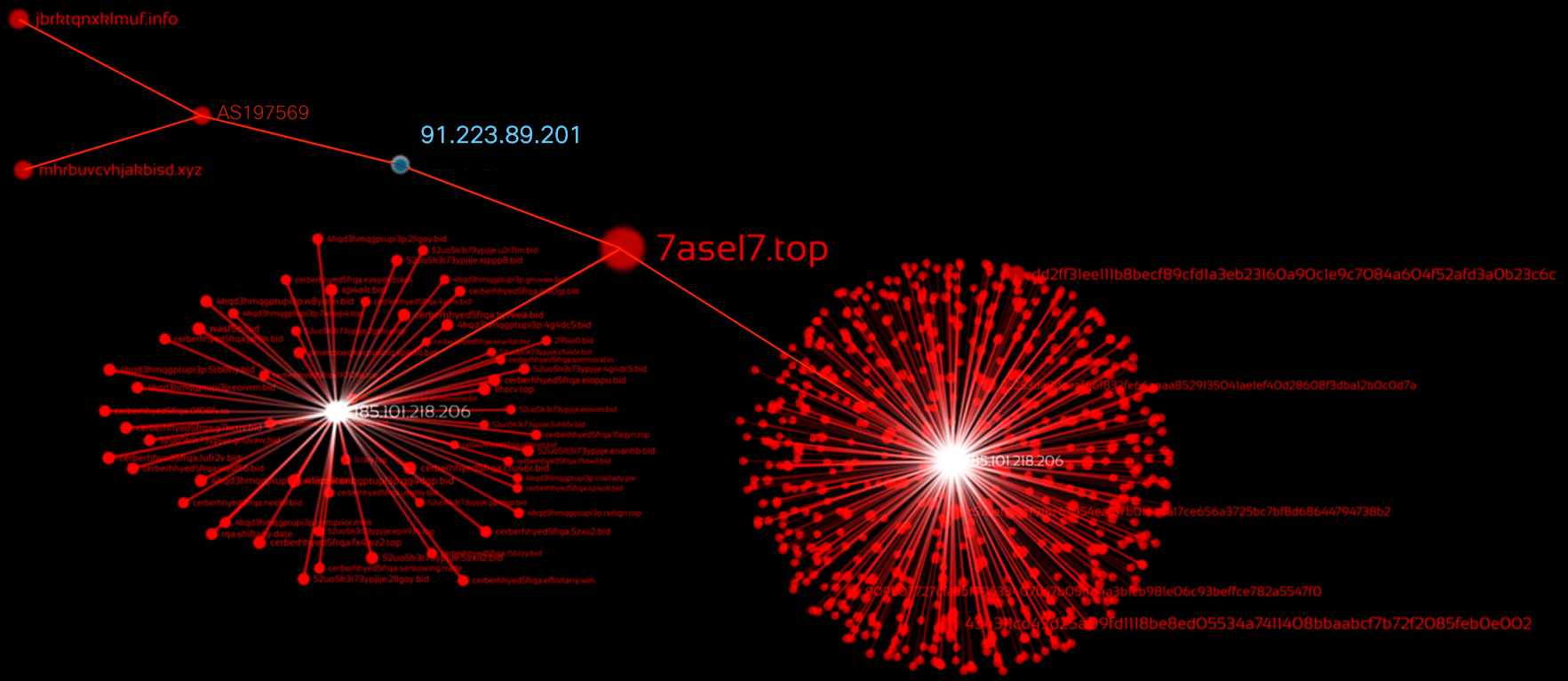
- Target expansion
- Wide-scale expansion
- Defense signatures built



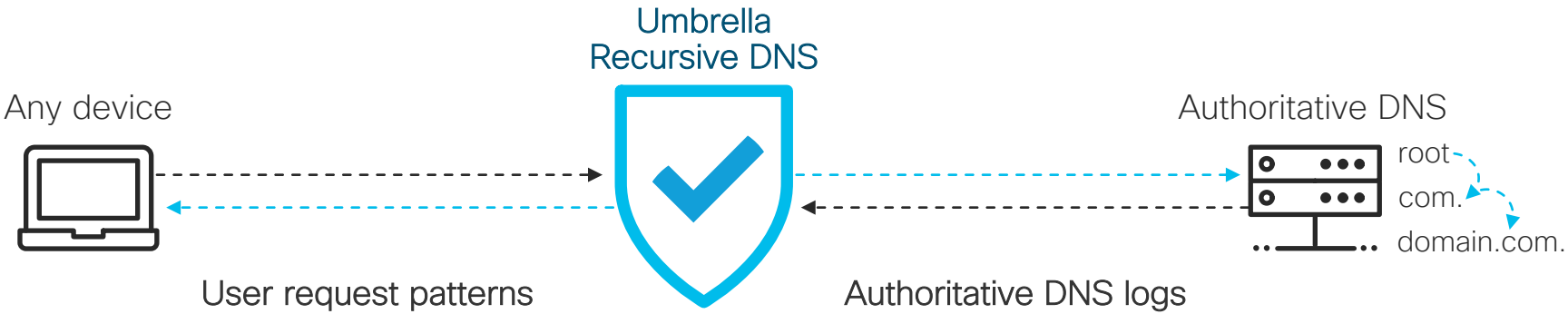
91% of C2 can be blocked at the DNS layer

15% of C2 bypasses web ports 80 & 443

Our View of the Internet



Ako získavame dáta



User request patterns

Used to detect:

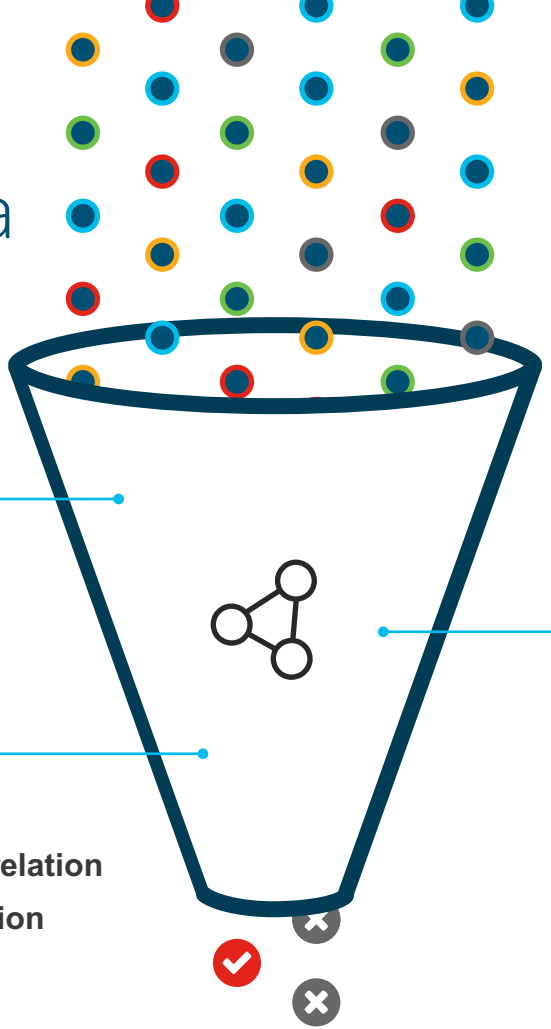
- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative DNS logs

