@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. 75/2021

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.

05/02/2021

- Eletrobras y Copel, empresas energéticas brasileñas, fueron afectadas por ataques ransomware.
  https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/
  https://threatpost.com/ransomware-attacks-major-utilities/163687/

- Los servidores Plex Media que utilizan SSDP permiten a los DDoSers amplificar los ataques por un factor de 5.
  https://arstechnica.com/information-technology/2021/02/ddosers-are-abusing-the-plex-media-server-to-make-attacks-more-potent/
  https://thehackernews.com/2021/02/cybercriminals-now-using-plex-media.html

- El grupo TeamTNT utiliza el malware Hildegard para atacar los sistemas Kubernetes.
  https://securityaffairs.co/wordpress/114241/malware/teamtnt-hildegard-malware-kubernetes.html

06/02/2021

- Google ha eliminado de su Chrome Web Store, a The Great Suspender, una popular extensión que permite reducir uso de memoria utilizada por millones de usuarios, por contener malware.
  https://thehackernews.com/2021/02/warning-hugely-popular-great-suspender.html

- El mayor centro internacional de phishing (en Ucrania) ha sido bloqueado.
  https://www.ehackingnews.com/2021/02/the-largest-international-phishing.html

- Serco confirma el ataque de ransomware Babuk.
  https://www.ehackingnews.com/2021/02/serco-affirms-babuk-ransomware-attack.html

07/02/2021

- Signal fue bloqueada recientemente por el gobierno iraní y sugirió una solución de proxy TLS.
  https://www.bleepingcomputer.com/news/security/signal-ignores-proxy-censorship-vulnerability-bans-researchers/

- Un nuevo ataque de phishing utiliza el código Morse para ocultar las URL peligrosas.
  https://www.bleepingcomputer.com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/

- Ciberactivistas desfiguran varios dominios de Sri Lanka, incluido Google.lk.
  https://www.zdnet.com/article/hacktivists-deface-multiple-sri-lankan-domains-including-google-lk/

08/02/2021

- Microsoft alerta a los usuarios de Office 365 sobre la actividad de hacking de estados nacionales.
  https://www.zdnet.com/article/microsoft-to-add-nation-state-activity-alerts-to-defender-for-office-365/

- El ataque de ransomware de WestRock dificulta la producción de envases. https://threatpost.com/westrock-ransomware-attack/163717/
- Miles de millones de contraseñas se ofrecen por 2 dólares en el ciberespacio. https://threatpost.com/billions-passwords-cyber-underground/163738/
- **Un hacker entró en una instalación de agua de Florida para alterar el nivel de hidróxido de sodio.** https://www.cyberscoop.com/florida-hacker-water-plant-sodium-hydroxide/

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

- Nueva hoja informativa sobre *ransomware* publicada por el FBI, CISA y otras agencias de EE.UU. https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf
- Las redes industriales experimentan un fuerte aumento de los brechas de seguridad *pirateables*. https://threatpost.com/industrial-networks-hackable-security-holes/163708/
- Por actualización una aplicación maliciosa para Android se apoderó de millones de dispositivos https://www.zdnet.com/article/with-one-update-this-malicious-android-app-hijacked-10-million-devices/

NOTAS DE INTERÉS

- El ex jefe de ciberseguridad de EE.UU., Chris Krebs, pide que los militares ataquen a los hackers. https://www.ft.com/content/27c09769-ceb5-46dd-824f-40b684d681ae
- La función de sincronización de Google Chrome puede ser aprovechada para obtener *"comando y control"* y la *exfiltración* de datos. https://www.zdnet.com/article/google-chrome-syncing-features-can-be-abused-for-c-c-and-data-exfiltration/
- Se descubren vínculos financieros entre conocidas bandas de *ransomware*. https://www.cyberscoop.com/ransomware-links-chainalysis-maze-egregor-doppelpaymer-suncrypt/
- Investigadores de seguridad impulsan un "programa de recompensas (bug bounty) para encontrar errores de último recurso". https://www.darkreading.com/application-security/security-researchers-push-for-bug-bounty-program-of-last-resort/d/d-id/1340081
- En un ciberataque el Reino Unido atacó aviones no tripulados y servidores en línea de Isis. https://www.ft.com/content/360a8e1c-b241-40f7-b944-45a4f8854ac5
- Así es como Irán espía a los disidentes con la ayuda de hackers. https://thehackernews.com/2021/02/researchers-reveal-how-iran-spies-on.html

ACTUALIZACIONES DE SEGURIDAD

- La actualización de Chrome 88 incluye una importante corrección de seguridad para una vulnerabilidad de *"día cero"*. https://www.theverge.com/2021/2/5/22267872/chrome-88-zero-day-vulnerability-government-backed-hackers-security-researchers
- Mozilla resuelve el error de corrupción del NTFS de Windows 10 que genera Firefox. https://betanews.com/2021/02/07/mozilla-firefox-update-windows-10-ntfs-corruption-bug/