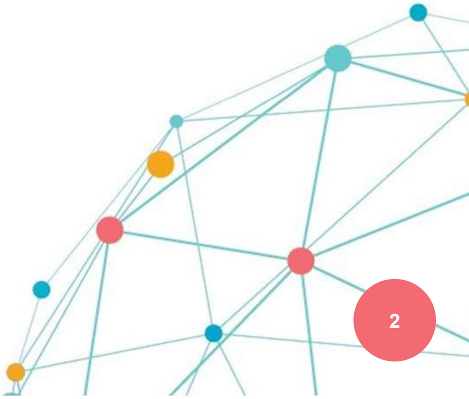
Datanet
SYSTEMSINTEGRATION
SOITRON GROUP

# Stop Hackers at the DNS Level – Get to know Cisco Umbrella

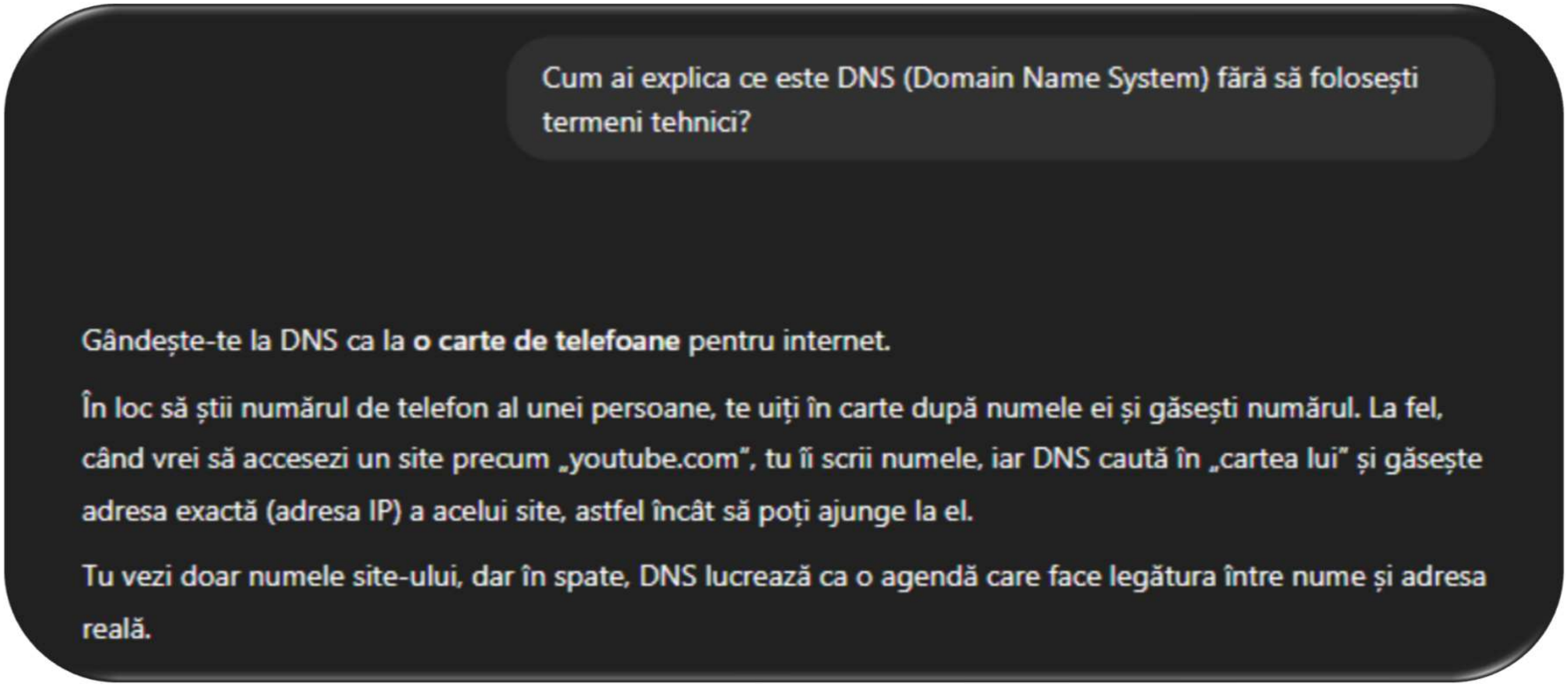
**Ștefan Radu**
Consultant Presales, Datanet Systems

# AGENDA

- What, Why, How’s of DNS
- DNS vulnerabilities & types of attacks
- Cisco Umbrella capabilities
- CTF Time



# What is Domain Name System?

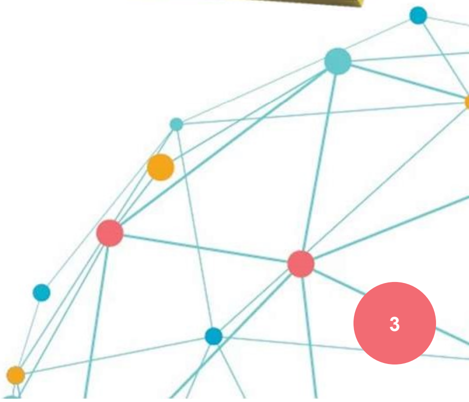


Cum ai explica ce este DNS (Domain Name System) fără să folosești termeni tehnici?

