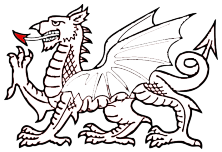
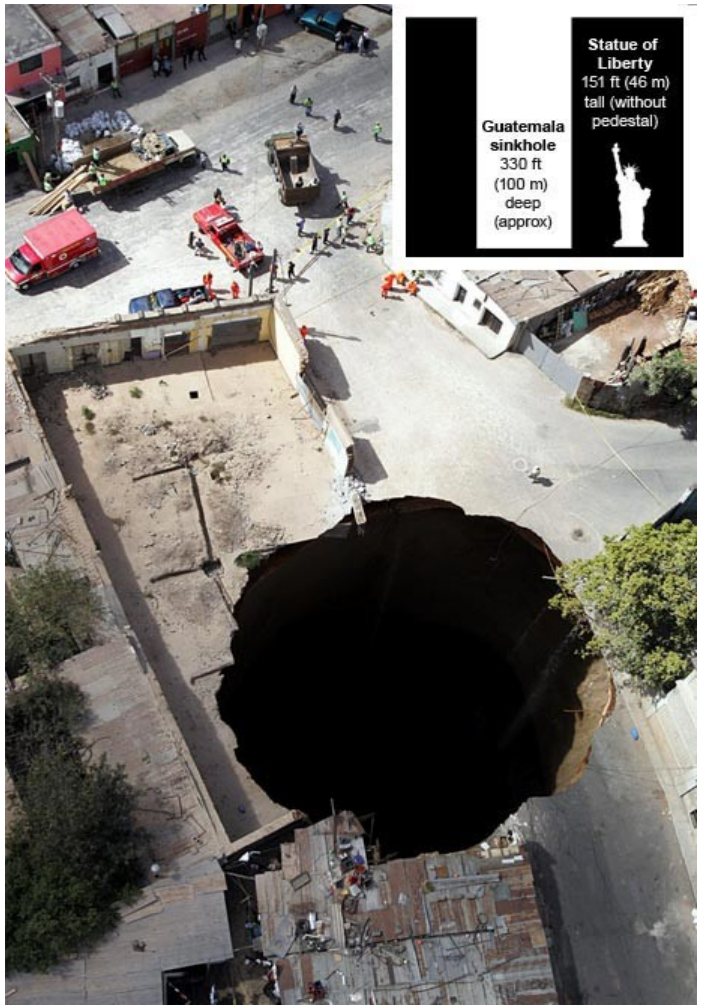
Experiences with Conficker C Sinkhole Operation and Analysis

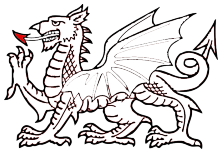
John Kristoff
Research Analyst
jtk@cymru.com



Sinkholes

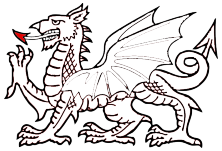

Guatemala sinkhole
330 ft (100 m) deep (approx)
Statue of Liberty
151 ft (46 m) tall (without pedestal)

The Great Conficker DNS Hijack of 2009?



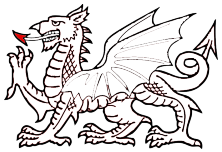
Conficker C mitigation

- Over 100 TLDs (gTLDs and ccTLDs) contacted
- The majority participated in mitigation efforts
  - Registry/registrar outreach was significant
  - Sinkhole operators answered domains names
  - The “coordination” effort was mostly a success
  - Most credit goes to registries, ICANN, Wesson
- The absence of a **BOOM!!** is notable



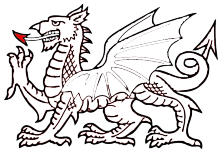
Becoming a sinkhole operator

Timing	:	Just do it
Friends	:	Who do you know?
Reputation	:	Build bridges, don't burn them



Why do this?

Fonzie	:	All the cool kids are doing it
Einstein	:	Publish or perish
Superhero	:	Eat, save world, sleep, repeat

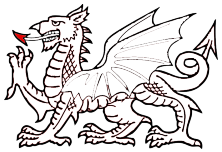


Team Cymru Conficker Sinkhole

Goal : Get data to people who can take action

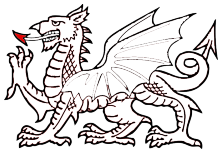
Constraint : Setup time

Challenge : Minimize false positives



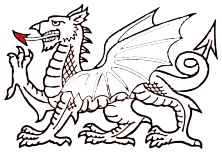
System requirements

- A Linux virtual machine (VM)
- Some memory, some disk
- No cute tricks needed



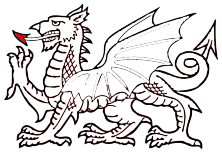
Web server requirements

- Apache httpd
- Customized LogFormat config option
- Cronolog for YYYYMMDDHH named log files
- Some performance related tweaks
  - e.g. MinSpareServers
  - e.g. disable unneeded code with ./configure
- Nothing particularly cute here either



Sinkhole addressing

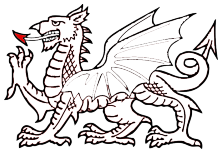
```
/sbin/ip addr add 192.0.2.0/24 dev lo
```



D'oh!

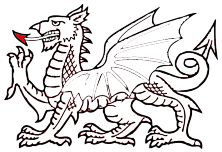
```
ip_conntrack: table full, dropping packet.
      printk: 9 messages suppressed.
```

- Tune `net.ipv4.ip_conntrack_max`
- ...or disable netfilter/iptables



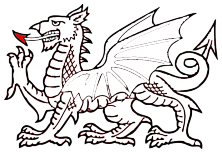
Got sockets?

```
$ netstat -an | grep :80 | wc -l
 29294
```



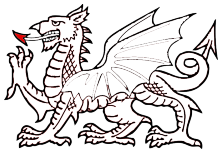
Got disk?

```
1,266,673,941 sinklogs-20090402.tar.gz
1,217,023,512 sinklogs-20090403.tar.gz
1,195,396,709 sinklogs-20090407.tar.gz
1,153,551,360 sinklogs-20090406.tar.gz
1,129,146,938 sinklogs-20090408.tar.gz
1,054,142,889 sinklogs-20090414.tar.gz
1,039,420,867 sinklogs-20090413.tar.gz
```



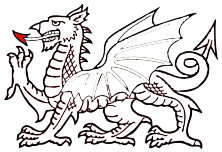
Raw “HTTP GET /” logs - hourly

```
71,289,550 200904011400.log.gz
68,978,096 200904021400.log.gz
68,740,712 200904021500.log.gz
67,982,356 200904011600.log.gz
67,246,989 200904021600.log.gz
67,116,856 200904021300.log.gz
67,091,407 200904011500.log.gz
67,079,419 200904020900.log.gz
66,978,650 200904071400.log.gz
```



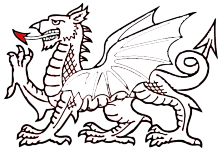
Ops “HTTP GET /” logs - hourly

```
24,861,070 200904011400.csv.gz
24,292,611 200904021400.csv.gz
24,008,038 200904021500.csv.gz
23,884,012 200904020900.csv.gz
23,821,208 200904021300.csv.gz
23,568,062 200904020800.csv.gz
23,562,925 200904071400.csv.gz
23,489,223 200904011600.csv.gz
23,410,348 200904021000.csv.gz
```



Got documentation?

