

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



ALERTA INTEGRADA DE SEGURIDAD DIGITAL

055-2025-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 Aérea del 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 las empresas 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

Grandoreiro, el troyano global con metas grandiosas..... 4

Vulnerabilidades en productos Cisco 7

Múltiples vulnerabilidades en Western Digital My Cloud OS 5 8

Vulnerabilidad en editor de texto de línea de comandos VIM 9

Índice alfabético 10

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 055		Fecha: 06-03-2025
			Página: 4 de 10
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Grandoreiro, el troyano global con metas grandiosas		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Grandoreiro es un conocido troyano bancario brasileño, parte del paraguas Tetrade, que permite a los actores de amenazas llevar a cabo operaciones bancarias fraudulentas utilizando la computadora de la víctima para eludir las medidas de seguridad utilizadas por las instituciones bancarias. Ha estado activo desde al menos 2016 y hoy en día es uno de los troyanos bancarios más extendidos por todo el mundo.

Interpol y los organismos policiales a nivel mundial están luchando contra Grandoreiro, y Kaspersky coopera con ellos, compartiendo TTPs e IoCs. Sin embargo, a pesar de la interrupción de las actividades de algunos operadores locales de este troyano en 2021 y 2024, y la detención de miembros de la banda en España, Brasil y Argentina, se mantienen activos. Ahora sabemos con certeza que sólo se arrestó una parte de esta banda: los operadores restantes detrás de Grandoreiro continúan atacando a usuarios en todo el mundo, desarrollando aún más malware y estableciendo nuevas infraestructuras.

Cada año observamos nuevas campañas de Grandoreiro dirigidas a entidades financieras que usan nuevos trucos en muestras cuyas tasas de detección por soluciones de seguridad son bajas. El grupo ha evolucionado a lo largo de los años, expandiendo el número de objetivos en cada nueva campaña que rastreamos. En 2023, el troyano bancario lanzó ataques contra 900 bancos en 40 países; en 2024, las versiones más recientes del troyano apuntaron a 1700 bancos y 276 carteras de criptomonedas en 45 países y territorios, ubicados en todos los continentes del mundo. Más adelante, agregó a Asia y África a la lista de sus objetivos, convirtiéndolo en una verdadera amenaza financiera global. Sólo en España, Grandoreiro ha sido responsable de actividades fraudulentas que ascienden a 3.5 millones de euros, según estimaciones conservadoras, y es que varios intentos fallidos podrían haber generado más de 110 millones de euros para la organización criminal.

En este artículo, detallaremos cómo opera Grandoreiro, su evolución con el tiempo, y los nuevos trucos que ha ido adoptando, como el uso de 3 DGAs (algoritmos de generación de dominios) en sus comunicaciones C2, la adopción del cifrado de robo de texto cifrado (CTS), y el seguimiento del comportamiento del ratón, con el objetivo de eludir las soluciones antifraude. Esta evolución culmina con la aparición de versiones más ligeras y locales, enfocadas ahora en México, lo que posiciona al grupo como un desafío global para el sector financiero, las agencias policiales y las soluciones de seguridad.



2. DETALLES:

Campañas 2024

Durante un período específico en febrero de 2024, unos días después del anuncio del arresto de algunos operadores de grupos delictivos en Brasil, observamos un aumento significativo en los correos electrónicos detectados por trampas de spam. Hubo una prevalencia notable de mensajes temáticos de Grandoreiro que se hacían pasar por notificaciones de CFDI mexicanas. El CFDI mexicano, abreviatura de “Comprobante Fiscal Digital por Internet”, es un sistema de facturación electrónica administrado por el SAT, Servicio de Administración Tributaria. Facilita la creación, transmisión y almacenamiento de documentos fiscales digitales, y las empresas en México están obligadas a expedirla para registrar transacciones con fines fiscales.

En nuestra investigación, hemos adquirido 48 muestras asociadas no sólo con este caso, sino también con varias otras campañas.

