MNEMO

Boletín mensual de Ciberamenazas

Ciberboletín

PRESS TO START

mnemo.com/ciberboletin

MARZO 2026

MNEMO

SUMARIO

Una compañía global a la vanguardia en Transformación Digital, Data & Ciberseguridad, desde 2001

Somos una empresa española con proyección internacional, a través de nuestras oficinas en **España, Colombia y Panamá.** En la actualidad tenemos proyectos en más de 10 países, dando servicios de ciberseguridad 24×7 a través de nuestra red global de **Centro de Operaciones SOC/CERT.**

+700 Empleados

+100 Clientes

8 Productos propios de I+D+i

10 Países con operaciones

3 Centros propios SOC/CERT

CSIRT Sectorial

CoE en Seguridad Cloud

MNEMO Focus Europa La Identidad Sintética

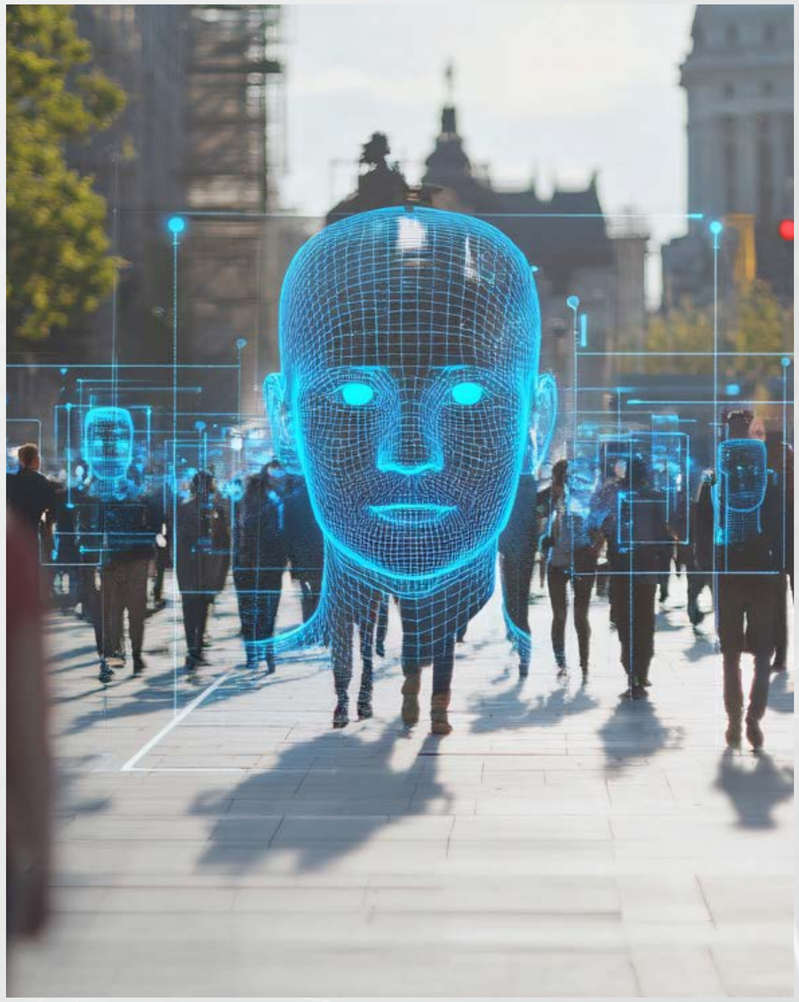
Belén Viqueira Sierra
Directora de Inteligencia

El nuevo campo de batalla de la ingeniería social

La **ciberseguridad tradicional** se basaba en la **identificación de fallos humanos en el engaño**: errores ortográficos, voces artificiales o la falta de capacidad para escalar los ataques. Estas eran nuestras defensas naturales.

Sin embargo, la llegada de la **Inteligencia Artificial generativa** ha borrado estas fronteras. Hoy, nos enfrentamos a una Tríada de la Suplantación: algoritmos que simulan la comunicación de un alto ejecutivo, clones de voz indistinguibles y sistemas automatizados que manipulan a miles de víctimas a la vez. En este nuevo panorama de ingeniería social sintética, la vulnerabilidad ya no reside solo en el usuario como eslabón débil, sino en el **hackeo de nuestra propia percepción de la realidad**.

Imaginaros estar en una **videoconferencia con el director financiero de vuestra empresa y varios colegas y que todos ellos fueran deepfakes**. Esto mismo le ocurrió a un empleado de Arup en Hong Kong, resultando en una pérdida de 25,6 millones de dólares para la empresa.



Todo comenzó con un correo en el cual, el CFO de la compañía le comentaba al empleado que debía hacer una transferencia de dinero, urgente y confidencial, lo que hizo que el empleado sospechara. Por ello y para eliminar cualquier duda, se organizó una videollamada entre el CFO, el empleado y varios compañeros. Con cámara y audio, lo que facilitó que la víctima realizará las transferencias requeridas a cuentas de los cibercriminales.

Sin embargo, las nuevas amenazas requieren de nuevas estrategias de protección. Por ejemplo, algo tan sencillo como una palabra clave o una pregunta personal puede evitar que seamos víctimas de un fraude, como le sucedió a Ferrari, que gracias al ingenio del directivo al que querían estafar, evitó lo que seguramente sería, pérdidas millonarias.

