BOLETÍN DE ALERTA

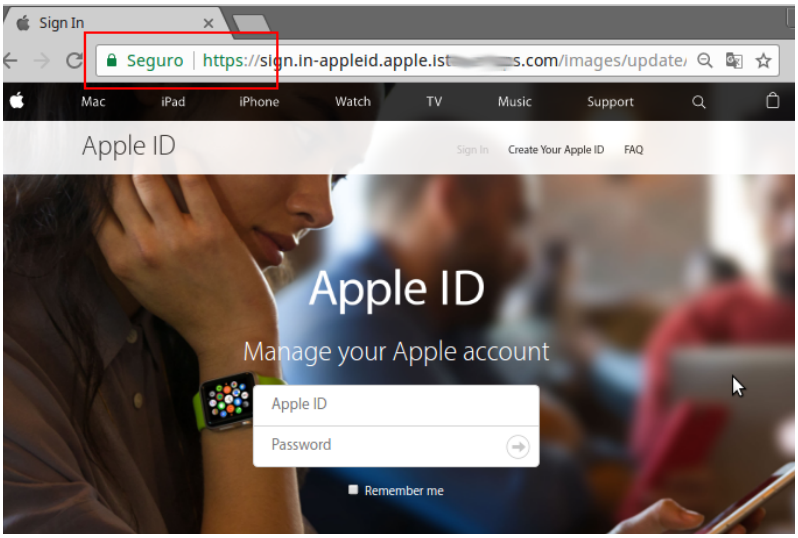
Boletín Nro.: 2017-08
Fecha de publicación: 02/06/2017
Tema: Phishing sobre HTTPs y con certificados válidos

Descripción:

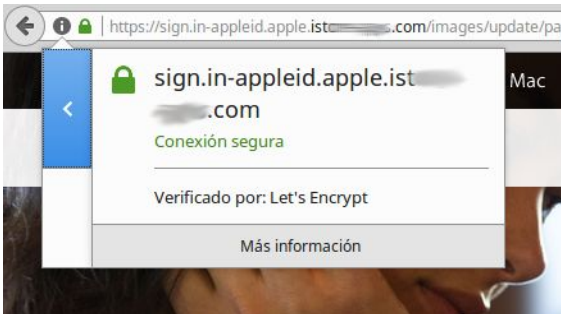
El día de ayer se ha detectado una campaña de distribución de correos falsos, supuestamente de Apple, con un agradecimiento por una supuesta compra de una aplicación y con un archivo pdf con los detalles de la supuesta compra. Por supuesto, se trata de una compra que nunca hicimos.

Debido a que el archivo pdf en sí no contiene código ejecutable malicioso, ningún antivirus lo detectará porque, efectivamente, no se trata de un troyano ni otro tipo de malware. Sin embargo, en el pdf, que simula ser una factura por la compra, se encuentra un enlace para la cancelación de la supuesta compra.

Al abrir dicho enlace, la víctima será redirigida a una falsificación del sitio web del iStore de Apple, el cual se ve idéntico al original. Sin embargo, se trata de un dominio malicioso. Lo llamativo del caso es que el sitio web se encuentra sobre HTTPs y que cuenta con un certificado válido emitido por Let's Encrypt para este dominio malicioso. Por lo tanto, al contar con un certificado válido reconocido, los navegadores lo clasifican como un sitio seguro, mostrando el candado verde en la barra de navegación.



CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py



Let's Encrypt es un proyecto relativamente reciente, que provee certificados válidos gratuitos, mediante un proceso de validación automatizado, de modo a que todos los sitios web pueda estar sobre HTTPs sin costo y mediante un proceso ágil. Todos los navegadores reconocen a Let's Encrypt como una autoridad certificadora confiable y por tanto reconocen sus certificados y lo indican con un candado verde.
El problema de esta validación automatizada es que existe un menor control sobre la identidad y/o las intenciones reales de la persona que solicita el certificado y sobre el contenido de la página web.
Esto hace que una víctima desprevenida pueda fiarse de la falsa sensación de seguridad que le proporciona el candado verde y el https:// y cayera en el engaño, ingresando sus credenciales en el sitio falso.

Impacto:

Un cibercriminal puede obtener las credenciales (usuario, contraseña, PIN, etc.) de víctimas desprevenidas que las ingresen en un sitio falso.

Mitigación:

Debido a que no se trata del compromiso de un certificado, sino de un mal uso de un servicio legítimo como es el de la emisión de certificados gratuitos automatizados de Let's Encrypt, las medidas preventivas de concienciación son fundamentales para evitar que usuarios caigan en el engaño:

- Evitar ingresar a enlaces dudosos de los cuales no tenga la absoluta certeza que son legítimos.
- Observar con detenimiento la URL del sitio web en el que uno va a ingresar sus credenciales. Muchas veces, la URL puede ser muy similar, pudiendo un único caracter diferenciarla de la real.
- No fiarse del candado verde que aparece en la barra de direcciones. Éste es únicamente un indicador de que la conexión se encuentra cifrada con un certificado válido emitido por una entidad reconocida, pero no es garantía alguna sobre la legitimidad de la misma ni de su contenido.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py