Notablemente, esta nueva campaña agregó un nuevo mecanismo de detección de entornos de sandbox, que consiste en mostrar un CAPTCHA antes de la ejecución de la carga principal, como una forma de impedir el análisis automático utilizado por algunas empresas:

Cabe destacar que las campañas de Grandoreiro de 2024 implementan el nuevo código de evasión de sandbox en el descargador. Aunque la muestra principal también tiene funcionalidad antisandbox, si detecta un sandbox, simplemente no se descarga. Además, la nueva versión también añadió a su arsenal la detección de muchas herramientas, con el objetivo de evitar el análisis.



La lista completa de herramientas de análisis detectadas por las versiones más recientes es la siguiente:

regmon.exe	hopper.exe	nessusd.exe	OmniPeek.exe
procmon.exe	jd-gui.exe	PacketSled.exe	netmon.exe
fiemon.exe	carvas.exe	prtg.exe	colasoft.exe
Wireshark.exe	pebrowsepro.exe	cain.exe	netwitness.exe
ProcessHacker.exe	gdb.exe	NetworkAnalyzerPro.exe	netscanpro.exe
PCHunter64.exe	scylla.exe	OmniPeek.exe	packetanalyzer.exe
PCHunter32.exe	volatility.exe	netmon.exe	packettotal.exe
JoeTrace.exe	cffexplorer.exe	colasoft.exe	tshark.exe
ollydbg.exe	anqr.exe	netwitness.exe	windump.exe
ida.exe	pestudio.exe	netscanpro.exe	PRTG Probe.exe
x64dbg.exe	die.exe	packetanalyzer.exe	NetFlowAnalyzer.exe
cheatengine.exe	ethereal.exe	packettotal.exe	SW.JobEngineWorker2x64.exe
ollyce.exe	Capsa.exe	tshark.exe	NetPerfMonService.exe
fiddler.exe	tcpdump.exe	windump.exe	SolarWinds>DataProcessor.exe
devenv.exe	NetworkMiner.exe	PRTG Probe.exe	ettercap.exe
radare2.exe	smartsniff.exe	NetFlowAnalyzer.exe	apimonitor.exe
ghidra.exe	snort.exe	SW.JobEngineWorker2x64.exe	apimonitor-x64.exe
frida.exe	pcap.exe	NetPerfMonService.exe	apimonitor-x32.exe

En términos de protección por análisis estático, en las versiones de 2024, Grandoreiro ha implementado medidas de cifrado optimizadas. Para dejar de depender de los algoritmos de cifrado que son comunes en otro malware, Grandoreiro ha adoptado un enfoque de cifrado de múltiples capas. El proceso de descifrado en las versiones más recientes es el siguiente. Al principio, la cadena pasa por un proceso de desofuscación a través de un algoritmo de reemplazo simple. A continuación, Grandoreiro emplea el algoritmo de cifrado basado en XOR y la resta condicional característica del malware brasileño; sin embargo, se desvía incorporando una larga cadena de 140759 bytes en lugar de las cadenas mágicas más pequeñas que hemos visto en las muestras de 2022 y 2023. Más adelante, la cadena descifrada se somete a una decodificación base64 antes de descifrarla mediante el algoritmo AES-256. En particular, la clave AES y el IV están cifrados dentro del código de Grandoreiro. Una vez completados todos estos pasos, se recupera la cadena descifrada.

En muestras más recientes, Grandoreiro mejoró una vez más el algoritmo de cifrado utilizando AES con CTS, o Ciphertext Stealing, un modo de cifrado especial que se utiliza cuando el texto plano no es un múltiplo del tamaño del bloque, que en este caso es el tamaño de bloque de 128 bits (16 bytes) utilizado por AES. A diferencia de esquemas de relleno más comunes, como PKCS#7, donde el bloque final se rellena con bytes extra para asegurar que se ajuste a un bloque completo, CTS funciona sin relleno. En cambio, manipula el último bloque parcial de datos cifrando el último bloque completo y usando un bloque parcial para hacer XOR a su salida. Esto permite el cifrado de cualquier entrada de longitud arbitraria sin agregar bytes de relleno extra, preservando el tamaño original de los datos.

