TIC

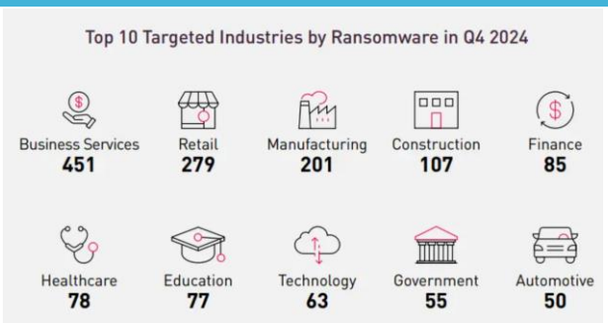
Alerta de Seguridad

COLCERT AL-20250207-062

TLP:CLEAR

Campaña de Ransomware Phobos - Variante "core_visual.exe"

Se ha identificado una nueva variante del ransomware Phobos, distribuida a través del ejecutable malicioso core_visual.exe. Esta amenaza muestra capacidades avanzadas de cifrado, persistencia, evasión de defensas y eliminación de copias de seguridad, lo que la convierte en un riesgo crítico para infraestructuras tanto corporativas como personales. Cifra archivos y añade la extensión .core, elimina copias de seguridad mediante comandos del sistema y modifica el registro de Windows para garantizar su persistencia.



Fuente:CHECK POINT

https://cyberint.com/blog/research/ransomware-annual-report-2024/

Detalles técnicos:

1. Indicadores de Compromiso (IOCs):

- Nombre del archivo malicioso: core_visual.exe
- Hash MD5: F3F1C4B0746B99A513876F5C61E2AD47
- Hash SHA-256:
- 4D5368EA6488CEDCE01F8B2C1ED77E45D37DC2ADF1ED0BADA3932412BC0732F0
- Extensión de archivos cifrados: .core
- Ejemplo de archivo cifrado: documento.txt.core

2. Técnicas de Infección y Propagación:

- Uso de PowerShell y cmd.exe para la ejecución de comandos maliciosos.
- Eliminación de copias de seguridad mediante vssadmin delete shadows /all /quiet.
- Persistencia mediante modificaciones en el registro de Windows (Run y Explorer).
- Alteración de asociaciones de archivos .exe para redirigir su ejecución al ransomware.

3. Cifrado y Comportamiento Malicioso:

- Cifrado de archivos locales y en recursos de red, utilizando algoritmos robustos (probable AES o RSA).
- Eliminación de logs de eventos para dificultar el análisis forense.
- Técnicas de ofuscación en secciones del binario (.ndata con entropía de 7.972).

4. Librerías Identificadas en el Análisis del Binario

- Durante el análisis del binario malicioso core_visual.exe, se identificó el uso de librerías críticas de Windows que facilitan la ejecución del malware y su interacción con el sistema. Destacan MPR.dll para la comunicación con recursos de red, y KERNEL32.dll junto a ADVAPI32.dll para el manejo de procesos, memoria y funciones de seguridad, lo que sugiere un posible abuso para la persistencia y control del sistema.
- Asimismo, librerías como USER32.dll, GDI32.dll, SHELL32.dll, y ole32.dll permiten la manipulación de la interfaz gráfica, archivos y la comunicación entre aplicaciones, mientras que MSIMG32.dll se asocia a funciones de procesamiento de gráficos. Su presencia refleja la capacidad del malware para interactuar de forma avanzada con el entorno comprometido.

Análisis del Stub DOS y Hash SHA-256

Refleja el análisis de la cabecera DOS del binario junto con el hash SHA-256.

property	value
dos-stub > sha256	DA5B8273F69C62206C060B300D0B55669302355D90A03E160C71FB154C604C2D
dos-stub > location	0x00000040 - 0x000000E0
size	0xA0 (160 bytes)
entropy	4.825
file > ratio	0.32 %
first 32 bytes (hex)	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20...
first 32 bytes (hex)	.....!....L..!This program canno
message	!This program cannot be run in DOS mode.