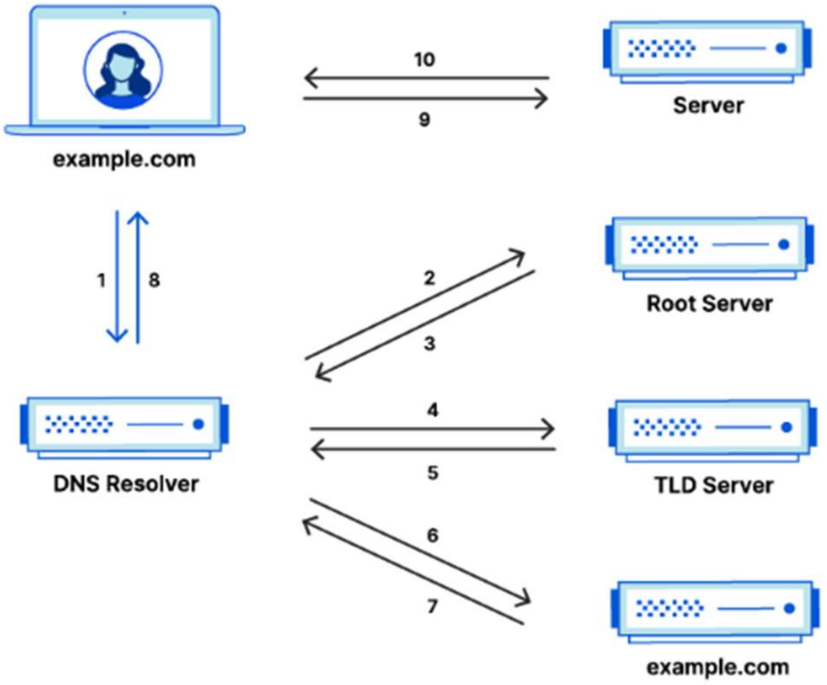
Gândește-te la DNS ca la **o carte de telefoane** pentru internet.

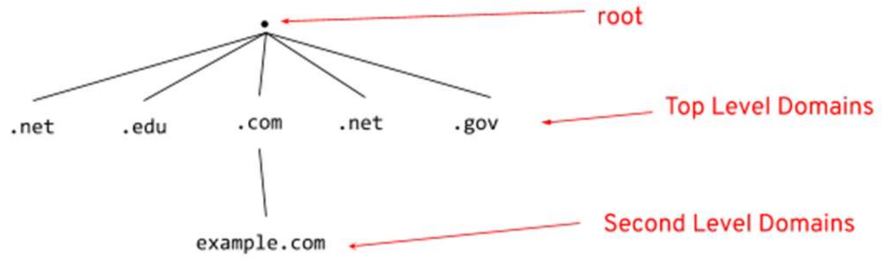
În loc să știi numărul de telefon al unei persoane, te uiți în carte după numele ei și găsești numărul. La fel, când vrei să accesezi un site precum „youtube.com", tu îi scrii numele, iar DNS caută în „cartea lui" și găsește adresa exactă (adresa IP) a acelui site, astfel încât să poți ajunge la el.

Tu vezi doar numele site-ului, dar în spate, DNS lucrează ca o agendă care face legătura între nume și adresa reală.

