

# Identifying 3rd Party Sinkhole Operations for Computer Network Defense and Threat Analysis

Michael B Jacobs

CERT Coordination Center  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213



Software Engineering Institute

Carnegie Mellon University

Identifying 3<sup>rd</sup> Party Sinkhole Operations

© 2015 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and distribution. Please see Copyright notice for non-US Government use and distribution.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0003324



# Outline

How I got here

Applying heuristics

Validation

Some open questions

# Heuristics for Finding Sinkholes

Some things just stand out

Parking services and sinkholes

Odd patterns of behavior (Gaps in known sinkhole IP)

Multiple actors on same infrastructure

Significant gaps in activity

# Pull this thread

frickl.purpledaily.com	54.248.229.24	30-Apr-14	30-Apr-14
zyxel.webhop.net	254.0.0.88	30-Apr-14	30-Apr-14
naver.ironybl00dy.net	23.253.46.64	30-Apr-14	30-Apr-14
news.firewall-gateway.com	109.169.77.230	29-Apr-14	29-Apr-14
publics-dns.com	91.194.254.94	29-Apr-14	24-Nov-14
baatarhuu.com	216.108.231.122	29-Apr-14	1-May-14
dataday3.no-ip.org	108.62.211.195	29-Apr-14	30-Apr-14
<b>uiop.wekby.com</b>	<b>23.253.46.64</b>	29-Apr-14	29-Apr-14
service.purpledaily.com	54.248.229.24	28-Apr-14	28-Apr-14
www.eshow-online.com	95.211.172.143	27-Apr-14	27-Apr-14
cancunluxurystyle.com	184.168.221.91	26-Apr-14	27-Apr-14
upinfo.biz	192.31.186.21	26-Apr-14	28-Apr-14
opmsecurity.org	184.168.221.39	26-Apr-14	28-Apr-14

# Pull this thread

uiop.wekby.com	173.212.56.174	21-Jun-12	28-Jul-12
uiop.wekby.com	108.61.4.52	4-Sep-12	4-Sep-12
uiop.wekby.com	69.43.161.172	10-May-12	31-Dec-12
uiop.wekby.com	199.59.163.207	1-Feb-13	7-Feb-13
uiop.wekby.com	69.43.161.179	27-Jun-11	12-Mar-13
uiop.wekby.com	141.8.224.25	1-Apr-13	1-Apr-13
uiop.wekby.com	69.43.161.174	19-Apr-13	19-Apr-13
uiop.wekby.com	<b>208.91.197.27</b>	28-Mar-14	28-Mar-14
uiop.wekby.com	23.253.46.64	29-Apr-14	29-Apr-14
uiop.wekby.com	208.91.197.132	18-Nov-15	20-Dec-15

# Identifying some patterns of behavior

<b>uiop.wekby.com</b>	208.91.197.27	28-Mar-14	28-Mar-14
<b>update.cnonlie.com</b>	208.91.197.216	23-Mar-13	30-Mar-13
updateie.net	208.91.197.134	11-Feb-14	11-Feb-14
wekby.com	208.91.197.27	9-Nov-13	8-Jan-14
<b>ww2.wekby.com</b>	208.91.197.132	18-Nov-15	20-Dec-15
www.cartek.com	208.91.197.132	3-Jul-15	4-Jul-15
www.didoa.dns-dns.com	208.91.197.132	7-Jan-13	7-Jan-13
www.syscation.net	208.91.197.44	21-Mar-13	1-May-13
www.twitterdocs.com	208.91.197.115	13-Jun-13	13-Jun-13
<b>www.update-adobe.com</b>	208.91.197.133	13-Dec-11	19-Jan-12
<b>filesassociate.net</b>	208.91.197.101	16-Jul-13	21-Jul-13
<b>cryptoanalysis.net</b>	208.91.197.101	1-Apr-13	1-Apr-13