Used to find:

- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains

Využitie dát algoritmami strojového učenia



2M+ live events per second

11B+ historical events

Guilt by inference

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

Guilt by association

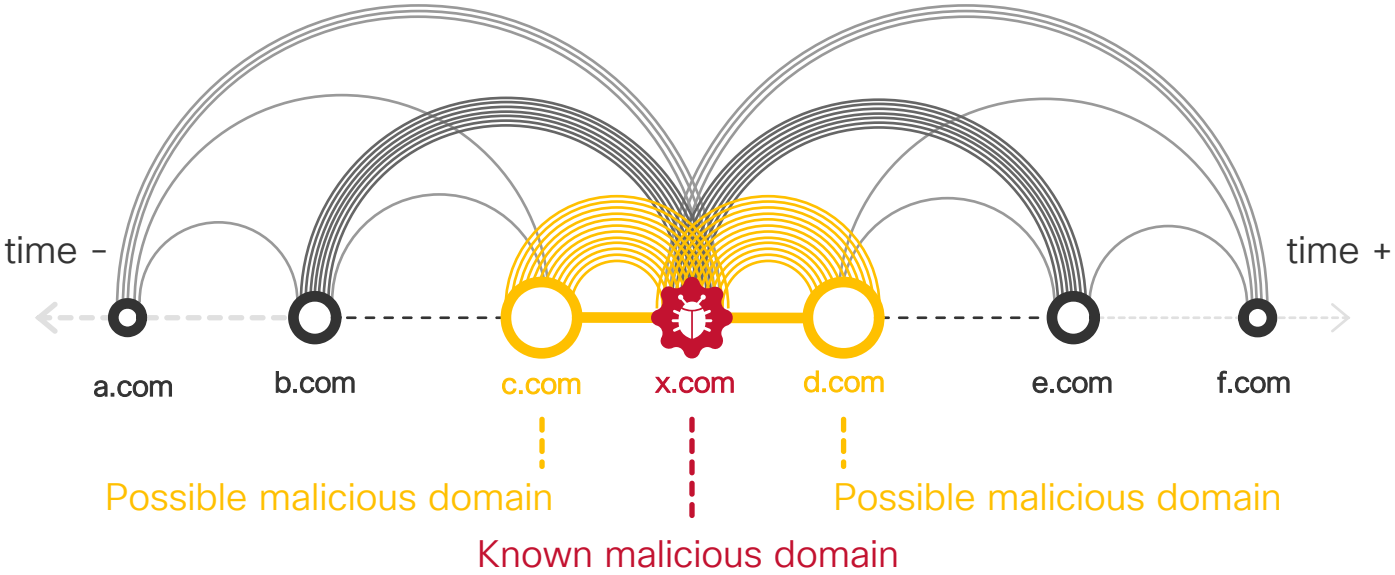
- **Predictive IP Space modeling**
- **Passive DNS and WHOIS correlation**
- **Threat Grid malware association**

Patterns of guilt

- **Spike Rank model**
- **Natural Language Processing Rank model**
- **Live DGA (Domain Generation Algorithm) Detection**
- **Punycode** (RFC 3492)

Co-occurrence Model

Domains guilty by inference



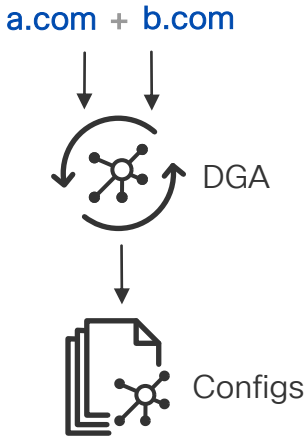
Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

Live DGA Prediction

Automated at an unparalleled scale

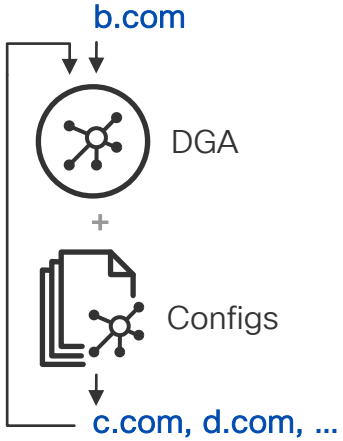
Live DNS log stream

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

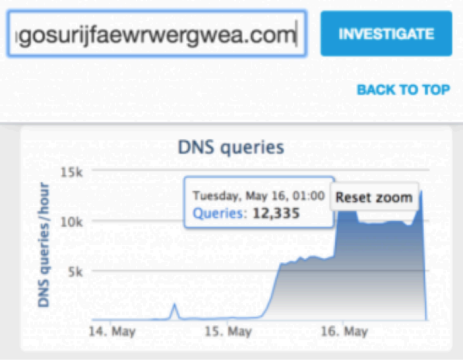
Combine newly-identified configs with DGA to identity C2 domains continuously

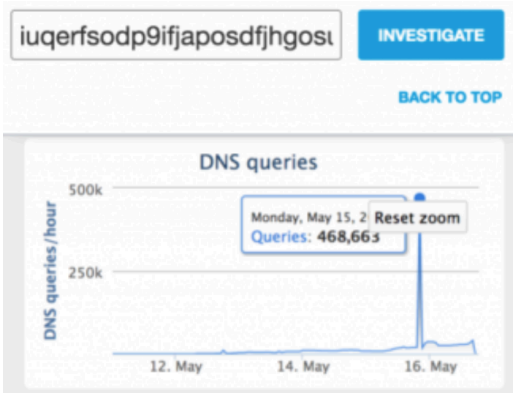
Automate blocking pool of C2 domains

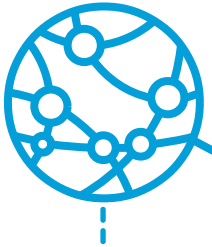
Used by thousands of malicious samples now and in the future

