Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 179 – Año 2022

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 08/08/22 y el 21/08/22

- Proveedor de la industria automovilística fue atacado por tres bandas de ransomware en dos semanas.
  https://www.bleepingcomputer.com/news/security/automotive-supplier-breached-by-3-ransomware-gangs-in-2-weeks/
- Cisco confirma la violación de la red a través de la cuenta de Google de un empleado hackeado.
  https://threatpost.com/cisco-network-breach-google/180385/
- **Satélite de Starlink fue hackeado con éxito usando un modchip de 25 dólares.**
  https://threatpost.com/starlink-hack/180389/
- Proveedor de agua del Reino Unido sufre un ataque del ransomware Clop.
  https://threatpost.com/water-supplier-hit-clop-ransomware/180422/
- Unos 1.900 números de teléfono de usuarios de Signal son expuestos por el phishing a Twilio.
  https://arstechnica.com/information-technology/2022/08/twilio-phishing-attack-exposes-phone-numbers-for-1900-signal-users/

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

- Cómo los hackers están robando tarjetas de crédito de los sitios de anuncios clasificados.
  https://www.bleepingcomputer.com/news/security/how-hackers-are-stealing-credit-cards-from-classifieds-sites/
- Descubren detalles sobre el ataque de ransomware de Maui por parte de hackers norcoreanos.
  https://thehackernews.com/2022/08/experts-uncover-details-on-maui.html
- **Los chips de Intel, APIC/EPIC, filtran secretos que incluso el kernel no debería ver.**
  https://nakedsecurity.sophos.com/2022/08/10/apic-epic-intel-chips-leak-secrets-even-the-kernel-shouldnt-see/
- **El instalador de Zoom permitió a un investigador hackear el acceso a la raíz en macOS.**
  https://www.theverge.com/2022/8/12/23303411/zoom-defcon-root-access-privilege-escalation-hack-patrick-wardler
- El troyano bancario SOVA para Android regresa con nuevas capacidades y objetivos.
  https://thehackernews.com/2022/08/sova-android-banking-trojan-returns-new.html
- Herramienta de ataque USB "Rubber Ducky".
  https://www.schneier.com/blog/archives/2022/08/usb-rubber-ducky-attack-tool.html
- El grupo TA558 tiene como objetivo las organizaciones de hostelería, hoteles y viajes
  https://securityaffairs.co/wordpress/134622/cyber-crime/ta558-targets-hospitality-travel.html
- Un malspam en Brasil impulsa el malware Astaroth (Guildma).
  https://isc.sans.edu/diary/rss/28962

- CISA añade 7 vulnerabilidades a la lista de fallos explotados por los hackers.
  https://www.bleepingcomputer.com/news/security/cisa-adds-7-vulnerabilities-to-list-of-bugs-exploited-by-hackers/
- El malware bancario Grandoreiro se centra en fabricantes de España y México.
  https://www.bleepingcomputer.com/news/security/grandoreiro-banking-malware-targets-manufacturers-in-spain-mexico/
- **Un archivo ZIP encriptado puede tener dos contraseñas correctas. Aquí se explica el porqué.**
  https://www.bleepingcomputer.com/news/security/an-encrypted-zip-file-can-have-two-correct-passwords-heres-why/

NOTAS DE INTERÉS

- Un bug de día cero es el responsable de la masiva brecha en Twitter.
  https://www.infosecurity-magazine.com/news/zeroday-bug-responsible-massive/
- Red de bots Orchard usa datos de la cuenta del fundador de Bitcoin para generar dominios falsos.
  https://thehackernews.com/2022/08/new-orchard-botnet-uses-bitcoin.html
- La herramienta colaborativa Slack admite que filtró contraseñas durante cinco años.
  https://nakedsecurity.sophos.com/2022/08/08/slack-admits-to-leaking-hashed-passwords-for-three-months/
- 10 paquetes de código malicioso se infiltran en el repositorio de PyPI.
  https://securityaffairs.co/wordpress/134253/malware/pypi-malicious-packages-3.html
- **Meta inyecta código en los sitios web para rastrear a sus usuarios, según una investigación.**
  https://www.theguardian.com/technology/2022/aug/11/meta-injecting-code-into-websites-visited-by-its-users-to-track-them-research-says
- Los teléfonos Xiaomi con chips MediaTek son vulnerables a la falsificación de pagos.
  https://thehackernews.com/2022/08/xiaomi-phones-with-mediatek-chips-found.html
- **El Pentágono pone a prueba la tecnología de microrredes en la DEF CON, usando el ingenio de los hackers que participan del evento.**
  https://www.cyberscoop.com/pentagon-hackers-secure-the-microgrid/
- El APT41, respaldado por China, atacó a 13 organizaciones en todo el mundo el año pasado.
  https://thehackernews.com/2022/08/china-backed-apt41-hackers-targeted-13.html
- La herramienta "Oculus" rusa, usará la IA para escanear sitios en busca de información prohibida.
  https://www.bleepingcomputer.com/news/security/russias-oculus-to-use-ai-to-scan-sites-for-banned-information/

ACTUALIZACIONES DE SEGURIDAD

- El parche del martes de agosto de 2022 de Microsoft corrige un día cero explotado y 121 fallos.
  https://thehackernews.com/2022/08/microsoft-issues-patches-for-121-flaws.html
- **Kali Linux 2022.3 añade 5 nuevas herramientas, actualiza el núcleo de Linux, y más.**
  https://www.bleepingcomputer.com/news/security/kali-linux-20223-adds-5-new-tools-updates-linux-kernel-and-more/
- **VMware presenta actualizaciones de seguridad.**
  https://www.cisa.gov/uscert/ncas/current-activity/2022/08/09/vmware-releases-security-updates
- Zoom para Mac parchea un error crítico.
  https://nakedsecurity.sophos.com/2022/08/15/zoom-for-mac-patches-get-root-bug-update-now/
- Google corrige el quinto fallo de día cero de Chrome detectado este año.
  https://www.bleepingcomputer.com/news/security/google-fixes-fifth-chrome-zero-day-bug-exploited-this-year/
- Apple publica actualización de seguridad para parchear dos nuevas vulnerabilidades de día cero.
  https://techcrunch.com/2022/08/17/iphone-ipad-mac-zero-days/