# Find the Sinkhole

www.update-adobe.com	208.91.197.133	13-Dec-11	19-Jan-12
www.update-adobe.com	208.91.197.134	13-Dec-11	19-Jan-12
www.update-adobe.com	<b>23.22.175.89</b>	18-Oct-12	29-Nov-12

filesassociate.net	37.46.127.76	29-Jun-12	30-Oct-12
filesassociate.net	208.91.197.7	4-Jun-13	6-Jun-13
filesassociate.net	<b>95.211.172.143</b>	9-Sep-13	9-Feb-16

cryptoanalysis.net	208.91.197.101	1-Apr-13	1-Apr-13
cryptoanalysis.net	<b>81.166.122.234</b>	18-Dec-13	18-Dec-13
cryptoanalysis.net	69.195.129.72	31-Jul-15	31-Jul-15

# Gaps Between Known Sinkholes

phil-army.gotdns.org	123.232.63.3	4-Jun-14	4-Jun-14
phil-army.gotdns.org	87.106.24.200	1-Aug-14	11-Feb-15
phil-army.gotdns.org	<b>87.106.20.192</b>	3-Mar-15	23-Jan-16
phil-army.gotdns.org	213.165.83.176	3-Mar-15	23-Jan-16
phil-army.gotdns.org	74.208.164.166	22-Mar-15	6-Nov-15
phil-army.gotdns.org	<b>87.106.250.34</b>	22-Mar-15	6-Nov-15
phil-army.gotdns.org	108.175.9.189	22-Mar-15	6-Nov-15
phil-army.gotdns.org	<b>74.208.153.9</b>	31-Mar-15	23-Jan-16
phil-army.gotdns.org	<b>87.106.253.18</b>	2-Apr-15	23-Jan-16
phil-army.gotdns.org	<b>50.21.181.152</b>	3-Apr-15	23-Jan-16

# Multiple Actors on Same Infrastructure

Consider sinkhole IP candidate **81.166.122.234**

**454** domains

**148** Malware samples associated with domain

**18** Unique malware families

# Significant Gaps in Activity

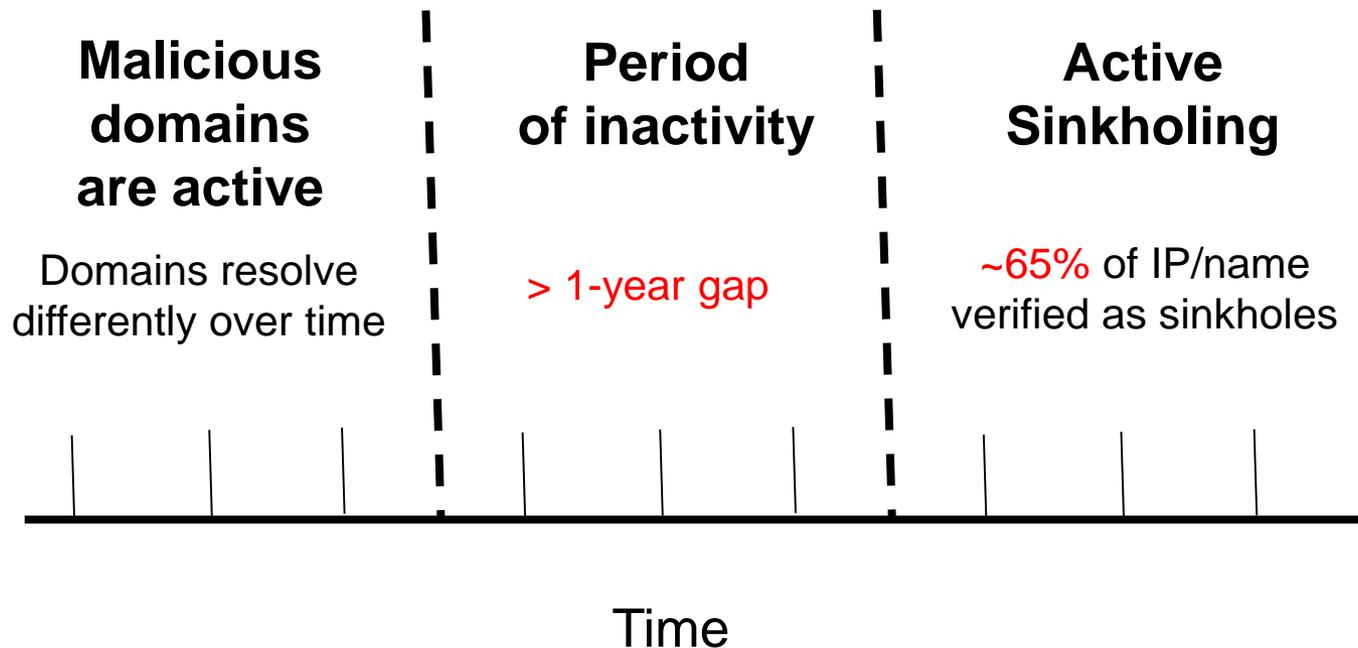
01ret.mrslove.com	46.37.162.57	28-Oct-12	4-Nov-12
01ret.mrslove.com	92.242.132.8	7-Feb-13	<b>7-Feb-13</b>
01ret.mrslove.com	<b>188.226.194.251</b>	<b>29-Jul-14</b>	17-Oct-15