Spike Rank Model

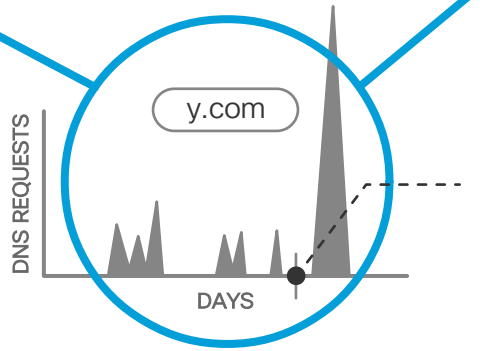
Patterns of guilt







Massive amount of DNS request volume data is gathered and analyzed

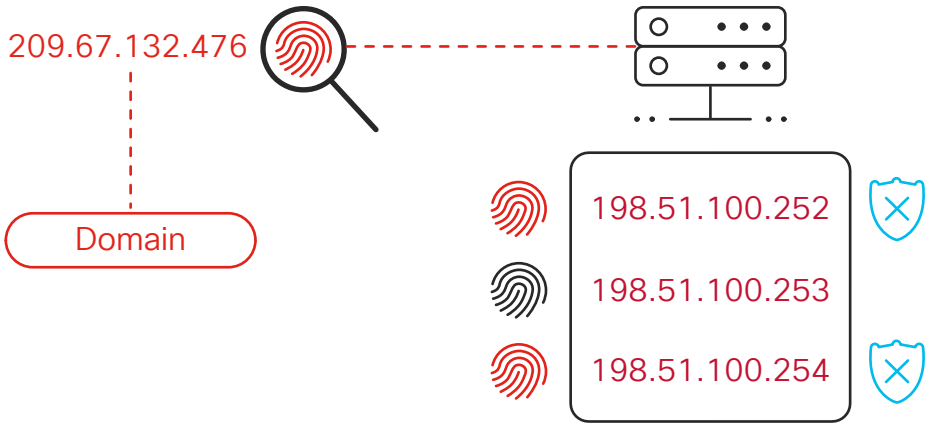


y.com is blocked before it can launch full attack

DNS request volume matches known exploit kit pattern and predicts future attack

Predictive IP Space Monitoring

Guilt by association

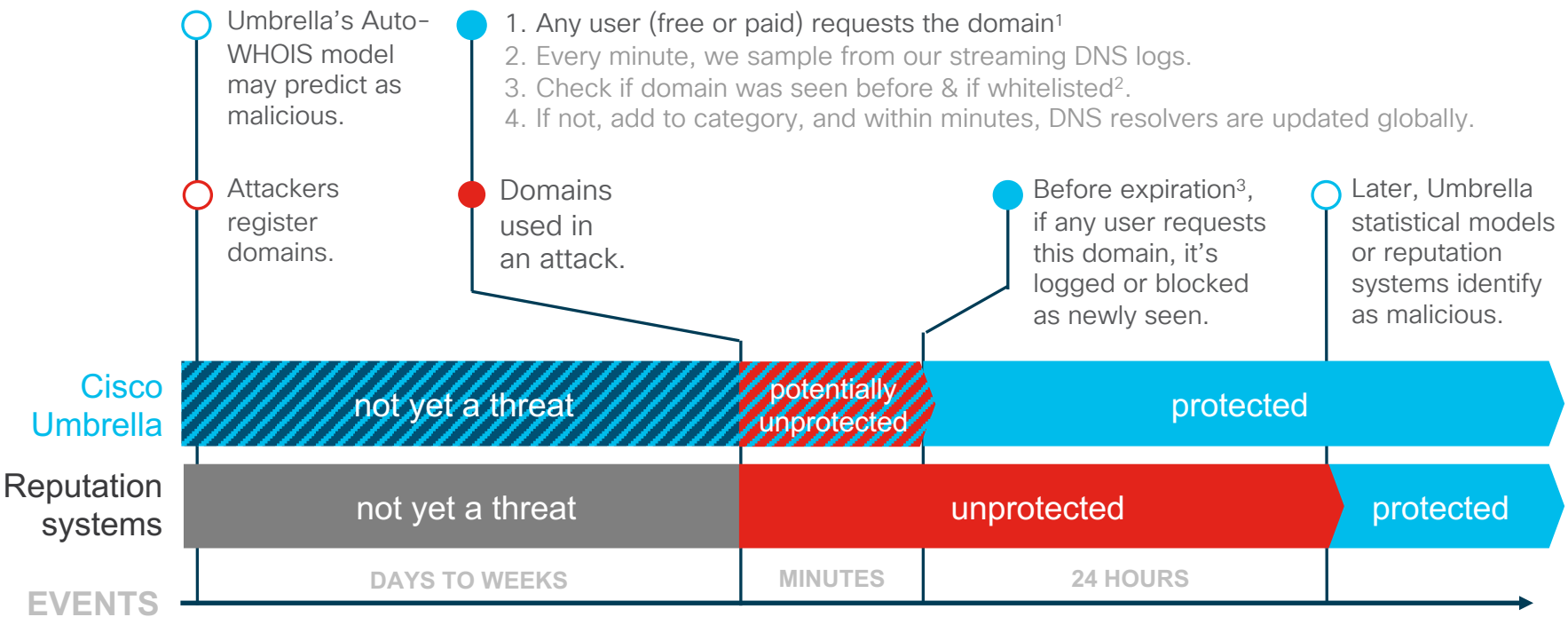


Pinpoint suspicious domains and observe their IP's fingerprint

Identify other IPs – hosted on the same server – that share the same fingerprint

Block those suspicious IPs and any related domains

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.

Predictive Detector: NLPRank

Identifies malicious domain-squatting, targeted C2 and phishing domains

1

Analyse APT reports

2

Patterns in domains used in attacks

- Domain spoofing used to obfuscate
- Often saw brand names and terms like “update”
- Examples: update-java[.]net adobe-update[.]net

3

Checked data & confirmed intuition

- Dictionary & company names merged
- Change small # of characters to obfuscate
- Domains hosted on ASNs unassociated w/company
- Different webpage fingerprints

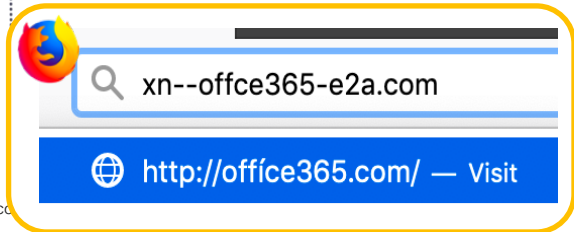
4

Built model and continue to tune

- Detects fraudulent brand domains:

1inkedin.net

linkedin.com



NLP = natural language processing

Umbrella Investigate Demo: Proactive Blocking

sso.anbtr.com

Details for sso.anbtr.com

This domain is currently in the Umbrella block list

Co-occurrences

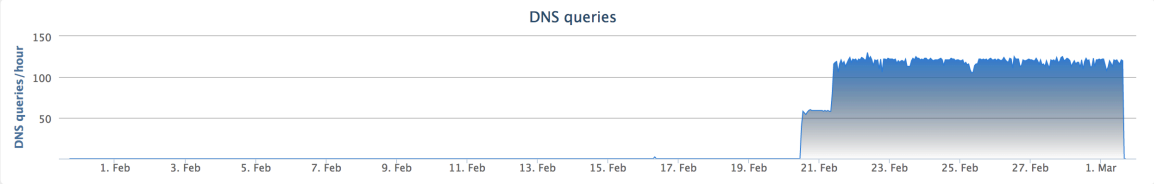
report.serverpol.net (33.65)

