PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

200-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°200	Fecha: 29-08-2024
		Página: 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ransomware BlackByte explota vulnerabilidades en VMware ESXi		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los creadores del ransomware BlackByte se han unido al creciente número de ciberdelincuentes que atacan una reciente vulnerabilidad de omisión de autenticación en VMware ESXi para comprometer la infraestructura central de las redes empresariales.

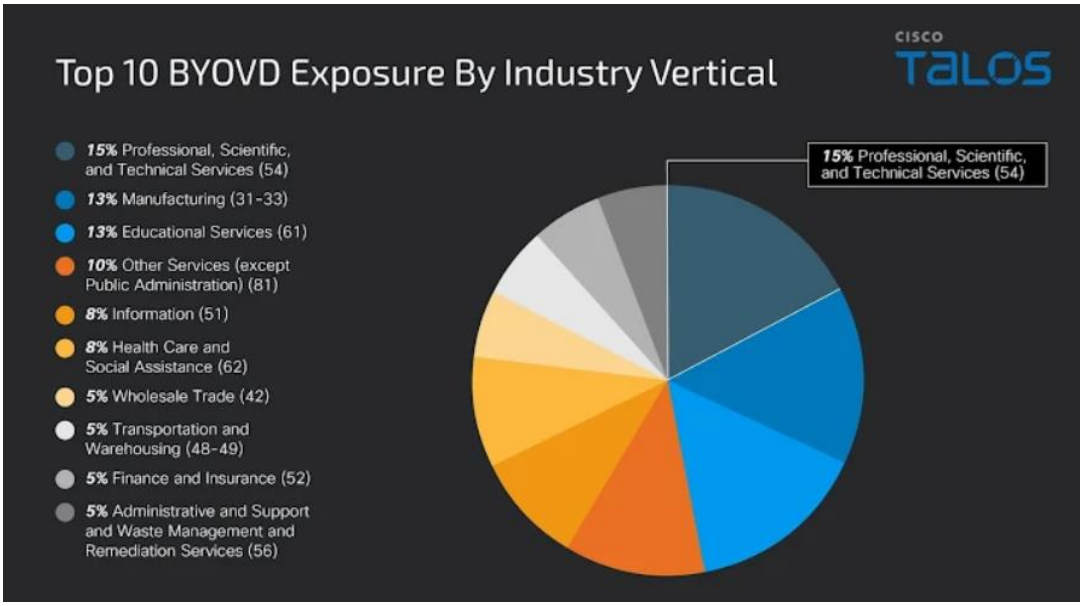
BlackByte hizo su debut en la segunda mitad de 2021 y supuestamente es una de las derivaciones autónomas de ransomware que surgieron en los meses previos al cierre del infame equipo de ransomware Conti.

El grupo de ransomware como servicio (RaaS) tiene antecedentes de explotar vulnerabilidades de ProxyShell en Microsoft Exchange Server para obtener acceso inicial, evitando al mismo tiempo sistemas que usan ruso y varios idiomas de Europa del Este.

Al igual que los grupos RaaS, también aprovecha la doble extorsión como parte de los ataques, adoptando un enfoque de denuncia a través de un sitio de filtración de datos operado en la red oscura para presionar a las víctimas a pagar. Hasta la fecha, se han observado múltiples variantes del ransomware, escritas en C, .NET y Go .

Si bien Trustwave lanzó un descifrador para BlackByte en octubre de 2021, el grupo siguió perfeccionando su modus operandi, llegando incluso al extremo de emplear una herramienta personalizada llamada ExByte para la exfiltración de datos antes de comenzar el cifrado.

Un aviso publicado por el gobierno de Estados Unidos a principios de 2022 atribuyó al grupo RaaS a ataques con motivaciones financieras dirigidos a sectores de infraestructura críticos, incluidos los financieros, los alimentarios y agrícolas, y las instalaciones gubernamentales.



