STUXNET, LA PRIMERA CIBERARMA

Erwin Frederick Rivadeneira*

El año 2010 el mundo conoció la existencia de un programa informático malicioso que por primera vez fue mucho más allá de denegar servicios, robar información u obtener dinero, provocando daños materiales en instalaciones físicas, equivalente a un bombardeo de precisión, es decir, se conoció la primera ciberarma.

En el mes de marzo de 2010, los operadores de la planta de enriquecimiento de uranio en Natanz, Irán, se sobresaltaron al darse cuenta que nuevamente los rotores de varias cascadas de centrífugas a gas se aceleraron y desaceleraron sin control, provocando que centenares de ellas presentaran fallas en un muy corto período de tiempo y debiendo dejarlas fuera de servicio. La producción de uranio enriquecido estaba disminuyendo notablemente.

Un par de meses atrás había sucedido algo parecido y lo mismo ocurrió a fines de 2009. El año anterior problemas de sobrepresión habían dejado inservibles varias decenas de centrífugas. Los ingenieros, operadores y mantenedores se preguntaban: ¿Tan mal hechas están las centrífugas IR-1 producidas localmente? Aunque al menos eran baratas y fáciles de fabricar por lo que había bastantes en stock ¿Debimos haber comprado más centrífugas pakistaníes P1 en el mercado negro?, ¿es tan difícil de manejar la tecnología del enriquecimiento de uranio?, ¿qué está pasando en la Planta?, ¿sabotaje?, ¿agentes enemigos infiltrados? Había llegado el momento de analizar a fondo el problema y verificar todos los equipos involucrados, porque por alguna razón desconocida y más allá de su control, se habían destruido más de un millar de centrífugas.

Aunque los iraníes en ese momento no lo sabían, eran víctimas de *Stuxnet*, el primer malware[1] informático, específicamente un gusano,[2] que conseguía ocasionar daños físicos en una instalación industrial y no sólo limitarse a afectar las redes de computadores, equipos informáticos o robar información sensible. En esta ocasión se estaba produciendo la destrucción material de las centrífugas a gas. Era la primera vez que un programa informático estaba siendo usado como armamento, consiguiendo a través de 500 KB de líneas de código, almacenados inicialmente en un dispositivo USB del tipo *pendrive*, un efecto similar a un bombardeo aéreo de precisión o a un misil del tipo Dispara y Olvida *(Fire and Forget)*. La primera ciberarma había entrado en acción.

El uranio y su enriquecimiento

La razón del uso de *Stuxnet* contra Irán está relacionada con el elemento químico uranio y su posible uso en la construcción de bombas atómicas. En su estado natural el uranio tiene dos

* Capitán de Corbeta, Guerra Electrónica. (efrederick@armada.cl).
1. Malware: Abreviatura de malicious software o programa malicioso.
2. Gusano informático: Tipo de malware que puede reproducirse automáticamente e infectar a otros computadores sin necesitar acciones por parte del usuario.

isótopos, el U-238 que se encuentra concentrado al 99,3% y el U-235 con el 0,7% restante, siendo este último el único fisible, es decir, que puede ser dividido en dos o tres fragmentos y podría hacer una reacción nuclear en cadena, si es que contiene la masa crítica o concentración necesaria para desencadenarla. El uranio 238 puede convertirse también en otro material fisible, el plutonio, mediante procesos en reactores nucleares, algo que sólo puede ser ejecutado actualmente por las grandes potencias nucleares.

Dependiendo del grado de enriquecimiento del uranio, se puede producir energía eléctrica con el denominado *Low Enriched Uranium* entre el 3% y el 20% de concentración de Uranio 235 o bombas atómicas con el *High Enriched Uranium*, enriquecido por sobre el 90%. Para enriquecer Uranio uno de los métodos posibles, quizás el más accesible para los países que dan los primeros pasos en esta materia, es el uso de centrífugas a gas. El gas Hexafloruro de Uranio (UF6) es separado por la diferencia de peso molecular entre los gases del uranio 235 y 238 mediante centrífugas de alta velocidad.

