Stuxnet: Revolución de Ciberguerra en los Asuntos Militares

Mayor Paulo Shakarian, USA

EL 17 DE JUNIO DE 2010, investigadores de seguridad en una pequeña empresa belarusa conocida como VirusBlockAda identificó un software malicioso (malware) que infectó memorias USB.[1] En los meses siguientes, hubo una oleada de actividades en la comunidad de seguridad informática—revelando que este descubrimiento identificaba solamente un componente de un nuevo gusano informático [2] conocido como Stuxnet. Este software fue diseñado específicamente para afectar equipo industrial. Una vez que se reveló que la mayoría de las infecciones fueron descubiertas en Irán,[3] junto con un inexplicable retiro del servicio de centrífugas en la planta de enriquecimiento de combustible (FEP, por su siglas en inglés) iraní en Natanz,[4] muchos en los medios de comunicación especularon que la meta final de Sutxnet era atacar las instalaciones nucleares iraníes. En noviembre de 2010, algunas de esas sospechas fueron confirmadas cuando el presidente iraní, Mahmoud Ahmadinejad, aceptó públicamente que un gusano informático había creado problemas para una "cifra limitada de nuestras centrífugas nucleares". [5] Expertos acreditados en la comunidad de seguridad informática ya han catalogado al Stuxnet como "sin precedentes"[6], un "salto evolutivo "[7], y el "tipo de amenaza que esperamos nunca más ver nuevamente".[8] En este artículo, yo sostengo que este software malicioso representa una revolución de asuntos militares (RMA, por sus siglas en inglés)[9] en el ámbito virtual—o sea, que Stuxnet básicamente cambia la naturaleza de la ciberguerra. Hay cuatro razones para sustentar lo anterior: (1) Stuxnet representa el primer caso en el que equipo industrial es atacado con un arma cibernética, (2) hay pruebas que el gusano tuvo éxito en su ataque de dicho equipo, (3) esto representa un adelanto significativo en el desarrollo de software maliciosos y (4) Stuxnet ha mostrado que varias suposiciones comunes acerca de la seguridad cibernética no siempre son válidas. En este artículo analizo estos cuatro puntos al igual que exploro las implicaciones futuras del Stuxnet RMA.

STUXNET ATACA EQUIPOS INDUSTRIALES

Varias empresas importantes de seguridad informática han analizado el Stuxnet[10] a cabalidad y todas concuerdan que la meta principal de este software fue causar fallas imperceptibles al equipo industrial. Aunque la posibilidad de atacar ese equipo por medios cibernéticos hace mucho tiempo fue planteada como una hipótesis, este nuevo gusano cibernético en realidad intentó la hazaña. Además, este tipo de ataque fue probablemente la única meta del software. Por ejemplo, otros malware incluyen códigos estándares para una variedad de actividades delictivas—inclusive robo de identidad y de contraseñas, lanzamiento de ataques de denegación de servicio y envío de correos electrónicos spam.[11] A pesar de su alto grado de complejidad técnica, Stuxnet no fue concebido para llevar a cabo ninguna de esas actividades.[12] Más bien, el software intenta auto propagarse con la meta de infectar una computadora basada en Microsoft Windows que se comunica con el equipo industrial. Esto es en marcado contraste con el gran número de software en la Internet que se emplea para una variedad de fines delictivos. Stuxnet fue concebido para el sabotaje, no para la delincuencia.

El tipo de equipo industrial que Stuxnet infecta se conoce como los sistemas SCADA (Control de Supervisión y Adquisición de Datos). Estos sistemas están diseñados para la recopilación, control y vigilancia de datos en tiempo real de infraestructuras críticas, inclusive plantas de ener-

gía, oleo/gasoductos, refinerías, sistemas de agua u otras aplicaciones que requieren equipo controlado por computadoras.[13] Los sistemas SCADA a menudo utilizan PLCs (controladores lógicos programables) —hardware para controlar un componente físico. Para programar el PLC, el administrador lo conecta a una computadora Windows estándar. Entonces por lo regular el PLC se desconecta de la computadora cuando está listo para usarse. Por ejemplo, si el administrador desea que las centrífugas funcionen a una velocidad más rápida, conecta el PLC a la computadora Windows, instala un software que se comunica con el PLC y sube las nuevas instrucciones. Supongamos que Stuxnet ha infectado la computadora conectada al PLC. El malware básicamente lleva a cabo un "ataque mediante intermediario" en contra del sistema. El administrador intenta enviar los comandos al PLC. Stuxnet los intercepta y envía sus propias instrucciones. Sin embargo, el software somete un informe falso a la computadora Windows que las instrucciones originales fueron cargadas. Al someter un informe falso, Stuxnet se esconde, convirtiéndolo más difícil de detectar.

