COVID-Related DNS Abuse Webinar
(Hosted by the Contracted Party House)

Agenda

• Overview
• Siôn Lloyd, ICANN SSR
• Chris Lewis-Evans, UK National Crime Agency
• Graeme Bunton, Tucows
• James Galvin, Afilias
• Brian Cimbolic, PIR
• Q&A
  • Registry/Registrar Experiences
  • Community Q&A
COVID-19, What we see
Siôn Lloyd
ICANN SSR
Big events have associated bursts of domain name registration

COVID-19 no different
  - The extra working from home makes it the perfect storm
Domain trends update

(Source: John Conwell, DomainTools)
How does our identification approach work?

• Our approach for identification:
  • Pandemic-related keyword search within zone files (gTLDs + a few ccTLDs)
How many domains have we identified?

- 662,111 domains were identified since January 2020
What keywords do these domains contain?

- Most of the domains related to 3 keywords
  - 4 keywords account for 73% of the domains
- Different keywords categories:
  - Disease name (covid, ncov, sars, ...)
  - Pandemic countermeasures (mask, lockdown, quarantine,...)
  - Collateral (zoom, webex, conference, ...)
- Significant number of domains matches non-English terms

<table>
<thead>
<tr>
<th>Language</th>
<th>%Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>94.21%</td>
</tr>
<tr>
<td>German</td>
<td>2.13%</td>
</tr>
<tr>
<td>French</td>
<td>1.26%</td>
</tr>
<tr>
<td>Spanish</td>
<td>0.71%</td>
</tr>
<tr>
<td>Dutch</td>
<td>0.68%</td>
</tr>
<tr>
<td>Turkish</td>
<td>0.59%</td>
</tr>
<tr>
<td>Italian</td>
<td>0.14%</td>
</tr>
<tr>
<td>Hindi</td>
<td>0.11%</td>
</tr>
<tr>
<td>Malay</td>
<td>0.08%</td>
</tr>
<tr>
<td>Japanese</td>
<td>0.04%</td>
</tr>
<tr>
<td>Portuguese</td>
<td>0.02%</td>
</tr>
<tr>
<td>Chinese</td>
<td>0.02%</td>
</tr>
</tbody>
</table>
So far so good...

This is “data”, not “intelligence”

There will be benign domains, unrelated domains, defensive registrations, parked domains... along with anything malicious

What evidence can we find, do we trust it?
## API calls – VirusTotal

![Image of VirusTotal dashboard]

### DETECTION DETAILS RELATIONS COMMUNITY

<table>
<thead>
<tr>
<th>Detection</th>
<th>Details</th>
<th>Relations</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlienVault</td>
<td>Malicious</td>
<td>CyRadar</td>
<td>Malicious</td>
</tr>
<tr>
<td>Emsisoft</td>
<td>Phishing</td>
<td>ESET</td>
<td>Phishing</td>
</tr>
<tr>
<td>Fortinet</td>
<td>Phishing</td>
<td>G-Data</td>
<td>Phishing</td>
</tr>
<tr>
<td>Google Safebrowsing</td>
<td>Phishing</td>
<td>Kaspersky</td>
<td>Phishing</td>
</tr>
<tr>
<td>Netcraft</td>
<td>Malicious</td>
<td>Sophos AV</td>
<td>Malicious</td>
</tr>
<tr>
<td>Spamhaus</td>
<td>Phishing</td>
<td>ADMINUS Labs</td>
<td>Clean</td>
</tr>
<tr>
<td>AegisLab WebGuard</td>
<td>Clean</td>
<td>Antiy-AVL</td>
<td>Clean</td>
</tr>
<tr>
<td>Artists Against 419</td>
<td>Clean</td>
<td>Avira (no cloud)</td>
<td>Clean</td>
</tr>
<tr>
<td>BADWARE.INFO</td>
<td>Clean</td>
<td>Baidu-International</td>
<td>Clean</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Clean</td>
<td>BlockList</td>
<td>Clean</td>
</tr>
</tbody>
</table>
API calls - AlienVaultOTX

CCTC Top Indicators

Indicators of Compromise (66067)    Related Pulses (2215)    Comments (0)    History (0)

<table>
<thead>
<tr>
<th>TYPE</th>
<th>INDICATOR</th>
<th>TITLE</th>
<th>ADDED</th>
<th>ACTIVE</th>
<th>RELATED PULSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>tempatidurpasien.com</td>
<td></td>
<td>Jun 3, 2020, 2:17:16 PM</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://t.co/GppFoYNAN">https://t.co/GppFoYNAN</a></td>
<td></td>
<td>Jun 3, 2020, 2:17:16 PM</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://www.meduchet.com/crm/21381/33051d1a676653c26.71326395/install">http://www.meduchet.com/crm/21381/33051d1a676653c26.71326395/install</a>...</td>
<td></td>
<td>Jun 3, 2020, 2:17:16 PM</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
API calls - phishtank
The site ahead contains malware

Attackers currently on malware.testing.google.test might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

☐ Automatically report details of possible security incidents to Google. Privacy policy

Details

Back to safety
Reporting Data Flow

1. **Input:** zone files, etc.

