S21sec
Committed to security

White_Paper

¡Fuera luces! ¿Quién es el siguiente?

Como anticiparse al siguiente “Ciberapagón”

Autores

Daniel Trivellato, PhD - Product Manager Industrial Line - SecurityMatters
Dennis Murphy, MSc - Senior ICS Security Engineer - SecurityMatters

Traducido por:

Enrique Martín García – Key Account Manager Industrial Cyber Security and CIP Services – S21sec

4 de Febrero de 2016

CONTENIDO

PRÓLOGO

El 23 de Diciembre de 2015, por primera vez en la historia, un gran ciberataque a una infraestructura crítica estatal afectó de manera significativa a la población civil. Tal y como fue informado por numerosas fuentes [1, 5], cientos de miles de habitantes de la región Ucraniana de Ivano-Frankivsk estuvieron sin electricidad cerca de seis horas.

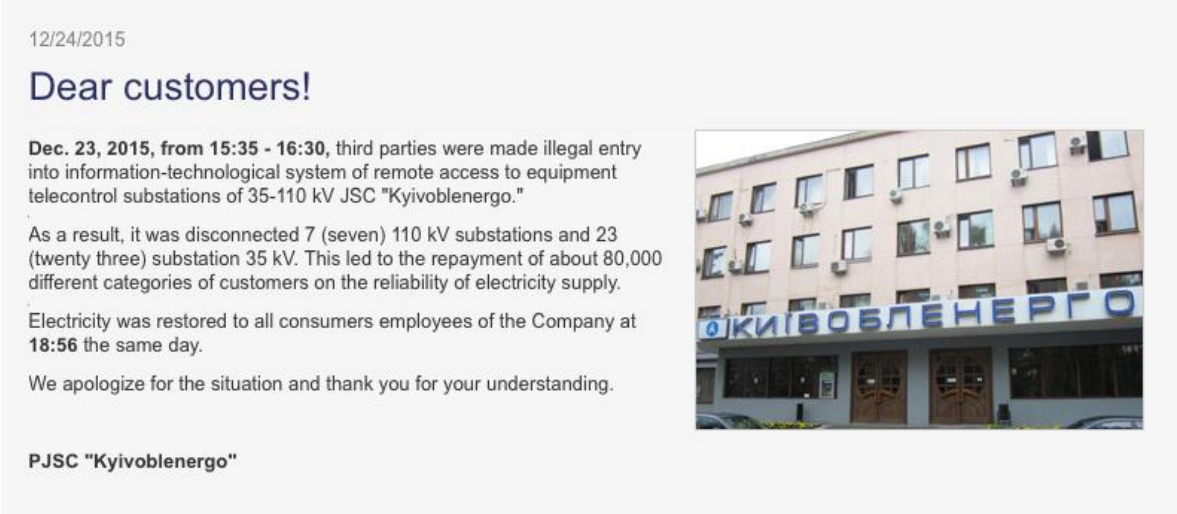
Investigadores y analistas de los principales agentes de ciberseguridad a nivel mundial están investigando el incidente en detalle [1, 5, 2, 4, 8, 7]. A pesar de que aún hay muchas cuestiones abiertas acerca del origen y dinámica del incidente, todas estas fuentes coinciden en que detrás del gran apagón hay claros indicios de un ciberataque intencional y coordinado contra varias compañías de electricidad Ucranianas.

Esta breve nota técnica presenta las averiguaciones y los resultados de las investigaciones realizadas sobre el incidente hasta la fecha y discute como la parte clave de este ataque podría haber sido detectada rápidamente aplicando las medidas correctas de monitorización sobre las zonas vitales de las redes de control de las distribuidoras eléctricas

EL ATAQUE COORDINADO A LA RED ELÉCTRICA UCRANIANA

Comenzamos nuestro análisis del ataque a la red eléctrica Ucraniana con los hechos registrados el 23 de Diciembre de 2015. Entre las 15:35 y las 16:30 horas locales, la distribuidora Kyivoblenergo sufrió una intrusión de terceros en su infraestructura ICT.

Durante esta intrusión, siete subestaciones de 110kV y veintitrés subestaciones de 35 kV fueron "desconectadas" de la red, produciéndose un corte de suministro para cerca de 80.000 consumidores. Esta intrusión fue comunicada por Kyivoblenergo a través de un anuncio publicado en su sitio Web (Figura 1)



12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Figura 1: Anuncio publicado por Kyivoblenergo [2]

De acuerdo con el anuncio, la alimentación fue restablecida a todos los usuarios aproximadamente tres horas más tarde, a las 18:56 hora local.

En otro anuncio público, Kyivoblenergo informó de otro fallo técnico en las infraestructuras del Call Center que impidió a muchos usuarios contactar con la compañía durante el apagón. (Figura 2)

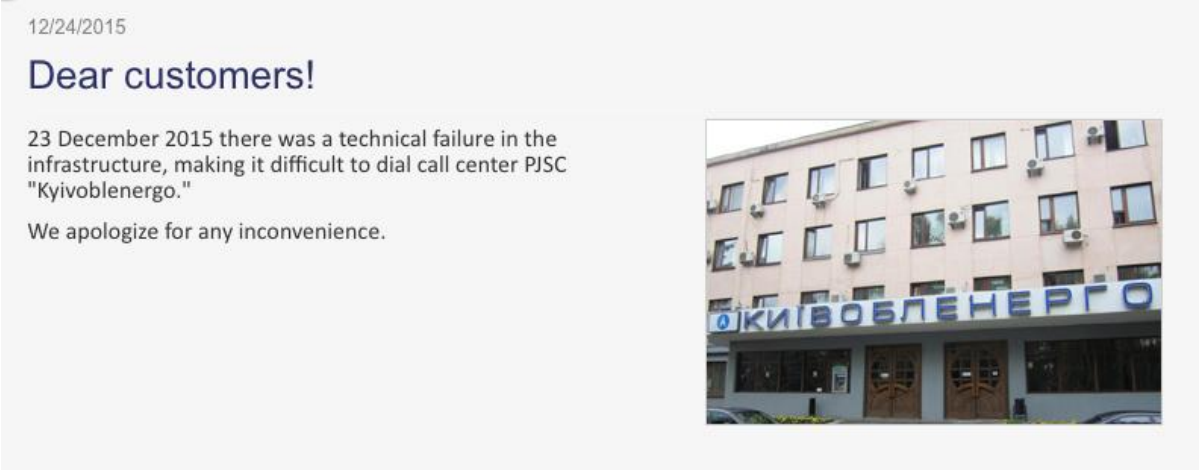


Figura 2: Anuncio sobre los problemas registrados en el Call Center de Kyivoblenergo [2]

Al mismo tiempo que el incidente de Kyivoblenergo, otras compañías eléctricas Ucranianas registraron intrusiones e incidencias. El análisis publicado por TrendMicro [5] informa de otras dos compañías fueron objetivo de los atacantes y de acuerdo con los informes de SANS ICS [2] y ESET [1] (una empresa de Software basada en Bratislava), mencionan a la autoridad de la energía de Ucrania del oeste Prykarpattyaoblenergo en particular.

De acuerdo con ESET [1], alrededor de 700.000 personas en la región Ucraniana de Ivano-Frankivsk (la mitad de la población local) sufrieron el apagón.

TrendMicro [5] informa de manera más general que “cientos de miles de hogares fueron víctimas del ataque”.

Los pasos del ataque

Es pronto para determinar la dinámica exacta del ataque, en cualquier caso, todos los investigadores y analistas involucrados en el análisis coinciden en que el apagón fue el resultados de un ataque extremadamente bien coordinado. Tal y cómo describe SANS [2], el ataque utilizó, al menos, estos tres vectores:

- Un componente malware que posiblemente permitió el acceso de los atacantes a la red y que actuó para causar daños a los sistemas SCADA de las compañías atacdas, con objeto de retrasar el proceso de restablecimiento de la normalidad y complicar el estudio forense del ataque. La variante del malware utilizado en el ataque contenía código diseñado para el sabotaje de sistemas industriales [1, 8].
- Una denegación de servicio a los *Call Centers* de las compañías eléctricas mediante un aluvión de llamadas durante el ataque que evitó que los usuarios pudieran avisar de manera efectiva del apagón

- La apertura de los interruptores en las subestaciones para producir el apagón. Esta es aún la pieza más misteriosa del rompecabezas. Lo más probable es la apertura directa mediante comandos ejecutados por los atacantes desde la red de control, antes que por la actividad del malware encontrado en las redes de las víctimas.

Estos vectores fueron puestos en marcha por los atacantes y secuenciados en pasos precisos para producir el máximo daño al proceso de distribución eléctrica.

Un posible escenario del incidente y de los pasos seguidos por los atacantes es el siguiente:

1. Los atacantes infectaron los servidores principales del proceso de distribución de Kyivoblenergo y de otras dos compañías con malware
2. Se infiltraron en las redes de las víctimas (posiblemente usando un backdoor del malware) y ejecutaron los comandos de apertura de los interruptores en varias subestaciones.
3. El malware dejó a ciegas y engañó a los empleados de las compañías para prevenir la rápida reacción a los comandos ejecutados por los atacantes, mediante la finalización y bloqueo posterior de ciertos servicios clave en los servidores SCADA.
4. Los atacantes iniciaron la denegación de servicio sobre los *call centers* limitando la visibilidad de sus objetivos sobre las consecuencias del ataque.

Dadas las circunstancias, las compañías víctimas del ataque han sido extremadamente rápidas en la recuperación de la alimentación eléctrica a sus clientes. De hecho, dada la imposibilidad de controlar el proceso remota y automáticamente a través de sus sistemas SCADA, tuvieron que desplegar personal de campo a todas las subestaciones afectadas para cerrar los interruptores de forma manual y volver a dejar los sistemas en su estado de funcionamiento habitual.

Durante algún tiempo después del incidente, todo el proceso de distribución eléctrica se ha ejecutado en una especie de “modo emergencia”, dado que los SCADA estaban aún infectados.

El papel del malware

En esta sección vamos a presentar los resultados del análisis del malware identificado en las redes de las compañías afectadas y su papel en el ataque. De acuerdo con los investigadores de ESET [1] y TrendMicro [5], las víctimas fueron infectadas por una variedad de malware perteneciente a la campaña BlackEnergy, el cuál habría sido distribuido a través phising con un fichero Microsoft Excel adjunto que contenía una macro maliciosa:

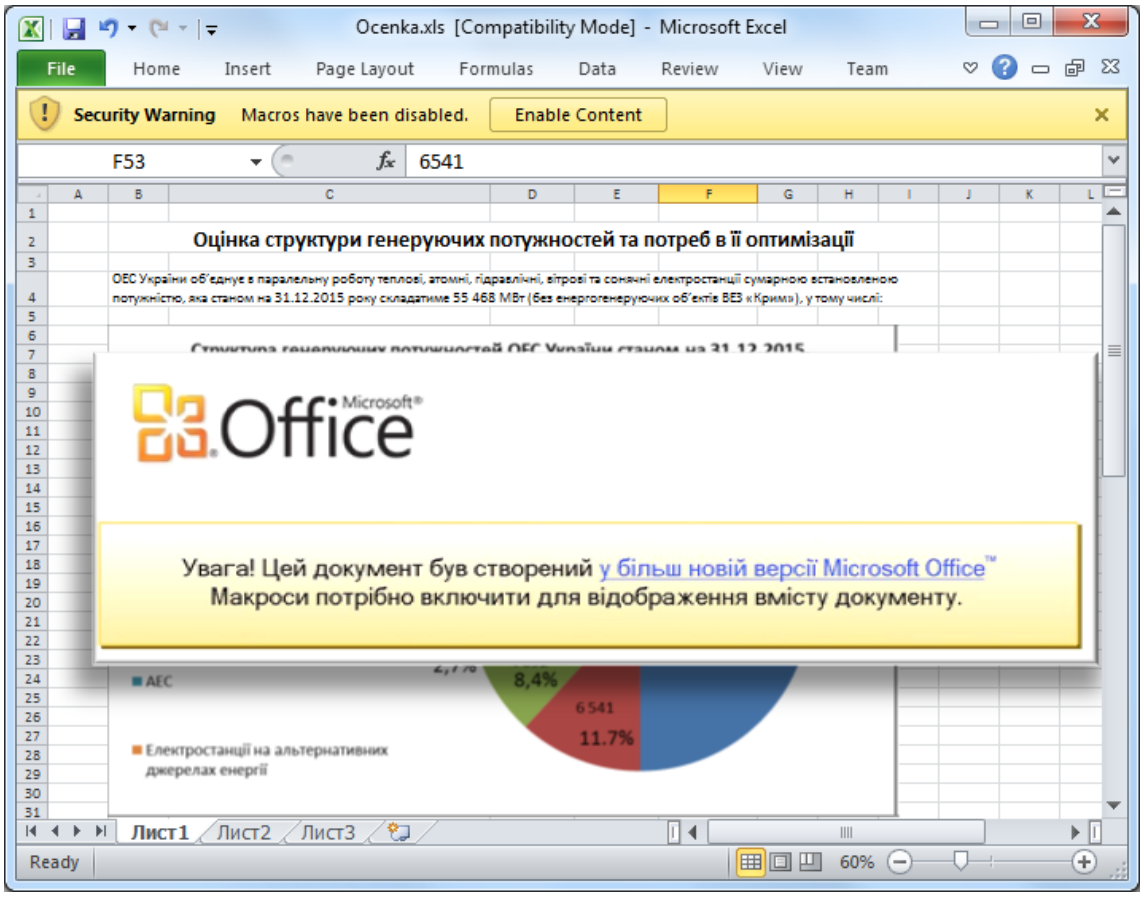


Figura 3: Documento Microsoft Excell infectado con una Macro

Una vez ejecutado, este documento habría descargado los componentes apropiados para garantizar la persistencia en las máquinas infectadas. El componente del malware responsable específicamente del borrado de los sistemas SCADA de las compañías objetivo es llamado “KillDisk”

Lo siguiente es un extracto del informe de ESET [1]:

“La primera conexión entre BlackEnergy y KillDisk fue anunciada por la agencia Ucraniana de Ciberseguridad, CERT-UA, en Noviembre de 2015. En esa ocasión, cierto número de empresas de comunicación fueron atacadas coincidiendo con las elecciones locales de 2015. El informe de este incidente afirma que un gran número de videos y documentos fueron destruidos cómo resultado del ataque”

Un análisis exhaustivo del componente KillDisk se puede encontrar el informe publicado por Symantec [8].En este informe, KillDisk (detectado por Symantec como el troyano Disakil) es calificado como un troyano multi-etapa altamente destructivo, que inutiliza el sistema infectado sobrescribiendo el Master Boot Record y otros sectores con información “basura”.

Pero lo más interesante de la variante del malware encontrada en las compañías eléctricas Ucranianas es que contiene código especialmente diseñado para **interrumpir** procesos industriales. En particular, esta variante de KillDisc

“intenta parar y eliminar un servicio llamado sec_service. Este servicio parece pertenecer al Software 'Serial to Ethernet Connector' de Eltima. Este Software permite acceso serie remoto a través de conexiones de red. Muchos sistemas SCADA antiguos todavía utilizan conexiones serie para las comunicaciones con las RTUs. [. . .] Si un atacante supiera que su objetivo está usando este Software para comunicarse con sus dispositivos SCADA más antiguos, podría para el servicio e interrumpir cualquier comunicación aumentando el daño potencial causado en su entorno”.

El extenso análisis de una muestra de malware realizado por SentinelOne [7] indica que, más allá de la rutina de borrado, el malware ejecuta código para capturar y alterar el tráfico de los interfaces de red en las máquinas infectadas, incluyendo los adaptadores inalámbricos. Toda la información recolectada se envía al servidor de *Command & Control* vía mensajes HTTP.

A pesar de todos estos resultados, el papel exacto e impacto del malware en el ataque todavía no está confirmado. SANS ICS [1] afirma que junto a investigadores que atribuyen a BlackEnergy y KillDisk toda la responsabilidad del incidente, hay otra línea de pensamiento que considera que la presencia del malware en las redes de la compañía no está directamente relacionado con el apagón (en otras palabras, el malware estaba allí y operando en la red al mismo tiempo que se produjo el apagón).

La posición de SANS está cercana a algo intermedio: el malware fue un facilitador más que el ejecutor, permitió el acceso a los atacantes a las redes de las compañías y fue responsable de la inutilización de los sistemas SCADA tras el ataque, pero el comando que causó el apagón (apertura de interruptores en múltiples subestaciones en un corto periodo de tiempo) fue **ejecutado manualmente** por los atacantes.

Atribución

Los actuales informes y análisis de los investigadores del incidente proporcionan distintas opiniones acerca de quién está detrás del ataque. El Servicio de Seguridad Ucraniano (USB) fue rápido al apuntar a Rusia y también lo fue el análisis de iSIGHT Partners [4]. Esto es debido principalmente por la presencia de malware BlackEnergy en la red de las compañías eléctricas Ucranianas objetivo de este ataque.

Detrás de BlackEnergy está el grupo basado en Moscú Sandworm, quién tiene un largo historial de apuntar a objetivos en Ucrania, países Occidentales y compañías del sector energía. [4,8].

A pesar de no mencionar a Rusia, SentinelOne [7] está segura de que esta última variante de BlackEnergy es producto de una campaña sostenida por un estado y de un equipo multidisciplinar trabajando de manera conjunta.

Otros investigadores son más cuidadosos o al menos no tan directos al atribuir este ataque a conocidos grupos sustentados por algún estado.

Por ejemplo, SANS ICS afirma en sus dos informes [2, 3] que aún es muy pronto para determinar si el incidente está relacionado con la campaña de BlackEnergy.

También en el último comentario de Ray Parks [6] en la lista de correo SCADASEC, dedica especial atención en la atribución de este ataque. En su análisis, Ray Parks apunta que un ataque sostenido por un estado “hubiera apuntado más alto”. (Por ejemplo STUXNET, que se diseñó para ralentizar el programa nuclear Iraní) o a objetivos mucho más estratégicos (estaciones de radar críticas). La compañía de electricidad Ucraniana objeto del ataque está en la parte oeste de Ucrania por lo que no parece que el ataque apuntara a objetivos estratégicos (militares).

La conclusión de Ray Parks es, por tanto, que el ataque probablemente haya sido ejecutado por alguien “ligado a un estado” (demostrado por el uso de herramientas especiales), pero actuando por su cuenta y movido por motivos personales.

¿PODÍA HABER SIDO EVITADO?

La respuesta es probablemente no, pero algunos síntomas del ataque y acciones de los atacantes se podrían haber detectado antes en todo el proceso. Por ejemplo, algún sistema antivirus o de prevención de intrusión como Symantec [8] ya disponían de firmas capaces de detectar el módulo KillDisc del malware.

En cualquier caso, es discutible si esas firmas hubieran descubierto esa variante especial del malware encontrado en las compañías Ucranianas [7].

Sin embargo, hay dos pasos que sí que hubieran sido detectados de una manera certera según se hubieran producido:

a. Las comunicaciones entre los sistemas infectados y el servidor Command & Control para informar sobre la información de tráfico recolectada
b. La acción ejecutada por los atacantes para abrir de manera remota los interruptores de las subestaciones, lo que causó el apagón.

La detección de ambas acciones habría sido posible monitorizando las redes SCADA de las compañías eléctricas usando la plataforma SilentDefense de SecurityMatters, que haciendo uso de su comprensión de los protocolos de comunicaciones industriales y su ***librería de inteligencia de amenazas***, puede reportar en tiempo real cualquier actividad que pueda afectar negativamente a los procesos de control.

SilentDefense

SilentDefense es una plataforma avanzada de monitorización e inteligencia utilizada por los operadores de infraestructuras críticas de todo el mundo, para preservar la estabilidad de sus redes SCADA.

SilentDefense monitoriza y analiza constantemente las comunicaciones de la red de control, las compara con un patrón legítimo de funcionamiento operacional y con el uso de la librería de inteligencia de amenazas industriales de SecurityMatters informa en tiempo real de cualquier problema o amenaza a la red SCADA y a los procesos que controla dicha red. Algunos ejemplos incluyen:

- Intentos de intrusión
- Dispositivos mal configurados o con comportamientos anormales
- Operaciones de procesos no deseadas
- Errores operacionales
- Ataques zero-day

Todas estas amenazas son detectadas y se presentan al operador de dos maneras distintas:

- **Visual Analytics:** El operador se puede beneficiar de la representación gráfica de la red en distintos aspectos y sobre distintos tipos de gráficos. (Figura 4). Estos gráficos y tablas están pre configurados para obtener de un primer vistazo los aspectos más importantes de la actividad actual de la red de control, pero puede ser fácilmente personalizable por el operador para obtener la información deseada. De hecho, visual Analytics está construido sobre una plataforma completa de Data Warehouse, lo que significa que el operador puede consultar sobre cualquier aspecto de interés sobre la red en cualquier momento,

ofreciéndole la posibilidad de ver que es lo que está pasando o que es lo que pasó, pudiendo detectar de manera rápida cualquier comportamiento extraño.

- **Alertas en tiempo real**: Tan pronto como algo malo o inesperado sucede en la red de control, SilentDefense notifica al operador y le proporciona la información necesaria para reaccionar antes este evento. Esto incluye información sobre la fuente del problema, el dispositivo(s) amenazado, la naturaleza del problema (p.e. un dispositivo desconocido que inicia una comunicación con algún dispositivo de campo, el servidor SCADA enviando algún comando no deseado o dañino, dispositivos de campo que devuelven valores no usuales, etc.) e incluso una captura del tráfico detectado (compatible PCAP). Esto último es fundamental cuando nos enfrentamos a amenazas zero-day, ya que podemos enviar de manera rápida la información a proveedores de seguridad especializados en estudio avanzado de incidentes como S21sec, Symantec, McAfee, etc.

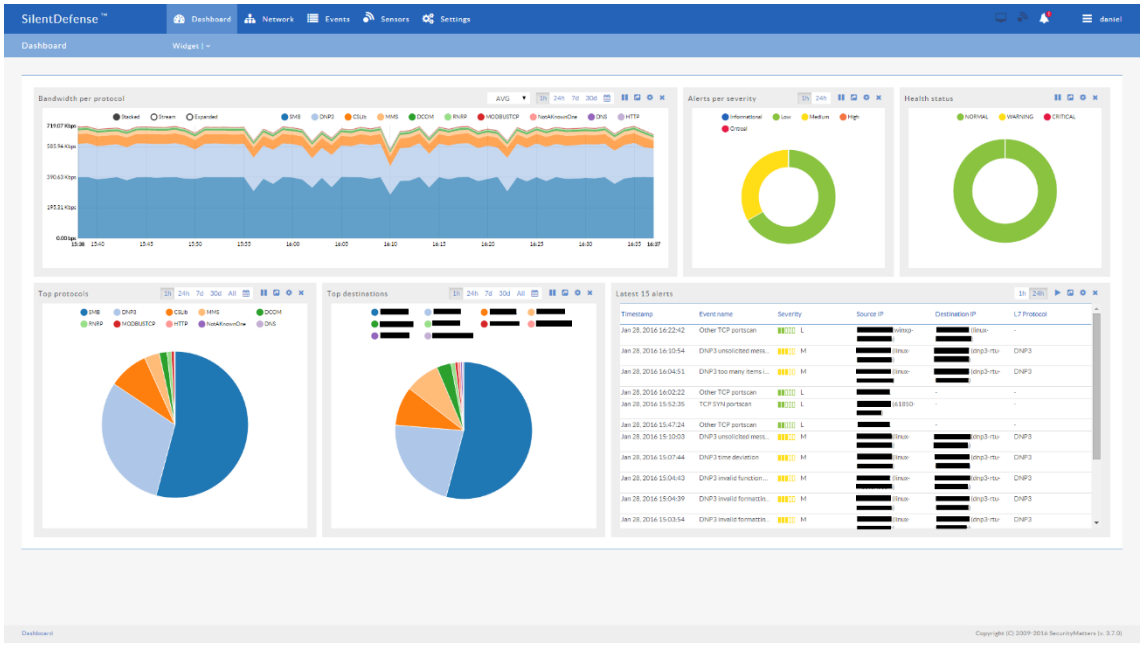


Figura 4: Cuadro de mando principal de SilentDefense

SilentDefense ya ha probado su efectividad contra intentos de intrusión y problemas muy específicos del entorno SCADA en distintos operadores de infraestructuras críticas.

Dos de los últimos ejemplos de problemas identificados en nuestros clientes incluyen una intrusión satisfactoria en la red de control (aprovechando una mala configuración ene un Firewall) durante la cual los atacantes fueron detectados al enviar mensajes de protocolo malformados al servidor SCADA, y un problema de potencial inestabilidad en la red eléctrica de una ciudad debida a la mala configuración de los dispositivos de control y no detectada por el servidor SCADA.

Detección del ataque Ucraniano

SilentDefense posee diferentes motores de detección complementarios para poder detectar todos los problemas y amenazas descritos anteriormente.

En particular, los operadores se pueden beneficiar de:

- Los módulos de detección “de serie” para la detección de los primeros estados de ejecución de un ataque (Escaneo de puertos, ataques de “Man In The Middle) y verificación de cumplimiento de protocolo de red.
- Generación automática de patrones de comunicación para definir los dispositivos de red, flujos de tráfico, protocolos y comandos legítimos y detección de dispositivos desconocidos, protocolos inseguros y operaciones no deseadas
- Generación automática de patrones de protocolos de control para definir las operaciones de proceso legítimas y detección de comandos inesperados o desviaciones inesperadas del proceso
- Un marco de inteligencia de red de control soportada por la librería de amenazas industriales de SecurityMatters y que permite activar la verificación de ciertas comprobaciones (detección de la apertura de una válvula en un horario no deseado, verificación de la apertura de un interruptor de una subestación solo si otro está cerrado, etc.)

Analizando las comunicaciones de la red de control en tiempo real y comparando el tráfico actual con los patrones previamente generados y validados, SilentDefense podría haber identificado e informado inmediatamente las comunicaciones entre las máquinas infectadas y el servidor de C&C. En particular, podría haber informado al personal de la distribuidora Ucraniana de la comunicación del servidor SCADA con un dispositivo externo desconocido (Figura 5).

Aunque alguien pudiera discutir que este tipo de amenaza puede ser mitigada mediante el uso de Firewalls y otros sistemas de detección de intrusión, hemos visto en numerosas circunstancias que estos sistemas pueden estar mal configurados o sobrecargados.

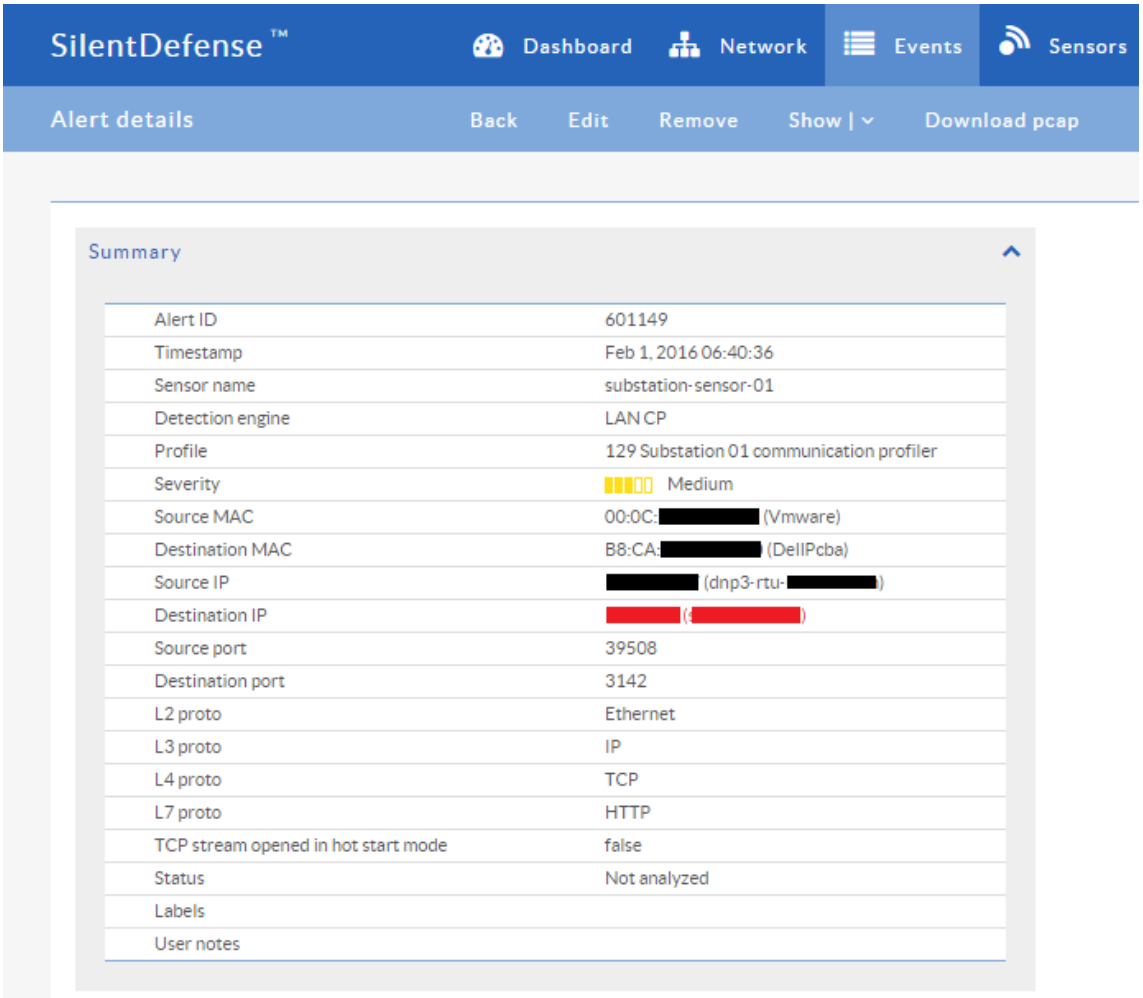


Figura 5: Alerta generada por la comunicación con un destino desconocido

De todas maneras, el motor de detección más notable de SilentDefense para este caso específico, es el marco de inteligencia de red. Este motor es una característica única de SilentDefense que se ha probado fundamental en la detección de un gran número de problemas en las redes de los clientes. La librería de amenazas industriales de SecurityMatters contiene las lecciones aprendidas en diferentes entornos y experiencias en campo traducidas en verificaciones sobre la red, que notifican al operador tan pronto algo va mal.

Una de las comprobaciones en nuestra librería de amenazas industriales hubiera podido reportar la actividad de los atacantes al abrir los interruptores de las subestaciones. Esta comprobación ha sido escrita a petición de uno de nuestros clientes para detectar cuando su sistema de aislamiento de fallas entra en funcionamiento, y fue luego generalizado para cubrir exactamente este caso de uso ocurrido en el ataque Ucraniano.

De hecho, el sistema de aislamiento de fallas hubiera actuado de manera similar a los atacantes en la red eléctrica de distribución de Ucrania (Hubiera abierto/cerrado un número de interruptores de subestación en un corto periodo de tiempo)

La Figura 6 muestra un ejemplo de la alerta generada por esta comprobación.

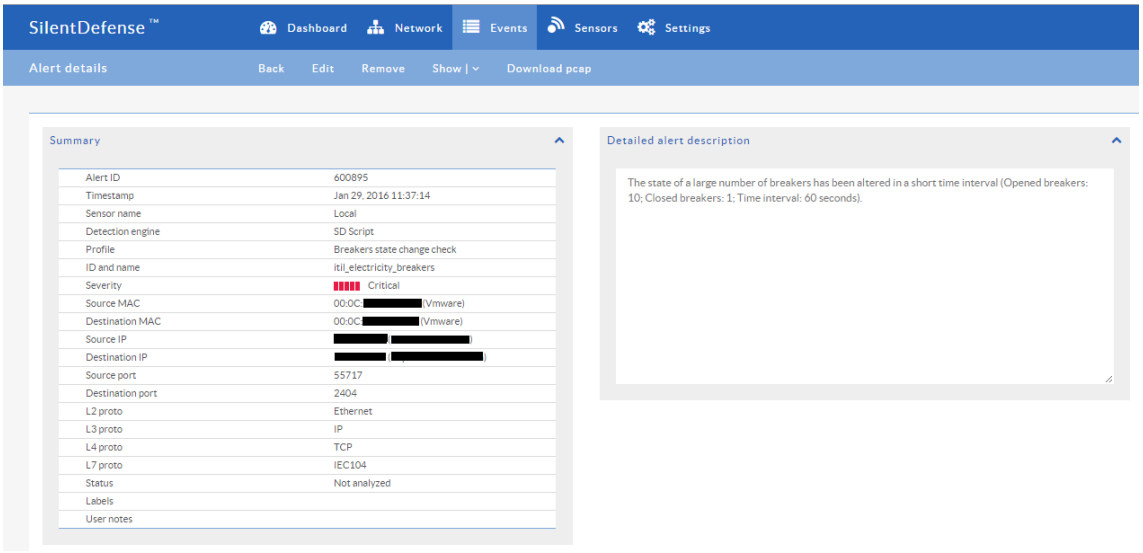


Figura 6: Alerta generada por la apertura o cierre de un número de interruptores determinado en un corto periodo de tiempo

Nótese que aquí estamos asumiendo el caso más probable, que el comando de apertura de interruptores de las subestaciones fue ejecutado por los atacantes desde un puesto remoto de operación legítimo a todas las subestaciones. En el caso menos probable en que los atacantes se hubieran conectado una a una a todas las subestaciones objetivo para abrir los interruptores, SilentDefense habría reportado la presencia de conexiones inusuales a los dispositivos de campo de manera similar al mostrado en las comunicaciones con el server de C&C (Figura 5).

Tal y cómo apuntamos en la introducción de esta sección, la detección en tiempo real del evento no habría impedido el apagón, pero los operadores del sistema habrían tenido toda la información para entender, de manera instantánea, la razón del mismo, y las subestaciones atacadas, pudiendo enviar a su personal de mantenimiento de manera más rápida para solucionar el problema y minimizar el efecto del corte de suministro eléctrico.

Adicionalmente, con una solución de monitorización de su red de control como SilentDefense activa, las compañías Ucranianas no habrían estado completamente ciegas acerca de la actividad y procesos su red incluso después de que su sistema SCADA estuviera abajo.

CONCLUSIONES Y RECOMENDACIONES

El apagón de Ucrania ha sido el primer tipo de ataque a un operador de infraestructura crítica que ha tenido un efecto directo sobre la población civil. Hasta el momento, este tipo de escenario había sido discutido solamente en teoría. A pesar de su pequeña escala, este ataque ha demostrado que un grupo de atacantes motivados tiene los conocimientos y medios suficientes para causar daños catastróficos a la economía y seguridad de un país.

La mayor parte del problema es, por supuesto, el hecho de que los operadores de infraestructuras críticas se están quedando atrás en la protección de sus sistemas y redes de control SCADA, posiblemente perdiendo de vista que la industria 4.0 ha traído muchos riesgos a la vez que muchas ventajas.

Pensando en que es lo siguiente que deberíamos hacer para impedir este tipo de incidentes, estamos de acuerdo en lo presentado en el último informe de SANS ICS [3]: Las instalaciones de control a lo largo del mundo necesitan poner en marcha sus defensas y en particular su capacidad para monitorizar sus redes de control SCADA para responder a las amenazas.

En primer lugar debemos formar equipos con los correctos conocimientos y capacidades en cada organización, un equipo capaz de ejecutar un rápido análisis de riesgo y responder rápido ante actividades sospechosas mediante claros procedimientos de respuesta en los que esté perfectamente definido como escalar un incidente de este tipo y a quién pedir ayuda.

En segundo lugar, estos equipos deben estar equipados con las herramientas correctas para monitorizar sus redes y detectar rápidamente cuando algo va mal. La adopción de soluciones genéricas de seguridad IT clásicas no ayudaría para este propósito.

Como se demuestra en esta nota técnica, la adopción de una solución específicamente diseñada para los entornos industriales y SCADA, como SilentDefense, es clave para permitir la rápida detección de amenazas dirigidas.

Acerca de SecurityMatters

SecurityMatters es una compañía internacional con negocio en todos los grandes operadores de infraestructuras críticas y en sectores de automatización industrial. Su solución de monitorización y plataforma de inteligencia SilentDefense ha sido desplegada durante años en clientes de distintos continentes, proporcionando valor diariamente a las operaciones y protegiendo sus redes de Ciberamenazas emergentes.

Acerca de S21sec

S21sec es una multinacional especializada en servicios y tecnología de seguridad cuya finalidad es garantizar el desarrollo efectivo de los negocios. Nuestro objetivo es la protección de los activos digitales de mayor valor y críticos en las organizaciones: la información y la imagen de la compañía.

Nos centramos en lo que para nosotros es la esencia de la seguridad: la prevención. Apostamos por un nuevo modelo de ciberseguridad: gestionando la seguridad de nuestros clientes, llevando la confianza a las nuevas tecnologías, a las infraestructuras críticas, a los usuarios.

.

BIBLIOGRAFÍA

[1] ESET. Eset finds connection between cyber espionage and electricity outage in ukraine.

http://www.eset.com/int/about/press/articles/malware/article/eset-_nds-connection-between-cyber-espionage-and-electricity-outage-in-ukraine/

[2] SANS ICS. Con_rmation of a coordinated attack on the ukrainian power grid.

https://ics.sans.org/blog/2016/01/09/con_rmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[3] SANS ICS. Potential sample of malware from the ukrainian cyber attack uncovered.

https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

[4] iSIGHT Partners. Sandworm team and the ukrainian power authority attacks.

http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/

[5] Trend Micro. First malware-driven power outage reported in ukraine.

http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/_rst-malware-driven-power-outage-reported-in-ukraine .

[6] Infracritical SCADASEC mailing list. New wave of attacks against ukrainian power industry. http://news.infracritical.com/mailman/listinfo/scadasec

[7] SentinelOne. Sentinelone discovers a new delivery tactic for blackenergy 3.

https://www.sentinelone.com/blog/sentinelone-discovers-a-new-delivery-tactic-for-blackenergy-3/.

[8] Symantec. Destructive disakil malware linked to ukraine power outages alsoused against media organizations.

http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations.

[9] ESET welivesecurity. New wave of cyberattacks against ukrainian power industry.

http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/