proofpoint

MESSAGING ABUSE AND THREAT TRENDS

Kevin San Diego

Cloudmark Product Management

November 8, 2018

JP AAWG

1st General Meeting

450+ Million Protected Email / Mobile Users Worldwide

5+ Billion Messages Scanned Daily

15 Second Live Threat Updates

100+ Security Threat Operations & Researchers

120+ ISP, Mobile Network Operators & Hosting Customers

98% Customer Retention

GMO INTERNET GROUP · NTT Communications · verizon · COX COMMUNICATIONS · CTC Challenging Tomorrow's Changes · PCCW 電訊盈科 · Comcast · OCN OPEN COMPUTER NETWORK · SoftBank

Changes in Domain Name Registrations

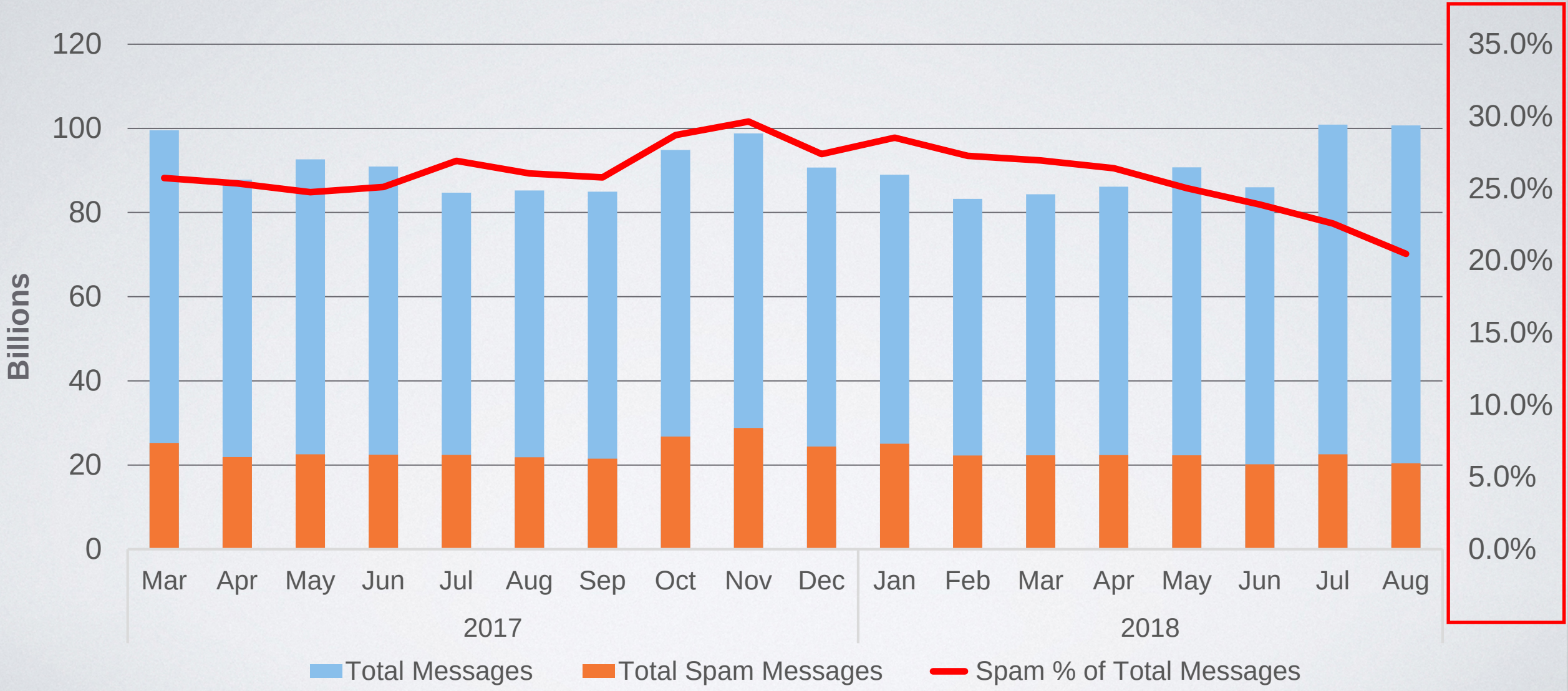
- Explosion of Generic Top-Level Domains (gTLDs)
- Registrars offer bulk discounts for gTLD registrations

Top 30% of gTLDs seen in 2018 send 90+% Malicious Content.

