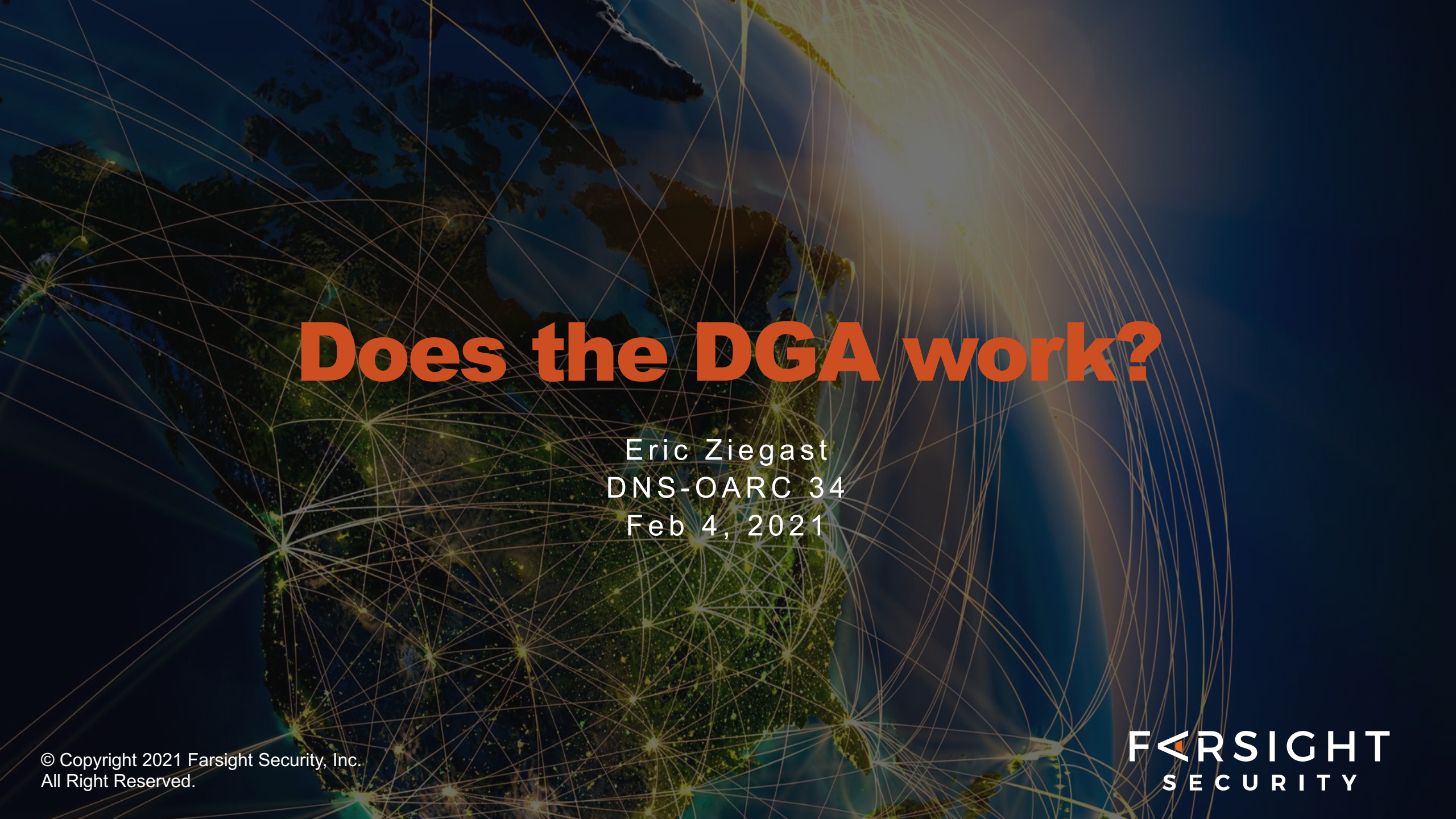


# Does the DGA work?

Eric Ziegast

DNS-OARC 34

Feb 4, 2021



FARSIGHT SECURITY

# We've been here before …

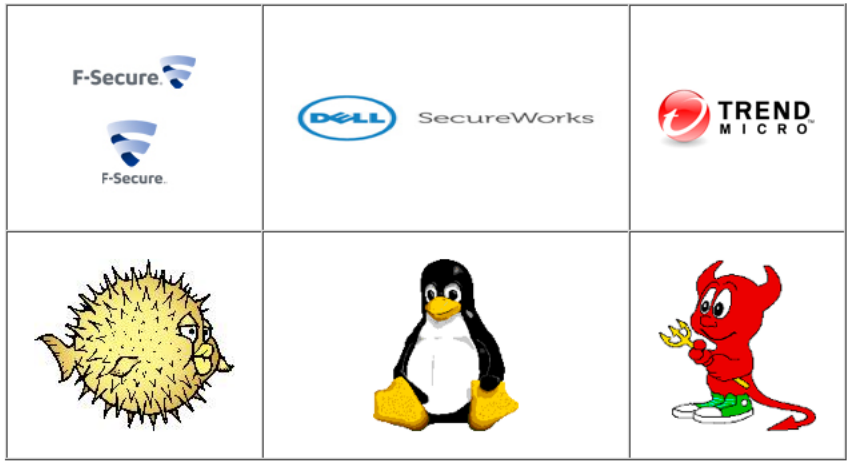
## conficker.[ccTLD]

Eric Ziegast / ISC

DNS-OARC/ICANN

March 14th, 2011

