BOLETÍN DE CIBERSEGURIDAD

OCTUBRE 2022

ADV

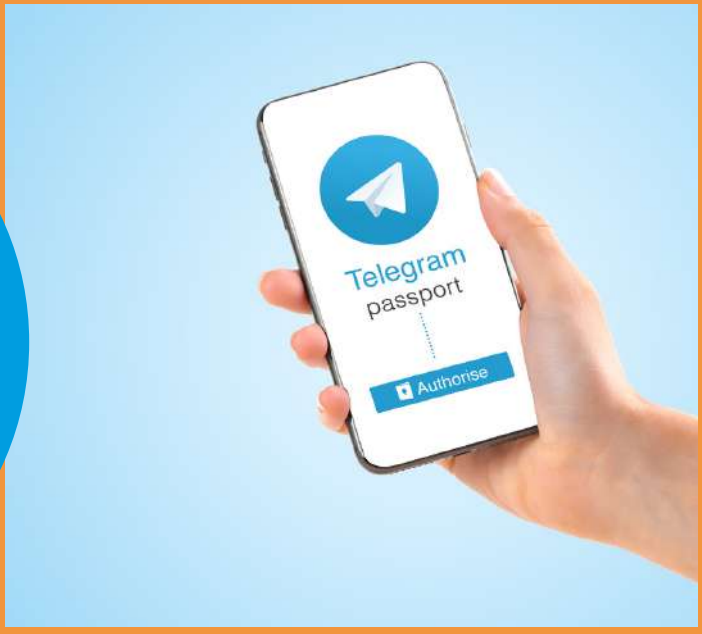
ÍNDICE

NOTICIAS INTERNACIONALES

DESCUBREN SPYWARE EN TELEGRAM QUE ES CAPAZ DE ROBAR DATOS MÓVILES DE LOS USUARIOS

10/10/2022

UN EQUIPO DE INVESTIGADORES HA DESCUBIERTO UN SOFTWARE ESPÍA DIRIGIDO A DISPOSITIVOS ANDROID



Agencia Europa Press. (2022, 10 octubre). Descubren spyware en Telegram que es capaz de robar datos móviles de los usuarios. El Comercio Perú. https://elcomercio.pe/tecnologia/actualidad/descubren-spyware-en-telegram-que-es-capaz-de-robar-datos-moviles-de-los-usuarios-ciberseguridad-malware-noticia/

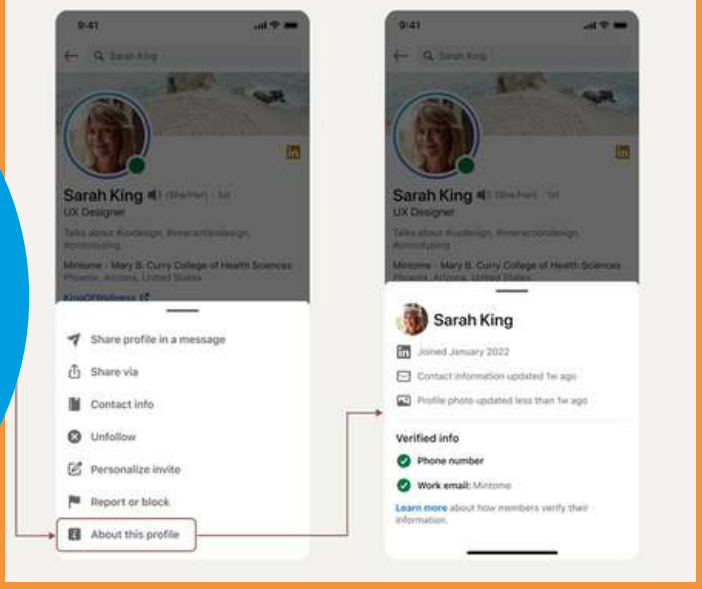
Un equipo de investigadores ha descubierto un software espía dirigido a dispositivos Android y oculto en una aplicación ilegítima distribuida a través de Telegram, capaz de monitorizar la actividad de los usuarios y robar los datos de los smartphones infectados.

