@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. 138 – 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 21/10/21 y el 27/10/21

- Ferrara Candy Co., con sede en Chicago, EE.UU., confirmó públicamente que un ciberincidente ransomware encriptó algunos de sus sistemas.
https://threatpost.com/ransomware-candy-corn-halloween/175630/
- La empresa Gigabyte ha sido presuntamente atacada por el ransomware AvosLocker.
https://threatpost.com/gigabyte-avoslocker-ransomware-gang/175642/
- Un grupo de hackers "Lone Wolf" ataca a Afganistán e India con RATs.
https://thehackernews.com/2021/10/lone-wolf-hacker-group-targeting.html
- Un pirata informático vende los datos de millones de conductores de Moscú por 800 dólares.
https://www.bleepingcomputer.com/news/security/hacker-sells-the-data-for-millions-of-moscow-drivers-for-800/
- La banda de ciberdelincuentes FIN7 crea una falsa empresa de ciberseguridad para reclutar pentesters para ataques de ransomware.
https://securityaffairs.co/wordpress/123673/cyber-crime/fin7-fake-cybersecurity-firm.html
- La biblioteca NPM fue pirateada para instalar programas de robo de contraseñas y mineros
https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/
- Gasolineras iraníes fuera de servicio tras el hackeo de la red de distribución.
https://www.bleepingcomputer.com/news/security/iranian-gas-stations-out-of-service-after-distribution-network-hacked/
- Los piratas informáticos utilizan el cargador Squirrelwaffle para desplegar Qakbot y Cobalt Strike
https://thehackernews.com/2021/10/hackers-using-squirrelwaffle-loader-to.html
- Un ciberataque afecta a los proveedores de telefonía por Internet del Reino Unido.
https://www.bbc.com/news/technology-59053876

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

- Controles que pueden ayudarle a identificar el ransomware.
https://securityintelligence.com/posts/detections-help-identify-ransomware/
- Los 5 principales vectores de ataque a tener en cuenta en 2022.
https://securityaffairs.co/wordpress/123636/security/top-5-attack-vectors-2022.html
- Cómo obtiene el FBI la información de localización.
https://www.schneier.com/blog/archives/2021/10/how-the-fbi-gets-location-information.html
https://www.vice.com/en/article/m7vqkv/how-fbi-gets-phone-data-att-tmobile-verizon

NOTAS DE INTERÉS

- Microsoft, Intel y Goldman Sachs liderarán el nuevo grupo de trabajo del TCG para abordar los retos de seguridad de la cadena de suministro.
  https://www.darkreading.com/attacks-breaches/microsoft-intel-and-goldman-sachs-to-lead-new-tcg-work-group-to-tackle-supply-chain-security-challenges
- Cuentas de los creadores de YouTube fueron pirateadas con un malware que roba cookies.
  https://securityaffairs.co/wordpress/123630/hacking/youtube-creators-accounts-hijacked-malware.html
- EE.UU. frenará las exportaciones de herramientas de *hackeo* a Rusia y China.
  https://www.securityweek.com/us-curb-hacking-tool-exports-russia-china
- Un estudio revela que dispositivos IoT de uso familiar aparecen... en las redes corporativas.
  https://www.theregister.com/2021/10/21/iot_devices_corporate_networks_security_warning/
- Un defecto en el software WinRAR podría permitir a los atacantes *hackear* su ordenador.
  https://thehackernews.com/2021/10/bug-in-free-winrar-software-could-let.html
- El Gobierno de EE.UU. advierte de los ataques del ransomware BlackMatter contra las infraestructuras críticas.
  https://www.tripwire.com/state-of-security/security-data-protection/us-government-warns-of-blackmatter-ransomware-attacks-against-critical-infrastructure/
- Un nuevo ataque permite recoger y falsificar huellas digitales de los usuarios de navegadores.
  https://thehackernews.com/2021/10/new-attack-let-attacker-collect-and.html
- La OTAN publica su primera estrategia para la Inteligencia Artificial para la Defensa..
  https://securityaffairs.co/wordpress/123715/security/nato-strategy-artificial-intelligence.html
- Emsisoft ha creado un descifrador gratuito para viejas víctimas del ransomware BlackMatter.
  https://securityaffairs.co/wordpress/123736/security/blackmatter-decryptor-pat-victims.html
- Nobelium ha hackeado al menos 14 empresas de la cadena de suministro de TI desde mayo.
  https://www.bleepingcomputer.com/news/microsoft/microsoft-russian-svr-hacked-at-least-14-it-supply-chain-firms-since-may/
- Ciberdelincuentes utilizaron software de facturación de día cero para desplegar el ransomware.
  https://www.bleepingcomputer.com/news/security/hackers-used-billing-software-zero-day-to-deploy-ransomware/
- Correos electrónicos de phishing utilizan códigos QR para burlar las defensas.
  https://www.zdnet.com/article/these-phishing-emails-use-qr-codes-to-bypass-defences-and-steal-microsoft-365-usernames-and-passwords/

ACTUALIZACIONES DE SEGURIDAD

- Cisco anuncia actualizaciones de seguridad para el software IOS XE SD-WAN.
  https://us-cert.cisa.gov/ncas/current-activity/2021/10/21/cisco-releases-security-updates-ios-xe-sd-wan-software
- Ya se puede descargar la versión candidata 1 de Microsoft PowerShell 7.2.0
  https://betanews.com/2021/10/23/microsoft-powershell-7-2-0-release-candidate-1-now-available-to-download/
- Apple corrige 22 problemas de seguridad que afectan a los iPhones.
  https://www.securityweek.com/apple-patches-22-security-flaws-haunting-iphones