Este directivo, recibió un mensaje de audio en WhatsApp de, supuestamente, Benedetto Vigna, CEO de la marca. El motivo, el tradicional, una operación financiera ultrasecreta. La voz era de Vigna y todo parecía real, sin embargo, el directivo quiso asegurarse y le preguntó cuál era el título del libro que Vigna le había recomendado hacía unos días. Entonces, la llamada se cortó.

MNEMO Focus Europa La Identidad Sintética

Belén Viqueira Sierra
Directora de Inteligencia

El nuevo campo de batalla de la ingeniería social

Estos casos demuestran que la **biometría humana** -nuestro rostro y nuestra voz- **ha dejado de ser una prueba de identidad irrefutable**. Si un atacante puede estar "presente" en una reunión de Zoom o enviarnos una nota de voz personalizada, la confianza ya no puede basarse en lo que vemos u oímos, sino en protocolos de verificación que existan fuera del alcance del algoritmo.

Pero la IA no solo imita nuestra apariencia física; también ha aprendido a **dominar nuestra forma de escribir**. Si el deepfake es el ataque de alto impacto contra directivos, el uso de Modelos de Lenguaje Extensos (LLM) es el arma de precisión para el engaño cotidiano. Hemos pasado de los correos mal redactados que terminaban en la carpeta de spam a una nueva generación de **phishing sintético**: mensajes con una gramática impecable, un tono corporativo indistinguible y una capacidad de persuasión que hace que incluso el usuario más escéptico baje la guardia.

En este escenario, aparecen nuevas IA generativas con un lado oscuro: WormGPT y FraudGPT. Ambas se comercializan en la Deep y Dark Web y no tienen ningún tipo de restricción ética ni moral, al contrario, están diseñadas para cometer todo tipo de delitos en la red.

Por un lado, FraudGPT, que destaca por su capacidad para escribir códigos maliciosos, crear malware indetectable, páginas de phishing, herramientas de hacking y correos de estafas, sin embargo, también tiene capacidades para encontrar vulnerabilidades o filtraciones de objetivos específicos, localizar sitios donde puedan realizarse pagos online, automatizar scripts para obtener logs o cookies en sitios vulnerables, ofuscar código y crear bots. Su precio está en torno a los 200 dólares mensuales o 1.700 dólares anuales.

WormGPT, por su parte, está diseñado para la vulneración de cuentas en plataformas sociales (como TikTok, Telegram, WhatsApp o Facebook), el compromiso de diversos dispositivos (incluyendo PCs, portátiles, teléfonos celulares, cámaras e IoT), la generación de código malicioso, el lanzamiento de campañas de ingeniería social (como phishing o spam), y la ejecución de ataques de denegación de servicio distribuido (DDoS).

Y esto es solo el principio, ya que es esperado que a medida que la Inteligencia Artificial evoluciona, también lo hagan este tipo de inteligencias orientadas al cibercrimen.

Conclusión:

El retorno al factor humano en un mundo sintético

La Inteligencia Artificial ha logrado algo que parecía imposible: automatizar la confianza. Al eliminar las señales tradicionales del engaño, como la mala redacción o la voz robótica, los atacantes han desplazado el campo de batalla de nuestros firewalls digitales a nuestros sesgos cognitivos. Casos como el de la estafa millonaria en Hong Kong o el intento de suplantación en Ferrari no son anomalías, sino el nuevo estándar de una industria del cibercrimen que ya no descansa.

Sin embargo, la misma tecnología que perfecciona la mentira nos obliga a rescatar lo más esencialmente humano: el pensamiento crítico y la verificación directa. En un mundo donde un vídeo o una voz pueden ser fabricados en segundos, la seguridad ya no reside en el software que usamos, sino en los protocolos que establecemos. La mejor defensa contra un algoritmo de suplantación no es otra IA, sino una cultura de escepticismo saludable donde una simple pregunta personal o una llamada de confirmación valen más que cualquier sistema de cifrado.

	Phishing Tradicional	Ingeniería Social con IA
Gramática	Errores comunes y lenguaje robótico.	Perfección lingüística y tono corporativo.
Verificación	Se detectaba por el remitente o el link.	Se apoya en voz y vídeo (identidad sintética).
Alcance	Manual o mediante plantillas genéricas.	Hiper-personalización automática masiva.

MNEMO Focus Europa MNEMO completa en marzo sus proyectos IECPI con INCIBE

Fernando García Vicent
Director de Innovación y Producto

Las iniciativas concluyen en marzo impulsando la innovación en ciberseguridad.

MNEMO afronta en este mes de marzo el cierre de la Fase 4 (Paso a TRL 8) y por consiguiente el cierre de los proyectos **PRESEACYBER y VULNTRACK,** ambos incluidos en la Iniciativa Estratégica de Compra Publica de Innovación (IECPI) del Instituto Nacional de Ciberseguridad (INCIBE) para la contratación de **"Servicios de investigación y desarrollo en materia de ciberseguridad" (ACTUACIÓN 1).**

INCIBE, como entidad pública para el desarrollo de la ciberseguridad, decidió desarrollar la iniciativa IECPI en 2021, con el objetivo de ejecutar un conjunto de actuaciones dirigidas a impulsar la I+D+i y la creación de productos y soluciones en el ámbito de la ciberseguridad. El 1 de julio de 2022 fue publicado en la Plataforma de Contratación del Sector Público el citado Documento Regulador, a adjudicar por los cauces del procedimiento de diálogo competitivo.