En el caso de Grandoreiro, la rutina de cifrado del malware no agrega relleno estándar a los bloques de datos incompletos. Su objetivo principal es complicar el análisis: se necesita tiempo para descubrir que se utilizó CTS, y luego más tiempo para implementar el descifrado en este modo, lo que hace que la extracción y la ofuscación de cadenas sea más complicada. Esta es la primera vez que se observa este método particular en una muestra de malware.

A medida que evolucionan las técnicas de los actores de amenazas, y cambia el cifrado en cada iteración del malware, el uso de CTS en malware puede señalar un cambio hacia prácticas de cifrado más avanzadas.

Cómo roban el dinero de las víctimas

Los operadores de Grandoreiro reciben una amplia variedad de comandos remotos a ejecutar, incluyendo una opción para bloquear la pantalla del usuario y mostrar una imagen personalizada (superposición) para pedirle información adicional a la víctima. Estos suelen ser OTPs (contraseñas de un solo uso), contraseñas de transacción o tokens que se reciben por SMS, enviados por instituciones financieras.

Una nueva táctica que hemos descubierto en las versiones más recientes de julio de 2024 y posteriores sugiere que el malware está capturando patrones de entrada del usuario, en particular movimientos del ratón, para eludir sistemas de seguridad basados en aprendizaje automático. Dos cadenas específicas encontradas en el malware, "GRAVAR_POR_5S_VELOCIDADE_MOUSE_CLIENTE_MEDIA" ("Grabar durante 5 segundos la velocidad media del ratón del cliente") y "Medição iniciada, ¡aguarde 5 segundos!" ("¡Medición iniciada, espere 5 segundos!"), indican que Grandoreiro monitorea y graba la actividad del ratón del usuario durante un corto período de tiempo. Este comportamiento parece ser un intento de imitar las interacciones legítimas de los usuarios para evadir la detección de sistemas antifraude y soluciones de seguridad que se basan en el análisis de comportamiento. Las herramientas modernas de ciberseguridad, especialmente aquellas impulsadas por algoritmos de aprendizaje automático, analizan el comportamiento del usuario para distinguir entre usuarios humanos y bots o scripts de malware automatizados. Al capturar y reproducir estos patrones de movimiento natural del ratón, Grandoreiro podría engañar a estos sistemas para que identifiquen la actividad como legítima, eludiendo así ciertos controles de seguridad.

Este descubrimiento resalta la evolución continua de malware como Grandoreiro, donde los atacantes están incorporando cada vez más tácticas diseñadas para derrotar soluciones de seguridad modernas que dependen de la biometría conductista y el aprendizaje automático.

Para realizar el retiro de efectivo en la cuenta de la víctima, los integrantes de la banda de Grandoreiro pueden optar por transferir dinero a la cuenta de mulas de dinero locales, utilizando aplicaciones de transferencia, comprar criptomonedas, tarjetas de regalo, o incluso ir a un cajero automático. Por lo general, buscan mulas de dinero en los canales de Telegram, pagando de US\$200 a US\$500 por día.

3. RECOMENDACIONES:

- Usar rutas absolutas y esperar que la aplicación cargue solo DLLs en ubicaciones seguras.
- Implementar la firma digital en las DLL para verificar su integridad y autenticidad.
- Aprovechar las configuraciones del sistema que restrinjan la búsqueda de DLL en directorios específicos.
- Mantener los sistemas y aplicaciones actualizados para corregir vulnerabilidades relacionadas con la carga de DLL.
- Utilizar un software antivirus y antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar malware y otro software malicioso antes de que puedan cifrar sus archivos.
- Implementar controles de acceso y autenticación.

