BOLETÍN DE CIBERSEGURIDAD

MAYO 2022

ÍNDICE

NOTICIAS INTERNACIONALES

EXPLOTACIÓN MASIVA DE F5 BIG-IP CVE-2022-1388 (RCE)

11/05/2022

UNA FALLA CRÍTICA QUE PODRÍA SER EXPLOTADA PARA DESPLEGAR ATAQUES DE EJECUCIÓN REMOTA DE CÓDIGO (RCE).

Motos, V. (2022, 11 mayo). Explotación masiva de F5 BIG-IP CVE-2022-1388 (RCE). hackplayers. https://www.hackplayers.com/2022/05/explotacion-masiva-de-f5-big-ip-cve.html

50 VULNERABILIDADES EN DIVERSAS VERSIONES DE BIG-IP POR PARTE DE F5 NETWORKS

Se trata de una omisión de autenticación crítica que conduce a la ejecución remota de código en la interfaz REST de iControl de F5 BIG-IP:
http.title:"BIG-IP®-+Redirect" +"Server"

Esta mañana la compañía actualizó su alerta, recomendando a las organizaciones que usan sus controladores de entrega de aplicaciones actualizar, ya que la falla crítica está siendo explotada en escenarios reales.
En F5 BIG-IP se están ejecutando dos servidores HTTP diferentes:

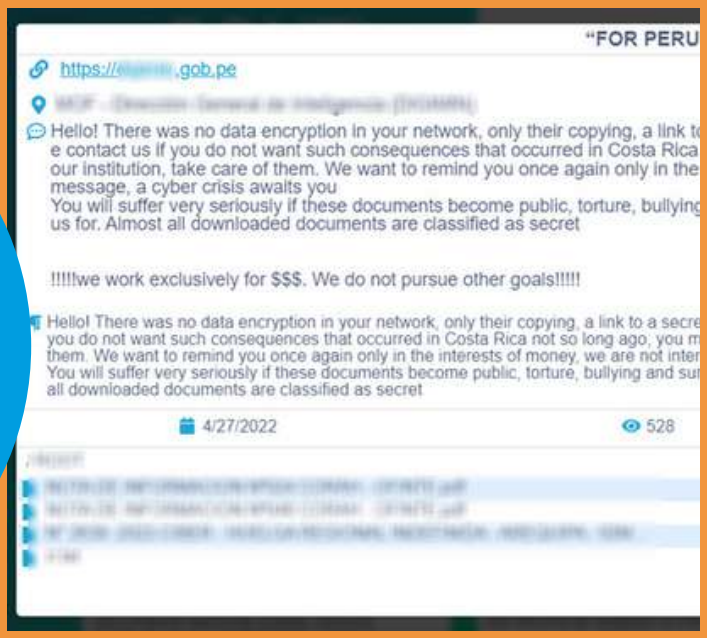
1/ un servidor httpd es Apache escuchando en el puerto 443, que ejecuta el front-end

2/ un servidor java es en realidad jetty, que ejecuta la API REST de iControl en el puerto 8100.

HACKERS DEL RANSOMWARE CONTI ASEGURAN HABER INFECTADO SISTEMAS DE LA AGENCIA DE INTELIGENCIA DE PERÚ; 9 GB DE DATOS ROBADOS

27/05/2022

CONTI GROUP ATACARON A MIEMBROS DE LA DIRECCIÓN GENERAL DE INTELIGENCIA DEL MINISTERIO DEL INTERIOR



R. (2022c, mayo 17). Hackers rusos atacan al servicio de inteligencia peruano y exigen millonaria recompensa. RPP. https://rpp.pe/tecnologia/mas-tecnologia/hackers-rusos-atacan-al-servicio-de-inteligencia-peruano-y-exigen-millonaria-recompensa-noticia-1405437

HAN REVELADO EL SEGUIMIENTO A FUNCIONARIOS PÚBLICOS

Los reportes fueron dados por Sudaca, Hildebrant en sus Trece y La Encerrona, mostrando el proceder de Conti Group, atacantes que utilizan malware para secuestrar información malware para secuestrar información y pedir recompensas millonarias para no revelar la información.

Conti Group es uno de los grupos de ransomware más famosos del mundo y, a causa de sus actividades más recientes, ha estado en la mira de Estados Unidos por un devastador ataque a los sistemas informáticos del Gobierno de Costa Rica a fines del mes pasado. El Gobierno estadounidense anunció una recompensa de 10 millones de dólares por información de sus líderes.

