RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-R01**

Power of DNS as an Added Defense Against Modern Attacks

Artsiom Holub
Senior Security Research Analyst
Cisco Umbrella
@messiagh

CISCO

Disclaimer

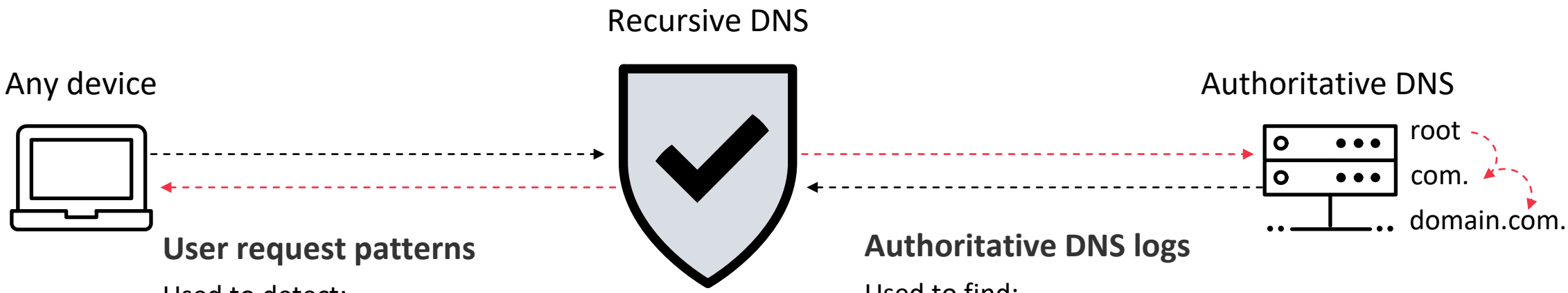
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

DNS data gathering, analysis and use cases

Gathering Intelligence at the DNS Layer



User request patterns

Used to detect:

- Compromised systems
- Command and control callbacks
- Algorithm-generated domains
- Domain co-occurrences
- Newly seen domains

Authoritative DNS logs

Used to find:

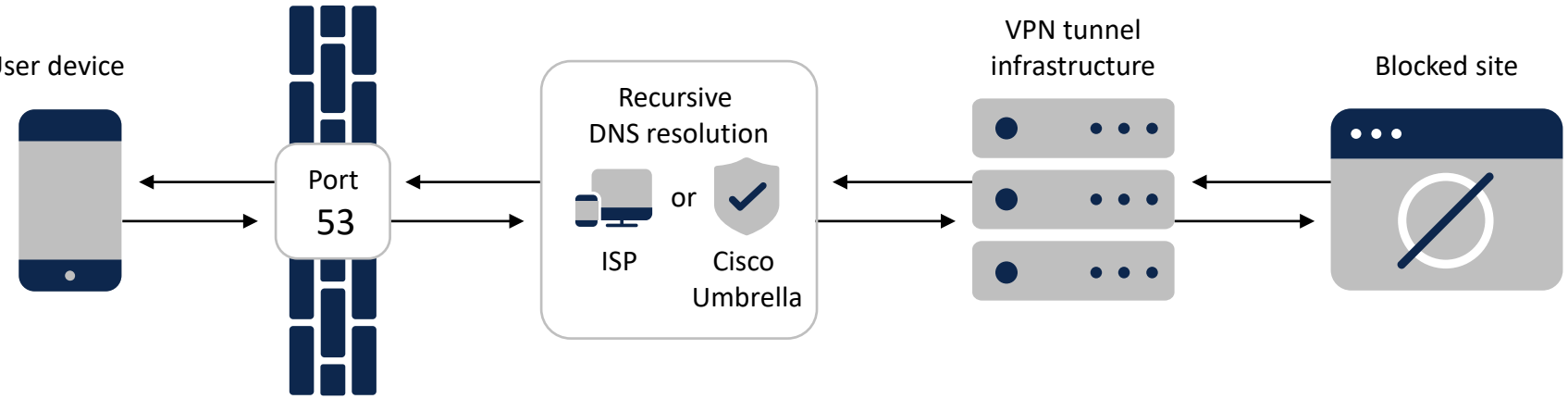
- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- BulletProofHostings

