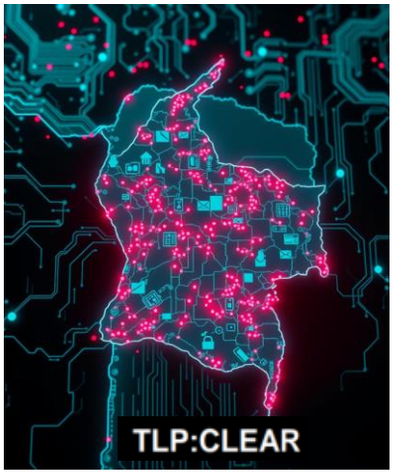
TIC

ALERTA

Amenaza de Ransomware Ymir y RustyStealer en Colombia

COLCERT AL-1511-057

Recientemente se ha identificado un nuevo ransomware conocido como Ymir en Colombia, que presenta características avanzadas para evadir la detección y comprometer sistemas. Este ransomware a menudo se despliega tras una infección inicial por RustyStealer, un malware especializado en robar credenciales. Éste se infiltra en los sistemas a través de correos electrónicos de phishing y vulnerabilidades de software, permitiendo a los atacantes obtener acceso privilegiado. Posteriormente, Ymir utiliza comandos de PowerShell y técnicas de gestión de memoria para ejecutar herramientas maliciosas y cifrar datos críticos en los sistemas afectados.



¿Por qué ajustar la postura de seguridad?

Si no se ajustan los controles y la postura de seguridad para prevenir ataques de ransomware, las entidades y organizaciones pueden enfrentar incidentes de seguridad que causen la pérdida permanente de datos críticos, interrupciones significativas en sus operaciones y costos económicos elevados. Además, pueden sufrir daños a su reputación, sanciones legales y la exposición de datos sensibles de clientes y empleados, lo que puede llevar a fraudes y robo de identidad. La recuperación de un ataque de este tipo puede ser lenta y costosa, afectando gravemente la capacidad para operar normalmente.

Características del Ransomware Ymir

- Método de infección: Los atacantes utilizan comandos de PowerShell para acceder a los sistemas y ejecutar el ransomware.
- Estrategia de evasión: Ymir realiza operaciones en memoria, lo que dificulta su detección por software antivirus.
- Cifrado de archivos: Utiliza el algoritmo ChaCha20 para cifrar archivos, añadiendo la extensión .6C5oy2dVr6 a los archivos afectados.
- Nota de rescate: Genera un archivo PDF llamado INCIDENT_REPORT.pdf en cada directorio afectado, informando a la víctima sobre el ataque y las instrucciones para contactar a los atacantes.

Recomendaciones para Mitigar el Riesgo

1. Actualización de Sistemas y Software

✓ Mantener todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad. Esto incluye software antivirus, sistemas operativos y aplicaciones críticas.

2. Implementación de Soluciones de Seguridad

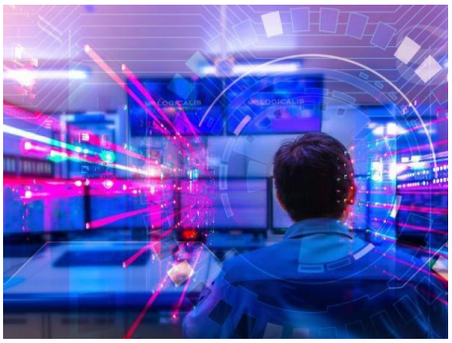
✓ Utilizar software antiransomware y soluciones de seguridad avanzadas, que incluyen protección en tiempo real y capacidades de detección y respuesta ante incidentes (EDR/XDR).

COLCERT

ALERTA

Amenaza de Ransomware Ymir y RustyStealer en Colombia

COLCERT AL-1511-057



3. Educación y conciencia de los usuarios

✓ Capacitar a los colaboradores sobre las amenazas cibernéticas, incluyendo cómo identificar correos electrónicos sospechosos y enlaces maliciosos. La concienciación del personal es crucial para prevenir ataques de este tipo.

4. Restricciones en el Uso de PowerShell

✓ Limitar el uso de PowerShell a usuarios autorizados y deshabilitar su ejecución si no es necesaria para las operaciones diarias.

5. Copias de Seguridad Regulares

✓ Realizar copias de seguridad periódicas de datos críticos y asegurarse de que estas copias estén almacenadas en un entorno seguro y desconectado de la red principal. Esto garantiza que los datos puedan recuperarse en caso de un ataque exitoso.

6. Control de Acceso

✓ Implementar autenticación multifactor (MFA) para todas las cuentas, especialmente aquellas que tienen acceso a datos sensibles o sistemas críticos. Esto añade una capa adicional de seguridad contra accesos no autorizados

7. Monitoreo y Respuesta a Incidentes

✓ Implementar soluciones de monitoreo continuo para detectar actividades inusuales en la red y establecer un plan de respuesta ante incidentes cibernéticos.

8. Evitar Prácticas Inseguras

✓ Establecer políticas claras sobre la apertura de correos electrónicos desconocidos, descarga de archivos adjuntos y navegación en sitios web no seguros.

9. Revisión de Credenciales

✓ Auditar regularmente las credenciales utilizadas en la red, asegurando que no haya cuentas con privilegios innecesarios o comprometidas.

La aparición de éste nuevo ransomware, representa una amenaza significativa para las entidades y organizaciones en Colombia. La implementación proactiva de medidas de seguridad es crucial para prevenir ataques cibernéticos y proteger datos críticos. Es fundamental mantener una postura de seguridad activa y estar preparados para responder rápidamente ante cualquier incidente potencial.

COLCERT

ALERTA

Amenaza de Ransomware Ymir y RustyStealer en Colombia

COLCERT AL-1511-057

En la siguiente tabla se describen los Indicadores de Compromiso (IoC) asociados a las muestras analizadas. Para obtener un mayor contexto sobre esta amenaza, se recomienda revisar la información publicada en las fuentes de esta alerta.

Tipo	Valor	Descripción
MD5	12acbb05741a218a1c83eaa1cfc2401f	Hash del archivo Ymir.
SHA-1	3648359ebae8ce7cacae1e631103659f5a8c630e	Hash del archivo Ymir.
SHA-256	cb88edd192d49db12f444f764c3bdc287703666167a4ca8d533d51f86ba428d8	Hash del archivo Ymir.
MD5 (PDF)	f954d1b1d13a5e4f62f108c9965707a2aa2a3c89	Hash del archivo PDF de nota de rescate.
MD5 (RustyStealer)	5ee1befc69d120976a60a97d3254e9eb	Hash del archivo RustyStealer.
MD5 (Script 1)	5384d704fadf229d08eab696404cbba6	Hash del primer script PowerShell.
MD5 (Script 2)	39df773139f505657d11749804953be5	Hash del segundo script PowerShell.
IP	74.50.84[.]181:443	IP del servidor C2 asociado con el ataque.
IP	94.158.244[.]69:443	IP del servidor C2 asociado con el ataque.
IP	5.255.117[.]134:80	IP del servidor C2 asociado con el ataque.
Extensión	.6C5oy2dVr6	Extensión de archivos cifrados por el ransomware Ymir.
Nombre de archivo (PDF)	INCIDENT_REPORT.pdf	Nombre del archivo PDF utilizado como nota de rescate.
Comando (PowerShell)	powershell -w h -c Start-Sleep -Seconds 5; Remove-Item -Force -Path	Comando para eliminarse a sí mismo usando PowerShell.

NIVEL DE RIESGO

ALTO

FUENTES:

https://securelist.com/new-ymir-ransomware-found-in-colombia/114493/

https://otx.alienvault.com/pulse/6731e6e06cc8432d76e8e4d7

COLCERT