RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: TV-T07

DOES MALWARE HAVE CITIZENSHIP? WHO'S INFECTING US AND DOES IT MATTER?

Chester Wisniewski
@chetwisniewski

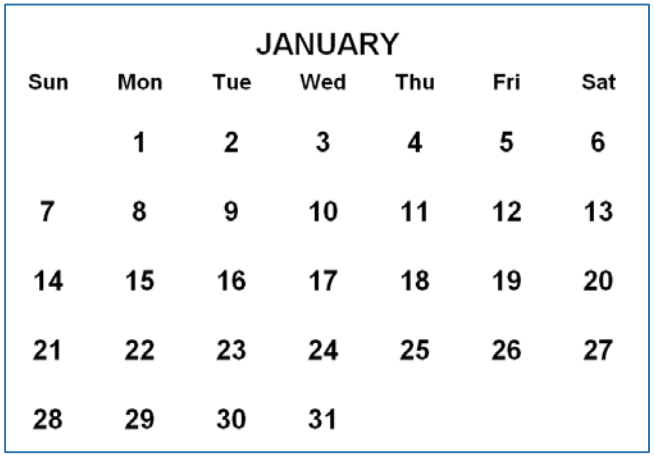
Principal Research Scientist
Sophos Inc.

Is region blocking effective?

Image CC-SA by ICMA

The data – What was analyzed?

- AS(N)s
- Countries
- Threat types
  - C2/Command & Control
  - Infected sites
  - Malware repositories
- ISPs/Providers



