

#126



BOLETÍN INFORMATIVO MAINSOFT



INCIDENTES DE SEGURIDAD

CSIRT INFORMA VULNERABILIDADES PARCHADAS EN FIREFOX 116

El CSIRT de Gobierno comparte información de vulnerabilidades parchadas por Mozilla en Firefox 116, Firefox ESR 115.1 y Firefox ESR 102.14.

[**Más Información**](#)



CAMPAÑA DE MALWARE DIRIGIDA A ECUADOR DISTRIBUYE EL TROYANO NJRAT Y UTILIZA CORREOS FALSOS DE DEMANDAS JUDICIALES

Investigadores de ESET analizaron una campaña para espiar y robar información dirigida a empresas privadas, entidades gubernamentales y entidades del sector de salud durante el primer semestre de 2023.

[**Más Información**](#)

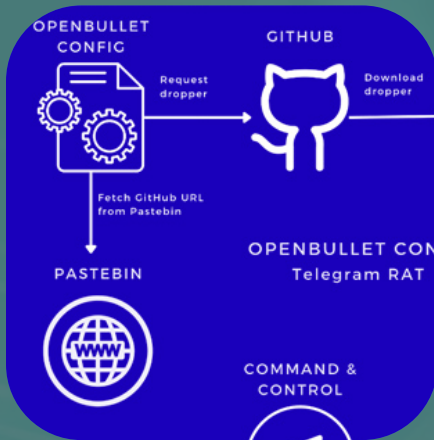
CSIRT COMPARTE INFORMACIÓN DE DOS VULNERABILIDADES PARCHADAS POR UBUNTU

El CSIRT de Gobierno comparte información de vulnerabilidades de alto riesgo que afectan al módulo OverlayFS de Ubuntu, y que ya fueron parchadas por Ubuntu.

[**Más Información**](#)



NUEVA CAMPAÑA DE MALWARE DIRIGIDA A CIBERDELINCUENTES SIN EXPERIENCIA CON CONFIGURACIONES DE OPENBULLET



Se ha observado una nueva campaña de malware que utiliza archivos de configuración maliciosos de OpenBullet para atacar a ciberdelincuentes sin experiencia con el objetivo de entregar un troyano de acceso remoto (RAT) capaz de robar información confidencial.

[Más Información](#)

NUEVA VARIANTE DE MALWARE SKIDMAP LINUX DIRIGIDA A SERVIDORES REDIS VULNERABLES

Los servicios vulnerables de Redis han sido atacados por una variante "nueva, mejorada y peligrosa" de un malware llamado SkidMap que está diseñado para atacar una amplia gama de distribuciones de Linux.

[Más Información](#)

```

[selinux/config ]; then
cho "SELINUX=disabled" > /etc/selinux/
cho "SELINUXTYPE=targeted" >> /etc/seli

/RefuseManualStop=yes/RefuseManualStop=
e 0
/var/empty ];then
mkdir /var/empty
shown root.root /var/empty

/RefuseManualStop=yes/RefuseManualStop=
etc/systemd/system/aegis.service
etc/systemd/system/aliyun.service
etc/systemd/system/AssistDaemon.service
c/systemd/system/multi-user.target.want
c/systemd/system/multi-user.target.want
sr/sbin/abrt-dbus
/sbin/auditd
auditd

```

EL RANSOMWARE EN LA INDUSTRIA MANUFACTURERA CAUSÓ \$ 46 MIL MILLONES EN PÉRDIDAS

Entre 2018 y 2023, 478 empresas de fabricación sufrieron un ataque de ransomware, lo que provocó una pérdida de aproximadamente \$ 46,2 mil millones solo en tiempo de inactividad.

[Más Información](#)





EL NUEVO 'ATAQUE DE APRENDIZAJE PROFUNDO' DESCIFRA LAS PULSACIONES DE TECLAS DE LAS COMPUTADORAS PORTÁTILES CON UN 95 % DE PRECISIÓN



Un grupo de académicos ha ideado un "ataque de canal lateral acústico basado en aprendizaje profundo" que se puede usar para clasificar las pulsaciones de teclas de una computadora portátil que se registran usando un teléfono cercano con un 95% de precisión.

[***Más Información***](#)

PREVISIÓN DEL MARTES DE PARCHES DE AGOSTO DE 2023: MEJORAS EN LA SEGURIDAD DEL SOFTWARE



La avalancha continua de ataques de phishing , la implementación de ransomware y otras formas de explotación está obligando a la comunidad a prestar más atención a la identificación temprana.

[***Más Información***](#)



CYLANCE

EVALUACIÓN DE HERRAMIENTAS PAM Y SU PRÓXIMO PASO EN LA GESTIÓN DE ACCESO PRIVILEGIADO

La identidad es el nuevo perímetro, y la gestión de acceso privilegiado (PAM) es la piedra angular de la seguridad moderna de acceso e identidad. Ninguna identidad, humana o de máquina, es más imperativa de proteger que aquellas con acceso privilegiado a sistemas, datos, aplicaciones y otros recursos confidenciales.

[Más Información](#)



DARKTRACE



DARKTRACE

REVELANDO LA VERDAD DETRÁS DE LAS AMENAZAS INTERNAS DE OT Y CÓMO DETECTARLAS

La amenaza interna se refiere a las amenazas cibernéticas que se originan dentro de una organización. Las amenazas internas pueden venir en forma de empleados, proveedores, contratistas o cualquier persona con acceso a sistemas, datos o información confidencial.

[Más Información](#)

BEYONDTRUST

UN NUEVO INFORME REVELA UN AUMENTO DE MALWARE ÚNICO Y UN AUMENTO REPENTINO DE ATAQUES AL SECTOR PÚBLICO

El BlackBerry Global Threat Intelligence Report, recién publicado, revela un aumento del 40 % en los ataques cibernéticos contra el gobierno y las organizaciones de servicios públicos en comparación con el trimestre anterior.

[Más Información](#)



BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

[HAZ CLICK](#)

DARKTRACE



CYLANCE

BeyondTrust

EVENTOS CERCANOS DE NUESTROS PARTNERS

DARKTRACE <https://bit.ly/3Cd0x8g>

CYLANCE <https://bit.ly/3EIP748>

IBM <https://ibm.co/2Z1YVA3>

BEYONDTRUST <https://bit.ly/3EwkngX>



www.mainsoft.cl