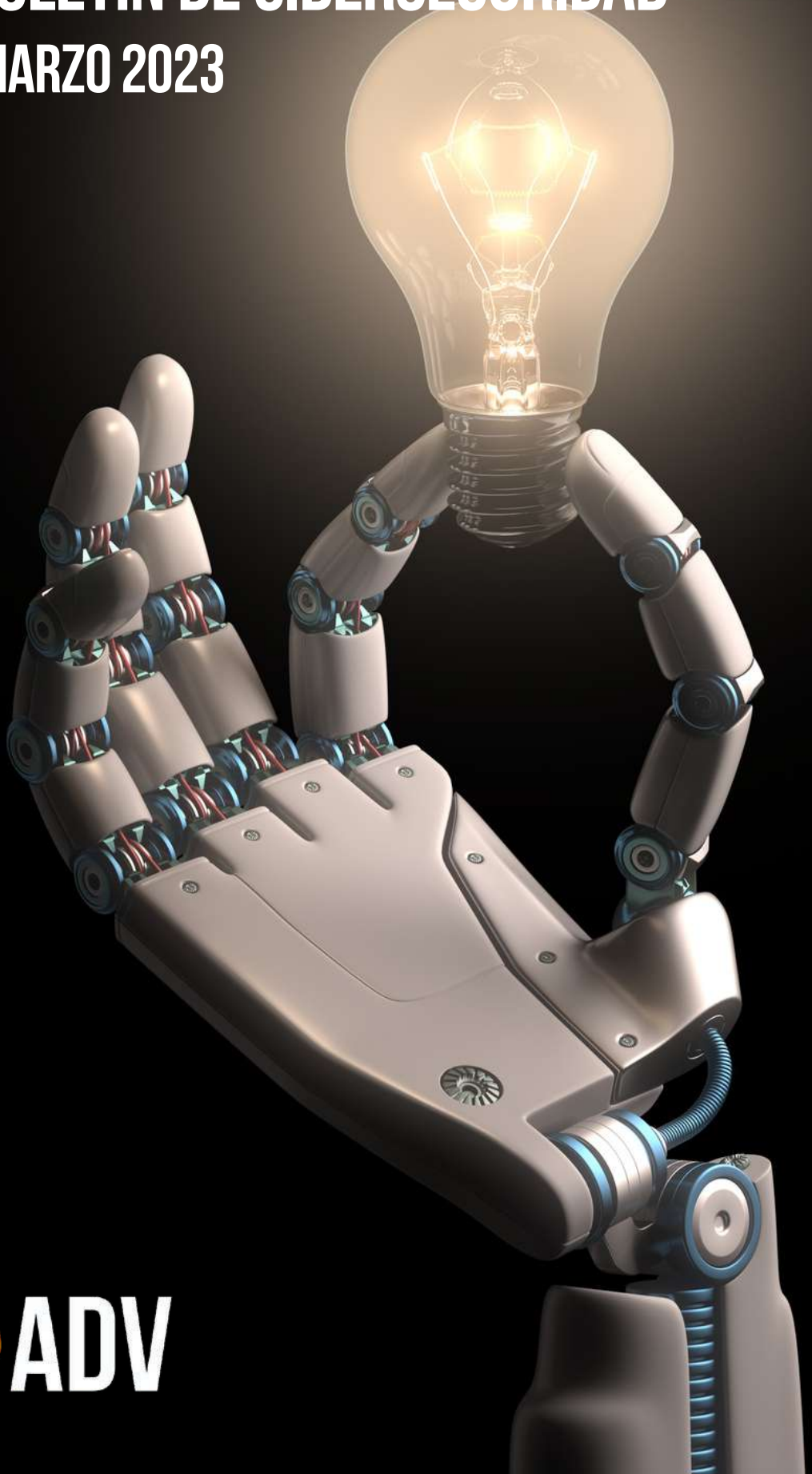
BOLETÍN DE CIBERSEGURIDAD

MARZO 2023



ADV

ÍNDICE

NOTICIAS INTERNACIONALES

EL FBI Y LA CISA LANZAN UN AVISO PARA COMBATIR ROYAL RANSOMWARE

28/03/2023

EL PASADO 2 DE MARZO, EL FBI Y LA CISA LANZARON EL AVISO DE SEGURIDAD CIBERNÉTICA #STOPRANSOMWARE: ROYAL RANSOMWARE

Patchstack. (s. f.). Page not found. https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privileRoyal+Ransomwarege-escalation-vulnerability-exploited-in-the-wild/

Desde septiembre de 2022, muchas empresas de distintos sectores de infraestructura crítica como industria, telecomunicaciones, salud, educación, entre otros, han sido vulneradas con esta variante de ransomware.