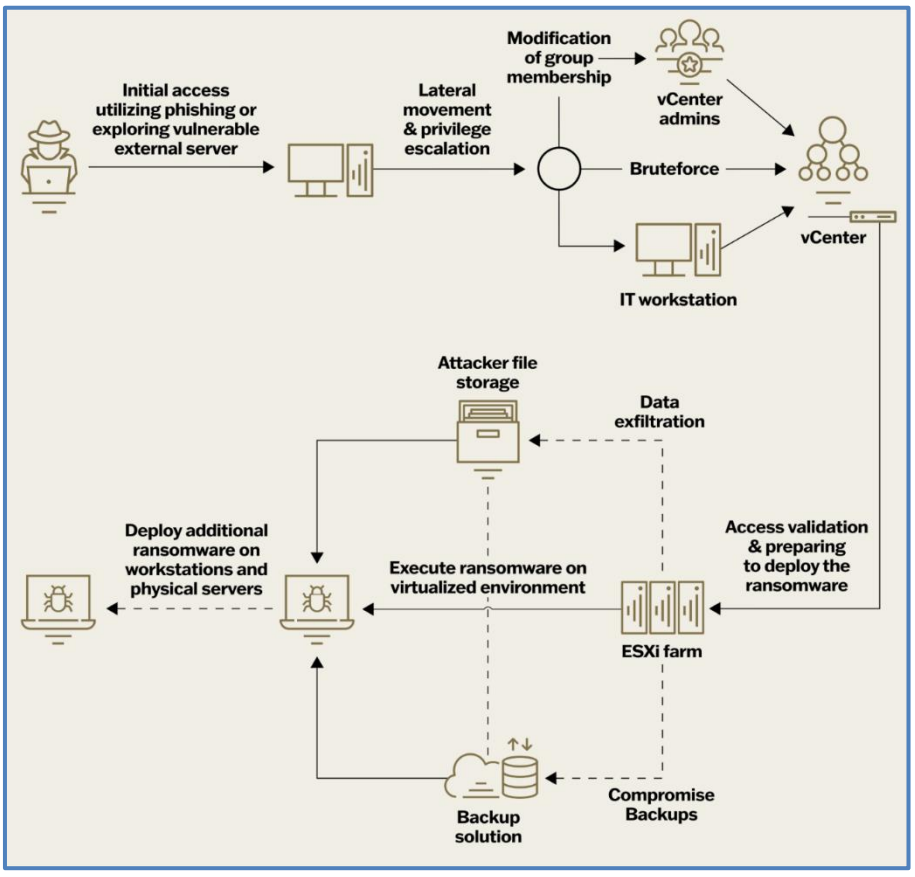
Microsoft y otros proveedores de seguridad identificaron previamente grupos de ransomware como Black Basta, Manatee Tempest, Scattered Spider y Storm-1175 que aprovechan CVE-2024-37085 para implementar cepas de ransomware como Akira y Black Basta. En estos ataques, los adversarios usaron sus privilegios de AD para crear o cambiar el nombre de un grupo llamado "ESX Admins" y luego usar el grupo para acceder al hipervisor ESXi como un usuario con privilegios completos.

2. DETALLES:

Los investigadores de Cisco Talos que observaron que los actores de amenazas de BlackByte apuntaban a CVE-2024-37085 en ataques recientes describieron la táctica como uno de varios cambios que realizaron recientemente para mantenerse por delante de los defensores.

Otros cambios incluyen el uso de BlackByteNT, un nuevo cifrador de BlackByte escrito en C/C++, que agrega hasta cuatro controladores vulnerables, en sistemas comprometidos y utiliza las credenciales AD de la organización víctima para autopropagarse.

Sygnia, que investigó numerosos ataques de ransomware contra VMWare ESXi y otros entornos virtualizados a principios de este año, describió que los ataques se desarrollan en un patrón específico en la mayoría de los casos:



Acceso inicial: Los actores de amenazas obtienen acceso inicial a la organización utilizando técnicas establecidas, como realizar ataques de phishing, descargar archivos maliciosos o explotar vulnerabilidades conocidas en activos conectados a Internet.

