Messaging, Malware and Mobile Anti-Abuse Working Group

Using Generic Top Level Domain Registration Information (WHOIS Data) in Anti-Abuse Operations

July 2016

Domain registration information (WHOIS data) provides the ability to look up "the information that registrants provide when registering a domain name and that registrars or registries collect."[1] Whether the report of abuse must be submitted to the registrar or the Registrant, the contact details for the specific domain name will be displayed in the WHOIS data.

WHOIS information plays a key role in determining where to report instances of abuse involving domain names. In order to address and mitigate issues that impact the safety or the security of internet users – or the security, stability or resiliency of the internet itself – accurate and reliable WHOIS information is a valuable resource. Examples of the types of incidents that can be addressed by making use of the information displayed in domain name WHOIS include:

- Spam
- Phishing and fraud
- Copyright and trademark infringement
- Malware distribution, botnet command and control
- Distributed Denial of service attacks (DDoS) that use the Domain Name System (DNS) as an attack vector

WHOIS Elements

In the gTLD[2] space, WHOIS records contain sets of elements related to the domain name itself, the Registry that operates the TLD, the sponsoring registrar, the registrant of the domain name and its Administrative Contact, Technical Contact and, optionally, its Billing Contact. All registrars and registries collect this information and publish it via services that make use of the WHOIS Protocol or via web-based interfaces.

This information is public and available for anyone to query. An example of the WHOIS information of the domain name "internic.net" can be found on ICANN's WHOIS webpage.

[1] SAC 051, Report on Domain Name WHOIS Terminology and Structure. ICANN's Security, Stability and Advisory Committee (SSAC), page 6, 19 September 2011.

[2] gTLD means generic Top Level Domain. For a definition, visit ICANN's Glossary at https://www.icann.org/resources/pages/glossary-2014-02-03-en#g

WHOIS Elements with Operational Value

The following are examples of WHOIS elements that usually have operational value and are frequently used in investigations of abuse.

Registrar's Abuse Contact

Some types of abuse should be reported directly to the registrar and some can be reported to the Registrant or the Administrative Contact of each domain name. Reports of abuse to be submitted to the registrars directly include those related to domain names registered and used for phishing, botnet command and control, malware distribution, or pharming. Another example might be a legitimate domain whose name servers were changed by an attacker after compromising the Registrant's access credentials to the administrative interface of its domain name. Note that if there are doubts regarding the identity of the registrant, the most appropriate path is to file a WHOIS inaccuracy complaint.

ICANN's Registrar Accreditation Agreement (RAA) provides that registrars must maintain an abuse point of contact to receive reports of abuse involving their sponsored domain names. The RAA provides that this information must be displayed by the registrars on the homepage of their websites, however many registrars also include their abuse contact details via the WHOIS output of the domain names that they sponsor.

Registrant or Administrative Contact

There may be times when reaching out to the Registrant or the Administrative Contact of the domain name will be more effective than reaching out to the registrar. An example is a phishing site hosted on a compromised webserver. In this case the domain name is usually legitimate but the webserver is hosting a phishing site without the Registrant's knowledge. The Registrant and the Administrative Contact are in the best position to mitigate the threat by securing the hardware and software associated with the administration and operation of the domain name and removing the fraudulent webpage.

Authoritative Name Servers

Authoritative name servers provide definitive responses to DNS queries, such as the IP address for the web server or the mail server associated with the queried domain name. A name server associated with a malicious domain name can, in certain cases, also be associated with many other malicious domain names. Thus determining all the domain names associated with a given name server can help identify a portion of, or all of, the criminal infrastructure associated with the activity being investigated.

On the other hand, DNS hijacking attacks can involve replacing the legitimate name servers of a domain name with those operated by the attacker, who can then redirect the victims' traffic to its own criminal servers. Users and organizations should be aware of the existence of these types of attacks and include their DNS resources as assets worthy of protection in their internet security assessments.

Dates and Time Stamps

Changes to the domain registration information are usually infrequent. Review the time stamps when suspecting fraud or a compromise with a domain. Both the creation and last updated time stamps can be found on the WHOIS record. While not a definitive indicator of abuse, a newly created or recently updated domain name may require further investigation, depending on the circumstances.

Additional Information

Proxy and Privacy Services

Some users of domain names avail themselves of services to maintain the privacy of their contact information. These services replace information in the WHOIS record with information provided by a third party that (ideally) will pass on the inquiry to the licensee of the domain name or reveal its identity. (The exact process depends on whether the domain was registered behind a proxy service or a privacy service.)

Note: Proxy and privacy services can make it difficult to identify and contact the actual domain licensee.

WHOIS Accuracy

Registrants have an obligation to provide current, accurate and reliable registration information. When it is not accurate, you can submit a complaint to ICANN's Contractual Compliance Team through the complaint form.

Historical WHOIS Information

Some third parties provide access to historical WHOIS information, typically for a fee. Historical WHOIS records can be valuable in determining names, email addresses, name servers, resellers or other types of data previously associated with the domain names being investigated.

Conclusion

WHOIS data is used to identify the parties responsible for the registration and operation of a domain name. It is also commonly used to identify and defend against various types of abuse, including spam, malware, DDoS attacks and other threats. This paper briefly outlines the most operationally relevant fields displayed in the gTLD WHOIS output that can help address instances of abuse appropriately and in a timely manner.

With the availability of all this data, security researchers and law enforcement officers must always be sure to make their own assessments regarding the accuracy of the WHOIS information for the domain names they are looking into, the type of abuse that is associated with each domain name, and how they will use the data. They must also decide whether they should send the registrar, the Registrant or the Administrative Contact a report of abuse, depending on the potential implications; i.e., the domain name may get suspended or canceled, or the registrar may contact the Registrant, who may or may not be associated with the malicious activity.

Analysis of large amounts of WHOIS data – corresponding to thousands of malicious domain names – can help define trends and patterns, identify modus operandi, identify probably-involved parties and provide other relevant information. Although this may require some specific skills, and might require a more distributed and robust infrastructure, the benefits of an investigation frequently will outweigh any additional cost.