¡En el caso del ataque a la entidad gubernamental de Perú, los atacantes publicaron también una invitación para que desde el organismo se comuniquen para llegar a un acuerdo. En el mensaje Conti también amenaza a Perú que puede ocurrir lo mismo que sucedió en Costa Rica.

Conti es un conocido grupo de ransomware que opera bajo la modalidad de ransomware-as-a-service desde 2019 y ha sido una de las bandas más prolíficas en el último año, con importantes organizaciones de distintas partes del mundo.

LA UE ACUERDA UNA NUEVA LEGISLACIÓN SOBRE CIBERSEGURIDAD PARA LAS ORGANIZACIONES DE SERVICIOS CRÍTICOS

11/05/2022

EL PARLAMENTO DE LA UE Y EL CONSEJO ALCANZARON UN ACUERDO PROVISIONAL SOBRE LA LEY DE RESILIENCIA OPERATIVA DIGITAL (DORA)

P. (2022c, mayo 15). EU Agrees on Cybersecurity Laws. PYMNTS.Com. https://www.pymnts.com/es/cybersecurity/2022/eu-agrees-on-new-cybersecurity-laws-to-protect-financial-sector/

LA NUEVA DIRECTIVA SUSTITUIRÁ A LA ACTUAL NORMATIVA DE LA UE SOBRE LA SEGURIDAD DE LAS REDES

El miércoles (11 de mayo), el Parlamento de la UE y el Consejo alcanzaron un acuerdo provisional sobre la Ley de Resiliencia Operativa Digital (DORA), y aunque el acuerdo aún debe ser aprobado en sesión plenaria, esto se considera normalmente una formalidad una vez que hay consenso político.

La nueva directiva sustituirá a la actual normativa de la UE sobre la seguridad de las redes y los sistemas de información (Directiva NIS), que requiere una actualización debida “al creciente grado de digitalización e interconexión de nuestra sociedad y al aumento de las actividades cibermaliciosas a nivel mundial”.

La Directiva NIS 2 abarcará a las organizaciones medianas y grandes que operan en sectores críticos. Entre ellos se encuentran los proveedores de servicios públicos de comunicaciones electrónicas, servicios digitales, gestión de aguas residuales y residuos, fabricación de productos críticos, servicios postales y de mensajería, asistencia sanitaria y administración pública.

"La nueva legislación garantizará que los bancos, las aseguradoras y las instituciones financieras de la Unión Europea estén mejor equipados para prevenir, detectar y resolver los riesgos e interrupciones operativas digitales", dijo el eurodiputado Alfred Sant en un comunicado de prensa.

HACKER Y DISEÑADOR DE RANSOMWARE ENFRENTA CARGOS POR USO Y VENTA DE RANSOMWARE Y POR HACER ARREGLOS DE REPARTICIÓN DE FONDOS CON CIBERCRIMINALES

11/05/2022

LOS FISCALES DE NUEVA YORK PRESENTARON ESTA SEMANA CARGOS CRIMINALES EN CONTRA DE MOISÉS LUIS ZAGALA GONZÁLEZ,

Pérez, H. (2022, 17 mayo). Gobierno de EEUU acusa a médico venezolano de crear y vender ransomware usado por hackers. DiarioBitcoin. https://www.diariobitcoin.com/paises/norte-america/estados-unidos/medico-venezolano-acusado-crear-software-malicioso-para-ransomware/

VENEZOLANO DISEÑA UN TIPO RANSOMWARE

Los fiscales de Nueva York presentaron esta semana cargos criminales en contra de Moisés Luis Zagala González, un cardiólogo de 55 años residenciado en Venezuela, por haber presuntamente diseñado un tipo ransomware y haberlo vendido a organizaciones de ciberdelincuentes. El Departamento de Justicia (DOJ) de los Estados Unidos informó sobre las acusaciones en un comunicado el lunes.

De acuerdo con el informe, Zagala, quien supuestamente utiliza los seudónimos de “Nosophoros“, “Esculapio” y “Nabucodonosor”, construyó a finales de 2019 una herramienta llamada “Thanos“, un tipo de ransomware como servicio (RaaS) que permitió a sus usuarios crear e implementar sus propias variantes de ransomware.

