Boletín de Ciberseguridad | CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Miércoles 19 de Junio del 2019

8FPH-00028-001 correos de phishing que buscan explotar vulnerabilidad CVE-2018-0802

Características
Alerta de Seguridad Informática (8FPH-00028-001)
Nivel de Riesgo: Alto
Tipo: Phishing - Malware
Fecha de lanzamiento original: 13 de junio de 2019 | Última revisión 13 de Junio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de correos electrónicos que tienen la apariencia de casillas de Gmail, pero en realidad los correo de origen provienen de “gasatex.com” y “sinspam.com”, los que contienen un archivo adjunto en formato Word, el que se utiliza para explotar la vulnerabilidad CVE-2018-0802 de Office.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00028-001.pdf

8FPH-00029-001 Phishing Bancario Ofrece 500 Mil Pesos por Actualizar Datos

Características
Alerta de Seguridad Informática (8FPH-00029-001)
Nivel de Riesgo: Alto
Tipo: Phishing
Fecha de lanzamiento original: 17 de Junio de 2019 | Última revisión 17 de Junio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), en colaboración con el Departamento de Tecnologías de la Información del Servicio Agrícola y Ganadero, han identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco de Chile. El correo trata de persuadir a los clientes para que actualicen sus datos y ofrecen como incentivo $500.000 mil pesos, lo que serían supuestamente depositados de forma automática con la actualización de los datos. Adicionalmente, los clientes reciben un segundo estímulo, el de estar participando en un sorteo de 30 ipads mini, 20 televisores 4k, entre otros. Bajo las premisas anteriores, los delincuentes intentan convencer a sus víctimas para que accedan a un enlace malicioso ubicado en el correo y de esta forma, entregar las credenciales de acceso de la cuenta bancarias.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00029-001.pdf

8FPH-00030-001 Lista de Dominios de Phishing Bancario

Características
Alerta de Seguridad Informática (8FPH-00030-001)
Nivel de Riesgo: Alto
Tipo: Phishing
Fecha de lanzamiento original: 17 de Junio de 2019 | Última revisión 17 de Junio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado 26 dominios de suplantación del Banco Chile que intentan engañar a los clientes utilizando técnicas de phishing. Los delincuentes intentan convencer a sus víctimas a través de correos electrónicos u otros medios para que accedan a los sitios aquí indicados, con la finalidad de que los clientes entreguen sus credenciales de acceso a sus cuentas bancarias.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00030-001.pdf

8FPH-00031-001 Phishing Suplanta al Servicio de Impuestes Internos

Características
Alerta de Seguridad Informática (8FPH-00031-001)
Nivel de Riesgo: Alto
Tipo: Phishing - Malware
Fecha de lanzamiento original: 17 de Junio de 2019 | Última revisión 17 de Junio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing con Malware asociado, a través de un correo electrónico que supuestamente proviene del Servicio de Impuesto Internos. Los delincuentes buscan engañar a los usuarios insinuando en el título del correo que se trataría de un segundo aviso. El contenido del mensaje advierte a los usuarios que, para evitar una sanción económica que podría ascender a 75 UTM, deben descargar un supuesto documento de restitución de la declaración. Al seleccionar dicho enlace, se desencadena la descarga de archivos maliciosos, que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando además, puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00031-001.pdf

ALERTA (AA19-168A) VULNERABILIDAD BLUEKEEP EN EL SISTEMA OPERATIVO DE MICROSOFT

Características
Alerta de Seguridad Informática (AA19-168A)
Fecha de lanzamiento Original: 17 de Junio de 2019 | Última revisión 18 de Junio de 2019
Emitido por: CISA | Department of Homeland Security | US Government

Resumen
La Agencia de Ciberseguridad y de Seguridad de las Infraestructuras de los Estados Unidos, por sus siglas en inglés, CISA, está emitiendo esta Alerta para proporcionar información sobre la vulnerabilidad conocida como "BlueKeep", que existe en los siguientes Sistemas Operativos de Microsoft Windows (OS), incluidas las versiones de 32 y 64 bits, así como todas las versiones del Service Pack:

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

Detalle disponible en el enlace:
Información disponible en español en:
https://www.csirt.gob.cl/media/2019/06/ALERTA-AA19-168A.pdf
Información publicada originalmente en: https://www.us-cert.gov/ncas/alerts/AA19-168A

ACTUALIZACIÓN DE SEGURIDAD PARA VULNERABILIDAD EN FIREFOX, FIREFOX ESR

Características
Alerta de Seguridad Informática de Mozilla
Nivel de Riesgo: Crítico
Fecha de lanzamiento Original: 18 de Junio de 2019 | Última revisión 18 de Junio de 2019
Emitido por: Mozilla Foundation Security Advisory

Resumen
Mozilla ha lanzado actualizaciones de seguridad para abordar una vulnerabilidad en Firefox y Firefox ESR. Se puede producir un tipo de vulnerabilidad de confusión cuando se manipulan objetos de JavaScript debido a problemas en Array.pop. Un atacante que abuse de esta falla podría aprovechar esta vulnerabilidad para tomar el control de un sistema afectado.
Se recomienda a los usuarios y administradores a revisar el Aviso de Seguridad de Mozilla para Firefox 67.0.3 y Firefox ESR 60.7.1 y aplicar las actualizaciones necesarias.

Detalle disponible en el enlace:
https://www.mozilla.org/en-US/security/advisories/mfsa2019-18/