CYBERSEC 2024
臺灣資安大會

5/14 Tue – 5/16 Thu
臺北南港展覽二館

Generative
Future

Threat Research Forum

Tunneling and C2 over DNS

Thursday, May 16 at 4:30pm

netskope

Hubert Lin

Sr. Staff Researcher
Netskope

CYBERSEC 2024 Organized by iThome

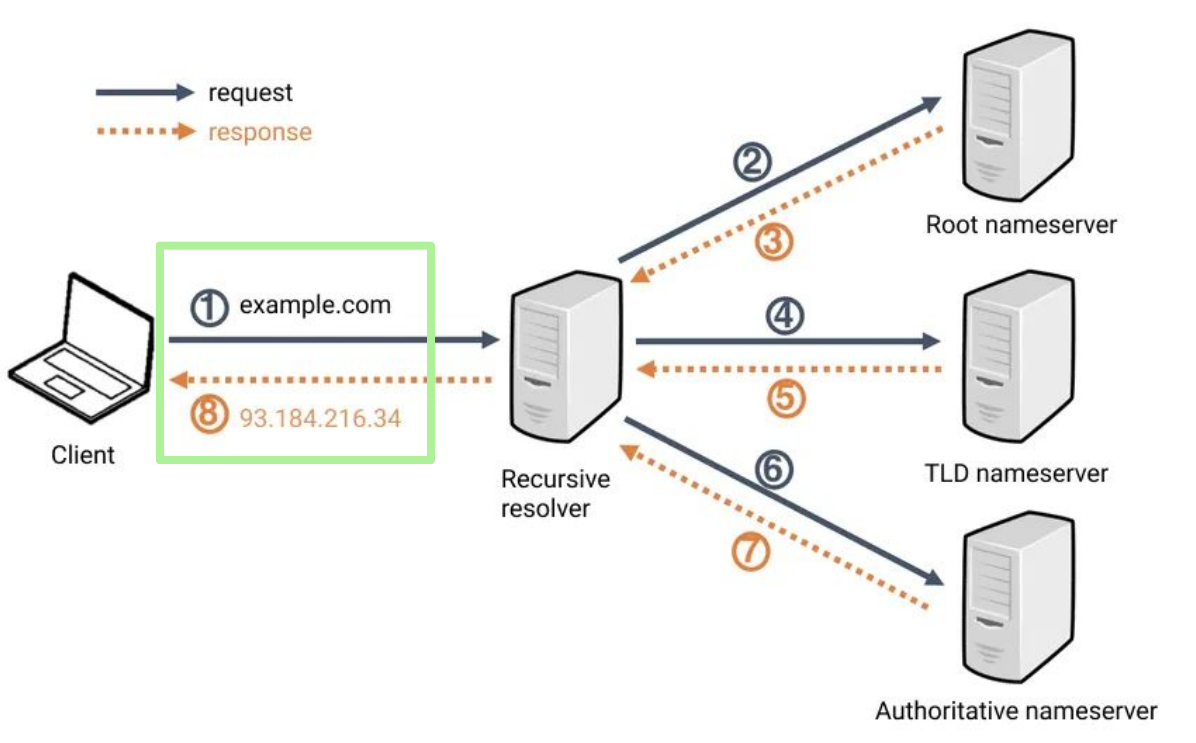
Agenda

- DNS 101
- Tunneling over DNS
  - Iodine
  - dnscat2
- C2 over DNS/DoH
  - Sliver
  - Brute Ratel
- Countermeasures and Takeaways

DNS 101

Name resolution in DNS

- Regular lookup
  - Over 53/UDP
- Zone Transfer
  - Over 53/TCP



https://miro.medium.com/v2/resize:fit:1400/format:webp/1*goSb1oow5UBNF3KkzvOX8A.png

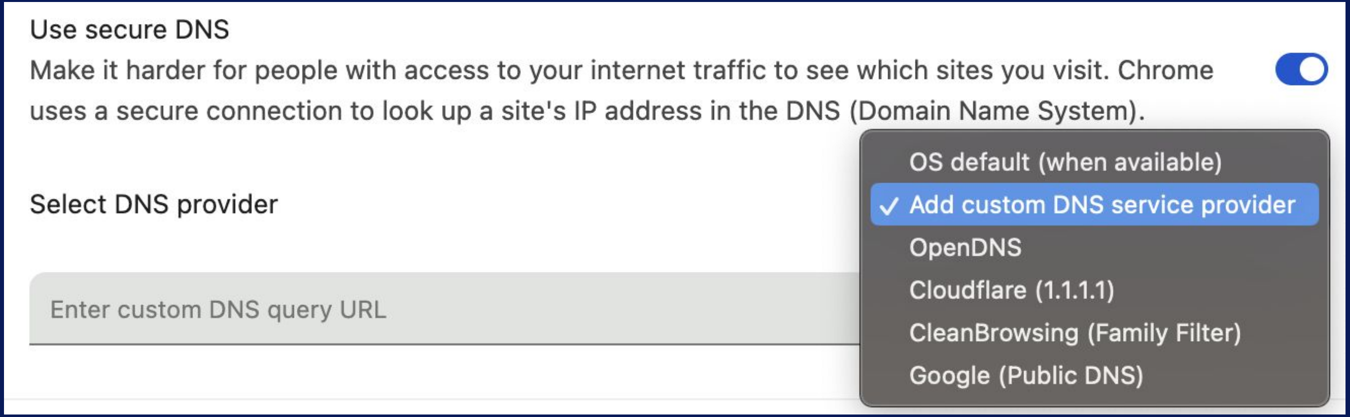
Commonly (ab)used record types

Record Type	Description
A	Stores an IPv4 address
AAAA	Stores an IPv6 address
MX	Mail exchanger
CNAME	An alias for another domain name
TXT	Stores a text string

```
;; QUESTION SECTION:
;_acme-challenge.example.com.  IN      TXT
;; ANSWER SECTION:
_acme-challenge.example.com. 3600 IN   TXT     "TglI7jzpo9O4q7VUkMAutwBuBAjhPStwy_0GbICVKWY"
```

DNS over HTTPS (DoH)

- Enabled in modern browsers



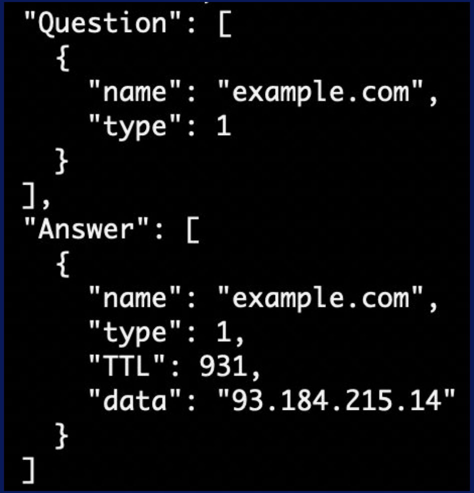
Use secure DNS

Make it harder for people with access to your internet traffic to see which sites you visit. Chrome uses a secure connection to look up a site's IP address in the DNS (Domain Name System).

Select DNS provider

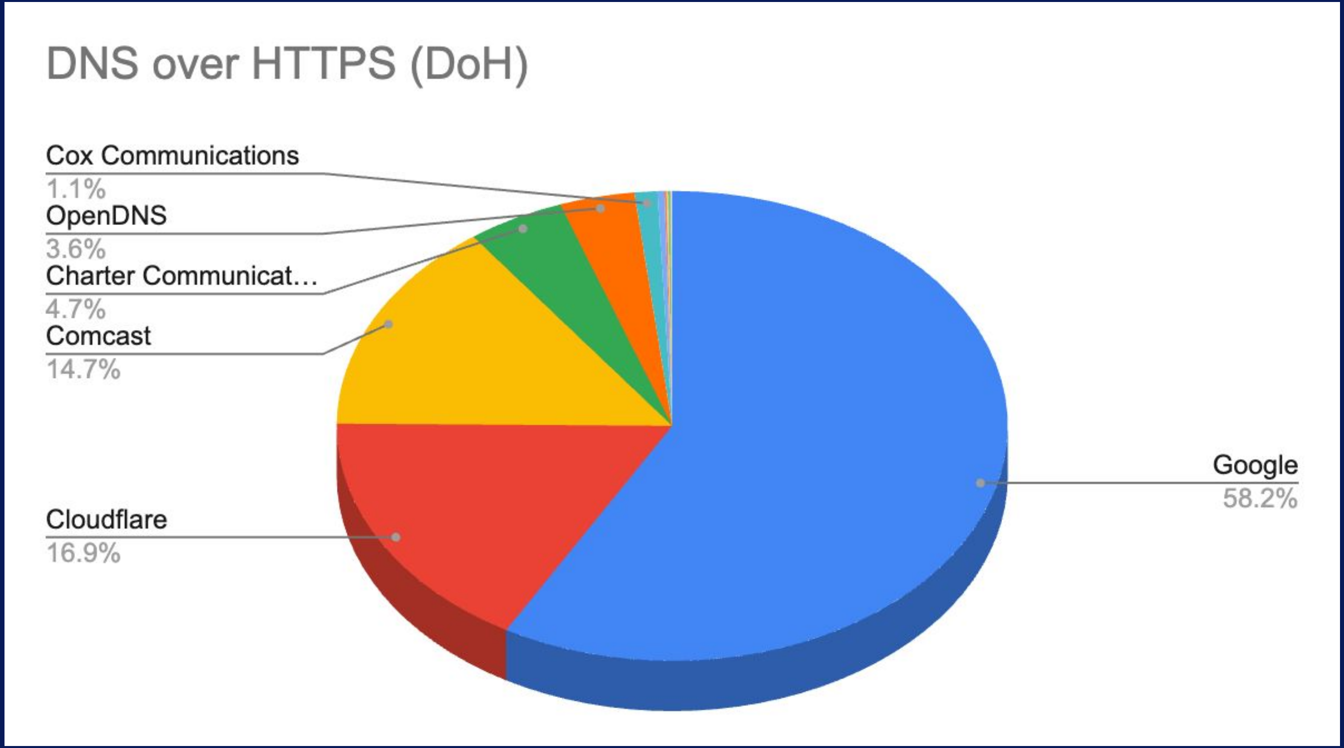
Enter custom DNS query URL

OS default (when available)
✓ Add custom DNS service provider
OpenDNS
Cloudflare (1.1.1.1)
CleanBrowsing (Family Filter)
Google (Public DNS)

