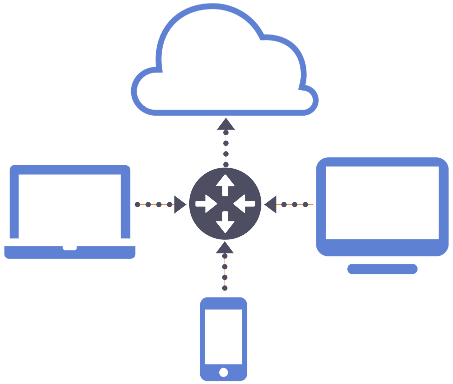
Do you analyze your DNS traffic? You should!

Szilard Csordas, Security Consultant

scsordas [at] cisco.com

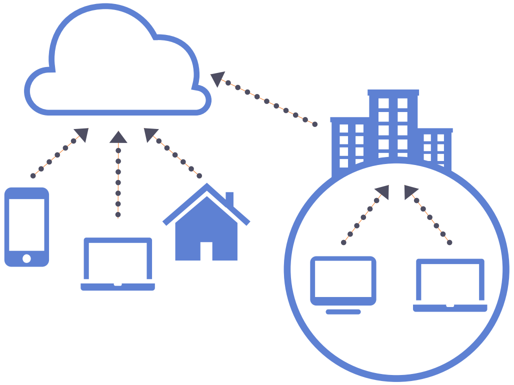
Can we predict attacks?

DNS is *Used by Every Device* on Your Network



ANY OWNER

network's DHCP tells
every connected device
where to point DNS



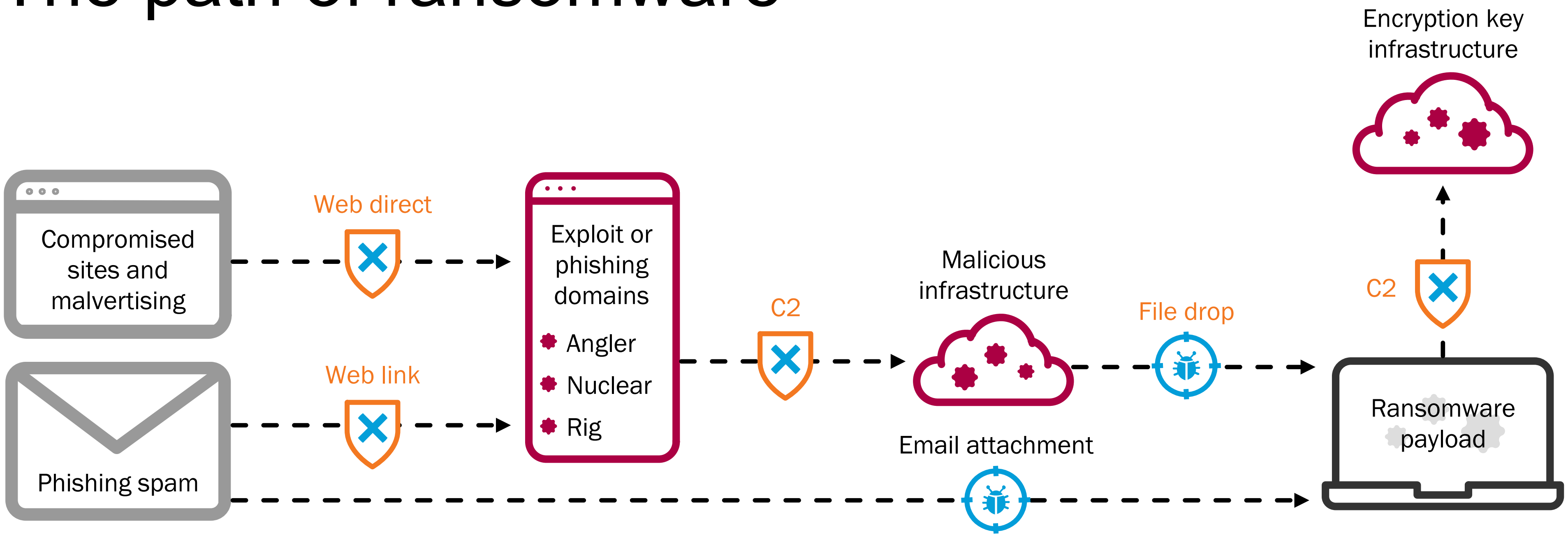
ANY TOPOLOGY

no matter how your
LAN or WAN is set up,
it simply works

ANY OPERATING SYS

Win, Mac, iOS, Android,
Linux, custom app servers,
and even IoT

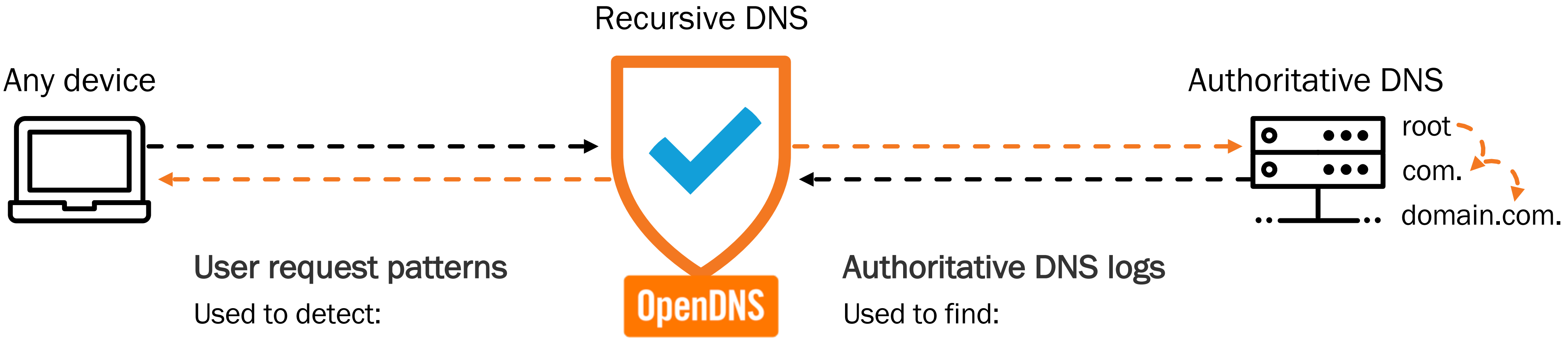
The path of ransomware



☒ Blocked by Cisco Umbrella

Blocked by Cisco AMP for Endpoints

Gather intelligence and enforce security at the DNS layer



User request patterns

Used to detect:

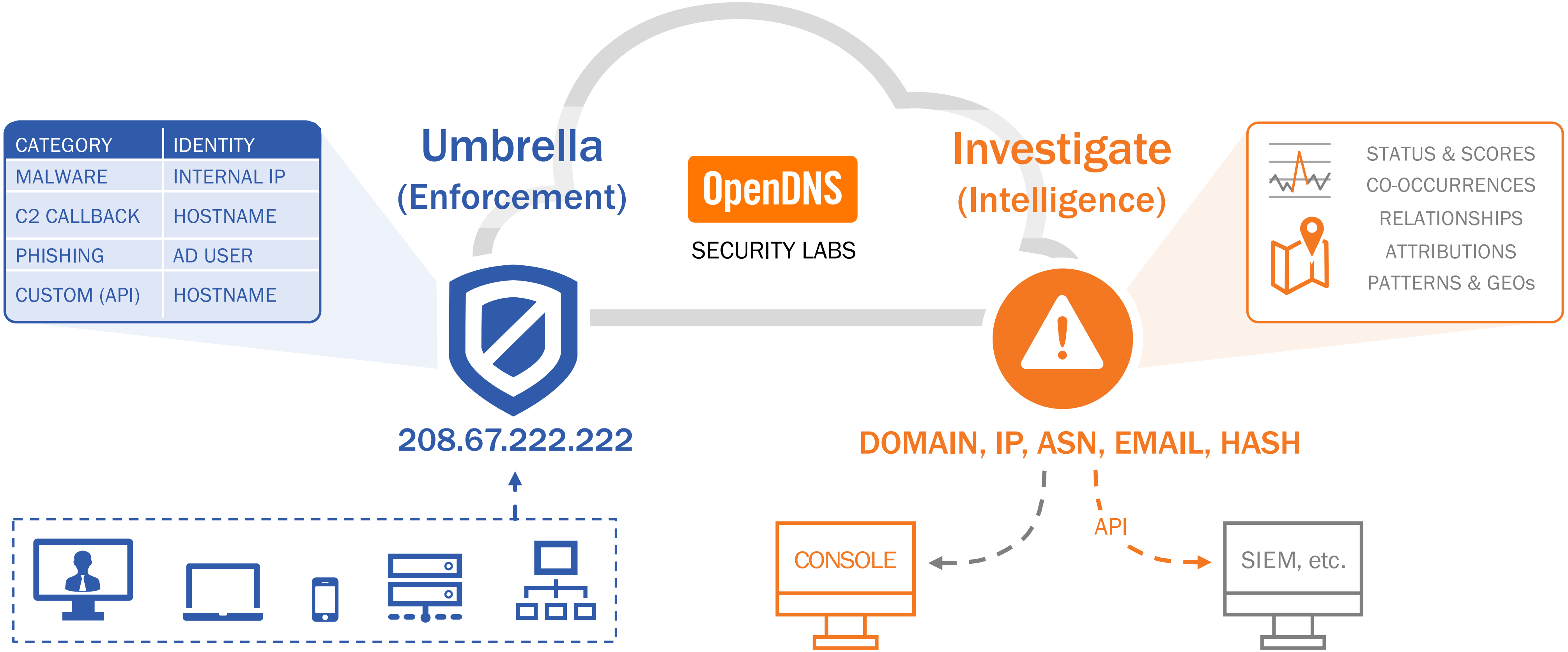
- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative DNS logs

Used to find:

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

What does OpenDNS Provide



CATEGORY	IDENTITY
MALWARE	INTERNAL IP
C2 CALLBACK	HOSTNAME
PHISHING	AD USER
CUSTOM (API)	HOSTNAME

Umbrella (Enforcement)

OpenDNS SECURITY LABS

Investigate (Intelligence)

STATUS & SCORES
CO-OCCURRENCES
RELATIONSHIPS
ATTRIBUTIONS
PATTERNS & GEOs

208.67.222.222

DOMAIN, IP, ASN, EMAIL, HASH

Our efficacy

Discover

3M+

daily new domain names

Identify

60K+

daily malicious destinations

Enforce

7M+

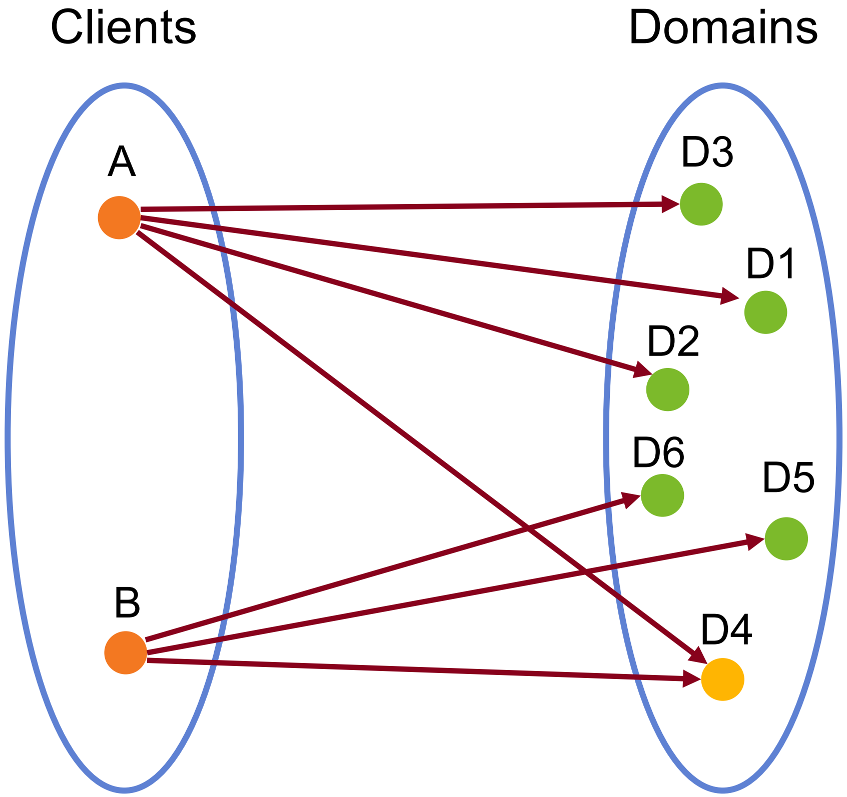
malicious destinations while resolving DNS

Predictive Detectors Used by OpenDNS

- SecureRank
- Co-Occurrences
- NLPRank
- DGA Detectors
- Spike Detectors
- Predictive IP Space Monitoring

