@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. 212 – 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 11/08/23 y el 28/08/23

1. La nueva APT "Carderbee" atacó el software de seguridad chino en la cadena de suministro.
https://www.securityweek.com/new-carderbee-apt-targeted-chinese-security-software-in-supply-chain-attack/

2. El ciberataque a la empresa australiana Energy One se extiende a los sistemas del Reino Unido.
https://www.infosecurity-magazine.com/news/cyberattack-australian-utility/

3. El gigantesco consultor de seguridad Kroll ha revelado que un ataque de intercambio de SIM contra uno de sus empleados condujo al robo de información de usuarios de múltiples plataformas de criptomonedas.
https://krebsonsecurity.com/2023/08/kroll-employee-sim-swapped-for-crypto-investor-data/

4. El nuevo malware MMRat de Android utiliza el protocolo Protobuf para robar sus datos.
https://www.bleepingcomputer.com/news/security/new-android-mmrat-malware-uses-protobuf-protocol-to-steal-your-data/

5. Alerta de vulnerabilidad crítica: redes de operaciones de VMware Aria en riesgo de ataques remotos.
https://thehackernews.com/2023/08/critical-vulnerability-alert-vmware.html

6. Los crecientes incidentes cibernéticos desafían a las organizaciones sanitarias.
https://www.helpnetsecurity.com/2023/08/30/cyber-incidents-challenge-healthcare-organizations/

7. Un grupo de hackers chino explota Barracuda Zero-Day para atacar al gobierno, el ejército y Telecom
https://thehackernews.com/2023/08/chinese-hacking-group-exploits.html

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

1. Informe de ESET sobre amenazas para el primer semestre de 2023.
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h12023.pdf

2. La reutilización de la infraestructura del Grupo Lazarus permite descubrir nuevos programas maliciosos.
https://blog.talosintelligence.com/lazarus-collectionrat/

3. En Crates.io se encuentran indicios de un ataque de malware dirigido a desarrolladores de Rust.
https://blog.phylum.io/rust-malware-staged-on-crates-io/

4. Análisis de archivos de exploits RAR (CVE-2023-38831).
https://isc.sans.edu/diary/Analysis+of+RAR+Exploit+Files+CVE202338831/30164

5. El nuevo malware "Whiffy Recon" triangula la ubicación del dispositivo infectado a través de Wi-Fi cada minuto.
https://thehackernews.com/2023/08/new-whiffy-recon-malware-triangulates.html

6. La falta de visibilidad de las políticas de acceso a la nube deja a las empresas a ciegas.
https://www.helpnetsecurity.com/2023/08/24/visibility-cloud-access-policies/

NOTAS DE INTERÉS

1. Internet se está convirtiendo en una caja negra de datos. Una "API de inspección" podría abrirla.
https://www.wired.com/story/inspectability-api-app-transparency/

2. Microsoft Excel permite ejecutar scripts de Python como fórmulas.
https://www.bleepingcomputer.com/news/microsoft/microsoft-excel-to-let-you-run-python-scripts-as-formulas/

3. La botnet Crypto en X (Twitter) es potenciado por ChatGPT.
https://arstechnica.com/information-technology/2023/08/chatgpt-boosts-crypto-botnet-with-ai-generated-tweets/

4. Google Chrome advertirá a los usuarios sobre las extensiones que generen problemas.
https://betanews.com/2023/08/17/google-chrome-to-warn-users-about-problematic-extensions/

5. Una vulnerabilidad de alta gravedad en WinRAR podría permitir la ejecución de código al abrir archivos.
https://arstechnica.com/information-technology/2023/08/chatgpt-boosts-crypto-botnet-with-ai-generated-tweets/

6. La preparación cuántica: Migración a la criptografía postcuántica.
https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

7. ¿Qué es la Directiva sobre Seguridad de las Redes y de la Información 2 (NIS2) de la Unión Europea?
https://www.tripwire.com/state-of-security/what-network-and-information-security-2-directive-nis2

8. Microsoft advierte del aumento de los " atacantes en el medio " en las plataformas de phishing.
https://www.infosecurity-magazine.com/news/microsoft-aitm-uptick-phishing/

9. Qué software "parchear" primero: priorizar las actualizaciones.
https://www.kaspersky.com/blog/patching-priorities/48867/

10. Dos semanas en seguridad :

(a)14/08 al 20/08 https://www.malwarebytes.com/blog/news/2023/08/a-week-in-security-august-14-august-20
(b) 21/08 al 27/08 https://www.malwarebytes.com/blog/news/2023/08/a-week-in-security-august-21-august-27

ACTUALIZACIONES DE SEGURIDAD

1. ¿Usando WinRAR? Asegúrese de corregir estos errores de ejecución de código.
https://nakedsecurity.sophos.com/2023/08/23/using-winrar-be-sure-to-patch-against-these-code-execution-bugs/

2. Vulnerabilidades de corrupción de memoria de alta gravedad actualizadas en Firefox y Chrome.
https://www.securityweek.com/high-severity-memory-corruption-vulnerabilities-patched-in-firefox-chrome/

3. Los investigadores lanzaron un exploit PoC para la falla CVE-2023-38035 de Ivanti Sentry.
https://securityaffairs.com/149837/breaking-news/poc-exploit-ivanti-sentry-cve-2023-38035.html

4. Lanzamiento de Kali Linux 2023.3: rediseño de la aplicación Kali NetHunter, 9 nuevas herramientas y más.
https://www.helpnetsecurity.com/2023/08/24/kali-linux-2023-3-released/