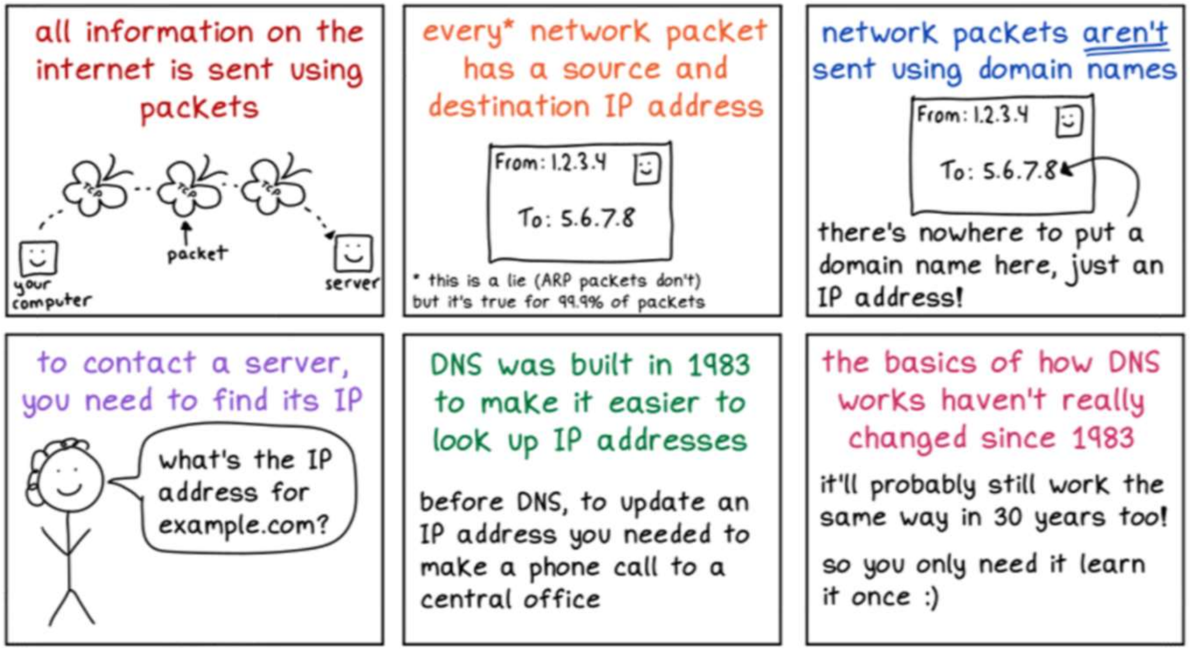


# How DNS works?

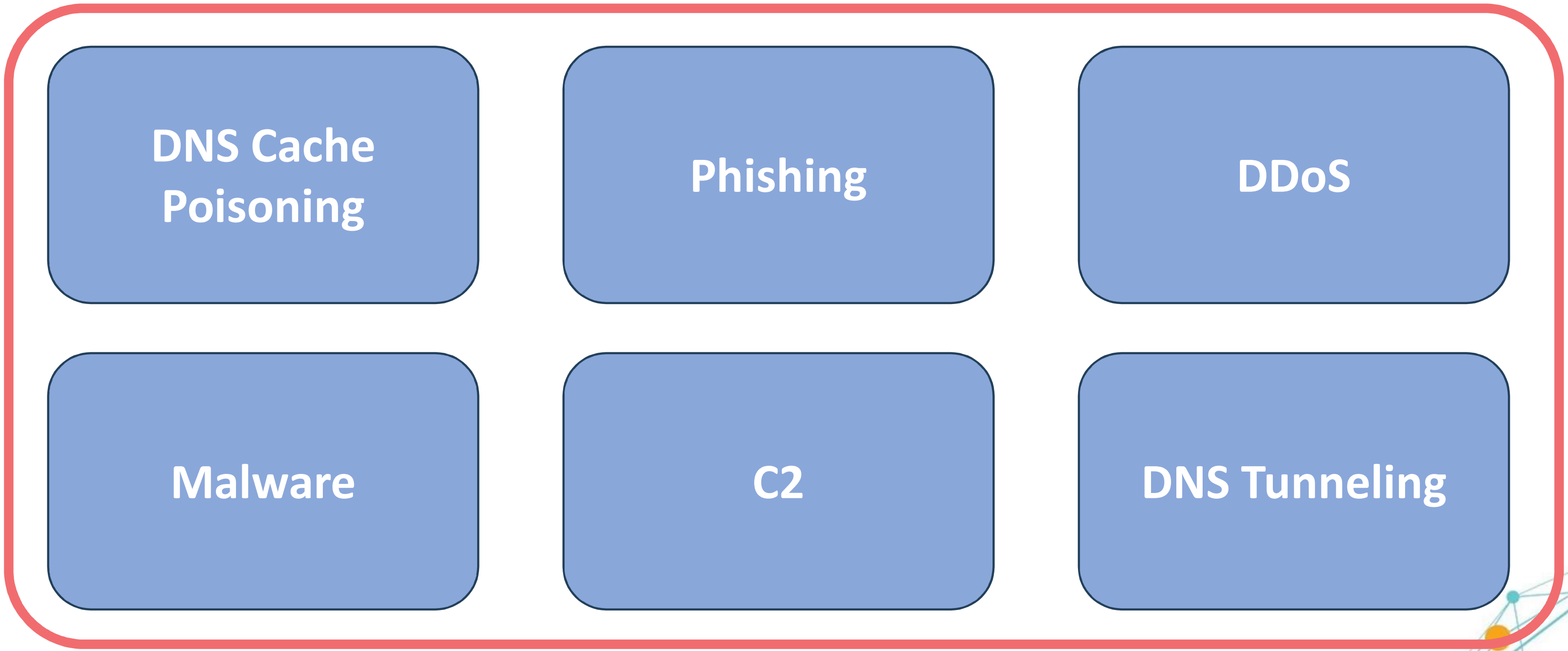




# Why do we need DNS?


all information on the internet is sent using packets
TCP
TCP
TCP
packet
your computer
server
every* network packet has a source and destination IP address
From: 1.2.3.4
To: 5.6.7.8
* this is a lie (ARP packets don't) but it's true for 99.9% of packets
network packets aren't sent using domain names
From: 1.2.3.4
To: 5.6.7.8
there's nowhere to put a domain name here, just an IP address!
to contact a server, you need to find its IP
what's the IP address for example.com?
DNS was built in 1983 to make it easier to look up IP addresses
before DNS, to update an IP address you needed to make a phone call to a central office
the basics of how DNS works haven't really changed since 1983
it'll probably still work the same way in 30 years too!
so you only need it learn it once :)