asdepy.my03.com	188.165.95.15	26-Sep-12	<b>2-Oct-12</b>
asdepy.my03.com	<b>192.241.149.43</b>	<b>24-Jun-14</b>	24-Jun-14
asdepy.my03.com	188.226.194.251	18-Apr-15	14-Sep-15
asdepy.my03.com	46.101.26.41	30-Jan-16	30-Jan-16

astor1.xxuz.com	91.211.88.62	14-Apr-12	<b>12-Oct-12</b>
astor1.xxuz.com	<b>198.199.78.132</b>	<b>27-Mar-14</b>	27-Mar-14
astor1.xxuz.com	188.226.194.251	19-Aug-14	19-Aug-14

# Activity Gaps as a feature of (APT) sinkholing?

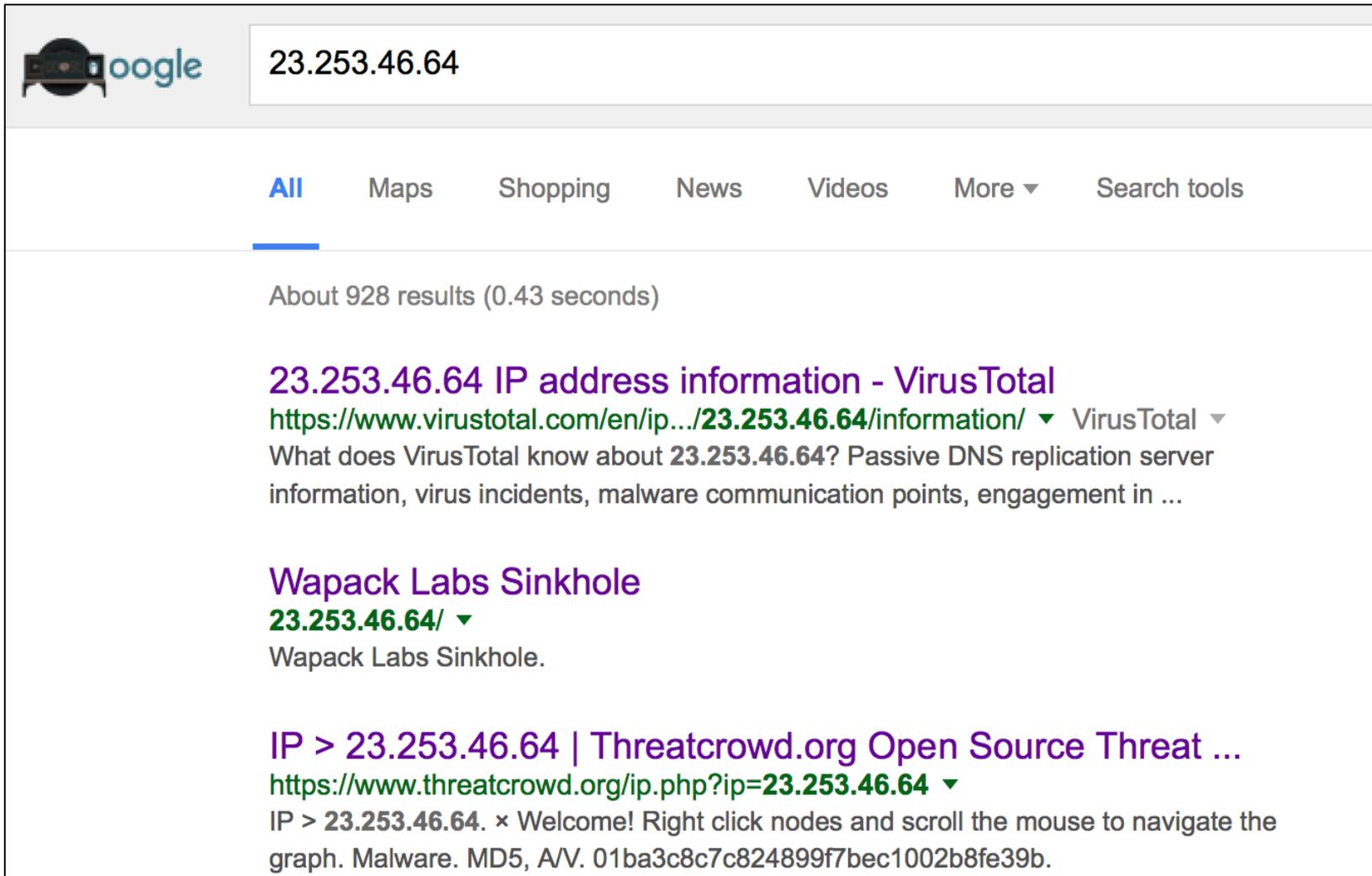
Starting with 683 domain/IP candidates...



