Domain Hijacking

Matthew C. Stith, Spamhaus
Eddy Winstead, ISC

April 29th, 2020

https://www.isc.org

What we're going to covering

- What why and how of domain hijacking
- Examples of various hijacking methods
- High profile stories about hijacked domains
- What can be done to protect domains and networks
- Q&A

What is Domain Hijacking?

- Malicious actors gaining access to the DNS records of a legitimate domains (which they do not own):
- In some cases only the root domain's DNS is changed. This is reflected in the WHOIS.
- In other cases a new host (subdomain) is created with new DNS settings. This practice is called domain shadowing. This is not visible at the WHOIS level.

Why is it exploited?

These following two factors lead to a positive reputation:

- The age of the domain
- The legitimacy of the domain

Meaning many of these domains could be able to send email or serve content without much scrutiny from content or reputation filters.

How is it happening?

Phishing

Social engineering

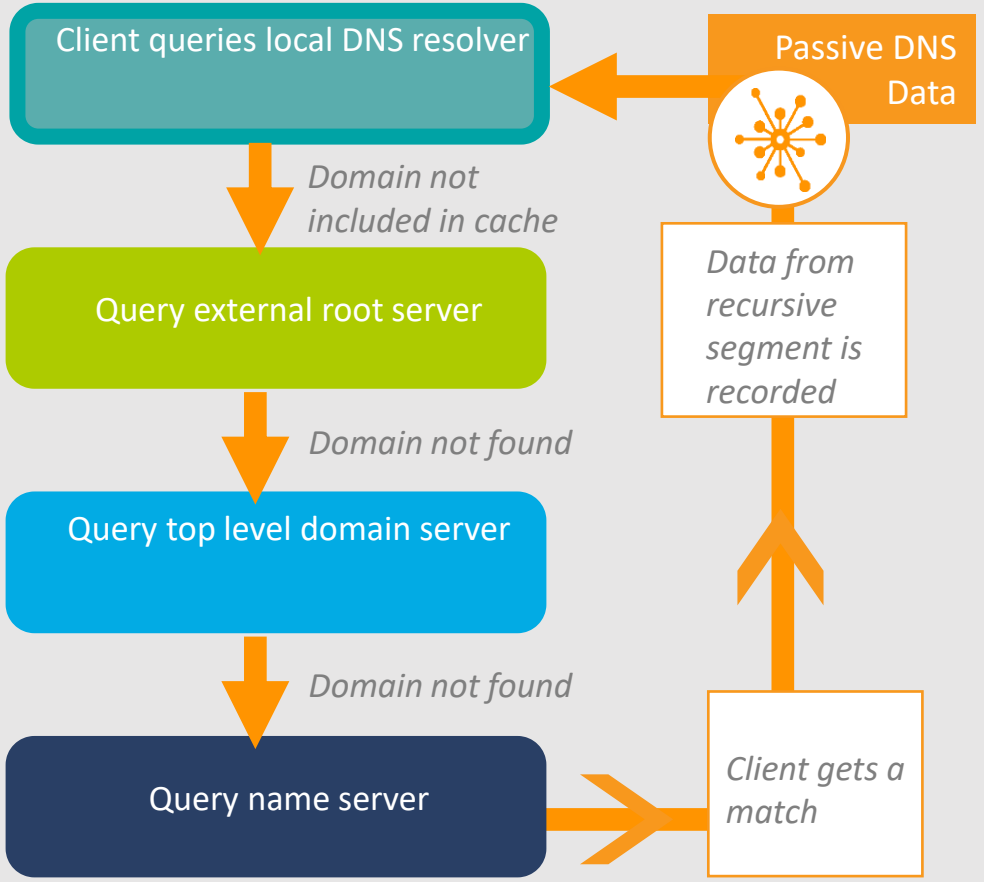
Compromised DNS

Exploiting weaknesses in applications

Malware

Investigating domain hijacking

- Passive DNS data is collected with special probes activated on a DNS Resolver.
- The probes record anonymized cache miss.
- Data is collected through DNS recursive servers.
- Simple and extensive search functionalities make this data easy to search.