El médico ahora enfrenta hasta 10 años de prisión por intento de intrusión informática y cargos de conspiración, en caso de ser llevado efectivamente ante la justicia en los Estados Unidos."

LA BOTNET SYSRV ES MÁS PODEROSA QUE NUNCA: NUEVOS EXPLOITS PARA TOMAR EL CONTROL DE DISPOSITIVOS LINUX Y WINDOWS

13/05/2022

EN SU MÁS RECIENTE VERSIÓN, LOS OPERADORES DE LA BOTNET SYSRV INCLUYERON NUEVO EXPLOITS PARA USAR MÁS VULNERABILIDADES

Narula, A. (2022, 18 mayo). La botnet Sysrv es más poderosa que nunca: Nuevos exploits para tomar el control de dispositivos Linux y. . . Ciberseguridad - Cibertip - Noticias de Hacking- Ciber Tips. https://www.cibertip.com/virus/la-botnet-sysrv-es-mas-poderosa-que-nunca-nuevos-exploits-para-tomar-el-control-de-dispositivos-linux-y-windows/

REPRESENTA UNA SERIA AMENAZA PARA SISTEMAS WINDOWS Y LINUX.

En su más reciente versión, los operadores de la botnet Sysrv incluyeron nuevo exploits para usar más vulnerabilidades, lo que representa una seria amenaza para sistemas Windows y Linux. Identificada como Sysrv-K, esta nueva cepa de malware también escanea Internet en busca de servidores web con fallas de seguridad para su explotación.

Las vulnerabilidades explotadas por estos hackers, todas con parches disponibles, incluyen fallas en plugins de WordPress, como el error de ejecución remota de código (RCE) en Spring Cloud Gateway identificado como CVE-2022-22947 y divulgado por la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA).

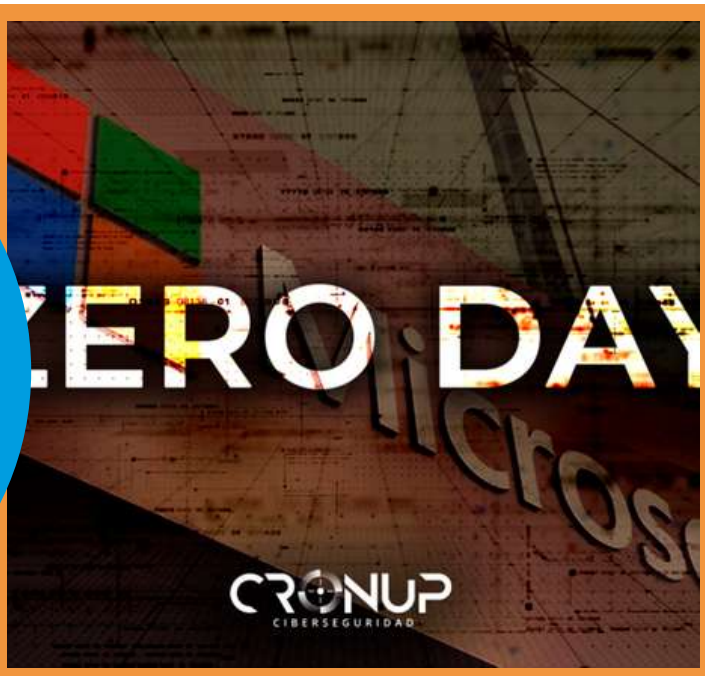
Posteriormente, la amenaza aprovecha las credenciales robadas para hacerse con el control del servidor web. Las capacidades de comunicación de la amenaza también se han mejorado con la inclusión de la capacidad de usar Telegram como canal de comunicación.

Al mismo tiempo, Sysrv-K ha conservado la capacidad de buscar claves SSH, direcciones IP o nombres de host en las máquinas violadas. Esta información es necesaria para que la amenaza intente propagarse aún más a través de conexiones SSH.

