Malware Detection and Prevention Using Website Categorization API!

Posted on September 17, 2019

Cybercrime has taken on the mantle of being the biggest security threat to global information systems of the 21st century. With an increasing number of utilities, services and businesses connecting themselves to online platforms, the number of systems that are potentially under threat of becoming cybercrime targets is increasing by the day. Recent spates of cyber attacks such as the *WannaCry* and *NotPetya* have shown how easily important business processes and public utility systems can fall prey to such nefarious acts of digital felony. According to the latest estimates by *thebestvpn.com*, ransomware alone is slated to cost businesses to the tune of *$11.5 billion* in 2019. Furthermore, the costs of damage caused by cybercrime cannot be measured in terms of money alone. Cybercrime has far reaching consequences that go beyond mere monetary considerations. The loss of private data, breach of personal and privileged information as well as leak of sensitive records may snowball into global security risks. As a result, it becomes a matter of prime importance that such heinous attacks are nipped in the bud.

Malware Attacks: A Global Threat

One of the biggest causes of cyber security breaches stems from the presence of malware in the internal networks of an organization or business. Malware is a broad term that essentially covers any type of computer program that is designed to cause harm, inflict damage or compromise the security of a computer, or computer networks. The presence of malware in any computer system can lead to data leakages, system failures as well as denial of service. As every business of today conducts a major part of their operations and financial transactions online, the threat of malware attacks is fast becoming even more pronounced. Malware can often enter a system from simple acts such as visiting an insecure website, clicking unverified links or downloading shady software.

How Malware Threatens Businesses?

Malware includes any harmful software such as computer viruses, ransomware, worms or spyware that are designed to cause harm, steal information from or take control of your organization's internal computer systems. Malware can harm your business in any of the following ways:

- By taking control of your computer networks.
- Altering, damaging or deleting digital data.
- Steal proprietary information or customer data such as credit card information.
- Use your company network to spread misinformation about your business.
- Hold your business data hostage and demand monetary compensation for restoration of the same.

These are only some of the ways in which malware can harm your business. Due to the wide capability of malware to cause damage, it is still considered one of the biggest threats to the operation of digital networks in 2019. A large percentage of the malware that infects computers comes from malicious websites that inject these harmful programs into the systems of unsuspecting visitors. Therefore, the timely detection of websites that may contain malware such as viruses and spyware can help protect the internal systems of a company's network. This is exactly where our *Website Categorization API* can help you.

Using Website Categorization API To Guard Against Malware

When dealing with any online entity, the website is the single point of contact. In such a scenario it pays to know the category of the website you are dealing with before conducting operations or business transactions related to the website. Our *Website Categorization API* uses a combination of machine learning based AI- authentication as well as human inputs to categorize over 152 million websites. This allows any business to quickly and efficiently identify malicious sites and take the necessary actions to protect their company networks and data from potential infections. Using the *Website Categorization API* allows businesses to investigate potential threats at the URL level. The API analyzes the content of the target website and applies natural language processing to categorize the site based on over 25 supported categories. The efficacy of the *Website Categorization API* is complemented by our other product, the *Website Contacts & Categorization Database*. This product gives businesses access to website category as well as

contact details based on category and location in the form of a downloadable database. Website contact details and domain names segregated in terms of category and location enables businesses to expedite the process of identifying the offending website and start taking the required legal action against the owners of the malicious site. All the categorization data is made available in XML and JSON formats for easy integration and use by businesses. The *Website Categorization API* can also be used to automatically block access to website categories that violate the protocols of a business organization. For example, the API can be used to filter and prevent browsing of websites containing adult content, or the unauthorized use of social media in the workplace.

Conclusion

Malware continues to be a looming threat on the horizon for major businesses even today. The *Website Categorization API* provides a seamless way to categorize and detect malicious websites and acts as a shield against possible malware infection.