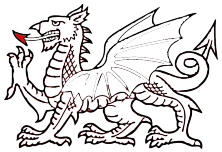
```
$ head README.cymru

$Id: README.cymru,v 1.8 2009/04/29 18:20:16 jtk Exp $

Team Cymru Conficker C Sinkhole
http://www.team-cymru.org

1. Sinkhole Overview
2. Repository Data Format
   a. ops
   b. raw
3. Operational History
```

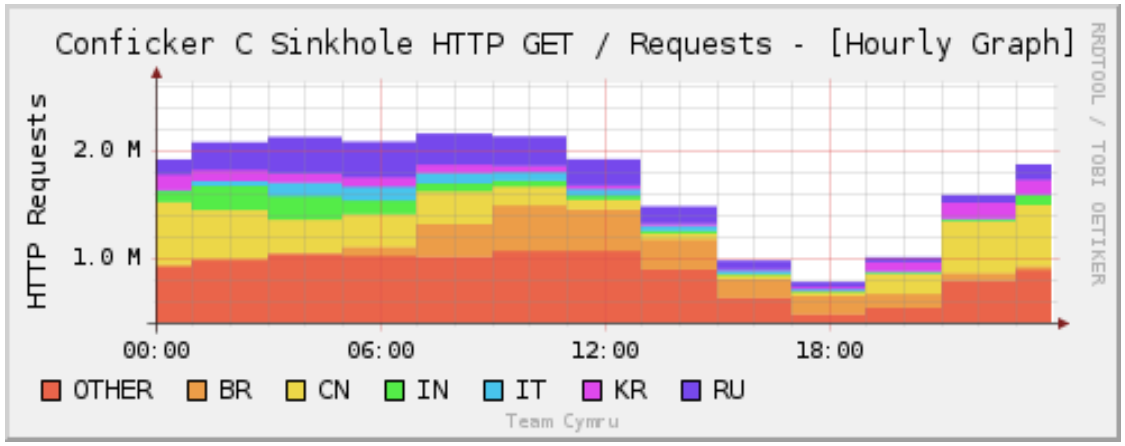


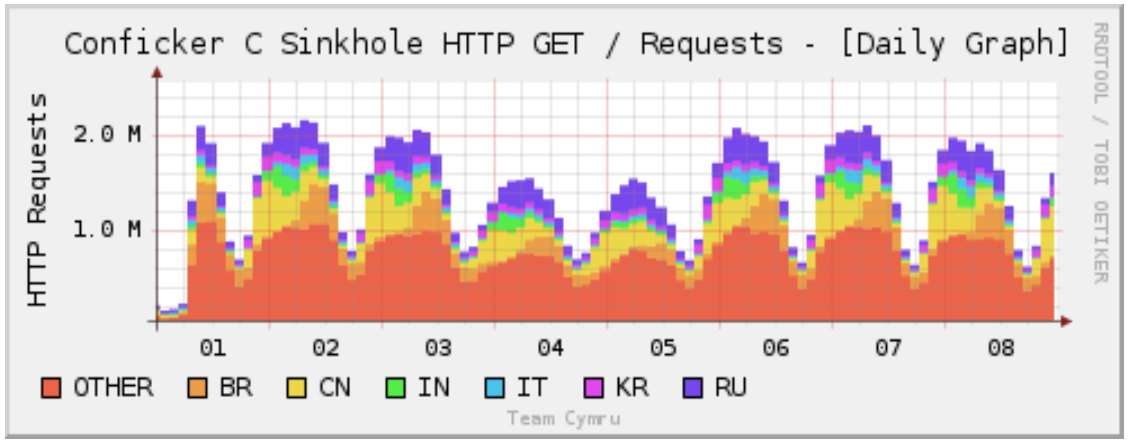
!! WARNING !!

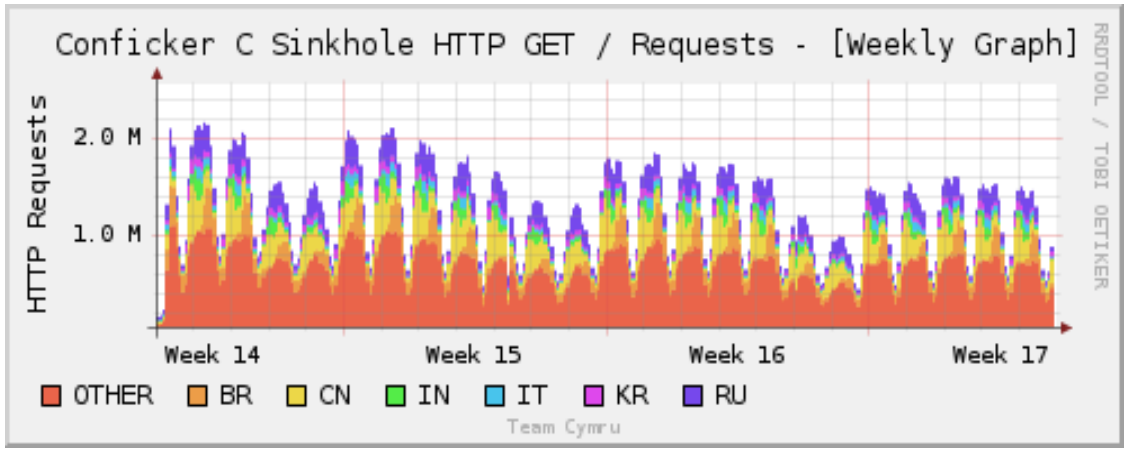
This is NOT a rigorous examination of our sinkhole data.

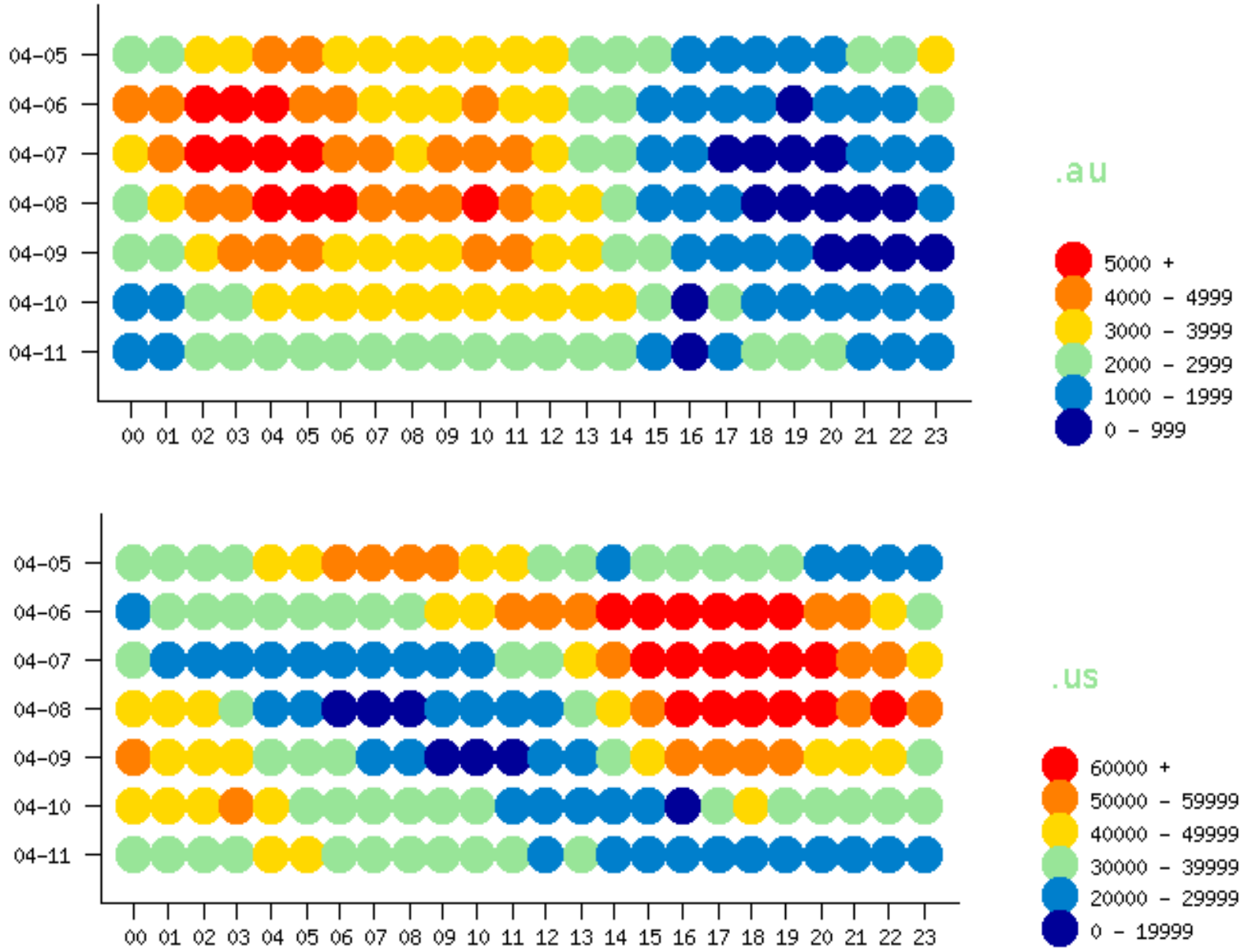
Just enjoy the pretty pictures. :-)

