

# Fighting Fire with Fire – detecting DNS-tunneling with DNS.

Artsiom Holub

Senior Security Analyst

2022

# DNS tunneling adoption





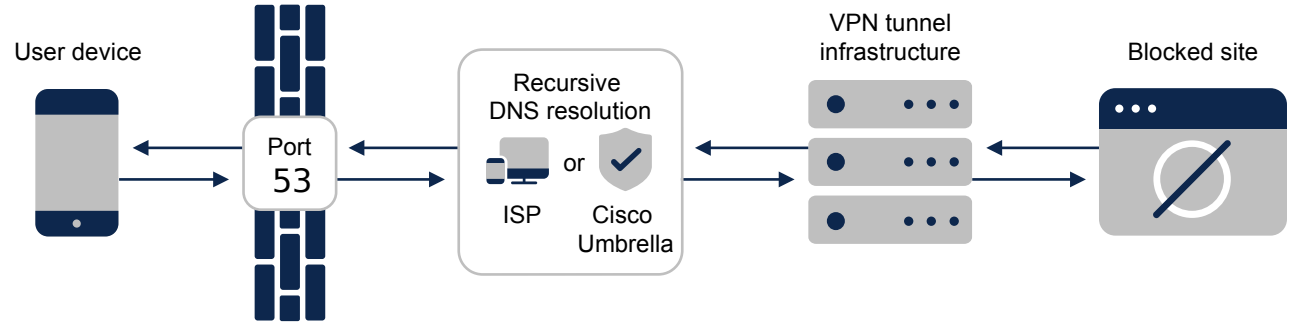


.my.tun.com

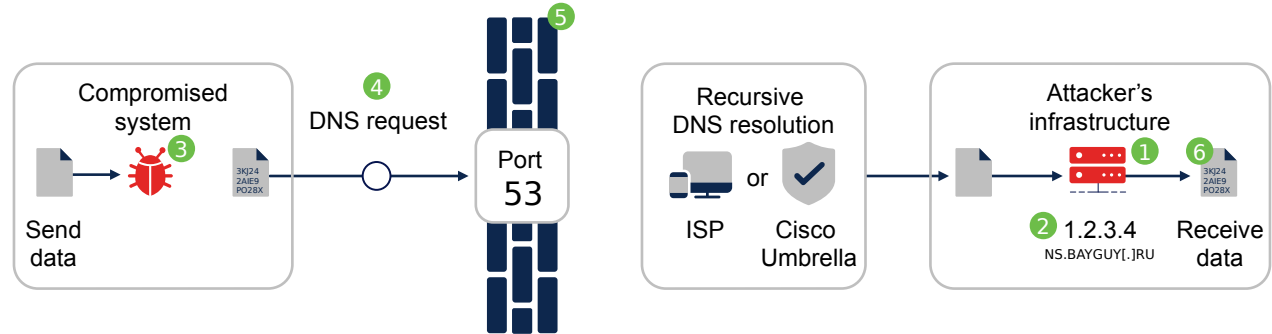


# DNS tunneling

IT policy avoidance  
and guest Wi-Fi abuse



Data exfiltration  
and C2 callbacks



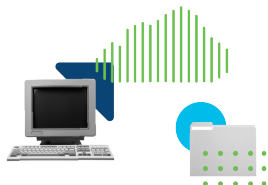
# Threat Actors utilize DNS-Tunneling in malware attacks



# Technique is adopted by various APT groups

Iran-linked APT group OilRig is heavily leveraging on DNS tunneling for its cyber espionage campaigns

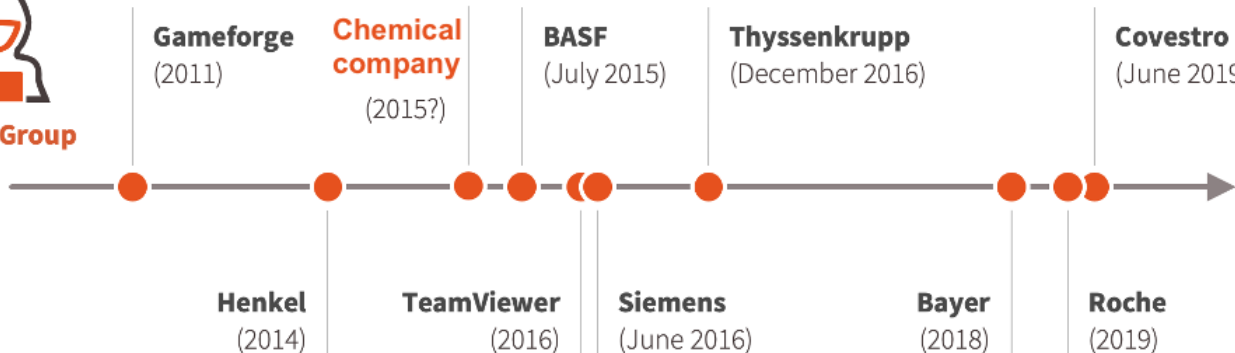
```
lnit.nbwy3dpfv3w64tmmphidupqzta.base32.tun2.test.com.
0.ccf3pqbliu6.yfp2e3hf4.lchncyur9e.sqqrz.tun2.test.com.
1.sircp2x1w4.u6nyjx3pyh.4e55g5xlnk.iznaa.tun2.test.com.
unhg.kehqf6bia6.xpjga.tun2.test.com.
o5k5.wlej7ba64n.kyife.tun2.test.com.
gkjt.azn3bf27yr.qb2ub.tun2.test.com.
3pny.4l2spfn3z.6mtds.tun2.test.com.
tsrv5.q5avdhrdbb.zh5ay.tun2.test.com.
g7mlkx.ajag2.tun2.test.com.
4qmbu.dcg2v.tun2.test.com.
xsmr2q.6tph2s.dea7k.tun2.test.com.
kr6ns.4gnkrampcy.32bpt.tun2.test.com.
swmnv.74pcagsk2v.x7mr2.tun2.test.com.
12.i5gerhcd5fd.4okqc3hr7v.exp7vfrzqk.icedj.tun2.test.com.
13.z6hgflqay7.gohjhazx3z.sk4amt7qab.j66zn.tun2.test.com.
14.d2j6hvv234.uinloao5km.rqjfqyikva.w2efx.tun2.test.com.
15.ymeoysh3sg.v2wo2ermpg.swcyw.jmex.zayhx.tun2.test.com.
16.hqh3tco7tr.d6zacz25x4.rzbrchpxop.lhac.
17.3amhergfoe.sh67axl.jmv.gycow4tpev.5g4qx.
18.cfeewg5ipn.bwl45evrtr.bys1zh5uh1.zorrr.
19.wp6our7oww.yungf3mog6.j4pele4144.edww.
20.jnbgmybuor.tz7ywd55ol.5vccppvfxn.rzfb.
21.lanxkxza5g.4gt4ylawf7.6prnzeswu.gefb.
22.4mm6wef8be.bio6wwwt.zg.qssx.dnzs5y.z47e.
23.mbkns1znvs.7wjku7pbqb.55kjnv7avh.7dxbl.
24.4oyrsyy4pg.oj5mnb3sbu.16mzfw3njw.1dguc.
25.lrz7bby7tk.127lqp33qj.ye7v2slpcd.6r7ql.
26.h3kzc43qky.6dx7u3ay3l.rm747hbeyj.qibj6.tun2.test.com.
```