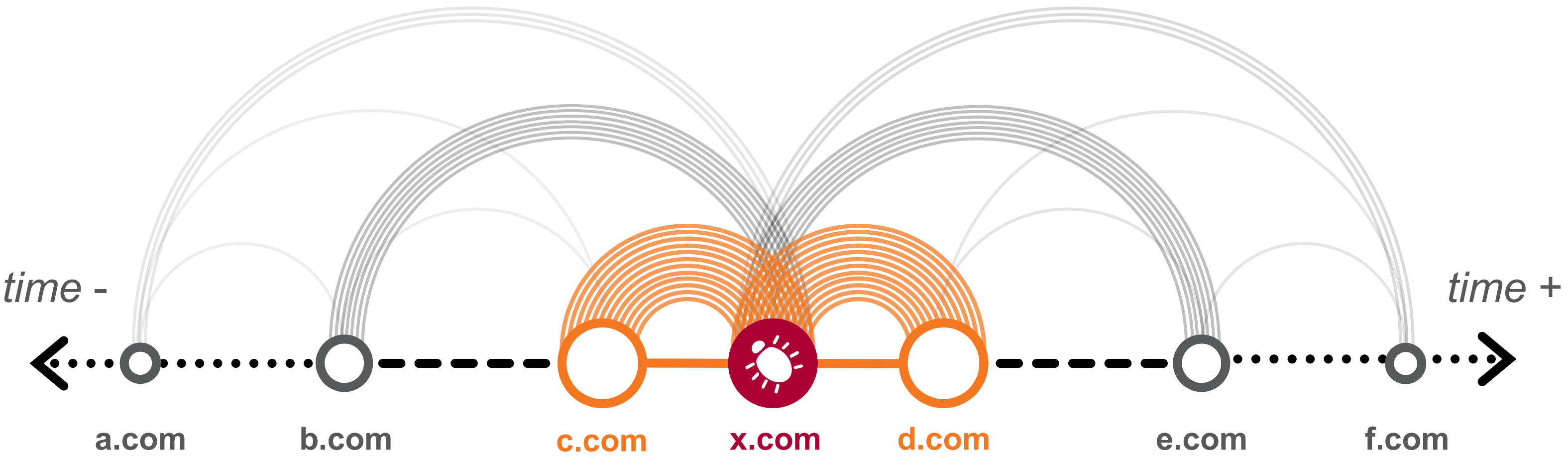
SecureRank

- Abstract DNS traffic in a bipartite graph
- **Domains requested by known infected clients but never requested by clean ones are most likely to be bad.**
- **The less visited by good clients, the higher chance a domain is bad**
- SecureRank2 is designed to identify these domains
- Negative ranks to known blacklisted domains and positive ranks to known whitelisted domains.
- Nodes are either visited or being visited, but never both



Co-Occurrence Rank

Domains Guilty by Inference



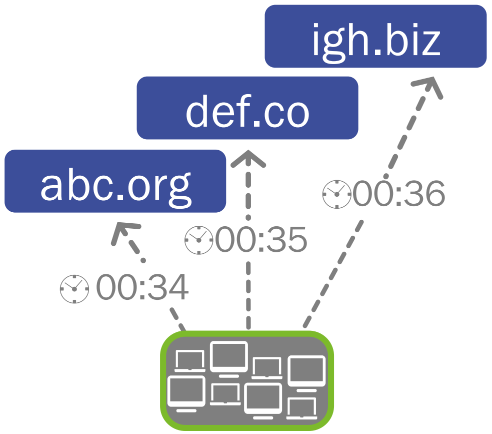
Possible Malicious Domain

Known Malicious Domain

Possible Malicious Domain

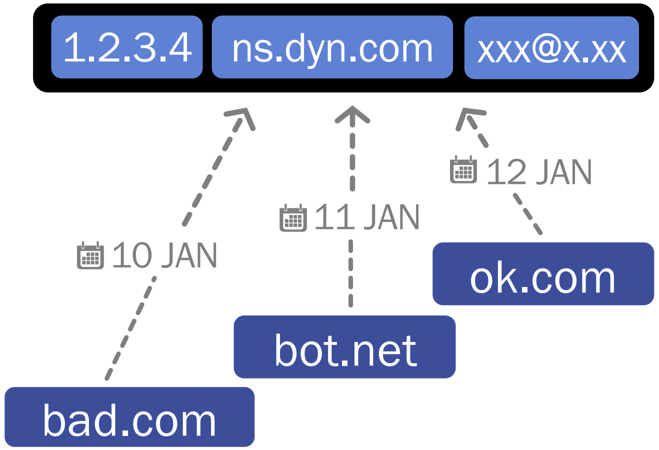
Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

Co Occurrences can be correlated with more “traditional” Techniques



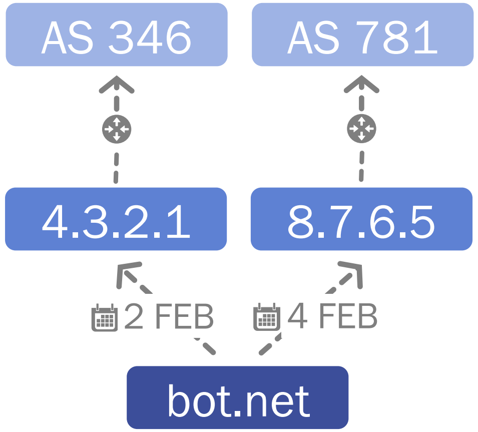
CO-OCCURRENCES

domain-to-domain request sequences via recursive DNS



PASSIVE DNS & WHOIS

present & past relationships for domains-to-IP/nameserver/email via authoritative DNS & DNS registrars