Movimiento lateral y escalamiento de privilegios: Al obtener acceso, los actores de amenazas aumentan sus privilegios para obtener credenciales para hosts ESXi o vCenter. Esta escalada se puede lograr mediante varios métodos, como alterar las membresías de grupos de dominio para VMware conectados al dominio, emplear ataques de fuerza bruta, ejecutar intentos de secuestro de RDP dirigidos al personal de TI o utilizar exploits como ESXiArgs.

Validación de acceso: Después de asegurar el acceso inicial a la infraestructura de virtualización, los actores de amenazas validan su capacidad para interactuar con ella. Si se deniega el acceso directo, los atacantes utilizan vCenter para habilitar SSH en todos los servidores ESXi y también pueden restablecer las contraseñas del servidor o ejecutar comandos de forma remota mediante paquetes de instalación de vSphere (VIB) personalizados.

Implementación de ransomware virtualizado: Los actores de amenazas utilizan su acceso para conectarse a ESXi y ejecutar el ransomware en los hosts ESXi.

Compromiso de las copias de seguridad: Apuntando más allá del entorno virtualizado, los actores de amenazas podrían intentar tomar el control de los sistemas de copias de seguridad. Al cifrar o eliminar el almacenamiento de respaldo y, en algunos casos, cambiar las contraseñas del sistema de respaldo, los actores de amenazas pretenden obstaculizar la recuperación del entorno virtualizado y así obtener una influencia adicional sobre sus víctimas.

Exfiltración de datos: Los actores de amenazas a menudo intentan implementar un esquema de doble extorsión, exfiltrando datos a ubicaciones externas. Esto permite a los actores de amenazas no solo cifrar los archivos existentes, sino también divulgar públicamente los datos exfiltrados, para causar un daño adicional a la reputación.

Ejecución de ransomware: En este punto, los actores de amenazas apagan todas las máquinas virtuales e inician un ransomware que cifra la carpeta "/vmfs/volumes" del sistema de archivos ESXi.

Implementación adicional de ransomware: Los actores de amenazas que obtienen acceso previo a los mecanismos de implementación (como SCCM o Active Directory) pueden propagar ransomware adicional a servidores y estaciones de trabajo no virtualizados, amplificando el impacto del ataque más allá del ámbito de la virtualización.

Los recientes ataques de BlackByte culminaron con la reescritura de los archivos cifrados con la extensión de archivo "blackbytent_h", y el cifrador también dejó caer cuatro controladores vulnerables como parte del ataque BYOVD . Los cuatro controladores siguen una convención de nombres similar: ocho caracteres alfanuméricos aleatorios seguidos de un guion bajo y un valor numérico incremental.

- AM35W2PH (sistema RtCore64)
- AM35W2PH_1 (DBUtil_2_3.sys)
- AM35W2PH_2 (zamguard64.sys también conocido como Terminator)
- AM35W2PH_3 (sistema gdrv)

Los sectores de servicios profesionales, científicos y técnicos son los más expuestos a los factores de riesgo observados, ya que representan el 15% del total, seguidos de la industria manufacturera (13%) y los servicios educativos (13%). Talos también ha evaluado que el actor de la amenaza es probablemente más activo de lo que parece y que solo se estima que entre el 20% y el 30% de las víctimas se publican, aunque la razón exacta de esta disparidad sigue sin estar clara.