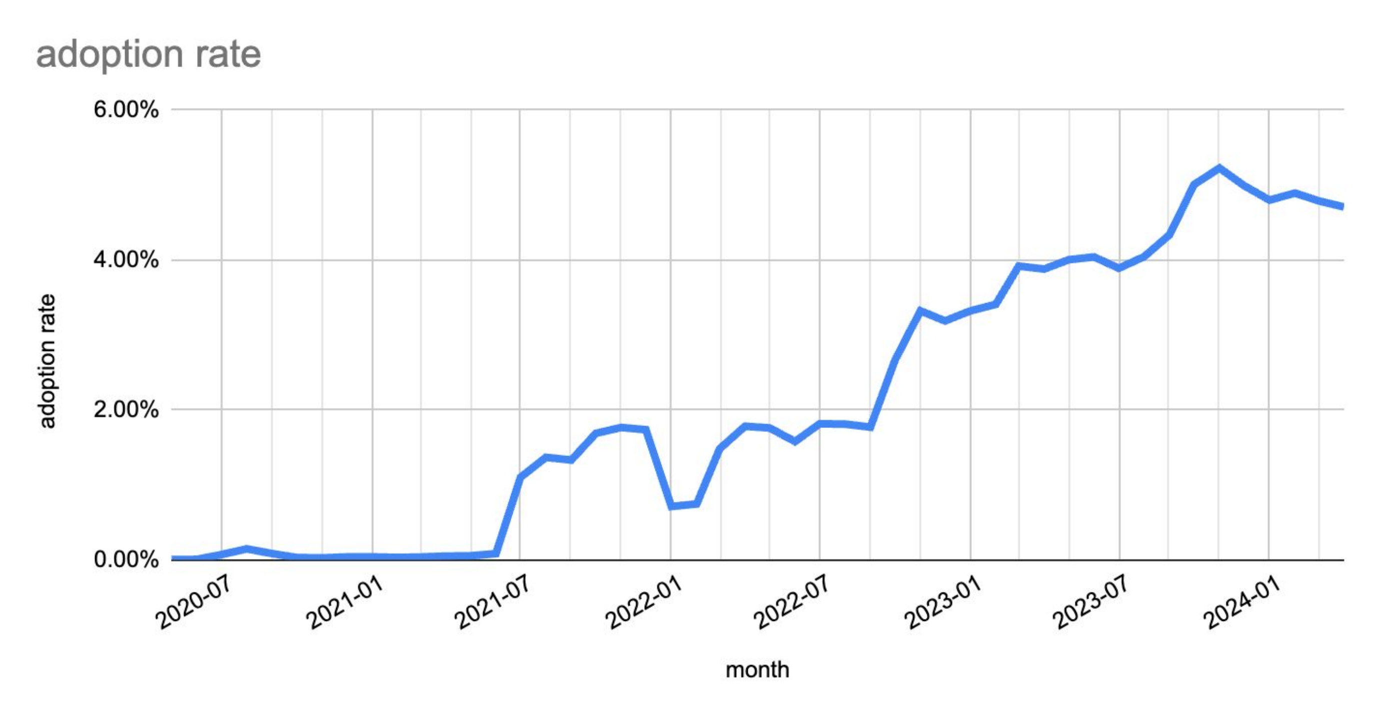


```
"Question": [
  {
    "name": "example.com",
    "type": 1
  }
],
"Answer": [
  {
    "name": "example.com",
    "type": 1,
    "TTL": 931,
    "data": "93.184.215.14"
  }
]
```

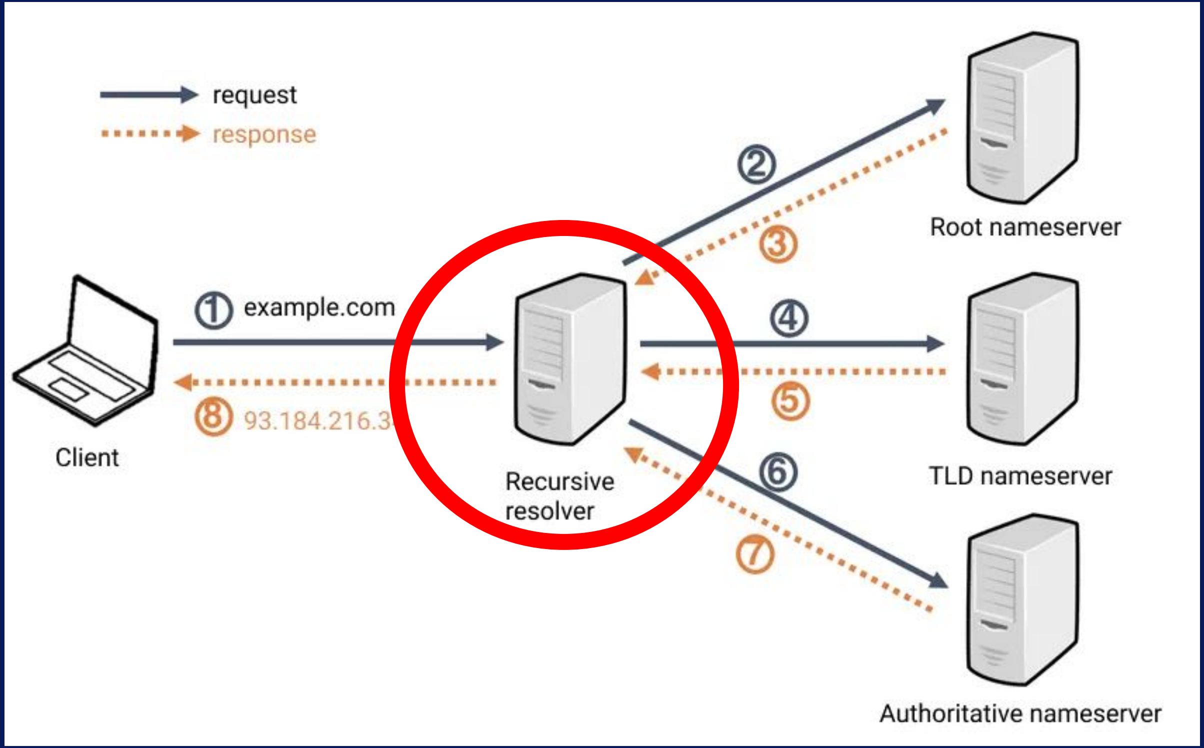
DoH Providers Distribution



DoH Adoption

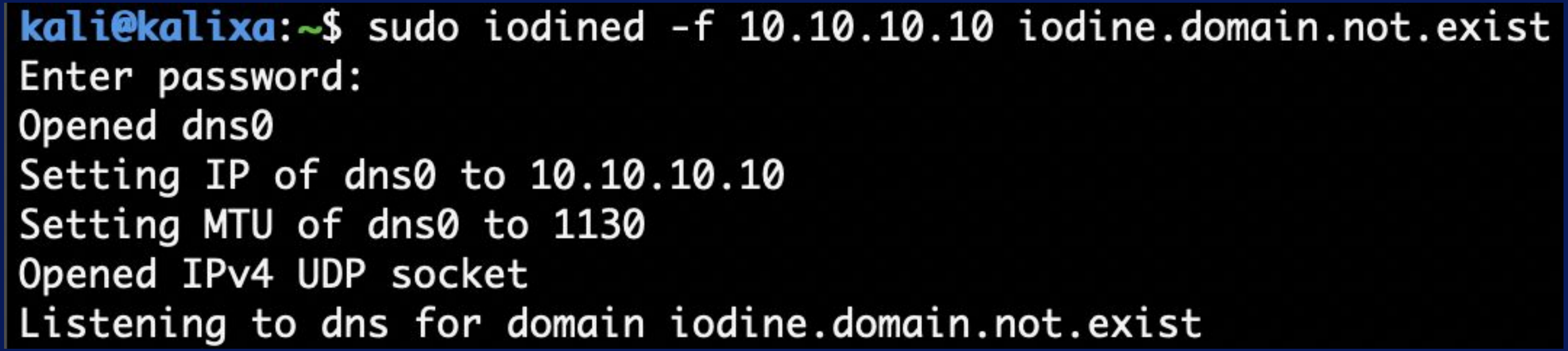


Tunneling over DNS


request
response
Root nameserver
②
③
① example.com
Recursive resolver
④
⑤
TLD nameserver
Client
⑧ 93.184.216.3
⑥
⑦
Authoritative nameserver