Análisis de Secciones del Binario

Describe el desglose de las secciones del ejecutable, incluyendo entropía, direcciones de memoria y tamaños

property	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]
name	.text	.rdata	.data	.ndata	.rsrc
section > sha256	C3DF6E87B16BF6B29FCFE6A...	496972B65549DB1401470B81...	n/a	EBC2666FAF93F50ABBC725...	C79A33F966BD5E7FD132816...
entropy	6.377	5.105	n/a	7.972	2.324
file > ratio (97.98%)	65.66 %	8.08 %	n/a	22.22 %	2.02 %
raw-address (begin)	0x00000400	0x00008600	0x00000000	0x00009600	0x0000C200
raw-address (end)	0x00008600	0x00009600	0x00000000	0x0000C200	0x0000C600
raw-size (49664 bytes)	0x00008200 (33280 bytes)	0x00001000 (4096 bytes)	0x00000000 (0 bytes)	0x00002C00 (11264 bytes)	0x00000400 (1024 bytes)
virtual-address	0x00001000	0x0000A000	0x0000B000	0x00020000	0x00023000
virtual-size (131291 bytes)	0x00008024 (32804 bytes)	0x00000F62 (3938 bytes)	0x000142BC (82620 bytes)	0x00002BA1 (11169 bytes)	0x000002F8 (760 bytes)

COLCERT

Alerta de Seguridad

Campaña de Ransomware Phobos - Variante "core_visual.exe"

COLCERT AL-20250207-062

TLP:CLEAR

Resumen General de la variante del Ransomware Phobos

Origen y Primera Aparición (2018): Phobos fue detectado por primera vez en 2018, derivado del ransomware Dharma, compartiendo varias técnicas de cifrado y distribución, pero con mejoras en la persistencia y en los métodos de extorsión.

Tácticas de Distribución: Las variantes de Phobos, incluyendo Elking, Devos y Faust, han sido propagadas principalmente a través de ataques de phishing, explotación de servicios RDP mal configurados y documentos de Office con macros maliciosos

Advertencia de CISA sobre Phobos (febrero de 2024): La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) emitió una alerta conjunta con el FBI y el MS-ISAC, advirtiendo sobre las tácticas, técnicas y procedimientos asociados con las variantes de Phobos observadas hasta esa fecha. La advertencia enfatizó la necesidad de proteger los puertos RDP para evitar accesos no autorizados. CISA.GOV.

Ha afectado sectores críticos como salud, educación y gobiernos locales, impactando tanto a grandes organizaciones como a pequeñas empresas.

Recomendaciones de mitigación

Para mitigar el riesgo de ser víctima de esta campaña de ransomware, se recomienda a las entidades/organizaciones implementar las siguientes medidas de seguridad:

A. Contención Inmediata:

- ❑ Desconectar los sistemas afectados de la red para prevenir la propagación.
- ❑ Bloquear IPs/dominios sospechosos detectados en el tráfico de red.
- ❑ Gestión Segura de Credenciales, revocar inmediatamente las credenciales comprometidas, especialmente aquellas con privilegios de administrador. Implementar la autenticación multifactor (MFA) para cuentas críticas.
- ❑ No reiniciar sistemas comprometidos hasta finalizar el análisis forense.

B. Recuperación:

- ❑ Verificar la disponibilidad de copias de seguridad externas.
- ❑ Intentar la recuperación de archivos con herramientas forenses antes de considerar el pago del rescate.
- ❑ Reinstalación y Reconfiguración. Para garantizar la eliminación completa del malware, se recomienda reinstalar sistemas desde cero y restaurar únicamente datos validados como seguros. Evitar la reutilización de configuraciones antiguas sin una auditoría previa.

C. Limpieza del Sistema:

- ❑ Análisis de Memoria y Volcado de Procesos: Utilizar herramientas avanzadas de análisis de memoria (como Volatility o Rekall) para identificar cargas maliciosas persistentes en PowerShell, scripts ofuscados y procesos inusuales en ejecución.
- ❑ Eliminación de Persistencia: Revisar y restaurar claves de registro afectadas, especialmente en las rutas:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Además, verificar tareas programadas y servicios de Windows para eliminar configuraciones de persistencia maliciosa.

- ❑ Análisis de Integridad: Implementar herramientas de verificación de integridad de archivos críticos del sistema (como OSSEC o Tripwire) para identificar modificaciones no autorizadas.

COLCERT

Alerta de Seguridad

Campaña de Ransomware Phobos - Variante "core_visual.exe"

D. Prevención Futura:

- ❑ Implementar segmentación de red y restricciones de ejecución de PowerShell, vssadmin.exe, y wbadmin.exe.
- ❑ Activar auditoría avanzada de eventos y soluciones EDR/XDR para la detección temprana de amenazas.
- ❑ Actualizar planes de respuesta ante incidentes con protocolos específicos para ransomware.