File Types

txt, jpg, png, pdf, mov...

WINNTI (also known as APT41, BARIUM, and Blackfly) relies on a DNS Tunneling communication channel with a custom implementation





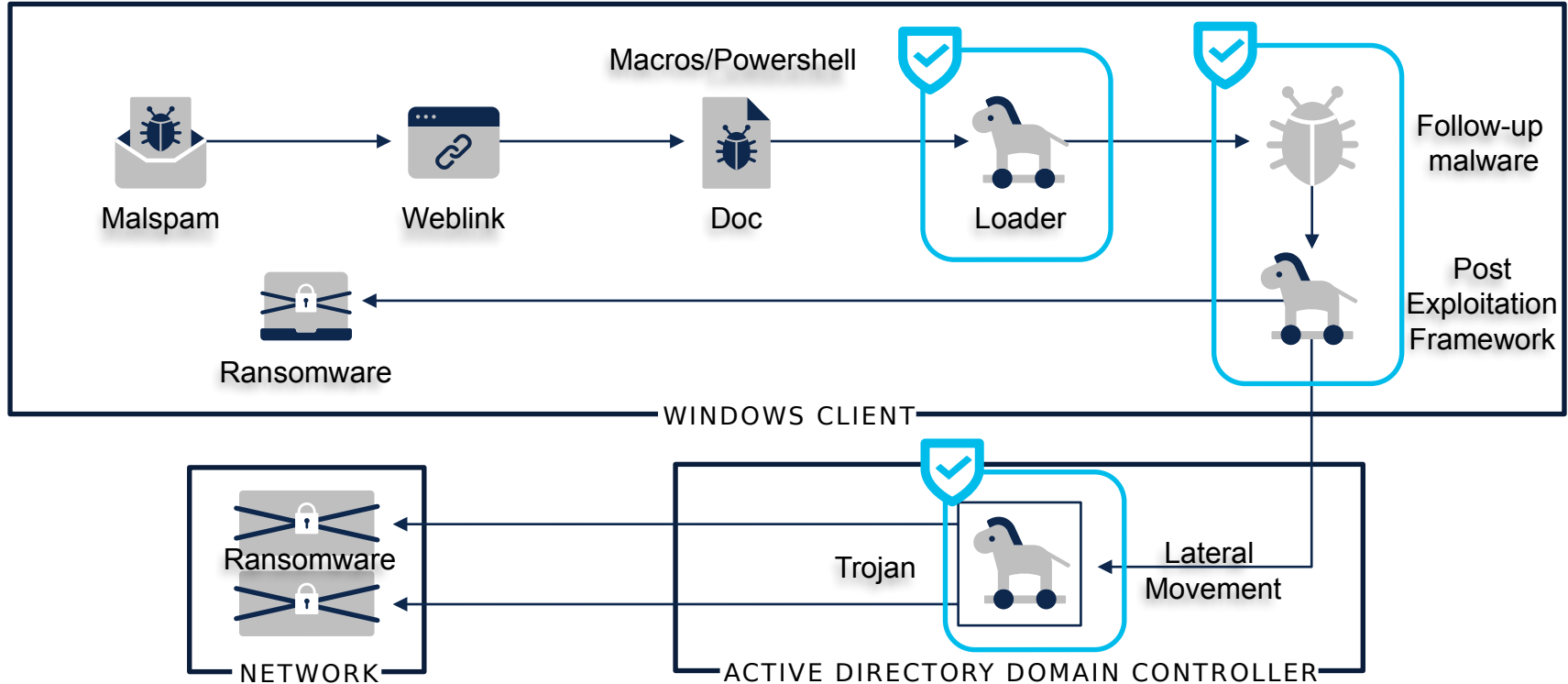
# SUNBURST

Supply Chain Attack most likely associated with APT

```
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.  
ajlcd4r3cc8j1r0orveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.  
sj8312vqo4eaah86hirhe0ge2h.appsync-api.us-east-2.avsvmcloud.com.  
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.  
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.  
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.  
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.  
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.  
sj8312vqo4eaah86hirhe0ge2h.appsync-api.us-east-2.avsvmcloud.com.
```

- Trojanized DLL in digitally signed SolarWinds – thought to occur around Spring 2020
- Post-compromised communication used previously unknown algorithm
  - Network traffic designed to mimic normal SolarWinds API communications
  - DNS exfiltration
- Follow up malware **TEARDROP** and **COBALT STRIKE**
  - Lateral movement, data theft

