Campaña de Ciberespionaje a las empresas de Energía

La solución SCAB ayuda a la detección y prevención de esta amenaza

Autores:

Joel Langill – Industrial Cyber Security Expert, Founder of SCADAhacker.com
Emmanuele Zambon, Ph D – SecurityMatters Founder and CTO
Daniel Trivellato, Ph D – SecurityMatters Product Manager

Traducido por Enrique Martín García

TELVENT Global Services

C/ Valgrande, 6
28018 Alcobendas
Madrid – Spain

enrique.martingarcia@telvent.com

Contenidos

Introducción 2

La campaña de ciberespionaje Dragonfly..... 2

El atacante 3
Los objetivos 3
Los vectores de ataque 3
Operación del malware..... 4

SCAB detecta el malware utilizado por Dragonfly . 5

El patrón de comportamiento de red 5
Detección de análisis de la red 6
Detección de la comunicación con C & C 7

Conclusiones 7

Agradecimientos..... 7

Referencias..... 8

Introducción

En el mes de Julio de 2014, algunos fabricantes de soluciones de ciberseguridad [1,2,3] han anunciado el descubrimiento de una exitosa campaña de ciberespionaje llevada a cabo por el grupo de hackers Dragonfly. En la última cadena de atentados que Dragonfly ha dirigido a varias empresas de energía estadounidenses y europeas, lograron recoger información valiosa en lo que parece ser el siguiente paso en la campaña de guerra cibernética contra las organizaciones de infraestructura crítica, después de Stuxnet en 2010. Algunos proveedores de ciberseguridad han analizado la campaña y han presentado un análisis del malware empleado por Dragonfly para robar información de los ordenadores infectados.

Este breve artículo revisa los puntos principales de esta investigación e ilustra por qué la implementación de una estrategia de defensa en profundidad es la clave para hacer frente con éxito a las ciberamenazas como Dragonfly.

La campaña de ciberespionaje Dragonfly

El grupo de hackers Dragonfly ha montado con éxito una operación de ciberespionaje contra compañías estadounidenses y europeas, principalmente en el sector energético. El grupo logró instalar una herramienta de acceso remoto (RAT) en los ordenadores utilizados para el funcionamiento de sistemas de control industrial (ICS), y para recoger datos desde las máquinas infectadas utilizando un *payload* diseñado para detectar un protocolo industrial específico. De acuerdo con Symantec [1], la campaña de Dragonfly parece tener un enfoque mucho más amplio que el de la campaña Stuxnet: "Mientras Stuxnet fue dirigido contra el programa nuclear iraní y tenía el sabotaje como meta principal, Dragonfly parece tener un enfoque mucho más amplio, con el espionaje y el acceso persistente como su objetivo principal, siendo el sabotaje una capacidad opcional si fuera necesario. "No ha habido ninguna prueba de que las capacidades de sabotaje fueran utilizadas por el grupo Dragonfly a fecha de hoy, pero pueden existir estas capacidades en las herramientas empleadas, lo que representa, posiblemente, la más temible parte de la historia, ya que podría abrir las puertas a potenciales escenarios dramáticos.

¿Ha sido el robo de información de control industrial de las empresas de energía sólo el primer paso de una campaña destructiva de ciberguerra?

El atacante

El grupo de hackers Dragonfly (también conocido como Energetic Bear) parece que está en funcionamiento desde el año 2011. Inicialmente estaba destinado a organizaciones en las industrias de defensa y aviación en EE.UU. y Canadá, antes de pasar su atención a las empresas de energía de Estados Unidos y Europa del Oeste en 2013. Un análisis de el código de malware utilizado en la campaña ha demostrado que el grupo operó en su mayoría desde Europa del Este durante las horas de trabajo (de lunes a viernes de 9am a 6pm, hora UTC +4), lo que sugiere que la mayoría de los miembros del grupo trabajaron en esa región. La complejidad de la operación lleva a muchos a creer que Dragonfly es un grupo bien financiado, posiblemente patrocinado por estados adversarios.