RSAConference2022

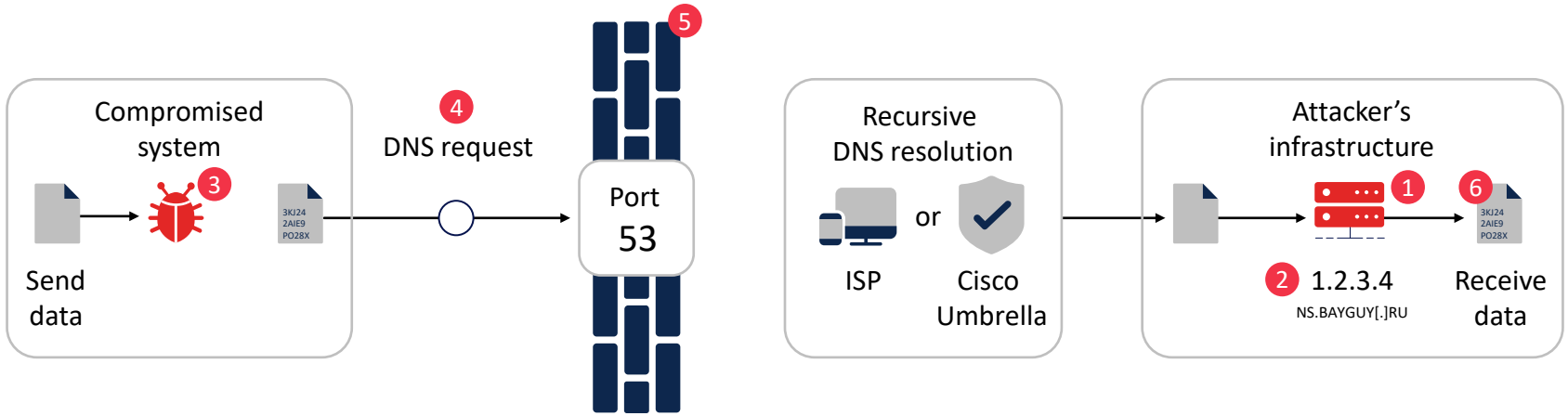
DNS tunneling adoption for C&C and data exfiltration

DNS tunneling

IT policy avoidance and guest Wi-Fi abuse



Data exfiltration and C2 callbacks



.my.tun.com

Sunburst – Supply Chain Attack

- 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

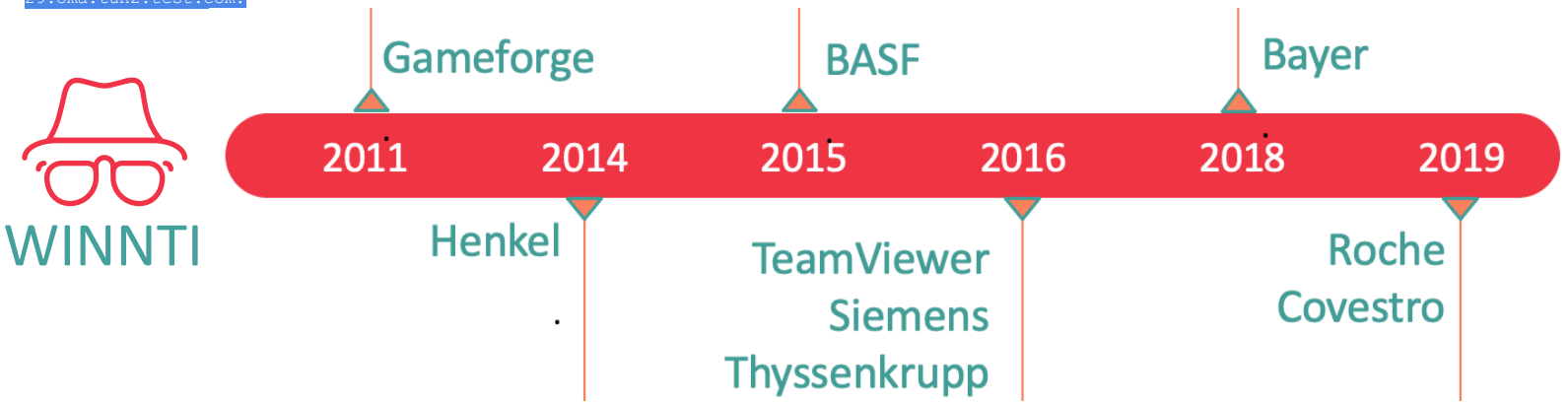
```
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.
ajlcd4r3cc8j1r0orveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.
sj8312vqo4eaah86hirhe0ge2h.appsync-api.us-east-2.avsvmcloud.com.
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.
kbl0pqk3l38n7v7yrveuvu0ie2h.appsync-api.us-east-1.avsvmcloud.com.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

Technique is adopted by various APT groups

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