# Multistage attacks often results in ransomware





# ChaChi RAT delivers PYSA ransomware

## DNS traffic generated by ChaChi

dns.qry.type == 16									
No.	Time	Source	Destination	Protcl	Length	Info			
2185	34.482899	192.168.2.4	8.8.8.8	DNS	195	Standard query	0x3f1d	TXT	658fe29f498bdef4587298ba1a72b31dd85deb2649754398a9a846c3a123722.d9b3f7b130b2f5bdc7ba26aef05d
2186	34.483739	192.168.2.4	8.8.8.8	DNS	204	Standard query	0x599a	TXT	20c816f7a8f20ff29713928c43429e1760f0f7941169a51eb24ca0f104c8d10.eae8675c45cfff5f35534f0ed84
2187	34.545519	8.8.8.8	192.168.2.4	DNS	209	Standard query response	0x3f1d	TXT	658fe29f498bdef4587298ba1a72b31dd85deb2649754398a9a846c3a123722.d9b3f7b130b2f5bdc7b
2188	34.545960	8.8.8.8	192.168.2.4	DNS	218	Standard query response	0x599a	TXT	20c816f7a8f20ff29713928c43429e1760f0f7941169a51eb24ca0f104c8d10.eae8675c45cfff5f35
2189	34.550247	192.168.2.4	8.8.8.8	DNS	291	Standard query	0x993c	TXT	36db830a4b09bea94b34daa341c029e4d9b4fc6b57bd67b1007414407836c99.fbb46a6d0cc4589be43ce7748313
2190	34.616509	8.8.8.8	192.168.2.4	DNS	305	Standard query response	0x993c	TXT	36db830a4b09bea94b34daa341c029e4d9b4fc6b57bd67b1007414407836c99.fbb46a6d0cc4589be43
2191	34.620449	192.168.2.4	8.8.8.8	DNS	295	Standard query	0xc8a1	TXT	b9bc750edca5fa77594472882c0329a0243bce90aed9e101b84c1d60fd3313f.0a10ff374de5eb65dabf7937ea8b
2192	34.686036	8.8.8.8	192.168.2.4	DNS	309	Standard query response	0xc8a1	TXT	b9bc750edca5fa77594472882c0329a0243bce90aed9e101b84c1d60fd3313f.0a10ff374de5eb65dab
2193	34.689510	192.168.2.4	8.8.8.8	DNS	214	Standard query	0xf5be	TXT	17b79eb7bb8768302db7acbea467d4151728d1b2cdfb559d6ea8d08eaeca9a2.4929073790a589ebcee00efed87
2194	34.755069	8.8.8.8	192.168.2.4	DNS	228	Standard query response	0xf5be	TXT	17b79eb7bb8768302db7acbea467d4151728d1b2cdfb559d6ea8d08eaeca9a2.4929073790a589ebcee
2195	34.780388	192.168.2.4	8.8.8.8	DNS	187	Standard query	0x4345	TXT	65d389c5bb6cdd674695a4733f72bbb4b3e58aa00edf57a9b962836c7318fff.58c3db60a20f93eee3dab91e321b
2196	34.843876	8.8.8.8	192.168.2.4	DNS	294	Standard query response	0x4345	TXT	65d389c5bb6cdd674695a4733f72bbb4b3e58aa00edf57a9b962836c7318fff.58c3db60a20f93eee3d
2197	34.849673	192.168.2.4	8.8.8.8	DNS	187	Standard query	0x1f7a	TXT	e4eb3d1e6307bb8575c9ff3b2eeb207d3770ddd9ffe41f56d2195f07a8f98c0.3c00a20cd372bf13ccbf3ea359e
2198	34.918535	8.8.8.8	192.168.2.4	DNS	366	Standard query response	0x1f7a	TXT	e4eb3d1e6307bb8575c9ff3b2eeb207d3770ddd9ffe41f56d2195f07a8f98c0.3c00a20cd372bf13ccbf3ea359e

▶ Frame 2185: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)

▶ Ethernet II, Src: Dell\_ea:15:88 (ec:f4:bb:ea:15:88), Dst: VMware\_82:cb:33 (00:0c:29:82:cb:33)

▶ Internet Protocol Version 4, Src: 192.168.2.4, Dst: 8.8.8.8

▶ User Datagram Protocol, Src Port: 55046, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x3f1d

▶ Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▶ 658fe29f498bdef4587298ba1a72b31dd85deb2649754398a9a846c3a123722.d9b3f7b130b2f5bdc7ba26aef05db26e130913585535ecda2f98a370.transnet.wiki: type TXT, class IN

[Response In: 2187]



# ChaChi RAT C2 DNS Tunneling analysis

## Modified Chashell

```
▼ Answers
▼ 0ff5530eabfaf81c28007b1a7e031f3c0d0e0a092a0112f259ef00b7e4a3dbb.39ca87c582a941a116ddd778b26a1733d0bf3ec7cebef8c40.englishdialoge.xyz: type TXT, class IN
  Name: 0ff5530eabfaf81c28007b1a7e031f3c0d0e0a092a0112f259ef00b7e4a3dbb.39ca87c582a941a116ddd778b26a1733d0bf3ec7cebef8c40.englishdialoge.xyz Query
  Type: TXT (Text strings) (16)
  Class: IN (0x0001)
  Time to live: 3599 (59 minutes, 59 seconds)
  Data length: 97
  TXT Length: 96
  TXT: 09ba8f3068beed9d130acece52faf48caad9af0c2aab2181c8bcfcf4d688a51c56152bab042b37ab53d0c4d1a180f4d6 Response
```