Iodine - server

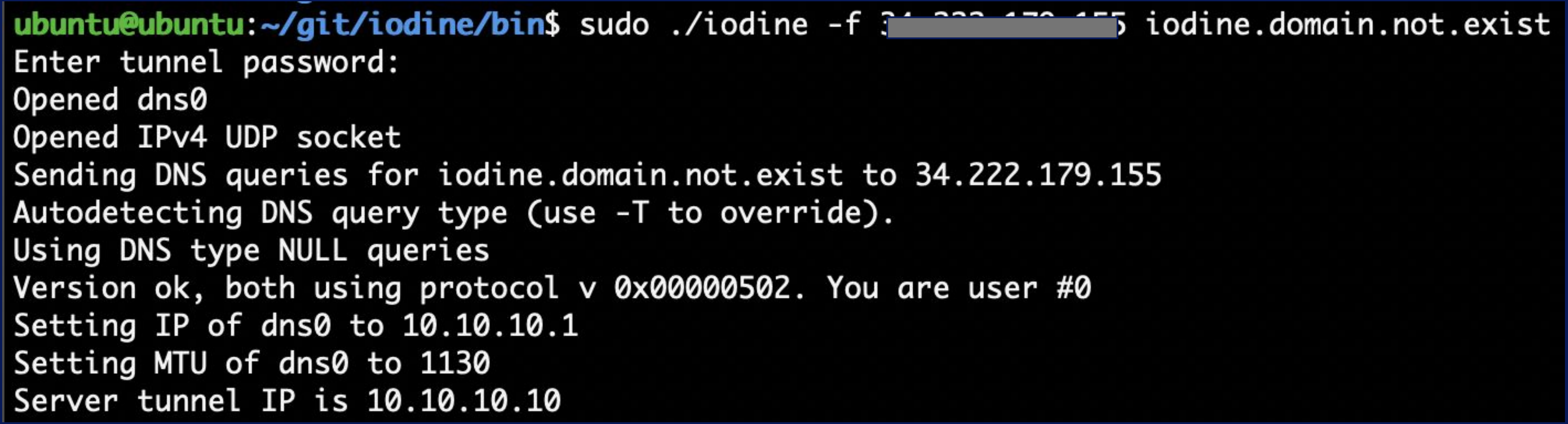
- Tunnelling of IPv4 data through a DNS server



```
kali@kalixa:~$ sudo iodined -f 10.10.10.10 iodine.domain.not.exist
Enter password:
Opened dns0
Setting IP of dns0 to 10.10.10.10
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Listening to dns for domain iodine.domain.not.exist
```

Iodine - client

- Tunnelling of IPv4 data through a DNS server

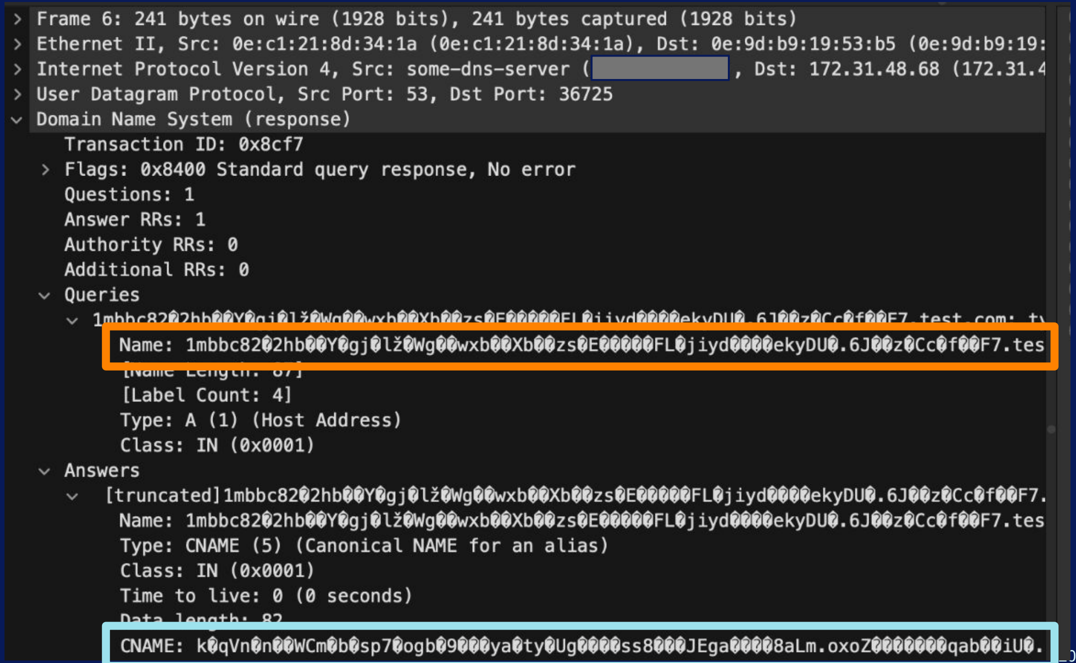


```
ubuntu@ubuntu:~/git/iodine/bin$ sudo ./iodine -f [redacted] iodine.domain.not.exist
Enter tunnel password:
Opened dns0
Opened IPv4 UDP socket
Sending DNS queries for iodine.domain.not.exist to 34.222.179.155
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of dns0 to 10.10.10.1
Setting MTU of dns0 to 1130
Server tunnel IP is 10.10.10.10
```

$ wget 10.10.10.10/secret.txt

Iodine

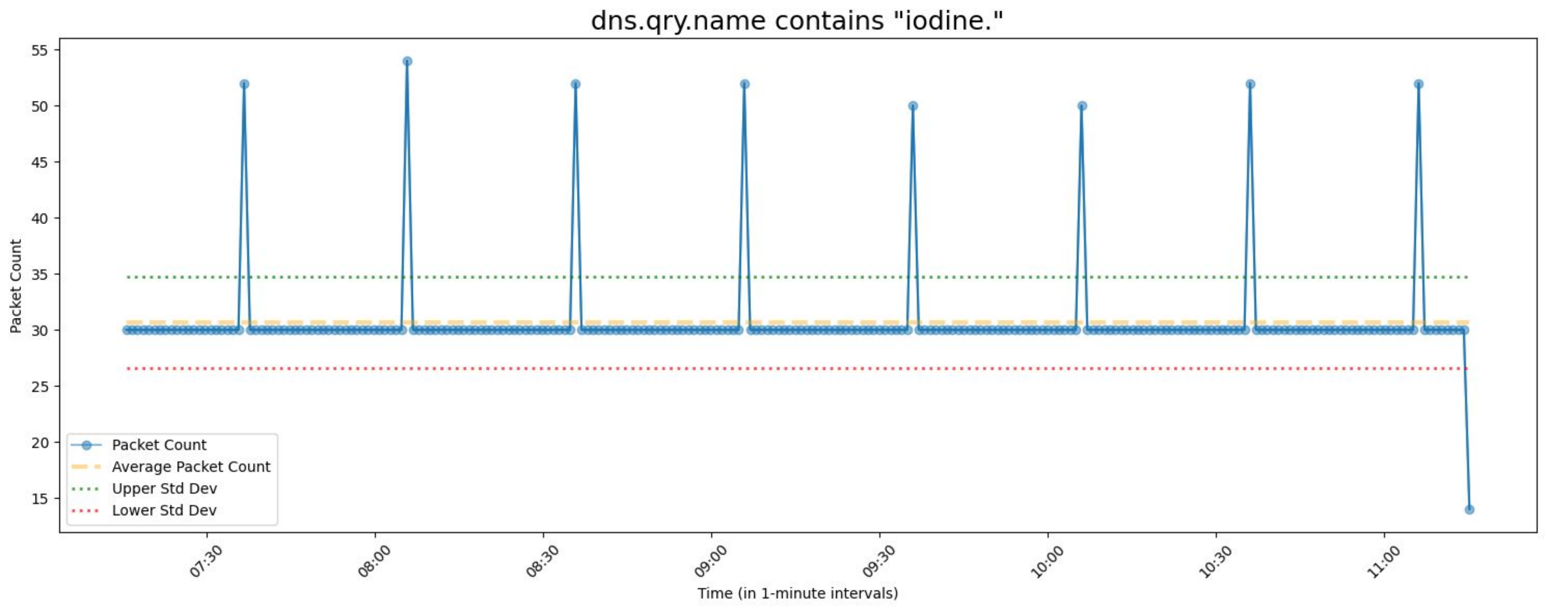
- DNS type supported: NULL, PRIVATE, TXT, SRV, MX, CNAME, A



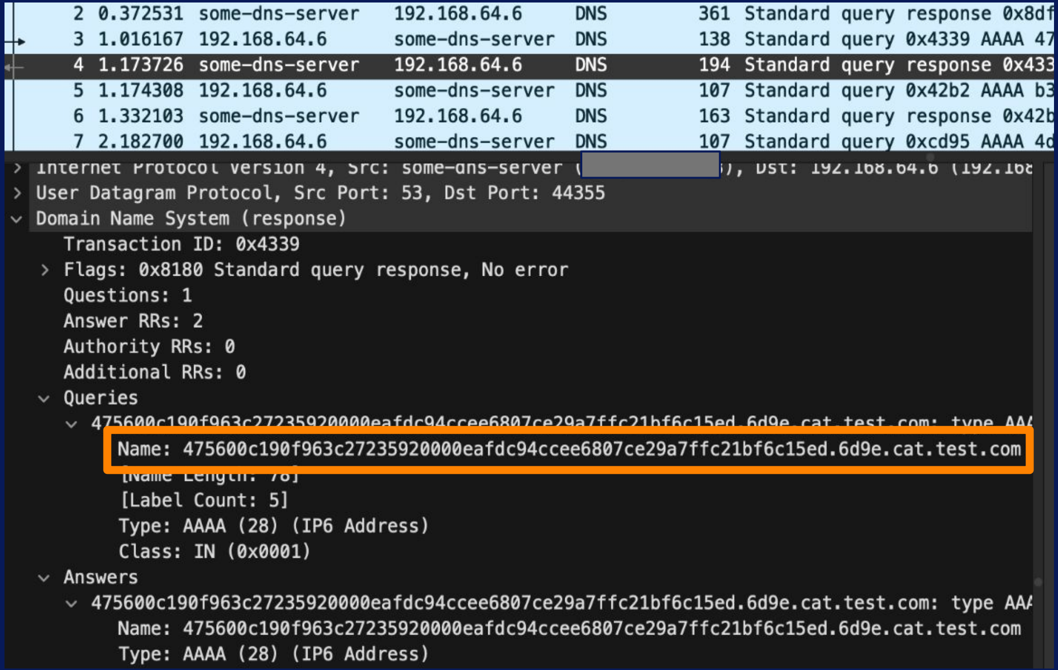
```
> Frame 6: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits)
> Ethernet II, Src: 0e:c1:21:8d:34:1a (0e:c1:21:8d:34:1a), Dst: 0e:9d:b9:19:53:b5 (0e:9d:b9:19:
> Internet Protocol Version 4, Src: some-dns-server ([redacted], Dst: 172.31.48.68 (172.31.4
> User Datagram Protocol, Src Port: 53, Dst Port: 36725
v Domain Name System (response)
    Transaction ID: 0x8cf7
  > Flags: 0x8400 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 1mbbc82�2hb��Y�gj�lž�Wg��wxb��Xb��zs�E�����FL�jiyd����ekyDU�.6J��z�Cc�f��F7.test.com: ty
        Name: 1mbbc82�2hb��Y�gj�lž�Wg��wxb��Xb��zs�E�����FL�jiyd����ekyDU�.6J��z�Cc�f��F7.tes
        [Name Length: 87]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  v Answers
    v [truncated]1mbbc82�2hb��Y�gj�lž�Wg��wxb��Xb��zs�E�����FL�jiyd����ekyDU�.6J��z�Cc�f��F7.
        Name: 1mbbc82�2hb��Y�gj�lž�Wg��wxb��Xb��zs�E�����FL�jiyd����ekyDU�.6J��z�Cc�f��F7.tes
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 0 (0 seconds)
        Data length: 82
        CNAME: k�qVn�n��WCm�b�sp7�ogb�9���ya�ty�Ug����ss8���JEga����8aLm.oxoZ�������qab��iU�.
```

