Alerta de Seguridad

Variante del Ransomware MEDUSA

COLCERT AL-20250301-063

TLP:CLEAR

Se ha identificado una nueva variante del Ransomware Medusa, distribuida a través del archivo malicioso bh156.exe. Esta amenaza altamente peligrosa cifra archivos críticos, elimina copias de seguridad para impedir su recuperación y modifica el registro del sistema para garantizar su persistencia, dificultando su detección y eliminación.

Detalles técnicos

1. Indicadores de Compromiso (IOCs):

Archivos Maliciosos Identificados

- Nombre del archivo: bh156.exe
- MD5: 1bd52fa74393f79b5a481b4e45e983c6
- SHA1: 2662a13bab2530bbd6548972446e84eda0792118
- SHA256: 4fd9af8db121171c2bc232f4d1bad76ff225bee5f52e88ab178e9966ef8195bc

Dominios y URLs Relacionados

- api[.]ipify[.]org
- http://c[.]pki[.]goog/r/gsr1[.]crl0
- http://ctldl[.]windowsupdate[.]com/msdownload/update/v3/static/trustedr/en/disallowedcertstl[.]cab?40378f0995bb787c
- https://api[.]ipify[.]org/
- http://i[.]pki[.]goog/we1[.]crt0!
- http://o[.]pki[.]goog/s/we1/ATw0
- http://i[.]pki[.]goog/gsr1[.]crt0-
- http://c[.]pki[.]goog/we1/BR1mWoHyxgA[.]crl0
- http://ctldl[.]windowsupdate[.]com:80/msdownload/update/v3/static/trustedr/en/disallowedcertstl[.]cab?40378f0995bb787c
- http://c[.]pki[.]goog/r/r4[.]crl0
- http://c[.]pki[.]goog/
- http://i[.]pki[.]goog/gsr1[.]crt
- http://ctldl[.]windowsupdate[.]com/msdownload/update/v3/static/trustedr/en/disallowedcertstl[.]cab
- http://c[.]pki[.]goog:80/r/gsr1[.]crl
- http://c[.]pki[.]goog/r/gsr1[.]crl
- http://i[.]pki[.]goog/r4[.]crt0+
- http://ctldl[.]windowsupdate[.]com/

Eventos de Red Identificados

- Conexiones DNS a: api[.]ipify[.]org y c[.]pki[.]goog
- Procesos asociados a las consultas DNS: bh156.exe

Procesos Maliciosos Identificados

- C:\Windows\SysWOW64\cmd.exe
- C:\Windows\System32\taskkill.exe
- C:\Windows\System32\wbadmin.exe
- C:\Windows\System32\conhost.exe
- C:\Windows\System32\cmd.exe

Archivos Creado por el Malware

- C:\Users\Administrator\AppData\Local\Temp\bh156.exe
- C:\read_to_decrypt_files.html
- C:\$RECYCLE.BIN\read_to_decrypt_files.html
- C:\Users\Administrator\AppData\Local\Temp\external_ip.blackheart156
- C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8B2B9A00839EED1DFDCCC3BFC2F5DF12
- C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B46811C17859FFB409CF0E904A4AA8F8

"Los siguientes procesos son legítimos del sistema operativo Windows, pero han sido utilizados por Medusa Ransomware para ejecutar comandos maliciosos, eliminar copias de seguridad y persistir en el sistema. No se recomienda su bloqueo total, sino el monitoreo de su uso inusual."

Alerta de Seguridad
Variante del Ransomware MEDUSA

COLCERT AL-20250301-063

TLP:CLEAR

2. Técnicas de Infección y Propagación:

Métodos de Infección:

- El malware bh156.exe es un ejecutable Portable Executable (PE) que se ejecuta en entornos Windows sin una firma digital válida, facilitando su distribución mediante phishing, adjuntos maliciosos o descargas fraudulentas.
- Ejecuta comandos del sistema para cargar código malicioso en memoria, evitando ser detectado por soluciones antivirus tradicionales.
- Importa la librería urlmon.dll, lo que sugiere que puede descargar más componentes maliciosos desde servidores remotos.
- Se conecta a **api[.]ipify[.]org** para determinar la ubicación geográfica del sistema infectado, posiblemente ajustando el comportamiento del ataque en función del país.