*Chashell DNS tunnelling Query and Response*



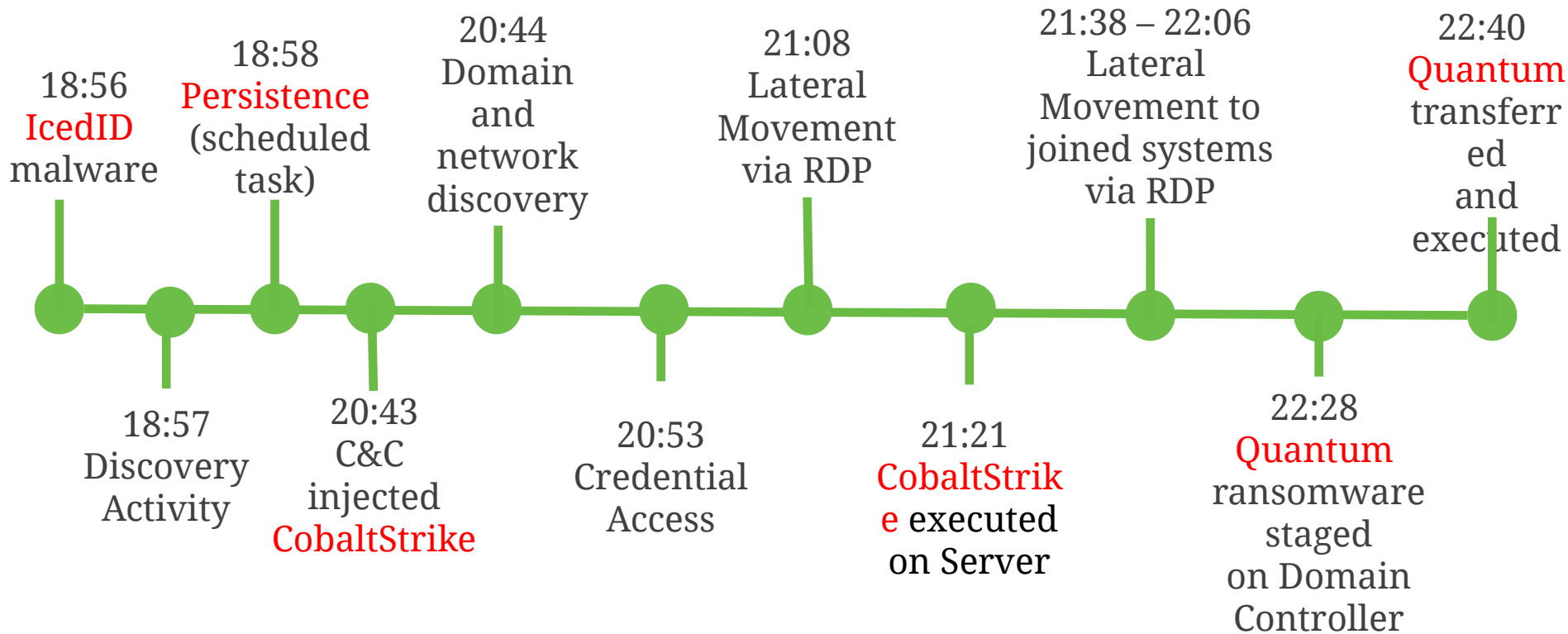
SECURE

© 2022 Cisco and/or its affiliates. All rights reserved.