Confirming what I've found are actually sinkholes...



# Just Google it!



The image shows a screenshot of a Google search interface. The search bar contains the IP address "23.253.46.64". Below the search bar, the "All" tab is selected. The search results show "About 928 results (0.43 seconds)". The first result is titled "23.253.46.64 IP address information - VirusTotal" with a URL starting with "https://www.virustotal.com/en/ip.../23.253.46.64/information/". The second result is titled "Wapack Labs Sinkhole" with a URL starting with "https://www.wapacklabs.com/sinkhole/23.253.46.64/". The third result is titled "IP > 23.253.46.64 | Threatcrowd.org Open Source Threat ..." with a URL starting with "https://www.threatcrowd.org/ip.php?ip=23.253.46.64".

23.253.46.64

All Maps Shopping News Videos More ▾ Search tools

About 928 results (0.43 seconds)

**23.253.46.64 IP address information - VirusTotal**  
<https://www.virustotal.com/en/ip.../23.253.46.64/information/> ▾ VirusTotal ▾  
What does VirusTotal know about **23.253.46.64**? Passive DNS replication server information, virus incidents, malware communication points, engagement in ...

**Wapack Labs Sinkhole**  
[23.253.46.64/](https://www.wapacklabs.com/sinkhole/23.253.46.64/) ▾  
Wapack Labs Sinkhole.

**IP > 23.253.46.64 | Threatcrowd.org Open Source Threat ...**  
<https://www.threatcrowd.org/ip.php?ip=23.253.46.64> ▾  
IP > **23.253.46.64**. × Welcome! Right click nodes and scroll the mouse to navigate the graph. Malware. MD5, A/V. 01ba3c8c7c824899f7bec1002b8fe39b.

# Keep It Simple Stupid (KISS)

... right there on the Unix command line:

```
$ host 87.106.253.18  
18.253.106.87.in-addr.arpa domain name pointer  
87-106-253-18.sinkhole.shadowserver.org
```

# Thank you, Passive DNS

Sometimes the nameserver says it all

```
/usr/bin/curl -Sks -H "X-API-Key: $key" -H "Accept:
application/json"
https://api.dnsdb.info/lookup/rrset/name/kabsersky.com/NS

[ "ns1-sinkhole.xaayda.com.", "ns2-sinkhole.xaayda.com." ]
```

For a list of all domains on the nameserver

```
/usr/bin/curl -Sks -H "X-API-Key: $key " -H "Accept:
application/json" https://api.dnsdb.info/lookup/rdata/name/ns1-
sinkhole.xaayda.com/
```

# Whois - Domaintools

Whois Server	whois.enom.com
<b>— Website</b>	
Website Title	 <b>Wapack Labs Sinkhole</b> 
Server Type	Microsoft-IIS/7.5
Response Code	200
SEO Score	95%
Terms	0 (Unique: 0, Linked: 0)
Images	1 (Alt tags missing: 0)
Links	1 (Internal: 0, Outbound: 1)
<b>Whois Record</b> ( last updated on 2016-01-26 )	
<pre>Domain Name: GOODMONGOL.COM Registry Domain ID: 1954607334_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.enom.com Registrar URL: www.enom.com</pre>	