3. Cifrado y Comportamiento Malicioso:

- Utiliza funciones criptográficas como **CryptEncrypt** y **CryptFile** para cifrar archivos del sistema.
- Los archivos cifrados reciben la extensión .MEDUSA, bloqueando el acceso a la información.
- Genera claves únicas por víctima y borra las claves criptográficas **(CryptDestroyKey)** para impedir la recuperación de datos sin pagar el rescate.

4. Librerías Identificadas en el Análisis del Binario

Durante el análisis técnico del ransomware Medusa (bh156.exe), se identificaron múltiples librerías del sistema de Windows utilizadas para llevar a cabo sus actividades maliciosas.

Librerías Relacionadas con Cifrado:

- CRYPT32.dll → Contiene funciones de cifrado, lo que sugiere el uso de técnicas de encriptación de archivos.
- ADVAPI32.dll → Utilizada para la manipulación de claves criptográficas, generación de valores aleatorios y cifrado de datos (CryptEncrypt, CryptGenRandom, CryptDestroyKey).

Métodos de Propagación:

- Persistencia en el sistema: Modifica el Registro de Windows **(HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run)** para ejecutarse automáticamente en cada reinicio.

Manipula la clave **HKEY_CURRENT_USER\Software\Classes\exefile\shell\open\command** para redirigir la ejecución de programas a bh156.exe, bloqueando el uso normal del sistema.

- Movimientos laterales en red: Usa **WNetGetConnection** para identificar unidades de red mapeadas y potencialmente propagarse a otros dispositivos en la misma infraestructura.
- Eliminación de copias de seguridad: Ejecuta los comandos:
  - **vssadmin delete shadows /all /quiet** (borra las Shadow Copies del sistema).
  - **wbadmin delete catalog -quiet** (elimina catálogos de copias de seguridad).
  - **bcdedit /set {default} recoveryenabled** No (desactiva la recuperación automática).
- Manipulación de procesos y permisos:Usa funciones como **OpenProcess, CreateProcessW** y **GetTokenInformation** para escalar privilegios, inyectarse en procesos legítimos y ocultar su ejecución.

Librerías Relacionadas con Manipulación del Sistema:

- KERNEL32.dll → Proporciona acceso a funciones críticas del sistema, incluyendo manipulación de procesos, memoria y archivos (OpenProcess, CreateProcessW).
- ADVAPI32.dll → Permite modificar el Registro de Windows y gestionar privilegios de usuario, asegurando la persistencia del malware.

Librerías Relacionadas con Conectividad y Descarga de Payloads:

- urlmon.dll → Indica la capacidad de descargar archivos maliciosos desde servidores remotos (URLDownloadToFile).
- MPR.dll → Puede ser utilizada para manipular conexiones de red y acceder a recursos compartidos, lo que sugiere intentos de propagación lateral.