<https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat>



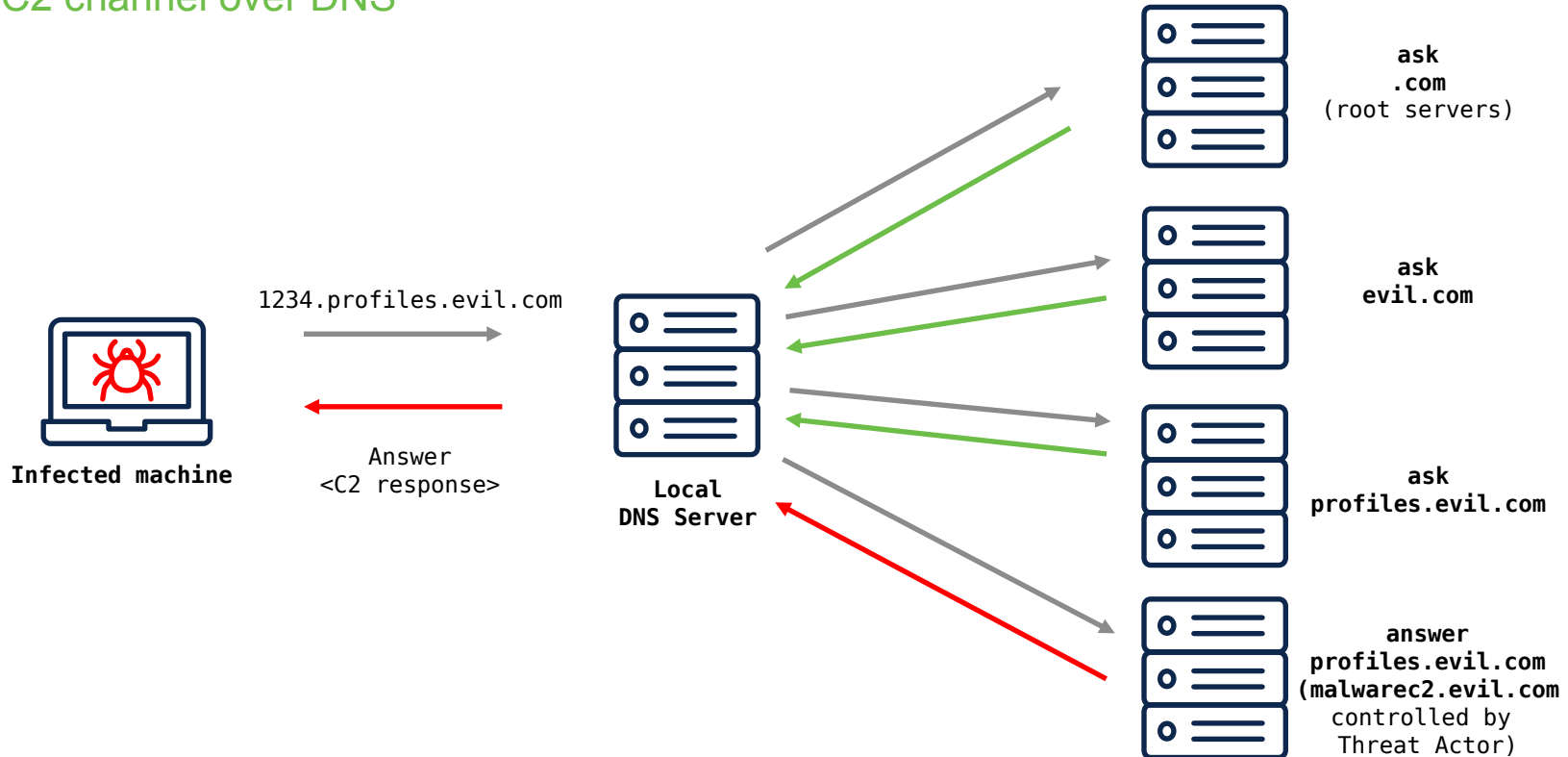
# Quantum ransomware in 4 hours





# CobaltStrike DNS beacon

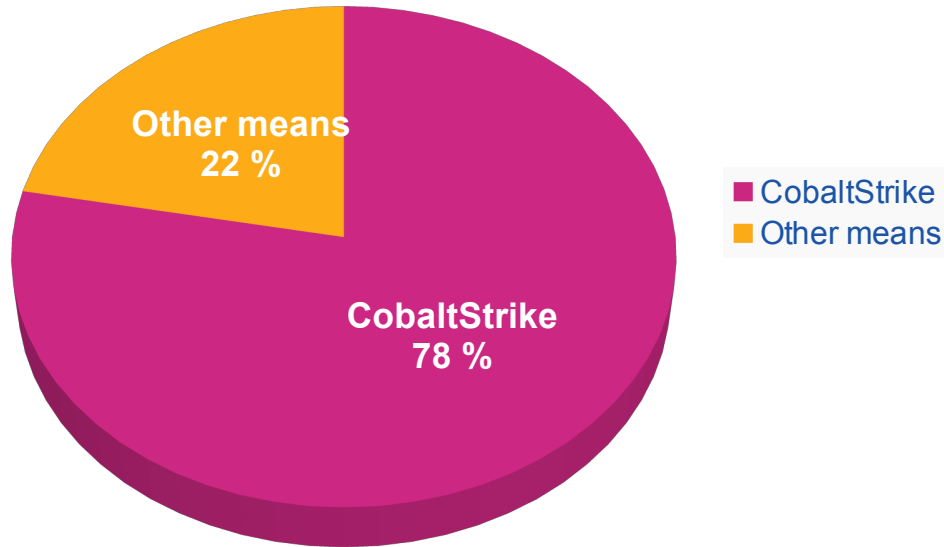
## C2 channel over DNS





# Ransomware utilizing CobaltStrike

## Ransomware Attacks



- DNS Beacon is one of the most used Cobalt Strike features
- DNS Beacon is a DNS-only payload (no HTTP communication)
- A beacon can be configured with Malleable C2 configuration



# Analyzing DNS Traffic

## Wireshark view of Cobalt Strike DNS traffic

No.	Time	Source	Destination	Protocol	Stream index	Info
15354	2021-11-10 16:09:29,784176	192.168.111...	54.246.181.1	DNS		Standard query 0xc4ea A 19997cf2.wallet.thedarkestdside.org OPT
15358	2021-11-10 16:09:29,824396	54.246.181.1	192.168.111.5	DNS		Standard query response 0xc4ea A 19997cf2.wallet.thedarkestdside.org A 8.8.4.246
15463	2021-11-10 16:09:39,831448	192.168.111...	54.246.181.1	DNS		Standard query 0x2bda A api.046cd40cb.19997cf2.wallet.thedarkestdside.org
15464	2021-11-10 16:09:39,867367	54.246.181.1	192.168.111.5	DNS		Standard query response 0x2bda A api.046cd40cb.19997cf2.wallet.thedarkestdside.org A 8.8.4.52
15582	2021-11-10 16:09:49,898012	192.168.111...	54.246.181.1	DNS		Standard query 0xcbe7 TXT api.146cd40cb.19997cf2.wallet.thedarkestdside.org OPT
15584	2021-11-10 16:09:49,934897	54.246.181.1	192.168.111.5	DNS		Standard query response 0xcbe7 TXT api.146cd40cb.19997cf2.wallet.thedarkestdside.org TXT
15691	2021-11-10 16:09:59,938836	192.168.111...	54.246.181.1	DNS		Standard query 0xb076 A post.130.01b902135.19997cf2.wallet.thedarkestdside.org
15692	2021-11-10 16:09:59,977018	54.246.181.1	192.168.111.5	DNS		Standard query response 0xb076 A post.130.01b902135.19997cf2.wallet.thedarkestdside.org A 8.8.4.4
15769	2021-11-10 16:10:09,990881	192.168.111...	54.246.181.1	DNS		Standard query 0xc5d3 A post.2d195d35695d92484de7c5ec120e69b4d488d5c7c3de95c4a.ef3c54f0cf699db3850445febf2528
15770	2021-11-10 16:10:10,032850	54.246.181.1	192.168.111.5	DNS		Standard query response 0xc5d3 A post.2d195d35695d92484de7c5ec120e69b4d488d5c7c3de95c4a.ef3c54f0cf699db385044
15901	2021-11-10 16:10:23,066076	192.168.111...	54.246.181.1	DNS		Standard query 0x604b A 19997cf2.wallet.thedarkestdside.org
15902	2021-11-10 16:10:23,102986	54.246.181.1	192.168.111.5	DNS		Standard query response 0x604b A 19997cf2.wallet.thedarkestdside.org A 8.8.4.4
16007	2021-11-10 16:10:36,124801	192.168.111...	54.246.181.1	DNS		Standard query 0xc44 A 19997cf2.wallet.thedarkestdside.org OPT
16011	2021-11-10 16:10:36,170850	54.246.181.1	192.168.111.5	DNS		Standard query response 0xc44 A 19997cf2.wallet.thedarkestdside.org A 8.8.4.246
16124	2021-11-10 16:10:46,178810	192.168.111...	54.246.181.1	DNS		Standard query 0x9211 A api.03dd750ef.19997cf2.wallet.thedarkestdside.org
16125	2021-11-10 16:10:46,219201	54.246.181.1	192.168.111.5	DNS		Standard query response 0x9211 A api.03dd750ef.19997cf2.wallet.thedarkestdside.org A 8.8.4.84
16214	2021-11-10 16:10:56,228989	192.168.111...	54.246.181.1	DNS		Standard query 0xc78a TXT api.13dd750ef.19997cf2.wallet.thedarkestdside.org OPT
16215	2021-11-10 16:10:56,266308	54.246.181.1	192.168.111.5	DNS		Standard query response 0xc78a TXT api.13dd750ef.19997cf2.wallet.thedarkestdside.org TXT

From <https://blog.nviso.eu/2021/11/29/cobalt-strike-decrypting-dns-traffic-part-5/>



SECURE

© 2022 Cisco and/or its affiliates. All rights reserved.



