

Julia Blanco

Latam Marketing Coordinator

UL International

Julia.Blanco@ul.com

+54.11.3984.2600.

**UL 2900-2-3 ayuda a mitigar los riesgos de seguridad de Internet de las Cosas (Iot)**

*Medidores de energía eléctrica, cámaras de seguridad, sensores y cajeros automáticos están menos expuestos a problemas de seguridad de ciber con el protocolo UL 2900-2-3*

**San Pablo, febrero de 2018 -**  Según Gartner Inc., empresa de investigación y asesoramiento de mercado, habrá 8.400 millones de dispositivos conectados en uso en 2017 y la expectativa es de 20.400 millones para 2020. El crecimiento exponencial de aparatos conectados a Internet, tales como Smart TVs, consolas de HDTV, medidores de energía y cámaras de seguridad ofrecen tanto a los usuarios B2B como a B2C, varias oportunidades de servicios por llamada, más conveniencia, entre otros beneficios.

En el caso de sistemas de seguridad electrónica, Internet de las Cosas (IoT por sus siglas en inglés) permite a las organizaciones el monitoreo remoto, así como la identificación y la respuesta a cuestiones de seguridad. Las contraseñas digitales se pueden cambiar rápidamente, por ejemplo, para limitar o permitir el acceso, añadiendo un nivel adicional de seguridad al sistema.

Con la tecnología interconectada también vienen amenazas digitales en forma de phishing (una manera deshonesta que los cibercriminales usan para engañar y revelar información personal, como contraseñas de tarjeta de crédito, CPF y número de cuentas bancarias, enviando correos electrónicos falsos o dirigiendo a los sitios web falsos), los bots (destructor de robots, también conocido como Internet bot o web robot, una aplicación de software diseñada para simular acciones humanas repetidas veces de manera estándar, al igual que lo haría un robot), ransomware: el tipo de software nocivo que restringe el acceso al sistema infectado y cobra un rescate para que el acceso pueda ser restablecido y, si no ocurre, los archivos pueden ser perdidos e incluso publicados) y malware (software nocivo), entre otras técnicas usadas por quien ataca de esta forma para manipular las vulnerabilidades de la red del software y los sistemas operativos.

**¿Qué está en juego?**

Symantec (empresa de seguridad cibernética), en su Informe de Amenazas de Seguridad en Internet de 2017, presenta estas estadísticas, obtenidas a partir de análisis llevados a cabo en 2016:

* 1 de cada 2,596 mensajes de correo electrónico contiene intentos de phishing
* Hay 357 millones de nuevas variantes de malware
* 98.6 millones de bots
* 229 mil ataques web bloqueados por día, en promedio
* Los aparatos conectados a Internet fueron atacados por media una vez cada dos minutos.

Para contextualizar estos números, un ataque ocurrido en octubre de 2016 ganó los titulares cuando las cámaras hackeadas llevaron a una impresionante negación de servicio distribuido (DDOS por sus siglas en inglés), afectando a sitios web como Amazon, Twitter, Spotify, Yelp, Netflix y Reddit. Un ejército de botnets, conocidos como Mirai, causó un problema gigantesco derribando sitios o disminuyendo severamente su frecuencia operativa.

Los nuevos artículos reportan que el tráfico fue conducido por varios tipos de aparatos de IoT, incluyendo, enrutadores, grabadoras de vídeo y cámaras. Los aparatos conectados como estos se utilizan como opción para hackear redes legítimas.

En Brasil, hospitales fueron blancos de ataques que derribaron sus redes y causaron problemas en la atención de pacientes.

En 2017 Brasil se ubicó detrás de China en el ranking de más casos de ataques cibernéticos con daños de USD 22 mil millones a empresas, organizaciones y personas víctimas de estas acciones.

**Seguridad del diseño**

La Comisión Federal de Comunicación de los Estados Unidos (FCC en inglés) alertó a los fabricantes de aparatos IoT, a principios del año pasado, de informar sobre los riesgos de ciberseguridad, o enfrentarse a más interferencia del gobierno y nuevas regulaciones normativas.