Los expertos en ciberseguridad de Zimperium zLabs han llamado a este troyano de acceso remoto (RAT, por sus siglas en inglés) RatMilad, que habría afectado a teléfonos de empresas de países de Oriente Próximo.Los atacantes han integrado este malware espía en una aplicación fraudulenta llamada NumRent, que adopta el aspecto y el diseño de otra existente, TextMe, y que se distribuye mediante enlaces para su descarga a través de Telegram.

LINKEDIN LANZA NUEVA FUNCIÓN DE SEGURIDAD PARA IDENTIFICAR PERFILES FALSOS

28/10/2022

LINKEDIN ES EL ESCENARIO DE ENGAÑOS, DESDE LAS FALSAS OFERTAS DE TRABAJO HASTA FRAUDES COMO ESTAFAS PIRAMIDALES.



ESET. (2022, 28 octubre). https://www.welivesecurity.com/la-es/2022/10/28/linkedin-lanza-funcion-seguridad-identificar-perfiles-falsos/

Al igual que las demás redes sociales, LinkedIn es el escenario de engaños, desde las falsas ofertas de trabajo hasta fraudes como estafas piramidales. Como hemos visto con ejemplos como Lazarus, un grupo que en varios ataques en los últimos años ha utilizado LinkedIn para distribuir malware, varios actores maliciosos utilizan LinkedIn para realizar estafas, robar credenciales o distribuir malware que les permite robar información sensible o incluso moverse dentro de una red corporativa.

Si bien muchas personas tienen esa percepción de que LinkedIn es una plataforma segura, un entorno profesional donde podemos bajar la guardia, lamentablemente la realidad muestra que aprovechada por cibercriminales.

De hecho, en febrero de este año los ataques de phishing simulando ser correos oficiales de LinkedIn aumentaron más de 230%.

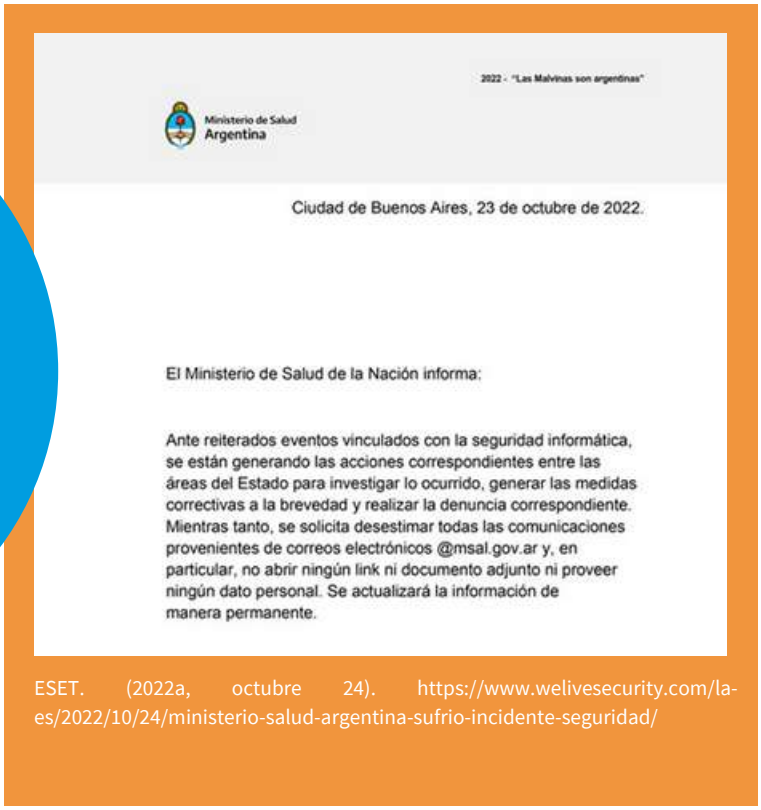
En este contexto LinkedIn anunció el lanzamiento en las próximas semanas de nuevas funcionalidades de seguridad para brindar más herramientas a la hora de identificar la autenticidad de una cuenta.