Examples – Domain

Domain Name	R.Type	RDATA	First seen	Last seen
glararug.com (⏪)	A	217.8.117.8		2020-04-24
glararug.com (⏪)	NS	ns2.nsnewline.com (⏩)	2020-04-19	2020-04-24
glararug.com (⏪)	NS	ns1.nsnewline.com (⏩)	2020-04-19	2020-04-24
glararug.com (⏪)	NS	ns2.glararug.com (⏩)	2020-04-24	2020-04-24
glararug.com (⏪)	NS	ns1.glararug.com (⏩)	2020-04-24	2020-04-24
glararug.com (⏪)	A	50.63.202.47	2020-03-23	2020-03-23
glararug.com (⏪)	NS	ns08.domaincontrol.com (⏩)	2019-04-16	2020-03-23
glararug.com (⏪)	NS	ns07.domaincontrol.com (⏩)	2019-04-16	2020-03-23
glararug.com (⏪)	A	50.63.202.37	2019-10-21	2019-10-21
glararug.com (⏪)	A	184.168.221.51	2019-05-15	2019-05-15

Domain

```
root@DESKTOP-7V1QQ3F:~# whois glararug.com
   Domain Name: GLARARUG.COM
   Registry Domain ID: 2380362674_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2020-04-18T13:55:35Z
   Creation Date: 2019-04-14T19:03:37Z
   Registry Expiry Date: 2021-04-14T19:03:37Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.NSNEWLINE.COM
   Name Server: NS2.NSNEWLINE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-04-24T12:54:47Z <<<
```

Domain and Subdomain

stoolcomments.com (⏪)	A	217.8.117.8	2020-04-08	2020-04-16
stoolcomments.com (⏪)	NS	ns2.stoolcomments.com (⏩)		2020-04-16
stoolcomments.com (⏪)	NS	ns1.nsnewline.com (⏩)	2020-03-23	2020-04-20
stoolcomments.com (⏪)	NS	ns2.nsnewline.com (⏩)	2020-03-23	2020-04-20
stoolcomments.com (⏪)	NS	ns1.stoolcomments.com (⏩)	2020-04-16	2020-04-16
stoolcomments.com (⏪)	SOA	ns1.stoolcomments.com. dns-admin.stoolcomments.com. 0 900 900 1800 60		2020-04-06
stoolcomments.com (⏪)	MX	10 mx3.stoolcomments.com (⏩)		2020-04-06
stoolcomments.com (⏪)	MX	20 mx4.stoolcomments.com (⏩)		2020-04-06
stoolcomments.com (⏪)	A	217.8.117.31	2020-03-23	2020-03-23
stoolcomments.com (⏪)	A	208.91.198.30	2019-11-02	2019-11-02
stoolcomments.com (⏪)	NS	ns21.domaincontrol.com (⏩)		2019-11-02
stoolcomments.com (⏪)	NS	ns22.domaincontrol.com (⏩)	2019-07-02	2019-11-02
stoolcomments.com (⏪)	A	184.168.221.39	2019-09-12	2019-09-23
stoolcomments.com (⏪)	A	184.168.221.41		2019-09-23
stoolcomments.com (⏪)	A	50.63.202.37	2019-09-13	2019-09-23
stoolcomments.com (⏪)	A	50.63.202.33	2019-09-12	2019-09-13
stoolcomments.com (⏪)	SOA	ns21.domaincontrol.com. dns.jomax.net. 0 28800 7200 604800 600	2019-07-02	2019-09-23
stoolcomments.com (⏪)	A	184.168.221.38	2019-07-03	2019-07-03
stoolcomments.com (⏪)	A	184.168.221.34	2019-07-02	2019-07-02
stoolcomments.com (⏪)	A	184.168.221.43	2019-07-03	2019-07-03
stoolcomments.com (⏪)	A	50.63.202.35	2019-07-02	2019-07-02

Domain and Subdomain

aant.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abandonnais.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abbatiale.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abbatoire.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abhorrant.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abord.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abroge.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abrougui.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
absurdite.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
abusives.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
accepterait.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
accessibilite.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
accoutrement.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
accrochages.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
acheterais.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
acheteurs.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
achezmoi.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
acquis.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
actuell.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
additif.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
adepte.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
adjoint.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
administration.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06

Domain and Subdomain

arcitecture.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
ardisson.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
arielariel.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
armchair.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
arrayreverse.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
arrentent.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
arrl.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
arrosai.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
arrrg.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
ascorbique.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
asphalte.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
assault.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
assomption.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
asticots.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
atheniens.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
atomixtazy.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
atribu.stoolcomments.com (⋘)	A	193.187.173.210	2020-04-06
attaquables.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
attent.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
atteste.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
attitude.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
attrister.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
aubervilliers.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
aujord.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
auras.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06

