Grupo de ransomware: BlackNevas Ransomware

Resumen ejecutivo

BlackNevas es un ransomware emergente, observado por primera vez a finales de 2024, que opera como **Ransomware-as-a-Service (RaaS)** y se ha consolidado rápidamente como un grupo de doble extorsión. Al igual que otras familias de ransomware modernas, cifra archivos locales y de red y publica información robada en portales de la dark web, presionando a las víctimas para pagar rescates y evitar la filtración de datos sensibles.

Los **accesos iniciales** de BlackNevas suelen lograrse mediante **credenciales comprometidas**, **explotación de servicios expuestos** a internet y, en algunos casos, mediante campañas de **phishing**. Operativamente, el grupo reutiliza y adapta código y metodologías de familias previas, mostrando **similitudes con Trigona**, lo que facilita la rápida escalada de campañas y la adaptación a entornos corporativos.

Técnicamente, el malware utiliza algoritmos de cifrado robustos que combinan **AES y técnicas de clave pública** para bloquear archivos, haciendo prácticamente imposible su recuperación sin la clave del atacante. También incluye mecanismos para eliminar copias de seguridad y dificultar la restauración, incrementando la presión sobre las víctimas.

Desde la perspectiva del modelo de negocio cibercriminal, BlackNevas mantiene portales en la dark web donde publica **listas de víctimas y muestras de datos robados y plazos de pago**, siguiendo el modelo de doble extorsión. Desde su aparición, varias empresas globales han sido registradas como víctimas, destacando su capacidad de operar a nivel internacional y un riesgo creciente para sectores críticos y corporativos.

Grupo de ransomware: BlackNevas

BlackNevas opera bajo un modelo **Ransomware-as-a-Service (RaaS)**, proporcionando a sus afiliados herramientas, infraestructura y asistencia técnica para ejecutar campañas de **doble extorsión**. Estas campañas combinan el cifrado de los sistemas comprometidos con la exfiltración y posterior publicación de los datos robados en entornos de la dark web, con el fin de incrementar la presión sobre las víctimas.

Este grupo muestra similitudes con el ransomware Trigona y se distingue por su estrategia de colaboración con otros grupos cibercriminales, como por ejemplo Hunters International, DragonForce, Embargo Team, …. Durante sus operaciones, BlackNevas deja una nota de rescate con el nombre “**how_to_decrypt.txt**”, en la que instruye a las víctimas sobre el proceso de pago. En caso de no recibir el pago exigido, amenaza con divulgar la información sustraída a través de plataformas de filtración asociadas.

Países y sectores afectados

La actividad de BlackNevas es global, con víctimas confirmadas en Estados Unidos, Alemania, Reino Unido, Australia y varios países de Europa.

En **España**, se han documentado al menos 3 incidentes, incluyendo:

- Undefasa (industria manufacturera),
- Cartonajes Bernabeu SAU (industria manufacturera)
- Cash and carry – Cosean Grup (retail).

Los sectores más atacados incluyen **finanzas, manufactura, tecnología, salud y educación,** apuntando principalmente a empresas medianas y grandes que manejan datos críticos, empleando la doble extorsión para aumentar la presión y maximizar la posibilidad de pago.

Análisis técnico

Desde el punto de vista técnico, BlackNevas hereda la base criptográfica de Trigona e **implementa cifrado híbrido**, AES-256 para cifrar los ficheros junto a RSA para cifrar las claves que permiten descifrarlos. El malware soporta **diferentes arquitecturas de sistema** y tiene versiones específicas para **entornos de virtualización** (ESXi) y **dispositivos NAS**, con parámetros especiales para cada caso. En **sistemas operativos Windows y Linux** proporciona múltiples funcionalidades que los operadores pueden utilizar, como por ejemplo, borrar datos del dispositivo de la víctima, cifrar sin renombrar los archivos, cambiar la prioridad de ejecución o apagar la máquina tras el cifrado. Además, este ransomware genera persistencia y permite buscar y cifrar archivos en recursos compartidos de red (SMB).

Características técnicas principales:

- **Modelo operativo**: Variante del ransomware Trigona que opera de forma independiente y con características de RaaS.
- **Cifrado:** Usa AES-256 y RSA para bloquear archivos y proteger las claves, impidiendo su recuperación.
- **Sistemas afectados:** Ataca Windows, Linux, NAS y servidores ESXi.
- **Acceso inicial:** Mediante phishing, vulnerabilidades sin parchear y servicios remotos expuestos.
- **Exfiltración:** Roba y publica datos en su sitio de filtraciones en la dark web para extorsionar a las víctimas

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1190** — Exploitation of Public-Facing Application **T1566** — Phishing **T1078** — Valid Accounts
Execution	**T1059** — Command and Scripting Interpreter **T1203** — Exploitation for Client Execution
Persistence	**T1547** — Boot/Logon Autostart **T1547.001** — Registry Run Keys/Startup Folder
Privilege Escalation	**T1068** — Exploitation for Privilege Escalation
Defense Evasion	**T1070** — Indicator Removal on Host **T1027** — Obfuscated Files or Information **T1562** — Impair Defenses
Discovery	**T1135** — Network Share Discovery **T1012** — Query Registry **T1083** — File and Directory Discovery
Command and Control	**T1071** — Application Layer Protoco
Impact	**T1486** — Data Encrypted for Impact **T1561.001** — Disk Content Wipe

Medidas de mitigación

Proactivas

- ❑ Aplicar parches de seguridad, proteger servicios públicos con firewall/WAF, implementar autenticación multifactor y formación frente a phishing. (T1566 – Phishing, T1190 – Exploit Public-Facing Application, T1078 – Valid Accounts)

- ❑ Restringir scripts y macros no firmados, controlar el uso de intérpretes como PowerShell o CMD, y monitorizar claves y carpetas de inicio automático. (T1203 – Exploitation for Client Execution , T1059 – Command and Scripting Interpreter, T1547 – Boot or Logon Autostart Execution)

- ❑ Limitar cuentas con privilegios, mantener sistemas actualizados y proteger logs frente a borrados. (T1068 – Exploitation for Privilege Escalation, T1070 – Indicator Removal, T1562 – Impair Defenses)

- ❑ Aplicar el principio de mínimo privilegio, segmentar la red y monitorizar accesos a recursos compartidos. (T1083 – File and Directory Discovery, T1135 – Network Share Discovery)

- ❑ Mantener copias de seguridad offline, probar restauraciones periódicas, filtrar tráfico saliente y detectar patrones de comunicación sospechosos. (T1486 – Data Encrypted for Impact, T1561.001 – Disk Wipe: Disk Content Wipe, T1071 – Application Layer Protocol):

Reactivas

- ❑ Usar antivirus con AMSI, aplicar reglas ASR y formar a los usuarios para bloquear archivos ofuscados. (T1027 - Obfuscated Files or Information)

Conclusiones y recomendaciones

BlackNevas ha ganado notoriedad en 2025 como una de las variantes de ransomware más activas, destacando por su capacidad de adaptación y su impacto en múltiples sectores y regiones. Su actividad muestra una operación bien estructurada, con una rápida expansión global y un aumento de víctimas en Europa, Asia y América, incluyendo varias empresas españolas, lo que confirma su alcance internacional.

El grupo parece mantener **vínculos con la familia de ransomware Trigona**, compartiendo técnicas de cifrado y tácticas de doble extorsión, aunque opera de forma independiente y con recursos propios. Esta tendencia refleja la diversificación del ecosistema del ransomware, donde distintas familias comparten infraestructuras y herramientas para maximizar su efectividad.

Para reducir el riesgo ante BlackNevas, se recomienda reforzar los accesos remotos con **MFA**, mantener los sistemas **actualizados y segmentados**, proteger las copias de seguridad offline y contar con **monitorización y respuesta rápida** ante posibles incidentes.