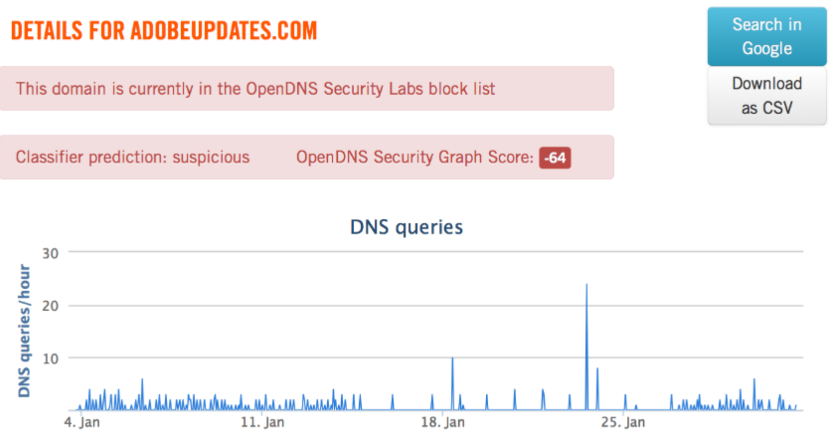


INFRASTRUCTURES

domain-to-IP-to-AS relationships via graphing BGP routing data

NLPRank Detections: DarkHotel

- adobeupdates[.]com

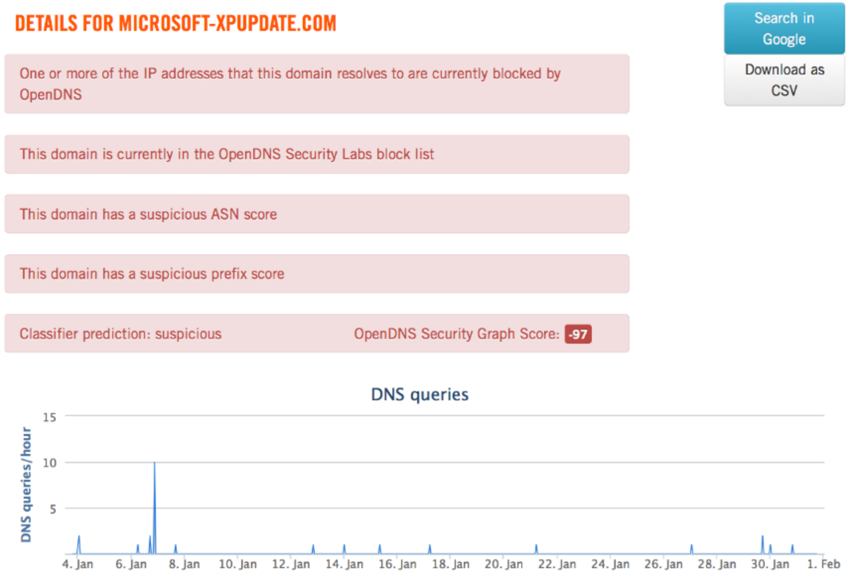


DETAILS FOR ADOBEUPDATES.COM

This domain is currently in the OpenDNS Security Labs block list

Classifier prediction: suspicious OpenDNS Security Graph Score: -64

- microsoft-xpupdate[.]com



DETAILS FOR MICROSOFT-XPUPDATE.COM

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

This domain is currently in the OpenDNS Security Labs block list

This domain has a suspicious ASN score

This domain has a suspicious prefix score

Classifier prediction: suspicious OpenDNS Security Graph Score: -97

Anomaly Detection: Live DGA Detection

Domain Generation Algorithms: technique to generate malware domains on-the-fly & avoid hardcoding domains in payload

N-gram" analysis

Do letter pairings match normal language patterns?

yfrscsddkkdl.com

qgmcgoqeasgommee.org

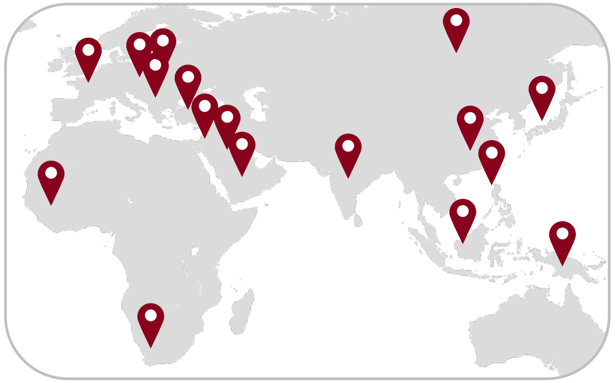
iyyxtyxdeypk.com

diiqngijkpop.ru

Does the probability distribution of letters appear random?

IP Geo-Location Analysis

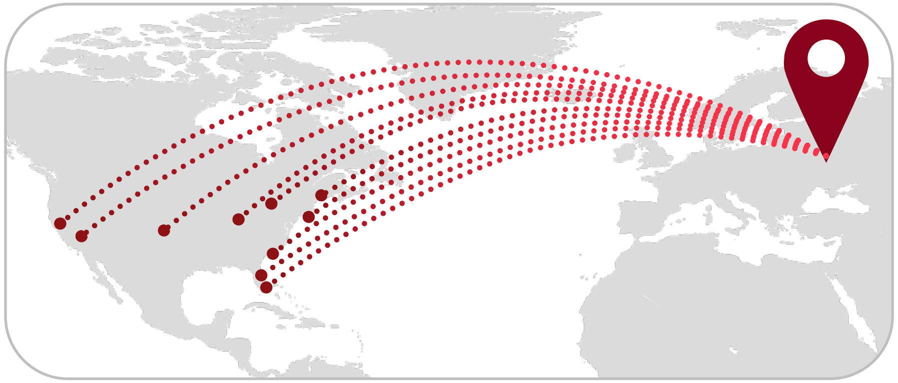
hosted across 28+ geo-locations



HOST INFRASTRUCTURE

location of the server
IP addresses mapped to domain

only US-located users requesting a .RU TLD



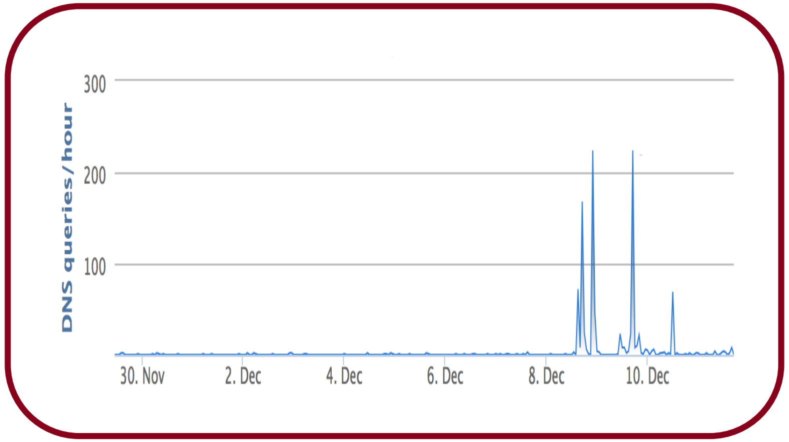
DNS REQUESTERS

location of the network & off-network device
IP addresses requesting the domain

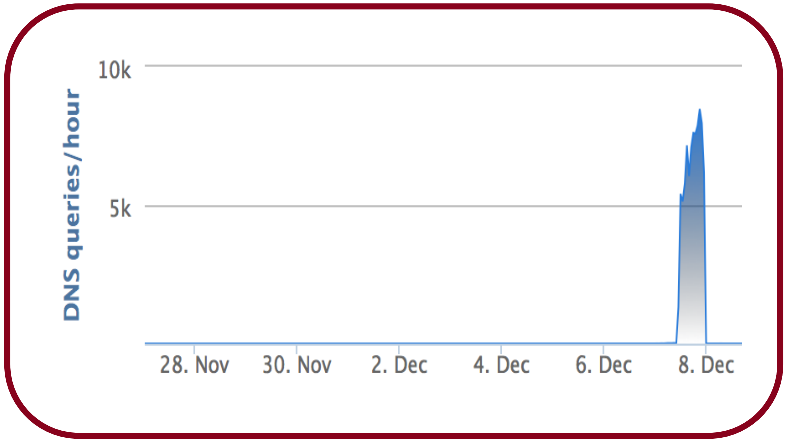
What Does a Malicious Connection Sounds Like?

Spike detector

What if we could model the traffic spikes as sound waves and identifies “spike behavior” typical of domains used for malware campaigns such as exploit kits, DGAs, fake software, phishing, etc…



Example of An Exploit Kit



Example of a DGA

Predictive IP Space Monitoring

Predictive IP Space Monitoring is used to further drill into associated indicators by analyzing 8 different recorded hosting patterns:

- Compromised domains, i.e. “domain shadowing”
- Domain shadowing on multiple hosting IPs
- Sibling peripheral ASNs and bulk malware IP setup
- Leaf ASNs
- Offshore registration and diversification of IP space
- Rogue ASN and affiliated hosters
- Abuse of large hosting providers
- Shady hosts within larger hosting providers

For

1

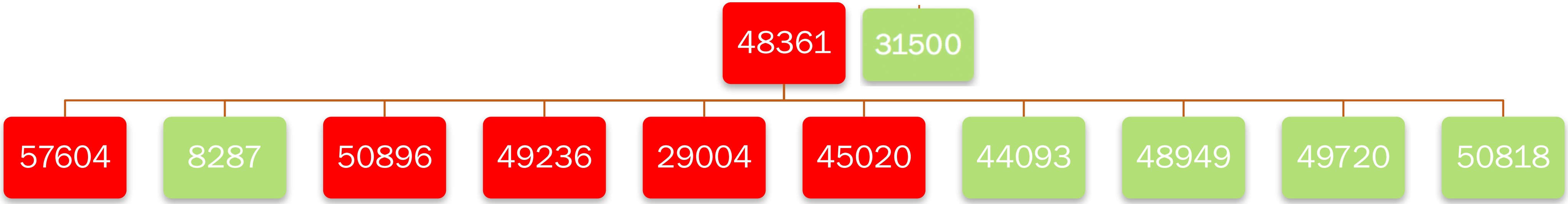
malicious domain identified by SPRank, Predictive IP Space Monitoring predicted

340

Additional domains

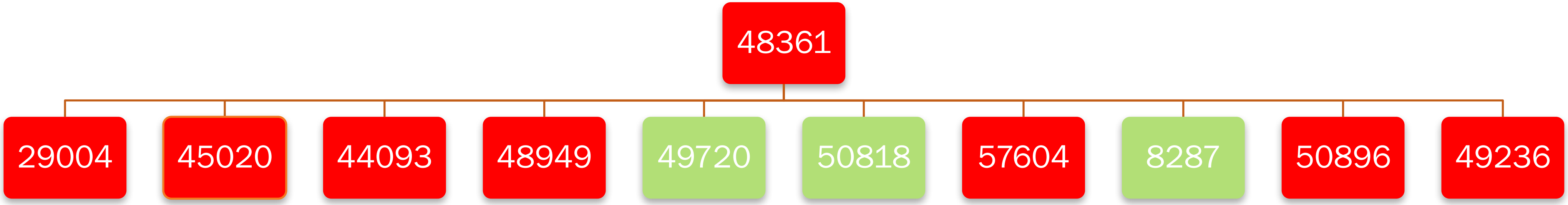
Malicious ASN subgraph

Whitepaper: Defcon 22 - openDNS



🟥 48361 🟩 31500

🟥 57604 🟩 8287 🟥 50896 🟥 49236 🟥 29004 🟥 45020 🟩 44093 🟩 48949 🟩 49720 🟩 50818



🟥 48361

🟥 29004 🟥 45020 🟥 44093 🟥 48949 🟩 49720 🟩 50818 🟥 57604 🟩 8287 🟥 50896 🟥 49236

6 weeks later

3100+ malware domains on 1020+ IPs

- nmap fingerprint (50 IPs)

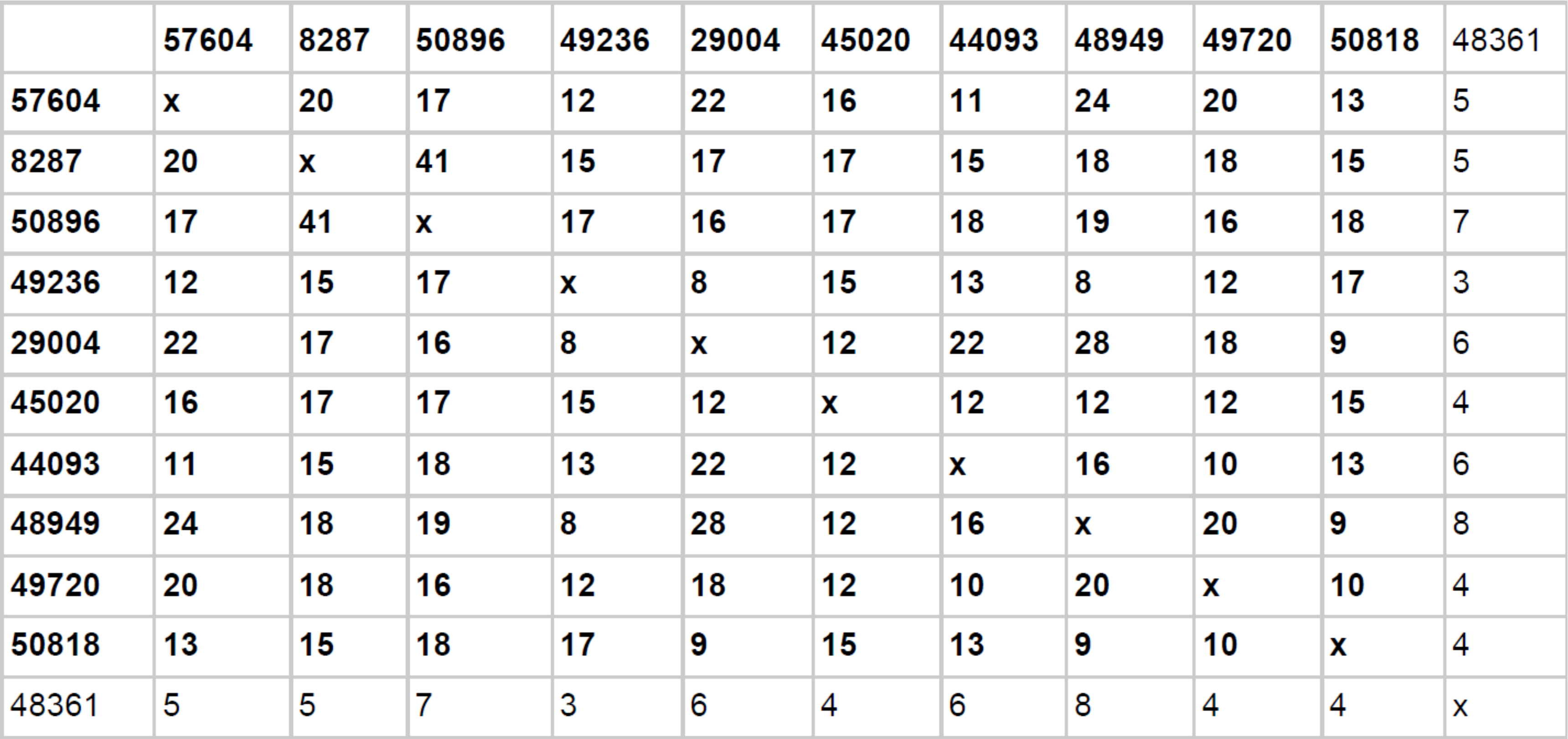
```
22/tcp open ssh  OpenSSH 6.2_hpn13v11 (FreeBSD 20130515; protocol 2.0)
8080/tcp open http-proxy 3Proxy http proxy
Service Info: OS: FreeBSD
```

