Digital Security

H_D

REcon 2019

Digital Security

Leading information security services provider

870+ clients

1802 projects

ТАСС ФОСАГРО ВТБ24 mail.ru group МТС

ГАЗПРОМ QIWI LEROY MERLIN

16 years in information security

1300 vulnerabilities found in 2018

Acknowledgments

Adobe APACHE hp Microsoft vmware SAP ORACLE cisco

75 research papers

100+ experts

19 industries

- Software development
- Banks and finance
- Transport and logistics
- Production
- Energy
- Telecom
- Retail
- Media
- Blockchain, etc.

165 talks at international conferences

HITB
CONFidence

DEFCON
BlackHat

YSTS
RSA

CONFidence
Infosec in the City ...

Who dat boy?

- Twitter: @hd_421
- Pentester @Digital Security
- SynAck Red Team member
- Bug hunter (Yandex, Mail.ru, Kyivstar, QIWI, Unity)
- Sometimes a speaker (PHDays, ZeroNights, Revuln)

Agenda

- What is Recon/OSINT
- Internal & External scope
- Discovering IP Space
- Diff between Red Team Ops and Penetration testers
- Search engines for hackers
- Good ol’ bruteforce
- Lookup popular 3rd party cloud storages
- Mitigations

Cat Food

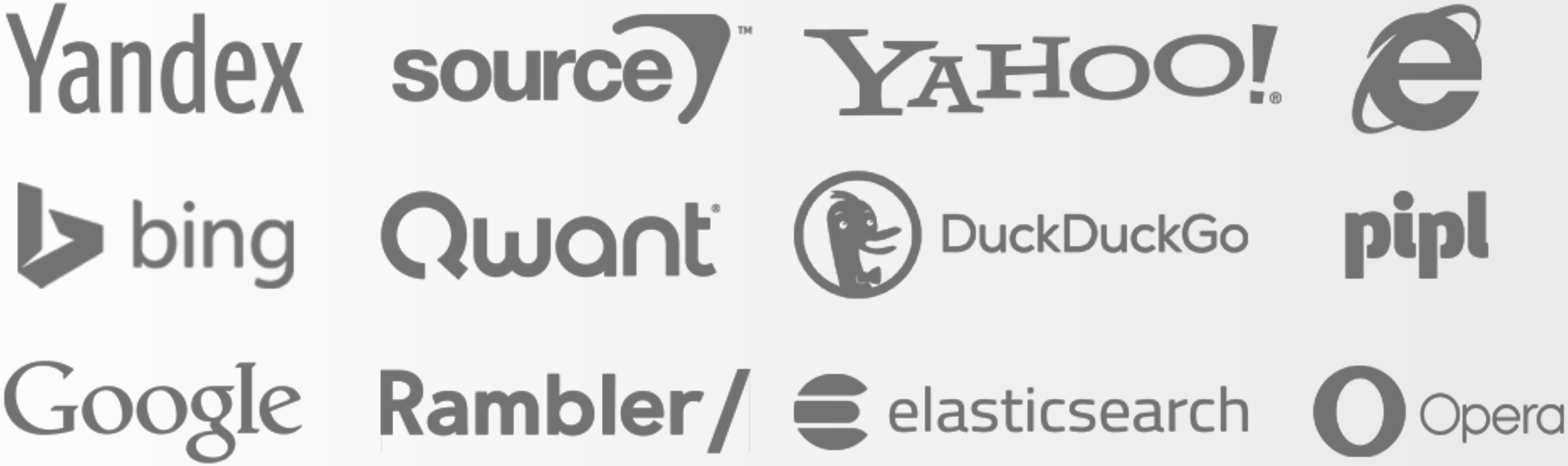
Dog Food

Food for you

Conclusion

- Don’t re-invent the wheel
- Understand whole cycle of automated work
- Improve what exist
- Don’t be a script kiddie

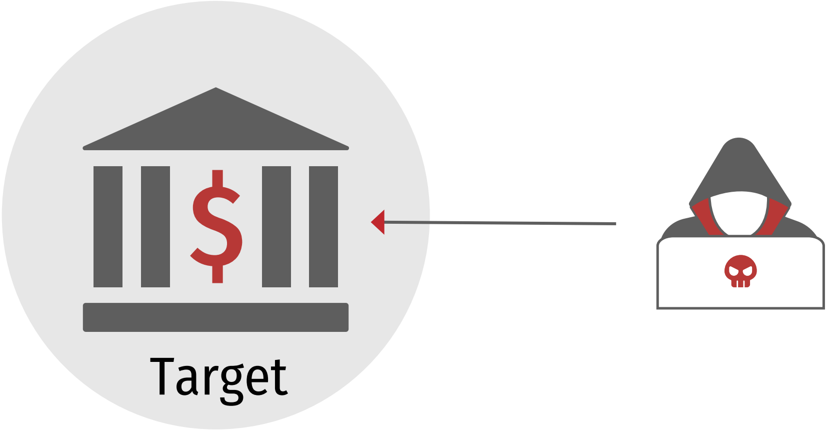
OSINT


Yandex
source™
YAHOO!®
bing
Qwant®
DuckDuckGo
pipl
Google
Rambler/
elasticsearch
Opera

Recon

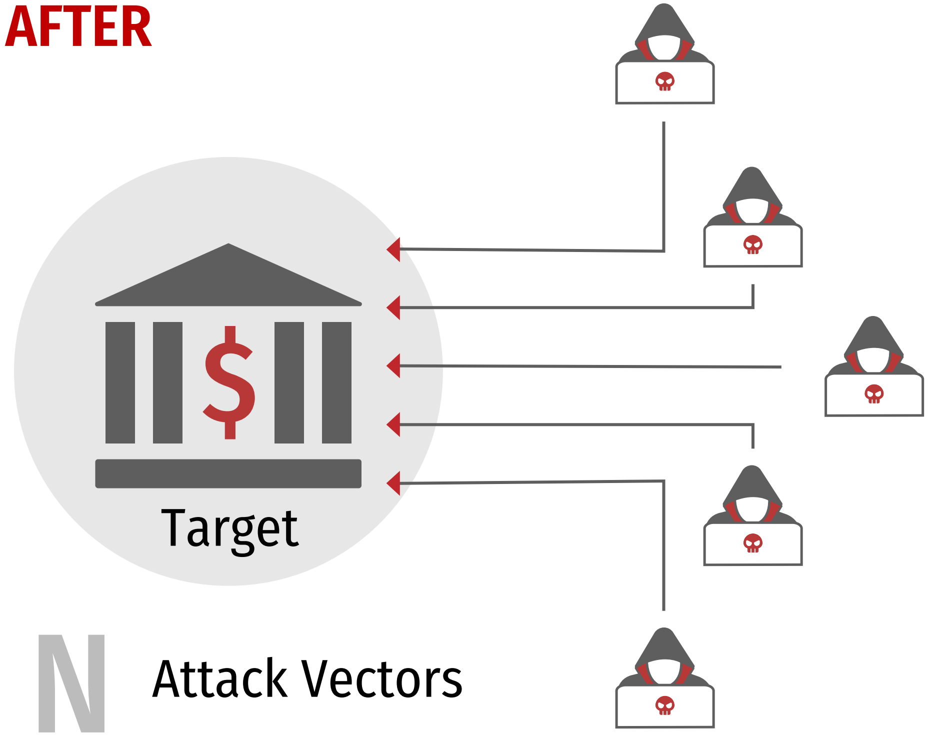
Why should we care about it?

BEFORE



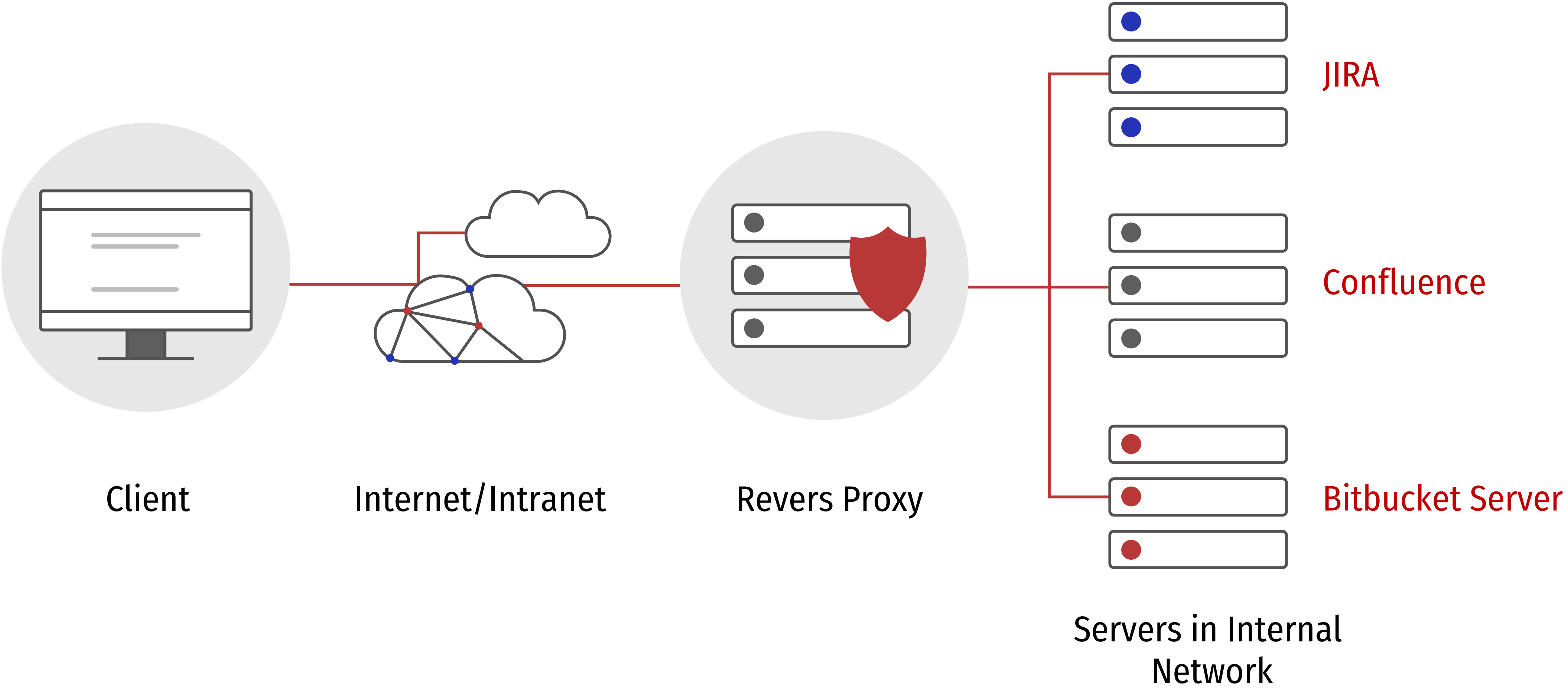
1 Attack Vector

AFTER



N Attack Vectors

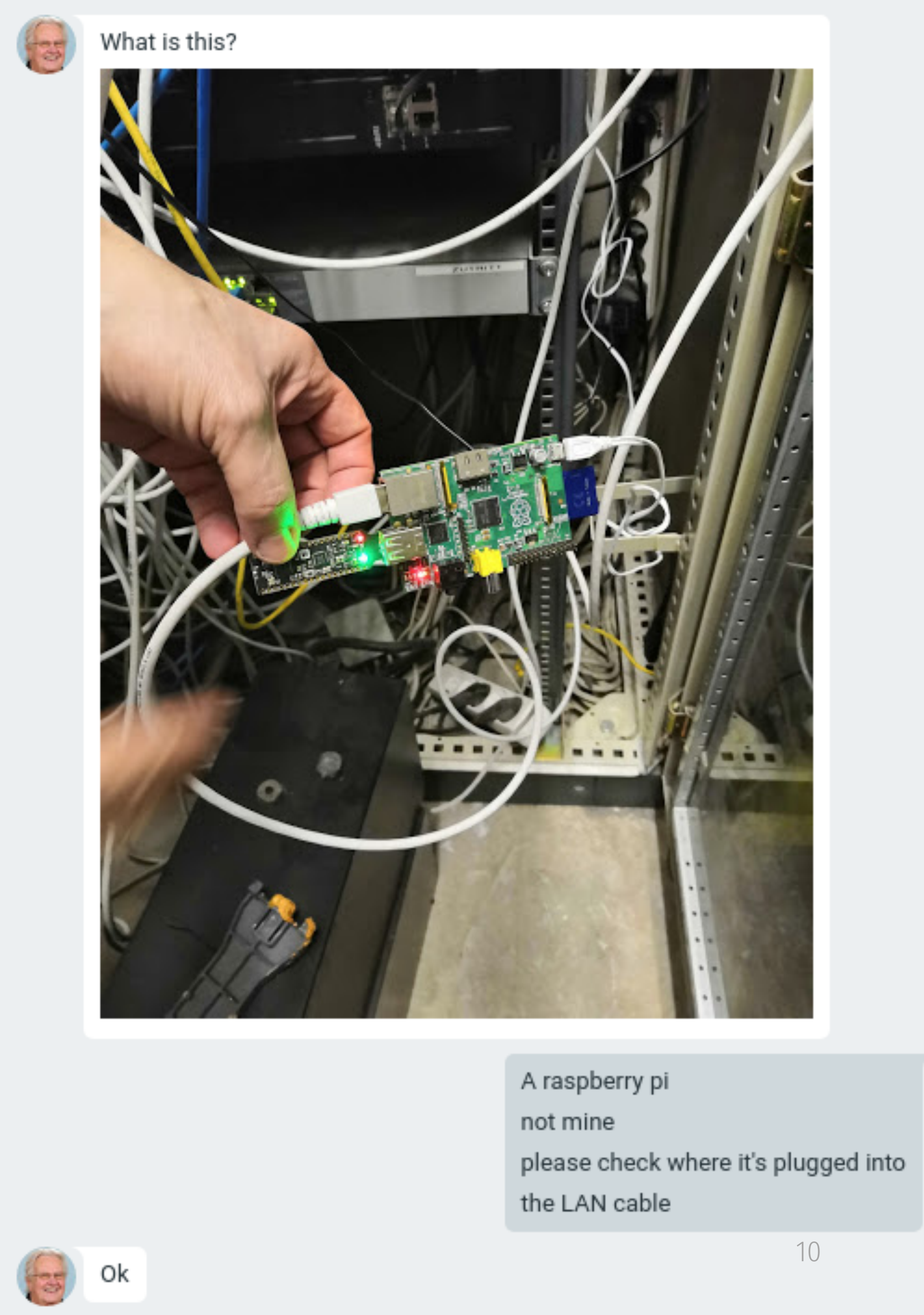
External Scope vs. Internal Scope



Adversary models

Internal adversary:

- Knows how the system works
- Experienced user
- Familiar with processes and lifecycles inside the company



What is this?

A raspberry pi
not mine
please check where it's plugged into
the LAN cable

Ok

Adversary models

External adversary:

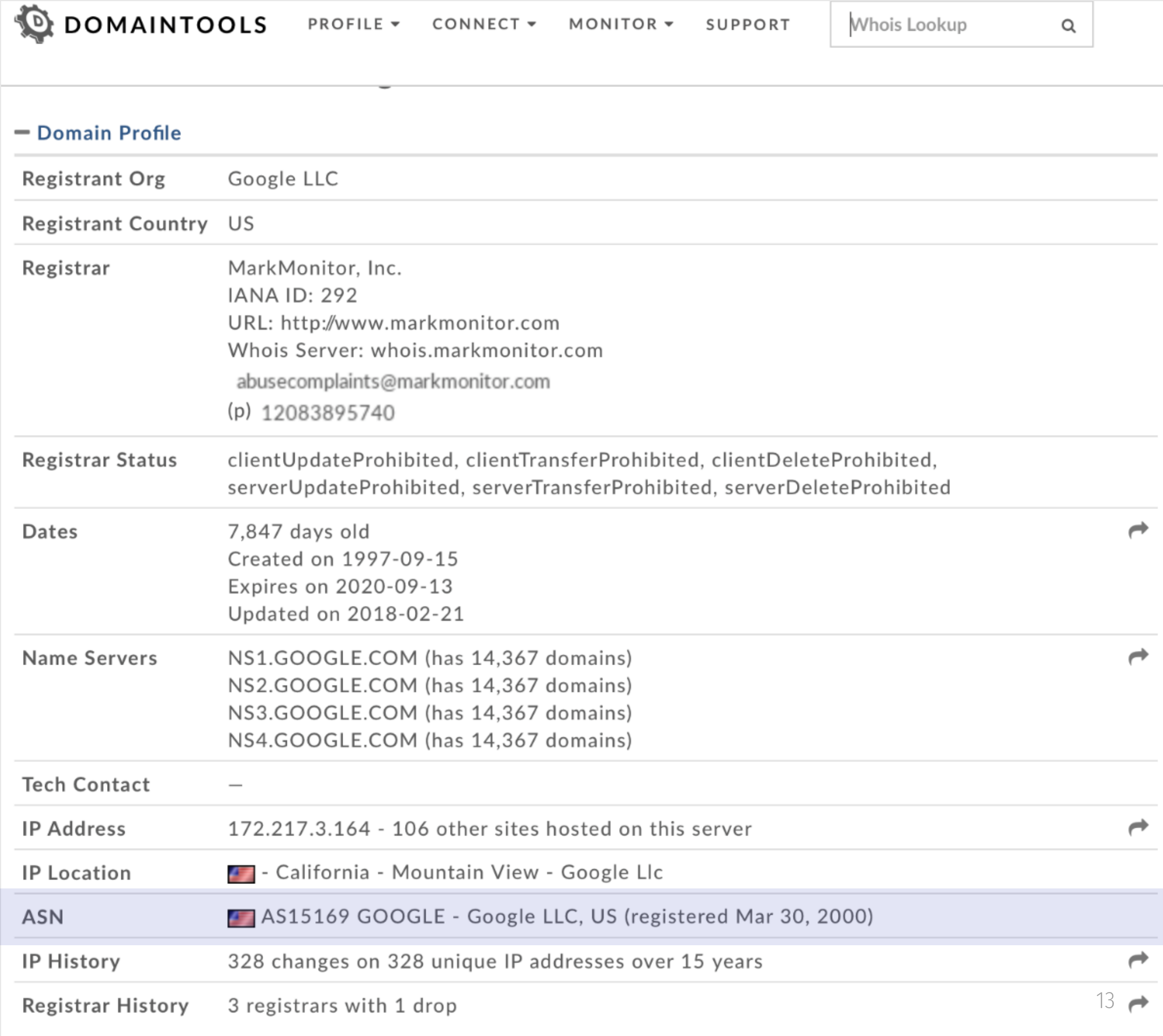
- Knows only things they have found
- Relies on their background skills
- Forced to spend time studying the system

IF THE EMPEROR KNEW LUKE COULD TARGET WOMP RATS, MAYBE HE WOULD HAVE PROTECTED HIS EXHAUST PORT.

Lets go

Our main target is maximum coverage of given asset. But what is our entry point?

Who is



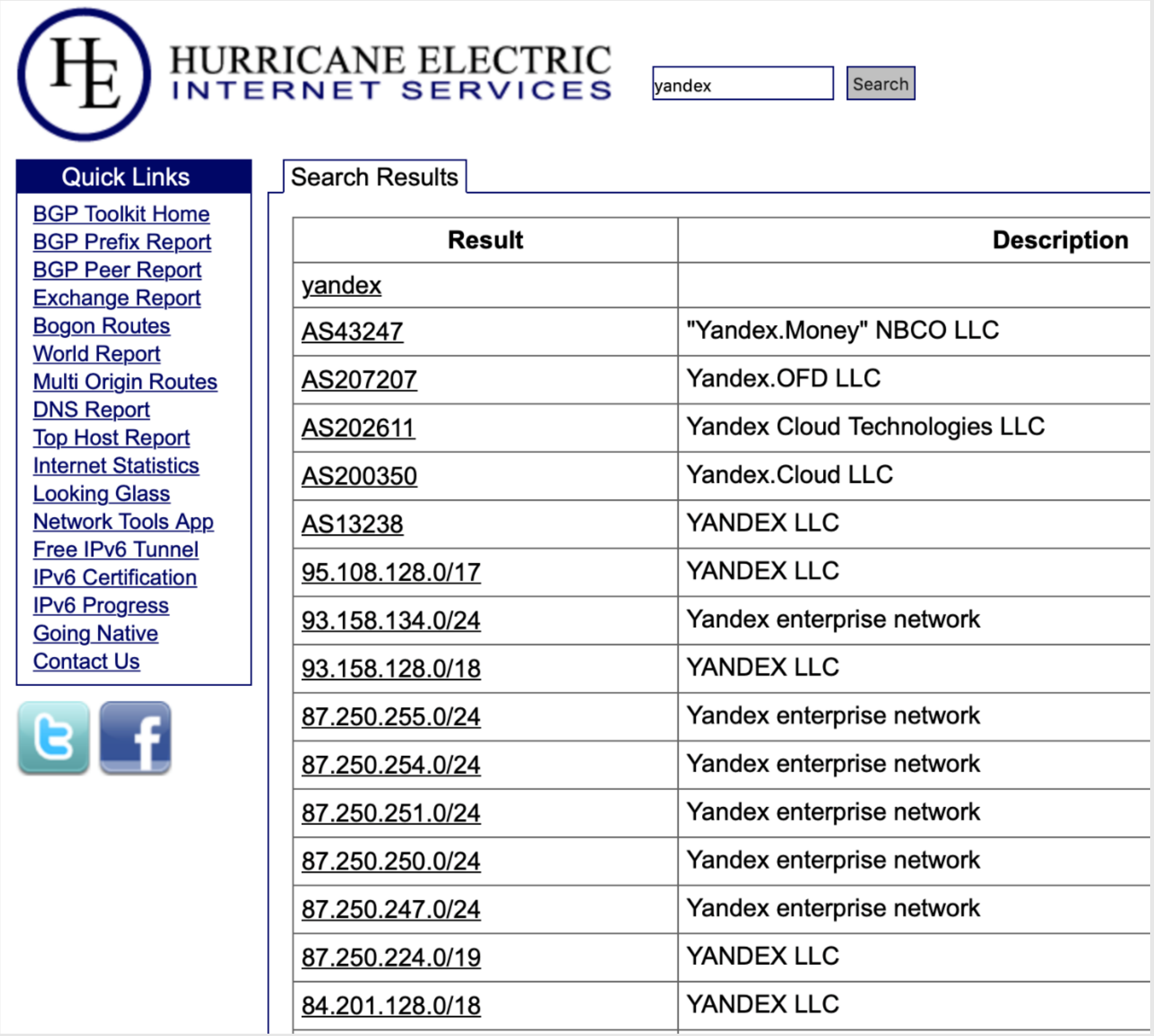
— Domain Profile

Registrant Org	Google LLC
Registrant Country	US
Registrar	MarkMonitor, Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895740
Registrar Status	clientUpdateProhibited, clientTransferProhibited, clientDeleteProhibited, serverUpdateProhibited, serverTransferProhibited, serverDeleteProhibited
Dates	7,847 days old Created on 1997-09-15 Expires on 2020-09-13 Updated on 2018-02-21
Name Servers	NS1.GOOGLE.COM (has 14,367 domains) NS2.GOOGLE.COM (has 14,367 domains) NS3.GOOGLE.COM (has 14,367 domains) NS4.GOOGLE.COM (has 14,367 domains)
Tech Contact	—
IP Address	172.217.3.164 - 106 other sites hosted on this server
IP Location	- California - Mountain View - Google Llc
ASN	AS15169 GOOGLE - Google LLC, US (registered Mar 30, 2000)
IP History	328 changes on 328 unique IP addresses over 15 years
Registrar History	3 registrars with 1 drop