```
init.nbswy3dpfv3w64tmmqxhi6dupqzta.base32.tun2.test.com.
0.ccf3pqbiu6.ypfp2e3hf4.lchncynr5e.soqrz.tun2.test.com.
1.sircpzxlw4.u6nyjr3pyh.4e55g5xlnk.iznsa.tun2.test.com.
                fu2vgeunhg.kehqfb6ia6.xpjga.tun2.test.com.
                cbmkb4o5k5.wlejfba64n.kyife.tun2.test.com.
                rzzjb6gkjt.azn3bf27yv.qb2ub.tun2.test.com.
                hh2fdp3pny.4lzspfng3z.6mtds.tun2.test.com.
                3pymlhtyv5.q5swdurwbb.zh5ay.tun2.test.com.
                h66ub4zlix.an7jpg7mlk.ajag2.tun2.test.com.
                ailsjo67zh.abnwz4gmbu.dcq2v.tun2.test.com.
                u3b47v7xsm.bqem6tph2s.dea7k.tun2.test.com.
                .h2nk3kr6ns.4gnkramjcy
                .dscf4swwnv.74pragsk2w
                .4okqc3hr7v.ewp7vfsrqk
                .gohjhzsx3z.skwhmt7qab
                .uinokao5km.rqjfqyikva
                .v2wo2ermpg.swcywtjmex
                .d6zacx25x4.rzbrchpxop
                .sh67axljmv.gycow4hpev
                .bwi45evfwr.bysizb5uhl
                .yungf3moq6.j4peie4l44
                .tz7ywd55ol.5vccppvfxr
                .4gtdylxwf7.6prm2eswnu
                .bio6wwwtzg.qssrdmnz5y
                .7wjku7pbqb.55kjnv7avh
                .oj5mvb3sbu.i6mzfw3mjw
                .127iqp33qj.ye7v2slpcc
