Alerta

Técnica Campaña Phishing Notificación Judicial – Distribución de VJW0rm

COLCERT AL – 20260803 - 105

TLP:CLEAR

Resumen Ejecutivo

NIVEL DE RIESGO

ALTO

Se identificó una campaña activa de distribución de malware que utiliza el señuelo temático de “notificación judicial” para inducir a la víctima a descargar y ejecutar un dropper en VBScript. El análisis técnico confirma con nivel de confianza alto que el payload final corresponde a la familia VJW0rm (Vengeance Justice Worm), un troyano de acceso remoto (RAT) tipo gusano, modular y de código público, con capacidades documentadas para extraer credenciales, ejecutar comandos remotamente, registrar pulsaciones de teclado, interceptar video perimetral y autopropagarse vía medios extraíbles.

La cadena de intrusión inicia con un archivo bajo el patrón “NOTIFICACION JUDICIAL_BEB428_.vbs”, contenido en un ZIP descargado desde un dominio de phishing (wind2365[.]juridico[.]bond). Este despliega scripts de PowerShell, compila dinámicamente ensamblados .NET en la memoria del equipo, y establece persistencia mediante una tarea programada enmascarada como “WindowsUpdate” junto a una clave de registro de inicio. Finalmente, contacta a la infraestructura de comando y control (C2) operando sobre el proveedor de DNS dinámico gratuito kozow.com. Esta comunicación fue clasificada como maliciosa validando la firma Suricata específica para VJW0rm (check-in HTTP hacia la ruta /Vre).

Contexto de la amenaza

VJW0rm (Vengeance Justice Worm) es un artefacto malicioso híbrido que opera como gusano y troyano de acceso remoto (RAT), documentado desde 2016 y atribuido al desarrollador “v_B01” en la comunidad DevPoint. La variante procesada emplea VBScript como vector de distribución nativo, una táctica operativa plenamente consistente con las campañas de ciberespionaje previamente asociadas a esta familia.

La infraestructura analizada exhibe una alta consistencia con el protocolo C2 característico de VJW0rm, el cual se basa en tráfico HTTP hacia el recurso “/Vre” para emitir comandos de ejecución remota, creación de archivos, control de persistencia y administración del implante. La identificación del endpoint c2nuevpoder[.]kozow[.]com:7575/Vre coincidiendo con este patrón conductual permite atribuir, con un grado de confianza alto, la muestra interceptada a la infraestructura de VJW0rm.

Los mecanismos de permanencia identificados, tales como la inyección en el registro y la tarea programada “WindowsUpdate”, concuerdan con las técnicas de evasión históricamente documentadas para esta amenaza. Adicionalmente, la inteligencia de amenazas reporta el uso frecuente de VJW0rm como stager inicial para descargar familias secundarias destructivas como AsyncRAT o FormBook; no obstante, durante la contención de esta muestra en particular, no se materializó la ejecución de cargas útiles secundarias.

El uso del señuelo “Notificación Judicial” constituye una táctica recurrente de ingeniería social dirigida a perfiles administrativos y jurídicos, abusando de la confianza implícita en las comunicaciones gubernamentales. En Colombia, este pretexto es altamente crítico y efectivo debido a la estandarización de notificaciones electrónicas por la Rama Judicial y la Fiscalía General de la Nación, siendo un vector repetitivo contra el sector público. En conclusión, la evidencia técnica confirma una campaña activa de phishing orientada a desplegar VJW0rm RAT mediante droppers VBScript, cuyo objetivo inminente es establecer acceso remoto, asegurar persistencia y preparar el entorno para compromisos adicionales.

Mapeo Táctico MITRE ATT&CK

A continuación, se presenta la tabla detallada de las Tácticas, Técnicas y Procedimientos (TTPs) identificadas, mapeadas con el marco de MITRE ATT&CK.

