Using certificate transparency streams to hunt down phishing sites

Sean Gallagher

@thepacketrat

IT/NatSec Editor, Ars Technica

Certificate data , and why it's great for OSINT

- More phishing sites are using SSL certs, other tools to evade filters
- LetsEncrypt is free, programmatic, as is cPanel – which auto-cert registers new domains
- While DNS holds domain names of sites, don't identify malicious domains in DNS until they go active.
- Phishing domains may have already switched by the time activity is detected.
- Certificate data can be scanned actively to discover phishing sites before they go live, and used to proactively collect forensic data on kits, etc. while the sites are still being set up.

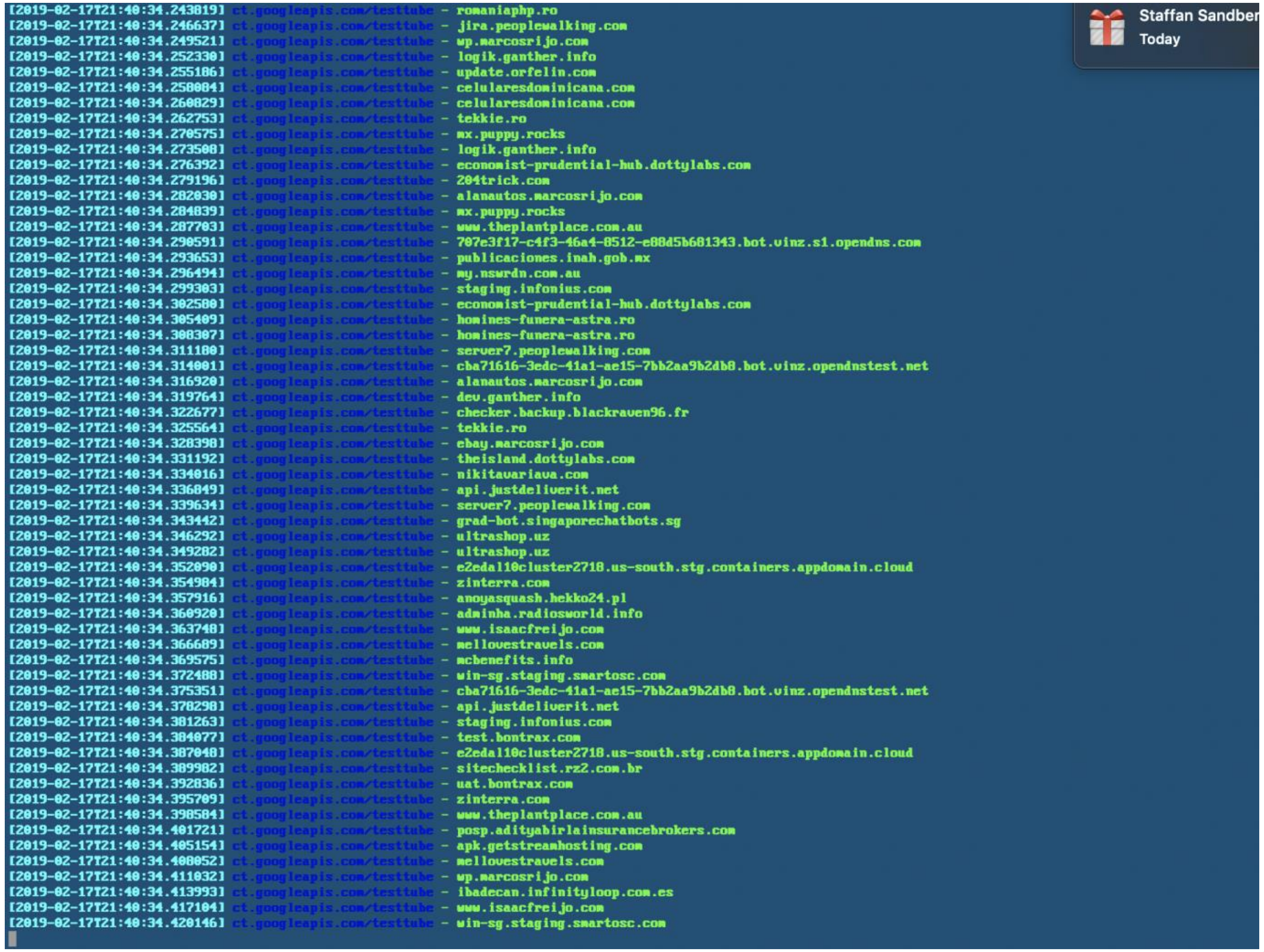
Certificate Transparency Logs

- Were created to help track the validity of SSL certificates issued by the major certificate authorities
- Data helps detect mistakenly issued certificates, stolen or otherwise maliciously acquired certs, among other things.
- Each CA logs each new certificate, flags revocations, etc.

The ”Certstream"

- Service created by Ryan Sears of Cali Dog Security that generates a near-realtime data feed from all of the major certificate authorities' transparency logs.
- Data is published over a web socket, can be directly accessed via a command line interface published in pip (pip install certstream)
- Gives you a timestamp for an event, the source url for the log it came from, and the domain associated with the certificate.
- This by itself, with a little grepping with regular expressions, or minor coding, could be used to hunt for threats spoofing specific domain name patterns.