La primera de las nuevas funciones se llama **“About this profile”** y permite obtener más información de una cuenta. Por ejemplo, fecha de creación de un perfil, fecha de la última actualización, si el número de teléfono está verificado o si el correo asociado a una cuenta de LinkedIn es de una empresa.

MINISTERIO DE SALUD DE ARGENTINA SUFRIÓ INCIDENTE DE SEGURIDAD

24/10/2022

DURANTE EL FIN DE SEMANA EL MINISTERIO DE SALUD DE LA NACIÓN ARGENTINA LANZÓ UN COMUNICADO CONFIRMANDO QUE ESTÁ INVESTIGANDO UN INCIDENTE DE SEGURIDAD QUE AFECTÓ A SUS SISTEMAS.



2022 - "Las Malvinas son argentinas"

Ministerio de Salud
Argentina

Ciudad de Buenos Aires, 23 de octubre de 2022.

El Ministerio de Salud de la Nación informa:

Ante reiterados eventos vinculados con la seguridad informática, se están generando las acciones correspondientes entre las áreas del Estado para investigar lo ocurrido, generar las medidas correctivas a la brevedad y realizar la denuncia correspondiente. Mientras tanto, se solicita desestimar todas las comunicaciones provenientes de correos electrónicos @msal.gov.ar y, en particular, no abrir ningún link ni documento adjunto ni proveer ningún dato personal. Se actualizará la información de manera permanente.

ESET. (2022a, octubre 24). https://www.welivesecurity.com/la-es/2022/10/24/ministerio-salud-argentina-sufrio-incidente-seguridad/

Según explicaron fuentes oficiales a los medios, el incidente comenzó por el compromiso de la cuenta de una trabajadora del Ministerio. Por el momento se está investigando la situación. Igualmente, desde la cuenta oficial del Ministerio recomiendan desestimar cualquier correo electrónico oficial (@msal.gov.ar) y sobre todo no abrir ningún enlace ni archivo adjunto que pueda incluir.

Según reveló Infobae, el domingo recibieron un correo desde una cuenta del Ministerio que contenía un listado de supuestos pacientes de Argentina portadores de HIV y luego recibieron decenas de mensajes que informaban sobre supuestas cuentas comprometidas. Además, durante el fin de semana estuvieron circulando noticias falsas que hacía referencia a información extraída de una plataforma del Gobierno, más específicamente del Registro de Audiencias (RUA), que daba cuenta de reuniones que habían tenido funcionarios del organismo con famosos. Según explicaron, desde la cuenta de la cuenta comprometida fue que se subieron los registros de las supuestas reuniones.

La semana pasada investigadores habían reportado que en foros estaban comercializando accesos al Ministerio de Salud que incluían credenciales de acceso al Sistema Integrado de Información Sanitaria Argentina que contiene información de pacientes.

CONTINÚA EL ENGAÑO DEL TURNO DE LAS VACUNAS PARA ROBAR CUENTAS DE WHATSAPP

23/10/2022

ESET, COMPAÑÍA LÍDER EN DETECCIÓN PROACTIVA DE AMENAZAS, ALERTA QUE LOS ESTAFADORES CONTINÚAN UTILIZANDO EL MISMO MODUS OPERANDI DEL AÑO PASADO PARA ROBAR CUENTAS DE WHATSAPP A USUARIOS.

Continúa el engaño del turno de las vacunas para robar cuentas de WhatsApp – EMPREFINANZAS. (2022, 23 octubre). https://emprefinanzas.com.mx/2022/10/23/continua-el-engano-del-turno-de-las-vacunas-para-robar-cuentas-de-whatsap

Luego, se hacen pasar por los titulares de las cuentas y escriben a sus contactos para intentar engañarlos haciéndoles creer que tienen una urgencia y solicitan un préstamo o que realicen una transferencia. Muchas veces, las personas contactadas, creyendo que están hablando con el titular de la cuenta, caen en la trampa y realizan la transferencia.