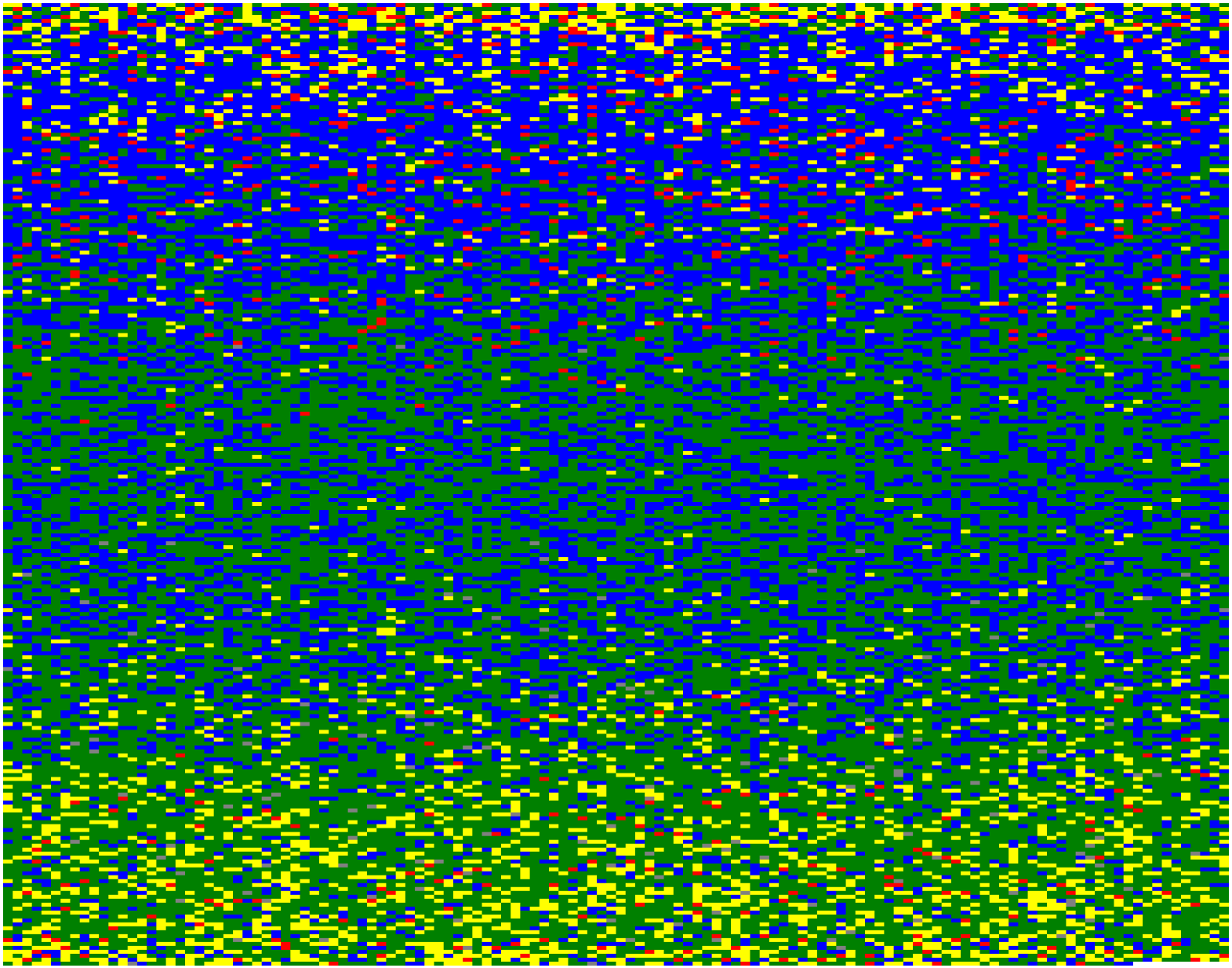


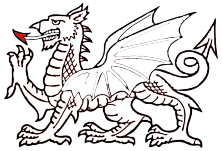

Conficker C Sinkhole HTTP GET / Requests - [Hourly Graph]
HTTP Requests
2.0 M
1.0 M
00:00
06:00
12:00
18:00
OTHER
BR
CN
IN
IT
KR
RU
Team Cymru
RRDTOOL / TOBI OETIKER

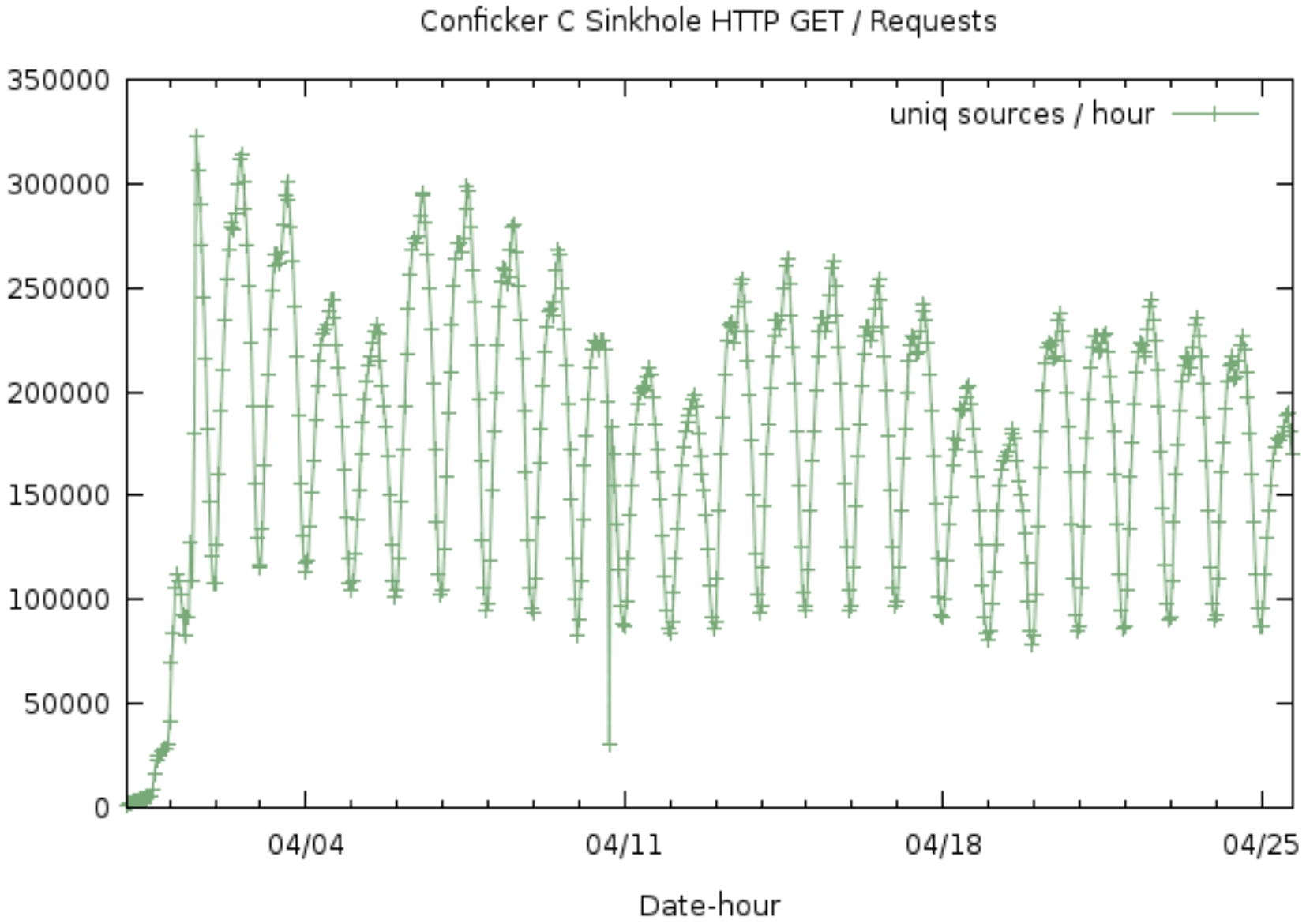

Conficker C Sinkhole HTTP GET / Requests - [Daily Graph]
HTTP Requests
2.0 M
1.0 M
01
02
03
04
05
06
07
08
OTHER
BR
CN
IN
IT
KR
RU
Team Cymru
RRDTOOL / TOBI OETIKER

