Detecting Cyber Threats with WhoisXmlApi

Posted on October 9, 2017

Predicting & proactively identifying cyber threats have become one of the biggest goals of cyber security analysts in today's time. Not only have the types of threats increased over the years but also the increase in the sheer velocity of them has become a matter of concern for security professionals. One of WhoisXmlApi's customers, IBM, a US based computer, IT consulting and world's biggest technology company is at the forefront in the cyber security space. With IBM X-Force Threat Intelligence they tap into serious data breaches, major cyber security attacks, and new cyber security vulnerabilities.

One of the key findings in the 2017 IBM X-Force Threat Intelligence Index is the dramatic growth in the volume of spam throughout 2016. Their team found that besides malicious attachments containing Trojans and Ransomware, spams containing malicious domains have increased drastically. They saw a new trend wherein spams enticed recipients to click on malicious websites, thereby allowing attackers to infiltrate their networks. With the growth in the domain name choices and new TLDs becoming easily & cheaply available this has become one of the choicest methods for spammers now.

To delve deeper into the trends and various TLDs that are being used as bait, IBM X-Force partnered with WhoisXmlApi for our comprehensive data. With more than a decade of historical Whois domain records at their disposal consisting of over 3 billion Whois records covering over thousands of TLDs, their security team began running high volume analysis, which helped them to identify questionable domains and connect various malicious entities together. Also with over 300 million active, real-time domain Whois records and with about 100,000 domains being added daily, their research team had all the data at their disposal to analyze various TLDs through their domain Registration data.

Looking at the various domain TLD registration trends, Whois information on their registrants and combining high-level analysis, with the Whois records from WhoisXmlApi, the IBM X-force team could predict & analyze the various TLDs that are being used by spammers for dubious activities. This information can help security analyst to keep an active eye on domains and help prevent cyber-crime beforehand.

You can check their detailed report on the same at https://securityintelligence.com/enticing-clicks-with-spam

This is just the start of a long and fruitful journey. With our comprehensive Whois products and services, government agencies & cyber security solution providers can trust the data provided by WhoisXmlApi

for threat prevention & investigation!