                .6dx7u3sy3i.rm747hbeyj
27.nmsxtgdazg.vgtkp7cz23.twpei7grf5.ayiwd.tun2.test.com.
28.5jqe3c7dkk.wyvkcigeqb.lpcvtlbc3i.eaq72.tun2.test.com.
29.oma.tun2.test.com.
```

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



WINNTI malware C2 DNS Tunneling analysis

C2 configuration

Root domain : dick[.]mooo[.]com

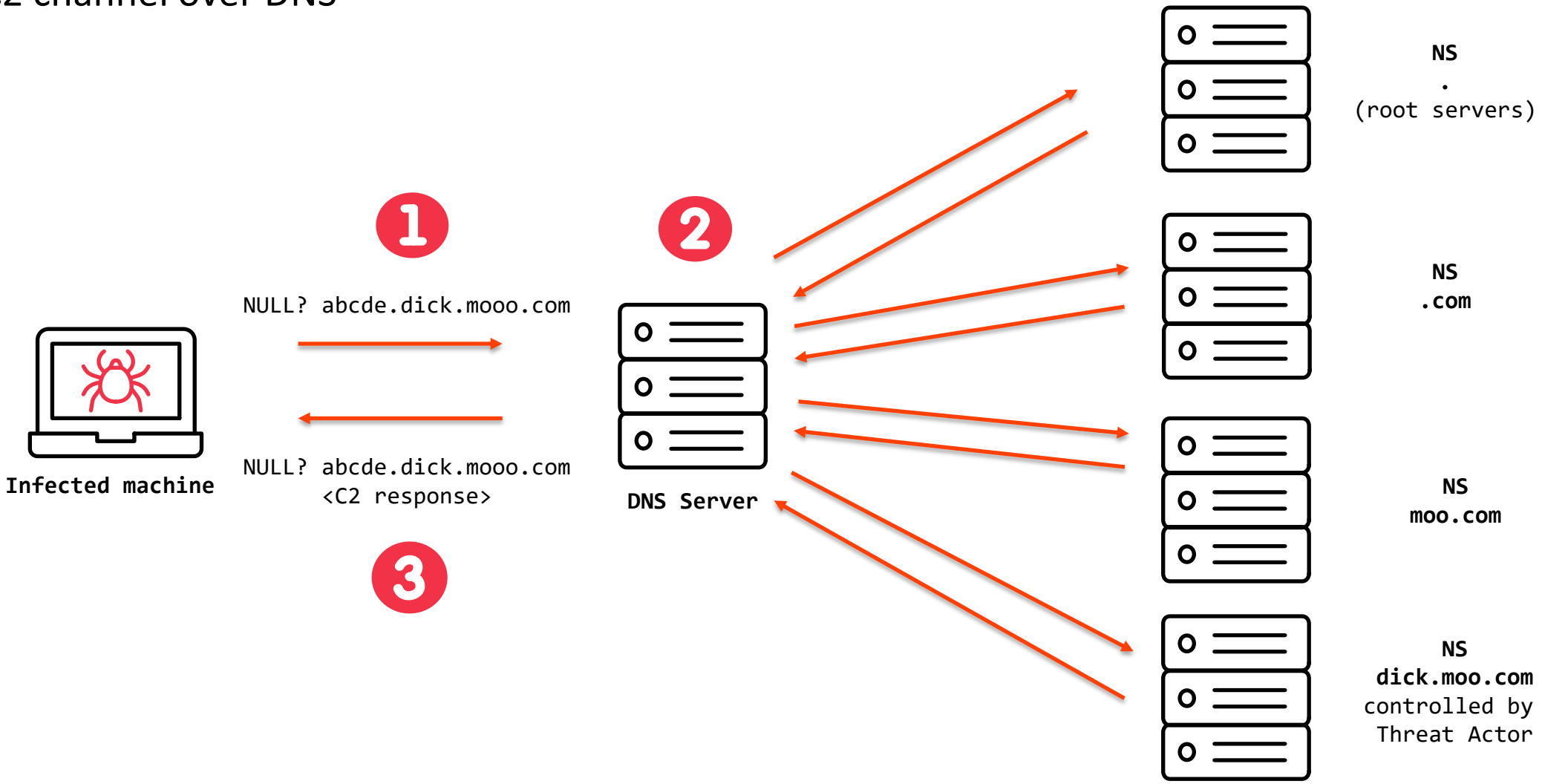
```
dst_domain_offset = (char *)dst + strlen((const char *)dst)-1
if ( *dst_domain_offset != '.' )
     *++dst_domain_offset = '.'; //add dot if previous part does not end with it
strncpy(dst_domain_offset + 1, domain, strlen(domain) + 1
```

Use of Iodine for C2 DNS Tunneling:

build_hostname	base32_handles_dots	base128_decode
inline_dotify	base64_decode	base128_encode
base32_decode	base64_encode	base128_reverse_init
base32_encode	base64_reverse_init	base128_blksize_enc
base32_reverse_init	base64_blksize_enc	base128_blksize_raw

WINNTI malware C2 DNS Tunneling analysis

C2 channel over DNS



WINNTI malware C2 DNS Tunneling analysis

The NULL DNS record type

The implementation of NULL type tunneling:

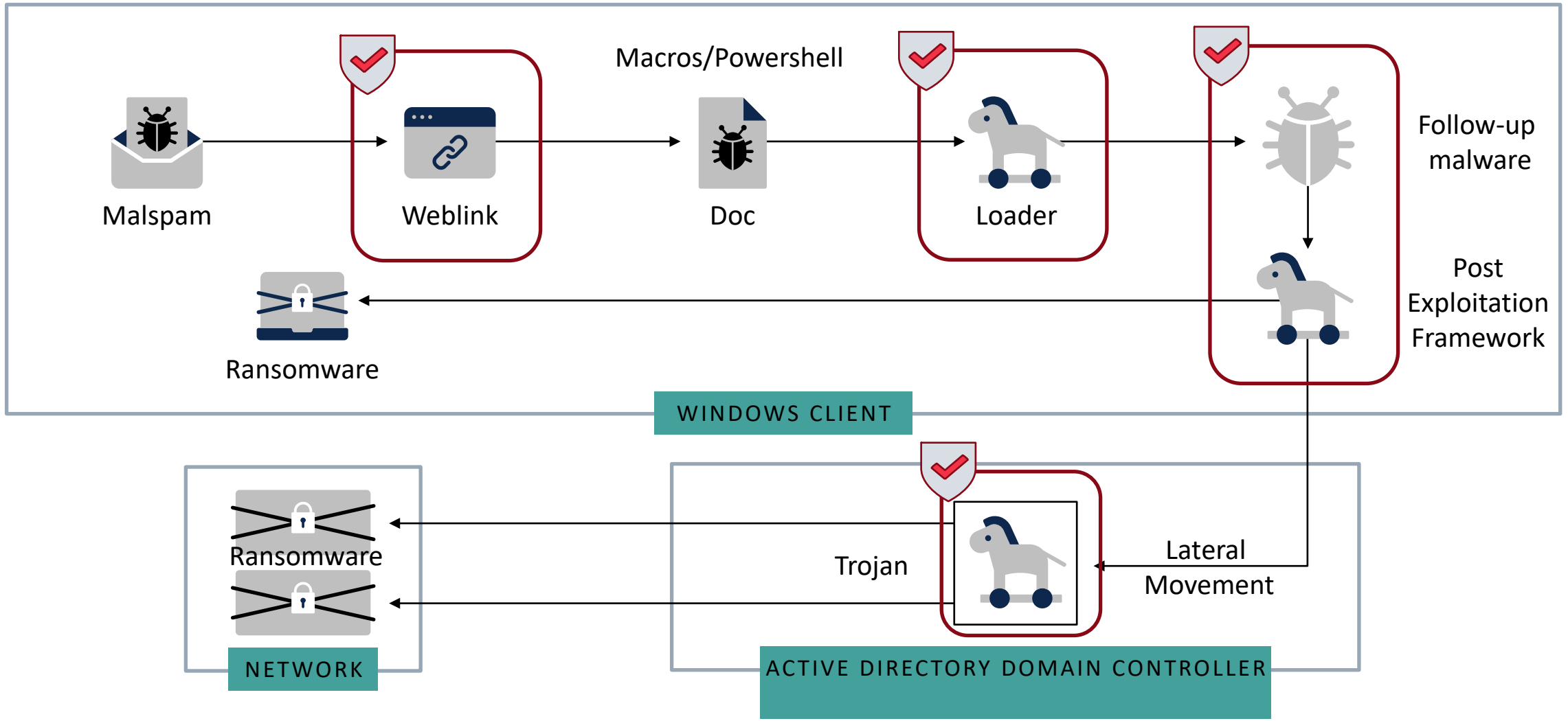
```
LOWORD(query[128]) = 0xA;
result = dns_encode((int *)a1, (unsigned int)v8, (__int64)query, 0, (const char *)v13, strlen((const char*)v13));
```

Iodine's dns.c:

```
/* Only used when iodined gets an NS type query */
/* Mostly same as dns_encode_a_response() below */
int dns_encode_ns_response(char *buf, size_t buflen, struct query *q,
                           char *topdomain)
{
        HEADER *header;
        int len;
        short name;
        short topname;
        short nsname;
        char *ipp;
        int domain_len;
        char *p;

        if (buflen < sizeof(HEADER))
                return 0;

        memset(buf, 0, buflen);

        header = (HEADER*)buf;
```

```
struct query {
        char name[QUERY_NAME_SIZE];
        unsigned short type;
        unsigned short rcode;
        unsigned short id;
        struct sockaddr_storage destination;
        socklen_t dest_len;
        struct sockaddr_storage from;
        socklen_t fromlen;
        unsigned short id2;
        struct sockaddr_storage from2;
        socklen_t fromlen2;
};
```

Multistage attacks often results in ransomware



ChaChi RAT deliver PYSA (aka Mespinoza) ransomware

DNS traffic generated by ChaChi

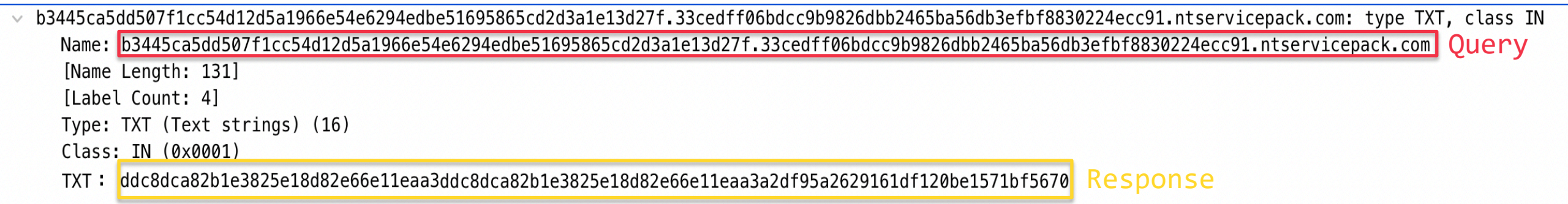
dns.qry.type == 16

No.	Time	Source	Destination	Protocol	Length	Info
39	65.308881	192.168.1.198	192.168.1.1	DNS	199	Standard query 0xb96d TXT e40b5d50382162fef09daa0df5a3daec5bc0240e059c5d46d31f0e436e8d914.24a8601f4a668495495cc12…
40	65.643349	192.168.1.1	192.168.1.198	DNS	254	Standard query response 0xb96d No such name TXT e40b5d50382162fef09daa0df5a3daec5bc0240e059c5d46d31f0e436e8d914.2…
42	66.754094	192.168.1.198	192.168.1.1	DNS	191	Standard query 0xdd25 TXT b3445ca5dd507f1cc54d12d5a1966e54e6294edbe51695865cd2d3a1e13d27f.33cedff06bdcc9b9826dbb2…
43	67.002999	192.168.1.1	192.168.1.198	DNS	246	Standard query response 0xdd25 No such name TXT b3445ca5dd507f1cc54d12d5a1966e54e6294edbe51695865cd2d3a1e13d27f.3…
44	67.906287	192.168.1.198	192.168.1.1	DNS	191	Standard query 0x2fe4 TXT ddc8dca82b1e3825e18d82e66e11eaa3a2df95a2629161df120be1571bf5670.398c6ae5cc6620f96d9918b…
45	68.143977	192.168.1.1	192.168.1.198	DNS	246	Standard query response 0x2fe4 No such name TXT ddc8dca82b1e3825e18d82e66e11eaa3a2df95a2629161df120be1571bf5670.3…
47	68.986950	192.168.1.198	192.168.1.1	DNS	191	Standard query 0xb670 TXT f3fa04aa86c4393c49c0dcce1ebabd5d4c8e5d5b6322385aa57e22d3be8a0ce.fd1a60e1ac0f8eb83f63e2a…
48	69.215378	192.168.1.1	192.168.1.198	DNS	246	Standard query response 0xb670 No such name TXT f3fa04aa86c4393c49c0dcce1ebabd5d4c8e5d5b6322385aa57e22d3be8a0ce.f…
49	70.080905	192.168.1.198	192.168.1.1	DNS	191	Standard query 0x91f6 TXT 0c95080421a9304c99e7f054b505612c2b4c72c54969f7c4b9dad83972a8e4f.0800bdc686fee08827a29f7…
50	70.315366	192.168.1.1	192.168.1.198	DNS	246	Standard query response 0x91f6 No such name TXT 0c95080421a9304c99e7f054b505612c2b4c72c54969f7c4b9dad83972a8e4f.0…
52	71.236699	192.168.1.198	192.168.1.1	DNS	191	Standard query 0x5981 TXT c00c65c142a90dcad78a6e88970cdf861cb96f8b0d0dbaf6dd335b705884080.0ec561124ac08ce00e26f4a…
53	71.475307	192.168.1.1	192.168.1.198	DNS	246	Standard query response 0x5981 No such name TXT c00c65c142a90dcad78a6e88970cdf861cb96f8b0d0dbaf6dd335b705884080.0…
54	72.289232	192.168.1.198	192.168.1.1	DNS	191	Standard query 0x35a7 TXT b061ab703cfd1652256241887f01b4e6d2df7a58ffad996a39026ea31e0b618.63bf80746964463174dcccf…
56	72.521202	192.168.1.1	192.168.1.198	DNS	246	Standard query response 0x35a7 No such name TXT b061ab703cfd1652256241887f01b4e6d2df7a58ffad996a39026ea31e0b618.6…
57	72.869128	192.168.1.198	192.168.1.1	DNS	191	Standard query 0x1c87 TXT 27e8f01c4a6a643bf8d75ab7468f93c14df992d2ca4e2d3d35d56a30f3c4e8b.a64f31b5203f67568158f14…
58	73.110265	192.168.1.1	192.168.1.198	DNS	246	Standard query response 0x1c87 No such name TXT 27e8f01c4a6a643bf8d75ab7468f93c14df992d2ca4e2d3d35d56a30f3c4e8b.a…

