WHOIS Databases for Cybersecurity, Threat Intelligence, and Law Enforcement

Posted on February 14, 2019

Organizations that wish to keep their defenses up always have to look for new ways to combat dangerous cyber threats. This can be done by supporting traditional cybersecurity approach with threat intelligence and threat hunting efforts.

WHOIS databases can supplement these practices and become a source of valuable information not only for professionals in these areas but also for law enforcement specialists responsible for the apprehension and prosecution of cybercriminals. Let us see how.

Cybersecurity

In 2018, 50,000 security incidents were recorded, about 2,000 of which were from data breaches. Experts in the field of cybersecurity are hard-pressed in finding solutions so they can fight back against scammers and hackers whose proficiency in today's technology continues to increase.

Cybersecurity specialists can use **WHOIS databases** to retrieve specific domain details that can help them identify threats and prevent cyber attacks. For instance, obtaining the registration dates of a target website and comparing them with the length of time the entity claims to have been operating online, can help professionals detect an attempt of social engineering.

Threat Intelligence and Threat Hunting

Companies need to be proactive in their cybersecurity rather than reactive. This means that teams assigned to this task will need to identify and stop perpetrators even before they strike. That's why threat intelligence (TI) and threat hunting need to go hand in hand.

Access to **WHOIS databases** can give both TI professionals and threat hunters the insights they need to improve the discovery and containment of cyber menaces. WHOIS records allow these experts to proactively cross-examine domain information to identify malicious websites and links.

Law Enforcement

Criminals in the online world are becoming trickier to apprehend, and this has made prosecution a lot more difficult. WHOIS data is one way professionals can obtain leads, gather intuitive information and contribute to the success of investigation. It can also be used to build legal cases, track down and seize malevolent entities, and support liaising with courts and governmental authorities.

Cybersecurity, threat intelligence, and law enforcement teams can use **WHOIS databases** to get the information they need to successfully counteract the cyber threats of today.

Read our whitepaper WHOIS Databases: Business, Cybersecurity, and Many More Applications Explored to learn more about how WHOIS information can benefit you.