Retrieved from: <http://whois.domaintools.com/goodmongol.com>

# Cool Tools - ThreatCrowd

## DNS RESOLUTIONS

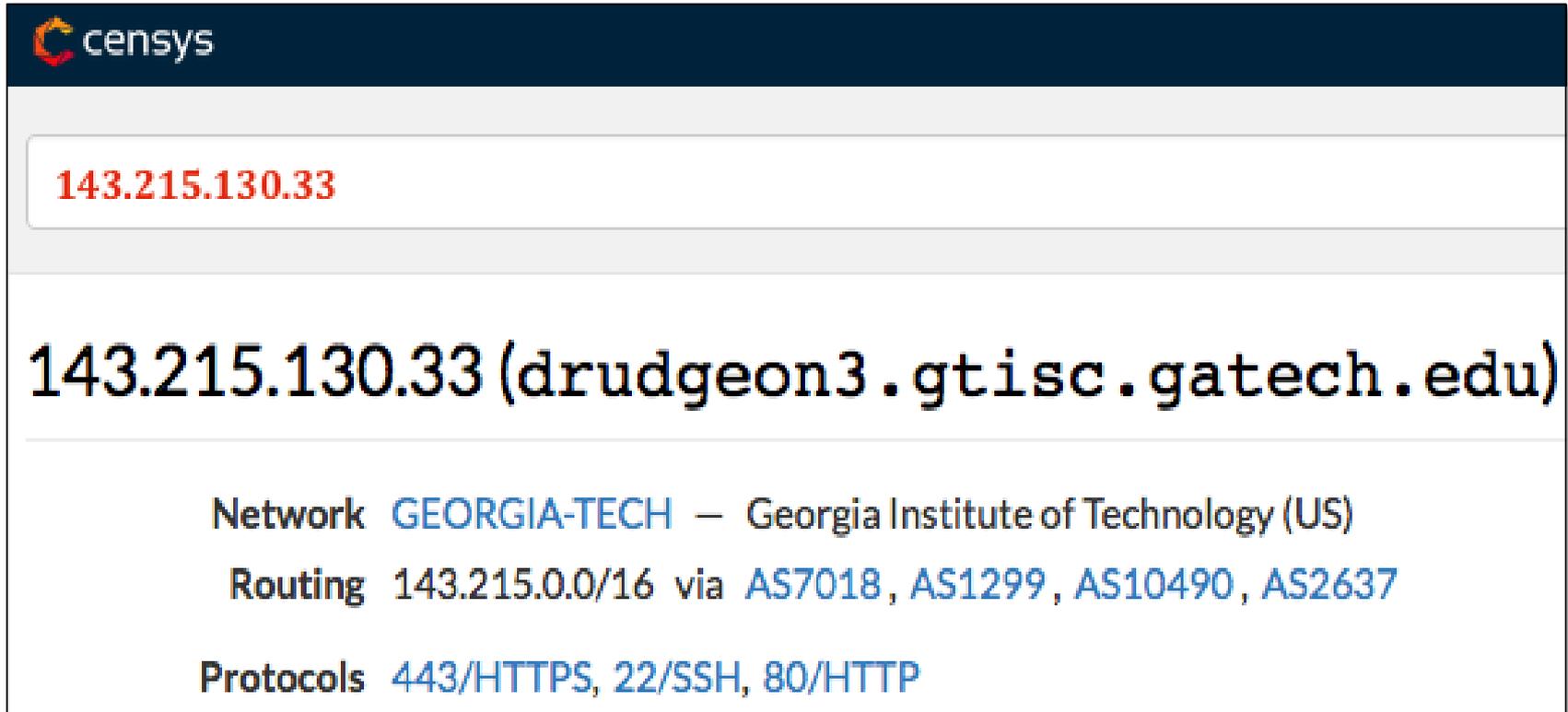
Date	IP Address
2015-08-26	23.253.46.64 (263 , ClassC=Browse , ClassB=Browse)
2016-02-15	-

```
HTTP/1.1 200 OKContent-Type: text/htmlLast-Modified: Thu, 12 Feb 2015
15:37:37 GMTAccept-Ranges: bytesETag: 503450d4d946d01:0Server: Microsoft-
IIS/7.5X-Powered-By: ASP.NETDate: Sat, 31 Oct 2015 21:34:55 GMTContent-
Length: 682
```

```
!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN http://www.w3.org
/TR/xhtml1/DTD/xhtml1-strict.dtd>html xmlnshttp://www.w3.org
/1999/xhtml>head>meta http-equivContent-Type contenttext/html; charsetiso-
8859-1 />title>Wapack Labs Sinkhole'title>style typetext/css>!--body {
color:#000000;background-color:#B3B3B3: marain:0;}#container { marain-
```

