@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. 211 – 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 25/07/23 y el 10/08/23

1. Perfil de amenaza: ransomware Rhysida.
https://socradar.io/threat-profile-rhysida-ransomware/

2. Cado Security Labs descubre un nuevo malware, el Redis P2Pinfect, que actúa como botnet.
https://www.cadosecurity.com/redis-p2pinfect/

3. Nueva variante de malware SkidMap Linux dirigida a servidores Redis vulnerables.
https://thehackernews.com/2023/08/new-skidmap-redis-malware-variant.html

4. Clop ransomware ahora usa torrents para filtrar datos y evadir derribos.
https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/

5. Amenaza de ciberataques a la seguridad nacional de Reino Unido vs seguridad de las armas químicas.
https://www.itpro.com/security/cyber-attacks/threat-of-cyber-attacks-to-national-security-compared-to-that-of-chemical-weapons

6. Nueva campaña de malware dirigida a ciberdelincuentes sin experiencia con configuraciones de OpenBullet.
https://thehackernews.com/2023/08/new-malware-campaign-targets.html

7. El grupo 8BASE Ransomware realiza ataques cibernéticos arbitrarios y recluta a 7 nuevas organizaciones como víctimas.
https://thecyberexpress.com/8base-ransomware-group-cyber-attack-series/

8. Los ataques de ransomware a organizaciones industriales se duplicaron el año pasado: Informe.
https://www.securityweek.com/ransomware-attacks-on-industrial-organizations-doubled-in-past-year-report/

9. Incremento de las extensiones maliciosas de Chrome que atacan a Latinoamérica.
https://securityintelligence.com/posts/rise-of-malicious-chrome-extensions-targeting-latin-america/

10. Los ciberdelincuentes utilizan cada vez más el kit de phishing de EvilProxy para atacar a los ejecutivos.
https://thehackernews.com/2023/08/cybercriminals-increasingly-using.html

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

1. Seis pasos para proteger el software del gobierno en medio de amenazas crecientes.
https://www.c4isrnet.com/opinions/2023/08/01/six-steps-to-safeguarding-government-software-amid-rising-threats/

2. Los investigadores observaron actores de amenazas que utilizan un rootkit de código abierto llamado Reptile en ataques dirigidos a sistemas en Corea del Sur.
https://securityaffairs.com/149203/malware/reptile-rootkit-south-korea.html

3. Preguntas frecuentes: ¿Cómo funciona la reversión del ransomware Malwarebytes?
https://www.malwarebytes.com/blog/business/2023/08/faq-how-does-malwarebytes-ransomware-rollback-work

4. Cómo eliminar Akira Ransomware y descifrar archivos .akira.
https://www.bugsfighter.com/es/remove-akira-ransomware-and-decrypt-akira-files/

5. La parte más importante de Internet de la que probablemente nunca hayas oído hablar.
https://www.cisa.gov/news-events/news/most-important-part-internet-youve-probably-never-heard

NOTAS DE INTERÉS

1. Zenbleed: cómo la búsqueda del rendimiento de la CPU podría poner en riesgo sus contraseñas.
https://nakedsecurity.sophos.com/2023/07/26/zenbleed-how-the-quest-for-cpu-performance-could-put-your-passwords-at- risk/

2. El Instituto de Ciberseguridad avisa: tu suscripción a Netflix no ha caducado; es un "phishing".
https://efe.com/ciencia-y-tecnologia/2023-08-02/aviso-suscripcion-netflix-phishing/

3. El CISO de Zoom, Michael Adams, analiza las amenazas de ciberseguridad, las soluciones y el futuro.
https://www.helpnetsecurity.com/2023/08/07/michael-adams-zoom-ciso-cybersecurity/

4. Una semana en seguridad (31 de julio - 6 de agosto). https://www.malwarebytes.com/blog/news/2023/08/a-week-in-security-july-31-august-06

5. Notificación pública de ciberataque a los sistemas de la Comisión Electoral en Reino Unido.
https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems

6. Plan Estratégico CISA: Cambiando el Arco del Riesgo Nacional de USA para crear un Futuro más Seguro.
https://www.cisa.gov/news-events/news/cisa-cybersecurity-strategic-plan-shifting-arc-national-risk-create-safer-future

ACTUALIZACIONES DE SEGURIDAD

1. Martes de Actualizaciones de Microsoft. Guía de actualización de seguridad.
https://msrc.microsoft.com/update-guide/

2. CVE-2023-38180 afecta a .NET y Visual Studio puede desencadenar una DoS.
https://securityaffairs.com/149382/security/cisa-known-exploited-vulnerabilities-catalog-cve-2023-38180.html

3. Firefox corrige una serie de fallas en el primero de los dos lanzamientos de este mes. (CVE-2023-4045, CVE-2023-4047, CVE-2023-4048, CVE-2023-4050, CVE-2023-4051, CVE-2023-4057,CVE-2023-4058)
https://nakedsecurity.sophos.com/2023/08/01/firefox-fixes-a-flurry-of-flaws-in-the-first-of-two-releases-this-month/

4. CISA: Resumen de vulnerabilidades del 24 de julio de 2023. Publicado el 31 de julio de 2023.
https://www.cisa.gov/news-events/bulletins/sb23-212

5. Vulnerabilidades relacionadas con la escalada de privilegios locales en Ubuntu Linux afectan al 40% de las "workloads" en la nube construidas con este SO. (CVE-2023-2640 Y CVE-2023-32629)
https://www.wiz.io/blog/ubuntu-overlayfs-vulnerability

6. PaperCut corrige el error que puede conducir a RCE, ¡actualice rápidamente! (CVE-2023-39143)
https://www.helpnetsecurity.com/2023/08/07/cve-2023-39143/

7. Fortinet anuncia una actualización de seguridad para FortiOS.
https://www.fortiguard.com/psirt