The WhoDat project: an interactive pivotable tool for analysts and researchers to work with Whois data

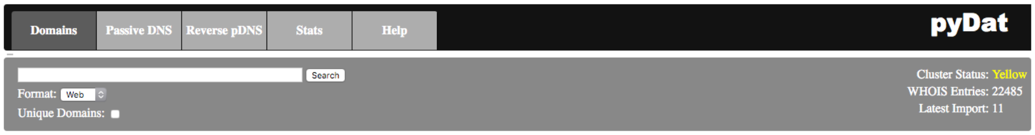
A WhoisXML API User Success Story

The developer

The MITRE Corporation [1] is a not-for-profit company providing innovative solutions for critical challenges in various security related domains including cybersecurity. They operate multiple federally funded research and development centers. They assist the US government with several activities such as scientific research and analysis, development and acquisition, systems engineering and integration. In order to provide cutting-edge solutions for these important challenges they run an independent research program.

A front-end in Python

As the analysis and research of Whois data is crucial in cybersecurity, the MITRE cooperation develops a front-end for WhoisXML API data in support of researchers' and analysts' work. The front-end is developed in the framework of the project named "WhoDat", publicly available at GitHub [2] under General Public License [3]. It integrates Whois data, current IP resolutions and passive DNS.



Format: Web

Unique Domains: □

Cluster Status: Yellow

WHOIS Entries: 22485

Latest Import: 11

A legacy version of WhoDat written in PHP by Chris Clark is available in the repository, too. The current version under the name of PyDAT is written by Wesley Shields and Murad Khan. It is entirely implemented in Python [4]. This makes it especially handy for researchers as Python is one of the most prevalent languages in scientific computing. If once data are accessible in this framework, they can be further processed by a large variety of software libraries. The front-end provides a flexible and extensible tool for searching and analyzing current and historic data. It includes a scriptable API to make search requests and obtain JSON data. Version 3.0 of the software provides an experimental support for the ElasticSearch distributed search and analytics engine [5], facilitating large-scale distributed processing.

Application in search of spear-phishing link domains

An example of the practical use of PyDAT is described in Ref. [6]. Spear phishing attacks are directed at individuals and companies by adversaries aiming at obtaining sensitive information with malicious goals. These attacks occur very frequently: according to Ref. [7] this is the most successful technique on the Internet today, accounting for 91% of attacks.

When cyber threat intelligence analysts are facing such threats they need to collect intelligence information on the adversary's infrastructure. The technique for searching on a spear-phishing link domain is WHOIS pivoting. It consists in looking up suspicious domains and pivoting on each result to find additional information on the domain registrations. In this way as the cited article concludes, "gathering intelligence about an adversary infrastructure could be methodically achieved just by using WHOIS information, making note of missing or incorrect information as you traverse and retrace each finding" [6].

Summary

The research and analysis of Whois data is an important branch of cybersecurity generating challenging novel ideas for research [8]. Obviously such research tasks are of high technical importance and, owing to the broad significance of cybersecurity, they potentially have a high societal impact. The data provided by WhoisXML API can serve as a solid basis of such activity, as demonstrated by the MITRE Corporation. It can be directly useful in security analytics, e.g. revealing spear-phishing domains by whois pivoting. Moreover, their front-end is open-source, and it is fully available for the community.

References

[1] https://www.mitre.org

[2] https://github.com/MITRECND/WhoDat

[3] https://www.gnu.org/licenses/gpl-3.0.en.html

[4] https://www.python.org

[5] https://www.elastic.co

[6] W. Shields: *Using WHOIS and Passive DNS for Intelligence*, MITRE Corporation, 2015. https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/using-whois-and-passive-dns-for-intelligence

[7] D. Stephenson: *Spear Phishing: Who's Getting Caught?* Firmex. https://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught

[8] A. Kott, C. Wang, R. F. Erbacher (eds.): *Cyber Defense and Situational Awareness*, Springer International Publishing, 2014.