3. RECOMENDACIONES:

- Implementar MFA para todos los servicios en la medida de lo posible, especialmente para correo web, VPN, accesos remotos, conexiones a la nube y cuentas que acceden a sistemas críticos. Priorizar el "push verificado" como método MFA sobre opciones menos seguras como SMS o llamadas telefónicas.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware.
- Auditar la configuración de VPN. Hay que confirmar que se eliminen las políticas de VPN heredadas y que los intentos de autenticación que no coincidan con una política de VPN actual se rechacen de forma predeterminada. Restringir el acceso VPN sólo a los segmentos y servicios de red necesarios, limitando la exposición de activos críticos como controladores de dominio.
- Configurar alertas para cualquier cambio en grupos privilegiados, como la creación de nuevos grupos de usuarios o la adición de cuentas a administradores de dominio. Asegurarse de que los privilegios administrativos se otorguen solo cuando sea necesario y se auditen de forma rutinaria a partir de entonces. Se puede utilizar una solución de gestión de acceso privilegiado (PAM) para optimizar el control y la supervisión de cuentas privilegiadas.
- Limitar o deshabilitar el uso de NTLM cuando sea posible y aplicar métodos de autenticación más seguros como Kerberos. Limitar la tasa de intentos y fallas de autenticación en interfaces internas y de cara al público para evitar el escaneo de autenticación automatizado.

- Desactivar SMBv1 y aplicar la firma y el cifrado de SMB para proteger contra el movimiento lateral y la propagación de malware.
- Implementar clientes EDR en todos los sistemas del entorno. Configurar una contraseña de administrador en los clientes EDR para evitar la manipulación o eliminación no autorizada del cliente.
- Deshabilitar las cuentas de proveedores y las capacidades de acceso remoto cuando no estén en uso activo.
- Crear detecciones de cambios de configuración no autorizados que se puedan realizar en varios sistemas del entorno, incluidos cambios en las políticas de Windows Defender, cambios no autorizados en los objetos de política de grupo y creación de tareas programadas y servicios instalados inusuales.
- Desarrollar y documentar procedimientos para restablecer contraseñas empresariales para garantizar que todas las credenciales de usuario se puedan restablecer rápida y completamente. Incluir procedimientos para transferir tickets Kerberos críticos en esta documentación.
- Reforzar y parchear los hosts ESX para reducir la superficie de ataque de estos servidores críticos en la medida de lo posible y garantizar que las vulnerabilidades recién descubiertas se corrijan lo más rápido posible.
- Desconectar ESXi de AD y eliminar cualquier grupo utilizado anteriormente en AD que administrara ESXi.
- Actualizar ESXi a 8.0 U3, donde se soluciona la vulnerabilidad.
- No hacer clic en enlaces sospechosos o no solicitados, ni descargar adjuntos de correos desconocidos
- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión y realizar evaluaciones de vulnerabilidad periódicas.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Implementar un plan de recuperación.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2024/08/ransomware-blackbyte-explota.html • hxxps://thehackernews.com/2024/08/blackbyte-ransomware-exploits-vmware.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°200	Fecha: 29-08-2024 Página: 8 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en el software de gestión ThinManager ThinServer de Rockwell Automation		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Nicholas Zubrisky (@NZubrisky) de Trend Micro, ha reportado múltiples vulnerabilidades de severidad **CRÍTICA** de tipo gestión inadecuada de privilegios, asignación incorrecta de permisos para recursos críticos y validación de entrada inadecuada que afecta a variadas versiones del software de gestión de clientes "ThinManager ThinServer" de Rockwell Automation. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto leer archivos arbitrarios y ejecutar código arbitrario con privilegios del sistema.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2024-7986 de tipo gestión inadecuada de privilegios, podría permitir a un atacante remoto divulgar información confidencial. Un agente de amenazas puede aprovechar esta vulnerabilidad abusando del servicio ThinServer para leer archivos arbitrarios mediante la creación de una unión que apunte al directorio de destino.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-7987 de tipo asignación incorrecta de permisos para recursos críticos, podría permitir a un atacante ejecutar código arbitrario con privilegios del sistema. Para aprovechar esta vulnerabilidad, un atacante debe abusar del servicio ThinServer creando una unión y utilizándola para cargar archivos arbitrarios.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-7988 de tipo validación de entrada inadecuada, podría permitir a un atacante ejecutar código arbitrario con privilegios del sistema. Esta vulnerabilidad existe debido a la falta de una validación adecuada de la entrada de datos, lo que permite que se sobrescriban los archivos.