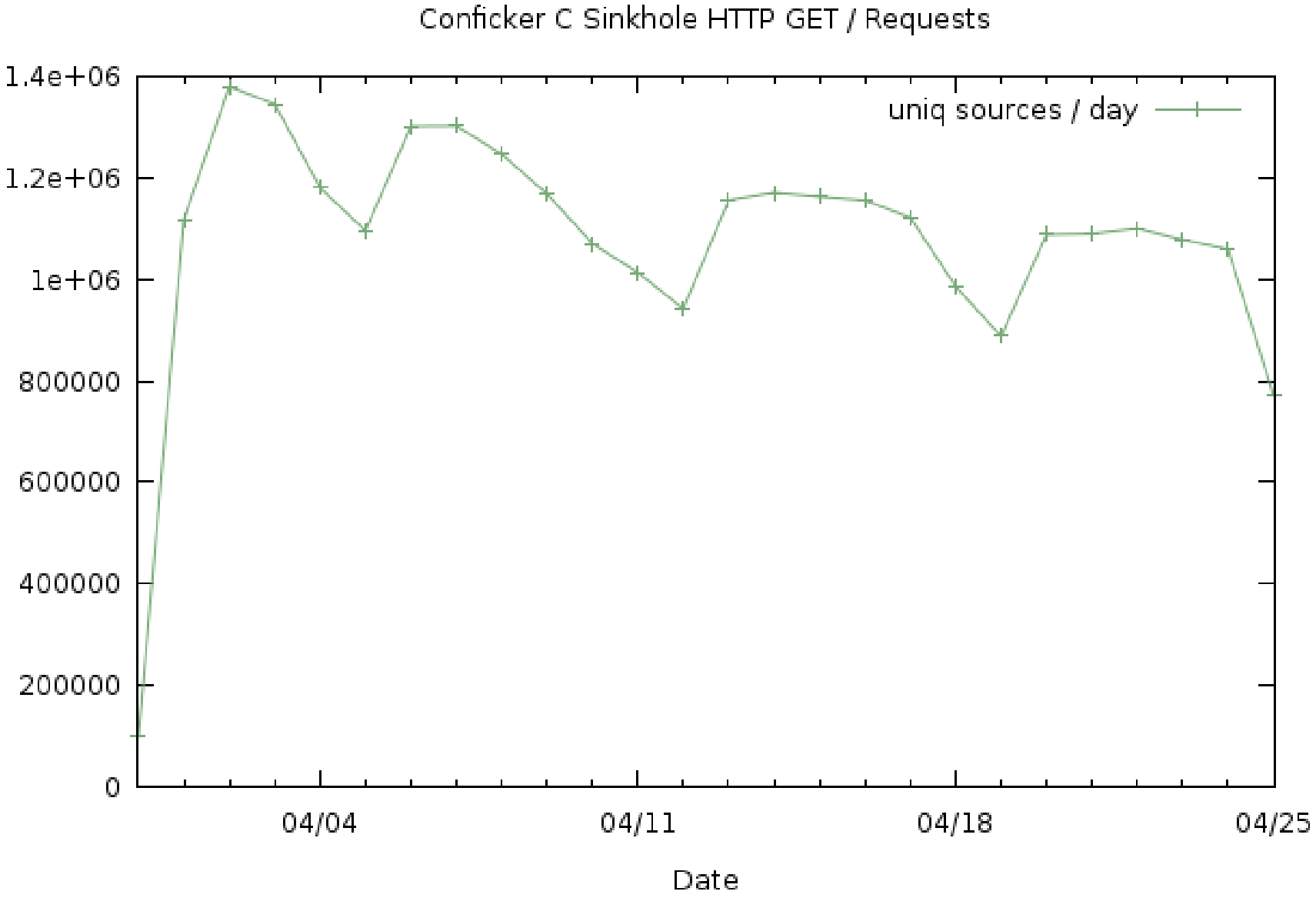

Conficker C Sinkhole HTTP GET / Requests - [Weekly Graph]
HTTP Requests
2.0 M
1.0 M
Week 14
Week 15
Week 16
Week 17
OTHER
BR
CN
IN
IT
KR
RU
Team Cymru
RRDTOOL / TOBI OETIKER

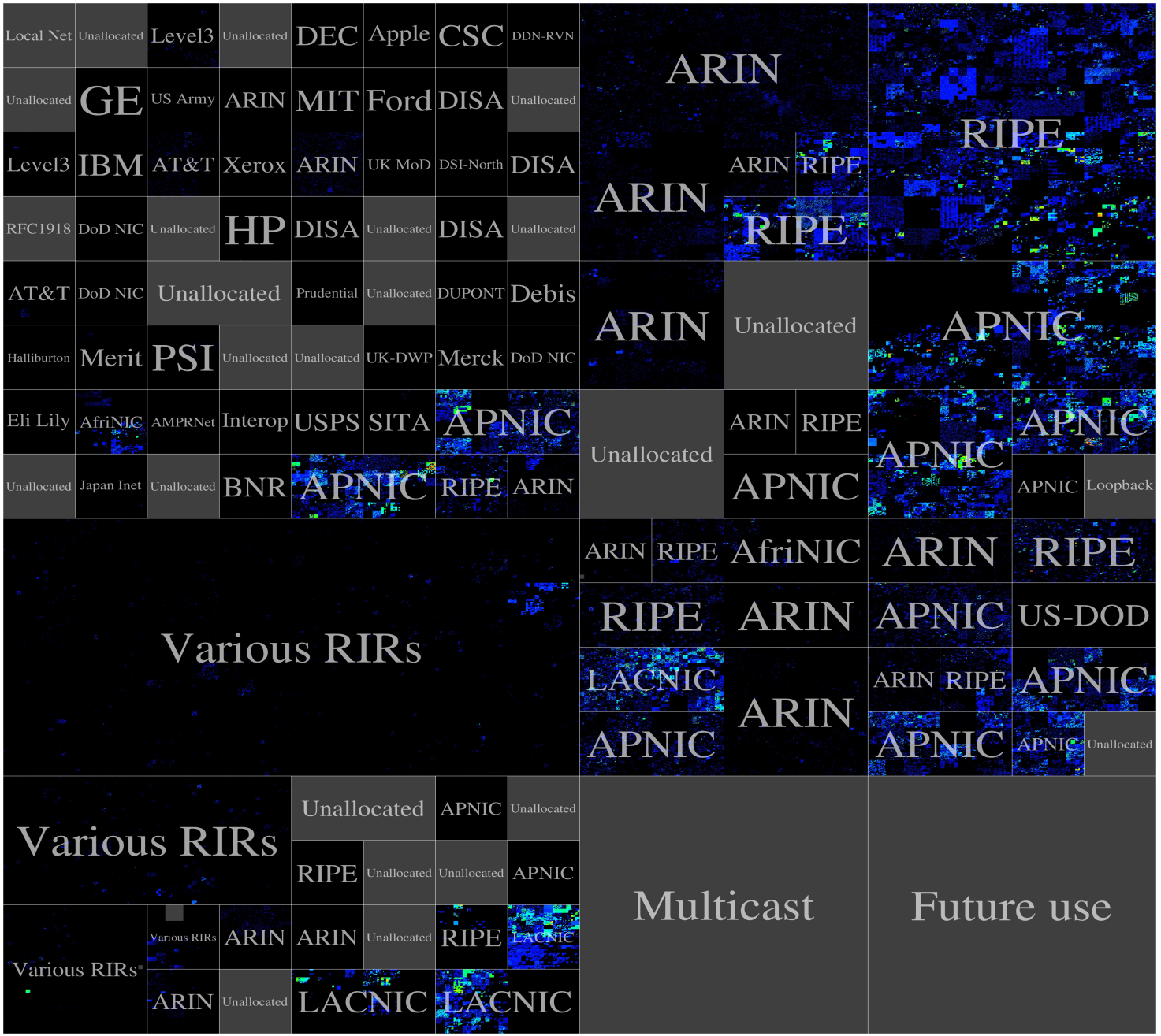

04-05
04-06
04-07
04-08
04-09
04-10
04-11
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
.au
5000 +
4000 - 4999
3000 - 3999
2000 - 2999
1000 - 1999
0 - 999
04-05
04-06
04-07
04-08
04-09
04-10
04-11
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
.us
60000 +
50000 - 59999
40000 - 49999
30000 - 39999
20000 - 29999
0 - 19999