COLCERT

Alerta de Seguridad

Variante del Ransomware MEDUSA

COLCERT AL-20250301-063

TLP:CLEAR

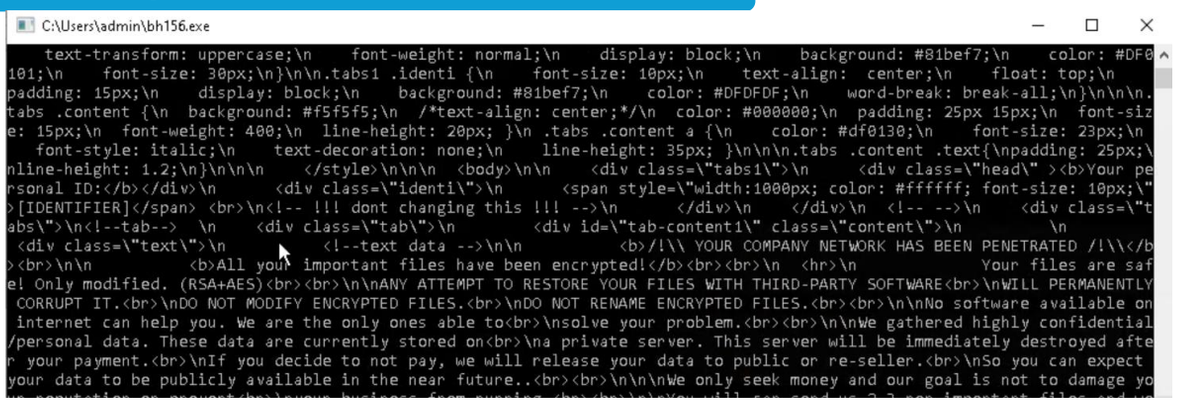
Análisis de Secciones del Binario

property	value
file	
file > sha256	4FD9AF8DB121171C2BC232F4D1BAD76FF225BEE5F52E88AB178E9966EF8195BC
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first 32 bytes (text)	MZ.....@.....
file > info	size: 743936 bytes, entropy: 6.591
file > type	executable, 64-bit, console
file > version	n/a
file > description	n/a
entry-point > first 32 bytes (hex)	48 83 EC 28 E8 63 06 00 00 48 83 C4 28 E9 72 FE FF FF CC CC 48 83 EC 28 4D 8B 41 38 48 8B CA 49
entry-point > location	0x00042118 (section[.text])
file > signature	Microsoft Linker 14.42 | Visual Studio 2015

El archivo bh156.exe presenta un hash SHA-256 único, es un ejecutable de Windows y fue compilado con Microsoft Linker 14.42. Su alta entropía y la ausencia de una firma digital legítima indican que podría estar ofuscado, lo que sugiere intenciones maliciosas y evasión de detección.

Cifrado y Extensión de Archivos Afectados

"Mensaje de rescate generado por Medusa Ransomware, informando a la víctima sobre el cifrado de archivos y advirtiendo contra intentos de recuperación sin el pago del rescate. Se menciona el uso de cifrado RSA y AES para bloquear el acceso a los archivos.



Resumen General de la variante del Ransomware MEDUSA

Historia y Origen: también conocido como MedusaBlog, es un ransomware que afecta a sistemas Windows. Surgió en junio de 2021, ganando prominencia a principios de 2023. cyberguru.it

No confundir con MedusaLocker: Aunque comparten nombres similares, MedusaLocker es una variante diferente que apareció en 2019 como Ransomware-as-a-Service (RaaS). ecucert.gob.

Casos destacados

En 2023, las Escuelas Públicas de Minneapolis (MPS) fue víctima de un ataque de Medusa. Al negarse a pagar un rescate de 1 millón de dólares, aproximadamente 92 GB de datos robados fueron divulgados públicamente. Tripwire

En enero de 2025, el Hospital de Alta Complejidad El Cruce "Néstor Kirchner" sufrió un ataque de Medusa, comprometiendo datos sensibles de pacientes y operaciones internas. . suspectfile.com

COLCERT

Alerta de Seguridad

Variante del Ransomware MEDUSA

COLCERT AL-20250301-063

TLP:CLEAR

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. Aislamiento y Contención

- ❑ Desconectar sistemas infectados de la red y deshabilitar RDP si no es necesario.
- ❑ Bloquear direcciones IP maliciosas en firewalls y revisar logs de red.
- ❑ Evitar pagar el rescate y contactar a equipos de respuesta a incidentes (COLCERT/CSIRT).

B. Recuperación y Eliminación del Malware:

- ❑ Restaurar desde backups seguros y offline en un entorno aislado.
- ❑ Analizar y limpiar claves de Registro afectadas para eliminar persistencia.
- ❑ Usar sandbox y herramientas forenses para identificar payloads ocultos.

C. Fortalecimiento de Seguridad:

- ❑ Aplicar restricciones en GPO para bloquear vssadmin.exe y wbadmin.exe.
- ❑ Implementar segmentación de red y listas blancas de aplicaciones (AppLocker/WDAC).
- ❑ Actualizar sistemas y software para mitigar vulnerabilidades explotadas.

.

D. Monitoreo y Prevención:

- ❑ Implementar EDR/XDR y auditoría avanzada para detectar actividad maliciosa.
- ❑ Monitorear tráfico de red con IDS/IPS para identificar conexiones sospechosas.
- ❑ Desarrollar y probar planes de respuesta a incidentes ante ataques de ransomware.

