Feedback to ICANN's proposed GDPR-complaint WHOIS model

April 23, 2018

Summary

BitSight believes third-party cyber security risk solutions are an important but underrepresented use case of WHOIS data, and the proposed interim model poses challenges to the efficiency of these products without additional adjustments. We highly recommend that if the disambiguation between legal and natural persons cannot be made using the registrant-provided information, then the domain portion of the registrant email address should remain available in public WHOIS data. Secondly, we join others in recommending the inclusion of a unique identifier or GUID if the plaintext registrant email cannot remain available in public WHOIS data. Lastly, we encourage that organizations performing security threat research and providing security products are permitted members of the accreditation program. These important organizations require access to WHOIS data to research malicious actors as well as aggregate domain asset information on individual businesses and organizations for the purposes of external security assessments.

Background

BitSight created the security ratings market with a focus on empirical risk measurement and has led the growth and evolution of the market. Much like credit ratings, BitSight Security Ratings are generated through the analysis of externally observable data. BitSight measures cybersecurity robustness by collecting and analyzing large amounts of data on security behaviors and mapping those behaviors to organizations. The platform gathers data on daily security outcomes from sensors deployed across the global Internet, which includes information on machine compromise, network vulnerabilities, and other critical security issues.

Security ratings have become a critical foundation for many organizations' vendor risk management strategies. Security ratings are used when investigating potential prospects, while at the same time providing the ability for companies to continuously monitor key relationships and partnerships. The cyber insurance industry has adopted security ratings as a part of the underwriting function where the ratings provide insight into new applicants and allow insurers to take proactive measures to mitigate security concerns and improve the cybersecurity posture to reduce the probability of breaches for their existing insureds.

As part of offering this service, BitSight also contributes to the larger security community through its ongoing threat intelligence research. BitSight actively collaborates and assists with partners through the Europol EC3 Advisory Group on Internet Security, as well as shaping security risk management discussions as a partner organization within the Global Cybersecurity Alliance. BitSight also makes publicly available a free domain-based reputation service that is used by many organizations and individuals for spam reduction efforts.

Use of WHOIS Data

WHOIS data plays an important role in our provision of our services in both (a) investigations into malware activity, and (b) the association of data points between our repository of threat intelligence and risk indicators and the inventory of organizations that are continuously monitored, as described in greater detail below.

- Investigations into Malware Activity - Threat intelligence research includes discovering when various machines at organizations across the world are compromised, as well as the groups responsible for such attacks. WHOIS data allows researchers to find related assets as well as research the source and origin of infrastructure and of the malware itself. This function expands to being able to observe the extent of the botnet, assess the risks posed to individual machines, and coordinate with the appropriate legal authorities for investigations and takedowns.
- Association of Data Points - Third-party risk management tools, in addition to security rating services, allow for organizations to understand the security posture of their business partners. WHOIS plays an important role for discovering and understanding the footprint of a corporation or organization on the internet. Threat intelligence telemetry is subsequently joined to organizations and assessed for its severity, frequency, duration, and confidence to create an overall rating of that organization's current security health. Without this association, it is more difficult to attribute these threats to organizations.

The reduction of WHOIS data can add an additional risk to individuals when members of the security community are less effective in performing the aforementioned tasks for which BitSight currently relies upon the WHOIS system. It can also hinder companies' abilities to measure and monitor their third-party risk.

Recommendations

BitSight is supportive of many aspects of the Proposed Interim Model, but suggests the recommended changes below so that our industry can continue to provide important services to its customers and other impacted parties.

Public WHOIS Data

As described above, access to WHOIS data is critical to our ability to provide our services, and BitSight uses that data as an input to its products and services. BitSight understands from members of the Contracted Parties House (CPH) that disambiguating natural and legal persons is a difficult task. However, given the importance of this data to legitimate users of the WHOIS data, BitSight recommends that if the disambiguation cannot be made using the registrant information, the domain portion of a registrant's email address remain available, leaving the mailbox name obfuscated when necessary. This approach would allow for a simple and effective way of disambiguating between domain names most likely owned by legal persons and those owned by natural persons without having to expose any personal information about the registrant. BitSight recognizes that this proposal cannot disambiguate all registrations between legal persons and natural persons, such as cases when a natural person uses his or her personal information when registering a domain controlled by a legal person. Nonetheless, it allows for significantly greater access to important data than the current Proposed Interim Model.

In addition, as has been discussed in previous public comments, one of the most important and popular queries on the WHOIS dataset is to perform a lookup on all domains managed by a particular registrant. This applies for both threat research as well as the third-party risk management use case. It is currently unclear whether bulk access and "bulk actions" would be permitted under the accreditation program, and it is important to have the ability to perform this function under the public WHOIS data as well. If ICANN ultimately determines that the plaintext version of the registrant email cannot remain available, BitSight proposes the use of a GUID or other identifier that is unique to each registrant as a way of allowing the beneficial uses of this data without the legal concerns associated with leaving the plaintext version publicly available.

Accreditation Program

BitSight joins the many other organizations who have commented on the Proposed Interim Model in supporting the creation of an accreditation program for organizations that require full WHOIS data to perform in an effective manner. Given the importance of the work done by these organizations, BitSight strongly recommends that security research, threat intelligence, and security rating companies be included in any accreditation program. Their ability to operate efficiently affects many downstream industries and individuals.

BitSight also supports the proposed accreditation program put forth by ICANN's Intellectual Property and Business Constituencies, which outlines the accreditation process, specific types of organizations permitted for accreditation, as well as specific uses of data from WHOIS. In addition to the use cases already defined in version 1.3, BitSight strongly recommends including the ability to use the WHOIS data to discover and aggregate business and organizational assets

for such cases as performing third-party risk assessments, evaluating a company's security posture for cyber insurance policies, and monitoring the security of critical national infrastructure.

We look forward to continuing to work with ICANN in developing an approach to making WHOIS data available that complies with applicable law, as well as allows for the beneficial uses described above.

Tom Turner
Chief Executive Officer