Ref. 913660

Contribution to the Public Review of ICANN's "gTLD Registration Dataflow Matrix"

Europol is the European Law Enforcement agency which provides strategic and operational support to the European law enforcement community. The European Cybercrime Centre (EC3) is the cybercrime division of Europol. This contribution is based on EC3's operational experience in supporting major transnational cybercrime operations.

1. Purpose

EC3 cybercrime analysts and investigators use TLD registration information (here after WHOIS data) mainly for two purposes:

- To identify a contact point for a domain name;
- To gather investigative leads related to the owner/purchaser of the domain.

In identifying the most needed data elements, however, it is necessary to take into consideration that in certain specific cases, law enforcement agencies (LEAs) need to access additional data elements in order to carry out meaningful investigations. The contribution focuses on those registration data elements routinely used by investigators.

2. Data

2.1. Domain name details (name, nameservers)

LEAs use WHOIS data to orientate and focus investigative efforts as well as to skim relevant information about suspects and victims from the rest.

- domain name
- IP address (Domain hosting)
- Name Server
- Creation date
- Update date
- Expiry date
- Domain Status
- Registrar WHOIS server
- Registrar's URL

User Story: Banking malware

A WHOIS lookup leads an investigator to one of the domain used to administrate a botnet used to distribute a banking malware. This allows the identification of an e-mail address used for registering the domain within the WHOIS Database. A reverse WHOIS lookup revealed that several other domains were registered with the same e-mail address.

In this case the WHOIS proved to be accurate enough to facilitate LEA investigations and the final arrest of a botnet administrator.

2.2. Registrar

LEAs need to access up-to-date and validated contact details of registrars and registrants in order to carry out sinkholing activities. The same applies for information on resellers: if they behave as registrars, LEA might need to access contact information to further investigate leads.

- Registrar
- Registrar's URL
- Registrar's WHOIS server

- Registrar abuse mail
- Registrar abuse phone
- Reseller (data as above)

User Story: RAMNIT

In February 2015, a law enforcement joint operation of UK NCA, Germany, Italy, the Netherlands with support of Europol EC3 took down the Ramnit botnet affecting 3.2 million computers worldwide. The botnet was acting as banking information stealer, using fast flux technique to redirect the traffic to compromised domains.

During the operation 7 servers were seized, 300 domains generated by Domain Generation Algorithm (DGA) were seized; the entire infrastructure of the botnet was taken down and sinkholed. Investigations revealed that one of the 7 seized servers was registered in the DNS WHOIS as provided by a Russian Registrar and officially located in Germany. The registered location of the server proved to be inaccurate as the server was actually geo-located in the Netherlands, probably due to the usage of the fast-flux technique.

The Russian Registrar promptly collaborated with LEAs to support the investigation, revealing the correct location of the server. But incorrect registration information in the DNS WHOIS drastically slowed down the investigations, impeding LEAs from easily addressing gTLDs and ccTLDs and geo-locating servers.

It is essential not only to attribute criminal conducts but also to apply mitigation measures and clean-up infected systems: for example, by contacting a registrar to shut down a CSE website. If the details are inaccurate, not updated or not used, the website cannot be closed through domain abuse notification.

2.3. Registered Name Holder (Registrant)

Registrant data is by far the most useful for LEAs when investigating online crime. **E-mail data is the most important field**: even if all the rest of data is inaccurate, the e-mail provides a link towards a possible identity. It should be mandatory to verify both email and phone contacts provided.

- Registrant name, street, org,…fax
- Reg mail

User Story: TORPIG Botnet

In 2012, UK SOCA identified batches of generic gTLD registrations allocated by the ICANN accredited gTLD Registrar OnlineNIC that were connected to suspects responsible for spreading the Torpig Botnet. These domains were all registered with the name and full address of a victim of identity theft (personal details stolen for use of online crime).

UK LEA conducted investigations on the registered holder of the domains, who was proved to be unaware and not responsible of the unlawful activities of these domains or the registration, payment, ownership or access to them. However, evidence collected showed that the same Registrar (OnlineNIC) was repeatedly behind the registration of domains used to control botnets.

Investigators had to use alternative and lengthy investigation techniques. Evidences collected showed that Russian organized criminal groups were using Chinese infrastructure to attack the UK. SOCA notified ICANN and involved Registrars of the DNS abuses and of breaches of the Registrar Accreditation Agreement (RAA) by the registrar OnlineNIC. The registrar OnlineNIC was alerted but did not take much action against the abused domains.

2.4. Administration Contact and Technical Contact

The accuracy of these fields should be ensured, so that if LEAs need to access it there is a guarantee of truthfulness. Administration and technical contacts can sometime be used as an alternative means to identify the owner of a domain or the registrar. However these contacts tend to be more related to the registrar than to the registrant, therefore limiting its use in terms of identification of a perpetrator. Even for sinkholing activities, LEAs tend to refer to registry data rather than to admin/tech information.

2.5. Billing Contact

Records of billing contacts are important for investigators, as registrants need to provide at least one valid email address to communicate with the registrar for billing purposes. They should be kept by registrars and registries and be shared with LEAs, when served with a legal order (or an MLAT when the requester is not based in the same jurisdiction than the registrar).

User Story: Compromised website with valid registration

A number of websites on the clear web, controlled by an organised crime group, were distributing child abuse material. For a monthly fee clients could have unlimited access to child abuse material.

Investigators gathered the domain names linked to those websites using open source monitoring or on the basis of contribution from LE partners or NGOs. Investigators then gathered the DNS information linked to those domain names (the IP associated to the domain names). They also gathered the WHOIS data associated to those identified domains.

Cross-matching the three data sets they could identify a valid email address that linked the three sets of information.

This email address was used by the registrants to register the different domains. **The registrants need to provide at least one valid email address to communicate with the registrar for billing purposes.** When WHOIS data is accurate (email address), cross-checked against other data sets, it is a useful tool for crime attribution.

2.6. Data elements not listed

- Payment method and its linked entities (e.g. Bitcoin and the relevant Bitcoin addresses and corresponding transaction IDs) should be added as new fields and maintained and made available to LEAs upon request.
- LEAs should also have access to IP logs (ideally with source port numbers if possible). IP logs (ideally with source port numbers if possible) should also be stored by registrars and made available to LEAs because they can provide the IP address of registrants when they access to registrar's services.
- IP logs are essential for investigators because they might provide the IP address for each registrant's access to registrar's services and might therefore provide critical information which will contribute to the identification of the possible suspects.
- Historical data should be available for consultation by LEAs. Historical registrant's data is as relevant as the one related to IP hosting.
- IP hosting information is very important. For investigative purposes, LEAs need to retrieve information on the geographical location and the hosting provider.
- Hash of the password used for registering a domain is a useful and missing field to be stored and made available to LEAs upon request. This information can be used to cross-match and identify those malicious users who register multiple domains.

4. Comments from EC3

- The idea is that it should be a set of data publicly available (as it is now) and another set that can be shared with LE based on filling in a form (payments, logins, hashed password, a simple query form, which enables an easy access to information such as the LE form at Facebook/Twitter).
- Some data contained in WHOIS can be useful when investigating a non-cooperative or malicious registrar.
- Proxy/Privacy data needs to be stored by the registrar and provided to LE upon request in line with the provision of the Privacy and Proxy Services Accreditation IRT currently being negotiated.
- Both phone and email contacts provided by the registrant should be regularly validated in line with RAA provisions (3.7.7.1[1]).

5. Reference

EDOC#812762 - PSWG - Abuses of WHOIS - Repository of Case Studies

[1] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en