WHOIS and the Health Industry

Posted on April 22, 2019



The standard of WHOIS is important to the health industry, especially when it is incorporated into a multi-faceted threat intelligence program. Before we get to that, it is clear in this day and age that many information technology organizations recognize that threat intelligence is a valuable tool, which is, in fact, essential to a strong security posture. However, throughout many industries one of the main issues out there is that the sheer volume of threat data combined with a gap in staff expertise stand to reduce the potential effectiveness of threat intelligence programs. Despite these challenges, threat intelligence programs that include sharing are a critical tool for healthcare organizations, especially with the current state of cybersecurity and the variety of threats of today. Everyone is trying to incorporate this, and here is how WHOIS can be a big part of that.

It's obvious that threat intelligence programs are relevant in every industry, but they are of particular importance in healthcare. There is a spectrum of sophisticated and evolving threats at the gate, on a constant basis. In the face of these growing threats, market sectors have had to mobilize as quickly as healthcare organizations. Healthcare hosts a significant payload of personal, identity, financial, and health data throughout countless subsectors, locations, and technology platforms. The value of this data can be leveraged to cause significant damage to individuals and organizations. When you add in the widespread and nefarious elements of black markets and the dark web with all the intent-filled damage that can be caused, the value becomes astronomical.

Awareness and Cybersecurity

Every organization has at least some cybersecurity in place and is (hopefully) trying to do better. Each organization is different in terms of the circumstances, business propositions, customers, and threat profiles. Focusing on that last part, it’s the threat profiles where cybersecurity starts. Each organization has its needs based on a combination of business goals and threats, which drives the nature of cybersecurity. You build a framework from the basics, bring in the mandated regulation-based security, and drive beyond that with a tailored approach. Hopefully, most organizations are already on their way to awareness through threat intelligence.

That’s the essence of threat intelligence – awareness, preparedness, and knowing, because otherwise, you might end up groping in the dark. If you are trying to build virtual walls and

obstacles to protect yourself against everybody, there's simply no way you can do that. The threats are too many, too constant, and too rapid to effectively protect against on a continual basis. Information is the currency behind everything and you need information on who to protect against, when and how.

Enter WHOIS

The only intelligence that is going to help you and your organization is actionable intelligence. This means that subscribing to threat intelligence information is a tremendous foundation to a program. But this activity only becomes successful when the information is actionable and it is combined with specific actions.

Somewhere within the systems across the technology environment lie pieces of traceable information. In logs, event viewers, and other informational resources, both silent and overt threats touch systems within and on the perimeter of technology systems.

One way to actively integrate information is to explore information from WHOIS. Tracing log events, attack information, correlating public information, and many other activities gain relevance when the ability to research information directly is added to a threat intelligence program. Within WHOIS, one can find the source of information, the destination for suspicious traffic, detect increases in activity from unverified networks, and much more. Implementing a tool such as WHOISXMLAPI allows security teams to implement thorough research by using threat intelligence as a source and information that is specific to the organization.

In any organization, reducing the attack surface of digital operations is a must-do. Improving response and reducing threats are important components of attack surface reduction. When combined with specific research and awareness of particular threats against the organization, knowledge and awareness of ongoing threats make an organization better secured, especially when the information used implements WHOIS, a valuable resource in the war against cyberthreats.