Desde ESET se alertó a los usuarios en 2021 sobre esta forma de actuar los delincuentes, dado que estaban al tanto de casos en los que se estaban haciendo pasar por el Gobierno de la Ciudad de Buenos Aires en Argentina.

En los últimos meses, el equipo de investigación observó varias denuncias donde las personas alertan que son contactados por un teléfono con la imagen del Ministerio de Salud de la Provincia de Buenos Aires.

CAMPAÑA DOMESTIC KITTEN PARA MONITOREAR A CIUDADANOS IRANÍES UTILIZA EL NUEVO MALWARE FURBALL

22/10/2022

UNA NUEVA VERSIÓN DEL MALWARE PARA ANDROID FURBALL QUE SE UTILIZA EN UNA CAMPAÑA DE DOMESTIC KITTEN LLEVADA ADELANTE POR EL GRUPO DE APT-C-50.

Aplicación de traducción esconde malware para monitorear a ciudadanos iraníes. (2022b, octubre 22). https://www.revistaseguridad.cl/2022/10/22/aplicacion-de-traduccion-esconde-malware-para-monitorear-a-ciudadanos-iranies/

Se sabe que la campaña Domestic Kitten busca monitorear a través de los dispositivos móviles la actividad que realizan ciudadanos iraníes y esta nueva versión de FurBall no es diferente en su objetivo final. Desde junio de 2021 este malware se distribuye como una app de traducción a través de un sitio web falso que imita un sitio legítimo iraní que ofrece artículos y libros traducidos. La aplicación maliciosa fue subida a VirusTotal y activó una de nuestras reglas YARA (utilizadas para clasificar e identificar muestras de malware), lo que nos dio la oportunidad de analizarla.

Esta versión de FurBall cuenta con las mismas funcionalidades para espiar que las versiones anteriores; sin embargo, los actores de amenazas ofuscaron ligeramente los nombres de las clases y métodos, las strings, los registros y los URI del servidor. Esta actualización también requirió pequeños cambios en el servidor C&C, precisamente, los nombres de los scripts PHP del lado del servidor. Dado que la capacidad del malware no ha cambiado en esta variante, el objetivo principal de esta actualización parece ser evitar la detección por parte soluciones de seguridad. Sin embargo, estas modificaciones no han tenido efecto en el software de ESET, ya que los productos de ESET detectan esta amenaza como Android/Spy.Agent.BWS.

NOTICIAS NACIONALES

“URGENTE LEGISLAR SOBRE CIBERSEGURIDAD”: EL CONGRESO PREPARA UNA LEY QUE PROTEJA A MÉXICO DE HACKEOS FUTUROS

20/10/2022

“ES URGENTE LEGISLAR SOBRE CIBERSEGURIDAD”, DECLARÓ ANTE LAS CÁMARAS. AL RESPECTO, SEÑALÓ QUE HAN EXISTIDO NUMEROSOS INTENTOS DE HACKEO A DEPENDENCIAS FEDERALES, DONDE EL SENADO NO HA SIDO LA EXCEPCIÓN; INCLUSO, LA INICIATIVA PRIVADA (IP) HA SIDO SUJETO DE ATAQUES DE ESTA NATURALEZA.

NVD - Results. (s. f.). Recuperado 30 de octubre de 2022, de https://nvd.nist.gov/vuln/search/results?form_type=Advanced

Es en este contexto en el que explicó que tanto la Cámara de Diputados como el Senado de la República trabajarán de manera conjunta para que en este periodo ordinario de sesiones se tenga una Ley de Ciberseguridad que atienda las necesidades del Siglo XXI.

Con ello se espera prevenir ataques de hackers nacionales e internacionales que vulneran la información del Estado mexicano, particularmente, la relacionada a gobernabilidad y seguridad nacional. Detalló que la legislación que emane de estas discusiones en las diferentes mesas de trabajo aprobará de todas las corrientes parlamentarias y modernizará, entre otras cosas, el marco punitivo a quien violente la privacidad de las instituciones.

