

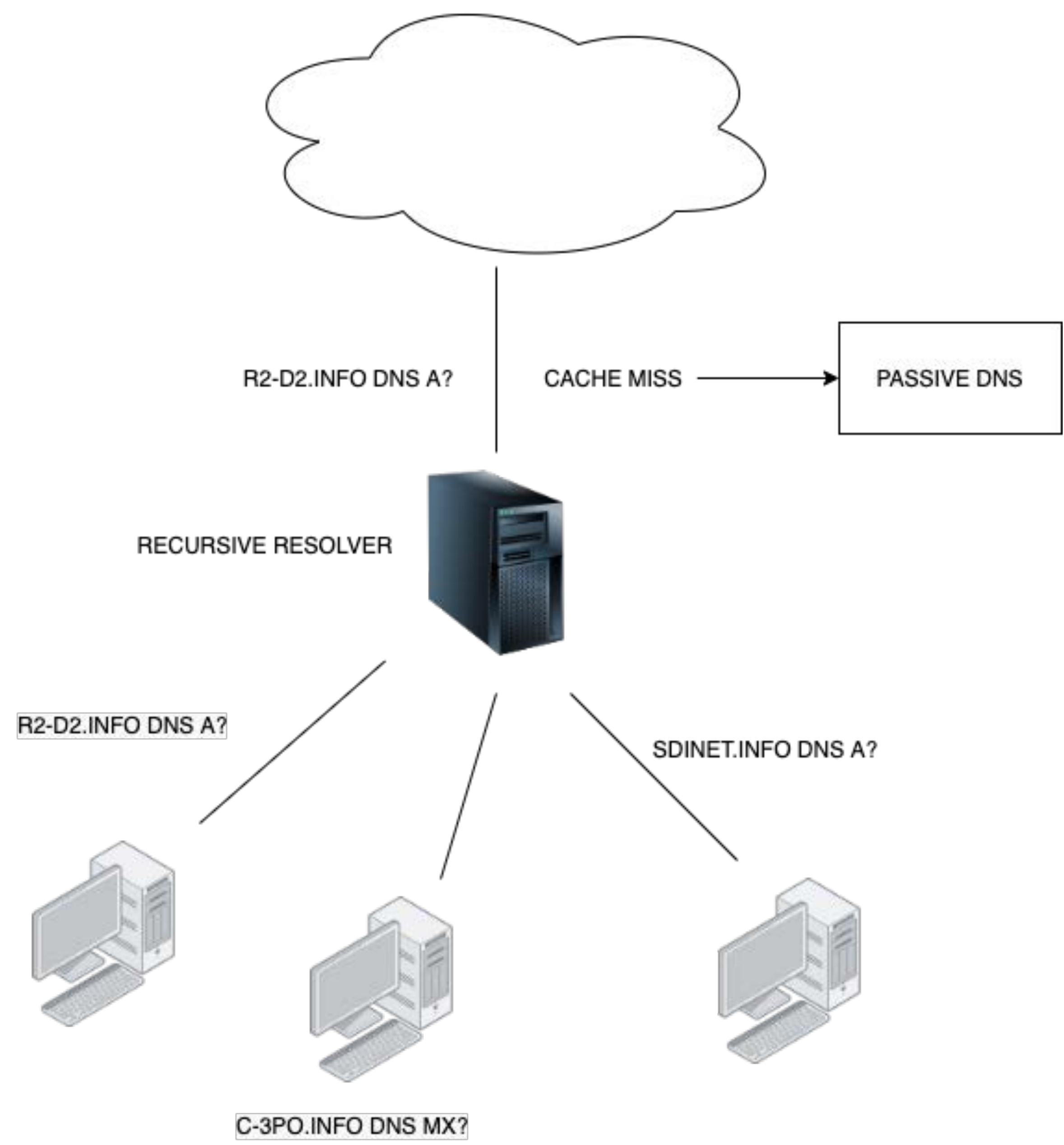
Uncovering badness using Passive DNS

Agenda

- What is Passive DNS ? Benefits of using passive DNS
- Who should be using Passive DNS ?
- Use cases
- Q&A

Passive DNS 101

- Passive DNS Replication - Florian Weimer paper at 17th [FIRST.org](#) 2005
- Collecting cache miss traffic using sensors
- DNS transactions into a simple format