# Types of DNS Attacks



DNS Cache Poisoning

Phishing

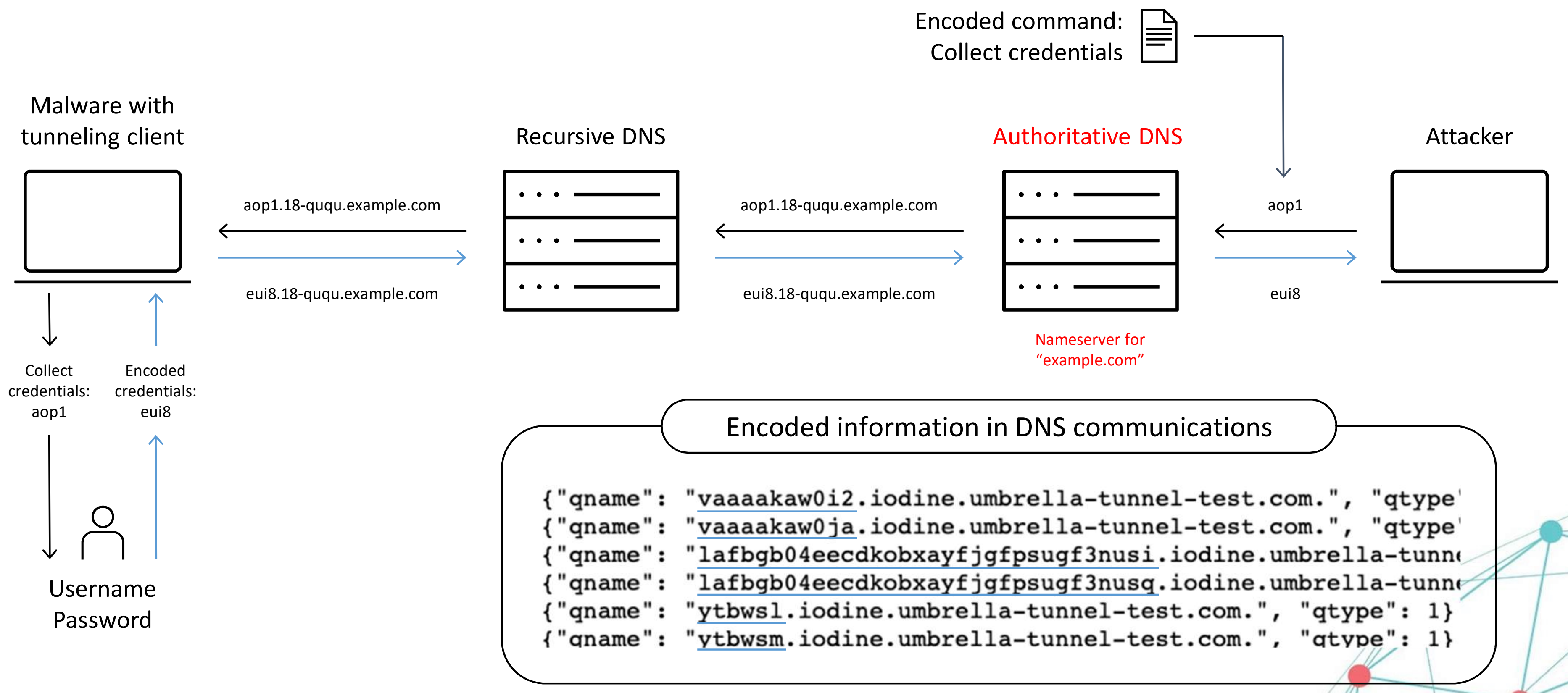
DDoS

Malware

C2

DNS Tunneling

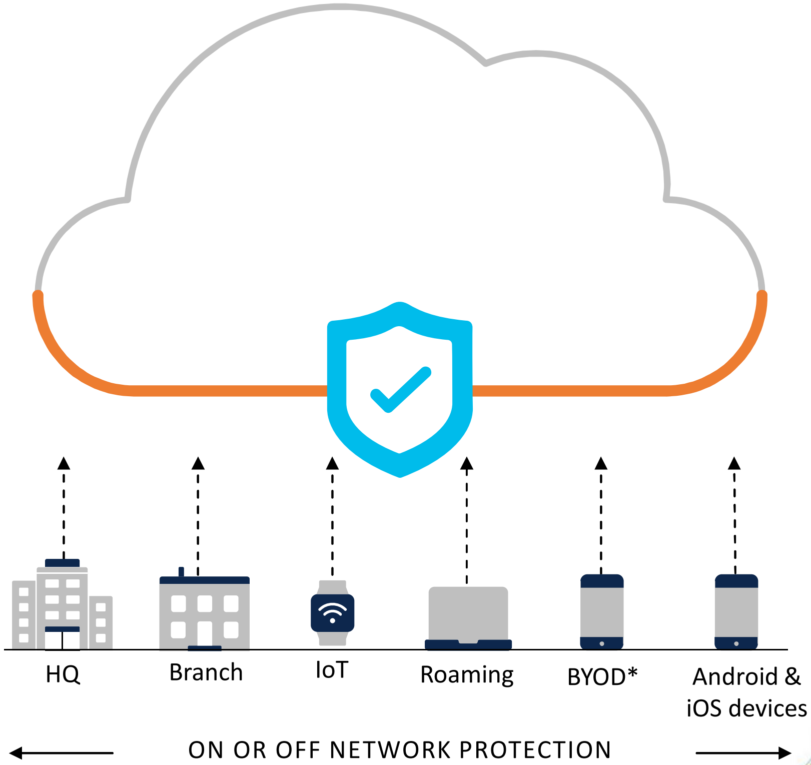
# DNS Tunneling Attack



```
{"qname": "vaaaakaw0i2.iodine.umbrella-tunnel-test.com.", "qtype
{"qname": "vaaaakaw0ja.iodine.umbrella-tunnel-test.com.", "qtype
{"qname": "lafbgb04eecdkobxayfjgfpsugf3nusi.iodine.umbrella-tunne
{"qname": "lafbgb04eecdkobxayfjgfpsugf3nusg.iodine.umbrella-tunne
{"qname": "ytbwsl.iodine.umbrella-tunnel-test.com.", "qtype": 1}
