Public Source Information - Untapped Power or a Dangerous Game by Eccuni

Article published on December 15th 2011 | Internet

For a while now, law enforcements have asked for help from the public on recognizing and tracking suspects who are charged with crimes. They used the method of putting up WANTED signs and as more criminals appeared, a television shows was made like "Cops". In today's time, law enforcements make use of the public's aid nowadays. They receive useful information and whereabouts from the public when leads weren't acquired through the investigation of the law enforcements. Even though the public has vast resources and great knowledge in their hands compared the law enforcements, the method crowd sourcing is insufficient. Yes, I am discussing about the cybercrime world.

Even though the investigators who have undergone computer forensics training of the law enforcement are good, but cyber investigations are what the public knows best. The public is full of experienced hackers, researchers, security professionals and private investigators. They have unlimited access to security mailings, investigation resources online and other more. Even though you can not expect the assists from public on helping the law enforcements, you can however expect them assisting on connecting the links between activities and malicious websites. They can also obtain information of the cybercriminal's cyber names and other nicknames used before. Other investigations of cybercrimes are available for the public in the internet in open source resource pages. Collecting information can be compared on building a jigsaw puzzle which even one piece of evidence can make a difference of finding out the identity of the criminal or arrive at a dead-end.

The idea was even been attempted in September 2003. Axel Gembe is a German hacker who hacked into the network of the famous Valve, a game developing company. He stole source codes of the game "Half Life 2" which at that time was still under development. He also stole other intellectual related property. The co-founder and CEO of Valve, Gabe Newell, asked help from the law enforcements but he also asked help from his loyal fans in order to identify the hacker. He posted in the forums of the game a message asking the community to give information or leads. Even though the community didn't really direct to a desirable breakthrough of the investigation of finding the culprit, the hacker himself confronted Newell of his plan of going to jail.

A recent and applicable example to the skills of the public in cybercrime search would be the Sony breach. Many of misinformation was given and unbelievable claims were made from the underground. Claims were made that information on the objects stolen were given, who did the crime and the chat logs of the hacker. Several days after, the Wired's blog of security "Threat level" posts that the cyber detectives was searching for the PlayStation hackers and also they posted an uncensored chat log of the hackers. They also identified the identities of the hackers who hacked the Sony Company. One of the members has a nickname of "Trixter". Another identity was found and his nickname is "SKFU".

Examples are also found for the other camp or the cybercriminals. Fraudsters usually out their member of the fraudster's communities who trick or deceive with each other. They post the traitor's real identity in public, which includes their name, their address and their pictures. There is a group which is called The "Anonymous". They also serve as an example. In May, a member decided to overthrow the leader in order to declare himself as the leader. The member's name is "Ryan" and started a DDoS attack on the resources the group uses. The group immediately split into two, "Ryan" had domains that were used by "Anonymous" in his grasp. The opposing group gain control on Ryan's domain. They used it to post Ryan's information regarding his identity in real life. They

posted his real name, mobile number, address, aliases, host name, E-mail address, Paypal accounts and Skype accounts. Due to the attempted revolution of "Ryan", members were forced to share his private information about his identity. Members searched for all of the information concerning his identity in real life.

Even information sharing in an on-going case has disadvantages also. Law enforcements should only use this procedure when there is not hope or they are stuck. Even though they have undergone computer forensic courses, computer forensics can sometimes be stuck. The public can be a great help in manhunts or investigations. The "public" can even acquire domains, e-mail addresses, IP addresses, aliases and other useful information that can greatly help in the investigations. They can use that information to acquire more leads and evidences. This is similar to the WANTED posters law enforcements put up. They give information to the public about the appearance of the suspect and the place where they were last seen and ask the public to share any leads they might have.

Due to the large effort of the community of the cyber investigations, it would be a hard to manage all the information that the public might pass on. The bigger the community though, the bigger the change of acquiring good leads but it also means that the criminal or a accomplice might have access to the investigation and able to change the data or submit a fake information. The law enforcements should do a proper control in order for the criminal not know the location or distance of the pursuers. The criminal may also cover the tracks he left behind on the internet. Some information online are often misleading though. They could track the wrong person with the name or information. They could let the investigation go off-track or they could sabotage the case. During an investigation, the law enforcements need to go through a process in order to gain access to the suspect's E-mail address and the contents. The public aren't so careful like the law enforcements. Actions like that can really cause heavy consequences.

There are groups and organizations in agencies of the law enforcement and other security companies discussing cybercriminal activities. The discussions aren't similar to the WANTED posters that the posted of criminals. One method the agencies is crowd sourcing investigations. They could really control the unlimited power of the internet and the people in it. The power is still untouched. In order to use it, law enforcement companies should really share the information retrieved but not to the security industry alone but also to the whole world.

Article Source:
http://www.articleside.com/internet-articles/public-source-information-untapped-power-or-a-dangerous-game.htm - Article Side

Eccuni - About Author:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in computer forensics.

More information about EC-Council is available at www.eccouncil.org, a computer forensics training, a computer forensic courses, a computer forensics

Article Keywords:
computer forensics, computer forensic course, computer forensics training, Source Information,

Untapped Power, Dangerous Game, WANTED, Cops, law enforcements, cybercrime, security professionals, Threat level, Trixter, DDoS attack, Anonymous, fraudster, Sk

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!