As a nation we are hemorrhaging; our government, military, corporate, and financial institutions are being robbed of their intellectual property and critical resources continuously due to cyber attacks. Individual banks measure their losses in the millions per month. Commercial corporations watch their intellectual property stream overseas. Our government, military, and critical infrastructures, the backbone of what keeps the United States functioning and safe, are breached regularly, sensitive information is accessed, and we are challenged to stop the majority of these attacks. Why? One of the key issues has been our inability to attribute the attacks, attribute the source and intent of the threats. Without attribution, we struggle to develop adequate defenses to match the threats as they evolve. Without attribution, we cannot execute effective Courses of Action (COAs) against cyber threats or establish effective foreign policies governing responses to such threats.

This is not new information. The government and intelligence community have been aggressively looking for attribution solutions since the CNCI was signed by President Bush in early 2008. It was a top priority then and remains one of the top cyber priorities in 2010. Over the years, the security industry has struggled to develop the necessary capabilities and methodologies that advance attribution solutions.

Until today.

HBGary's FingerPrint, a freeware tool released today, represents a breakthrough in the development of a viable attribution solution. It enables the clustering of previously unrelated malware specimens, which in turn enables the individual pieces of intelligence associated with each specimen to be clustered and analyzed collectively. The tool exposes key identifying markings that are very difficult to hide or fake. For example, Fingerprint takes advantage of the fact that an author leaves behind his markers in the thing that he writes, the malware. Like styles used by authors or artists, Malware creators have specific styles, use specific tools, and develop in specific environments in specific ways. All of these markers are identifiable, even fingerprintable to an author or set of authors. Previously unassociated malware shows tight clustering based on these threat markers. The FingerPrint tool extracts these variables from the malware and puts them into a standard, readable format allowing for rapid association and correlation of malware that was created in the same development environment by the same authors. The results are significant -- providing a crucial starting point for connecting malware events to authors and providing a better understanding of the evolution of threat capabilities and intent.

Aaron Barr

CEO

HBGary Federal Inc.