@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. 74/2021

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.

02/02/2021

- Kobalos, un malware para Linux, está pirateando los superordenadores de todo el mundo.
  https://www.zdnet.com/article/this-linux-malware-is-hijacking-supercomputers-across-the-globe/
  https://threatpost.com/kobalos-malware-supercomputers-logins/163604/
  https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/
- Una vulnerabilidad *"zero-day"* de SonicWall está siendo explotada activamente afectando a dispositivos de la serie SMA 100.
  https://www.helpnetsecurity.com/2021/02/02/actively-exploited-sonicwall-zero-day-affects-sma-100-series-appliances/
- El incidente del ransomware Netgain afecta a las administraciones locales en EE.UU.
  https://www.bleepingcomputer.com/news/security/netgain-ransomware-incident-impacts-local-governments/
- El FBI acusó a un detective privado de California del robo de 11 millones de dólares a inversores, con la ayuda del actor Steven Seagal.
  https://threatpost.com/crypto-crook-steven-segal-scam/163612/

03/01/2021

- Se encontraron 3 nuevas vulnerabilidades de seguridad, graves, en el software de SolarWinds.
  https://thehackernews.com/2021/02/3-new-severe-security-vulnerabilities.html
  https://www.infosecurity-magazine.com/news/three-more-vulnerabilities/
- Investigadores del Red Team Research (RTR) de TIM descubrieron 2 nuevas vulnerabilidades de día cero en el plugin de WordPress.
  https://securityaffairs.co/wordpress/114186/hacking/zero-day-wordpress.html

04/02/2021

- La nueva red de bots Matryosh tiene como blanco los sistemas Android.
  https://www.zdnet.com/article/android-devices-ensnared-in-ddos-botnet/
- Se han encontrado fallos críticos en el popular módulo Wi-Fi de Realtek para dispositivos integrados.
  https://thehackernews.com/2021/02/critical-bugs-found-in-popular-realtek.html
- Los servidores de Plex Media se utilizan activamente para intensificar los ataques DDoS.
  https://www.bleepingcomputer.com/news/security/plex-media-servers-actively-abused-to-amplify-ddos-attacks/
- El proveedor de productos de seguridad de red Stormshield revela que ciberdelincuentes robaron información de algunos de sus clientes.

https://securityaffairs.co/wordpress/114204/data-breach/stormshield-discloses-data-breach.html

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

- El malware Agent Tesla fue detectado utilizando nuevas técnicas de entrega y evasión.
https://thehackernews.com/2021/02/agent-tesla-malware-spotted-using-new.html
- Más novedades sobre SolarWinds.
https://www.schneier.com/blog/archives/2021/02/more-solarwinds-news.html
- Más de una docena de extensiones de Chrome y Edge han sido descubiertas alterando los resultados de búsquedas en Google de usuarios, sustituyendo las URL por sitios maliciosos.
https://thehackernews.com/2021/02/over-dozen-chrome-extensions-caught.html

NOTAS DE INTERÉS

- El hackeo de SolarWinds induce al Congreso de EE.UU. a que la NSA ponga el foco en la encriptación.
https://threatpost.com/solarwinds-nsa-encryption/163561/
- El gobierno chino podría haber robado datos personales del 80% de los adultos de Estados Unidos.
https://www.infosecurity-magazine.com/news/china-steals-personal-data-of-80/
- El éxito del CISO: Se trata de algo más que de habilidades técnicas.
https://securityintelligence.com/articles/ciso-success-more-than-tech-skills/
- Un sistema *skimmer* de tarjetas de crédito de comercio electrónico está siendo utilizado por un segundo *skimmer* para robar datos de pago y ambos están en el sitio web de Costway.
https://threatpost.com/magento-web-skimmers-costway/163593/
- Microsoft Defender detecta vulnerabilidades del sistema macOS y a las actualizaciones de Chrome como puertas traseras.
https://www.bleepingcomputer.com/news/security/microsoft-defender-now-detects-macos-system-app-vulnerabilities/
https://www.bleepingcomputer.com/news/security/microsoft-defender-atp-detects-chrome-updates-as-php-backdoors/
- ¡Café gratis! Un investigador holandés hackea las máquinas expendedoras de prepago.
https://nakedsecurity.sophos.com/2021/02/04/free-coffee-dutch-researcher-hacks-prepaid-vending-machines/

ACTUALIZACIONES DE SEGURIDAD

- CISA publica 2 nuevas advertencias sobre sistemas de control industrial.
https://us-cert.cisa.gov/ics/advisories
- Cisco resuelve los fallos críticos de ejecución de código en los routers VPN SMB.
https://us-cert.cisa.gov/ncas/current-activity/2021/02/04/cisco-releases-security-updates
- Microsoft corrige el problema que hace que las apps de Windows 10 olviden las contraseñas
https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-issue-causing-windows-10-apps-to-forget-passwords/