Details for report.serverpol.net

SEARCH IN GOOGLE

SEARCH IN VIRUSTOTAL

This domain is currently in the Umbrella block list



Timeline

Current Categorization: Malware

categories Added

Feb 10, 2018

Malware Added

First Queried: Feb 10, 2018

Registered: Jan 19, 2018

Newly Seen Domains example

Security Category: Newly Seen Domains

sednerenforbo.info	Allowed	Malware, Newly Seen Domains	Jan 30, 2019 at 6:16 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 5:34 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 5:34 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 5:16 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 5:15 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 5:14 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:50 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:35 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:26 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:26 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:19 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:16 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:15 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 4:09 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 3:51 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 2:51 PM
sednerenforbo.info	Allowed	Newly Seen Domains	Jan 30, 2019 at 2:43 PM

Page: 1 Rows per page: 100 1 - 45 of 45

Malware added

3,5 hours later

1st seen

Umbrella Investigate Demo: Blocking Malicious Domains Based of Inference

kdvm5fd6tn6jsbwh.onion.to

INVESTIGATE

Details for kdvm5fd6tn6jsbwh.onion.to

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 185.100.85.150

Details for 185.100.85.150

Hosting 27 malicious domains for 1 week

This IP is currently in the Umbrella block list as malware

AS

Prefix	ASN	Network Owner Description
185.100.84.0/23	AS 200651	FLOKINET, SC 86400

Malicious domains hosted by 185.100.85.150

pmenboeqhyrpvomq.onion.to 7vhbukzxypxh3xfy.onion.to ccjlwb22w6c22p2k.onion.to 6dtxgqam4crv6rr6.onion.to i3ezlvkoi7fwyood.onion.to f5xraa2y2ybtrefz.onion.to krrewiaog3u4npcg.onion.to f76kjv7z3rnymawr.onion.to 2v3ojv6gnmpuqiv6.onion.to jhomitevd2abj3fk.onion.to kpai7ycr7jxqkilp.onion.to ejmv6pxsuwqrofa3.onion.to teensexaqb2wbloa.onion.to zpr5huq4bgmutfnf.onion.to zjfq4lnfbs7pncr5.onion.to 2dzmdacevbadfjvu.onion.to mphtadhci5mrdlju.onion.to 25z5g623wpqpdwis.onion.to zutzt67dcxr6mxcn.onion.to i5tbhsq567bemcgp.onion.to twbers4hmi6dc65f.onion.to 27lelchgcvs2wpm7.onion.to lpholfnvwbukqwye.onion.to 32kl2rwsjvqjeui7.onion.to kpvz7ki2v5agwt35.onion.to satan6dll23napb5.onion.to unocl45trpuoefft.onion.to

Associated Samples

Threat Score	SHA256 Signature	AV Result
100	10a989df54eade354e008122324547bfcec3efd2816ffe994dc56ae898b190eb	
100	3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370	Win.Trojan.TeslaCrypt
100	3488289c3ded3096aa26ad3b2fabbfd94c2d88bc9241738d655b7698c8ba65e1	Win.Malware.Agent22
100	470516ae60f0ee5e61c07c6c216bdbe7397bf8bb6fc73389f70aad37bec67fc5	
100	87f78ea61c32559a40ff736848fd264546af6559102a88031139c54b24f6a9cd	
100	99af3dbc03d800e7c27ef194db9884fa28b49f159dbb033d88221133772df42a	
100	a0c2667576009d1143e93998db8daaf9c1decd242b41a0b820ff6c76d5c309bd	
100	a43ed07b16163340e746e29fbeee2421e1f760f3bb1651a12400a675edfe50b7	
100	e8b4982e5ffa167892cabeb7869ff98614a869d0c2f9566f25b56efc12bd4c93	
100	f52873fafd78d48a587591213c0643e0ddff3cd2afc1095c1e00353d46e96e66	

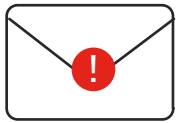
Alex BHP (Bulletproof Hosting Provider) harvests a variety of toxic content

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

Meet the World's Biggest 'Bulletproof' Hoster
https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/

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 and positioned for data extraction

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

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

Thank you for flying with us
Delta Airlines

Maldoc URL

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

Reference: hazmalware.wordpress.com

August 30, 2017: Peak of malicious redirect

myhearthstonehomes.org

INVESTIGATE

Details for myhearthstonehomes.org

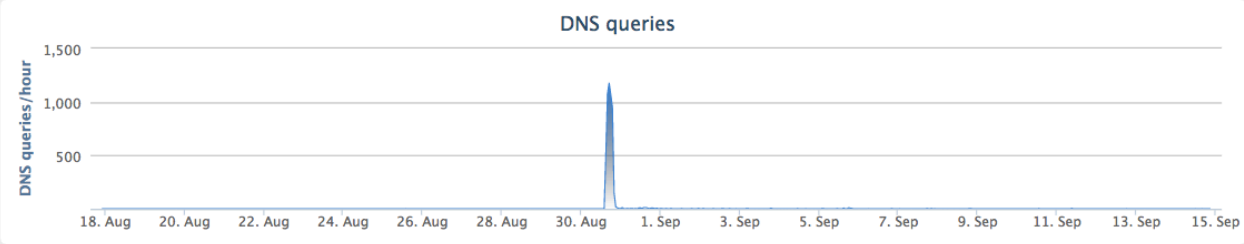
SEARCH IN GOOGLE

SEARCH IN VIRUSTOTAL

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 184.168.221.49

This domain is currently in the Umbrella block list

This domain is associated with the following attack: Hancitor Dropper



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 domain

agentssellingtips.info
heymamaradio.com
rexahunter.com
www.heymamaradio.co
greathomesellingtips.in
wgopodcastbooking.co
zasbiopharm.com
protectorsuperhero.com
myhearthstonehomes.i
ourrealtyguy.us

heymamaradio.com

INVESTIGATE

BACK TO TOP

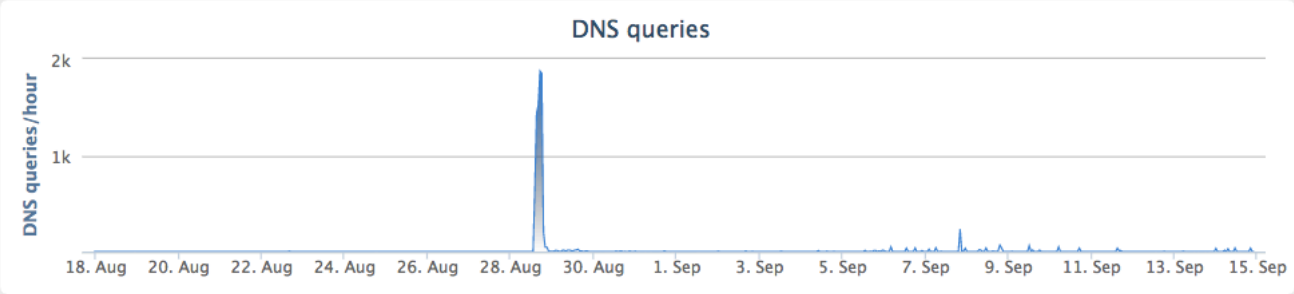
This domain is associated with the following attack: Hancitor Dropper

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 BHP provider. The BHP provider abuses AWS IPs and offers them as hosting space to his criminal customers.