- nmap fingerprint (108 IPs)

and 108 IPs shared the following fingerprint:

```
22/tcp open ssh OpenSSH 5.3 (protocol 1.99)
80/tcp open http?
```

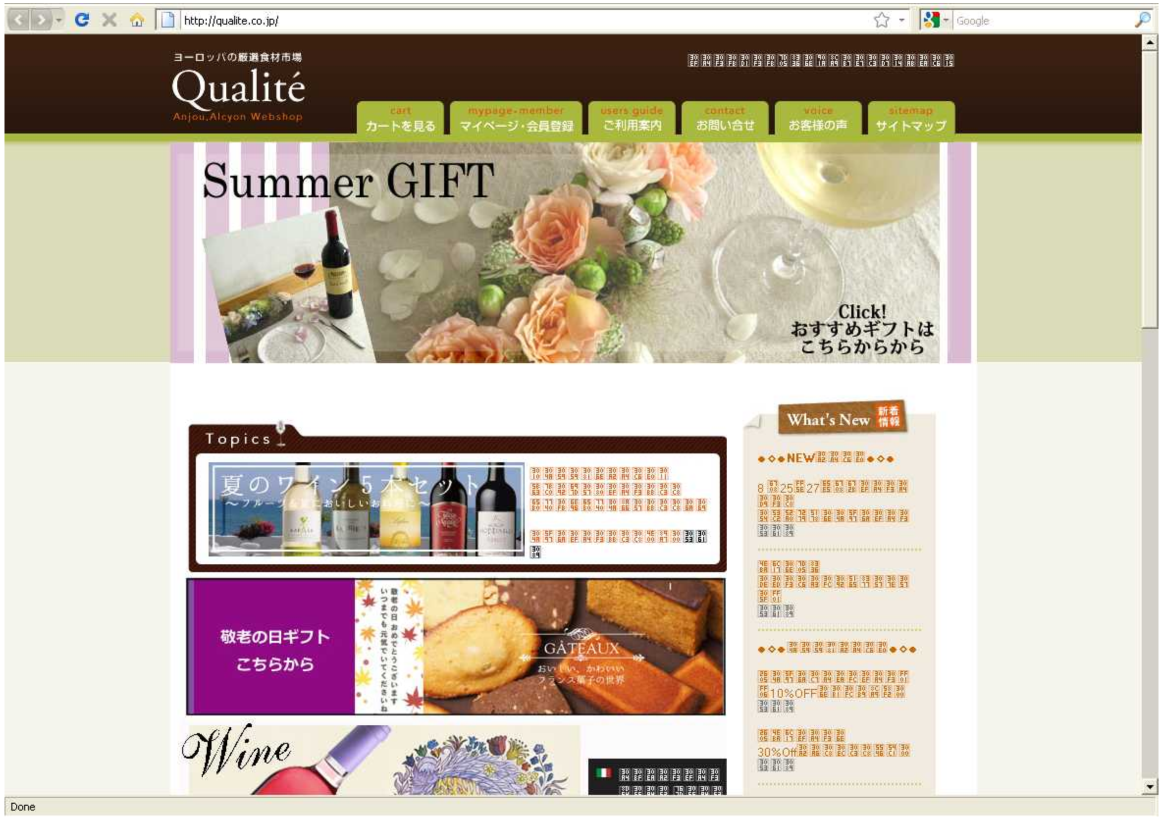
Overlapping outages between sibling ASNs