```
> Frame 39: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Ethernet II, Src: IntelCor_22:db:73 (00:15:17:22:db:73), Dst: 0c:d6:5a:de:de:27 (0c:d6:5a:de:de:27)
> Internet Protocol Version 4, Src: 192.168.1.198, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 51421 (51421), Dst Port: 53 (53)
v Domain Name System (query)
    [Response In: 40]
    Transaction ID: 0xb96d
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > e40b5d50382162fef09daa0df5a3daec5bc0240e059c5d46d31f0e436e8d914.24a8601f4a668495495cc12fafdb57bec245c18497981befd72d6c3d5.ntservicepack.com: type TXT, class IN
```

ChaChi RAT C2 DNS Tunneling analysis

Modified Chashell



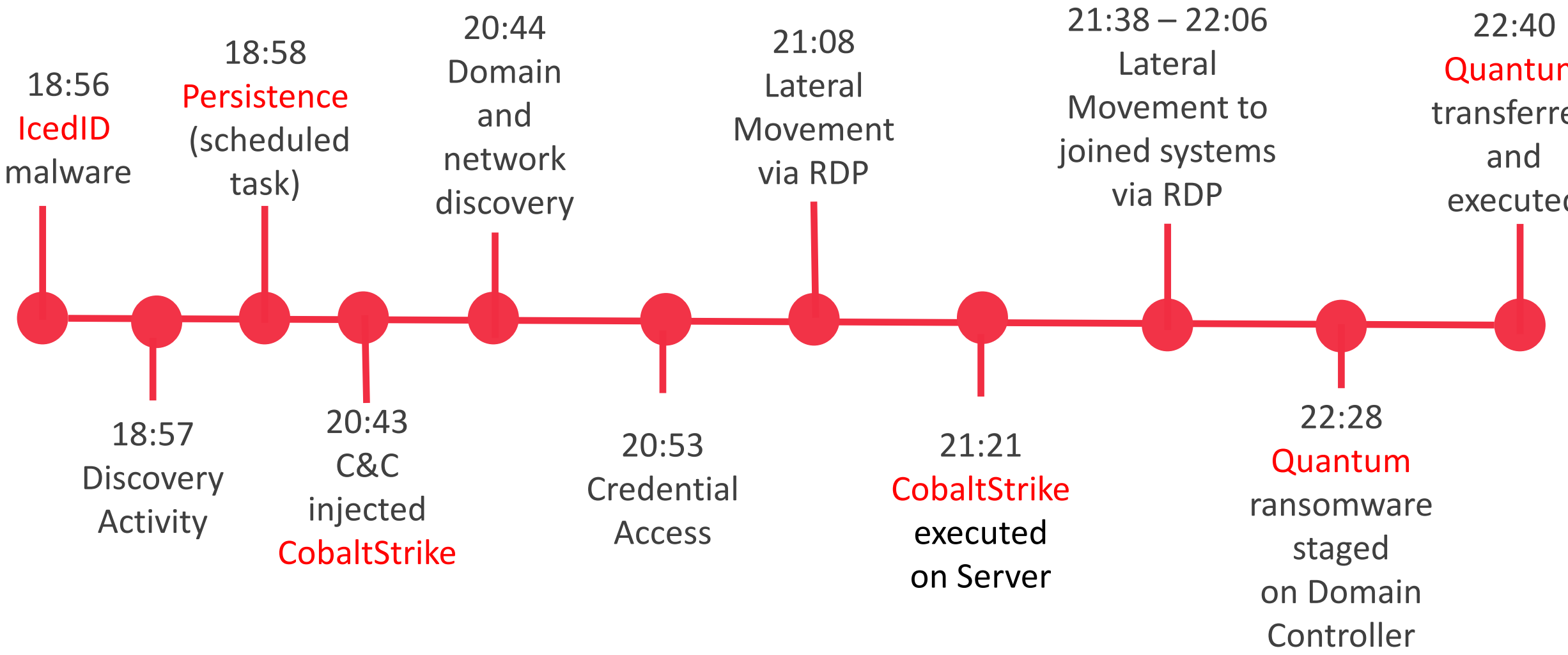
Chashell DNS tunnelling Query and Response

ChaChi RAT C2 DNS Tunneling analysis

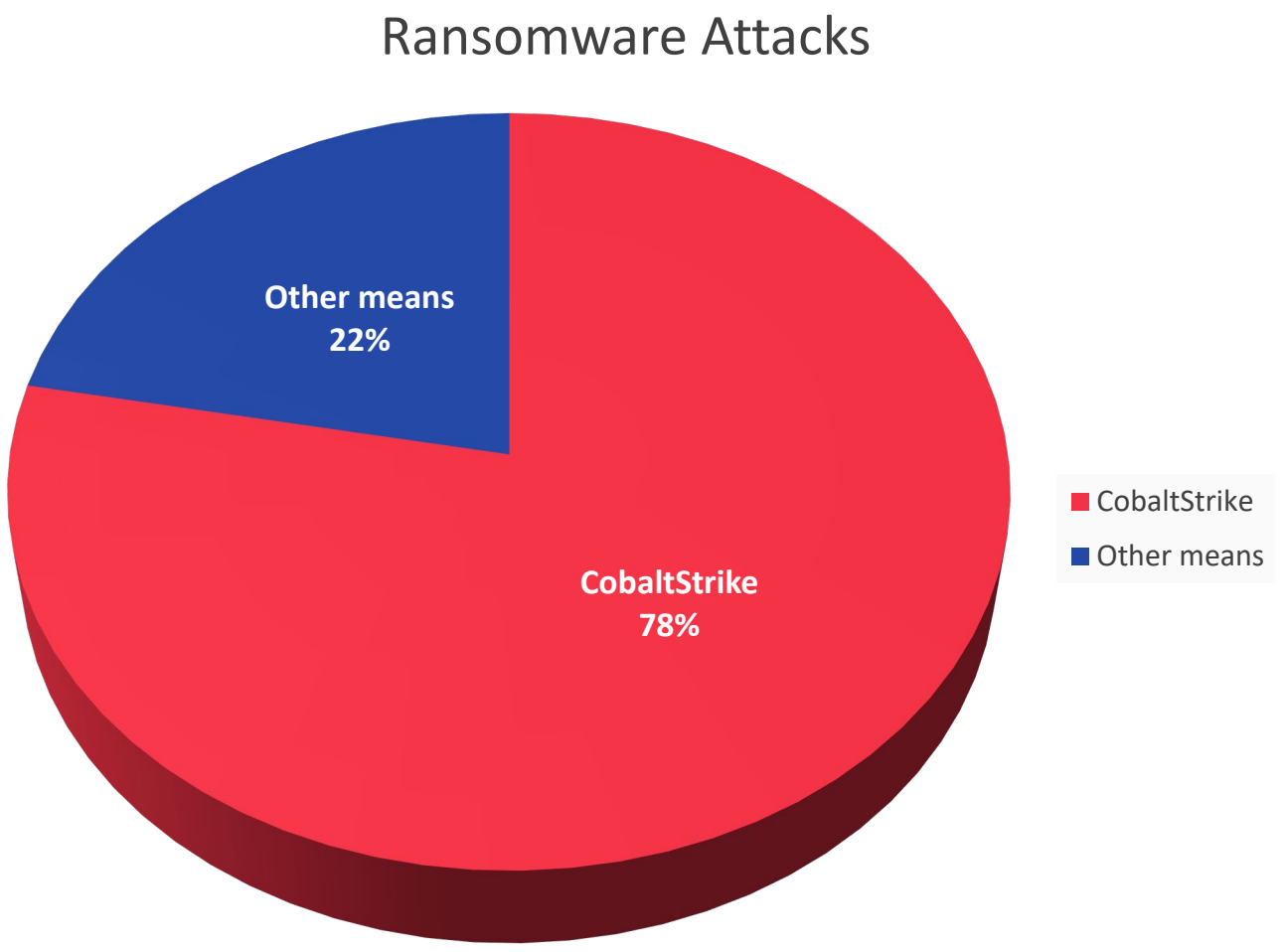
Chashell Protocol Buffer Message.

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

Quantum ransomware in 4 hours



CobaltStrike DNS Beacon



- 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 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";

}
```