TTPs (Tácticas, Técnicas y Procedimientos)

Táctica	Técnica Identificada	Procedimiento Específico en Medusa Ransomware
Initial Access (TA0001)		Medusa Ransomware se propaga mediante phishing con archivos maliciosos (.exe), explotación de RDP expuesto y descargas desde sitios comprometidos.
Execution (TA0002)	Windows Command Shell (T1059.003)	Usa cmd.exe para ejecutar comandos maliciosos, incluyendo la eliminación de backups con vssadmin delete shadows /all /quiet.
	Native API (T1106)	Utiliza funciones API de Windows (CryptEncrypt, OpenProcess) para cifrar archivos y manipular procesos.
	Windows Management Instrumentation (T1047)	Ejecuta comandos remotos con wmic.exe para manipular servicios y propagarse en la red.
	Malicious File (T1204.002)	Se distribuye en archivos .exe (bh156.exe), ejecutándose automáticamente tras su descarga.
	Command and Scripting Interpreter (T1059)	Usa PowerShell y cmd.exe para ejecutar scripts maliciosos y cargar payloads en memoria ([System.Reflection.Assembly]::Load(...)).
	Shared Modules (T1129)	Inyecta DLLs maliciosas en procesos legítimos para evadir detección (rundll32.exe malicious.dll).
Persistence (TA0003)	Registry Run Keys / Startup Folder (T1547.001)	Modifica HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run para ejecutarse en cada inicio.
	Windows Service (T1543.003)	Se instala como un servicio persistente usando sc.exe create.

COLCERT

Alerta de Seguridad

Variante del Ransomware MEDUSA

COLCERT AL-20250301-063

TLP:CLEAR

TTPs (Tácticas, Técnicas y Procedimientos)

Táctica	Técnica Identificada	Procedimiento Específico en Medusa Ransomware
⬆️ Privilege Escalation (TA0004)	Registry Run Keys / Startup Folder (T1547.001)	Usa claves de registro para obtener ejecución con privilegios elevados.
	Parent PID Spoofing (T1134.004)	Asigna su ejecución a procesos legítimos para ocultarse en el sistema.
	Make Impersonation Token (T1134.001)	Crea tokens de usuario y los usa para ejecutar comandos con privilegios.
	Token Impersonation / Theft (T1134)	Roba tokens de autenticación (SeImpersonatePrivilege) para ejecución con privilegios.
	Windows Service (T1543.003)	Se instala como servicio del sistema (sc.exe) para ejecutarse con permisos elevados.
🛡️ Defense Evasion (TA0005)	File Deletion (T1070.004)	Borra archivos temporales y registros para ocultar su actividad.
	Parent PID Spoofing (T1134.004)	Se hace pasar por procesos legítimos para evitar detección.
	Hidden Files and Directories (T1564.001)	Oculta archivos maliciosos en %APPDATA%, %TEMP%.
	Deobfuscated/Decoded Files or Information (T1140)	Desofusca código malicioso en memoria.
	Obfuscated Files or Information (T1027)	Usa técnicas de ofuscación para evitar detección.
	Modified Registry (T1112)	Modifica claves de registro para persistencia y evasión.
	Embedded Payloads (T1027.002)	Incrusta código malicioso dentro de procesos legítimos.
	Debugger Evasion (T1622)	Detecta si se ejecuta en entornos de depuración.
	Virtualization/Sandbox Evasion (T1497.001)	Evita ejecución en entornos virtuales o de análisis.
	Timed Execution (T1497.003)	Introduce retardos en su ejecución (Sleep()).
	Make and Impersonate Token (T1134.001)	Crea e impersona tokens de usuario.
	Indicator Removal from Tools (T1070.006)	Borra logs del sistema (wevtutil cl System).
	Impair Defenses (T1562.001)	Desactiva antivirus y soluciones EDR/XDR (taskkill /F /IM defender.exe).
	Modify Timestamps (T1070.006)	Manipula fechas de archivos (Timestomping).
	Disable or Modify Tools (T1562.001)	Desactiva herramientas de seguridad (Windows Defender).
	Execution Guardrails (T1480)	Se ejecuta solo si detecta ciertas condiciones del sistema.
	Match Legitimate Name or Location (T1036.005)	Usa nombres similares a procesos legítimos (explorer.exe).
🔑 Credential Access (TA0006)	Keylogging (T1056.001)	Captura pulsaciones de teclado para robar credenciales.
🔍 Discovery (TA0007)	File and Directory Discovery (T1083)	Escanea directorios en busca de archivos valiosos.
	Query Registry (T1012)	Consulta claves de registro para identificar software de seguridad.
	System Information Discovery (T1082)	Recopila datos del sistema operativo.
	System Network Configuration Discovery (T1016)	Obtiene información de red para propagación.
	Process Location Discovery (T1057)	Enumera procesos en ejecución.
	Application Window Discovery (T1010)	Identifica qué aplicaciones están activas.
	System Checks (T1497)	Evalúa configuraciones de seguridad antes de ejecutar carga útil.
➡️ Lateral Movement (TA0008)		Se ha reportado el uso de WMI y RDP para propagarse.
📥 Collection (TA0009)	Data from Local System (T1005)	Extrae archivos importantes antes del cifrado.
	Screen Capture (T1113)	Toma capturas de pantalla del sistema comprometido.
	Keylogging (T1056.001)	Registra pulsaciones del teclado.
	Local Data Staging (T1074.001)	Almacena datos antes de la exfiltración.

