@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. 130 – 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.

03/09/21

- La FTC de EE.UU. ordena a SpyFone que elimine todos sus datos de vigilancia.
https://www.zdnet.com/article/ftc-orders-spyfone-to-delete-all-of-its-surveillance-data/
- La ruptura de Accellion afecta a Beaumont Health.
https://www.infosecurity-magazine.com/news/accellion-breach-beaumont-health/
- El paquete NPM con 3 millones de descargas semanales tenía una grave vulnerabilidad.
https://arstechnica.com/information-technology/2021/09/npm-package-with-3-million-weekly-downloads-had-a-severe-vulnerability/
- **La interrupción de Internet en Nueva Zelanda se atribuye a un ataque DDoS contra el tercer mayor proveedor de Internet del país.**
https://www.theregister.com/2021/09/03/nz_outage/
https://securityaffairs.co/wordpress/121856/hacking/new-zealand-ddos.html

04/09/21

- Microsoft afirma que hackers chinos estaban detrás del ataque SSH 0-Day de SolarWinds Serv-U.
https://thehackernews.com/2021/09/microsoft-says-chinese-hackers-were.html
- Empresas con sede en el Reino Unido, Voip Unlimited y Voipfone bajo ataque DDoS.
https://www.ehackingnews.com/2021/09/uk-based-firms-voip-unlimited-and.html

05/09/21

- La bolsa de criptomonedas Bilaxy es atacada.
https://www.ehackingnews.com/2021/09/cryptocurrency-exchange-bilaxy-under.html
- **El servicio sanitario irlandés sigue recuperándose meses después del hackeo.**
https://www.bbc.com/news/world-europe-58413448

06/09/21

- **Los ataques al IoT se disparan y se duplican en 6 meses.**
https://threatpost.com/iot-attacks-doubling/169224/
- Desarrollador de la banda TrickBot fue detenido cuando intentaba salir de Corea.
https://www.bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/
- La Gardai (policía) irlandesa toma medidas contra los ciberatacantes del HSE.
https://www.infosecurity-magazine.com/news/garda-seize-infrastructure-hse/

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

- Una nueva familia de malware utiliza los archivos de registro CLFS para evitar su detección.
https://thehackernews.com/2021/09/this-new-malware-family-using-clfs-log.html

- Más de 60.000 dominios en *parking* (registrados sin uso) vulnerables al secuestro de AWS.
https://www.bleepingcomputer.com/news/security/over-60-000-parked-domains-were-vulnerable-to-aws-hijacking/

- **El código fuente completo del ransomware Babuk se ha filtrado en un foro de hackers.**
https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/#.YTJHSxKrZ2A.twitter

- **Nueve importantes iniciativas gubernamentales de ciberseguridad de 2021.**
https://www.csoonline.com/article/3630632/9-notable-government-cybersecurity-initiatives-of-2021.html

NOTAS DE INTERÉS

- Los delincuentes de FIN7 utilizan documentos temáticos de Windows 11 para instalar un backdoor de Javascript.
https://thehackernews.com/2021/09/fin7-hackers-using-windows-11-themed.html

- El Cibercomando de EE.UU. alerta a las empresas de ese país de los "continuos" *hackeos* dirigidos al software empresarial de Atlassian.
https://www.cyberscoop.com/atlassian-confluence-ransomware-cyber-command/
https://thehackernews.com/2021/09/us-cyber-command-warns-of-ongoing.html

- Este defecto de seguridad de Android podría permitir a los hackers seguir todos tus movimientos.
https://www.techradar.com/news/this-android-flaw-could-let-hackers-follow-all-your-movements

- **Apple "pone en pausa" la controvertida función de detección de CSAM.**
https://gizmodo.com/apple-hits-pause-on-controversial-csam-detection-featur-1847612602

- Cómo mejorar la seguridad de los datos biométricos.
https://www.weforum.org/agenda/2021/09/untangling-the-benefits-and-risks-of-biometrics/

- Se han encontrado vulnerabilidades en los sistemas ferroviarios de Moxa, empresa de Taiwán, que pueden causar trastornos.
https://www.ehackingnews.com/2021/09/vulnerabilities-found-in-moxa-railway.html

- **BrakTooth: investigadores de seguridad revelan 16 graves fallos de Bluetooth que afectan a miles de millones de dispositivos.**
https://betanews.com/2021/09/06/braktooth-security-researchers-reveal-16-serious-bluetooth-flaws-affecting-billions-of-devices/

- La nueva herramienta Chainsaw ayuda a los equipos de IR a analizar los registros de eventos de Windows,
https://www.bleepingcomputer.com/news/security/new-chainsaw-tool-helps-ir-teams-analyze-windows-event-logs/

ACTUALIZACIONES DE SEGURIDAD

- Es posible que Windows 11 no reciba actualizaciones de seguridad en los dispositivos no compatibles.
https://www.bleepingcomputer.com/news/microsoft/windows-11-may-not-get-security-updates-on-unsupported-devices/

- Netgear soluciona graves fallos de seguridad en 20 de sus productos.
https://securityaffairs.co/wordpress/121899/security/netgear-vulnerabilities.html