@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. 85/2021**

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.

### 19/03/2021

- Ahora el antivirus MS Defender reduce las vulnerabilidades del Exchange Server.
  https://www.zdnet.com/article/microsoft-defender-antivirus-now-patches-exchange-server-vulnerabilities/
- El grupo informático Acer sufre un ataque de ransomware por valor de 50 millones de dólares.
  https://securityaffairs.co/wordpress/115777/cyber-crime/acer-revil-ransomware.html
- El malware CopperStealer afecta a las cuentas empresariales de Facebook e Instagram.
  https://threatpost.com/copperstealer-hijacks-accounts/164919/
- La interrupción global de Facebook afecta a WhatsApp, Messenger e Instagram.
  https://www.bleepingcomputer.com/news/technology/facebook-outage-affecting-whatsapp-messenger-and-instagram/
- El ataque de phishing a Office 365 tiene como destinatarios a los ejecutivos financieros.
  https://threatpost.com/office-365-phishing-attack-financial-execs/164925/

### 20/03/2021

- Un grupo de piratas informáticos utilizó 11 *días cero* para atacar a usuarios de Windows, iOS y Android.
  https://www.bleepingcomputer.com/news/security/hacking-group-used-11-zero-days-to-attack-windows-ios-android-users/
  https://securityaffairs.co/wordpress/115786/hacking/11-zero-day-flaws-hacking-group.html
- Microsoft detiene el lanzamiento de la actualización de emergencia de Windows 10 KB5001649.
  https://www.bleepingcomputer.com/news/microsoft/microsoft-halts-rollout-of-windows-10-kb5001649-emergency-update/

### 21/03/2021

- Dos sitios web del gobierno polaco fueron *hackeados* con el objeto de difundir información falsa acerca de una "fuga" de residuos nucleares en la vecina Lituania.
  https://www.ehackingnews.com/2021/03/polish-authorities-got-hacked-for-sake.html

### 22/03/2021

- Podcast diario de seguridad de redes de SANS del lunes 22 de marzo de 2021.
  https://isc.sans.edu/podcastdetail.html?id=7422
- Una vulnerabilidad crítica RCE fue encontrada en el software Apache OFBiz ERP - Aplicar parche!
  https://thehackernews.com/2021/03/critical-rce-vulnerability-found-in.html
- Una campaña de malware tiene como objetivo la aplicación de escritorio de Telegram.
  https://www.ehackingnews.com/2021/03/malware-campaign-targets-telegram.html

- Shell, el gigante de la energía, revela una filtración de datos tras el hackeo de Accellion.
https://www.bleepingcomputer.com/news/security/energy-giant-shell-discloses-data-breach-after-accellion-hack/
- ADVERTENCIA: Nueva vulnerabilidad "zero-day" de Android sometida a ataques continuos.
https://thehackernews.com/2021/03/warning-new-android-zero-day.html

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

- Dos análisis de IBM-xForce sobre el troyano Metaformo que ha afectado a Latinoamérica y el *adware* de macOS escrito en lenguaje Rust.
https://exchange.xforce.ibmcloud.com/collection/6e934f1121d09aff346710499c02e8e4
https://exchange.xforce.ibmcloud.com/collection/1ee3ace54cba8a565358db2e30e9792f
- El backdoor "XcodeSpy" de Mac ataca a los desarrolladores de Xcode.
https://nakedsecurity.sophos.com/2021/03/19/serious-security-mac-supply-chain-backdoor-takes-aim-at-xcode-devs/
- Microsoft Edge prueba la corrección de los problemas de rendimiento de DNS-sobre-HTTPS.
https://www.bleepingcomputer.com/news/microsoft/microsoft-edge-tests-fix-for-dns-over-https-performance-issues/
- Los sistemas de distribución de electricidad corren un riesgo cada vez mayor de sufrir ciberataques. Un informe de la GAO de EE.UU.
https://www.securityweek.com/electricity-distribution-systems-increasing-risk-cyberattacks-gao-warns
https://www.gao.gov/assets/gao-21-81.pdf

## NOTAS DE INTERÉS

- ¿Qué son los ataques de smishing? ¿Cómo prevenirlos?
https://www.ehackingnews.com/2021/03/what-are-smishing-attacks-how-to.html
- Cyber Polygon es un evento anual de ciberseguridad, *en línea,* entre países y organizaciones mundiales, para entrenar e incrementar capacidades e intercambiar mejores prácticas.
https://cyberpolygon.com/
- Ahora los "*booters*" de DDoS aprovechan los servidores DTLS para amplificar los ataques.
https://www.bleepingcomputer.com/news/security/ddos-booters-now-abuse-dtls-servers-to-amplify-attacks/
- Otra operación de ransomware conocida como "BlackKingdom" aprovecha las vulnerabilidades de Microsoft Exchange Server ProxyLogon para cifrar servidores.
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-now-targeted-by-blackkingdom-ransomware/
- Las 3 principales lecciones de ciberseguridad aprendidas de la pandemia.
https://www.darkreading.com/operations/top-3-cybersecurity-lessons-learned-from-the-pandemic/a/d-id/1340375

## ACTUALIZACIONES DE SEGURIDAD

- El CISA difunde CHIRP, una herramienta para detectar la actividad maliciosa en SolarWinds.
https://securityaffairs.co/wordpress/115821/security/cisa-chirp-solarwinds-tool.htm
- Adobe corrige un fallo crítico de ColdFusion en una actualización de emergencia.
https://threatpost.com/adobe-critical-coldfusion-flaw-update/164946/