**Conficker Eye Chart**




Anyone want to help temporarily register 50000 domains each day?

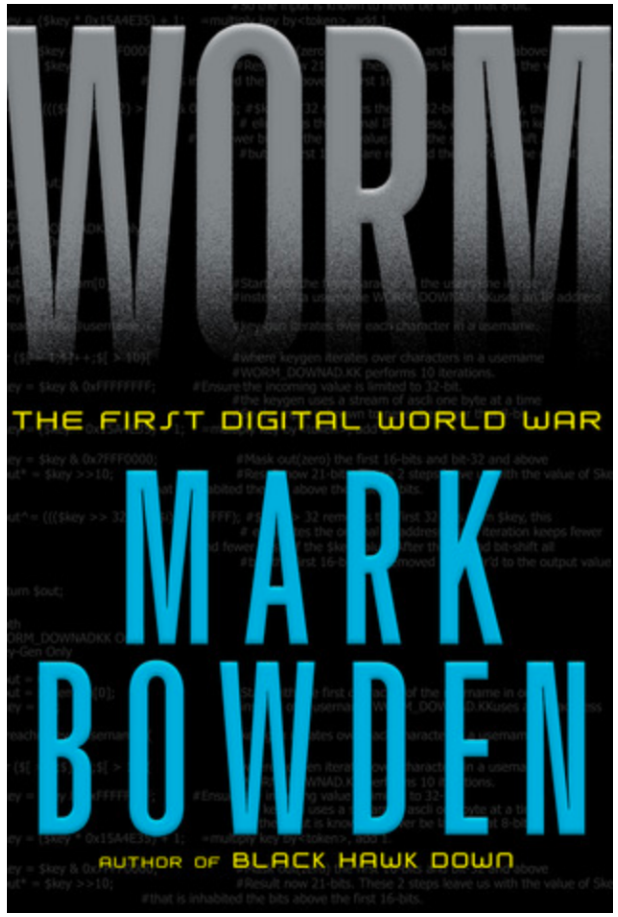
https://archive.icann.org/en/meetings/siliconvalley2011/bitcache/cc Conficker Sinkhole – Eric Zeigast, ISC-vid=23179&disposition=attachment&op=download.pdf