FOLLINA: DOCUMENTOS DE MS OFFICE COMO VULNERABILIDAD

27/05/2022

LA GRAN VULNERABILIDAD ZERO-DAY SE ENCUENTRA EN LA HERRAMIENTA MICROSOFT WINDOWS SUPPORT DIAGNOSTIC TOOL



Editorial Team. (2022, 2 junio). Follina: documentos de MS Office como puerta de entrada. Kaspersky. https://www.kaspersky.es/blog/follina-cve-2022-30190-msdt/27225/

LA VULNERABILIDAD PUEDE EXPLOTARSE A TRAVÉS DE UN DOCUMENTO

MSDT es una aplicación que se utiliza para recopilar automáticamente información de diagnóstico y enviarla a Microsoft cuando algo falla en Windows. La herramienta puede activarse desde otras aplicaciones (Microsoft Word es el ejemplo más popular) a través del protocolo especial URL MSDT. Si la vulnerabilidad se explota con éxito, los atacantes pueden ejecutar código arbitrario con los privilegios de la aplicación que activó el MSDT, es decir, en este caso, con los derechos del usuario que abrió el archivo malicioso. La vulnerabilidad CVE-2022-30190 puede explotarse en todos los sistemas operativos de la familia Windows, tanto en escritorio como en un servidor.

Los atacantes crean un documento malicioso de MS Office y de alguna forma se lo hacen llegar a la víctima.La forma más común de hacerlo es mediante phishing (un correo electrónico con un archivo adjunto malicioso) con la intención de que el usuario abra dicho archivo y desencadenar la vulnerabilidad.

El archivo infectado contiene un enlace a un archivo HTML que contiene un código JavaScript que ejecuta código malicioso en la línea de comandos a través de MSDT. Cuando la explotación es exitosa, los atacantes consiguen el control para instalar programas, ver, modificar o destruir datos, así como crear nuevas cuentas, es decir, hacer todo lo que permiten los privilegios de la víctima en el sistema.

NOTICIAS NACIONALES

EN UN TRIMESTRE, MÉXICO REGISTRÓ 80,000 MILLONES DE INTENTOS DE CIBERATAQUES

11/05/2022

AL MENOS 40 MIL PERSONAS ACCEDIERON A DATOS E INFRAESTRUCTURA DE RED DEL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA (SAT).

Herrera, E. (2022, 11 mayo). México sufrió 80 mil millones de intentos de ciberataques. Grupo Milenio. https://www.milenio.com/negocios/mexico-sufrio-80-mil-millones-intentos-ciberataques

"35 MIL PUERTOS DE USUARIOS QUE TENÍAN ACCESO A TODA LA INFORMACIÓN DEL SAT"

Los ataques cibernéticos en México no se detienen. Durante el primer trimestre del año, el país sufrió 80,000 millones de intentos de ciberataques y si bien hay una mayor atención hacia este tema, hace falta prevención y transparencia para generar entornos más efectivos.

México ha sido el país de América Latina con mayor actividad de distribuciones de ransomware en el primer trimestre del año con más de 14 mil detecciones, lo cual representa un 85.9 por ciento del total de la región.

Eduardo Zamora, director general de Fortinet México comentó: "Ahora más que nunca es indispensable contar con una estrategia integral de ciberseguridad si tenemos en cuenta que la digitalización de actividades cotidianas como el trabajo, la educación y el comercio han puesto al alcance de los ciberdelincuentes una superficie de ataque más amplia". https://www.milenio.com/negocios/mexico-sufrio-80-mil-millones-intentos-ciberataques

A la fecha se encuentra parchada la vulnerabilidad, es importante actualizar nuestros navegadores con frecuencia.

ATAQUE DE RANSOMWARE CAUSA PROBLEMAS EN UNA FÁBRICA DE FOXCONN EN MÉXICO

31/05/2022

EL GRUPO DE RANSOMWARE COMO SERVICIO LOCKBIT SE HAN HECHO RESPONSABLES DEL ATAQUE

Valdeolmillos, C. (2022, 3 junio). Ataque ransomware causa problemas en una fábrica de Foxconn en México. MuyComputerPRO. https://www.muycomputerpro.com/2022/06/03/ataque-ransomware-fabrica-foxconn

FOXCONN SUFRIÓ UN ATAQUE DE RANSOMWARE QUE OCASIONÓ PROBLEMAS DE FUNCIONAMIENTO

A finales de mayo sufrió un ataque de ransomware que ocasionó problemas de funcionamiento y operaciones en una de sus plantas de producción en México. Concretamente, en la localidad de Tijuana, que está situada en la zona de Baja California y cerca de la frontera con California (EEUU).

Foxconn no ha querido confirmar si los atacantes pudieron acceder a datos de la compañía como resultado del ataque, ni señalar si se hicieron con información o quién ha sido responsable del ciberataque.

