{vozmestart}

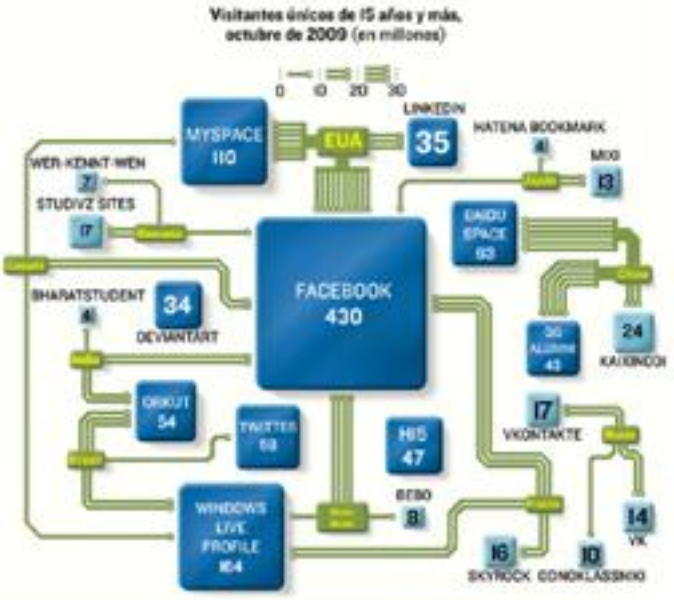
Guerra cibernética 4GL

JUAN RAMÓN JIMÉNEZ DE LEÓN*

Mucho se escribe en estos días acerca de cómo el movimiento insurreccional de los jóvenes en el Magreb se debe en parte a la prohibición de las autoridades a acceder a las redes sociales y a la comunicación instantánea de la información cibernética a nivel global. Son importantes los casos de la Republica Popular China por cerrar los accesos de Google, y es ejemplar la información inmediata del gigantesco terremoto y maremoto en Japón.

Sin embargo, las redes sociales se han convertido en el escenario de guerras cibernéticas de cuarta generación (4GL). Viene a mencionarse el caso de ***Wikileaks*****,** que es asombroso cómo desde una terminal de computadora personal (PC), con el conocimiento adecuado -precisamente los japoneses dicen que se necesita el *hardware*, el *software* y el *humanware*, para estar en el nivel 4GL-, se puede penetrar las sofisticadas computadoras del Pentágono de los Estados Unidos, el complejo militar más difícil de introducir virus, *troyanos*

, gusanos, etcétera, y aun así se obtuvo una cantidad impresionante de información clasificada como
top secret
.



Entre las diferentes hipótesis que circulan en la Internet, se habla de una dura lucha por el poder imperial, entre los ***Obamites*** y los ***Clintonites***, y que ***Wikileaks*** tiende a golpear a la poderosa secretaria de Estado Hillary Clinton, a la que ya le llaman, por su descrédito ante los diferentes jefes de Estado, como
Hillarious
. Entonces, la llamada “

rebelión del Facebook
", se especula es el contragolpe
clintonite
contra los
obamites
, debido a que
Barack Obama
fue agarrado fuera de base en las crisis árabes del Magreb y la gran "negociadora" es ahora
Hillary Clinton
.

Claro que hay muchos intereses en el camino, entre ellos el hartazgo de la gente joven y sobre todo estudiantil, de las monarquías y cuasi-monarquías (Kadafi) árabes, conta sus continuas políticas represivas, anti-democráticas y antifeministas, pero el hecho es que hay un virtual levantamiento popular en el Magreb, en Yemen, en Arabia Saudita, en los Emiratos, en Irak y en Irán (persa), y se especula que pronto seguirá China.

Los ***clintonites***, que ahora están regresando el golpe, están "atacando" lugares hostiles como
La Jornada
, de México, que tiene una de sus bases virtuales en la UNAM. Inaugurada el 16 de enero del 2007 como una supercomputadora, llamada
kan-balam
, está clasificada en la posición 126 de las 500 supercomputadoras más rápidas en el mundo y en el número 44 en los sitios académicos. "
Esta nueva supercomputadora es siete mil veces más potente que aquella que apenas 15 años se les mostraba, aquella que era prototipo de un avance formidable la
Craig
en materia de cómputo
", señaló el rector de entonces
Juan Ramón de la Fuente,

un prospecto presidenciable para el 2012. Dicha supercomputadora tuvo un costo de tres millones de dólares. La asesoría técnica corre a cargo de
Oracle
, que siendo una firma
high tech
de primera, en México se comporta como de cuarta, pues en la actual situación, la supercomputadora esta sufriendo un ataque cibernético, especialmente en los clientes externos, llamados
Uranio
, como el periódico
La Jornada
, que en México publica los cables de
Wikileaks
y que ha golpeado duramente al embajador de EU en México, Carlos Pascual, pupilo de
Zbigniew Brzezinski
, muy cercano a los Clinton. Dicen los expertos que esto es parte del operativo llamado
Plataforma México-RAND
que comanda
Carlos Slim
, Vea ud youtube http://www.youtube.com/watch?v=uMZcqJiI7eU, en donde parece que la UNAM fue contagiada del pavoroso gusano llamado
Stuxnet
,
desarrollado en Medio Oriente y aplicado exitosamente a las computadoras del programa nuclear de Irán en Bushehr. Esto fue denunciado por el experto alemán en cómputo,
Ralph Langner
. Stuxnet que fue desarrollado por Siemens causa enorme caos en los sistemas cibernéticos haciéndolos inestables,
Stuxnet
es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad radicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares. La compañía europea de seguridad digital Kaspersky Labs describía a
Stuxnet
en una nota de prensa como "
un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial
". Kaspersky concluye que los ataques sólo pudieron producirse "con el apoyo de una nación soberana", convirtiendo a Irán en el primer objetivo de una guerra cibernética real.