Todos los detalles de la IECPI se pueden encontrar en la web de INCIBE: https://www.incibe.es/industria-cpi.

MNEMO cerró el pasado 30 de enero los desarrollos planificados para la fase 3 en ambos proyectos, completando el despliegue de las plataformas **PRESEACYBER y VULNTRACK** en un entorno pre-comercial, con características a escala idénticas a un sistema real, y cubriendo todos los objetivos que se perfilaron en la memoria de cada proyecto. Después de dos años y medio, MNEMO completará el próximo 31 de marzo de 2026 un proceso que se inició en octubre de 2023, cumpliendo de esta forma con el final de los trabajos y el cierre del proyecto global.

En la Fase 4 se abordan tareas esenciales para el cierre de ambas plataformas como son la certificación de calidad de producto en base al estándar ISO25000, la certificación de seguridad sobre metodología del CCN-CERT para su inclusión en el catálogo CPSTIC y la certificación de accesibilidad sobre el estándar WCAG 2.1. Todos los procesos cuentan con certificación externa, asegurando la fiabilidad y conformidad mediante auditores independientes.

El proyecto PRESEACYBER ha permitido construir una **nueva y ambiciosa solución tecnológica de gestión integral de la ciberseguridad** que mejora de forma significativa la gestión del riesgo corporativo y protege a las organizaciones frente a todo tipo de amenazas de carácter digital.

El proyecto **VULNTRACK** por su lado constituye una **plataforma de gestión integral de vulnerabilidades que cubre el ciclo completo de la vulnerabilidad y permite conocer en tiempo real el riesgo efectivo de una organización** en función de su estado de salud respecto a las vulnerabilidades detectadas, el nivel de amenaza asociado a las mismas y el contexto interno/externo.

El resultado final de la plataforma integrada, que dispondrá de un nombre comercial específico y una estrategia de lanzamiento y preventa detalladas, permitirá disponer de una solución que podrá comercializarse en modo On-Premise o SaaS, con una estrategia de despliegue completamente modular, con los siguientes servicios disponibles:

- Vigilancia Digital
- Inteligencia de Amenazas / CSIRT Sectorial
- Monitorización de Eventos de Seguridad
- Gestión de Incidentes
- Gestión de Vulnerabilidades
- Alerta Temprana

MNEMO Focus Europa MNEMO completa en marzo sus proyectos IECPI con INCIBE

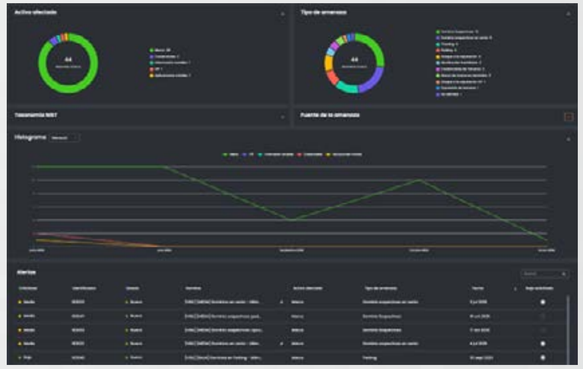
Fernando García Vicent
Director de Innovación y Producto

Las iniciativas concluyen en marzo impulsando la innovación en ciberseguridad.

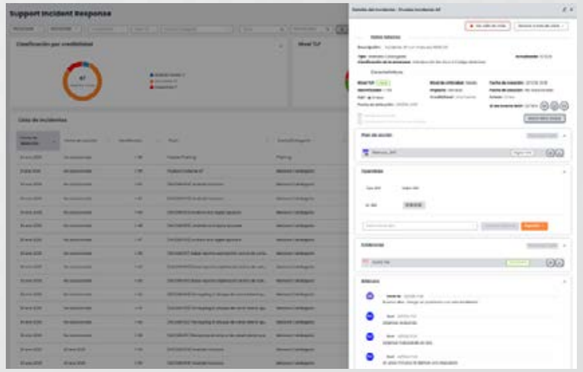
Un usuario de la plataforma integral de ciberseguridad puede obtener información para la toma inmediata de decisiones en base a cuadros de mando que le dan una posición inmediata sobre el nivel de amenaza corporativo:

O sobre el estado de salud corporativo en cuanto a las vulnerabilidades existentes y la eficacia en su remediación:

O sobre el detalle de las alertas que componen un determinado nivel de Riesgo en cada servicio:



O bien trabajar de forma colaborativa entre todos los departamentos y terceros involucrados en cada servicio:



En todos los casos, la potencia de la nueva plataforma radica en disponer de toda la información en un punto común, con capacidad de decisión y aumento de la eficacia operativa.

