FINDINGS

World SSR Threat

Since its founding, ICANN has had a remit to help ensure the security, stability and resiliency of the Internet's unique identifier systems. While there's a strong record of ICANN's policies and actions supporting competition and growth in the domain space, ICANN's record on supporting impactful security, stability and resiliency measures is extremely limited – to the detriment of public safety.

Societies worldwide are increasingly at risk of attacks against critical infrastructures, malicious political interference, and a range of cybercrimes capitalizing on ICANN's failure to fulfill responsibilities relating to DNS security, stability and resiliency. Damages associated with cybercrime globally are projected to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015[cite]. The *2019 Official Annual Cybercrime Report* notes that "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined."[1]

We've seen a significant upward trend in multiple DNS attack vectors that capitalize on lax or non-existent domain name security measures, especially since the first SSR Review Team report was adopted by the Board in 2012 .

- Malware - from 2016 to 2018 the number of unique URLs recognized as malicious by antivirus software more than doubled to 554,159,6213 [cite], and mobile malware attacks nearly doubled from 2017 to 2018 to over 116 million [cite].
- Digital Certificate fraud - APWG reports that phishers are increasingly using digital certificates to make attacks look legitimate and to defeat browser fraud detection warnings. [add stats]
- Phishing - APWG reported that phishers are registering domain names directly to perpetrate fraud. [Phishing trend stats to be added]
- Business Email Compromise - The US FBI Internet Crime Center reported a 136% increase in identified global exposed losses from 2016 to 2018 resulting from Business Email Compromise, affecting all 50 United States and 150 countries worldwide. From October 2013 to May 2018, the FBI documented a multi-billion-dollar growth in BEC, which often involves fraudulent registration of domain names that are deceptively similar to one of the targeted parties [cite]
- Scams - the Australian Competition and Consumer Commission (ACCC) ScamWatch reported a near doubling in losses from scams in roughly the last three years, rising to AU$11.8 million in losses in 2019. Domain names used to perpetrate online scams very typically infringe on brand or business name. These names are registered by the scammer with little or no controls over the volumes of similar names the scammer can register and limited access to information that investigators can use to identify the criminal actors.
- Botnets -- In 2017, Spamhaus DBL listed 50,000 botnet controller domain names registered and set up by cybercriminals for the sole purpose of hosting a botnet controller. More than 25% of these registered botnet domain names have been registered through a single registrar, Namecheap[cite]. In 2018, Spamhaus listed 103,503 botnet controller domain names, a 106% increase. Namecheap remained the most abused registrar, with a 220% increase in registered botnet controller domain names[cite].
- Spam, [stats to be added]
- DDOS attacks [stats to be added]