Ante la pregunta directa sobre el peso que cree que tuvo este atentado contra las instituciones del Estado, Monreal Ávila sentenció que no se trata de una vulneración menor, la cual debe de ser atendida con toda seriedad para que cada poder de la unión, motivo por el cual será trabajo del legislativo entregar una redacción que amplíe el marco jurídico en materia de seguridad digital para el gobierno.

Asimismo, señaló que mantener estos mecanismos de protección atienden a la conducta congruente en materia de seguridad promovida en el Senado, por lo que también mencionó que se debe de revisar la estrategia nacional de seguridad del gobierno federal para lograr tener un Estado mejor preparado en este rubro.

“URGENTE LEGISLAR SOBRE CIBERSEGURIDAD”: EL CONGRESO PREPARA UNA LEY QUE PROTEJA A MÉXICO DE HACKEOS FUTUROS

20/10/2022

Cabe destacar que Ricardo Monreal ya había publicado una reflexión mayor al respecto, en la que planteó tres preguntas tras el hackeo:

1.-¿Qué pasaría si se filtrara información que pusiera en riesgo la seguridad nacional? 2.- ¿Qué tan vulnerable es la información confidencial, de volverse pública mediante ataques como los ocurridos? 3.- ¿Cómo se defenderá en el futuro el Estado mexicano de grupos que pretendan violentar la seguridad digital?

Finalmente, cabe recordar que en materia legal, el Código Penal Federal (CPF) tiene estipulado un marco endeble en materia de protección de datos del Estado, pues dicha información es de suma importancia para la gobernabilidad y, los castigos que se tienen en materia, son pequeños.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2021-38733	10/28/2022	SEMCMS SHOP 1.1 - SQL injection	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2021-38733

Descripción: SEMCMS SHOP v 1.1 is vulnerable to SQL Injection via Ant_BlogCat.php.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-3385	10/28/2022	Path Traversal, Stack-based Buffer Overflow	CVSS v3.1:9.8 [critical]	nvd.nist.gov/vuln/detail/CVE-2022-3385

Descripción: Advantech R-SeeNet Versions 2.4.17 and prior are vulnerable to a stack-based buffer overflow. An unauthorized attacker can remotely overflow the stack buffer and enable remote code execution.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-39976	10/27/2022	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-39976

Descripción: School Activity Updates with SMS Notification v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /modules/announcement/index.php?view=edit&id=.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
VE-2022-3719	10/28/2022	Out-of-bounds Write	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-3719

Descripción: A vulnerability has been found in Exiv2 and classified as critical. This vulnerability affects the function QuickTimeVideo::userDataDecoder of the file quicktimevideo.cpp of the component QuickTime Video Handler. The manipulation leads to heap-based buffer overflow. The attack can be initiated remotely. The name of the patch is a38e124076138e529774d5ec9890d0731058115a. It is recommended to apply a patch to fix this issue. VDB-212350 is the identifier assigned to this vulnerability.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-3717	10/28/2022	Improper Restriction of Operations	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-3717

TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2022

Descripción: A vulnerability, which was classified as critical, has been found in Exiv2. Affected by this issue is the function BmffImage::boxHandler of the file bmffimage.cpp. The manipulation leads to memory corruption. The attack may be launched remotely. The name of the patch is a58e52ed702d3bc7b8bab7ec1d70a4849eebece3. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-212348

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-3714	10/28/2022	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-3714

Descripción: A vulnerability classified as critical has been found in SourceCodester Online Medicine Ordering System 1.0. Affected is an unknown function of the file admin/?page=orders/view_order. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. VDB-212346 is the identifier assigned to this vulnerability

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-2782	10/28/2022	Insufficient Session Expiration	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-2782

Descripción: In affected versions of Octopus Server it is possible for a session token to be valid indefinitely due to improper validation of the session token parameters.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-39355	10/28/2022	Improper Authentication	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-39355