Los objetivos

Hasta ahora, la campaña ha dado lugar a la fuga de información de múltiples organizaciones, muchas de las cuales operan en el sector de la energía, que van desde empresas de generación de electricidad, los operadores de distribución de redes de Gas y petróleo, y los proveedores de equipos industriales. La mayoría de las víctimas se encuentran en Europa, seguida por los EE.UU. La figura 1 muestra los 10 primeros países por infecciones activas (es decir, cuando el atacante ha extraído información de los ordenadores infectados). En total, el número de máquinas infectadas que intentaron informar a un servidor de malware de comando y control (C & C) es de aproximadamente 1500 [3]. Estos números representan los sistemas que han sido comprometidos y que han establecido las comunicaciones de C & C, lo que no necesariamente representan el número de sistemas de control industrial reales comprometidos (esto se discutirá con más detalle más adelante en este artículo). La información precisa sobre el alcance del compromiso de dispositivos de control no está disponible en el momento de la redacción de este estudio, pero se espera que sea significativamente menor que la que se muestra en el siguiente cuadro.

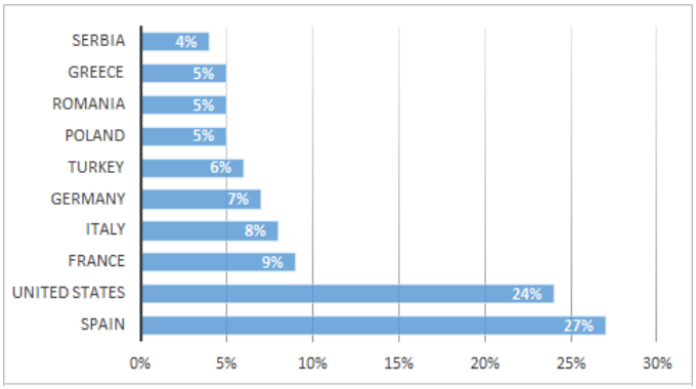

Figura 1. Los 10 países por infecciones activas [1]

Los vectores de ataque

Dragonfly usa dos piezas de malware en el ataque; ambas eran herramientas de acceso remoto (RAT) diseñadas para llevar a cabo las operaciones de ciberespionaje. Las RAT fueron distribuidas y llegaron las máquinas de las víctimas a través de tres tipos de ataque:

- Campañas de E-mail: ejecutivos seleccionados y empleados de alto rango de las empresas en cuestión recibirían correos electrónicos con un archivo PDF adjunto malicioso que contiene la RAT. Symantec identificó siete organizaciones diferentes receptoras de la campaña; el número de correos electrónicos enviados a cada organización fue de 1 a 84 [1].
- Ataques tipo *Watering Hole*: estos ataques se dirigieron una serie de sitios web legítimos con muchas posibilidades de ser visitados por personas que trabajan en el sector energético. Al visitar uno de los sitios web infectados, el visitante sería redirigido a otro sitio web legítimo comprometido que contendría un paquete de exploits. Este kit de exploits instalaría la RAT en el ordenador del visitante.
- Software descargado de proveedores de Sistemas de Control Industrial: Los miembros de Dragonfly lograron hackear los sitios web de al menos tres diferentes proveedores de sistemas de control industrial, e insertar el malware en el software legítimo que estaba disponible para su descarga a sus clientes. El malware entonces se instalaría en el ordenador de la víctima al descargar la actualización de software de confianza. Los fabricantes comprometidos se encuentran en Alemania,

Suiza y Bélgica. El primer paquete de software identificado como *troyanizado* se utiliza para proporcionar acceso VPN a un controlador lógico programable (PLC) y dispositivos similares. La segunda empresa fabrica un dispositivo de tipo PLC, y tenía uno de sus drivers de comunicación *troyanizado*. La tercera compañía incluida en esta campaña desarrolla sistemas de control industrial para los mercados de la energía, principalmente renovables.