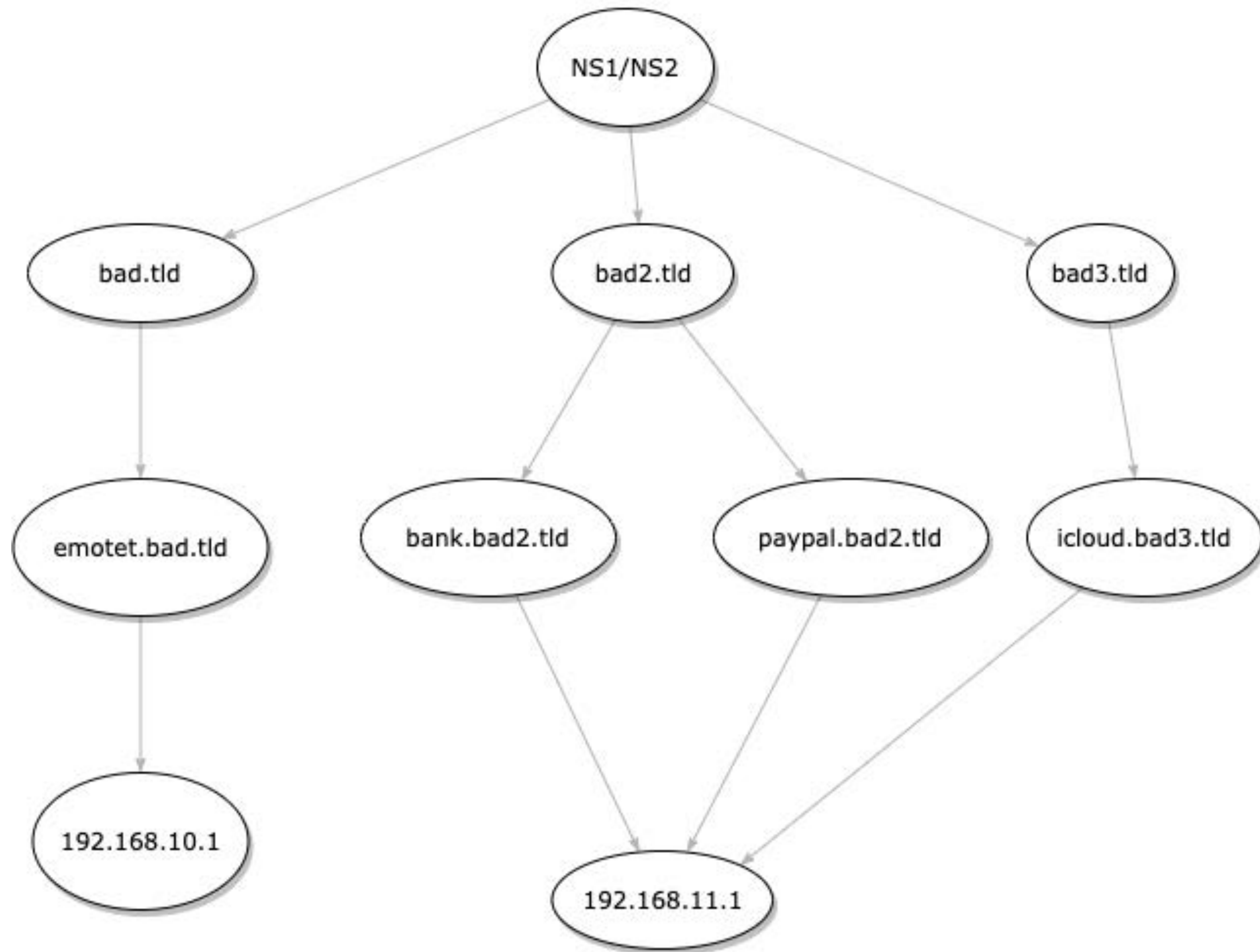
Why Passive DNS ?

- Everything begins with a DNS query
- DNS is used (legitimate queries)
- DNS is also used for abuse by malware -
 1. Phishing domains
 2. Legitimate domains with scripts/web hosting accounts compromised
 3. Botnets, ransomware - C2C mothership
- Domain names are cheap. 99% domains registered are used for malicious purposes

Mapping of the interconnections

- Doing forward lookups(active) poses a risk - targeted domains
- Correlation of domains, name servers, IP addresses
- What other domains are hosted on the same IP address ?
- What other domains are using the same name servers ?
- What other domains are having the same MX ?

Mapping of the interconnections



Who should be using Passive DNS ?

- Malware researchers
- Security professionals
- Incident Responders
- SOC Analysts
- Law Enforcement


Passive DNS operators

- Spamhaus Technology
- Farsight Security
- RiskIQ
- CIRCL
- VirusTotal

hacked Start your ~~domain~~ name search

What is going on over at GoDaddy? ...