Stuxnet fue diseñado para atacar los PLC controlados por el software Step 7 de Siemens.[14] Además, solamente infecta dos modelos de PLC—el Siemens S7-315 y el S7-417. El S7-315 es un controlador de uso general que funciona una sola gama de dispositivos. Esa gama, o grupo, de dispositivos controlados por el S7-315 puede, por ejemplo, operar diferentes fases de un proceso de fabricación. El S7-417 es el mejor modelo en la línea, operando múltiples gamas de dispositivos—por ende, capaz de controlar más equipo que el S7-315.[15] Expertos en seguridad han concluido que Stuxnet solamente lanza ataques si el PLC está conectado a dispositivos configurados de una manera muy específica. Por ejemplo, cuando el gusano detecta el S7-315, solamente ataca si el PLC está conectado a 33 o más convertidores de frecuencia—dispositivos empleados para controlar la velocidad de cierto equipo (por ejemplo, las revoluciones por minuto de un motor).[16] Asimismo, al atacar el PLC S7-417, espera encontrar 6 cascadas de 164 convertidores de frecuencia.[17] El malware también garantizaba que los convertidores de frecuencia fuesen fabricados por la compañía iraní Fararo Paya o la compañía finlandesa Vacon.[18]

Una vez que Stuxnet ha determinado que ha infectado la configuración objetivo de los convertidores de frecuencia, lanza el ataque. Con base en el análisis del software, expertos han descubierto que esperan que los convertidores de frecuencia estén funcionando entre los 807 y 1.210 Hz. Luego, periódicamente altera estos valores entre 2 y 1.410 Hz.[19] De esta manera, el dispositivo que está controlado por el convertidor de frecuencia funciona de una manera inesperada. A medida que Stuxnet reporta que el PLC fue programado correctamente, el operador daría por sentado que los dispositivos están funcionando en la gama normal. El hecho de que Stuxnet ajusta estas configuraciones ilustra un punto importante—que el propósito del gusano cibernético era en realidad dañar el equipo industrial. Si Stuxnet fuese tan solo una prueba del concepto, o un truco, el ajuste de las frecuencias probablemente sería innecesario.[20]

STUXNET PROBABLEMENTE TUVO EXITO

Stuxnet fue concebido no solamente para atacar equipo industrial sino que hay pruebas que tuvo éxito en ello. Los indicadores del éxito surgen del siguiente razonamiento. Primero, parece que las infecciones iniciales del gusano ocurrieron en Irán. Segundo, las estructuras de los datos en el código Stuxnet se asemejan a la configuración de las centrífugas en el FEP iraní en Natanz. Tercero, funcionarios del gobierno iraní admitieron que las operaciones de sus centrífugas fueron afectadas por el gusano.

Tal parece que Irán fue el epicentro de los ataques. Esto es corroborado por el volumen de infecciones al igual que los análisis de las muestras de malware. La empresa de seguridad Symantec rastreó 100.000 máquinas infectadas a partir del 29 de septiembre de 2010—aproximadamente 60.000 de las cuales se encontraban en Irán. Luego le siguió Indonesia con 15.000 infecciones.[21] Symantec, en combinación con otras empresas de seguridad, recopiló 3.280 ejemplos singulares

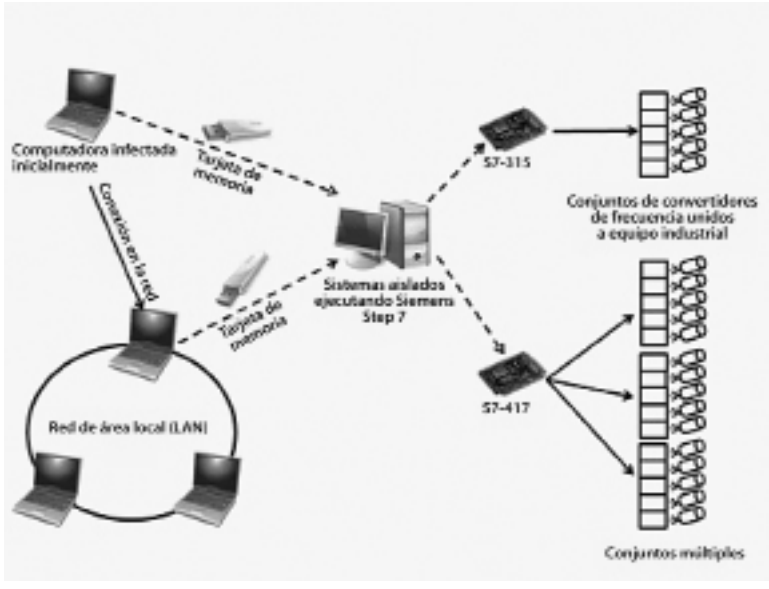


Figura: La propagación del gusano cibernético Stuxnet

del software Stuxnet y sus variantes.[22] Esas muestras representaron un total de 12.000 infecciones. Stuxnet mantiene una lista de sistemas infectados anteriormente. Por ende, para una muestra en particular, los investigadores pudieron determinar la trayectoria que el gusano cibernético propagó para poder llegar a esa computadora. Al revisar esas muestras, Symantec pudo rastrear el historial de la infección a una de cinco organizaciones diferentes—las cuales todas tienen una presencia en Irán.[23]