A. Productos afectados:

- ThinManager ThinServer: versiones 11.1.0 a 11.1.7.
- ThinManager ThinServer: versiones 11.2.0 a 11.2.8.
- ThinManager ThinServer: versiones 12.0.0 a 12.0.6.
- ThinManager ThinServer: versiones 12.1.0 a 12.1.7.
- ThinManager ThinServer: versiones 13.0.0 a 13.0.4.
- ThinManager ThinServer: versiones 13.1.0 a 13.1.2.
- ThinManager ThinServer: versiones 13.2.0 a 13.2.1.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda estas vulnerabilidades.
- Implementar las mejores prácticas de seguridad sugeridas para minimizar el riesgo de vulnerabilidad.

Fuente de Información:	• hxxps://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1692.html • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-242-01 • hxxps://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°200	Fecha: 29-08-2024
		Página: 9 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en DTN Soft de Delta Electronics		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

Kimiya, en colaboración con Trend Micro Zero Day Initiative, ha reportado una vulnerabilidad de severidad **ALTA** de tipo deserialización de datos no confiables en el control de temperatura "DTN Soft" de Delta Electronics. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución remota de código.

2. **DETALLES:**

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-8255 de tipo deserialización de datos no confiables en el control de temperatura "DTN Soft" de Delta Electronics, podría permitir a un atacante remoto la ejecución remota de código.

A. **Productos afectados:**

- DTN Soft: Versión 2.0.1 y anteriores.

3. **RECOMENDACIÓN:**

- Actualizar el producto afectado a la versión 2.1 que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-242-02 • hxxps://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=dtn&sort_expr=cdate&sort_dir=DESC

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°200	Fecha: 29-08-2024 Página: 10 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Grupo APT-C-60 explota vulnerabilidad en WPS Office para desplegar el backdoor "SpyGlace"		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Los investigadores de ESET han descubierto una vulnerabilidad de severidad **CRÍTICA** de ejecución de código en WPS Office para Windows (CVE-2024-7262), que estaba siendo explotada por el grupo de ciberespionaje aliado con Corea del Sur "APT-C-60" para instalar una puerta trasera (backdoor) personalizada, denominada "SpyGlace" y dirigido a objetivos de Asia Oriental. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código.

2. DETALLES:

WPS Office, es un conjunto de aplicaciones de productividad desarrollado por la empresa china Kingsoft, cuenta con más de 500 millones de usuarios activos en todo el mundo.

El grupo APT-C-60, ha estado explotando una vulnerabilidad de ejecución de código de día cero (zero-day) en la versión de Windows de WPS Office para instalar el backdoor "SpyGlace" en objetivos de Asia Oriental.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-7262 de tipo recorrido de ruta, ha sido utilizada en múltiples ataques desde finales de febrero de 2024. Las versiones afectadas van desde la 12.2.0.13110 (agosto de 2023) hasta la 12.1.0.16412 (marzo de 2024).

Kingsoft corrigió reservadamente esta vulnerabilidad en marzo de 2024 sin informar a sus clientes que el fallo estaba siendo explotado activamente, lo que llevó a la compañía de software de ciberseguridad que descubrió la campaña y la vulnerabilidad, a publicar un informe detallado recientemente. Además de la CVE-2024-7262, la investigación reveló una segunda vulnerabilidad de severidad **ALTA**, identificada por MITRE como CVE-2024-7263 de tipo recorrido de ruta, que Kingsoft corrigió en mayo de 2024 con la versión 12.2.0.17119.

La vulnerabilidad CVE-2024-7262, reside en la forma en que el software maneja los manejadores de protocolos personalizados, específicamente "ksoqing://", lo que permite la ejecución de aplicaciones externas a través de URLs especialmente diseñadas dentro de documentos. Debido a la falta de validación y saneamiento adecuados de estas URLs, los atacantes pueden crear enlaces maliciosos que llevan a la ejecución arbitraria de código.

