@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. 80/2021

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.

02/03/2021

- El troyano ObliqueRAT ahora acecha en las imágenes de sitios web comprometidos.
https://www.zdnet.com/article/obliquerat-trojan-now-hides-in-images-on-compromised-websites/
- Malaysia Airlines sufre un "incidente" de seguridad de datos que dura nueve años.
https://www.zdnet.com/article/malaysia-airlines-suffers-data-security-incident-spanning-nine-years/
- Los hackers que están detrás de las anteriores herramientas de jailbreak del iPhone han lanzado una actualización basada en una vulnerabilidad recientemente descubierta y parcheada.
https://threatpost.com/jailbreak-tool-works-on-iphones-up-to-ios-14-3/164420/
- Oxfam Australia confirma el robo de datos cuando aparecieron en venta en Internet.
https://www.bleepingcomputer.com/news/security/oxfam-australia-confirms-data-breach-after-stolen-info-sold-online/
- La caída del gigante de software de pagos, PrismHR, se debe a un ataque ransomware.
https://krebsonsecurity.com/2021/03/payroll-hr-giant-prismhr-hit-by-ransomware/

03/03/2021

- Microsoft emite una advertencia para una actualización crítica debido a que hackers chinos atacan a los servidores de Exchange.
https://www.forbes.com/sites/daveywinder/2021/03/03/microsoft-issues-critical-update-warning-as-chinese-hackers-attack-exchange-servers/
- RTM Cybergang añade un nuevo ransomware llamado Quoter a su ola de crímenes.
https://threatpost.com/rtm-banking-trojan-quoter-ransomware/164447/
- Francia advierte que el ransomware Ryuk desarrolla capacidades similares a las de un gusano.
https://www.cyberscoop.com/ryuk-ransomware-develops-worm-like-capabilities-anssi-france/
- Un investigador encuentra 5 vulnerabilidades de incremento de privilegios en el kernel de Linux.
https://www.scmagazine.com/home/security-news/vulnerabilities/researcher-finds-5-privilege-escalation-vulnerabilities-in-linux-kernel/

04/03/2021

- Ciberatacantes tienen como blanco a los principales foros rusos de ciberdelincuencia.
https://threatpost.com/cyberattackers-target-russian-cybercrime-forums/164511/
https://www.zdnet.com/article/maza-russian-cybercriminal-forum-suffers-data-breach/
- FireEye encuentra un nuevo malware probablemente vinculado a los hackers de SolarWinds.
https://www.bleepingcomputer.com/news/security/fireeye-finds-new-malware-likely-linked-to-solarwinds-hackers/
https://securityaffairs.co/wordpress/115291/malware/sunshuttle-backdoor-solarwinds-hack.html

- CISA ordena a las agencias federales que *parcheen* los servidores Exchange.
https://threatpost.com/cisa-federal-agencies-patch-exchange-servers/164499/
https://us-cert.cisa.gov/ncas/alerts/aa21-062a
https://cyber.dhs.gov/ed/21-02/

- El ataque del ransomware DarkSide daña a CompuCom MSP.
https://www.bleepingcomputer.com/news/security/compucom-msp-hit-by-darkside-ransomware-cyberattack/

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

- **Lista de filtraciones de datos y ciberataques en febrero de 2021.**
https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2021-2-3-billion-records-breached

- Ahora los hackers ocultan el *payload* de ObliqueRAT en imágenes, para evitar su detección.
https://thehackernews.com/2021/03/hackers-now-hiding-obliquerat-payload.html

- Los paquetes NPM maliciosos atacan a Amazon y Slack con nuevos ataques de dependencia.
https://www.bleepingcomputer.com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/

NOTAS DE INTERÉS

- Un plan sólido de EUA para competir con China en inteligencia artificial.
https://www.defenseone.com/ideas/2021/03/solid-plan-compete-china-artificial-intelligence/172360/

- Los troyanos bancarios Cerberus y Anubis se enfocan en los hablantes de lengua turca.
https://exchange.xforce.ibmcloud.com/collection/eb07ec90a9aaf7d07d85dcf49e4aca9b
https://community.riskiq.com/article/85b3db8c/description

- Microsoft Teams añade el cifrado de extremo a extremo (E2EE) a las llamadas individuales.
https://www.bleepingcomputer.com/news/security/microsoft-teams-adds-end-to-end-encryption-e2ee-to-one-on-one-calls/

- La nueva integración del antivirus y del Office 365 de Microsoft permite escanear macro scripts maliciosos escritos en XLM en tiempo de ejecución.
https://www.zdnet.com/article/microsoft-were-cracking-down-on-malware-that-uses-excel-macros/

- Un informe revela que los programas de armamento del Departamento de Defensa de EE.UU. carecen de directrices claras en materia de ciberseguridad.
https://www.zdnet.com/article/gao-report-finds-dods-weapons-programs-lack-clear-cybersecurity-guidelines/

ACTUALIZACIONES DE SEGURIDAD

- Google soluciona un fallo que es explotado activamente en el navegador Chrome.
https://threatpost.com/google-patches-actively-exploited-flaw-in-chrome-browser/164468/

- Se han encontrado y corregido agujeros de seguridad de alta gravedad en redes Linux.
https://www.zdnet.com/article/linux-network-security-holes-found-fixed/

- Cisco publica actualizaciones de seguridad.
https://us-cert.cisa.gov/ncas/current-activity/2021/03/04/cisco-releases-security-updates