Iodine

- Downstream encoding: Base32, Base64, Base64u, Base128, or (only for TXT:) Raw (default: autodetect)

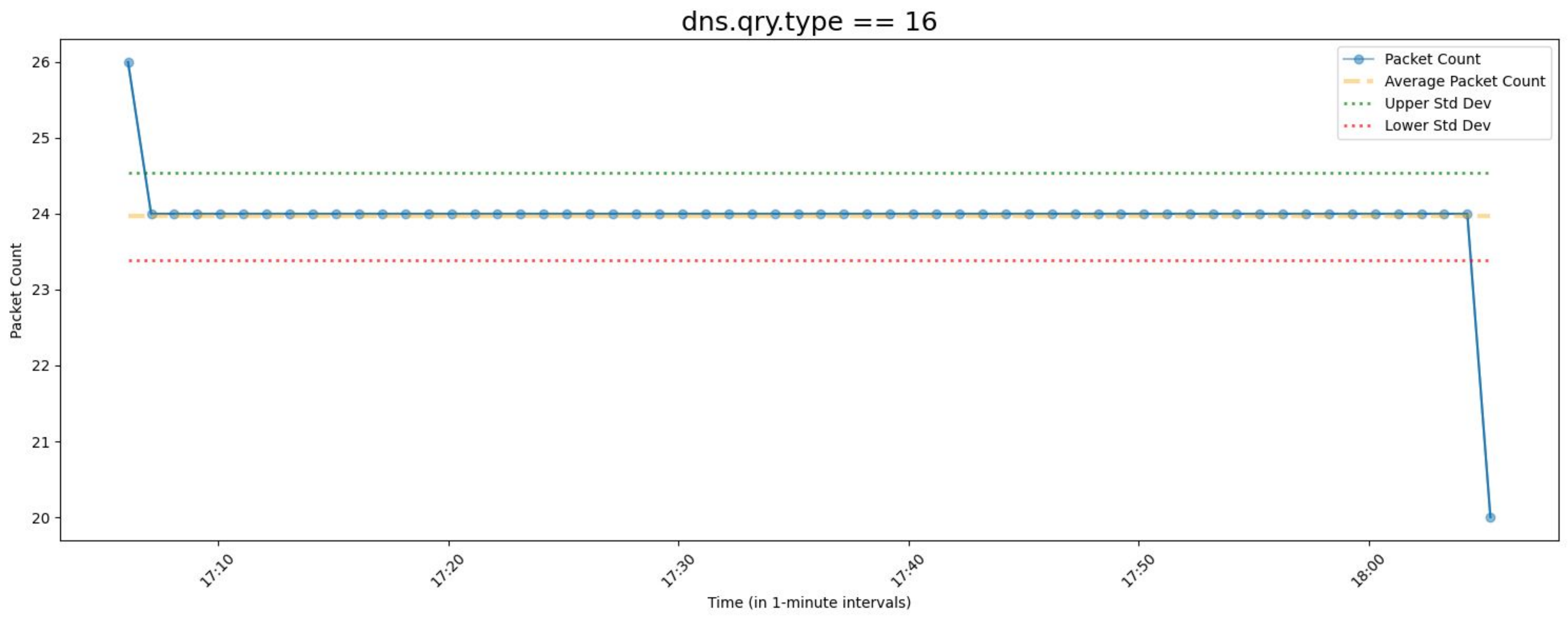


dnscat2

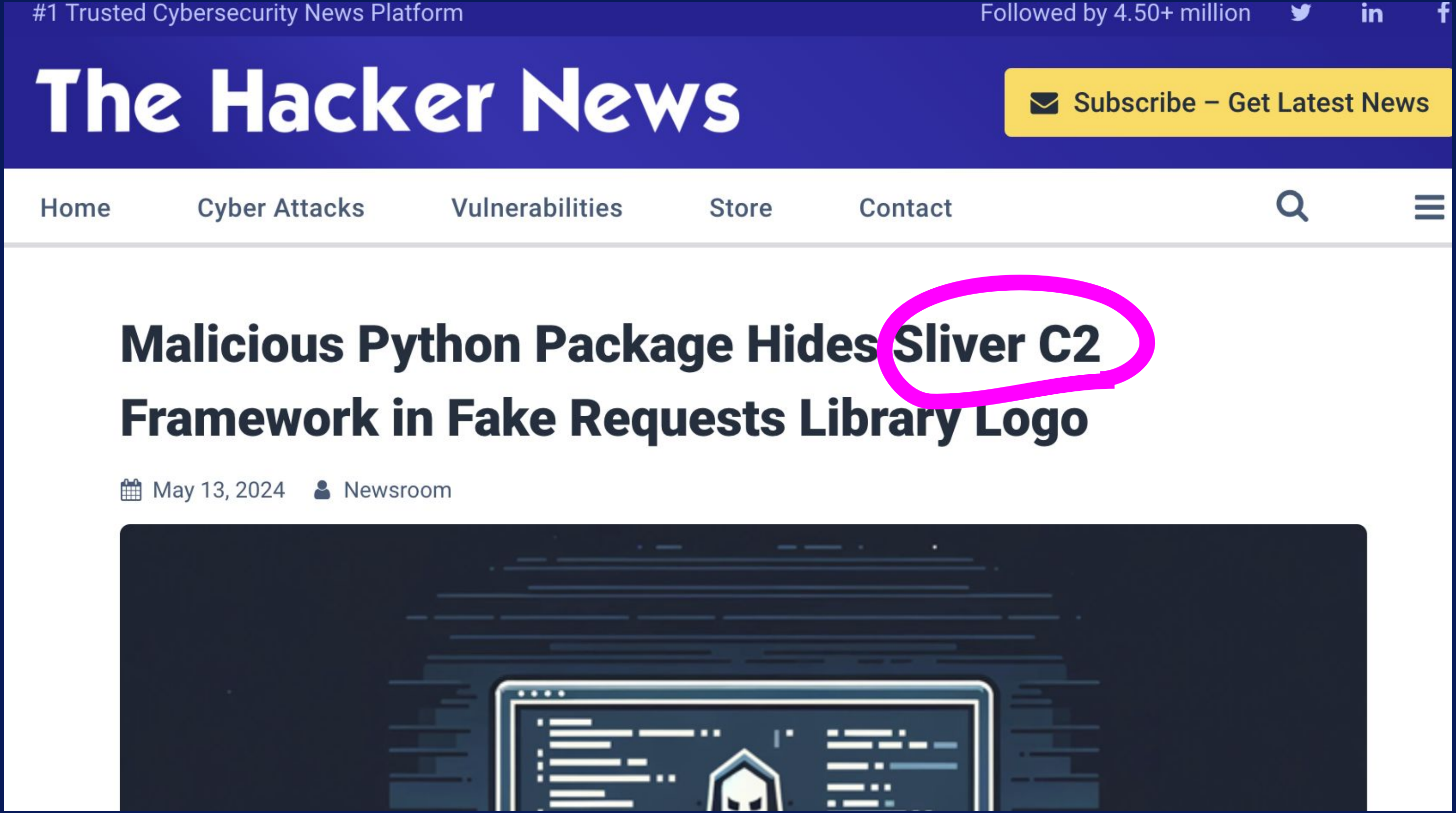


```
  2 0.372531  some-dns-server   192.168.64.6      DNS        361 Standard query response 0x8df
  3 1.016167  192.168.64.6      some-dns-server   DNS        138 Standard query 0x4339 AAAA 47
  4 1.173726  some-dns-server   192.168.64.6      DNS        194 Standard query response 0x433
  5 1.174308  192.168.64.6      some-dns-server   DNS        107 Standard query 0x42b2 AAAA b3
  6 1.332103  some-dns-server   192.168.64.6      DNS        163 Standard query response 0x42b
  7 2.182700  192.168.64.6      some-dns-server   DNS        107 Standard query 0xcd95 AAAA 4d
> Internet Protocol Version 4, Src: some-dns-server ([redacted]), Dst: 192.168.64.6 (192.168
> User Datagram Protocol, Src Port: 53, Dst Port: 44355
v Domain Name System (response)
     Transaction ID: 0x4339
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 2
     Authority RRs: 0
     Additional RRs: 0
   v Queries
     v 475600c190f963c27235920000eafdc94ccee6807ce29a7ffc21bf6c15ed.6d9e.cat.test.com: type AAA
         Name: 475600c190f963c27235920000eafdc94ccee6807ce29a7ffc21bf6c15ed.6d9e.cat.test.com
         [Name Length: 78]
         [Label Count: 5]
         Type: AAAA (28) (IP6 Address)
         Class: IN (0x0001)
   v Answers
     v 475600c190f963c27235920000eafdc94ccee6807ce29a7ffc21bf6c15ed.6d9e.cat.test.com: type AAA
         Name: 475600c190f963c27235920000eafdc94ccee6807ce29a7ffc21bf6c15ed.6d9e.cat.test.com
         Type: AAAA (28) (IP6 Address)
```