El programa nuclear iraní

Irán entró al programa nuclear con fines pacíficos a partir de 1950 y recibió apoyo incluso de Estados Unidos. Se adhirió al Tratado de No Proliferación Nuclear y comenzó a recibir desde 1957, por mandato de la ONU, inspecciones de parte de la Agencia Internacional de Energía Atómica. Sin embargo, el objetivo inicial de sólo producir energía eléctrica fue derivando secretamente en los primeros pasos del desarrollo de armas nucleares, lo que produjo que la Agencia no pudiera comprobar el uso pacífico de las instalaciones y pusiera la voz de alerta. En el año 2003, producto de presiones internacionales, detuvo sus trabajos y reconoció haber hecho avances en el proceso de enriquecimiento del uranio a partir de 1997 y de haber recibido apoyo e información a través de una red en el mercado negro dirigida por el físico nuclear pakistaní Abdul Kadeer Khan. Este era un antiguo diseño de centrífugas a gas de los años setenta obtenido en Europa Occidental y eficazmente implementado por Pakistán. A partir del año 2006, el nuevo presidente de Irán, Mahmoud Ahmadinejad, en contraposición a todo lo dispuesto por la Agencia y la ONU, reinició los trabajos y dio un gran apoyo a los proyectos nucleares, reanudando los procesos de enriquecimiento de uranio, de producción de agua pesada y de investigación y desarrollo en esta materia.

Durante el año 2008, desafiando abiertamente a Occidente, Irán mostró al mundo su capacidad de enriquecer uranio en la planta piloto de enriquecimiento de Uranio, ubicada sobre la superficie en Natanz, provincia de Isfahan, explicando que habían desarrollado exitosamente la capacidad para enriquecer el Uranio hasta el 3,5% y que podrían llegar a enriquecer hasta un 20%. Teóricamente y en un tiempo difícil de determinar, este uranio podría ser sometido al proceso las veces necesarias para obtener un enriquecimiento que permitiera su empleo en bombas atómicas.

Esta situación no podía ser tolerada por Estados Unidos, al comprometer su política de no proliferación, ni menos aún por Israel que posiblemente sería el primer blanco de una bomba nuclear iraní. Aparentemente la vía diplomática y las sanciones económicas no estaban logrando los efectos deseados, por el contrario, parecían darle más fuerza a Irán para conseguir su objetivo, por lo que la vía militar clásica parecía ser la única opción válida para evitar que Irán obtuviera su bomba. Se analizaron las opciones y probablemente la más efectiva resultaba ser la misma que se había empleado contra Irak en 1981, que terminó con la destrucción de un reactor nuclear en construcción en Osirak y la misma opción se utilizó contra Siria en el año 2007, en ambos casos se emplearon bombardeos aéreos efectuados por la Fuerza Aérea Israelí. En aquella última oportunidad, el ataque presentó una convergencia perfecta entre la guerra electrónica y la guerra informática para suprimir las defensas aéreas sirias y permitir un bombardeo de precisión sobre el objetivo, que terminó con la completa destrucción del blanco y sin bajas en los aviones atacantes. Pero Natanz presentaba serias dificultades en cuanto a la distancia al objetivo, la profundidad en que se encontraba la nueva planta, 15 metros bajo tierra, y en cuanto a la fuerte protección antiaérea de las instalaciones, por ende el riesgo de efectuar

un ataque aéreo era muy alto. Probablemente sin descartar totalmente un eventual ataque aéreo en el futuro, Estados Unidos pudo convencer a Israel de emplear una estrategia alternativa para retrasar los planes de Irán, la cual fue supuestamente denominada "Operación Juegos Olímpicos" y que constituiría el primer empleo del ciberespacio como un campo de batalla con ciberarmas. Ni Estados Unidos ni Israel reconocieron oficialmente su participación en esta operación: el empleo del malware que el mundo conocería posteriormente como *Stuxnet*.