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 ZUZBozZmBil0KvISBcqS0nxp32b7h6WxUBw4n70cOLP13eN7PgcnUVOWdO+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

RSAConference2022

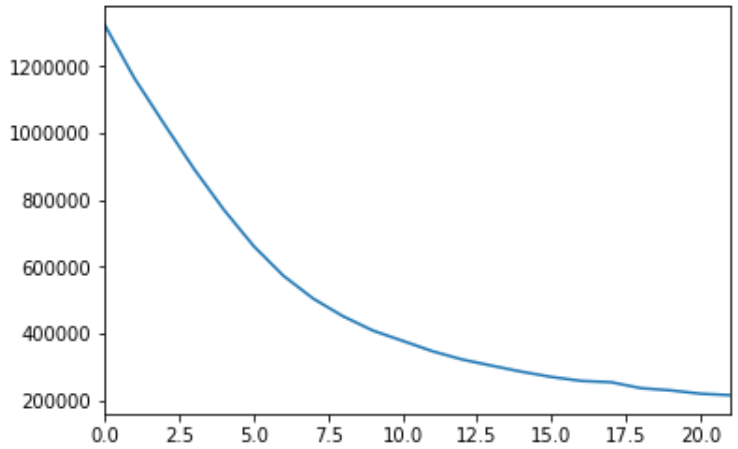
Detecting and stopping DNS tunneling

DNS Tunneling Detections

- **Reactive**
  - Identifies tunneling domains based on querylog data
- **Realtime Heuristics**
  - Rule based method to detect known tunneling tools
  - Run in the resolver
- **Realtime Behavioral Detection**
  - Behavioral based detection that mimics the detection capability of the reactive system
  - System based on client query activity and sits in the resolver