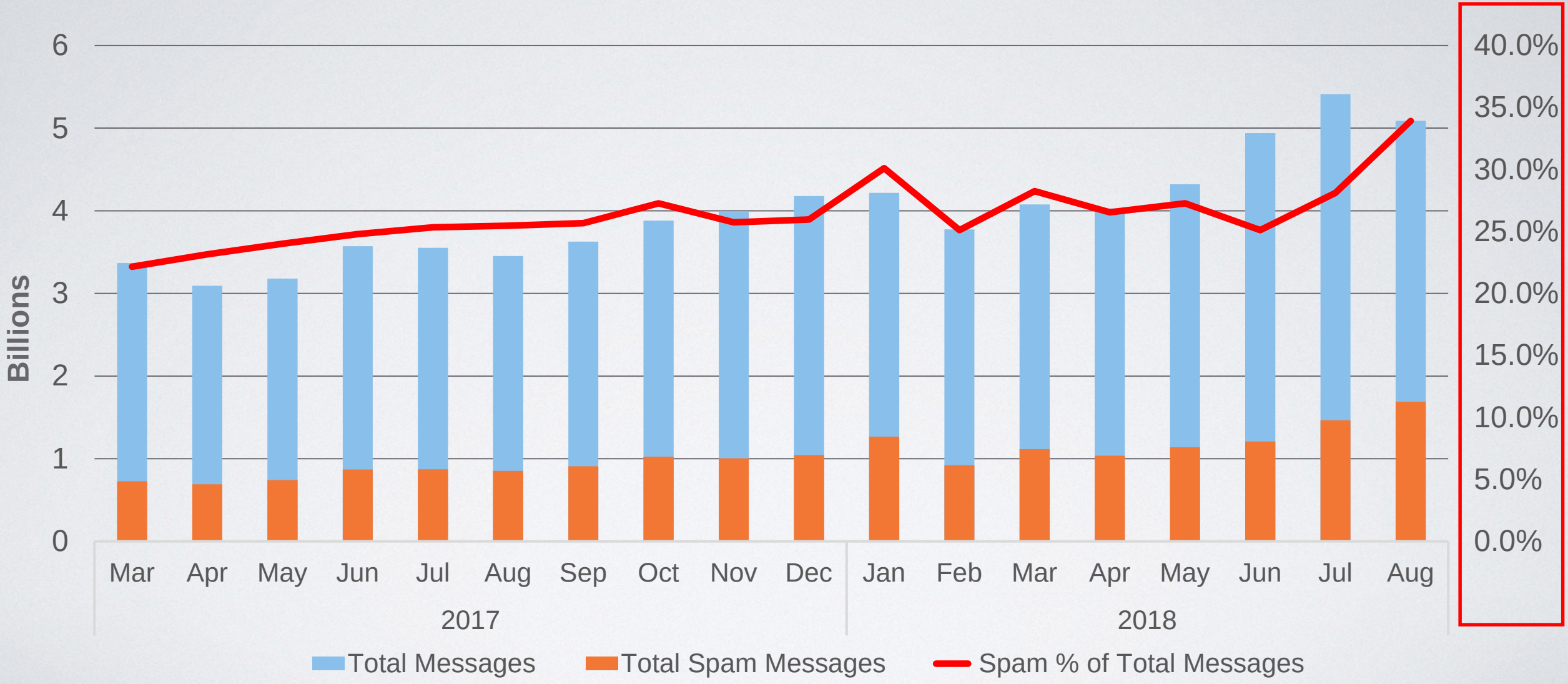
Source: Cloudmark Authority, +10,000 registered domains