Domain and Subdomain

moiselles.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
moldaves.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
moldavie.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
moleenbeek.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
moment.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
monarchie.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
mondialisation.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
mondialoproductiviste.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
monitorer.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
monnais.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
monnayable.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
monocellulaires.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
monocles.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
monogatari.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
montagneuse.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
montparnoasse.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
montpelli.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
mooooomennt.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
morbides.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
mordra.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
morteau.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
mortier.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
motdepasse.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06
motivationnelles.stoolcomments.com (⋘)	A	217.8.117.8	2020-04-06

Subdomain Only: Domain Shadowing

Everything looks normal at the root domain level

Domain Name	R.Type	RDATA	First seen	Last seen
apebbleintheroad.org (⏪)	A	50.63.202.57	2015-02-13	2020-04-18
apebbleintheroad.org (⏪)	NS	ns16.domaincontrol.com (⏩)	2018-01-18	2020-04-18
apebbleintheroad.org (⏪)	NS	ns15.domaincontrol.com (⏩)	2018-01-18	2020-04-18
apebbleintheroad.org (⏪)	SOA	ns15.domaincontrol.com. dns.jomax.net. 0 28800 7200 604800 600	2019-02-07	2020-04-18
apebbleintheroad.org (⏪)	MX	0 smtp.secureserver.net (⏩)		2019-12-26
apebbleintheroad.org (⏪)	MX	10 mailstore1.secureserver.net (⏩)	2016-02-26	2019-12-26

Subdomain Only: Domain Shadowing

But when we look a right-side search of the domain, we find something quite different happening

Domain Name	R.Type	RDATA	First seen	Last seen
apebbleintheroad.org (⋘)	A	50.63.202.57	2015-02-13	2020-04-18
apebbleintheroad.org (⋘)	NS	ns16.domaincontrol.com (⋙)	2018-01-18	2020-04-18
apebbleintheroad.org (⋘)	NS	ns15.domaincontrol.com (⋙)	2018-01-18	2020-04-18
apebbleintheroad.org (⋘)	SOA	ns15.domaincontrol.com. dns.jomax.net. 0 28800 7200 604800 600	2019-02-07	2020-04-18
vm.apebbleintheroad.org (⋘)	A	217.8.117.31	2020-01-28	2020-01-30
vm.apebbleintheroad.org (⋘)	NS	ns1.qk.denverbudandbreakfast.com (⋙)	2020-01-28	2020-01-30
rx.apebbleintheroad.org (⋘)	NS	ns1.rx.apebbleintheroad.org (⋙)	2019-12-26	2019-12-26
rx.apebbleintheroad.org (⋘)	NS	ns2.rx.apebbleintheroad.org (⋙)	2019-12-26	2019-12-26
www.apebbleintheroad.org (⋘)	CNAME	apebbleintheroad.org (⋙)	2015-02-13	2019-12-26
rx.apebbleintheroad.org (⋘)	SOA	ns1.rx.apebbleintheroad.org. dns-admin.rx.apebbleintheroad.org. 0 900 900 1800 60	2019-12-26	2019-12-26
apebbleintheroad.org (⋘)	MX	0 smtp.secureserver.net (⋙)		2019-12-26
apebbleintheroad.org (⋘)	MX	10 mailstore1.secureserver.net (⋙)	2016-02-26	2019-12-26
rx.apebbleintheroad.org (⋘)	MX	20 mx4.rx.apebbleintheroad.org (⋙)	2019-12-26	2019-12-26
rx.apebbleintheroad.org (⋘)	MX	10 mx3.rx.apebbleintheroad.org (⋙)	2019-12-26	2019-12-26

Domain Shadowing in the wild

```
Received: from ragalonragdolls.com (unknown [117.212.90.45])
by Redacted (Postfix) with ESMTP id C1E03C0506
for <XXXXXXXXXXX>; Fri, 27 Dec 2019
Envelope-To: .fr
Delivery-Date: Fri, 27 Dec 2019
 From: Mondial Relay <Redacted@ragalonragdolls.com>
 Content-Type: multipart/mixed; boundary="------------I305M09060309060P_365415389083760"
X-Mril-Campaign: [ wymdjppebfuzjvaryknajxczybxsdpnqqftaut//f6cfc= ]
To:
MIME-Version: 1.0
Subject: Livraisonufyn
Date: Fri, 27 Dec 2019

<small><a href=3D"http://rx.apebbleintheroad.org//racontaient~Cagne/~Junkyf=
XXXXXXXXXXXXX/">tena</a> Mondial RELAY</small><br>
<table><tr><td><a href=3D"http://rx.apebbleintheroad.org//racontaient~Cagne=
/~JunkyXXXXXXXXXXXXX/"><img src=3D"cid:defrag.jpg" alt=3D""></a></td><t=d></td></tr></table><br>
<br><div style=3D"color: #987"><br>
<br>  iblocklist Terrifiant Retrouve Pacino invalidant gauchi<br> =C2=A9 Mondial Relay, 1601 Willow Road, Menlo Park, CA 94025.
<br>=C2=A9 This <a href=3D"http://rx.apebbleintheroad.org//racontaient~Cagne/~J=    unkyfaitchier.Nimeyer/">message</a> was sent to and
intended for Not your account? 93937 Remove your <a href=3D"http://rx.apebbleintheroad.org//racont=
aient~Cagne/~JunkyXXXXXXXXXXXXXXX/">email</a> from this account.<br> Reported Parcequ comedique Aquatique reservees Larcher<br>
</div><br>
```

