ANONYMOUS: Movimiento altermundista o ciberdelincuente

Casabón Martínez Iván Darío
sis_icasabon@hotmail.com
Universidad Piloto de Colombia

Resumen— La organización hacktivista se ha hecho presente en todo el mundo después de tomar acciones que han sido señaladas como delincuencia informática y cuya denominación ha sido objeto de calificaciones alusivas a terroristas cibernéticos, Sin embargo, su acción nada tiene que ver con estos calificativos que cómodamente y sin ningún tipo de análisis se les asignan.Por ello se pone a consideración todo lo que gira alrededor de esta organización y su manera de actuar.

Índice de Términos—Activismo, Delito, Organización, globalización, Hackers.

I. INTRODUCCIÓN

Para comprender un poco acerca del tema a analizar, se debe definir activismo, cuyo concepto en particular busca efectuar un cambio de índole social, político o religioso, usualmente dirigido a una postura popular. Es una resistencia a aquellas demostraciones que van en contra de una iniciativa para el pueblo y por el pueblo. Pero el complemento que le da sentido a esta definición es lo que en el mundo de la informática se conoce como hacking, que en términos generales es una actividad de apropiación social o comunitaria de las tecnologías que una comunidad de entusiastas programadores y apasionados por la seguridad informática lo utilizan para promover conocimiento y apoyo a los procesos de cambio para volver los sistemas más seguros.

Cuando un Hacker hace uso de sus conocimientos como forma de protesta, se le denomina hacktivista, por lo que es un tipo de desobediencia civil y/o digital. Esto implica que un pirata informático no haga hacktivismo y tampoco un hacktivista es un delincuente. Cabe resaltar que los hacktivistas no siempre comparten las mismas visiones ni formas de acción, incluso, pueden llegar a contraponerse unos con otros.

Desde la década pasada, ha habido un acercamiento entre redes de activistas altermundistas y jóvenes que dominan la tecnología, el internet y el software libre. Esta concomitancia ha contribuido con el auge del Movimiento Altermundista (MA).

El MA se caracteriza por su heterogeneidad, ya que en su interior confluyen actores, organizaciones y movimientos de diferentes corrientes, ideas, demandas, formas de acción, etcétera; que incluso llegan a contraponerse unos con otros. Es así que se puede encontrar movimientos como la Coalición Jubileo 2000 ligado a la iglesia católica, movimientos pacifistas u otros que usan abiertamente la violencia contra símbolos capitalistas (FMI, OMC, BM, etc.), como el denominado “Black Block”, entre muchos otros.

Estas alianzas se dan no sólo a nivel local, sino global. En consecuencia, hay una descentralización, falta de jerarquía, no hay un líder en común y destaca la ausencia de intermediarios. Los hacktivistas también han sido participes de este movimiento y presentan las características de un MA. Es por ello que, como el título del presente artículo lo indica, seha calificarlo de Altermundista. Para ejemplificar un poco estos aspectos se dará una breve descripción sobre Anonymous.

II. "SOMOS UNA LEGIÓN, NO PERDONAMOS, NO OLVIDAMOS, ESPÉRANOS"

A. Quienes son

Son un movimiento internacional de ciberactivistas, que en su interior cuentan con un indeterminado número de miembros que no revelan su identidad. Su característica es el anonimato, he ahí una de las razones de su nombre. "Anonymous, que ha sido definida por uno de sus miembros en España como una organización que no existe y que por definición es una (des)organización". En la red social de Facebook se presentan con el nombre de Anonymous Link y mencionan que evidentemente ese no es su nombre. "Uso este para mantener mi anonimato en la red cuando me relaciono con el activismo y el ciberactivismo a través de Anonymous"

La simbología que utilizan les ha permitido mantener el anonimato. Pero al mismo tiempo contribuye a que causen mayor impacto mediático, los hacen más visibles. Una de ellas es la máscara que representa a GuyFawkes y que utiliza el revolucionario *V* de la novela *V for Vendetta* que inspiró una película bajo el mismo título. También, entre las banderas con las que cuentan, destaca una en la que se muestra el cuerpo de una persona vestida de traje y en lugar de la cabeza aparece un signo de interrogación.

Figura No 1. Simbología Anonymous

Anonymous funciona en realidad según una estructura digital que, como el agua, se escapa entre los dedos. Por supuesto, parece que hay "militantes" más comprometidos que otros, "hackers" que crean el programa inicial con el que se va a atacar a una institución, pero, a partir de ese primer momento, ese programa se difunde por blogs y redes sociales de una forma tan amplia y anónima que, llegar al punto del programador inicial, siempre ha sido un problema irresoluble.

B. Forma de lucha

Anonymous ha generado códigos e identidades. Se fundamentan en una lucha por la transparencia, la libertad de expresión y los derechos humanos. Así lo dan cuenta números videos subidos al sitio web"Youtube" por el propio movimiento y los diversos pronunciamientos que han hecho: "estamos creando una plataforma de base estable en la que los movimientos y los defensores de causas humanitarias pueden discutir los métodos legales de protesta y difusión de la información. Desde hace varios años "WhyWeProtest" ha servido como el centro mundial de protesta contra la censura y violaciones de los derechos humanos"[1].

