Cybercrime After the Sunrise: are the new gTLDs nests of abuse? - a customer success story

WhoisXML API, Inc.

ICANN's new gTLD program, initiated in 2007 and started in 2013, resulted in the appearance of more than a thousand generic top-level domains, confirming the significant business demand for these. Some are related to regions or locations (like .amsterdam), some to communities (e.g. .pharmacy) or brands, and many of them are just words having a marketing value. But apart from the opportunities for customers, unfortunately they also pave new ways for cybercriminals for abusing the domain name system. Even though ICANN has built safeguards into the process to mitigate this risk, it has become a widely accepted surmise that new gTLDs are frequently the base camps of spamming, phishing, botnets and other forms of abuse. Is it really the case?

In a recent conference paper, which was presented at the ACM Asia Conference on Computer and Communications Security (AsiaCCS 2018) in Korea, M. Korczynski and his co-workers have investigated this question comprehensively for the first time. They define and investigate measurable security metrics. Their main research question is : "how do abuse rates in the new gTLDs compare to legacy gTLDs, since the implementation of the new gTLD program?" They evaluate the abuse rates on the basis of diverse data sources including spam and phishing blacklist feeds, DNS zone files, active DNS and web scans and WHOIS data, the latter obtained from WhoisXML API, Inc. The study covers a period between 2014 and 2016.

After the initial delegation of a top-level domain, there is a "sunrise" period of at least 30 days during which trademark holders have privileges to register their domains. Apart from certain restricted TLDs (like those controlled by a community), the generic ones become open for the public. Managed by various registrars, the policies and practices of the domain name registration vary. ICANN prescribes 9 safeguards the operators have to maintain. For instance, the fifth safeguard is that operators have to create and maintain "Thick WHOIS" records, i.e. complete WHOIS information from all the registrars on all domains corresponding to a given new gTLD. The the mentioned paper focuses on the generic new TLDs open for registration (i.e. "after the sunrise"), and employs elaborate statistical tools to answer its main research question, thereby also assessing the efficiency of the current safeguards.

With respect to phishing domains it is observed that while the number of abused domains remains relatively constant in legacy gTLDs a clear upward trend in the absolute number of phishing domains in new ones. Phishing attackers often succeed in maliciously registering strings containing trademarked words. The study finds that "Manual analysis of maliciously registered domains in the fourth quarter of 2015 revealed 88 abused .top domains 75 out of which contain the words: Apple, iCloud, iPhone, their combinations, or misspelled variants of these strings suggesting that they may have been all used in the same phishing campaign against users of Apple Inc. products".

From the registration rates it can be concluded that miscreants more frequently choose to

maliciously register domain names using one of the new gTLDs. Apart from phishing, similar trend can be observed with respect to domains compromised by malware. Spam rates show an even more dramatic behavior: they are found to be an order of magnitude higher for new gTLDs than to legacy ones.

The number of parked (registered but not used) domains is typically considered as relevant: that the more parked domains in a new gTLD, the more abused domains. This can be expected since the landing pages of parked domains can serve malware. Interestingly the statistical analysis confirms the existence of this effect but also shows that it is not very strong. The use of DNSSEC has been considered as an important element of the current ICANN safeguards, albeit it clearly does not prevent abuse. Indeed, it is found that there is a weak positive correlation between the number of malicious and DNSSEC-signed domains: attackers are probably interested in deploying DNSSEC and signing their maliciously registered domains.

The use of Privacy and Proxy services to hide the identity of the registrant is often considered as a potential indicator of malicious activity. In spite of that the present study finds that the use of such a service is not, in itself, a reliable indicator of malicious activity. In fact these services are more frequently used in legacy gTLDs than the new ones in the studied period.

It is interesting that registry operators appear not to have a significant impact on abuse count, the compromised domains are evenly distributed amongst registries. Assessing the reputation of the accredited registrars, on the other hand, is a very fruitful approach. Counting the number of abused domains per registrar shows that some registrars are really highly affected. As an example, the study reveals a large concentration of blacklisted domains associated with "Nanjing Imperiosus Technology" in early 2016. ICANN terminated the accreditation of this registrar in this case in early 2017. Yet certain other registrars with the same observed behavior are still active today.

The main conclusion of the paper is that the implementation of the 9 safeguards currently in action has proven to be insufficient to maintain the security of new gTLDs: the malicious activity in these domains is increasing. From amongst the reasons, the regression and descriptive analysis presented in the paper suggests that "unrestrictive registration practices, low registration pricing, and the possibility of bulk domain name registration lower barriers to abuse". The more stringent penalization of high abuse rate at registries or registrars could also lead to an improved self-regulation.

The work of Korczynski et al. has a significant impact: their results are now at ICANN, contributing significantly to the revision of the safeguards before the next new gTLD rollout.