GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición °51

En alianza con

TD SYNNEX FORTINET

# BOLETÍN DE CIBERINTELIGENCIA DE AMENAZAS

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

## VISTA RÁPIDA

| | CRÍTICO | URGENTE | IMPORTANTE |
|---|---|---|---|
| **VULNERABIILIDADES** | 1 | 0 | 4 |
| **MALWARE** | 0 | 0 | 4 |
| **BRECHAS DE SEGURIDAD** | 0 | 1 | 4 |
| **SECTOR CORPORATIVO** | 0 | 0 | 3 |
| **SECTOR SALUD** | 0 | 0 | 1 |

## VULNERABILIDADES

### Fortinet soluciona falla crítica de ejecución de comando remoto de FortiNAC

Fortinet en su más reciente actualización para el acceso de confianza llamada cero FortiNAC, la cual, permite abordar una vulnerabilidad de gravedad crítica en la que los atacantes ejecutaban códigos y comandos. Permitiendo a las organizaciones administrar políticas de acceso en toda su red, obtener visibilidad de dispositivos, así como de usuarios protegiendo la red contra accesos no autorizados o amenazas.

**Prioridad: 1 Crítico**

**Ampliar información:**

- https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-fortinac-remote-command-execution-flaw/
- https://www.fortiguard.com/psirt/FG-IR-23-074
- https://securityaffairs.com/147770/security/fortinet-fortinac-critical-flaw.html

---

## CISA agrega cinco vulnerabilidades explotadas

CISA ha agregado cinco nuevas vulnerabilidades a su catálogo, con base en evidencia de explotación activa.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://www.cisa.gov/news-events/alerts/2023/06/23/cisa-adds-five-known-exploited-vulnerabilities-catalog
- https://www.bleepingcomputer.com/news/security/cisa-orders-agencies-to-patch-iphone-bugs-abused-in-spyware-attacks/
- https://securityaffairs.com/147782/hacking/known-exploited-vulnerabilities-catalog-apple-bugs.html

---

## Juniper Networks publica aviso de seguridad

Aborda una vulnerabilidad en Junos OS y Junos OS Evolved, en la cual, un atacante remoto podría explotar esta vulnerabilidad para causar una condición de denegación de servicio.

**Prioridad:** **3 Importante.**

**Ampliar información:**

- https://www.cisa.gov/news-events/alerts/2023/06/22/juniper-networks-releases-security-advisory-junos-os-and-junos-os-evolved
- https://supportportal.juniper.net/s/article/2023-06-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-BGP-session-will-flap-upon-receipt-of-a-specific-optional-transitive-attribute-CVE-2023-0026

---

## ISC publica avisos de seguridad para múltiples versiones de BIND 9

El Consorcio de Sistemas de Internet (ISC) ha publicado avisos de seguridad que abordan vulnerabilidades provocadas por atacantes remotos, quienes podrían causar condiciones de denegación de servicio que afecten a múltiples versiones del denominado Dominio de nombres de internet de Berkeley (BIND).

**Prioridad:** **3 Importante.**

**Ampliar Información:**

- https://www.cisa.gov/news-events/alerts/2023/06/22/isc-releases-security-advisories-multiple-versions-bind-9
- https://therecord.media/bind-9-patches-internet-dns-vulnerabilities}

---

## Violaciones/Hacks/Fugas

Estos ataques comenzaron el 27 de mayo de 2023, cuando la banda de ransomware CLOP comenzó a explotar una vulnerabilidad de día cero de MOVEit Transfer para robar datos de cientos de empresas.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/

---

**Recomendaciones generales sobre vulnerabilidades:**

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.
- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.

Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

## MALWARE

### Aviso: IDOR, de los equipos de Microsoft, permite que los inquilinos externos introduzcan malware

Max Corbridge (@CorbridgeMax) y Tom Ellson (@tde_sec), colaboradores del equipo rojo de JUMPSEC identificaron una vulnerabilidad en la última versión de Microsoft Teams que permite el acceso de malware en cualquier organización.

**Prioridad: 3 importante.**

**Ampliar información:**

- https://labs.jumpsec.com/advisory-idor-in-microsoft-teams-allows-for-external-tenants-to-introduce-malware/
- https://www.darkreading.com/vulnerabilities-threats/microsoft-teams-attack-phish-deliver-malware-directly
- https://www.helpnetsecurity.com/2023/06/23/microsoft-teams-deliver-malware/

---

### Descripción general de las diferentes versiones del Trigona (ransomware)

Trigona es una familia de ransomware relativamente nueva que comenzó sus actividades a finales de octubre de 2022, aunque ya existían muestras en junio de 2022. Desde entonces, los operadores de Trigona se han mantenido muy activos actualizando continuamente sus archivos binarios.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://www.trendmicro.com/en_us/research/23/f/an-overview-of-the-trigona-ransomware.html

---

## 5 datos que debes saber sobre el grupo Royal Ransomware

El equipo de Malwarebytes Threat Intelligence ha rastreado la asombrosa cantidad de 195 incidentes de ransomware acreditados a Royal desde noviembre de 2022 hasta junio de 2023 y se han convertido en una de las amenazas más potentes dentro de sus informes mensuales.

