

## Subsecretaría de Ciberdefensa

# Boletín de Noticias de Ciberseguridad

### Informe sobre incidentes y ciberamenazas Nro. 107 – 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.

#### 08/06/2021

- **Un apagón masivo acaba de dejar fuera de servicio a grandes sectores de Internet.**  
<https://www.zdnet.com/article/a-massive-outage-just-took-large-sections-of-the-internet-offline/>  
<https://www.bleepingcomputer.com/news/security/stackoverflow-twitch-reddit-others-down-in-fastly-cdn-outage/>
- El Dpto. de Justicia de EE,UU. incauta parte de los millones pagados por Colonial Pipeline a los piratas de Darkside.  
<https://www.infosecurity-magazine.com/news/department-justice-seizes/>  
<https://www.techrepublic.com/article/feds-recover-2-3-million-in-cryptocurrency-paid-by-colonial-pipeline-in-ransomware-attack/>
- El fabricante de memorias para computadoras ADATA se ve afectado por el ransomware Ragnar Locker.  
<https://www.bleepingcomputer.com/news/security/computer-memory-maker-adata-hit-by-ragnar-locker-ransomware/>
- Hackers chinos implicados en la intrusión en agencias gubernamentales rusas.  
<https://www.cyberscoop.com/china-hackers-russia-fsb-biden-putin/>

#### 09/06/2021

- Ataques de PuzzleMaker aprovechan las vulnerabilidades de Windows de día cero y de Chrome.  
<https://www.zdnet.com/article/puzzlemaker-attacks-exploit-windows-chrome-zero-day-vulnerabilities/>
- El Ministerio de Trabajo y Economía Social de España sufre un ciberataque.  
<https://www.bleepingcomputer.com/news/security/spains-ministry-of-labor-and-social-economy-hit-by-cyberattack/>
- Un solo cliente de Fastly provocó el colapso global de Internet.  
<https://www.infosecurity-magazine.com/news/internet-outage-single-settings/>

#### 10/06/2021

- Ransomware: La empresa del sector de la carne JBS informa de que ha pagado 11 millones de dólares tras el ataque.  
<https://www.zdnet.com/article/ransomware-meat-firm-jbs-says-it-paid-out-11m-after-attack/>
- Electronics Art: El gigante de los juegos fue hackeado y se le robó código fuente.  
<https://www.bleepingcomputer.com/news/security/hackers-breach-gaming-giant-electronic-arts-steal-game-source-code/>

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

- El FBI y la AFP crearon una falsa plataforma de chat encriptado para atrapar a los delincuentes.



<https://www.bleepingcomputer.com/news/security/fbi-and-afp-created-a-fake-encrypted-chat-platform-to-catch-criminals/>

- Los ciberespías furtivos Gelsemium se vinculan al ataque a la cadena de suministro de NoxPlayer.  
<https://www.bleepingcomputer.com/news/security/stealthy-gelsemium-cyberspies-linked-to-noxplayer-supply-chain-attack/>
- **Los piratas informáticos pueden interferir con las conexiones HTTPS enviando datos a su servidor de correo electrónico.**  
<https://arstechnica.com/gadgets/2021/06/hackers-can-mess-with-https-connections-by-sending-data-to-your-email-server/>  
<https://thehackernews.com/2021/06/new-tls-attack-lets-attackers-launch.html>

### **NOTAS DE INTERÉS**

- **Cómo los hackers han manipulado el algoritmo de tendencias de Twitter durante años.**  
<https://thenextweb.com/news/twitter-trending-topics-algorithm-has-vulnerability-hackers-using-ephemeral-astrourfing-attacks>
- El acceso no autorizado representa el 43% de todas las filtraciones a nivel mundial.  
<https://www.helpnetsecurity.com/2021/06/08/unauthorized-access-breaches/>
- El 77% de las aplicaciones financieras tienen al menos una vulnerabilidad grave.  
<https://www.helpnetsecurity.com/2021/06/09/mobile-finance-apps/>
- Huawei presenta un "marco de ciberseguridad" con el inicio de su centro de transparencia en China.  
<https://www.zdnet.com/article/huawei-reveals-cybersecurity-framework-with-launch-of-china-transparency-centre/>
- El grupo DarkSide pilló a Colonial utilizando su antigua contraseña de VPN.  
<https://threatpost.com/darkside-pwned-colonial-with-old-vpn-password/166743/>
- El uso de datos de Amazon será objeto de una nueva investigación antimonopolio en el Reino Unido.  
<https://www.zdnet.com/article/amazon-data-usage-to-feature-in-new-uk-antitrust-probe/>
- Los hackers pueden aprovechar fallas de aplicaciones preinstaladas de Samsung para espiar.  
<https://www.bleepingcomputer.com/news/security/hackers-can-exploit-bugs-in-samsung-pre-installed-apps-to-spy-on-users/>

### **ACTUALIZACIONES DE SEGURIDAD**

- Adobe publica actualizaciones de seguridad para 41 vulnerabilidades en 10 productos.  
<https://www.bleepingcomputer.com/news/security/adobe-issues-security-updates-for-41-vulnerabilities-in-10-products/>
- **Martes de parches de Microsoft de junio de 2021.**  
<https://isc.sans.edu/forums/diary/Microsoft+June+2021+Patch+Tuesday/27506/>
- Intel corrige 73 vulnerabilidades en la actualización de la plataforma de junio de 2021.  
<https://www.bleepingcomputer.com/news/security/intel-fixes-73-vulnerabilities-in-june-2021-platform-update/>  
<https://threatpost.com/intel-security-holes-cpus-bluetooth-security/166747/>
- Google soluciona un fallo crítico de RCE en Android.  
<https://threatpost.com/android-critical-rce-bug/166723/>