Threat Trends: Japan vs. Rest-of-World

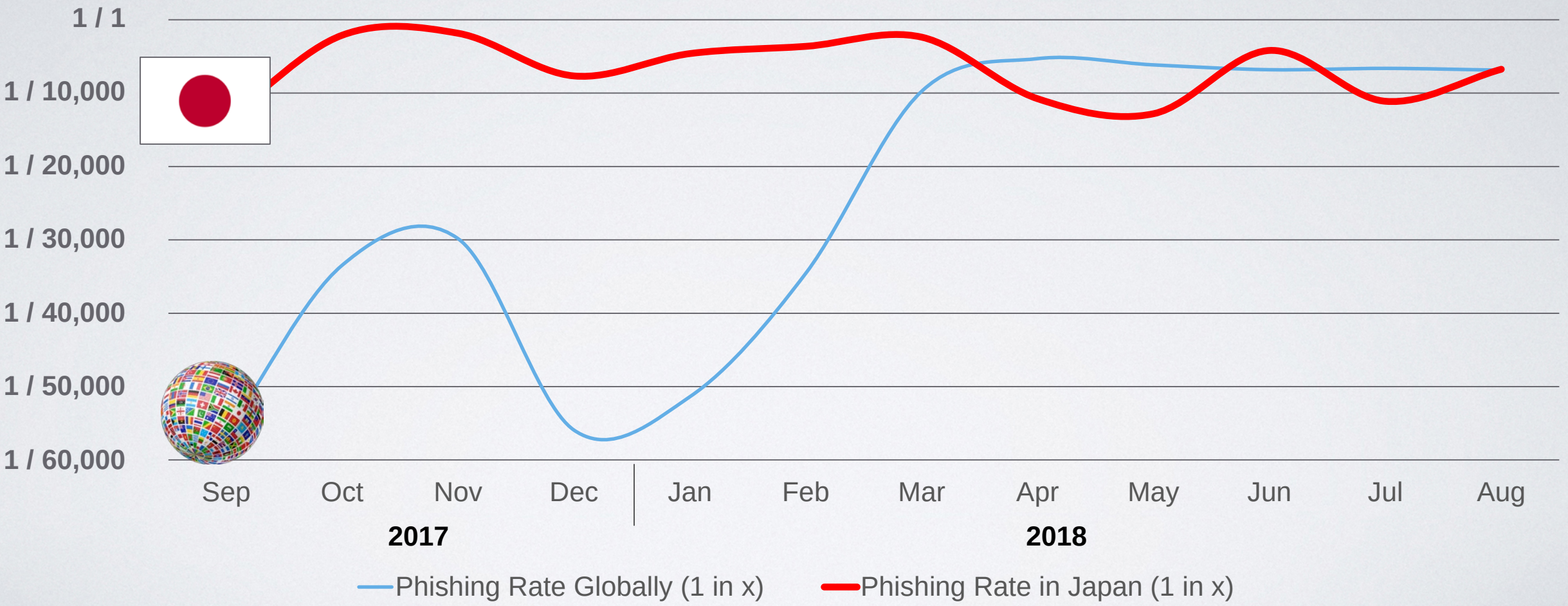
Overall and Spam Message Rates Globally



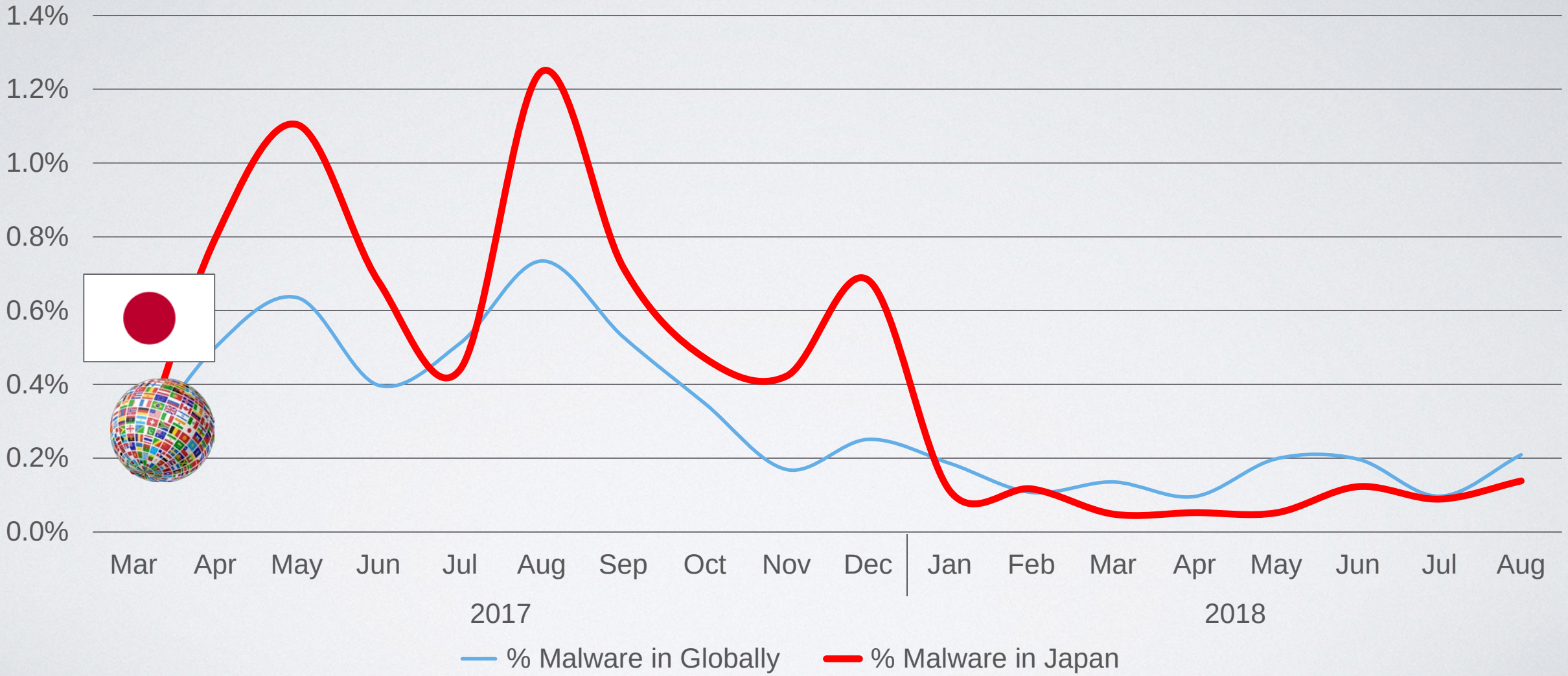
Overall Spam Message Rates in Japan