De lo que se sabe de la FEP en Natanz, parece haber una semejanza asombrosa entre la configuración de su centrífuga y el código Stuxnet. Según la Agencia Internacional de Energía Atómica (IAEA, por sus siglas en inglés), las centrífugas IR-1 en el FEP en Natanz funcionan en cascadas de 164.[24] Esto se alinea justamente con la configuración que Stuxnet busca cuando ataca el controlador S7-417. Otro indicador potencial es la velocidad máxima de una centrífuga IR1: 1.400-1.432 Hz.[25] Este alcance de frecuencia es muy cerca a la velocidad máxima que el malware establece durante el ataque—1.410 Hz.[26] Una centrífuga IR-1 configurada a una frecuencia tan elevada probablemente causaría daños.

El proceso de enriquecimiento de uranio se puede optimizar si se divide en una serie de fases con centrífugas múltiples funcionando en cada fase.[27] En una entrevista en el 2006 se dio a conocer que los iraníes estaban llevando a cabo su enriquecimiento de uranio con ese método utilizando quince fases.[28] En cada fase, cierto número de centrífugas se distribuyen para lograr una producción óptima. Alexander Glaser, un profesor en el laboratorio de Futuros Nucleares de Princeton, analizó el arreglo óptimo de las centrífugas en una cascada de centrífugas de 164. Ralph Langer, fundador de Langer Communications GmbH, que se especializa en los sistemas SCADA, comparó este análisis a las estructuras de datos en Stuxnet. Él descubrió que el malware posiblemente funciona de una manera que interfiere significativamente con la distribución óptima de las centrífugas en cada fase. La distribución resultante parece ser lo contrario de óptimo según lo establecido por Glaser.[29] Si Stuxnet atacó las centrífugas en Natanz, hubiese resultado en

la producción menos que optima de uranio enriquecido—por ende la cantidad producida probablemente sería muy por debajo de la capacidad.

Además del análisis técnico mencionado anteriormente, también hay pruebas de la posible eficacia del software en las declaraciones de los líderes iraníes. En noviembre de 2010, el Presidente Ahmadinejad confirmó que la presencia de software malicioso había afectado sus centrífugas—aunque no describió explícitamente la presencia de Stuxnet.[30] En una entrevista con SPIEGEL ONLINE al secretario general del Consejo Supremo de Seguridad Nacional de Irán, Saeed Jalili, se le preguntó específicamente acerca del uso de Stuxnet para atacar a Natanz. Aunque Jalili no entró en detalles sobre los daños ocasionados por el gusano (nuevamente minimizando los efectos que tuvo), reconoció que había ocurrido un incidente al declarar que "nuestros expertos ya habían prevenido sobre este ataque hace mucho tiempo".[31]

Además, es interesante destacar que hay una posibilidad que Stuxnet fue instalado en Natanz por un saboteador utilizando una tarjeta de memoria.[32] En ese caso, los diseñadores del gusano aumentarían en gran medida sus probabilidades de éxito en lugar de esperar pasivamente que el software se propague a la instalación. En octubre de 2010, el ministro de inteligencia de Irán, Heydar Moslehi, anunció que una cifra no especificada de "espías nucleares" fueron arrestados en conexión con el Stuxnet.[33] Aunque se desconocen los detalles y la naturaleza de los arrestos, esto (como mínimo) ilustra que Irán reconoce que los diferentes métodos mediante los cuales el gusano pudo haberse propagado—al igual que la gravedad de su impacto en sus operaciones.

Cabe destacar que a finales del 2009, inicios del 2010, Irán retiró del servicio y reemplazó alrededor de mil centrífugas IR-1 en el FEP en Natanz (seis cascadas de 164 centrífugas cada una).[34] El momento escogido para retirar del servicio, junto con la cantidad de centrífugas que se sacaron del servicio, concuerda con el momento y las estructuras de datos del Stuxnet. La explicación obvia de la falla es un defecto de fábrica pero no está claro por qué un defecto de esa índole tomaría tanto tiempo en manifestarse.[35] Del análisis mencionado anteriormente, parece que Stuxnet no intenta destruir inmediatamente las centrífugas. Más bien, ajusta las frecuencias de una manera más sutil con el tiempo—lo que dificulta determinar si un problema fue ocasionado por el gusano o alguna otra parte del proceso de enriquecimiento. Este comportamiento del malware es una explicación más consistente con la retirada del servicio de las centrífugas. Además de retirar las IR-1, el FEP en Natanz también experimentó niveles menos que óptimos de la producción de uranio del 2009-2010. Informes de la IAEA muestran que la cantidad de uranio enriquecido producido en Natanz permaneció relativamente estable en ese momento a pesar del incremento considerable en la cifra de centrífugas.[36] Esto indica que el sistema estaba produciendo uranio por debajo del nivel óptimo.

