COMMENT OF THE INTELLECTUAL PROPERTY CONSTITUENCY ON THE DRAFT FRAMEWORK FOR THE REGISTRY OPERATOR TO RESPOND TO SECURITY THREATS

July 31, 2017

The GNSO Intellectual Property Constituency (IPC) appreciates this opportunity to comment on the Draft Framework for the Registry Operator to Respond to Security Threats ("Framework"). The IPC appreciates the work of the Security Framework Drafting Team ("SFDT") in creating a thoughtful and comprehensive non-binding framework, addressing Registries' responses to notifications of security threats.

The IPC wishes to take this opportunity to draw attention to the significant overlap between online intellectual property infringement and security threats such as malware and phishing, which is supported by existing data and experience. There are several recent studies which highlight this overlap, noting that cybercriminals use well-known brands and popular copyrighted content, without authorization, in order to attract users, propagate malware and carry out cybercrime activities. In particular:

- A July 2016 study by the European Intellectual Property Office (EU IPO) finds that a number of business models supporting cybercriminal activity such as phishing make use of well-known brands in the email address and/or body of an email in order to deceive recipients into believing that the email comes from an authentic source. Another method uses a website spoofed to look like a legitimate site, in order to deceive users to disclose bank accounts and other personal data.[1]

- A recent example of this activity, demonstrating its applicability to the domain name space, involves Microsoft's enforcement efforts against the notorious hacking entity known as Fancy Bear, which had made illegitimate, infringing use of Microsoft's brands to carry out their security threats. Microsoft was recently successful in seizing control of hundreds of domain names referencing their brands, in order to disrupt Fancy Bear's cybercriminal network.[2] This strategy, highlighting the important link between security

[1] https://euipo.europa.eu/ohimportal/en/web/observatory/news/-/action/view/3078465

[2] https://www.documentcloud.org/documents/3898760-Gov-Uscourts-Vaed-348662-55-3.html

threats and cybersquatting, is not new. Microsoft has previously launched similar actions to take control of domains used in the propagation of Zeus and Ruckstock botnets.[3]

- In November 2016, Fairwinds Partners published details of their analysis of typosquatting activity, which identified a link between typo domains owned by squatters and malware. The study focused on the top 50 brands (excluding those whose names were based on descriptive terms, or which weren't associated with houses of brands) with names comprising 6 characters or more. The study found that amongst typo domains owned by squatters infringing these brands, 39% of them contained malware, phishing and ransomware and/or involved affiliate fraud.[4]

- A study by RiskIQ and the Digital Citizens Alliance also found that amongst a sample of 800 sites dedicated to distributing infringing movies and TV shows, one out of every three contained malware.[5] As such, consumers are 28 more times likely to get malware from visiting a content theft site than visiting a licensed provider. Merely visiting such sites may place a consumer at risk, since malware is often delivered via "drive-by downloads", invisibly downloading malware to a user's computer without the user clicking on any link. The majority of malware from these sites took the form of Trojans to spy on the consumer's computer, or adware to co-opt the consumer's computer into advertising fraud schemes.

- One subset of data that is important to note is the ratio of domains which are registered initially for purposes linked to security threats, versus those that are compromised following their registration. For example, a recent report by the Anti-Phishing Working Group (APWG) noted that the overall ratio between domains that were registered for phishing purposes and those that were compromised by phishers is about 49% to 51%.[6] However, the APWG's analysis revealed that certain registrars had a rate which far exceeded that, indicating a high volume of malicious registrations. It is important to understand the factors contributing to that, and how better policies and practices amongst registrars can reduce the number of malicious registrations, and thus reduce security threats as well.

This important data demonstrates the need to better understand how security threats are propagated via various types of abusive activity (as that term is used in registries and registrars' contractual obligations to ICANN), including intellectual property infringement. More data would be helpful , as well as a recognition that addressing intellectual property infringement, as a species of abuse, is an integral part of carrying out ICANN's mission to ensure the stable and secure operation of the DNS.

In order to track and understand the various threats, IPC suggests that registries should begin collecting and sharing data, which can form the basis of future research and threat-mitigation

[3] https://arstechnica.com/business/2012/03/microsoft-uses-racketeering-law-to-seize-servers-take-down-botnets/

[4] http://www.fairwindspartners.com/resources-2/reports/cybermonday2016

[5] https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf

[6] http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2H_2014.pdf

procedures. Establishment of a cross-registry security threat depository system where reported data will be shared and accessed by approved members such as law enforcement authorities, registries, cybersecurity firms, private investigators, brandowner representatives, etc. would be beneficial to contracted parties, consumers and as others having an interest in abuse mitigation and ensuring the stable and secure operation of the DNS. This data should not only include security threat data but also data about other abuse complaints.

Leading on from that, the IPC also wishes to note that the Framework may serve as a useful template to help promote transparency and effectiveness in registrars' and registries' responses to other types of abuse complaints. We anticipate that many of the points addressed in the Framework would be applicable to responses to IP-related abuse, including suggested actions which could be taken in response to an abuse complaint.

Respectfully Submitted,

Intellectual Property Constituency