Barómetro Internacional
Análisis Político y Social, Nacional e Internacional de Venezuela y el Mundo
www.barometrointernacional.com.ve - Director: *Diego Olivera E.*

¡Alerta, que están tratando de intensificar la guerra cibernética!

Por Carlos E. Lippo

Como hemos venido señalando en artículos anteriores, el ataque informático o cibernético ("hackeo"), se ha venido consolidando entre nosotros como un arma más del arsenal de la contrarrevolución, que la viene aplicando a sistemas operativos automatizados, asociados o no a la prestación de servicios públicos, así como a portales web del gobierno y de organizaciones revolucionarias, con el apoyo de sus asociados del exterior y de una quinta columna enquistada en la administración pública. Tales ataques suelen ser intensificados en la víspera de acontecimientos importantes, aplicados en forma aislada o en combinación con otro tipo de acciones de desestabilización, con el propósito de apoyar la guerra económica y la guerra psicológica que nos han venido aplicando.

Antes de comenzar a desarrollar el tema en detalle consideramos conveniente referirnos a la naturaleza y los efectos de algunas de las modalidades más comunes de este tipo de confrontación; tales son:

*La intrusión en sistemas operativos de organismos y empresas estadales dotados con un grado significativo de automatización informática, con el propósito de inducirles fallas importantes de funcionamiento capaces de generar una interrupción del servicio prestado por el sistema bajo ataque. Siendo oportuno señalar que en nuestra opinión, todos los procesos de nuestra CANTV, de altísimo componente tecnológico; los procesos altamente automatizados de nuestra Industria Petrolera, en especial los del Área de Refinación; algunos de los procesos del Banco Central de Venezuela, la Cámara de Compensación Electrónica entre ellos, y evidentemente

que el CNE, representan blancos potenciales más que apetecibles para los piratas cibernéticos de la contra. *La intrusión en sistemas informáticos con grandes bases de datos y sistemas de comunicaciones de instituciones del estado de primer orden, comola Fuerza Armada Nacional Bolivariana y los Ministerios, con propósitos fundamentalmente de espionaje, con el doble objetivo de apropiarse de nuestra “información sensible” e inducirnos elementos de desmoralización.

La intrusión en portales web de medios de comunicación de la revolución, para propagar falsas noticias de carácter desestabilizador así como en portales informativos de instituciones de gobierno, como apoyo a actividades subversivas de distinta naturaleza y alcance

La utilización de Redes Sociales como Twitter y Facebook por parte de los opositores, para la propagación de rumores desestabilizadores y para promover la incorporación de sus adherentes al desarrollo de actividades más o menos subversivas.

La difusión en portales web, de contenidos de apoyo franco a la guerra económica, en materia de especulación y en materia de ataque a la integridad de la moneda.

Probablemente el primer ataque cibernético de importancia ocurrido en nuestro país fue el perpetrado por INTESA (empresa mixta conformada por PDVSA en asociación minoritaria con la gringa SAIC, íntimamente ligada a la CIA), durante el paro sabotaje petrolero de 2002-2003, que además de proporcionarle con gran anticipación el pago de salarios a todos los huelguistas y saboteadores vende patria de la meritocracia petrolera de la época, bloqueó las claves de acceso a los controles de los sistemas automatizados en las diferentes instalaciones operativas y manejó remotamente, de manera incorrecta, una serie de procesos operativos automatizados, con grave riesgo para las instalaciones y, por supuesto para los trabajadores leales de la industria que intentaban neutralizar el efecto de tales acciones.

Desde este primer ataque hasta nuestros días, la contrarrevolución ha venido estando detrás de una inmensa cantidad de intentos de intrusión y de ataques de todos los tipos listados en los párrafos anteriores. En aras de la brevedad sólo referiremos dos de ellos, que consideramos emblemáticos por los daños causados o que pudieron haber causado en el caso de haber sido perpetrados exitosamente en toda su magnitud; éstos son:

Los numerosísimos intentos de sabotaje y/o intrusión en el portal web del Consejo Nacional Electoral (www.cne.gob.ve), el día 14 de abril de 2013, antes, durante y después del acto electoral, aunados al ataque contra la cuenta Twitter del entonces Candidato Presidencial Nicolás Maduro, lo que motivó la decisión gubernamental de bloquear temporalmente el acceso a Internet a través de CANTV, según lo informase en aquella oportunidad el entonces Ministro de Ciencia, Tecnología e Información, Jorge Arreaza

El perpetrado sobre el sistema de interconexión de CANTV, base de la plataforma tecnológica del Consorcio CREDICARD, el 02 de diciembre pasado (1), que aunado a una falla total del sistema de respaldo de esa plataforma, causado por sabotaje y/o negligencia culposa interna, dejó prácticamente al país sin cajeros ni medios de pago electrónico durante un poco más de un día, ya que CREDICARD atiende a toda la banca pública y a buena parte de la banca privada nacional.