MNEMO Focus LATAM PromptSpy

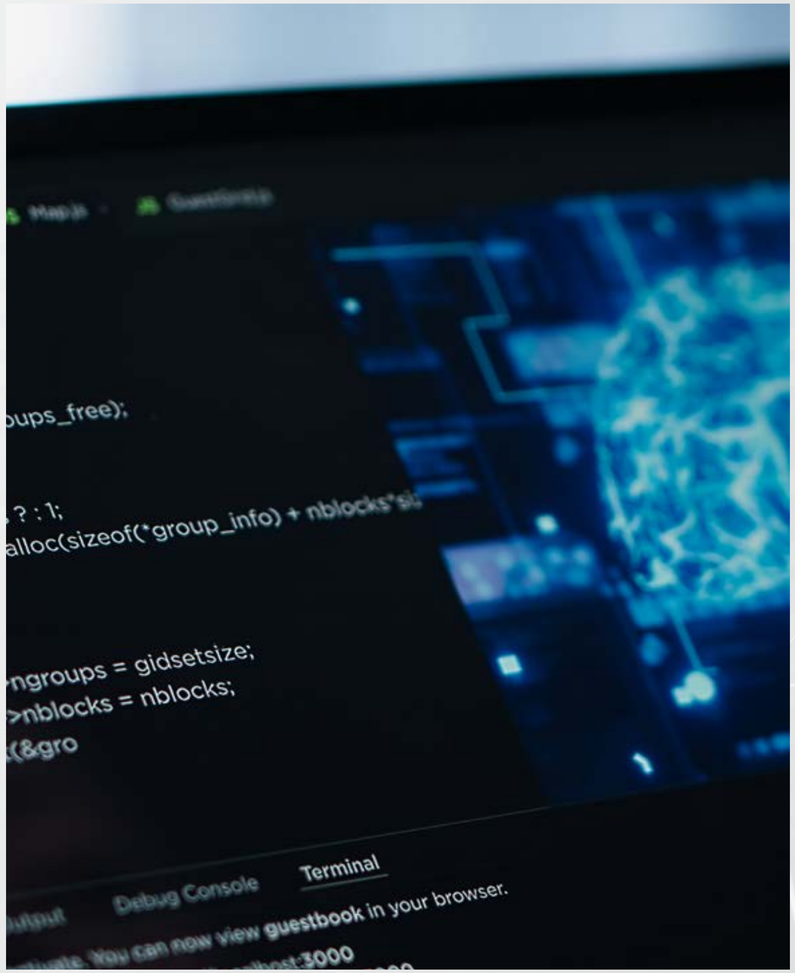
Edward Martínez
SOC Manager

El Surgimiento de la Inteligencia Artificial Ofensiva y el Secuestro de la Interfaz

En el complejo ecosistema de las amenazas móviles de 2026, la aparición de **PromptSpy** marca un punto de inflexión crítico. Mientras que familias de ransomware como VolkLocker exponen fallas de implementación humana, PromptSpy representa una sofisticación distinta: la delegación del razonamiento táctico a modelos de lenguaje de gran escala (LLM). Lo que estamos presenciando no es solo un malware, sino un "agente cognitivo" diseñado para subvertir la voluntad del usuario mediante el uso de la Inteligencia Artificial Generativa (GenAI).

El Surgimiento de la "Neurona Maliciosa"

PromptSpy no opera bajo los parámetros de la programación estática tradicional. Se integra en la categoría de **Malware Adaptativo**, aprovechando la infraestructura de Google Gemini para interpretar y manipular interfaces de usuario en tiempo real. Este cambio de paradigma permite que el atacante no necesite pre-programar cada interacción; el malware "razona" sobre cómo bloquear al usuario basándose en lo que ve en la pantalla.



Bajo la fachada de aplicaciones legítimas de banca o herramientas de productividad, este vector de ataque utiliza la psicología de la "espera técnica" para ocultar su actividad inicial. Mientras el usuario observa una pantalla de carga convencional, se está produciendo un proceso de exfiltración de metadatos de la interfaz que redefine el concepto de intrusión.

Anatomía de la Amenaza: Razonamiento vía API

La arquitectura de PromptSpy es una obra de ingeniería social y técnica que se divide en tres fases críticas:

1. **Extracción de la Jerarquía Visual**: El malware utiliza los servicios de accesibilidad para extraer el árbol XML de la pantalla actual. Este archivo contiene la ubicación exacta de cada botón, campo de texto y opción de seguridad.

2. **Consulta al Oráculo (GenAI)**: A diferencia de sus predecesores, PromptSpy envía este XML a los servidores de Gemini mediante un prompt diseñado meticulosamente. El modelo de IA interpreta el mapa visual y devuelve coordenadas precisas para neutralizar las defensas del sistema.

MNEMO Focus LATAM PromptSpy

Edward Martínez
SOC Manager

El Surgimiento de la Inteligencia Artificial Ofensiva y el Secuestro de la Interfaz

3. **Ejecución Dinámica:** Utilizando las coordenadas proporcionadas por la IA, el malware dibuja capas invisibles (overlays) sobre los botones de "Desinstalar" o "Configuración".

¿Alguna vez ha sentido que su dispositivo no responde a pesar de que la pantalla parece intacta? Esa disonancia cognitiva es el producto de una "pared invisible" generada por IA, un gaslighting digital donde el usuario duda de su hardware mientras el software lo mantiene cautivo.

	Función Técnica	Impacto Psicologico
Integración LLM	Navegación dinámica de UI vía API de Gemini.	Sensación de omnipotencia del atacante.
Capas de Accesibilidad	Bloqueo de botones críticos de sistema.	Frustración y desamparo del usuario (Lock-in).
Persistencia Adaptativa	Auto-configuración según la versión de Android.	Inutilidad percibida de los tutoriales de limpieza.

