Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 205 – 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 11/3/23 y el 21/4/23

1. Ferrari informa que un ataque de ransomware expuso datos de clientes
https://www.securityweek.com/ferrari-says-ransomware-attack-exposed-customer-data/

2. Cómo Zero Trust cambió el curso de la ciberseguridad.
https://securityintelligence.com/articles/how-zero-trust-changed-cybersecurity/

3. Un nuevo malware, apodado Domino, desarrollado por el grupo de ciberdelincuentes FIN7 ha sido utilizado por la banda de ransomware Conti, ya desaparecida.
https://securityaffairs.com/144943/cyber-crime/relationships-fin7-conti-ransomware.html

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

1. Por qué no debe compartir datos con su proveedor de telefonía móvil.
https://krebsonsecurity.com/2023/03/why-you-should-opt-out-of-sharing-data-with-your-mobile-provider/

2. DataSurgeon (ds) es una herramienta versátil diseñada para la respuesta a incidentes y las pruebas de penetración.
https://www.darknet.org.uk/2023/03/datasurgeon-extract-sensitive-information-pii-from-logs/

3. Bad magic: nueva APT identificada en la zona del conflicto ruso-ucraniano.
https://securelist.com/bad-magic-apt/109087/

4. Lo que TikTok sabe de usted y lo que usted debería saber de TikTok.
https://www.welivesecurity.com/2023/03/24/what-tiktok-knows-you-should-know-tiktok/

5. Seis fases del mundo post-GPT.
https://danielmiessler.com/blog/6-phases-post-gpt-world/

NOTAS DE INTERÉS

1. España necesita más transparencia sobre Pegasus: Legisladores de la Unión Europea.
https://www.securityweek.com/spain-needs-more-transparency-over-pegasus-eu-lawmakers/

2. Están empezando a atacar a los desarrolladores de .NET con paquetes NuGet de código malicioso.
https://jfrog.com/blog/attackers-are-starting-to-target-net-developers-with-malicious-code-nuget-packages/

3. Ataque masivo de ransomware.
https://www.schneier.com/blog/archives/2023/03/mass-ransomware-attack.html

4. Cisco parchea vulnerabilidades de alta gravedad en el software IOS.
https://www.securityweek.com/cisco-patches-high-severity-vulnerabilities-in-ios-software/

5. Un grupo avanzado tiene como objetivo Fortinet FortiOS en ataques a entidades gubernamentales.
https://securityaffairs.com/143458/hacking/attacks-fortinet-fortios.html

6. Microsoft publica las actualizaciones de seguridad de marzo de 2023.
https://www.cisa.gov/news-events/alerts/2023/03/14/microsoft-releases-march-2023-security-updates

7. Microsoft lanza parches para 80 vulnerabilidades, 2 0-day(s)
https://unaaldia.hispasec.com/2023/03/microsoft-lanza-parches-para-80-vulnerabilidades-2-0-days.html

8. Europol advierte sobre el uso delictivo de ChatGPT.
https://securityaffairs.com/144132/cyber-crime/europol-warns-cybercrime-chatgpt.html

9. El sector de la energía nuclear de China es objetivo de una campaña de ciberespionaje.
https://www.securityweek.com/chinas-nuclear-energy-sector-targeted-in-cyberespionage-campaign/

10. El grupo APT Winter Vivern aprovecha un error del correo web de Zimbra para atacar a entidades gubernamentales.
https://www.csoonline.com/article/3692249/apt-group-winter-vivern-exploits-zimbra-webmail-flaw-to-target-government-entities.html

11. Cómo proteger su dispositivo móvil: 8 consejos para 2023.
https://www.tripwire.com/state-of-security/secure-mobile-device-six-steps

12. Hackers pakistaníes utilizan el malware Poseidon para Linux con el fin de atacar a agencias gubernamentales indias.
https://thehackernews.com/2023/04/pakistani-hackers-use-linux-malware.html

13. La APT28 aprovecha una vulnerabilidad conocida para llevar a cabo tareas de reconocimiento y desplegar malware en routers Cisco.
https://www.cisa.gov/news-events/alerts/2023/04/18/apt28-exploits-known-vulnerability-carry-out-reconnaissance-and-deploy-malware-cisco-routers

ACTUALIZACIONES DE SEGURIDAD

1. Apple actualiza a iPhones y iPads antiguos la corrección de un fallo de WebKit (CVE-2023-23529) y +.
https://nakedsecurity.sophos.com/2023/03/28/apple-patches-everything-including-a-zero-day-fix-for-ios-15-users/

2. Actualizaciones de Mozilla, Fortinet, Apple y Microsoft de abril de 2023
https://www.cisa.gov/news-events/alerts/2023/04/11/mozilla-releases-security-advisories-multiple-products

3. Una vez más, se han encontrado vulnerabilidades muy graves en los sistemas operativos de Apple.
https://www.kaspersky.com/blog/ios-macos-vulnerabilities-april-2023/47938/

4. Google corrige otro día cero de Chrome que se explota activamente.
https://www.bleepingcomputer.com/news/security/google-patches-another-actively-exploited-chrome-zero-day/