Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 213 – 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 28/08/23 y el 25/09/23

1. La multinacional Clorox Company admite que un ciberataque está causando trastornos a gran escala.
https://www.theregister.com/2023/09/19/the_clorox_company_admits_cyber/

2. Espías chinos infectaron docenas de redes con malware para memorias USB.
https://www.wired.com/story/china-usb-sogu-malware/

3. La NSA, el FBI, el CISA y sus socios japoneses publican sobre los ciberactores vinculados a la RPC.
https://www.cisa.gov/news-events/alerts/2023/09/27/nsa-fbi-cisa-and-japanese-partners-release-advisory-prc-linked-cyber-actors

4. La APT28, respaldada por Rusia, intentó atacar una instalación de energía crítica ucraniana.
https://www.infosecurity-magazine.com/news/russia-apt28-attack-ukraine-power/

5. Atacantes accedieron a datos militares británicos a través de la plataforma Windows 7 de una empresa de vallas de alta seguridad.
https://www.theregister.com/2023/09/04/zaun_breach_windows_7/

6. Los agentes de amenazas, UNC4841, penetraron en servidores de correo electrónico del gobierno de EE.UU., aprovechando el día cero de Barracuda ESG.
https://securityaffairs.com/150055/apt/barracuda-esg-us-gov-server.html

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

1. Análisis del código de una nueva variante del Gusano X (Xworm).
https://thehackernews.com/2023/09/inside-code-of-new-xworm-variant.html

2. El grupo de ransomware "Snatch" expone las direcciones IP de los usuarios que los visitan.
https://krebsonsecurity.com/2023/09/snatch-ransom-group-exposes-visitor-ip-addresses/

3. Origen de contraseñas de honeypots y nombres de usuario más comunes.
https://isc.sans.edu/diary/Common%20usernames%20submitted%20to%20honeypots/30188

4. Cómo evitar que ChatGPT robe contenido y tráfico de una red.
https://thehackernews.com/2023/08/how-to-prevent-chatgpt-from-stealing.html

5. MITRE y CISA publican una herramienta de código abierto para la emulación de ataques OT.
https://www.securityweek.com/mitre-and-cisa-release-open-source-tool-for-ot-attack-emulation/

6. Los ciberataques revelan verdades incómodas sobre las defensas estadounidenses
https://www.c4isrnet.com/opinion/2023/09/21/cyber-attacks-reveal-uncomfortable-truths-about-us-defenses/

7. Conclusiones del ciberataque en Colombia: impacto y lecciones aprendidas.
https://www.enter.co/empresas/seguridad/conclusiones-del-ciberataque-en-colombia-impacto-y-lecciones-aprendidas/

NOTAS DE INTERÉS

1. El nuevo backdoor para Linux SprySOCKS de Earth Lusca está enfocado a entidades gubernamentales
https://thehackernews.com/2023/09/earth-luscas-new-sprysocks-linux.html

2. Operación Rusty Flag: Azerbaiyán en el blanco de una nueva campaña de malware basado en Rust.
https://thehackernews.com/2023/09/operation-rusty-flag-azerbaijan.html

3. Son informadas 10 nuevas vulnerabilidades, por Talos, incluido un problema de uso después de la liberación en Google Chrome.
https://blog.talosintelligence.com/vulnerability-roundup-sept-27-23/

4. Ciberdelincuentes atacan servidores MS SQL para distribuir ransomware.
https://www.helpnetsecurity.com/2023/09/06/ms-sql-cyberattack/

5. Cómo optimizar la seguridad del Internet de las cosas mientras se promueve la innovación.
https://www.c4isrnet.com/opinion/2023/09/20/how-to-optimize-internet-of-things-security-while-promoting-innovation/

6. Qué significa la nueva política federal de ciberseguridad para los contratistas gubernamentales.
https://www.c4isrnet.com/opinion/2023/09/11/what-new-federal-cybersecurity-policy-means-for-government-contractors/

ACTUALIZACIONES DE SEGURIDAD

1. Se ha resuelto "día cero" de Android con las actualizaciones de seguridad de septiembre de 2023.
https://www.securityweek.com/android-zero-day-patched-with-september-2023-security-updates/

2. Martes de actualizaciones de septiembre de 2023
https://www.ivanti.com/blog/september-2023-patch-tuesday

3. Cisco lanzó actualizaciones de seguridad para una falla de día cero explotada activamente (CVE-2023-20109) que reside en la función GET VPN del software IOS e IOS XE.
https://securityaffairs.com/151647/hacking/cisco-cve-2023-20109-actively-exploited.html