@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. 117 – 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.

13/07/2021

- Hackers iraníes se hicieron pasar por profesores y estudiantes universitarios en un intento de robar contraseñas de correo electrónico.
https://www.zdnet.com/article/these-iranian-hackers-posed-as-academics-in-a-bid-to-steal-email-passwords/

- Se reportan fallas críticas en Etherpad, una popular alternativa a Google Docs.
https://thehackernews.com/2021/07/critical-flaws-reported-in-etherpad.html

- **Los sitios web de la banda de ransomware REvil se tornan inaccesibles, "desaparecen".**
https://www.theguardian.com/technology/2021/jul/13/ransomware-gang-revils-websites-become-unreachable
https://www.zdnet.com/article/revil-websites-down-after-governments-pressured-to-take-action-following-kaseya-attack/

- Hackers chinos aprovechan el último día 0 de SolarWinds en ataques específicos.
https://thehackernews.com/2021/07/chinese-hackers-exploit-latest.html
https://securityaffairs.co/wordpress/120084/apt/china-dev-0322-solarwinds-attacks.html

14/07/2021

- Una actualización del malware Joker actualizado inunda las aplicaciones de Android.
https://threatpost.com/updated-joker-malware-android-apps/167776/

- Ciberdelincuentes detrás de los troyanos bancarios Mekotio y Grandoreiro detenidos en España.
https://thehackernews.com/2021/07/16-cybercriminals-behind-mekotio-and.html

- Google: hackers rusos del SVR atacaron a los usuarios de LinkedIn con un día cero de Safari.
https://www.bleepingcomputer.com/news/security/google-russian-svr-hackers-targeted-linkedin-users-with-safari-zero-day/

- Banda de "*criptojacking*" centrada en Linux es rastreada hasta Rumanía.
https://threatpost.com/linux-cryptojacking-gang-romania/167783/

- SonicWall publica un aviso urgente sobre un "inminente" ransomware dirigido al firmware.
https://www.zdnet.com/article/sonicwall-releases-urgent-notice-about-imminent-ransomware-targeting-firmware/

15/07/2021

- Una campaña a gran escala de ciberespías chinos afecta a entidades de gobiernos asiáticos.
https://thehackernews.com/2021/07/chinas-cyberspies-targeting-southeast.html
https://www.bleepingcomputer.com/news/security/chinese-cyberspies-wide-scale-apt-campaign-hits-asian-govt-entities/

- Las infecciones de malware específicas de IoT se elevaron un 700% en medio de la pandemia.
https://beta.darkreading.com/endpoint/iot-specific-malware-infections-jumped-700-amid-pandemic

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

- El nuevo malware BIOPASS transmite en directo la pantalla del ordenador de la víctima.
https://www.bleepingcomputer.com/news/security/new-biopass-malware-live-streams-victims-computer-screen/
- **El malware Trickbot regresa con un nuevo módulo VNC para espiar a sus víctimas.**
https://thehackernews.com/2021/07/trickbot-malware-returns-with-new-vnc.html
- Cómo Zoom avanzó hacia el cifrado de extremo a extremo.
https://www.kaspersky.com/blog/rsa2021-zoom-end-to-end-encryption/40562/
- Aplicación falsa de Zoom creada por la nueva APT 'LuminousMoth'
https://threatpost.com/zoom-apt-luminous-moth/167822/

NOTAS DE INTERÉS

- La clonación de la voz interesa cada vez más a los actores y a los ciberdelincuentes.
https://www.bbc.com/news/business-57761873
- Modipwn: vulnerabilidad de ejecución de código fue descubierta en los PLCs Modicon de Schneider Electric.
https://www.zdnet.com/article/modipwn-critical-vulnerability-discovered-in-schneider-electric-modicon-plcs/
- A usuarios les robaron 350 mil dólares por falsas aplicaciones de minería de criptomonedas.
https://www.ehackingnews.com/2021/07/350000-stolen-from-users-by-fake.html
- Amazon implementa encriptación en los timbres Ring que produce.
https://www.zdnet.com/article/amazon-rolls-out-encryption-for-ring-doorbells/
- Informe sobre una empresa israelí de software espía vinculada a sitios web falsos de Black Lives Matter y Amnistía.
https://www.theguardian.com/technology/2021/jul/15/spyware-company-impersonates-activist-groups-black-lives-matter

ACTUALIZACIONES DE SEGURIDAD

- SolarWinds parchea un día cero, explotado activamente en la web (CVE-2021-35211).
https://www.helpnetsecurity.com/2021/07/13/solarwinds-patches-zero-day-exploited-in-the-wild-cve-2021-35211/
- Mozilla difunde actualizaciones de seguridad para Firefox.
https://us-cert.cisa.gov/ncas/current-activity/2021/07/13/mozilla-releases-security-updates-firefox
- **El parche del martes de julio de 2021 de Microsoft corrige 9 días cero y 117 errores.**
https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2021-patch-tuesday-fixes-9-zero-days-117-flaws/
https://threatpost.com/microsoft-crushes-116-bugs/167764/
- Las actualizaciones de Adobe corrigen 28 vulnerabilidades en 6 programas.
https://www.bleepingcomputer.com/news/security/adobe-updates-fix-28-vulnerabilities-in-6-programs/
- Nota con lista de actualizaciones de software de julio 2021 de varios empresas.
https://thehackernews.com/2021/07/update-your-windows-pcs-to-patch-117.html