2. **Filter on keywords** ("COVID", etc.)
   - **Yes**
     - **Lookup in threat intelligence sources** (APIs, blacklists, whitelists, etc.)
       - **APIs**
       - **3rd party threat intelligence**
         - **No**
           - **Stop**
         - **Yes**
           - **Sufficient evidence to continue?**
             - **No**
               - **Stop**
             - **Yes**
               - **Gather other information** (DNS, geolocation, etc.)
                 - **No**
                   - **Stop**
                 - **Yes**
                   - **Submit report to registrar/registry**
                     - **Yes**
                       - **Sufficient evidence to report?**
                         - **No**
                           - **Stop**
                         - **Yes**
                           - Continue process

3. **Stop**
COVID-19 Our output

Roughly an order of magnitude lost at each gate:

- Thousands of registrations per day
- Some reports on hundreds
- Sufficient evidence on tens
Conclusion
Conclusion

Sure, there is bad stuff out there

BUT; it is not anywhere near as bad as some figures would suggest
Initial encounters

• Receiving high numbers of reported domains
• Receiving repetitive notifications
• Majority of domains parked
• Cross Governmental response
  • Healthcare Regulatory Bodies
  • Trading Standards
  • Tax and welfare bodies
Week 11 first full country enters lockdown

Co-vid related Domains registered per Week
source: holdintegrity.com

Series 1

<table>
<thead>
<tr>
<th>Week</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>33</td>
</tr>
<tr>
<td>2</td>
<td>66</td>
</tr>
<tr>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>4</td>
<td>433</td>
</tr>
<tr>
<td>5</td>
<td>1168</td>
</tr>
<tr>
<td>6</td>
<td>668</td>
</tr>
<tr>
<td>7</td>
<td>1335</td>
</tr>
<tr>
<td>8</td>
<td>1495</td>
</tr>
<tr>
<td>9</td>
<td>3158</td>
</tr>
<tr>
<td>10</td>
<td>1098</td>
</tr>
<tr>
<td>11</td>
<td>2324</td>
</tr>
<tr>
<td>12</td>
<td>2068</td>
</tr>
<tr>
<td>13</td>
<td>1658</td>
</tr>
<tr>
<td>14</td>
<td>1164</td>
</tr>
<tr>
<td>15</td>
<td>1688</td>
</tr>
<tr>
<td>16</td>
<td>6214</td>
</tr>
<tr>
<td>17</td>
<td>1238</td>
</tr>
<tr>
<td>18</td>
<td>5293</td>
</tr>
<tr>
<td>19</td>
<td>8085</td>
</tr>
<tr>
<td>20</td>
<td>3187</td>
</tr>
<tr>
<td>21</td>
<td>7681</td>
</tr>
<tr>
<td>22</td>
<td></td>
</tr>
</tbody>
</table>
Activity

- Interaction with ccTLD around enhanced validation
- Information sharing with a number of rr/ry's
- Validating Maliciousness across all identified domains
- Providing evidential packages for suspension
- Over 2000 reports of COVID related scams
Outcomes and Work in Progress

- Provided single point of contact for UK
- Received Co-vid contact points
- No new criminal groups, tools or vulnerabilities
- Educational material to prevent and protect the public
- Need for better information sharing mechanism
- Arrests and disruptions
COVID-19 and Domain Registration
First COVID-19 related domain registered on 2020-01-22

“Oh shit” on 2020-03-15
Realization that this is an *exceptional* circumstance

- Run COVID-19 related keyword search on new registrations (%covid%, %corona%, ...)
- Load daily keyword matches in to Google Sheet
- Review and categorize
- Compliance team investigates potential harm
- Harm: Leaning on DNS Abuse Framework - threats to human safety foremost, more broadly anything our team found concerning
## Manual Review Results