Fuente de Información:

- <https://securelist.lat/grandoreiro-banking-trojan/99206/>
- <https://www.welivesecurity.com/la-es/2020/04/28/grandoreiro-troyano-bancario-dirigido-brasil-espana-mexico-peru/>

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 055		Fecha: 06-03-2025
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en productos Cisco		
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			
<p>1. ANTECEDENTES:</p> <p>Cisco Systems, Inc. ha publicado dos vulnerabilidades de severidad ALTA de tipo verificación incorrecta de la firma criptográfica y Cross-site Scripting que afectan a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante ejecutar código arbitrario en la máquina afectada con privilegios de SYSTEM. Asimismo, un atacante puede ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2025-20206 de tipo verificación incorrecta de la firma criptográfica en el canal de comunicación entre procesos (IPC) de Cisco Secure Client para Windows, podría permitir que un atacante local autenticado realice un ataque de secuestro de DLL en un dispositivo afectado si Secure Firewall Posture Engine, anteriormente HostScan, está instalado en Cisco Secure Client. Esta vulnerabilidad se debe a una validación insuficiente de los recursos que carga la aplicación en tiempo de ejecución. Un atacante podría aprovechar esta vulnerabilidad enviando un mensaje IPC diseñado a un proceso específico de Cisco Secure Client. Una explotación exitosa podría permitir al atacante ejecutar código arbitrario en la máquina afectada con privilegios de SYSTEM. Para aprovechar esta vulnerabilidad, el atacante debe tener credenciales de usuario válidas en el sistema Windows.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2025-20208 de tipo Cross-site Scripting en la interfaz de administración basada en web de Cisco TelePresence Management Suite (TMS), podría permitir que un atacante remoto con pocos privilegios realice un ataque de secuencias de comandos entre sitios (XSS) contra un usuario de la interfaz. Esta vulnerabilidad se debe a una validación de entrada insuficiente por parte de la interfaz de administración basada en la web. Un atacante podría aprovechar esta vulnerabilidad insertando datos maliciosos en un campo de datos específico de la interfaz. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> - La vulnerabilidad CVE-2025-20206 afecta a Cisco Secure Client, anterior a la versión 5.1.8.105 para Windows cuando tiene instalado Secure Firewall Posture Engine. - La vulnerabilidad CVE-2025-20208 afecta a Cisco TMS versión 15.13.6. <p>3. RECOMENDACIÓN:</p> <ul style="list-style-type: none"> • Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar la vulnerabilidad CVE-2025-20206. No existen soluciones alternativas. Cisco no ha publicado ni publicará actualizaciones de software para solucionar la vulnerabilidad CVE-2025-20208. Cisco TMS ha entrado en el proceso de fin de vida útil. 			
Fuente de Información:	<ul style="list-style-type: none"> • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-dll-injection-AOyzEqSg • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tms-xss-vuln-WbTcYwxG 		

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 055		Fecha: 06-03-2025
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Western Digital My Cloud OS 5		
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			
<p>1. ANTECEDENTES:</p> <p>Se ha publicado múltiples vulnerabilidades de severidad ALTA de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria, exposición de información confidencial a un actor no autorizado, desbordamiento de búfer basado en el montón y control externo del nombre o ruta de archivo en Western Digital My Cloud OS 5. Podría permitir a un atacante local / remoto aumentar privilegios en el sistema, obtener acceso a información confidencial, ejecutar código arbitrario en el sistema e inyectar cookies arbitrarias en la solicitud.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2023-38545 de tipo desbordamiento de búfer basado en el montón, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite en el protocolo de enlace del proxy SOCKS5. Un atacante remoto puede engañar a la víctima para que visite un sitio web malicioso, desencadenar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso del sistema vulnerable, pero requiere que se utilice el proxy SOCKS5 y que el protocolo de enlace SOCKS5 sea lento.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2023-4154 de tipo exposición de información confidencial a un actor no autorizado, podría permitir a un usuario remoto obtener acceso a información confidencial. La vulnerabilidad existe debido a un error de diseño en la implementación del control DirSync de Samba, que puede permitir la replicación de contraseñas y secretos de dominio críticos por parte de cuentas de AD autorizadas para realizar cierta replicación, pero no para replicar atributos confidenciales. Un usuario remoto puede obtener información confidencial del controlador de dominio de AD y comprometer Active Directory.</p> <p>La vulnerabilidad de severidad baja identificada por MITRE como CVE-2023-4911 de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria, podría permitir a un usuario local provocar una corrupción de memoria y ejecutar código arbitrario con privilegios elevados. Puede explotarse localmente. La vulnerabilidad existe debido a una validación insuficiente de la variable de entorno GLIBC_TUNABLES.</p> <p>La vulnerabilidad de severidad baja identificada por MITRE como CVE-2023-38546 de tipo control externo del nombre o ruta de archivo, podría permitir a un atacante inyectar cookies arbitrarias en la solicitud. La vulnerabilidad existe debido a la forma en que libcurl maneja las cookies. Si una transferencia tiene cookies habilitadas cuando se duplica el identificador, el estado de habilitación de cookies también se clona, pero sin clonar las cookies reales. Si el identificador de origen no leyó ninguna cookie de un archivo específico en el disco, la versión clonada del identificador almacenaría en su lugar el nombre del archivo como none (usando las cuatro letras ASCII, sin comillas). El uso posterior del identificador clonado que no establece explícitamente una fuente desde la cual cargar cookies cargaría inadvertidamente cookies desde un archivo llamado none- si dicho archivo existe y se puede leer en el directorio actual del programa que usa libcurl.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> - My Cloud (P/N: WDBCTLxxxxx-10): todas las versiones. - My Cloud EX2100 / DL4100 / EX4100 / PR4100 / PR2100: todas las versiones. - My Cloud Mirror Gen 2: todas las versiones. - My Cloud EX2 Ultra: todas las versiones. - My Cloud OS 5: anterior a 5.30.103. <p>3. RECOMENDACIÓN:</p> <ul style="list-style-type: none"> • Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades. 			
Fuente de Información:	<ul style="list-style-type: none"> • hxxp://www.westerndigital.com/support/product-security/wdc-25001-western-digital-my-cloud-os-5-firmware-5-30-103 		