Recent Incidents with Domain Hijacking

- Openprovider
- Nation State DNS Hijacking
- GoDaddy DNS Management issues and after

OpenProvider (E-hawk.net hijack)

- E Hawk: A fraud prevention company
- In December 2019 The Attacker used social engineering of the customer support at OpenProvider to gain access to the domain.
- After waiting almost 3 weeks that changed the Attacker changed the DNS settings. E Hawk was made aware of this change immediately.
- Less than 48 hours later E Hawk was able to regain ownership of their domain, which would have not been possible without industry relationships.

Nation State DNS Hijacking

- From 2017 to 2019 multiple Middle Eastern, African, US companies and governments had their domain's DNS setting hijacked.
- Cisco, FireEye, Crowdstrike, and the US Government warned about the group, named DNSpionage.
- Compromise of a domain registrar to gain access to DNS settings.
- The sites that were hijacked were used for redirection purposes.
- The group used fake job website, malware, macros in files to also attempt to compromise users.
- Hijackers registered SSL certificates for the domains, allowing them to gain access to encrypted passwords, and email messages and VPN credentials

GoDaddy – Timeline

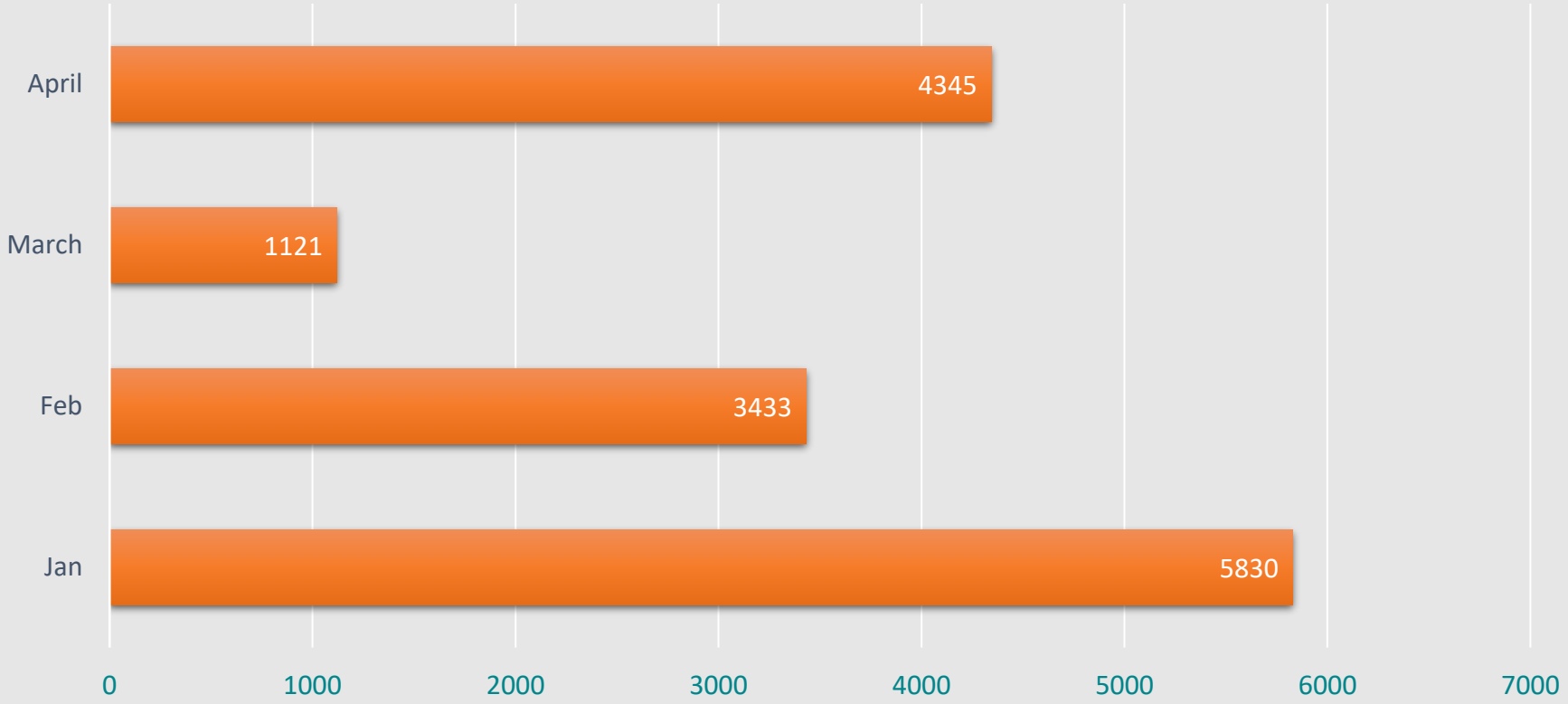
- 2016, a vulnerability identified in Managed DNS at Cloud providers.
- Late 2018, Bomb Threat Emails sent by big name brand domains
- Jan 2019, reports come out regarding the incidents along with other campaigns being sent.
- An entity, dubbed Spammybear, was responsible and hijacked upwards of 4,000 domains.
- Feb 2019 remnants of that hijack remained and were snuffed out.