Súčasné zneužívanie 184.168.221.49

SEARCH PATTERN SEARCH

184.168.221.49 INVESTIGATE

Google VirusTotal

Details for 184.168.221.49

Hosting 9 malicious domains

AS

Prefix	ASN	Network Owner Description
184.168.0.0/16	AS 26496	AS-26496-GO-DADDY-COM-LLC, US 86400
184.168.220.0/22	AS 26496	AS-26496-GO-DADDY-COM-LLC, US 86400

Malicious domains hosted by 184.168.221.49

15minutecoronavirustest.com 19covid.app 2020coronavirus.com 2020coronavirusstatistics.com 2020theyearofcovid-19.com 222805.com 31t55.com 3sprouts.in 401kgoldirarollover.com 411coronacovid19.com 4chd.com 4thquarterquarantine.com 50t55.com 51t55.com 53t55.com 6192004.com 6422004.com 69covid.com 71t55.com 76t55.com 81t55.com 86covid.com 95t55.com abagifts.com abejaproducciones.com academynext.com acoronapocalypse.com acoronasurvivor.com actupagainstcovid19.com adascorp.com adioscoronavirusparty.com aftercorona19.net aftercovid-19.com agritechholding.com aidcovid.com alienmade.com aliveaftercorona.com allaboutthecoronaviruscrisis.info allchiro.org allegiant.info ambiasys.info ameericans.com americacovid19.com americanacademycovidsafedentists.com americancovidassociation.com analyticpoweredcovid19.info anti-coronavirus.eu anti-covid.co anticoronapills.com anticoronavirus.me anticoronavirus19.com anticovid19.solutions applycoronavirusloan.com apscovid19.org assistance4corona.com astonishing-gameroll.com athomewithcorona.com auctionagenda.org avpenergy.com awesomeinaustin.com baltimoreaccidents.com bansofamerica.com bayareacovidresponse.org beatcorona.biz beatcovid19.info beatingcovid.com becovidsafe.com bespoke-healthcare.com bettercovid19filtration.com beyondhealthrecords.com binaryliberty.net

Vidieť útok ešte predtým ako sa stane

Data

- 200B DNS requests resolved per day
- Diverse dataset gathered across 100M users across 190 countries and 18K enterprise customers

Security Researchers

- Industry renown researchers across Cisco Talos and Umbrella
- Build models that can automatically classify and score domains and IPs

Models

- Dozens of models continuously analyze millions of live events per second
- Automatically score and identify malware, ransomware, and other threats

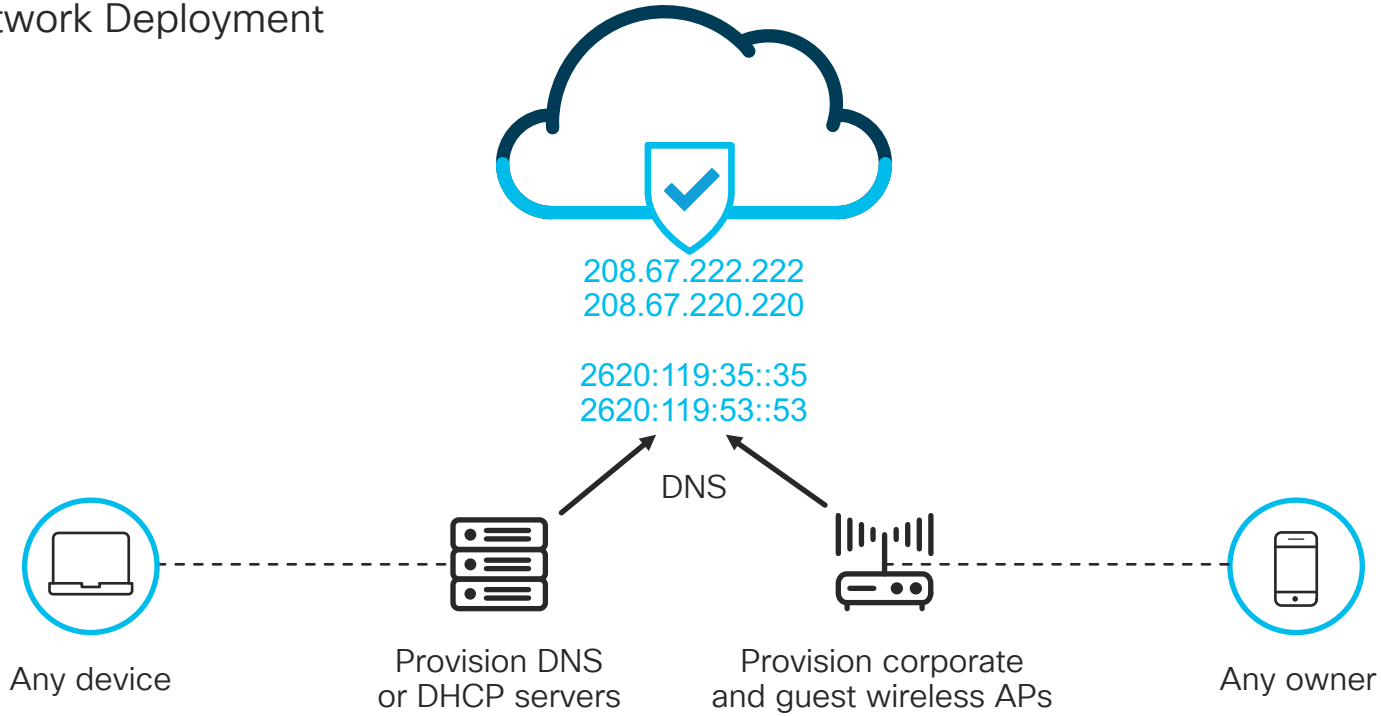
Agenda

- Ako používame DNS
- Ako Umbrella analyzuje DNS dátové toky
- Ako “ne“obchádzať Umbrella