Descripción: Discourse Patreon enables syncronization between Discourse Groups and Patreon rewards. On sites with Patreon login enabled, an improper authentication vulnerability could be used to take control of a victim's forum account. This vulnerability is patched in commit number 846d012151514b35ce42a1636c7d70f6dcee879e of the discourse-patreon plugin. Out of an abundance of caution, any Discourse accounts which have logged in with an unverified-email Patreon account will be logged out and asked to verify their email address on their next login. As a workaround, disable the patreon integration and log out all users with associated Patreon accounts.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-43003	10/28/2022	Out-of-bounds Write	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-43003

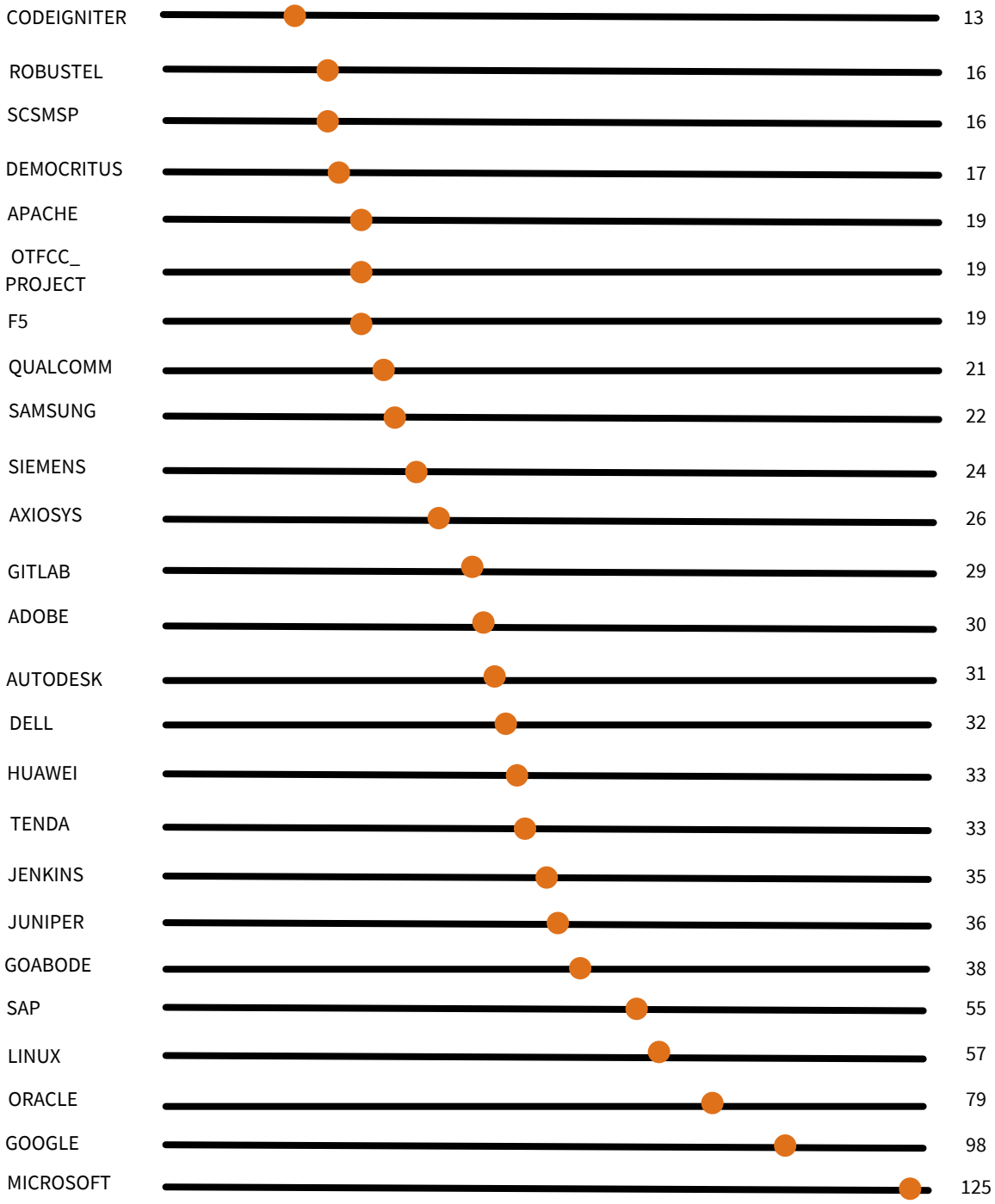
TABLA DE VULNERABILIDADES RELEVANTES: OCTUBRE 2022

Descripción: D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the pskValue parameter in the setRepeaterSecurity function.