The Certstream

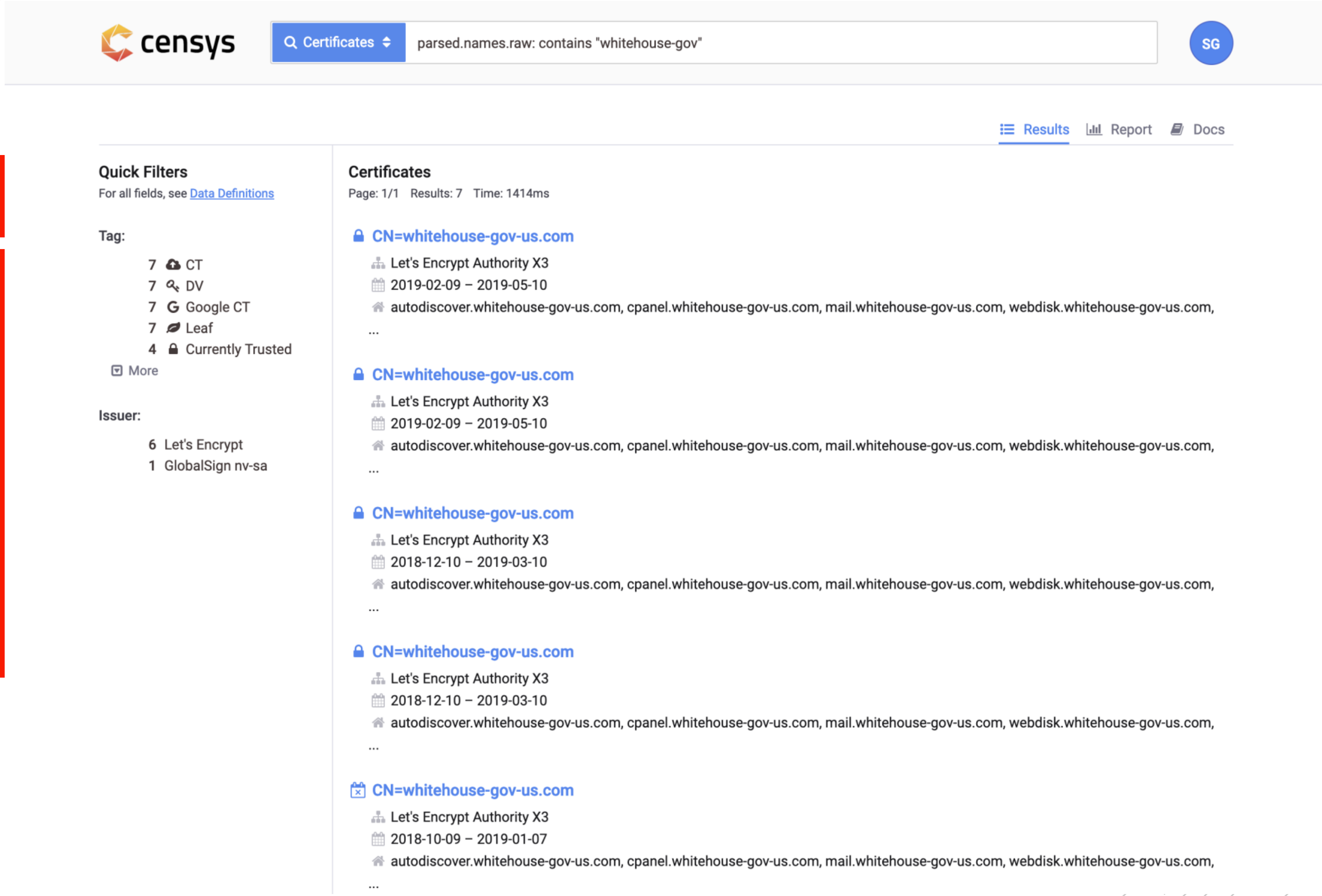


```
[2019-02-17T21:40:34.243819] ct.googleapis.com/testtube - romaniaphp.ro
[2019-02-17T21:40:34.246637] ct.googleapis.com/testtube - jira.peoplewalking.com
[2019-02-17T21:40:34.249521] ct.googleapis.com/testtube - wp.marcosrijo.com
[2019-02-17T21:40:34.252330] ct.googleapis.com/testtube - logik.ganther.info
[2019-02-17T21:40:34.255186] ct.googleapis.com/testtube - update.orfelin.com
[2019-02-17T21:40:34.258084] ct.googleapis.com/testtube - celularesdominicana.com
[2019-02-17T21:40:34.260829] ct.googleapis.com/testtube - celularesdominicana.com
[2019-02-17T21:40:34.262753] ct.googleapis.com/testtube - tekkie.ro
[2019-02-17T21:40:34.270575] ct.googleapis.com/testtube - mx.puppy.rocks
[2019-02-17T21:40:34.273508] ct.googleapis.com/testtube - logik.ganther.info
[2019-02-17T21:40:34.276392] ct.googleapis.com/testtube - economist-prudential-hub.dottylabs.com
[2019-02-17T21:40:34.279196] ct.googleapis.com/testtube - 204trick.com
[2019-02-17T21:40:34.282030] ct.googleapis.com/testtube - alanautos.marcosrijo.com
[2019-02-17T21:40:34.284839] ct.googleapis.com/testtube - mx.puppy.rocks
[2019-02-17T21:40:34.287703] ct.googleapis.com/testtube - www.theplantplace.com.au
[2019-02-17T21:40:34.290591] ct.googleapis.com/testtube - 707e3f17-c4f3-46a4-8512-e88d5b681343.bot.vinz.s1.opendns.com
[2019-02-17T21:40:34.293653] ct.googleapis.com/testtube - publicaciones.inah.gob.mx
[2019-02-17T21:40:34.296494] ct.googleapis.com/testtube - my.nswrdn.com.au
[2019-02-17T21:40:34.299303] ct.googleapis.com/testtube - staging.infonius.com
[2019-02-17T21:40:34.302580] ct.googleapis.com/testtube - economist-prudential-hub.dottylabs.com
[2019-02-17T21:40:34.305409] ct.googleapis.com/testtube - homines-funera-astra.ro
[2019-02-17T21:40:34.308307] ct.googleapis.com/testtube - homines-funera-astra.ro
[2019-02-17T21:40:34.311180] ct.googleapis.com/testtube - server7.peoplewalking.com
[2019-02-17T21:40:34.314001] ct.googleapis.com/testtube - cba71616-3edc-41a1-ae15-7bb2aa9b2db8.bot.vinz.opendnstest.net
[2019-02-17T21:40:34.316920] ct.googleapis.com/testtube - alanautos.marcosrijo.com
[2019-02-17T21:40:34.319764] ct.googleapis.com/testtube - dev.ganther.info
[2019-02-17T21:40:34.322677] ct.googleapis.com/testtube - checker.backup.blackraven96.fr
[2019-02-17T21:40:34.325564] ct.googleapis.com/testtube - tekkie.ro
[2019-02-17T21:40:34.328398] ct.googleapis.com/testtube - ebay.marcosrijo.com
[2019-02-17T21:40:34.331192] ct.googleapis.com/testtube - theisland.dottylabs.com
[2019-02-17T21:40:34.334016] ct.googleapis.com/testtube - nikitavariava.com
[2019-02-17T21:40:34.336849] ct.googleapis.com/testtube - api.justdeliverit.net
[2019-02-17T21:40:34.339634] ct.googleapis.com/testtube - server7.peoplewalking.com
[2019-02-17T21:40:34.343442] ct.googleapis.com/testtube - grad-bot.singaporechatbots.sg
[2019-02-17T21:40:34.346292] ct.googleapis.com/testtube - ultrashop.uz
[2019-02-17T21:40:34.349282] ct.googleapis.com/testtube - ultrashop.uz
[2019-02-17T21:40:34.352090] ct.googleapis.com/testtube - e2edal10cluster2718.us-south.stg.containers.appdomain.cloud
[2019-02-17T21:40:34.354984] ct.googleapis.com/testtube - zinterra.com
[2019-02-17T21:40:34.357916] ct.googleapis.com/testtube - anoyasquash.hekko24.pl
[2019-02-17T21:40:34.360920] ct.googleapis.com/testtube - adminha.radiosworld.info
[2019-02-17T21:40:34.363748] ct.googleapis.com/testtube - www.isaacfreijo.com
[2019-02-17T21:40:34.366689] ct.googleapis.com/testtube - mellovestravels.com
[2019-02-17T21:40:34.369575] ct.googleapis.com/testtube - mcbenefits.info
[2019-02-17T21:40:34.372488] ct.googleapis.com/testtube - win-sg.staging.smartosc.com
[2019-02-17T21:40:34.375351] ct.googleapis.com/testtube - cba71616-3edc-41a1-ae15-7bb2aa9b2db8.bot.vinz.opendnstest.net
[2019-02-17T21:40:34.378298] ct.googleapis.com/testtube - api.justdeliverit.net
[2019-02-17T21:40:34.381263] ct.googleapis.com/testtube - staging.infonius.com
[2019-02-17T21:40:34.384077] ct.googleapis.com/testtube - test.bontrax.com
[2019-02-17T21:40:34.387048] ct.googleapis.com/testtube - e2edal10cluster2718.us-south.stg.containers.appdomain.cloud
[2019-02-17T21:40:34.389982] ct.googleapis.com/testtube - sitechecklist.rz2.com.br
[2019-02-17T21:40:34.392836] ct.googleapis.com/testtube - uat.bontrax.com
[2019-02-17T21:40:34.395709] ct.googleapis.com/testtube - zinterra.com
[2019-02-17T21:40:34.398584] ct.googleapis.com/testtube - www.theplantplace.com.au
[2019-02-17T21:40:34.401721] ct.googleapis.com/testtube - posp.adityabirlainsurancebrokers.com
[2019-02-17T21:40:34.405154] ct.googleapis.com/testtube - apk.getstreamhosting.com
[2019-02-17T21:40:34.408052] ct.googleapis.com/testtube - mellovestravels.com
[2019-02-17T21:40:34.411032] ct.googleapis.com/testtube - wp.marcosrijo.com
[2019-02-17T21:40:34.413993] ct.googleapis.com/testtube - ibadecan.infinityloop.com.es
[2019-02-17T21:40:34.417104] ct.googleapis.com/testtube - www.isaacfreijo.com
[2019-02-17T21:40:34.420146] ct.googleapis.com/testtube - win-sg.staging.smartosc.com
```

Targeted hunting in CTL

- Censys.io stores certificate log data so it can be used for searching against recent and historical certificate registration.

Targeted hunting in CTL: search by pattern



parsed.names.raw: contains "whitehouse-gov"

Quick Filters

For all fields, see Data Definitions

Tag:

- 7 CT
- 7 DV
- 7 Google CT
- 7 Leaf
- 4 Currently Trusted
- More

Issuer:

- 6 Let's Encrypt
- 1 GlobalSign nv-sa

Certificates

Page: 1/1 Results: 7 Time: 1414ms

CN=whitehouse-gov-us.com
Let's Encrypt Authority X3
2019-02-09 – 2019-05-10
autodiscover.whitehouse-gov-us.com, cpanel.whitehouse-gov-us.com, mail.whitehouse-gov-us.com, webdisk.whitehouse-gov-us.com, ...

