Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS -20251031- 013

TLP:CLEAR

Resumen Ejecutivo

Durante la última semana se observó un panorama activo en materia de ciberseguridad, marcado por interrupciones en servicios de Azure, la explotación acelerada de vulnerabilidades críticas y un incremento en el uso de inteligencia artificial para perfeccionar ataques de ingeniería social y *phishing*. Asimismo, se identificaron troyanos y herramientas de captura de credenciales con mayor presencia, lo que evidencia una evolución en las tácticas de acceso inicial. A nivel regional, continuaron los ataques de *ransomware* contra sectores como transporte, comercio y salud, mientras que se reportaron vulnerabilidades críticas (CVSS 9.8) en plataformas. Este escenario refuerza la necesidad de mantener una gestión proactiva de vulnerabilidades, fortalecer la segmentación de redes y promover la capacitación del personal ante la creciente automatización y sofisticación de las amenazas.

Incidentes de la semana

Durante la última semana se identificó un único caso reportado de incidente cibernético en el país, correspondiente a un ataque de *ransomware* dirigido a una empresa del sector Comercio, Industria y Turismo. El hecho fue atribuido al grupo Stormous, reconocido por sus campañas contra organizaciones de distintos sectores productivos.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Ransomware	27/10/2025	Una compañía del sector de Comercio, Industria y Turismo ha sido reportada como la más reciente afectada por un incidente de *ransomware*.	**Stormous**

Tabla 1. Incidentes de la semana. Fuente: COLCERT.

Tendencias observadas

- **Interrupciones en servicios de Azure**: esta semana se registró una caída significativa de los servicios de Azure que afectó también a entidades en Colombia y a sistemas de instituciones académicas, debido a un cambio de configuración en el servicio Azure Front Door, lo que provocó interrupciones en notificaciones, portales web y otros servicios digitales. Esta interrupción sucede inmediatamente después de otro evento similar en Amazon Web Services (AWS) la semana anterior, lo que evidencia una mayor vulnerabilidad del ecosistema de nubes corporativas.

- **Explotación de vulnerabilidades:** Los adversarios están reduciendo significativamente el tiempo entre la divulgación de vulnerabilidades y su explotación, lo que exige que los equipos de seguridad prioricen la aplicación inmediata de parches, refuercen la segmentación de la red y mantengan un monitoreo continuo para detectar posibles intrusiones.

- **Uso de IA para mejorar ataques de ingeniero social y phishing:** los ciberdelincuentes emplean IA para automatizar y personalizar campañas de phishing, realizar reconocimiento del blanco, generar mensajes convincentes y evadir controles tradicionales.

- **Avances en enforcement**: se registró esta semana un avance importante en la aplicación de la ley, las autoridades capturaron en Antioquia (en el marco de una investigación de ocho meses) a alias “El Socio”, identificado como uno de los hackers más buscados de Suramérica, miembro clave del grupo delincuencial Los Ilegales, dedicado al hurto informático, clonación de tarjetas y *skimming* en cajeros automáticos.

Panorama nacional

Durante la última semana, el kit de *phishing* **Tycoon 2FA** se mantuvo como la amenaza más detectada, con un leve incremento respecto a la semana anterior. **XWorm** también registró un ligero aumento, mientras que **EvilProxy**, asociado al robo de credenciales y bypass de autenticación multifactor, mostró una disminución significativa en su actividad. En contraste, **Rhadamanthys** presentó un repunte moderado. Por otro lado, **Remcos**, **Sally 2FA** y **Sneaky 2FA** experimentaron descensos notables, lo que sugiere una posible rotación en las campañas activas. Finalmente, destaca la aparición de **Vidar**, que no había sido detectado la semana anterior, lo que podría indicar el inicio de nuevas campañas de distribución.