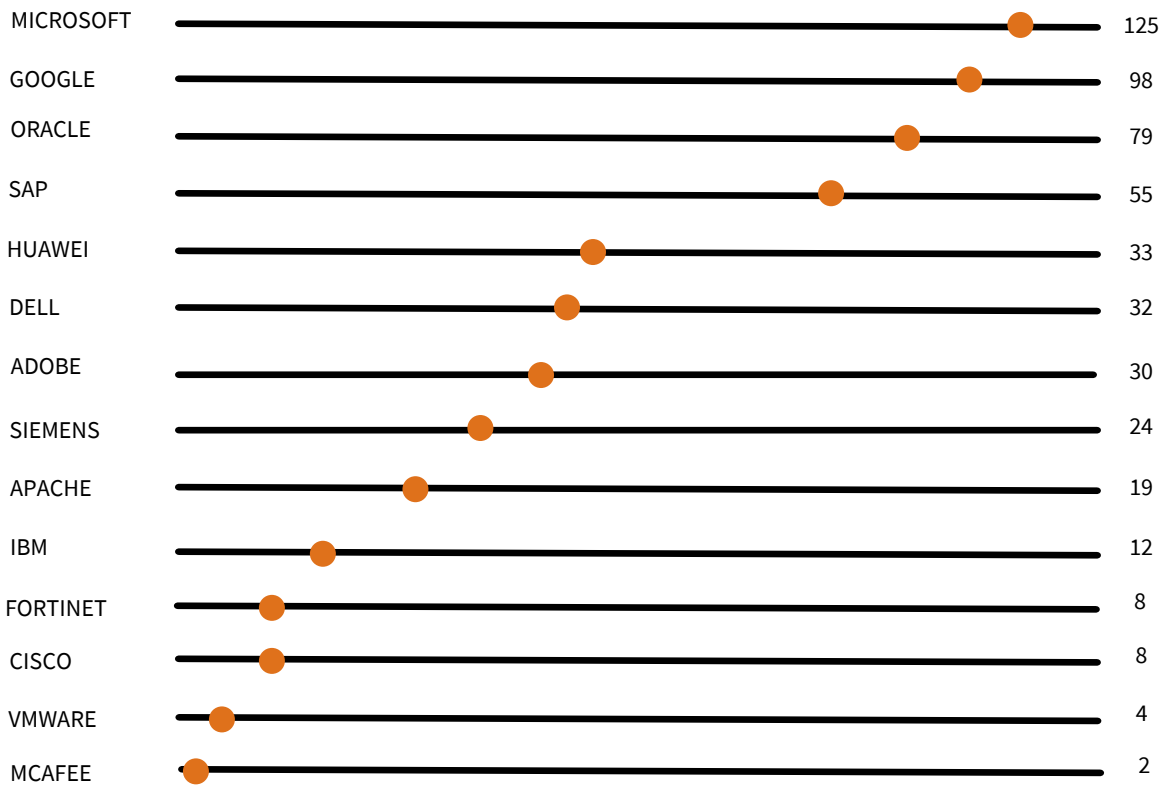
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-43002	10/28/2022	Stack overflow vulnerability	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-43002

Descripción: D-Link DIR-816 A2 1.10 B05 was discovered to contain a stack overflow via the wizardstep54_pskpwd parameter at /goform/form2WizardStep54.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: OCTUBRE DE 2022



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: OCTUBRE DE 2022



CULTURA DE CIBERSEGURIDAD

¿QUÉ ES EL PHISHING?