Published on February 12, 2020

 Simon Forster | [Follow](#)

 21  4  0

One of our researchers has reported over 5,000 hijacked domains to GoDaddy and there seems to be no end in sight. Another 700 today.

The Current State of Domain Hijacking, and a specific look at the ongoing issues at GoDaddy

[Tweet Follow @spamhaus](#)

2020-04-17 12:04:54 UTC | by Spamhaus Team | Category: [domains](#), [dbl](#), [domain hijacking](#), [godaddy](#)

Recent News Articles

Spamhaus Botnet Threat Update: Q2-2020

Tracking Qbot

Spamhaus Botnet Threat Update: Q1-2020

The Current State of Domain Hijacking, and a specific look at the ongoing issues at GoDaddy

It was the best of times, it was the worst of times

Weaponizing Domain Names: how bulk registration aids global spam campaigns

Amazon Web Services - thwarting spam with a decade-old best practice

Spamhaus Botnet Threat Report 2019

Older News Articles:
▶ Spamhaus News INDEX

Domain hijacking is not a new problem, but it is one that gains strength if it is not countered effectively, and we have seen some disturbing trends in the last 6 months.

Cyber criminals are increasingly relying on legitimate and well established domains in order to carry out their maliciousness on the internet. Because of a recent sharp increase in "[Business Email Compromise](#)" (BEC) we are seeing more and more domain hijacking.

- The criminals carrying out this activity are using many weapons in their arsenal to gain access to legitimate domains: phishing, social engineering, exploiting vulnerabilities in DNS management software, and delivering malware that gives them access to the unsuspecting user's information.
- Once they have gained the access to manipulate the DNS of the targeted domains, they will create new hostnames (domain shadowing) that point to a different IP range that is not associated with the root domain, while keeping the root domain intact. Alternatively, they will change the name servers of the domain to point to a new location.
- After they have changed the DNS, they use the positive and well-established reputation of these domains to carry out large scale spam sending and malware hosting campaigns. These are meant to gather more user credentials, infect systems with malware, or disrupt users and businesses to suit their own needs. Using the positive reputation of the stolen domains allows them to evade spam filters and other protection methods that depend on reputational data.

It would be logical to expect that registrars would be on top of the ever-changing landscape that is allowing criminal elements to exploit their users. However, Spamhaus is not seeing enough proactive and mitigating efforts by the world's largest registrar, GoDaddy. In February we published an article [What is going on at GoDaddy?](#). Two months have passed and we still are seeing a continual issue with legitimate domains registered at GoDaddy being hijacked for nefarious purposes.

Domain Shadowing Attack

- Attackers gain access to credentials of legitimate domain names
- Create subdomains pointing to hosting infrastructure (phishing, malware etc)

Dive in #1- Godaddy Domain shadowing

- Bad actors create pxi.domain.tld CNAME pointing to voxpk.duckdns.org
- voxpk.duckdns.org pointing to 104.250.187.36
- pxi.domain.tld contains scripts (phishing, spam etc)
- AS3223 - VOXILITY, GB