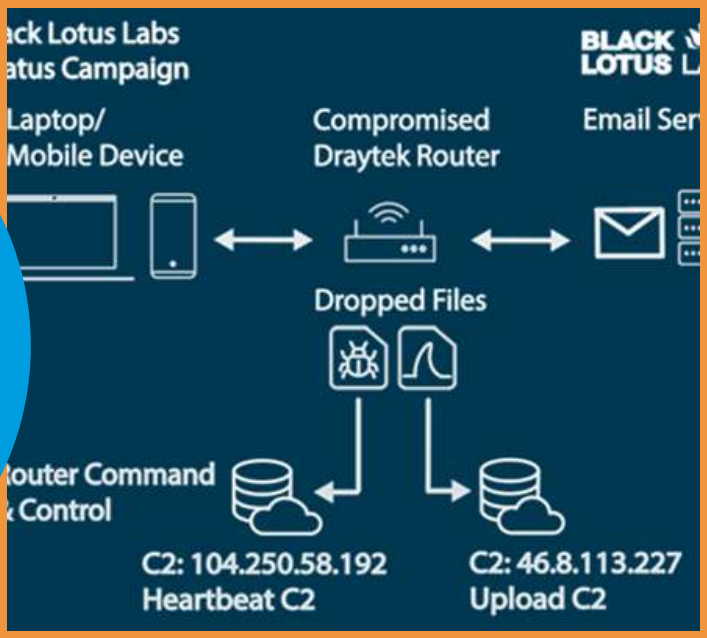
El FBI y la CISA creen que Royal utiliza su propio programa de cifrado de archivos, además, desactivan el antivirus al conseguir acceder a un sistema y filtran los datos antes de implementar finalmente el ransomware.

Posteriormente, solicitan rescates de entre uno y once millones de dólares en Bitcoin y en la nota que dejan a las víctimas indicado un sitio .onion para establecer contacto.
Se recomienda a las organizaciones implantar las recomendaciones y mitigaciones del aviso para evitar estos ataques.

HIATUS: CAMPAÑA MUNDIAL CONTRA ROUTERS EMPRESARIALES

6/03/2023

SOLO NUEVE MESES DESPUÉS DE DESCUBRIR ZUORAT, UN NUEVO MALWARE DIRIGIDO A ENRUTADORES DE OFICINAS PEQUEÑAS Y DOMÉSTICAS (SOHO)



Black Lotus Labs. (2023, 6 marzo). New HiatusRAT router malware covertly spies on victims. Lumen. https://blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/

Lumen Black Lotus Labs ® identificó otra campaña nunca antes vista que involucraba enrutadores comprometidos. Esta es una campaña compleja que llamamos "Pausa". Infecta enrutadores de nivel empresarial e implementa dos binarios maliciosos, incluido un troyano de acceso remoto (RAT) que llamamos HiatusRAT, y una variante de tcpdump que permite la captura de paquetes en el dispositivo de destino.

Una vez que un sistema objetivo está infectado, HiatusRAT permite que el actor de amenazas interactúe de forma remota con el sistema, y utiliza funcionalidades preconstruidas, algunas de las cuales son muy inusuales, para convertir la máquina comprometida en un proxy encubierto para el actor de amenazas. El binario de captura de paquetes permite al actor monitorear el tráfico del enrutador en los puertos asociados con las comunicaciones de transferencia de archivos y correo electrónico.

Usando telemetría patentada de la red troncal de IP global de Lumen, enumeramos la infraestructura de comando y control (C2) asociada con la actividad y hemos identificado al menos 100 víctimas infectadas, predominantemente en Europa y América Latina. La última versión del malware, la versión 1.5, se activó en julio de 2022.

POC DE MALWARE POLIMÓRFICO EMPLEANDO INTELIGENCIA ARTIFICIAL

18/03/2023

PARA DEMOSTRAR DE LO QUE ES CAPAZ EL MALWARE BASADO EN IA, HEMOS CREADO UNA PRUEBA DE CONCEPTO (POC) SIMPLE QUE EXPLOTA UN MODELO DE LENGUAJE GRANDE PARA SINTETIZAR LA FUNCIONALIDAD DEL REGISTRADOR DE TECLAS POLIMÓRFICO SOBRE LA MARCHA

BlackMamba: Using AI to Generate Polymorphic Malware. (s. f.). https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware

Infraestructura de control y entrega para entregar o verificar la funcionalidad del registrador de teclas malicioso. Dada la amenaza que representa este tipo de malware, llamamos a nuestro PoC BlackMamba en referencia a la serpiente mortal.