Simplest Security Deployment on the Planet

Point external DNS traffic to Umbrella

Network Deployment

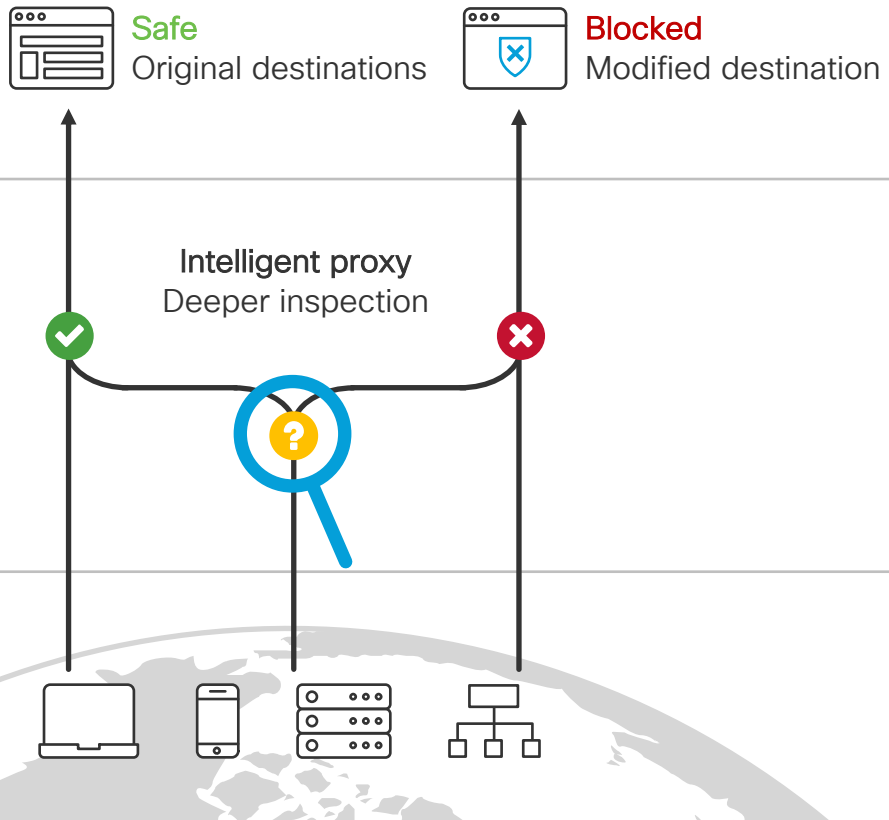


Umbrella DNS Resolver Flow

Destinations
Original destination or block page

Security controls
- DNS and IP enforcement
- Risky domain inspection through proxy
- SSL decryption available

Internet traffic
On- and off-network



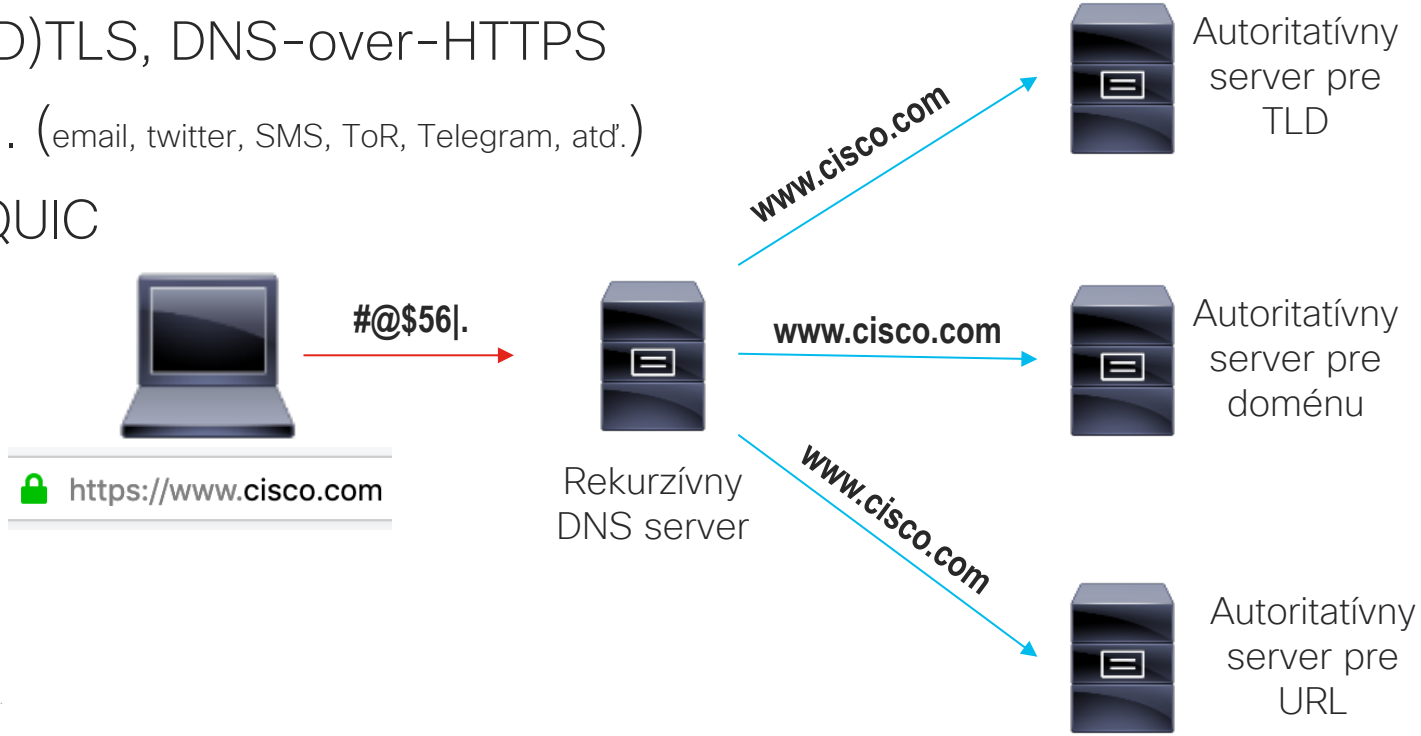
Šifrované DNS

DNSCRYPT

DNS-over-(D)TLS, DNS-over-HTTPS

DNS-over-... (email, twitter, SMS, ToR, Telegram, atď.)

DNS-over-QUIC



Porovnanie šifrovacích mechanizmov DNS

DNSCRYPT

- Open source (dnscrypt.info), nie je IETF štandard
- Šifrovanie a autenticita prostredníctvom UDP 443

DNS-over-(D)TLS

- RFC 7858 (TCP 853) a RFC 8094 (UDP 853)
- https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Public+Resolvers
- https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby

DNS-over-HTTPS

- DNS požiadavky zapuzdrené do HTTP/2 vnútri TLS zašifrovaného tunelu (TCP 443)
- Hlavní propagátori sú Google a Mozilla (zatiaľ nie by default)