incometaxnotice.in

whois.registry.in

Domain Name: incometaxnotice.in
Registry Domain ID: D414400000007463855-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2019-04-02T05:54:23Z
Creation Date: 2019-02-16T05:57:19Z
Registry Expiry Date: 2021-02-16T05:57:19Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientRenewProhibited <http://www.icann.org/epp#clientRenewProhibited>
Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited <http://www.icann.org/epp#clientUpdateProhibited>
Domain Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>
Registry Registrant ID:
Registrant Name:
Registrant Organization: P.M. Bagrecha and co
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: Gujarat

```
"records": [
  {
    "id": "2BF14A2CF2DCE6391CCA69CF18FED193",
    "rdata": "34.102.136.180",
    "domain": "incometaxnotice.in",
    "rclass": "IN",
    "rrname": "incometaxnotice.in",
    "rrtype": "A",
    "time_last": 1594172528
  },
  {
    "id": "671FA3C2A30795D65B5AB3D7063C551D",
    "rdata": "ns06.domaincontrol.com",
    "domain": "incometaxnotice.in",
    "rclass": "IN",
    "rrname": "incometaxnotice.in",
    "rrtype": "NS",
    "time_last": 1594153895
  },
  {
    "id": "9DC7C87EF72C5953D25E1335309866FB",
    "rdata": "ns05.domaincontrol.com",
    "domain": "incometaxnotice.in",
    "rclass": "IN",
    "rrname": "incometaxnotice.in",
    "rrtype": "NS",
    "time_last": 1594153895
  },
  {
    "id": "B1B7A96418E25FDCC9053947D17CD3F7",
    "rdata": "voxpki.duckdns.org",
    "domain": "incometaxnotice.in",
    "rclass": "IN",
    "rrname": "pxi.incometaxnotice.in",
    "rrtype": "CNAME",
    "time_last": 1594153895
  },
  {
    "id": "A94F7402A890F1923A8C95CCA124B4D5",
    "rdata": "ns05.domaincontrol.com. dns.jomax.net. 0 28800 7200 604800 600",
    "domain": "incometaxnotice.in",
    "rclass": "IN",
    "rrname": "incometaxnotice.in",
    "rrtype": "SOA",
    "time_last": 1594172528
  }
],
```

```
{
  "id": "B1B7A96418E25FDCC9053947D17CD3F7",
  "rdata": "voxpk.duckdns.org",
  "domain": "incometaxnotice.in",
  "rclass": "IN",
  "rrname": "pxi.incometaxnotice.in",
  "rrtype": "CNAME",
  "time_last": 1594153895
},
```



```

$ dig pxi.incometaxnotice.in

; <<>> DiG 9.10.6 <<>> pxi.incometaxnotice.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55486
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;pxi.incometaxnotice.in.                IN      A

;; ANSWER SECTION:
pxi.incometaxnotice.in. 335      IN      CNAME   voxpki.duckdns.org.
voxpki.duckdns.org.    60       IN      A       104.250.187.36

;; AUTHORITY SECTION:
duckdns.org.          545      IN      NS      ns2.duckdns.org.
duckdns.org.          545      IN      NS      ns3.duckdns.org.
duckdns.org.          545      IN      NS      ns1.duckdns.org.

;; ADDITIONAL SECTION:
ns2.duckdns.org.      61991   IN      A       54.191.117.119
ns3.duckdns.org.      149     IN      A       52.26.169.94
ns1.duckdns.org.      154     IN      A       54.187.92.222

;; Query time: 281 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Tue Sep 08 11:28:29 IST 2020
;; MSG SIZE rcvd: 200

```

~/securedrop/passive-dns on  master  12:01:00

\$



Index of /

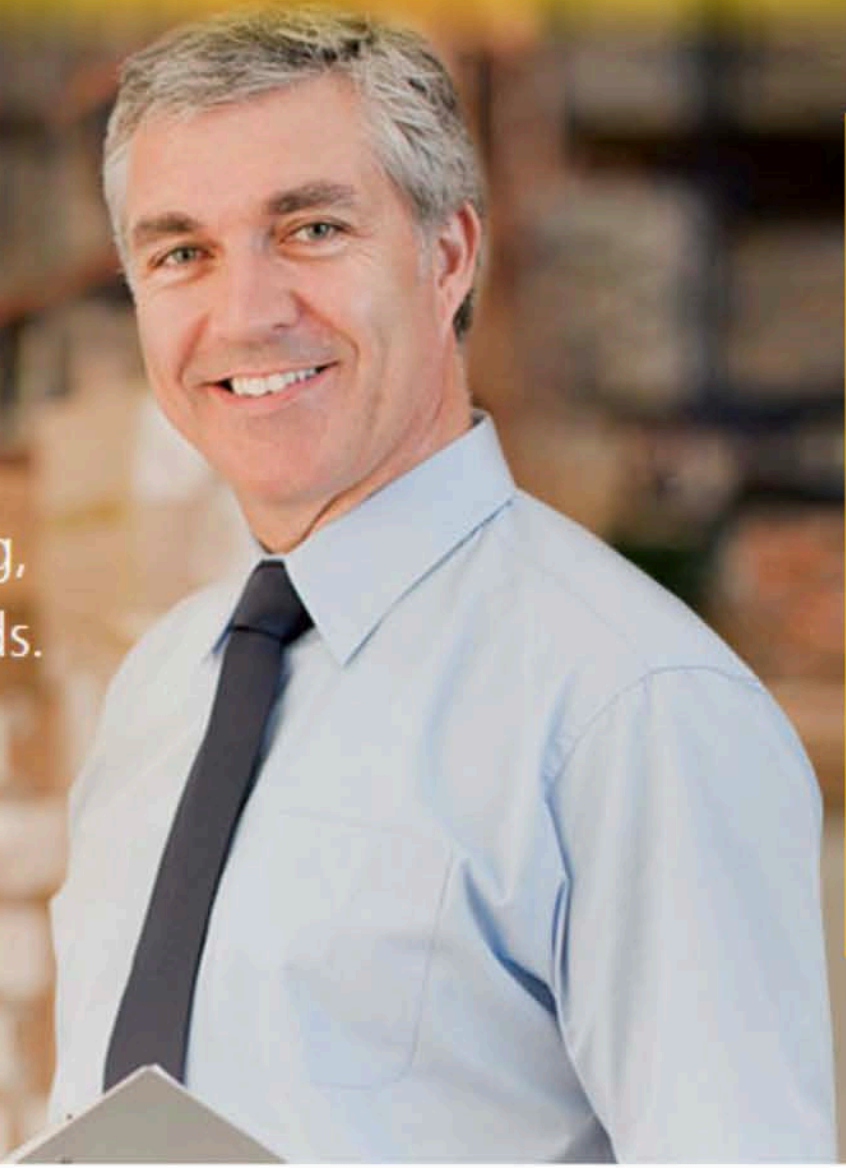
Name	Last modified	Size	Description
cgi-bin/	2020-07-09 19:30	-	
test.php	2020-06-29 06:13	670	