Periodic rare query type (TXT)



C2 over DNS


#1 Trusted Cybersecurity News Platform
Followed by 4.50+ million
The Hacker News
Subscribe – Get Latest News
Home
Cyber Attacks
Vulnerabilities
Store
Contact

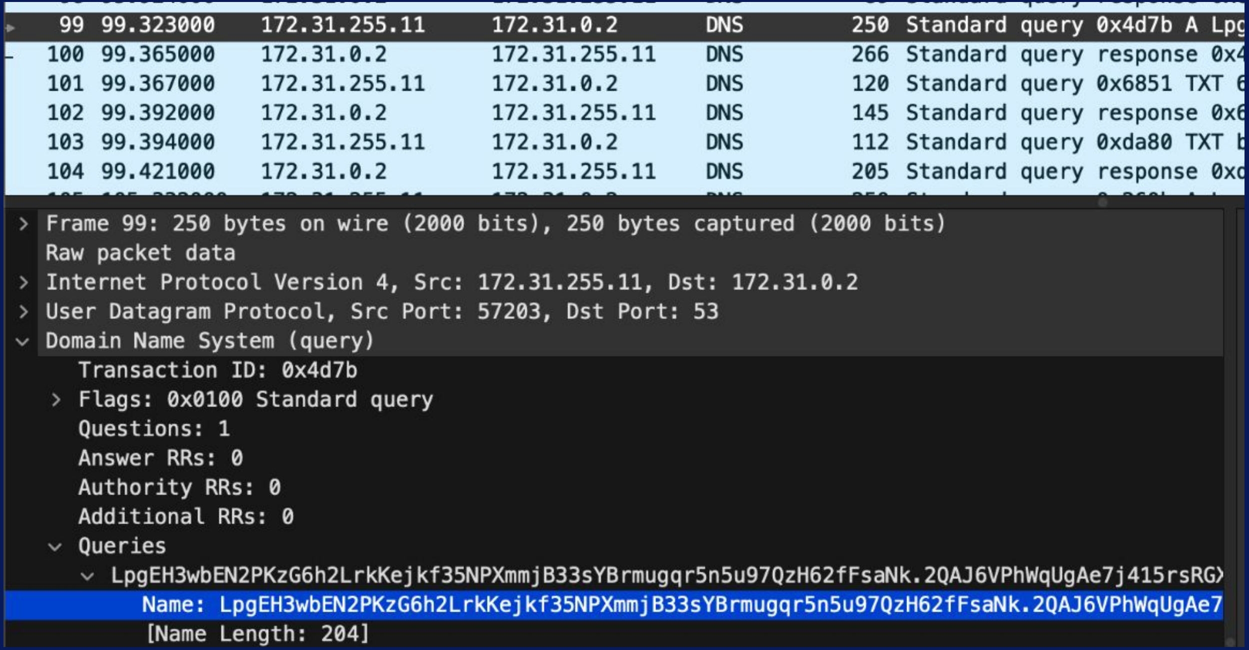
Malicious Python Package Hides Sliver C2 Framework in Fake Requests Library Logo

May 13, 2024 Newsroom

https://thehackernews.com/2024/05/malicious-python-package-hides-sliver.html

Sliver

- Other than Cobalt Strike, gaining popularity among threat actors

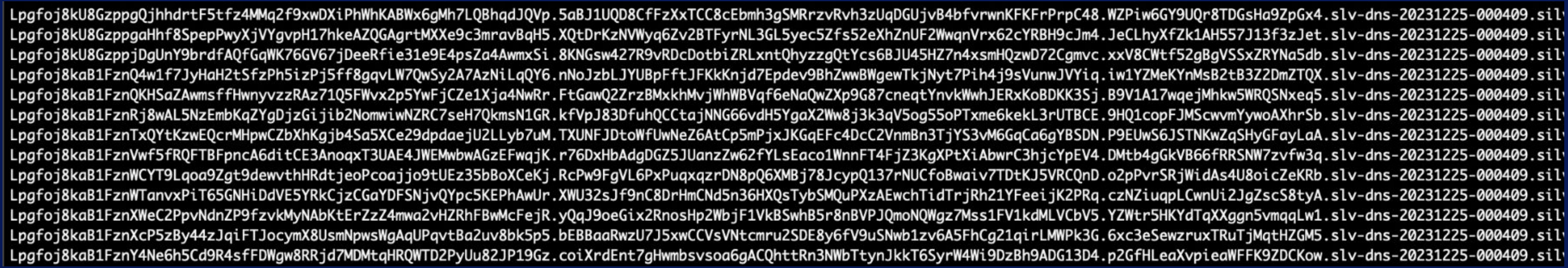


```
 99  99.323000    172.31.255.11    172.31.0.2       DNS         250 Standard query 0x4d7b A Lpg
100  99.365000    172.31.0.2       172.31.255.11    DNS         266 Standard query response 0x4
101  99.367000    172.31.255.11    172.31.0.2       DNS         120 Standard query 0x6851 TXT 6
102  99.392000    172.31.0.2       172.31.255.11    DNS         145 Standard query response 0x6
103  99.394000    172.31.255.11    172.31.0.2       DNS         112 Standard query 0xda80 TXT b
104  99.421000    172.31.0.2       172.31.255.11    DNS         205 Standard query response 0xd
```

```
> Frame 99: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 172.31.255.11, Dst: 172.31.0.2
> User Datagram Protocol, Src Port: 57203, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x4d7b
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v LpgEH3wbEN2PKzG6h2LrkKejkf35NPXmmjB33sYBrmugqr5n5u97QzH62fFsaNk.2QAJ6VPhWqUgAe7j415rsRGX
        Name: LpgEH3wbEN2PKzG6h2LrkKejkf35NPXmmjB33sYBrmugqr5n5u97QzH62fFsaNk.2QAJ6VPhWqUgAe7
        [Name Length: 204]
```

