WHOIS data for vulnerability notifications

A WhoisXML API User Success Story

October 2017.

One of the cornerstones of cybersecurity is threat intelligence sharing. Maintenance of the security of our IT systems their protection against malicious activity requires an up-to-date knowledge of the entire field. There are significant efforts to assist experts in this activity, including those of market leaders such as IBM X-Force Exchange.

Due to the decentralized architecture of the Internet, however, the collaboration of the actors as well as voluntary campaigns in order to detect vulnerabilities are also of utmost importance. If, however, the owners of the affected systems cannot be notified, these efforts can hardly achieve their positive goal. And in this notification process, Whois data have their use.

O. Cetin et al. [1], researchers of University of Delft, the Netherlands have recently presented some research results in this vein, leading to important conclusions regarding cybersecurity.

The problem

Surprisingly many domain name servers (DNS) are vulnerable to so-called "zone poisoning". This consists in the possibility of replacing existing `A` or `MX` records of a name server by a malicious actor who can then use the domain for phishing or intercepting e-mail. This vulnerability was studied in detail in Ref. [3].

It seems quite trivial that the existence of such vulnerable domains is harmful for the global cybersecurity in general. Hence it would be beneficial if the affected domains would be fixed. In their research, Cetin *et al.* conduct a global campaign against this vulnerability and studied in detail the efficacy of e-mail notifications resulting from their activity.

But how to contact those who can do anything against the vulnerability of a DNS. The trivial idea would be to build on RFC 2142 [2], which specifies that the `RNAME` field of the given name server's `SOA` (Start of Authority) record is supposed to contain information about the contact of the operator of the DNS. It is found, however, that these records are frequently missing or inaccurate.

WHOIS records to reach domain owners

As one of the alternatives, the researchers have purchased WHOIS data from WhoisXML API for the purpose of their campaign. Domain whois data contain contact information to the domain owners, who typically have a stronger incentive to act against the DNS vulnerability than the DNS operators themselves. In addition, though unfortunately Domain Whois data are unfortunately not perfect, it is still the maybe most reliable of all available data.

In Ref. [1] it was indeed found that using e-mail addresses from Domain Whois data significantly decreases the bounce probability of the e-mail notifications sent.

Conclusions

One of the main lessons to learn from the contribution of Cetin *et al.* is that unfortunately at the moment there is no really efficient way to efficiently deploy vulnerability messages. It is likely that e-mail is a too limited tool to achieve this task, and something else should replace it in the future.

So what now? If you want to access the owner of a domain for any reason (e.g. to draw their attention to a security vulnerability), the best approach is still to use as reliable WHOIS data as possible. And if you are an honest domain owner, you should keep your WHOIS data up-to-date, or you may miss some important messages.

References

[1] Orcun Cetin, Carlos Ganan, Maciej Korczyński, and Michel van Eeten. Make notifications great again: Learning how to notify in the age of large-scale vulnerability scanning. In *16th Annual Workshop on the Economics of Information Security - WEIS 2017*, La Jolla, California, June 26-27 2017.

[2] D. Crocker. Mailbox Names for Common Services, Roles and Functions. RFC 2142, Internet Mail Consortium, May 1997.

[3] Maciej Korczyński, Michał Król, and Michel van Eeten. Zone poisoning: : The How and Where of Non-Secure DNS Dynamic Updates *Proceedings of the 2016 ACM on Internet Measurement Conference - IMC 16*, 2016.