Para crear esta prueba de concepto, los investigadores de HYAS unieron dos conceptos aparentemente dispares. El primero fue eliminar el canal de comando y control (C2) mediante el uso de malware que podría estar equipado con automatización inteligente y podría hacer retroceder cualquier dato vinculado al atacante a través de algún canal de comunicación benigno. El segundo fue aprovechar las técnicas generativas de código de IA que podrían sintetizar nuevas variantes de malware, cambiando el código para que pueda evadir los algoritmos de detección.

BlackMamba utiliza un ejecutable benigno que llega a una API de alta reputación (OpenAI) en tiempo de ejecución, por lo que puede devolver el código malicioso sintetizado necesario para robar las pulsaciones de teclas de un usuario infectado. Luego ejecuta el código generado dinámicamente dentro del contexto del programa benigno usando la función exec() de Python, con la porción polimórfica maliciosa permaneciendo totalmente en la memoria. Cada vez que BlackMamba se ejecuta, vuelve a sintetizar su capacidad de registro de teclas, lo que hace que el componente malicioso de este malware sea realmente polimórfico. BlackMamba se probó contra un EDR líder en la industria que permanecerá sin nombre, muchas veces, lo que resultó en cero alertas o detecciones.

NUEVA VERSIÓN DEL TROYANO BANCARIO XENOMORPH

13/03/2023

VARIOS SITIOS WEB DE LA OTAN HAN SUFRIDO UN ATAQUE INFORMÁTICO EN LA NOCHE DE ESTE DOMINGO, DEJANDO TEMPORALMENTE INOPERATIVAS LA WEB DEL CUARTEL GENERAL DE OPERACIONES ESPECIALES DE LA OTAN

Xenomorph v3: a new variant with ATS targeting more than 400 institutions — ThreatFabric. (s. f.). https://www.threatfabric.com/blogs/xenomorph-v3-new-variant-with-ats.html

"Los expertos cibernéticos de la OTAN están tratando activamente un incidente que afecta a algunos sitios web de la Alianza. La OTAN se ocupa de los incidentes cibernéticos de forma regular, y se toma muy en serio la seguridad cibernética", ha afirmado un funcionario de la Alianza Atlántica a la agencia DPA.

El comentario ha tenido lugar después de que los informes publicados en redes sociales sugirieran que piratas informáticos pro-rusos habían atacado el sitio web del Cuartel General de Operaciones Especiales de la OTAN (NSHQ) y otros, haciéndolo temporalmente inaccesible.

Entre los posibles atacantes, según detallan los informes mencionados anteriormente, podría encontrarse el grupo de piratas informáticos ruso Killnet, asociado con otros ataques recientes, incluso en Alemania, dirigidos contra los sitios web del Bundestag, la Policía e instalaciones de infraestructuras críticas, según la citada agencia.

YOROTROOPER: NUEVO ACTOR AMENAZA ENFOCADO AL CIBERESPIONAJE

16/03/2023

CISCO TALOS HA IDENTIFICADO UN NUEVO ACTOR DE AMENAZAS, AL QUE LLAMAMOS "YOROTROOPER", QUE HA ESTADO EJECUTANDO VARIAS CAMPAÑAS DE ESPIONAJE EXITOSAS DESDE AL MENOS JUNIO DE 2022.

Malhotra, A. (2023, 16 marzo). Talos uncovers espionage campaigns targeting CIS countries, embassies and EU health care agency. Cisco Talos Blog. https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/

Los objetivos principales de YoroTrooper son organizaciones gubernamentales o energéticas en Azerbaiyán, Tayikistán, Kirguistán y otros Estados Independientes (CEI), según nuestro análisis. También observamos cuentas comprometidas de YoroTrooper de al menos dos organizaciones internacionales: una agencia crítica de atención médica de la Unión Europea (UE) y la Organización Mundial de la Propiedad Intelectual (OMPI). Los compromisos exitosos también incluyeron embajadas de países europeos, incluidos Azerbaiyán y Turkmenistán. Evaluamos que el actor probablemente también apunte a otras organizaciones en toda Europa y agencias gubernamentales turcas (Türkiye).

