Experiences with Conficker C
Sinkhole Operation and Analysis

John Kristoff
Research Analyst
jtk@cymru.com
Sinkholes
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. :-(
User Agent Tokens

Mozilla/4.0 
.NET CLR 2.0.50727 
SV1
.NET CLR 1.1.4322 
Windows NT 5.1 
MSIE 7.0 
MSIE 6.0

http://www.wordle.net
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