TIC

Alerta de Seguridad

Variante del Ransomware MEDUSA

COLCERT AL-20250301-063

TLP:CLEAR

TTPs (Tácticas, Técnicas y Procedimientos)

Táctica	Técnica Identificada	Procedimiento Específico en Medusa Ransomware
Command and Control (TA0011)	External Proxy (T1090.002)	Usa proxies externos para ocultar su tráfico.
	DNS (T1071.004)	Establece comunicación con servidores de C2 mediante DNS tunneling.
Exfiltration (TA0010)		Puede exfiltrar archivos clave antes de cifrarlos.
Impact (TA0040)	Data Encrypted for Impact (T1486)	Cifra archivos del sistema con la extensión .MEDUSA.
	Inhibit System Recovery (T1490)	Elimina copias de seguridad (wbadmin delete catalog).
	Service Stop (T1489)	Finaliza procesos críticos (taskkill /F /IM sqlserver.exe).
	Data Destruction (T1485)	Puede eliminar archivos clave si la víctima no paga el rescate.

Conclusiones

- Medusa Ransomware no solo cifra archivos críticos, sino que también exfiltra información confidencial para presionar a las víctimas a pagar el rescate. Su impacto es significativo en sectores como salud, educación y entidades gubernamentales, donde la disponibilidad de datos es clave para la continuidad operativa.
- Implementa técnicas de ofuscación de código, ejecución en memoria y modificación del Registro de Windows para asegurar su persistencia en los sistemas comprometidos. Además, elimina copias de seguridad y deshabilita mecanismos de recuperación, dificultando la restauración sin intervención externa.
- Puede expandirse dentro de la red interna explotando credenciales débiles y utilizando herramientas nativas de Windows como WMI y RDP. Esto permite que un solo punto de infección escale rápidamente, comprometiendo múltiples dispositivos dentro de la infraestructura afectada.
- Utiliza técnicas de evasión de sandbox, modificación de marcas de tiempo y manipulación de procesos para evitar la detección por herramientas EDR/XDR. Su capacidad para inyectar código en procesos legítimos lo hace especialmente difícil de detectar y contener.
- La variante Medusa sigue evolucionando con nuevas capacidades, incluyendo ajustes en su cifrado, técnicas de exfiltración mejoradas y adaptación a nuevas medidas de seguridad. Esto refuerza la necesidad de un monitoreo constante y actualizaciones en las estrategias de defensa.

Medusa Ransomware representa una amenaza altamente sofisticada y destructiva, combinando persistencia, evasión y doble extorsión. La rápida respuesta ante incidentes y una estrategia de detección proactiva son esenciales para mitigar su impacto.

NIVEL DE RIESGO

ALTO

FUENTES:

1. **CISA** – Alertas de ransomware e indicadores de compromiso. cisa.gov
2. **MITRE ATT&CK** – Base de datos de tácticas y técnicas. attack.mitre.org
3. **EcuCERT** – Reportes de amenazas en Latinoamérica. ecucert.gob.ec
4. **ENISA** – Informes de seguridad y respuesta a incidentes. enisa.europa.eu
5. **MalwareBazaar** – Repositorio de muestras de malware. bazaar.abuse.ch
6. **CyberGuru** – Análisis de ransomware. cyberguru.it
7. **Tripwire** – Seguridad y mitigación de ransomware. tripwire.com
8. **SuspectFile** – Investigación sobre ciberamenazas. suspectfile.com

HERRAMIENTAS UTILIZADAS:

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

COLCERT