Security and WHOIS

Posted on January 17, 2019

The WHOIS system is a critical research and security component. Its information provides valuable background information that helps affirm proper network connectivity, domain source information, and contributes towards critical security and service continuity.

Cybersecurity professionals use WHOIS information to quickly assess and eliminate cyberthreats every day. To limit access to this information because of GDPR and other forthcoming privacy mandates would be to hamper this resource. Even with all of its flaws and a significant data accuracy challenge, WHOIS continues to prove to be a valuable forensic tool. Due to human nature and ease of registrations, researchers can quickly cross-compare domain registration information that can be associated with foreign nationals, cybercriminal groups, and other nefarious actors.

In some cases, researchers could correlate networks belonging to bad actors through inter-related domain registrations, common IP information, and other telling information that is gathered through the WHOIS system. Some of the largest organizations today rely heavily on domain registration data to add to their organizational security intelligence, to protect networks and applications, and secure data where it expected to be protected.

Email spam, malware, ransomware, virus distribution, insider threats, data leaks, advanced persistent threats, payloaded software, and many other types of threats can often be traced back to domain-sourced certificates and registrations. Therefore, protecting information proactively by using public information is the ultimate value of WHOIS to a security-minded organization.

The future of WHOIS information and security lies in maintaining an active, open environment and open database via which intelligence can be freely gathered and referenced. Every day, thousands of incidents can be and are protected by proactive investigative discoveries through this valuable system.

Want to know more about WHOIS and Security?

This free white paper - "What you should know about WHOIS and Security" delivers a comprehensive report about how Whois data is used in cyber-security and threat investigation.

Discover:

- What you should know about WHOIS and Security
- WHOIS, from the field
- The Future of WHOIS
- Security and WHOIS