La forma en protestan se basa principalmente en ataques de "denegación de servicios distribuidos" (DDOS). Estos consisten en lanzar numerosas peticiones a un servidor que aloja una página web, es decir, saturan los servidores y cuando estos no soportan la carga, quedan suspendidos.

Pero la acción de Anonymous no sólo se queda en el ciberespacio, ya que ahí coordinan y estructuran movimientos y protestas que posteriormente trasladan del mundo virtual al real. Por ello, Anonymous se vale de la protesta pacífica tanto en la calle como en la red, a través de manifestaciones, ataques DDOS y otro tipo de operaciones. Anonymous se ha convertido en un movimiento que se ha extendido por todo el globo y que ha apoyado varias iniciativas de otros grupos que perseguían los mismos principios e ideales.

Ante todo esto, Anonymous se presenta como una forma de protesta alternativa que apela a la indignación social. En su acción pone en evidencia la fragilidad no sólo de un país, sino del mundo entero. El hecho de que usen los canales no institucionales para protestar, no los convierte en delincuentes. Ellos han usado la red como un

escenario para hacer política, para la difusión de la información, para la organización y la acción.

Han logrado construir espacios comunes y han tendido puentes con otros activistas y organizaciones. “Los avances tecnológicos anuncian una época en que la razón y la compasión en verdad pueden cruzar las fronteras nacionales, trascienden las fronteras imaginarias de la orientación política y religiosa, y llenar los vacíos generacionales.” [2].

C. Ataques, Denegación de servicios distribuidos (DDOS).

*¿Se considera un ataque? :*Es un **ataque** porque se trata de una ofensiva dirigida en contra de un sitio web. El arma puede ir desde un simple clic para actualizar la página hasta un sofisticado software que automatiza el envío el envío de paquetes de red hacia el enemigo.
*¿Porqué denegación de servicio? :*Como consecuencia del ataque el sitio web deja de conceder sus servicios de forma normal (la página no carga o es lenta en exceso, por ejemplo). Este impedimento puede causar pérdidas millonarias en algunos casos. La duración del ataque puede ir de algunos minutos a varias semanas, según la pericia de los administradores del sitio web para detenerlo.de red hacia el enemigo.
*¿Por qué distribuido? :*Porque hay una multitud de atacantes repartidos por toda la red, donde la suma de fuerzas puede colapsar el acceso al sitio web del enemigo en turno.

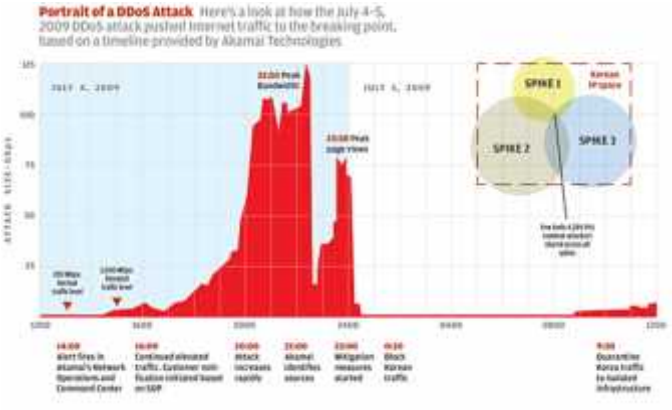
Normalmente son personas las que participan por decisión propia en el ataque, como en las operaciones organizadas por Anonymous. En otros casos, se suele hablar debotnets, o redes de computadoras controladas de forma remota mediante un malware, ofrecidas por mercenarios de la red al precio del mejor postor. Ambas prácticas son cada vez más comunes. [3]

D. ¿Qué NO es un ataque DDOS?

Este tipo de ataques no representan un hackeo tradicional, es decir, no hay intrusión o vulneración de una computadora por acceso no autorizado. El agresor no tiene acceso a los archivos o información personal contenida en el servidor o computadora objetivo del ataque.

E. Impacto del ataque

En la siguiente imagen de **Akamai**, puede verse claramente la forma en que el tráfico impacta en los servidores, lo que sucede cuando se toman las medidas de bloqueo y mitigación y cuando finaliza el ataque.



Una vez conocido el impacto de los ataques de DDoS es necesario conocer los controles disponibles y que se pueden implementar para contrarrestar este tipo de ataques.

El grupo Anonymous generalmente utiliza un software para este tipo de ataques **LOIC** (LowOrbit Ion Cannon). La idea es que permita participar en estos ataques incluso si no se tiene conocimientos sobre cómo hackear

F. Nueva arma.

La nueva herramienta, llamada #RefRef, usará JavaScript y SQL para atacar sitios y aprovechar un tipo de vulnerabilidad en los servidores para usar su propio poder de procesamiento contra ellos mismos. RefRef podrá ser usado desde cualquier dispositivo que soporte Javascript, incluyendo teléfonos, o al menos ese es el plan[4].

