@mindefarg
argentina.gob.ar/defensa

Ministerio de Defensa
Argentina

Edificio Libertador
Azopardo 250 (CABA)
(54 11) 4346-8836/9

## Subsecretaría de Ciberdefensa

# Boletín de Noticias de Ciberseguridad

**Informe sobre incidentes y ciberamenazas Nro. 128 – Año 2021**

Este boletín periódico es un resumen seleccionado de las últimas vulnerabilidades, incidentes de seguridad e informes recopilados de fuentes internacionales conocidas dedicadas a la seguridad informática. Está destinado a las áreas de ciberseguridad de la Defensa como información de interés general para su difusión.

### 20/08/2021 al 30/08/21

- El Consorcio de Sistemas de Internet (ISC) resolvió un defecto de denegación de servicio (DoS) de alta gravedad (CVE-2021-25218) que afecta al software BIND DNS.
https://securityaffairs.co/wordpress/121316/security/bind-dns-dos-flaw.html
- Hackers publican imágenes de las cámaras de seguridad del interior de la prisión iraní de Evin.
https://www.jpost.com/breaking-news/hackers-release-security-camera-footage-from-inside-irans-evin-prison-677431
- **El Departamento de Estado de EE.UU. es víctima de un ciberataque.**
https://www.infosecurity-magazine.com/news/us-state-department-cyber-attack/
- Se expusieron 38 millones de registros de Microsoft Power Apps de decenas de organizaciones.
https://thehackernews.com/2021/08/38-million-records-exposed-from.html
- **Un error crítico de la base de datos Cosmos afectó a miles de clientes de Microsoft Azure.**
https://thehackernews.com/2021/08/critical-cosmos-database-flaw-affected.html
https://www.theverge.com/2021/8/28/22646439/t-mobile-data-breach-ceo-security-mandiant-kpmg
- Samsung presenta un Kill Switch que puede desactivar a distancia los televisores robados.
https://www.forbes.com/sites/leemathews/2021/08/27/samsung-reveals-kill-switch-that-can-remotely-disable-stolen-tvs/
- Decenas de sitios web israelíes reciben mensajes de hackers de "DragonForceMalaysia".
https://www.jpost.com/israel-news/dozens-of-israeli-websites-see-hacker-message-from-dragonforcemalaysia-678047
- Ciberdelincuentes vuelven a atacar la plataforma DeFi.
https://www.infosecurity-magazine.com/news/cyberthieves-hit-defi-platform/

### TRABAJOS, ESTUDIOS Y ANÁLISIS ABOCADOS A LAS TEMÁTICAS DE LA CIBERSEGURIDAD

- El malware ShadowPad se ha convertido en la opción favorita de los grupos de espionaje chinos.
https://thehackernews.com/2021/08/shadowpad-malware-is-becoming-favorite.html
- Los derechos de administrador de Windows 10 son arrebatados por los dispositivos Razer.
https://threatpost.com/windows-10-admin-rights-razer-devices-mouse-peripherals/168855/
- **El FBI comparte los detalles técnicos del ransomware Hive.**
https://www.bleepingcomputer.com/news/security/fbi-shares-technical-details-for-hive-ransomware/
- Las 15 principales vulnerabilidades que los atacantes han aprovechado innumerables veces para hackear sistemas Linux.
https://thehackernews.com/2021/08/top-15-vulnerabilities-attackers.html
- El script de la banda de ransomware Pysa muestra exactamente los archivos que buscan.

https://www.bleepingcomputer.com/news/security/ransomware-gangs-script-shows-exactly-the-files-theyre-after/

- El bug de Microsoft Exchange ProxyToken puede permitir a los hackers robar el correo electrónico de los usuarios.
https://threatpost.com/microsoft-exchange-proxytoken-email/169030/

## NOTAS DE INTERÉS

- Grupo estatal de InkySquid que explota fallos conocidos de Internet Explorer.
https://threatpost.com/inkysquid-exploiting-ie-bugs/168833/
- **Los ataques de ransomware son ahora el segundo incidente de seguridad más denunciado.**
https://betanews.com/2021/08/19/ransomware-second-most-common-security-incident/
- La botnet Mozi IoT ahora también ataca a las entradas de red de Netgear, Huawei y ZTE.
https://thehackernews.com/2021/08/mozi-iot-botnet-now-also-targets.html
- El descifrador del ransomware SynAck permite recuperar los archivos de manera gratuita.
https://www.bleepingcomputer.com/news/security/synack-ransomware-decryptor-lets-victims-recover-files-for-free/
- Internet Explorer está de manera oficial en sus últimos días.
https://www.forbes.com/sites/leemathews/2021/08/19/internet-explorer-is-officially-on-its-last-legs/
- **Advierten de 4 grupos emergentes de ransomware que pueden causar estragos.**
https://thehackernews.com/2021/08/researchers-warn-of-4-new-ransomware.html
- Una compilación personalizada de WhatsApp contiene el malware Triada.
https://threatpost.com/custom-whatsapp-build-malware/168892/
- **Linux cumple 30 años.**
https://www.networkworld.com/article/3630374/linux-turns-30.html
- Estados Unidos firma acuerdos de ciberseguridad con Singapur.
https://www.infosecurity-magazine.com/news/us-signs-cybersecurity-agreements/
- La banda de ciberdelincuentes FIN8 abre las puertas traseras de organizaciones de EE.UU. con el nuevo malware Sardonic.
https://thehackernews.com/2021/08/researchers-uncover-fin8s-new-backdoor.html
https://threatpost.com/fin8-bank-sardonic-backdoor/168982/
- **Microsoft y Google invertirán 30.000 millones de dólares en ciberseguridad durante los próximos 5 años.**
https://thehackernews.com/2021/08/microsoft-google-to-invest-30-billion.html
- Un grupo de derechos aconseja a los afganos que borren sus datos.
https://www.infosecurity-magazine.com/news/rights-groups-advises-afghans-to/

## ACTUALIZACIONES DE SEGURIDAD

- CISA advierte a los administradores que corrijan urgentemente los bugs de Exchange ProxyShell.
https://www.bleepingcomputer.com/news/security/cisa-warns-admins-to-urgently-patch-exchange-proxyshell-bugs/
- Se ha publicado un parche ante un fallo crítico en el APIC para switches de Cisco.
https://thehackernews.com/2021/08/critical-flaw-discovered-in-cisco-apic.html