☑

Autonomus System

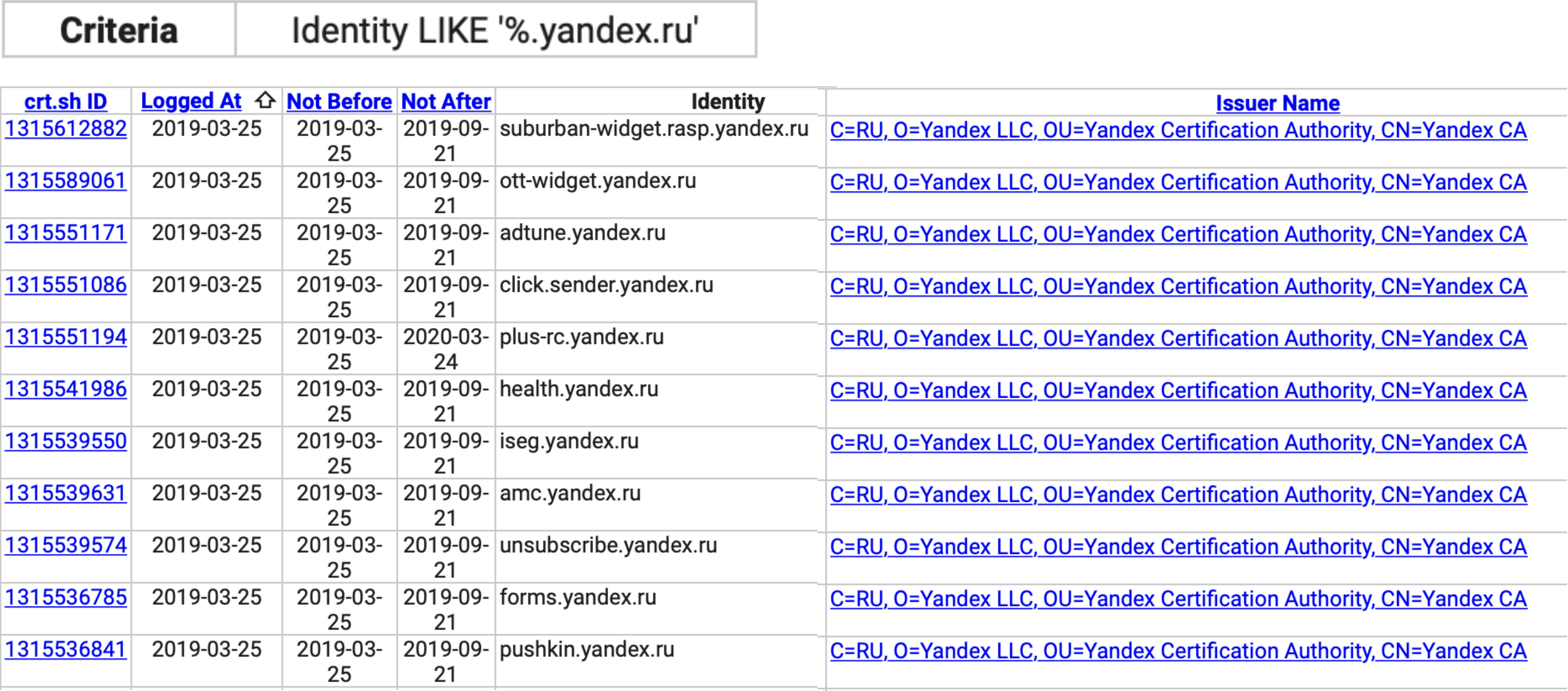
https://bgp.he.net



Result	Description
yandex	
AS43247	"Yandex.Money" NBCO LLC
AS207207	Yandex.OFD LLC
AS202611	Yandex Cloud Technologies LLC
AS200350	Yandex.Cloud LLC
AS13238	YANDEX LLC
95.108.128.0/17	YANDEX LLC
93.158.134.0/24	Yandex enterprise network
93.158.128.0/18	YANDEX LLC
87.250.255.0/24	Yandex enterprise network
87.250.254.0/24	Yandex enterprise network
87.250.251.0/24	Yandex enterprise network
87.250.250.0/24	Yandex enterprise network
87.250.247.0/24	Yandex enterprise network
87.250.224.0/19	YANDEX LLC
84.201.128.0/18	YANDEX LLC

Certificates

https://crt.sh

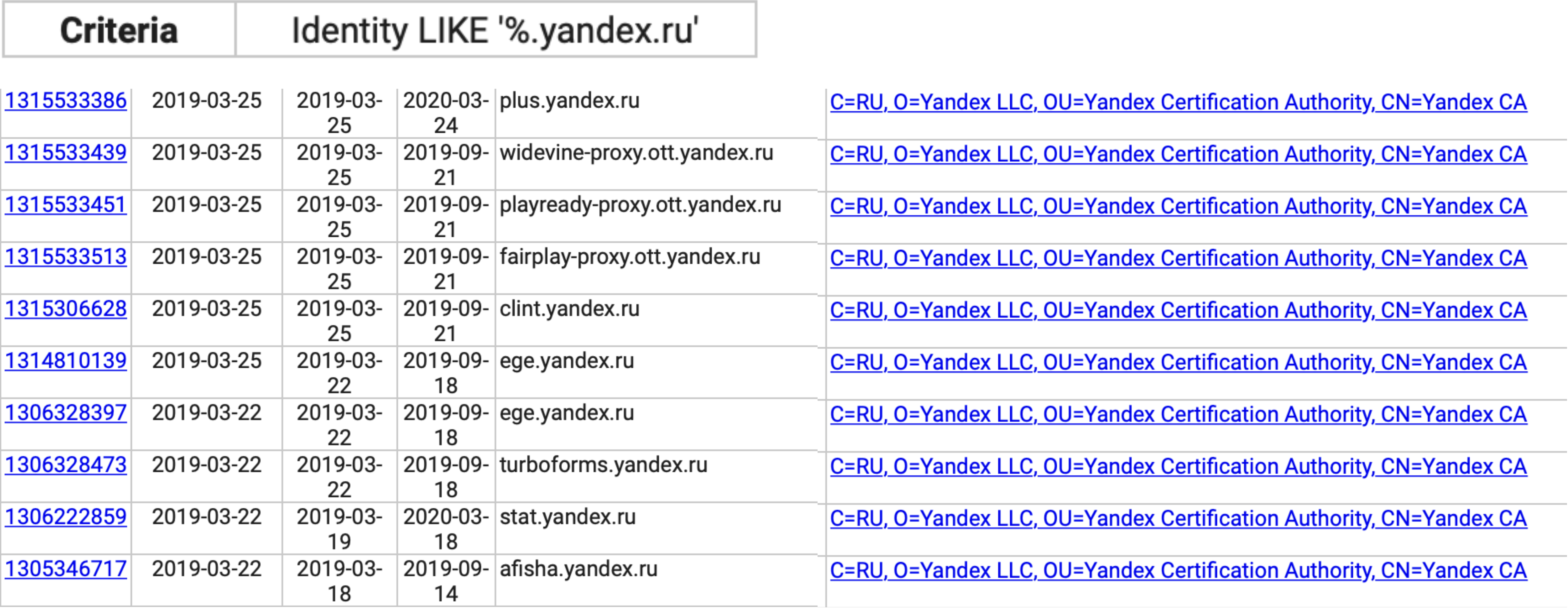


Criteria	Identity LIKE '%.yandex.ru'

crt.sh ID	Logged At ⇧	Not Before	Not After	Identity	Issuer Name
1315612882	2019-03-25	2019-03-25	2019-09-21	suburban-widget.rasp.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315589061	2019-03-25	2019-03-25	2019-09-21	ott-widget.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315551171	2019-03-25	2019-03-25	2019-09-21	adtune.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315551086	2019-03-25	2019-03-25	2019-09-21	click.sender.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315551194	2019-03-25	2019-03-25	2020-03-24	plus-rc.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315541986	2019-03-25	2019-03-25	2019-09-21	health.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315539550	2019-03-25	2019-03-25	2019-09-21	iseg.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315539631	2019-03-25	2019-03-25	2019-09-21	amc.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315539574	2019-03-25	2019-03-25	2019-09-21	unsubscribe.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315536785	2019-03-25	2019-03-25	2019-09-21	forms.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315536841	2019-03-25	2019-03-25	2019-09-21	pushkin.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA

Certificates

https://crt.sh

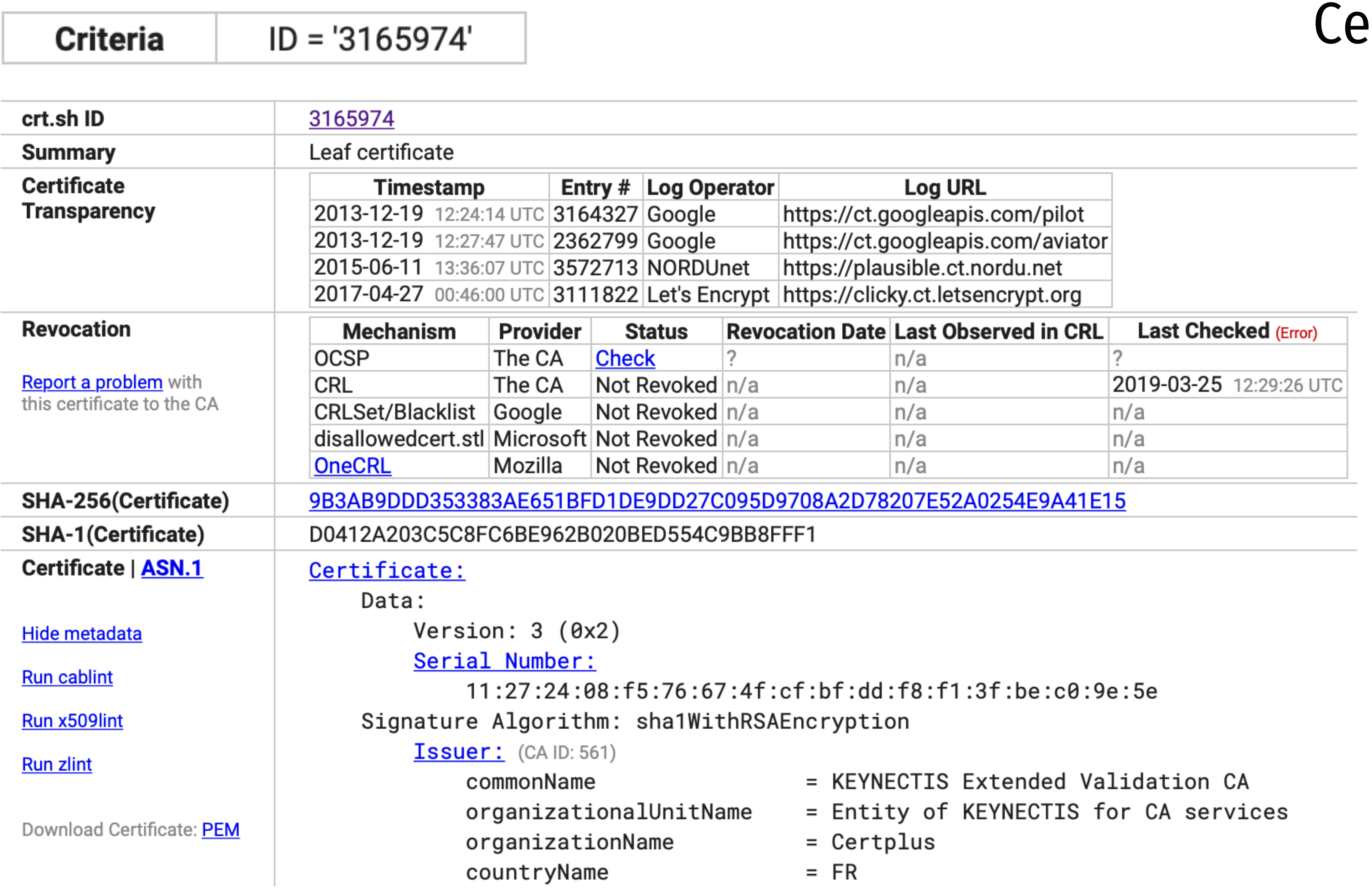


Criteria	Identity LIKE '%.yandex.ru'

1315533386	2019-03-25	2019-03-25	2020-03-24	plus.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315533439	2019-03-25	2019-03-25	2019-09-21	widevine-proxy.ott.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315533451	2019-03-25	2019-03-25	2019-09-21	playready-proxy.ott.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315533513	2019-03-25	2019-03-25	2019-09-21	fairplay-proxy.ott.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1315306628	2019-03-25	2019-03-25	2019-09-21	clint.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1314810139	2019-03-25	2019-03-22	2019-09-18	ege.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1306328397	2019-03-22	2019-03-22	2019-09-18	ege.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1306328473	2019-03-22	2019-03-22	2019-09-18	turboforms.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1306222859	2019-03-22	2019-03-19	2020-03-18	stat.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA
1305346717	2019-03-22	2019-03-18	2019-09-14	afisha.yandex.ru	C=RU, O=Yandex LLC, OU=Yandex Certification Authority, CN=Yandex CA

Certificates

https://crt.sh



Criteria	ID = '3165974'

crt.sh ID	3165974
Summary	Leaf certificate

Certificate Transparency

Timestamp	Entry #	Log Operator	Log URL
2013-12-19 12:24:14 UTC	3164327	Google	https://ct.googleapis.com/pilot
2013-12-19 12:27:47 UTC	2362799	Google	https://ct.googleapis.com/aviator
2015-06-11 13:36:07 UTC	3572713	NORDUnet	https://plausible.ct.nordu.net
2017-04-27 00:46:00 UTC	3111822	Let's Encrypt	https://clicky.ct.letsencrypt.org

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked	n/a	n/a	2019-03-25 12:29:26 UTC
CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

SHA-256(Certificate)	9B3AB9DDD353383AE651BFD1DE9DD27C095D9708A2D78207E52A0254E9A41E15
SHA-1(Certificate)	D0412A203C5C8FC6BE962B020BED554C9BB8FFF1

Certificate | ASN.1

Hide metadata

Run cablint

Run x509lint

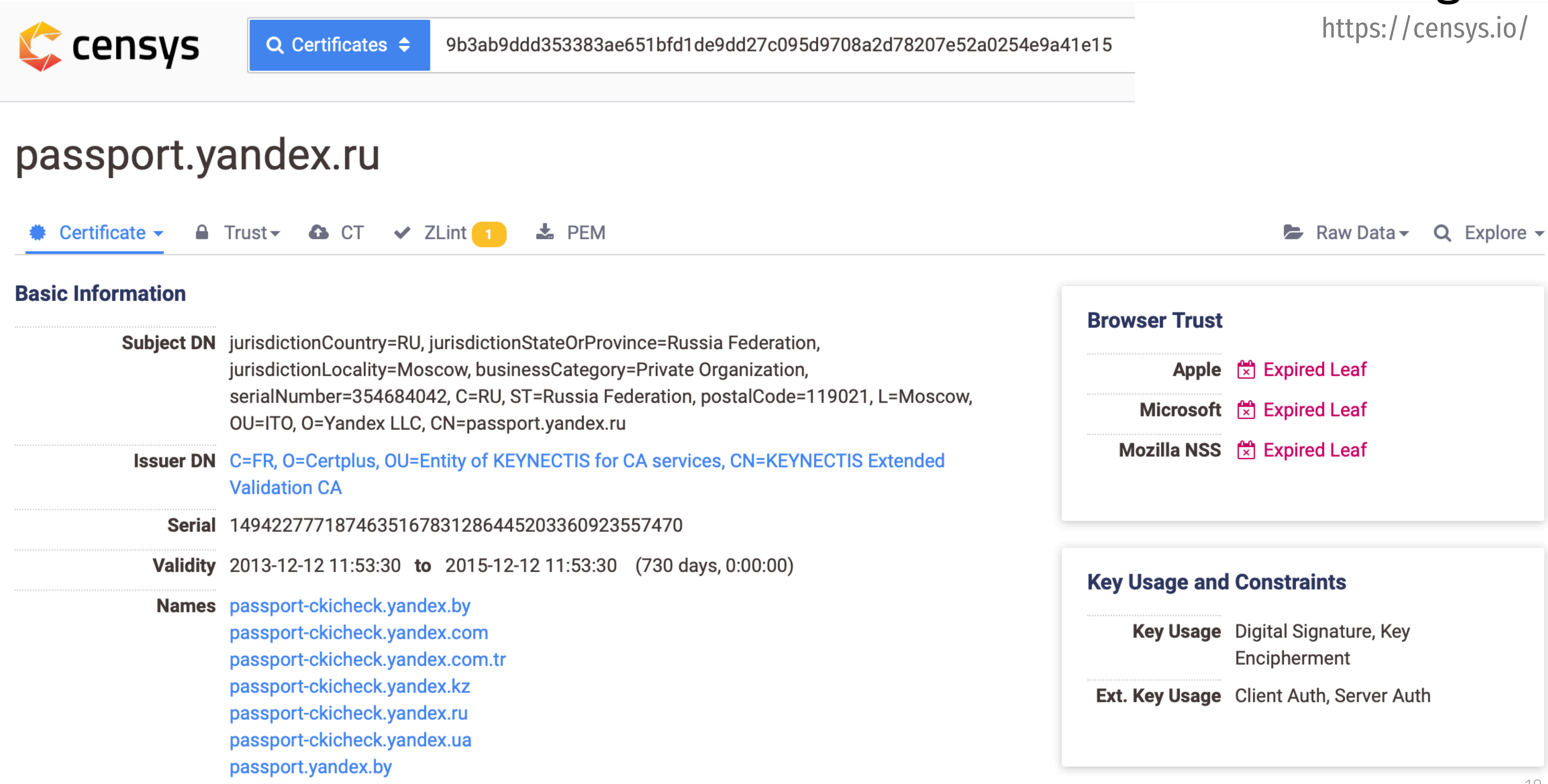
Run zlint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            11:27:24:08:f5:76:67:4f:cf:bf:dd:f8:f1:3f:be:c0:9e:5e
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: (CA ID: 561)
            commonName                = KEYNECTIS Extended Validation CA
            organizationalUnitName    = Entity of KEYNECTIS for CA services
            organizationName          = Certplus
            countryName               = FR
```

Search engine

https://censys.io/



9b3ab9ddd353383ae651bfd1de9dd27c095d9708a2d78207e52a0254e9a41e15

passport.yandex.ru

Basic Information

Subject DN jurisdictionCountry=RU, jurisdictionStateOrProvince=Russia Federation, jurisdictionLocality=Moscow, businessCategory=Private Organization, serialNumber=354684042, C=RU, ST=Russia Federation, postalCode=119021, L=Moscow, OU=ITO, O=Yandex LLC, CN=passport.yandex.ru

Issuer DN C=FR, O=Certplus, OU=Entity of KEYNECTIS for CA services, CN=KEYNECTIS Extended Validation CA

Serial 1494227771874635167831286445203360923557470

Validity 2013-12-12 11:53:30 **to** 2015-12-12 11:53:30 (730 days, 0:00:00)

Names passport-ckicheck.yandex.by
passport-ckicheck.yandex.com
passport-ckicheck.yandex.com.tr
passport-ckicheck.yandex.kz
passport-ckicheck.yandex.ru
passport-ckicheck.yandex.ua
passport.yandex.by

Browser Trust

Apple	Expired Leaf
Microsoft	Expired Leaf
Mozilla NSS	Expired Leaf

Key Usage and Constraints

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

Search engine

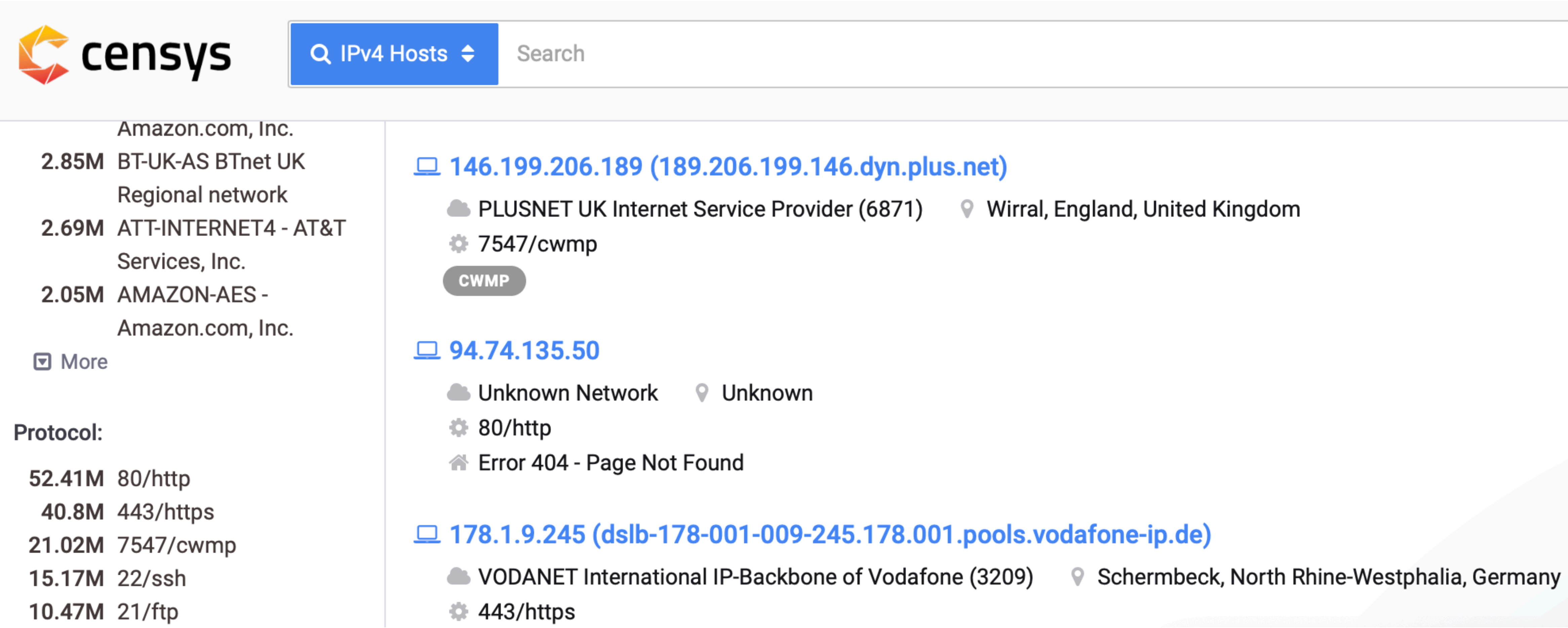
Why does it matter?

Don’t spend your time doing monkey work

Just check whether somebody has already done the thing

Search engine

https://censys.io/



	Amazon.com, Inc.
2.85M	BT-UK-AS BTnet UK Regional network
2.69M	ATT-INTERNET4 - AT&T Services, Inc.
2.05M	AMAZON-AES - Amazon.com, Inc.

More

Protocol:

52.41M	80/http
40.8M	443/https
21.02M	7547/cwmp
15.17M	22/ssh
10.47M	21/ftp

146.199.206.189 (189.206.199.146.dyn.plus.net)

PLUSNET UK Internet Service Provider (6871) Wirral, England, United Kingdom

7547/cwmp

CWMP

94.74.135.50

Unknown Network Unknown

80/http

Error 404 - Page Not Found

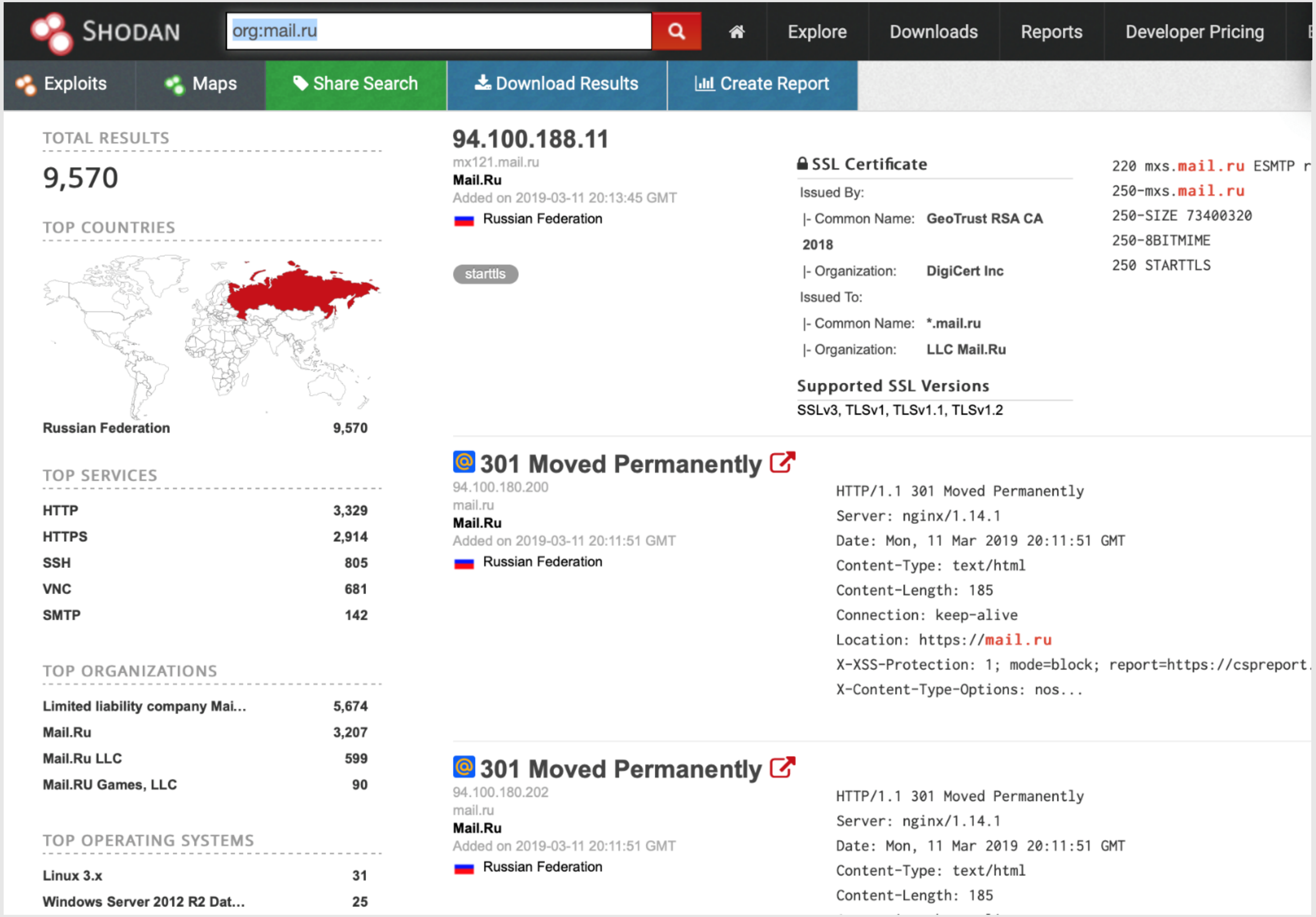
178.1.9.245 (dslb-178-001-009-245.178.001.pools.vodafone-ip.de)

VODANET International IP-Backbone of Vodafone (3209) Schermbeck, North Rhine-Westphalia, Germany

443/https

Search engine

https://shodan.io/



TOTAL RESULTS

9,570

TOP COUNTRIES

Russian Federation	9,570

TOP SERVICES

HTTP	3,329
HTTPS	2,914
SSH	805
VNC	681
SMTP	142

TOP ORGANIZATIONS

Limited liability company Mai...	5,674
Mail.Ru	3,207
Mail.Ru LLC	599
Mail.RU Games, LLC	90

TOP OPERATING SYSTEMS

Linux 3.x	31
Windows Server 2012 R2 Dat...	25

94.100.188.11

mx121.mail.ru

Mail.Ru

Added on 2019-03-11 20:13:45 GMT

Russian Federation

starttls

SSL Certificate

Issued By:

|- Common Name: GeoTrust RSA CA 2018

|- Organization: DigiCert Inc

Issued To:

|- Common Name: *.mail.ru

|- Organization: LLC Mail.Ru

Supported SSL Versions

SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
220 mxs.mail.ru ESMTP r
250-mxs.mail.ru
250-SIZE 73400320
250-8BITMIME
250 STARTTLS
```