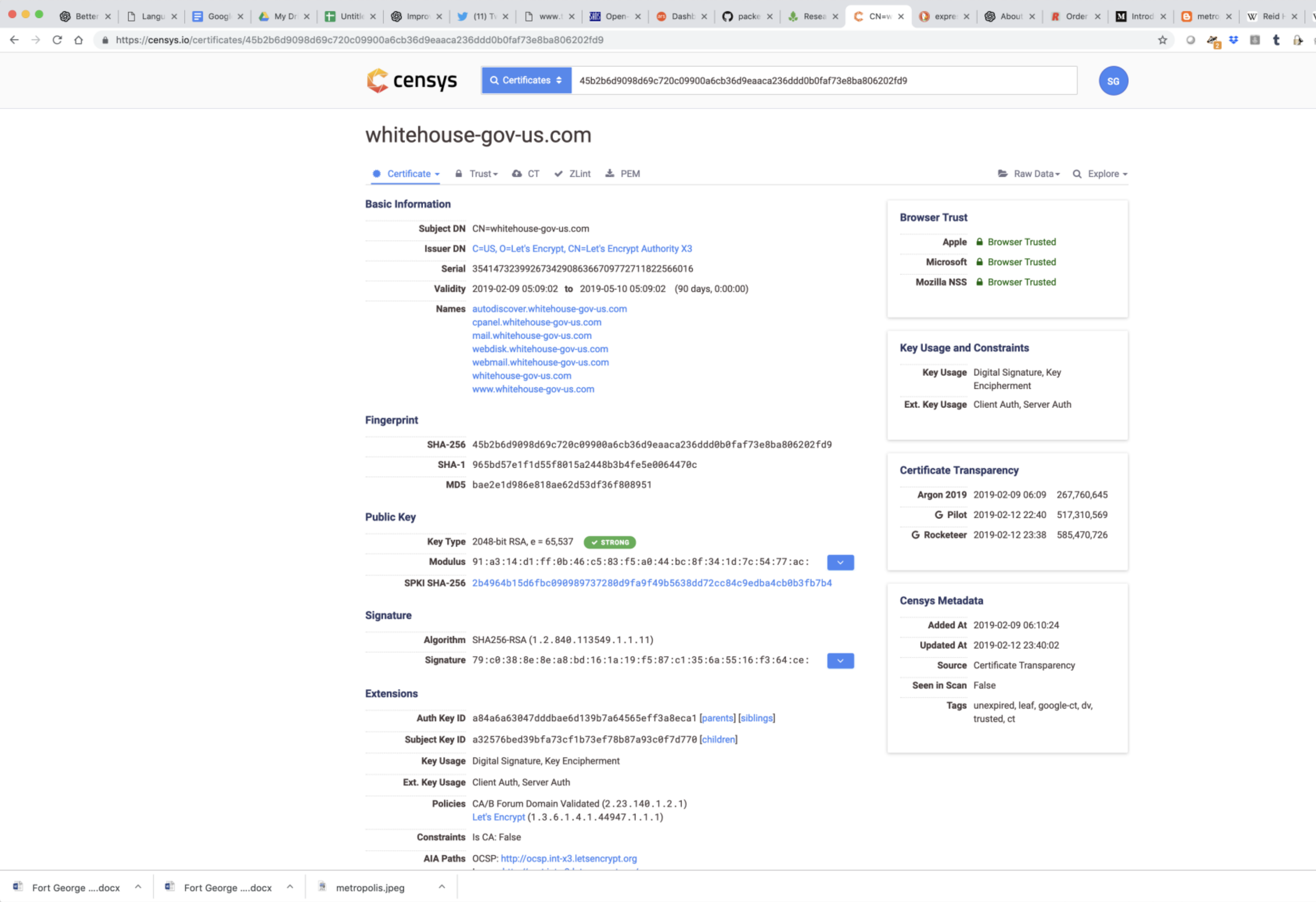
CN=whitehouse-gov-us.com
Let's Encrypt Authority X3
2019-02-09 – 2019-05-10
autodiscover.whitehouse-gov-us.com, cpanel.whitehouse-gov-us.com, mail.whitehouse-gov-us.com, webdisk.whitehouse-gov-us.com, ...

CN=whitehouse-gov-us.com
Let's Encrypt Authority X3
2018-12-10 – 2019-03-10
autodiscover.whitehouse-gov-us.com, cpanel.whitehouse-gov-us.com, mail.whitehouse-gov-us.com, webdisk.whitehouse-gov-us.com, ...

CN=whitehouse-gov-us.com
Let's Encrypt Authority X3
2018-12-10 – 2019-03-10
autodiscover.whitehouse-gov-us.com, cpanel.whitehouse-gov-us.com, mail.whitehouse-gov-us.com, webdisk.whitehouse-gov-us.com, ...

CN=whitehouse-gov-us.com
Let's Encrypt Authority X3
2018-10-09 – 2019-01-07
autodiscover.whitehouse-gov-us.com, cpanel.whitehouse-gov-us.com, mail.whitehouse-gov-us.com, webdisk.whitehouse-gov-us.com, ...

Targeted hunting in CTL: certificate history


https://censys.io/certificates/45b2b6d9098d69c720c09900a6cb36d9eaaca236ddd0b0faf73e8ba806202fd9
censys
Certificates
45b2b6d9098d69c720c09900a6cb36d9eaaca236ddd0b0faf73e8ba806202fd9
SG
Certificate
Trust
CT
ZLint
PEM
Raw Data
Explore
Fort George ....docx
Fort George ....docx
metropolis.jpeg

whitehouse-gov-us.com

Basic Information

Subject DN	CN=whitehouse-gov-us.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	354147323992673429086366709772711822566016
Validity	2019-02-09 05:09:02 to 2019-05-10 05:09:02 (90 days, 0:00:00)
Names	autodiscover.whitehouse-gov-us.com cpanel.whitehouse-gov-us.com mail.whitehouse-gov-us.com webdisk.whitehouse-gov-us.com webmail.whitehouse-gov-us.com whitehouse-gov-us.com www.whitehouse-gov-us.com

Fingerprint

SHA-256	45b2b6d9098d69c720c09900a6cb36d9eaaca236ddd0b0faf73e8ba806202fd9
SHA-1	965bd57e1f1d55f8015a2448b3b4fe5e0064470c
MD5	bae2e1d986e818ae62d53df36f808951

Public Key

Key Type	2048-bit RSA, e = 65,537 ✓ STRONG
Modulus	91:a3:14:d1:ff:0b:46:c5:83:f5:a0:44:bc:8f:34:1d:7c:54:77:ac:
SPKI SHA-256	2b4964b15d6fbc090989737280d9fa9f49b5638dd72cc84c9edba4cb0b3fb7b4

Signature

Algorithm	SHA256-RSA (1.2.840.113549.1.1.11)
Signature	79:c0:38:8e:8e:a8:bd:16:1a:19:f5:87:c1:35:6a:55:16:f3:64:ce:

Extensions

Auth Key ID	a84a6a63047dddbae6d139b7a64565eff3a8eca1 [parents] [siblings]
Subject Key ID	a32576bed39bfa73cf1b73ef78b87a93c0f7d770 [children]
Key Usage	Digital Signature, Key Encipherment
Ext. Key Usage	Client Auth, Server Auth
Policies	CA/B Forum Domain Validated (2.23.140.1.2.1) Let's Encrypt (1.3.6.1.4.1.44947.1.1.1)
Constraints	Is CA: False
AIA Paths	OCSP: http://ocsp.int-x3.letsencrypt.org

Browser Trust

Apple	🔒 Browser Trusted
Microsoft	🔒 Browser Trusted
Mozilla NSS	🔒 Browser Trusted

Key Usage and Constraints

Key Usage	Digital Signature, Key Encipherment
Ext. Key Usage	Client Auth, Server Auth