Táctica	ID	Técnica	Evidencia / Contexto
Desarrollo de Recursos	T1583.001	Adquisición de Infraestructura: Dominios	Uso de wind2365.juridico.bond como infraestructura de entrega y c2nuevpoder.kozow.com como servidor de comando y control (C2) administrado por el atacante.
Desarrollo de Recursos	T1588.002	Obtención de Capacidades: Herramientas	Uso de la familia pública VJW0rm como cargador (loader) y troyano de acceso remoto (RAT).
Acceso Inicial	T1566.002	Phishing: Enlace de Spearphishing	Uso de una URL con parámetros de seguimiento individualizados (uid/nonce/ts/rid/sig) que redirige a la descarga de un archivo ZIP malicioso.
Ejecución	T1204.002	Ejecución por el Usuario: Archivo Malicioso	La víctima ejecuta manualmente el archivo .vbs después de extraer el contenido del archivo ZIP recibido.
Ejecución	T1059.005	Intérprete de Comandos y Scripts: Visual Basic	Uso de wscript.exe para ejecutar el dropper inicial y los scripts auxiliares en formato .vbs.
Ejecución	T1059.001	Intérprete de Comandos y Scripts: PowerShell	Ejecución de scripts mediante powershell.exe con los parámetros -ExecutionPolicy Bypass y -WindowStyle Hidden para ejecutar wc80152.ps1 y agent_1784154434.ps1.
Ejecución	T1053.005	Tareas Programadas / Trabajos: Tarea Programada	Uso de schtasks.exe para crear la tarea programada denominada “WindowsUpdate”.
Persistencia	T1053.005	Tareas Programadas / Trabajos: Tarea Programada	La tarea “WindowsUpdate” utiliza un disparador de inicio de sesión (onlogon) y privilegios elevados (HIGHEST) para garantizar la ejecución persistente del malware.
Persistencia	T1547.001	Claves de Registro de Ejecución / Carpeta de Inicio	Modificación de claves de registro de inicio confirmada en ANY.RUN, consistente con el mecanismo de persistencia histórico asociado a VJW0rm mediante HKCU\vjw0rm.
Evasión de Defensas	T1027	Archivos o Información Ofuscados	Uso de nombres de archivos y carpetas pseudoaleatorios, además de contenido de scripts ofuscado para dificultar el análisis y la detección.
Evasión de Defensas	T1027.004	Compilación Posterior a la Entrega	Uso de csc.exe y cvtres.exe para compilar un ensamblado .NET directamente en el equipo víctima a partir de código fuente entregado localmente.
Evasión de Defensas	T1620 (Inferida)	Carga de Código Reflexivo	Secuencia observada PowerShell → csc.exe → DLL compilada localmente, compatible con técnicas de carga dinámica de código y posibles mecanismos de evasión de AMSI.
Evasión de Defensas	T1562.001	Deterioro de Defensas: Deshabilitar o Modificar Herramientas	Ejecución de taskkill.exe /IM cmstp.exe /F. La intención no es concluyente; podría estar relacionada con técnicas de anti-análisis o eliminación de artefactos previos.
Descubrimiento	T1082	Descubrimiento de Información del Sistema	Consulta de información del sistema mediante Win32_OperatingSystem utilizando PowerShell, junto con actividad de consulta de registro identificada por el motor Bale.
Descubrimiento	T1016	Descubrimiento de la Configuración de Red del Sistema	Consulta hacia api.ipify.org para obtener la dirección IP pública del sistema comprometido (ip-check).
Comando y Control	T1071.001	Protocolo de Capa de Aplicación: Protocolos Web	Comunicación HTTP de tipo beacon hacia c2nuevpoder.kozow.com:7575/Vre, correspondiente al canal de comando y control de VJW0rm.
Comando y Control	T1105 (Inferida)	Transferencia de Herramientas hacia el Sistema Comprometido	Capacidad documentada de VJW0rm para descargar y ejecutar componentes adicionales mediante instrucciones recibidas desde el servidor C2.

Táctica	ID	Técnica	Evidencia / Contexto
Recolección	T1056.001 (Inferida)	Captura de Entrada: Registro de Pulsaciones (Keylogging)	Capacidad documentada de la familia VJW0rm para capturar pulsaciones del teclado; no fue observada durante la ventana de análisis.
Impacto	T1529	Apagado o Reinicio del Sistema	Técnica identificada en el mapeo MITRE ATT&CK generado por el motor Trellix (Bale) para esta muestra.
Movimiento Lateral	T1091 (Inferida)	Replicación mediante Medios Extraíbles	Capacidad de autopropagación documentada públicamente para VJW0rm mediante dispositivos extraíbles; no fue observada en las muestras analizadas.