El grupo APT-C-60 utilizó en sus ataques, documentos de hoja de cálculo (archivos MHTML) en los que incrustaron hipervínculos maliciosos ocultos bajo una imagen usada como señuelo para engañar a las víctimas para que hagan clic en ellos y así poder activar el exploit. Los parámetros de URL procesados incluyen un comando codificado en base64 para ejecutar un plugin específico (promecefpluginhost.exe) que intenta cargar una DLL maliciosa (ksojscore.dll) que contiene el código del atacante. Esta DLL actúa como componente de descarga de APT-C-60, diseñado para obtener la carga final (TaskControler.dll) desde el servidor del atacante, un backdoor personalizado llamado "SpyGlace".

Durante la investigación de los ataques de APT-C-60, los investigadores descubrieron la vulnerabilidad CVE-2024-7263, un segundo fallo de ejecución arbitraria de código que impacta a WPS Office y que surgió como resultado de un parche incompleto de la CVE-2024-7262. La solución inicial de Kingsoft consistió en agregar validación a parámetros específicos; sin embargo, algunos, como "CefPluginPathU8", aún no estaban adecuadamente asegurados, lo que permitía a los atacantes apuntar a rutas de DLL maliciosas a través de promecefpluginhost.exe nuevamente.

Aunque ESET no observó a APT-C-60 ni a otros actores aprovechando esta segunda vulnerabilidad en la práctica, la posibilidad de que eventualmente descubrieran esta brecha de seguridad es alta.

Los investigadores advirtieron que el exploit es especialmente astuto debido a que es lo suficientemente engañoso como para que cualquier usuario haga clic en una hoja de cálculo que parece legítima, siendo además muy efectivo y confiable. El uso del formato de archivo MHTML permitió a los atacantes convertir una vulnerabilidad de ejecución de código en una de ejecución remota.

A. Productos afectados:

- WPS Office para Windows, desde la 12.2.0.13110 hasta la versión 12.2.0.17119.

B. Indicadores de Compromiso:

Servidores de C&C:

- rammenale[.]com;
- 162.222.214[.]48;
- 131.153.206[.]231.

Hashes:

- SHA-1: 7509B4C506C01627C1A4C396161D07277F044AC6 / Exploit CVE-2024-7262 de WPS Office / HTML/Agent.HQ;
- SHA-1: 08906644b0ef1ee6478c45a6e0dd28533a9efc29 / Componente de descarga APT-C-60 / Win32/TrojanDownloader.Agent.HRP;
- MD5: b14ef85a60ac71c669cc960bdf580144;
- MD5: 9F88234068D7ABAD65979EB1DF63EFB5;
- SHA-256: 861911e953e6fd0a015b3a91a7528a388a535c83f4b9a5cf7366b8209d2f00c3;
- SHA-256: 6174276F94219BC386BDC628CA18EAEC261998B7BD03077562FE93C268B42446.

3. RECOMENDACIONES:

- Actualizar WPS Office a la última versión de software disponible que aborda estas vulnerabilidades.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.
- Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Escanear el software descargado de Internet antes de la ejecución y solo de sus sitios web oficiales.
- Reportar inmediatamente cualquier actividad anómala a los encargados de seguridad de la información de su entidad.

Fuente de Información:	• hxxps://www.welivesecurity.com/en/eset-research/analysis-of-two-arbitrary-code-execution-vulnerabilities-affecting-wps-office/ • hxxps://threatbook.io/blog/Analysis-of-APT-C-60-Attack-on-South-Korea • hxxps://www.wps.com/office/windows/ • hxxps://github.com/eset/malware-ioc/tree/master/apt_c_60 • Equipo de Anti-Fraude y Dark Web Intelligence SecureSoft

Índice alfabético