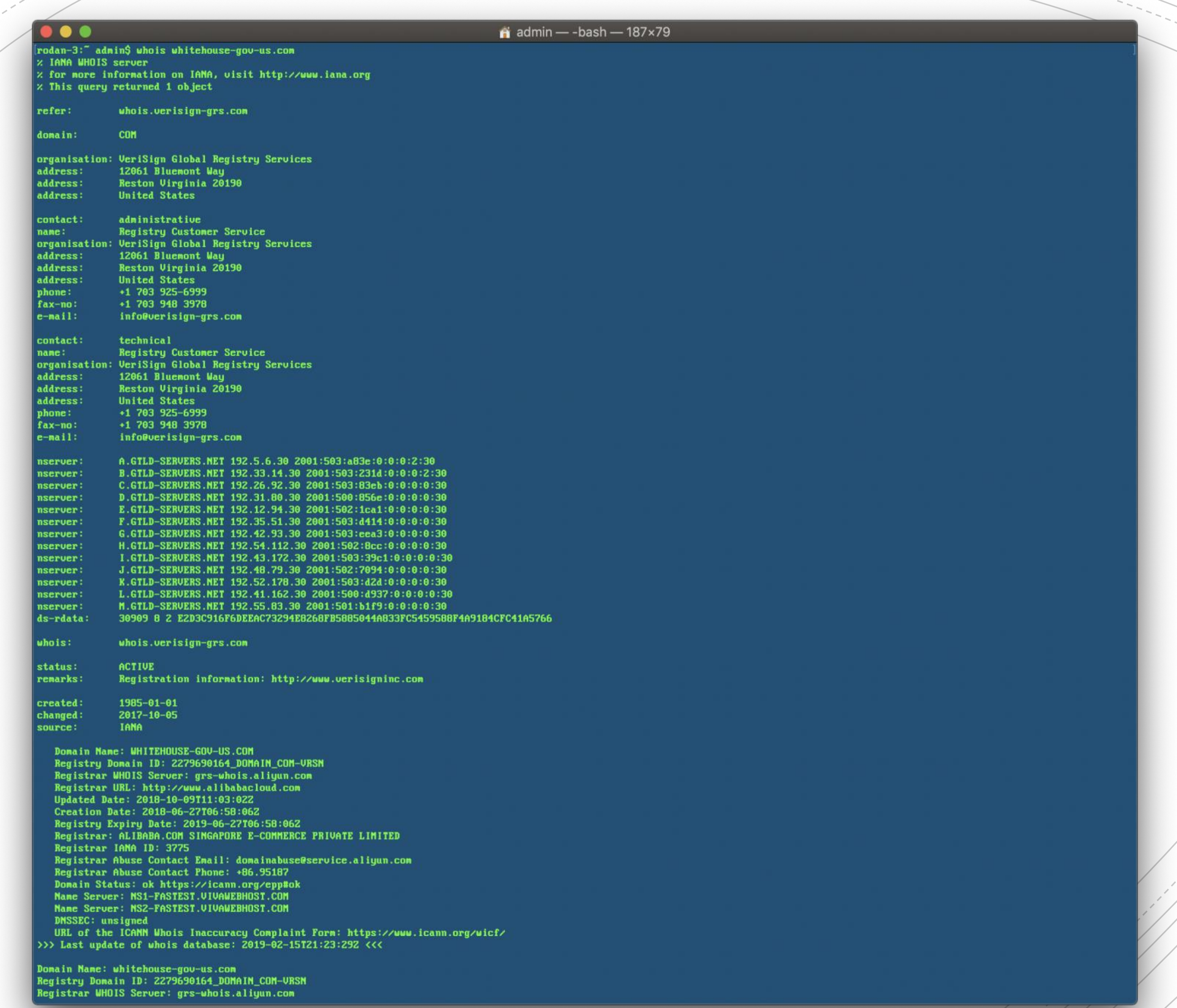
Certificate Transparency

Argon 2019	2019-02-09 06:09	267,760,645
G Pilot	2019-02-12 22:40	517,310,569
G Rocketeer	2019-02-12 23:38	585,470,726

Censys Metadata

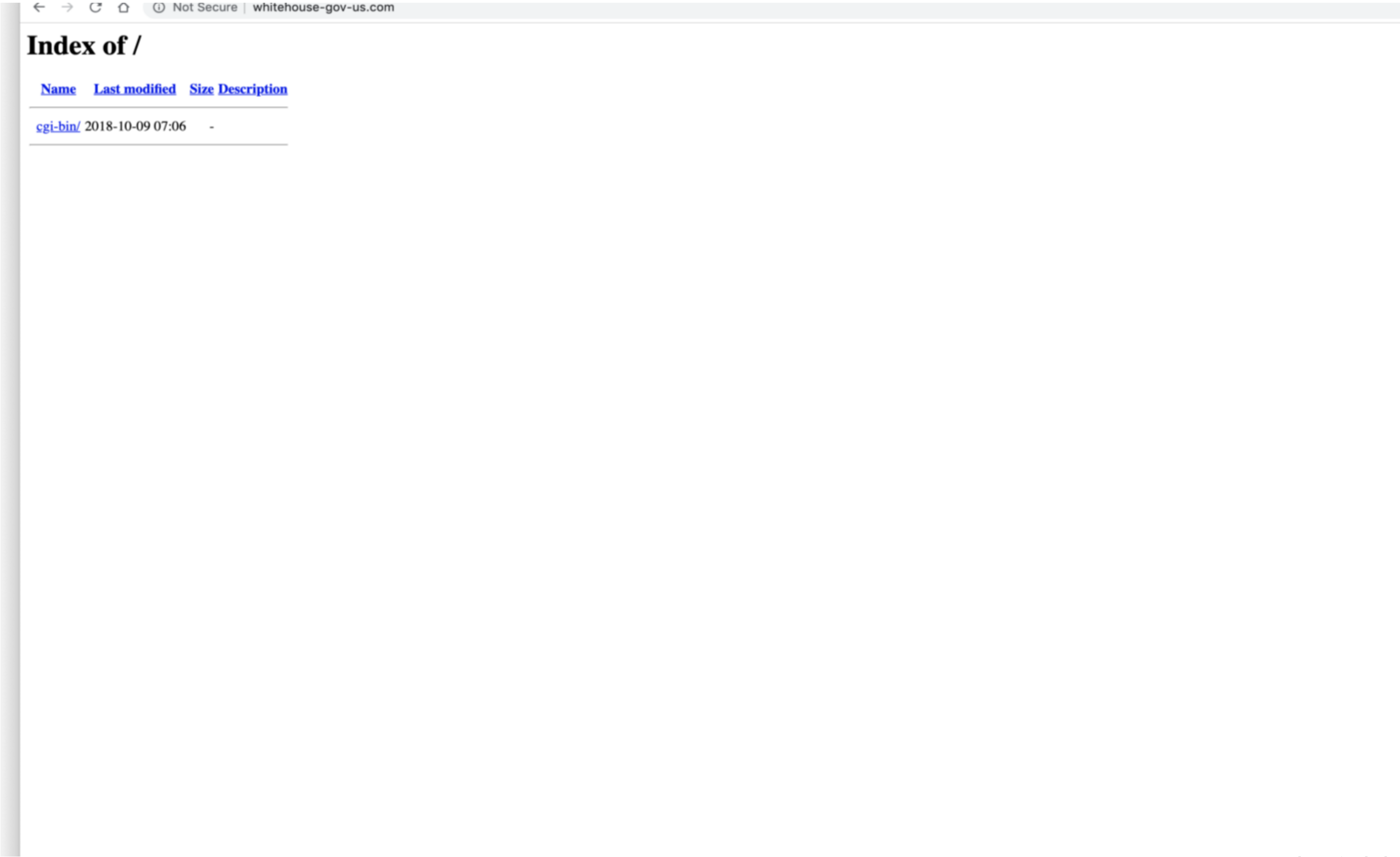
Added At	2019-02-09 06:10:24
Updated At	2019-02-12 23:40:02
Source	Certificate Transparency
Seen in Scan	False
Tags	unexpired, leaf, google-ct, dv, trusted, ct

Targeted hunting in CTL: whois



```
rodan-3:~ admin$ whois whitehouse-gov-us.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston Virginia 20190
address:      United States
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CFC41A5766

whois:        whois.verisign-grs.com

status:       ACTIVE
remarks:      Registration information: http://www.verisigninc.com

created:      1985-01-01
changed:      2017-10-05
source:       IANA

   Domain Name: WHITEHOUSE-GOV-US.COM
   Registry Domain ID: 2279690164_DOMAIN_COM-VRSN
   Registrar WHOIS Server: grs-whois.aliyun.com
   Registrar URL: http://www.alibabacloud.com
   Updated Date: 2018-10-09T11:03:02Z
   Creation Date: 2018-06-27T06:58:06Z
   Registry Expiry Date: 2019-06-27T06:58:06Z
   Registrar: ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED
   Registrar IANA ID: 3775
   Registrar Abuse Contact Email: domainabuse@service.aliyun.com
   Registrar Abuse Contact Phone: +86.95187
   Domain Status: ok https://icann.org/epp#ok
   Name Server: NS1-FASTEST.VIVAWEBHOST.COM
   Name Server: NS2-FASTEST.VIVAWEBHOST.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-02-15T21:23:29Z <<<

Domain Name: whitehouse-gov-us.com
Registry Domain ID: 2279690164_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.aliyun.com
```

