@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. 192 – Año 2022

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 11/11/22 y el 17/11/22

- El gigantesco supermercado canadiense Sobeys, se ve afectado por el ransomware Black Basta.
https://www.bleepingcomputer.com/news/security/canadian-food-retail-giant-sobeys-hit-by-black-basta-ransomware/
- El grupo de amenaza (0x_dump) afirma haber hackeado el banco multinacional Deutsche Bank.
https://securityaffairs.co/wordpress/138416/data-breach/deutsche-bank-alleged-data-breach.html
- Reuters informó que 1.000 millones de dólares de fondos de clientes de FTX se han desvanecido.
https://securityaffairs.co/wordpress/138449/digital-id/ftx-alleged-hack.html
- Sitios web de Magento y Adobe Commerce bajo ataque.
https://securityaffairs.co/wordpress/138663/cyber-crime/trojanorders-attacks-adobe-commerce-magento.html

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

- Nuevo malware para Android BadBazaar vinculado a ciberespías chinos.
https://www.bleepingcomputer.com/news/security/new-badbazaar-android-malware-linked-to-chinese-cyberspies/
- **CISA publica la guía SSVC para ayudar a las organizaciones a priorizar las vulnerabilidades.**
https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf
- Resuelven por accidente una forma de saltarse la pantalla de bloqueo de un teléfono Android.
https://www.bleepingcomputer.com/news/security/android-phone-owner-accidentally-finds-a-way-to-bypass-lock-screen/
- La APT "Earth Longzhi" se centra en Ucrania y países de Asia usando ataques "Custom Cobalt".
https://thehackernews.com/2022/11/new-earth-longzhi-apt-targets-ukraine.html
- El uso de la puerta trasera DTrack centrado en Europa y América Latina.
https://securelist.com/dtrack-targeting-europe-latin-america/107798/
- **Rompen seguridad (PCSpoof) de la red TTE (time-triggered Ethernet) usada en naves espaciales y aviones.**
https://arstechnica.com/information-technology/2022/11/researchers-break-security-guarantees-of-tte-networking-used-in-spacecraft/
- Análisis del grupo cibercriminal financiero que se autodenomina Disneyland Team.
https://krebsonsecurity.com/2022/11/disneyland-malware-team-its-a-puny-world-after-all/
- Cómo prevenir, detectar y responder al robo de tokens en la nube.
https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/
- **Los investigadores descifran calladamente las claves del ransomware Zeppelin.**
https://krebsonsecurity.com/2022/11/researchers-quietly-cracked-zeppelin-ransomware-keys/

NOTAS DE INTERÉS

- Microsoft culpa a hackers rusos de los ataques de ransomware del Prestige en Ucrania y Polonia.
https://thehackernews.com/2022/11/microsoft-blames-russian-hackers-for.html
- Europa propone una ciberdefensa conjunta para protegerse de Rusia.
https://www.theregister.com/2022/11/11/eu_joint_cyber_defense/
- Varios fallos de alta gravedad afectan al software de servidor web OpenLiteSpeed.
https://thehackernews.com/2022/11/multiple-high-severity-flaw-affect.html
- La NSA sugiere a las organizaciones que usen lenguajes de programación seguros para la memoria.
https://www.theregister.com/2022/11/11/nsa_urges_orgs_to_use/
- ''Barcos oscuros'' emergen de las sombras del misterio del Nord Stream.
https://www.wired.com/story/nord-stream-pipeline-explosion-dark-ships/
- **Aplicación maliciosa en Google Play Store que distribuye el troyano bancario Xenomorph.**
https://thehackernews.com/2022/11/these-two-google-play-store-apps.html
- Worok usa la API de Dropbox para exfiltrar datos a través de un backdoor oculto en imágenes.
https://thehackernews.com/2022/11/worok-hackers-abuse-dropbox-api-to.html
- Campaña masiva de SEO de Black Hat utilizando más de 15K sitios de WordPress.
https://securityaffairs.co/wordpress/138523/hacking/wordpress-sites-black-hat-seo.html
- Los hackers de Billbug se centran en agencias gubernamentales y las organizaciones de defensa.
https://arstechnica.com/information-technology/2022/11/state-sponsored-hackers-in-china-compromise-certificate-authority/
- Se informa de un fallo crítico de RCE en el catálogo de software Backstage y la plataforma para desarrolladores de Spotify.
https://thehackernews.com/2022/11/critical-rce-flaw-reported-in-spotifys.html
- La nueva campaña de RapperBot pretende realizar ataques DDoS a los servidores de juegos.
https://securityaffairs.co/wordpress/138615/malware/rapperbot-botnet-targets-game-servers.html
- **La actividad de los grupos APT respaldados por el Estado continúa.**
https://www.infosecurity-magazine.com/news/state-backed-apt-group-activity/
- Un grupo iraní penetró en una agencia federal de EE.UU. utilizando el exploit Log4Shell.
https://www.bleepingcomputer.com/news/security/us-govt-iranian-hackers-breached-federal-agency-using-log4shell-exploit/
https://www.zdnet.com/article/cybersecurity-warning-if-youve-not-patched-log4j-yet-assume-attackers-are-in-your-network/

ACTUALIZACIONES DE SEGURIDAD

- Cisco publica nuevas actualizaciones de seguridad.
https://www.cisa.gov/uscert/ncas/current-activity/2022/11/16/cisco-releases-security-updates-identity-services-engine
- Mozilla publica actualizaciones de seguridad para múltiples productos.
https://www.cisa.gov/uscert/ncas/current-activity/2022/11/16/mozilla-releases-security-updates-multiple-products
- Microsoft corrige problemas de autentificación de Windows Kerberos en las actualizaciones de emergencia.
https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-kerberos-auth-issues-in-emergency-updates/