La información robada de compromisos exitosos incluye credenciales de múltiples aplicaciones, historiales y cookies del navegador, información del sistema y capturas de pantalla.
Las principales herramientas de YoroTrooper incluyen ladrones de información de código abierto, personalizados y basados en Python, como el ladrón Stink envuelto en ejecutables a través del marco Nuitka y PyInstaller . Para el acceso remoto, YoroTrooper también ha implementado malware básico, como AveMaria/Warzone RAT, LodaRAT y Meterpreter.

La cadena de infección consta de archivos de acceso directo maliciosos (LNK) y documentos señuelo opcionales envueltos en archivos maliciosos entregados a los objetivos. El actor parece tener la intención de exfiltrar documentos y otra información, probablemente para usar en operaciones futuras.

HINATABOT: NUEVA BOTNET DEDICADA A ATAQUES DE DDOS

29/02/2023

SE HAN DESCUBIERTO UNA SERIE DE VULNERABILIDADES EN LOS ROUTERS NETCOMM YLOS INVESTIGADORES DE AKAMAI DEL EQUIPO DE RESPUESTA DE INTELIGENCIA DE SEGURIDAD (SIRT) HAN DESCUBIERTO UNA NUEVA BOTNET CENTRADA EN DDOS Y BASADA EN GO.

Access Denied. (s. f.). https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet

El malware parece haber sido llamado "Hinata" por el autor del malware en honor a un personaje de la popular serie de anime Naruto. Lo llamamos "HinataBot".

Se vio que HinataBot se distribuyó durante los primeros tres meses de 2023 y los autores/operadores lo están actualizando activamente.

La muestra se descubrió en los honeypots HTTP y SSH que abusaban de vulnerabilidades antiguas y credenciales débiles.

Los intentos de infección observados incluyen la explotación del servicio miniigd SOAP en dispositivos Realtek SDK (CVE-2014-8361), enrutadores Huawei HG532 (CVE-2017-17215) y servidores Hadoop YARN expuestos (CVE N/A).

A través de una combinación de ingeniería inversa del malware e imitación del servidor de comando y control (C2), pudimos obtener una visión profunda de cómo funciona el malware y qué tiene de único el tráfico de ataque resultante.

LA CISA EMITE OCHO AVISOS DE SEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL

22/03/2023

RECIENTEMENTE, CISA HA PUBLICADO HASTA UN TOTAL DE OCHO AVISOS DE SEGURIDAD ALERTANDO SOBRE VULNERABILIDADES CRÍTICAS EN SISTEMAS DE CONTROL INDUSTRIAL

Ivanova, D. (2023, 22 Marzo). Malicious (and fake) ChatGPT client for Windows. https://www.kaspersky.com/blog/chatgpt-stealer-win-client/47274/

En relación a estas nuevas vulnerabilidades, cabe destacar que afectan a varios productos de diferentes compañías como Siemens, Rockwell Automation, Delta Electronics, VISAM, Hitachi Energy y Keysight Technologies.

De entre todas ellas, destacan por su volumen las que afectan a la marca Siemens, de la cual se han recogido tres avisos que afectan a sus activos SCALANCE W-700, dispositivos RADIUS client of SIPROTEC 5 y la familia de productos RUGGEDCOM APE1808 con hasta un total de 25 vulnerabilidades cuyo CVSSv3 oscila entre 4.1 y 8.2 de puntuación.

Consecuentemente, debido a su impacto, destacan los avisos del equipamiento ThinManager ThinServer de Rockwell Automation, cuya criticidad de uno de sus tres fallos alcanza un CVSSv3 de 9.8, al igual que el activo InfraSuite Device Master de Delta Electronics, de la cual se han recogido hasta un total de 13 vulnerabilidades.

NOTICIAS NACIONALES

COMISIÓN DE SEGURIDAD DE LA INFORMACIÓN EN MÉXICO, AÚN SIN LEY DE CIBERSEGURIDAD

20/03/2023

PUEDE QUE LO HAYAMOS OLVIDADO, PERO, DURANTE LA PANDEMIA AMÉRICA LATINA TUVO EL DUDOSO PRIVILEGIO DE SER UNA DE LAS REGIONES CON MÁS ATAQUES CIBERNÉTICOS DEL MUNDO

Morales, L. E. (2023, 2 Marzo). Hackean al Buró de Crédito: descubren venta de la información de los clientes en redes sociales. El Heraldo de México. https://heraldodemexico.com.mx/nacional/2023/2/2/hackean-al-buro-de-credito-descubren-venta-de-la-informacion-de-los-clientes-en-redes-sociales-478457.html

Esto no ha mejorado: los países más poblados de la región siguen teniendo indicadores alarmantes de ataques en todos los tamaños de industrias, así como en todos los sectores incluyendo el público. Esto, por supuesto, ha venido generando el incremento en los presupuestos para protección, resguardo y recuperación de datos.