# We learned a lot…

Conficker Working Group:
Lessons Learned

June 2010 (Published January 2011)

http://docs.media.bitpipe.com/io_10x/io_102267/item_465972/whitepaper_76813745321.pdf




https://www.amazon.com/dp/0802145949


**Post-Mortem of a Zombie:
Conficker Cleanup After Six Years**

**Hadi Asghari, Michael Ciere, and Michel J.G. van Eeten, *Delft University of Technology***

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/asghari

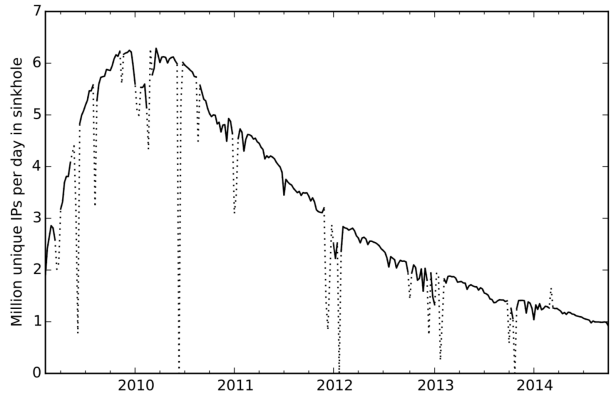



Figure 1: Conficker bots worldwide

# Time to make the doughnuts

FARSIGHT SECURITY

- Conficker A&B utilizes 500 pseudo-random domains daily across a few TLD – registry operators organized to front-run domains for containment.
- Conficker C utilizes about 50000 domains per day to phone home utilizing a more complex algorithm across 110 registries – not possible to contain.
- We received several years of domains from Dr. Chris Lee and populated them in DNS zones that would point infected clients into a sinkhole. Data from the web servers is distributed to remediators.
- Each December, I/we process the next year and relate lists of domains to registry operators. If they point domains to the sinkhole, we continue visibility. Idea of containment was already lost (C never materialized, A/B attrition started ~2012). Still, we had visibility.

# It’s 20-freakin-21

FARSIGHT SECURITY

- We only had domains until 2020 – who’d think we’d need them this long?
- I reached out to known recipients of the data and the CWG team and asked if it was worth continuing, especially if we are going to put registries through another year of registrations.
  - A remediator said yes.
  - A cyber-risk organization said, “Sadly, yes.”
- Alright, I need a 2021 list.
  - Dr. Lee offered to help.
  - Dr. Vixie dug up a domain generator out of his toolbox (Kaspersky).
- Their generated lists for A/B matched, but the C lists did not?!?  Uh oh.

# Kinda matched – a view of 2020-05-06

FARSIGHT SECURITY

Domains in sinkhole

aaamnv.is
aaboptq.hu
aabp.no
aabqn.tn
aacc.cl
aachlqaaw.sh
aacuxno.ae
aacv.mn
aadezabu.com.jm
aadhzjfio.su
. . . etc . . .

Kaspersky's generator on FreeBSD32

aaamnv.is
aabebg.com.pr
aabp.no
aabqn.tn
aacc.cl
aachlqaaw.sh
aacjewmm.hn
aacuxno.ae
aadezabu.com.jm
aaeisl.sc
. . . etc . . .

# Doubts about current domain generation

FARSIGHT SECURITY

- Out of 110 registries, only 2 participate.  Each day, ~50000 domains point to a different IP address per domain to accept HTTP “GET /”.
- Occasionally chasing false positives in web sinkhole observations
  - Q: “Why was this source IP flagged?”
  - A: “We logged a web hit at one of the sinkhole addresses.”
  - Domain assigned to destination address was from a non-participating registry
  - Background radiation of web scanners
- Solutions:
  - Make domain/IP list available
  - Provide some better filtering tips
- Still... Many more hits on unregistered IPs than registered IPs