301 Moved Permanently

94.100.180.200

mail.ru

Mail.Ru

Added on 2019-03-11 20:11:51 GMT

Russian Federation

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.1
Date: Mon, 11 Mar 2019 20:11:51 GMT
Content-Type: text/html
Content-Length: 185
Connection: keep-alive
Location: https://mail.ru
X-XSS-Protection: 1; mode=block; report=https://cspreport.
X-Content-Type-Options: nos...
```

301 Moved Permanently

94.100.180.202

mail.ru

Mail.Ru

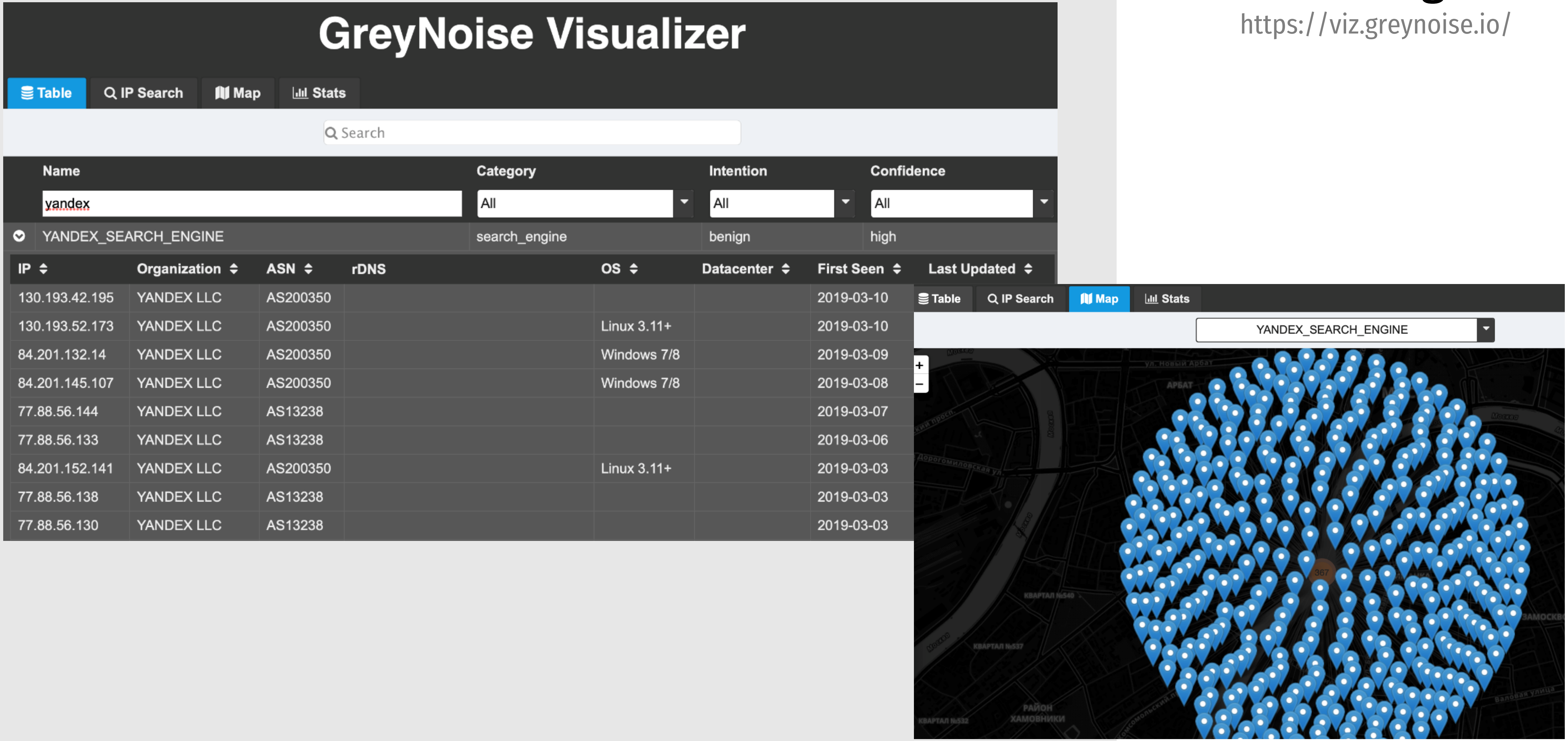
Added on 2019-03-11 20:11:51 GMT

Russian Federation

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.1
Date: Mon, 11 Mar 2019 20:11:51 GMT
Content-Type: text/html
Content-Length: 185
```

Search engine

https://viz.greynoise.io/



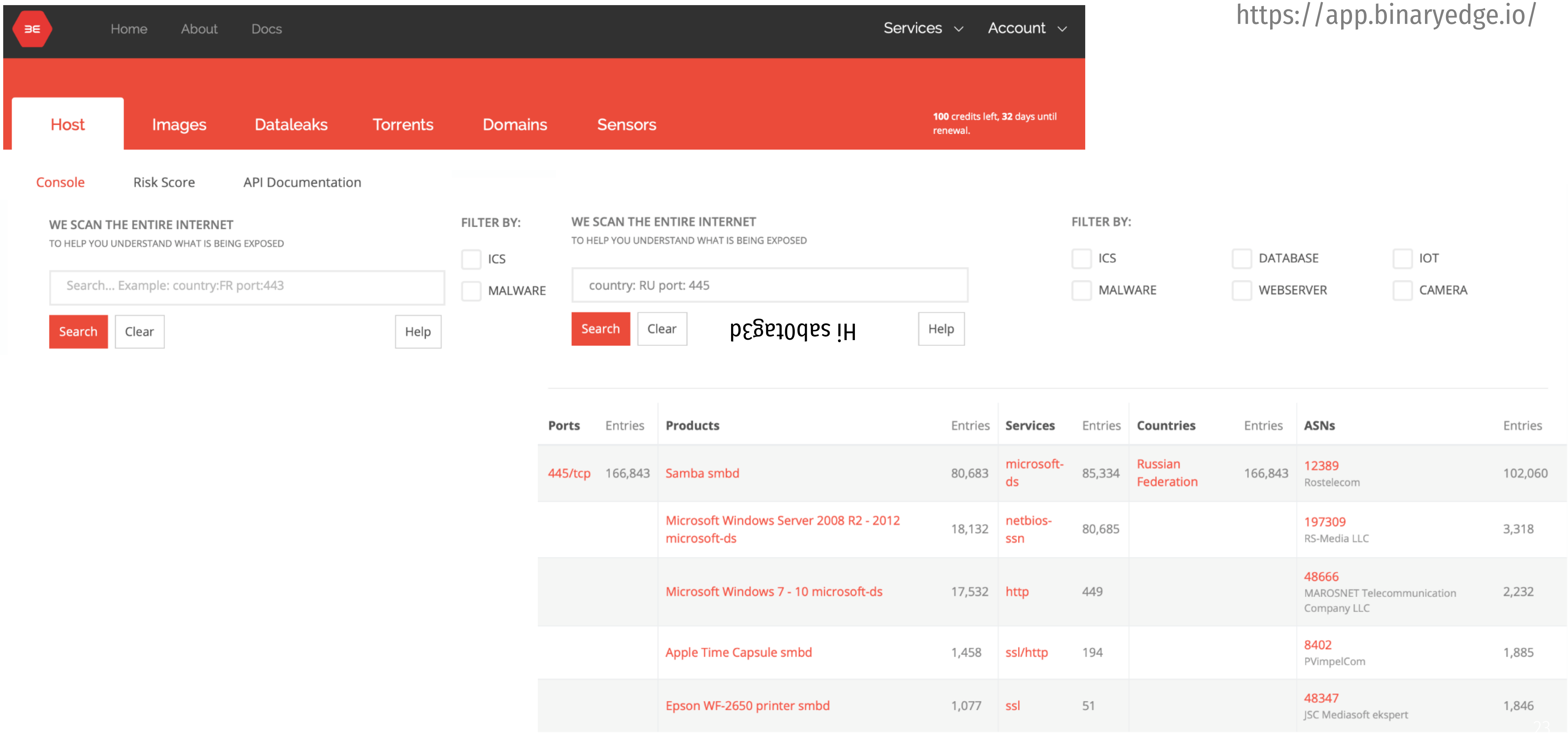
Name	Category	Intention	Confidence
yandex	All	All	All
YANDEX_SEARCH_ENGINE	search_engine	benign	high

IP	Organization	ASN	rDNS	OS	Datacenter	First Seen	Last Updated
130.193.42.195	YANDEX LLC	AS200350				2019-03-10	
130.193.52.173	YANDEX LLC	AS200350		Linux 3.11+		2019-03-10	
84.201.132.14	YANDEX LLC	AS200350		Windows 7/8		2019-03-09	
84.201.145.107	YANDEX LLC	AS200350		Windows 7/8		2019-03-08	
77.88.56.144	YANDEX LLC	AS13238				2019-03-07	
77.88.56.133	YANDEX LLC	AS13238				2019-03-06	
84.201.152.141	YANDEX LLC	AS200350		Linux 3.11+		2019-03-03	
77.88.56.138	YANDEX LLC	AS13238				2019-03-03	
77.88.56.130	YANDEX LLC	AS13238				2019-03-03	

YANDEX_SEARCH_ENGINE

Search engine

https://app.binaryedge.io/



WE SCAN THE ENTIRE INTERNET

TO HELP YOU UNDERSTAND WHAT IS BEING EXPOSED

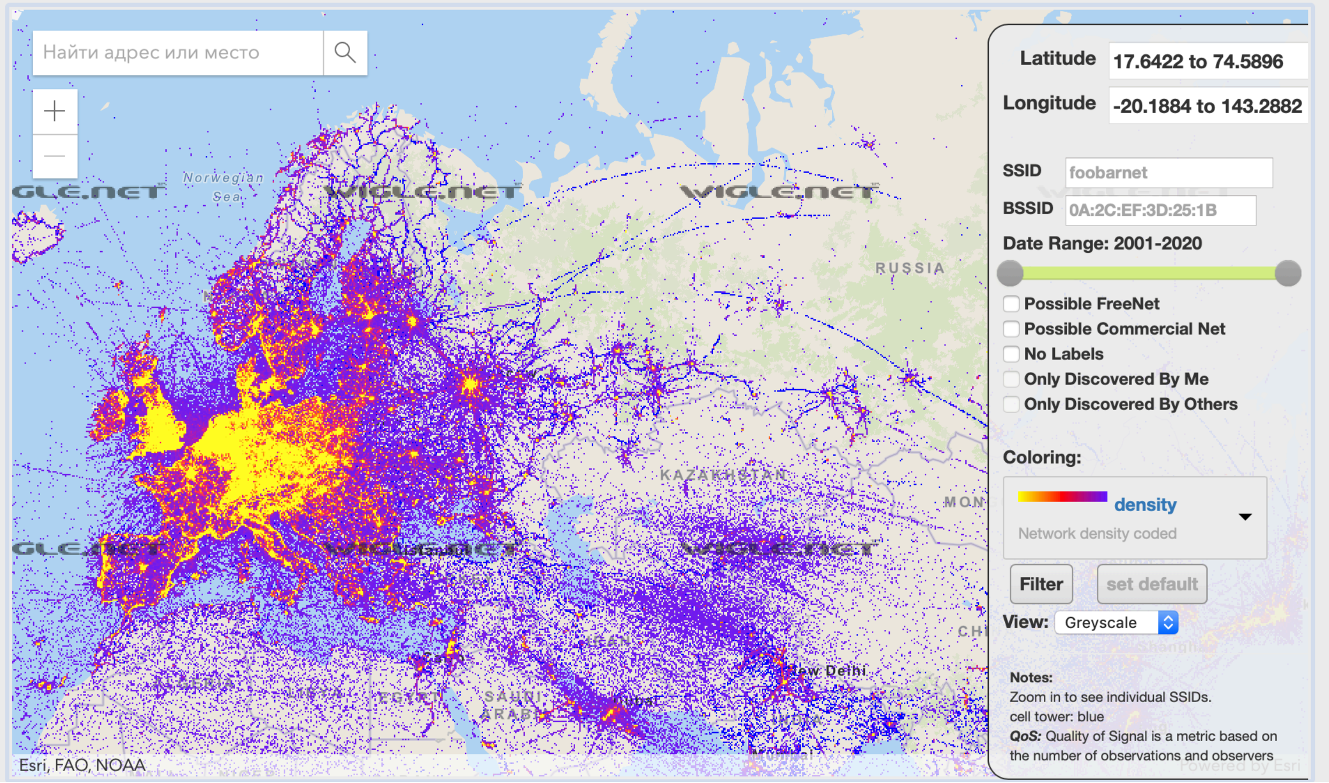
Search... Example: country:FR port:443

country: RU port: 445

Hi sab0tag3d

Ports	Entries	Products	Entries	Services	Entries	Countries	Entries	ASNs	Entries
445/tcp	166,843	Samba smbd	80,683	microsoft-ds	85,334	Russian Federation	166,843	12389 Rostelecom	102,060
		Microsoft Windows Server 2008 R2 - 2012 microsoft-ds	18,132	netbios-ssn	80,685			197309 RS-Media LLC	3,318
		Microsoft Windows 7 - 10 microsoft-ds	17,532	http	449			48666 MAROSNET Telecommunication Company LLC	2,232
		Apple Time Capsule smbd	1,458	ssl/http	194			8402 PVimpelCom	1,885
		Epson WF-2650 printer smbd	1,077	ssl	51			48347 JSC Mediasoft ekspert	1,846

Search engine



Latitude 17.6422 to 74.5896

Longitude -20.1884 to 143.2882

SSID foobarnet

BSSID 0A:2C:EF:3D:25:1B

Date Range: 2001-2020

- □ Possible FreeNet
- □ Possible Commercial Net
- □ No Labels
- □ Only Discovered By Me
- □ Only Discovered By Others

Coloring: density

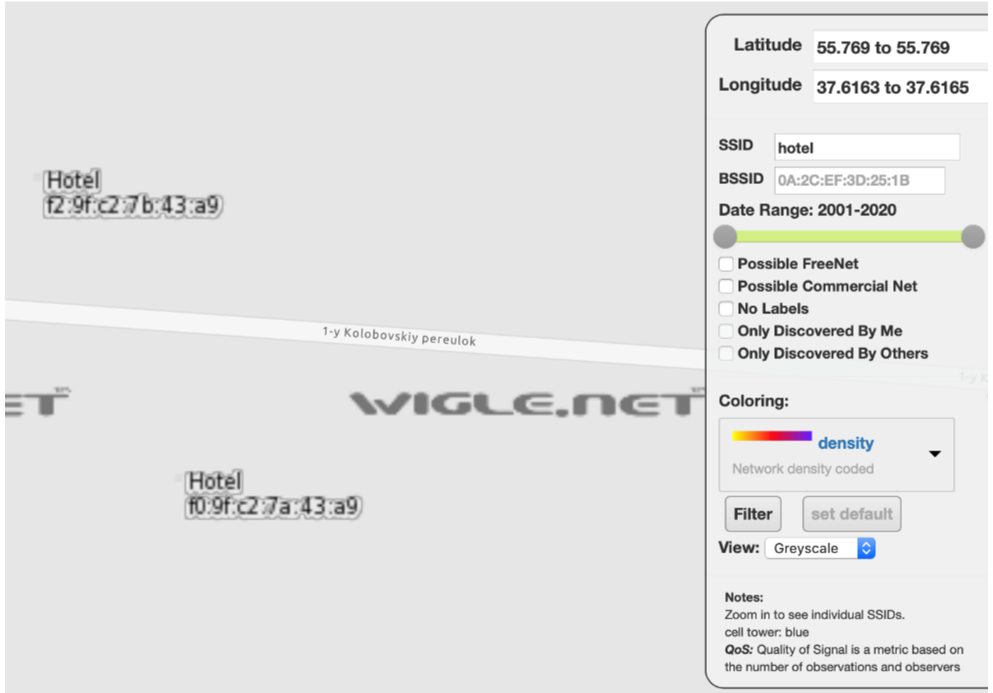
Network density coded

Filter · set default

View: Greyscale

Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

https://wigle.net/



Latitude 55.769 to 55.769

Longitude 37.6163 to 37.6165

SSID hotel

BSSID 0A:2C:EF:3D:25:1B

Date Range: 2001-2020

- □ Possible FreeNet
- □ Possible Commercial Net
- □ No Labels
- □ Only Discovered By Me
- □ Only Discovered By Others

Coloring: density

Network density coded

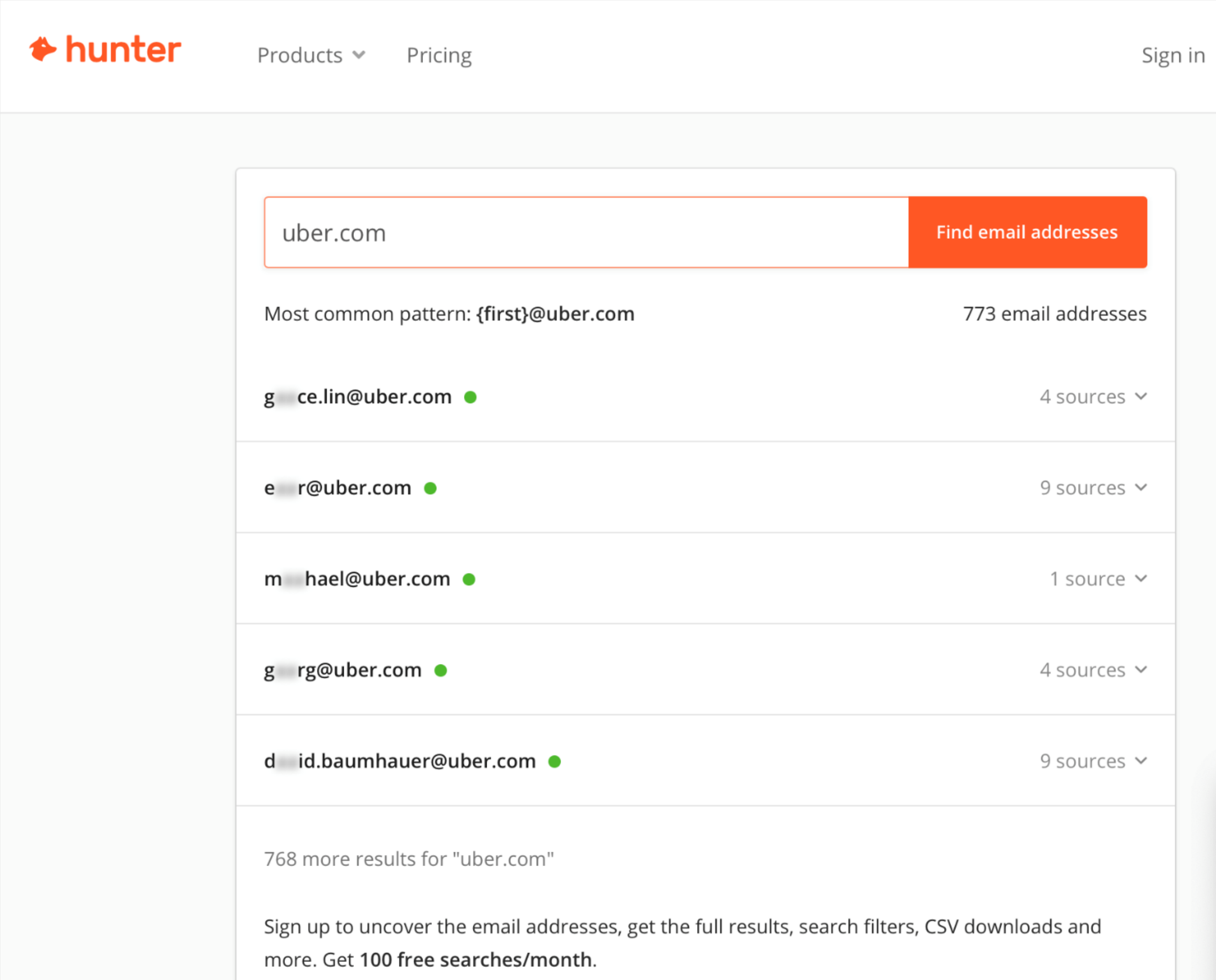
Filter · set default

View: Greyscale

Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

Search engine

https://hunter.io/



Most common pattern: **{first}@uber.com** 773 email addresses

g[redacted]ce.lin@uber.com ● 4 sources

e[redacted]r@uber.com ● 9 sources

m[redacted]hael@uber.com ● 1 source

g[redacted]rg@uber.com ● 4 sources

d[redacted]id.baumhauer@uber.com ● 9 sources

768 more results for "uber.com"

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get **100 free searches/month**.

Subdomain discovery

Take control over API

Isn't it a monkey work to check those resources one by one when their APIs have been already exposed?

Subdomain discovery

Why does it matter?

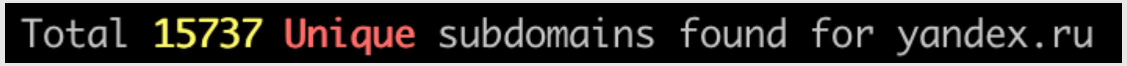
1. Subdomain takeovers

2. Any type of area-related bugs can be found, which will help to attack main target

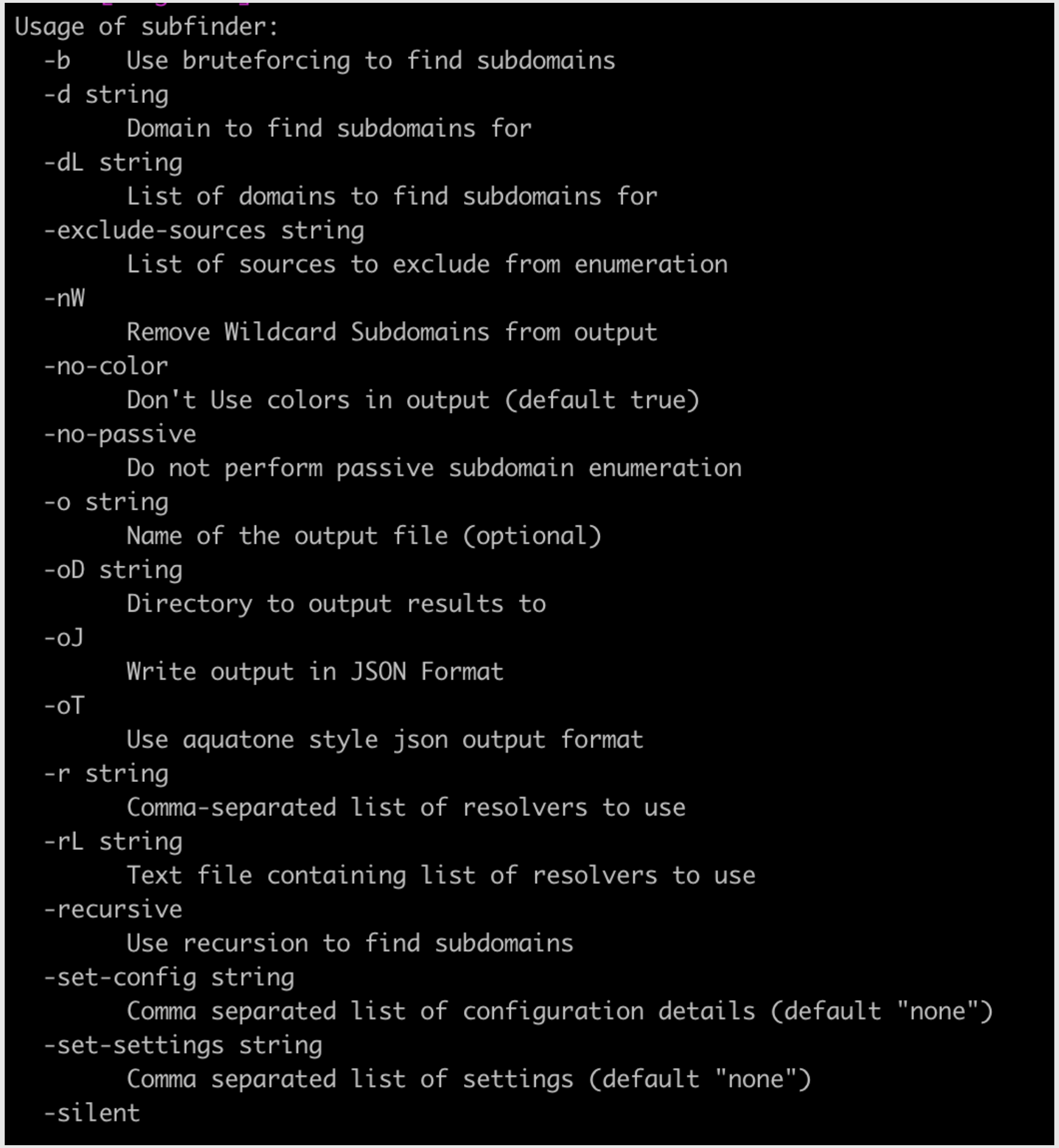
3. New targets which may be abandoned for a long time & be vulnerable to known issues

Subdomain discovery (Scraping)

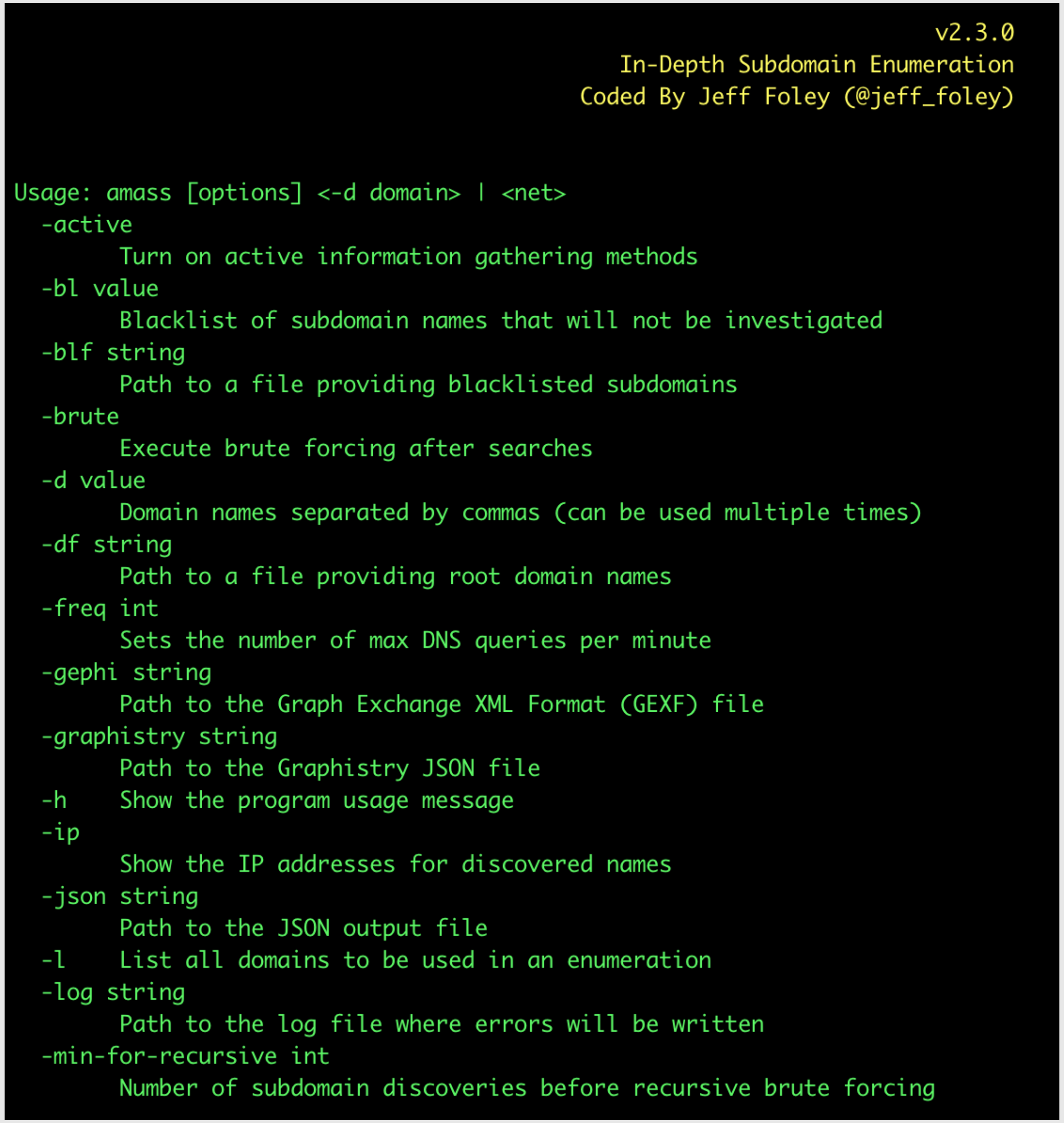
SubFinder



```
Total 15737 Unique subdomains found for yandex.ru
```



```
Usage of subfinder:
  -b    Use bruteforcing to find subdomains
  -d string
        Domain to find subdomains for
  -dL string
        List of domains to find subdomains for
  -exclude-sources string
        List of sources to exclude from enumeration
  -nW
        Remove Wildcard Subdomains from output
  -no-color
        Don't Use colors in output (default true)
  -no-passive
        Do not perform passive subdomain enumeration
  -o string
        Name of the output file (optional)
  -oD string
        Directory to output results to
  -oJ
        Write output in JSON Format
  -oT
        Use aquatone style json output format
  -r string
        Comma-separated list of resolvers to use
  -rL string
        Text file containing list of resolvers to use
  -recursive
        Use recursion to find subdomains
  -set-config string
        Comma separated list of configuration details (default "none")
  -set-settings string
        Comma separated list of settings (default "none")
  -silent
```



```
                                                  v2.3.0
                                  In-Depth Subdomain Enumeration
                               Coded By Jeff Foley (@jeff_foley)


Usage: amass [options] <-d domain> | <net>
  -active
        Turn on active information gathering methods
  -bl value
        Blacklist of subdomain names that will not be investigated
  -blf string
        Path to a file providing blacklisted subdomains
  -brute
        Execute brute forcing after searches
  -d value
        Domain names separated by commas (can be used multiple times)
  -df string
        Path to a file providing root domain names
  -freq int
        Sets the number of max DNS queries per minute
  -gephi string
        Path to the Graph Exchange XML Format (GEXF) file
  -graphistry string
        Path to the Graphistry JSON file
  -h    Show the program usage message
  -ip
        Show the IP addresses for discovered names
  -json string
        Path to the JSON output file
  -l    List all domains to be used in an enumeration
  -log string
        Path to the log file where errors will be written
  -min-for-recursive int
        Number of subdomain discoveries before recursive brute forcing
```

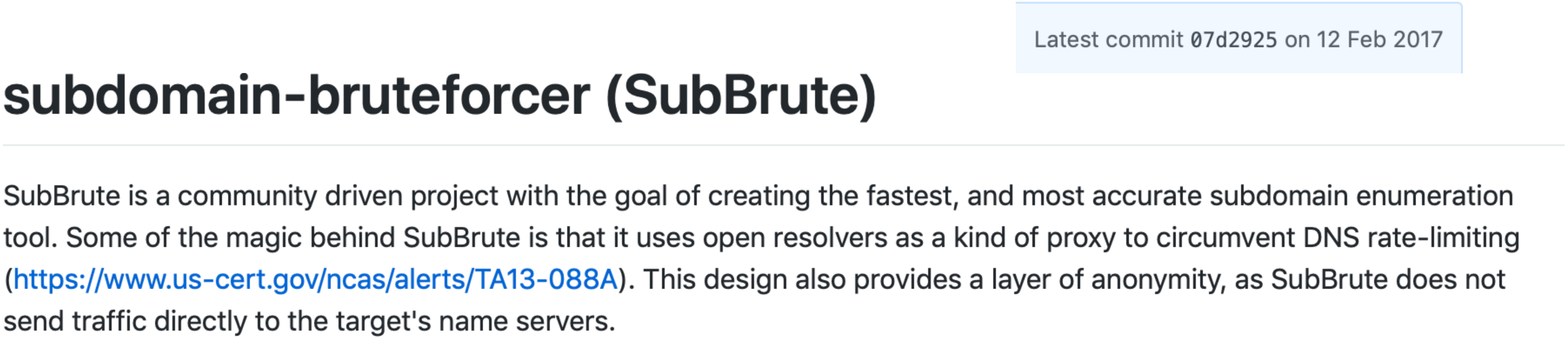
Subdomain discovery (Scraping)

AMASS

- Results depends on configuration
- 6600 by default launch

Subdomain discovery (Bruteforce)

Subbrute



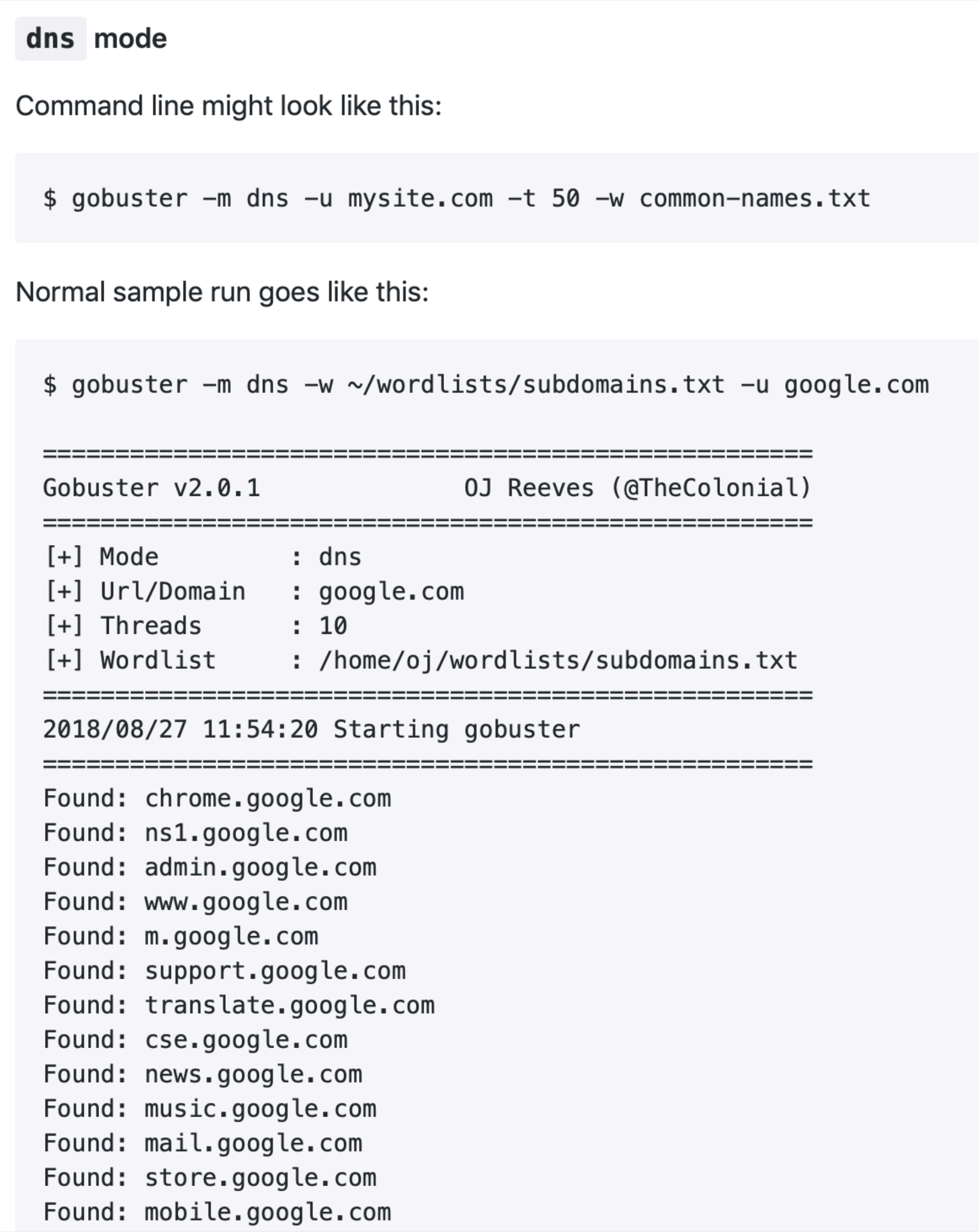
Latest commit `07d2925` on 12 Feb 2017

subdomain-bruteforcer (SubBrute)

SubBrute is a community driven project with the goal of creating the fastest, and most accurate subdomain enumeration tool. Some of the magic behind SubBrute is that it uses open resolvers as a kind of proxy to circumvent DNS rate-limiting (https://www.us-cert.gov/ncas/alerts/TA13-088A). This design also provides a layer of anonymity, as SubBrute does not send traffic directly to the target's name servers.

Subdomain discovery (Bruteforce)

Gobuster



`dns` mode

Command line might look like this:

```
$ gobuster -m dns -u mysite.com -t 50 -w common-names.txt
```

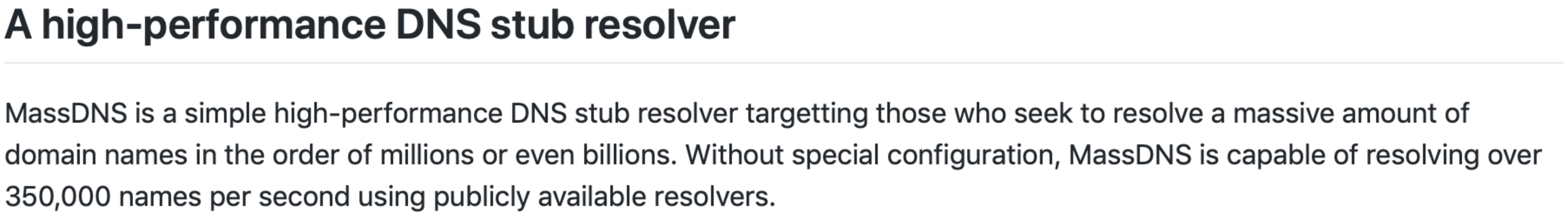
Normal sample run goes like this:

```
$ gobuster -m dns -w ~/wordlists/subdomains.txt -u google.com

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dns
[+] Url/Domain   : google.com
[+] Threads      : 10
[+] Wordlist     : /home/oj/wordlists/subdomains.txt
=====================================================
2018/08/27 11:54:20 Starting gobuster
=====================================================
Found: chrome.google.com
Found: ns1.google.com
Found: admin.google.com
Found: www.google.com
Found: m.google.com
Found: support.google.com
Found: translate.google.com
Found: cse.google.com
Found: news.google.com
Found: music.google.com
Found: mail.google.com
Found: store.google.com
Found: mobile.google.com
```

- Faster and flexible than subbrute

Subdomain discovery (Bruteforce)

MassDNS



A high-performance DNS stub resolver

MassDNS is a simple high-performance DNS stub resolver targetting those who seek to resolve a massive amount of domain names in the order of millions or even billions. Without special configuration, MassDNS is capable of resolving over 350,000 names per second using publicly available resolvers.

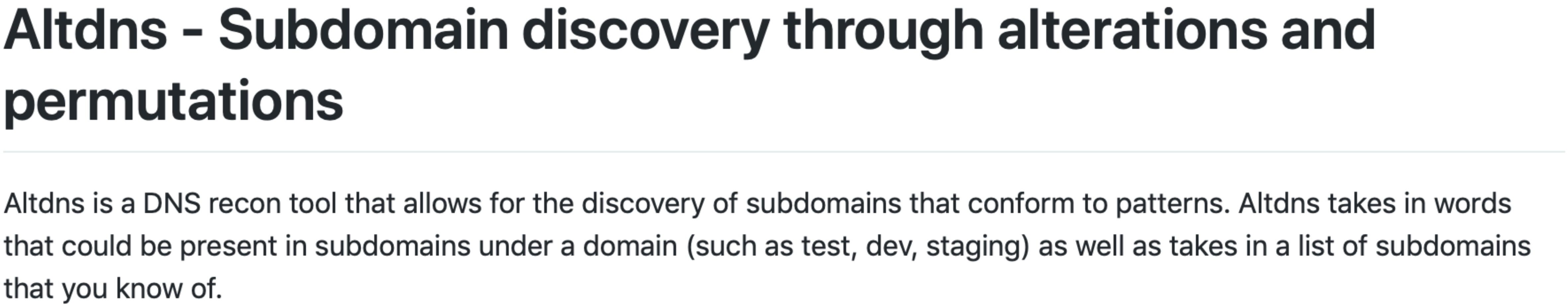
Result:

Depends on : Wordlist, Resolvers

Subdomain discovery (Bruteforce)

AltDNS

If we need to go deeper



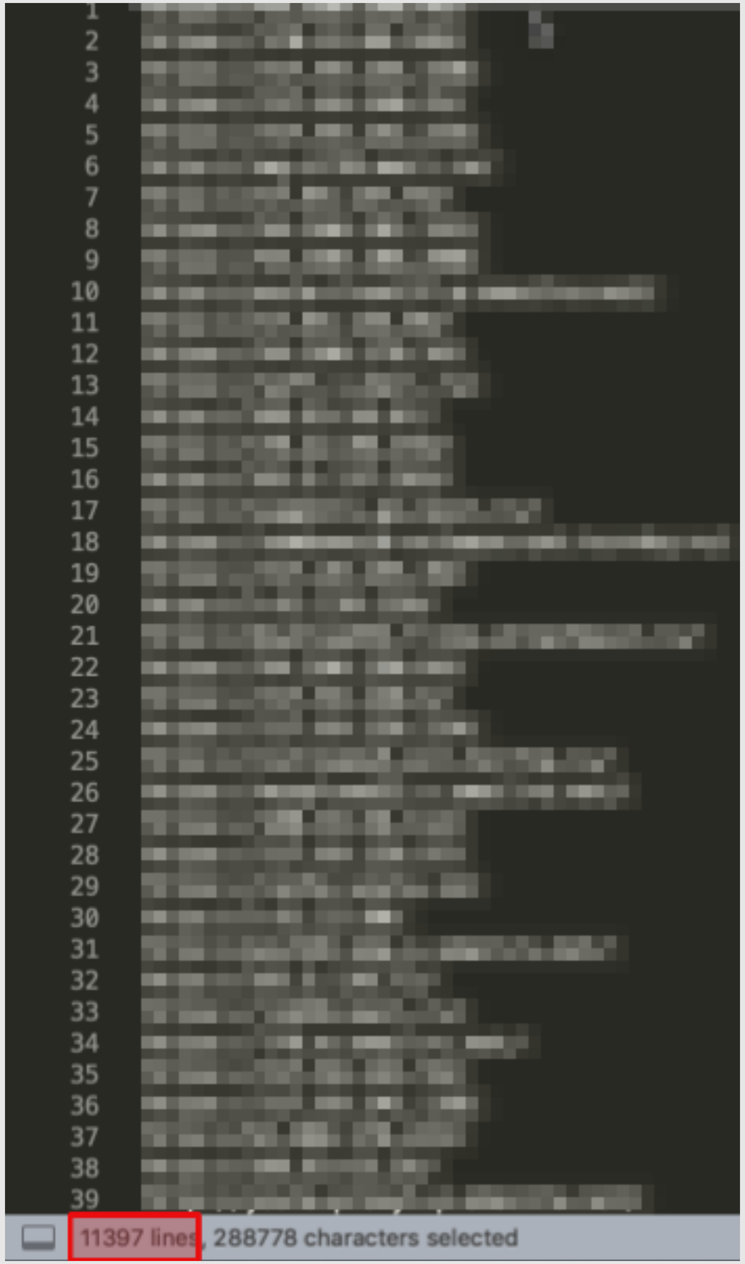
Altdns - Subdomain discovery through alterations and permutations

Altdns is a DNS recon tool that allows for the discovery of subdomains that conform to patterns. Altdns takes in words that could be present in subdomains under a domain (such as test, dev, staging) as well as takes in a list of subdomains that you know of.

Result

A huge list of targets is ready to be tested, but are you sure all of them are valid?

Identify availability

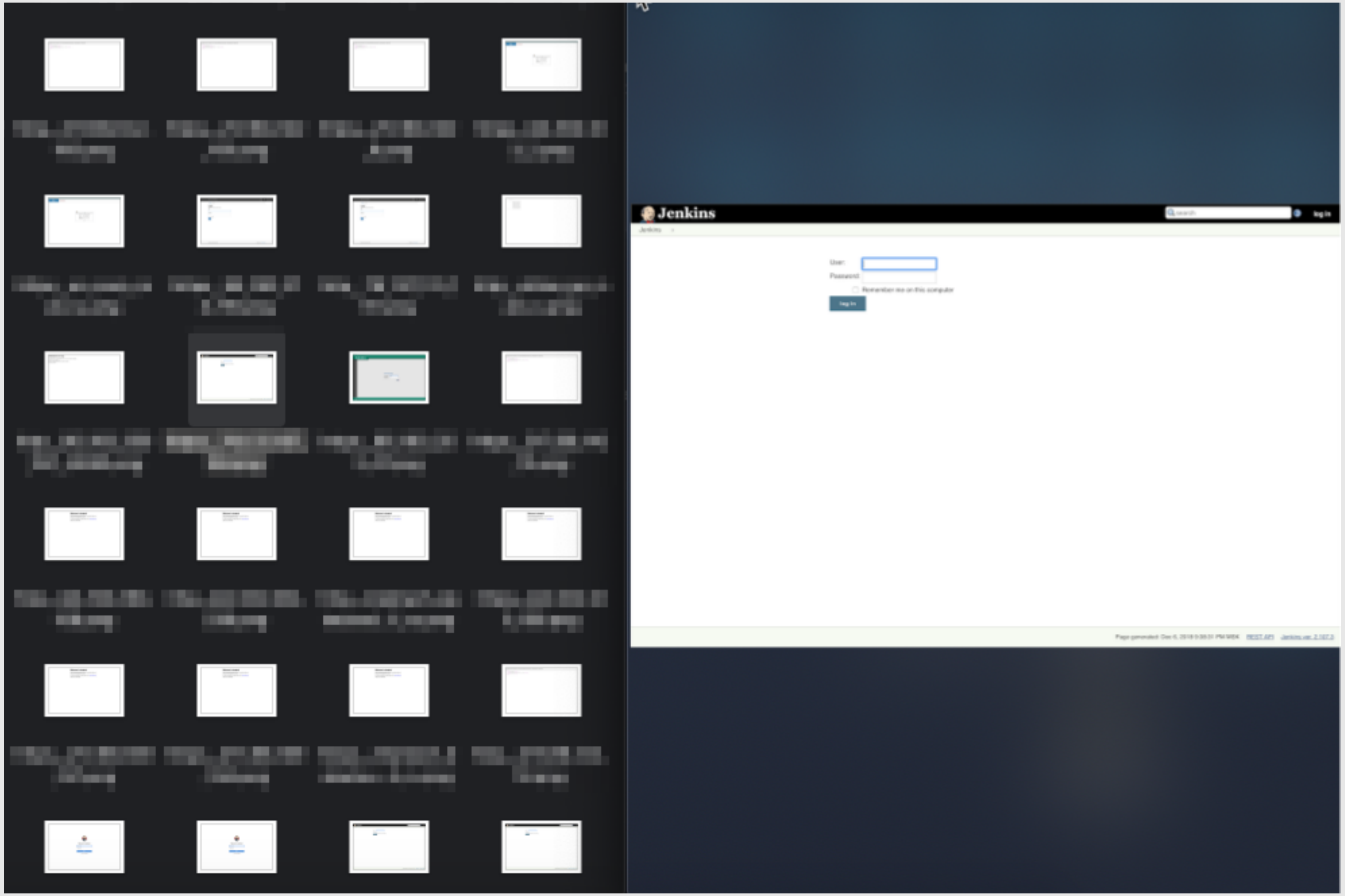


[redacted]

11397 lines, 288778 characters selected

11397 lines

How to deal with a lot of found assets?



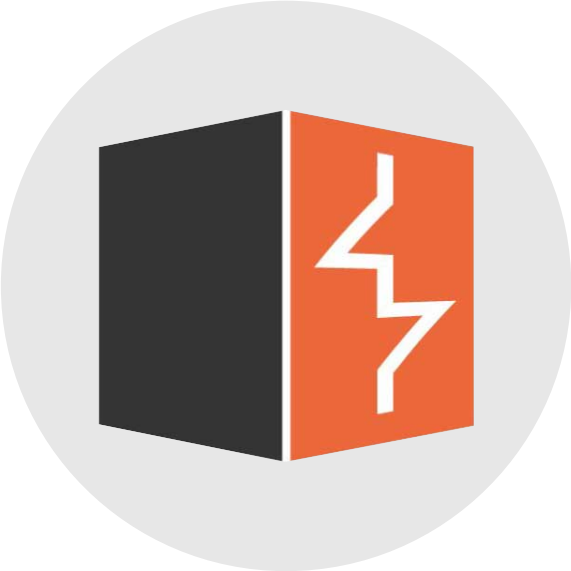
Identify availability

Screenshots

- https://github.com/michenriksen/aquatone
- https://github.com/FortyNorthSecurity/EyeWitness

Further Linked Resources Discovery

ZAP



Burp Suite

Further Linked Resources Discovery

Spidering/Crawling

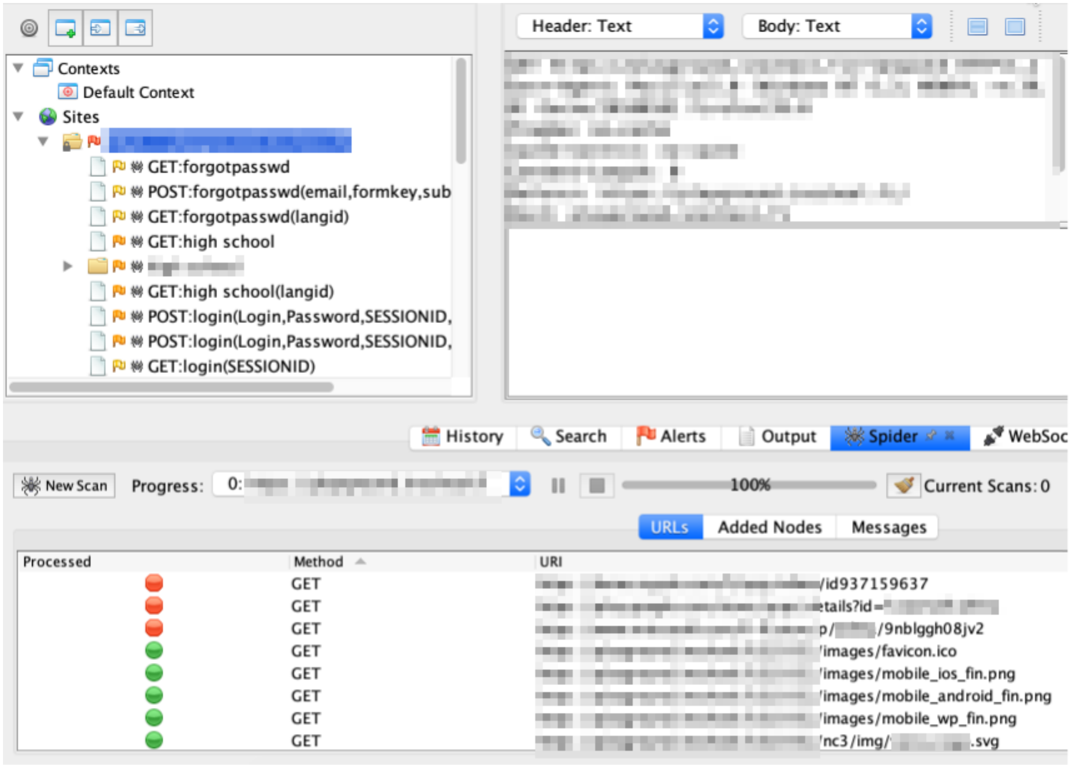
Why does it matter?