{"qname": "ytbwsm.iodine.umbrella-tunnel-test.com.", "qtype": 1}
```

# A versatile first line of defense

- All office locations
- Any device on your network
- Roaming laptops, supervised iOS devices, and managed Android devices



# Built into the internet foundation

## Destinations

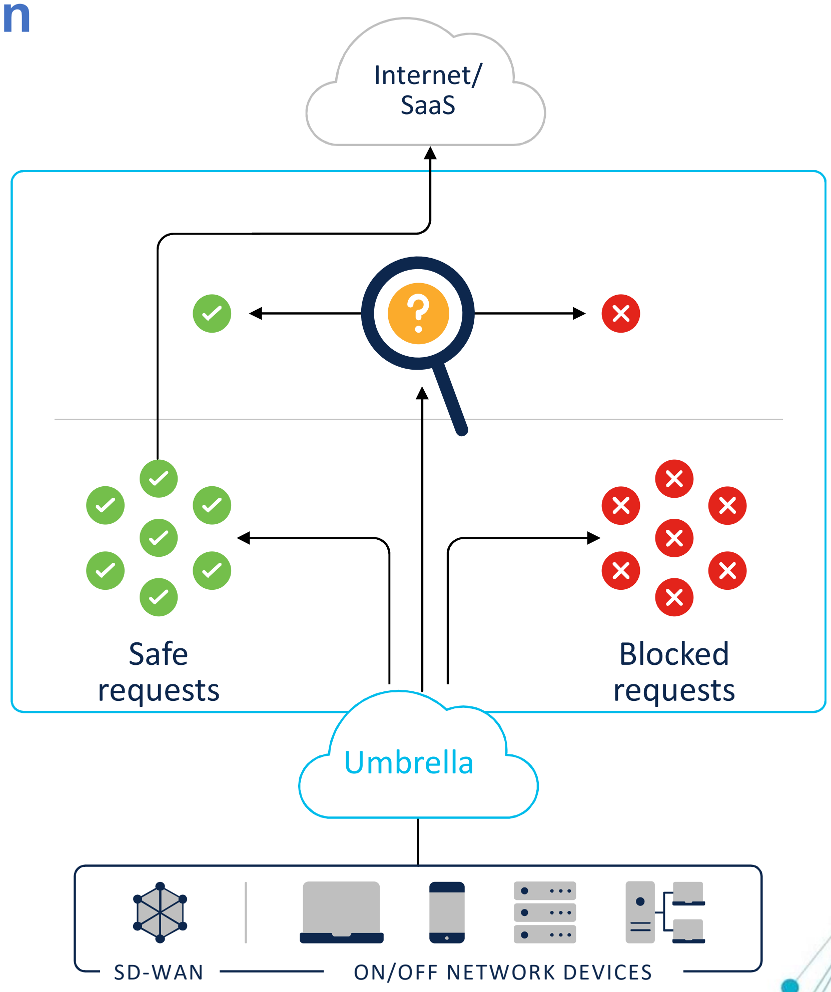
Original destination or block page

## Security controls

- DNS enforcement
- Risky domain inspection through proxy
- SSL decryption available