Retrieved from: <https://www.threatcrowd.org/domain.php?domain=goodmongol.com>

# Cool Tools - Censys



The screenshot shows the Censys interface for the IP address 143.215.130.33. The header features the Censys logo. The IP address is displayed in a red box. Below it, the host name is shown in large black text. Further down, network, routing, and protocol information are listed in blue text.

**143.215.130.33**

**143.215.130.33 (drudgeon3.gtisc.gatech.edu)**

Network **GEORGIA-TECH** – Georgia Institute of Technology (US)  
Routing **143.215.0.0/16** via **AS7018**, **AS1299**, **AS10490**, **AS2637**  
Protocols **443/HTTPS**, **22/SSH**, **80/HTTP**

Retrieved from: <https://www.censys.io/ipv4/143.215.130.33>

# Cool Tools - Censys

GET /

Status Line HTTP/1.1 302 Found

GET / [\[view page\]](#)

## Headers

content\_length 0

location <http://CP4TJT43A6PIKBRMHGPDCNBUQGE6U6XH7.IQHU3FKYGMINFO6FUAT7MFZGHBX.flask.sinkdns.org:80/>

content\_type text/html; charset=UTF-8

server TornadoServer/2.3

Retrieved from: <https://www.censys.io/ipv4/143.215.130.33>

# Cool Tools - Censys

## 443/HTTPS

### Chrome TLS Handshake

[Details](#) [Go](#)

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

Heartbleed Heartbeat Enabled. Immune to Heartbleed.