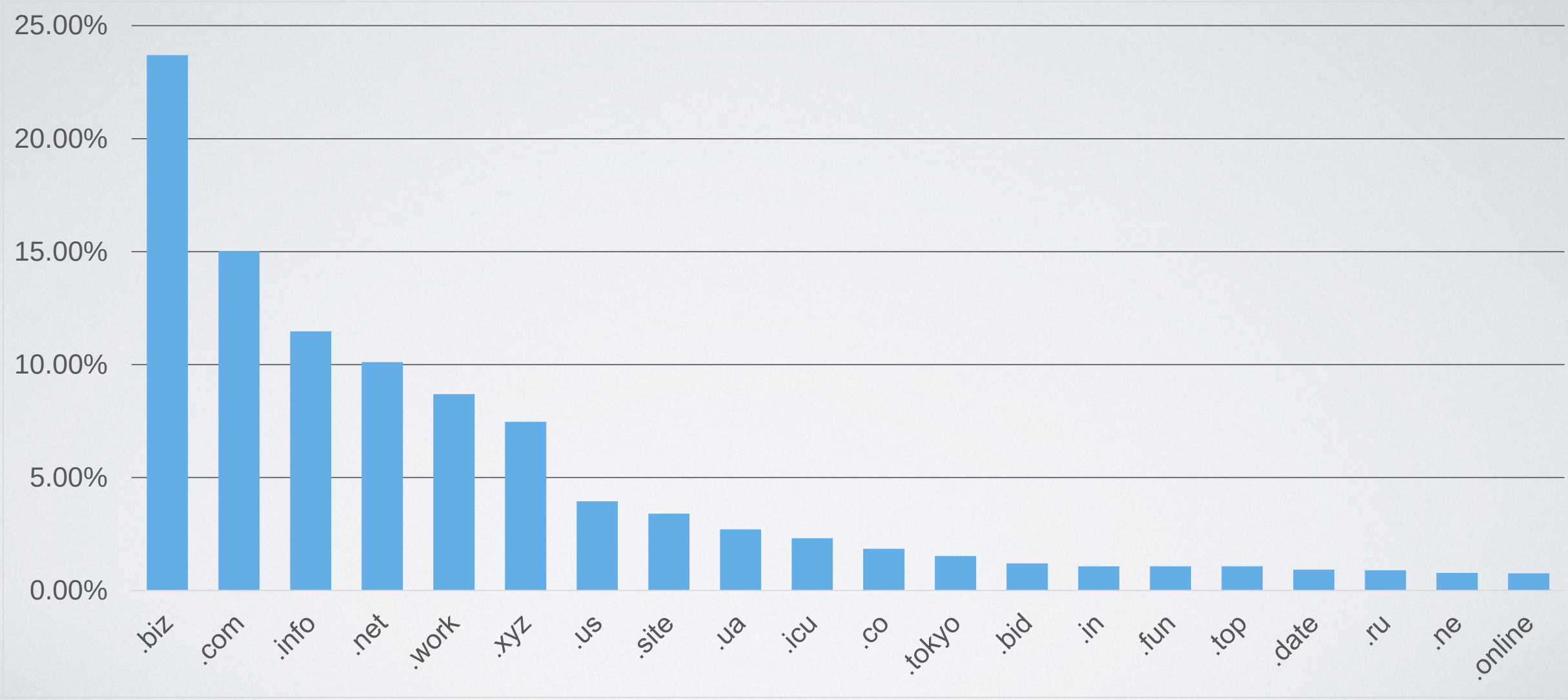
Phishing Ratio (1 Phish in every n Spam)



Malware Messages as Percentage of Unwanted Messages



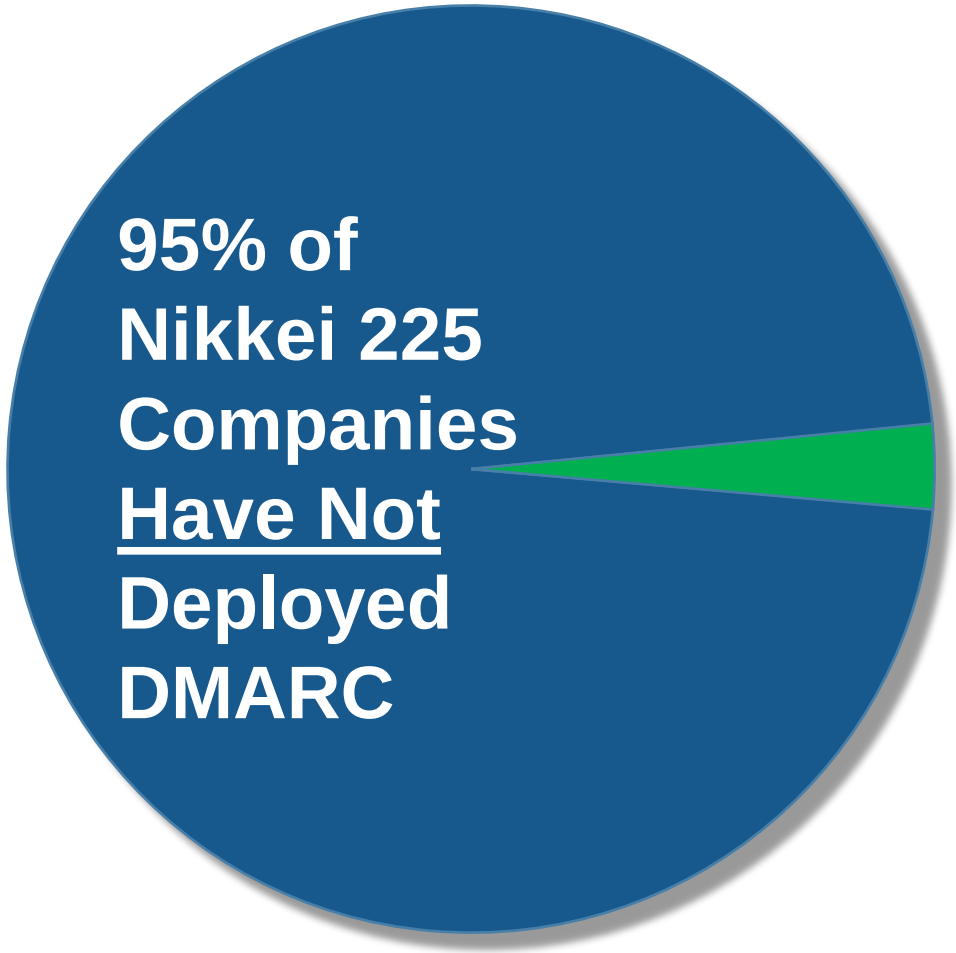
Main TLDs Observed in Spam Call-To-Action URLs