Comparativa entre semanas

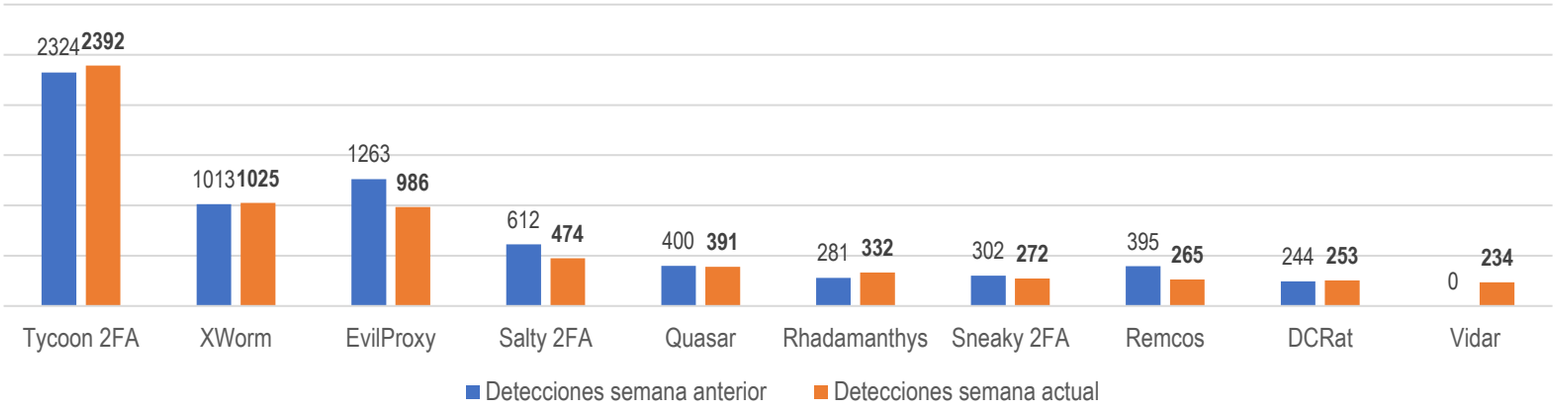

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la última semana se registraron múltiples incidentes en la región, principalmente de *ransomware* dirigidos a los sectores de transporte, salud, alimentación, comercio y gobierno. Destacaron los grupos Dragonforce, Nightspire e Incransom, junto con un caso de *defacement* en México atribuido a God Of Server.

Sector	Amenaza	Locación	Posible actor involucrado
Transporte	Ransomware	Brasil	**Nightspire**
Salud y Protección Social	Ransomware	Argentina	**Dragonforce**
Alimentación y Agricultura	Ransomware	El salvador	**Incransom**
Comercio	Ransomware	Republica Dominicana	**Dragonforce**
Comercio	Ransomware	Puerto Rico	**Sinobi**
Gobierno	Defacement	Mexico	**God Of Server**

Tabla 2. Incidentes detectados a nivel regional. Fuente: COLCERT.

Vulnerabilidades relevantes de la semana

Durante la última semana se identificaron vulnerabilidades críticas que afectan entornos ampliamente utilizados tanto en el sector corporativo como en el gubernamental. Entre ellas destacan fallas en Dell Storage Manager, WooCommerce Designer Pro y Windows Server Update Services (WSUS), todas con un puntaje CVSS de 9.8 (crítico), las cuales permiten desde la ejecución remota de código hasta el acceso no autorizado y la manipulación de configuraciones sensibles.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Dell Storage Manager (DSM)	**CVE-2025-43995**	Vulnerabilidad de autenticación incorrecta en el componente "Data Collector" de DSM que expone API protegidas. Un atacante remoto no autenticado puede acceder a dichas API usando claves de sesión y IDs de usuario especiales, lo que permite eludir mecanismos de seguridad y modificar usuarios o configuraciones críticas.	**9.8 (Critical)**
WooCommerce Designer Pro plugin para WordPress	**CVE-2025-6440**	Vulnerabilidad de carga arbitraria de archivos (arbitrary file upload) en la función wcdp_save_canvas_design_ajax: no se valida el tipo de archivo, lo que permite a un atacante no autenticado subir archivos (incluyendo scripts PHP) al servidor del sitio WordPress afectado, lo que podría derivar en ejecución remota de código, compromiso completo del sitio, manipulación de datos o servicio.	**9.8 (Critical)**
Windows Server Update Services (WSUS)	**CVE-2025-59287**	Una vulnerabilidad de deserialización insegura de datos en WSUS que permite a un atacante remoto y no autenticado enviar solicitudes maliciosas (por ejemplo al endpoint GetCookie() u otros) que desencadenan la ejecución de código como SYSTEM. Afecta sólo instancias con el rol WSUS habilitado.	**9.8 (Critical)**

Tabla 3. Vulnerabilidades relevantes de la semana. Fuente: COLCERT.

Análisis de Actores y campañas Activas

- **Stormous**: es un grupo proruso de *ransomware* con motivaciones duales (hacktivismo y extorsión financiera), activo en 2025 con campañas contra sectores críticos como gobierno, salud y energía.
- **Nightspire:** es un grupo de ransomware emergente a inicios de 2025, se enfoca en extorsión doble contra empresas. Han mantenido campañas activas durante el año, con énfasis en víctimas de alto valor en EE.UU. y Europa, utilizando accesos iniciales vía phishing y exploits. Su actividad se intensificó en Q2, según reportes de inteligencia.
- **Dragonforce:** operando como Ransomware-as-a-Service desde 2023, escaló en 2025 con ataques híbridos (extorsión y disrupción), enfocados en retail y cadenas de suministro. Evolucionaron de hacktivismo a cibercrimen puro, con campañas rápidas que causan interrupciones masivas en servicios.
- **Incransom:** grupo sofisticado de *ransomware* y extorsión de datos activo desde 2023 pero prominente en 2025, realiza campañas de cifrado selectiva y filtraciones en foros *dark web*.
- **Sinobi:** surgió en junio de 2025 como grupo de *ransomware* con extorsión doble, experimentando un rápido ascenso. Campañas activas incluyen despliegues vía credenciales comprometidas, afectando empresas globales; su enfoque en exfiltración previa a encriptación los hace altamente disruptivos.
- **God Of Server:** es un actor de amenaza emergente enfocado en *defacements* de sitios web, operando desde al menos mayo de 2025. Sus campañas activas incluyen ataques a portales gubernamentales y educativos en países como México, Argentina, Indonesia, India, Australia, Tailandia y Pakistán.