GoDaddy

Spamhaus has found that the hijacking has not stopped:

- Jun 2019, domain shadowing observed at over 10,000 domains:
- Pointing to Russian infrastructure
- Upon notification most of the shadowing was stopped
- Dec 2019, attackers switched from adding hostnames to directly hijacking
- The rate of hijacking is upwards of 100 domains daily.

GoDaddy – Domain Hijacking



Spamhaus' tracking of GoDaddy hijacks

- Spamtraps intercepting phishing mail from hijacked domains.
- Domain shadowing happening at GoDaddy in mid-2019. Shut down quickly after.
- Attackers switched to straight domain hijacking afterwards.
- Using Passive DNS and other tracking methods we were able to identify the pattern being used and score negatively the reputation of the domains that had been hijacked.

Protecting yourself (domain owners)

- Two-Factor Authentication
- Passphrase management and/or strong passwords
- DNSSEC
- Registry Lock
- Limit access to your domain(s) in a large organization
- Diversify account security
- Track any change to your domain(s) and DNS
- Research registrars

Protecting networks (customers and employees)

- Netflow Analysis (where applicable)
- Passive DNS
- BGP
- DNS Firewall
- Awareness around social engineering, phishing, etc.

Protecting Registrar Customers

- Robust reporting on account access
- High profile and/or high value domain identification
- Two-factor authentication
- Regular review of customer documents
- Social Engineering, Phishing, and other malicious scenario awareness
- Work with the Anti-Abuse Industry

Q & A

What Can I do …?

Passive DNS:

- Check domains, IPs, and Brands using our Free Passive DNS
  - What is Passive DNS? A beginner's Guide
  - Free Access to Passive DNS
- DNS Firewall Threat Feeds:
  - Protect your users
  - Add Spamhaus DNS RPZ feeds to BIND (and other resolvers) = DNS Firewall
  - Beginner's Guide to DNS Firewall/RPZ
  - DNS Firewall Factsheet
  - Rackspace DNS Firewall Case Study
  - Also a docker image available

Contact Us

info@securityzones.net

Arnie Bjorklund

SecurityZONES / Spamhaus Technology

- Questions, Free Trials
- Technical Assistance
- Expertise

Recommended Reads

All of the incidents I have mentioned have multiple articles and blogs referenced in them. Here they are. Please read and share.

Godaddy

https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/

https://arstechnica.com/information-technology/2019/01/godaddy-weakness-let-bomb-threat-scammers-hijack-thousands-of-big-name-domains/

https://krebsonsecurity.com/2019/02/crooks-continue-to-exploit-godaddy-hole/

https://thehackerblog.com/the-orphaned-internet-taking-over-120k-domains-via-a-dns-vulnerability-in-aws-google-cloud-rackspace-and-digital-ocean/

https://www.spamhaus.org/news/article/797/the-current-state-of-domain-hijacking-and-a-specific-look-at-the-ongoing-issues-at-godaddy

Openprovider

https://krebsonsecurity.com/2020/01/does-your-domain-have-a-registry-lock/

Nation State DNS Hijacking

https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

https://cyber.dhs.gov/blog/#why-cisa-issued-our-first-emergency-directive

https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/