@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. 134 – 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.

Noticias de ciberseguridad entre el 24/09/21 y el 30/09/21

- Los hackers de "Anonymous" afirman haber atacado a una empresa de alojamiento de sitios web popular entre los grupos de extrema derecha
https://www.infosecurity-magazine.com/news/anonymous-hackers-hosting-far-right/
- El ataque ransomware a United Health Centers de California, es reivindicado por Vice Society.
https://www.bleepingcomputer.com/news/security/united-health-centers-ransomware-attack-claimed-by-vice-society/
- Los ciberataques de agosto tuvieron como objetivo una docena de bancos rusos.
https://www.ehackingnews.com/2021/09/the-august-cyber-attacks-targeted-dozen.html
- Un atacante amenaza al gobierno indio con RATs comerciales.
https://www.securityweek.com/threat-actor-targets-indian-government-commercial-rats
- Ataque MSHTML se centra en el Centro Estatal de Cohetes y el Ministerio del Interior de Rusia.
https://www.ehackingnews.com/2021/09/mshtml-attack-targets-russian-state.html
- El gigante del transporte Forward Air informa de una filtración de datos por ransomware.
https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-reports-ransomware-data-breach/

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

- **Google advierte de una nueva forma en que los hackers pueden hacer que el malware sea indetectable en Windows.**
https://thehackernews.com/2021/09/google-warns-of-new-way-hackers-can.html
- SANS: Inventario de dispositivos móviles; ataques de detección automática; iOS 3x0Day; vulnerabilidad CAPWAP de Cisco; parche SMA 100 de Sonicall.
https://isc.sans.edu/podcastdetail.html?id=7688
- Apple Pay con VISA permite a los hackers forzar los pagos en iPhones bloqueados.
https://threatpost.com/apple-pay-visa-hacked-unlocked-iphones/175229/
- Un nuevo defecto permite romper por fuerza bruta la contraseña de Azure Active Directory y no tiene solución.
https://arstechnica.com/information-technology/2021/09/new-azure-active-directory-password-brute-forcing-flaw-has-no-fix/
- **Guía para combatir el ransomware de origen humano: Parte 2.**
https://www.microsoft.com/security/blog/2021/09/27/a-guide-to-combatting-human-operated-ransomware-part-2/
- ¿Qué es un ataque de botnet? Una guía para los profesionales de la seguridad.
https://securityintelligence.com/articles/what-is-botnet-attack/

NOTAS DE INTERÉS

- El malware TangleBot se adentra en las funciones de los dispositivos Android. https://threatpost.com/tanglebot-malware-device-functions/174999/
- Un investigador publica el código fuente de tres *exploits* para iPhone sin parchear. https://www.vice.com/en/article/k78dpx/researcher-publishes-source-code-for-three-unpatched-iphone-exploits
- Las cámaras de seguridad Hikvision, muy utilizadas, son vulnerables al pirateo remoto. https://www.forbes.com/sites/leemathews/2021/09/22/widely-used-hikvision-security-cameras-vulnerable-to-remote-hijacking/
- Unión Europea: Rusia está detrás de la campaña "Ghostwriter" centrada en Alemania. https://threatpost.com/eu-russia-ghostwriter-germany/175025/
- **Hackers descubren una técnica para hacer indetectable el malware en Windows.** https://www.ehackingnews.com/2021/09/hackers-discover-technique-to-make.html
- El grupo "Quad" busca establecer normas de seguridad para la industria tecnológica mundial. https://www.theregister.com/2021/09/27/quad_communqiue_technology_announcements/
- Telegram se está convirtiendo en el paraíso de los ciberdelincuentes. https://securityaffairs.co/wordpress/122609/cyber-crime/telegram-cybercrime.html
- El grupo ruso Turla APT despliega un nuevo backdoor en los sistemas objetivo. https://thehackernews.com/2021/09/russian-turla-apt-group-deploying-new.html
- **Ciberdelincuentes atacan el sistema de pago PIX de Brasil vaciando cuentas bancarias.** https://thehackernews.com/2021/09/hackers-targeting-brazils-pix-payment.html
- Los actores de la amenaza utilizan bots de Telegram para comprometer cuentas de PayPal. https://threatpost.com/telegram-bots-compromise-paypal/175099/
- El nuevo *backdoor* Tomiris fue probablemente desarrollado por hackers de SolarWinds. https://threatpost.com/tomiris-backdoor-solarwinds-malware/175091/
- Facebook publica una nueva herramienta que encuentra fallos de seguridad y privacidad en las aplicaciones de Android. https://thehackernews.com/2021/09/facebook-releases-new-tool-that-finds.html
- **El seguimiento mediante RFID de las armas puede poner en peligro a las tropas.** https://threatpost.com/military-rfid-track-guns-endanger-troops/175260/

ACTUALIZACIONES DE SEGURIDAD

- Cisco publica parches para 3 nuevos fallos críticos que afectan al software IOS XE. https://thehackernews.com/2021/09/cisco-releases-patches-3-new-critical.html
- Apple emparcha otros 3 “días cero” que están bajo ataque activo. https://threatpost.com/apple-patches-zero-days-attack/174988/
- Actualización de Chrome 94 resuelve una vulnerabilidad de día cero utilizada activamente. https://www.securityweek.com/chrome-94-update-patches-actively-exploited-zero-day-vulnerability
- Se publica un exploit para la vulnerabilidad de VMware tras la advertencia de CISA. https://www.zdnet.com/article/exploit-released-for-vmware-vulnerability-after-cisa-warning/