**Prioridad: 3 Importante.**

**Ampliar Información:**

- https://www.malwarebytes.com/blog/business/2023/06/5-facts-to-know-about-the-royal-ransomware-gang

---

## Un instalador troyano del juego Super Mario propaga el malware SupremeBot

Los Threat Actors (TA) usan instaladores de juegos para propagar varios programas maliciosos aprovechando la amplia base de usuarios que tienen los juegos y la confianza de los usuarios en los instaladores de juegos como software legítimo quienes por error descargan software malicioso.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://blog.cyble.com/2023/06/23/trojanized-super-mario-game-installer-spreads-supremebot-malware/
- https://securityaffairs.com/147809/malware/trojanized-super-mario-bros-game.html

## BRECHAS DE SEGURIDAD

### CID Lookout: relojes inteligentes no solicitados

Los miembros del servicio militar denunciaron haber recibido relojes inteligentes no solicitados vía correo electrónico, los cuales, se conectan automáticamente a Wi-Fi y comienzan a conectarse a teléfonos celulares sin que se les solicite, obteniendo acceso a una gran cantidad de datos de usuario.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://www.cid.army.mil/Media/Press-Center/Article-Display/Article/3429159/cid-lookout-unsolicited-smartwatches-received-by-mail/
- https://www.darkreading.com/threat-intelligence/suspicious-smartwatches-mailed-us-army-personnel
- https://www.hackread.com/us-military-unsolicited-smartwatches-data-breach/
- https://www.securityweek.com/us-military-personnel-receiving-unsolicited-suspicious-smartwatches/
- https://securityaffairs.com/147788/intelligence/unsolicited-smartwatches-us-army.html

## 2,5 millones de titulares de pólizas de Genworth, 769 000 trabajadores y beneficiarios jubilados de California afectados por hackeo

MOVEit hack: expuso la información personal de aproximadamente 769.000 empleados jubilados de California y 2,5 millones en titulares de pólizas de Genworth Financial.

**Prioridad: 2 Urgente**

**Ampliar información:**

- https://www.securityweek.com/2-5m-genworth-policyholders-and-769k-retired-california-workers-and-beneficiaries-affected-by-hack/

---

## American Airlines y Southwest Airlines revelan violaciones de datos que afectan a los pilotos

Dos de las aerolíneas más grandes del mundo revelaron violaciones de datos causadas por el pirateo de Pilot Credentials, un proveedor externo que administra las aplicaciones de pilotos y los portales de reclutamiento para múltiples aerolíneas.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://www.bleepingcomputer.com/news/security/american-airlines-southwest-airlines-disclose-data-breaches-affecting-pilots/

## ¿Por qué los usuarios de sistemas heredados priorizan el tiempo de actividad sobre la seguridad?

El miedo de que los sistemas de misión crítica se detengan anula, las preocupaciones de los ejecutivos de negocios ante la ciberseguridad. ¿Cómo pueden los CISO superar esto?

**Prioridad: 3 Importante**

- https://www.darkreading.com/edge/why-legacy-system-users-prioritize-uptime-over-security

---

## Ajustes sencillos a la configuración pueden proteger su servidor de ataques

En marzo de 2023, se robaron datos de más de 56 000 personas, dicho hackeo del mercado de seguros de salud en línea expuso los datos personales de los miembros del Congreso, sus familias, el personal y decenas de miles de otros residentes del área de Washington.

**Prioridad: 3 Importante**

**Ampliar Información:**

- https://securityintelligence.com/articles/easy-configuration-fixes-can-protect-your-server/

## SECTOR CORPORATIVO

## El FBI se apodera de BreachForums después de arrestar a su propietario Pompompurin en marzo

La policía de EE. UU. incautó el dominio web del foro de piratería BreachForums (también conocido como Breached) tres meses después de detener a su propietario Conor Fitzpatrick (también conocido como Pompompurin), bajo cargos de delito cibernético.

**Prioridad: 3 Importante.**

**Ampliar información:**

- https://www.bleepingcomputer.com/news/security/fbi-seizes-breachforums-after-arresting-its-owner-pompompurin-in-march/
- https://www.databreaches.net/law-enforcement-seizes-domains-owned-by-pompompurin-and-one-currently-owned-by-databreaches/
- https://therecord.media/breachforums-seized-by-fbi-months-after-arrest-of-alleged-administrator-dark-web-marketplace

---

## Hombre acusado de administrar el mercado de red oscura denominada 'Monopoly'

El Departamento de Justicia de EE. UU. acusó a un ciudadano croata-serbio de 33 años, por presuntamente operar una plataforma de tráfico de drogas llamada Monopoly Market en la red oscura.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://therecord.media/man-charged-with-running-monopoly-market-drug-dark-net-marketplace
- https://www.justice.gov/usao-dc/pr/citizen-croatia-and-serbia-charged-running-monopoly-drug-market-darknet

---

## Hacker de Twitter detrás del "gran hackeo" de 2020 sentenciado a 5 años de prisión

En 2020, cuentas de Twitter como las de Barack Obama y Joe Biden se vieron comprometidas en un "gran hackeo". Tras dicha violación a las cuentas del presidente anterior y al actual, así como a figuras públicas como Elon Musk o Bill Gates, los piratas informáticos enviaron tweets pregonando una estafa de criptomonedas.

**Prioridad: 3 Importante**

**Ampliar información:**

- https://thehackernews.com/2023/06/twitter-hacker-sentenced-to-5-years-in.html
- https://www.hackread.com/plugwalkjoe-jailed-twitter-hack-sim-swapping/
- https://securityaffairs.com/147801/cyber-crime/twitter-hacker-sentenced.html

## SECTOR SALUD

### Aumentan los ataques de posicionamiento SEO en el sector de la salud

Los reguladores federales de EE. UU (HHS) advierten sobre los ataques de posicionamiento en la optimización de motores de búsqueda, la cual, se basa en la manipulación intencional de los resultados de una búsqueda llevando a los usuarios a sitios web infectados con malware.

**Prioridad: 3 Importante**

**Ampliar Información:**

- https://www.bankinfosecurity.com/seo-poisoning-attacks-on-healthcare-sector-rising-hhs-warns-a-22365
- https://www.hhs.gov/sites/default/files/june-2023-seo-poisoning-analyst-note-tlpclear.pdf