# CobaltStrike Beacons

## Beacon configuration

```
Config found: xorkey ...
0x0001 payload type      0x0001 0x0002  1 windows-
beacon_dns-reverse_http
...
...
...
0x0008 server, get-uri    0x0003 0x0100
'malicious.domain.evil/search/'
...
...
...
0x0006 maxdns             0x0001 0x0002  245
0x0013 DNS_Idle           0x0002 0x0004  123443044
8.8.4.4
0x0014 DNS_Sleep          0x0002 0x0004  10000
0x003c DNS_beacon         0x0003 0x0021
(NULL ...)
0x003d DNS_A              0x0003 0x0021  'cdn.'
0x003e DNS_AAAA           0x0003 0x0021  'www6.'
0x003f DNS_TXT            0x0003 0x0021  'api.'
0x0040 DNS_metadata       0x0003 0x0021  'www.'
0x0041 DNS_output         0x0003 0x0021  'post.'
0x0042 DNS_resolver       0x0003 0x000f
(NULL ...)
```

## Malleable C2 configuration

```
dns-beacon {

    # Options moved into 'dns-beacon' group in 4.3:
    set dns_idle            "1.2.3.4";
    set dns_max_txt         "199";
    set dns_sleep           "1";
    set dns_ttl             "5";
    set maxdns              "200";
    set dns_stager_prepend  "doc-stg-prepend";
    set dns_stager_subhost  "doc-stg-sh.";

    # DNS subhost override options added in 4.3:
    set beacon              "doc.bc.";
    set get_A               "doc.1a.";
    set get_AAAA            "doc.4a.";
    set get_TXT             "doc.tx.";
    set put_metadata        "doc.md.";
    set put_output          "doc.po.";

    set ns_response         "zero";

}
```



# Analyzing DNS Traffic

Beacon sending results to the team server with DNS\_output queries

```
Query A post.140.09842910.19997cf2.wallet.thedarkestside.org
Response A 8.8.4.4
Query A post.2942880f933a45cf2d048b0c14917493df0cd10a0de26ea103d0eb1b3.4adf28c63a97deb5cbe4e20b26902d1ef427957323967835f7d18a42.19842910.19997cf2.wallet.thedarkestside.org OPT
Response A 8.8.4.4
Query A post.ldebfa06ab4786477.29842910.19997cf2.wallet.thedarkestside.org
Response A 8.8.4.4
```

From <https://blog.nviso.eu/2021/11/29/cobalt-strike-decrypting-dns-traffic-part-5/>

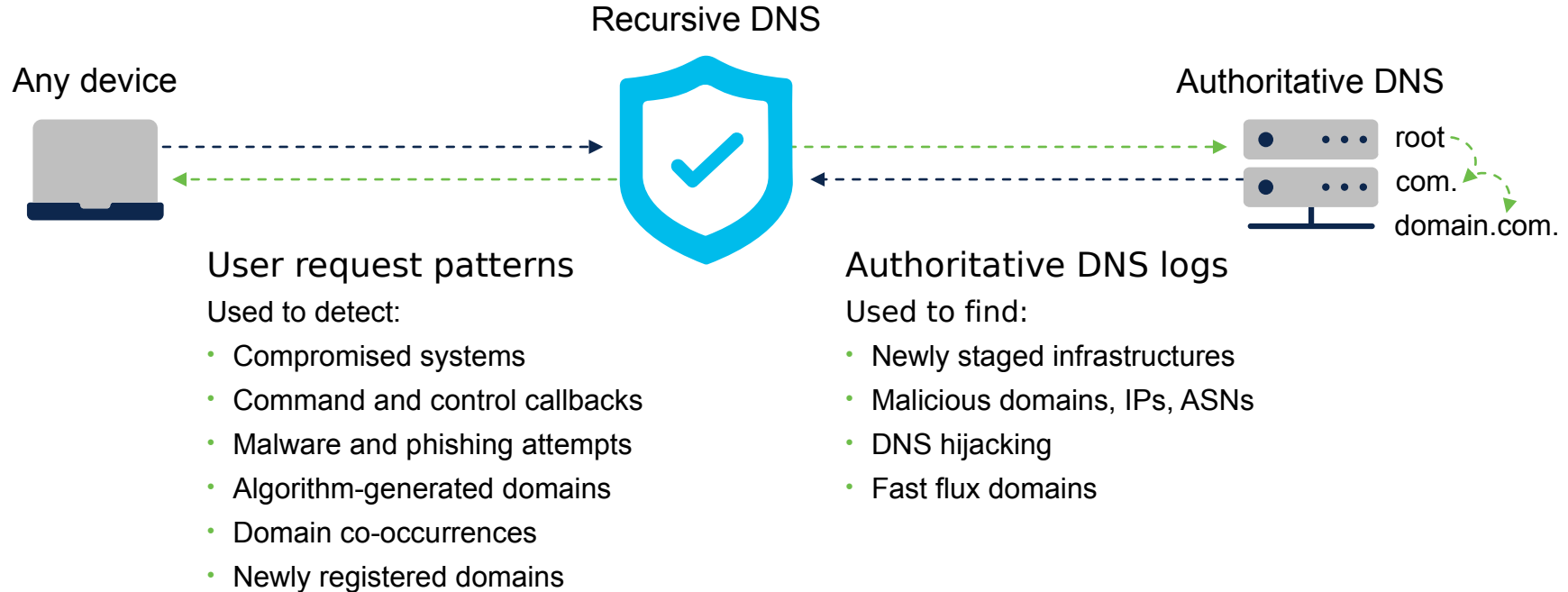
This name breaks down into the following labels:

- post: DNS\_output query
- 140: transmitted data
- 09842910: counter + random number
- 19997cf2: beacon ID
- wallet[.]thedarkestside.org: domain chosen by the operator