Long domain length in Sliver’s DNS C2 beacons

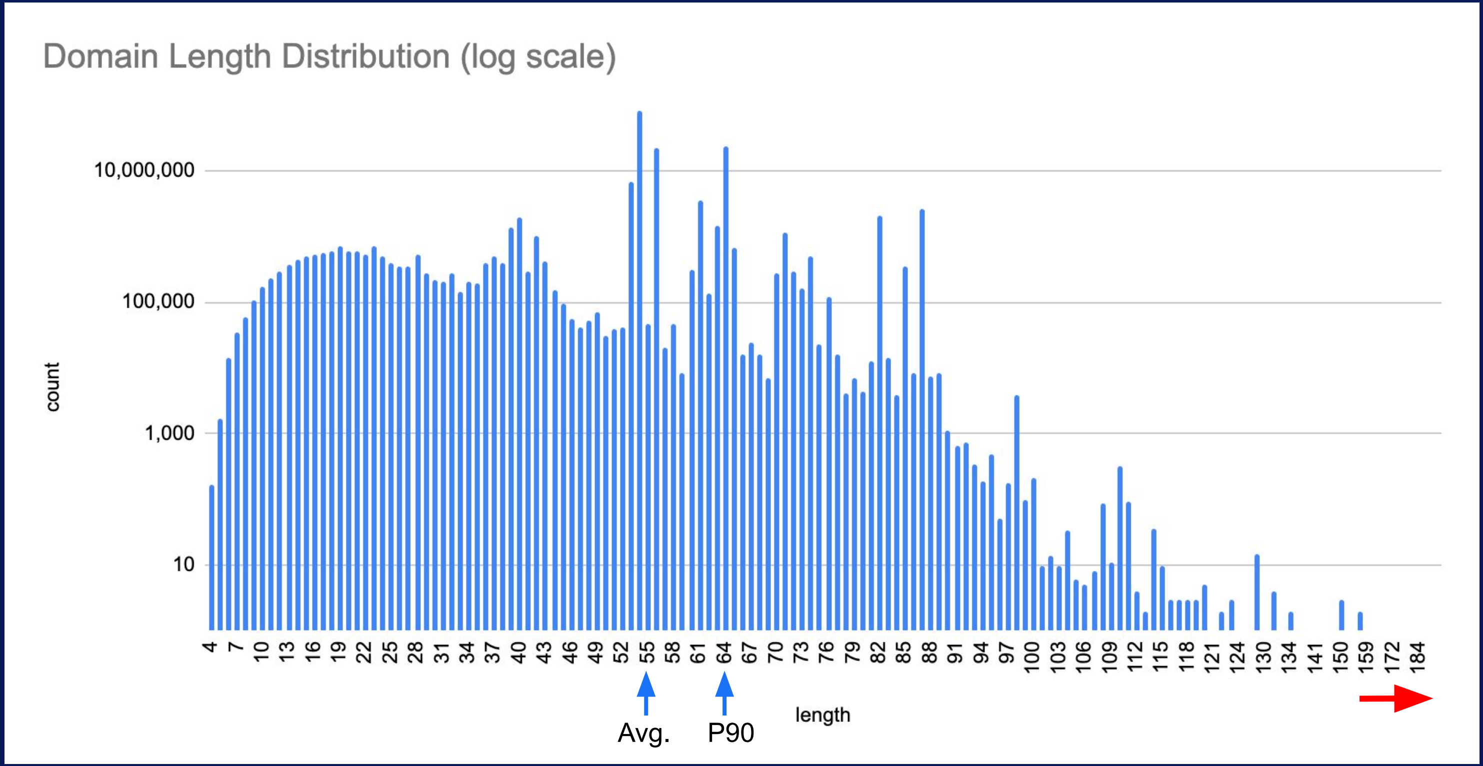
63 bytes 63 bytes 27 bytes



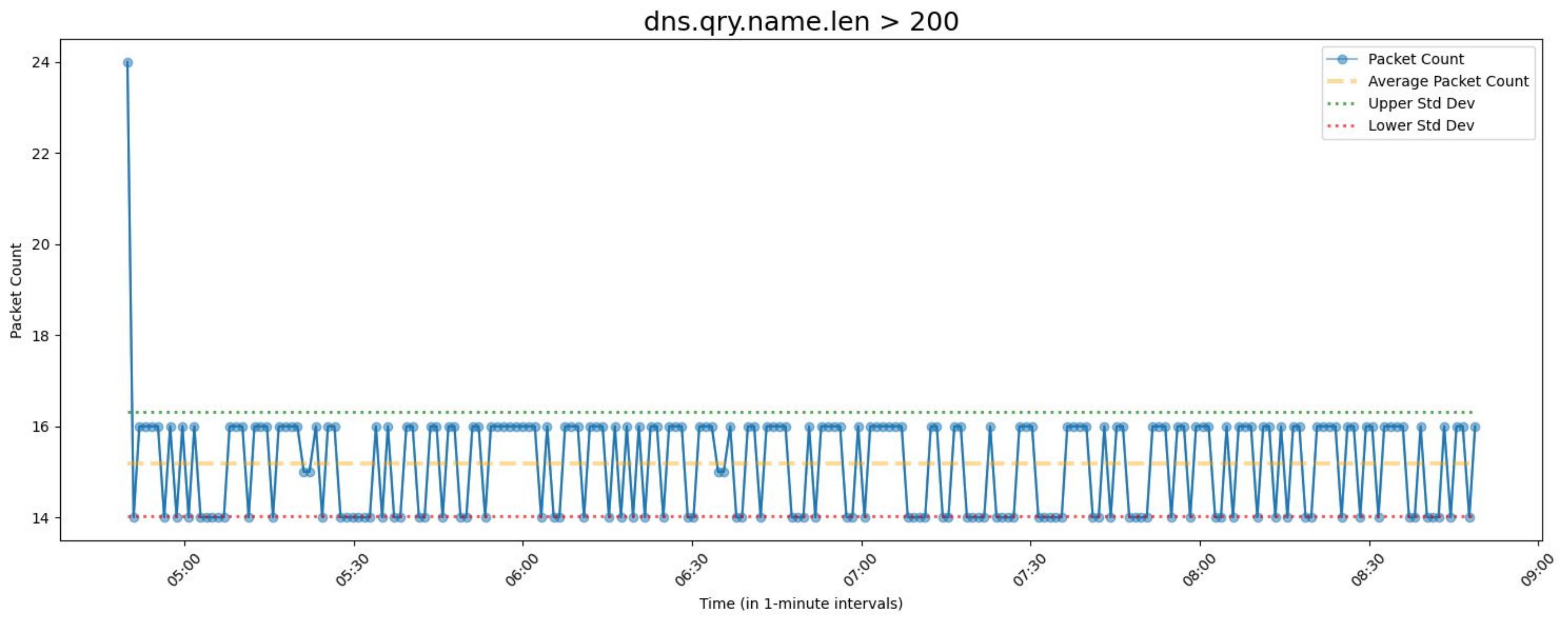
```
Lpgfoj8kU8GzppgQjhhdrtF5tfz4MMq2f9xwDXiPhWhKABWx6gMh7LQBhqdJQVp.5aBJ1UQD8CfFzXxTCC8cEbmh3gSMRrzvRvh3zUqDGUjvB4bfvrwnKFKFrPrpC48.WZPiw6GY9UQr8TDGsHa9ZpGx4.slv-dns-20231225-000409.sil
Lpgfoj8kU8GzppgaHhf8SpepPwyXjVYgvpH17hkeAZQGAgrtMXXe9c3mravBqH5.XQtDrKzNVWyq6Zv2BTFyrNL3GL5yec5Zfs52eXhZnUF2WwqnVrx62cYRBH9cJm4.JeCLhyXfZk1AH557J13f3zJet.slv-dns-20231225-000409.sil
Lpgfoj8kU8GzppjDgUnY9brdfAQfGqWK76GV67jDeeRfie31e9E4psZa4AwmxSi.8KNGsw427R9vRDcDotbiZRLxntQhyzzgQtYcs6BJU45HZ7n4xsmHQzwD72Cgmvc.xxV8CWtf52gBgVSSxZRYNa5db.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznQ4w1f7JyHaH2tSfzPh5izPj5ff8gqvLW7QwSy2A7AzNiLqQY6.nNoJzbLJYUBpFftJFKkKnjd7Epdev9BhZwwBWgewTkjNyt7Pih4j9sVunwJVYiq.iw1YZMeKYnMsB2tB3Z2DmZTQX.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznQKHSaZAwmsffHwnyvzzRAz71Q5FWvx2p5YwFjCZe1Xja4NwRr.FtGawQ2ZrzBMxkhMvjWhWBVqf6eNaQwZXp9G87cneqtYnvkWwhJERxKoBDKK3Sj.B9V1A17wqejMhkw5WRQSNxeq5.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznRj8wAL5NzEmbKqZYgDjzGijib2NomwiwNZRC7seH7QkmsN1GR.kfVpJ83DfuhQCCtajNNG66vdH5YgaX2Ww8j3k3qV5og55oPTxme6kekL3rUTBCE.9HQ1copFJMScwvmYywoAXhrSb.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznTxQYtKzwEQcrMHpwCZbXhKgjb4Sa5XCe29dpdaejU2LLyb7uM.TXUNFJDtoWfUwNeZ6AtCp5mPjxJKGqEFc4DcC2VnmBn3TjYS3vM6GqCa6gYBSDN.P9EUwS6JSTNKwZqSHyGFayLaA.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznVwf5fRQFTBFpncA6ditCE3AnoqxT3UAE4JWEMwbwAGzEFwqjK.r76DxHbAdgDGZ5JUanzZw62fYLsEaco1WnnFT4FjZ3KgXPtXiAbwrC3hjcYpEV4.DMtb4gGkVB66fRRSNW7zvfw3q.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznWCYT9Lqoa9Zgt9dewvthHRdtjeoPcoajjo9tUEz35bBoXCeKj.RcPw9FgVL6PxPuqxqzrDN8pQ6XMBj78JcypQ137rNUCfoBwaiv7TDtKJ5VRCQnD.o2pPvrSRjWidAs4U8oicZeKRb.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznWTanvxPiT65GNHiDdVE5YRkCjzCGaYDFSNjvQYpc5KEPhAwUr.XWU32sJf9nC8DrHmCNd5n36HXQsTybSMQuPXzAEwchTidTrjRh21YFeeijK2PRq.czNZiuqpLCwnUi2JgZscS8tyA.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznXWeC2PpvNdnZP9fzvkMyNAbKtErZzZ4mwa2vHZRhFBwMcFejR.yQqJ9oeGix2RnosHp2WbjF1VkBSwhB5r8nBVPJQmoNQWgz7Mss1FV1kdMLVCbV5.YZWtr5HKYdTqXXggn5vmqqLw1.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznXcP5zBy44zJqiFTJocymX8UsmNpwsWgAqUPqvtBa2uv8bk5p5.bEBBaaRwzU7J5xwCCVsVNtcmru2SDE8y6fV9uSNwb1zv6A5FhCg21qirLMWPk3G.6xc3eSewzruxTRuTjMqtHZGM5.slv-dns-20231225-000409.sil
Lpgfoj8kaB1FznY4Ne6h5Cd9R4sfFDWgw8RRjd7MDMtqHRQWTD2PyUu82JP19Gz.coiXrdEnt7gHwmbsvsoa6gACQhttRn3NWbTtynJkkT6SyrW4Wi9DzBh9ADG13D4.p2GfHLeaXvpieaWFFK9ZDCKow.slv-dns-20231225-000409.sil
```

2024 © Netskope. All rights reserved.

