CIBERGUERRILLA EN BOLIVIA

Nancy Mamani Mamani
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de información
nancy.lib.30@gmail.com

RESUMEN

Este presente artículo trata sobre la marcha indígena por el TIPNIS que desata por primera vez una ciberguerrilla en Bolivia por medio de las redes sociales (**Facebook y Twitter**), la resistencia contra la carretera que destruiría una región mega diversa en el corazón de Bolivia y del continente sudamericano, lo cual nos llevo una Ciberguerrilla en Bolivia alrededor del TIPNIS? todo gracias a los comentarios en las redes sociales donde entraron en acción Anonymous y wara Isabel (hackers).

PALABRAS CLAVE

Ciber guerrilla, Ciberconflicto, hacker , virus.

1. INTRODUCCION

1.1 CIBERGUERRILLA

La Ciberguerrilla es el desplazamiento de un conflicto cibernetico, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, en lugar de los campos de batalla convencionales. Los protagonistas son los Jackes los que atacan a través del maligno virus informático.

1.2 MARCHA INDIGENA DESATA UNA CIBERGUERRILLA EN BOLIVIA

Y es que el TIPNIS (Territorio Indígena y Parque Nacional Isiboro Sécure), que se encuentra exactamente emplazada en la faja subandina Cochabambina, entre los departamento del Beni (provincia de Moxos) y Cochabamba (provincia del Chapare el territorio en cuestión, contiene tesoros naturales y riquezas de biodiversidad incalculables.

Lo cierto es que la represión desmesurada desatada en día 25 de septiembre, provocó que Wara Ysabel y hasta el colectivo Anonymous ingresara en escena, atacando instituciones y empresas del estado boliviano.

Es probable que quienes integran este colectivo, ni siquiera se conozcan entre sí. Sus acciones, tales como hackear páginas de gobiernos, 'tumbar' páginas web de grandes empresas, etc. son acciones que parecen rayanas al delito.

1.2.1 Annonymous

El famoso hacker Anonymous, (*véase figura 1*) si bien está coordinado a través de toda la red; no tiene un sitio oficial ni nada que se le parezca. Sin embargo, el debate sobre los gobiernos y estados, que determina sus prioridades de ataques, tiene lugar en un servidor de IRC (Internet relay chat) donde los usuarios pueden chatear en tiempo real, sin necesidad de establecer contacto previo; basta encontrarse en un canal de los tantos que existen. Su símbolo, es la máscara del anonimato.

Una de las herramientas con las que efectúan sus ataques es un software llamado LOIC (*Low Orbit Ion Cannon*) que permite lanzar ataques de denegación de servicio de forma coordinada.

Figura 1. Annonymous

Figura 2. Wara Ysabel.

1.2.2 Wara Isabel

Tal vez Wara (*véase figura 2*) no sea hacker , pero para el grupo "Amigos de TIPNIS", es imprescindible a la hora de ejecutar y eliminar todo intento de infiltración.

Wara Ysabel se encarga de distribuir información, evitar la censura y la represión gubernamental en internet, y animando a quienes creen que oponerse a ESA CARRETERA, darle una oportunidad a la vida.

Dice Wara, "*En el mundo informático no sólo se emplean programas, la "ingeniería social" lo que hacen no es más que lo que hacíamos nosotros a los 15 años.*

La politóloga Helena Argirakis. Ex militante del MIR (Movimiento de Izquierda Revolucionaria), manifiesta su temor frente a la actividad de los colectivos horizontales que se crean a través de las redes sociales. En el periódico Cambio (oficialista), declara que las redes sociales son "armamentos de destrucción social", lo cual las califica como más peligrosas, que la televisión .

Argirakis explica que las redes sociales, en el conflicto por el TIPNIS, fueron tomadas como un nuevo campo de lucha con la finalidad de dirimir conflictos políticos.

"*Como se dan en tiempo real, es decir, sucede el hecho y automáticamente alguien 'tuitea' y da su criterio o su opinión, más que un análisis racional, genera una cadena de rumorología que a mi criterio no es aséptico sino un interés velado donde se infiltran operadores a través de estos medios para tergiversar y manipular información*", para cerrar con un contundente "*son perversas*".

Estas opiniones constituyen un reconocimiento, no solo que la ciberbatalla política estaba perdida en las redes sociales, sino y sobre todo, que tal ciber-batalla había existido.

Sin embargo Wara no cree que haya existido ni exista una ciber-guerrilla en Bolivia alrededor del TIPNIS. No en estos términos.