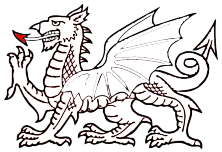


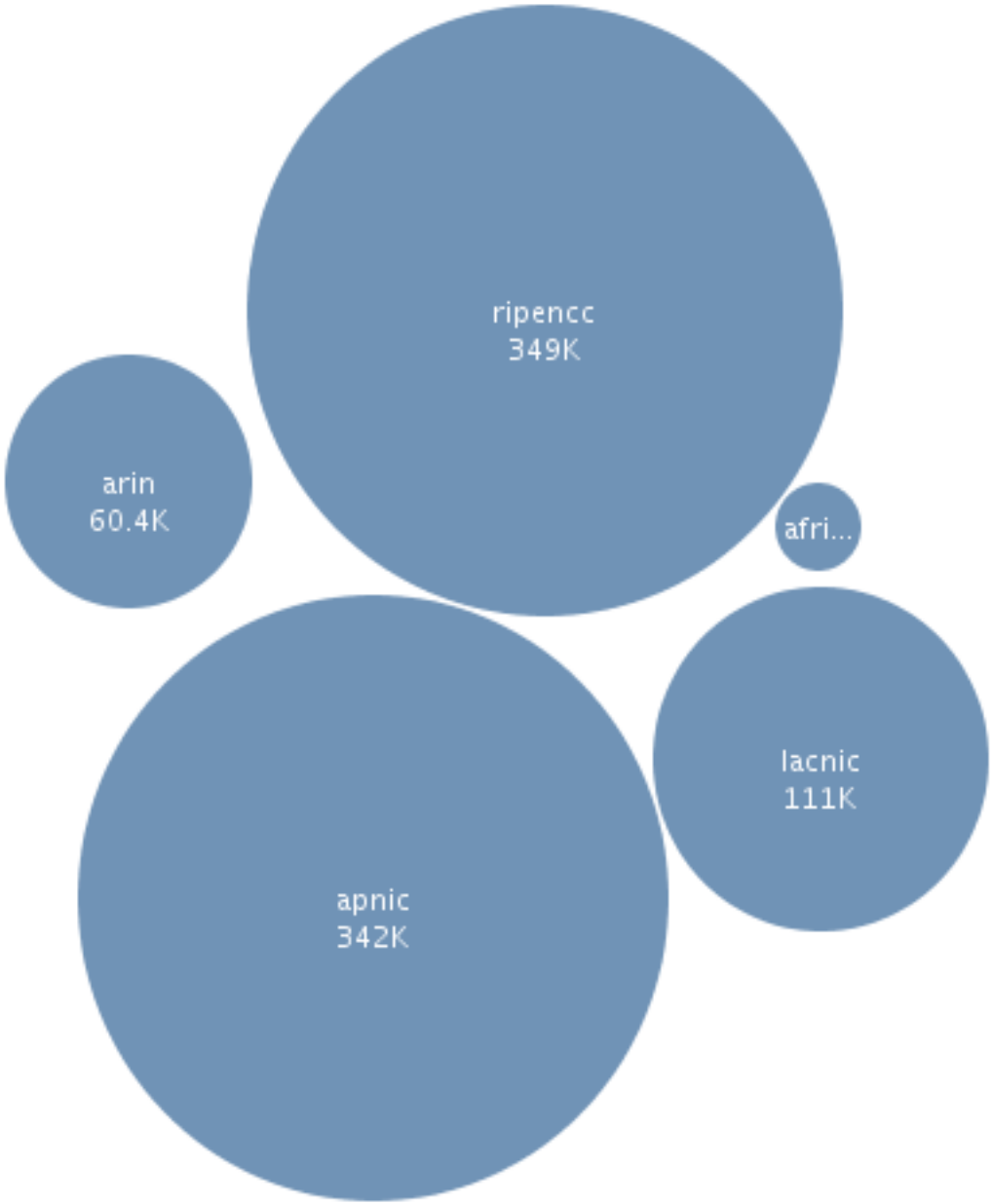


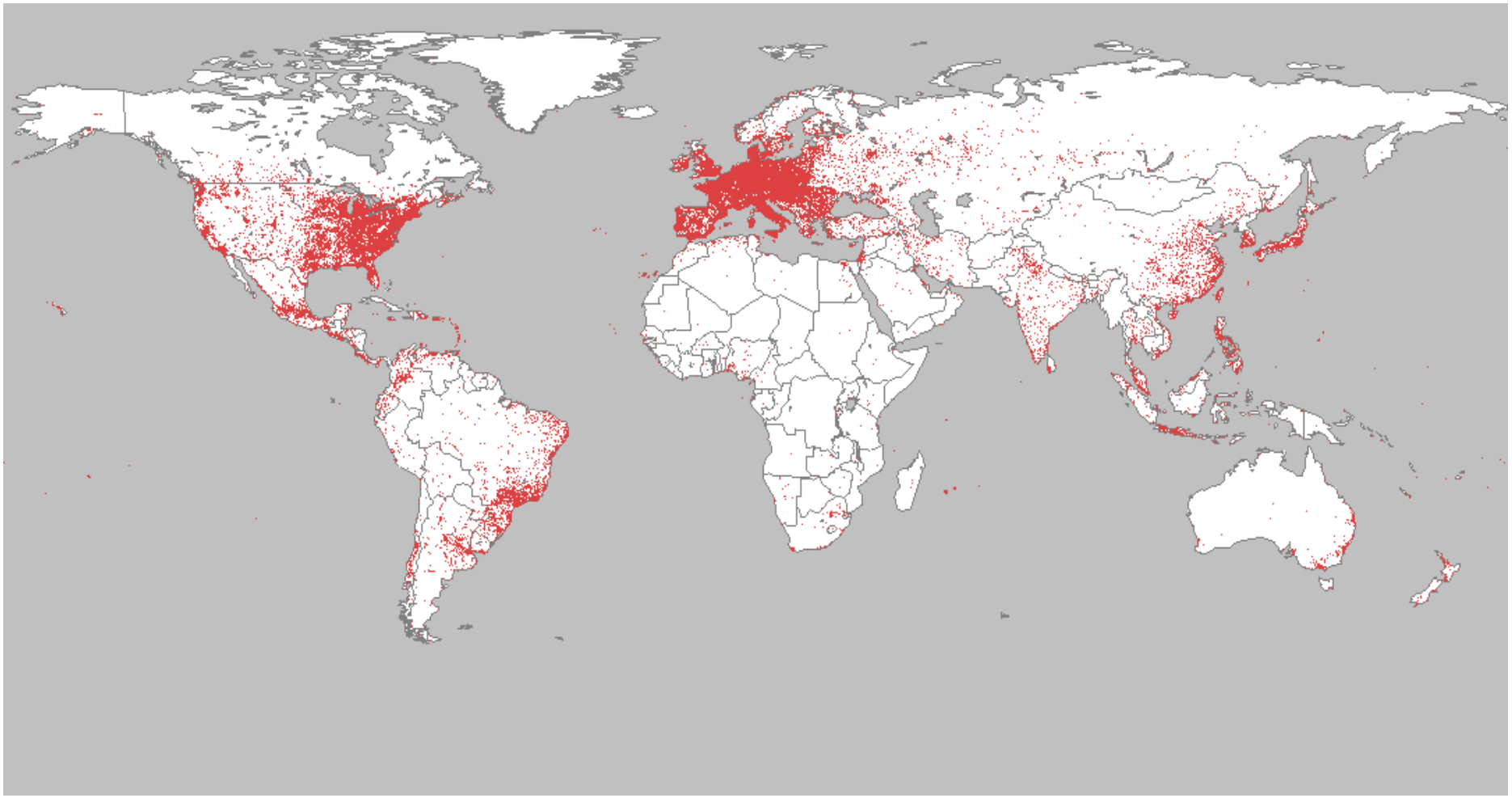

Conficker C Sinkhole HTTP GET / Requests
uniq sources / hour
350000
300000
250000
200000
150000
100000
50000
0
04/04
04/11
04/18
04/25
Date-hour