Stuxnet 0.5: El ataque de sobrepresión en las centrífugas

En su planta de Natanz, los iraníes implementaron un proceso de enriquecimiento de uranio con centrífugas a gas empleando varias etapas, denominado en cascada ya que la salida de una etapa era la entrada de la siguiente, en las cuales el uranio pasaba por varios grupos de centrífugas que iban progresivamente enriqueciéndolo. El sistema de protección de esta arquitectura, Sistema de Protección de Cascada, se implementó con la intención de tener maneras de aislar centrífugas individualmente cuando presentaran inconvenientes[3] e incluso permitir cambiarlas sin detener el proceso productivo. Cada centrífuga contaba con tres válvulas de activación rápida que podían cortar el flujo de alimentación de gas, de descarga del producto enriquecido y de descarga del producto empobrecido, de manera de poder aislarlas parcial o totalmente, asimismo, también existían válvulas auxiliares que conectaban las etapas y un sistema de monitoreo central y protección que permitía vigilar permanentemente desde la Sala de Control el funcionamiento de cada una de ellas, de los controladores y dispositivos asociados y de las etapas de cada una de las cascadas.

La debilidad intrínseca, que ofrecía la posibilidad de ser explotada, era la fragilidad material de las centrífugas a gas, por lo que los autores diseñaron un método para hacer fallar el enriquecimiento de uranio iraní dañándolas lentamente, pero en forma progresiva. Para conseguir su objetivo había que diseñar y ejecutar un sofisticado ciberataque que comprendiera las tres capas involucradas: La capa de las Tecnologías de Información (TI), es decir, los Sistemas Operativos, las redes y la aplicaciones informáticas, para introducir y propagar el malware; la capa de los Sistemas de Control Industrial, que involucra los sistemas de control automático y controladores industriales como los conversores de frecuencia o controladores de presión, para poder manipularlos a voluntad y finalmente la capa física, es decir, las válvulas, líneas eléctricas, bombas o rotores que es donde finalmente se buscaba producir la destrucción o daños materiales.

La primera versión de *Stuxnet* empleaba una vulnerabilidad de día-cero, es decir, un error de programación no descubierto previamente en una aplicación o sistema operativo que podía ser usado para vulnerar o tomar el control de un dispositivo informático, al permitir modificar la carga de archivos de librerías del software Step 7, un software de la empresa alemana Siemens, empleado para crear en un computador con sistema operativo Windows, una interfaz hombre-máquina simple que permitiera programar o modificar un Controlador Lógico Programable (PLC), dispositivo empleado para el control automático de sistemas industriales.

Este programa se ejecutaba al cargarse un archivo malicioso en vez del correcto, el cual podía ingresar al computador principalmente a través de un dispositivo USB, mediante la transferencia del archivo entre computadores o como adjunto por correo electrónico. Es importante mencionar que esta vulnerabilidad fue descubierta y corregida recién el año 2012. Para propagarse a otros computadores, este malware infectaba cualquier dispositivo USB que se conectara en un computador infectado, y por medio de la red local a través de un uso abusivo de las comunicaciones punto a punto.

Una vez instalado en un computador infectado, el malware, desde el año 2005, reconocía las características del computador en que se encontraba e intentaba conectarse con sus servidores de mando y control a cuatro sitios aparentemente comerciales en Internet alojados en diferentes lugares del mundo, de manera de reportarse y recibir actualizaciones o nuevas instrucciones mediante un canal encriptado, si no tenía éxito,

3. Los iraníes sabían que sus centrífugas, copiadas de las pakistaníes, eran de regular calidad y esperaban tener una cierta tasa de fallas.

estaba programado para ser completamente autónomo. Posteriormente, buscaba la presencia de su único blanco válido, el PLC Siemens S7-417, con ciertos componentes asociados específicos y en la exacta configuración para lo cual estaba programado. Si no los encontraba no producía daño alguno, sólo intentaba seguir propagándose, pero si encontraba su objetivo pasaba a la etapa siguiente.