## Internet traffic

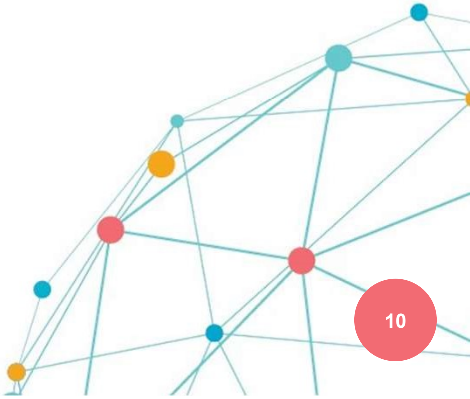
On and off-network



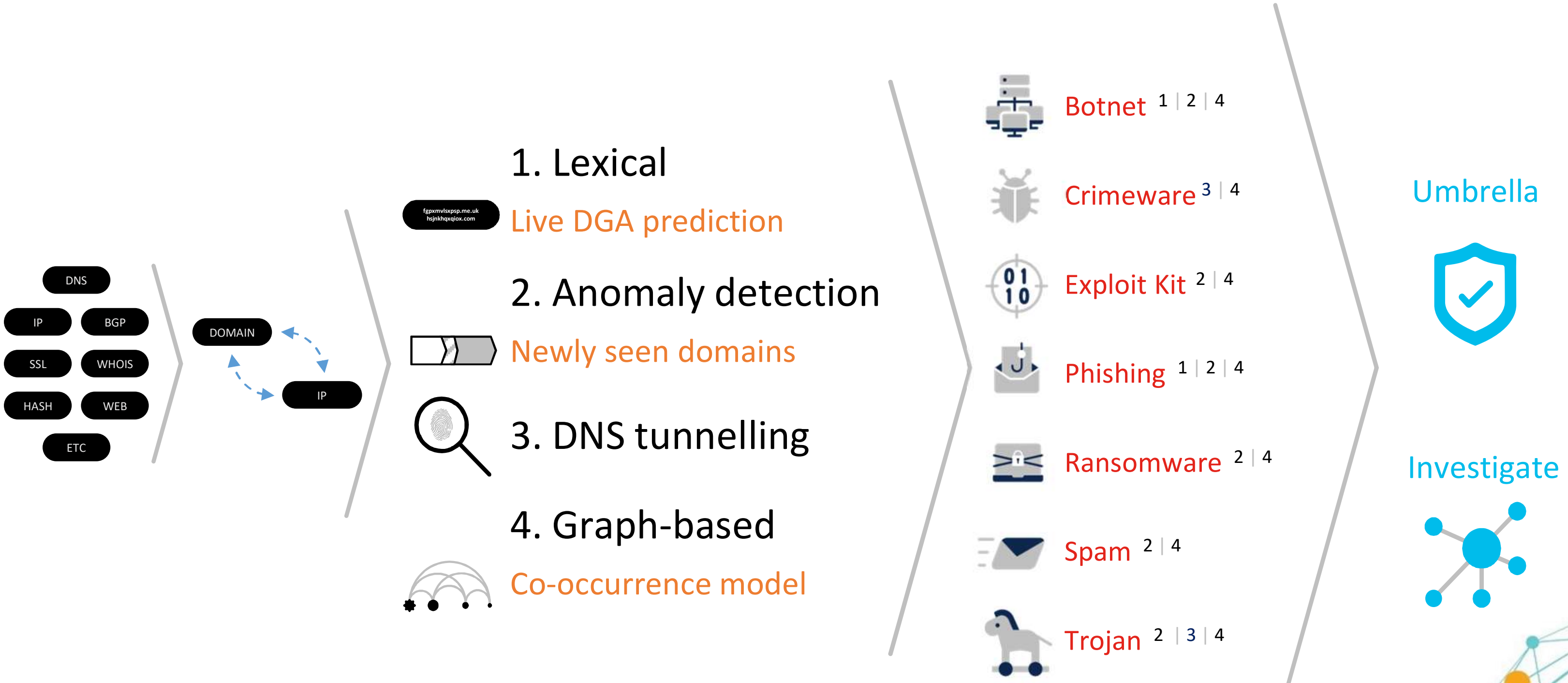
# Cisco Talos: the largest threat intelligence organization on the planet

- 400+ full-time threat researchers and data scientists
- 2 billion malware samples analyzed daily
- 200+ new vulnerabilities discovered each year

We see more so you can block more and respond faster to threats.



