Cybercrime y Cyber Cops en la Deep Web

Univ. Elfy J. Lazo Monroy
Universidad Mayor de San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Informática
elfyjho@hotmail.com

RESUMEN
Este artículo intenta dar una visión de la Deep Web, desde la perspectiva de la búsqueda incansable de los autores y colaboradores en los diferentes crímenes dentro de la Deep Web

Palabras Clave
Deep Web, Cyber Crime, Cyber Cops, The Onion Router, Seguridad Web, Darknet, Free Hosting.

1. INTRODUCCIÓN
En los últimos tiempos, el resplandor ha brillado en el misterioso mundo oscuro de la Deep Web, ese territorio en línea estimada es mucho más grande que la internet ordinaria, la mayoría de nosotros el accede a diario desde la comodidad de nuestros ordenadores y smartphones utilizando navegadores como Google, Yahoo! y Safari.

La Deep Web, donde la droga, pornógrafos, asesinos y los terroristas han podido hacer negocios impunemente durante mucho tiempo, ahora gracias a esfuerzos internacionales de Cyber Cops intentan encontrar la las personas responsables de dichos crímenes día a día.

2. CYBERCRIMEN
La ciberdelincuencia o Cyber Crime engloba cualquier acto criminal que trata con las computadoras y redes (llamado hacking). Además, el crimen cibernético también incluye los delitos tradicionales realizados a través de Internet. Por ejemplo; los crímenes de odio, el telemarketing, el fraude en Internet, el robo de identidad, y de la cuenta de tarjeta de crédito robos son considerados como delitos cibernéticos cuando las actividades ilegales se cometen mediante el uso de una computadora y el Internet.

Sabiendo esto podemos decir que el Cybercrime que se encuentra en la Deep Web es mucho peor, la ciberdelincuencia es un área de rápido crecimiento. Cada vez son más los delincuentes que aprovechan la rapidez, la comodidad y el anonimato de la Internet para cometer una amplia gama de actividades delictivas que no conocen fronteras, ya sea físico o virtual.

Estos crímenes se pueden dividir en tres grandes áreas:

* Los ataques contra los ordenadores y programas informáticos, por ejemplo, botnets, malware e intrusiones de red;
* Los delitos financieros, como el fraude en línea, la penetración de los servicios financieros en línea y phishing;
* Abuso, especialmente de los jóvenes y niños o 'sexploitation', Narcotráfico y Trafico ilegal

2.1 Ataques contra los ordenadores
Los ataques contra los ordenadores y programas informáticos, varios ejemplos de estos son los botnets, malware e intrusiones de red. Una botnet es una red de ordenadores que son controlados de forma remota por una o más personas, llamadas bot-pastores. Los equipos de la red de bots, denominados nodos o zombies, pueden ser ordenadores ordinarios que están siempre en las conexiones de banda ancha (ADSL), en hogares y oficinas en todo el mundo

La Deep Web no es una red separada, y ha sido estimada como 500 veces más grande que la World Wide Web común.

Pero para encontrar uno de los sitios web secretos del darknet, los usuarios ya deben conocer su dirección web URL exacta, y que a menudo cambia por la forma en que funciona el sistema. La red disfraza identidad de los usuarios por el rebote al azar entre diferentes servidores Tor, o nodos.

Las víctimas van desde empresas en peligro de ataques cibernéticos donde los delincuentes cerrarán sus operaciones a menos que paguen sumas exorbitantes, ya que pueden infectar sus máquinas con software viral que congela su ordenador y exige una cuota de liberación de $ 1000.

2.2 Delitos Financieros y Fraudes
Un ejemplo de fraude Online es el phishing, una modalidad de estafa con el objetivo de intentar obtener los datos de un usuario, claves, cuentas bancarias, números de tarjeta de crédito, identidades, "todos los datos posibles" para luego ser usados de forma fraudulenta. También existen servicios de Hacking donde podemos encontrar personas dispuestas a esto llegando a acuerdos monetarios e intercambio de información.

2.3 Abuso, Tráfico y Narcotráfico
La mayoría de los usuarios que han ingresado a Deep Web incluyendo empresas, periodistas y la propia policía disfrutan del anonimato en línea que proporciona para los propósitos legítimos, pero la angustia de los usuarios son de repente enfrentarse a horrores ocultos de la Internet.

Hace un tiempo atrás, el delito cibernético fue cometido principalmente por individuos o pequeños grupos. Hoy en día, las organizaciones criminales que trabajan con profesionales de la tecnología para cometer delitos informáticos, a menudo para financiar otras actividades ilegales. El objeto de muchas de estas redes de ciberdelincuentes es reunir a personas de todo el mundo en tiempo real para cometer crímenes en una escala sin precedentes.