De esa forma, el malware empezaba a ocupar su carga útil e iniciar un ataque del tipo hombre en el medio, en el cual capturaba y podía modificar todas las comunicaciones entre el computador y el programador lógico programable en ambos sentidos, con lo cual quedaba en condiciones de dar cualquier orden al controlador lógico y responder o presentar lo que quisiera al programa de control o monitoreo, o en último caso no efectuar modificación alguna. De esta manera conseguía tomar el control completo de los sistemas de control automático y podía forzarlos a operar fuera de sus parámetros de seguridad. Cabe destacar que de esta manera el malware podía abrir o cerrar una válvula, variar la lectura de un sensor, etc., mientras para el software de control y para el personal operador o supervisor todo seguía normal, con valores dentro de parámetros y funcionando correctamente. Con esto el sistema SCADA (Supervisory Control and Data Acquisition), de control y supervisión de procesos industriales estaba absolutamente comprometido.

El paso siguiente fue saber correctamente qué hacer para causar daño, para lo cual se requería una gran información de inteligencia previa y profundos conocimientos técnicos del funcionamiento del enriquecimiento de uranio iraní y sus sistemas de seguridad, además de poder contar con un grupo de trabajo multidisciplinario provisto de expertos en el área informática y de diversas ramas de la ingeniería y control industrial, de tal forma de ser realmente efectivo.

Básicamente, lo que el malware hacía era grabar un período de tiempo de operación normal y reproducirlo en un ciclo constante en los sistemas de monitoreo, mientras en una etapa completa se cortaba el flujo de salida del producto uranio, tanto del enriquecido como del empobrecido, manteniendo la alimentación de gas UF6. Al mismo tiempo, se aislaban progresivamente un elevado número de centrífugas, para aumentar la presión del gas en aquellas no aisladas, hasta llegar teóricamente a una solidificación de éste, lo que causaría la destrucción casi inmediata de la centrífuga o de varias de ellas.

Se estima que este método de ataque no fue descubierto por los iraníes hasta bastante tiempo después y solo gracias al análisis de la versión posterior de *Stuxnet*, que mantenía parte de este código, pero se encontraba desactivado, por lo que el personal de la Planta de Natanz debe haber atribuido las fallas en las centrífugas a cualquier otra causa.

Stuxnet 1: El ataque de sobrevelocidad en los rotores de las centrífugas

No sabemos si los atacantes se decepcionaron de los resultados del primer método, era muy complicado y preveían que en corto plazo no resultaría exitoso, no querían causar una falla total del software la cual podría ser fácilmente descubierta, querían evitar la destrucción de varias cascadas simultáneamente, querían hacerse notar, querían probar algo nuevo; o simplemente cambiaron los mandos o sus órdenes, por lo que entró en acción la segunda versión del que fue posteriormente bautizado *Stuxnet* y fue el que realmente se hizo conocido a nivel mundial el año 2010.

Si bien *Stuxnet* 0.5 era más simple en sus aspectos informáticos, lo que lo hacía bastante sigiloso, tenía un tremendo potencial para causar muy graves daños en su objetivo; por otra parte *Stuxnet* 1 mostró una mayor sofisticación y agresividad en los aspectos técnicos del área informática, aunque produciendo acciones físicas más simples y directas. Sin embargo, al incluir varias formas de propagarse, era posible perder el control de su propagación y por ende era más fácil de detectar.

Esta evolucionada y más compleja versión ocupaba no menos de cuatro vulnerabilidades de día-cero del sistema operativo Windows,[4]

4. Cada una de ellas podría tener en esos años un costo en el "mercado gris", supuestamente reservado para agencias de inteligencia, fuerzas armadas y policías, de entre US $ 50.000 y US $ 150.000, duplicándose dicho costo en el "mercado negro" empleado por cibercriminales.

además de dos certificados digitales robados, pertenecientes a las empresas RealTek y JMicron, marcas conocidas y hasta ese momento confiables, ambas ubicadas en un mismo centro tecnológico en Taiwán. Al igual que *Stuxnet* 0,5 la manera de ingresar a las redes desconectadas de Internet era a través de memorias USB, que al conectarse a un computador hacía que este se infectara inmediatamente.