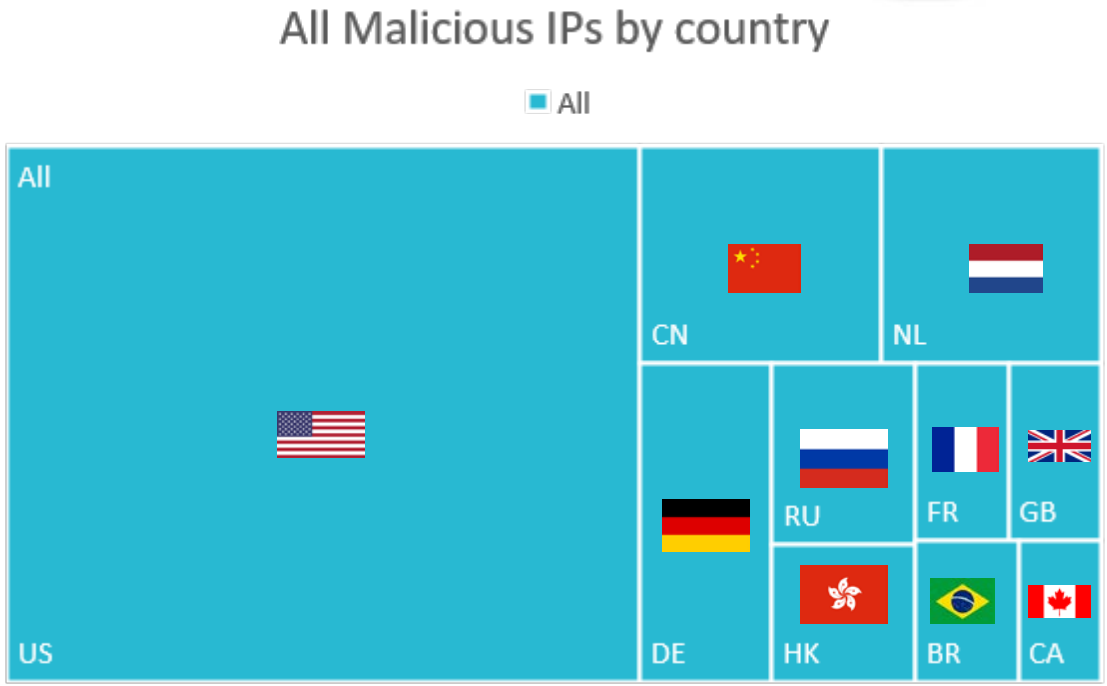
SOPHOS labs

By the numbers

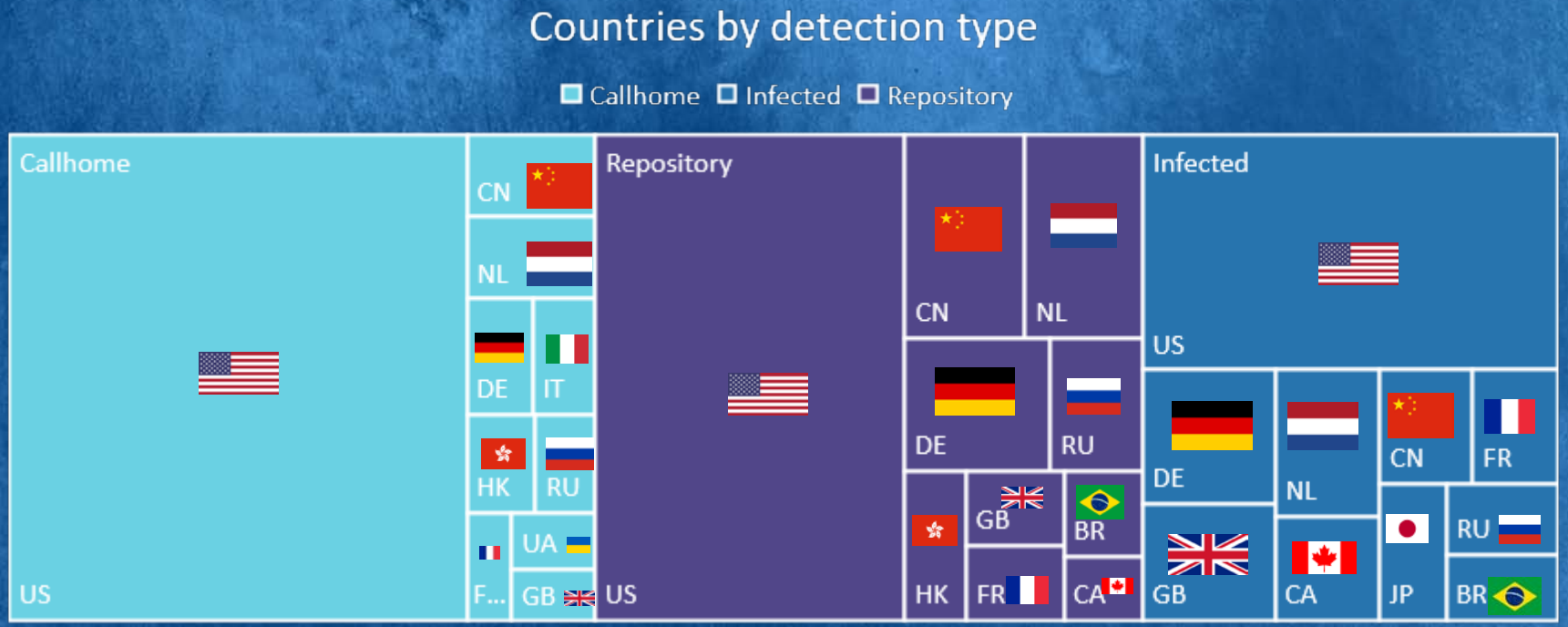
- 1,166,479 Unique blocked network items
  - 12,695 Call home/C2 items
  - 17,956 Infected domains/pages
  - 1,135,828 Repositories/sites hosting threats
- 152,261 Unique domains
- Hosted on 43,151 unique IP addresses

Where is the bad stuff

# of hosts	Country	Percent
19952	US	46.45
3082	CN	7.18
2826	NL	6.58
2471	DE	5.75
1525	RU	3.55
1155	HK	2.69
968	FR	2.25
965	GB	2.25
856	BR	1.99
691	CA	1.61