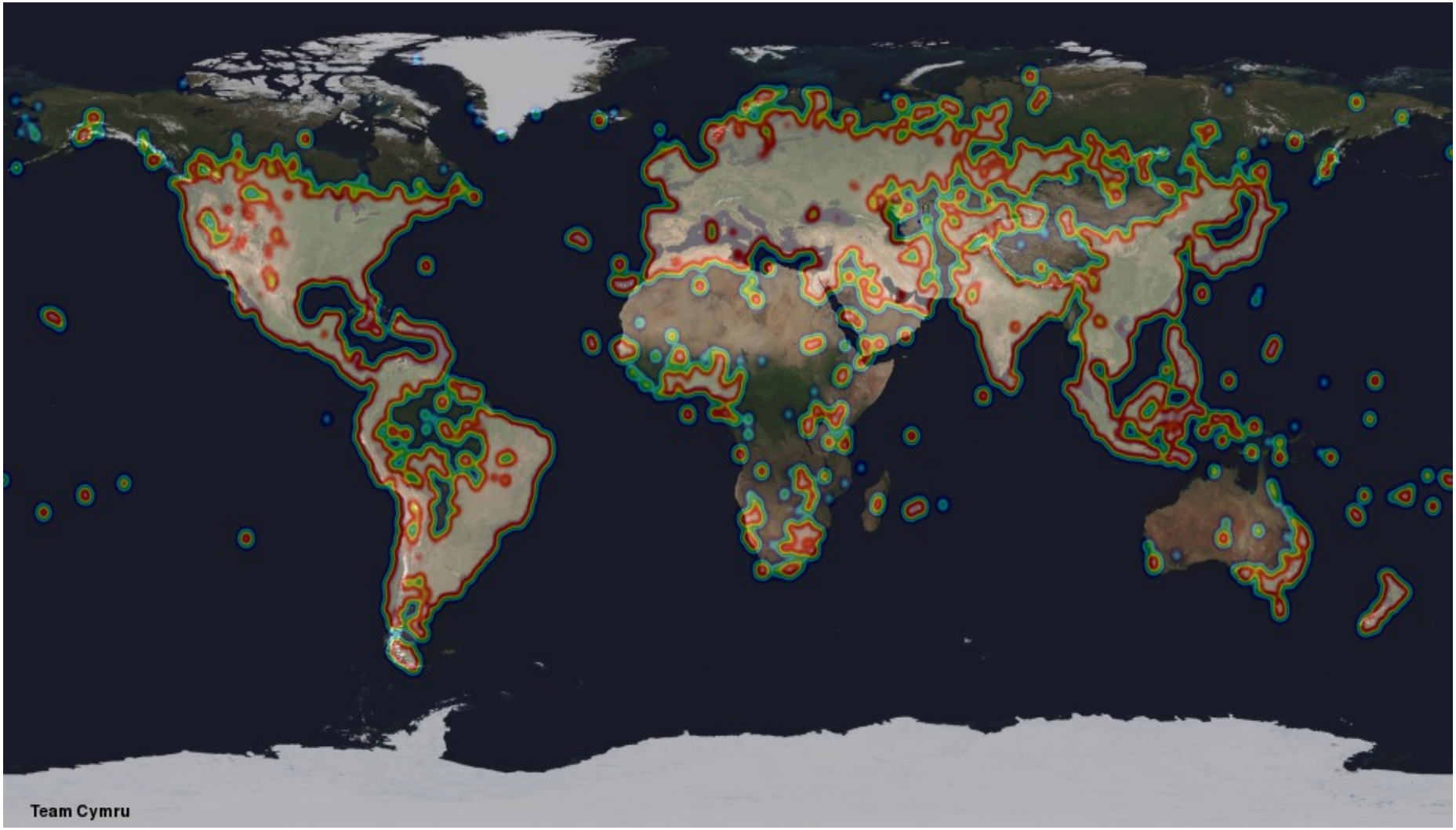

Conficker C Sinkhole HTTP GET / Requests
uniq sources / day
1.4e+06
1.2e+06
1e+06
800000
600000
400000
200000
0
04/04
04/11
04/18
04/25
Date

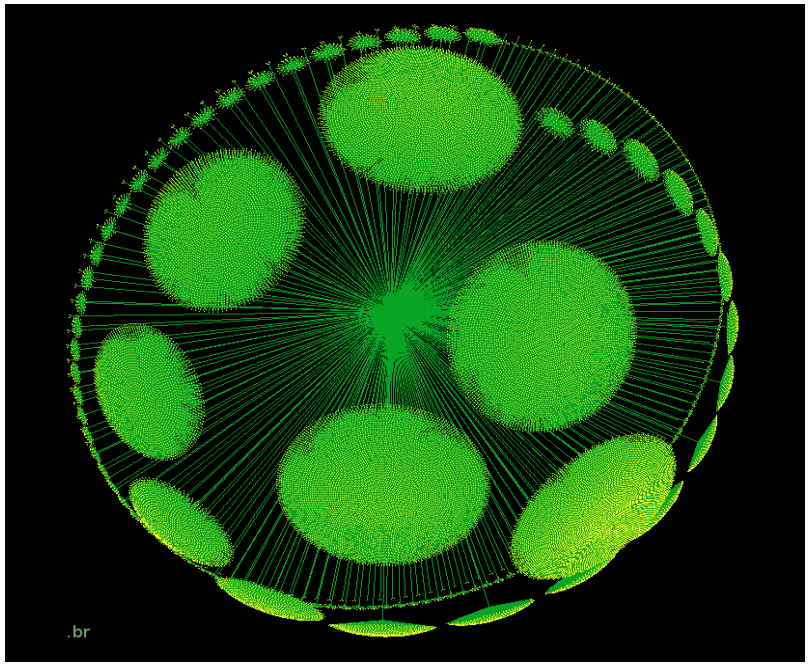

Local Net
Unallocated
Level3
Unallocated
DEC
Apple
CSC
DDN-RVN
Unallocated
GE
US Army
ARIN
MIT
Ford
DISA
Unallocated
Level3
IBM
AT&T
Xerox
ARIN
UK MoD
DSI-North
DISA
RFC1918
DoD NIC
Unallocated
HP
DISA
Unallocated
DISA
Unallocated
AT&T
DoD NIC
Unallocated
Prudential
Unallocated
DUPONT
Debis
Halliburton
Merit
PSI
Unallocated
Unallocated
UK-DWP
Merck
DoD NIC
Eli Lily
AfriNIC
AMPRNet
Interop
USPS
SITA
APNIC
Unallocated
Japan Inet
Unallocated
BNR
APNIC
RIPE
ARIN
Various RIRs
Various RIRs
Various RIRs
ARIN
Unallocated
ARIN
Unallocated
LACNIC
Unallocated
RIPE
Unallocated
Unallocated
APNIC
Unallocated
APNIC
RIPE
Unallocated
Unallocated
APNIC
Various RIRs
ARIN
Unallocated
LACNIC
RIPE
LACNIC
ARIN
ARIN
RIPE
ARIN
RIPE
ARIN
RIPE
Unallocated
ARIN
RIPE
APNIC
ARIN
RIPE
AfriNIC
RIPE
ARIN
RIPE
ARIN
APNIC
US-DOD
LACNIC
ARIN
ARIN
RIPE
APNIC
APNIC
APNIC
APNIC
Unallocated
Multicast
Future use