Dragonfly empleó estos vectores de ataque en tres fases sucesivas de la campaña. Los ataques de correo electrónico se realizaron entre febrero y junio de 2013; fueron seguidos por los ataques de *Water Holing* comenzando en junio de 2013 que incluía el compromiso de los sitios web de proveedores del ICS. La primera página web del fabricante de sistemas de control se vio comprometida durante el período de junio-julio de 2013, seguido por el segundo proveedor en enero de 2014. Este segundo proveedor fue capaz de identificar la violación, notificando a los usuarios afectados y mitigando la situación. Se estima que alrededor de 250 descargas del software infectado se produjeron durante esta fase [4]. El compromiso de la página web del último proveedor se produjo en abril de 2014.

Operación del malware

Los atacantes utilizaron dos RAT para robar información de los ordenadores infectados y enviarla a los servidores C & C bajo el control de los atacantes. Ambos RAT proporcionan la capacidad de descargar y ejecutar archivos de forma remota a través de los servidores C & C:

- El Havex RAT (también conocido como Backdoor.Oldrea): Permite al atacante extraer los datos de la libreta de direcciones de Outlook y archivos de configuración de software utilizados para el acceso remoto desde el ordenador infectado a otros sistemas industriales de control. Además, recoge información de los programas instalados en el sistema, listas de archivos locales y unidades disponibles.
- Karagany (Trojan.Karagany): Permite a los atacantes subir y descargar archivos desde el ordenador infectado y ejecutar programas. También contiene funciones avanzadas para recoger contraseñas, realizar capturas de pantalla, y la catalogación de los documentos almacenados en la máquina de la víctima. Karagany ya estaba disponible en el mercado negro, aunque el grupo Dragonfly podría haber modificado el código fuente para que se adaptara mejor a sus propósitos.

La mayoría de las víctimas fueron infectadas con el Havex RAT; Karagany fue identificado sólo en el 5% de los ordenadores infectados. Havex parece ser malware hecho a medida, ya sea escrito por el propio grupo Dragonfly o encargado por ellos. Los analistas de seguridad de F-Secure [3] han identificado y analizado **88** variantes de Havex, que contactaron **146** servidores C & C para comunicar la información robada. La mayoría de los servidores C & C hospedaban blogs y sistemas de gestión de contenidos, supuestamente comprometidos por los atacantes utilizando *exploits* similares. Estas cifras refuerzan la creencia de que la operación es patrocinada por algún Estado.
Desde un punto de vista operativo, ciertos *payloads* desplegados con la RAT de Havex RAT mostraban la intención de realizar un escaneo a redes de control industrial. En particular, trata de enumerar y clasificar los dispositivos de control conectados a la red local, y enviar los resultados a los servidores C & C. Un análisis de los ejecutables de malware pone de relieve que los atacantes buscaban servidores OPC (Open Platform Comunicaciones [5]). OPC es un protocolo de intercambio de datos bidireccional en tiempo real que soporte lectura / escritura de variables de proceso, pero no admite la capacidad de realizar funciones más avanzadas, como las actualizaciones de configuración de dispositivos y *firmware*. OPC es una forma estándar para los sistemas de control de procesos, aplicaciones y dispositivos para interactuar con los demás.

Es importante tener en cuenta que no todas las variantes del Havex RAT y sus *payloads* asociados contenían el código utilizado para enumerar los servicios OPC en una red. Los únicos *payloads* que contienen referencias a la detección de servidores OPC se cree que se instalaron sólo a través de las descargas de software infectado de los tres sitios web de proveedores de sistemas de control mencionados. Esta conclusión se basa en el análisis de malware apuntado por F-Secure [3] y la obtenida a través de VirusTotal. Esto significa que el número real de sistemas de control comprometidos es probablemente mucho menor que el número identificado de hosts / sitios infectados por el malware Havex.

La siguiente figura muestra el extracto correspondiente al *payload* Havex que contiene el código de enumeración de Servidores OPC en la red[3].

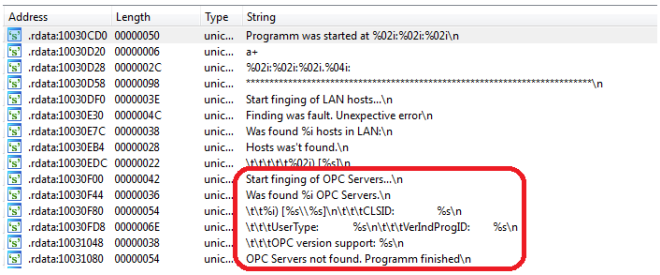

Figura 2. Extracto del ejecutable Havex [3]

Mirando el código del malware, podemos ver que utiliza los interfaces del Microsoft Component Object Model (COM) para detectar si las máquinas identificadas durante la exploración ejecutan servicios OPC. Las dos interfaces COM que se encuentran en el código son los siguientes:

- IOPCServerList (IID = 13486D51-4821-11D2-A494-3CB306C10000)
- IOPCServerList2 (IID = 9DD0B56C-AD9E-43EE-8305-487F3188BF7A)

El hecho de que Dragonfly esté reuniendo información acerca de los servidores OPC y las conexiones VPN a PLC podría indicar que el objetivo final es tener acceso a los propios autómatas, lo que permitiría a los atacantes modificar, dañar o alterar los procesos críticos a cargo de las organizaciones afectadas.

SCAB detecta el malware utilizado por Dragonfly

La solución Security Control Awareness Box (SCAB) para Sistemas SCADA de TELVENT Global Services está basada en el producto SilentDefense ICS de Security Matters. SCAB es capaz de detectar Havex en varias etapas de su funcionamiento, e inmediatamente alertar al equipo de seguridad de la amenaza, lo que permite a la víctima afectada tomar medidas antes de que se produzca algún daño o se logre extraer información sensible de la red. En particular, SCAB detecta Havex tanto cuando intenta conectar con el servidor C & C para descargar o cargar archivos e información, y cuando busca en la red para enumerar los dispositivos. En los párrafos siguientes se ilustra cómo SCAB habrían detectado y alertado sobre el comportamiento Havex.

El patrón de comportamiento de red

SCAB es un sistema de detección de intrusiones de red y monitorización que genera automáticamente el modelo de comportamiento aceptable y normal de la red y alerta cada vez que algún dispositivo de red realiza actividades que se apartan de su funcionamiento esperado. SCAB opera en dos fases. En primer lugar, se analizan las comunicaciones de la red y se genera el patrón de comportamiento de la red de control (ICS Network Behavioral Blueprint ™).

El patrón de comportamiento define los flujos de comunicación, protocolos, tipos de mensajes, los campos de mensajes y valores de los campos que son normales para el proceso. El patrón de comportamiento revela inmediatamente una mala configuración de la red o de algún sistema (por ejemplo, los dispositivos no autorizados), las comunicaciones no deseadas, y los valores de campo inusuales empleadas en la red, en caso de que Havex ya hubiera infectado algunos dispositivos. Después de esta fase de instalación, SCAB se puede utilizar para la monitorización continua y detectar cuando los dispositivos de red realizan actividades no deseadas.
En el caso de Havex, estas actividades no deseadas están representados por el análisis de la red y la comunicación con los servidores C & C. Las figuras 3 y 4 muestran algunos ejemplos del patrón de comportamiento obtenido por SCAB.

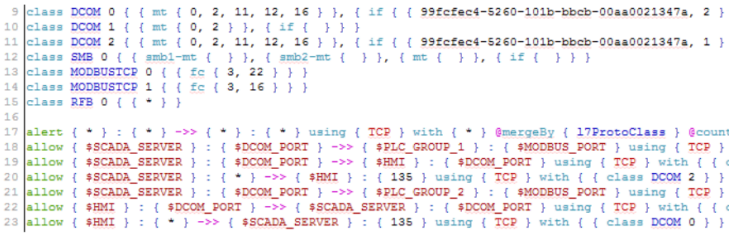

Figura 3. Un ejemplo del patrón de comportamiento obtenido por el LAN Communication Profiler

Los ejemplos representan las dos "tipos" de patrón de comportamiento que SCAB puede generar. En particular, la figura 3 muestra el modelo de comunicaciones de red normal generado automáticamente por el motor *Communication LAN Profile* (LAN CP) del SCAB. El LAN CP reporta las comunicaciones de red observadas en función de los flujos de comunicación, protocolos y tipos de mensajes de protocolo que se utilizan habitualmente en los dispositivos de la red. Tenga en cuenta que esto incluye los detalles de qué dispositivo se ha comunicado y con qué interfaces (D) COM.

Los controles implementados por el LAN CP aseguran de que cada vez que un dispositivo de red se conecta a una dirección IP inusual (por ejemplo, el servidor C & C), o invoca un interfaz COM que nunca ha utilizado antes o que se supone que no utiliza (por ejemplo, los utilizados por Havex), SCAB dispara una alerta.

La figura 4 muestra el modelo de uso normal del protocolo generado automáticamente por el motor de inspección profunda de comportamiento de protocolo del SCAB (DPBI). Este modelo presenta todos los campos (por ejemplo, tipos de mensajes) y los valores de campo que se utilizan normalmente para un cierto protocolo dentro de la red analizada en forma de un árbol de protocolo. El árbol representado fue construido para el protocolo DCOM. A la derecha del árbol, se muestra cómo para cada campo del protocolo, es posible visualizar en detalle y editar los valores observados. Una vez más, el motor DPBI garantiza que si los dispositivos de red utilizan campos DCOM inusuales, el equipo de seguridad será inmediatamente alertado.

Figura 4. Un ejemplo del patrón de comportamiento obtenido mediante inspección profunda de comportamiento de protocolo.

Detección de análisis de la red

SCAB puede detectar Havex a través de ambos motores CP LAN y DPBI. Más precisamente, el LAN CP podría generar una alerta para dos tipos de actividades inusuales de la red. El primero es el análisis de la red realizado por la máquina infectada (Figura 2). De hecho, al analizar la red, la máquina infectada puede conectarse a dispositivos con los que normalmente no se comunican, o se supone que no debe comunicar. La segunda actividad inusual es la invocación de las interfaces COM IOPCServer. Estas interfaces se utilizan normalmente sólo cuando se instala o actualiza el software de control en un determinado dispositivo. Su invocación daría lugar a la alerta generada por SCAB. Si la invocación de estas interfaces es seguida por una comunicación con una dirección IP externa desconocida (por ejemplo, el servidor C & C - como se describe en la sección siguiente), el host que origina la comunicación probablemente está infectado por Havex.

La siguiente figura muestra un ejemplo de alerta generada por el LAN CP cuando detecta el uso de interfaces COM inusuales. Las interfaces inusuales se indican a la derecha: se resaltan en rojo y se marcan con una señal de advertencia. A la izquierda, la alerta informa de detalles de los dispositivos que participan en la comunicación. Esto permite detectar inmediatamente cualquier dispositivo infectado por Havex (el dispositivo origen).

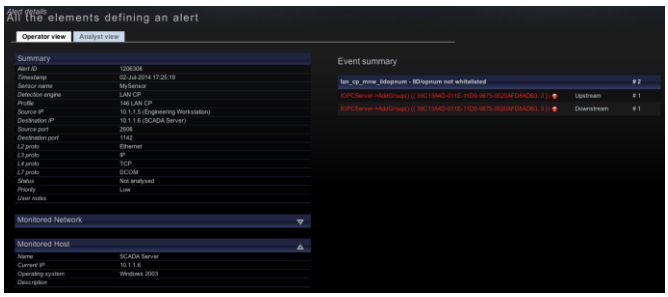

Figura 5: Alerta generada por el SCAB cuando Havex invoca los interfaces COM para identificar servidores OPC.

Detección de la comunicación con C & C

A raíz de la detección de la exploración de la red, el motor del LAN CP del SCAB alertaría al equipo de seguridad cada vez que el equipo infectado intentara comunicarse con el servidor C & C del malware. De hecho, el equipo infectado se conectaría a una dirección IP que no está en la "lista blanca" en el modelo del LAN CP. Esto permite que el equipo de seguridad pueda detener la comunicación antes de que se filtre ninguna información de red sensible, por ejemplo, mediante "listas negras" de la IP del C&C en el firewall de la compañía.

La Figura 6 ilustra un ejemplo de alerta generada por el motor de CP LAN cuando un dispositivo de red contacta con una dirección IP inusual. La dirección IP inusual es destacada en color rojo para que pueda ser añadida de inmediato en la lista negra si no es reconocida por el equipo de seguridad.

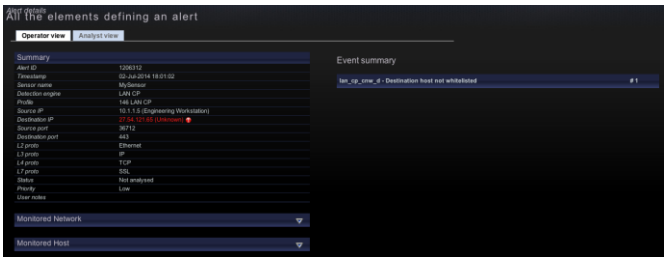

Figura 6. Alerta generada por SCAB cuando Havex comunica con el servidor C & C

Conclusiones

El grupo de hackers Dragonfly está llevando a cabo una campaña de ciberespionaje contra las empresas de energía en los EE.UU. y Europa. Hasta ahora, la campaña ha tenido como resultado la sustracción de información estratégica de las redes operacionales de las empresas. El malware utilizado en la campaña, sin embargo, puede dar a los atacantes la capacidad de lanzar ataques posteriores con mayores consecuencias.

Es fundamental que los operadores de infraestructuras críticas empiecen a adoptar contramedidas más modernas a las ciberamenazas de hoy. El tiempo de espera ha terminado - se ha demostrado más de una vez que los atacantes debidamente motivados pueden penetrar fácilmente en las redes de dichas infraestructuras críticas, con el potencial de causar daños incalculables a la economía, la seguridad y la salud de los ciudadanos de un país.

En SecurityMatters creemos que la implantación de una estrategia de defensa en profundidad es clave para contrarrestar con éxito la creciente amenaza cibernética. La primera capa de defensa está compuesta por los servidores de seguridad y / o sistemas de prevención de intrusión, que mantienen fuera de una red los ataques conocidos y fáciles de detectar. Algunos proveedores de Seguridad ya han lanzado firmas para la prevención de intrusión y soluciones basadas en host para detectar y detener el malware utilizado por Dragonfly. Sin embargo, como se indica por F-Secure, se han identificado hasta el momento **88** variantes del malware Havex.

Las firmas no ofrecen protección a las nuevas variantes a usar por Dragonfly, o al siguiente malware empleado en su próxima campaña. Por tanto, es vital que, junto con las soluciones de ciberseguridad tradicionales las empresas implanten una solución de monitorización de red no basada en firmas como SCAB, que no se basa en el conocimiento de una amenaza para detectarla y alertarla.

La solución SCAB es única en su tipo, ya que no hay otra solución capaz de definir automáticamente las "operaciones normales de la red", y de analizar las comunicaciones y los valores intercambiados por los dispositivos de la red de control. Este enfoque único garantiza la protección tanto frente a las amenazas actuales, como a las amenazas de mañana, aumentando la resiliencia de nuestra infraestructura crítica.

Agradecimientos

A Damiano Bolzoni y a Cliff Gregory por sus útiles consejos.

Me gustaría dar las gracias a SecurittyMatters y a SCADAhacker por su permiso para la traducción al castellano de este interesante estudio.

Referencias

[1] Dragonfly: Western Energy Companies Under Sabotage Threat - Symantec Security Response Official Blog - http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

[2] Active malware operation let attackers sabotage US energy industry - Ars Technica - http://arstechnica.com/security/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/

[3] Havex Hunts For ICS/SCADA Systems - F-Secure News from the Lab - http://www.f-secure.com/weblog/archives/00002718.html

[4] Talk2M Incident Report - http://www.talk2m.com/en/full_news.html?cmp_id=7&news_id=51

[5] OPC was renamed from “Object Linking and Embedding (OLE) for Process Control” to “Open Platform Communications” in November 2011.