El objetivo más probable del gusano, según corroboran medios como BBC o el ***Daily Telegraph***, pudieron ser infraestructuras de alto valor pertenecientes a Irán y con sistemas de control de Siemens. Medios como ***India Times*** apuntan que el ataque pudo haber retrasado la puesta en marcha de la planta nuclear de Bushehr. Algunos medios como el norteamericano ***New York Times*** han atribuido su autoría a los servicios secretos estadounidenses e israelíes.

Kadafi.

El número de vulnerabilidades de día cero de Windows que aprovecha *Stuxnet* también es poco habitual. Este tipo de errores de Windows son muy valorados por *crackers* y diseñadores de malware puesto que permiten acceder a sistemas incluso aunque hayan instalado todas las actualizaciones de seguridad, al no ser conocidos públicamente.

Un ataque *malware* normal no desperdiciaría cuatro de estos errores en un solo gusano. Además, *Stuxnet* es extrañamente grande, ocupando medio *megabyte*, y está escrito en distintos lenguajes de programación, incluyendo C y C++, lenguajes de 4GL algo que se ve con poca frecuencia en otros ataques de este tipo. Recordemos que ***Arpanet*** de donde salió Internet, fue desde su origen, un arma militar. ***Anonymous*** comenta en *Twitter* que ya tiene el código de *Stuxnet*. Este grupo seguidor de ***Wikileaks***, es considerado el más activo en atacar *banksters* y *macrosicarios*. Al cabo de un tiempo, otra cuenta en *Twitter*, del grupo publicó lo que parecía ser una parte de descompilado de *Stuxnet*.

La pregunta ahora es: ¿qué pueden hacer con el gusano? ¿Podrían llevar a cabo algún ataque con el virus? La magnitud de *Stuxnet*, tal y como se ha estado estudiando desde su aparición, es compleja y muy peligrosa. El gusano se transmitió en sus inicios a través de un programa de la multinacional alemana Siemens en el mes de septiembre de 2010, y aunque actualmente se trabaja en sistemas operativos para evitar un posible ataque con el gusano, sigue siendo a día de hoy un arma demasiado sofisticada para lanzarla a la ligera. Aún hoy, no se sabe con exactitud el origen de *Stuxnet,* aunque se apunta una posible alianza entre Israel (¿
Rahmbo
?, recién electo Alcalde de Chicago) y Estados Unidos (
Clintonites
).

Algunos expertos en seguridad se muestran escépticos ante el mensaje de ***Anonymous***, declarando que aunque posean el binario y su desmontaje, no tienen la fuente original para desarrollarlo. Otros como Orla Cox, analista de seguridad de Symantec, decían al respecto para ***The Guardian***
que: “Podría ser posible, aunque se necesitaría mucho trabajo, ciertamente no es algo trivial”.
The New York Times
publica que se ha descubierto dentro del código del virus una críptica alusión al
Antiguo Testamento
. Concretamente la palaba "
Myrtus
" denomina un fichero contenido en el código. Los expertos lo interpretan como una alusión, en hebreo, a
Esther
. El
Libro de Esther
relata un complot persa para destruir Israel. Esta cita tanto puede ser interpretada como una firma que implicaría al gobierno israelí en la fabricación del virus como, por el contrario, un intento de sus reales autores de orientar falsas sospechas hacia Israel y confundir a los investigadores.

Otra hipótesis es que la palabra se refiera al mirto, un arbusto. Por otra parte, *Stuxnet* recorre China. La agencia oficial china
Xinhua
afirma que el origen estaría en un ataque desde servidores ubicados en Estados Unidos.
Stuxnet
ya habría afectado a
seis millones de ordenadores
y a unas mil empresas en aquel país. Empresas que integran sectores claves de la economía china como el transporte, la metalurgia y la energía.

En las últimas investigaciones sobre las características técnicas del virus se afirma que tiene capacidad de preparar los ordenadores para futuros ataques aunque se haya procedido a la desinfección de los mismos. En principio, el virus se difunde sin necesidad de Internet. Basta con que esté albergado en una memoria USB que se conecte a la máquina, pero ya se ha desatado la alarma sobre su potencial destructivo. Los expertos consideran que no se trata de una creación personal. Aunque inicialmente se habló de la posibilidad de que un grupo mafioso lo empleara para la extorsión a las empresas contaminadas, crece la convicción de que la autoría debe buscarse en algún grupo ciberterrorista o en alguna agencia secreta gubernamental.