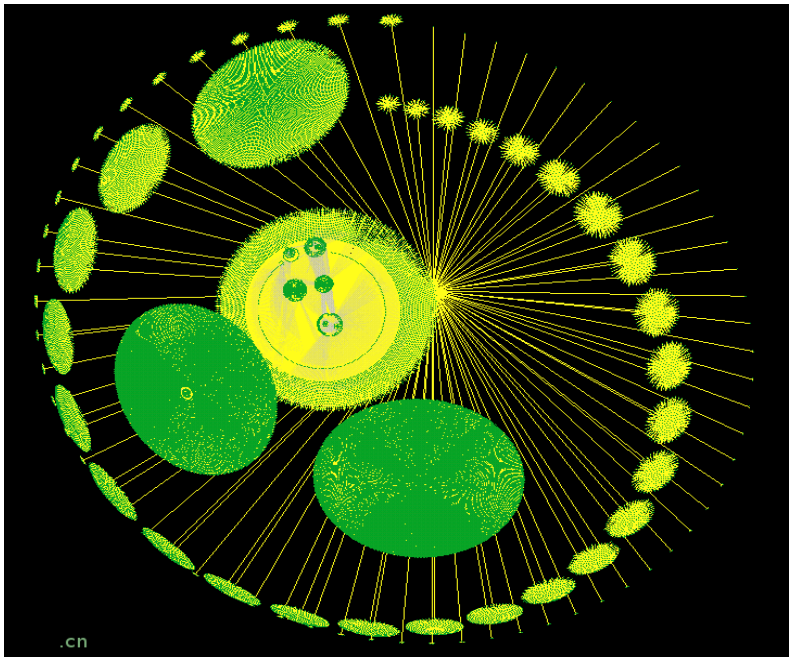


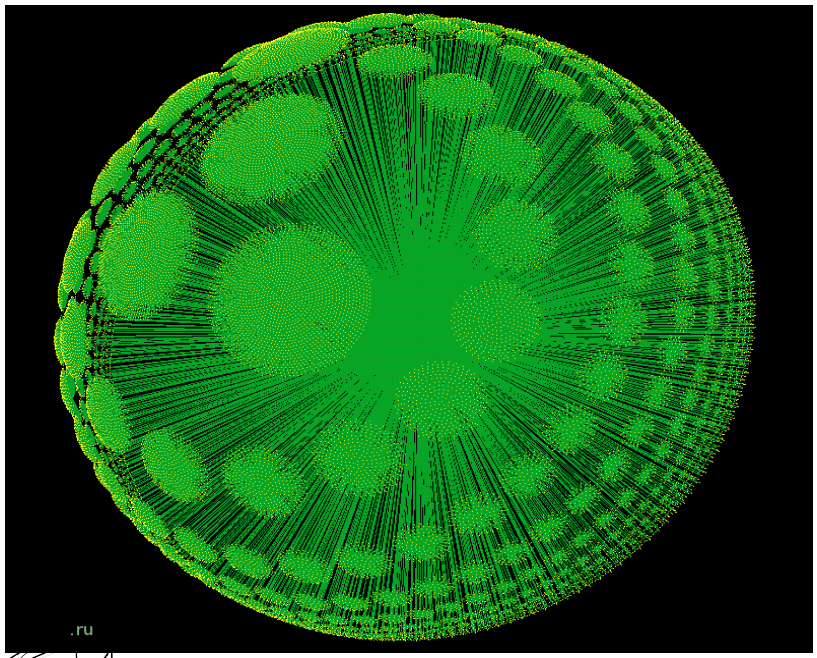

ripencc
349K
arin
60.4K
afri...
lacnic
111K
apnic
342K

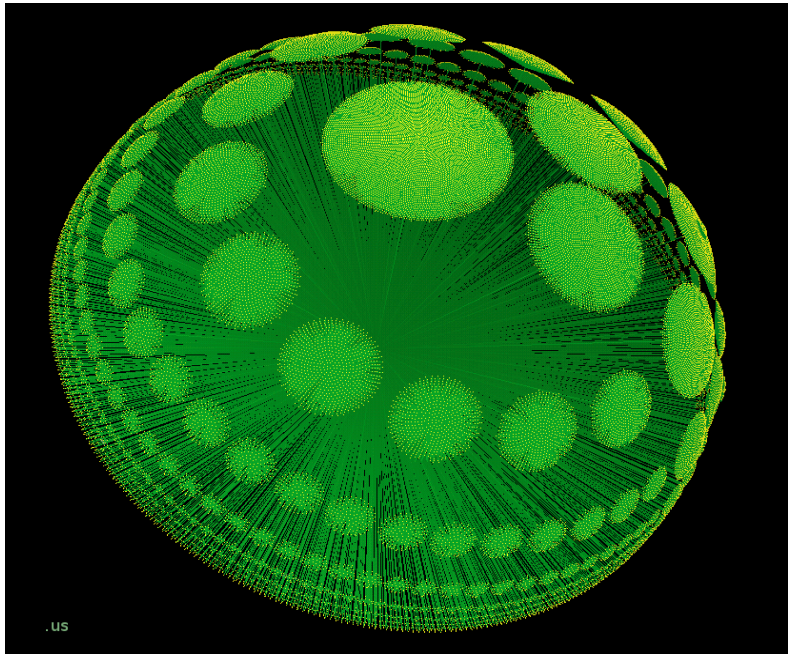



Team Cymru

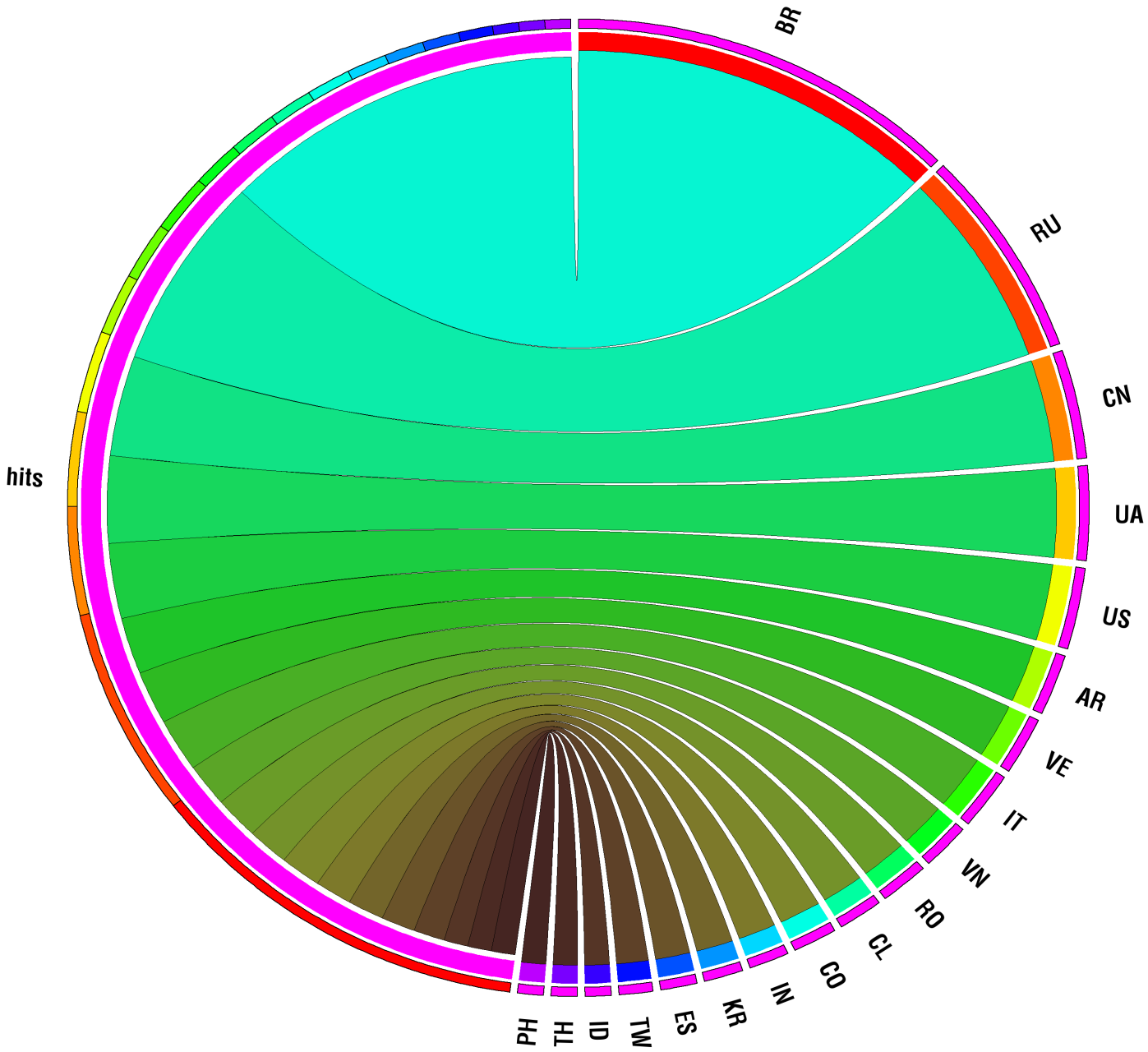

.br

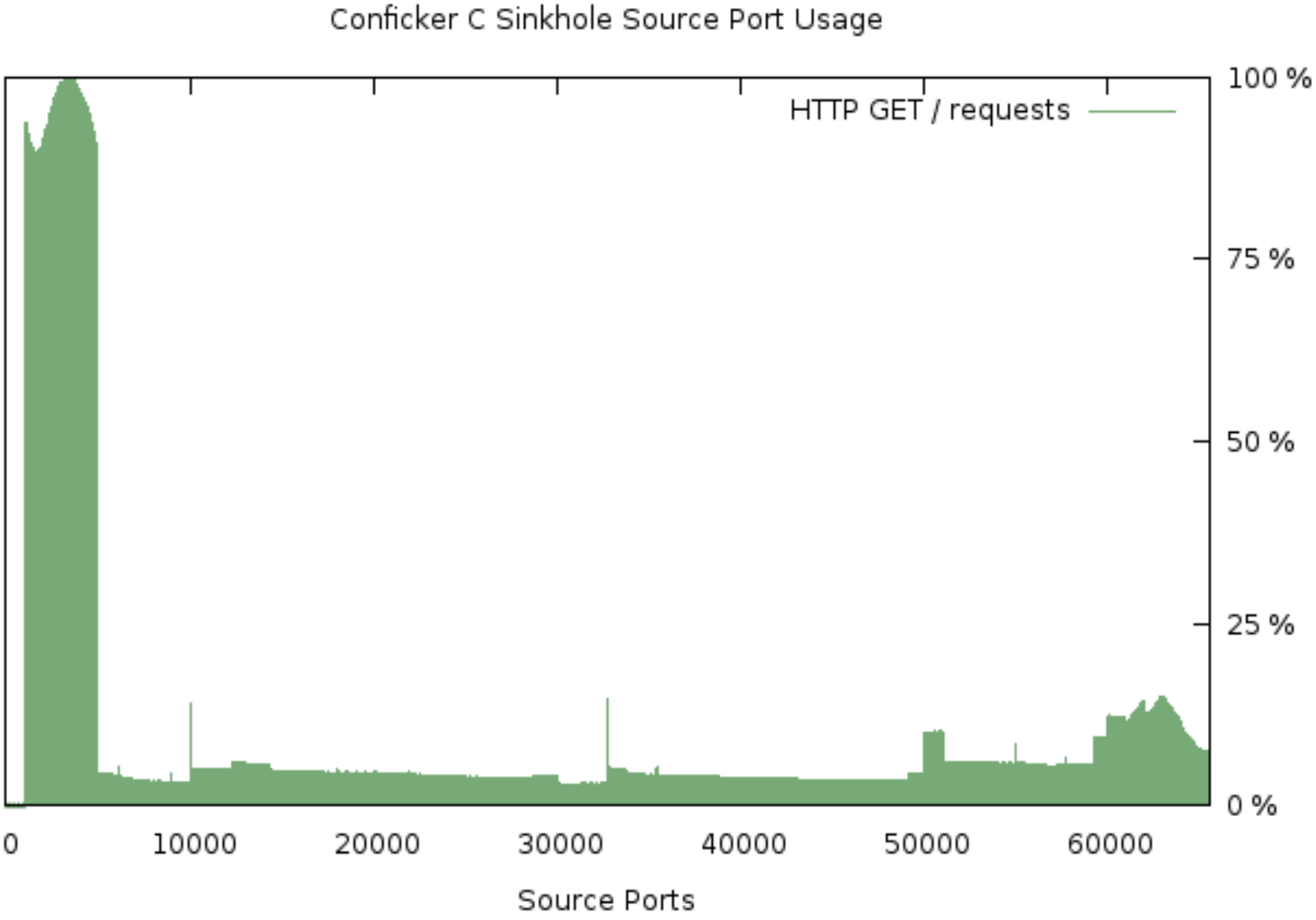

.cn


.ru


.us


Infections
BR
Telecomunicacoes da Bahia S.A.
TELECOMUNICACOES DE SAO PAULO SA - TELESP
Tim Brasil S.A.
Telesp Celular S.A.
Global Village Telecom
Embratel
TELESC - Telecomunicacoes de Santa Catarina SA
Telet S.A.
NET Servicos de Comunicao S.A.
KR
KIXS-AS-KR Korea Telecom
HANARO-AS Hanaro Telecom Inc.
LG DACOM Corporatio
IN
BSNL-NIB National Internet Backbone
TATA-AS Tata
BHARTI-MOBILIT Bharti Airtel Ltd. AS
MTNL-AP Mahanag
TCISL Tata
RIL-IDC Reliance Infocom Ltd
AIRTELBRO Bharti Airtel Ltd..
CN
CHINA169-BACKBONE CNCGROUP China169 Backbone
CHINANET-BACKBONE No.31,Jin-rong Street
CHINANET-China Telecom (Group)
CRNET CHINA RAILWA
RU
OTHE RU
TI-AS NetBy
MY
TMNET-AS-AP TM Net, Internet Service Provider
RO
RTD RTD-ROMTELEC
IT
TW
HINET Data Communication Business Group
US
VZG
OTH US
DE
DTAG Deutsche Telekom
SA
MX
Uninet S.A. de C.V.
EU
GB
ES
PK
PKTELECO Pakistan Telecommur
PT
PL
HU
FR
TR
TH
TOTNET-TH-AS-AP TOT Public
