



## Subsecretaría de Ciberdefensa

# Boletín de Noticias de Ciberseguridad

### Informe sobre incidentes y ciberamenazas Nro. 110 – 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.

#### 18/06/2021

- La cadena de supermercados estadounidense Wegmans notifica a sus clientes la vulneración de sus datos.  
<https://www.bleepingcomputer.com/news/security/us-supermarket-chain-wegmans-notifies-customers-of-data-breach/>
- El regreso de la APT TA402 Molerats tras una breve pausa.  
<https://securityaffairs.co/wordpress/119085/apt/ta402-molerats-apt-return.html>

#### 19/06/2021

- La APT Kimsuky de Corea del Norte aprovechó un fallo de la VPN para hackear el Instituto de Investigación Nuclear de Corea del Sur.  
<https://thehackernews.com/2021/06/north-korea-exploited-vpn-flaw-to-hack.html>  
<https://securityaffairs.co/wordpress/119147/apt/kimsuky-apt-hacked-south-korea-kaeri.html>

#### 20/06/2021

- Una clínica de fertilidad divulga una filtración de datos que expone la información de pacientes.  
<https://www.bleepingcomputer.com/news/security/fertility-clinic-discloses-data-breach-exposing-patient-info/>

#### 21/06/2021

- El personal parlamentario del Reino Unido perdió 96 dispositivos en los últimos dos años.  
<https://www.infosecurity-magazine.com/news/parliament-staffers-devices-two/>
- El MI5 confiscó el teléfono de Boris Johnson por temor a riesgos de seguridad.  
<https://securityaffairs.co/wordpress/119174/security/mi5-seized-boris-johnson-phone.html>
- Se publica un informe sobre la seguridad del sector del agua en EE.UU. justo cuando sale a la luz otro hackeo de una planta.  
<https://www.securityweek.com/water-sector-security-report-released-just-another-water-plant-hack-comes-light>  
<https://krebsonsecurity.com/2021/06/how-cyber-safe-is-your-drinking-water-supply/>
- ADATA, fabricante taiwanés de chips de memoria y almacenamiento, sufre una fuga de datos de 700 GB en el ataque del ransomware Ragnar Locker.  
<https://www.bleepingcomputer.com/news/security/adata-suffers-700-gb-data-leak-in-ragnar-locker-ransomware-attack/>

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

- La semana del ransomware - 18 de junio de 2021 - Las fuerzas del orden contraatacan.  
<https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-18th-2021-law-enforcement-strikes-back/>



- El ciberespionaje de los hackers chinos en las naciones vecinas va en aumento.  
<https://thehackernews.com/2021/06/cyber-espionage-by-chinese-hackers-in.html>
- Un nuevo fallo puede romper permanentemente la conectividad WiFi del iPhone.  
<https://securityaffairs.co/wordpress/119157/hacking/iphone-bug-wifi-connectivity.html>
- DroidMorph demuestra que los antivirus populares de Android no detectan las aplicaciones clonadas dañinas.  
<https://thehackernews.com/2021/06/droidmorph-shows-popular-android.html>
- El futuro del aprendizaje automático (*machine learning*) y la ciberseguridad.  
<https://www.schneier.com/blog/archives/2021/06/the-future-of-machine-learning-and-cybersecurity.html>

### **NOTAS DE INTERÉS**

- Google presenta un nuevo marco para prevenir ataques a la cadena de suministro de software.  
<https://thehackernews.com/2021/06/google-releases-new-framework-to.html>
- La NSA publica una guía para asegurar los sistemas de comunicación de las empresas.  
[https://media.defense.gov/2021/Jun/17/2002744049/-1/-1/1/CSI\\_DEPLOYING%20SECURE%20VVOIP%20SYSTEMS.PDF](https://media.defense.gov/2021/Jun/17/2002744049/-1/-1/1/CSI_DEPLOYING%20SECURE%20VVOIP%20SYSTEMS.PDF)
- La banda "DarkSide" ataca a los sectores energético y alimentario mundiales  
<https://threatpost.com/darkside-global-energy-food/167056/>
- Rusia prohíbe Opera VPN y VyprVPN, los clasifica como amenazas.  
<https://www.bleepingcomputer.com/news/security/russia-bans-opera-vpn-and-vyprvpn-classifies-them-as-threats/>
- Los piratas informáticos encuentran una nueva forma de explotar Google Docs para el phishing.  
<https://www.darkreading.com/vulnerabilities---threats/attackers-find-new-way-to-exploit-google-docs-for-phishing-/d/d-id/1341342>
- Una falsa banda DarkSide se centra en la industria energética y alimentaria mediante correos electrónicos extorsivos.  
<https://www.bleepingcomputer.com/news/security/fake-darkside-gang-targets-energy-food-industry-in-extortion-emails/>
- El gobierno ruso planea crear un sistema de videovigilancia unificado.  
<https://www.ehackingnews.com/2021/06/the-russian-government-plans-to-create.html>
- El secuestro de Lazarus: cómo Corea del Norte estuvo a punto de realizar un hackeo de mil millones de dólares.  
<https://www.bbc.com/news/stories-57520169>

### **ACTUALIZACIONES DE SEGURIDAD**

- Google Chrome en iOS está incorporando una función de privacidad mejorada.  
<https://www.bleepingcomputer.com/news/google/google-chrome-on-ios-is-getting-an-enhanced-privacy-feature/>
- Tor Browser corrige la vulnerabilidad que rastrea el uso de las aplicaciones instaladas.  
<https://www.bleepingcomputer.com/news/security/tor-browser-fixes-vulnerability-that-tracks-you-using-installed-apps/>