Messaging, Malware and Mobile Anti-Abuse Working Group

A M3AAWG Introduction to Addressing Malicious Domain Registrations

June 2018

The reference URL to this document is: www.m3aawg.org/MaliciousDomainRegistrations

I. Introduction

The vast majority of domain name registrations are made for legitimate purposes, most often to provide an online home for a lawful business or organization. However, there are some domain names registered exclusively to cause consumer harm. This document focuses on defining malicious domain names and provides a non-exhaustive list of possible actions that can be taken to address them once they have been found.

II. Illegal Activities that Warrant Designation of Domain Names as Malicious

Under Section 1.13 of ICANN's Registrar Accreditation Agreement (RAA[1]), "illegal activity" is defined as "conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law." Depending on the jurisdiction, this definition would include domain names used for purposes such as the following:

1. Online child sexual exploitation materials.

2. Promotion or encouragement of terrorism, fundraising in support of terrorism, training and equipping terrorists, or sites encouraging the development, deployment and use of weapons of mass destruction.

3. Sites involved in the illegal production, sale or distribution of narcotics and dangerous drugs ("Scheduled Controlled Substances"), or the illegal production, sale or distribution of listed precursor chemicals (aka "DEA List I or List II Chemicals").

4. Money laundering or related financial offenses.

5. Hacking/cracking, or conducting or directing attacks against other sites, including so-called "denial of service" (DoS) attacks; unauthorized intrusions or attempted intrusions; unauthorized network scanning or reconnaissance; or the production, distribution or operation of malware (malicious software) including the hosting of botnets or their "command and control" servers.

[1] ICANN's Registrar Accreditation Agreement is available at https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

6. Carding, which is trading in stolen credit cards or similar financial credentials, or the sale or other disposition of private personally identifiable information (PII).

7. Fraudulent or deceptive schemes, including but not limited to Ponzi schemes, advance fee fraud, auction fraud, sale of mislabeled or misbranded products including "knock-off" consumer goods such as illegally branded watches, jewelry, handbags, shoes, sports jerseys, etc.

8. Sending unsolicited commercial communications ("spamming") or facilitating the sending of such communications, including the compilation, marketing and sale of compilations of addresses or phone numbers.

9. Illegal trafficking in copyrighted intellectual property, including pirated software ("warez"), pirated music, pirated movies, pirated books or other pirated intellectual property.

III. Missing or Inaccurate Registration Information and Malicious Activity

Domain names registered under generic Top Level Domains (gTLDs) are required to have accurate WHOIS information.[2] However, some domain names may lack WHOIS data for required fields or contain inaccurate WHOIS information.

Missing or inaccurate WHOIS information, where it is otherwise required, could indicate a possible breach of agreement, either with the registrant's Terms and Conditions with the corresponding registrar or the registrar's Registrar Accreditation Agreement with ICANN, or both. But that does not mean it was registered in violation of applicable laws governing registration and use of domain names. It also does not mean that it was registered exclusively to cause consumer harm.

However, depending on the information used to register the domain, there may be circumstantial evidence that the domain was registered for malicious purposes. In certain cases, if a registrant does not update or correct missing or inaccurate WHOIS information after being given an opportunity to do so, a rebuttable presumption – assumed to be true – may arise that the domain was registered exclusively for malicious purposes.

If the information is not updated or corrected, then the domain may be suspended even if it is not malicious. If, based on other factors, it appears that the domain was registered exclusively to cause consumer harm and that the domain is being used for such purposes, the false or inaccurate WHOIS may be used as an indicator to meet the preponderance of evidence standard, especially if it has gone uncured within a reasonable timeframe.[3]

IV. Unauthorized Use of Contact Details and Malicious Activity

When individual or organizational contact details are likely being used intentionally without authorization, a presumption arises that the domain name has been registered for malicious purposes and is currently being used illegally. Unauthorized use of someone else's identity is usually considered an indicator that the domain name was registered and is, or will be, used for malicious purposes only.

---

[2]ICANN WHOIS, 2013 RAA - Registrant Benefits and Responsibilities, https://whois.icann.org/en/2013-raa-registrant-benefits-and-responsibilities states, "Domain Name Registrants' Responsibilities: [...] You must provide accurate information for publication in directories such as WHOIS, and promptly update this to reflect any changes."