En el centro del problema están los ataques DDOS a través de los botnets, como los Mirai, y un creciente escrutinio de canales poco seguros que pueden ser fácilmente interceptados por hackers. Muchos fabricantes producen aparatos fáciles de romper, como se muestra en una investigación al QuickLock Padlock, conducida por el estado de Nueva York (EEUU).

La FCC propuso en un documento sobre reducción de riesgos de ciberseguridad (Cybersecurity Risk Reduction White Paper, 18 de enero de 2017) la implementación de prácticas inteligentes de ciber diseño, como la autenticación de seguros y la adherencia a las mejores prácticas antes de priorizar el lanzamiento del producto. La FCC prefiere utilizar asociaciones público-privadas, pero complementa que "la Comisión tiene las herramientas para hacer ajustes para restaurar el equilibrio, si es necesario".

**La solución**

Para ayudar a mejorar la seguridad de los sistemas de seguridad electrónica existe el protocolo UL 2900-2-3, la nueva contribución a la serie UL 2900 de normas de ciberseguridad. Desarrollada con la ayuda de distintos participantes de la industria, proporciona un conjunto fundamental de rendimiento de ciberseguridad y requisitos de seguridad que los fabricantes de productos conectables pueden establecer como base de protección contra vulnerabilidades y malware.

El Programa de Seguridad Cibernética de UL (UL CAP) puede probar y evaluar el software de un producto y certificar la arquitectura y el diseño de software de este producto de acuerdo con las especificaciones enumeradas en la Descripción de la investigación (Outline of Investigation).

Las infraestructuras de seguridad electrónica incluyen sistemas de comunicación de emergencia, sistemas de alarma de fuego, sistemas de recepción de alarmas, sistemas de cajeros automáticos, sistemas de control de acceso, cámaras de seguridad, grabadoras de vídeo, grabadoras de vídeo digitales y otros.

El protocolo UL 2900-2-3 ha sido desarrollado de forma que hay una exigencia de seguridad mayor a cada nivel. Las pruebas incluyen detección de fallos conocidos, análisis de código y binario, análisis de control de riesgos, pruebas de penetración estructurada y evaluación de riesgos de seguridad.

Nivel 1: incluye los requisitos de seguridad básica para la evaluación de riesgos de seguridad en software de productos incluidos en la Descripción de la investigación (Outline of Investigation). Este nivel se recomienda como nivel mínimo de evaluación.

Nivel 2 - incluye todos los requisitos del primero y los requisitos de evaluación de riesgos de seguridad en el software de productos. Este nivel también proporciona una evaluación de las capacidades de seguridad de un producto con conocimientos de controles internos de seguridad.

Nivel 3 - incluye requisitos de evaluación y pruebas de los dos anteriores y requisitos adicionales de proceso del fabricante y administración. También proporciona la evaluación de las capacidades de seguridad de un producto con conocimiento de los controles internos de seguridad y las prácticas de negocio del fabricante para endosar la vida útil del producto.

En el mundo conectado de hoy, hay una variedad enorme de dispositivos que ofrecen puntos de entrada para ataques cibernéticos. Ahora es el momento en que los desarrolladores de software y fabricantes entiendan las vulnerabilidades de los sistemas y protejan sus productos contra ataques. El protocolo UL 2900-2-3 puede ayudar a garantizar el rendimiento y la confiabilidad del software del producto a mitigar estos riesgos.

Para conocer más acerca de las iniciativas y servicios de UL para combatir la ciberseguridad visite <https://industries.ul.com/cybersecurity>.

+++++++

**Sobre a UL**

UL es una compañía global independiente de primer nivel dedicada a la ciencia de la seguridad que promueve el progreso desde hace más de 120 años. Sus casi 11.000 profesionales están guiados por la misión de UL de fomentar entornos seguros para vivir y trabajar para todas las personas. UL utiliza la investigación y los estándares para progresar continuamente y satisfacer las necesidades de seguridad en constante evolución. Nos asociamos con empresas, fabricantes, asociaciones comerciales y autoridades regulatorias internacionales para brindar soluciones a una cadena de suministro global cada vez más compleja. Para más información acerca de nuestros servicios de certificación, prueba, inspección, capacitación y educación, visite [http://www.UL.com.](http://www.ul.com/)