Upload is **WORKING**
Check Mailling ..

E-Mail	Order ID
<input type="button" value="Send test >>"/>	

Welcome to MyDHL

DHL Express is the leader in global express shipping. With MyDHL we offer you an easy-to-use online shipping, tracking and billing solution — customized for your needs.



Login to MyDHL

Signin with a valid Email Address and Password to review package information.

 Remember Me ⓘ

[Forgot Password or User ID?](#)

Learn About the Benefits of MyDHL and Register Now



Fast and Easy Online Shipping



Easy Tracking



One Login for Everything



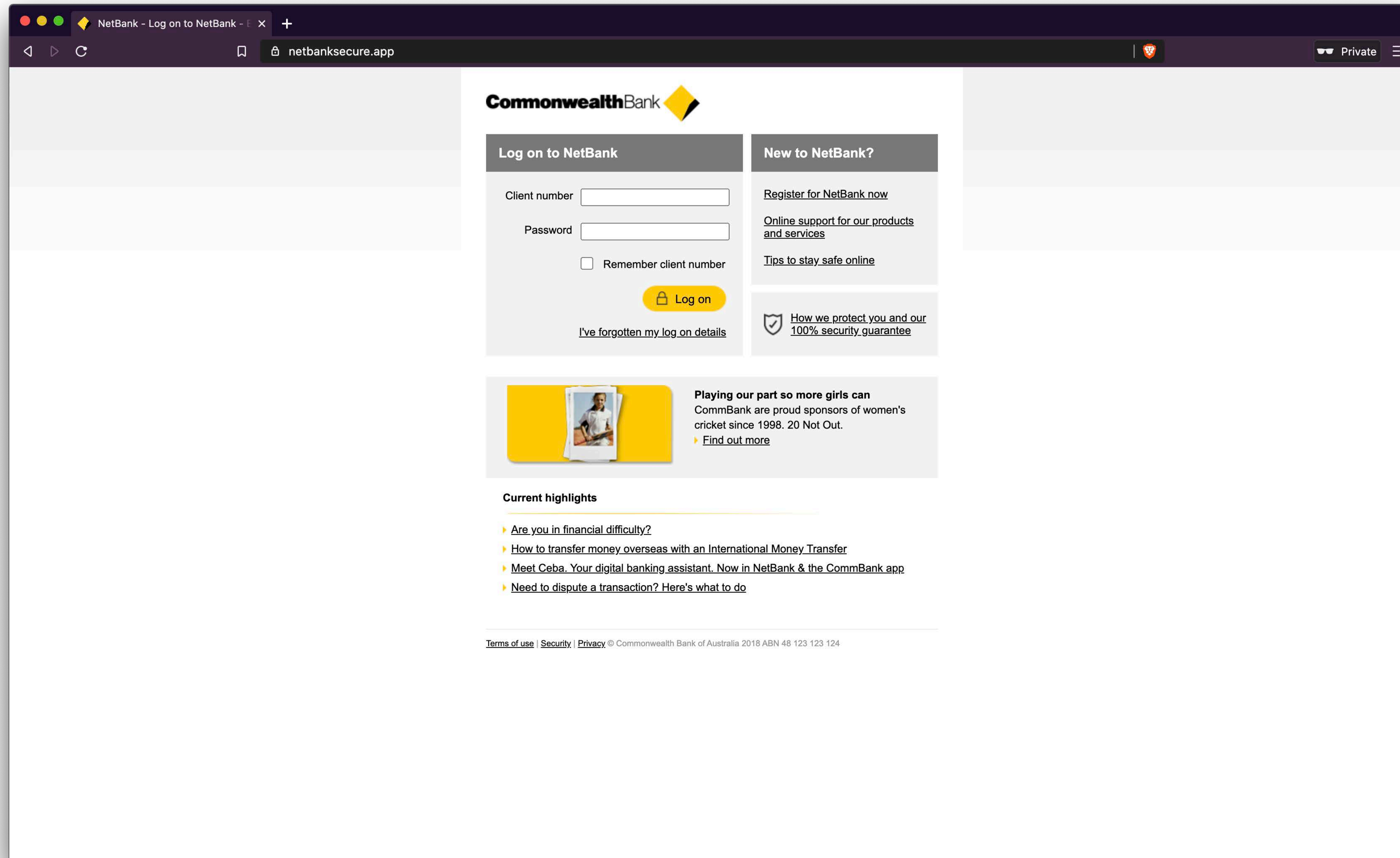
Manage your Profile



Secure and Convenient Access

MyDHL makes it easier than ever for you

Dive in #2



```
"records": [
  {
    "id": "27D7491C032B652595C10B4DF04443A9",
    "rdata": "ns-cloud-c1.googledomains.com",
    "domain": "netbanksecure.app",
    "rclass": "IN",
    "rrname": "netbanksecure.app",
    "rrtype": "NS",
    "time_last": 1594429924
  },
  {
    "id": "E8F76196B8DBA2FBB7D3DB89852C4866",
    "rdata": "ns-cloud-c3.googledomains.com",
    "domain": "netbanksecure.app",
    "rclass": "IN",
    "rrname": "netbanksecure.app",
    "rrtype": "NS",
    "time_last": 1594429924
  },
  {
    "id": "EF6E6A84C70C30D99268B413AC8FC2DA",
    "rdata": "ns-cloud-c4.googledomains.com",
    "domain": "netbanksecure.app",
    "rclass": "IN",
    "rrname": "netbanksecure.app",
    "rrtype": "NS",
    "time_last": 1594429924
  },
  {
    "id": "FA6C3C3068A0C9BE4179538858968627",