# Multi-faceted threat intel



1. Lexical

Live DGA prediction

2. Anomaly detection

Newly seen domains

3. DNS tunnelling

4. Graph-based

Co-occurrence model

Botnet 1 | 2 | 4

Crimeware 3 | 4

Exploit Kit 2 | 4

Phishing 1 | 2 | 4

Ransomware 2 | 4

Spam 2 | 4

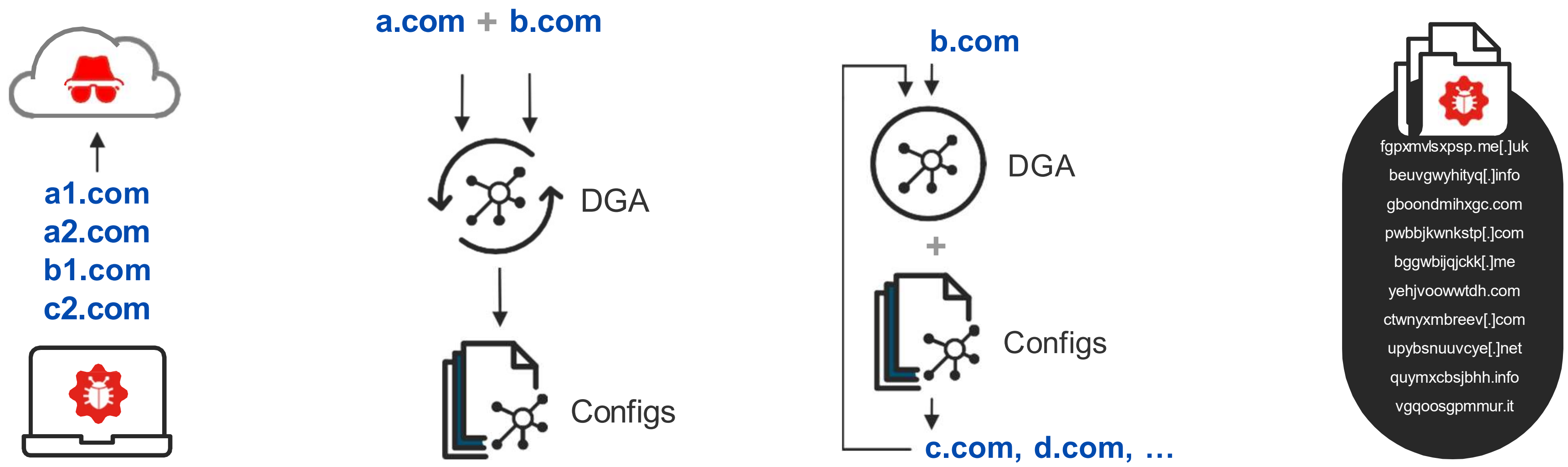
Trojan 2 | 3 | 4

Umbrella

Investigate

# Live DGA Prediction

## Automated at an unparalleled scale



a1.com
a2.com
b1.com
c2.com

a.com + b.com

DGA

Configs

b.com

DGA

+

Configs

c.com, d.com, …

fgpxmvlsxpsp.me[.]uk
beuvgwyhityq[.]info
gboondmihxgc.com
pwbbjkwnkstp[.]com
bggwbijqjckk[.]me
yehjvoowwtdh.com
ctwnyxmbreev[.]com
upybsnuuvcye[.]net
quymxcbsjbhh.info
vgqoosgpmmur.it

**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**

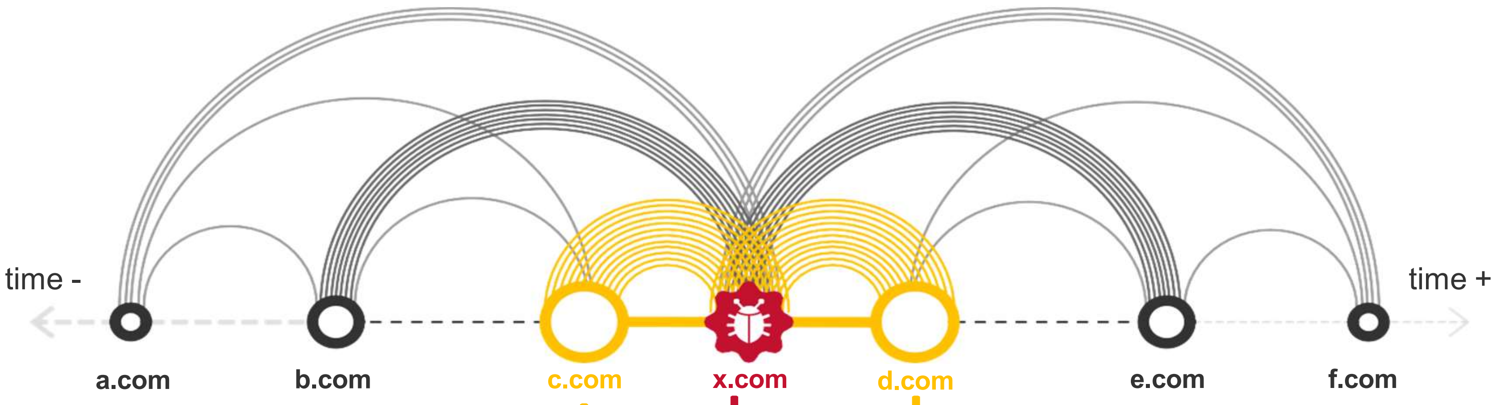
Combine newly-identified configs with DGA to identity C2 domains continuously