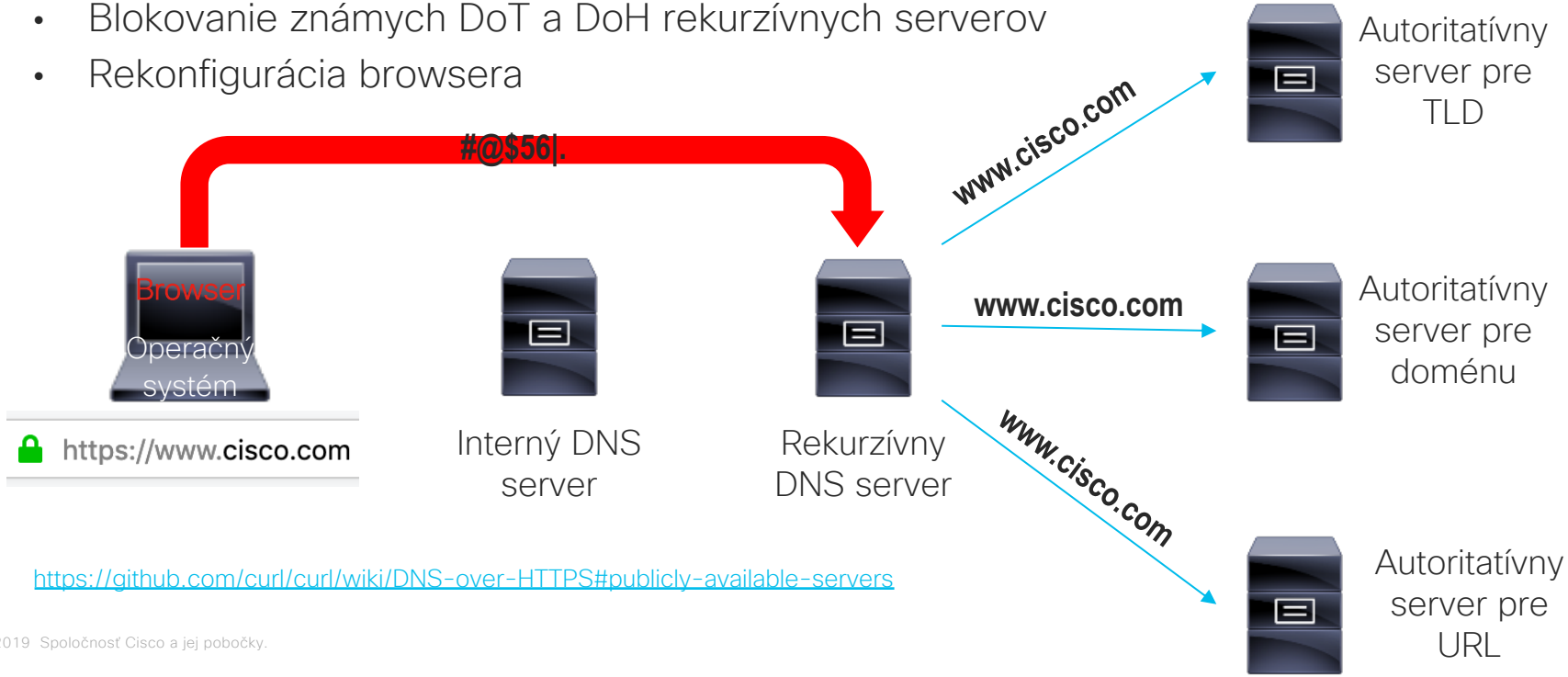
DNS-over-QUIC

- QUIC (IETF, v súčasnosti draft) + TLS v1.3 + HTTP/2 = HTTP/3

Aký je problém s D-o-T, D-o-H, D-o-...?

A aké je riešenie?

- Blokovanie známych DoT a DoH rekurzívnych serverov
- Rekonfigurácia browsera



https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers

Príklad konfigurácie Firefox

Firefox about:config 133% ; over HTTPS

Search: trr

Preference Name	Status	Type	Value
network.trr.allow-rfc1918	default	boolean	false
network.trr.blacklist-duration	default	integer	60
network.trr.bootstrapAddress	**modified**	**string**	**1.1.1.1**
network.trr.confirmationNS	default	string	example.com
network.trr.credentials	default	string	
network.trr.custom_uri	default	string	
network.trr.disable-ECS	default	boolean	true
network.trr.early-AAAA	default	boolean	false
network.trr.max-fails	default	integer	5
network.trr.mode	default	integer	0
network.trr.request-timeout	default	integer	1500
network.trr.uri	**modified**	**string**	**https://cloudflare-dns.com/dns-query**
network.trr.useGET	default	boolean	false
network.trr.wait-for-portal	default	boolean	true

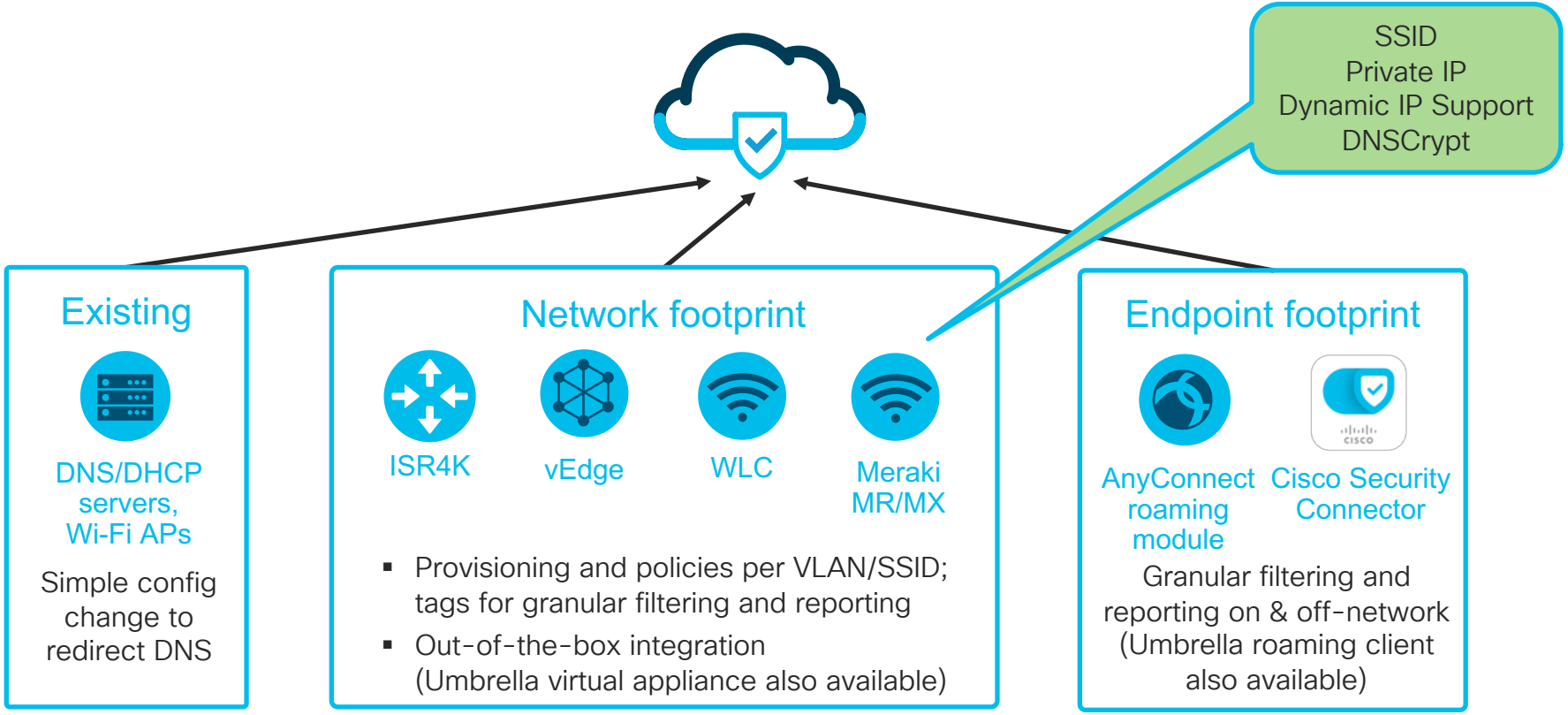
default: (none) by setting this field to the IP address of the host name used in "network.trr.uri", you can bypass using the system native resolver for it.

