Enable Active Phishing Protection With Domain Reputation API.

Posted on September 3, 2019

In the digital world, just as in the real one, reputation matters. While in real-world dealings and transactions there exist multiple ways in which we can gauge the reputation of a person or organization with which we have to engage in any capacity, the complexity and sheer volume of the web makes this task exponentially difficult in the virtual world.

The modern economic and technological landscape has silently nudged us into a world of online social interactions, financial transactions as well as business dealings. This has resulted in a large amount of data being stored in and exchanged across digital media on a daily basis.

Consequently, data has emerged as the new currency in the cyber-world, and this is exactly where cyber criminals can take advantage of security loopholes and compromise sensitive and financially significant information.

Domain Reputation: A Key Factor In Effective Security Measures

The cyber-world has made it increasingly convenient to set up and run websites. However, this very same feature has made it easy for cyber-criminals to set up malicious websites and host malware that can severely compromise data and network security, resulting in information leaks that can have potentially disastrous consequences. In such a scenario, careful reputation analysis of any online entity becomes imperative before connecting with the same.

The Domain Reputation API can prove to be a significantly useful tool for assessing the credibility of any online resource. This has multiple use-cases in the field of cyber security. The uses to which the Domain Reputation API can be put are best described by the following hypothetical situation.

The Crime

John receives an email from his bank asking him to take part in an investment scheme with attractive returns. Being a budding investor, John is interested and clicks on the email link to visit the associated webpage.

There, John logs in to a page which asks him to input his bank details and credit card number along with the CVV; this, he learns, is essential for being eligible for the scheme. Unsuspecting, John does the needful and receives a confirmation that his name has been registered for the process.

Later in the day, John learns that several transactions have been made from his bank account, and a considerable sum has been stolen. John realizes he has become the victim of a cybercrime, and immediately contacts the authorities.

How Domain Reputation API Provides The Solution

The above scenario is a classic case of a phishing scam, where the victim is lured by email into revealing sensitive information. A cyber-security professional looking into the above case can take the help of Domain Reputation API to detect the perpetrators and prevent further occurrences of the same act.

How exactly does this work? Let’s find out.

Cyber security professionals can approach the case in the following way: it is evident that the victim was lured to a domain which was probably similar to his bank website. The perpetrators impersonated his bank and thus gained access to his banking details. The problem, in this case, would be to speedily identify the source of the offending website and apprehend the perpetrators.

A scan with the Domain Reputation API can reveal multiple data points which may prove essential in resolving the case. The scan assigns a reliability score to the website which is indicative of its level of risk. The API performs a complete infrastructure check, along with, a malware scan to determine the domain or IP address’s proximity to risk.

The Domain Reputation API also provides an added advantage in the form of Predictive Scoring.

The predictive scoring method utilizes advanced algorithms that use real-time, dynamic datasets to assign a reputation score to domains immediately after registration, regardless of whether they have any past records of being considered risky or not.

This significantly speeds up the threat detection and prevention process by warning cyber-security professionals of potential security risks before even visiting the website. The utilization of predictive scoring can prove indispensable to the timely recognition of any potential threat and adopting protective measures.

Combined with different tools like Whois & Reverse Whois professionals can quickly identify the person or organization in whose name the offending domain has been registered or other domains connected with them. Using this information, the authorities can take the necessary steps to bring in the offenders & prevent any future threats.

Conclusion

The above use-case effectively demonstrates one of the varied uses to which the Domain Reputation API can be put. By providing cyber security professionals with an effective tool for quickly identifying risky domains, the Domain Reputation API takes an important step towards a safer web.