Tras los Pasos de LongNosedGoblin: El Factor Geopolítico

La atribución de PromptSpy apunta hacia el grupo de amenaza LongNosedGoblin, un actor con base en Asia Oriental que ha demostrado una capacidad inusual para la integración de herramientas de IA en campañas de espionaje financiero. La presencia de cadenas de depuración en lenguajes específicos sugiere que PromptSpy es un prototipo avanzado para operaciones de "Denegación de Acceso Personalizado" **(P-DoS).**

Este grupo no busca el cifrado masivo de archivos al estilo de VolkLocker; busca la permanencia silenciosa. El objetivo es que el usuario siga utilizando su dispositivo mientras una IA en la nube decide qué botones puede presionar y cuáles no, transformando el smartphone en una terminal de vigilancia activa.

Estrategias de Defensa y Mitigación

La naturaleza dinámica de PromptSpy requiere una defensa proactiva que vaya más allá del escaneo de firmas. Las organizaciones deben adoptar un enfoque de Confianza Cero (Zero Trust) en los servicios de accesibilidad:

- **Auditoría de Permisos Críticos:** Implementar soluciones MTD (Mobile Threat Defense) que alerten sobre aplicaciones que soliciten "Control Total" sobre la interfaz sin una justificación clara de accesibilidad.
- **Monitoreo de Tráfico a APIs de IA**: Analizar patrones de tráfico inusuales hacia dominios de Google Generative AI provenientes de aplicaciones que no deberían tener integración con LLMs.
- Resiliencia del Usuario: Educar sobre la técnica de las "capas invisibles". Si un botón de sistema no responde tras una descarga reciente, el reinicio en **Modo Seguro** debe ser la respuesta inmediata para romper el ciclo de ejecución de la IA.

En conclusión, aunque PromptSpy utiliza la potencia de la IA para crear una trampa psicológica y técnica casi perfecta, su dependencia de la conectividad y de los servicios de accesibilidad sigue siendo su talón de Aquiles. La seriedad de esta amenaza radica no solo en su código, sino en su capacidad de hacernos dudar de nuestra propia percepción tecnológica.

Radar CERT Tips mundiales de febrero de 2026

03 FEBRERO

Criticidad:Alto

"Amatera" su descubrimiento, Modus Operandi y PotencialesImpactos

El equipo del CTI notifica nuevos indicadores de compromiso relacionados con la amenazallamada Amatera, este es un malware tipo information stealer (infostealer) que ha surgido comouna evolución de la familia ACR Stealer (AcridRain) y ha ganado prominencia en campañasactivas desde mediados de 2025, especialmente en operaciones de entrega sofisticadas contécnicas de evasión y múltiples vectores de distribución.

Accede a toda la información ⟶

23 FEBRERO

Criticidad: Alto

React2Espionage se centra en la explotación de CVE-2025-55182, apodada "React2Shell"

La campaña maliciosa en curso llamada React2Espionage se centra en la explotación de CVE-2025-55182, apodada "React2Shell", una vulnerabilidad crítica de ejecución remota de código (RCE) sin autenticación en React Server Components con una puntuación CVSS de 10. Lo que comenzó en diciembre de 2025 como una ola de explotación oportunista y automatizada que desplegaba criptomineros y botnets ha evolucionado hacia una amenaza más sofisticada. Actualmente, un actor de amenazas desconocido (posiblemente patrocinado por un estado) está utilizando un toolkit recién descubierto llamado "ILovePoop" para realizar un reconocimiento masivo.

Accede a toda la información ⟶

25 FEBRERO

Criticidad: Alto

Medusa Alliance que representa una evolución significativa en las tácticas del Grupo Lazarus

La campaña maliciosa en curso llamada "Medusa Alliance" representa una evolución significativa en las tácticas del Grupo Lazarus, patrocinado por Corea del Norte, al adoptar por primera vez el ransomware Medusa, operado bajo el modelo de Ransomware-as-a-Service (RaaS) por el grupo Spearwing . Esta actividad maliciosa, descubierta por el equipo de investigadores de Symantec y Carbon Black, se materializó en un ataque exitoso contra una gran empresa en Medio Oriente y un intento fallido contra una organización del sector salud en Estados Unidos.

Accede a toda la información ⟶

Radar CERT Tips mundiales de febrero de 2026

28 FEBRERO

Criticidad:Alto

"Avast Scam" es una sofisticada operación de phishing que suplanta la identidad corporativa de Avast

La campaña "Avast Scam" es una sofisticada operación de phishing que suplanta la identidad corporativa de Avast, empresa de seguridad antivirus, para engañar a usuarios francófonos y robar información completa de tarjetas de crédito. Los atacantes crearon una réplica casi perfecta del portal oficial de Avast donde, al acceder, la víctima recibe una notificación urgente de un cargo no autorizado de 499,99€ por una suscripción. Utilizando código JavaScript, la fecha del cargo se genera dinámicamente desde el reloj local de la víctima, haciendo que el "recibo" parezca emitido el mismo día de la visita.

Accede a toda la información ⟶

28 FEBRERO

Criticidad:Alto

Phexia, una amenaza híbrida y sofisticada que ataca específicamente el ecosistema macOS

La actividad maliciosa identificada corresponde al malware Phexia, una amenaza híbrida y sofisticada que ataca específicamente el ecosistema macOS, combinando las funcionalidades de un ladrón de información avanzado y una puerta trasera de control remoto. Esta operación maliciosa se caracteriza por su capacidad para infiltrarse sigilosamente en los sistemas, desplegando módulos diseñados para la recolección masiva de datos confidenciales, como credenciales de acceso, información bancaria y claves de criptomonedas, mientras establece un canal de comunicación persistente con los atacantes para garantizar el control a largo plazo del dispositivo y la posterior descarga de cargas maliciosas adicionales.