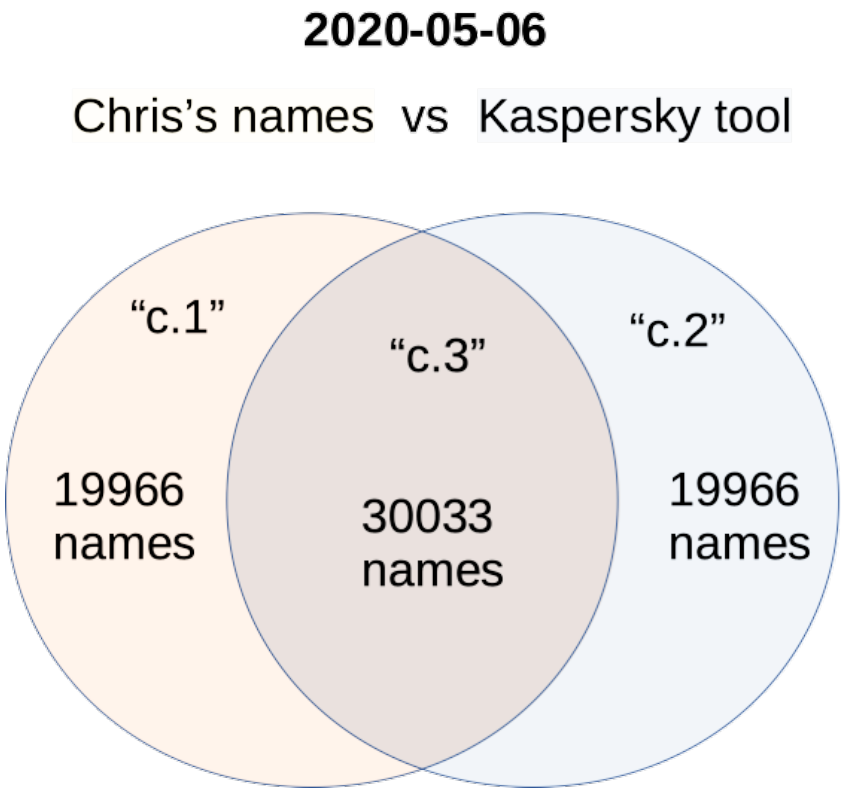
# How do we verify?

FARSIGHT SECURITY

- Run an infected client – see what domain names it tries to query
  - Cumbersome to set up (Win 95 32-bit, logging DNS server)
  - Only a few tries per day
- Wouldn't the correct algorithm look for Conficker domains of nameservers more often than other names?
- Recursive servers would only see names if their clients are infected. Ignoring qname minimization, root servers might have a complete view.
- DITL!

# Counting names against DITL

- Let’s group the domain names into which method generates them.



# DNS-OARC data processing

FARSIGHT SECURITY

- Saw someone running this on `an1` against DITL clean pcaps:

```
tshark -r FILE.gz -n -T fields -e dns.qry.name -e dns.qry.type -e ip.src
```

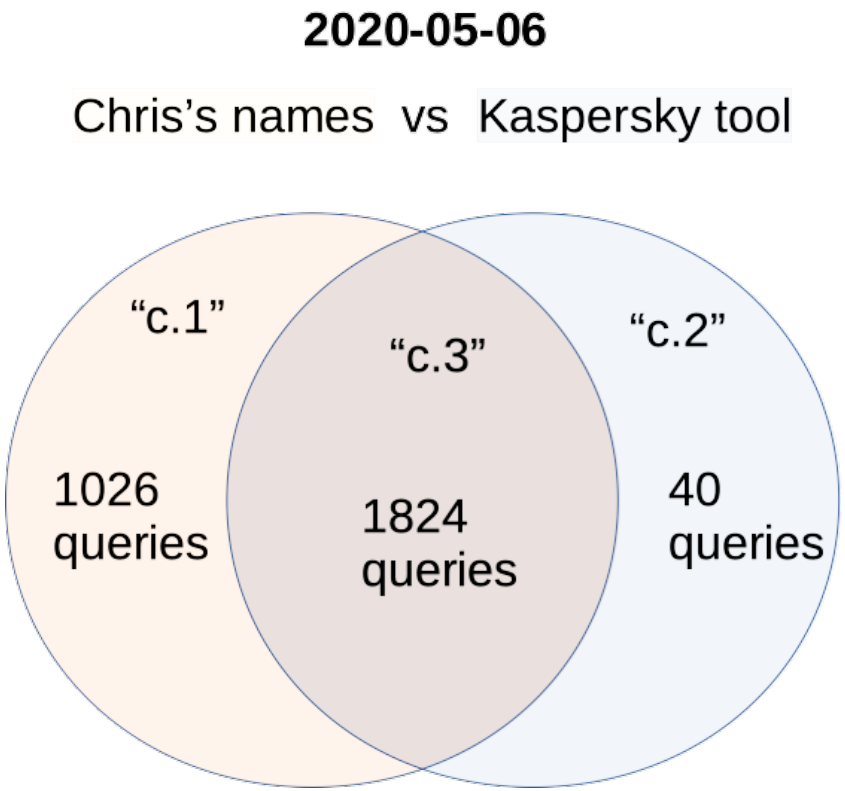
- Take output and use perl associative arrays to tag “1” or “2” or “3” depending which dns.qry.name matched.
- Parallelize with:

```
find DITL-20200505 -name 20200506.*.gz -type f |\
   xargs -P 8 -n 1 -I {} process.sh {}
```

