@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. 169 – 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 27/5/22 y el 2/6/22

- El ransomware BlackCat/ALPHV pide 5 millones de dólares para desbloquear el estado de Carinthia de Austria.
  https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-asks-5-million-to-unlock-austrian-state/
- Un hacker accede a una base de datos de empleados de Verizon e intenta pedir un rescate de 250.000 dólares.
  https://www.theverge.com/2022/5/27/23144418/hacker-verizon-employee-database
- **Italia advierte a las organizaciones que se preparen para los próximos ataques DDoS.**
  https://www.bleepingcomputer.com/news/security/italy-warns-organizations-to-brace-for-incoming-ddos-attacks/
- La agencia de salud pública de Costa Rica es afectada por el ransomware Hive.
  https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/

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

- Los atacantes pueden utilizar señales electromagnéticas para controlar las pantallas táctiles de forma remota.
  https://thehackernews.com/2022/05/attackers-can-use-electromagnetic.html
- Una nueva variante del malware Chaos cambia el borrado por la encriptación.
  https://www.darkreading.com/threat-intelligence/chaos-yashma-variant--wiper-encryption
- CISA publica el Plan del Proceso de Evaluación de la Seguridad 5G.
  https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf
- El malware *Windows Subsystem* para Linux, roba las cookies de autentificación del navegador.
  https://www.bleepingcomputer.com/news/security/new-windows-subsystem-for-linux-malware-steals-browser-auth-cookies/
- **La red de bots Linux EnemyBot aprovecha ahora las vulnerabilidades de los servidores web, Android y CMS.**
  https://thehackernews.com/2022/05/enemybot-linux-botnet-now-exploits-web.html
- **Listado de las violaciones de datos y ciberataques en mayo de 2022.**
  https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-may-2022-49-8-million-records-breached
- Neutralización de nuevos ataques Trickbot con IA.
  https://www.darkreading.com/dr-tech/neutralizing-novel-trickbot-attacks-with-ai
- **Ataques con bombas lógicas: 4 ejemplos famosos.**
  https://www.csoonline.com/article/2115905/logic-bomb.html

- Alerta de CISA y análisis del Grupo de extorsión de datos Karakurt.
https://www.cisa.gov/uscert/ncas/alerts/aa22-152a
- ¿Qué pasaría si el ransomware evolucionara y afectara al IoT en la empresa?
https://www.theregister.com/2022/06/01/ransomware_iot_devices/
- Desarrollan un ransomware para dispositivos IoT que se dirige a las redes de TI y OT.
https://thehackernews.com/2022/06/researchers-demonstrate-ransomware-for.html

NOTAS DE INTERÉS

- El CISA añade 75 bugs que son activamente utilizados, a su lista de parches imprescindibles en sólo una semana.
https://www.zdnet.com/article/cisa-adds-75-actively-exploited-bugs-to-its-must-patch-list-in-just-a-week/
- **Nota sobre el robot que camina por control remoto más pequeño de la historia.**
https://news.sky.com/story/meet-the-smallest-ever-remote-controlled-walking-robot-12622380
- El malware ChromeLoader sabotea los navegadores con archivos ISO.
https://www.darkreading.com/application-security/chromeloader-malware-hijacks-browsers-iso-files
- Microsoft encuentra fallos críticos en las aplicaciones preinstaladas en millones de dispositivos Android.
https://thehackernews.com/2022/05/microsoft-finds-critical-bugs-in-pre.html
- **El grupo TA413 chino comienza a explotar la vulnerabilidad de día cero "Follina" de MS Office.**
https://securityaffairs.co/wordpress/131843/apt/china-apt-exploits-follina-flaw.html
- **Más de 3.6 millones de servidores MySQL expuestos en Internet.**
https://www.bleepingcomputer.com/news/security/over-36-million-mysql-servers-found-exposed-on-the-internet/
- El malware EnemyBot añade fallas empresariales al arsenal de exploits.
https://www.theregister.com/2022/06/01/enemybot-botnet-exploits/
- La nueva versión de la botnet XLoader utiliza la teoría de la probabilidad para ocultar sus servidores.
https://thehackernews.com/2022/06/new-xloader-botnet-version-using.html
- El FBI confisca dominios con datos personales robados.
https://www.darkreading.com/attacks-breaches/domains-dealing-stolen-personal-data-seized-by-feds
- Autoridades internacionales desmontan la red de malware Flubot.
https://threatpost.com/international-authorities-take-down-flubot-malware-network/179825/
- **Millones de *smartphones* económicos con chips UNISOC son vulnerables a ataques de DDoS.**
https://www.securityweek.com/millions-budget-smartphones-unisoc-chips-vulnerable-remote-dos-attacks
- Chats filtrados de Conti confirman su capacidad para realizar ataques basados en firmware.
https://securityaffairs.co/wordpress/131885/hacking/conti-leaked-chat-firmware-attacks.html
- **Hackers militares estadounidenses llevan a cabo operaciones ofensivas en apoyo de Ucrania, afirma el jefe del Mando Cibernético.**
https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139

ACTUALIZACIONES DE SEGURIDAD

- Microsoft comparte la reparación del día cero de Office que ha sido utilizado en ataques.
https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-mitigation-for-office-zero-day-exploited-in-attacks/