Accede a toda la información ⟶

Intelligence Insights ValleyRAT

El RAT sigiloso

Natalia Meliza Arias
Analista L2

ValleyRAT es un troyano de acceso remoto (RAT) aparentemente de origen chino, identificado a principios de 2023 y dirigido a sistemas operativos Windows. Diversas investigaciones lo atribuyen al grupo de amenazas SilverFox (TA558). Este malware se distingue por su arquitectura modular y sigilosa, diseñada para operar principalmente en memoria, lo que le permite evadir soluciones de seguridad tradicionales basadas en firmas y minimizar su huella en disco.

Entre sus capacidades se encuentran el control y la monitorización remota del sistema comprometido, el registro de pulsaciones de teclado (keylogging), la captura de pantalla, la finalización de procesos del sistema y la eliminación de registros de eventos con el fin de dificultar la detección y el análisis forense. Su diseño modular facilita la incorporación de funcionalidades adicionales según los objetivos de la campaña.

Campañas relevantes asociadas

Durante 2024 y 2025, ValleyRAT ha sido observado en múltiples campañas como la operación BYOVD (Bring Your Own Vulnerable Driver), en la que los atacantes explotaron un controlador WatchDog firmado por Microsoft, pero vulnerable, utilizándolo para deshabilitar mecanismos de protección en endpoints antes de desplegar el RAT como carga final.

Otra campaña significativa fue PNGPlug Loader, que empleó un esquema de infección multietapa iniciado desde sitios de phishing que distribuían instaladores MSI maliciosos. Estos instaladores desplegaban aplicaciones aparentemente legítimas mientras descifraban y cargaban en memoria los componentes de **ValleyRAT**, reforzando su naturaleza fileless.

Asimismo, se identificaron campañas que utilizaban instaladores falsos de Google Chrome, donde el malware se ejecutaba completamente en memoria mediante técnicas de DLL sideloading e inyección en procesos legítimos como svchost.exe. Posteriormente, **SilverFox** amplió su alcance hacia sectores críticos como salud y entidades públicas, distribuyendo software médico trojanizado y visores falsos alojados en servicios en la nube.

Vector de infección

ValleyRAT se distribuye mediante múltiples vectores, destacando campañas de phishing y descargas engañosas que suplantan instaladores de navegadores o software especializado. También se ha observado la explotación de binarios legítimos para facilitar la ejecución del código malicioso, así como el uso de técnicas de evasión que inducen al usuario a iniciar la infección de manera inadvertida.

Durante el análisis realizado por el equipo de Inteligencia de Amenazas se identificó que la muestra obtenida corresponde a un binario para Windows. La presencia de la sección UPX0 evidenció que el ejecutable había sido empaquetado con el famoso packer UPX.

Distribución y vector de ataque

Gh0st RAT suele acceder a los sistemas comprometidos mediante ingeniería social, principalmente a través de campañas de phishing con archivos adjuntos maliciosos que simulan documentos o software legítimo. Al ser ejecutados por el usuario, estos archivos activan la cadena de infección y permiten la instalación del RAT.
De forma complementaria, este RAT también se distribuye mediante de la descarga de software desde fuentes no confiables, como aplicaciones falsificadas, cracks o instaladores fraudulentos, que incorporan loaders o droppers encargados de desplegar Gh0st RAT de manera silenciosa, reduciendo la probabilidad de detección temprana.

Imagen 1. Información de la muestra. CTI

Intelligence Insights ValleyRAT

El RAT sigiloso

Natalia Meliza Arias
Analista L2

Tras el desempaquetado, se obtuvo un volcado de memoria (.DUMP) en el que se identificaron funciones sospechosas importadas desde librerías legítimas del sistema como KERNEL32.DLL y SHELL32.DLL. Entre las funciones más relevantes destacan:

- **VirtualAlloc**: utilizada para reservar memoria y ejecutar payloads sin escribirlos en disco.
- **CopyFileA**: empleada para replicación y persistencia.
- **LoadLibraryA / LoadLibraryW y GetProcAddress:** resolución dinámica de funciones en tiempo de ejecución para evadir detección estática.
- **IsDebuggerPresent:** implementación de técnicas antidebugging para obstaculizar el análisis manual.

Imagen 2. Funciones sospechosas. CTI

Dentro de las cadenas embebidas se identificó la URL:

hxxps://yuyuc-12531804881[.]cos[.]ap-guangzhou[.]myqcloud[.]com/yuyuc[.]bin

Desde esta dirección se descarga un archivo .BIN que contiene la configuración del servidor de comando y control (C2). Se observó que la dirección IP almacenada en dicho archivo cambia entre ejecuciones, lo que indica una estrategia de rotación dinámica de infraestructura C2 sin necesidad de modificar el ejecutable principal.

Imagen 3. Strings relevantes. CTI

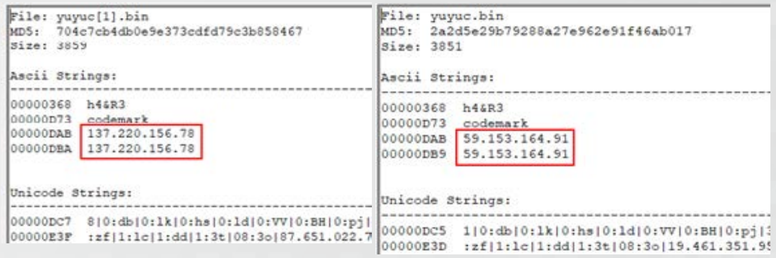


Imagen 4. Configuración C2 archivo .BIN. CTI

En ejecución controlada, se identificó la creación del archivo C:\Users\Public\RuntimeUpdate\runtime.exe. La verificación de hash confirmó que se trata de una copia de la muestra original, evidenciando replicación bajo un nombre distinto como mecanismo de persistencia.