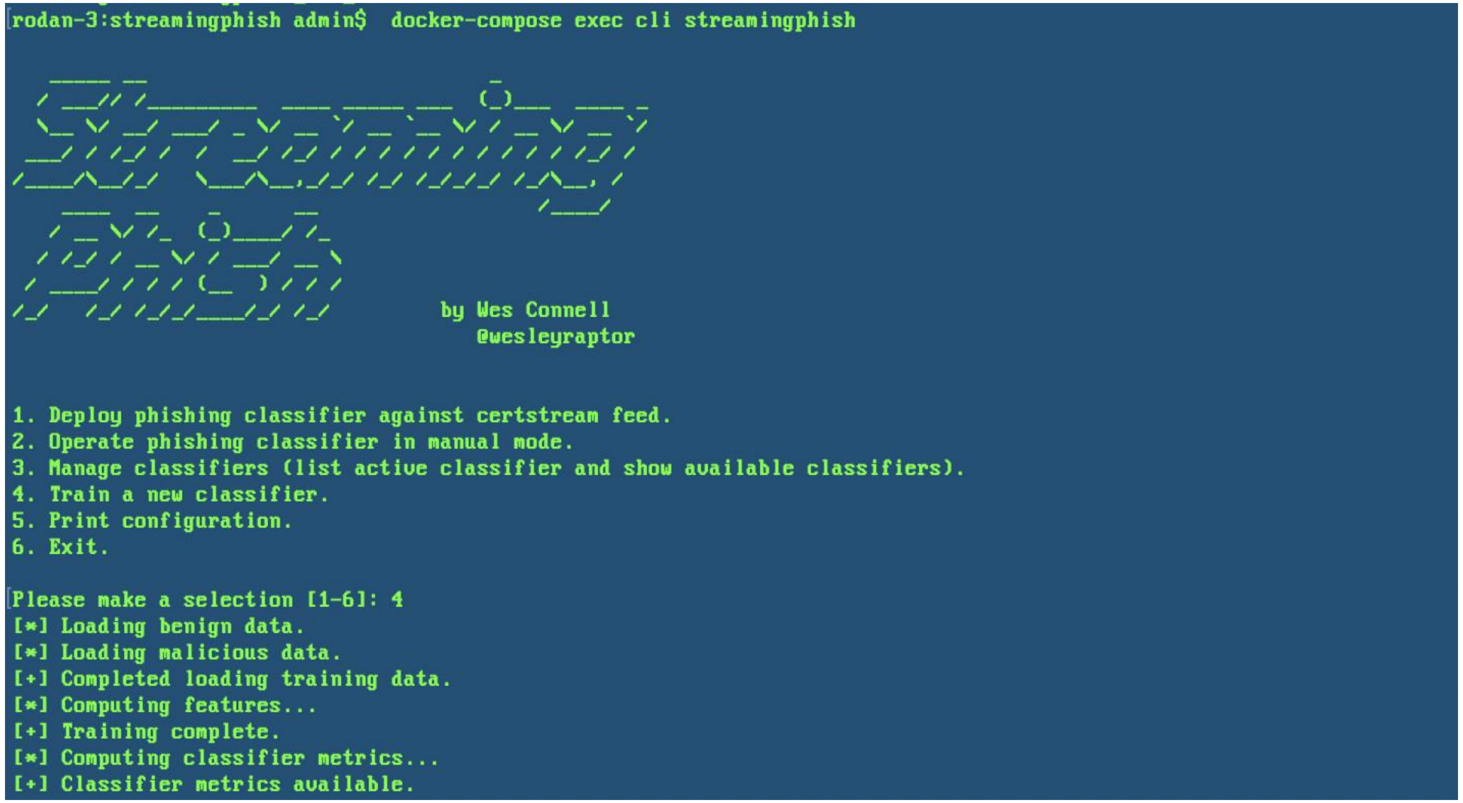
Targeted hunting in CTL: browsing/capture



Index of /

Name	Last modified	Size	Description
cgi-bin/	2018-10-09 07:06	-	

Using ML to scan: StreamingPhish

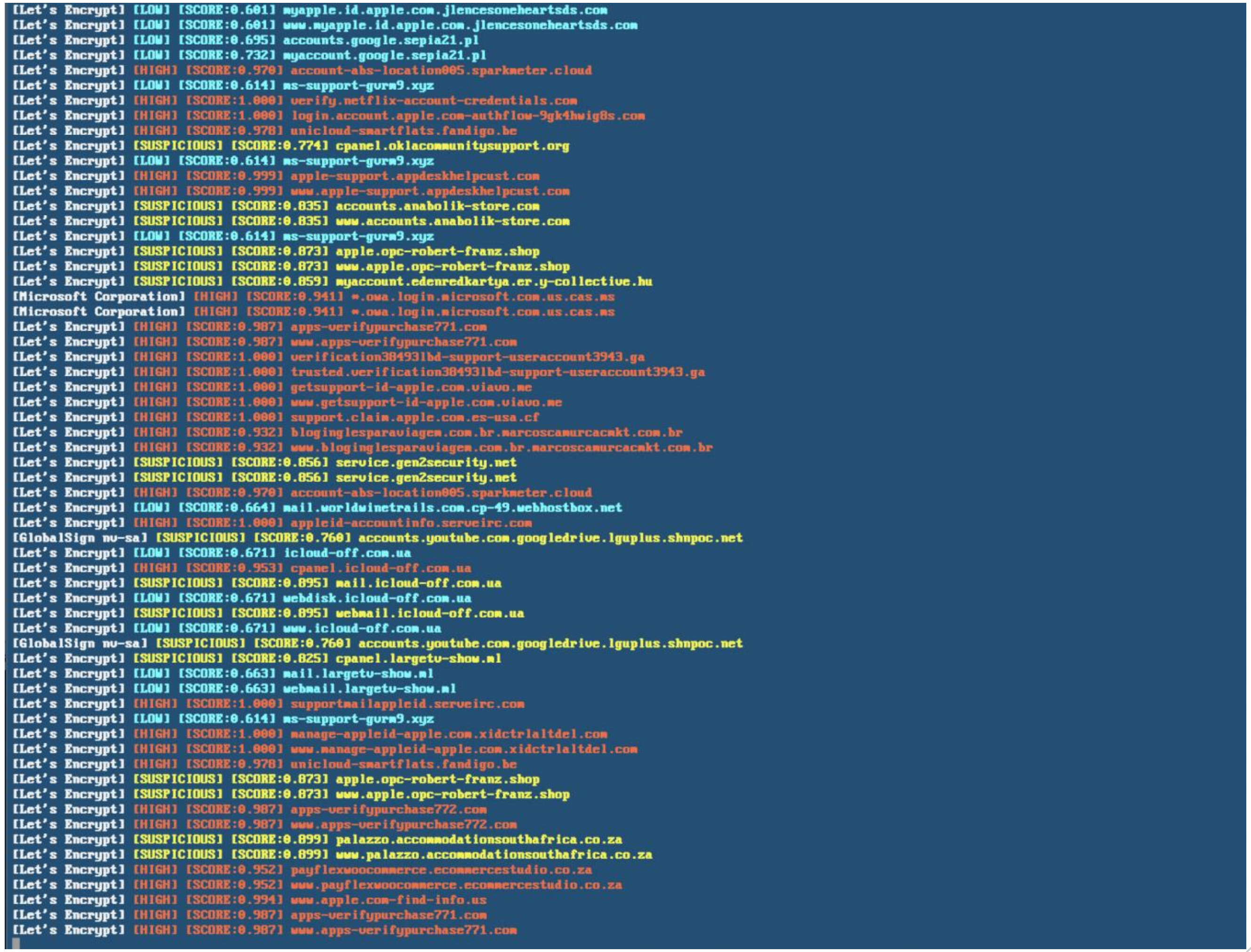


```
rodan-3:streamingphish admin$  docker-compose exec cli streamingphish

   _____ __                            _
  / ___// /_________  ____ _____ ___  (_)___  ____ _
  \__ \/ __/ ___/ _ \/ __ `/ __ `__ \/ / __ \/ __ `/
 ___/ / /_/ /  /  __/ /_/ / / / / / / / / / / /_/ /
/____/\__/_/   \___/\__,_/_/ /_/ /_/_/_/ /_/\__, /
                                           /____/
    ____  __    _      __
   / __ \/ /_  (_)____/ /_
  / /_/ / __ \/ / ___/ __ \
 / ____/ / / / (__  ) / / /
/_/   /_/ /_/_/____/_/ /_/          by Wes Connell
                                       @wesleyraptor


1. Deploy phishing classifier against certstream feed.
2. Operate phishing classifier in manual mode.
3. Manage classifiers (list active classifier and show available classifiers).
4. Train a new classifier.
5. Print configuration.
6. Exit.

Please make a selection [1-6]: 4
[*] Loading benign data.
[*] Loading malicious data.
[+] Completed loading training data.
[*] Computing features...
[+] Training complete.
[*] Computing classifier metrics...
[+] Classifier metrics available.
```