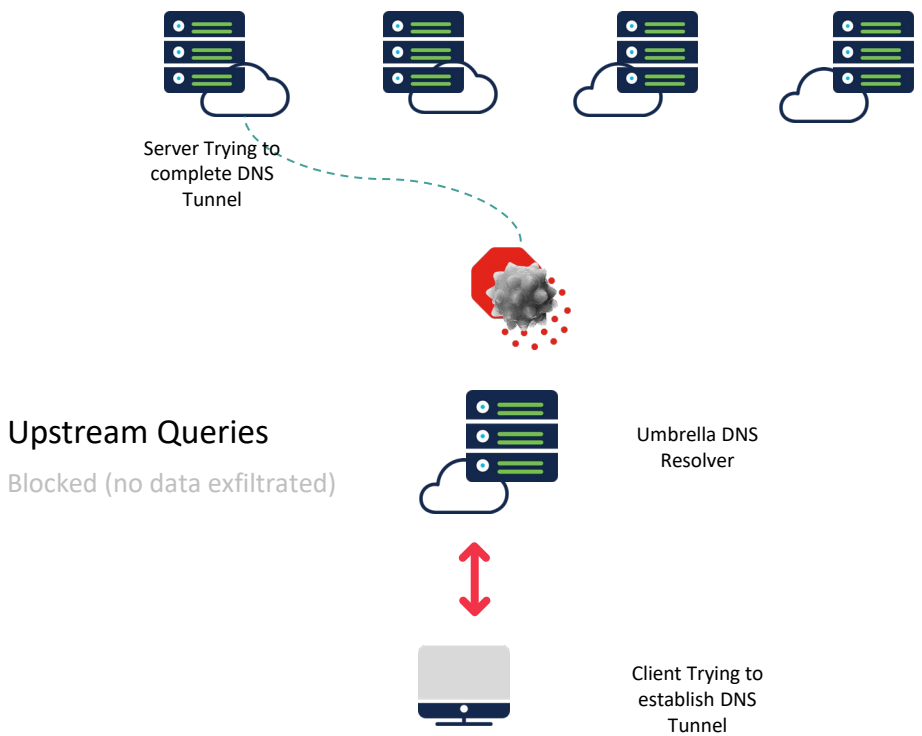
Statistics, Communication, and Detection

- 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



DNS Resolver (Real-time Detection)

Protection against malicious tunneling tools and query techniques



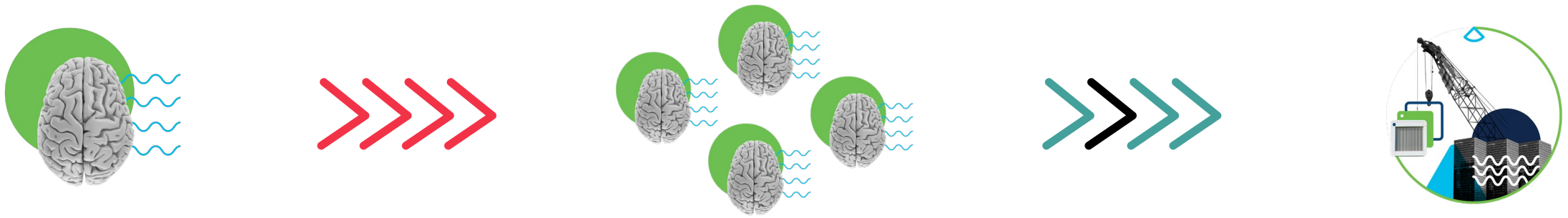
Tools

- 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

RSAConference2022

Protection for the unknown

Newly Seen Domains Category Reduces Risk of the Unknown

1. Any user requests the domain
2. Check if domain was seen before & if whitelisted[1].
3. If not, add to category, and apply inspection

Attackers register domains.

Domains used in an attack.

Before expiration[2], if any user requests this domain, log it and block as newly seen.

Statistical models, automated analysis or manual analysis identify as malicious.

1. E.g. domain generated for CDN service.
2. Usually 24 hours, but can be modified for best results, as needed based on the behaviour.

Wrapping It UP

- Malicious actors and the TTPs are constantly evolving, but DNS is still involved in 90% of the Attacks. To have a DNS monitoring system and DNS security is a MUST
- DNS isn't just initial vector of attack or C&C point. It is often utilized by malicious actors as covert channel for data exfiltration, command and control activities and beaconing. Not being able to detect such activities poses significant risk.
- To successfully counter malicious use of DNS apply combination of three approaches: detect known bad patterns, identify anomalies and apply scrutiny to unknown.

Apply What You Have Learned Today

- Next week you should:
  - Identify weak links in your DNS protection by testing existing solution against open-source DNS tunneling tools
- In the first three months following this presentation you should:
  - Test against known implementations used by the active Threat Actors and APTs
  - Define strategy to improve existing security controls or add new
- Within six months you should:
  - Proactively monitor anomalies and perform inhouse tests according to your organization's needs