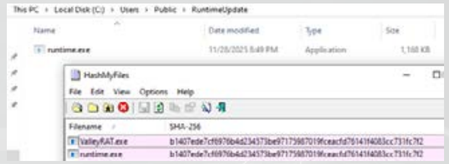


Imagen 5. Verificación de hash. CTI

Adicionalmente, se creó una entrada en HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run con el valor WindowsUpdateService, apuntando a la ejecución de runtime.exe, asegurando su ejecución automática en cada inicio de sesión.

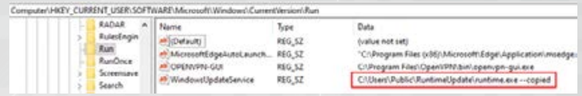


Imagen 6. Persistencia de la muestra. CTI

También se detectó la escritura del archivo C:\Users\<usuario>\AppData\Local\Microsoft\Windows\INetCache\IE\W3MF3FXY\yuyuc[1].bin. Este archivo corresponde a la configuración remota del C2 previamente descrita. El análisis de tráfico reveló comunicaciones hacia la IP 159.75.57.35, asociada al dominio yuyuc-1253104881[.]cos[.]ap-guangzhou[.]myqcloud[.]com

También se observaron conexiones hacia las IP:

- 137[.]220[.]156[.]78
- 59[.]153[.]164[.]91

Intelligence Insights ValleyRAT

El RAT sigiloso

Natalia Meliza Arias
Analista L2

Estas direcciones coinciden con los servidores C2 identificados en los archivos de configuración .BIN.

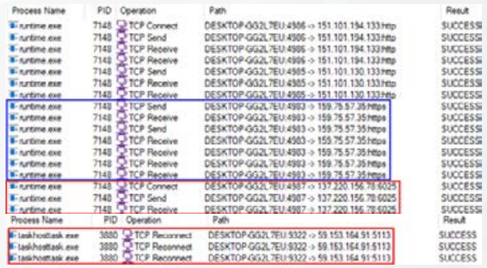


Imagen 7. Direcciones IP con las que conecta la muestra. CTI

La comunicación se realiza mediante el puerto TCP/6025, un puerto no estándar que facilita la evasión de controles de seguridad. La presencia reiterada de paquetes PSH, ACK indica transmisión activa de información desde el host comprometido hacia el C2, evidenciando un canal persistente de comando, control y posible exfiltración de datos.

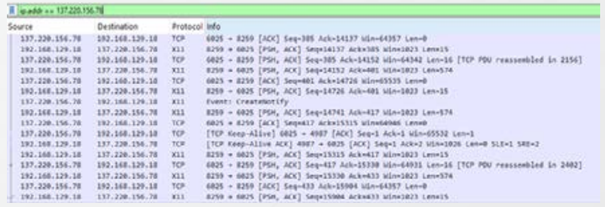


Imagen 8. Tráfico entre el host comprometido y el C2. CTI

ValleyRAT puede categorizarse con un nivel de amenaza alto, considerando los resultados del análisis de la muestra, sus capacidades de control remoto, evasión y persistencia, así como su arquitectura modular y operación fileless lo que dificulta su detección por mecanismos tradicionales. Además, su posible atribución al grupo APT SilverFox y su presencia en múltiples campañas recientes evidencian un riesgo significativo para sistemas Windows y para organizaciones que puedan ser objetivo de estas campañas.

Recomendaciones

- Bloquear la ejecución de binarios desde C:\Users\Public\ y subdirectorios como RuntimeUpdate\ mediante AppLocker o WDAC.
- Restringir la ejecución de archivos .EXE y .DLL desde rutas de caché y directorios temporales de usuario.
- Monitorear la creación o modificación de valores en HKCU\Software\Microsoft\Windows\CurrentVersion\Run, especialmente aquellos que apunten a rutas fuera de Program Files.
- Habilitar la Microsoft Vulnerable Driver Blocklist y la integridad de memoria (HVCI) para mitigar ataques tipo BYOVD.
- Detectar procesos que ejecuten llamadas encadenadas a VirtualAlloc, LoadLibrary y GetProcAddress seguidas de actividad de red saliente.
- Restringir la ejecución de procesos del sistema como svchost.exe cuando sean invocados desde ubicaciones distintas a System32.

SOC Learnings Principales vulnerabilidades de **febrero de 2026**

CVE-2026-1281 CVSS v3.1: 9.8 [Crítica]

Vulnerabilidad de inyección de código en Ivanti Endpoint Manager Mobile

Vulnerabilidad deinyección de código que afecta a Ivanti Endpoint Manager Mobile, para todas las versiones anteriores a la 12.x.0.x, permite que un atacante remoto y no autenticado ejecute código arbitrario en el sistema afectado.

CVE-2024-43468 CVSS v3.1: 9.8 [Crítica]

Vulnerabilidad de ejecución remota de código en Microsoft Configuration Manager

Vulnerabilidad de ejecución remota de código que afecta a Microsoft Configuration Manager, desde la versión 1.0.0 a las anteriores de la 5.00.9106, y podría permitir que un atacante ejecute código arbitrario en el sistema afectado.