Pero desde el grupo de ransomware como servicio LockBit se han hecho responsables del ataque, realizado el pasado 31 de mayo, y amenazan con filtrar datos robados a Foxconn a no ser que les paguen un rescate antes del próximo 11 de junio.

Esta no es la primera vez que Foxconn sufre un ataque de ransomware, ya que en diciembre de 2020, según confirmó la empresa, algunos de sus sistemas en EEUU fueron atacados con el ransomware DoppelPaymer, por atacantes que pidieron un pago de 34 millones de dólares en Bitcoin.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: MAYO 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-27342	04/22/2022	SQL inyection a via Link-Admin	CVSS v3.1: [crítico]	https://nvd.nist.gov/vuln/detail/CVE-2022-26708

Descripción: This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4. An attacker may be able to cause unexpected application termination or arbitrary code execution.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-30516	05/26/2022	Falla en Hospital-Management-System v1.0	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-30516

Descripción: In Hospital-Management-System v1.0, the editid parameter in the doctor.php page is vulnerable to SQL injection attacks.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-30493	05/26/2022	Inyección SQL en oretnom23 Automotive Shop	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-30493

Descripción: In oretnom23 Automotive Shop Management System v1.0, the product id parameter suffers from a blind SQL Injection Vulnerability allowing remote attackers to dump all database credential and gain admin access(privilege escalation).

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-30500	05/26/2022	Vulnerabilidad inyección SQL en Jfinal cms 5.1.0	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-30500

Descripción: Jfinal cms 5.1.0 is vulnerable to SQL Injection.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-30477	05/26/2022	Buffer overflow en el modulo httpd en Tenda AC Series	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-30477

Descripción: Tenda AC Series Router AC18_V15.03.05.19(6318) was discovered to contain a stack-based buffer overflow in the httpd module when handling /goform/SetClientState request.

TABLA DE VULNERABILIDADES RELEVANTES: MAYO 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-30838	05/24/2022	Covid-19 Travel Pass Management System v1.0	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-30838

Descripción: Covid-19 Travel Pass Management System v1.0 is vulnerable to SQL Injection via /ctpms/classes/Master.php?f=update_application_status.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28932	05/24/2022	D-Link DSL-G2452DG HW:T1\\tFW:ME_2.00	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-28932

Descripción: D-Link DSL-G2452DG HW:T1\\tFW:ME_2.00 was discovered to contain insecure permissions.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-0781	05/23/2022	El plugin Nirweb de WordPress no sanitiza	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-0781

Descripción: The Nirweb support WordPress plugin before 2.8.2 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action (available to unauthenticated users), leading to an SQL injection.

