@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. 111 – Año 2021

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.

22/06/2021

- **La plataforma en la nube de la OTAN ha sido hackeada.**
  https://www.ehackingnews.com/2021/06/natos-cloud-platform-hacked.html
- Las impresoras Lexmark están expuestas a un día cero de ejecución de código arbitrario.
  https://threatpost.com/lexmark-printers-code-execution-zero-day/167111/
- SonicWall dejó una falla del VPN parcialmente sin parchear en medio de ataques de "día cero".
  https://thehackernews.com/2021/06/sonicwall-left-vpn-flaw-partially.html

23/06/2021

- El ransomware Clop vuelve a la carga tras las recientes detenciones.
  https://www.bleepingcomputer.com/news/security/clop-ransomware-is-back-in-business-after-recent-arrests/
- El ransomware PYSA abre puertas traseras de sedes educativas mediante el RAT ChaChi.
  https://www.bleepingcomputer.com/news/security/pysa-ransomware-backdoors-education-orgs-using-chachi-malware/
- La UE propone una unidad cibernética conjunta ante el aumento de los ataques.
  https://www.infosecurity-magazine.com/news/eu-proposes-joint-cyber-unit/
- La ciudad belga de Lieja es víctima de un ciberataque.
  https://cisomag.eccouncil.org/belgium-city-of-liege-cyberattack/

24/06/2021

- **El pionero del antivirus John McAfee es encontrado muerto en una cárcel española.**
  https://thehackernews.com/2021/06/antivirus-pioneer-john-mcafee-found.html
- Los errores de ejecución de código de BIOSConnect afectan a millones de dispositivos Dell.
  https://www.zdnet.com/article/biosconnect-code-execution-bugs-impact-millions-of-dell-devices/
- Un ataque a la cadena de suministro podría haber extraído información sensible de Jira, como los problemas de seguridad en la nube de Atlassian, Bitbucket y otros.
  https://threatpost.com/atlassian-bugs-could-have-led-to-1-click-takeover/167203/
- Una marca de moda y una empresa de diagnósticos médicos son las últimas víctimas de REvil.
  https://threatpost.com/fcuk-fashion-medical-diagnostics-revil/167245/

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

- El ransomware DarkRadiation se enfoca en instalaciones de Linux y Docker.
  https://thehackernews.com/2021/06/wormable-darkradiation-ransomware.html
- El tiempo medio para solucionar las vulnerabilidades críticas de ciberseguridad es de 205 días: informe.

https://www.zdnet.com/article/average-time-to-fix-critical-cybersecurity-vulnerabilities-is-205-days-report/

- Misterioso pago de ransomware rastreado hasta un sitio de masajes sensuales. https://www.bleepingcomputer.com/news/security/mysterious-ransomware-payment-traced-to-a-sensual-massage-site/
- Un fallo en la cadena de suministro sin parches afecta a las plataformas 'Pling Store' para usuarios de Linux. https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.html
- **El NIST publica una guía sobre el ransomware.** https://www.infosecurity-magazine.com/news/nist-publishes-ransomware-guidance/ https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf
- Herramienta de MITRE ATT&CK para intercambio Workbench y D3FEND, apoyada por la NSA. https://www.zdnet.com/article/mitre-att-ck-unveils-workbench-sharing-tool-and-nsa-backed-d3fend/

NOTAS DE INTERÉS

- **La evolución de la seguridad de las infraestructuras críticas.** https://www.tripwire.com/state-of-security/ics-security/evolution-of-securing-critical-infrastructure/
- La mayoría de los enlaces de correo electrónico conducen a sitios maliciosos. https://betanews.com/2021/06/22/email-links-malicious-sites/
- Los criptomineros se cuelan en los proyectos de Python. https://threatpost.com/cryptominers-python-supply-chain/167135/
- Splunk lanza productos de seguridad y mejoras en la seguridad de AWS. https://www.techrepublic.com/article/splunk-launches-security-products-and-aws-security-enhancements/
- **Monero se convierte en la criptomoneda preferida por los ciberdelincuentes.** https://arstechnica.com/information-technology/2021/06/monero-emerges-as-crypto-of-choice-for-cybercriminals/
- **Las cadenas de suministro tienen un problema cibernético.** https://www.rand.org/blog/2021/06/supply-chains-have-a-cyber-problem.html
- Binance ayudó a localizar a los que blanqueaban el dinero del ransomware Clop. https://www.bleepingcomputer.com/news/security/binance-exchange-helped-track-down-clop-ransomware-money-launderers/

ACTUALIZACIONES DE SEGURIDAD

- Zephyr RTOS corrige errores de Bluetooth que pueden conducir a la ejecución de código. https://www.bleepingcomputer.com/news/security/zephyr-rtos-fixes-bluetooth-bugs-that-may-lead-to-code-execution/
- Brave ha presentado, 22 de junio, su motor de búsqueda centrado en la privacidad sin rastreo. https://www.bleepingcomputer.com/news/software/brave-launches-its-privacy-focused-no-tracking-search-engine/
- VMware corrigió una vulnerabilidad de alta gravedad en VMware Tools para Windows. https://securityaffairs.co/wordpress/119294/security/vmware-fixes-privilege-escalation-issue-in-vmware-tools-for-windows.html