@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. 68/2021

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.

12/01/2021

- Intel 11th Gen Core vPro CPUs: agrega capacidades de detección de ransomware a nivel del "*hardware*".
  https://www.zdnet.com/article/ces-2021-intel-adds-ransomware-detection-capabilities-at-the-silicon-level/
- Ubiquiti pide a sus clientes de IoT que cambien las contraseñas después de una ruptura de seguridad.
  https://www.zdnet.com/article/ubiquiti-tells-customers-to-change-passwords-after-security-breach/
- Se descubrió una tercera cepa de malware del ataque a la cadena de suministro de SolarWinds.
  https://securityaffairs.co/wordpress/113316/malware/sunspot-solarwinds-attack.html
- Las empresas de energía y metalúrgicas de Colombia bajo una nueva ola de ataques troyanos.
  https://www.zdnet.com/article/colombian-energy-metal-firms-under-fire-from-new-trojan-attack-wave/
  https://thehackernews.com/2021/01/experts-uncover-malware-attacks-against.html
- Mimecast revela el riesgo del certificado SSL 365 de Microsoft.
  https://www.bleepingcomputer.com/news/security/mimecast-discloses-microsoft-365-ssl-certificate-compromise/

13/01/2021

- El mercado de la *dark web* más grande del mundo se cerró después de que ciberpolicías europeos arrestaran a ciudadanos australianos.
  https://www.theregister.com/2021/01/13/darkmarket_europol_shutdown/
- Skype está fuera de servicio en todo el mundo. Microsoft está trabajando para solucionarlo.
  https://www.bleepingcomputer.com/news/microsoft/skype-is-down-worldwide-microsoft-working-on-issues/
- *Hackers* divulgan datos robados de la vacuna Pfizer-BioNTech COVID-19.
  https://threatpost.com/hackers-leak-pfizer-covid-19-vaccine-data/163008/
- Ciberespías iraníes están detrás de la gran campaña navideña de *phishing* por SMS.
  https://www.zdnet.com/article/iranian-cyberspies-behind-major-christmas-sms-spear-phishing-campaign/
- **¡Finalmente terminó! Es hora de desinstalar Adobe Flash Player.**
  https://www.bleepingcomputer.com/news/software/its-finally-over-time-to-uninstall-adobe-flash-player/

14/01/2021

- El servicio de phishing basado en Telegram, Classiscam, golpea los mercados europeos.

https://www.bleepingcomputer.com/news/security/telegram-based-phishing-service-classiscam-hits-european-marketplaces/

- La NSA recomienda usar sólo los ´DNS resolvers´ "designados". https://www.darkreading.com/cloud/nsa-recommends-using-only-designated-dns-resolvers/d/d-id/1339901
- Se hackearon cuentas verificadas de Twitter en la criptoestafa "Elon Musk" por 580 mil dólares. https://www.bleepingcomputer.com/news/security/verified-twitter-accounts-hacked-in-580k-elon-musk-crypto-scam/

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

- Kaspersky Lab hace una autopsia a las pruebas del hacking de SolarWinds. https://www.theregister.com/2021/01/12/solarwinds_russia_kaspersky/
- La APT37 usa la autodescarga para inyectar RokRat. https://exchange.xforce.ibmcloud.com/collection/fe715d42b511f480bf901f344e93bd2b https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-self-decode-technique-to-inject-rokrat
- WhatsApp vs. Signal vs. Telegram vs. Facebook: ¿Qué datos tienen sobre Ud.? Comparaciones. https://www.zdnet.com/article/whatsapp-vs-signal-vs-telegram-vs-facebook-what-data-do-they-have-about-you/ https://securityaffairs.co/wordpress/113354/social-networks/parler-social-media-data-policies-compare.html
- CISA: *hackers* puentearon el MFA para acceder a las cuentas de servicios en la nube. https://www.bleepingcomputer.com/news/security/cisa-hackers-bypassed-mfa-to-access-cloud-service-accounts/

NOTAS DE INTERÉS

- El malware de Mac utiliza AppleScripts de "sólo ejecución" para evadir análisis. https://www.bleepingcomputer.com/news/security/mac-malware-uses-run-only-applescripts-to-evade-analysis/
- La NSA publica el Informe del Año 2020 de la Ciberseguridad. https://www.securityweek.com/nsa-publishes-cybersecurity-year-review-report
- Los expertos dan la alarma sobre el nuevo malware de Android vendido en los foros de hacking. https://thehackernews.com/2021/01/experts-sound-alarm-on-new-android.html
- Google detecta una sofisticada operación de hacking de Windows y Android. https://www.zdnet.com/article/google-reveals-sophisticated-windows-android-hacking-operation/
- Los hackers usaron 4 días cero para infectar dispositivos Windows y Android. https://arstechnica.com/information-technology/2021/01/hackers-used-4-0days-to-infect-windows-and-android-devices/

ACTUALIZACIONES DE SEGURIDAD

- Parches de Microsoft, martes 12 de enero de 2021. *Zero-day* y otras 82 vulnerabilidades. https://msrc.microsoft.com/update-guide/en-us
- Adobe arregla 7 fallas críticas y bloquea el contenido de Flash Player. https://threatpost.com/adobe-critical-flaws-flash-player/162958/