A pesar de las alegaciones de los iraníes a fines del 2010 que el gusano Stuxnet tuvo un impacto mínimo en sus operaciones nucleares, el experto en seguridad, Ralph Langer, asegura que el malware atrasó dos años el programa nuclear de Irán.[37] Hay dos motivos por ello. Primero, como se mencionó anteriormente, el daño ocasionado por Stuxnet es más sutil—aunque probablemente muy eficaz. Por lo tanto, es difícil atribuir que la falla del equipo fue ocasionada por el software. Segundo, a causa de la naturaleza prolífera de Stuxnet, es muy difícil limpiar el malware de todos los dispositivos de computadora que participaron en el proceso de enriquecimiento. Puede que estas inquietudes expliquen por qué Irán detuvo temporalmente todas las operaciones de enriquecimiento en Natanz en noviembre de 2010 (por motivos desconocidos).[38]

Una pregunta natural de plantear es "¿Qué otros países fueron afectados por el Stuxnet?" Aunque hubo informes del gusano en equipo SCADA en Alemania[39], Finlandia[40] y China[41], ninguna de esas infecciones resultó en daños a los sistemas industriales. Esto puede que se deba a la configuración específica del PLC, ya que Stuxnet solamente lanza ataques en ciertos sistemas. Siemens alega que usuarios de solamente quince sistemas que usan su software reportaron infecciones. De esos quince sistemas, ninguno experimentó daños.[42] Es muy probable que Irán no informara las infecciones a Siemens. Aunque en el periodo de 2002-2003 adquirieron tarjetas controladoras S7-

315 y S7-417, la IAEA estableció que Irán desvió ese hardware a su programa nuclear—lo que resultó en Siemens poniéndole fin a las ventas.[43] Sin embargo, se sabe que la S7-417 fue instalada en Bushehr, que puede haber sido un blanco Stuxnet.[44] En Bushehr, la S7-417 no se obtuvo directamente de Siemens, sino de una empresa rusa conocida como Power Machines Corp., que bajo su contrato iraní la instaló como parte de su sistema Teleperm.

STUXNET ES UN ADELANTO SIGNIFICATIVO EN MALWARE

Al igual que con otros malware maliciosos, Stuxnet se aprovecha de fallas de seguridad no identificadas anteriormente en el software del sistema conocidas como vulnerabilidades tipo "día cero". Ya que este tipo de hazaña no se ha detectado anteriormente, un software anti-virus no las puede identificar. Como punto de referencia, el malware "Arora", responsable de los ataques a Google a fines del 2009 (que fueron generalmente atribuidos a China)[45] depende de una vulnerabilidad tipo día cero. El uso de dos vulnerabilidades tipo día cero sería inaudito.[46] Stuxnet contiene cuatro vulnerabilidades tipo día cero para el sistema operativo Microsoft Windows y una adicional para el software de Siemens. Dos de las vulnerabilidades de Windows que se emplean en Stuxnet tienen que ver con la escalada de privilegios. Estos le permiten al gusano acceso ilegítimo básico o a nivel de administrador al sistema infectado. Los otros dos tienen que ver con la propagación del gusano ya sea a través de una tarjeta de memoria o una red local. Al momento que este artículo fue redactado, la auto-propagación es menos común en malware ya que a menudo es difícil de controlar. Por ejemplo, veamos un "botnet"–una gran cantidad de computadoras infectadas con malware y controladas por un servidor de "mando y control" que no está afiliado legítimamente con las máquinas infectadas.[47] Esta es una plataforma muy común para llevar a cabo delitos cibernéticos. Con un botnet, la propagación ocurre principalmente mediante correos electrónicos basura y sitios web maliciosos—los métodos de auto-propagación son muy limitados.[48]

STUXNET INVALIDA VARIAS SUPOSICIONES DE SEGURIDAD

Nuestro aspecto final del Stuxnet RMA es que invalida varias suposiciones de seguridad. La primera de esas suposiciones es que los sistemas aislados son más seguros. En vista de que los sistemas SCADA, por definición, controlan maquinaria crítica para la misión, muchos administradores no conectan esas computadoras a la red—tratando de lograr la seguridad mediante el aislamiento. Como resultado, la transferencia de archivos a esas máquinas se hace por medios removibles. Los diseñadores de Stuxnet se aprovecharon de esta suposición permitiéndole al gusano propagarse a través de tarjetas de memoria. Una vez que la tarjeta está infectada, el software Stuxnet se auto instala en las computadoras que posteriormente utilizan la tarjeta infectada. La infección comienza cuando el usuario sencillamente hace clic en el ícono asociado en Windows. Esta es una aplicación directa de una de las vulnerabilidades tipo día cero de las cuales Stuxnet se aprovecha.