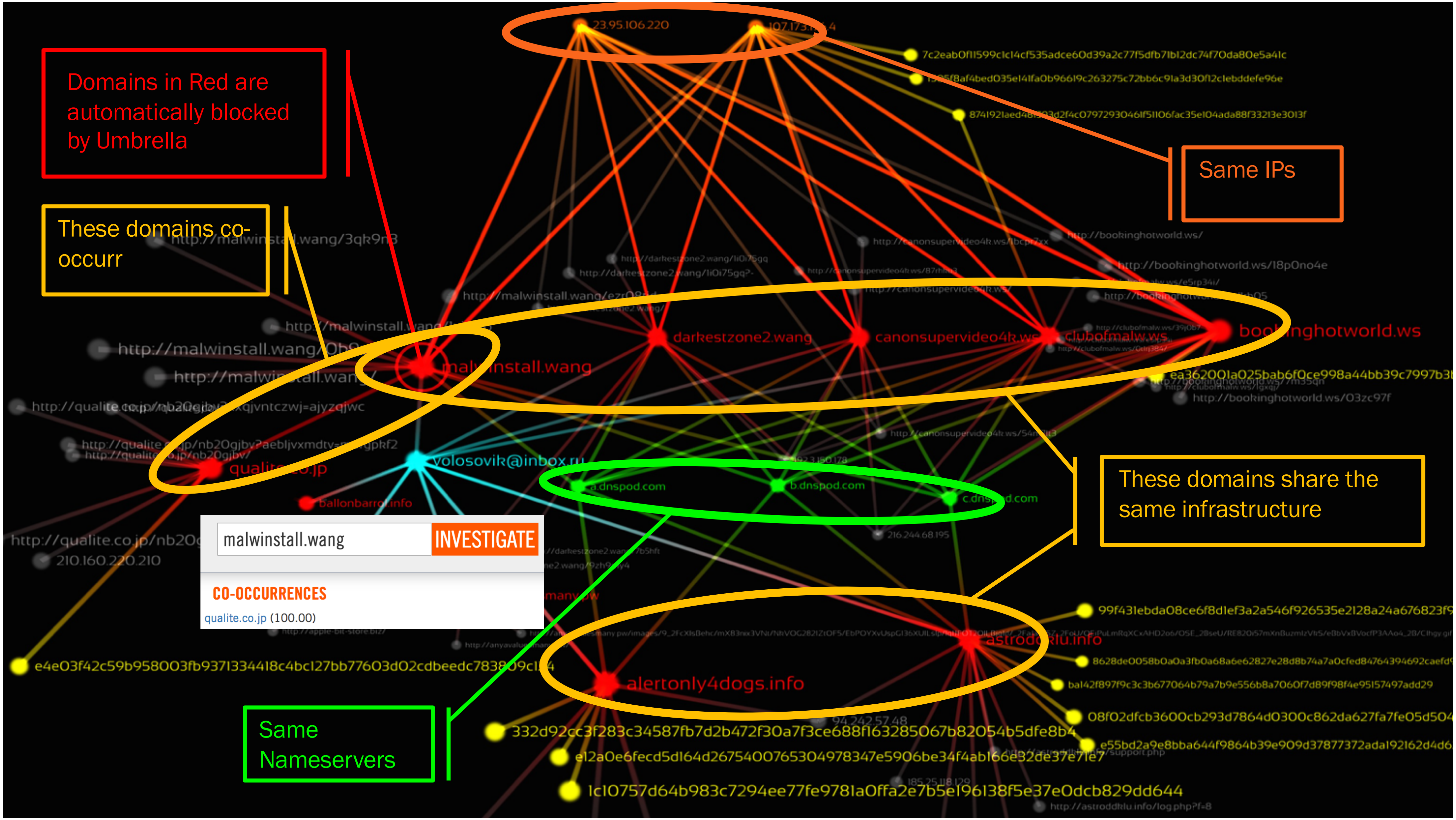
	57604	8287	50896	49236	29004	45020	44093	48949	49720	50818	48361
57604	x	20	17	12	22	16	11	24	20	13	5
8287	20	x	41	15	17	17	15	18	18	15	5
50896	17	41	x	17	16	17	18	19	16	18	7
49236	12	15	17	x	8	15	13	8	12	17	3
29004	22	17	16	8	x	12	22	28	18	9	6
45020	16	17	17	15	12	x	12	12	12	15	4
44093	11	15	18	13	22	12	x	16	10	13	6
48949	24	18	19	8	28	12	16	x	20	9	8
49720	20	18	16	12	18	12	10	20	x	10	4
50818	13	15	18	17	9	15	13	9	10	x	4
48361	5	5	7	3	6	4	6	8	4	4	x

Do You Fancy a Glass of Wine?

Well… This could be particularly bitter…



qualite.co.jp: Screenshot @ 2016-09-06 12:18:41



23.95.106.220
107.173.
7c2eab0f11599c1c14cf535adce60d39a2c77f5dfb71b12dc74f70da80e5a41c
8af4bed035e141fa0b96619c263275c72bb6c91a3d30f12c1ebddefe96e
874192 1aed4
d2f4c0797293046f5f1106fac35e104ada88f33213e3013f
http://bookinghotworld.ws/
http://canonsupervideo4k.ws/lbcpr7xx
http://darkestzone2.wang/1i0i75gq
http://darkestzone2.wang/1i0i75gq?-
http://bookinghotworld.ws/18pOno4e
http://malwinstall.wang/3qk9n3
http://malwinstall.wang/ezr08
http://malwinstall.wang
http://malwinstall.wang/0b9
http://malwinstall.wang/
darkestzone2.wang
canonsupervideo4k.ws
clubofmalw.ws
bookinghotworld.ws
malwinstall.wang
ea362001a025bab6f0ce998a44bb39c7997b3
http://bookinghotworld.ws/03zc97f
http://qualite.co.jp/nb20gjbv?xqjvntczwj=ajyzqjwc
http://qualite.co.jp/nb20gjbv?aebljvxmdtv=
http://qualite.co.jp/nb20gjbv/
qualite.co.jp
volosovik@inbox.ru
ballonbarrel.info
a.dnspod.com
b.dnspod.com
c.dnspod.com
216.244.68.195
http://qualite.co.jp/nb20
210.160.220.210
99f431ebda08ce6f8d1ef3a2a546f926535e2128a24a676823f
8628de0058b0a0a3fb0a68a6e62827e28d8b74a7a0cfed8476439 4692caefd
ba142f897f9c3c3b677064b79a7b9e556b8a70607d89f98f4e95157497add29
astroddrlu.info
alertonly4dogs.info
e4e03f42c59b958003fb937 1334418c4bc127bb77603d02cdbeedc783809c1
08f02dfcb3600cb293d7864d0300c862da627fa7fe05d504
332d92cc3f283c34587fb7d2b472f30a7f3ce688f163285067b82054b5dfe8b4
e55bd2a9e8bba644f9864b39e909d37877372ada192162d4d6
e12a0e6fecd5d164d26754007653049783 47e5906be34f4ab166e32de37e71e7
94.242.57.48
185.25.118.129
1c10757d64b983c7294ee77fe9781a0ffa2e7b5e196138f5e37e0dcb829dd644
http://astroddrlu.info/log.php?f=8

