Criminal Use of Domain Names

Greg Aaron, Illumintel
Colin Strutt, Interisle Consulting Group
Maliciously Registered Domain Names

• Domain names registered to perpetrate cybercrime.

• Scope of the problem?
  • 197,876,195 gTLD domain names in zone files.
  • Over the course of a year, about 6 million gTLD domains appear on major blocklists. And that 3% is the floor.

• Harms: cybercrime impacts reliability and trust on the Internet. More specifically, it has very human costs: theft of money and personal information.

• “harm” vs. “crime” vs. “abuse”

• Here’s an example of what you can do with data…
Study:
“Criminal Abuse of Domain Names: Bulk Registration and Contact Information Access”

by Dave Piscitello and Dr. Colin Strutt
Interisle Consulting Group

http://interisle.net/criminaldomainabuse.html
Hypothesis

• Cybercriminals take advantage of *bulk registration services* to “weaponize” large numbers of domains for their attacks.

• Bad domains get recognized and blocked

• Some criminals need to rapidly, cheaply, and repeatedly acquire domain names
Methodology

• Assembled composite **blocklist and reputation data** from a variety of threat intelligence and reputation lists.
  • Including APWG, SURBL, Spamhaus, Abuse.CH
  • Indicate a variety of criminal activities, including malware, phishing, spamming
• Found where thousands of such domains were blocklisted in short time frames. Selected batches in five TLDs.
• Documented when those domains were registered, and at what registrars. This required **domain registration data (WHOIS)**.
• Studied the registrars with these high concentrations of blocklisted domains. Did they offer domains cheaply and in bulk?
• Studied the behaviors of the registrants who made those bulk registrations.
Example:
Blocklisted domains in .TOKYO

- Blocklisted in .TOKYO from December 12-25, 2018 = 8,715 blocklisted domain names

<table>
<thead>
<tr>
<th>Registrar</th>
<th>IANA ID</th>
<th>Abuse Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMO Internet, Inc. d/b/a Onamae.com</td>
<td>49</td>
<td>8,713 (100%)</td>
</tr>
<tr>
<td>NameCheap, Inc.</td>
<td>1068</td>
<td>2 (0%)</td>
</tr>
</tbody>
</table>

Nearly all of these were registered using a single registrar.
Blocklistings corresponded with spike in registrations

Above: # of domains in .TOKYO registry. Source: ntldstats.com

The blocklisted domains represented 7% of the domains in the TLD
Most of the blocklistings occurred on Dec 17, 2018
Why this registrar, GMO?
- Very cheap domain registrations
- Offers tools to register in volume
- Customers can generate random domain strings

1 ¥ = €0.0083

Web site will create random names

Customers can upload a file of names
Finding Criminal Actors and Assets: Search

• SEARCH historical WHOIS records for registrant Name, registrant Street Address, registrant Email address.

• Suspect provided a registrant address in Japan

• Also registered domains in .INFO, .CLUB, .ONLINE, .XYZ, .BIZ, .SPACE, and .WORK

• Assume that criminals submit inaccurate/fraudulent contact data

• Only some WHOIS records contain contact data (post-GDPR)

• PIVOT to other databases or social media to identify related records and the criminal actors.
Finding Criminal Actors and Assets: Pivot

- Triangulate against additional data sources: IP address data, passive DNS records (nameservers), malware data, spamples, etc. Each is a different specialty.
- Suspect hosted phishing sites and malware, at three hosting providers: InterQ GMO Internet, Inc.; IDC Frontier, Inc.; Sakura Internet, Inc.
- Heatmap of phishing and malware activity at INTERQ GMO, AS 7506:

![Heatmap Image]

- Examining what’s on that hosting often leads to yet more domains, additional bogus pseudonyms, etc.
General Findings

• Study confirms the hypothesis that cybercriminals take advantage of bulk registration services to use large numbers of domains for their attacks

• The findings corroborate those of others (2017 ICANN report *Statistical Analysis of DNS Abuse in gTLDs (SADAG)*)

• [Disparate data sources are necessary.]

• [This is where you can stop play whack-a-mole and where you can make a difference with one intervention.]
Recommendations

- The report offers nine recommendations.
- Some could become binding policy through ICANN.
- Others could be implemented by registrars and registry operators themselves.
- Others are requests to make better data available.
- [http://interisle.net/criminaldomainabuse.html](http://interisle.net/criminaldomainabuse.html)