FS-ISAC

High Risk Domains with a **COVID-19** and Financial Theme

High Risk Domains with a COVID-19 and Financial Theme

16 April 2020

Scope and Purpose

As part of its continued monitoring efforts on threats related to COVID-19, FS-ISAC reviewed the DomainTools' curated list of high-risk domains, using a COVID-19 theme, to determine the risk to the sector.[1] Fraudsters and cybercriminals are using these domains to take advantage of the COVID-19 crisis for financial fraud, scams, and potentially malicious activity with a financial-themed lure. FS-ISAC analyzed the resulting dataset. This document details the identified trends and conclusions.

Analysis

Keywords

As of early April 2020, over 1500 domains were identified during this research: created on or after 1 January 2020, with a high-risk score (calculated by DomainTools) and containing both a COVID-19 **and** financial theme. According to domain name keyword analysis, the biggest category by far is **Loans** with 44% of domain names containing keywords such as Loan, Financing, Credit. This is likely malicious actors and scammers attempting to lure people in financial need caused or worsened by the COVID-19 crisis.

A related theme, financial support (keywords: Help, Aid, Support) was observed in 5% of the domain names. This is also likely an attempt to prey on the financial needs of people, but we are not sure the nature of what was "offered" to those visiting the site.

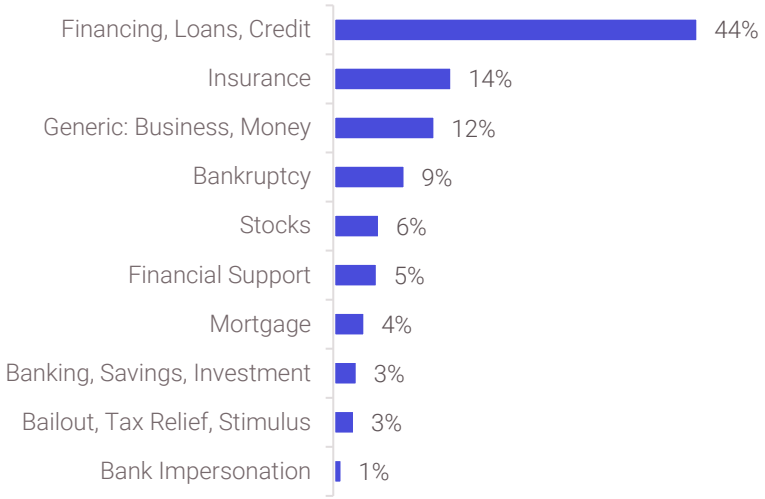

Figure 1: Financial Theme by Keywords, COVID-19 High-Risk Domains

Of note, 3% of the domains in the dataset contained keywords related to **government bailouts, stimulus and tax relief plans**; however, it is important to remember that the researched dataset contained only domains that have financial services related keywords in their name to begin with. It is quite likely that government aid-related scam domains were created in far greater numbers, but they are outside the scope of this research because they contained no other financially themed keywords. Considering the stimulus packages being made available in various countries to both individuals and businesses, members should be aware of the potential for fraud.

Bank Impersonation domains were rare in the dataset and account for 1%. This can be attributed to a number of factors:

- No specific bank names were included in the search (although, terms such as 'Banking', 'eBanking', and a sub search for 'online' were in the search, which should capture a significant portion of online banking impersonation domains).
- FS-ISAC is aware of members proactively registering domains with their institution's name and COVID-19 (and other high-profile events that are likely to attract scammers) before scammers can get to them. If FIs are willing to make the investment, this can possibly prevent scammers from using the firm's name in fraud.

[1] https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats

- Domain name registrars are highly aware of banking impersonation attempts regardless of the COVID-19 crisis, but these types of domain names can still be generated. FS-ISAC members actively report on these types of imitation sites.

Top Level Domain

The most common Top Level Domain (TLD), unsurprisingly is *.com which accounts for 71% of the total domains. This is followed by *.org (7%), *.co.uk (5%), *.net (4%), and *.info (3%), but the total list of TLD in this dataset of high-risk domains is quite varied with 47 types including the financially-themed *.money, *.loans, *.capital, each accounting for less than 1%.

Country

Going by the geographic location of the main IP address the domain names point to, 80% of the domains are hosted in the United States; 3% in Germany; 2% in the United Kingdom. A significantly smaller number of domains point to Australia, Canada, Europe (including Eastern Europe), Asia, South America, and the Caribbean.

Takedowns

Between the initial data pull on 6 April and a week later on 13 April, 92% of the identified high-risk domains in our research containing a COVID-19 and financial theme no longer exist. This is likely due to decisive action taken by domain name registrars, manually reviewing domain names that contain COVID-19 relevant keywords and working with authorities to take down fraudulent or abusive domains. Over 75% of the domains identified during this research were registered on GoDaddy (63%), Google (9%), and Namecheap (4%) who have declared taking action[2].

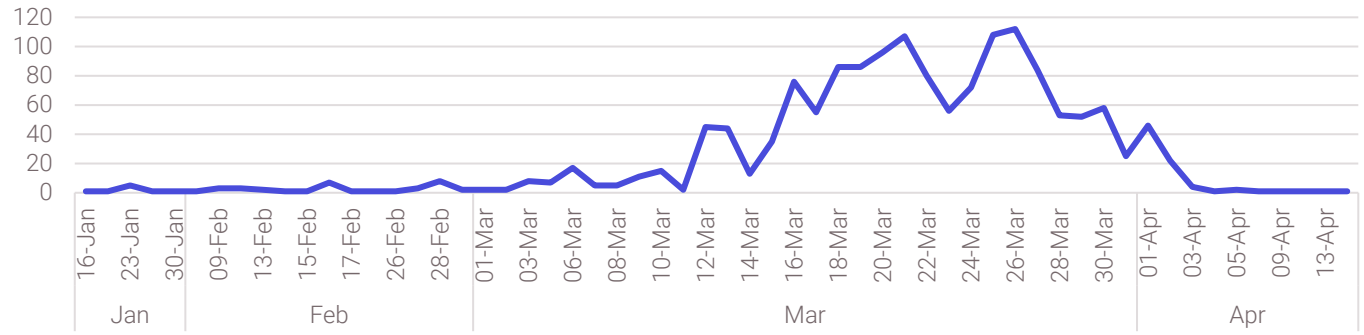

Figure 2: Creation of High-Risk Domains with a COVID-19 and Financial Theme

Figure 2 shows the creation rate of domains included in the research. At its peak in mid- to late March, as the magnitude of the global crisis was realized, scammers and fraudsters were quick to react by setting up an average of 66 financially themed COVID-19 high risk domains per day. However, as domain name registrars ceased to automatically approve COVID-19 themed domain names and cracked down on suspicious and high-risk entries, the creation rate plummeted and today it is practically non-existent.

According to our research, from over 1500 high-risk COVID-19 and financially-themed domain names registered during the peak roughly 200 still exist today, with an average age of 28 days. This is a total decrease of 87%, and takedown efforts and legal action are sure to continue.

[2] https://www.infosecurity-magazine.com/news/domain-registrars-combat-covid-19/