Evidentemente los ataques de DDoS seguirán entre todos los usuarios y las organizaciones por mucho tiempo más y es hora de comenzar a pensar en si la organización ya se encuentra preparada para

afrontarlos, porque el ciberterrorismo y la ciberguerra ya están entre nosotros y deberemos decidir de qué lado jugar.

III. ANONYMOUS EN COLOMBIA

En Colombia la recordada Ley Lleras, intento de regulación del ciberespacio que, en abril de 2011, desencadenó el bloqueo de la página del Ministerio del Interior, ataque que se convirtió en la primera manifestación de Anonymous en ese país.

En los últimos tres años todos los intentos de regulación de Internet, que han promovido los gobiernos del mundo, han tenido algo que ver con esta "des-organización" que, como el colectivo de hackers afirma, no tiene un centro, carece de voceros y no puede identificarse.

A. ¿CloudFlare?

Se trata de un servicio que gracias a su red trata de actuar como intermediario entre Internet y la web para balancear carga, implementar su propio caché de información, filtrar ataques web, gestionar estadísticas y bloqueos de clientes, etc. Aparte de las ventajas que proporciona en cuanto a rendimiento, ahorro de carga, seguridad y control, hay un punto que llama la atención.

Si por cualquier motivo el sitio web original deja de responder, cuando un cliente intente visitarCloudFlare mostrará de forma casi transparente al usuario la última copia del sitio de la que disponga. Y se dice casi transparente, porque en la parte superior mostrará un pequeño aviso informando de la situación.

Cuando el sitio original vuelva a responder se volverá a servir a los nuevos clientes. Es una opción realmente interesante de cara a proteger de ataques de denegación de servicio, ya que el contenido seguirá siendo accesible por los clientes, incluidos bots de buscadores, que no se penalizarán.[5]

IV. CONCLUSIONES

1. Después de haber realizado el trabajo se ha comprendido que los Anonymous realmente son un grupo de personas que luchan por sus derechos o sus ideales, aunque se apunten al alguno indeseado que aprovechan para realizar actos delictivos usando el nombre de Anonymous.

2. Es por esto por lo que la gente piensa al escuchar hablar de Anonymous que es una organización de delincuentes, a esta forma de pensar contribuyen los diferentes gobiernos contra los que Anonymous lucha, pero ni mucho menos es así, ya que en ocasiones han realizado transferencia de cuentas de diferentes gobiernos pero no para su beneficio propio sino con el objetivo de ayudar a los más necesitados.

3. Un ataque DOS es bastante efectivo al momento de causar algún daño a algún sistema y es especialmente molesto y efectivo si hay mucha gente detrás del ataque involucrada… estos ataques han tenido tanto éxito que se han llegado a posponer eventos importantes en países que quieren imponer leyes en contra de la libre expresión y relacionado con la web.

4. La complejidad de los ataques DDoS requiere de una mezcla de metodologías de mitigación. La manera más eficaz de hacer frente a los ataques multi-vectoriales es aprovechar los appliances dedicados in situ. Los firewalls, así como los Sistemas de Prevención de Intrusiones (IPS), se convierten en piezas fundamentales en la estrategia de mitigación y los dispositivos de seguridad DDoS ofrecen una capa adicional de defensa para identificar y bloquear amenazas en tiempo real.

5. Aumentar la capacidad de la industria para compartir información ayudaría a elevar la capacidad de las empresas para hacer frente a las actividades DDoS y llevaría en su conjunto a un nivel superior de preparación ante los mismos. [6]

REFERENCIAS

[1] Invitado, "Anonymous: un hacktivismoaltermundista", (2011, 24 Octubre), [Online]. Available:http://www.escrutinio.com.mx/revista/internacional/77/anonymous-un-hacktivismo-altermundista.html#_ftn7

[2] Staff_RR, "Anonymous¿Heroes o villanos? (2012, 28 Marzo)[Online]. Available:http://revistaradical.mx/?p=827

[3] Lazalde Alan, "*DDOS*. Que es y como se ve este ataque informático"(2013, 29 Abril)[Online]. Available:http://www.eldiario.es/turing/DDoS-seguridad-Anonymous-botnet_0_125638394.html

[4] Gomez Treviño Joel, "Hackivismo y ataques DDoS: ¿Herramientas de protesta social o delitos informáticos? 1ª Parte", (2011, 10 Octubre) [Online]. Available: http://www.bsecure.com.mx/opinion/laley-y-eldesorden/hackivismo-y-ataques-ddos-herramientas-de-protesta-social-o-delitos-informaticos-1-parte/

[5] Ortega, Alberto, "CloudFlare, una posible solución frente a ataques (D)DOS",(2011, 8 Junio)[Online]. Available:http://www.securitybydefault.com/2011/06/cloudflare-una-posible-solucion-frente.html

[6] García, Mario, "5 recomendaciones clave para frenar ataques DDoS", (2013, 1 Octubre) [Online]. Available: http://www.portalinformatico.com/directortic/seguridad/check-point-ofrece-5-recomendaciones-clave-para-frenar-ataques-ddos-201310019001.html

Autor

Iván Darío Casabón Martínez
Ingeniero de Sistemas
Universidad Piloto de Colombia
2013