DMARC Deployment

Examining Companies in the Nikkei 225

DMARC Deployment Statistics in Japan
Analysis of Nikkei 225



5% Have DMARC Deployed*

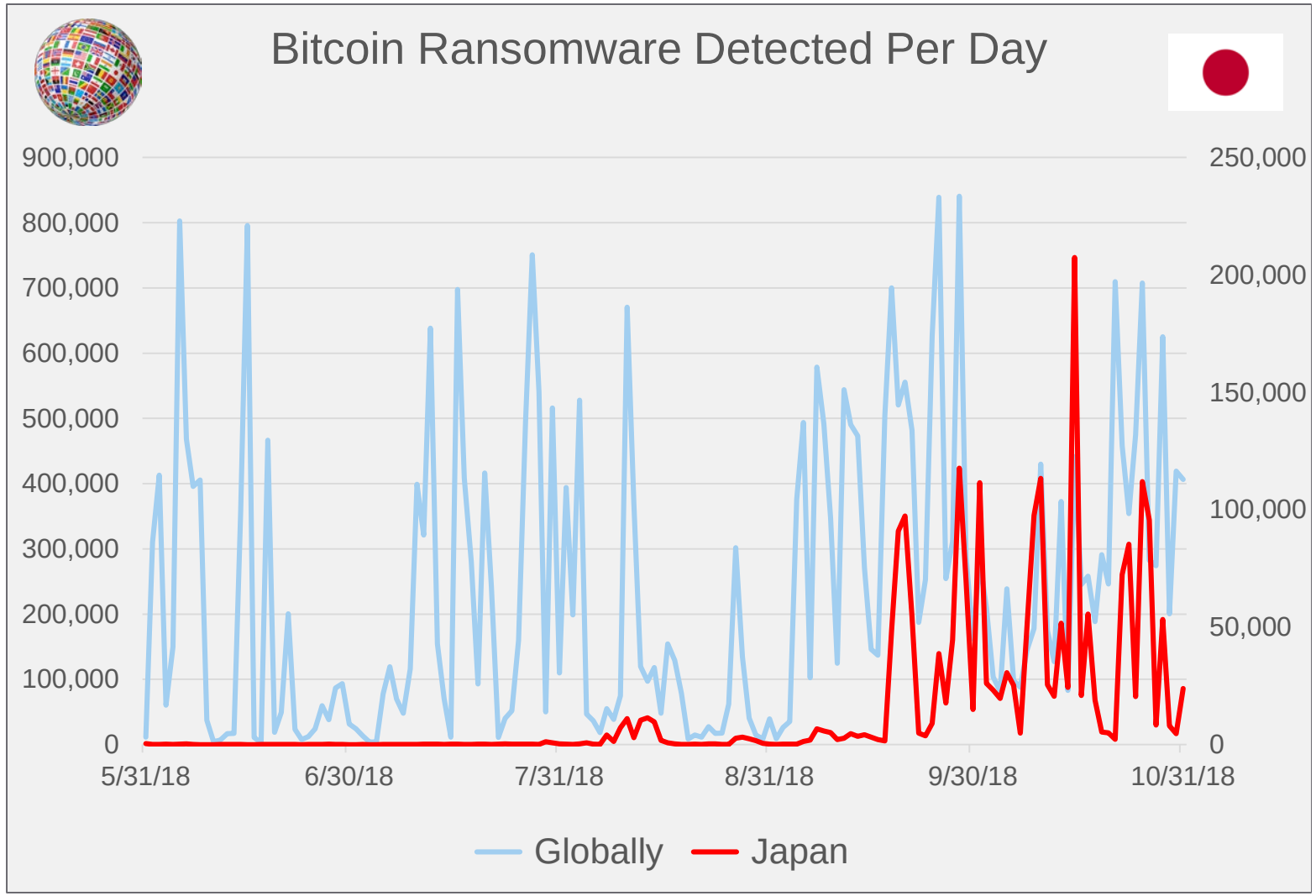
- Asahi Glass
- Eisai
- Fast Retailing
- Mitsubishi Estate
- Mitsubishi UFJ Financial
- Mizuho Financial
- NTT DATA
- Olympus
- Rakuten
- Sumitomo Mitsui
- Trend Micro

**All are in "p=none" mode*

Phishing Threat Trends

“I Hacked You” Bitcoin Extortion Scheme

- Social Engineering scheme
  - Fakes “From:” header
  - Threatens to release embarrassing information unless ransom paid in Bitcoin
- Exploiting email/password dumps
  - In many examples, user’s password listed in “Subject:” line
- Very little technical investment required, but campaign has collected over ¥12,000,000 in just a month

