FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 OCT 2020

Alert Number

CP-000135-DM

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This product was coordinated with DHS' Office of Intelligence & Analysis, DHS-CISA, the Department of Commerce, and Census Bureau. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP:WHITE** Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Unattributed Entities Register Domains Spoofing the US Census Bureau's Websites, Likely for Malicious Use

Summary

The FBI has observed entities not associated with the US Census Bureau registering numerous domains spoofing the Bureau's websites, likely for malicious purposes. These suspicious spoofed domains are easily mistaken for legitimate Census Bureau websites and can be used for advertising, credential harvesting, and other malicious purposes. Spoofed domains (aka typosquatting) mimic legitimate domains by either altering character(s) within the domain or associating another domain with similar characteristics to the legitimate domain, such as "Censusburea[.]com" or "census-gov[.]us" Spoofed domains are increasingly used by cyber criminal and state-sponsored groups to propagate the spread of malware, which can lead to further compromise and financial losses. This activity poses a risk to both the US Census Bureau and the public.

Threat Summary

The Census Bureau continually collects and provides data about the people and economy of the US. This creates opportunities for cyber actors to attempt to exploit respondents and users of the data for financial gain and other nefarious purposes. Cyber actors can use spoofed domains similar to Census Bureau websites to target businesses and the public. In the past, cyber actors have used spoofed domains to gather valid usernames, passwords, and email addresses;

collect personally identifiable information; and spread malware, leading to further compromises and potential financial losses.

As part of the US government's facilities sector, the Census Bureau remains a target for both criminal and nation-state actors aiming to negatively affect the US Government and create distrust among US citizens. In order to prevent website confusion for site visitors, the Census Bureau is actively working to disable spoofed domains.

Recommended Mitigations

- Users should pay close attention to the spelling of web addresses, or websites that look trustworthy but may be close imitations of legitimate Census Bureau websites.
- Devise a continuity of operations plan for a potential cyber attack; prioritize the systems most important to continued operations.
- Ensure the SSL (Secure Sockets Layer) certificate is present, and the top-level domain is ".gov" for the website.
- Regularly patch operating systems, software, and firmware.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Use multi-factor authentication where possible.
- Audit networks and systems for unauthorized remote communication.
- Disable or remove unneeded software, protocols, macros, and portals.

Appendix A: Registered Domains

The following 63 domains are not registered to the Census Bureau but are similar to legitimate Census Bureau websites.

Suspicious Domains		
Arrecensust[.]cf	gf.ensus[.]org	uscensus[.]net
bendus.ensus[.]org	lists.us-census[.]org	us-census[.]net
Cacensusfactsheets[.]online	mycensus[.]io	us-census[.]org
californiac.ensus[.]org	njcensus[.]com	uscensus[.]us
Censusarchive[.]com	nycensus[.]com	uscensusbureau[.]co
Censusburea[.]com	ocensus[.]cn	us-census-bureau[.]co
census-bureau[.]com	onlinecensusform[.]com	us-census-bureau[.]com
census-bureau[.]us	online-census-form[.]com	uscensusbureau[.]net
Censusbureaudata[.]com	onlinecensusform[.]net	us-census-bureau[.]net
census-bureau-gov[.]us	online-census-form[.]net	uscensusbureau[.]org
Censuscareers[.]com	onlinecensussurvey[.]com	us-census-bureau[.]org
census-careers[.]com	online-census-survey[.]com	uscensusbureau[.]us
census-gov[.]us	onlinecensussurvey[.]net	us-census-bureau[.]us
census-info[.]us	online-census-survey[.]net	uscensusbureau-gov[.]us
census-jobs[.]com	rnicensus[.]com	us-census-bureau-gov[.]us
Censusnj[.]org	server.censusarchive[.]com	uscensuscareers[.]com
Censusofsurvey[.]com	startcensusonline[.]com	us-census-careers[.]com
Censusonline[.]us	start-census-online[.]com	uscensus-gov[.]us
censuspeer[.]cf	startcensusonline[.]net	us-census-jobs[.]com

censuspell[.]ml	start-census-online[.]net	usgennet.us-census[.]org
censusprint[.]com	store.2016census[.]com	web01.censusonline[.]us
census-records[.]us	test.census-info[.]us	www.censusonline[.]us
census-work[.]com	the-census[.]com	www.census-online[.]us
covidcensus[.]com	uc.ensus[.]org	www.ensus[.]org
ensus[.]org	uchs.ensus[.]org	www.u.s.censusburea[.]com
ftp.2016census[.]com	uscensus[.]co	wwwmyaccountascensus[.]com
ftp.2016census[.]org	us-census[.]co	wwwmycensus[.]com
arrecensust[.]cf	gf.ensus[.]org	uscensus[.]net
bendus.ensus[.]org	lists.us-census[.]org	us-census[.]net
cacensusfactsheets[.]online	mycensus[.]io	us-census[.]org
californiac.ensus[.]org	njcensus[.]com	uscensus[.]us
censusarchive[.]com	nycensus[.]com	uscensusbureau[.]co
censusburea[.]com	ocensus[.]cn	us-census-bureau[.]co
census-bureau[.]com	onlinecensusform[.]com	us-census-bureau[.]com
census-bureau[.]us	online-census-form[.]com	uscensusbureau[.]net
censusbureaudata[.]com	onlinecensusform[.]net	us-census-bureau[.]net
census-bureau-gov[.]us	online-census-form[.]net	uscensusbureau[.]org

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity,

number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only.