@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. 83/2021

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.

12/03/2021

- El ransomware DEARCRY ataca servidores de Microsoft Exchange con exploits de ProxyLogon.
  https://thehackernews.com/2021/03/icrosoft-exchange-ransomware.html
- Hackeo del correo electrónico Exchange: Cientos de empresas británicas comprometidas.
  https://www.bbc.com/news/technology-56365372
- La cervecera Molson Coors abre una investigación por ciberataque.
  https://threatpost.com/molson-coors-cyberattack-investigation/164722/
- Grupos hackearon sitios del gobierno indio a través de archivos git y env expuestos.
  https://www.bleepingcomputer.com/news/security/researchers-hacked-indian-govt-sites-via-exposed-git-and-env-files/

13/03/2021

- El primer ministro Johnson dice que Gran Bretaña debe aumentar su capacidad de ciberataque.
  https://www.reuters.com/article/uk-britain-defence/britain-must-boost-cyber-attack-capacity-pm-johnson-says-idUSKBN2B50OP
- Expertos han encontrado tres defectos de hace 15 años en un módulo del kernel de Linux.
  https://securityaffairs.co/wordpress/115565/security/linux-kernel-flaws.html
- **El complejo militar-industrial ruso anunció la prohibición del uso de WhatsApp y Zoom para el trabajo.**
  https://www.ehackingnews.com/2021/03/russian-military-industrial-complex.html

14/03/2021

- Un error de Twitter te suspende la cuenta automáticamente cuando se tuitea 'Memphis'.
  https://www.bleepingcomputer.com/news/technology/twitter-bug-automatically-suspends-you-when-tweeting-memphis/
  https://www.theguardian.com/technology/2021/mar/15/twitter-accidentally-blocks-users-who-post-the-word-memphis
- Australia, India, Japón y Estados Unidos crean un grupo de trabajo conjunto sobre tecnologías críticas.
  https://www.theregister.com/2021/03/14/quad_critical_tech_working_group/
- Los piratas informáticos de Black Shadow vuelven a atacar y filtran documentos en un nuevo ciberataque.
  https://www.jpost.com/jpost-tech/israeli-car-financing-company-hacked-private-information-held-for-ransom-661865

15/03/2021

- EE.UU. acusa al director general de la empresa de telefonía encriptada 'Sky', por narcotráfico.
  https://www.vice.com/en/article/4adzdj/sky-secure-global-indictment

- El incendio del centro de datos de OVH, en Estrasburgo, afecta a los ciberdelincuentes. https://www.infosecurity-magazine.com/news/ovh-data-center-fire-impacts/#.YE-d5RQW5hc.twitter
- Ahora los sitios de phishing detectan máquinas virtuales para eludir la detección. https://www.bleepingcomputer.com/news/security/phishing-sites-now-detect-virtual-machines-to-bypass-detection/
- Más de 80.000 servidores Exchange siguen afectados por vulnerabilidades las cuales son explotadas activamente. https://www.securityweek.com/over-80000-exchange-servers-still-affected-actively-exploited-vulnerabilities

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

- Aumento de la demanda del mercado de software de protección DDoS para 2020-2028. https://thehackernews.com/2021/03/rising-demand-for-ddos-protection.html
- Cinco pasos para que su SOC corporativo pueda detectar y responder rápidamente a las amenazas de IoT/OT. https://www.microsoft.com/security/blog/2021/03/15/5-steps-to-enable-your-corporate-soc-to-rapidly-detect-and-respond-to-iot-ot-threats/
- Cómo elegir el marco de ciberseguridad adecuado. https://www.darkreading.com/risk/how-to-choose-the-right-cybersecurity-framework/a/d-id/1340319
- Análisis de seguridad del protocolo "*Find My...*" de Apple. https://www.schneier.com/blog/archives/2021/03/security-analysis-of-apples-find-my-protocol.html
- Ingeniería inversa: un kit de herramientas para el investigador de seguridad. https://www.tripwire.com/state-of-security/podcast/reverse-engineering-a-security-researchers-toolkit/

NOTAS DE INTERÉS

- El ransomware Darkside 2.0 promete las velocidades de cifrado más rápidas de la historia. https://www.infosecurity-magazine.com/news/darkside-20-ransomware-fastest/
- El nuevo malware *botnet* ZHtrap utiliza honeypots para encontrar más objetivos. https://www.bleepingcomputer.com/news/security/new-zhtrap-botnet-malware-deploys-honeypots-to-find-more-targets/
- El troyano bancario Metamorfo recurre a AutoHotKey para evitar su detección. https://threatpost.com/metamorfo-banking-trojan-autohotkey/164735/
- Investigadores han detectado un malware escrito en el lenguaje de programación Nim. https://thehackernews.com/2021/03/researchers-spotted-malware-written-in.html
- Investigación: Las agencias de seguridad divulgan información a través de PDFs incorrectamente desinfectados. https://www.securityweek.com/research-security-agencies-expose-information-improperly-sanitized-pdfs

ACTUALIZACIONES DE SEGURIDAD

- Este mes Google corrige el segundo "*día cero*" de Chrome que es explotado activamente. https://www.bleepingcomputer.com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-this-month/