@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. 171 – 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 10/6/22 y el 16/6/22

- Una filtración en la Fundación Kaiser, en Washington, expone los datos de 70.000 pacientes.
  https://www.darkreading.com/attacks-breaches/kaiser-permanente-breach-exposes-70k-patients-data
- Cloudflare sufrió un ataque DDoS que batió el récord de 26 millones de peticiones por segundo.
  https://thehackernews.com/2022/06/cloudflare-saw-record-breaking-ddos.html
- La banda DragonForce desencadena ataques contra el Gobierno de la India.
  https://threatpost.com/hackers-india-government/179968/
- Una banda ransomware extorsiona a Shoprite, la mayor cadena de supermercados de África.
  https://www.bleepingcomputer.com/news/security/extortion-gang-ransoms-shoprite-largest-supermarket-chain-in-africa/

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

- Investigadores detallan cómo los ciberdelincuentes se dedican a los usuarios de criptodivisas.
  https://thehackernews.com/2022/06/researchers-detail-how-cyber-criminals.html
- **Fuerza bruta práctica del cifrado de grado militar AES-1024.**
  https://research.kudelskisecurity.com/2022/05/11/practical-bruteforce-of-aes-1024-military-grade-encryption/
- Han descubierto que las señales de Bluetooth pueden tomarse como huellas dactilares para rastrear los teléfonos inteligentes.
  https://thehackernews.com/2022/06/researchers-find-bluetooth-signals-can.html
- **Investigadores del MIT descubren un nuevo fallo en las CPUs M1 de Apple que no se puede parchear.**
  https://thehackernews.com/2022/06/mit-researchers-discover-new-flaw-in.html
- Los hackers iraníes se centran en el sector energético con una nueva puerta trasera DNS.
  https://www.bleepingcomputer.com/news/security/iranian-hackers-target-energy-sector-with-new-dns-backdoor/
- Grupos de amenaza chinos patrocinados por el Estado comprometen a los proveedores de servicios de telecomunicaciones y de red.
  https://www.techrepublic.com/article/chinese-compromise-telecommunications/
- **Los hackers rusos comienzan a atacar a Ucrania con los exploits Follina.**
  https://securityaffairs.co/wordpress/132227/apt/cert-ua-sandworm-follina-rce.html
- El rootkit Syslogk para Linux utiliza paquetes inteligentes para activar una puerta trasera.
  https://securityaffairs.co/wordpress/132232/malware/syslogk-linux-rootkit.html
- Los hackers clonan las carteras móviles de Coinbase y MetaMask para robar criptomonedas.
  https://www.bleepingcomputer.com/news/security/hackers-clone-coinbase-metamask-mobile-wallets-to-steal-your-crypto/

- Investigadores describen el cargador PureCrypter que utilizan los ciberdelincuentes para distribuir malware.
https://thehackernews.com/2022/06/researchers-detail-purecrypter-loader.html

- **La reciente vulnerabilidad detectada en el correo electrónico Zimbra podría permitir a los atacantes robar las credenciales de inicio de sesión.**
https://thehackernews.com/2022/06/new-zimbra-email-vulnerability-could.html

- **Nuevo ataque de canal lateral conocido como Hertzbleed, permite a los atacantes remotos robar claves criptográficas completas observando las variaciones en la frecuencia de la CPU.**
https://www.bleepingcomputer.com/news/security/new-hertzbleed-side-channel-attack-affects-intel-amd-cpus/

NOTAS DE INTERÉS

- **Rusia: Los ciberataques podrían intensificar el conflicto militar.**
https://www.infosecurity-magazine.com/news/russia-cyberattacks-escalate/

- Una potente variante de Emotet se propaga a través de credenciales de correo electrónico robadas.
https://threatpost.com/potent-emotet-variant-spreads-via-stolen-email-credentials/179932/

- **Los servicios de agua de Estados Unidos son el principal objetivo de los ciberataques.**
https://threatpost.com/water-cyberattack-target/179935/

- El nuevo backdoor ultra sigiloso de Linux no es el típico descubrimiento de malware.
https://arstechnica.com/information-technology/2022/06/novel-techniques-in-never-before-seen-linux-backdoor-make-it-ultra-stealthy/

- **HTTP/3 evoluciona hacia el RFC 9114, una ventaja de seguridad, pero no sin desafíos.**
https://portswigger.net/daily-swig/http-3-evolves-into-rfc-9114-a-security-advantage-but-not-without-challenges

- Los hackers chinos "Gallium" utilizan el reciente malware PingPull en ataques de ciberespionaje.
https://thehackernews.com/2022/06/chinese-gallium-hackers-using-new.html

- Internet Explorer emite su último byte el miércoles 15 de junio.
https://www.bleepingcomputer.com/news/microsoft/internet-explorer-almost-breathes-its-final-byte-on-wednesday/

- Un novedoso botnet y criptominero denominado Panchan, ataca a los servidores Linux.
https://www.techrepublic.com/article/botnet-panchan-attacking-server/

- El malware 'MaliBot' para Android roba información financiera y personal.
https://www.securityweek.com/malibot-android-malware-steals-financial-personal-information

- Función de Microsoft 365 deja los archivos de SharePoint y OneDrive abiertos a ransomware.
https://www.darkreading.com/vulnerabilities-threats/office-365-files-stored-in-the-cloud-vulnerable-to-ransomware-encryption

ACTUALIZACIONES DE SEGURIDAD

- Metasploit 6.2.0, el marco de pruebas de penetración más utilizado del mundo, viene con 138 nuevos módulos, 148 mejoras y características
https://www.helpnetsecurity.com/2022/06/13/metasploit-6-2-0-released/

- Martes de parches de Microsoft de junio de 2022. Repara el bug Follina.
https://isc.sans.edu/forums/diary/Microsoft+June+2022+Patch+Tuesday/28742/

- Ubuntu Core 22: Está disponible el S.O. de IoT seguro y centrado en las aplicaciones.
https://www.helpnetsecurity.com/2022/06/15/canonical-ubuntu-core-22/