OAC Boletín de Octubre

"El mayor riesgo para la seguridad en Internet no son los delincuentes informáticos, sino los Estados que han encontrado en la tecnología una herramienta de control casi absoluto"

Yolanda Quintana

Contenidos

CIBERDEFENSA

- Documento de Interés: Síntesis de los Ciberconflictos de 2017

CIBERSEGURIDAD

- Documento de Interés: Estrategia Nacional de Cyber de los EE.UU.
- La relación con un app, no termina cuando se desinstala del dispositivo móvil

CIBERCRIMEN

- La internet de las cosas y los riesgos para la seguridad en el Hogar

CIBERFORENCIA

- Vulnerabilidades en Facebook
- Vulnerabilidades en Whatsapp video llamadas, podrían comprometer tu cuenta

CIBERDEFENSA

Documento de Interés

Síntesis de los Ciberconflictos (Hotspots) de 2017

En 2016 y 2017, los incidentes cibernéticos ocuparon titulares en todo el mundo, ellos constituyen una herramienta accesible para diversidad de actores.

Los ataques cibernéticos han demostrado ser efectivos pese a no haber evolucionado en su concepción tecnológica sobre los originales empleos para ciberdelitos, desde la aparente participación Rusa en las elecciones presidenciales de Estados Unidos y Europa, hasta la paralización de la compañía naviera más grande del mundo, Maersk, a través del malware NotPetya.

El documento ofrece una visión general acerca de: La politización de las acciones en el ciberespacio, los cibermedios como herramientas no aisladas de las operaciones convencionales y analiza las posturas adoptadas por las potencias respecto del uso legítimo de los cibermedios. El empleo de cibermedios en los contextos estratégicos o en los conflictos políticos, son diferentes.

Cada vez más, los estados politizan, militarizan y aseguran el ciberespacio como dominio estratégico, demostrando que sin dudas están ligadas las operaciones cibernéticas a sus contextos políticos, y los problemas cibernéticos deben analizarse como tales.

En el próximo número del boletín, publicaremos un reporter sobre el link que adjuntamos.

http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-06.pdf

_ _ _

CIBERSEGURIDAD

Documento de Interés

Estrategia Nacional de Cyber de los EE.UU.

Los EE.UU., han presentado su Estrategia de Ciberseguridad, llama la atención, que no emplean este nombre sino el genérico de Cyber, ello se debe a que tras el concepto de ciberseguridad como lo explica su presidente Donald Trump, el ciberespacio atraviesa todas las facetas de la vida de los estadunidenses.

Se trata de un documento compacto de fácil lectura que contiene aspectos que van desde la seguridad de las redes federales y las infraestructuras críticas hasta aspectos relacionados con el cibercrimen, para luego tratar el desarrollo de una fuerza capaz en el ciberespacio y aspectos esenciales como la resiliencia y las conductas en el ciberespacio, entre otros aspectos tratados.

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

La relación con un app, no termina cuando se desinstala del dispositivo móvil

Las herramientas para desinstalar software permiten a los desarrolladores identificar a los usuarios aún después de la desinstalación y borrado de la app. Ello permite a los desarrolladores obtener información y continuar enviando por ejemplo propagandas no deseadas.

https://www.bloomberg.com/news/articles/2018-10-22/now-apps-can-track-you-even-after-you-uninstall-them

– – –

CIBERCRIMEN

La internet de las cosas y los riesgos para la seguridad en el Hogar

Los nuevos dispositivos IoT (Internet de las cosas), podrían ser un riesgo por su alta conectividad permitiendo a los Hackers acceder a estos dispositivos, debido a que los mismos son tan vulnerables como los teléfonos inteligentes o las computadoras personales. Así lo advierte un informe de ciberseguridad de Panda, la empresa desarrolladora de software de seguridad informática.

https://www.pandasecurity.com/mediacenter/mobile-news/iot-robots-future/

– – –

CIBERFORENCIA

Vulnerabilidades en Facebook

En la tarde del martes 25 de septiembre, el equipo de ingeniería descubrió un problema de seguridad que afectó a casi 50 millones de cuentas. Guy Rosen, vicepresidente de gestión de productos de Facebook, dijo: “Nos lo estamos tomando muy en serio y queríamos que todos supieran lo que sucedió y las medidas inmediatas que hemos tomado para proteger la seguridad de las personas”.

Los detalles técnicos son suministrados por Pedro Canahuati, Vicepresidente de Ingeniería, Seguridad y Privacidad.

https://newsroom.fb.com/news/2018/09/security-update/

– – –

Vulnerabilidades en Whatsapp video llamadas, podrían comprometer tu cuenta

¿Qué pasaría si solo recibir una videollamada en WhatsApp pudiera hackear su teléfono inteligente?, la investigadora de seguridad de Google Project Zero, Natalie Silvanovich, encontró una vulnerabilidad crítica en el mensajero de de la citada aplicación que podría haber permitido a los piratas informáticos tomar el control total de su WhatsApp solo por videollamadas a través de la aplicación de mensajería.

https://thehackernews.com/2018/10/hack-whatsapp-account-chats.html?m=1

Detalles técnicos

https://bugs.chromium.org/p/project-zero/issues/detail?id=1654