08.10.2019

NOMINET

.UK Policy Consultation 2019

Introduction

The founding principles of the internet – freedom and open access to information for all – have made it a powerful force for growth and innovation in our society and economy.

However, this openness is also vulnerable to abuse. There are many troubling examples of serious criminal activity online, from child sexual abuse to terrorism and fraud.

Addressing these challenges and ensuring the safety of citizens online is essential to increasing public trust and confidence in the internet. It also supports social and economic wellbeing by enabling people to engage in the opportunities presented by the internet and the digital economy.

Since 1996 Nominet has operated at the heart of the UK's internet community as the .UK domain name registry. We believe in a world that is connected, inclusive and secure.

Our policies provide the framework of principles which ensure this ambition is reflected in the .UK namespace. As the environment in which we operate evolves, we actively engage with a wide variety of UK stakeholders to ensure that the policies we maintain reflect emerging threats, changes in stakeholder expectations and new industry practices. This ensures that .UK provides a platform for innovation and remains a competitive and trusted space preferred by businesses and consumers.

This consultation seeks input on three important issues:

I. Reducing the use of .UK domain names for phishing attacks

II. Implementing law enforcement landing pages following suspensions for criminal activity

III. Implementing a .UK drop list to provide a transparent and orderly process for the re-registration of expired domains

Ensuring .UK policies reflect current expectations of the UK internet community is an ongoing process of continuous improvement. We have therefore also included a forward looking roadmap and invite stakeholders to submit issues of interest for consideration in future .UK policy discussions.

We invite stakeholders to:

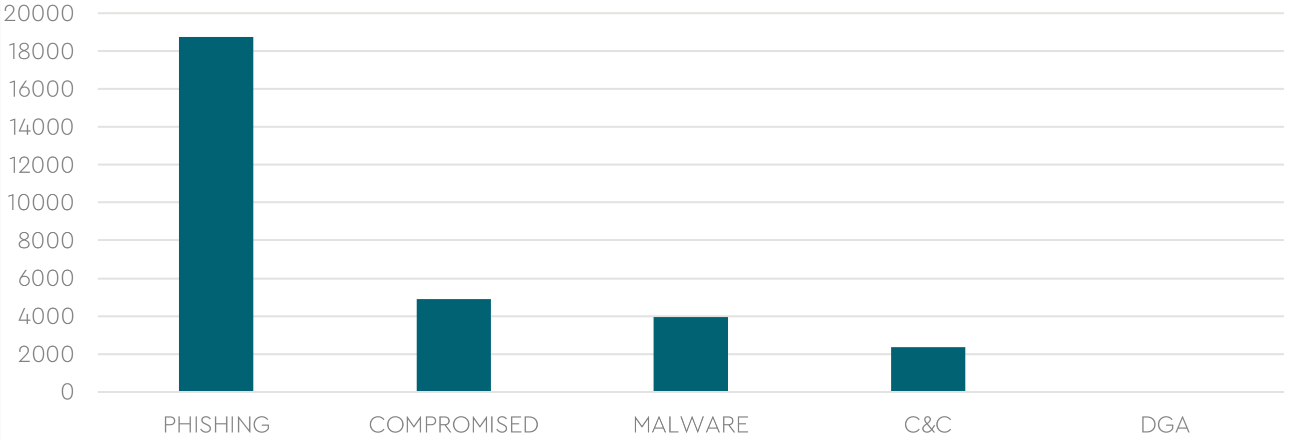
- Send written responses by 16th December 2019 visit www.nominet.uk/policy
- Attend a roundtable in London on 4th December. You can attend all sessions, or only the one that interests you. Phishing 9:30 – 11:00, Landing pages 11:30 – 13:00, Drop lists: 14:00 – 15:30. Register at www.nominet.uk/roundtable

Reducing phishing in .UK

Background

We conduct analysis of activity we see in the DNS for the .UK namespace, and in addition subscribe to independent feeds and reports. Whilst we have some questions about the precise metrics and methodology, it is quite apparent that by volume phishing accounts for the vast majority of reported security threats in .UK (see figure 1). Phishing is in essence the masquerading by criminals as an apparently trustworthy entity in order to acquire usernames, passwords, bank details or other information. It is reported by UK organisations as one of the most disruptive types of cyberattacks with estimated costs rising each year[1]. It is therefore clearly a priority issue for us in terms of our commitment to providing a trusted and secure .UK namespace.

Figure 1: Security Threats in .UK July 2018 - July 2019



Phishing. Using a domain to acquire usernames, passwords, bank details etc. by masquerading as a trustworthy entity.

Malware. Using a domain to serve malware (software used to disrupt computers, gather sensitive information, or gain access to private computer systems) e.g. Viruses and Trojans.

Compromised. The domain has been hijacked and is under the control of a malicious third party.