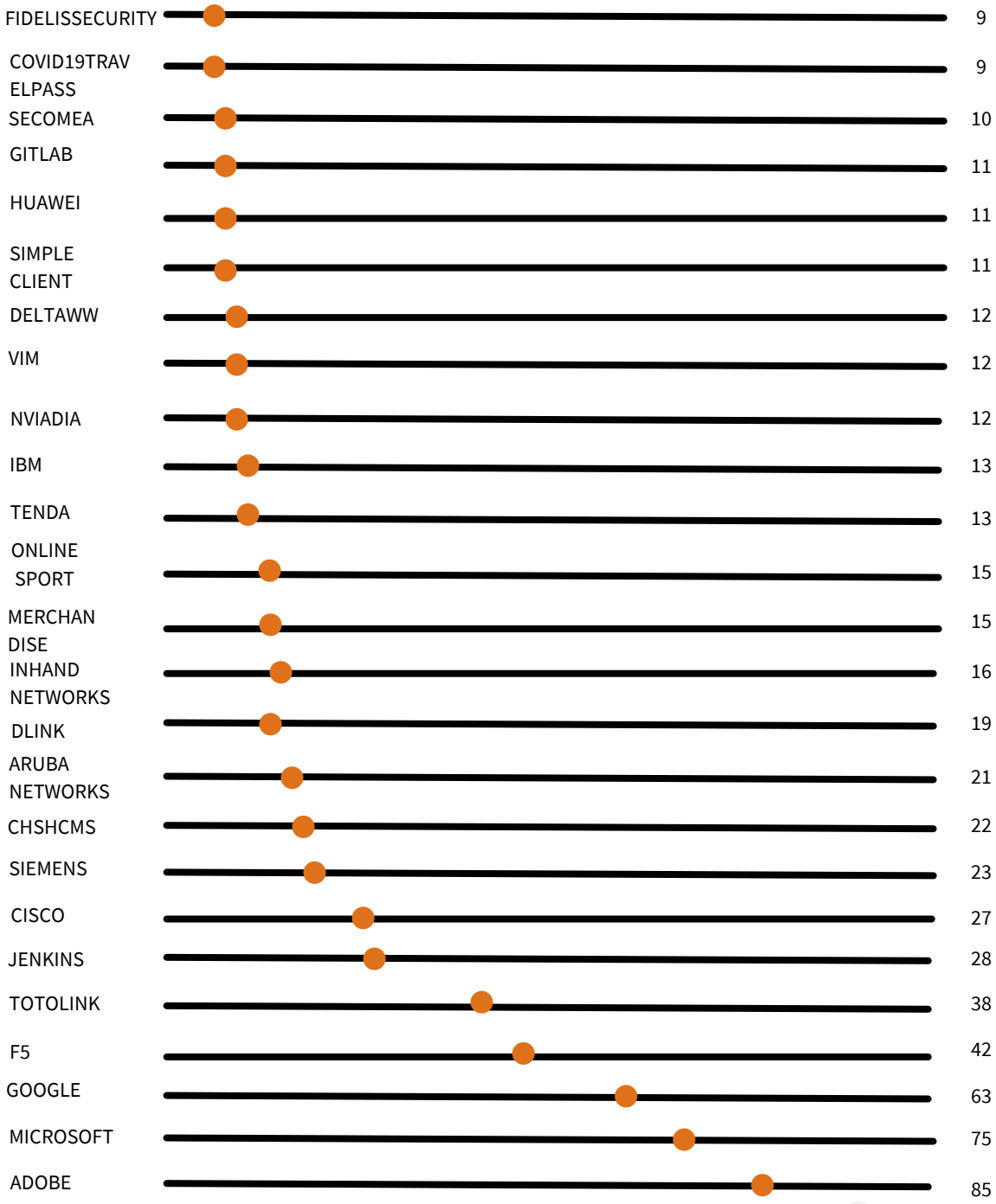
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28995	05/24/2022	Se descubre una posibilidad de ejecución de código	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-28995

Descripción: Rengine v1.0.2 was discovered to contain a remote code execution (RCE) vulnerability via the yaml configuration function.

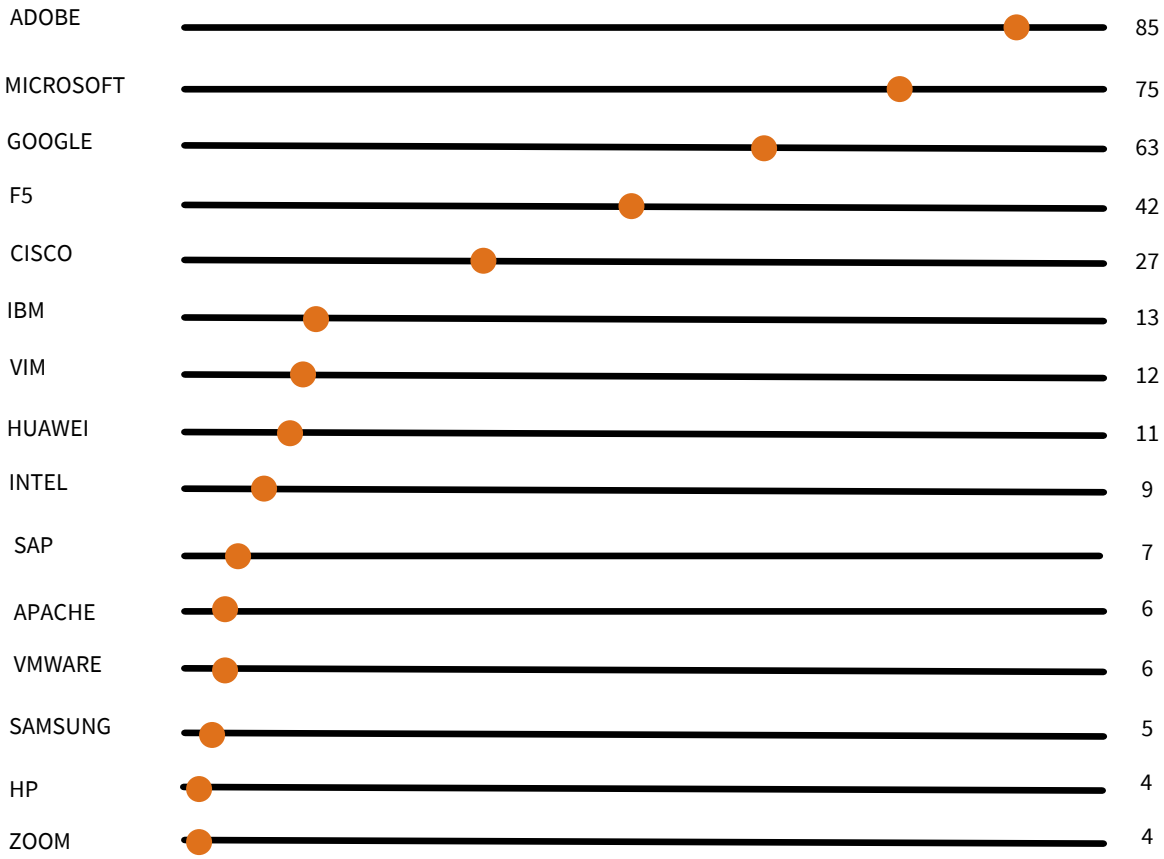
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28104	05/20/2022	el Editor PDF descubrió que contiene una vulnerabilidad	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-28104