StreamingPhish

- StreamingPhish: https://github.com/wesleyraptor/streamingphish
- Wes Connell – works in threat detection at Uber- developed this ML tool
- Uses training sets of data, including brands and TLDs, and editable set of malicious domains- to build an algorithm to spot potentially malicious domains as they appear in certstream.
- Docker based, can run in cloud

StreamingPhish CLI output

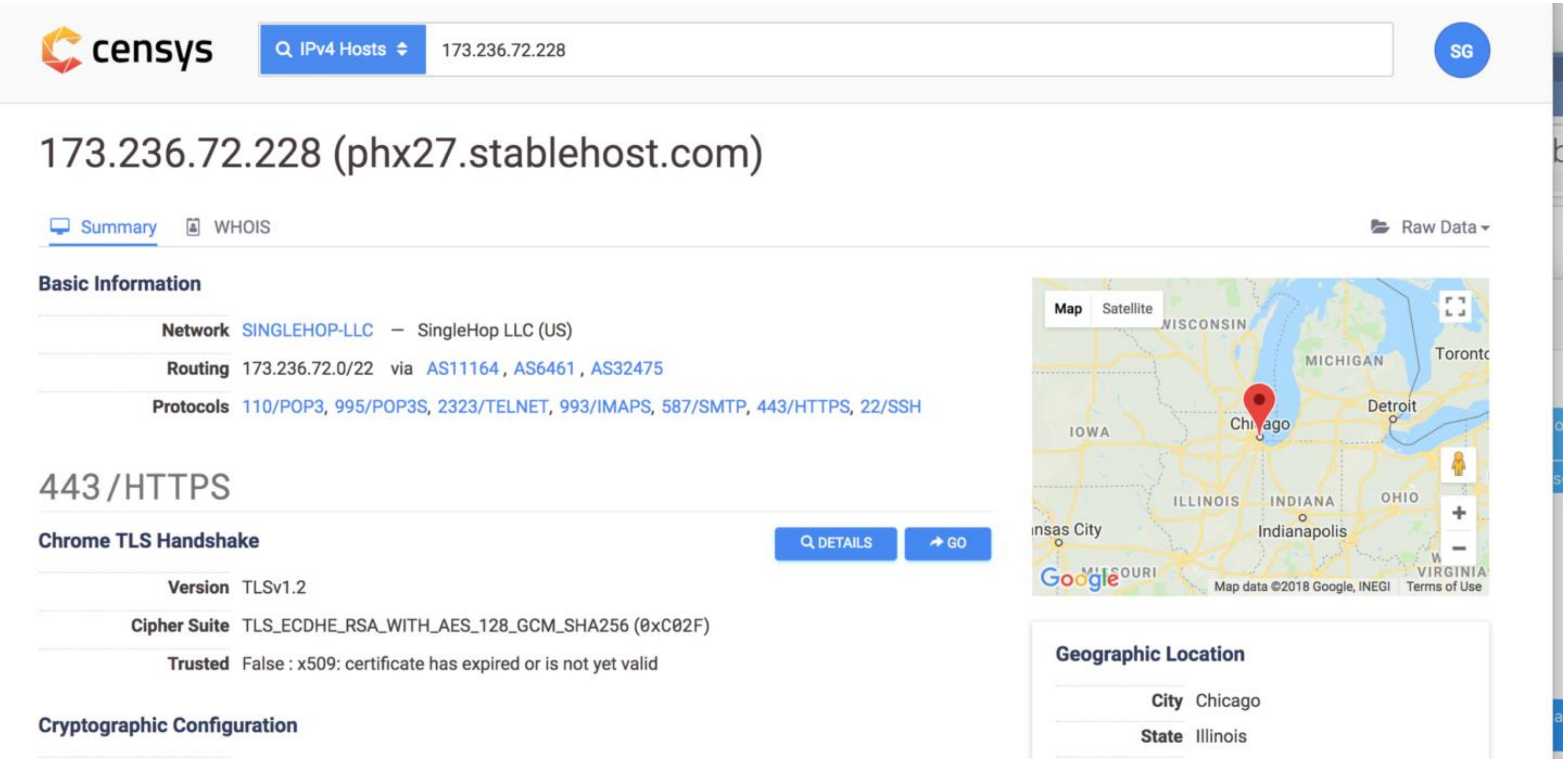


```
[Let's Encrypt] [LOW] [SCORE:0.601] myapple.id.apple.com.jlencesoneheartsds.com
[Let's Encrypt] [LOW] [SCORE:0.601] www.myapple.id.apple.com.jlencesoneheartsds.com
[Let's Encrypt] [LOW] [SCORE:0.695] accounts.google.sepia21.pl
[Let's Encrypt] [LOW] [SCORE:0.732] myaccount.google.sepia21.pl
[Let's Encrypt] [HIGH] [SCORE:0.970] account-abs-location005.sparkmeter.cloud
[Let's Encrypt] [LOW] [SCORE:0.614] ms-support-gvrm9.xyz
[Let's Encrypt] [HIGH] [SCORE:1.000] verify.netflix-account-credentials.com
[Let's Encrypt] [HIGH] [SCORE:1.000] login.account.apple.com-authflow-9gk4hwig8s.com
[Let's Encrypt] [HIGH] [SCORE:0.978] unicloud-smartflats.fandigo.be
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.774] cpanel.oklacommunitysupport.org
[Let's Encrypt] [LOW] [SCORE:0.614] ms-support-gvrm9.xyz
[Let's Encrypt] [HIGH] [SCORE:0.999] apple-support.appdeskhelpcust.com
[Let's Encrypt] [HIGH] [SCORE:0.999] www.apple-support.appdeskhelpcust.com
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.835] accounts.anabolik-store.com
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.835] www.accounts.anabolik-store.com
[Let's Encrypt] [LOW] [SCORE:0.614] ms-support-gvrm9.xyz
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.873] apple.opc-robert-franz.shop
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.873] www.apple.opc-robert-franz.shop
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.859] myaccount.edenredkartya.er.y-collective.hu
[Microsoft Corporation] [HIGH] [SCORE:0.941] *.owa.login.microsoft.com.us.cas.ms
[Microsoft Corporation] [HIGH] [SCORE:0.941] *.owa.login.microsoft.com.us.cas.ms
[Let's Encrypt] [HIGH] [SCORE:0.987] apps-verifypurchase771.com
[Let's Encrypt] [HIGH] [SCORE:0.987] www.apps-verifypurchase771.com
[Let's Encrypt] [HIGH] [SCORE:1.000] verification384931bd-support-useraccount3943.ga
[Let's Encrypt] [HIGH] [SCORE:1.000] trusted.verification384931bd-support-useraccount3943.ga
[Let's Encrypt] [HIGH] [SCORE:1.000] getsupport-id-apple.com.viavo.me
[Let's Encrypt] [HIGH] [SCORE:1.000] www.getsupport-id-apple.com.viavo.me
[Let's Encrypt] [HIGH] [SCORE:1.000] support.claim.apple.com.es-usa.cf
[Let's Encrypt] [HIGH] [SCORE:0.932] bloginglesparaviagem.com.br.marcoscamurcacmkt.com.br
[Let's Encrypt] [HIGH] [SCORE:0.932] www.bloginglesparaviagem.com.br.marcoscamurcacmkt.com.br
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.856] service.gen2security.net
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.856] service.gen2security.net
[Let's Encrypt] [HIGH] [SCORE:0.970] account-abs-location005.sparkmeter.cloud
[Let's Encrypt] [LOW] [SCORE:0.664] mail.worldwinetrails.com.cp-49.webhostbox.net
[Let's Encrypt] [HIGH] [SCORE:1.000] appleid-accountinfo.serveirc.com
[GlobalSign nv-sa] [SUSPICIOUS] [SCORE:0.760] accounts.youtube.com.googledrive.lguplus.shnpoc.net
[Let's Encrypt] [LOW] [SCORE:0.671] icloud-off.com.ua
[Let's Encrypt] [HIGH] [SCORE:0.953] cpanel.icloud-off.com.ua
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.895] mail.icloud-off.com.ua
[Let's Encrypt] [LOW] [SCORE:0.671] webdisk.icloud-off.com.ua
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.895] webmail.icloud-off.com.ua
[Let's Encrypt] [LOW] [SCORE:0.671] www.icloud-off.com.ua
[GlobalSign nv-sa] [SUSPICIOUS] [SCORE:0.760] accounts.youtube.com.googledrive.lguplus.shnpoc.net
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.825] cpanel.largetv-show.ml
[Let's Encrypt] [LOW] [SCORE:0.663] mail.largetv-show.ml
[Let's Encrypt] [LOW] [SCORE:0.663] webmail.largetv-show.ml
[Let's Encrypt] [HIGH] [SCORE:1.000] supportmailappleid.serveirc.com
[Let's Encrypt] [LOW] [SCORE:0.614] ms-support-gvrm9.xyz
[Let's Encrypt] [HIGH] [SCORE:1.000] manage-appleid-apple.com.xidctrlaltdel.com
[Let's Encrypt] [HIGH] [SCORE:1.000] www.manage-appleid-apple.com.xidctrlaltdel.com
[Let's Encrypt] [HIGH] [SCORE:0.978] unicloud-smartflats.fandigo.be
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.873] apple.opc-robert-franz.shop
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.873] www.apple.opc-robert-franz.shop
[Let's Encrypt] [HIGH] [SCORE:0.987] apps-verifypurchase772.com
[Let's Encrypt] [HIGH] [SCORE:0.987] www.apps-verifypurchase772.com
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.899] palazzo.accommodationsouthafrica.co.za
[Let's Encrypt] [SUSPICIOUS] [SCORE:0.899] www.palazzo.accommodationsouthafrica.co.za
[Let's Encrypt] [HIGH] [SCORE:0.952] payflexwoocommerce.ecommercestudio.co.za
[Let's Encrypt] [HIGH] [SCORE:0.952] www.payflexwoocommerce.ecommercestudio.co.za
[Let's Encrypt] [HIGH] [SCORE:0.994] www.apple.com-find-info.us
[Let's Encrypt] [HIGH] [SCORE:0.987] apps-verifypurchase771.com
[Let's Encrypt] [HIGH] [SCORE:0.987] www.apps-verifypurchase771.com
```