Cadena de Ataque (Kill Chain)

La operación describe una cadena de ataque por fases que inicia con la entrega de un archivo malicioso mediante phishing, continúa con la ejecución de scripts y técnicas de evasión, establece mecanismos de persistencia y finaliza con el establecimiento de comunicación C2 para el control remoto del equipo comprometido.

Indicadores de Compromiso (IOCs)

Archivos

Archivo	MD5	Rol
NOTIFICACION JUDICIAL_BEB428_C8BDC7.vbs	bfb7ae9ffe72a0c1c964f3225d8f0db6	Dropper inicial,
NOTIFICACION JUDICIAL_BEB428_E60F0F.vbs	3c6789b747604686212c0ba72167adf5	Dropper inicial,
E60F0F_NOTIFICACION JUDICIAL_BEB428.zip	7b9435f60f0fcf00382e27f2677d5797	Contenedor de entrega
wc80152.ps1 / health.ps1	3166e2716a9827c6ef501fd8d109eb01	Cargador PowerShell, ESTÁTICO
agent_1784154434.ps1	eb6a0a1b00bacbda1b7e75a1dc7d1ed1	Agente 2ª etapa / conector C2, ESTÁTICO
gj6p33828.vbs	639425790c0c8e260c6f31b8e3686ef2	Script auxiliar — varía por build
SearchProtocol.vbs	440513b91375aab90a91e7d3a6c4d378	Script de persistencia — varía por build
Tarea programada “WindowsUpdate”	545ac7e7174557494914d651606f3e6f	Definición de tarea de persistencia
o2sdhnol.dll (Win7x64) / 1xl-3pwa.dll (WinXP)	c4fa21dafe9973e31e46f4e93934ccc8 / 3b705e246a2059984ef3e85cb5105fc4	DLL .NET compilada in situ

Red

Indicador	Tipo	Contexto	Reputación
wind2365.juridico.bond	Dominio	Página de phishing / entrega del ZIP malicioso	Maliciosa
185.114.206.49	IP (ASN H4Y-TECHNOLOGIES)	Resolución de wind2365.juridico.bond	Maliciosa
c2nuevpoder.kozow.com	Dominio DNS dinámico	C2 activo — familia VJW0rm	Maliciosa
193.26.115.198:7575/TCP	IP:Puerto (DE, ASN 1337-Services-GmbH)	Endpoint C2 /Vre	Maliciosa; en lista Spamhaus DROP
http://c2nuevpoder.kozow.com:7575/Vre	URL	Endpoint de check-in C2 Vjw0rm	Maliciosa
api.ipify.org	Dominio (servicio legítimo)	Consulta de IP pública de la víctima (“ip-check”)	Legítimo — abusado por el malware
kozow.com	Proveedor DNS dinámico	Infraestructura de alojamiento del C2	Proveedor con historial de abuso documentado (phishing, C2 de RAT)

Recomendaciones de defensa

Con base en el análisis técnico realizado, se recomienda implementar medidas orientadas a fortalecer las capacidades de prevención, detección, contención y respuesta frente a campañas que utilicen mecanismos similares de distribución mediante phishing, ejecución de scripts y despliegue de herramientas de acceso remoto como VJW0rm.

Contención y erradicación

- Incorporar los indicadores de compromiso identificados en los equipos de seguridad existentes, incluyendo soluciones de EDR/XDR, antivirus, firewall, proxy y servicios de resolución DNS. Se recomienda bloquear o monitorear los dominios wind2365.juridico.bond y c2nuevpoder.kozow.com, así como las direcciones IP asociadas 185.114.206.49 y 193.26.115.198, incluyendo comunicaciones hacia el puerto 7575/TCP.

- Ejecutar búsquedas retrospectivas (retro-hunting) en los equipos corporativos utilizando los hashes, indicadores de red, rutas de archivos y patrones de comportamiento identificados, con el objetivo de detectar posibles compromisos previos o variantes relacionadas.