1 You shouldn’t do anything you can automate

2 Time matters

Further Linked Resources Discovery

Spidering/Crawling



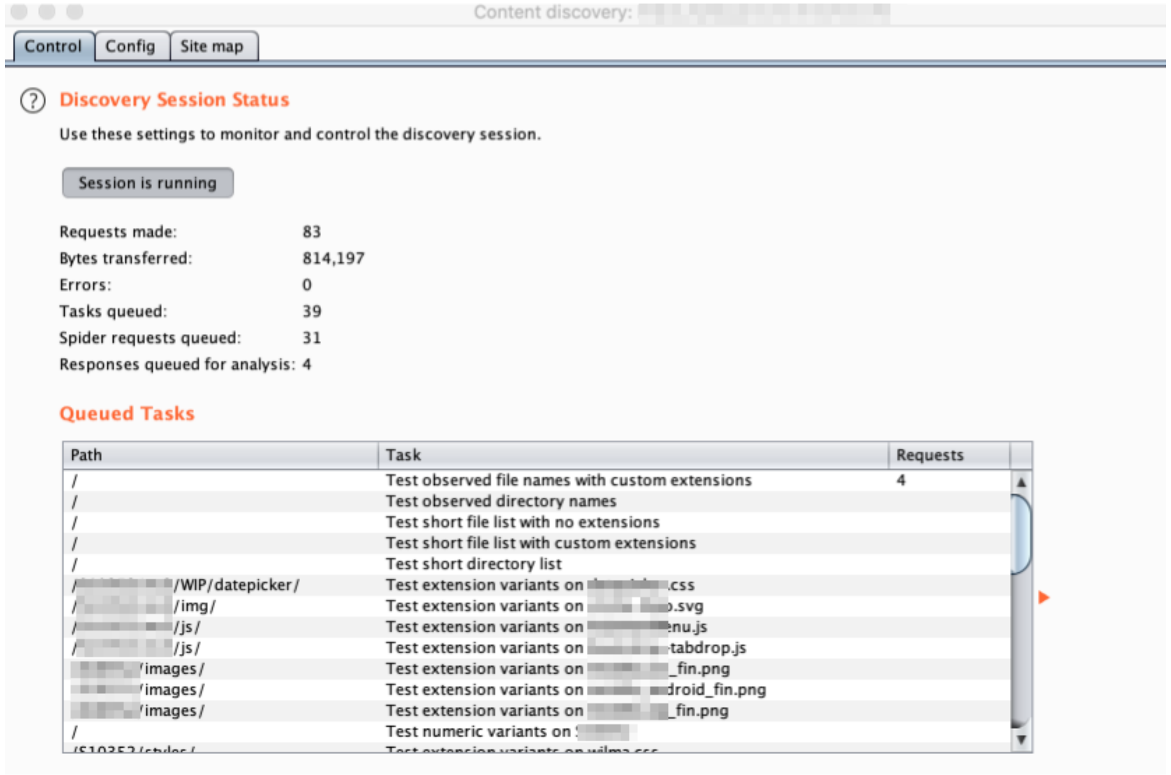
- Contexts
  - Default Context
- Sites
  - [redacted]
    - GET:forgotpasswd
    - POST:forgotpasswd(email,formkey,sub
    - GET:forgotpasswd(langid)
    - GET:high school
    - [redacted]
    - GET:high school(langid)
    - POST:login(Login,Password,SESSIONID,
    - POST:login(Login,Password,SESSIONID,
    - GET:login(SESSIONID)

[redacted]

Progress: 0:[redacted] 100% Current Scans: 0

Processed	Method	URI
🟥	GET	[redacted]/id937159637
🟥	GET	[redacted]tails?id=[redacted]
🟥	GET	[redacted]p/[redacted]/9nblggh08jv2
🟩	GET	[redacted]/images/favicon.ico
🟩	GET	[redacted]/images/mobile_ios_fin.png
🟩	GET	[redacted]/images/mobile_android_fin.png
🟩	GET	[redacted]/images/mobile_wp_fin.png
🟩	GET	[redacted]/nc3/img/[redacted].svg

OWASP ZAP



Discovery Session Status

Use these settings to monitor and control the discovery session.

Requests made:	83
Bytes transferred:	814,197
Errors:	0
Tasks queued:	39
Spider requests queued:	31
Responses queued for analysis:	4

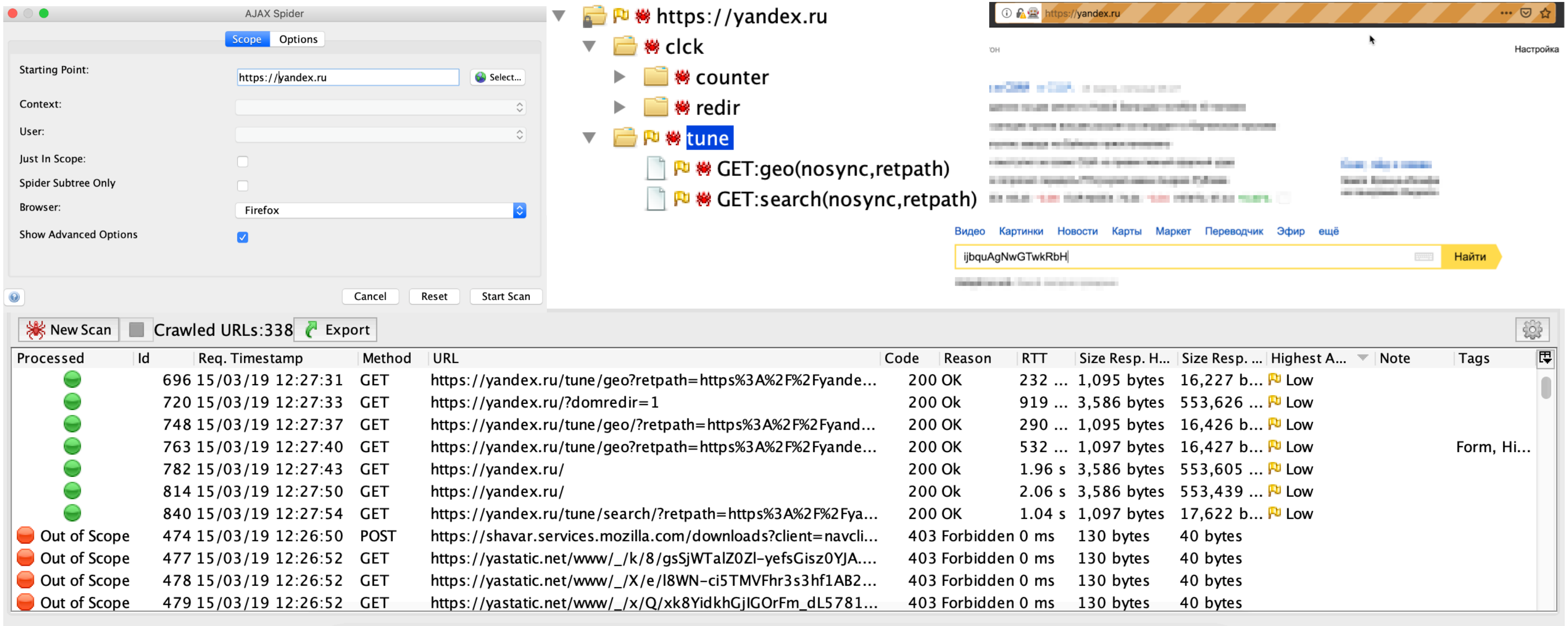
Queued Tasks

Path	Task	Requests
/	Test observed file names with custom extensions	4
/	Test observed directory names	
/	Test short file list with no extensions	
/	Test short file list with custom extensions	
/	Test short directory list	
/[redacted]/WIP/datepicker/	Test extension variants on [redacted].css	
/[redacted]/img/	Test extension variants on [redacted].svg	
/[redacted]/js/	Test extension variants on [redacted]nu.js	
/[redacted]/js/	Test extension variants on [redacted]tabdrop.js	
[redacted]/images/	Test extension variants on [redacted]_fin.png	
[redacted]/images/	Test extension variants on [redacted]droid_fin.png	
[redacted]/images/	Test extension variants on [redacted]_fin.png	
/	Test numeric variants on [redacted]	
/S10352/styles/	Test extension variants on wilma.css	

Burp Suite

Further Linked Resources Discovery

Ajax Spidering



AJAX Spider

Starting Point:	https://yandex.ru
Context:	
User:	
Just In Scope:	☐
Spider Subtree Only	☐
Browser:	Firefox
Show Advanced Options	☑

- https://yandex.ru
  - clck
    - counter
    - redir
  - tune
    - GET:geo(nosync,retpath)
    - GET:search(nosync,retpath)

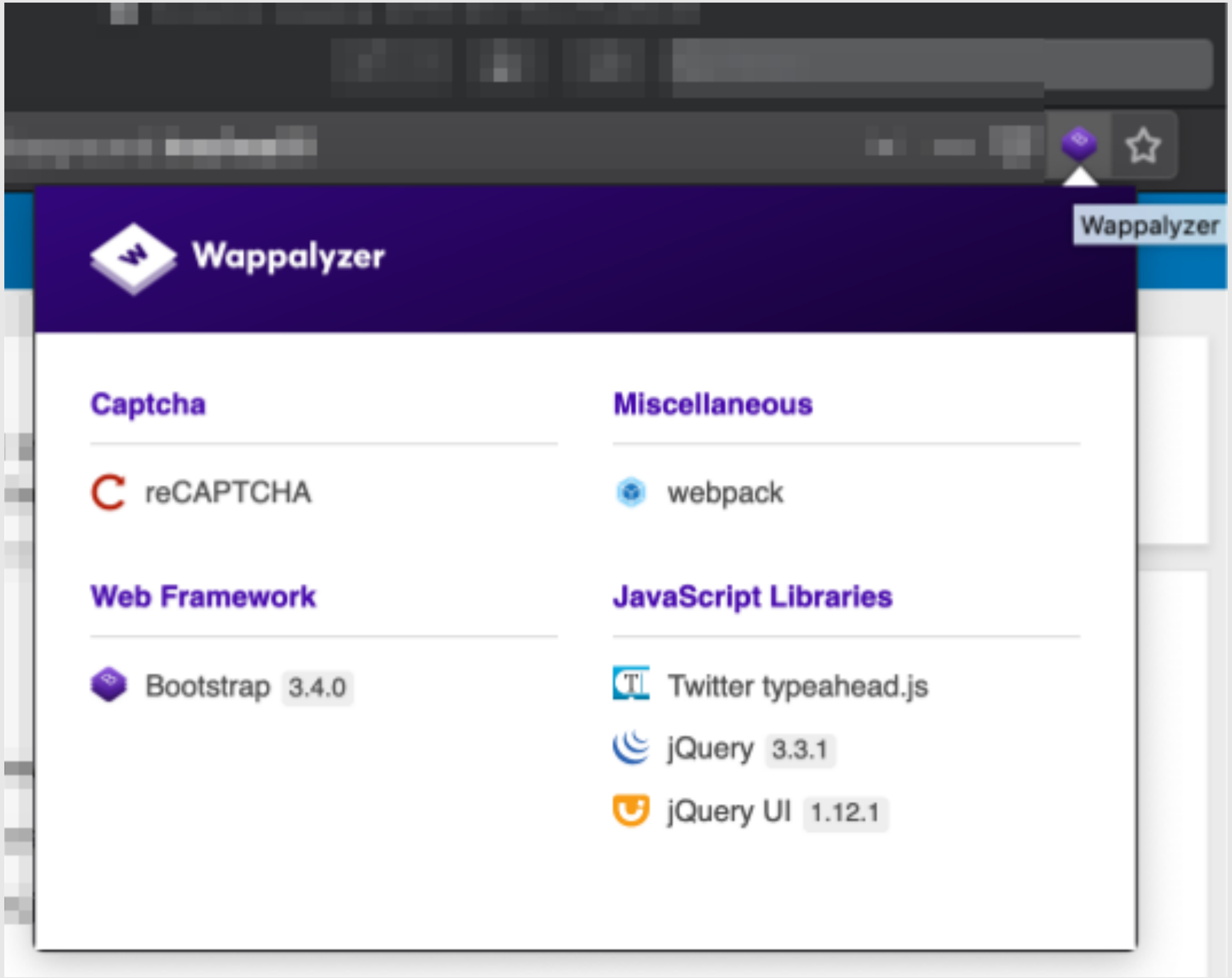
Processed	Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. H...	Size Resp. ...	Highest A...	Note	Tags
●	696	15/03/19 12:27:31	GET	https://yandex.ru/tune/geo?retpath=https%3A%2F%2Fyande...	200	OK	232 ...	1,095 bytes	16,227 b...	Low		
●	720	15/03/19 12:27:33	GET	https://yandex.ru/?domredir=1	200	Ok	919 ...	3,586 bytes	553,626 ...	Low		
●	748	15/03/19 12:27:37	GET	https://yandex.ru/tune/geo/?retpath=https%3A%2F%2Fyand...	200	OK	290 ...	1,095 bytes	16,426 b...	Low		
●	763	15/03/19 12:27:40	GET	https://yandex.ru/tune/geo?retpath=https%3A%2F%2Fyande...	200	OK	532 ...	1,097 bytes	16,427 b...	Low		Form, Hi...
●	782	15/03/19 12:27:43	GET	https://yandex.ru/	200	Ok	1.96 s	3,586 bytes	553,605 ...	Low		
●	814	15/03/19 12:27:50	GET	https://yandex.ru/	200	Ok	2.06 s	3,586 bytes	553,439 ...	Low		
●	840	15/03/19 12:27:54	GET	https://yandex.ru/tune/search/?retpath=https%3A%2F%2Fya...	200	OK	1.04 s	1,097 bytes	17,622 b...	Low		
● Out of Scope	474	15/03/19 12:26:50	POST	https://shavar.services.mozilla.com/downloads?client=navcli...	403	Forbidden	0 ms	130 bytes	40 bytes			
● Out of Scope	477	15/03/19 12:26:52	GET	https://yastatic.net/www/_/k/8/gsSjWTalZ0Zl-yefsGisz0YJA....	403	Forbidden	0 ms	130 bytes	40 bytes			
● Out of Scope	478	15/03/19 12:26:52	GET	https://yastatic.net/www/_/X/e/I8WN-ci5TMVFhr3s3hf1AB2...	403	Forbidden	0 ms	130 bytes	40 bytes			
● Out of Scope	479	15/03/19 12:26:52	GET	https://yastatic.net/www/_/x/Q/xk8YidkhGjIGOrFm_dL5781...	403	Forbidden	0 ms	130 bytes	40 bytes			

WHAT

Now let's narrow the focus area even more

Discover technology

Wappalyzer



Captcha

- reCAPTCHA

Miscellaneous

- webpack

Web Framework

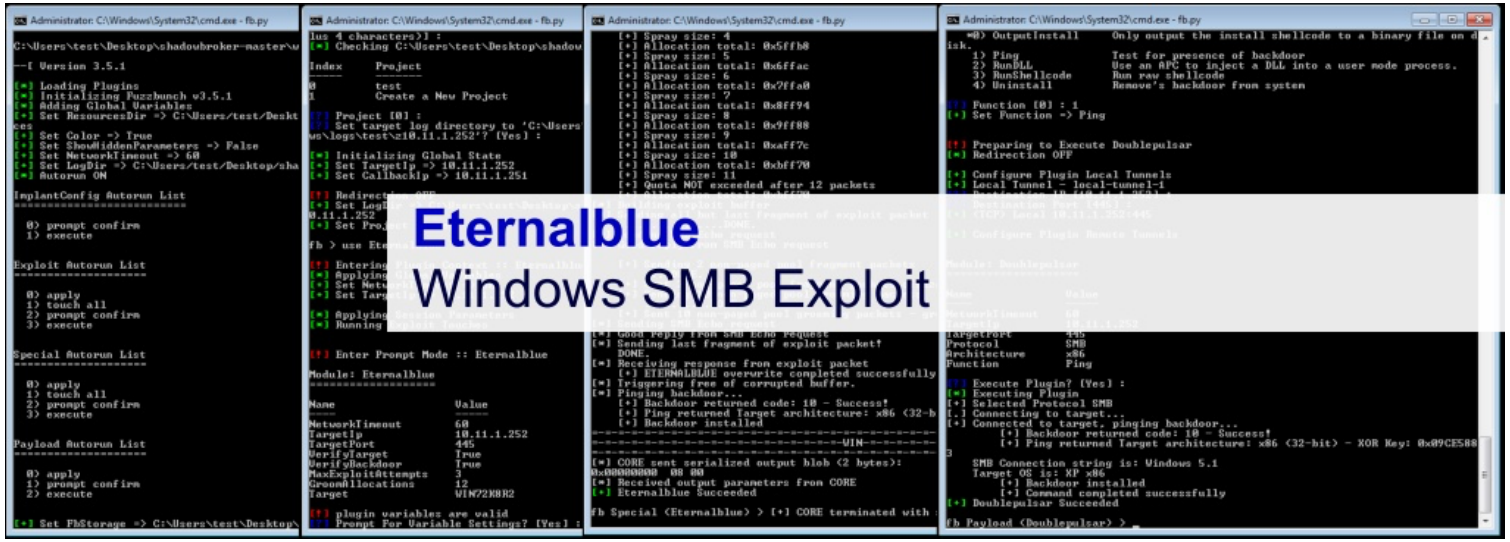
- Bootstrap 3.4.0

JavaScript Libraries

- Twitter typeahead.js
- jQuery 3.3.1
- jQuery UI 1.12.1

- Or WhatWeb script

Why it matters?

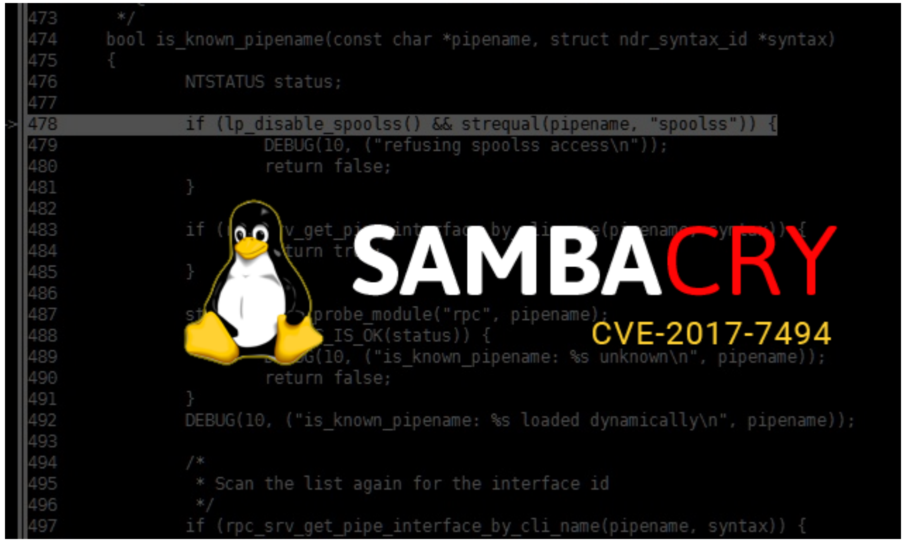


```
Administrator: C:\Windows\System32\cmd.exe - fb.py
C:\Users\test\Desktop\shadowbroker-master\w

--[ Version 3.5.1

[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => C:\Users/test/Deskt
ces
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => C:\Users/test/Desktop/sha
[*] Autorun ON

ImplantConfig Autorun List
==========================

  0) prompt confirm
  1) execute

Exploit Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute

Special Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute

Payload Autorun List
====================

  0) apply
  1) prompt confirm
  2) execute

[+] Set FbStorage => C:\Users\test\Desktop\
```

```
Administrator: C:\Windows\System32\cmd.exe - fb.py
lus 4 characters)] :
[*] Checking C:\Users\test\Desktop\shadow

Index     Project
-----     -------
0         test
1         Create a New Project

[?] Project [0] :
[?] Set target log directory to 'C:\Users'
ws\logs\test\z10.11.1.252'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 10.11.1.252
[+] Set CallbackIp => 10.11.1.251

[!] Redirect
[+] Set LogD
0.11.1.252
[+] Set Proj

fb > use Ete

[!] Entering
[*] Applying
[+] Set Netw
[+] Set Targ

[*] Applying
[*] Running


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                10.11.1.252
TargetPort              445
VerifyTarget            True
VerifyBackdoor          True
MaxExploitAttempts      3
GroomAllocations        12
Target                  WIN72K8R2

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :
```

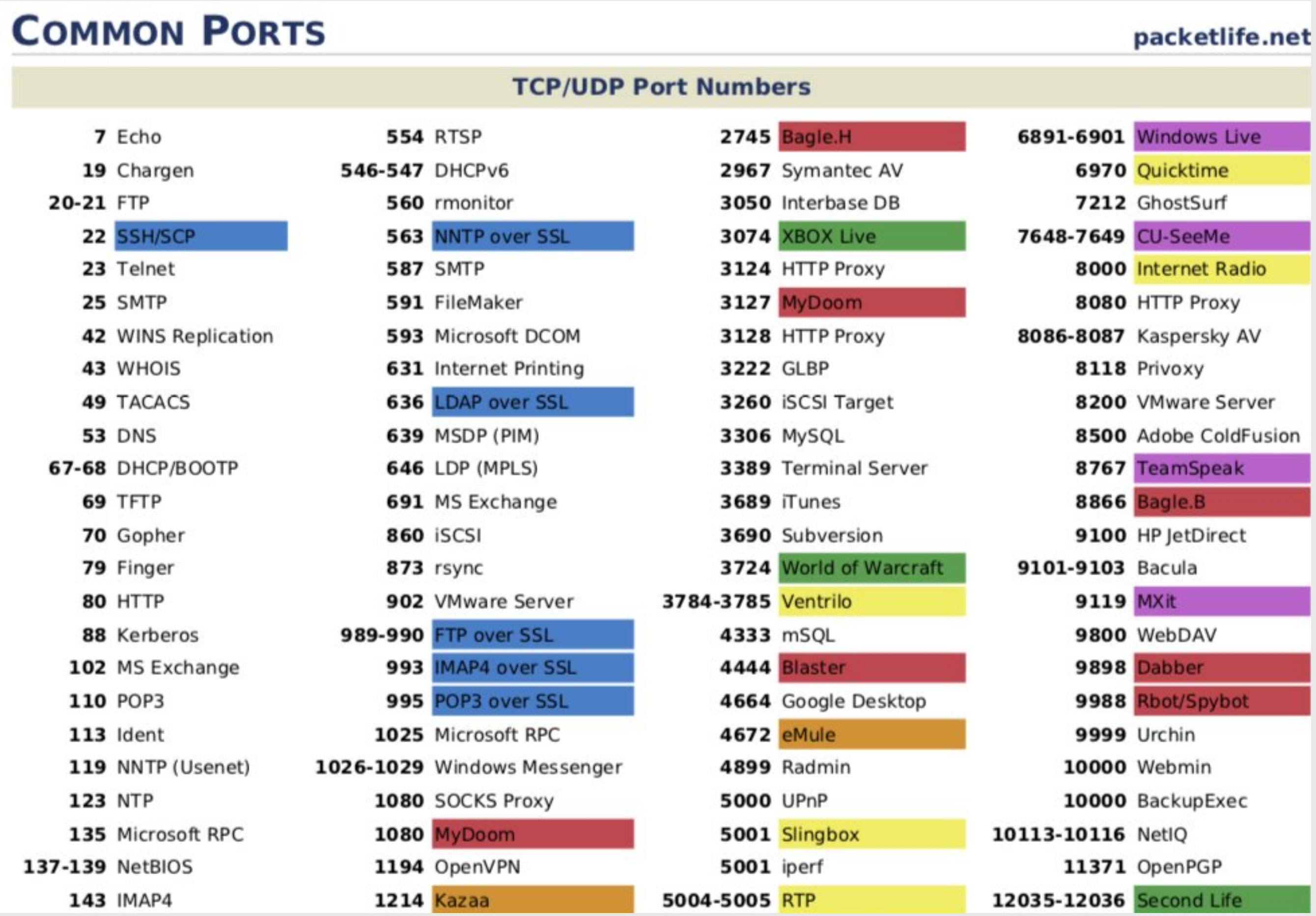
```
Administrator: C:\Windows\System32\cmd.exe - fb.py
    [+] Spray size: 4
    [+] Allocation total: 0x5ffb8
    [+] Spray size: 5
    [+] Allocation total: 0x6ffac
    [+] Spray size: 6
    [+] Allocation total: 0x7ffa0
    [+] Spray size: 7
    [+] Allocation total: 0x8ff94
    [+] Spray size: 8
    [+] Allocation total: 0x9ff88
    [+] Spray size: 9
    [+] Allocation total: 0xaff7c
    [+] Spray size: 10
    [+] Allocation total: 0xbff70
    [+] Spray size: 11
    [+] Quota NOT exceeded after 12 packets

[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x86 (32-b
    [+] Backdoor installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00
[*] Received output parameters from CORE
[+] Eternalblue Succeeded

fb Special (Eternalblue) > [+] CORE terminated with
```

```
Administrator: C:\Windows\System32\cmd.exe - fb.py
   *0) OutputInstall      Only output the install shellcode to a binary file on d
isk.
    1) Ping               Test for presence of backdoor
    2) RunDLL             Use an APC to inject a DLL into a user mode process.
    3) RunShellcode       Run raw shellcode
    4) Uninstall          Remove's backdoor from system

[?] Function [0] : 1
[+] Set Function => Ping


[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1

TargetPort          445
Protocol            SMB
Architecture        x86
Function            Ping

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x09CE588
3
    SMB Connection string is: Windows 5.1
    Target OS is: XP x86
        [+] Backdoor installed
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) > _
```



```
    */
    bool is_known_pipename(const char *pipename, struct ndr_syntax_id *syntax)
    {
            NTSTATUS status;

            if (lp_disable_spoolss() && strequal(pipename, "spoolss")) {
                    DEBUG(10, ("refusing spoolss access\n"));
                    return false;
            }

            if (  v_get_pi   int   fa   by   li   e(p  ename   syn   )) {
                    turn tr
            }

            st       probe_module("rpc", pipename);
                     _IS_OK(status)) {
                        G(10, ("is_known_pipename: %s unknown\n", pipename));
                    return false;
            }
            DEBUG(10, ("is_known_pipename: %s loaded dynamically\n", pipename));

            /*
             * Scan the list again for the interface id
             */
            if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
```