"*Más que ciberguerra hay resistencia. Podemos hablar de una especie de guerra en ciertos momentos, como cuando se atacó la página de la CIDOB menos de una hora después de que en esta se publicara la lista preliminar de heridos y desaparecidos. No pudimos establecer el origen del ataque, pero fue de tipo DDoS.*

1.2.3 Ataque DDos

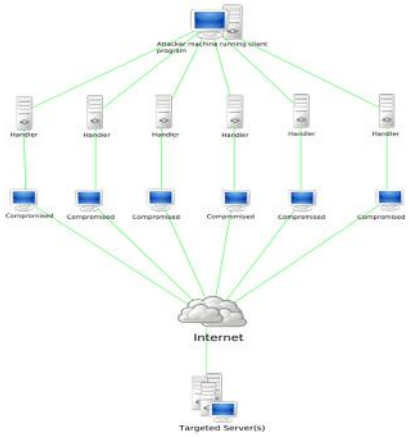

Figura 3 Ataques tipo DDoS.

En seguridad informática, un **Ataque de denegación de servicios (*vease figura 3*)**, también llamado ataque **DoS** (de las siglas en inglés ***D**enial **o**f **S**ervice*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Es aquí cuando **Annonymous** entra en escena, el ingreso de este colectivo de hackers, se produce en un momento álgido del conflicto indígenas - gobierno. La brutalidad de la represión desatada sobre el campamento de los marchistas, sin que mediara causa alguna; los métodos utilizados, como la mordaza, secuestro y traslado forzado de personas; las agresiones verbales por su condición étnica, mostraron un gobierno más emparentado con las peores dictaduras que un gobierno democrático, electo por una aplastante mayoría de votos. Con esas circunstancias, el ingreso a escena de Annonymous parecía significar el inicio de una cyber-guerra.

Hubo otra batalla también cuando Anonymous atacó con éxito varias páginas del gobierno, Ahora hay un ataque más peligroso, cuando nos califican de "disidentes del twitter" o "más peligrosos que la TV". Esa ya entra en un terreno más pedregoso. Ahora, en un sentido no bélico, sino más bien de lucha, tenemos una batalla por la naturaleza, por el respeto a los derechos más elementales y en esto hemos llevado a cabo intensas batallas. Yo creo que las redes han influido positivamente en un cambio de actitud del gobierno en el momento que se impedía el acceso al agua1. Esta "batalla" la peleamos en Twitter, cuando aún existía la cuenta @SachaLlorenti. Fue tan masivo el bombardeo de reclamos al ex ministro, que los primeros en enterarnos de los 2000 litros de agua (que el gobierno hizo llegar a los marchistas bloqueados por la policía y campesinos cocaleros) *fuimos los tuiteros, mediante un post que puso Llorenti*".

Sacha Llorenti, (Ex ministro de Gobierno)vinculado antaño a la defensa de los derechos humanos, es sindicado como uno de los responsables de la brutal represión a los indígenas que marchaban defendiendo sus derechos y su territorio. Foto: institucional.

1.3 CIBERACTIVISTAS ANONYMOUS EN BOLIVIA

La ciber-gerrilla estallaba en el país por vez primera, comenzó el ataque, primero haciendo caer la página de la Presidencia, luego liberan la base de datos de autos "truchos" de DIPROVE en homenaje a los niños que dejaron sin agua y enviaron una foto en la que se ve a un niño frente a los policías quienes le niegan el paso al arroyo. Seguidamente deforman la página de la fiscalía con la canción "Bolivia" de los Kjarkas de fondo y el mensaje "Pueblo boliviano no estás solo, somos legión, no obedecemos a un partido político, obedecemos al pueblo" En Twitter pasó un mensaje "Gobierno de Bolivia, deberías haberlo esperado" A continuación liberaron 2900 cuentas wi fi de ENTEL http://t.co/oDbWsPDf y en este momento, una lista de todos los policías de Bolivia.

No son pocos los rumores acerca de una firma rusa de seguridad informática, que está considerada como desarrolladora del antivirus más eficiente del mundo, fue contratada por el gobierno Boliviano para estar protegidos contra los hackers.

2. CONCLUSIONES

1. Durante los últimos han aumentado los ataques cibernéticos a nivel mundial y por ende se ha propagado a nuestro país Bolivia.
2. El ciber-activismo en Bolivia está siendo usado en la Internet y las redes Sociales para protestar y hacer escuchar la voz del pueblo.
3. En caso de futuros ciberAtaques que buscan dañar sin motivo alguno a los recursos informáticos del Estado se tomar medidas de Etical Haking y Pentesting. El cual obliga al Estado a contratar empresas que salvaguarden la seguridad se sus Sistemas Informáticos.

3. BIBLIOGRAFIA

Disponible en:

[1] https://es.wikipedia.org

[2]http://www.facebook.com/groups/215587215159303/?id=243111-649073526#!/pages/Evo-Morales/9972487874

[3] http://pastebin.com/U0Nj2VMK