Department of Commerce
RE: E.O. 13984: ANPRM

October 25, 2021

INTRODUCTION

APWG is a US-based international coalition of counter-cybercrime responders, forensic investigators, law enforcement agencies, technology companies, financial services firms, university researchers, NGOs and multilateral treaty organizations operating under as a 501(c)6 organization. Its directors, managers and research fellows advise national and sub-national governments as well as the United Nations (Office on Drugs and Crime) as recognized experts (as defined by the Doha Declaration of 2010 and Salvador Declaration of 2015) as well as multilateral organizations such as the European Commission, the G8 High Technology Crime Subgroup, Council of Europe's Convention on Cybercrime, Organization for Security and Cooperation in Europe, Europol and the Organization of American States. APWG is a founding member of the steering group of the Commonwealth Cybercrime Initiative at the Commonwealth of Nations.

Since 2004, APWG has operated clearinghouses of machine event data and Internet event data for industry, government regulatory agencies and multilateral treaty organizations to assist those enterprises in their workaday charges to prevent, suppress and investigate cybercrime as well as to help them forge relevant policies for the management of predictable, common cybercrimes. The APWG's eCrime eXchange (eCX) clears more than one billion data elements each month between its members, which includes a number of United States government agencies as data contributors as well as consumers. The joint US-CERT / APWG Phish Mail forwarding service <us-cert.cisa.gov/report-phishing> has been in operation for around a decade. The APWG and IRS established a database of telephone numbers used to abuse the IRS brand around a decade ago that has become a mainstay resource of the eCX for archiving telephone and fax numbers employed in cybercrimes reported to the APWG. It is a matter of record that APWG's first general meeting as an independent NGO was hosted by the United States Secret Service in October 2004 at the agency's headquarters in Washington, DC.

We welcome the opportunity to respond to the Department of Commerce's ANPRM concerning "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."

Commentary: Use of Domain Names for Phishing

The domain name registration infrastructure that all Web developers and maintainers are required to use for establishing and maintaining domain names that define a brand space or a trading platform on the World Wide Web has long been employed as a criminal instrument for deceiving users of email, web browsers and instant messaging applications into believing they are communicating with trusted enterprises (e.g. < **Campbellsouq.com**>) in order provoke disclosure of personnel or enterprise information – or to induce trust to convince a correspondent to act on behalf of the deceiver.

In its Q2 2021 Phishing Trends Report, APWG member RiskIQ analyzed 2,447 confirmed phishing URLs reported to the APWG in Q2 2021. RiskIQ found that they were hosted on 1,327 unique second-level domains (and 60 were hosted on unique IP addresses, without domains).

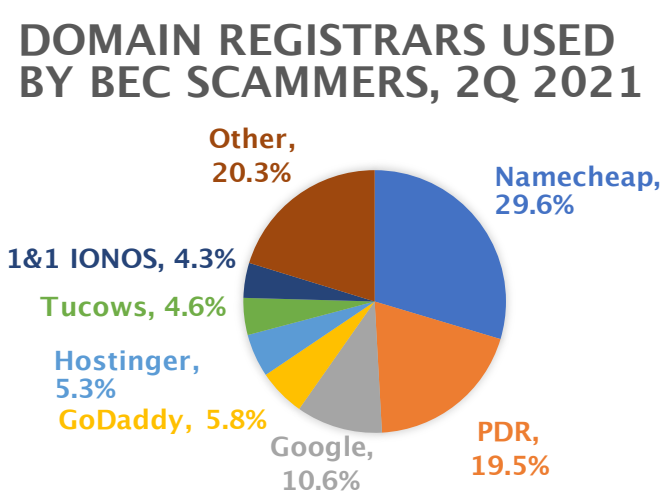
The TLDs that had the most unique second-level domains used for phishing were:

u	TLD	Category	# of Unique Domains in Sample Set (1Q 2021)
1	.COM	gTLD	767
2	.XYZ	nTLD	42
3	.UK	ccTLD	41
4	.NET	gTLD	40
5	.ME	ccTLD	34
6	.ORG	gTLD	34
7	.TK	ccTLD	30
8	.ML	ccTLD	23
8	.AU	ccTLD	19
10	.CF	ccTLD	19

In that same Q2 2021 report, APWG member Agari by HelpSystems found that domain name registrars Namecheap and Public Domain Registry (PDR) continue be the primary registrars used by cybercriminals to register the domain names that they use in Business Email Compromise (BEC) attacks that are designed to deceive key personnel

within enterprises to steal high-value corporate data or compel financial transactions by authorized personnel. (Some 39 percent of the total were registered at NameCheap, and 26 percent were registered at PDR.) Since Q4 2020, these two registrars have represented a majority of maliciously registered domains.

It has been clear for decades to professionals investigating and managing cybercrime that current curation practices by the industries that maintain the Domain Name System are easily and routinely defeated by criminal gangs that employ deceptive domain names to animate their cybercrimes.



Typically, cybercrime perpetrators preparing infrastructure to animate their crimes can register any number of domain names for those enterprises – hundreds or thousands at a time – with little if any intervention from the industries charged with curation of the DNS.

APWG research correspondent Interisle Consulting Group reported in September that their analysis of thousands of phishing events involving domain names registration showed that "during the yearly study period, 57% of domains reported for phishing were used within 14 days following registration and that the majority of these were reported within 48 hours. 84% of domain names associated with a phishing attack were reported within the first year of registration."[1]

These findings confirmed, yet again, that the programmatic abuse of the DNS had long been a standard operating procedure for cybergangs structuring and executing the most common and predictable cybercrimes like phishing that menace citizens with most every access of ICT.

[1] Phishing Landscape 2021: An Annual Study of the Scope and Distribution of Phishing, Interisle Consulting Group
LLC, https://interisle.net/PhishingLandscape2021.pdf

Policy Recommendations

Therefore, APWG's directors are moved to make the following recommendations regarding the rule-making discussion at hand:

U.S. domain name service providers should be classified as U.S. Infrastrucure-as-a-Service providers for purposes of this rulemaking. The establishment, maintenance and resolution of second-level domain names on the Domain Name System (DNS) contains operational elements of both land registries and the signaling systems of the public switched telephone network (PSTN). Functionally, the DNS is a globally distributed network of servers that represents a network number on the Internet to human beings in human-readable text (e.g. http:// https://apnews.com) for which there is no readily accessible substitute or competitive alternative. As such, the service providers who curate the DNS can be reasonably classified as infrastructure. Still. APWG directors stress that such a definition should be accompanied by precise and clear definitions for "U.S. domain name service providers" and "All U.S. domain name registries" so as to not over regulate and to ensure miscreants are covered by the regulations.

U.S. domain name registries should be required to maintain complete and accurate databases of the identity and contact information of all registrants for the domain names that such registries administer. A great deal of power of the WHOIS data that are archived with the registration of a new second-level domain name is in its utility for *preventing* cybercrime. APWG's members cited the loss of WHOIS data after ICANN's issuance of its Temporary Specification (in response to the GDPR) as a broadly damaging loss for preventative routines that allowed investigators and responders to key in on telling data elements in WHOIS to knock down cybercrime events before they happen. Accurate data would assist those stalwart, dogged interveners — and its requirement would dissuade miscreants from abusing the domain name system.

APWG directors thank you for the opportunity to comment on the ANPRM.

Sincerely,

Peter Cassidy, on behalf of
The Anti-Phishing Working Group (APWG)
Cambridge, MA USA