Recomendaciones

- Implementar planes de contingencia que contemplen el uso de entornos híbridos o multicloud. Configurar alertas automatizadas ante degradaciones o interrupciones de servicios esenciales. Documentar lecciones aprendidas tras los eventos de indisponibilidad para fortalecer la resiliencia operativa.
- Priorizar la aplicación de parches y actualizaciones de seguridad en sistemas y aplicaciones expuestas. Segmentar la red para limitar el movimiento lateral en caso de explotación exitosa. Implementar herramientas de gestión de vulnerabilidades que permitan detección temprana. Monitorear continuamente indicadores de explotación activa y reforzar controles de detección en endpoints y perímetros.
- Capacitar al personal en el reconocimiento de mensajes maliciosos. Implementar filtros avanzados de correo con detección de lenguaje anómalo o sintético. Simular campañas de *phishing* para fortalecer la conciencia organizacional. Promover políticas internas de verificación de identidad y canales oficiales de comunicación.
- Actualizar firmas antivirus y reglas YARA para incluir las variantes más recientes detectadas. Revisar políticas de acceso remoto y autenticación multifactor en infraestructuras críticas. Implementar controles de ejecución restringida (AppLocker, SRP o EDR) para bloquear comportamientos sospechosos. Analizar registros de red y endpoints en busca de conexiones o procesos asociados a RAT y stealer observados.
- Implementar copias de seguridad cifradas y desconectadas de la red principal. Restringir privilegios de usuario y aplicar el principio de mínimo privilegio. Actualizar todos los sistemas y fortalecer la autenticación en servicios expuestos a internet. Monitorear foros y canales de leak sites para detectar filtraciones tempranas de datos corporativos.

Resumen de las fuentes y nivel de confianza en la información proporcionada

Ransomware.live, 30/10/2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración, https://www.ransomware.live/
Any Run, 30 de octubre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
El Colombiano, 28/10/2025, Alias 'El Socio', hacker buscado en Latinoamérica, Fuente periodística nacional.
https://www.elcolombiano.com/antioquia/alias-el-socio-hacker-buscado-en-latinoamerica-II30380008
El Tiempo, 28/10/2025, Capturan a alias 'El Socio', uno de los hackers más buscados en Suramérica, Fuente periodística nacional.
https://www.eltiempo.com/colombia/medellin/antioquia-capturan-a-alias-el-socio-uno-de-los-hackers-mas-buscados-en-suramerica-3503352
NIST NVD, 14/10/2025, CVE-2025-59287 – Windows Server Update Services (WSUS) Insecure Deserialization Vulnerability, Fuente técnica oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-59287
NIST NVD, 24/10/2025, CVE-2025-43995 – Dell Storage Manager Authentication Bypass Vulnerability, Fuente técnica oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-43995
NIST NVD, 24/10/2025, CVE-2025-6440 – WooCommerce Designer Pro Arbitrary File Upload Vulnerability, Fuente técnica oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-6440
Reuters, 29/10/2025, Microsoft Azure experiences outage affecting thousands of users, Fuente periodística internacional.
https://www.reuters.com/technology/microsoft-azure-down-thousands-users-downdetector-shows-2025-10-29/
Daily Security Review, 03/07/2025, Stormous Ransomware: The pro-Russian cyber gang targeting global networks, Fuente especializada en ciberseguridad.
https://dailysecurityreview.com/security-spotlight/stormous-ransomware-the-pro-russian-cyber-gang-targeting-global-networks/
Cyble, 04/05/2025, Nightspire Ransomware Group – Threat Actor Profile, Fuente especializada en ciberinteligencia.
https://cyble.com/threat-actor-profiles/nightspire-ransomware-group/
Trend Micro, 25/10/2025, 30/10/2025, Ransomware Spotlight: Dragonforce, Fuente especializada en ciberseguridad.
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforce
Cyble, 29/10/2025, IncRansom – Threat Actor Profile, Fuente especializada en ciberinteligencia.
https://cyble.com/threat-actor-profiles/inc-ransom/
Moxfive, 01/10/2025, Threat Actor Spotlight: Sinobi, Fuente especializada en ciberseguridad.
https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-sinobi