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

TIPOS DE PHISHING

SPEAR PHISHING

Mientras la mayoría de las campañas de phishing envían correos electrónicos masivos al mayor número posible de personas, el spear phishing es un ataque dirigido. Spear phishing ataca a una persona u organización específica, a menudo con contenido personalizado para la víctima o víctimas. Requiere un reconocimiento previo al ataque para descubrir nombres, cargos, direcciones de correo electrónico y similares. Los hackers buscan en Internet para relacionar esta información con lo que han averiguado sobre los colegas profesionales del objetivo, junto con los nombres y las relaciones profesionales de los empleados clave en sus organizaciones. Con esto, el autor del phishing crea un correo electrónico creíble

PHISHING DE CLONACIÓN

En este ataque, los delincuentes hacen una copia, o clonan, correos electrónicos legítimos enviados anteriormente que contienen un enlace o un archivo adjunto. Luego, el autor del phishing sustituye los enlaces o archivos adjuntos con contenido malicioso disfrazado para hacerse pasar por el auténtico. Los usuarios desprevenidos hacen clic en el enlace o abren el adjunto, lo que a menudo permite tomar el control de sus sistemas. Luego el autor del phishing puede falsificar la identidad de la víctima para hacerse pasar por un remitente de confianza ante otras víctimas de la misma organización.

PHISHING TELEFÓNICO

Este método se refiere al phishing a través del teléfono, a veces llamados phishing de voz o "vishing," un ejemplo es el phisher llamando y afirmando representando a su banco local, policía o incluso la Agencia Tributaria. A continuación, le asustan con algún tipo de problema e insisten en que lo solucione inmediatamente facilitando su información de cuenta o pagando una multa. Normalmente le piden que pague con una transferencia bancaria o con tarjetas prepago, porque son imposibles de rastrear.

CÓMO PROTEGERSE DEL PHISHING

- No abra correos electrónicos de remitentes que no le sean familiares.
- No haga clic en un enlace dentro de un correo electrónico a menos que sepa exactamente a dónde le lleva.
- Para aplicar esa capa de protección, si recibe un correo electrónico de una fuente de que la que no está seguro, navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima del sitio web en su navegador.
- Busque el certificado digital del sitio web.
- Si se le pide que proporcione información confidencial, compruebe que la URL de la página comienza con “HTTPS” en lugar de simplemente “HTTP”. La “S” significa “seguro”. No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos utilizan HTTPS porque es más seguro. Los sitios HTTP, incluso los legítimos, son vulnerables para los hackers.
- Si sospecha que un correo electrónico no es legítimo, seleccione un nombre o parte del texto del mensaje y llévelo a un motor de búsqueda para ver si existe algún ataque de phishing conocido que utiliza los mismos métodos.
- Pase el cursor del ratón por encima del enlace para ver si es legítimo.

REFERENCIAS

REFERENCIAS

- https://elcomercio.pe/tecnologia/actualidad/descubren-spyware-en-telegram-que-es-capaz-de-robar-datos-moviles-de-los-usuarios-ciberseguridad-malware-noticia/
- https://www.welivesecurity.com/la-es/2022/10/28/linkedin-lanza-funcion-seguridad-identificar-perfiles-falsos/
- https://www.welivesecurity.com/la-es/2022/10/24/ministerio-salud-argentina-sufrio-incidente-seguridad/
- https://emprefinanzas.com.mx/2022/10/23/continua-el-engano-del-turno-de-las-vacunas-para-robar-cuentas-de-whatsap
- https://www.revistaseguridad.cl/2022/10/22/aplicacion-de-traduccion-esconde-malware-para-monitorear-a-ciudadanos-iranies/
- https://nvd.nist.gov/vuln/search/results?form_type=Advanced
- Malwarebytes. (2019, 7 enero). ¿Qué es el phishing? | Cómo protegerse de los ataques de phishing. https://es.malwarebytes.com/phishing/

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 55 6178 9397

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300