@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. 207 – 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 20/5/23 y el 6/6/23

1. El fabricante de armas Rheinmetall confirma el ataque del ransomware BlackBasta.
https://www.bleepingcomputer.com/news/security/arms-maker-rheinmetall-confirms-blackbasta-ransomware-attack/

2. Los repositorios de copia de seguridad, objetivo del 93% de los ataques de ransomware.
https://www.infosecurity-magazine.com/news/backup-targeted-93-per-cent/

3. El repositorio de código abierto PyPI se enfrenta a una oleada de malware.
https://nakedsecurity.sophos.com/2023/05/23/pypi-open-source-code-repository-deals-with-manic-malware-maelstrom/

4. Las brechas de ciberseguridad podrían poner en grave peligro a los astronautas.
https://spectrum.ieee.org/cybersecurity-in-space

5. Millones de motherboards de PC se vendieron con una puerta trasera en el firmware.
https://www.securityweek.com/organizations-warned-of-backdoor-feature-in-hundreds-of-gigabyte-motherboards/

6. El bug de XFS en el kernel Linux 6.3.3 coincide con la reaparición del código de SGI.
https://www.theregister.com/2023/05/31/bugs_in_ex_sgi_xfs/

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

1. Microsoft desvela un ataque informático chino a infraestructuras críticas de Estados Unidos.
https://blog.elhacker.net/2023/05/microsoft-informa-ataques-chinos-infraestructuras-criticas-estados-unidos.html

2. El ransomware Royal & BlackCat: Lo que debe saber.
https://www.tripwire.com/state-of-security/royal-blackcat-ransomware-what-you-need-know

3. CISA y socios actualizan la guía #StopRansomware, desarrollada a instancias de la Joint Ransomware Task Force (JRTF).
lhttps://www.cisa.gov/resources-tools/resources/stopransomware-guide

4. Los investigadores de ReversingLabs descubrieron dos paquetes maliciosos que contenían TurkoRat.
https://www.reversinglabs.com/blog/rats-found-hiding-in-the-npm-attic

5. ¿Qué es la autenticación multifactorial?
https://www.kaspersky.com/blog/what-is-two-factor-authentication/48289/

NOTAS DE INTERÉS

1. El nuevo troyano de acceso remoto GobRAT se centra en los routers Linux en Japón.
https://thehackernews.com/2023/05/new-gobrat-remote-access-trojan.html

2. Los investigadores de la firma de seguridad Uptycs informaron que los actores de amenazas vinculados al ransomware Cyclops están ofreciendo un ladrón de información basado en en lenguaje Go.
https://securityaffairs.com/147127/cyber-crime/cyclops-ransomware-gang-info-stealer.html

3. Aprovechar los modelos de lenguaje grande (LLM) para la seguridad y privacidad corporativa.
https://www.helpnetsecurity.com/2023/06/06/llms-privacy-concerns/

4. La influencia de la IA generativa en el gobierno y el cumplimiento de los datos.
https://www.helpnetsecurity.com/2023/06/06/generative-ai-data-governance-compliance-video/

5. KeePass solucionó el error que permite la extracción de la contraseña maestra de texto claro.
https://securityaffairs.com/147109/security/keepass-fixed-the-bug-that-allows-the-extraction-of-the-cleartext-master-password.html

6. 10 iniciativas notables de ciberseguridad de infraestructura crítica en 2023.
https://www.csoonline.com/article/3698190/10-notable-critical-infrastructure-cybersecurity-initiatives-in-2023.html

7. IA generativa: el nuevo vector de ataque a la confianza y la seguridad.
https://www.helpnetsecurity.com/2023/05/30/generative-ai-abuse/

ACTUALIZACIONES DE SEGURIDAD

1. Actualizaciones de Samsung corrigen un Día Cero.
https://security.samsungmobile.com/securityUpdate.smsb

2. Google corrige una nueva falla de día cero de Chrome con un exploit.
https://www.bleepingcomputer.com/news/security/google-fixes-new-chrome-zero-day-flaw-with-exploit-in-the-wild/

3. Actualizar! Vulnerabilidad de MOVEit Transfer explotada activamente.
https://www.malwarebytes.com/blog/news/2023/06/update-now-moveit-transfer-vulnerability-actively-exploited

4. CISA agrega Barracuda zero-day recientemente parcheado a su catálogo de Vulnerabilidades Explotadas Conocidas.
https://securityaffairs.com/146729/security/cisa-barracuda-0day-catalog.html