WHOIS: On the Front Line of Phishing Protection

Posted on February 5, 2019

Threat actors try all kinds of ways to spread their nefarious acts on as many victims as possible. When it comes to phishing, it's as simple as outright deception. Victims are made to believe they are dealing with a site they trust, after which a perilous cyber trap is triggered, and the damage that ensues can often be irreversible. WHOIS is a valuable tool that can help fortify protections against malicious acts of phishing, thwarting the malicious intent of threat actors before significant threats escalate.

How Domains Factor into Phishing

Every day, millions and millions of people around the world leverage the unlimited power of the web through a network of systems that look up and connect us to the information that we seek. Among those systems are DNS and internet domains. Malicious actors use domains to park phishing sites in a number of ways. Industry figures indicate that on average, four out of five phishing sites are parked on compromised domains. Loss of control and a loss of integrity underlie the spectrum of compromised domain phishing.

Chance is all around us, and there's always a possibility that control of a domain might slip into the hands of a phisher. In most cases, however, compromising a domain takes a bit of work. For this reason, many choose to self-register domains for their site deployments. This paradigm opens up a few interesting opportunities to detect suspicious activities and stop things ahead of time.

It's all in the Domain Information

If you've ever registered a domain, you probably know that it's a bit like registering a vehicle or registering to vote. You have to submit information to complete the registration. Even sites that only capture minimal info aggregate information such as:

- Registrant organization
- Registrant email
- Title of the website

Also, various available additional information uncovers deeper details including dates, business info, and more. This data is invaluable when you use it right.

Digging up Bad Guys

Logic dictates that the “bad guys” are typically not going to put truthful information into domain registration. That is fine because research shows breadcrumbs that should raise suspicion and cause one to double-check information. Registration dates, missing information, drop dates, and a wealth of information can complete the picture. Meanwhile, historical information, the correlation between domain registrations, organizational information and many other indicators of malfeasance occur throughout threads of malicious domain registrations.

Why WHOIS

Evaluating data is typically a time-consuming task. There are countless sources and bits of information to make use of. Active analysis of data from these sources should yield quick results that simply cannot be achieved by standard means. WHOISXML API is a powerful portal to this ocean of information. Aggregating data, digging into information, and finding the things that are typically hard to dig up, WHOISXML API leverages the power of WHOIS within the modern landscape and under present-day threat conditions. Since delivered in a portable database format, the API tool integrates across modern technology systems for rapid analysis and protection, which is suitable for technologies across cloud, hybrid, and traditional data center architectures.

You will find the value of WHOIS data on the front lines of security as a valuable tool in the fight againt digital fraud. Whois data plays an important role in any email security solution or antiphishing solution.

Phishing and Airbnb

A tool such as WHOISXML API can uncover these anomalies and help researches with intelligent

analysis of malicious bits and widespread patterns of domain registration information. We recently took a deep dive into the proliferation of phishing emails that emerged from a recent incident involving Airbnb.

We recommend this reading to all technologists and security-focused professionals.