<table>
<thead>
<tr>
<th>Category</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parked/Not Resolving</td>
<td>70.1%</td>
</tr>
<tr>
<td>COVID-19 Info</td>
<td>9.2%</td>
</tr>
<tr>
<td>Store/Shop</td>
<td>6.7%</td>
</tr>
<tr>
<td>Other</td>
<td>6.3%</td>
</tr>
<tr>
<td>PPE/ Virus Supplies</td>
<td>5.0%</td>
</tr>
<tr>
<td>Unrelated to COVID-19</td>
<td>1.3%</td>
</tr>
<tr>
<td>Exemplary Good</td>
<td>0.9%</td>
</tr>
<tr>
<td>Potentially Harmful</td>
<td>0.5%</td>
</tr>
</tbody>
</table>
The Good

- https://spreadartnotviruses.com/ - COVID-19 Art Project
- https://covidsurvey.ca/ - York University Study
The Bad

- Personal information gathering
- Anonymous exposure notification
- Fake tests & fake cures
  - Unclear boundaries: vitamin C
- Questionable products
  - COVID-19 resistant tents
  - PPE opportunists

- No examples of coordinated mis- or dis-information
Resellers

- Worked with larger resellers to share information
- Resellers have more tools and customer relationships to leverage
- Some implemented blanket bans on COVID-19 related terms
The Difficulty of Manual Review

- DNS Abuse was well covered

- Content abuse is difficult because:
  - Requires tooling Registrars don’t necessarily have
  - Content changes constantly
  - Lack of authorities available to review potential harm
  - Harm is difficult to identify in practice
  - Totally outside the realm of our expertise and purview
Thank you

gbunton@tucows.com

tucows.com
Afilias Anti-Abuse

vs

COVID-19

James M. Galvin, Ph.D.
Afilias, Inc.
Weekly COVID Related Registrations: Afilias TLDs

Based on 4,792 registrations with COVID-related names registered across 25 Afilias TLDs
COVID Names Peak at 13 Characters

Based on 4,792 registrations with COVID-related names registered across 25 Afilias TLDs
Based on 4,792 registrations with COVID-related names registered across 25 Afilias TLDs

“COVID” AND “VIRUS” Are Best Descriptors

Of all registered names, 40% include the term “COVID”
Only 27 include descriptor “WUHAN”

Names including a dash and multiple terms

- Virus 26%
- Coronavirus 16%
- COVID 40%
- “_” 15%
- Pandemic 3%

Based on 4,792 registrations with COVID-related names registered across 25 Afilias TLDs
Based on 4,792 registrations with COVID-related names registered across 25 Afilias TLDs

**COVID Registrants Bought Single Names**

- **Most were “privacy” services**: 20+ names purchased - 33%
- **6-20 names purchased**: 8%
- **2-5 names purchased**: 19%
- **1 name purchased**: 40%

- **40% of names** were bought by registrants who purchased **1 name**
- **Over 80% of registrants** bought only **1 name**
COVID Domains

Brian Cimbolic, General Counsel, PIR
Monitoring Begins

- Early March, spike in registrations related to COVID became clear.
- Concern regarding abuse/phishing related to these names.
- Also concerned regarding things like fake "cures" and "vaccines."
- Began screening certain keywords in registration.
- Act on limited instances of domains pursuant to our Anti-Abuse Policy. Informed by:
  - Framework to Address Abuse
  - Anti-Abuse Principles
14.7k ORG COVID-related DOMAIN names

Daily New Registrations

Cumulative New Registrations

Public Interest Registry
Cumulative and daily Daily and Cumulative New Registrations

Public Interest Registry
.ORG ABUSE MONITORING

PIR monitors the entire zone for evidence of abuse.

Targeting false treatments and vaccines, PIR looks for domains with e-Commerce platforms.

Using the content on the crawled page, the homepage text is reviewed for covid-19 related terms.

The create date helps us further narrow the zone.
Covid-19 Domain Abuse Tracker
Potentially abusive COVID-19 Names identified and Investigated - Total: 21

Abuse - COVID 2020

- March 2020: 11
- April 2020: 6
- May 2020: 4

COVID-19 Action

- Registrar Actioned – Registrar actioned the domain name by Suspending, Parking the Site or Deleting the domain name
- PIR No Action – Domain Investigated and found to be Legitimate – No Further action taken by PIR

Public Interest Registry
Registration Trends

Monthly New Creates

Common Keywords

Totals by Month

Public Interest Registry
Trends Observed

• Keywords: corona, korona, covid, kovid, virus, pandemic.
  • Small number of n95, ventilator included in grand total

• Additional terms have about 50-200 domains related to them.
  • Flatten the curve and social distancing, PPE, test kits, stimulus, Fauci, Cuomo

• Some of the domains ultimately flagged for abuse did not have any direct keywords whatsoever:
  • 6 of the 21 do not have COVID Related domain names (ex. give4cdcf.org, gatesfonudation[.]org)