0 - Off (default). use standard native resolving only (don't use TRR at all)
1 - Reserved (used to be Race mode)
2 - First. Use TRR first, and only if the name resolve fails use the native resolver as a fallback.
3 - Only. Only use TRR. Never use the native (This mode also requires the bootstrapAddress pref to be set)
4 - Reserved (used to be Shadow mode)
5 - Off by choice. This is the same as 0 but marks it as done by choice and not done by default.

Cisco Umbrella blokuje DoH cez proxy/anonymizer kategóriu, ak nie je nastavená IP v bootstrapAddress:

https://support.umbrella.com/hc/en-us/articles/360001371526-Firefox-and-DNS-over-HTTPS-default

Enterprise-wide deployment in minutes

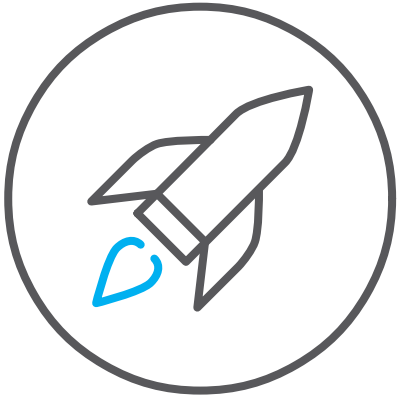


Sumár

Umbrella is Different

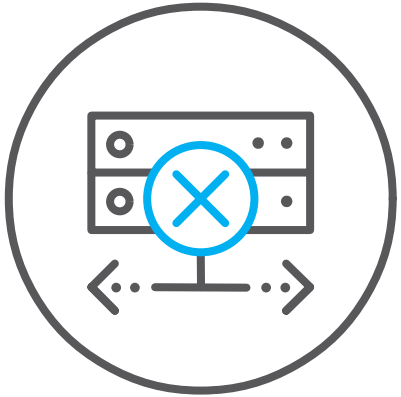
Emphasis is on Security

Productivity cannot be achieved by controlling the corporate network



Easy to Deploy & Manage

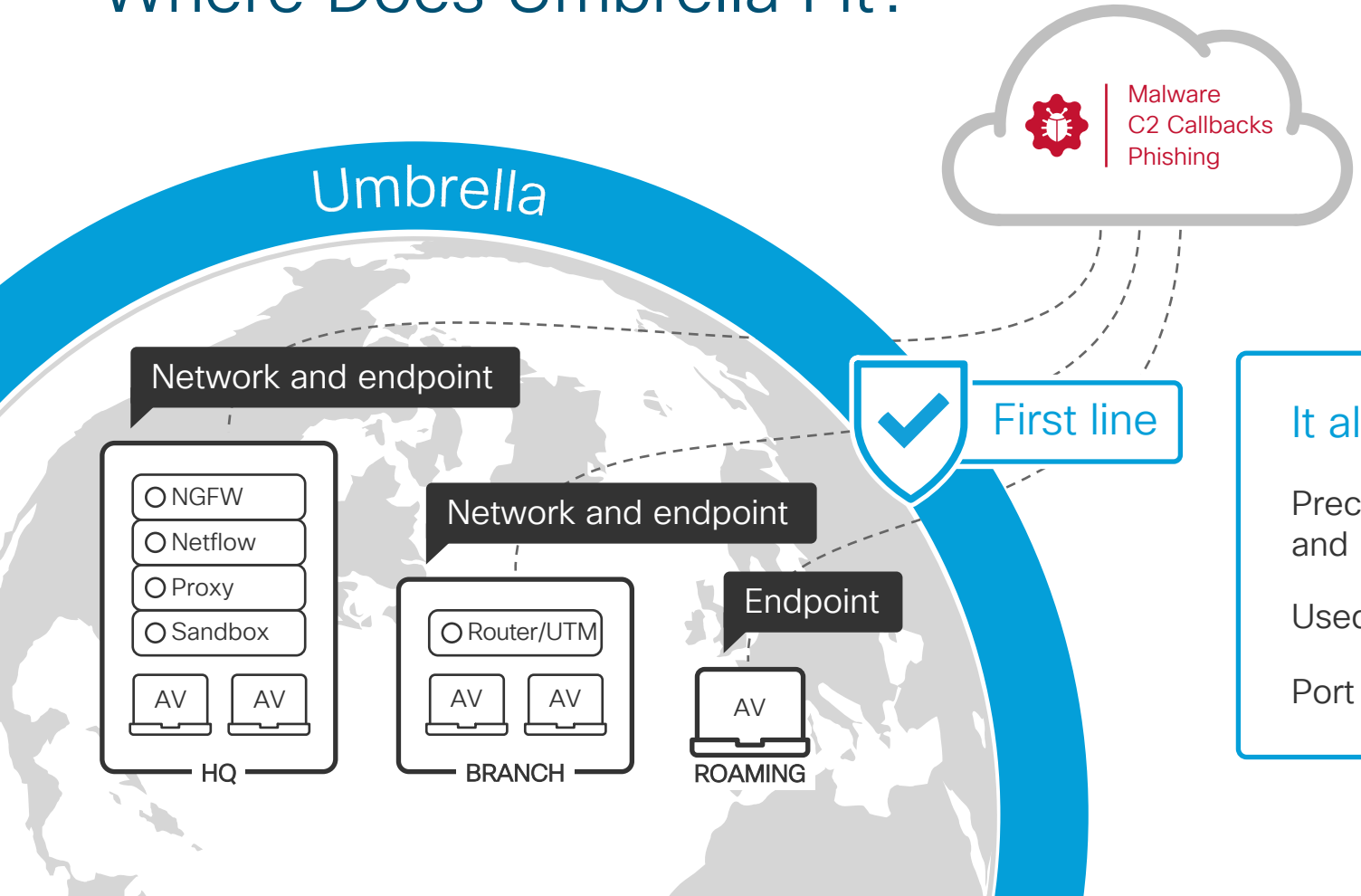
Leveraging DNS and Cisco's footprint for easy deployment



No Need to Proxy Everything

Proxying everything adds latency, but isn't necessary with our intelligence

Where Does Umbrella Fit?



It all starts with DNS

Precedes file execution and IP connection

Used by all devices

Port agnostic

Call to Action: The Easiest POV You'll Ever do!

1. Signup 2. Point DNS 3. Done.

After your POV, you'll receive a custom security report to help answer:

- How effective is this solution?
- How does it compare (or add) to my current security stack?
- Does it deliver great time-to-value?

signup.umbrella.com

dnsmonitoring.umbrella.com

Ďakujeme

Cisco Tech Club Webináře

Ako jednoducho a zároveň bezpečne pripojiť zamestnanca z home office do firemnej siete?
30. 4. 2020

cisco Engage

You make **possible**