- Realizar una revisión de endpoints para identificar artefactos asociados con la campaña, incluyendo:
  - Tareas programadas denominadas “WindowsUpdate” que ejecuten scripts mediante wscript.exe fuera de ubicaciones o procesos legítimos.
  - Presencia de archivos como SearchProtocol.vbs en rutas no habituales como %APPDATA%\Roaming\System\Temp.
  - Ejecuciones sospechosas de VBScript, PowerShell o compiladores .NET desde directorios temporales o rutas de usuario.

- Aislar y realizar análisis forense sobre aquellos equipos donde se confirme la ejecución del dropper inicial o comunicación con la infraestructura C2 identificada. Como medida preventiva, se recomienda realizar la rotación de credenciales de los usuarios afectados, considerando que la familia VJW0rm posee capacidades asociadas con captura de información y posible robo de credenciales.

Fortalecimiento de controles técnicos

Restringir o controlar la ejecución de intérpretes de scripting como wscript.exe y cscript.exe mediante mecanismos de control de aplicaciones como AppLocker o Windows Defender Application Control (WDAC). En aquellos entornos donde no sea posible su restricción completa, implementar alertas ante ejecuciones originadas desde ubicaciones como %TEMP% o %APPDATA%.

Habilitar y centralizar los registros de actividad de PowerShell, incluyendo Script Block Logging y Module Logging, además de evaluar la aplicación de Constrained Language Mode para reducir la ejecución de código no autorizado

Implementar mecanismos de detección sobre cadenas de ejecución anómalas, especialmente aquellas que involucren la secuencia: powershell.exe → csc.exe → cvtres.exe

Concienciación y capacitación

- Restringir Reforzar las campañas internas de concienciación frente a correos electrónicos o mensajes con temática de “Notificación Judicial”, “Citación Legal” u otros asuntos administrativos similares, especialmente cuando incluyan enlaces de descarga o archivos comprimidos con extensiones de scripting como .vbs.
- Incorporar este tipo de señuelos dentro de los ejercicios periódicos de simulación de phishing, debido a su alta efectividad en la región y su capacidad para generar confianza mediante la suplantación de comunicaciones oficiales.
- Mantener actualizados los mecanismos de inteligencia de amenazas mediante la incorporación de nuevos indicadores, patrones de comportamiento y técnicas asociadas con VJW0rm y actores que empleen campañas similares.

Fuentes

ANY.RUN Interactive Sandbox. (2026, 22 de julio). Análisis dinámico de malware — Task d4f78543-ef5d-473b-ac5f-ebf47f1ac3f5.
https://app.any.run/tasks/d4f78543-ef5d-473b-ac5f-ebf47f1ac3f5

Cofense Intelligence. (2024, 6 de noviembre). Hidden in the crowd: The risk of group-delivered malware.
https://cofense.com/blog/hidden-in-the-crowd-the-risk-of-group-delivered-malware

CirclelD. (2021, 17 de marzo). An in-depth look at the risks Kozow.com subdomains may pose to Internet users.
https://circleid.com/posts/20210317-an-in-depth-look-at-the-risks-kozowcom-subdomains

Fraunhofer FKIE. (s. f.). Malpedia: Vjw0rm malware family.
https://malpedia.caad.fkie.fraunhofer.de/details/win.vjw0rm

Misiones Online. (2026, 20 de mayo). Alertan sobre una nueva modalidad de phishing que simula notificaciones judiciales para robar correos y contraseñas.
https://misionesonline.net/2026/05/20/alertan-sobre-una-nueva-modalidad-de-phishing-que-simula-notificaciones-judiciales-para-robar-correos-y-contrasenas/

SecurityScorecard. (2023, 10 de enero). How to analyze JavaScript malware – A case study of Vjw0rm.
https://securityscorecard.com/research/how-to-analyze-javascript-malware-a-case-study-of-vjw0rm/

Trellix. (2026, 22 de julio). Reporte de análisis dinámico IVX Cloud — Muestra e5bcd964-c5d6-4687-ae90-2a9df0486bfb

The MITRE Corporation. (s. f.). MITRE ATT&CK®: Knowledge base of adversary tactics and techniques.
https://attack.mitre.org/