Command and control (C&C). The domain is acting as a control centre for a botnet. A botnet is a collection of compromised computers running unwanted software, often to send spam or execute DDOS (Distributed Denial of Service) attacks.

[1] Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey 2019: UK Business and Charity Findings*, 2019.

> **Domain Generating Algorithm (DGA).** The domain is associated with a DGA, which is often used as part of malware or botnets.

Speed is essential for effective mitigation of phishing attacks, where the most damage can be done in the first minutes and hours. In the case of domain names registered specifically for phishing, where this is visible at registration it may be preventable. However, there is always the risk of disruption to legitimate registrants and so action at the registry level needs to be carefully considered.

What we currently do to prevent phishing

Since 2018 we have been running Domain Watch, an anti-phishing initiative to further increase the security of the .UK zone and protect .UK end users from malicious phishing activity. The initiative operates as a risk-based enhanced verification of registration data for all newly-registered domains.

We use a combination of technical algorithms and manual intervention to highlight suspicious domains. When identified as high risk of phishing, we prevent domains from resolving in the DNS until extra diligence is conducted and we are satisfied that the registration does not pose a phishing risk. The registrant will receive an email informing them what has happened, together with the next steps required if they feel the suspension was not correctly applied.

Of the 3.6 million newly registered domains in the 12 month period July 2018 to July 2019, over 1,500 domains were blocked in the DNS as a result of our Domain Watch initiative.

Consultation questions

We are now seeking input from all interested .UK stakeholders on the following questions related to phishing in .UK.

Nominet's standard Terms and Conditions of Domain Name Registration include the requirement to provide correct and up to date contact information: " … any identity and contact information you (either through yourself or through your registrar) send us is correct and kept up to date … [and you will respond] … quickly to any request from us to confirm or correct the information on the register … [and] … you will not use the domain name for any unlawful purpose."

In addition, we may suspend a domain name (i.e. prevent from resolution in the DNS) if " … in our sole discretion we believe the domain name is being used in a way that is likely to endanger any part of the domain name system, other internet users (including but not limited to the distribution of viruses and malware, phishing activity or facilitating distributed denial of service attacks) or our systems and internet connections".

Our experience indicates that most registrants who register domains for the purposes of phishing tend not to be forthcoming with additional contact information when questioned. Currently, domains identified as a potential risk of phishing are blocked at the point of registration on the basis of identity verification. To improve clarity, we are considering updating these provisions to specifically allow us to prevent resolution in the DNS on the basis that we have identified a high risk the domain will be used for phishing.

1. Do you agree that we should update our policies to specifically allow us to prevent resolution in the DNS where we have identified a high risk of phishing use? [y/n] If no, why not? [freetext]

2. Do you have any other suggestions or thoughts as to how phishing may be prevented and/or mitigated in .UK? [freetext]

3. What other security threats should Nominet prioritise as part of our commitment to a secure and trusted .UK namespace, and reduce cybercrime in the UK? [freetext]

Law enforcement landing pages

Background

As the .UK domain name registry, we provide a registration database which effectively acts as a directory service for the .UK namespace. We do not host or hold any content. Where criminal behaviour occurs, we want to play our part in making .UK safe and trusted, but we do not have any technical means to remove content or alter websites. However, we can disrupt the impact of criminal behaviour by removing or suspending a domain name. While this is a limited intervention – the content will continue to exist on the server or cloud provider regardless, and where the relevant IP addresses have been cached by local internet service providers, the domain name may still resolve to the website in question for a period of time – it is the basis for a successful collaboration with UK law enforcement agencies to suspend domains used for criminal activity. We formalised this approach in 2014 following public consultation.

Suspension – removing the domain name from the zone file – will make it more difficult to find the associated content as the domain name will no longer resolve and in due course an error will appear.

When a UK law enforcement agency listed in Schedule 4 of our .UK Registry-Registrar Agreement formally certifies a domain is being used for criminal activity, Nominet will carry out additional administrative checks, notify the registrant they are in breach of our Terms and Conditions of Domain Name Registration, provide 48 hours notice to resolve the issue and then suspend the domain.

Law enforcement agencies must provide contact details for the referring agency, to be provided to the registrant. If the registrant ceases to engage in criminal activity - to the satisfaction of the law enforcement agency - the domain can be unsuspended. We report publicly on our efforts to prevent criminality in the .UK namespace. The annual report is published in November every year.[2]

We now seek views on what should happen following the suspension.

Feedback from law enforcement agencies and civil society indicates there may be a public benefit to Nominet directing web users, who may have bought dangerously illegal or unlicensed medical products, or been victims of a fraud, to an informational landing page. The Uniform Rapid Suspension (URS) procedures in new gTLDs has a similar provision in place. This could provide transparent information on why domains are suspended and what to do if you have been affected. For example, by providing advice on where to safely buy medicine online. It could also be used to encourage reporting to assist investigation, for example by directing the public to ActionFraud.