    "rdata": "ns-cloud-c2.googledomains.com",
    "domain": "netbanksecure.app",
    "rclass": "IN",
    "rrname": "netbanksecure.app",
    "rrtype": "NS",
    "time_last": 1594429924
  }
],
```

```
"records": [  
  {  
    "id": "01F82AC93840B30C046FB5770D9DDEDE",  
    "rdata": "52.189.217.143",  
    "domain": "netbanksecure.app",  
    "rclass": "IN",  
    "rrname": "netbanksecure.app",  
    "rrtype": "A",  
    "time_last": 1594429924  
  }  
],
```



```
"records": [
  {
    "id": "01F82AC93840B30C046FB5770D9DDEDE",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "netbanksecure.app",
    "rrtype": "A",
    "time_last": 1594429924
  },
  {
    "id": "2C9E128C0643A582569B2C4944E827C2",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "commbank.global",
    "rrtype": "A",
    "time_last": 1594384256
  },
  {
    "id": "331D3A9CD625BAEB3DA3461EC60C718D",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "commbank-secure.app",
    "rrtype": "A",
    "time_last": 1594005976
  },
  {
    "id": "50752362795E89A60072BD5E7F4D3660",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "netbank-secure.com.au",
    "rrtype": "A",
    "time_last": 1594211586
  },
  {
    "id": "679715421CFF54D55B93CC0C70FC53AF",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "commbanksecure.com",
    "rrtype": "A",
    "time_last": 1594005977
  },
  {
    "id": "A1AB4C12E2F9A32D46AD6F59468EABE8",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "secure-commbank.app",
    "rrtype": "A",