Otra suposición de seguridad clave que Stuxnet invalida es la relación de confianza establecida por certificados firmados digitalmente. Para poder ofrecer más estabilidad, los sistemas operativos modernos, inclusive Microsoft Windows, limitan el acceso de un programa de computadora a los componentes del sistema. Un programa normal solicita desarrollos del sistema al hardware mediante el controlador software. Como este es el caso, el controlador de software tiene más acceso a los componentes del sistema de nivel más bajo que otros programas. Para evitar la creación fácil de controladores de software maliciosos, Stuxnet utiliza certificados legítimos firmados digitalmente. Este es otro aspecto del malware que no se ha observado anteriormente. Versiones anteriores de Stuxnet empleaban certificados por sistemas semiconductores Realtek—versiones posteriores utilizaban certificados de JMicron Technology Corp. El uso de estos certificados la da al

gusano la apariencia de software legítimo de Windows. Expertos de seguridad en ESET destacan que ambas compañías estaban en Taiwán y que los certificados eran robados. Además, ellos creen que probablemente fue robo físico (quizás un trabajo interno) ya que los certificados digitales para los controladores de software por lo regular no se encuentran en los mercados negros en la Internet.[49]

CONSECUENCIAS PARA EL FUTURO

Stuxnet es sumamente significativo—es un pedazo de malware de la nueva generación que introdujo fallas a suposiciones de seguridad existentes y pudo ocasionar daño en los sistemas industriales que estaban fuera de la Internet. Veamos otros dos ataques como una comparación. Primero, los ciber ataques rusos contra Georgia en el 2008 dependieron principalmente de botnets y hackers activistas para llevar a cabo ataques de negación de servicios contra la infraestructura Internet de Georgia.[50] Estos ataques resultaron en que Georgia perdió temporalmente su acceso a la Internet, principalmente durante operaciones convencionales rusas. Si bien los métodos del ataque eran bien conocidos en la comunidad de seguridad en aquel momento, aún eran significativos por su escala y que ocurrieron a la par de las operaciones convencionales. No obstante, los ataques contra Georgia estaban dirigidos a la infraestructura de las computadoras—no SCADA. De muchas maneras, esos ataques fueron un ejemplo clásico de CBA (ataque a la red de computadoras) —la meta de la actividad cibernética fue degradar una red de computadoras.

En una operación cibernética más reciente conocida como Aora, hackers chinos se las arreglaron para penetrar las redes corporativas de Google en diciembre de 2009 para robar información, inclusive cuentas de correos electrónicos y posiblemente códigos fuentes de computadoras. Arora utilizó una vulnerabilidad tipo día cero en Microsoft Internet Explorer—aprovechándose de una aplicación común que las personas utilizan a diario.[51] Este ataque Cibernético en particular es un buen ejemplo de CNE—explotación de la red de computadoras—ya que los agresores buscaban robarle información al blanco.

Stuxnet es diferente de estos dos casos de varias maneras. Ambos ataques en Georgia y Google estaban dirigidos a redes de computadoras ligadas directa o indirectamente a la Internet. En cualquiera de esos dos casos, un sistema desconectado de la red no se hubiese dañado. Pero no con Stuxnet. Este gusano avanzado tenía la capacidad de cerrar la "brecha aérea". Los administradores de la red a cargo de la seguridad de esos sistemas aislados enfrentan un dilema interesante. Para poder garantizar que esos sistemas están protegidos del último malware, periódicamente deben llevar a cabo actualizaciones. No obstante, al hacerlo, corren el riesgo de propagar una infección (o sea, mediante una tarjeta de memoria o a través de una red en el área local—a través de las cuales Stuxnet se puede propagar).

Otra diferencia clave es que los blancos en los ataques Arora y de Georgia eran otras computadoras. Por otra parte, Stuxnet inflige daños mínimos a los sistemas de informática. En cambio, su meta es dañar un pedazo de equipo en el mundo físico. La admisión de los iraníes nos indica que Stuxnet afectó con éxito una identidad no virtual. Este es un adelanto significativo en armamento—una pieza de software que solamente existe cuando una computadora se enciende fue capaz de conducir un sabotaje con éxito en el mundo real. Stuxnet demuestra claramente que las armas cibernéticas pueden desempeñar un papel significativo en las operaciones—a diferencia de la idea anterior que ese software solamente equivale a "armas de irritación en masa".[52]

¿Cuáles son las consecuencias del software malicioso que pueden afectar equipo en el mundo real? Hay numerosas preguntas que ahora se deben tratar. Recientes audiencias del Senado a raíz del Stuxnet analizan cómo Estados Unidos puede mejorar la protección de sus infraestructuras críticas de esos ataques.[53] Sin embargo, esa es solamente una parte del rompecabezas. Hay muchas preguntas sobre directrices—algunas relacionadas con la ciberguerra en general—que se tornan más importantes.[54] ¿Cómo atribuimos ese tipo de ataque? ¿Cómo respondemos a ata-

ques cibernéticos en la infraestructura SCADA por parte de grupos fuera del gobierno? ¿Cómo el derecho de guerra terrestre aplica a las armas cibernéticas que pueden ocasionar daños en el mundo real?