Domain Length Distribution (log scale)

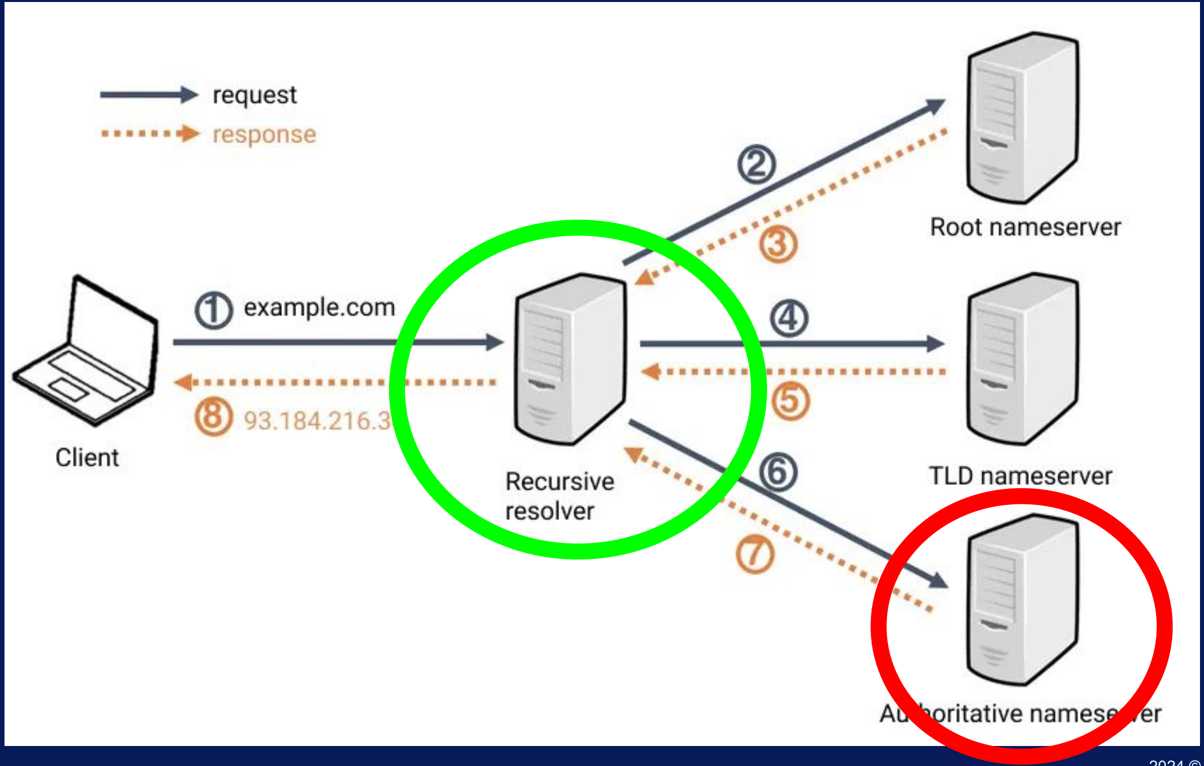


Abnormal query name length



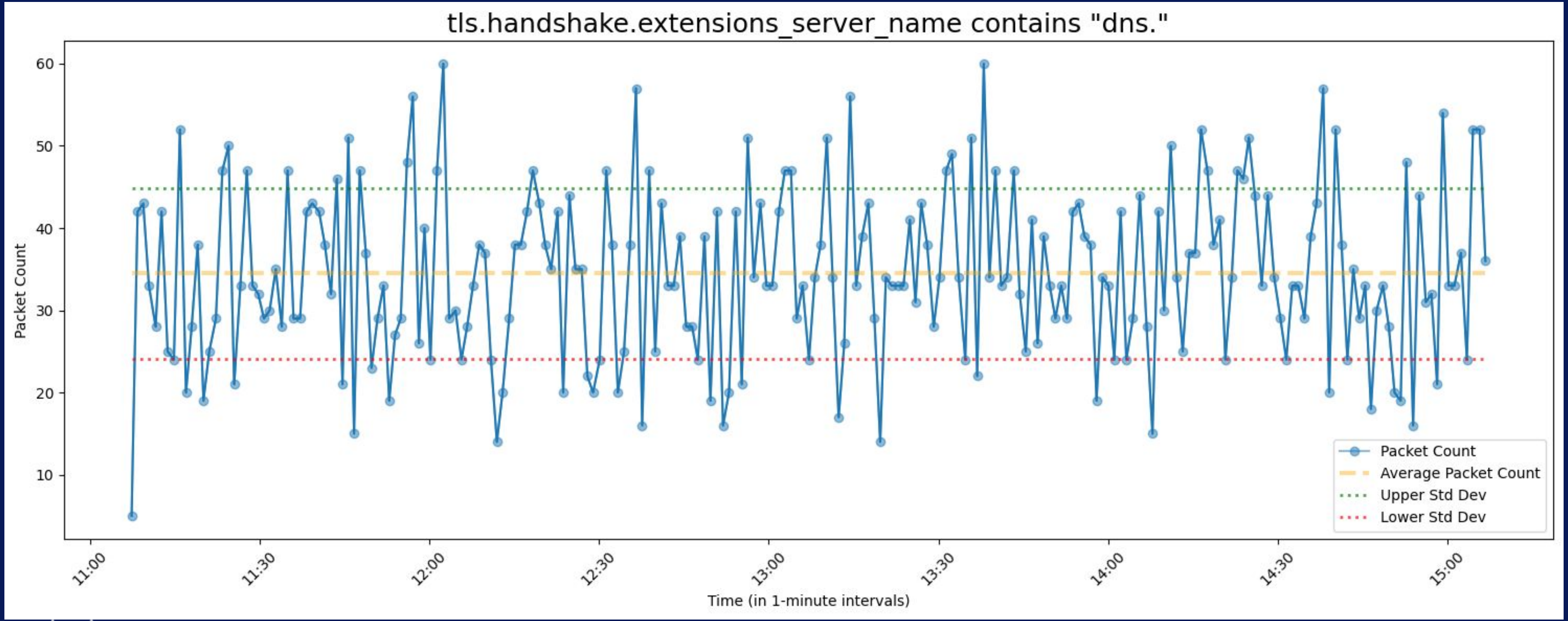
Brute Ratel C2 over DoH

- Commercial C2 framework



Brute Ratel C2 over DoH

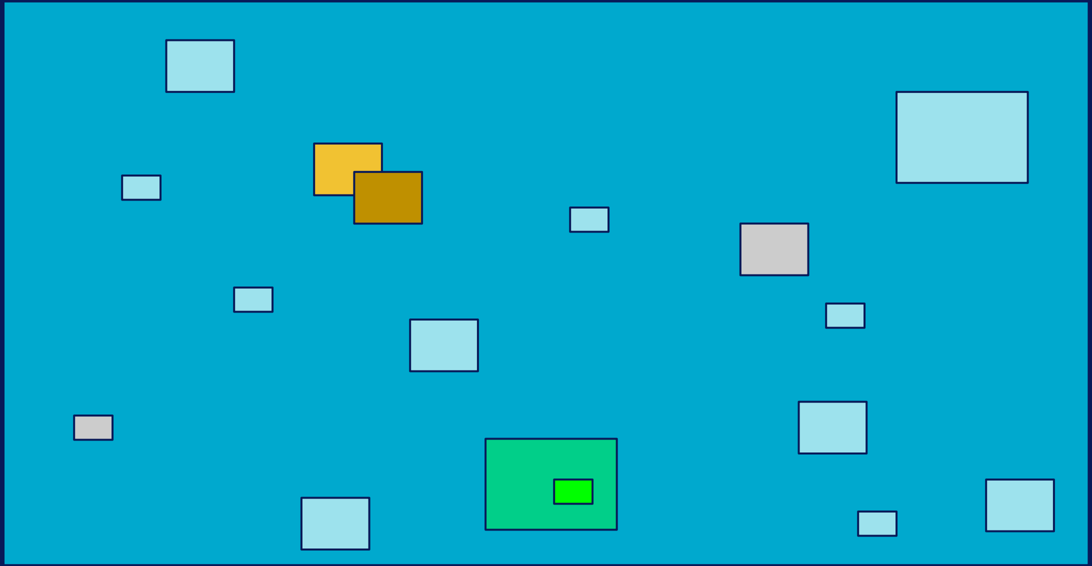
- cloudflare-dns.com
- dns.google
- doh.opendns.com



Countermeasures & Takeaways

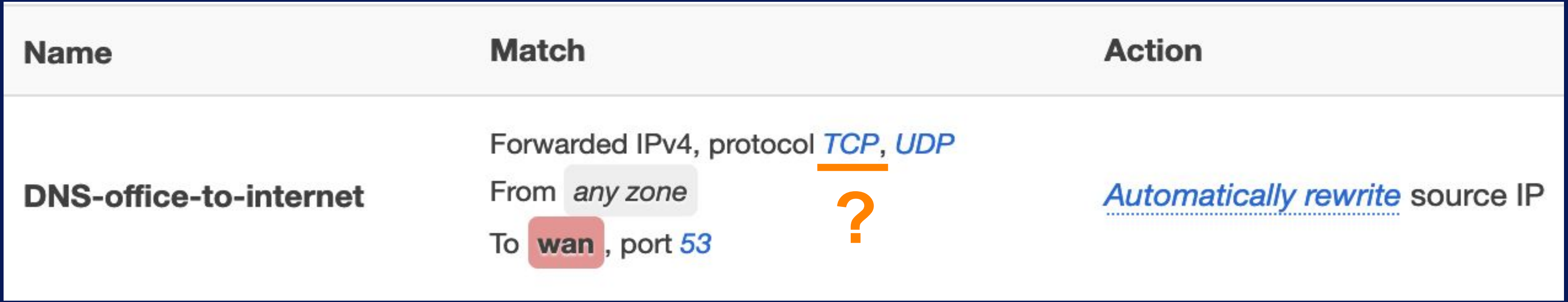
Mitigation

- Review of dormant firewall rules



Mitigation

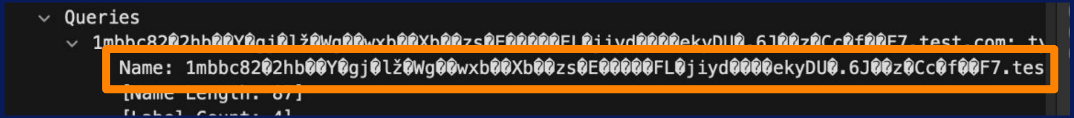
- Review of dormant firewall rules
- Restrict DNS access to a limited allowed list



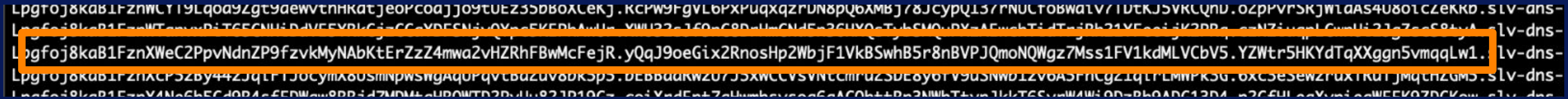
Name	Match	Action
DNS-office-to-internet	Forwarded IPv4, protocol *TCP*, *UDP* From *any zone* To **wan**, port *53*	*Automatically rewrite* source IP