- The process.sh is essentially the tshark + perl tagging part that writes matched name, tag, type, source_ip output.

# Counting names against DITL 2020

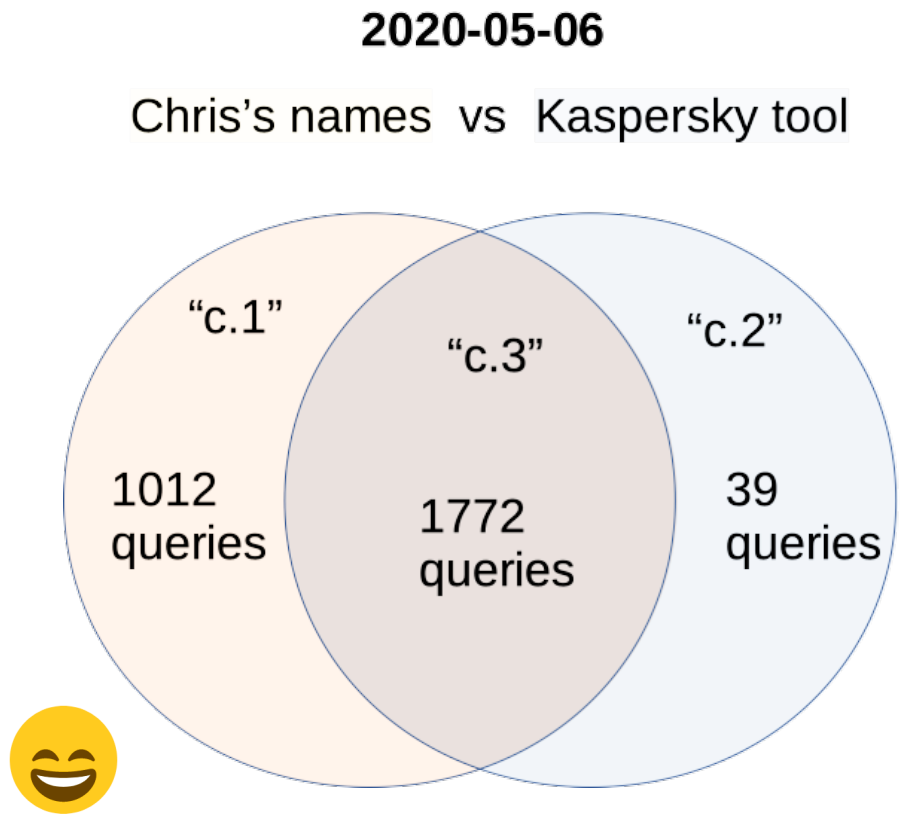
- Results for all domains:



# Counting names against DITL 2020

FARSIGHT SECURITY

- Results excluding registered domains (possible web crawling):