    "time_last": 1594176923
  },
  {
    "id": "BE96950B1E362F828C4E780D5E56773C",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "commbanksecure.app",
    "rrtype": "A",
    "time_last": 1594005975
  },
  {
    "id": "D716700B24AB5CBF2BA733DF2D9213E9",
    "rdata": "52.189.217.143",
    "rclass": "IN",
    "rrname": "commbanksecure.com.au",
    "rrtype": "A",
    "time_last": 1593738023
  }
],
```

```
$ dig verifyaccountxvconfirmationvxcentervstxlmopstui.tk

; <<>> DiG 9.10.6 <<>> verifyaccountxvconfirmationvxcentervstxlmopstui.tk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58236
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;verifyaccountxvconfirmationvxcentervstxlmopstui.tk. IN      A

;; ANSWER SECTION:
verifyaccountxvconfirmationvxcentervstxlmopstui.tk. 14400 IN A 178.159.36.237

;; AUTHORITY SECTION:
verifyaccountxvconfirmationvxcentervstxlmopstui.tk. 299 IN NS ns2.dnsbeonline.ru.
verifyaccountxvconfirmationvxcentervstxlmopstui.tk. 299 IN NS ns1.dnsbeonline.ru.

;; ADDITIONAL SECTION:
ns1.dnsbeonline.ru.      14377  IN      A        178.159.36.237
ns1.dnsbeonline.ru.      14377  IN      A        178.159.36.136
ns2.dnsbeonline.ru.      14377  IN      A        178.159.36.89
ns2.dnsbeonline.ru.      14377  IN      A        178.159.36.82

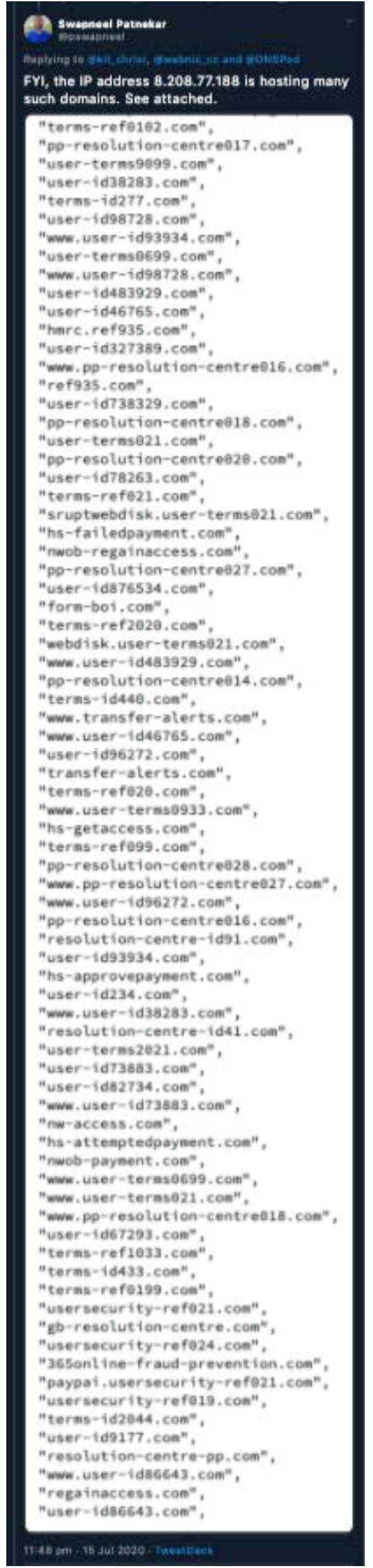
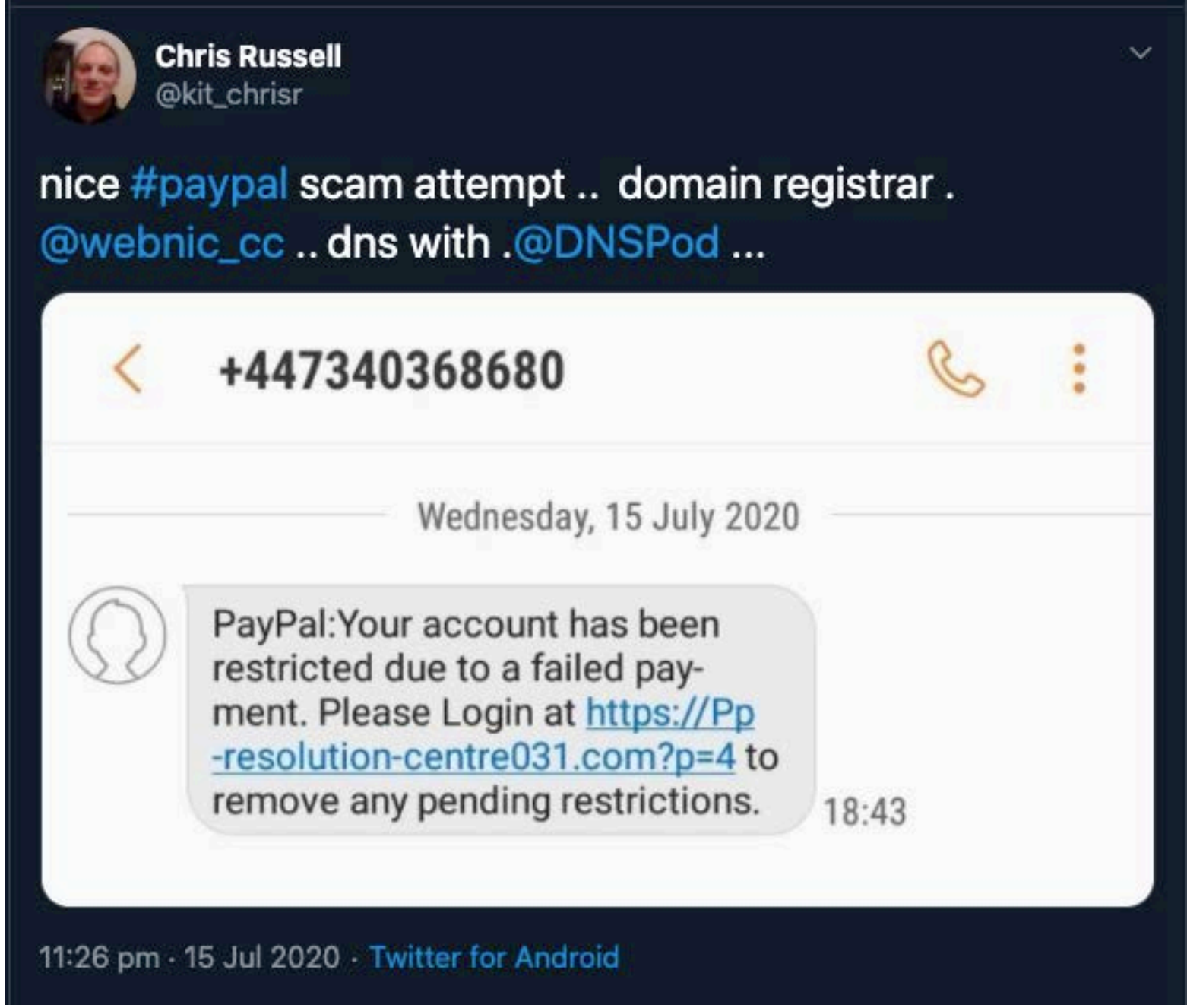
;; Query time: 1369 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Tue Sep 08 12:30:48 IST 2020
;; MSG SIZE rcvd: 210
```