Descripción: Foxit PDF Editor v11.3.1 was discovered to contain an arbitrary file upload vulnerability.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: MAYO DE 2022



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: MAYO DE 2022



CULTURA DE CIBERSEGURIDAD

BACKDOOR

¿QUÉ ES BACKDOOR?

Los Backdoors (troyanos de puerta trasera) están diseñados para dar a los usuarios maliciosos el control de un equipo infectado. En términos de funcionalidad, las “puertas traseras” son similares a muchos sistemas de administración diseñados y distribuidos por desarrolladores de programas legítimos.

Este tipo de programas maliciosos permiten que el operador del troyano haga lo que quiera en el equipo infectado: enviar y recibir archivos, ejecutar archivos o eliminarlos, mostrar mensajes, borrar datos, reiniciar la computadora, etc.

Como su nombre indica, es una puerta trasera de acceso a los equipos o servidores, de manera que los usuarios (ciberdelincuentes) que las utilizan, podrán enviar y recibir archivos, borrar o robar datos, reiniciar el ordenador, instalar nuevos programas.

O sea, pueden tener el control total de tu ordenador, como si lo tuvieran delante, pero a distancia.
Las vías por las que podemos tener un backdoor instalado son muchas. Puede ser porque un desarrollador lo haya dejado ahí a cosa hecha, o bien por programas o aplicaciones que hemos instalado, o porque existe una vulnerabilidad en el sistema.

No obstante, es cierto que los backdoor pueden no ser necesariamente virus, sino aplicaciones que se han instalado para controlar un equipo a distancia para tareas de mantenimiento. En este sentido, los backdoor no siempre se instalan aprovechando una vulnerabilidad del equipo, sino que se han desarrollado de esa forma a propósito.

TIPOS DE BACKDOOR

Podemos distinguir al menos dos tipos de backdoor. Aquellos que ya se encuentran en los sistemas operativos o aplicaciones que estamos utilizando, bien por una vulnerabilidad o porque el desarrollador lo ha hecho así a propósito.

Los backdoor que se han instalado en nuestro ordenador sin intención, como consecuencia de haber descargado un programa, archivo, etc.

En la mayoría de los casos, suele haber siempre

malas intenciones, pero puede ser también que haya una vulnerabilidad en nuestro equipo o aplicación y por tanto exista una puerta trasera que pueda ser aprovechada por los ciberdelincuentes.

¿CÓMO PROTEGERTE DE LOS BACKDOOR?

Para protegerte de los backdoor del segundo tipo, es esencial disponer de un antivirus. Si tenemos aplicaciones de malware que permiten el acceso a nuestro equipo en remoto, un buen antivirus debe poder detectar esas aplicaciones y eliminarlas de nuestro ordenador.

En el momento en el que se elimine la aplicación, la puerta trasera desaparecerá y ya no podrán conectarse a nuestro ordenador por esa vía. En cualquier caso, el antivirus también debe permitir eliminar otras posibles aplicaciones no deseadas que se nos hayan instalado por esa vía.

