DNS forensics using the big data extension of IBM's QRadar Security Intelligence Platform

A WhoisXML API usecase

The challenge

In the era of social networks and mobile devices organizations cannot keep their IT systems as closed as it was possible before. Ways of communication are more and more flexible but this introduces new kinds of IT security risks. Traditional approaches such as firewalls and antivirus software cannot provide sufficient protection against these threats.

Market leaders of security solutions including IBM put a significant research and development effort into this field. The IBM X Force® Research and Development Team [1] provides a vast amount of information on the subject including regularly published reports [2], which well illustrate these issues. Certainly, their product incorporate the benefits of their deep expertise.

The IBM QRadar SIEM

The basis of IBM's key security solutions is the QRadar Security Intelligence Platform, a security information and event management system (SIEM). This is a unified platform covering many security-related tasks and incorporating a broad spectrum of solutions including the use of X-Force® Threat Intelligence [3], IBM's cloud-based threat intelligence platform. It is capable of collecting information from various "traditional" sources such as log contents, user information, database activities, firewall activity, etc. from devices and subsystems, facilitating threat monitoring, vulnerability and risk management, forensics, and incident response.

The tremendous amount of data collected in this way and also the complexity of fraud detection requires the use of big data approach and data mining tech-

niques. For this reason IBM has enabled QRadar to interact with InfoSphere BigInsights, a Hadoop-based big data platform [5]. This approach also enables the inclusion of non-traditional data sources such as linguistic and predictive analytics of e-mail traffic and social networking activity. InfoSphere BigInsights can use the data collected by QRadar and provides a feedback to facilitate a closed-loop learning of the latter system.

QRadar can collect virtually all DNS transactions. Correlating this information with whois data can open additional important possibilities of fraud detection, e.g. in identification of suspicious domains used by botnets and can provide QRadar with information necessary to prevent such attacks. Indeed, InfoSphere BigInsights can be used for this purpose, and this is best achieved using WhoisXML API, as we describe briefly in what follows.

DNS Forensics made easy with IBM QRadar and WhoisXML API

In an online tutorial [6] it is demonstrated how the big data extension of QRadar can be used to do DNS forensics in order to identify

- risky domains,
- risky users, and
- risky IP addresses,

and feed this information back to QRadar in order to define new protection rules.

The idea is that QRadar collects the log data from various devices of the organization so that a large amount of communication events' data is collected. A record includes internal user identification, the source and target IP addresses, ports, and also, the domain names which are involved in the communication.

Domain names can be a subject of more detailed forensics using domain name whois data. It is possible, e.g., to verify when the domain had been registered and when its registration had been last updated. Also the registrant and admin contact data can be informative: by checking if the postal addresses are consistent, the phone numbers are existing, etc. To do all this, one needs an up-to-date and fast source of whois information. This might be a problem as the whois protocol is filtered out by many firewalls, the direct data are not always consistent, and also, it might need additional development to directly communicate with whois servers.

The data obtained from QRadar can be very easily fed to the WhoisXML API web services to provide detailed whois information in handy formats such as JSON or XML, which can then be easily handled by QRadar's big data security extension. This is demonstrated in the tutorial, where it is pointed out that WhoisXML API can (quoting [6])

- *Automatically follow the whois registry referral chains until it finds the correct registrars for the most complete data.*
- *Parse a variety of free-form whois data into well-structured fields (in XML and JSON) that your application can read.*
- *Parse out the name, organization, street, city, state/province, postal code, phone number, and fax from a free-form human-written contact address.*
- *Work over basic HTTP so you don't run into problems that are related to firewalls or accessing Whois servers on port 43.*
- *Return an indication of whether a domain is available.*
- *Return registry dates in their original format and in a normalized format.*

These capabilities, when used together with QRadar's big data security extension, produce impressive and useful results which significantly contribute to the cybersecurity of the organization's systems. This is demonstrated convincingly in the cited tutorial including also a video [7].

References

[1] IBM® X-Force® Research and Development Team, `https://www.ibm.com/security/xforce`

[2] `https://securityintelligence.com`

[3] IBM® X-Force® Exchange

http://www-03.ibm.com/software/products/en/xforce-exchange

[4] `http://www.ibm.com/software/products/en/qradar`

[5] IBM BigInsights, https://www.ibm.com/analytics/us/en/technology/biginsights

[6] J. Bravo, Run DNS forensics with QRadar's big data security extension. an IBM tutorial, 2014. Available at https://www.ibm.com/developerworks/library/se-qradarbigdataext

[7] The video presentation of the cited tutorial: `http://www.youtube.com/watch?v=HgKH5XiF3o4`