~/securedrop/passive-dns on  master!  12:43:30

\$



FYI, the IP address 8.208.77.188 is hosting many such domains. See attached.



Source: <https://twitter.com/pswapneel/status/1283465877908668417>

~/securedrop/passive-dns on  master!  13:31:44

\$



Summary

- Enables investigation of abuse in DNS
- Mapping of the interconnections provides an insight into scale of attack
- Passive DNS operator database may not have a full picture
- Passive DNS - Common Output Format (draft-dulaunoy-dnsop-passive-dns-cof-07)

References

- Passive DNS Replication
<https://www.enyo.de/fw/software/dnslogger/first2005-paper.pdf>
<https://www.first.org/conference/2005/papers/florian-weimer-slides-1.pdf>
- Passive DNS - Common Output Format
<https://tools.ietf.org/html/draft-dulaunoy-dnsop-passive-dns-cof-07>
- What is going on over at GoDaddy?
<https://www.linkedin.com/pulse/what-going-over-godaddy-simon-forster>
- The Current State of Domain Hijacking, and a specific look at the ongoing issues at GoDaddy
<https://www.spamhaus.org/news/article/797/the-current-state-of-domain-hijacking-and-a-specific-look-at-the-ongoing-issues-at-godaddy>
- Phish of GoDaddy Employee Jeopardized Escrow.com, Among Others
<https://krebsonsecurity.com/2020/03/phish-of-godaddy-employee-jeopardized-escrow-com-among-others/>
- Openphish Community Feed
<https://openphish.com/feed.txt>
- Spamhaus Technology Passive DNS
<https://www.spamhaustech.com/product/passive-dns/>
- Farsight Security Passive DNS (DNSDB)
<https://www.farsightsecurity.com/dnsdb-community-edition/>
- CIRCL Passive DNS
<https://www.circl.lu/services/passive-dns/>

Thank you!