Hay varias preguntas operacionales y técnicas que también se deben responder. En el ámbito de la ciberguerra, inquietudes técnicas y operacionales a menudo se unen. Por ejemplo, ¿cuál es la mejor manera de identificar vulnerabilidades tipo día cero (las cuales, por definición se desconocen)? ¿Cómo podemos localizar software malicioso, como el Stuxnet, que fue diseñado para no detectarse? ¿Cuáles suposiciones de seguridad estamos haciendo que se pueden invalidar? ¿Cómo hacemos una plantilla de una amenaza cibernética desconocida?

¿Se proliferarán las armas cibernéticas tales como el Stuxnet? Varios expertos de seguridad han pronosticado que variaciones tipo Stuxnet se tornarán más comunes en el 2011.[55] Ya ha habido informes de ataques cibernéticos que no son Stuxnet en equipo industrial en China.[56] Cabe destacar que los análisis gratis de Symantec, Kaspersky Labs, ESET y Langer Communications GmbH, si bien son útiles desde un punto de vista defensivo, pueden utilizarse a la inversa como una inspiración para gusanos tipo Stuxnet.

Por su naturaleza, la ciberguerra cambia rápidamente. Individuos y grupos motivados del gobierno, corporaciones, academia y comunidades de hackers de sombrero negro están escudriñando constantemente los sistemas en busca de las últimas vulnerabilidades. Sin embargo, Stuxnet representa un adelanto evidente en la tecnología de punta como un software y lo que logra. Ha revelado fallas en las suposiciones de seguridad que se deben retomar en niveles múltiples, pero quizás lo más importante es que mostró que el software también se puede emplear como un sistema de armamento decisivo. ❑

Fuente: Este artículo fue publicado anteriormente en Small Wars Journal, abril de 2011, small warsjournal.com

Notas

1. Kupreev Oleg and Ulasen Sergey, Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review, VirusBlockAda, julio de 2010.

2. Un gusano se define como un pedazo de software malicioso que se auto propaga.

3. Nicolas Falliere, Liam O Murchu y Eric Chien, W32.Stuxnet Dossier Version 1.4. Symantec Corporation, febrero de 2011, 7.

4. David Albright, Paul Brannan y Christina Walrond, Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security (ISIS), diciembre, 1.

5. Thomas Erdbrink, "Ahmadinejad: Iran's nuclear program hit by sabotage" (Ahmadinejad: Programa nuclear de Irán atacado por sabotaje), Washington Post, 29 de noviembre de 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html (consultado el 16 de febrero de 2011).

6. Cita de Roel Schouwenberg, Investigador superior de antivirus en Kaspersky Labs en una entrevista en la conferencia Virus Buletin, octubre de 2010, http://www.youtube.com/watch?v=C9H3MrtLgUc (consultado el 156 de febrero de 2011).

7. Martin Brunner, Hans Hofinger, Christoph Krauss, Christopher Roblee, Peter Schoo y Sascha Todt, Infiltrating Critical Infrastructures with Next-Generation Attacks W32.Stuxnet as a Showcase Threat (Infiltrando infraestructuras críticas con ataques de la próxima generación W32.Stuxnet como vehículos para amenazar) , Fraunhofer SIT, diciembre 2010, 23.

8. Falliere, et. al., 55.

9. Williamson Murray, Thinking about Revolutions in Military Affairs (Pensando en las revoluciones en asuntos militares), Joint Forces Quarterly, Verano 1997.

10. Estos incluyen Symantec, Kaspersky Labs, ESET y Langer Communications GmbH.

11. Paul Barford y Vinod Yegneswaran, "An Inside Look at Botnets" (Un vistazo a los botnets) en Malware Detection (Detección de malware), ed. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song y and Cliff Wang, Springer, 2007.

12. Aleksandr Matrosov, Eugene Rodionov, David Harley y Juraj Malcho, Stuxnet Under the Microscope (Stuxnet bajo el microscopio), Revision 1.2, ESET, noviembre de 2010, 5.

13. John D. Fernández y Andrés E. Fernández , "SCADA systems: vulnerabilities and remediation" (Sistemas SCADA: Vulnerabilidades y remedies), Journal of Computing Sciences in Colleges, Vol. 20, No. 4, Abril 2005, 160-168.

14. Thomas Brandstetter, "Stuxnet Malware" CIP Seminar, Siemens, November, 2010.

15. Ralph Langer, "How to Hijack a Controller - Why Stuxnet Isn't Just About Siemens PLCs" (Cómo secuestrar a un controlador – por qué Stuxnet no solo se trata de los PLCs de Siemens), Control Magazine, 13 de enero de 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html (consultado el 16 de febrero de 2011).

16. Falliere, et. al., 39.

17. Ralph Langer, "417 Data Structures = Cascade Structure = Reported Damage" (Estructuras de datos 417 = Estructura en Cascada = Daños reportados) Langer Communications GmbH Blog, 29 de diciembre de 2010, http://www.langner.com/en/2010/12/29/417-data-structures-cascade-structure-reported-damage/ (consultado el 16 de febrero de 2011).