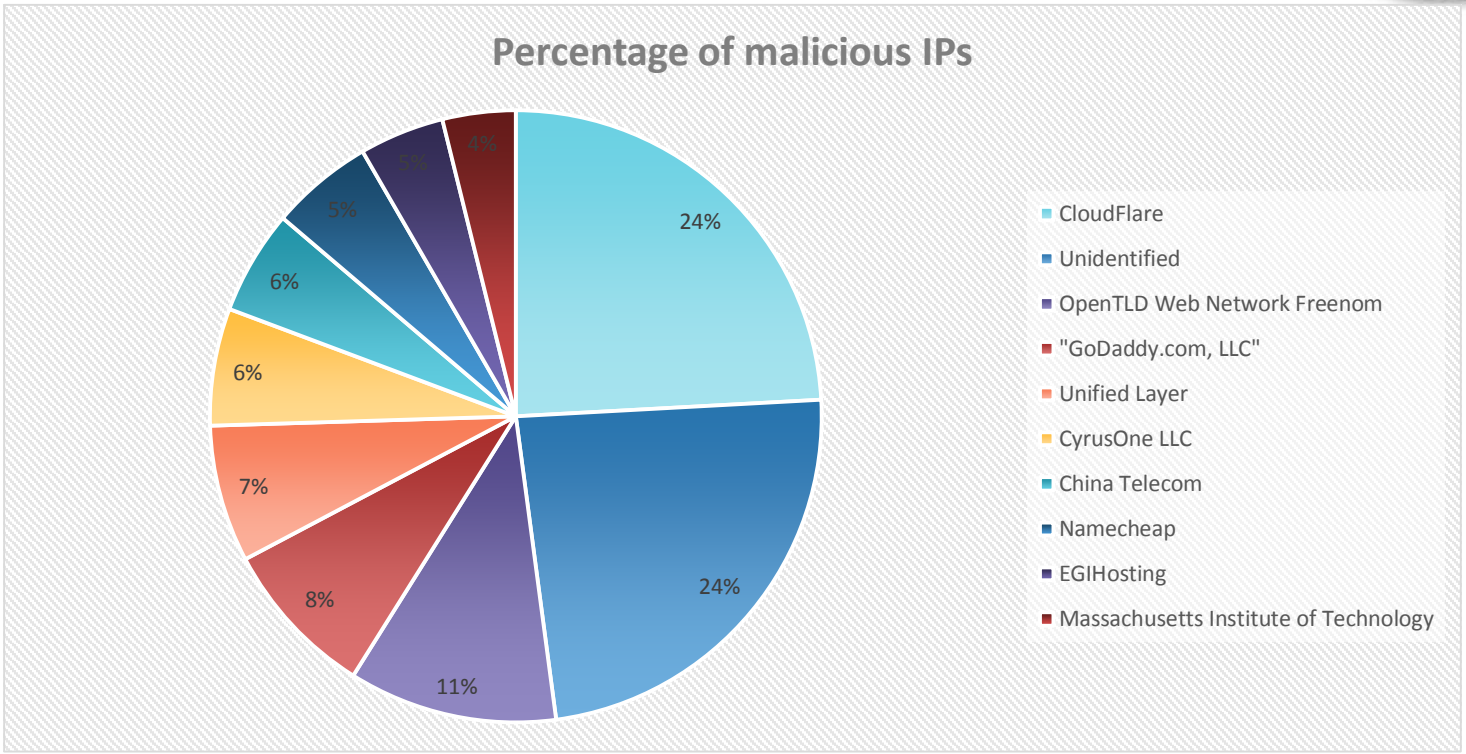


Does it vary by type?