# Using DNS to build Detection

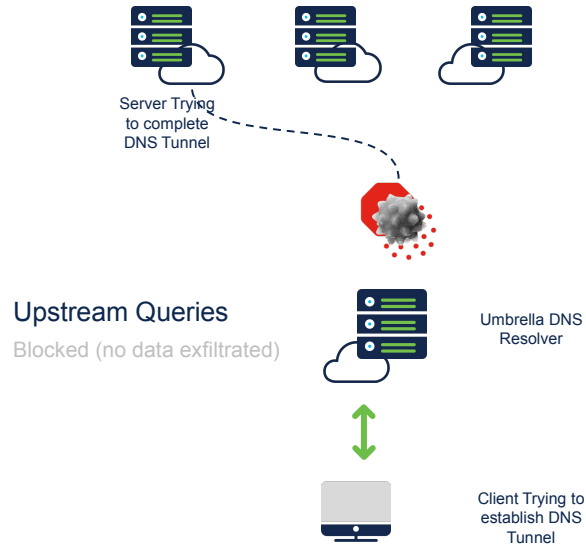


# Gathering intelligence at the DNS layer



# Acquiring datasets

Various tools, encoding techniques and queries



## Tools

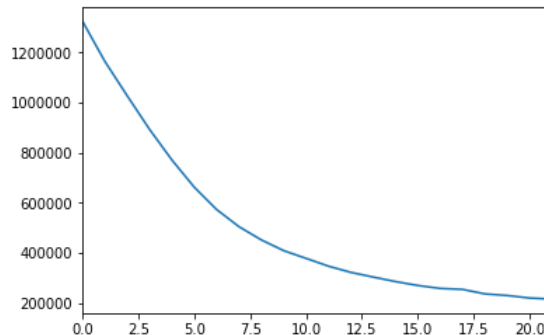
DNS2TCP  
DNSSCAT2  
DNSExfiltrator...

## Encoding techniques and query characteristics

Base64, Base32 ...  
Qtypes - TXT, SRV,  
MX, CNAME

# Statistics, Communication, and Features

- Interested in lexical features of subdomains
  - Subdomains contain the ‘payload’ of the message
- Features
  - Number of subdomains
  - Existence of particular trigrams
  - Compressibility of feature sets
- Lloyd's algorithm to identify groups
  - Measure distortion



# Behavioral profiles based on DNS queries

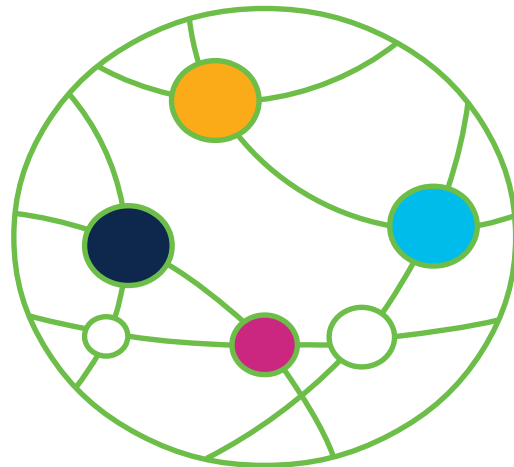
- Build statistical profile to identify groups of devices within the network that have a prescribed role
- The statistical profile is built from looking at graph data
- Build a large bi-partite graph between clients and FQDNs
- Decompose the graph into connected components
  - Each connected component represents as set of domains queried by a subset of clients
  - Smaller connected components usually indicate that a set of domains may be unique to only one or two clients

## Statistics:

- Jaccard Index over the hours a client is active
- The size of the connected component a client is part of
- The largest connected component a client is in
- Number of unique PLDs in the connected component

# Clustering

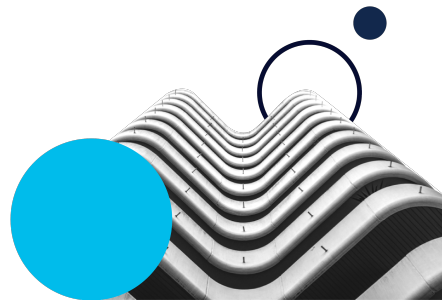
- At high level we can see these types of clusters:
  - Specialized Network Device Communication:
    - Behavior: Bursts of communication for ~1 hour only with easily identified PLDs
  - Service based devices with Continuous Communication:
    - Messaging > 15 on avg, High Jaccard.  
Examples :WebIT services, billing, login services
  - Network and Server like Devices
    - Behavior = 1 hour on + many messages to many clients
  - User devices
    - Huge cluster of clients with one to many relations





# Building Detections

- **Reactive**
  - Identifies tunneling domains based on statistics derived through querylog data
- **Realtime Heuristics**
  - Rule based method to detect known tunneling using signatures and rules
- **Realtime Behavioral Detection**
  - Behavioral based detection that mimics the detection capability of the reactive system
  - System based on client query activity



nbswy3dpfv3w64tmmqxhi6dupqztan

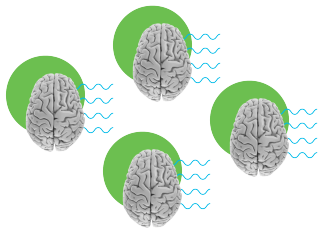
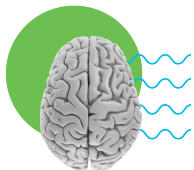
## Example of Stateful Algorithm Realtime Tunneling Detection

Technique to identify encrypted Base32 and Base64 messages in real-time. Relies on transition probabilities from one character to the next, identifying character combinations likely related to encrypted messages.



# DNS Resolver (Real-time Caching Detection)

Implementation of the detections directly in the resolver



## Name Server Cache

- Caches frequently requested DNS records.
- Name server info frequently cached.

## Tunneling Cache Signatures

- Developing proprietary caching strategy.
- Maintain signatures related to tunneling.