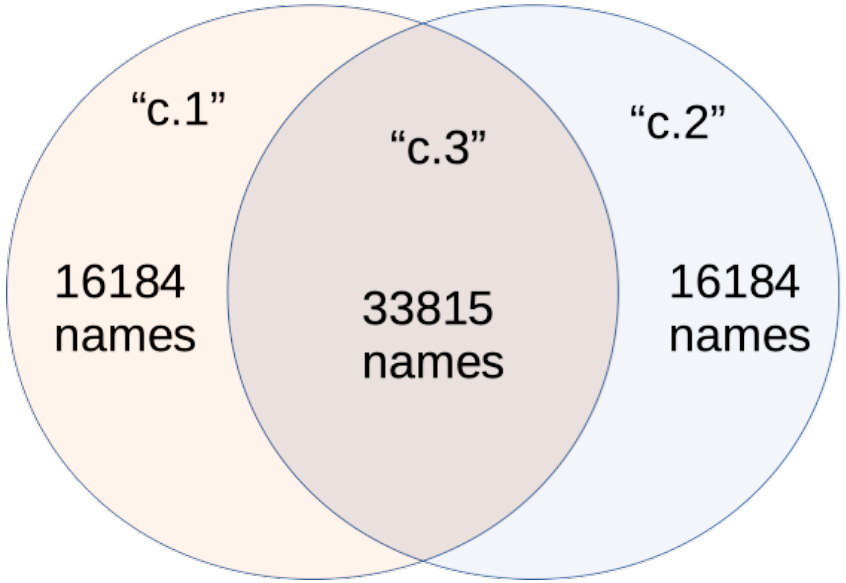


# Counting names against DITL 2019 (in progress)

- Results excluding registered domains (possible web crawling):

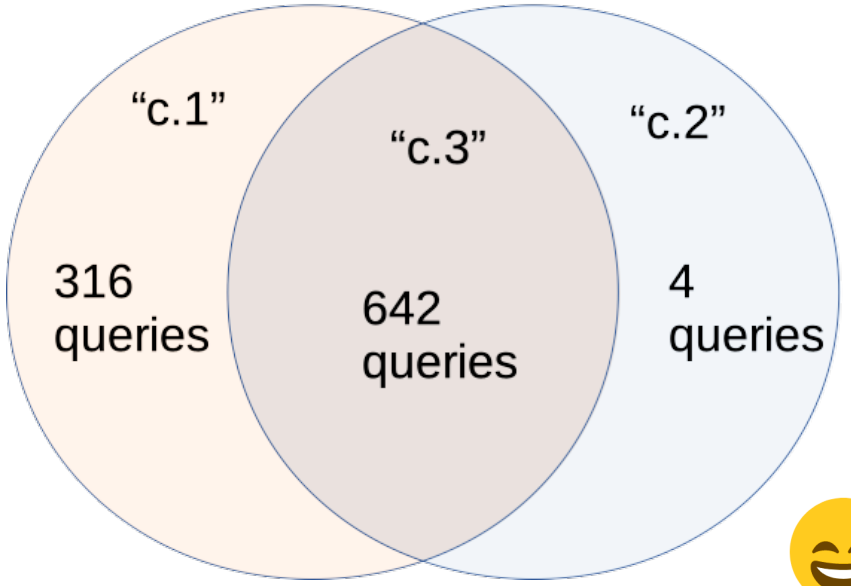
**2019-04-09**

Chris's names vs Kaspersky tool




**2019-04-09**

Chris's names vs Kaspersky tool



# Theory

FARSIGHT SECURITY

- There is a difference in the math library used between the Windows malware environment and the FreeBSD VM on which I was running the Kaspersky domain generation tool.  The bit copying between the floating point and integer values in the PRNG algorithm might diverge after repeated operations such that different domain names emerge.

- https://net.cs.uni-bonn.de/wg/cs/applications/containing-conficker/
- http://lira.epac.to/DOCS-TECH/Hacking/KYE%20-%20Conficker.pdf

  (page 13)

# Next

FARSIGHT SECURITY

- Get better filtering tools out to data recipients to avoid false positives in C “hits”.
- Try counts against a 2010 DITL when bot was more widespread.
- Low usage wouldn’t justify resources for IP addresses and registrations. Let’s see if we can wind down C resources after this year and continue A&B monitoring which still sees many more hits/day (500/sec).


- Thanks to Dr Chris Lee, participating registry operators, ISPs that provide addresses/connectivity, CWG members, and also Team Cymru for running some of the web servers.
- Thanks to DNS-OARC and root operators for making DITL data available.




DNS is in our DNA™

FARSIGHT SECURITY