@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. 141 – 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 11/11/21 y el 17/11/21

- Telnyx, proveedor de VoIP, fue afectado por ataques DDoS.
https://www.bleepingcomputer.com/news/security/telnyx-is-the-latest-voip-provider-hit-with-ddos-attacks/
- Fueron detectados hackers norcoreanos en la búsqueda de secretos de fabricación de vacunas.
https://news.sky.com/story/covid-19-north-korean-hackers-detected-searching-for-vaccine-manufacturing-secrets-12465280
- Costco confirma una filtración de datos tras encontrar un *skimmer* de tarjetas de crédito.
https://threatpost.com/costco-data-skimmer-customers-notification/176320/
- Facebook prohíbe a grupos de hackers pakistaníes y sirios por uso indebido de su plataforma.
https://thehackernews.com/2021/11/facebook-bans-pakistani-and-syrian.html

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

- Caracteres “invisibles” podrían estar escondiendo puertas traseras en el código JavaScript.
https://www.bleepingcomputer.com/news/security/invisible-characters-could-be-hiding-backdoors-in-your-javascript-code/
- Qué ocurre si la infraestructura de sincronización horaria es pirateada.
https://www.darkreading.com/vulnerabilities-threats/what-happens-if-time-gets-hacked
- La red de bots BotenaGo ataca a millones de dispositivos IoT con 33 exploits.
https://www.bleepingcomputer.com/news/security/botenago-botnet-targets-millions-of-iot-devices-with-33-exploits/
- Que funcionó y lo que no, en el segundo experimento de "Conectar todo" del ejército de EE.UU.
https://www.defenseone.com/technology/2021/11/armys-second-connect-everything-experiment-reveals-progress-future-hurdles/186783/
- Abcbot - Un nuevo malware botnet evolutivo dirigido a Linux.
https://thehackernews.com/2021/11/abcbot-new-evolving-wormable-botnet.html
- Moses Staff causa estragos en las organizaciones israelíes con encriptaciones sin pedir rescate.
https://www.bleepingcomputer.com/news/security/moses-staff-hackers-wreak-havoc-on-israeli-orgs-with-ransomless-encryptions/
- Demuestran un nuevo ataque de huellas dactilares en el tráfico cifrado de Tor.
https://thehackernews.com/2021/11/researchers-demonstrate-new.html
- Instancias de Alibaba ECS capturadas de manera activa por un malware de minería de criptomonedas.
https://www.bleepingcomputer.com/news/security/alibaba-ecs-instances-actively-hijacked-by-cryptomining-malware/
- Las nuevas campañas de spam de Emotet que llegan a los correos de todo el mundo.

https://www.bleepingcomputer.com/news/security/here-are-the-new-emotet-spam-campaigns-hitting-mailboxes-worldwide/

NOTAS DE INTERÉS

- Los gigantes farmacéuticos de la UE utilizan aplicaciones antiguas y vulnerables y no utilizan el cifrado en los formularios de acceso.
https://www.zdnet.com/article/eu-pharmaceutical-giants-run-old-vulnerable-apps-and-fail-to-use-encryption-in-login-forms/
- Los piratas informáticos iranies, del grupo Lyceum, tienen como objetivo las telecomunicaciones y los proveedores de servicios de Internet en Israel, Arabia Saudí y África.
https://thehackernews.com/2021/11/irans-lyceum-hackers-target-telecoms.html
- Palo Alto advierte de un fallo de día cero en los firewalls que utilizan GlobalProtect Portal VPN.
https://thehackernews.com/2021/11/palo-alto-warns-of-zero-day-bug-in.html
- "Actores de la amenaza" hackearon un servidor de un proveedor de agua de Queensland, Australia, y permanecieron sin ser detectados durante 9 meses.
https://securityaffairs.co/wordpress/124498/hacking/queensland-water-supplier-hacked.htm
- El presidente de EE.UU. firma una ley para prohibir que Huawei y ZTE reciban licencias de la FCC.
https://www.zdnet.com/article/us-president-biden-signs-law-to-ban-huawei-and-zte-from-receiving-fcc-licences/
- Millones de routers y dispositivos IoT en riesgo por un nuevo malware de código abierto.
https://threatpost.com/routers-iot-open-source-malware/176270/
- Un hacker envía correos electrónicos falsos desde una dirección real del FBI debido a un portal web mal configurado.
https://news.sky.com/story/hackers-target-fbi-emails-and-send-thousands-of-fake-messages-warning-of-cyber-attack-12468205
https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-incident-involving-fake-emails
- Hackers norcoreanos atacan a investigadores de ciberseguridad con un troyano en el IDA Pro.
https://thehackernews.com/2021/11/north-korean-hackers-target.html
- Un error del chip de Intel podría permitir ataques a laptops, automóviles y dispositivos médicos.
https://www.helpnetsecurity.com/2021/11/15/intel-chip-flaw-cve-2021-0146/
- Han demostrado otra variación del ataque Rowhammer que afecta a todos los chips DRAM.
https://thehackernews.com/2021/11/new-blacksmith-exploit-bypasses-current.html
- Una investigación encuentra vulnerabilidades en el 97% de las aplicaciones.
https://betanews.com/2021/11/16/vulnerabilities-in-97-percent-of-applications/
- Estados Unidos e Israel anuncian un grupo de trabajo conjunto sobre ciberseguridad.
https://justthenews.com/politics-policy/cybersecurity/us-and-israel-announce-cybersecurity-joint-task-force
- Estados Unidos, Reino Unido y Australia advierten de que piratas informáticos iraníes aprovechan los fallos de Microsoft y Fortinet.
https://thehackernews.com/2021/11/us-uk-and-australia-warn-of-iranian.html
- CISA: catálogo de vulnerabilidades conocidas y explotables.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

ACTUALIZACIONES DE SEGURIDAD

- Un fallo de día cero en todas las versiones de Windows recibe un parche no oficial gratuito.
https://www.bleepingcomputer.com/news/microsoft/zero-day-bug-in-all-windows-versions-gets-free-unofficial-patch/