18. Falliere, et. al., 39.

19. Ibid., 41.

20. Langer, Control Magazine.

21. Falliere, et. al., 5.

22. Los diseñadores del Stuxnet lanzaron ataques en tres fases, cada fase utilizando una versión actualizada del software. Los detalles técnicos aparecen en Falliere, et. al.

23. Ibid., 7.

24. Albright, et. al., 2.

25. Ibid., 4.

26. Falliere, et. al., 41.

27. Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)", (Características de la centrífuga de gas para el enriquecimiento de uranio y su relevancia para la proliferación de armas nucleares [corrección]), Science and Global Security, junio de 2008, 14.

28. Ibid.

29. Ralph Langer, "Applying Aqazadeh's revelations to Stuxnet forensic analysis" (Aplicando las revelaciones de Agazadeh al análisis forense de Stuxnet), Langer Communications GmbH Blog, 30 January 2011, http://www.langner.com/en/2011/01/30/applying-aqazadeh%E2%80%99s-revelations-to-stuxnet-forensic-analysis/ (consultado el 16 de febrero de 2011).

30. Erdbrink.

31. Dieter Bednarz y Erich Follath, "Iran's Chief Nuclear Negotiator: 'We Have to Be Constantly on Guard" (Negociador nuclear principal de Irán: Tenemos que estar constantemente alertas), SPIEGEL ONLINE, 18 de enero de 2011, http://www.spiegel.de/international/world/0,1518,739945-2,00.html (consultado 16 febrero de 2011).

32. Falliere, et. al., 3.

33. John Leyden, "Iran boasts of Stuxnet 'nuclear spies' arrests" (Irán se jacta de arrestos de "espías nucleares" Stuxnet), The Register, 4 de octubre de 2010, http://www.theregister.co.uk/2010/10/04/stuxnet_conspiracy_theories/ (consultado el 16 de febrero de 2011).

34. Albright, et. al., 2.

35. Ibid., 3.

36. Ibid., 9.

37. De una entrevista de Yaakov Katz con Ralph Langer en "Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years" (Virus Stuxnet atrasa por 2 años programa nuclear de Irán), Jerusalem Post, 15 de diciembre de 2010, http://www.studentnewsdaily.com/daily-news-article/stuxnet-virus-set-back-irans-nuclear-program-by-2-years/ (consultado el 16 de febrero de 2011).

38. Albright, et. al., 6.

39. "Stuxnet also found at industrial plants in Germany" (Se descubre Stuxnet en fábricas industriales en Alemania), The H Security, 17 de septiembre de 2010, http://www.h-online.com/security/news/item/Stuxnet-also-found-at-industrial-plants-in-Germany-1081469.html (consultado el 16 de febrero de 2011).

40. "Stuxnet Spreads to Finland" (Stuxnet se propaga a Finlandia), The New Internet, Octubre 2010, http://www.thenewnewinternet.com/2010/10/14/stuxnet-spreads-to-scandinavia/ (consultado el 16 de febrero de 2011).

41. John Leyden "Stuxnet worm slithers into China" (Gusano Stuxnet se desliza a China), The Register, 1 de octubre de 2010, http://www.theregister.co.uk/2010/10/01/stuxnet_china_analysis/ (consultado el 16 de febrero de 2011).

42. Brandstetter.

43. Albright, et. al., 5.

44. Ralph Langer, "417 Installed in Bushehr NPP" (Se instala 417 en Bushehr NPP), Langer Communications GmbH Blog, 14 de diciembre de 2010, http://www.langner.com/en/2010/12/14/417-installed-in-bushehr-npp/ (consultado el 16 de febrero de 2011).

45. Timothy L. Thomas, "Google Confronts China's 'Three Warfares,'"(Google confronta las "tres guerras" de China), Parameters, Verano 2010, 101.

46. Entrevista con Roel Schouwenberg en Virus Buletin (ver nota 2).

47. Barford y Yegneswaran, 2.

48. Ibid., 3.

49. Matrosov, et. al., 13. Además consultar el blog técnico ESET en http://blog.eset.com/2010/07/22/why-steal-digital-certificates (consultado el 16 de febrero de 2011).

50. Para más detalles sobre los ataques cibernéticas rusos en Georgia en el 2008, consultar a Stephen Korns y Joshua Eastenberg, "Georgia's Cyber Left Hook" Parameters, Winter 2008-09, 60-76 y Paulo Shakarian, "Analysis of the 2008 Russian Cyber-Campaign Against Georgia" (Análisis de la campaña cibernética rusa en el 2008 contra Georgia), Military Review, por publicarse.

51. Matrosov, et. al., 5.

52. Noah Shachtman, "Terrorists on the Net? Who cares?" (¿Terroristas en la red? ¿A quien le importa?), Wired, 20 de diciembre de 2002, http://www.wired.com/techbiz/it/news/2002/12/56935 (consultado el 16 de febrero de 2011).