Para evitar la pérdida o borrado de datos, lo ideal sería que tuvieras copias de seguridad, de manera que una vez desinstalado el malware, podemos recuperar nuestros datos, incluso si los que están en nuestro ordenador han resultado afectados.

En el caso de los backdoor que existen ya en nuestras aplicaciones o sistemas, la solución puede pasar por ponerse en contacto con el desarrollador e informarle de que existe una puerta trasera y confiar en su buena voluntad para eliminarla.

De lo contrario, lo conveniente es cambiar a otro sistema, o cambiar a otra aplicación que no tenga puertas secretas que permitan el acceso externo.

PROTEGE TUS EQUIPOS DE ATAQUES INFORMÁTICOS

Muchos clientes pueden tener un backdoor sin ser conscientes de ello. Pueden haber integrado nuestro equipo informático en una botnet, o red de ordenadores zombie, y utilizarlos cuando les venga en gana.

La mejor forma de combatir esto es realizar un mantenimiento informático eficaz de los ordenadores, eliminando los virus y comprobando los niveles de seguridad. Además, es conveniente que para evitar la pérdida de datos, utilicemos sistemas de copias de seguridad en la nube que nos permitan mantener nuestra información siempre a salvo.

ATT&CK puede ser útil para la inteligencia contra amenazas informáticas, ya que permite describir comportamientos adversarios de manera estándar. Se puede hacer un seguimiento de los actores con asociaciones respecto a las técnicas y tácticas en **ATT&CK**, que se sabe que utilizan. Tanto a nivel ofensivo, como defensivo, las matrices proporcionan gran información. A nivel ofensivo podrían utilizarse para acciones como:

- Tareas de pentesting.
- Equipos de Red team.
- Detección de comportamientos anómalos y búsqueda de amenazas (Threat Intelligence).
- Construcción de medidas a nivel defensivo.
- Mejora de equipos defensivos.

CONCLUSIÓN

El conocimiento sobre tácticas y técnicas de ataque en el sector industrial aporta un gran valor para la comunidad de expertos en material de ciberseguridad, tanto a nivel ofensivo como defensivo. Por ello, es importante que se siga trabajando en diferentes líneas a futuro para:

- Afinar más la descripción de las técnicas. Sectorizar, aún más si cabe, las tácticas y técnicas ya que, dependiendo del sector, en muchas ocasiones, tanto atacantes, como defensores se encuentran con protocolos y dispositivos diferentes.

- Aportar más medidas defensivas para la detección de algunas técnicas o para evitar la explotación de estas.

MITRE ATT&CK es una base de conocimiento accesible a nivel mundial basada en observaciones del mundo real. La base de conocimientos de **ATT&CK** se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

Con la creación de **ATT&CK, MITRE** está cumpliendo su misión de resolver problemas para un mundo más seguro, uniendo a las comunidades para desarrollar una ciberseguridad más efectiva. **ATT&CK** está abierto y disponible para cualquier persona u organización para su uso sin cargo.

REFERENCIAS

REFERENCIAS

- https://blog.elhacker.net/2022/04/el-fbi-hace-oficial-el-cierre-de-RaidForums-y-detieneadministrador-omnipotent-portugues-21-edad.html
- https://hackwise.mx/esta-grave-vulnerabilidad-de-java-permite-falsificar-certificados-y-firmas-tls/
- https://es.postsus.com/technology/208334.html
- https://www.microsoft.com/security/blog/2022/04/26/microsoft-findsnew-elevation-of-privilege-linux-vulnerability-nimbuspwn/
- https://expansion.mx/tecnologia/2022/01/18/qrishing-codigos-qrrobar-dinero-datos
- https://noticiasseguridad.com/vulnerabilidades/cve-2022-0778-vulnerabilidadopenssl-afecta-a-varios-productos-de-palo-alto-networks/
- https://www.elclarinete.com.mx/saqueo-dedatos-en-el-sat/
- https://www.anomali.com/es/resources/what-mitre-attck-is-and-how-itis-useful#:~:text=ATT%26CK%20puede%20ser%20%C3%BAtil%20para,que%2 0se%20sabe%20que%20utilizan.
- https://www.incibe-cert.es/blog/matriz-mitre-tacticas-y-tecnicasentornos-industriales https://attack.mitre.org/#

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