Varios de los crímenes más atroces están relacionados con seres humanos, pornografía infantil, tráfico de órganos, páginas con

experimentos humanos, venta de todo tipo de drogas, venta de armas.

3. CYBER COPS

El avance tecnológico da paso a nuevas tendencias en los delitos cibernéticos nuevas formas de que los criminales permanezcan en el anonimato están surgiendo todo el tiempo, con costos para la economía mundial que se ejecutan en miles de millones de dólares.

Estamos a merced de organizaciones criminales que trabajan con profesionales de la tecnología de mente criminal para cometer delitos informáticos atroces.

Las organizaciones criminales utilizan más a Internet para facilitar sus actividades y maximizar sus ganancias en el menor tiempo. Los delitos en sí no son necesariamente nuevos tales como el robo, el fraude, el juego ilegal, la venta de medicamentos falsos, pero están evolucionando en línea con las oportunidades que se presentan y por lo tanto cada vez más generalizado y perjudicial.

Dado que la Deep Web es el centro de delincuencia virtual donde nos topamos con cosas realmente escalofriantes, también encontramos gente comprometida con la justicia y cumplimiento de los Derechos Humanos, existen varias organizaciones que día a día luchan por encontrar a los autores físicos e intelectuales de la amplia gama de crímenes que se cometen mediante la Red Profunda (Deep Web).

3.1 INTERPOL

INTERPOL se ha comprometido a convertirse en un órgano de coordinación mundial en la detección y prevención de crímenes digitales a través de su Complejo Mundial de INTERPOL para la Innovación (IGCI), en Singapur.

Un componente clave de este nuevo centro de investigación y desarrollo de vanguardia es el Centro Transnacional digital INTERPOL. Este nuevo centro ofrece una investigación proactiva en áreas nuevas y últimas técnicas de formación, y coordina las operaciones en el campo.

3.2 FBI

Esta es la organización más grande que se encarga de investigar los delitos de alta tecnología, incluido el terrorismo basado en la cibernética, el espionaje, las intrusiones informáticas, y fraude cibernético. Para permanecer en el frente de las tendencias actuales y emergentes, se reúnen y comparten información e inteligencia con los socios del sector público y privado en todo el mundo.

Los que están en la industria de la seguridad cibernética que están tratando de proteger a los que ahora se enfrentan a un gran problema: determinar exactamente quién es el perpetrador es cuando ocurre un ataque. Los delincuentes aprenden de hacktivistas; agentes cyberintelligence recoger sugerencias de los delincuentes, y en el fondo, los estrategas militares están poniendo a prueba las defensas enemigas potenciales en todo el mundo. Esto significa que el mundo virtual está lleno de subterfugios, el malware y el engaño.

Un sitio web de venta de narcóticos y la pornografía extrema, sólo existía en la Web Profunda hasta que gracias al FBI detuvieron a uno de sus presuntos fundadores, de 29 años de edad, William Ross Ulbricht, más conocido en el negocio como "temible pirata Roberts." Para ver el "eBay de las drogas", como se denominó dicha página, el visitante tendría que entrar en la web profunda a través de la red TOR, un sistema gratuito diseñado para evitar que el seguimiento de la actividad web y una herramienta importante para aquellos que sufren de persecución política.

La existencia de complejos sistemas de comunicación más allá de la Web de la superficie hace que sea difícil de comprender exactamente lo que está pasando en el mundo de la Deep Web. A menudo es difícil para las fuerzas del orden y los analistas poder identificar dónde una actividad termina y el siguiente comienza.

4. Conclusiones

La deep web es el lugar ideal para el cybercrimen y los esfuerzos de los cyber cops para deternerlos o mermarlos cada vez son mas insuficiente al paracer es imposible pues cada vez que encuentran una pagina y la cierran al mes aparecen nuevas.

Con la aparicion de nuevos y mas complejos sistemas de comunicacion la tarea de localizarlos para los cybercops es titanica pues la navegacion en la deep web es de link en link.

5. REFERENCES

[1] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

[2] http://article.wn.com/view/2013/10/23/Cyber_cops_probe_the_deep_web/

[3] http://blog.trendmicro.com/trendlabs-security-intelligence/cybercrime-in-the-deepweb

[4] GLENNY MISHA (NWT)

http://www.nytimes.com/2013/11/28/opinion/cyber-subterfuge.html?pagewanted=all&_r=0