Sin embargo, el blanco principal fue el controlador Siemens S7-315, encargado de los rotores, asociado a conversores de frecuencia de un modelo y dos fabricantes específicos, el cual operaba de forma similar a *Stuxnet* 0,5. Cuando el malware tomaba el control de los PLC, aumentaba la velocidad de rotación de las centrífugas a gas de una velocidad normal de 63 000 RPM a 84 600 RPM, para después detenerlas casi completamente a 120 RPM, produciendo con el frenazo una alta carga de trabajo a los materiales de la centrífugas y degradar la eficiencia del proceso de enriquecimiento. Este proceso se podía repetir varias veces.

De acuerdo a los análisis posteriores, se ejecutaron al menos tres oleadas de ataques con *Stuxnet* 1 de una duración cercana a un mes, las cuales se desarrollaron en junio de 2009, marzo de 2010 y mayo de 2010, dañando centenares de centrífugas y causando serías dudas a los iraníes sobre la estabilidad de la Planta y la viabilidad de su programa de enriquecimiento de uranio.

Además, dadas las capacidades de este malware para comunicarse con sus servidores de mando y control, enviar información encriptada, abrir puertas traseras y comprometer computadores en forma remota, *Stuxnet* 1 también se empleó para acciones de espionaje y robo de información de varias empresas iraníes relacionadas con los sistemas de control industrial y con la fabricación de equipos metálicos como las centrífugas. Este espionaje permitió estudiar los progresos de Irán y analizar más detalladamente la mejor manera de producir fallas y retrasar el programa nuclear de ese Estado en ese momento y probablemente también en el futuro.

Sin embargo, la manera de infectar a los computadores también produjo que el malware se propagara sin control cuando el personal iraní encargado del mantenimiento de los sistemas conectó sus computadores portátiles infectados a Internet y el malware se expandió mucho más allá de las redes locales, por lo que *Stuxnet* traspasó fronteras y se propagó a otros países como Indonesia, India, Azerbaiyán, Pakistán y el mismo Estados Unidos, entre otros.

El descubrimiento

Al investigar inconvenientes en algunos computadores de un cliente en Irán, la empresa de antivirus bielorusa VirusBlokAda, fue la primera en detectar el malware el 24 de junio de 2010 y hacerlo público el 17 de julio de ese mismo año.

Las personas que analizaron el malware se dieron cuenta de inmediato de las características muy especiales de éste, que lo hacían completamente diferente a lo anteriormente visto. El tamaño del código, alrededor de 500 KB, era muchísimo mayor a los 10 o 15 KB que acostumbraban tener los programas maliciosos en ese momento, incluso el complicado gusano *Conficker* tenía solamente 35 KB y el malware buscaba reconocer objetivos muy específicos para actuar, como por ejemplo ciertas aplicaciones de monitoreo industrial de la empresa Siemens y en una configuración muy específica. Todo esto, sumado a los cuatro ataques de día-cero que no eran empleados para obtener dinero, sino que los autores tenían un blanco muy particular y apoyo o encargo de algún gobierno.

Tiempo después vino la mayor sorpresa al ser posible determinar cual era exactamente el blanco seleccionado por los autores de *Stuxnet*, la planta de enriquecimiento de Uranio de Natanz, la complejidad de su diseño, su precisión para detectar y atacar solamente su blanco y su novedosa forma de actuar que le permitía producir daños físicos. Por primera vez en la historia se había descubierto una ciberarma.