Domains in Red are automatically blocked by Umbrella

These domains co-occurr

Same IPs

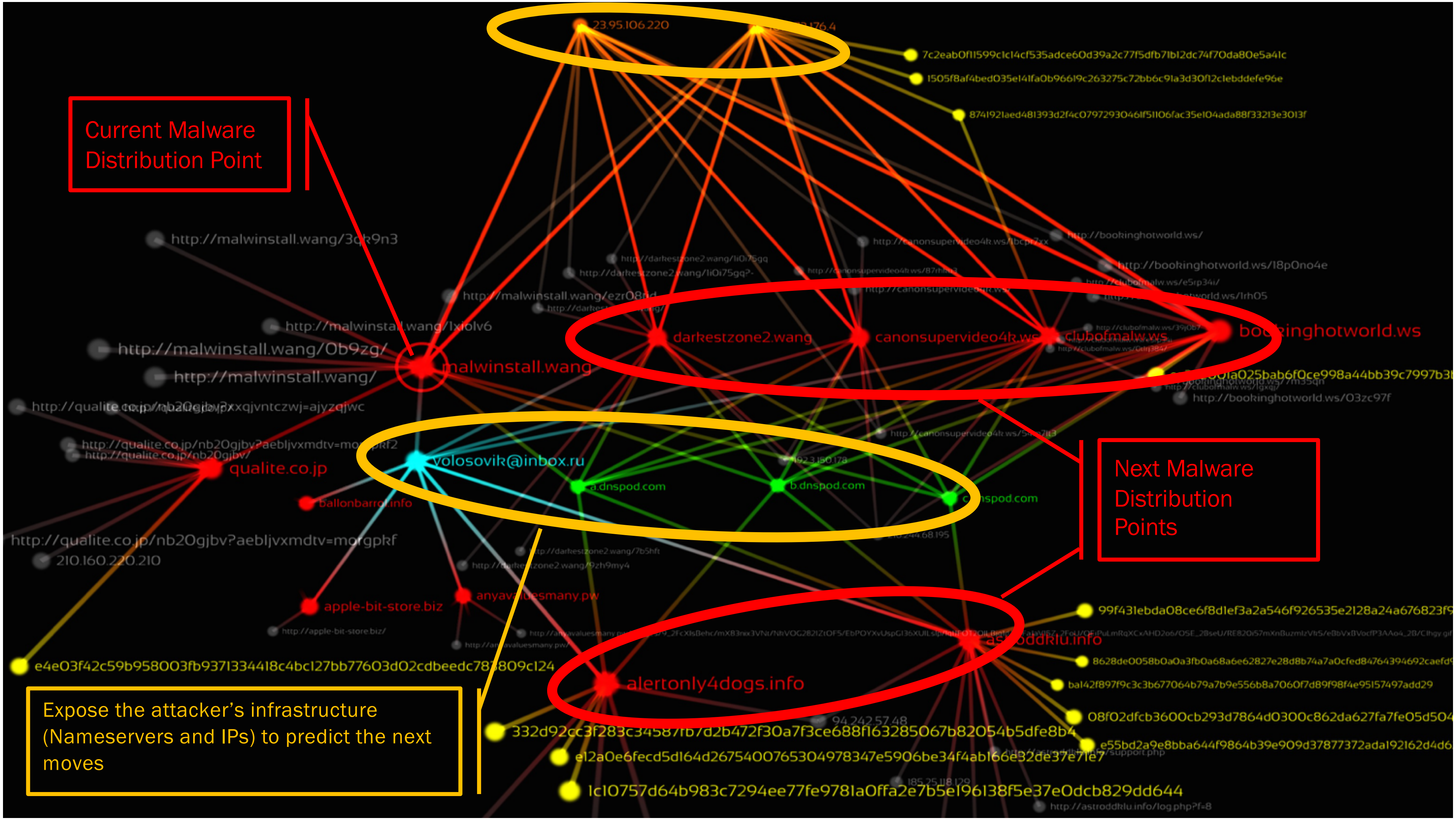
These domains share the same infrastructure

Same Nameservers

malwinstall.wang INVESTIGATE

CO-OCCURRENCES

qualite.co.jp (100.00)


23.95.106.220
7c2eab0f11599c1c14cf535adce60d39a2c77f5dfb71b12dc74f70da80e5a41c
1505f8af4bed035e141fa0b96619c263275c72bb6c91a3d30f12c1ebddefe96e
874192 1aed481393d2f4c07972930461f51106fac35e104ada88f33213e3013f
http://malwinstall.wang/3qk9n3
http://bookinghotworld.ws/
http://canonsupervideo4k.ws/lbcpr7xx
http://darkestzone2.wang/1i0i75gq
http://darkestzone2.wang/1i0i75gq?-
http://bookinghotworld.ws/18p0no4e
http://clubofmalw.ws/e5rp34i/
http://malwinstall.wang/ezr08nd
http://malwinstall.wang/1xiolv6
http://malwinstall.wang/0b9zg/
http://malwinstall.wang/
malwinstall.wang
darkestzone2.wang
canonsupervideo4k.ws
clubofmalw.ws
bookinghotworld.ws
http://bookinghotworld.ws/03zc97f
http://qualite.co.jp/nb20gjbv?xxqjvntczwj=ajyzqjwc
http://qualite.co.jp/nb20gjbv?aebljvxmdtv=morgpkf2
http://qualite.co.jp/nb20gjbv/
qualite.co.jp
volosovik@inbox.ru
a.dnspod.com
b.dnspod.com
c.dnspod.com
ballonbarrel.info
http://qualite.co.jp/nb20gjbv?aebljvxmdtv=morgpkf
210.160.220.210
http://darkestzone2.wang/7b5hft
http://darkestzone2.wang/9zh9my4
apple-bit-store.biz
anyavaluesmany.pw
http://apple-bit-store.biz/
http://anyavaluesmany.pw/
e4e03f42c59b958003fb9371334418c4bc127bb77603d02cdbeedc783809c124
alertonly4dogs.info
astroddklu.info
99f431ebda08ce6f8d1ef3a2a546f926535e2128a24a676823f9
8628de0058b0a0a3fb0a68a6e62827e28d8b74a7a0cfed84764394692caefd9
ba142f897f9c3c3b677064b79a7b9e556b8a7060f7d89f98f4e95157497add29
08f02dfcb3600cb293d7864d0300c862da627fa7fe05d504
332d92cc3f283c34587fb7d2b472f30a7f3ce688f163285067b82054b5dfe8b4
e55bd2a9e8bba644f9864b39e909d37877372ada192162d4d6
e12a0e6fecd5d164d26754007653049783 47e5906be34f4ab166e32de37e71e7
94.242.57.48
185.25.118.129
1c10757d64b983c7294ee77fe9781a0ffa2e7b5e196138f5e37e0dcb829dd644
http://astroddklu.info/support.php
http://astroddklu.info/log.php?f=8

Current Malware Distribution Point

Next Malware Distribution Points

Expose the attacker's infrastructure (Nameservers and IPs) to predict the next moves

Thank you

cisco

CISCOSEC