En días recientes fue descubierto y desactivado un centro de operaciones informáticas manejado por factores de la contrarrevolución, que estaba destinado a perpetrar un sabotaje y afectar la plataforma informática del Consejo Nacional Electoral (CNE), con el propósito de impedir la realización de las elecciones de los miembros a la Asamblea Nacional Constituyente (ANC) previstas para el 30 de julio próximo, que fue señalado oportunamente por el propio Presidente Maduro (2).

Adicional a lo anterior, ataques perpetrados sobre la plataforma tecnológica de CREDICARD y sobre las plataformas web de la banca pública, causantes de rechazos y demoras en la aprobación de transacciones de pago con tarjetas de débito y de la oportuna dispensa de dinero efectivo en los cajeros de los bancos Venezuela y Bicentenario, fundamentalmente, desde hace más de una semana, así como una falla en los sistemas informáticos del Banco Central de Venezuela, ocurrida el lunes 17, que impidió la ejecución de todo tipo de transacciones de la banca nacional e internacional con el instituto emisor, incluida la compensación electrónica de saldos, durante todo el día, son innegables indicios de que la contrarrevolución está tratando de elevar el apresto operacional de su ejército de terroristas informáticos con miras a su incorporación a la estrategia insurreccional que han dado en llamar la “hora 0”.

En confirmación de esta última aseveración es necesario señalar también que desde mediados de la semana pasada ha podido percibirse una inestabilidad importante y una anormal dificultad para el acceso en conocidas páginas del sistema nacional de medios públicos, como www.ciudadccs.info y www.rnv.gob.ve y hasta en este mismo portal, aunado al hecho de que durante todo el fin de semana, páginas revolucionarias como www.laiguana.info, www.lechuguinos.com y hasta la ambivalente www.aporrea.org, fueron atacadas con la inserción de propaganda del plebiscito, del mismo tipo y formato que la insertada en los portales de la contra.

Las nuevas “fallas” en CREDICARD, ocurridas poco tiempo después del retiro del personal del SEBIN que cumplía tareas de vigilancia en sus instalaciones desde la ocurrencia de la gran “falla” del mes de diciembre pasado, dan pie para pensar que tiene que existir una importante complicidad interna en la generación de estas “fallas”; así mismo, asumimos que tiene que haber responsabilidad interna en la falla registrada el lunes 17 en el Banco Central, porque ¿cómo podría explicarse que el centro de cómputos de respaldo, localizado en Maracaibo, diseñado para asumir de forma inmediata toda la carga del centro principal de Caracas, no entrase en funcionamiento sino al final de la tarde?

En relación a los ataques a las empresas mixtas y estadales de servicio y demás entes de la administración pública, tengo una razonable confianza en que, bajo las directrices del Consejo de Defensa de la Nación, se haya podido conformar un "ejército informático", capaz de neutralizar las agresiones externas o, en todo caso, de restaurar el normal funcionamiento de los sistemas una vez atacados; recordemos que en el año 2002, con mucho menos recursos, un grupo de técnicos informáticos venezolanos dirigidos por Socorro Hernández, actual rectora principal del CNE, fue capaz de restaurar el "cerebro informático" de PDVSA, colapsado por la acción de una empresa de mayoría gringa en connivencia con la meritocracia cipaya y vendepatria que se vanagloriaba de dirigir tan importante empresa.

Por otra parte, para intentar prevenir la ocurrencia de ataques en tales instituciones y habida cuenta que las mismas están penetradas en mayor o menor grado por técnicos comprobadamente opositores y/o presuntos chavistas integrantes de lo que hemos estado llamando a quinta columna, es necesario poner en cuarentena a este personal, poniéndolo bajo estricto control de personal comprobadamente patriota, de la misma institución o de otras instituciones que puedan ser ingresados bajo la figura de comisiones de servicio.

Para finalizar, consideramos oportuno alertar a todos los revolucionarios sobre la divulgación de falsas noticias a través de cualquier medio, pero en especial a través de los medios de la revolución que pudiesen haber sido hackeados, del mismo tipo de aquel falso positivo divulgado por Al Jazeera, sobre la caída de la Plaza Verde de Trípoli en poder de la contrarrevolución Libia. Ante noticias de tal naturaleza es necesario chequear exhaustivamente las fuentes antes de retransmitirlas y proceder en consecuencia. Así mismo, reiteramos la necesidad de diseñar planes de contingencia capaces de garantizar el funcionamiento de nuestros organismos de militancia (comunas, consejos comunales, CLAPs, UBCHs, etc.) ante la eventualidad de no poder disponer de las facilidades y aplicaciones comunicacionales asociadas a la internet, ya sea que dicha red nos haya sido bloqueada, o porque el gobierno revolucionario haya tenido necesidad de bloquearla por razones de carácter defensivo.

¡Hasta la Victoria Siempre!

Patria o muerte!

¡Venceremos!

(1)http://www.panorama.com.ve/contenidos/2016/12/07/noticia_0113.html
(2)http://www.panorama.com.ve/politicayeconomia/Maduro-Develamos-operacion-de-hackeo-del-sistema-del-CNE-para-impedir-elecciones-del-30-de-julio 20170624-0027.html

celippor@gmail.com

Publicación Barómetro 24-07-17

internacional.barometro@gmail.com