Controles Avanzados

- ❑ **Implementación de EDR/XDR:** Destacar su papel en la detección de actividades sospechosas en tiempo real.
- ❑ **Restricción de PowerShell:** Configurar políticas para que solo scripts firmados puedan ejecutarse.
- ❑ **Backups Inmutables:** Reforzar la importancia de mantener copias de seguridad protegidas contra modificaciones (almacenamiento WORM).

Conclusión

Esta variante de Phobos muestra un alto grado de sofisticación, empleando técnicas avanzadas de cifrado y evasión. La respuesta oportuna, junto con un enfoque proactivo en la detección y la prevención, es fundamental para mitigar su impacto. La implementación de controles técnicos robustos, combinados con la formación continua del personal, fortalece significativamente la postura de seguridad de cualquier organización.

TTPs (Tácticas, Técnicas y Procedimientos)

Fase ATT&CK	ID Técnica	Técnica	Descripción
Acceso Inicial	T1566.001	Phishing (Archivos Adjuntos)	Uso de documentos de Office maliciosos con macros para ejecutar el payload.
	T1204.002	Ejecución de Archivos Descargados	Engaño al usuario para ejecutar archivos maliciosos disfrazados de legítimos.
Ejecución	T1059	Intérprete de Comandos y Scripts	Uso de PowerShell y cmd.exe para ejecutar comandos maliciosos.
	T1106	API Nativa	Ejecución de código mediante llamadas a APIs de Windows.
Persistencia	T1547.001	Claves de Registro Run/Startup	Modificación de claves de registro para mantener persistencia.
	T1037	Servicio de Windows	Configuración de servicios maliciosos para ejecución continua.
Escalada de Privilegios	T1548	Abuso de Mecanismos de Control de Acceso	Uso de credenciales comprometidas y manipulación de permisos.
Evasión de Defensas	**T1027**	Ofuscación de Archivos o Información	Ofuscación del código para evadir antivirus.
	T1497	Evasión de Entornos de Análisis	Detección de entornos virtuales para evitar análisis en sandbox.
	T1218	Uso de Binarios de Confianza (LOLBAS)	Abuso de binarios legítimos de Windows para ocultar actividades maliciosas.
Acceso a Credenciales	T1056	Keylogging	Captura de pulsaciones de teclado para robar credenciales.
	T1556	API Hooking	Manipulación de APIs para interceptar datos de autenticación.

Alerta de Seguridad

Campaña de Ransomware Phobos - Variante "core_visual.exe"

COLCERT AL-20250207-062

TLP:CLEAR

Fase ATT&CK	ID Técnica	Técnica	Descripción
Descubrimiento	T1083	Descubrimiento de Archivos y Directorios	Enumeración de archivos para identificar datos valiosos.
	T1012	Consulta del Registro de Windows	Recolección de información del sistema mediante el registro.
	T1087	Descubrimiento de Cuentas	Identificación de cuentas de usuario y privilegios.
Movimiento Lateral	**T1021.001**	Protocolo de Escritorio Remoto (RDP)	Uso de RDP para moverse lateralmente dentro de la red.
Recolección de Información	T1113	Captura de Pantalla	Toma de capturas de pantalla para monitorear la actividad del usuario.
	T1115	Recolección de Datos del Portapapeles	Acceso a datos del portapapeles para extraer información sensible.
Comando y Control (C2)	T1071.001	Protocolo HTTP/S	Comunicación con servidores C2 mediante HTTP/S.
Impacto	T1486	Cifrado de Datos para Impacto	Cifrado de archivos críticos para extorsionar a la víctima.
	T1490	Eliminación de Copias de Seguridad	Uso de vssadmin delete shadows para eliminar copias de seguridad.

Análisis: ColCERT

"¡Actúe de Inmediato! La detección temprana y la respuesta rápida son clave para mitigar el impacto del ransomware Phobos."

"El ransomware emplea comandos como vssadmin delete shadows para eliminar copias de seguridad, dificultando la recuperación de datos sin el pago del rescate."

HERRAMIENTAS UTILIZADAS:

- ❑ Plataforma Detectic - COLCERT (Sandbox): https://detectic.colcert.gov.co/external-user/upload-sample
- ❑ PEStudio
- ❑ AnyRun Enterprise

NIVEL DE RIESGO

ALTO

FUENTES:

CISA (Cybersecurity and Infrastructure Security Agency)
Fortinet Threat Intelligence
Trend Micro
Malwarebytes Labs
Justice.gov (Departamento de Justicia de EE. UU.)
MITRE ATT&CK Framework

COLCERT