53. Para más detalles sobre audiencias del Senado de EE.UU. en noviembre de 2010 a raíz del Stuxnet consultar http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=954c3149-042e-4028-ae23-754868902c44 (consultado el 16 de febrero de 2011).

54. Ver Jeffrey Carr, Inside Cyber Warfare (Dentro de la ciberguerra) para un análisis detallado de estos problemas.

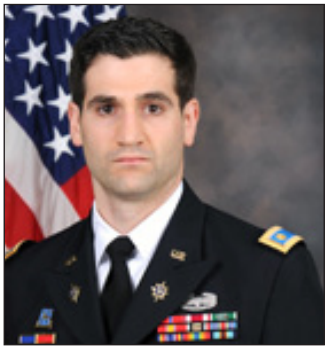
55. Ataques tipo Stuxnet han sido pronosticados por varias empresas profesionales de seguridad en las computadoras, inclusive Symantec Corporation (ver MessageLabs Intelligence: 2010 Annual Security Report). Varios expertos también han hecho esas predicciones en eWeek (http://www.eweek.com/c/a/Security/Stuxnet-Variants-Will-Wreak-Havoc-on-More-Information-Systems-in-2011-373179/) ComputerWeekly (http://www.computerweekly.com/Articles/2010/12/22/244626/StuxNet-prepare -for-worse-in-2011.htm).

56. Fahmida Rashid, "Stuxnet-Like Trojans Can Exploit Critical Flaw in Chinese Industrial Software" (Virus troyanos tipo Stuxnet pueden aprovecharse de fallas críticas en software industrial chino), eWeek, 12 de enero de 2011, http://www.eweek.com/c/a/Security/StuxnetLike-Trojans-Can-Exploit-Critical-Flaw-in-Chinese-Industrial-Software-296674/ (consultado el 16 de febrero de 2011).

REFERENCIAS:

1. Kupreev Oleg and Ulasen Sergey, Trojan-Spy.0485 and Malware-Cryptor.Win32.Inject.gen.2 Review, VirusBlockAda, julio de 2010.
2. Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier Version 1.4. Symantec Corporation, febrero de 2011, 7.
3. David Albright, Paul Brannan, and Christina Walrond, Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? (¿Stuxnet puso fuera de servicio 1.000 centrífugas en la planta de enriquecimiento en Natanz?), Institute for Science and International Security (ISIS), diciembre, 1.
4. Martin Brunner, Hans Hofinger, Christoph Krauss, Christopher Roblee, Peter Schoo, and Sascha Todt, Infiltrating Critical Infrastructures with Next-Generation Attacks (Infiltrando infraestructuras críticas con ataques modernos), W32.Stuxnet as a Showcase Threat, Fraunhofer SIT, diciembre de 2010, 23.
5. Williamson Murray, Thinking about Revolutions in Military Affairs (Pensando acerca de revoluciones en asuntos militares), Joint Forces Quarterly, Verano 1997.
6. Paul Barford and Vinod Yegneswaran, "An Inside Look at Botnets" (Un vistazo a los botnets), en Malware Detection, ed. Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song y Cliff Wang, Primavera, 2007.

7. Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, Stuxnet Under the Microscope Revision 1.2 (Stuxnet bajo el microscopio), ESET, Noviembre 2010, 5.
8. John D. Fernandez and Andres E. Fernandez , "SCADA systems: vulnerabilities and remediation" (Sistemas SCADA: Vulnerabilidades y remedies), Journal of Computing Sciences in Colleges, Vol. 20, No. 4, abril de 2005, 160-168.
9. Thomas Brandstetter, "Stuxnet Malware" (Malware Stuxnet), CIP Seminar, Siemens, noviembre de 2010.
10. Ralph Langer, "How to Hijack a Controller - Why Stuxnet Isn't Just About Siemens PLCs" (Cómo secuestrar un controlador – por qué Stuxnet no se trata solamente de los PLC de Siemens), Magazine, 13 de enero de 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html (consultado el 16 de febrero de 2011).
11. Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)", (Características de la centrífuga de gas para el enriquecimiento de uranio y su relevancia para la proliferación de armas nucleares [corrección]), Science and Global Security, junio de 2008, 14.
12. Timothy L. Thomas, "Google Confronts China's 'Three Warfares,'"(Google confronta las "tres guerras" de China), Parameters, Verano 2010, 101.



El Mayor Paulo Shakarian, Ejército de los EE.UU., es un Profesor Auxiliar en el Departamento de Ingeniería Eléctrica e Informática de la Academia Militar West Point, Ejército de Estados Unidos. Obtuvo su Doctorado y Maestría en Informática de la Universidad de Maryland en College Park y su licenciatura en Informática, con especialización en Seguridad de Información, en West Point. El Mayor Shakarian ha publicado numerosos artículos en varias revistas académicas y profesionales en una variedad de temas, inclusive ciberguerra, informática e inteligencia artificial.