Port Scan



Common Ports packetlife.net

TCP/UDP Port Numbers

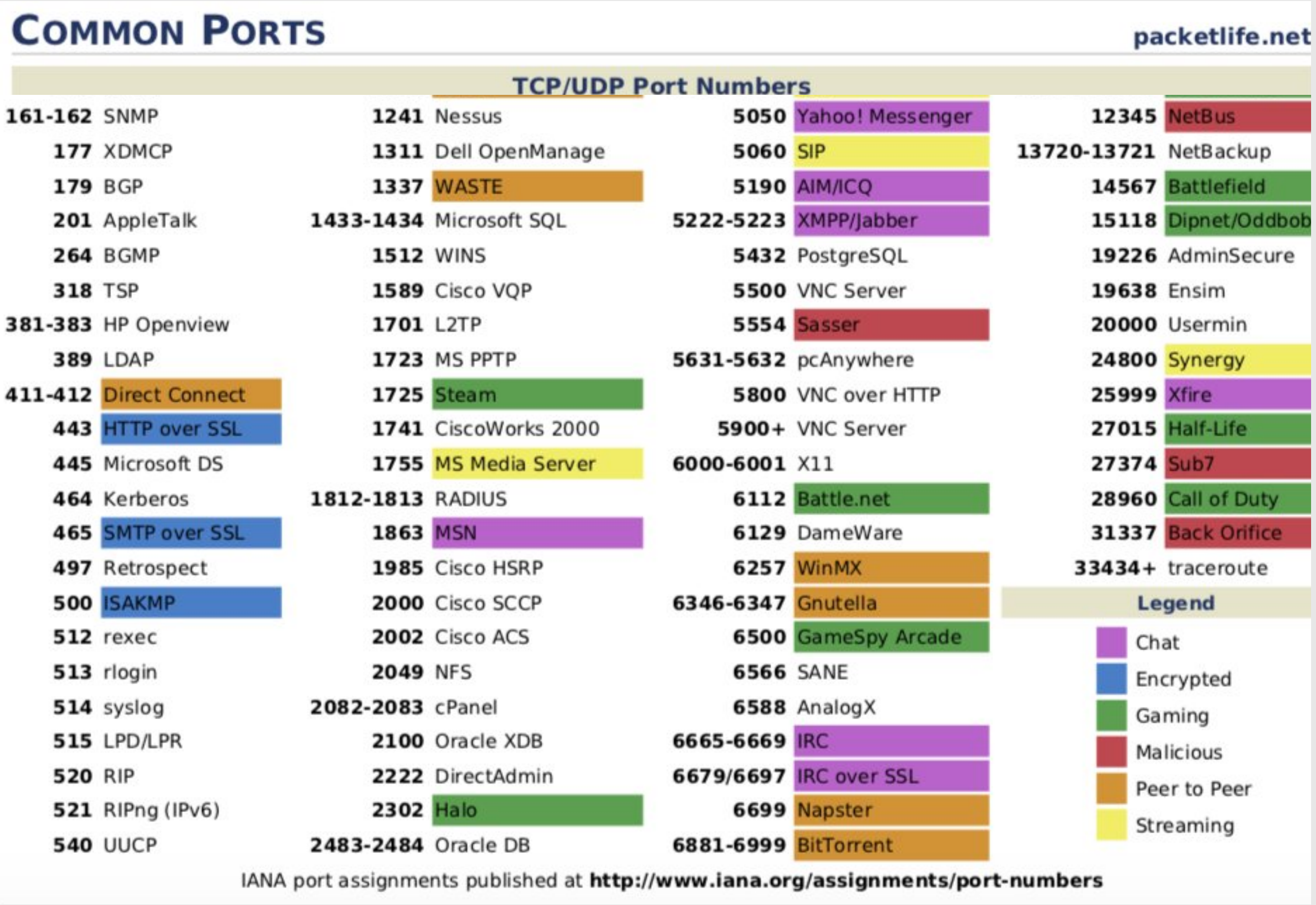
7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life

Tools:
Nmap & MasScan

Problems? => /8 = 16777214 hosts

Solution:
https://github.com/hoodoer/Top-Port-Slicer

Port Scan



Common Ports packetlife.net

TCP/UDP Port Numbers

161-162	SNMP	**1241**	Nessus	**5050**	Yahoo! Messenger	**12345**	NetBus
177	XDMCP	**1311**	Dell OpenManage	**5060**	SIP	**13720-13721**	NetBackup
179	BGP	**1337**	WASTE	**5190**	AIM/ICQ	**14567**	Battlefield
201	AppleTalk	**1433-1434**	Microsoft SQL	**5222-5223**	XMPP/Jabber	**15118**	Dipnet/Oddbob
264	BGMP	**1512**	WINS	**5432**	PostgreSQL	**19226**	AdminSecure
318	TSP	**1589**	Cisco VQP	**5500**	VNC Server	**19638**	Ensim
381-383	HP Openview	**1701**	L2TP	**5554**	Sasser	**20000**	Usermin
389	LDAP	**1723**	MS PPTP	**5631-5632**	pcAnywhere	**24800**	Synergy
411-412	Direct Connect	**1725**	Steam	**5800**	VNC over HTTP	**25999**	Xfire
443	HTTP over SSL	**1741**	CiscoWorks 2000	**5900+**	VNC Server	**27015**	Half-Life
445	Microsoft DS	**1755**	MS Media Server	**6000-6001**	X11	**27374**	Sub7
464	Kerberos	**1812-1813**	RADIUS	**6112**	Battle.net	**28960**	Call of Duty
465	SMTP over SSL	**1863**	MSN	**6129**	DameWare	**31337**	Back Orifice
497	Retrospect	**1985**	Cisco HSRP	**6257**	WinMX	**33434+**	traceroute
500	ISAKMP	**2000**	Cisco SCCP	**6346-6347**	Gnutella		**Legend**
512	rexec	**2002**	Cisco ACS	**6500**	GameSpy Arcade	🟪	Chat
513	rlogin	**2049**	NFS	**6566**	SANE	🟦	Encrypted
514	syslog	**2082-2083**	cPanel	**6588**	AnalogX	🟩	Gaming
515	LPD/LPR	**2100**	Oracle XDB	**6665-6669**	IRC	🟥	Malicious
520	RIP	**2222**	DirectAdmin	**6679/6697**	IRC over SSL	🟧	Peer to Peer
521	RIPng (IPv6)	**2302**	Halo	**6699**	Napster	🟨	Streaming
540	UUCP	**2483-2484**	Oracle DB	**6881-6999**	BitTorrent		

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

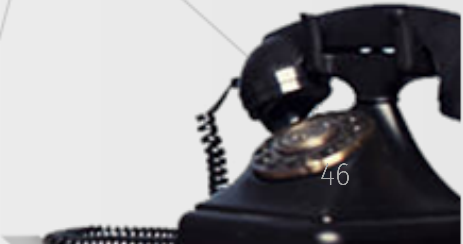
Tools:
Nmap & MasScan

Problems? => /8 = 16777214 hosts

Solution:
https://github.com/hoodoer/Top-Port-Slicer

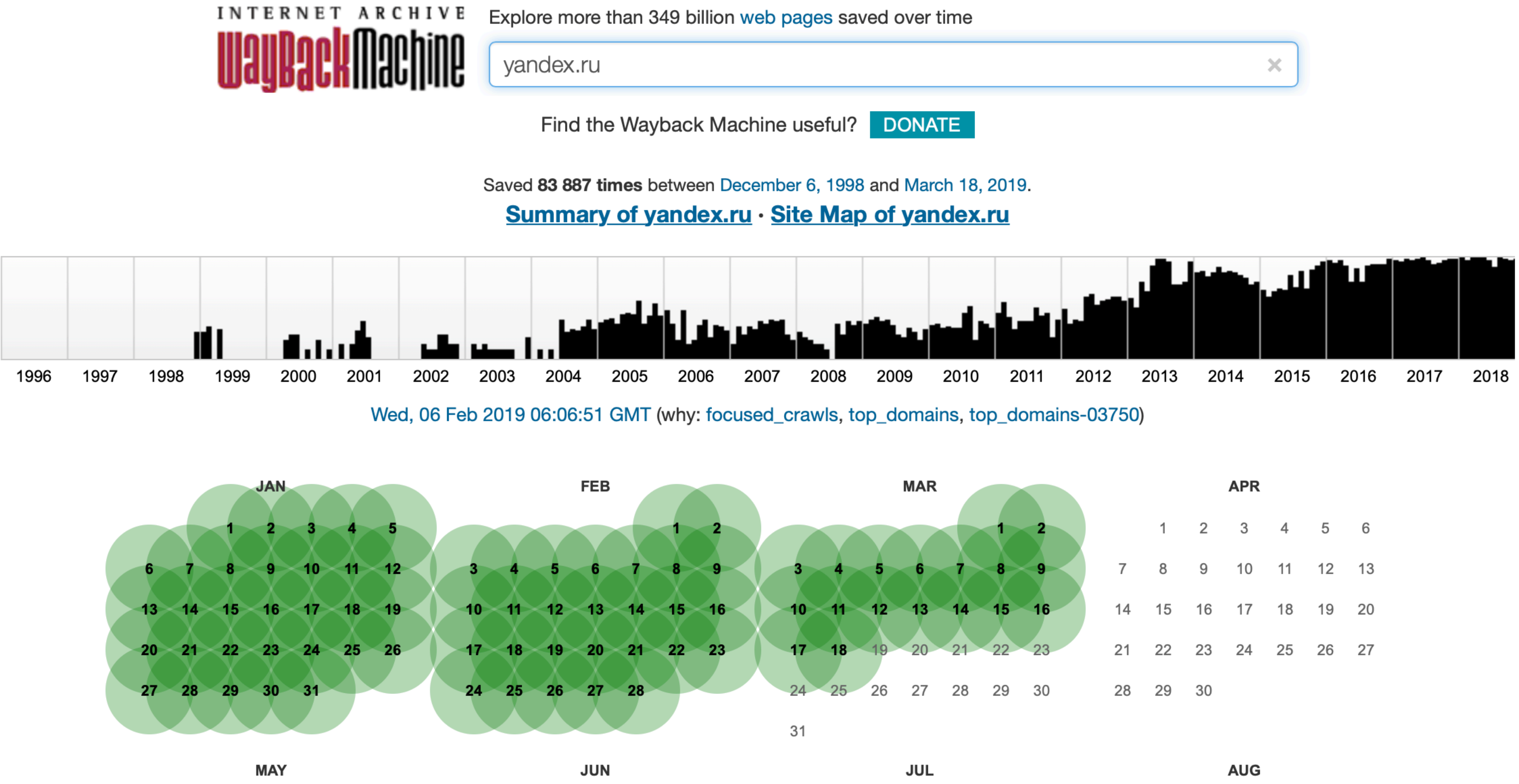
Further lookup

You probably found bunch of new services to test at this point. Good job.



Wayback Machine

Archive.org



Explore more than 349 billion web pages saved over time

yandex.ru

Find the Wayback Machine useful? DONATE

Saved **83 887 times** between December 6, 1998 and March 18, 2019.

Summary of yandex.ru · **Site Map of yandex.ru**

Wed, 06 Feb 2019 06:06:51 GMT (why: focused_crawls, top_domains, top_domains-03750)

JAN

1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31

FEB

1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28

MAR

1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31

APR

1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30

MAY

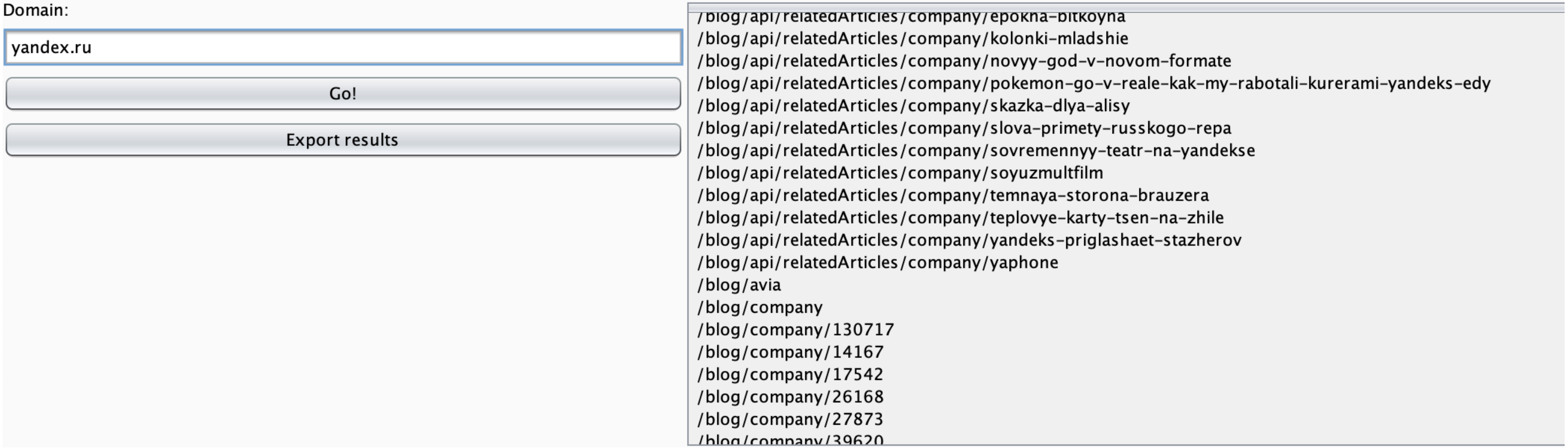
JUN

JUL

AUG

Wayback Machine

Burp Plugin Wayback Machine



Domain: yandex.ru

```
/blog/api/relatedArticles/company/epokna-bitkoyna
/blog/api/relatedArticles/company/kolonki-mladshie
/blog/api/relatedArticles/company/novyy-god-v-novom-formate
/blog/api/relatedArticles/company/pokemon-go-v-reale-kak-my-rabotali-kurerami-yandeks-edy
/blog/api/relatedArticles/company/skazka-dlya-alisy
/blog/api/relatedArticles/company/slova-primety-russkogo-repa
/blog/api/relatedArticles/company/sovremennyy-teatr-na-yandekse
/blog/api/relatedArticles/company/soyuzmultfilm
/blog/api/relatedArticles/company/temnaya-storona-brauzera
/blog/api/relatedArticles/company/teplovye-karty-tsen-na-zhile
/blog/api/relatedArticles/company/yandeks-priglashaet-stazherov
/blog/api/relatedArticles/company/yaphone
/blog/avia
/blog/company
/blog/company/130717
/blog/company/14167
/blog/company/17542
/blog/company/26168
/blog/company/27873
/blog/company/39620
```

Enumerating JS Endpoints

Why does it matter?

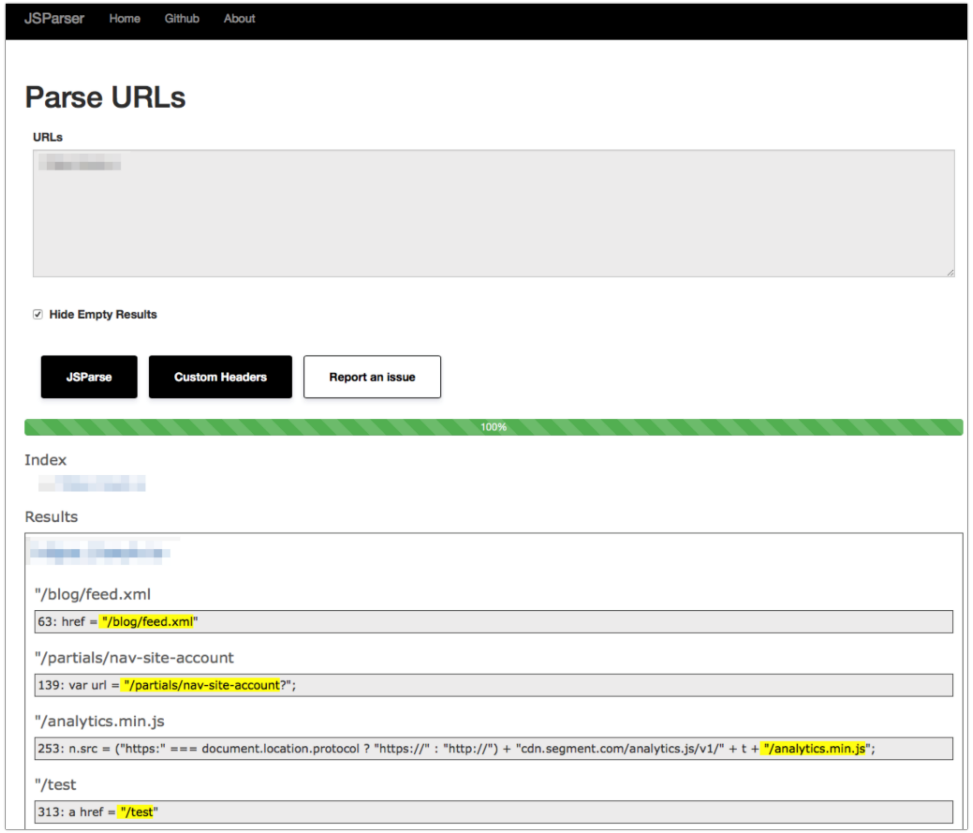
Top cases from my practice:

1. Loggers => Blind XSS
2. Proxy => Open redirect & SSRF
3. Server-side misconfigurations => RCE
4. Caching issues => injections

Enumerating JS Endpoints

JSParser

https://github.com/nahamsec/JSParser



Parse URLs

URLs

[redacted]

☑ Hide Empty Results

Index

[redacted]

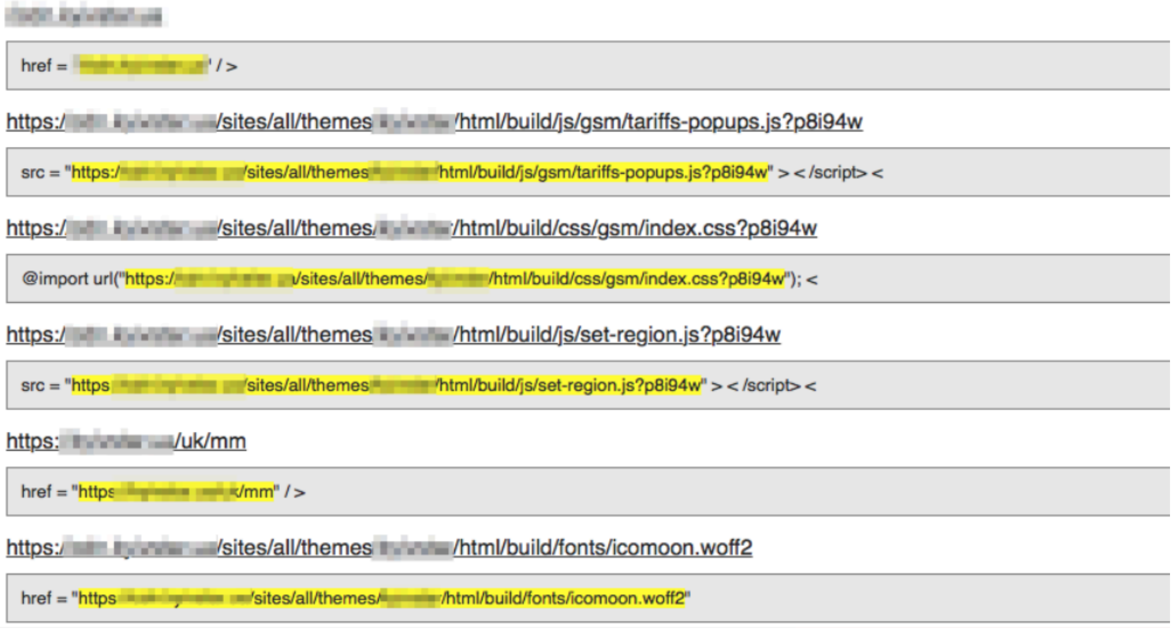
Results

[redacted]

```
"/blog/feed.xml
63: href = "/blog/feed.xml"

"/partials/nav-site-account
139: var url = "/partials/nav-site-account?";

"/analytics.min.js
253: n.src = ("https:" === document.location.protocol ? "https://" : "http://") + "cdn.segment.com/analytics.js/v1/" + t + "/analytics.min.js";

"/test
313: a href = "/test"
```

LinkFinder

https://github.com/GerbenJavado/LinkFinder



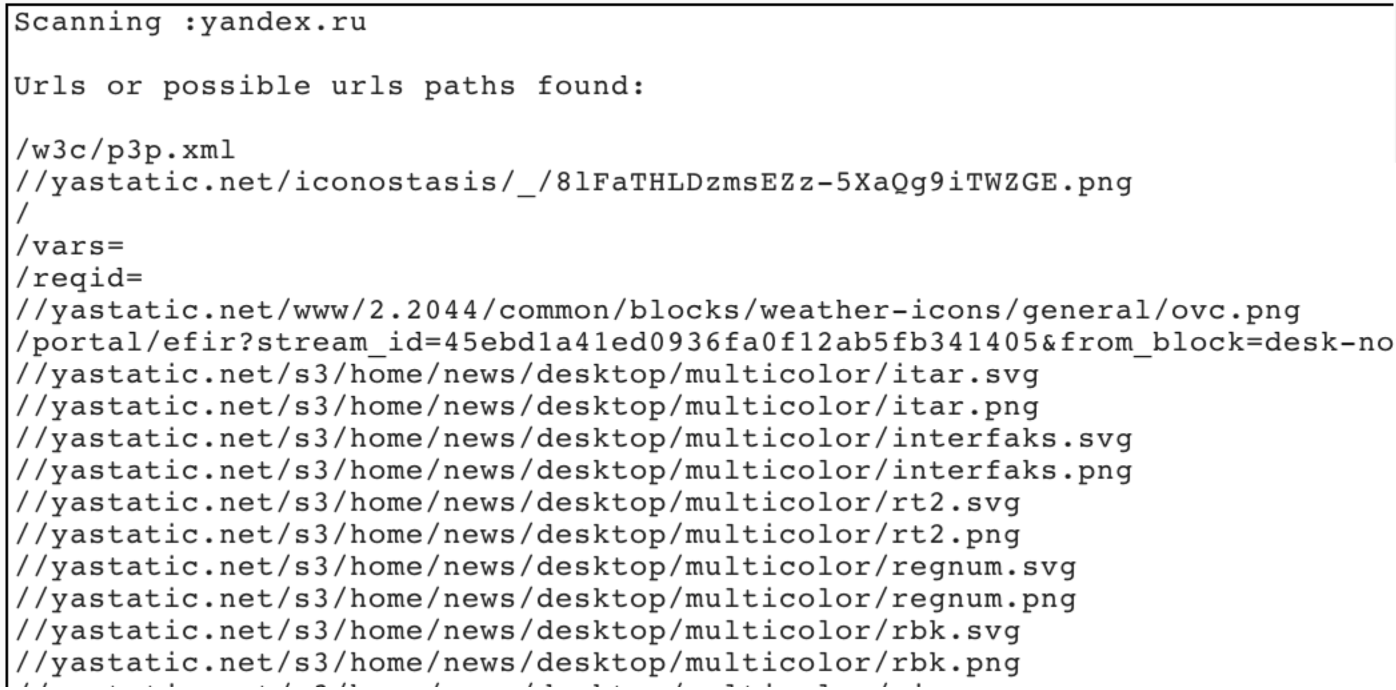
[redacted]

```
href = [redacted]' / >

https:/[redacted]/sites/all/themes[redacted]/html/build/js/gsm/tariffs-popups.js?p8i94w
src = "https:/[redacted]/sites/all/themes[redacted]html/build/js/gsm/tariffs-popups.js?p8i94w" > < /script> <

https:/[redacted]/sites/all/themes/[redacted]/html/build/css/gsm/index.css?p8i94w
@import url("https:/[redacted]/sites/all/themes/[redacted]/html/build/css/gsm/index.css?p8i94w"); <

https:/[redacted]/sites/all/themes[redacted]/html/build/js/set-region.js?p8i94w
src = "https[redacted]'sites/all/themes[redacted]'html/build/js/set-region.js?p8i94w" > < /script> <

https:[redacted]/uk/mm
href = "https[redacted]/mm" / >

https:/[redacted]/sites/all/themes[redacted]/html/build/fonts/icomoon.woff2
href = "https[redacted]'sites/all/themes/[redacted]/html/build/fonts/icomoon.woff2"
```