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 055		Fecha: 06-03-2025
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en editor de texto de línea de comandos VIM		
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			
<p>1. ANTECEDENTES:</p> <p>GitHub, Inc. ha publicado una vulnerabilidad de severidad ALTA de tipo validación de entrada incorrecta que afecta al editor de texto de línea de comandos de código abierto VIM. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos de shell a través de archivos tar especialmente diseñados.</p> <p>2. DETALLES:</p> <p>Vim se distribuye con el complemento tar.vim, que permite editar y visualizar fácilmente archivos tar (comprimidos o sin comprimir).</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2025-27423 de tipo validación de entrada incorrecta que afecta al editor de texto de línea de comandos de código abierto VIM, podría permitir a un atacante remoto no autenticado ejecutar comandos de shell a través de archivos tar especialmente diseñados. La ejecución de código arbitrario podría llevar al robo de datos, la implementación de ransomware o al movimiento lateral de la red.</p> <p>El complemento tar.vim usa la línea de comando ex ":read" para agregar debajo de la posición del cursor, sin embargo, no se desinfecta y se toma literalmente del archivo tar. Esto permite ejecutar comandos de shell a través de archivos tar especialmente diseñados. Si esto realmente sucede, depende del shell que se use (opción 'shell', que se establece usando \$SHELL).</p> <p>Cabe señalar que, hasta el momento, no hay evidencia de explotación activa ni de código de explotación disponible públicamente para esta vulnerabilidad.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> - Vim, versiones anteriores a v9.1.1164. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Actualizar el producto afectado a la versión 9.1.1164 o posterior que aborda esta vulnerabilidad. • Deshabilitar el complemento tar.vim eliminando o renombrando tar.vim en el directorio de ejecución de Vim. • Evitar archivos TAR de fuentes no confiables y utilizar herramientas de extracción dedicadas como tar o gunzip. • Configurar Vim para utilizar un shell restringido o un shell con configuraciones de seguridad mejoradas. 			
Fuente de Información:		<ul style="list-style-type: none"> • https://github.com/vim/vim/commit/129a8446d23cd9cb4445fcfea259c5ba5e0487d29 • https://github.com/vim/vim/commit/334a13bff78aa0ad206bc436885f63e3a0bab399 • https://github.com/vim/vim/security/advisories/GHSA-wfmf-8626-q3r3 	

Índice alfabético

Explotación de vulnerabilidades conocidas 7, 8, 9
Trojanos 4