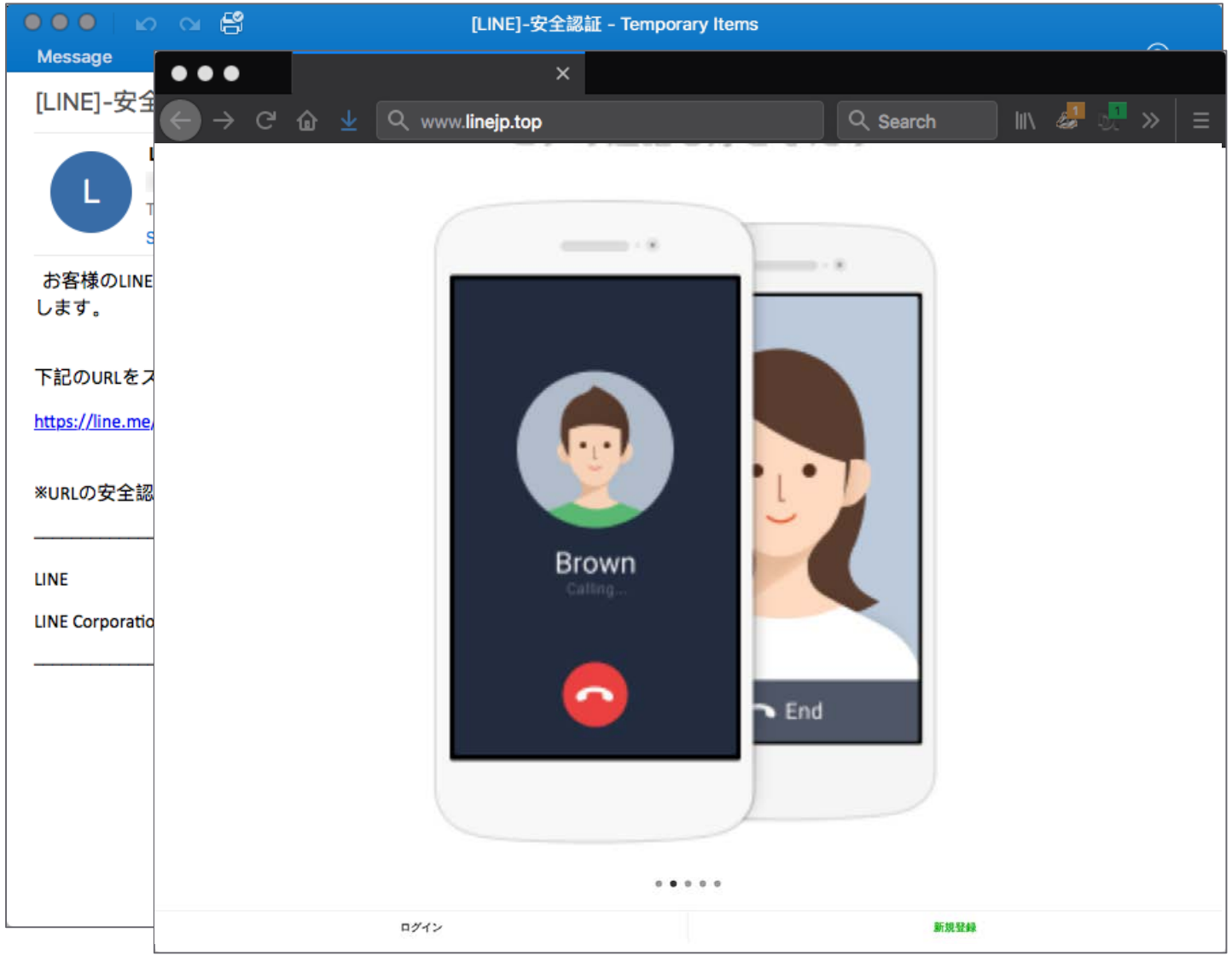


Apple Credential Phishing

- “Account Disabled” phish
  - Prompt users to “log in” to re-establish account
  - Other attacks also include malware payloads
- Once hackers have credentials:
  - Hold user device data for ransom (can wipe)
  - Leverage mac.com/icloud.com email access to reset other 3rd party passwords

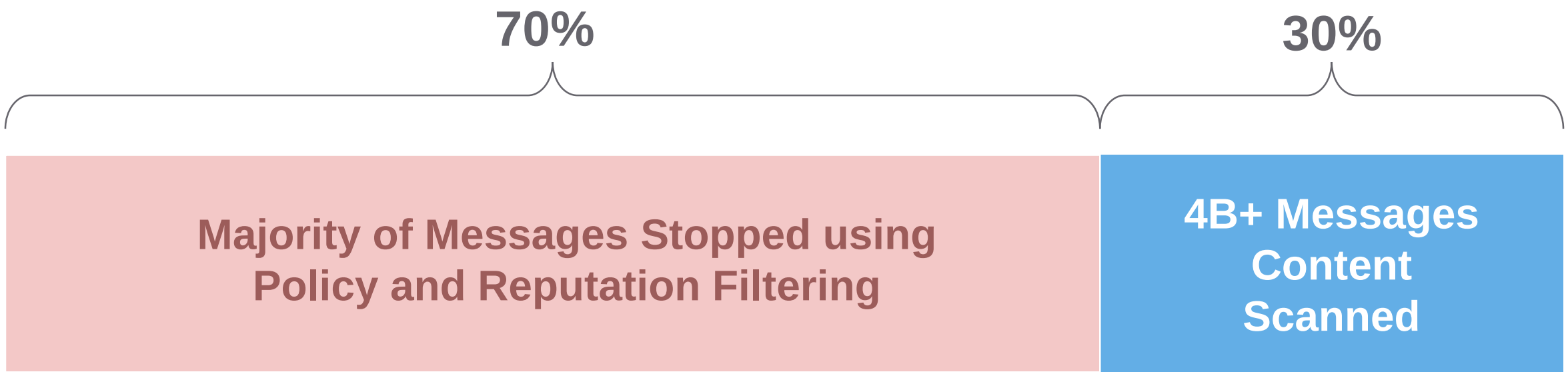
LINE Credential Phishing

- Social Engineering scheme
  - Spoofed “From:” header
  - Message appears to be plain text
- Obfuscated URL
  - Redirects to a look alike domain
- Attackers seeking credentials
  - Likely used for account hijacking
  - Extortion
  - “Friend” phishing