Enumerating JS Endpoints

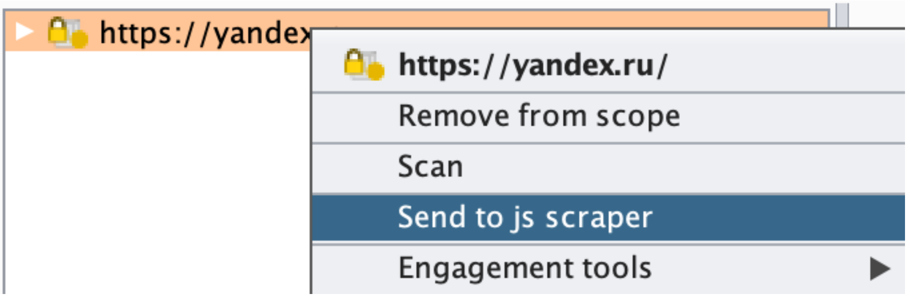
Js Path Extractor (Burp)

https://github.com/Lopseg/Jsdir



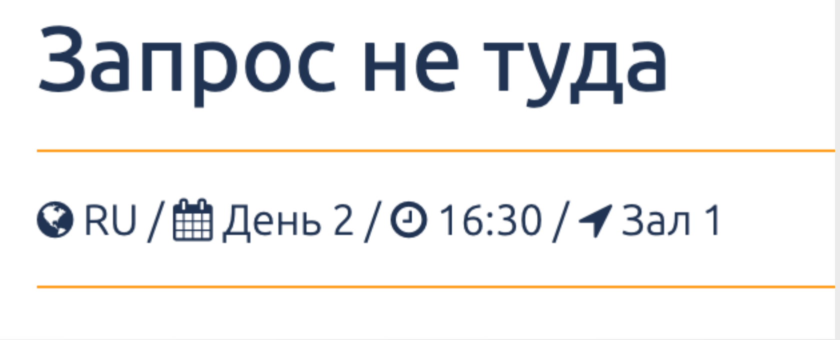
```
Scanning :yandex.ru

Urls or possible urls paths found:

/w3c/p3p.xml
//yastatic.net/iconostasis/_/81FaTHLDzmsEZz-5XaQg9iTWZGE.png
/
/vars=
/reqid=
//yastatic.net/www/2.2044/common/blocks/weather-icons/general/ovc.png
/portal/efir?stream_id=45ebd1a41ed0936fa0f12ab5fb341405&from_block=desk-notif-stream&from=morda
//yastatic.net/s3/home/news/desktop/multicolor/itar.svg
//yastatic.net/s3/home/news/desktop/multicolor/itar.png
//yastatic.net/s3/home/news/desktop/multicolor/interfaks.svg
//yastatic.net/s3/home/news/desktop/multicolor/interfaks.png
//yastatic.net/s3/home/news/desktop/multicolor/rt2.svg
//yastatic.net/s3/home/news/desktop/multicolor/rt2.png
//yastatic.net/s3/home/news/desktop/multicolor/regnum.svg
//yastatic.net/s3/home/news/desktop/multicolor/regnum.png
//yastatic.net/s3/home/news/desktop/multicolor/rbk.svg
//yastatic.net/s3/home/news/desktop/multicolor/rbk.png
```

Can I do it with burp? (Yes)



Place for your AD here

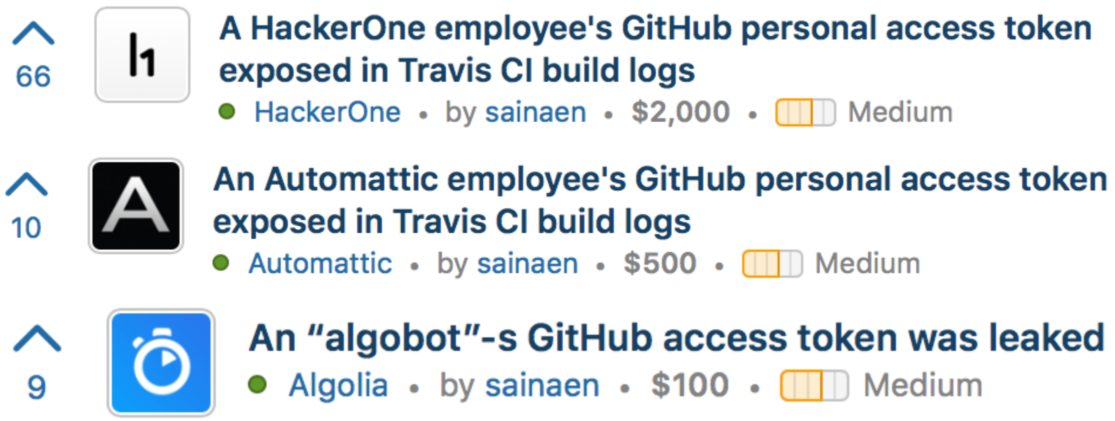
Want to know more about SSRF? You may want to visit this speech =>



Запрос не туда

RU / День 2 / 16:30 / Зал 1

Dive into .git leaks

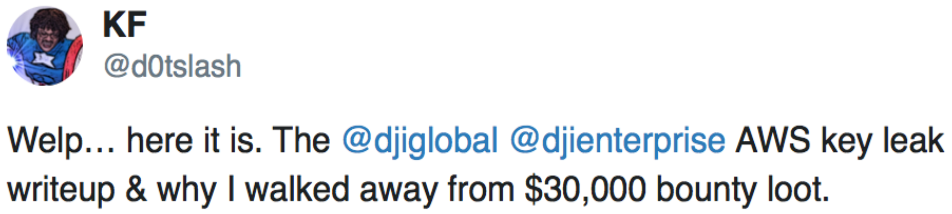


66 — A HackerOne employee's GitHub personal access token exposed in Travis CI build logs
● HackerOne • by sainaen • $2,000 • Medium

10 — An Automattic employee's GitHub personal access token exposed in Travis CI build logs
● Automattic • by sainaen • $500 • Medium

9 — An “algobot”-s GitHub access token was leaked
● Algolia • by sainaen • $100 • Medium

sainaen



KF
@d0tslash

Welp… here it is. The @djiglobal @djienterprise AWS key leak writeup & why I walked away from $30,000 bounty loot.

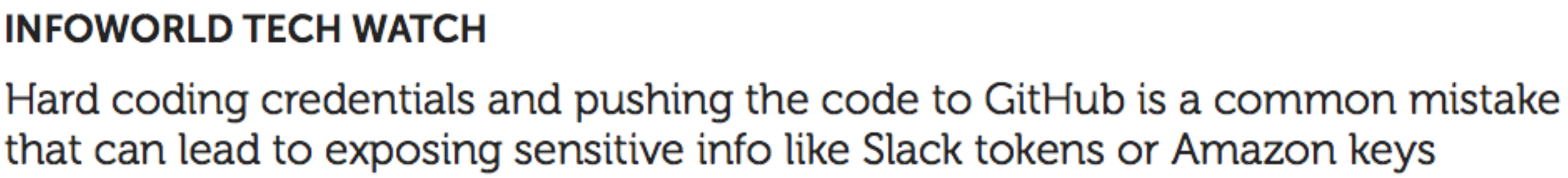
$30.000 or go to jail?

aws

Bug Price: $100 - $30.000

$1.500 Bounty, AWS key leak via GitHub

Dive into .git leaks

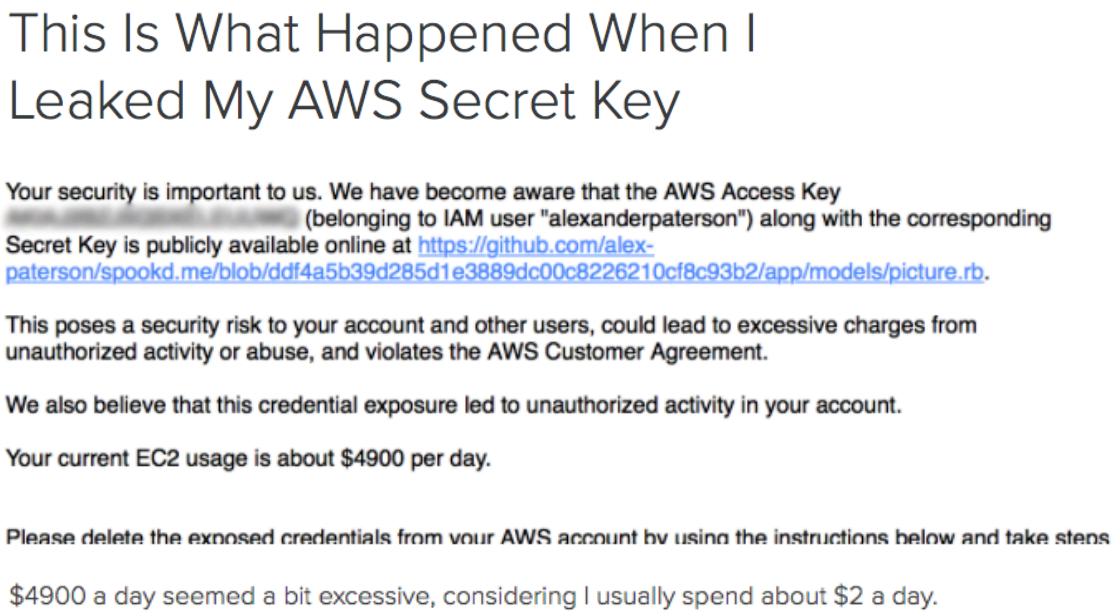


INFOWORLD TECH WATCH

Hard coding credentials and pushing the code to GitHub is a common mistake that can lead to exposing sensitive info like Slack tokens or Amazon keys

Miscreants racked up a $64,000 bill on DXC Technologies' tab after a techie accidentally uploaded the outsourcing firm's private AWS key to a public GitHub repo.

Private keys on public GitHub



This Is What Happened When I Leaked My AWS Secret Key

Your security is important to us. We have become aware that the AWS Access Key [redacted] (belonging to IAM user "alexanderpaterson") along with the corresponding Secret Key is publicly available online at https://github.com/alex-paterson/spookd.me/blob/ddf4a5b39d285d1e3889dc00c8226210cf8c93b2/app/models/picture.rb.

This poses a security risk to your account and other users, could lead to excessive charges from unauthorized activity or abuse, and violates the AWS Customer Agreement.

We also believe that this credential exposure led to unauthorized activity in your account.

Your current EC2 usage is about $4900 per day.

Please delete the exposed credentials from your AWS account by using the instructions below and take steps

$4900 a day seemed a bit excessive, considering I usually spend about $2 a day.

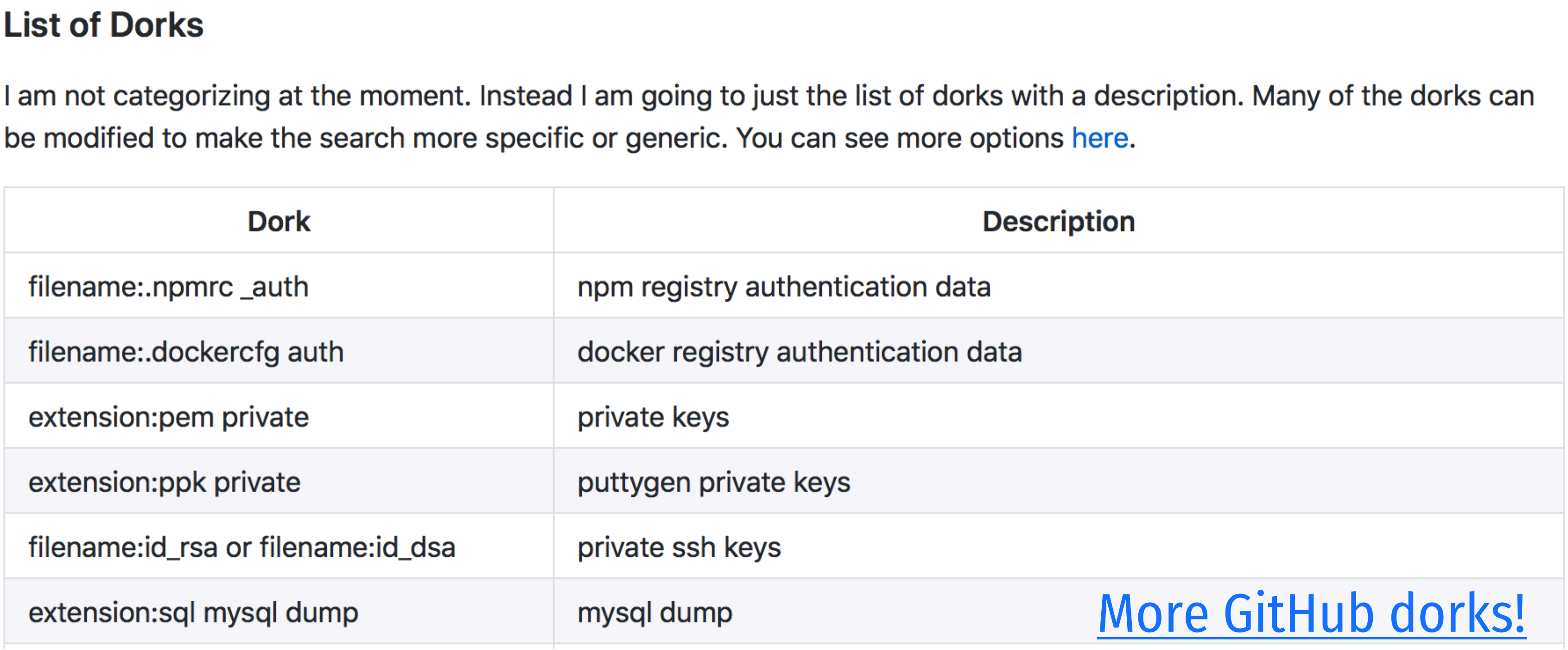
How to lost $4.900 in one day

Explore GitHub with Dorks

A couple of useful articles about Dorks:

https://xakep.ru/2015/07/08/google-hidden-functions/

https://xakep.ru/2017/09/21/google-dorks/



List of Dorks

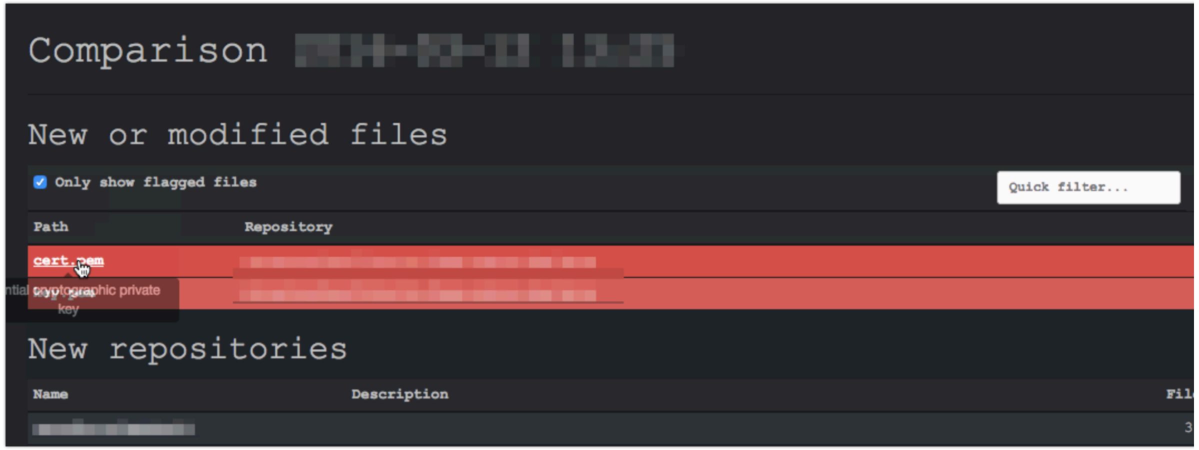
I am not categorizing at the moment. Instead I am going to just the list of dorks with a description. Many of the dorks can be modified to make the search more specific or generic. You can see more options here.

Dork	Description
filename:.npmrc _auth	npm registry authentication data
filename:.dockercfg auth	docker registry authentication data
extension:pem private	private keys
extension:ppk private	puttygen private keys
filename:id_rsa or filename:id_dsa	private ssh keys
extension:sql mysql dump	mysql dump

More GitHub dorks!

GitRob v1.1.2

https://github.com/michenriksen/gitrob



Comparison [redacted]

New or modified files

☑ Only show flagged files

Quick filter...

Path	Repository
cert.pem	[redacted]
	[redacted]

ntial cryptographic private key

New repositories

Name	Description	Fil
[redacted]		3

Additional info in developer blog post

Also some new features of v. 1.0.0

Good:

- Lots of cheks
- Flexible, also dig into the company's employees' personal GitHub pages
- Well structured
- Enables Continuous Monitoring

Bad:

- Signature checks
- Slow
- Last signature update was 2 years ago
- GitHub Only

GitMiner

https://github.com/michenriksen/gitrob

GitHub Dorks Cheat Sheet

+ **Good:**

- Easy to build, Docker is available too
- You can add your custom crafted GitHub Dorks

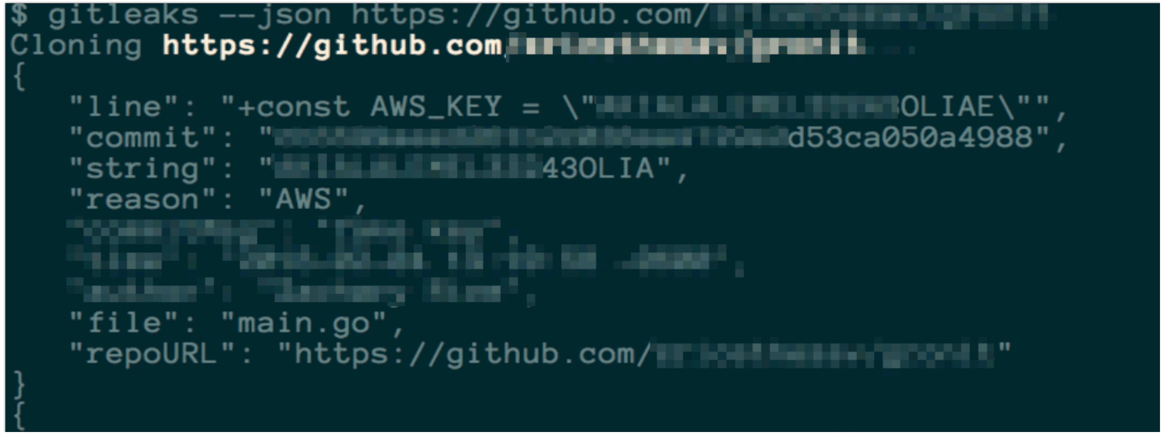
− **Bad:**

- Small list of hardcoded checks
- Slow
- GitHub Only

GitRob v1.1.2

https://github.com/michenriksen/gitrob

GITLEAKS



```
$ gitleaks --json https://github.com/[redacted]
Cloning https://github.com[redacted]
{
    "line": "+const AWS_KEY = \"[redacted]OLIAE\"",
    "commit": "[redacted]d53ca050a4988",
    "string": "[redacted]430LIA",
    "reason": "AWS",
    [redacted]
    "file": "main.go",
    "repoURL": "https://github.com/[redacted]"
}
{
```

RegExp CheatSheet

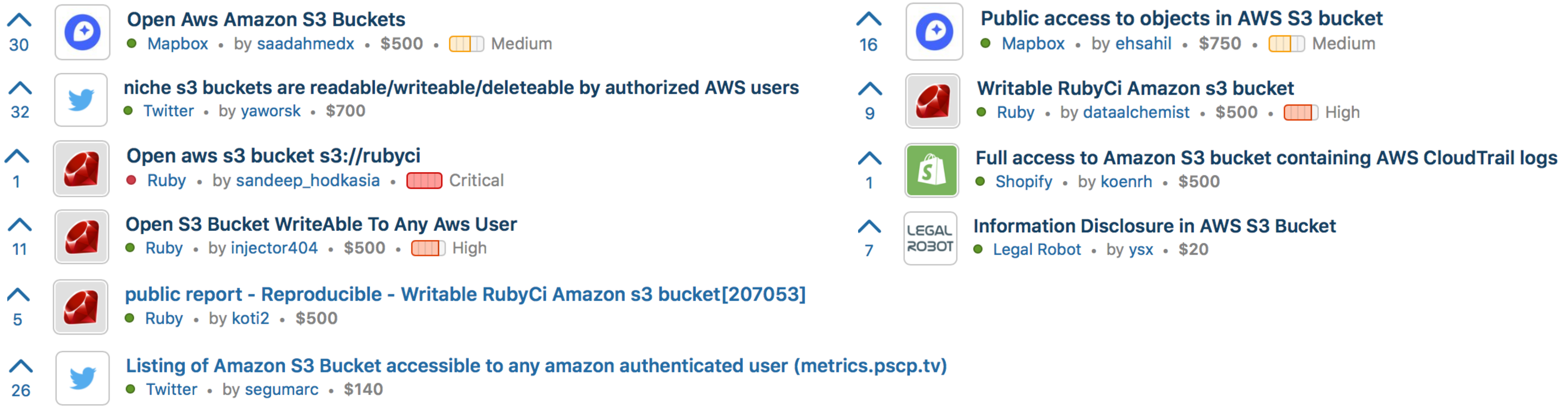
Good:

- Easy to build
- Works with any platform (any .git repos)
- Fast (Go lang)
- Search based on RegExp, you can add your own at any time

Bad:

- RegExp skill based tool
- Might be less effective with GitHub search than his GitHub-only analogs

Dive into .git leaks



30 **Open Aws Amazon S3 Buckets**
● Mapbox • by saadahmedx • $500 • Medium

32 **niche s3 buckets are readable/writeable/deleteable by authorized AWS users**
● Twitter • by yaworsk • $700

1 **Open aws s3 bucket s3://rubyci**
● Ruby • by sandeep_hodkasia • Critical

11 **Open S3 Bucket WriteAble To Any Aws User**
● Ruby • by injector404 • $500 • High

5 **public report - Reproducible - Writable RubyCi Amazon s3 bucket[207053]**
● Ruby • by koti2 • $500

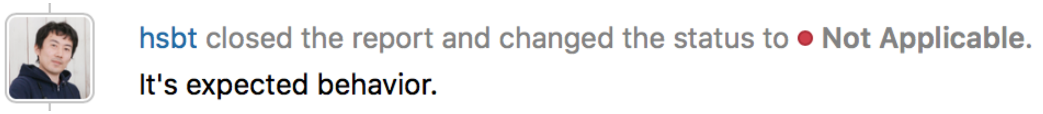
26 **Listing of Amazon S3 Bucket accessible to any amazon authenticated user (metrics.pscp.tv)**
● Twitter • by segumarc • $140

16 **Public access to objects in AWS S3 bucket**
● Mapbox • by ehsahil • $750 • Medium

9 **Writable RubyCi Amazon s3 bucket**
● Ruby • by dataalchemist • $500 • High

1 **Full access to Amazon S3 bucket containing AWS CloudTrail logs**
● Shopify • by koenrh • $500

7 **Information Disclosure in AWS S3 Bucket**
● Legal Robot • by ysx • $20

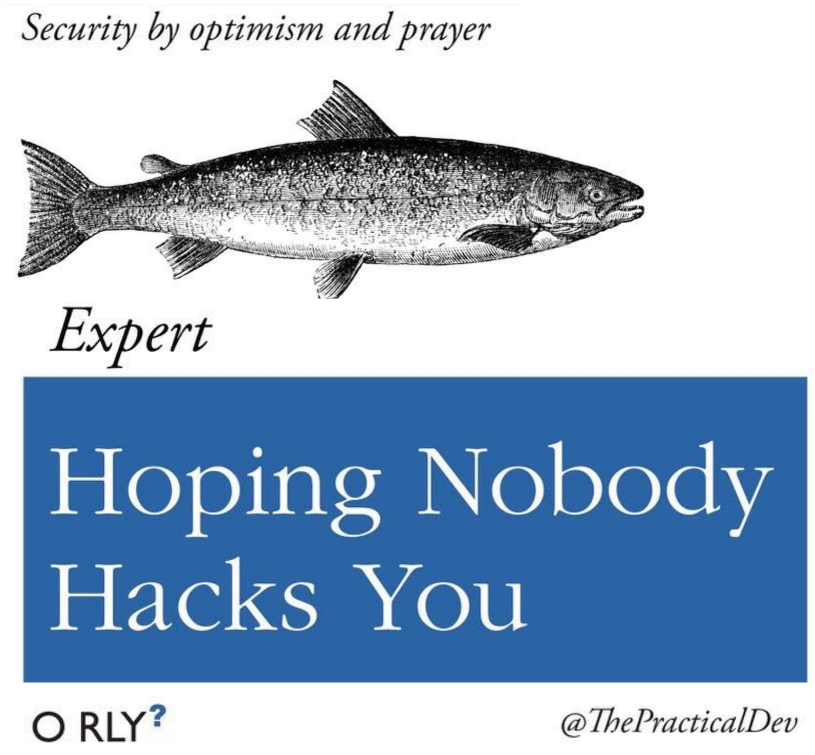


hsbt closed the report and changed the status to ● **Not Applicable.**

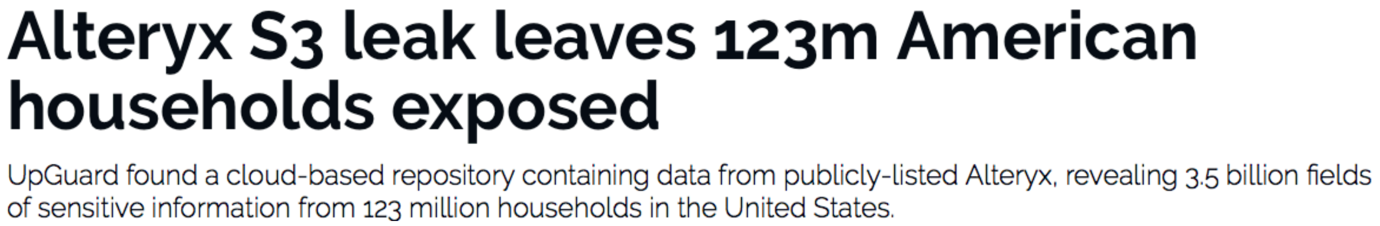
It's expected behavior.