CVE-2026-20127 CVSS v3.1: 10 [Crítica]

Bypass de autenticación en Cisco Catalyst SD-WAN Controller permite acceso administrativo remoto

Vulnerabilidad en el mecanismo de autenticación en Cisco Catalyst SD-WAN Controller y Cisco Catalyst SD-WAN Manager permite que un atacante remoto no autenticado pueda obtener privilegios administrativos en el sistema afectado. La explotación exitosa permitiría iniciar sesión como un usuario con permisos elevados y acceder a NETCONF, lo que posibilitaría manipular la configuración de red del entorno SD-WAN.

CVE- 2025-49113 CVSS v3.1: 9.9 [Crítica]

Ejecución remota de código en Roundcube Webmail por deserialización de objetos PHP

Vulnerabilidad de ejecución remota de código afecta a Roundcube Webmail, en las versiones desde la 0 hasta la 1.15.10 y desde la 1.6.0 hasta la 1.6.11, debido a la falta de validación del parámetro _from en la URL dentro del archivo program/actions/settings/upload.php. Esta falla permite a un atacante autenticado explotar un proceso de deserialización de objetos PHP, lo que podría derivar en la ejecución de código arbitrario en el servidor.

CVE-2026-22769 CVSS v3.1: 10 [Crítica]

Credenciales visibles en Dell RecoverPoint for Virtual Machines permiten acceso remoto no autorizado

Una vulnerabilidad en Dell RecoverPoint for Virtual Machines en versiones desde 5.3 SP4 P1 hasta antes de 6.0.3.1 HF1, permite la visualización de credenciales sin cifrar.

Inside MNEMO

Últimas noticias:

- **Webinar: PRESEACYBER Y VULNTRACK**

- **¡ El servicio #017 vuelve a ser reconocido!**

Active Campaigns Eaglesight

Tu nivel de salud en Ciberseguridad, medido, accesible y accionable en todo momento.

EAGLESIGHT by MNEMO

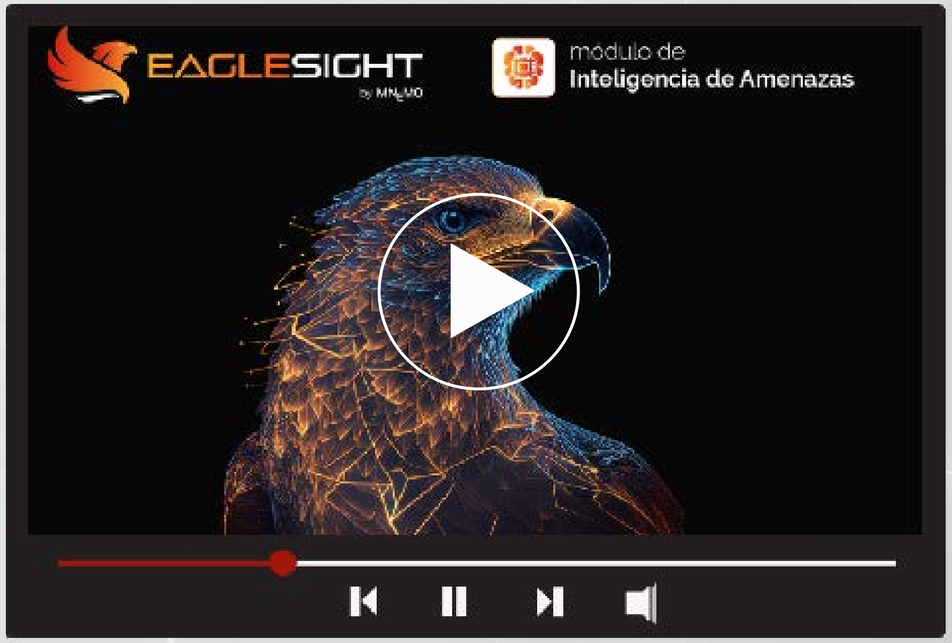
Módulo de Inteligencia de Amenazas

Conoce con más detalle nuestra Active Campaigns

Prueba gratuita

El **módulo de Inteligencia de Amenazas** pone en disponibilidad el conocimiento, trabajo colaborativo y las capacidades de respuesta de un **CSIRT**, para **prevenir** y **reaccionar** de manera efectiva ante **ciberamenazas**.

La utilización de nuestra plataforma **EAGLESIGHT** permite tener información on-line del proceso actualizada al momento, seguimiento de las acciones de respuesta y acceso a KPIs y cuadros de mando orientados a la priorización de tareas y a la toma de decisiones.



Servicio de ciber inteligencia:
Durante **1 semana** con envío de ciertas **alertas** de contenidos de inteligencia.

Sesión final de evaluación de resultados:
Walkthrough de EagleSight guiado por nuestro equipo de Cyber Threat Intelligence, revisando y explicando los contenidos de mayor interés.

Acceso al entorno de EagleSight
Se habilitarán hasta 3 cuentas de usuarios para el cliente con acceso en el periodo indicado a los dashboard, eventos, alertas, informes y otros contenidos

Acceso a contenidos:
Durante la PoC se accederán al histórico de alertas preventivas, informes de análisis personalizado y repositorio de APTs (Advanced Persistent Threats).

MNEMO

mnemo.com

info@mnemo.com