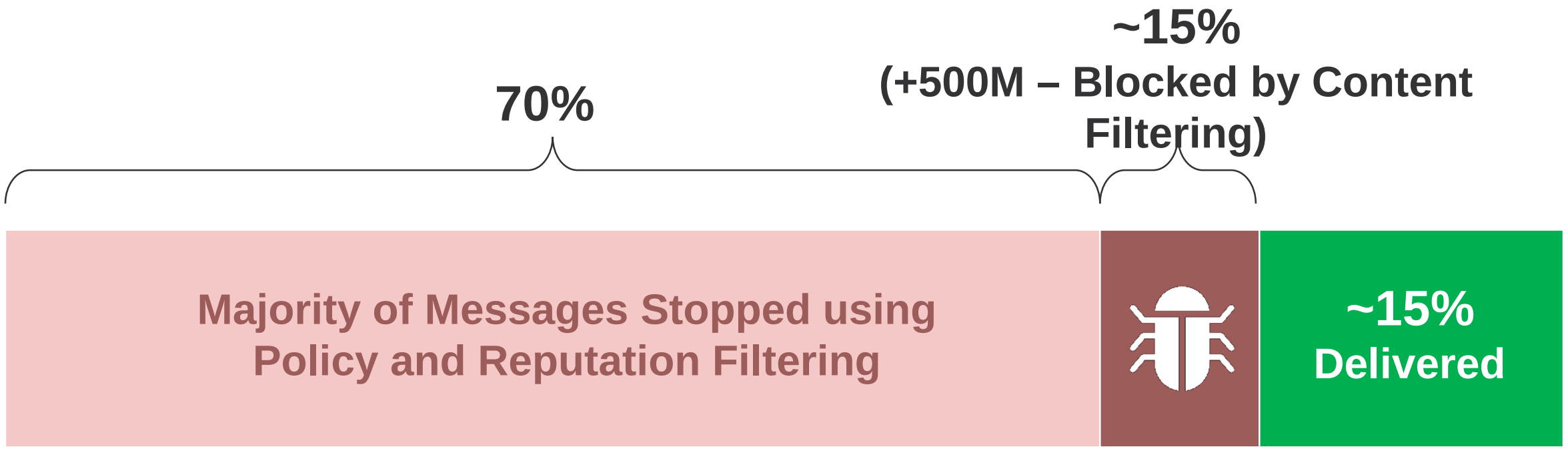

proofpoint®

Daily Spam & Virus Activity Q1-Q2 2018



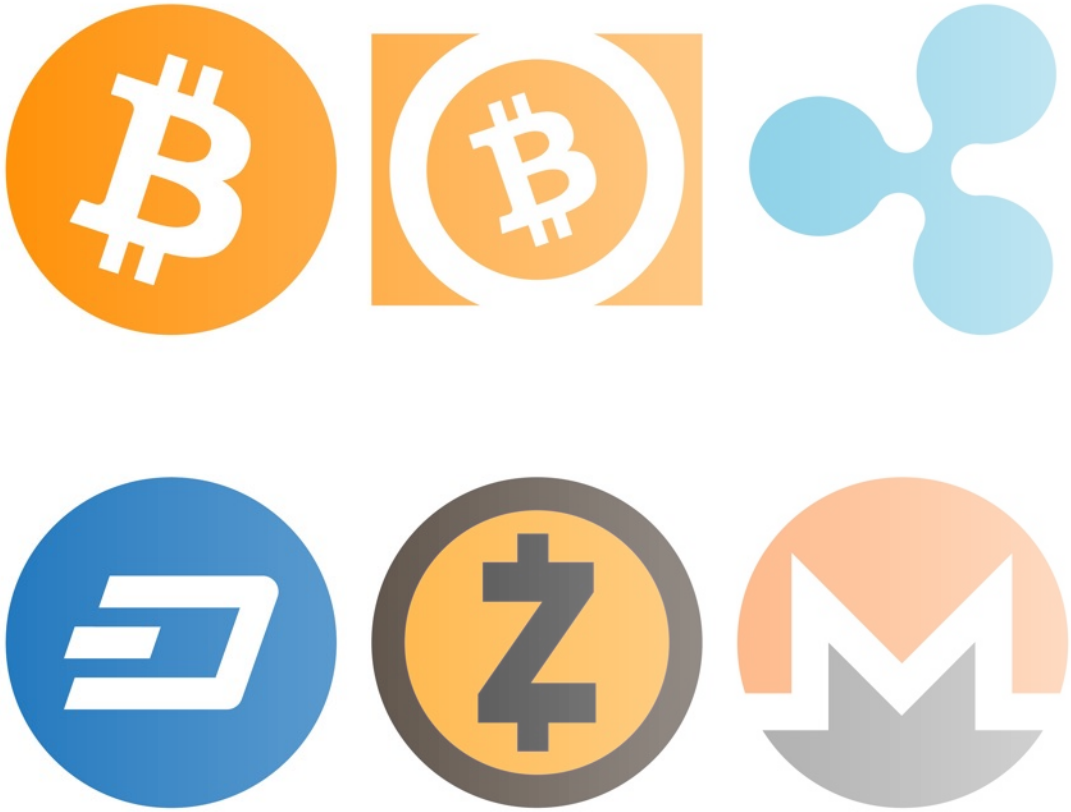
Activity detected by Cloudmark Authority.

Daily Spam & Virus Activity Q1-Q2 2018



Activity detected by Cloudmark Authority.