[2] https://www.nominet.uk/32000-uk-domains-suspended-as-law-enforcement-and-industry-keep-uk-safe/

Civil society groups have also suggested that a landing page would be useful to improve transparency on the reasons a domain may be suspended. We could also have a clearer policy on the duration of the suspension period before cancellation of the domain.

Consultation Questions

4. What do you think about the principle that a domain which has been suspended for criminal use should be directed by Nominet to an informational landing page? [freetext]

5. We currently suspend domains for the remainder of the term of registration, or 12 months if that is longer than the remaining unexpired term. But this practice is not currently formalised in policy. Do you agree that this period is sufficient, and that we should formalise the suspension period in our policies? [y/n] & [freetext]

.UK drop list

Background

Most domain name registrations are not retained indefinitely. Registrations expire over time and the domain becomes available for general registration on a first come, first served basis. With a limited number of words and letters that are short, memorable and reflect the intention of use there is interest in registering "second hand" domains.

Currently if we don't receive a renewal request within 30 days of the expiry date, we'll suspend the domain name. When a domain has been suspended for 60 days without being renewed, we'll schedule it for cancellation. Once cancelled, the domain name will become instantly available to others who may wish to re-register it.

There are several consequences as a result. Firstly, only those with technical expertise and industry insight can understand when a domain will become available for registration. Secondly, Nominet's whole database is excessively queried for registration and renewal status of all domains, in order for lists to target dropping domains to be generated. Finally, not all dropping domains are registered and actively used by the new registrant, reducing the vibrancy of .UK domains.

.UK drop list

Nominet is consulting on implementing a .UK drop list to provide a transparent and orderly process for the re-registration of expired domains. This is intended to provide clarity on when a domain will become available for registration, 'level the playing field' between registrars, and reduce generally the load on our systems.

Information on the date and time an expired domain name will become available for registration could be provided to registrars and the general public, via Registrar Resources or public list of domains scheduled to be released on any given day. To provide the time, in addition to the day, would also involve scheduling the release of cancelled .UK domain names to take place at a time that is not random.

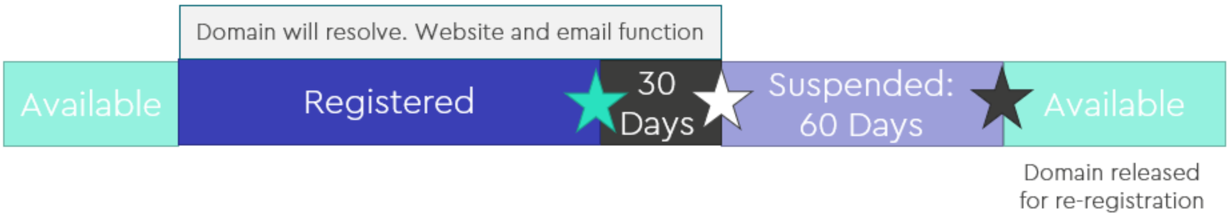
This information could be published when an expired domain is suspended – at which point, the registrant should have had prior notice their domain is due to expire. Registrars are required to issue an expiry notice before the expiry of the domain.[3] The current domain life cycle is illustrated visually below.

[3] .UK Registry-Registrar Agreement. (B.1.13)

★ **Expiry**. When a domain name comes to the end of its contracted registration period.

☆ **Suspension**. Domain is removed from the zone file. The domain will not work as part of a website or email while suspended.

★ **Cancellation**. Deleted from the register (will therefore not work as part of a website or email, and may be released for re-registration on a first come, first served basis).


Domain will resolve. Website and email function
Available
Registered
30 Days
Suspended: 60 Days
Available
Domain released for re-registration

Consultation Questions

You do not have to respond to every question, provide answers as you feel is appropriate.

6. In principle, do you think Nominet should publish official information for **registrars** to clarify when expired domains will become available for general registration? [y/n]

    a) If no, why not? [freetext]

7. Do you think that Nominet should encourage competition in the .UK secondary domains market? [y/n]

    a) If yes, why do you think this is important? [freetext]

    b) If no, why not? [freetext]

8. In principle, do you think Nominet should publish official information for the **general public** to clarify when expired domains will become available for general registration? [y/n]

    a) If no, why not? [freetext]

9. Any other comments [freetext]

Future policy discussions

Ensuring .UK policies reflect current expectations of the UK internet community is an ongoing process of continuous improvement.

We are considering several aspects of improvement for the .UK namespace including:

- Moving to an inter-registrar transfer system that is more widely adopted across the industry
- Standardising domain name renewals, expiry and cancellations in line with generic Top Level Domains (gTLDs) by implementing RFC 3915 and a life cycle to match gTLDs.
- Removing the option for direct registration of domains with Nominet, without operating through a registrar

We invite all stakeholders to suggest issues for consideration.

1. What is the issue?
2. Why is it important?
3. Who does it impact and how?
4. What suggestion do you think would provide a solution?