MESSAGING ABUSE AND THREAT TRENDS

Kevin San Diego
Cloudmark Product Management
November 8, 2018
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
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

- **Billions**
- **Overall and Spam Message Rates**
- **2017**
- **2018**
- **Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug**
- **Total Messages**
- **Total Spam Messages**
- **Spam % of Total Messages**

- **Spam % of Total Messages**
- **0.0% - 35.0%**
Overall Spam Message Rates in Japan

- Total Messages
- Total Spam Messages
- Spam % of Total Messages

<table>
<thead>
<tr>
<th>Month</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Apr</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>May</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Jun</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Jul</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Aug</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Sep</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Oct</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Nov</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Dec</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Jan</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Feb</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Mar</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Apr</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>May</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Jun</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Jul</td>
<td>3.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Aug</td>
<td>3.0</td>
<td>4.0</td>
</tr>
</tbody>
</table>

Billions

- 0.0%
- 5.0%
- 10.0%
- 15.0%
- 20.0%
- 25.0%
- 30.0%
- 35.0%
- 40.0%
- 45.0%
- 50.0%
- 55.0%
- 60.0%
Phishing Ratio (1 Phish in every n Spam)

- Phishing Rate Globally (1 in x)
- Phishing Rate in Japan (1 in x)
Malware Messages as Percentage of Unwanted Messages

- % Malware in Globally
- % Malware in Japan
Main TLDs Observed in Spam Call-To-Action URLs

- .biz: 25.00%
- .com: 15.00%
- .info: 10.00%
- .net: 5.00%
- .work: 2.00%
- .xyz: 1.00%
- .us: 0.50%
- .site: 0.25%
- .ua: 0.12%
- .icu: 0.06%
- .co: 0.05%
- .tokyo: 0.03%
- .bid: 0.02%
- .in: 0.02%
- .fun: 0.01%
- .top: 0.01%
- .date: 0.01%
- .ru: 0.01%
- .ne: 0.01%
- .online: 0.01%
DMARC Deployment
Examining Companies in the Nikkei 225
DMARC Deployment Statistics in Japan
Analysis of Nikkei 225

95% of Nikkei 225 Companies Have Not Deployed DMARC

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
Majority of Messages Stopped using Policy and Reputation Filtering

4B+ Messages Content Scanned

Activity detected by Cloudmark Authority.
Daily Spam & Virus Activity Q1-Q2 2018

70%

~15% (+500M – Blocked by Content Filtering)

Majority of Messages Stopped using Policy and Reputation Filtering

~15% Delivered

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

Coinhive cryptomining events jumped 460% vs Q1 2018

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