Resultados de los ataques

Los resultados materiales de los ataques aunque en un principio parecieron muy graves y causaron gran alarma y confusión a los iraníes, en realidad no lo fueron tanto. La destrucción de aproximadamente un 11% del total de centrífugas en Natanz, alrededor de mil, fue un golpe duro al

programa, pero los iraníes pudieron recuperarse gracias a la gran cantidad de centrífugas disponibles, las que fueron cambiadas progresivamente y en general el proceso de enriquecimiento de uranio continuó, aunque con algunos retrasos y una tasa de producción menor a la esperada. Se estima que *Stuxnet* produjo un retraso en el programa nuclear iraní de entre 12 y 18 meses.

La industria de los antivirus y de la seguridad informática estudiaron a fondo el malware, pudiendo comprender el detalle de su funcionamiento y las medidas de mitigación, prevención y de recuperación necesarias, así como su origen, las que sin duda ayudaron a Irán y a otros países afectados por el malware, que se propagó sin control por Internet.

Irán, al principio un país débil (en cuanto a organización y capacidades) en materias de ciberdefensa, aprendió duramente la lección y al igual que otros países que han recibido ciberataques de diversa índole, se encuentra en la actualidad mejor organizado y es mucho más fuerte en el ciberespacio, tanto en acciones defensivas como ofensivas, que bien podrían ser empleadas contra los países que están detrás de *Stuxnet*.

Pronto aparecieron nuevos malware similares e incluso más avanzados que *Stuxnet*. Nombres como *Duqu, the Flame* y otros se hicieron presentes en el ciberespacio, dispuestos a encontrar sus blancos y ejecutar su carga con oscuros propósitos. Posiblemente algunos tengan los mismos autores que *Stuxnet* intentando nuevos ataques sobre los mismos objetivos iniciales. El avance en el desarrollo nuclear de Irán en el tiempo, los resultados de las acciones diplomáticas o la realización de ataques convencionales sobre estos blancos nos darán una idea de los resultados que finalmente se obtengan.

Sin embargo, más de cinco años han pasado desde la aparición de la primera ciberarma con resultados muy prometedores, que abrieron una serie de posibilidades de empleo con fines militares, pero hasta el momento no ha aparecido ni se ha podido confirmar la existencia de otra de ellas con la capacidad de producir daños físicos contra objetivos militares como *Stuxnet*. ¿Qué habrá pasado con las ciberarmas? ¿Se dejaron de lado por no ser tan efectivas como se pensaba inicialmente?

Probablemente las naciones que tienen la capacidad no se han decidido todavía a usarlas y las que si tienen decidido utilizarlas todavía no tienen la capacidad para ejecutarlo de forma efectiva. O tal vez… ¿En ambos casos se están preparando silenciosamente para un devastador ataque en el futuro?

Conclusiones

Stuxnet nos abrió los ojos de cómo podría ser un ataque informático o la ejecución de una guerra informática ¿Estamos preparados? ¿Qué pasaría si un malware específicamente diseñado entrara en el sistema de control de la plataforma de un submarino? ¿Si un virus se instalara en la aviónica y sistema de combate de un cazabombardero? ¿Si ese computador desconectado de la red de los sistemas de armas de una fragata se contaminara con un malware? ¿Si un programa malicioso toma el control de la distribución de la energía eléctrica de una ciudad? ¿Si un malware compromete una planta de agua potable? Las respuestas son todas alarmantes y aunque las podamos ver como situaciones lejanas, *Stuxnet* demostró que la posibilidad que una compleja plataforma, sistema industrial o sistema de armas quede inutilizada o destruida por un malware, que consiste en nada más que líneas de código de un programa computacional, está mucho más cerca de lo que parece.

Este malware nos demostró que las ciberarmas ya existen y pueden llegar a producir efectos militares similares al armamento convencional.

El uso de ciberarmas aparentemente evitó (o al menos postergó por un tiempo indefinido) un ataque convencional israelí o estadounidense sobre el programa nuclear iraní.

Sin embargo, el resultado de un ataque solamente con ciberarmas en el denominado ciberespacio, sigue siendo bastante incierto, difícil de evaluar y no garantiza conseguir los objetivos o el cumplimiento de la misión, por lo que debería ser empleado en conjunto con otras acciones militares convencionales.

* * *