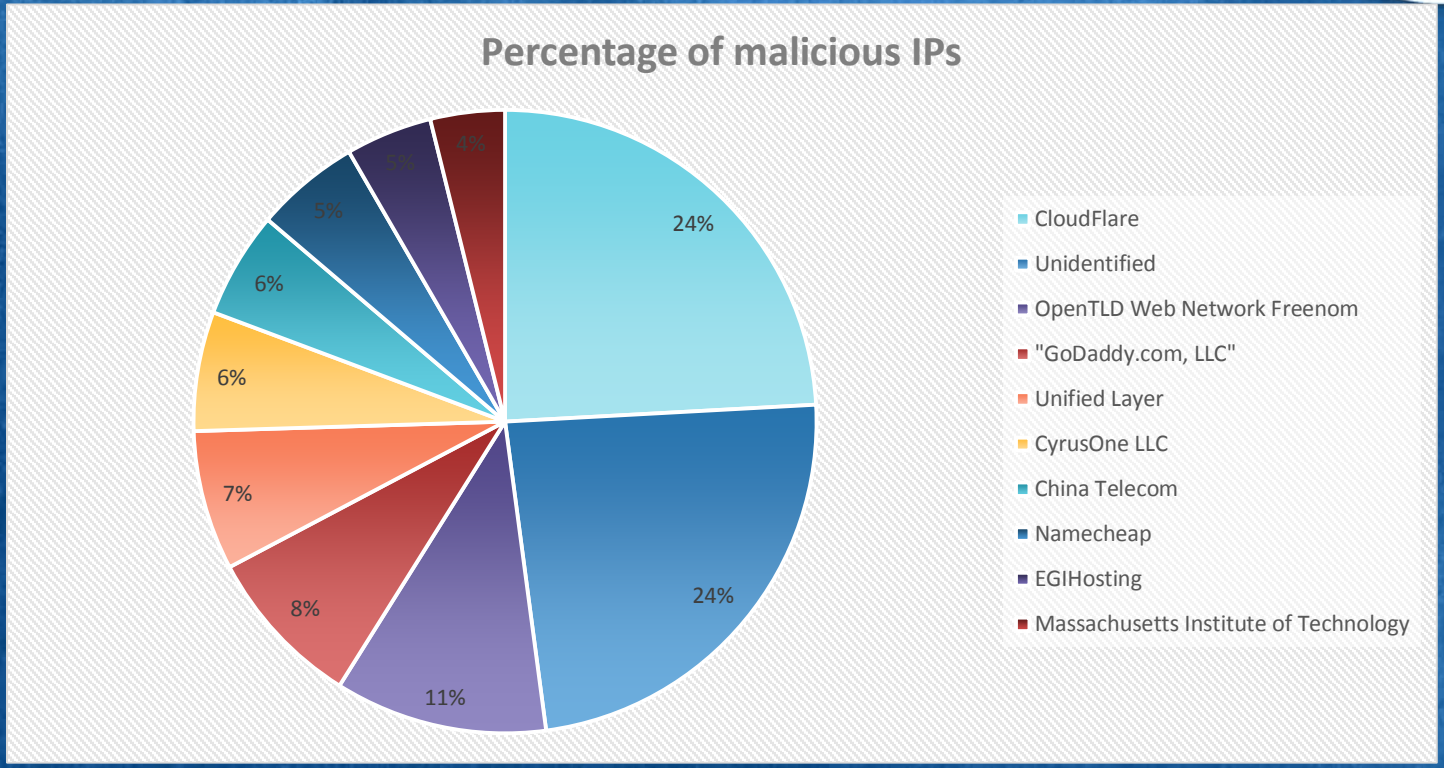


How else might we look at this?

Perhaps we can block ISPs



Maybe Organization (WHOIS)



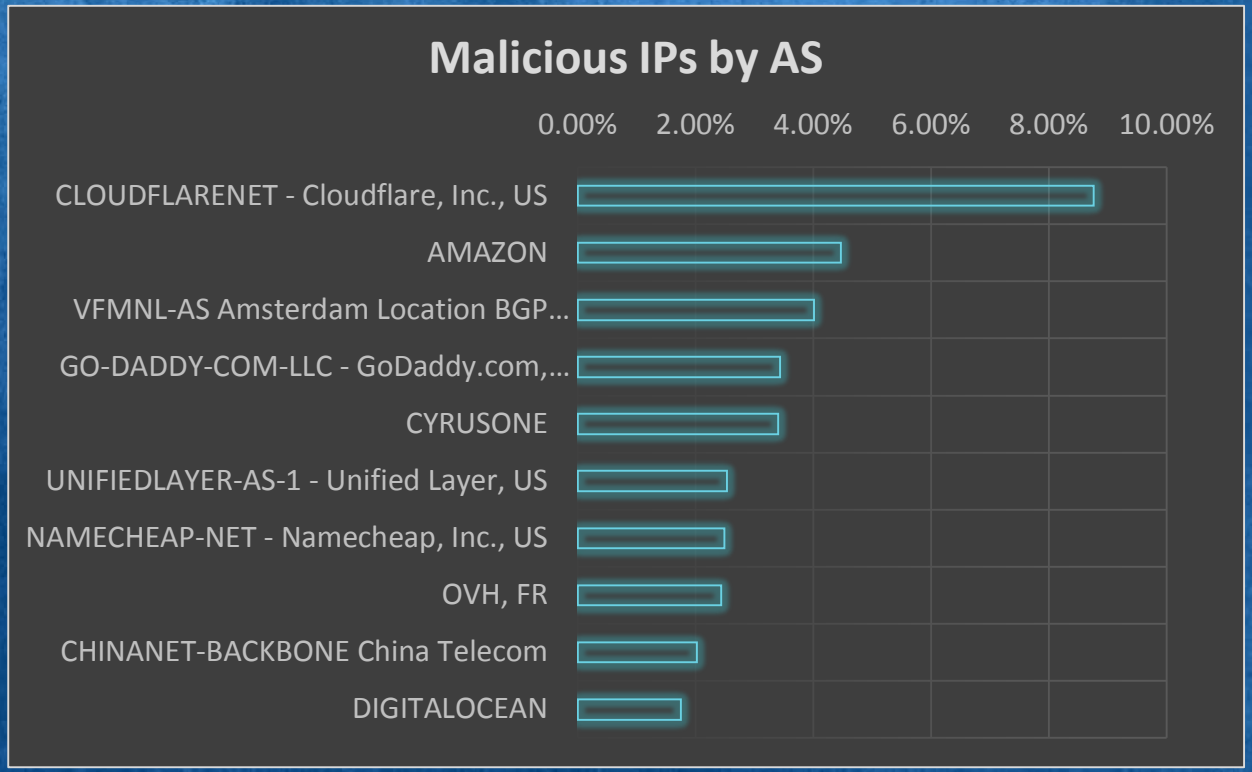
Too much collateral damage

Last try. Maybe we will have luck by AS

"Within the Internet, an **autonomous system** (**AS**) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity…"

- More accurate than WHOIS
- Reputation hard to repair
- Can't easily move about

Clearer, but not terribly useful



Where does this leave us?

- Blocking IPs by country/AS/IP block is ineffective at best
- Major providers could do a much better job monitoring for abuse
- Network blocks most effective as dynamically updated service
  - Threat intelligence feeds
  - Cloud lookup service
  - In-house curated phishing targets

Q&A

- Reach me:
  @chetwisniewski
  chesterw@Sophos.com
- More research at:
  https://www.sophos.com/en-us/labs.aspx
- Security news:
  https://nakedsecurity.sophos.com