Mitigation

- Review of dormant firewall rules
- Restrict DNS access to a limited allowed list
- Anomaly detection: charset, length, entropy, …



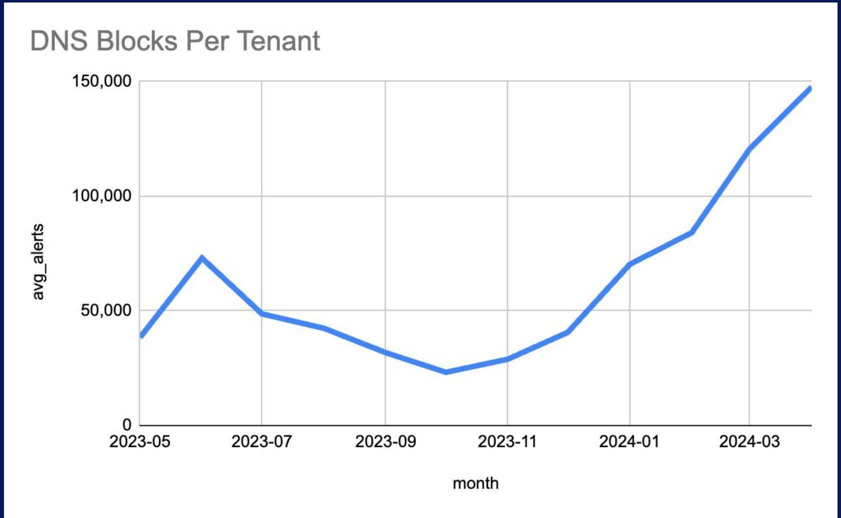
```
⌄ Queries
  ⌄ 1mbbc82�2hb��Y�gj�lž�Wg��wxb��Xb��zs�E�����FL�jiyd����ekyDU�.6J��z�Cc�f��F7.test.com: ty
      Name: 1mbbc82�2hb��Y�gj�lž�Wg��wxb��Xb��zs�E�����FL�jiyd����ekyDU�.6J��z�Cc�f��F7.tes
      [Name Length: 87]
      [Label Count: 4]
```



```
Lpgfoj8kaB1FznWCYT9Lqoa9Zgt9aeWvtnHKatjeoPcoajjo9tUEz35bBoXCeKj.KcPW9FgvL6PxPuqxqzrDN8pQ6XMBj78JcypQ137rNUCfoBWaiV7IDtKJ5VKCQnD.oZpPvrSKjWidAs4U8oiCZeKKb.slv-dns-
Lpgfoj8kaB1FznWTqnvxPjT65CNHjDdVF5XBkCjzCCaXDESNjvQXpc5KEPhAwUn.XWU33cJf9nC8DrHmCNdEn36HXQcTyhSMQuPXzAFwchTidTrjBh31XEocijK3PPq.ezNZiuqpLCwnUi3lgZacS8tyA.slv-dns-
Lpgfoj8kaB1FznXWeC2PpvNdnZP9fzvkMyNAbKtErZzZ4mwa2vHZRhFBwMcFejR.yQqJ9oeGix2RnosHp2WbjF1VkBSwhB5r8nBVPJQmoNQWgz7Mss1FV1kdMLVCbV5.YZWtr5HKYdTqXXggn5vmqqLw1.slv-dns-
Lpgfoj8kaB1FznXcP3ZBy44ZJqtFTJ0cymX8UsmNpwsWgAqUPqvtBuZuv8bkSp5.DEBBudRwZu7J5xWCCVsVNtcmruZ3DE8y6rV9uSNWb1Zv6A5FnCgZ1qtFLMWPk3G.6xC3eSew2ruxTRuTjMqtHZGM3.slv-dns-
Lpgfoj8kaB1FznY4NoGhECd9R4cfEDWqw8RBjdZMDMtqHROWTD2PvUu82JP19Gz.coiXrdEntZqHwmhsvseq6qACQhttRn3NWhTtvnJkkT6SvnW4Wj9DzBh9ADC13D4.n2CfHLoqXvnieqWFFK97DCKow.slv-dns-
```

Mitigation

- Review of dormant firewall rules
- Restrict DNS access to a limited allowed list
- Anomaly detection: charset, length, entropy, …
- Proxy DNS traffic for thorough security inspection, e.g., NRDs, NODs



netskope

THREAT LABS

@ CYBERSEC 2024
臺灣資安大會

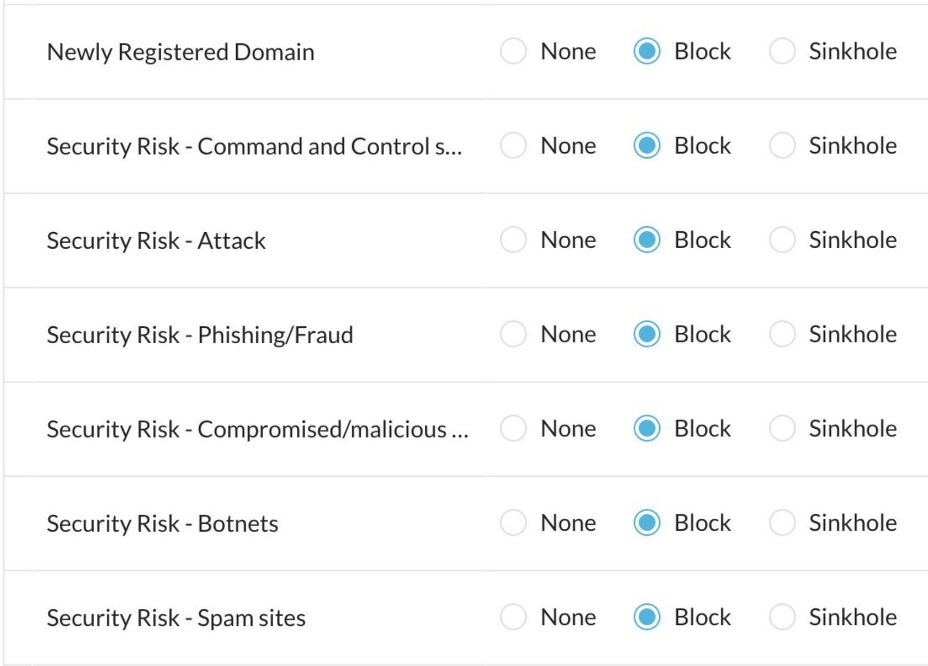
netskope.com/threat-labs

Hubert Lin
hlin@netskope.com

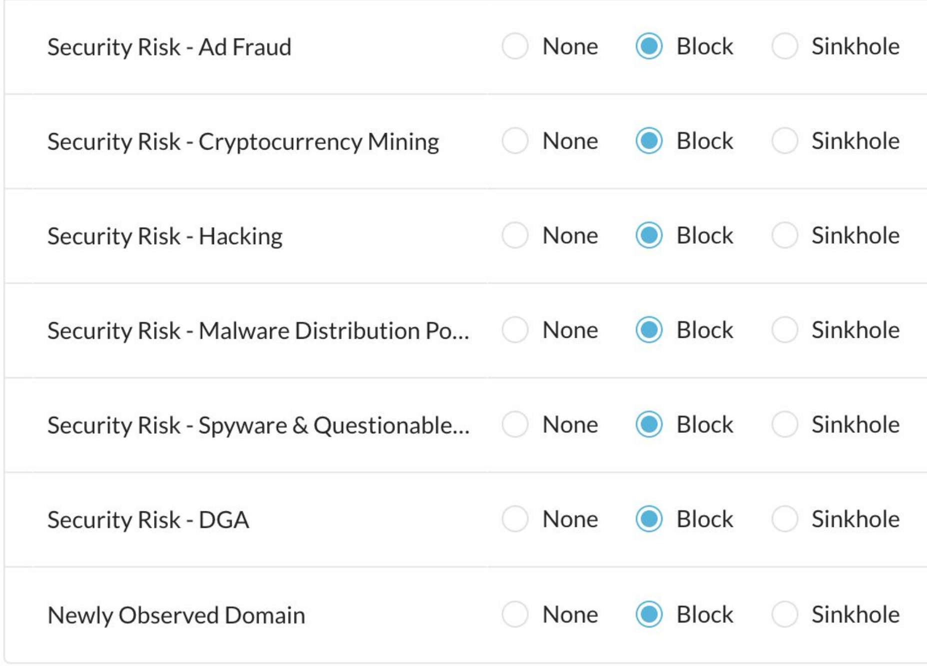
References

- https://datatracker.ietf.org/doc/html/rfc8484
- https://en.wikipedia.org/wiki/List_of_DNS_record_types
- https://github.com/yarrick/iodine
- https://github.com/iagox86/dnscat2
- https://github.com/BishopFox/sliver

DNS Profiles



Newly Registered Domain	○ None	● Block	○ Sinkhole
Security Risk - Command and Control s...	○ None	● Block	○ Sinkhole
Security Risk - Attack	○ None	● Block	○ Sinkhole
Security Risk - Phishing/Fraud	○ None	● Block	○ Sinkhole
Security Risk - Compromised/malicious ...	○ None	● Block	○ Sinkhole
Security Risk - Botnets	○ None	● Block	○ Sinkhole
Security Risk - Spam sites	○ None	● Block	○ Sinkhole



Security Risk - Ad Fraud	○ None	● Block	○ Sinkhole
Security Risk - Cryptocurrency Mining	○ None	● Block	○ Sinkhole
Security Risk - Hacking	○ None	● Block	○ Sinkhole
Security Risk - Malware Distribution Po...	○ None	● Block	○ Sinkhole
Security Risk - Spyware & Questionable...	○ None	● Block	○ Sinkhole
Security Risk - DGA	○ None	● Block	○ Sinkhole
Newly Observed Domain	○ None	● Block	○ Sinkhole