## Global Resolver Fleet

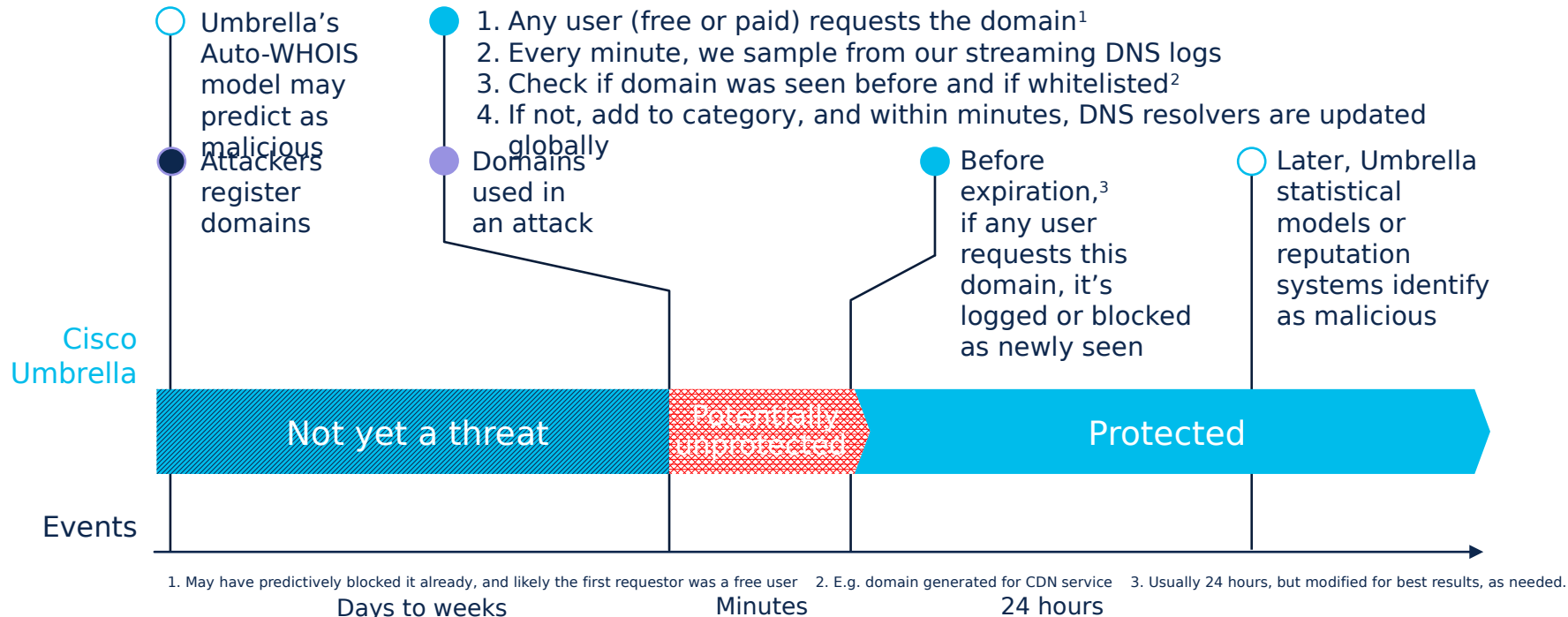
- DNS resolvers independently detect DNS tunneling

# Protection from unknown with Quarantine approach



# 'Newly seen domains' category

Reduces risk of the unknown





Medium Risk

## povertyboring2020b.com

The domain is classified as Medium Risk due to a combination of suspect security features.

### Security Categories

Newly Seen Domains

### Content Categories

—

### SECURITY INDICATORS ▾

## Timeline

Current Content Category: None

 DNS Queries

 Domain Events

 DNS Changes

May 4th, 2021 - Jun 3rd, 2021

3

Max. Queries: 3

2

1





/ 85

?



/ 88

?



Community  
Score



 1 detected URL under this domain

povertyboring2020b.com

Registrar

Key-Systems GmbH

Creation Date

4 hours ago

Last Updated

4 hours ago

 1 security vendor flagged this URL as malicious

http://povertyboring2020b.com/adda/ZMoDqRO/61231/8SwW54zjWxbcX7nbOaAnKvOluuubeYBvIhDo9hwsfiLLeaj/gD1foHFdVZVXIItqa4Be5RmXpqcHoA61IJx3DFtmP/38077/essTO4

povertyboring2020b.com

200

Status

text/html; charset=UTF-8

Content Type

2021-06-03 15:31:31 UTC

1 hour ago

DETECTION

DETAILS

SUBMISSIONS

COMMUNITY

URL detection partners on 2021-06-03T15:31:31 

Forcepoint ThreatSeeker

 Malicious

ADMINUSLabs

 Clean

AegisLab WebGuard

 Clean

AICC (MONITORAPP)

 Clean



?



Community  
Score



! 6 security vendors flagged this domain as malicious

povertyboring2020b.com

Creation Date

11 days ago

Last Updated

11 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

CRDF

! Malicious

CyRadar

! Malicious

ESET

! Malware

Forcepoint ThreatSeeker

! Malicious

Fortinet

! Malware

Sophos

! Malware



▼ 📄 General

Target  
order 06.21.doc

Filesize  
43KB

Completed  
03-06-2021 14:43



Score

10<sup>/10</sup>

MD5  
b1254d3fa38e2418734d4a2851fc22a6

SHA1  
7c71a7ae38ef95d36434f0b680b30393de9b95ec

SHA256  
95af2e46631be234a51785845079265629462e809e667081eb0b723116e265f3

icedid

531791608

banker

trojan

▶ ⚙️ Malware Config

▶ 📄 Signatures

▶ 🎯 Processes

▼ 🌐 Network

REQUESTS

TCP

UDP

DNS

povertyboring2020b.com

mshta.exe

GET

http://povertyboring2020b.com/adda/ZMoDqRO/61231/8SwW54zjWxbcX7nbOaAnKvOluuubeYBvIhDo9hwsfiLLeaj/gD1foHFdVZVXIItqa4Be5RmXpq...

mshta.exe






95af2e46631be234a51785845079265629462e809e667081eb0b723116e265f3

Category  
can be  
incorporated  
in the analysis  
as indicator  
of potentially  
malicious activity

## BEHAVIORAL INDICATORS

Indicator	Severity 
Artifact Flagged Malicious by Antivirus Service	100
A Document File with Embedded and Minimal Content Established Network Communications	100
Document Submission Contacted Domain Flagged By Cisco Umbrella	100
Executable Artifact has Misleading File Extension	60
Downloaded PE Executable	60
Cisco Umbrella Categorized Domain As A Newly Seen Domain	60

Twitter:

@Mesiagh

Email:

@artholub@cisco.com



TALOS™

Special Thanks:  
Thomas Mathew

TALOSINTELLIGENCE.COM