Next steps and further automation

- Censys Whois dig, DomainTools, SecurityTrails, ViewDNSinfo
  - Neighboring IPs
  - Additional domains at host
- Kit and shell hunting
- Lookout is automating the rest of kill chain with ML – download kits, analyze screens, block

Digging for phish: Censys Whois Dig



173.236.72.228

173.236.72.228 (phx27.stablehost.com)

Basic Information

Network SINGLEHOP-LLC — SingleHop LLC (US)

Routing 173.236.72.0/22 via AS11164 , AS6461 , AS32475

Protocols 110/POP3, 995/POP3S, 2323/TELNET, 993/IMAPS, 587/SMTP, 443/HTTPS, 22/SSH

443/HTTPS

Chrome TLS Handshake

Version TLSv1.2

Cipher Suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)

Trusted False : x509: certificate has expired or is not yet valid

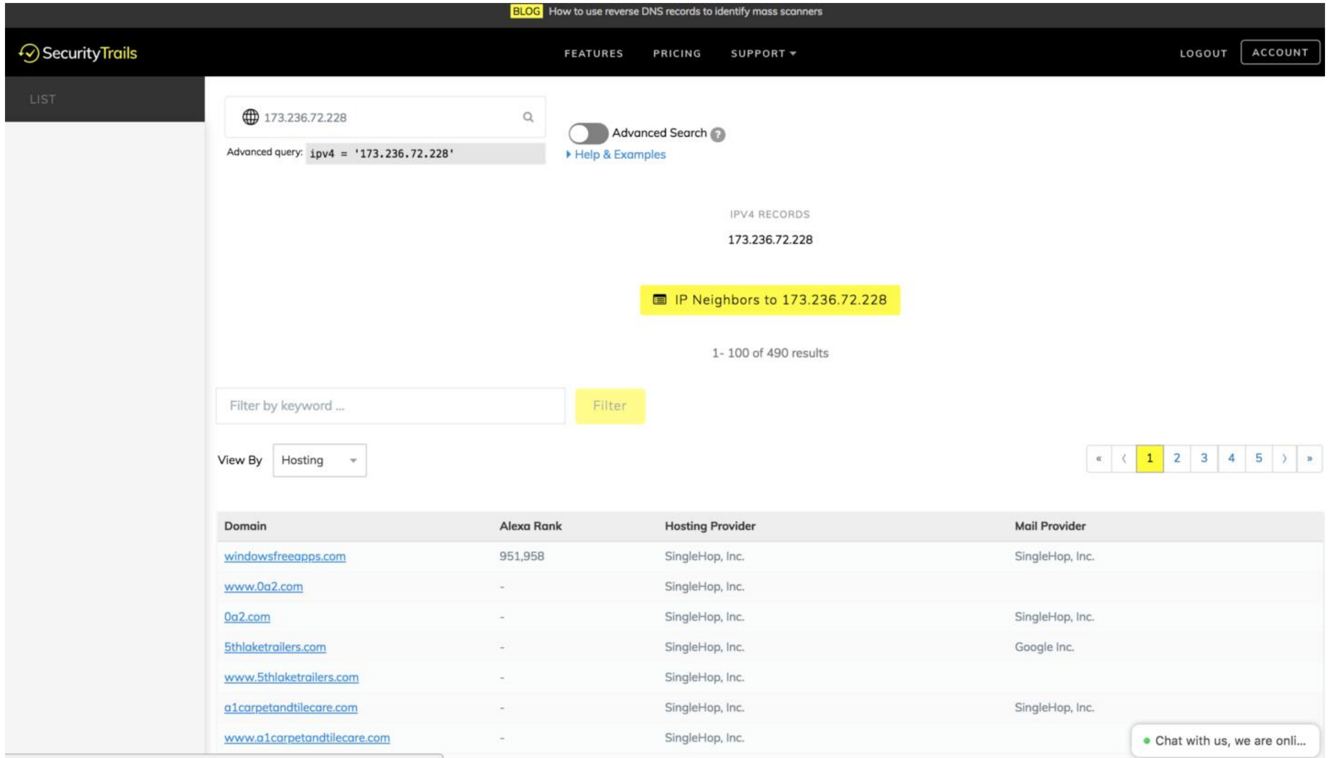
Cryptographic Configuration

Geographic Location

City Chicago

State Illinois

Digging for phish: SecurityTrails



173.236.72.228

Advanced query: `ipv4 = '173.236.72.228'`

IPV4 RECORDS

173.236.72.228

IP Neighbors to 173.236.72.228

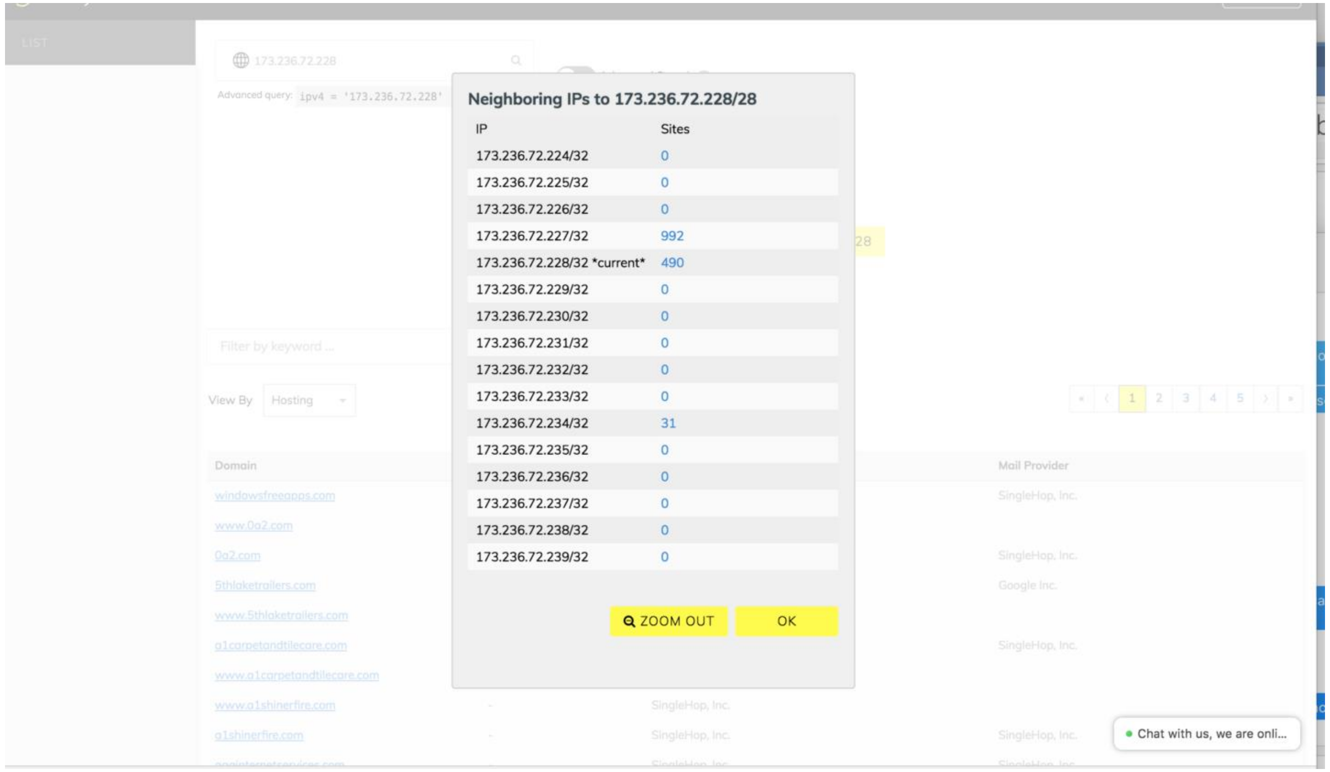
1- 100 of 490 results

Filter by keyword ...

View By Hosting

Domain	Alexa Rank	Hosting Provider	Mail Provider
windowsfreeapps.com	951,958	SingleHop, Inc.	SingleHop, Inc.
www.0a2.com	-	SingleHop, Inc.	
0a2.com	-	SingleHop, Inc.	SingleHop, Inc.
5thlaketrailers.com	-	SingleHop, Inc.	Google Inc.
www.5thlaketrailers.com	-	SingleHop, Inc.	
