@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. 202 – Año 2023

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.

NOTICIAS DE CIBERSEGURIDAD entre el 27/1/23 y el 10/2/23

1. BlackCat Ransomware hackeo a SOLAR INDUSTRIES INDIA y roba 2 TB de datos militares secretos.
   https://securityaffairs.com/141409/data-breach/blackcat-ransomware-solar-industries-india.html

2. Vulnerabilidad de Realtek bajo ataque: más de 134 millones de intentos de hackeo de dispositivos IoT.
   https://thehackernews.com/2023/01/realtek-vulnerability-under-attack-134.html

3. Lista de exclusión aérea de EE. UU. compartida públicamente en un foro de hackers.
   https://www.bleepingcomputer.com/news/security/us-no-fly-list-shared-on-a-hacking-forum-government-investigating/

4. GitHub: intrusos clonaron certificados de firma de código en un repositorio violado.
   https://arstechnica.com/information-technology/2023/01/github-says-hackers-cloned-code-signing-certificates-in-breached-repository/

5. Microsoft: más de 100 actores de amenazas implementan ransomware en ataques.
   https://www.bleepingcomputer.com/news/security/microsoft-over-100-threat-actors-deploy-ransomware-in-attacks/

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

1. Analizando Orcus RAT en un Sandbox de malware.
   https://thehackernews.com/2023/01/3-lifehacks-while-analyzing-orcus-rat.html

2. Nueva variante de malware PlugX que se propaga a través de dispositivos USB extraíbles.
   https://www.bleepingcomputer.com/news/security/plugx-malware-hides-on-usb-devices-to-infect-new-windows-hosts/

3. La gestión de parches es crucial para proteger los servidores de Exchange, advierte Microsoft.
   https://securityaffairs.com/141451/security/microsoft-exchange-servers-patch.html

4. Mejores prácticas para el mapeo de MITRE ATT&CK®.
   https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping

5. Error de Samba (programas de interoperabilidad de Windows para Linux y Unix) causado por criptografía obsoleta.
   https://nakedsecurity.sophos.com/2023/01/30/serious-security-the-samba-logon-bug-caused-by-outdated-crypto/

6. TV Android T95 de Amazon infectada con malware pre-instalado.
   https://www.malwarebytes.com/blog/news/2023/01/preinstalled-malware-infested-t95-tv-box-from-amazon

7. Auditoría de Kubernetes con SIEM y XDR de código abierto.
   https://thehackernews.com/2023/02/auditing-kubernetes-with-open-source.html

8. SaaS (Software como un Servicio) en el mundo real: ¿Quién es responsable de proteger estos datos?
   https://thehackernews.com/2023/02/saas-in-real-world-whos-responsible-to.html

NOTAS DE INTERÉS

1. CISA publica un script de recuperación para las organizaciones víctimas del ransomware ESXiArgs.
https://www.cisa.gov/uscert/ncas/current-activity/2023/02/07/cisa-releases-esxiargs-ransomware-recovery-script

2. La IA con toma de conciencia de usuarios crea una alianza que permite a organizaciones protegerse de ChatGPT.
https://www.darkreading.com/vulnerabilities-threats/why-chatgpt-isn-t-a-death-sentence-for-cyber-defenders

3. OpenAI presenta herramienta para detectar texto escrito por IA.
https://www.bleepingcomputer.com/news/technology/openai-releases-tool-to-detect-ai-written-text/

4. Los cazadores de satélites se preparan para una guerra espacial.
https://universemagazine.com/en/jackals-in-orbit-satellite-hunters-are-preparing-for-a-space-war/

5. Perspectivas cibernéticas 2023 | La computación cuántica y el próximo criptoapocalipsis.
https://www.securityweek.com/cyber-insights-2023-quantum-computing-and-the-coming-cryptopocalypse/

6. Sí, los CISO deberían preocuparse por los tipos de globos que pueden interceptar.
https://www.csoonline.com/article/3687222/yes-cisos-should-be-concerned-about-the-types-of-data-spy-balloons-can-intercept.html

7. 'Eventos cibernéticos catastróficos', otra violación de T-Mobile, y más problemas de LastPass.
https://portswigger.net/daily-swig/deserialized-web-security-roundup-catastrophic-cyber-events-another-t-mobile-breach-more-lastpass-problems

8. FBI: Los servidores de Hive ransomware finalmente se cerraron.
https://nakedsecurity.sophos.com/2023/01/27/hive-ransomware-servers-shut-down-at-last-says-fbi/

9. Herramientas legítimas de supervisión y gestión remotas en los ataques.
https://www.csoonline.com/article/3686610/hackers-abuse-legitimate-remote-monitoring-and-management-tools-in-attacks.html

10. KeePass: vulnerabilidad que permite el robo sigiloso de contraseñas.
https://www.bleepingcomputer.com/news/security/keepass-disputes-vulnerability-allowing-stealthy-password-theft/

ACTUALIZACIONES DE SEGURIDAD

1. Lexmark lanzó una actualización de firmware para corregir una falla que afecta a 100 modelos de impresoras.
https://securityaffairs.com/141428/hacking/lexmark-cve-2023-23560-rce.html

2. Microsoft: actualice el servidor de Exchange local ahora.
https://www.infosecurity-magazine.com/news/microsoft-patch-onpremises/

3. Actualice vRealize ahora. VMware parchea vulnerabilidades críticas de RCE.
https://www.malwarebytes.com/blog/news/2023/01/update-vrealize-now-vmware-patches-critical-rce-vulnerabilities

4. Microsoft lanza la actualización KB5022360 para solucionar numerosos problemas de Windows 11.
https://betanews.com/2023/01/27/microsoft-releases-kb5022360-update-to-fix-numerous-windows-11-issues/

5. QNAP soluciona una vulnerabilidad crítica en los dispositivos NAS con las últimas actualizaciones de seguridad.
https://www.bleepingcomputer.com/news/security/qnap-fixes-critical-bug-letting-hackers-inject-malicious-code/