Cryptojacking invitations: COINHIVE Events

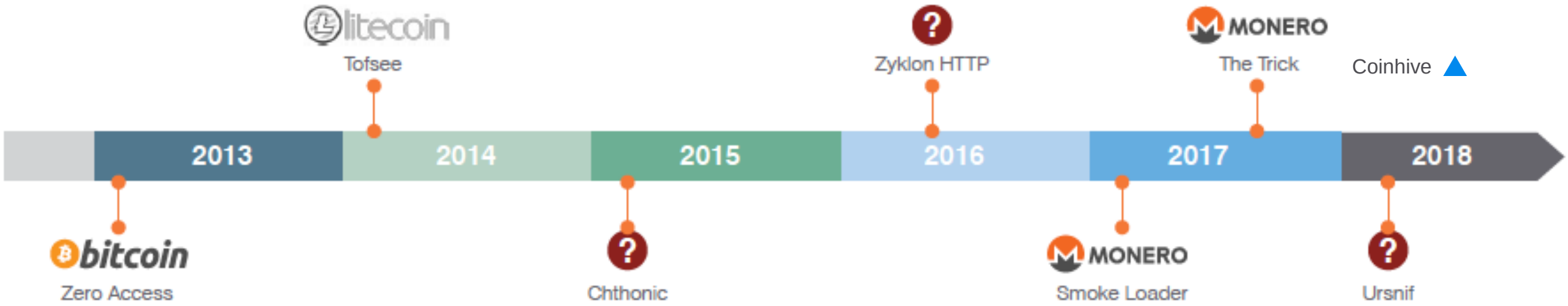


Hijacks computer resources to mine for cryptocurrency.

Undetected by anti-virus.

Targets users indiscriminately.

Timeline of Cryptocurrency Mining Malware



Source: Proofpoint Quarterly Threat Report Q22018.

Coinhive IDS Events

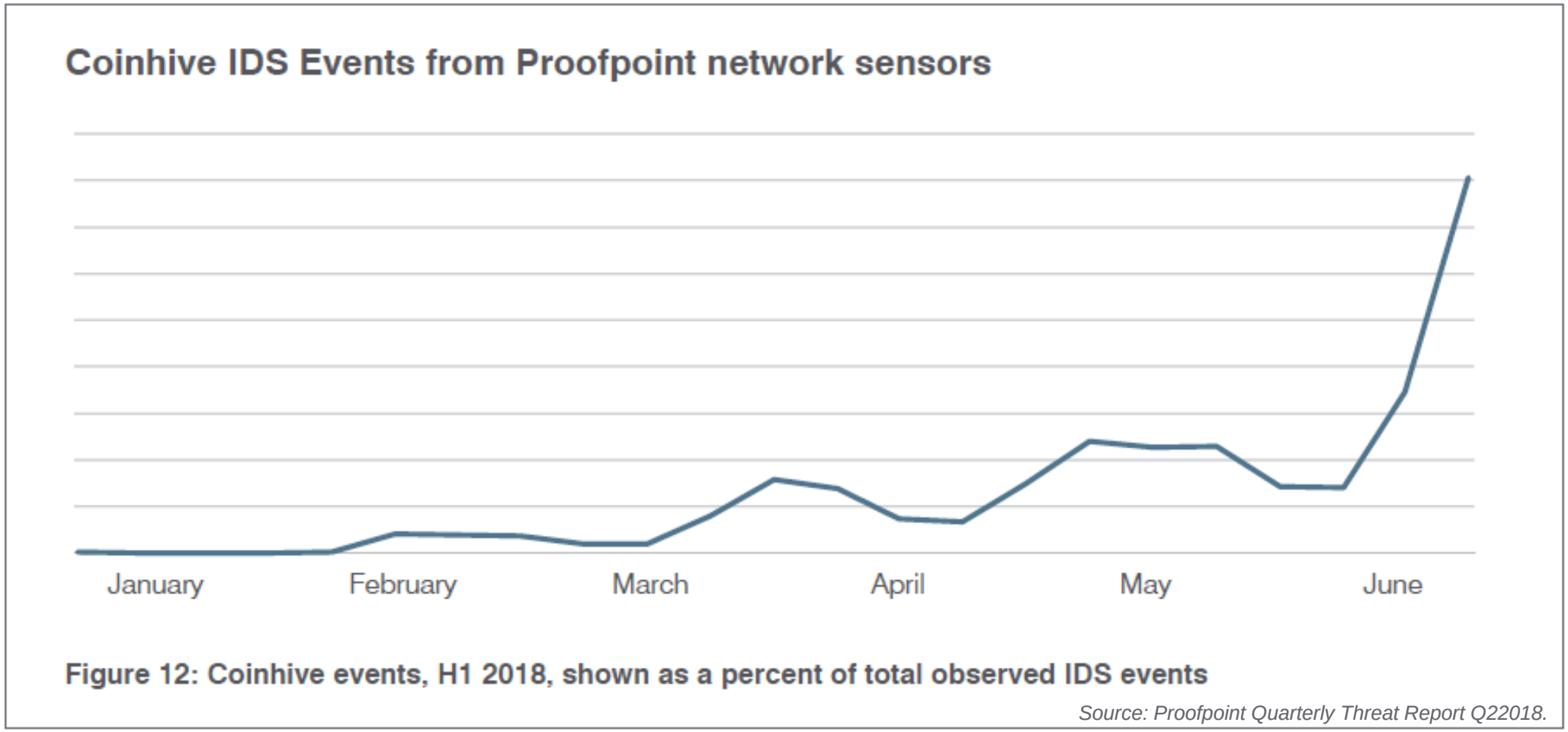


Figure 12: Coinhive events, H1 2018, shown as a percent of total observed IDS events

Source: Proofpoint Quarterly Threat Report Q22018.

Coinhive cryptomining events jumped 460% vs Q1 2018