Bug Price: $20 - $750

Cloud Storages

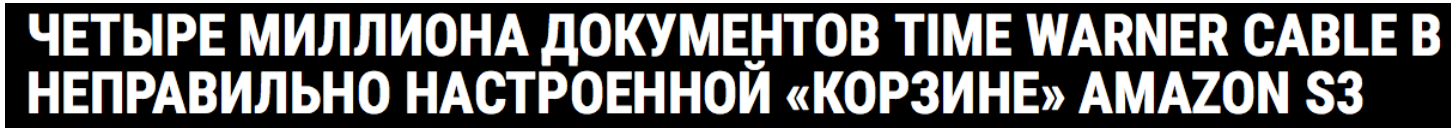


Bug Price: $20 - $750

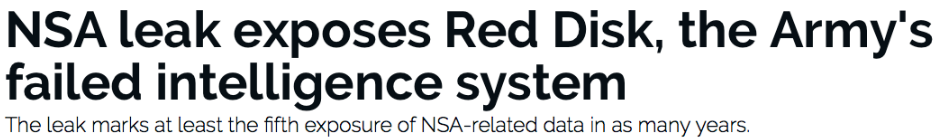


Alteryx S3 leak leaves 123m American households exposed

UpGuard found a cloud-based repository containing data from publicly-listed Alteryx, revealing 3.5 billion fields of sensitive information from 123 million households in the United States.

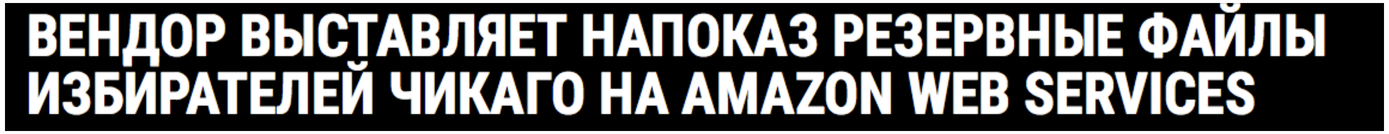


ЧЕТЫРЕ МИЛЛИОНА ДОКУМЕНТОВ TIME WARNER CABLE В НЕПРАВИЛЬНО НАСТРОЕННОЙ «КОРЗИНЕ» AMAZON S3

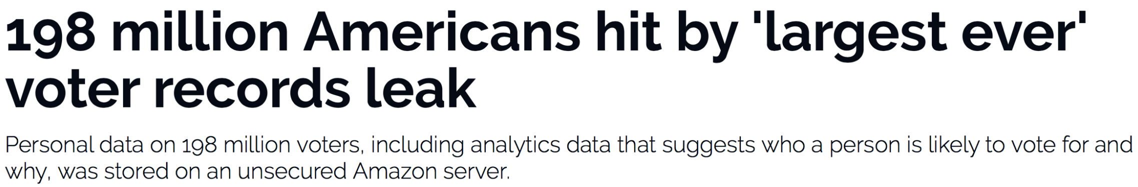


NSA leak exposes Red Disk, the Army's failed intelligence system

The leak marks at least the fifth exposure of NSA-related data in as many years.

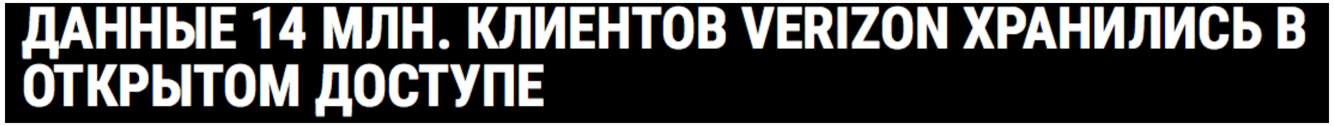


ВЕНДОР ВЫСТАВЛЯЕТ НАПОКАЗ РЕЗЕРВНЫЕ ФАЙЛЫ ИЗБИРАТЕЛЕЙ ЧИКАГО НА AMAZON WEB SERVICES



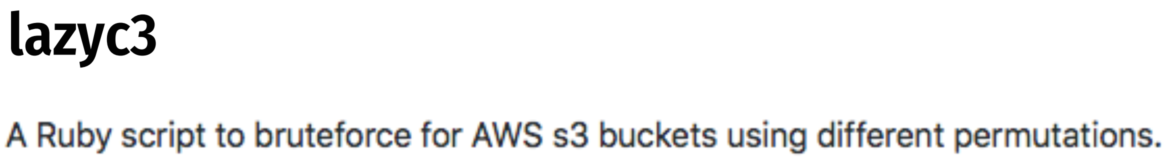
198 million Americans hit by 'largest ever' voter records leak

Personal data on 198 million voters, including analytics data that suggests who a person is likely to vote for and why, was stored on an unsecured Amazon server.



ДАННЫЕ 14 МЛН. КЛИЕНТОВ VERIZON ХРАНИЛИСЬ В ОТКРЫТОМ ДОСТУПЕ

Lookup

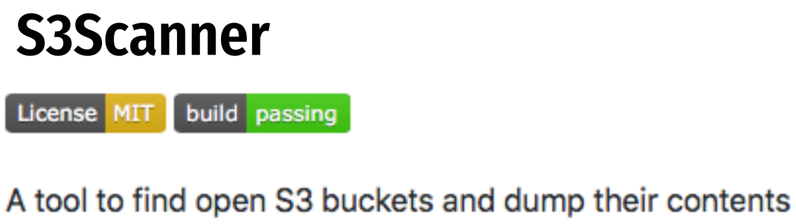


lazyc3

A Ruby script to bruteforce for AWS s3 buckets using different permutations.

https://github.com/nahamsec/lazys3.git

Read this first



S3Scanner

License MIT build passing

A tool to find open S3 buckets and dump their contents

https://github.com/sa7mon/S3Scanner

Lookup

And what about this two?

Google Cloud Storage

bucketNameHere.storage.googleapis.com/g

storage.googleapis.com/*bucketNameHere*

Azure Blob Storage

bucketNameHere.blob.core.windows.net

Google Dorks?

BucketSnoop

https://github.com/olihough86/BucketSnoop

BucketSnoop

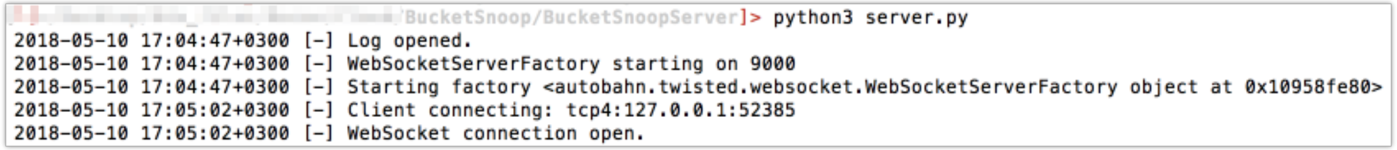
A Firefox extension and WebSocket handler that checks s3 buckets while your browse. All the checks are passive, I'm not a fan of just throwing files into storage that isn't mine, it's easy enough to check manually with aws cli.

amazon web services S3

Google Cloud Platform

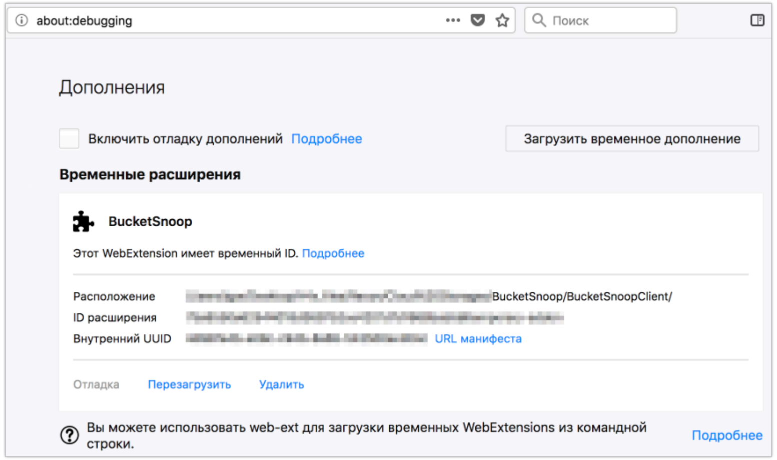
Ez lookup way

1 Launch Server



```
[redacted]BucketSnoop/BucketSnoopServer]> python3 server.py
2018-05-10 17:04:47+0300 [-] Log opened.
2018-05-10 17:04:47+0300 [-] WebSocketServerFactory starting on 9000
2018-05-10 17:04:47+0300 [-] Starting factory <autobahn.twisted.websocket.WebSocketServerFactory object at 0x10958fe80>
2018-05-10 17:05:02+0300 [-] Client connecting: tcp4:127.0.0.1:52385
2018-05-10 17:05:02+0300 [-] WebSocket connection open.
```

2 Install Extension



about:debugging

Поиск

Дополнения

□ Включить отладку дополнений Подробнее

Загрузить временное дополнение

Временные расширения

BucketSnoop

Этот WebExtension имеет временный ID. Подробнее

Расположение [redacted]BucketSnoop/BucketSnoopClient/

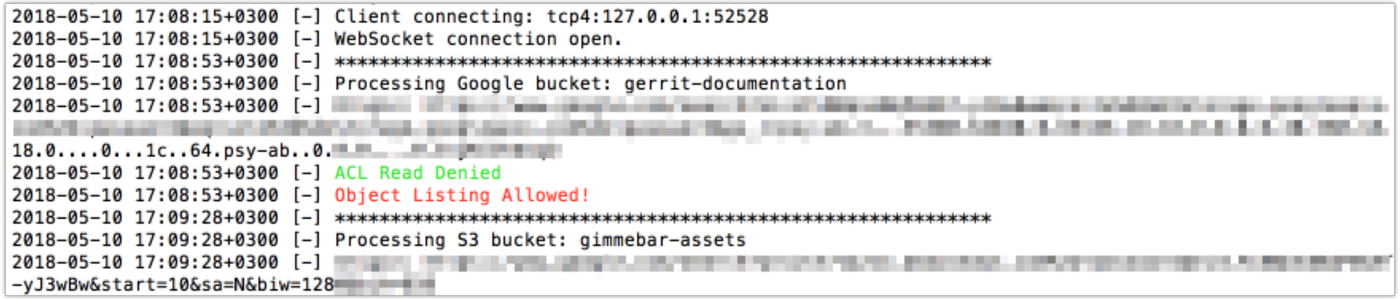
ID расширения [redacted]

Внутренний UUID [redacted] URL манифеста

Отладка Перезагрузить Удалить

Вы можете использовать web-ext для загрузки временных WebExtensions из командной строки. Подробнее

3 Just surf the web



```
2018-05-10 17:08:15+0300 [-] Client connecting: tcp4:127.0.0.1:52528
2018-05-10 17:08:15+0300 [-] WebSocket connection open.
2018-05-10 17:08:53+0300 [-] ***********************************************************
2018-05-10 17:08:53+0300 [-] Processing Google bucket: gerrit-documentation
2018-05-10 17:08:53+0300 [-] [redacted]
18.0....0...1c..64.psy-ab..0.[redacted]
2018-05-10 17:08:53+0300 [-] ACL Read Denied
2018-05-10 17:08:53+0300 [-] Object Listing Allowed!
2018-05-10 17:09:28+0300 [-] ***********************************************************
2018-05-10 17:09:28+0300 [-] Processing S3 bucket: gimmebar-assets
2018-05-10 17:09:28+0300 [-] [redacted]
-yJ3wBw&start=10&sa=N&biw=128[redacted]
```

Aws-extender

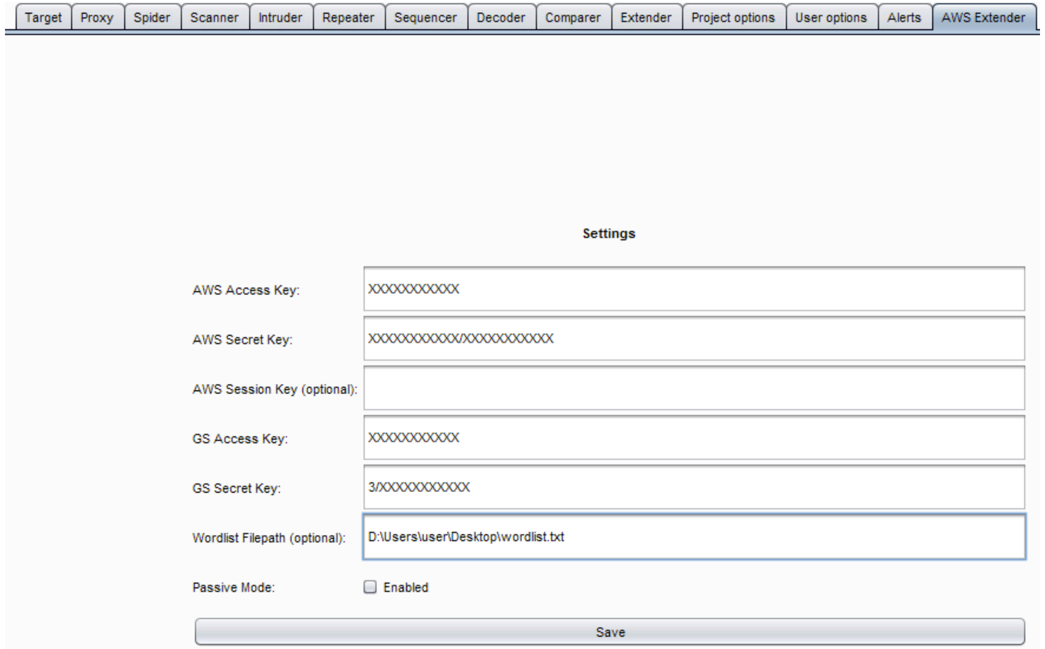
https://github.com/VirtueSecurity/aws-extender

AWS Extender

AWS Extender is a BurpSuite extension to identify and test S3 buckets as well as Google Storage buckets and Azure Storage containers for common misconfiguration issues using the boto/boto3 SDK library.

Probably the same as BucketSnoop, but in BURP!

1 Configure



Settings

AWS Access Key: XXXXXXXXXXXX

AWS Secret Key: XXXXXXXXXXXX/XXXXXXXXXXXX

AWS Session Key (optional):

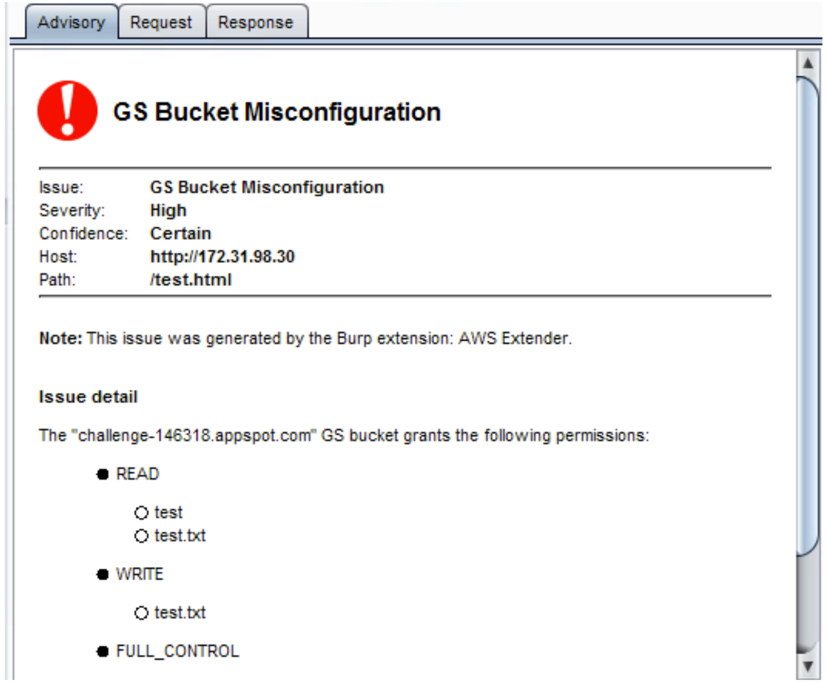
GS Access Key: XXXXXXXXXXXX

GS Secret Key: 3/XXXXXXXXXXXX

Wordlist Filepath (optional): D:\Users\user\Desktop\wordlist.txt

Passive Mode: □ Enabled

2 Surf



GS Bucket Misconfiguration

Issue: **GS Bucket Misconfiguration**
Severity: **High**
Confidence: **Certain**
Host: **http://172.31.98.30**
Path: **/test.html**

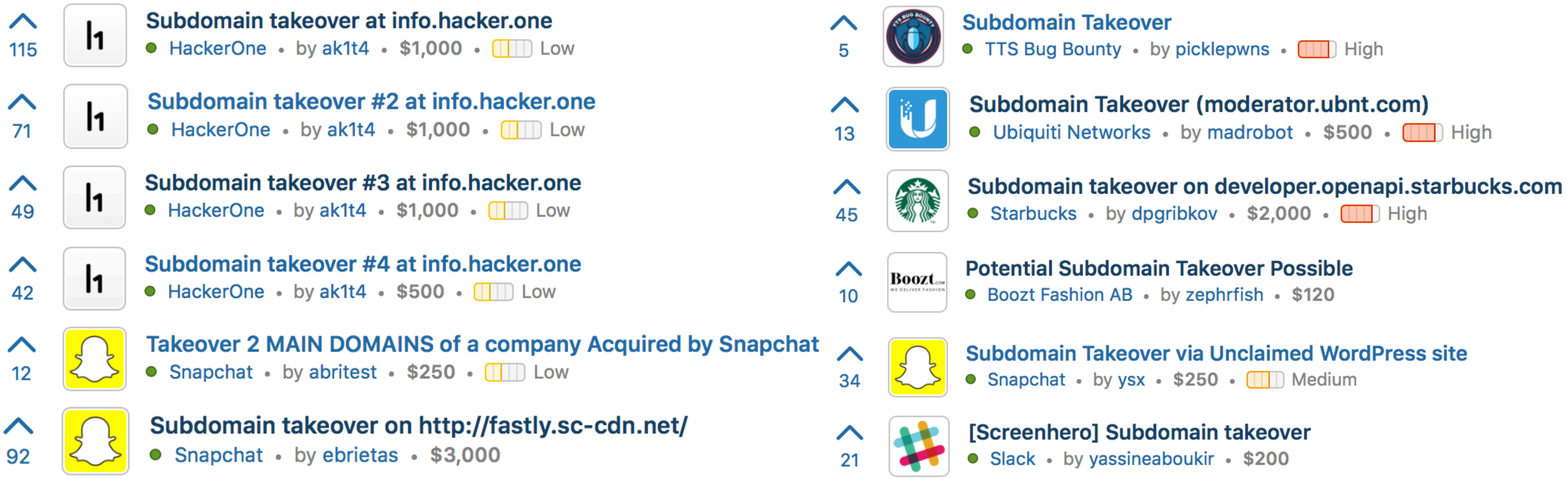
Note: This issue was generated by the Burp extension: AWS Extender.

Issue detail

The "challenge-146318.appspot.com" GS bucket grants the following permissions:

- READ
  - test
  - test.txt
- WRITE
  - test.txt
- FULL_CONTROL

Subdomain Takeover



115 **Subdomain takeover at info.hacker.one**
HackerOne • by ak1t4 • $1,000 • Low

71 **Subdomain takeover #2 at info.hacker.one**
HackerOne • by ak1t4 • $1,000 • Low

49 **Subdomain takeover #3 at info.hacker.one**
HackerOne • by ak1t4 • $1,000 • Low

42 **Subdomain takeover #4 at info.hacker.one**
HackerOne • by ak1t4 • $500 • Low

12 **Takeover 2 MAIN DOMAINS of a company Acquired by Snapchat**
Snapchat • by abritest • $250 • Low

92 **Subdomain takeover on http://fastly.sc-cdn.net/**
Snapchat • by ebrietas • $3,000

5 **Subdomain Takeover**
TTS Bug Bounty • by picklepwns • High

13 **Subdomain Takeover (moderator.ubnt.com)**
Ubiquiti Networks • by madrobot • $500 • High

45 **Subdomain takeover on developer.openapi.starbucks.com**
Starbucks • by dpgribkov • $2,000 • High

10 **Potential Subdomain Takeover Possible**
Boozt Fashion AB • by zephrfish • $120

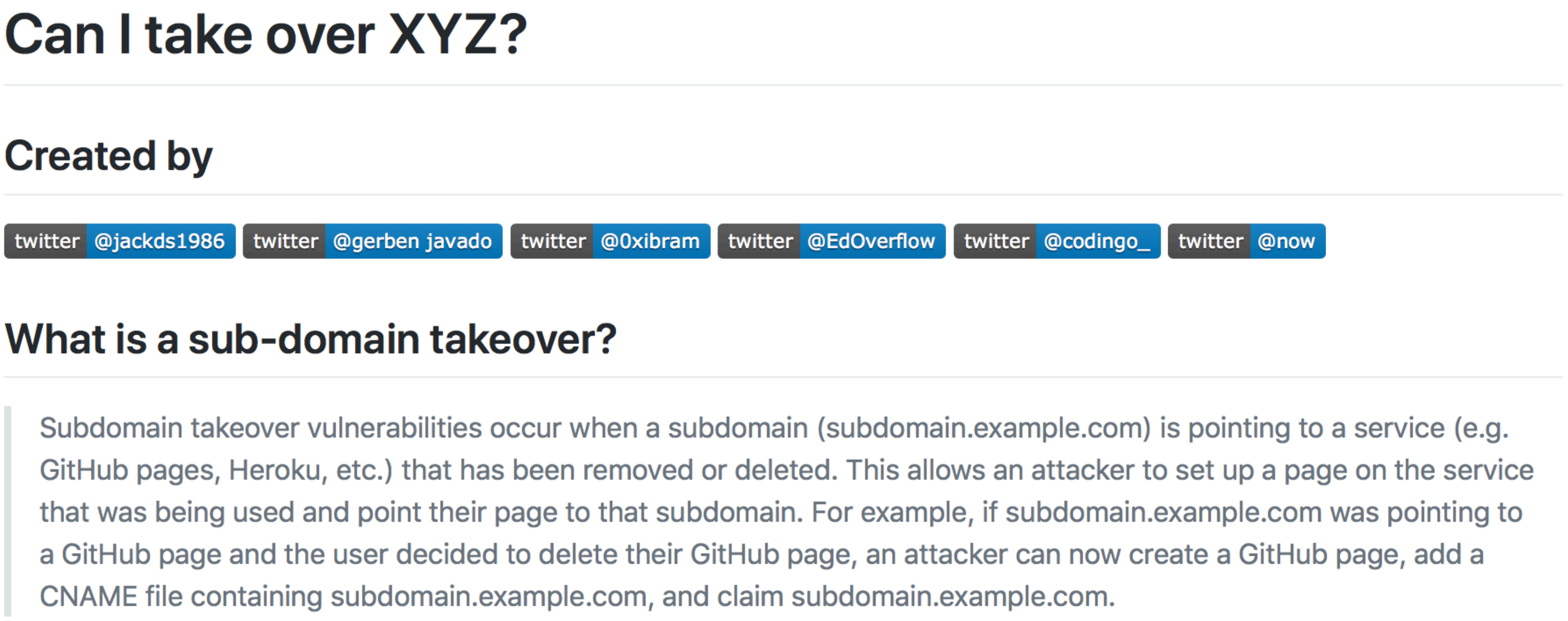
34 **Subdomain Takeover via Unclaimed WordPress site**
Snapchat • by ysx • $250 • Medium

21 **[Screenhero] Subdomain takeover**
Slack • by yassineaboukir • $200

Bug Price: $120 - $3000

Subdomain Takeover

DIG + Cheat Sheet



Can I take over XYZ?

Created by

twitter @jackds1986 twitter @gerben javado twitter @0xibram twitter @EdOverflow twitter @codingo_ twitter @now

What is a sub-domain takeover?

> Subdomain takeover vulnerabilities occur when a subdomain (subdomain.example.com) is pointing to a service (e.g. GitHub pages, Heroku, etc.) that has been removed or deleted. This allows an attacker to set up a page on the service that was being used and point their page to that subdomain. For example, if subdomain.example.com was pointing to a GitHub page and the user decided to delete their GitHub page, an attacker can now create a GitHub page, add a CNAME file containing subdomain.example.com, and claim subdomain.example.com.

Conclusion

- Don’t re-invent the wheel
- Understand whole cycle of automated work
- Improve what exist
- Don’t be a script kiddie

Digital Security

Thanks for your attention

inbox@dsec.ru

DSecRU

company/dsec/

company/dsecru

Moscow, headquaters

Saint Petersburg, R&D