Kroll Cyber Intelligence

Experts

Kroll experts have the ability to access the deep/dark web. In doing so, these specialized Kroll experts are able to provide a sophisticated analysis to companies or to individuals demonstrating how and where they may be vulnerable. Kroll provides a written report ranging from overall company exposure to more specified threats that could affect the critical infrastructure of the company or key individuals.

Kroll collects factual and credible information to identify individuals, instances and/or data over a period of time whether it be in the past, present or future. The calculated research of the cyber threat intelligence, coupled with the experience of the Kroll experts, creates informed proactive decisions about cyber threats to organizations and individuals. The strategic analysis of this information will further tactical decision making. Also, the outcome of the gathered intelligence will influence the root of the action needed to continue the pursuit of the appropriate response.

There are many benefits this proprietary information can provide. This information will help a company or individual to learn how to prevent future vulnerabilities and damages. It can provide defense against attacks. It will increase awareness in the scope and volume of fraud being perpetrated and facilitated via the internet and it could assist with the identification of individuals responsible for cyber-attacks.

Keith Wojcieszek is an Associate Managing Director in Kroll's Cyber Security and Investigations practice, based in Washington, D.C. Keith joined Kroll from the United States Secret Service, where he served with distinction for 15 years. Keith is a strategic problem-solver, who draws on not only his wealth of advanced technical expertise, but also his extensive experience working with diverse international stakeholders on complex transnational investigations and initiatives.

Most recently, Keith led the USSS Cyber Intelligence Section, Criminal Investigation Division, where he managed the agency's national response to cyber investigative initiatives focused on protecting the financial infrastructure of the United States. In this role, Keith also coordinated complex international investigations that targeted transnational organized crime networks with an emphasis on cyber and information security. Under Keith's leadership, a number of these cases resulted in the apprehension of highly sophisticated cyber criminals who collectively were responsible for causing over $1 billion in financial losses.

Previously, Keith served with the USSS Cyber Intelligence Section, leading top-priority initiatives and multi-agency efforts, international and domestic, to apprehend high-value targets of cyber investigations across the world. These cases resulted in the arrest of several criminals who caused financial losses of more than $800 million. During this time, Keith also headed the Cyber Incident Operations Center, which had responsibility for coordinating the investigation and response to attacks on the financial infrastructure of the United States that inflicted hundreds of millions of dollars of losses. The investigations spearheaded by this group resulted in 19 individuals being taken into custody and prosecuted.

Earlier in his career, Keith led several domestic and global investigations working with the U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS) and Office of International Affairs (OIA). From 2004-2010, Keith managed the Electronic Crimes Task Force in support

of all electronic crimes investigations, computer forensic examinations, and cell phone data extraction in the Louisville Field Office District. In this role, he also established the operation of a forensic laboratory; provided expert testimony in multiple state and federal cases; and coordinated training for USSS agents, local law enforcement, and industry representatives.

Cyber Intelligence/Criminal Intelligence

Cyber Intelligence can be defined as the collection and development of factual and credible information to identify individuals, instances and/or data over a period of time whether it be the past, present or future. The calculated research of cyber threat intelligence combined with the experience of Kroll experts generates informed proactive decisions about cyber threats to organizations and individuals. The strategic analysis of this information furthers tactical decision making. The outcome of the gathered intelligence influences the root of the action needed to pursue an appropriate response.

The definition of cyber intelligence can lend to be a diverse area of study and can stretch across different landscapes of use. There are several entities interested in the wealth of information that can be gathered from the sources most familiar with the dark web.

Private industry is involved in many aspects of the dark web for several reasons. The dark web can lead private industry to:

- Provide defense against cyber attacks
- Learn how to prevent future vulnerabilities and damages by seeking current trends and information
- Gather information to increase the awareness in the scope and volume of fraud being perpetrated and facilitated via the Internet
- Assist with the identification of individuals responsible for cyber-attacks

Government agencies are at the forefront when it comes to collecting intelligence through several methods that cannot be acquired by anyone else. Through the use of the court systems, law enforcement can utilize subpoenas, search warrants, interview suspects, interrogations, debriefings and confidential informants to provide them insight to the criminal world. They gather and use the information for:

- Attribution
- Investigations into criminal breaches and cyber attacks
- Notification to private industry
- Fighting the war on cyber

Through the consistent growth of technology and the development of advances in cyber security, academia has become a key component in educating and assisting law enforcement in investigating and fighting the cyber war. The tools developed from the academic world has given their partners an advantage in examining the capabilities of the offenders. In addition to the tools developed, academia needs cyber intelligence to:

- Help educate the next generation of professionals
- Assist government in research and development
- Provide research that would help fight the war on cyber

Cyber intelligence is utilized in many ways and can provide insight to what is unknown. When studying and researching the information, we tend to forget that not only the good guys are focusing on the results intelligence gathering will provide. The criminal and criminal networks want the intelligence to help develop their networks and provide them an edge over law enforcement to ensure they can maintain their enterprise. For the same reasons other entities want cyber intelligence, so do criminals. Criminal networks need to establish a baseline for their networks to run smoothly. With the intelligence gathered, they can incorporate an operation security (OPSEC) environment that will protect them against law enforcement and other criminal networks that may want to cause a disruption of service. In addition to OPSEC, criminals are also utilizing intelligence to gather the following:

- Personally Identifiable Information – PII
- Personal Health information – PHI
- Financial Information
- Intellectual property/ trade secrets

While discussing why everyone wants all this intelligence, the next question is how to obtain it. Law enforcement is unique because they are able to use the power of the courts to obtain intelligence that most cannot acquire. But in addition to the use of the courts, law enforcement and all the other groups that search for the wealth of intelligence utilize the dark web to gather this information. The dark web is defined as a network built on top of or in conjunction with another network that is accessible with specific software, configurations, or authorizations and often uses non-standard communication portals and ports. [1] The dark web consist of areas of the internet that are not indexed and searchable by any search engine.

The criminal who focuses on the use of the dark web and cyber intelligence is a very sophisticated individual with advanced knowledge in today's technology. The individual utilizes his/her expertise in stealing data at rest, in transit, and even encrypted data from multiple areas connected to the internet. This expertise they hold sets them apart from most other criminals because of several factors. These include:

- Maintaining a common language
- Professional relationships
- Operational Security
- Constantly evolving infrastructure

The criminal groups and networks that are responsible for the large part of the breaches maintain a very high standard of OPSEC entangled with the expertise of technological advances. They are consistently making it increasingly difficult to locate and identify who they are and what vectors they are utilizing to carry out a malicious attack.

[1] https://en.wikipedia.org/wiki/Dark_web - November 16, 2017