Ello se encuentra reflejado en el más reciente informe de Palo Alto Networks denominado What's Siguiente in Cyber, el cual revela – entre otras cosas – los hábitos y tendencias de ciberseguridad de las empresas en la regin, especialmente en México. Destacan entre sus conclusiones más significativas el que:

- La mitad de las empresas tendrán un aumento del 6 al 10% en el presupuesto para la inversión en ciberseguridad
- Mientras que un 28% aumentará de 11 a 20%
- Dejando al 14% en un aumento de 1 a 5%
- En contraste, un 8% no verá incremento.
- Cabe destacar que, entre las amenazas percibidas, las preocupaciones principales de las empresas son:
- Protegerse del Ransomware, con un 26%
- Seguido de la amenaza del correo electrónico empresarial comprometido con el 16%
- Proteger la virtualización

COMISIÓN DE SEGURIDAD DE LA INFORMACIÓN EN MÉXICO, AÚN SIN LEY DE CIBERSEGURIDAD

20/03/2023

Gracias a las respuestas de las empresas encuestadas en este informe, Palo Alto Networks dio a conocer los problemas más críticos a los que se enfrentan las organizaciones hoy en día y cómo los líderes pretenden impulsar la digitalización a medida que se preparan para las amenazas del mañana.

Entre los tres principales problemas comerciales que consideran las organizaciones son:

- La protección de datos y ciberseguridad con 42%
- Implementación de plataformas Zero Trust con 36%
- Y monitoreo, detección y respuesta ante posibles amenazas, con 34%

También resultó evidente que las iniciativas de tecnología digital son la prioridad para el 54% de las empresas, mientras que innovación, eficiencia y productividad representan el 32% para las empresas.
Los retos de transformación digital son, claramente, los que impulsa el crecimiento delà inversión en ciberseguridad.

Uno de ellos es desarrollar y mejorar la mano de obra híbrida lo cual precisa establecer una serie de requisitos previos como formar a los trabajadores sobre los protocolos y procedimientos de seguridad de los datos:

- Así lo considera – al menos – un 54% de las empresas mexicanas encuestadas.
- A lo cual se suma la protección de datos confidenciales en entornos multicloud (44%)
- Y la modernización de la infraestructura de acceso con despliegue de servicios de seguridad en el extremo de la nube (SSE) para consolidar la funcionalidad (70%)
- 4 de cada 10 empresas mexicanas reconocen que invierten entre un 25% y un 49% del presupuesto asignado a la ciberseguridad en ello.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: MARZO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-25909	03/27/2023	Unrestricted Upload of File with Dangerous Type	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-25909

Descripción: HGiga OAKlouds file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to upload and run arbitrary executable files to perform arbitrary command or disrupt service.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-21058	03/27/2023	Out-of-bounds Write	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-21058

Descripción: In lcsm_SendRrAcquiAssist of lcsm_bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-246169606References: N/A

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-42498	03/24/2023	Out-of-bounds Write)	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-42498

Descripción: In Pixel cellular firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-240662453References: N/A

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-20532	03/24/2023	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-20532

Descripción: In parseTrackFragmentRun() of MPEG4Extractor.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-232242894

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-28152	03/24/2023	Improper Restriction of XML External Entity Reference	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-28152

TABLA DE VULNERABILIDADES RELEVANTES: MARZO 2023

Descripción: An issue was discovered in Independentsoft JWord before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-20532	03/24/2023	Integer Overflow or Wraparound	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-20532

Descripción: In parseTrackFragmentRun() of MPEG4Extractor.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-232242894

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-28152	03/24/2023	Improper Restriction of XML External Entity Reference	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-28152

Descripción: An issue was discovered in Independentsoft JWord before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-1177	03/24/2023	Path Traversal: '\..\filename'	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-1177

Descripción: Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.2.1.

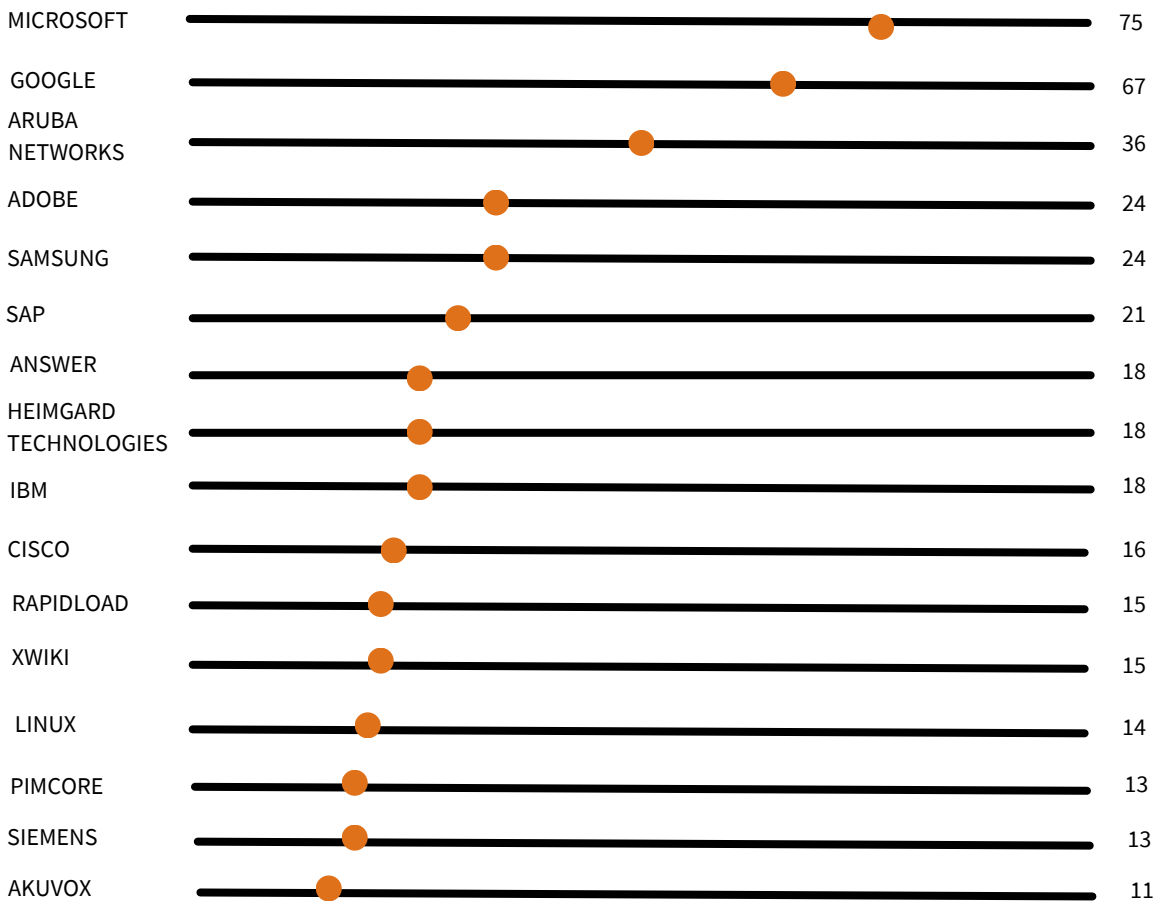
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28495	03/24/2023	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-28495

Descripción: TOTOLink outdoor CPE CP900 V6.3c.566_B20171026 is discovered to contain a command injection vulnerability in the setWebWlanIdx function via the webWlanIdx parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request..

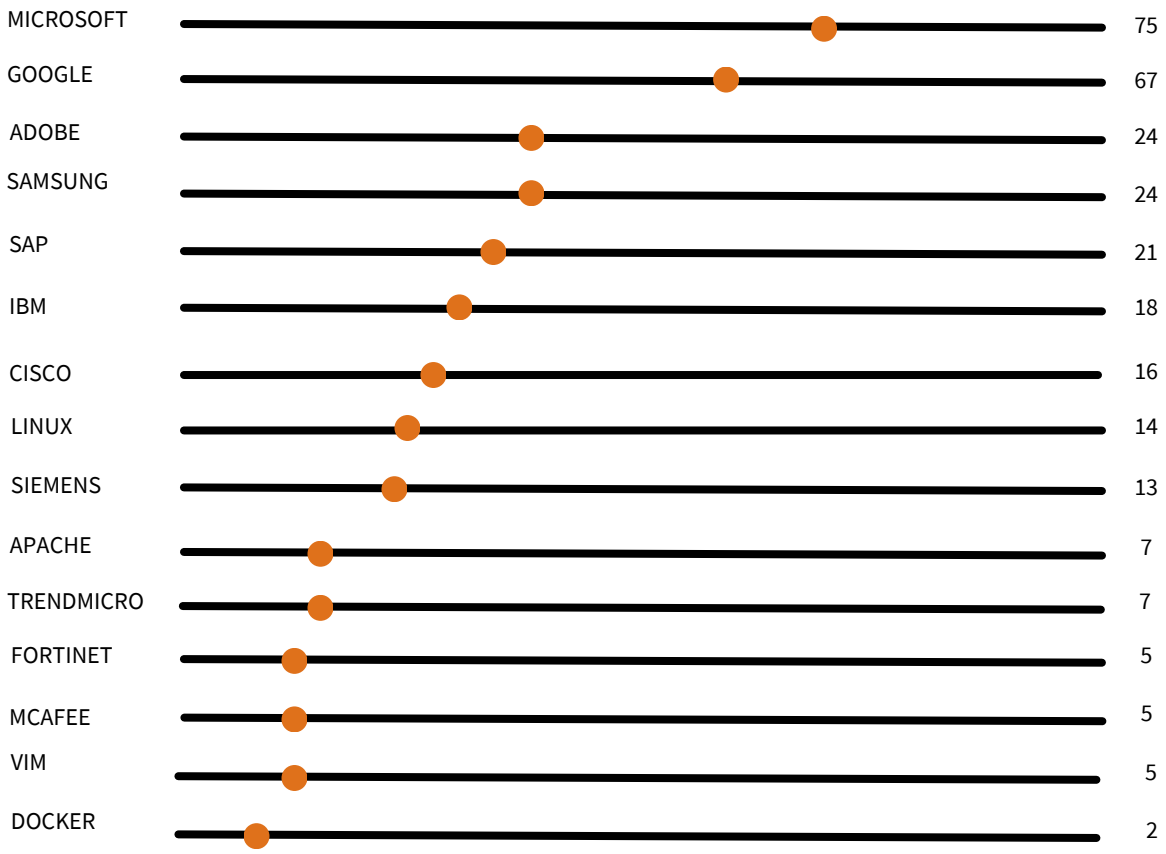
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-26360	03/23/2023	Improper Access Control	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-20532

Descripción: Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: MARZO DE 2023



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: MARZO DE 2023



CULTURA DE CIBERSEGURIDAD

REDES SOCIALES EN LA EMPRESA

La seguridad de las redes sociales son los ataques de phishing. Se trata de una de las técnicas más empleadas por ciberdelincuentes de todo el mundo para robar las credenciales. También es imprescindible prevenir los delitos de suplantación de identidad que tanto preocupan a empresas y usuarios.

El 67,5% de los empleados de empresa son víctimas de correos electrónicos de phishing y pierden información valiosa. Se calcula que los ciberdelincuentes extorsionarán más de 33 millones de registros solo en 2023.5 mar 2023

IDENTIFICANDO LOS CONCEPTOS CLAVE EN REDES SOCIALES

Gracias a las redes sociales muchas empresas pueden tener una mayor difusión de sus servicios y un mejor contacto con sus posibles clientes y la operación de TI, pero también se deben tener en cuenta y valorar los posibles riesgos derivados de su utilización.

Tener claros los conceptos fundamentales de este ámbito como son identidad digital o reputación online se considera imprescindible desde el punto de vista de la ciberseguridad.

ESTABLECER UNA POLÍTICA DE BUENAS PRÁCTICAS EN REDES SOCIALES

Definir una política de buenas prácticas en redes sociales es fundamental para garantizar su uso de manera responsable y segura dentro de la organización, ya que proporciona las claves fundamentales para garantizar la seguridad de los perfiles utilizados, evitando posibles incidentes ocasionados por la ausencia de medidas de seguridad.

Otro de los objetivos que se consigue al establecer esta política de seguridad en la empresa, consiste en que permite conocer las principales amenazas, malas configuraciones o fallos en su uso, que pueden afectar a la actividad, imagen y reputación del negocio.

REDES SOCIALES EN LA EMPRESA

RIESGOS DEL USO DE REDES SOCIALES

La utilización de redes sociales no está exenta de riesgos, entre los que destacan:

- Acceso no autorizado a los perfiles y cuentas. Es uno de sus mayores riesgos, ya que puede permitir a un ciberatacante acceder a información confidencial del perfil, como las conversaciones entre proveedores y clientes; o realizar un defacement en el perfil mediante publicaciones no autorizadas o modificando sus datos con la finalidad de hacer un daño reputacional a la empresa.
- Suplantación de perfiles. Es frecuente que, al utilizar un perfil de manera activa, los ciberdelincuentes generen perfiles intentando suplantar su identidad para robar los datos de los usuarios. Es muy frecuente cuando en el perfil se realizan acciones comerciales como pueden ser la venta de productos o sorteos.
- Mala gestión de la identidad online. El hecho de no disponer de los conocimientos necesarios en gestión de redes sociales puede ocasionar graves daños reputacionales a la imagen de la empresa.
- Fugas de información. Muchas veces en las redes sociales se mantienen comunicaciones privadas con proveedores, clientes o colaboradores. Esta información podría ser muy jugosa para los ciberdelincuentes.

Un estudio de TrendMicro4 sugiere que los grupos cibercriminales preparan esquemas de engaño (campañas de phishing) sobre acontecimientos mediáticos entre las dos (2) semanas anteriores y las tres (3) horas posteriores al mismo. Además, cabe destacar que hasta un 13 % de usuarios ha sido víctima de robo de identidad a través de redes sociales; que un 69 % de adultos y un 88 % de adolescentes son expuestos de alguna forma a acoso o crueldad en redes sociales; o que casi cinco (5) millones de personas anuncian habitualmente sus planes de viaje en redes sociales. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3009-ccn-cert-bp-08-redes-sociales/file.html

PRINCIPALES VECTORES DE ATAQUE

Ataques de ingeniería social. Es el principal vector de ataque que suelen utilizar los ciberdelincuentes para poder acceder a los perfiles de redes sociales. Con frecuencia se realizan ataques basados en las técnicas de phishing o smishing para suplantar a algún perfil de la organización o simular los mensajes de la propia plataforma para solicitar las credenciales de acceso

Contraseñas inseguras. El uso de contraseñas poco robustas, que no se cambian con regularidad, o que se compartan con otros servicios, puede suponer un punto de entrada para que los ciberdelincuentes accedan a los perfiles de redes sociales, o incluso a otros servicios de la empresa.

Empleados descontentos (insiders). Este tipo de actor puede realizar acciones malintencionadas sobre las redes sociales de la empresa, suponiendo un problema, tanto para la reputación, como para la información confidencial de la organización.

MEDIDAS DE SEGURIDAD

Además, existen otras medidas que deben ser consideradas:

- Gestores de contraseñas. Son herramientas que permite almacenar las credenciales de manera segura, permiten generar contraseñas robustas y ayudan a la hora de gestionar recursos compartidos.
- Herramientas multifactor. Es indispensable activar las herramientas multifactor de autenticación, de este modo se asegura que ante un acceso no autorizado, se evita que el ciberatacante pueda acceder al perfil de la red social
- Concienciación. Es un pilar fundamental para detectar cualquier posible ataque y poder evitar sus consecuencias. Conocer las técnicas empleadas por los ciberdelincuentes ayuda a prevenir cualquier posible ataque de ingeniería social.
- Estrategia de redes sociales. Es necesario que todas aquellas personas autorizadas a utilizar los perfiles de redes sociales sepan cómo deben gestionarlos de manera conjunta. Por ello, es vital que la empresa establezca una estrategia común que debe ser clara, concisa y homogénea.
- Verificar los perfiles de redes sociales. Es un pilar fundamental para detectar cualquier posible ataque y poder evitar sus consecuencias. Conocer las técnicas empleadas por los ciberdelincuentes ayuda a prevenir cualquier posible ataque de ingeniería social.

REFERENCIAS

REFERENCIAS

- https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privileRoyal+Ransomwarege-escalation-vulnerability-exploited-in-the-wild/
- https://blog.lumen.com/new-hiatusrat-router-malware-covertly-spies-on-victims/
- https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware
- https://www.threatfabric.com/blogs/xenomorph-v3-new-variant-with-ats.html
- https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/
- https://www.akamai.com/blog/security-research/hinatabot-uncovering-new-golang-ddos-botnet
- https://www.kaspersky.com/blog/chatgpt-stealer-win-client/47274/
- https://heraldodemexico.com.mx/nacional/2023/2/2/hackean-al-buro-de-credito-descubren-venta-de-la-informacion-de-los-clientes-en-redes-sociales-478457.html

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