SSLv3 Support True

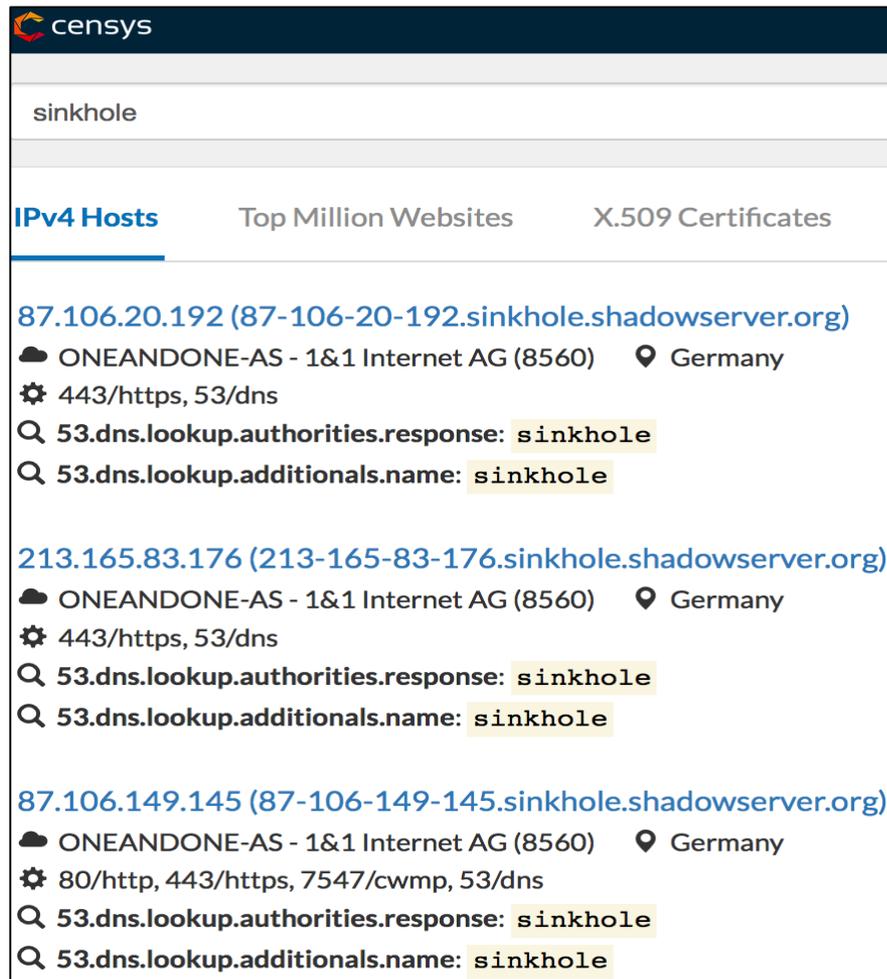
### Certificate Chain

[c4724bd2a1d35ed2b58c9b4e5fc0126f6152363fdb63f9d1c203eb2bf2e99ef9](#)

C=US, ST=Georgia, L=Atlanta, O=Georgia Tech, OU=GTISC, **CN=sinkhole, emailAddress=domainsink@gmail.com**

Retrieved from: <https://www.censys.io/ipv4/143.215.130.33>

# Wholesale Searches with Cool Tools



The screenshot shows the Censys search interface for the query 'sinkhole'. The 'IPv4 Hosts' tab is selected, displaying three search results. Each result includes the IP address, the host name, the AS number and name, the location, and the number of open ports. Additionally, two DNS lookup results are shown for each IP, both indicating a response of 'sinkhole'.

IP Address	Host Name	AS	Location	Ports	DNS Lookup Results
87.106.20.192	87-106-20-192.sinkhole.shadowserver.org	ONEANDONE-AS - 1&1 Internet AG (8560)	Germany	443/https, 53/dns	53.dns.lookup.authorities.response: sinkhole 53.dns.lookup.additional.name: sinkhole
213.165.83.176	213-165-83-176.sinkhole.shadowserver.org	ONEANDONE-AS - 1&1 Internet AG (8560)	Germany	443/https, 53/dns	53.dns.lookup.authorities.response: sinkhole 53.dns.lookup.additional.name: sinkhole
87.106.149.145	87-106-149-145.sinkhole.shadowserver.org	ONEANDONE-AS - 1&1 Internet AG (8560)	Germany	80/http, 443/https, 7547/cwmp, 53/dns	53.dns.lookup.authorities.response: sinkhole 53.dns.lookup.additional.name: sinkhole

Retrieved from: <https://www.censys.io/ipv4?q=sinkhole&page=3>

# Recap

Maintaining sinkhole lists for CND and cyber threat analysis

Parking/unparking patterns are telling

Multiple actors on the same IP address at same time

Don't miss the obvious: \*sinkole\*.[org,com,net]

Lots of different ways we can validate

# So, what's next?



Software Engineering Institute

Carnegie Mellon University

Identifying 3<sup>rd</sup> Party Sinkhole Operations

© 2015 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

# Open Questions

Can we quantify how well these heuristics work?

Can we automate?

Applying this work in operations

Sharing findings with community?

# Sources

PassiveTotal. *Know Your Foe: It Might Be a Sinkhole If...*,  
21 July 2015. <http://blog.passivetotal.org/kyf-if-might-be-a-sinkhole-if/>.

*SinkMiner: Mining Botnet Sinkholes for Fun and Profit*,  
<http://www.covert.io/research-papers/security/SinkMiner-%20Mining%20Botnet%20Sinkholes%20for%20Fun%20and%20Profit.pdf>

<https://github.com/stamparm/maltrail/commit/511166fa5e3ddceff2e5c0c483c4955c74e8d4e0>

# Contact Information

## Presenter / Point of Contact

Michael B Jacobs

Member of Technical Staff

Telephone: +1 703-247-1422

Email: [mbjacobs@cert.org](mailto:mbjacobs@cert.org)



Software Engineering Institute

Carnegie Mellon University

Identifying 3<sup>rd</sup> Party Sinkhole Operations

© 2015 Carnegie Mellon University

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.