[3] WHOIS Accuracy Program Specification, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#WHOIS-accuracy

V. Malicious Domain Names, the Uniform Domain-Name Dispute Resolution Policy (UDRP) and the Uniform Rapid Suspension (URS) System

ICANN (Internet Corporation for Assigned Names and Numbers) has implemented the Uniform Domain-Name Dispute Resolution Policy (UDRP) as a process that allows a business entity or individual to challenge the registration and use of internet domain names. The ICANN Uniform Rapid Suspension (URS) system complements this structure by offering a more efficient path to resolving "the most clear-cut cases of infringement."[4]

According to ICANN:

> "Under the [UDRP] policy, most types of trademark-based domain-name disputes must be resolved by agreement, court action, or arbitration . . . Disputes alleged to arise from abusive registrations of domain names (for example, cybersquatting) may be addressed by expedited administrative proceedings that the holder of trademark rights initiates by filing a complaint with an approved dispute-resolution service provider."[5]

It is important to note that, when a domain name is being used for malicious activity like phishing, botnet command and control or malware distribution in addition to any possible trademark violation, if clear and convincing evidence of such malicious activity is provided to the registrar of record through the corresponding report of abuse, it may decide to suspend the domain name without requiring a UDRP or URS decision.

To have the malicious domain transferred or deleted based on the trademark violation, however, it is usually necessary to initiate a UDRP or URS proceeding. An additional way to seek the transfer or suspension of a malicious domain name may be the initiation of an administrative proceeding, however many of the available administrative proceedings are based on the UDRP and were only designed to enforce rights based on intellectual property, and so there may be no recourse to transferring or deleting the domain outside the courts. For example, if a generic domain such as example.com is registered for phishing, and then a subdomain is created to mimic a famous bank brand, no remedy is available under the UDRP, even though the domain has clearly been registered for phishing purposes.

Also, many domains may be ordered to be transferred under a UDRP-like proceeding even if they are not currently being used to cause consumer deception and harm. Therefore, without specific findings that the domain was registered exclusively for causing consumer harm and is currently being used illegally, there is no basis to classify such infringing domain names as necessarily "malicious."

The term "malicious domain name" is a special category that usually implies there is a basis to suspend the domain name due to its having been registered under false pretenses exclusively to cause consumer harm and that the domain is currently being used for such purposes. Malicious domain names are not typically transferred to a complainant even if the domain is confusingly similar to a brand to which the complainant has established rights. That can typically only be done through a UDRP-like proceeding to ensure adequate safeguards for due process.

[4] See ICANN website, Uniform Rapid Suspension (URS), https://www.icann.org/resources/pages/urs-2014-01-09-en
[5] See ICANN website, Uniform Domain-Name Dispute-Resolution Policy, https://www.icann.org/resources/pages/policy-2012-02-25-en

VI. Addressing Malicious Domain Names

The following is a list of possible, non-exhaustive actions that can be taken to address domain names that have been identified as truly malicious. Some of these actions can be taken by any user, while others may require the development of the corresponding policies in the generic or the country code Top Level Domain spaces.

- Details concerning the malicious domain shall be forwarded to the registrar (and possibly the registry, if needed) operator(s) to see if the domain name may be suspended per its policies and procedures. The appropriate law enforcement agency or CERT (Computer Emergency Response Team) within the corresponding jurisdiction should be contacted as well, if needed.

- If a malicious domain's contact details are suppressed or obfuscated by a privacy or proxy service, that service should be contacted to evaluate if the domain's service may be terminated under applicable terms.

- If the registrar or registry operator does not respond, a complaint should be filed against the registrar or registry operator to the extent that such processes are available. For example, an ICANN Compliance complaint against the registrar may be in order for failure to investigate a report of abuse if the domain is a gTLD. At the same time, organizations should also consider using any administrative proceedings available, such as the URS for a new gTLD domain.

VII. Conclusion

This document illuminates the problem of malicious domains, which are defined as domains registered exclusively to cause harm to users. Examples of illegal activities that can be facilitated with malicious domain names, regardless of the jurisdiction, are online child sexual exploitation materials, money laundering, encouragement of terrorism or extremist recruitment and more.

Domain names with missing or inaccurate registration information may be an indicator of malicious activity, especially if combined with other evidence. Moreover, domain names that use third-party contact details without their permission are presumably registered for malicious purposes.

In order to have malicious domains transferred or deleted, an administrative proceeding such as UDRP or URS is usually required. However, there has to be clear and convincing evidence that the domain was registered and is being used exclusively in bad faith to cause harm.

Once a domain is identified as malicious, the user may submit a report of abuse to the registrar and, depending on the circumstances, to any involved privacy or proxy service, to the corresponding registry, to the appropriate law enforcement agency, and to the most appropriate CERT to ensure that the domain name is suspended according to applicable policies, terms and conditions.

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates