GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1823

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	3	1	1
MALWARE	2		
BRECHAS DE SEGURIDAD			3
NOTICIAS DE CIBERSEGURIDAD	1		1
SECTOR GOBIERNO	1		

VULNERABILIDADES

VMware corrige fallas críticas en software de virtualización

VMware solucionó una falla crítica (CVE-2023-20869) y tres importantes (CVE-2023-20870, CVE-2023-20871, CVE-2023-20872) en su software de sesión de usuario virtual VMware Workstation y Fusion.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.helpnetsecurity.com/2023/04/26/cve-2023-20869-cve-2023-20870/

- https://www.vmware.com/security/advisories/VMSA-2023-0008.html

---

Configuración insegura común abre los servidores Apache Superset

Un problema de configuración predeterminada inseguro (CVE-2023-27524) hace que la mayoría de los servidores Apache Superset con acceso a Internet sean vulnerables a los atacantes, según descubrieron los investigadores de Horizon3.ai.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.helpnetsecurity.com/2023/04/26/apache-superset-insecure-configuration-cve-2023-27524/

Vulnerabilidades de PaperCut son aprovechadas por Clop

Los afiliados de ransomware Clop y LockBit están detrás de los ataques recientes que explotan las vulnerabilidades en los servidores de aplicaciones PaperCut. Según los investigadores de Microsoft y Trend Micro, ya existe una PoC (prueba de concepto).

Prioridad: 1 Crítico.

Ampliar información:

- https://www.helpnetsecurity.com/2023/04/27/papercut-lockbit-clop/
- https://twitter.com/MsftSecIntel/status/1651346664630755334

- https://www.trendmicro.com/en_us/research/23/d/update-now-papercut-vulnerability-cve-2023-27350-under-active-ex.html?irclickid=005VE3XL5xyNTE7XN8SVdx8FUkAVOTTe-R--Vc0&irgwc=1
- https://blog.segu-info.com.ar/2023/04/confirman-el-uso-de-servidores-papercut.html
- https://thehackernews.com/2023/04/microsoft-confirms-papercut-servers.html

---

Atacantes intentan aprovechar las vulnerabilidades antiguas de DVR

Hace cinco años el investigador de seguridad, Fernández Ezequiel, descubrió una vulnerabilidad (CVE-2018-9995) en muchas marcas de grabadoras de video digital (DVR) y lanzó una herramienta para explotarla. La vulnerabilidad aún se está explotando en la naturaleza, advierte FortiGuard Labs: los sistemas de prevención de intrusiones de la empresa registraron más de 50.000 intentos únicos de explotación en el último mes.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.helpnetsecurity.com/2023/05/03/cve-2018-9995-cve-2016-20016/
- https://github.com/ezelf/CVE-2018-9995_dvr_credentials
- https://www.fortiguard.com/encyclopedia/ips/43737

Vulnerabilidad del servidor WebLogic de Oracle (CVE-2023-21839) agregada al catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA

El ataque tiene como objetivo el servidor Oracle WebLogic vulnerable específicamente en Oracle Fusion Middleware. La vulnerabilidad se rastrea bajo CVE-2023-21839 y explota la

falla que permite el acceso no autorizado a los servidores vulnerables a través de T3 e IIOP (protocolo propietario de Oracle). Las versiones afectadas son: 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0. La vulnerabilidad tiene una puntuación base CVSS de 7,5 y la complejidad del ataque se clasifica como "baja" en el aviso del proveedor.

Prioridad: 3 Importante.

Ampliar información:

- https://fortiguard.fortinet.com/threat-signal-report/5154

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.
- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema

perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

MALWARE

Por $1.000 al mes se puede hackear laptop con sistema operativo macOS con malware

Los investigadores descubrieron recientemente una nueva pieza de malware conocida como Atomic macOS Stealer (AMOS) cuando se ofrecía a la venta en Telegram. El actor de amenazas que lo promociona cobra $ 1.000 cada mes y actualiza continuamente el virus que vende. Atomic macOS Stealer es capaz de robar una gran variedad de información de la computadora de la víctima.

Prioridad: 1 Crítico.

Ampliar información:

- https://noticiasseguridad.com/malware-virus/solo-por-1000-almes-hackea-laptop-macos-con-este-malware-indetectable/
- https://es.beincrypto.com/nuevo-malware-atomic-macos-stealer-apunta-monederos-criptomonedas/

Malware Qbot infecta correos corporativos con archivos PDF maliciosos

Kaspersky ha descubierto recientemente un repunte del malware Qbot en usuarios corporativos que se propaga a través de una campaña de spam. Los atacantes utilizan técnicas avanzadas de ingeniería social, reenviando a hilos de correos archivos PDF

maliciosos. Desde el 4 de abril se han recibido más de 5,000 emails de este tipo en distintos países. La campaña continúa activa, tal y como comprobaron los expertos de Kaspersky, que han elaborado un análisis técnico de esta amenaza.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/05/05/repunte-del-peligroso-malware-qbot-infecta-correos-corporativos-con-archivos-pdf-maliciosos/
- https://infochannel.info/malware-qbot-vuelve-al-ataque/
- https://www.kaspersky.es/blog/qbot-pdf-mailout/28710/

Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíba las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.
- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma CyberAcademy ©.
- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.

- Mantener actualizadas sus soluciones de ciberseguridad.
- Descargar aplicaciones solo de fuentes de confianza, como la tienda oficial de aplicaciones de Google Play Store.
- Revisar las calificaciones y opiniones de otras personas antes de descargar cualquier aplicación, especialmente si es una aplicación bancaria o financiera.
- No responder a llamadas telefónicas de números desconocidos o sospechosos, especialmente si solicitan información personal o financiera.
- No compartir información personal o financiera a través del teléfono o correo electrónico, a menos que esté seguro de la identidad del destinatario.

BRECHAS DE SEGURIDAD

Coca-cola – Femsa vuelve a ser hackeada por cibercriminales

El embotellador más importante de Coca-Cola, Coca-Cola FEMSA México, fue quien dio a conocer el ciberataque que se reportó esta semana. Coca-Cola llevó a cabo una investigación forense y simultáneamente puso en marcha sus mecanismos de protección y respuesta de ciberseguridad para determinar la magnitud de la brecha.

Prioridad: 3 Importante.

Ampliar información:

- https://noticiasseguridad.com/hacking-incidentes/coca-cola-vuelve-a-ser-hackeada-por-cibercriminales/
- https://blog.elhacker.net/2023/04/hackean-coca-cola-femsa-mexico.html
- https://www.forbes.com.mx/hackean-a-coca-cola-femsa-evalua-alcance-del-ataque/

T-Mobile sufre segunda filtración de datos este año

T-Mobile ha revelado una segunda violación de datos que ocurrió en 2023, la cual, presuntamente expuso datos de los clientes y los PIN de las cuentas, lo que dejó a muchos usuarios de T-Mobile vulnerables a posibles fraudes y robos de identidad.

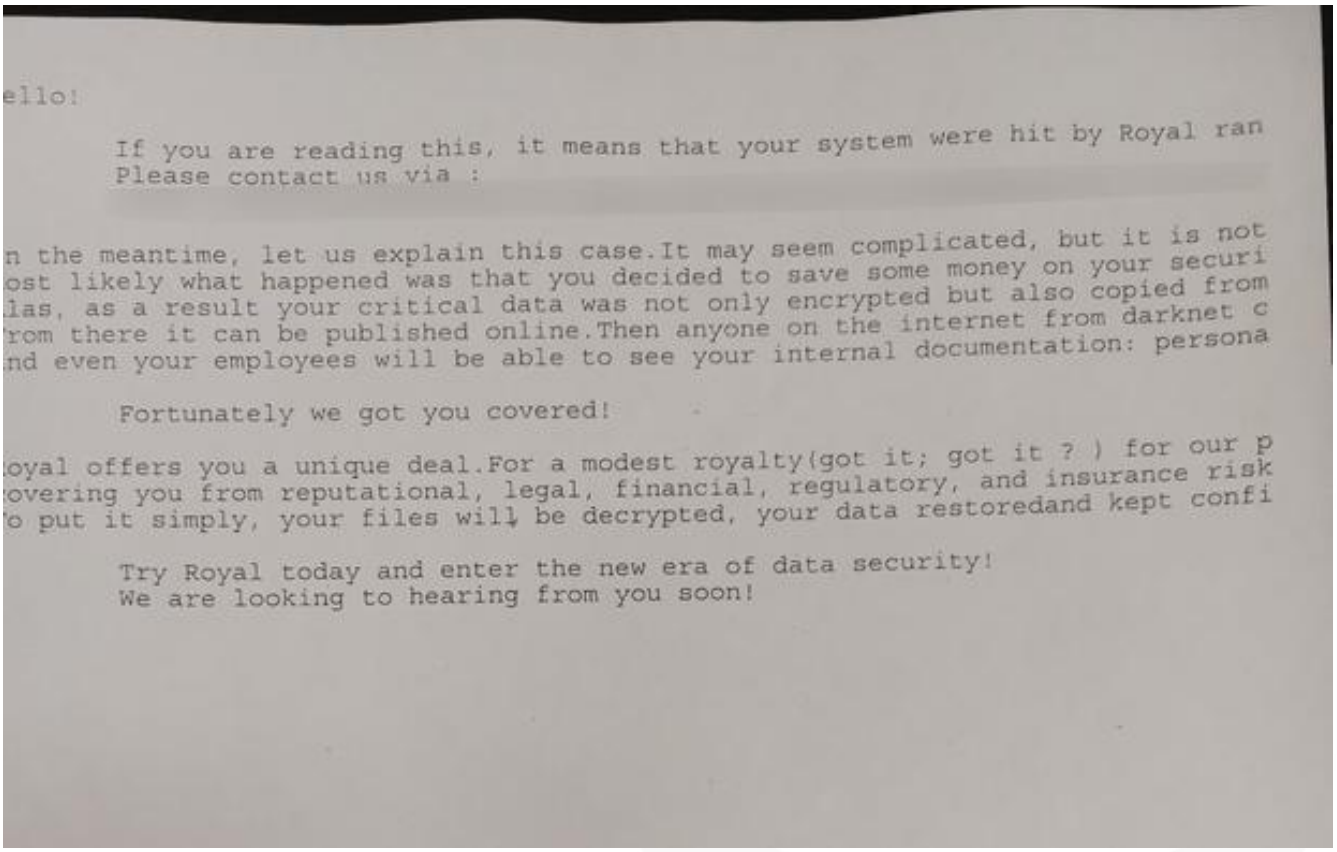
Prioridad: 3 Importante.

Ampliar información:

- https://www.helpnetsecurity.com/2023/05/03/t-mobile-breach-2023/
- https://apps.web.maine.gov/online/aeviewer/ME/40/ea3bf342-eca7-4833-b128-7b09f6893ac4/00363120-37a5-4248-aa8c-0be84d146071/document.html

Ciudad de Dallas atacada por ransomware

La ciudad de Dallas, Texas, sufrió un ataque de ransomware que resultó en la interrupción de varios de sus servicios.


ello!

If you are reading this, it means that your system were hit by Royal ran
Please contact us via :

n the meantime, let us explain this case.It may seem complicated, but it is not
ost likely what happened was that you decided to save some money on your securi
las, as a result your critical data was not only encrypted but also copied from
rom there it can be published online.Then anyone on the internet from darknet c
nd even your employees will be able to see your internal documentation: persona

Fortunately we got you covered!

oyal offers you a unique deal.For a modest royalty(got it; got it ?) for our p
overing you from reputational, legal, financial, regulatory, and insurance risk
o put it simply, your files will be decrypted, your data restoredand kept confi

Try Royal today and enter the new era of data security!
We are looking to hearing from you soon!

Imagen de archivo. Nota de Rescate.

Prioridad: 3 Importante.

Ampliar información:

- https://www.helpnetsecurity.com/2023/05/04/dallas-ransomware/
- https://www.dallascitynews.net/city-of-dallas-statement-on-network-outage
- https://www.cbsnews.com/texas/news/possible-cyber-attack-hampering-dallas-police-operations/

NOTICIAS DE CIBERSEGURIDAD

Robo de cookies, el método favorito para eludir 2FA

A medida que las organizaciones se trasladan a los servicios en la nube y la autenticación multifactor, las cookies vinculadas a la identidad y la autenticación brindan a los atacantes una nueva vía para comprometer.
En algunos casos, el robo de cookies en sí mismo es un ataque altamente dirigido, con adversarios que extraen datos de sistemas comprometidos dentro de una red y usan programas ejecutables legítimos para disfrazar la actividad maliciosa.

Prioridad: 3 Importante.

Ampliar información:

- https://blog.elhacker.net/2023/05/el-robo-de-cookies-el-metodo-favorito-para-eludir-saltar-mfa-2fa.html
- https://news.sophos.com/es-419/2022/08/22/robo-de-cookies-la-nueva-violacion-del-perimetro-2/?x-clickref=1101lwJvHpJq&affiliate=1101l112254
- https://www.computerweekly.com/es/noticias/252524447/Robo-de-cookies-tactica-de-hackers-contra-autenticacion-multifactor

---

Hackean portal de contratos de Colombia Compra Eficiente

El portal Secop ll de Colombia Compra Eficiente se encuentra sin funcionamiento, tras un ataque cibernético externo a la infraestructura de la nube y que ya cumple dos días.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.rcnradio.com/colombia/hackean-portal-de-contratos-de-colombia-compra-eficiente
- https://www.elespectador.com/tecnologia/secop-ii-completo-34-horas-de-fallas-investigan-posible-hackeo/
- https://www.lafm.com.co/colombia/portal-de-contratos-de-colombia-compra-eficiente-sin-funcionamiento-por-hackeo