**Automate blocking pool of C2 domains**

Used by thousands of malicious samples now and in the future

# Co-occurrence model

Domains guilty by inference

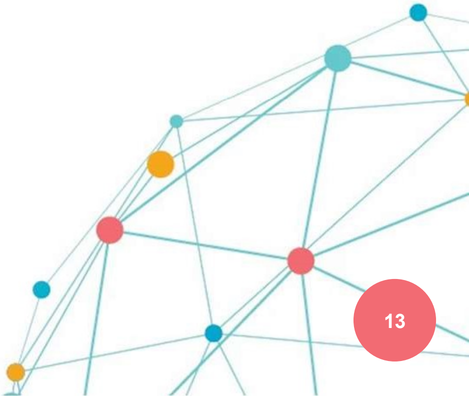


Possible malicious domain

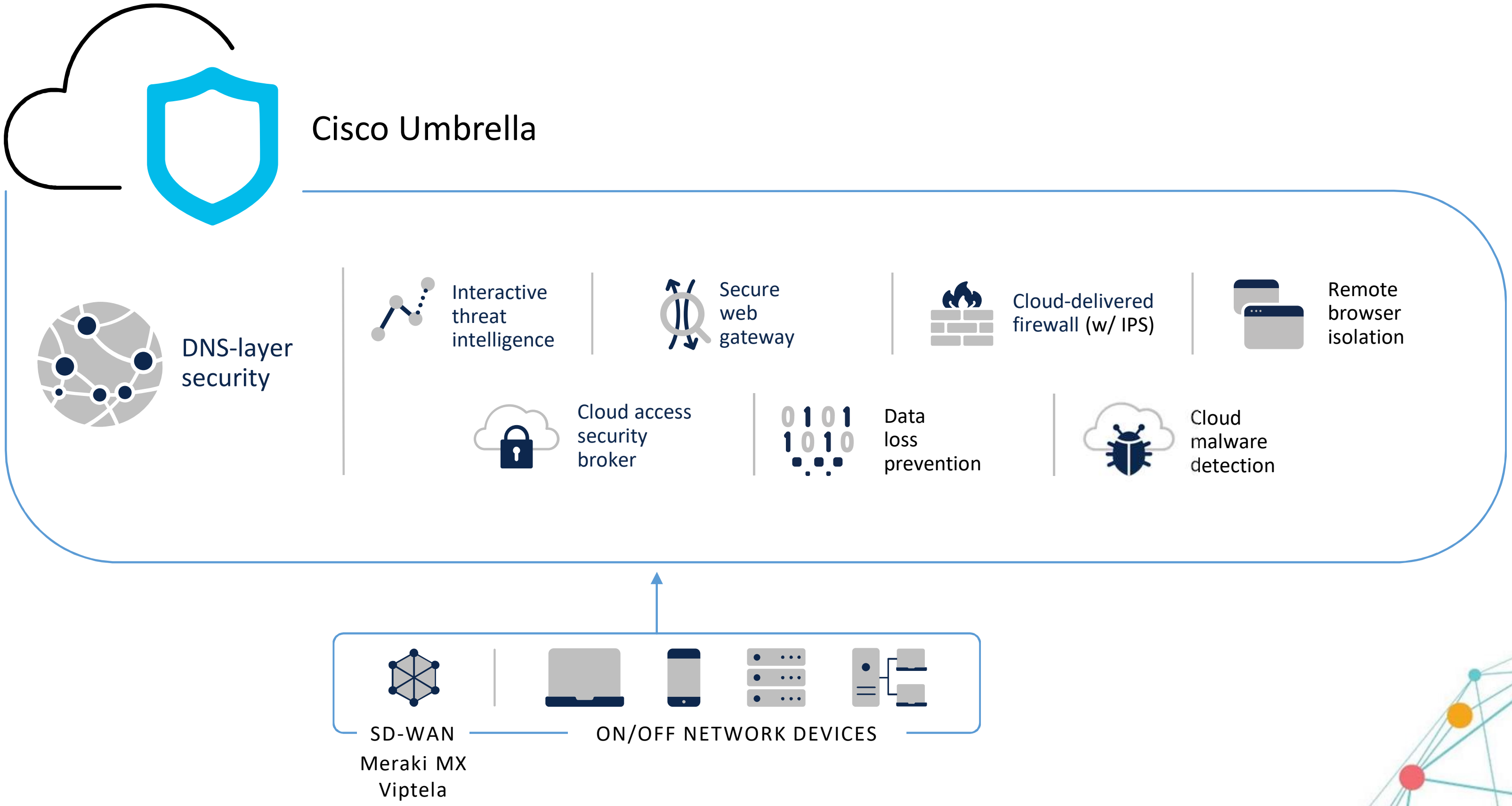
Possible malicious domain

Known malicious domain

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



# The Umbrella multi-function security solution



Cisco Umbrella

DNS-layer security

Interactive threat intelligence

Secure web gateway

Cloud-delivered firewall (w/ IPS)

Remote browser isolation

Cloud access security broker

Data loss prevention

Cloud malware detection

SD-WAN
Meraki MX
Viptela

ON/OFF NETWORK DEVICES

# It’s CTF time!