a1carpetandtilecare.com	-	SingleHop, Inc.	SingleHop, Inc.
www.a1carpetandtilecare.com	-	SingleHop, Inc.	

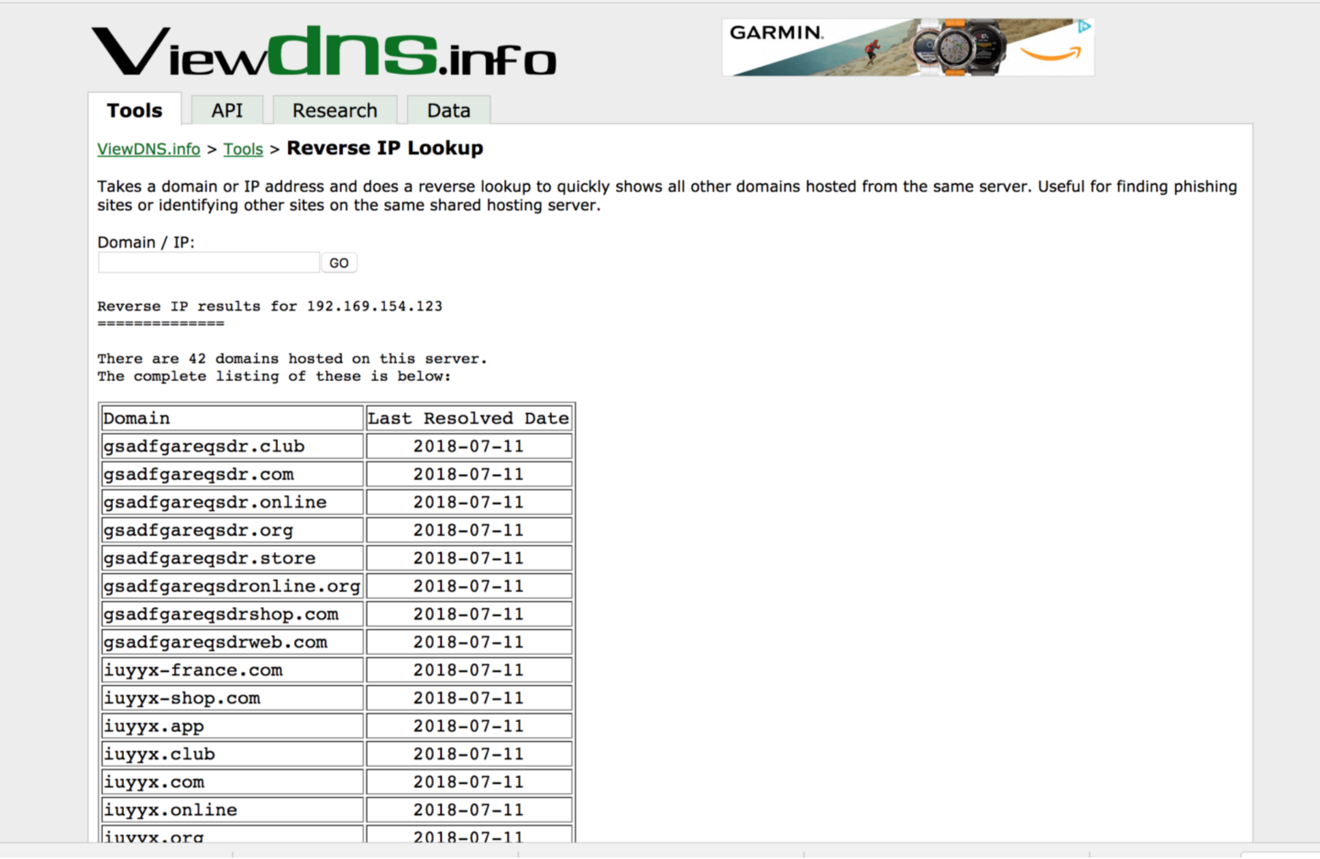
Digging for phish: SecurityTrails



Neighboring IPs to 173.236.72.228/28

IP	Sites
173.236.72.224/32	0
173.236.72.225/32	0
173.236.72.226/32	0
173.236.72.227/32	992
173.236.72.228/32 *current*	490
173.236.72.229/32	0
173.236.72.230/32	0
173.236.72.231/32	0
173.236.72.232/32	0
173.236.72.233/32	0
173.236.72.234/32	31
173.236.72.235/32	0
173.236.72.236/32	0
173.236.72.237/32	0
173.236.72.238/32	0
173.236.72.239/32	0

Digging for phish: ViewDNS.info



ViewDNS.info > Tools > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.

Domain / IP:

```
Reverse IP results for 192.169.154.123
==============

There are 42 domains hosted on this server.
The complete listing of these is below:
```

Domain	Last Resolved Date
gsadfgareqsdr.club	2018-07-11
gsadfgareqsdr.com	2018-07-11
gsadfgareqsdr.online	2018-07-11
gsadfgareqsdr.org	2018-07-11
gsadfgareqsdr.store	2018-07-11
gsadfgareqsdronline.org	2018-07-11
gsadfgareqsdrshop.com	2018-07-11
gsadfgareqsdrweb.com	2018-07-11
iuyyx-france.com	2018-07-11
iuyyx-shop.com	2018-07-11
iuyyx.app	2018-07-11
iuyyx.club	2018-07-11
iuyyx.com	2018-07-11
iuyyx.online	2018-07-11
iuyyx.org	2018-07-11

Questions?

- Email: sean.gallagher@arstechnica.com
- Sample kits found: https://github.com/packetrat/phishing-kits-I-found
- Twitter: @thepacketrat