ASIAINFO-AS ASIA INFONET Co..Ltd.
CL
Entel PCS Telec
VTR
Terra Networks Chile S.A.
CO
ETB - Colombia
TV Cable S.A.
VE
CANTV Servicios, Venezuela
VN
VNN-AS-AP Vietnam Posts and Telecommunications (VNPT)
VIETEL-AS Viettel Corporation
AR
Telecom Argentina S.A.
UA
ID
TELKOMSEL ASN-ID PT.
INDOSATM2-I
PH
BAYAN
DIGIT
TELEC Bayan
GLOBE
IPG-AS-AP Philippine Long Distance Telephone
HR
MD
CR
NZ
CH
PA
AU
BD
AZ
KW
DK
MK
SE
GR
DO
SI
LV
NP
UZ
HK
CZ
LK
BO
NG
MO
GE
DZ
LT
AT
UY
IL
PS
CS
BA
EC
CA
JO
BG
EG
NA
IR
JP
PE
BY
Telefonica del Peru S.A.A.
KZ

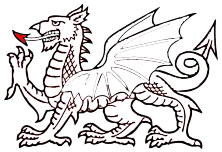

BR
RU
CN
UA
US
AR
VE
IT
VN
RO
CL
CO
IN
KR
ES
TW
ID
TH
PH
hits


Conficker C Sinkhole Source Port Usage
HTTP GET / requests
100 %
75 %
50 %
25 %
0 %
0
10000
20000
30000
40000
50000
60000
Source Ports

User Agent Tokens

Analysis cautions (aka areas for research)

- NATs, proxies, caches, filters and local sinkholes
- Transient address (e.g. DHCP, hot spots, dial)
- Researcher, human and bot false positives
- Missing, out-of-order and data parsing challenges
- Geoloc, routing and registry accuracy



Contact us

- jtk@cymru.com
- Team PGP key 0x79B109F9

  http://www.team-cymru.org/About/teamcymru-pgp.txt

FYI... we've got data

Reports for your nets/ASNs for the asking