@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. 203 – 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 11/2/23 y el 24/2/23

1. 1,000 sitios han sido infectados con malware que posee buena capacidad para evitar ser detectado.
   https://arstechnica.com/information-technology/2023/02/sneaky-malware-infecting-11000-sites-is-redirecting-visitors-to-scam-pages/

2. El Instituto Tecnológico de Israel Technion sufrió un ataque de ransomware.
   https://securityaffairs.com/142160/hacking/israeli-technion-suffered-ransomware-attack.html

3. Kaspersky alerta por troyano en ChatGPT falso.
   https://latam.kaspersky.com/about/press-releases/2023_nuevo-malware-roba-credenciales-de-redes-sociales-haciendose-pasar-por-app-de-chatgpt-advierte-kaspersky

4. Correos electrónicos militares de EE. UU. expuestos a través de una cuenta en la nube.
   https://www.darkreading.com/cloud/us-military-emails-exposed-via-cloud-account

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

1. Ciberdelincuentes monitorean los escritorios de las víctimas con Screenshotter.
   https://thehackernews.com/2023/02/hackers-targeting-us-and-german-firms.html

2. Honeypot-Factory: El uso del engaño en entornos de sistemas de control industrial (ICS) y tecnología operativa (OT).
   https://thehackernews.com/2023/02/honeypot-factory-use-of-deception-in.html

3. 11 países participan en un ejercicio militar de ciberguerra.
   https://www.securityweek.com/11-countries-take-part-in-military-cyberwarfare-exercise/

4. Planifica ahora para evitar un fallo de comunicación tras un ciberataque.
   https://www.csoonline.com/article/3687808/the-role-of-cisos-in-the-communication-response-following-an-incident.html

5. Construyendo el camino hacia la resiliencia cibernética: Explorando el Informe de defensa digital de Microsoft.
   https://www.csoonline.com/article/3687218/building-the-path-to-cyber-resilience-exploring-the-microsoft-digital-defense-report.html

6. La mayoría de las empresas toman decisiones de ciberseguridad sin información del atacante.
   https://www.infosecurity-magazine.com/news/cybersecurity-decisions-without/

7. GnuTLS corrige el error de ataque de sincronización.
   https://nakedsecurity.sophos.com/2023/02/13/serious-security-gnutls-follows-openssl-fixes-timing-attack-bug/

8. La ciberseguridad da un salto con herramientas y técnicas de IA.
   https://www.helpnetsecurity.com/2023/02/20/cybersecurity-ai-tools-techniques/

9. 10 herramientas de monitoreo de la dark web.
   https://www.csoonline.com/article/3688550/10-dark-web-monitoring-tools.html

10. ¿Qué es el Protocolo de Semáforo TLC? Así es como ayuda a los CISO a compartir datos sobre amenazas.
https://www.csoonline.com/article/3688554/what-is-traffic-light-protocol-and-how-it-supports-cisos-to-share-threat-data.html

NOTAS DE INTERÉS

1. Australia eliminará las cámaras de vigilancia chinas en medio de temores de seguridad.
https://www.bbc.com/news/world-australia-64577641

2. El misterio rodea los objetos derribados por el ejército de EE. UU.
https://www.bbc.com/news/world-us-canada-64620064

3. Muchas operaciones cibernéticas contra Ucrania y miembros de la OTAN aún no se han hecho públicas.
https://securityaffairs.com/142603/cyber-warfare-2/russia-cyber-operations-ukriane-nato.html

4. Lecciones de ciberguerra de la contienda en Ucrania.
https://www.schneier.com/blog/archives/2023/02/cyberwar-lessons-from-the-war-in-ukraine.html

5. Las estaciones de radio rusas emiten una advertencia de ataque aéreo "falsa" después del "hackeo".
https://news.sky.com/story/russian-radio-stations-play-out-fake-air-raid-warning-after-hack-kremlin-officials-claim-12817070

6. ¿ChatGPT podría llegar a utilizarse para escribir malware?
https://www.welivesecurity.com/la-es/2023/02/22/chatgpt-podria-utilizarse-escribir-malware/

7. Cloudflare bloquea un ataque DDoS récord de 71 millones de RPS.
https://www.bleepingcomputer.com/news/security/cloudflare-blocks-record-breaking-71-million-rps-ddos-attack/

8. Mi administrador de contraseñas fue hackeado: Cómo prevenir una catástrofe.
https://www.bleepingcomputer.com/news/security/my-password-manager-was-hacked-how-to-prevent-a-catastrophe/

9. La UE respalda el plan de tecnología publicitaria de las empresas de telecomunicaciones.
https://telecom.economictimes.indiatimes.com/news/eu-backs-telecom-firms-ad-tech-plan/97875168

ACTUALIZACIONES DE SEGURIDAD

1. Microsoft lanza actualizaciones de seguridad de febrero de 2023.
https://www.cisa.gov/uscert/ncas/current-activity/2023/02/14/microsoft-releases-february-2023-security-updates

2. Apple lanza actualizaciones de seguridad para varios productos.
https://www.cisa.gov/uscert/ncas/current-activity/2023/02/14/apple-releases-security-updates-multiple-products

3. Cisco publica avisos de seguridad para varios productos.
https://www.cisa.gov/uscert/ncas/current-activity/2023/02/16/cisco-releases-security-advisories-multiple-products

4. VMware corrige un fallo crítico en Carbon Black App Control (CVE-2023-20858).
https://www.helpnetsecurity.com/2023/02/22/cve-2023-20858/

5. Apple corrige el nuevo WebKit de día cero explotado para hackear iPhones, Macs.
https://www.bleepingcomputer.com/news/security/apple-fixes-new-webkit-zero-day-exploited-to-hack-iphones-macs/

6. Vulnerabilidad crítica de RCE descubierta en el software antivirus de código abierto ClamAV.
https://thehackernews.com/2023/02/critical-rce-vulnerability-discovered.html