Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVO RANSOMWARE 'YMIR' CIFRA DATOS DE UNA EMPRESA FINANCIERA EN COLOMBIA

13 / 11 / 2024

CONTENIDO

INTRODUCCIÓN

Se aborda un caso de intrusión cibernética que comenzó con un acceso no autorizado a un host RDP expuesto, utilizando credenciales legítimas de la cuenta de Administrador predeterminada. Lo destacado de este ataque radica en la ausencia de intentos de fuerza bruta, sugiriendo la posibilidad de acceso previo recurrente o la intervención de un intermediario de acceso. Una vez dentro, los perpetradores desplegaron diversas herramientas, incluyendo scripts por lotes, ejecutables y SoftPerfect Netscan, para realizar escaneos de red, identificar comparticiones y explorar documentos. La intrusión avanzó con movimientos laterales, deshabilitación de Windows Defender y exfiltración de datos hacia Mega.io mediante Rclone. La sorpresa llegó cuando, tras una desconexión, los atacantes se reconectaron desde una dirección IP diferente, indicando un conocimiento profundo de la red.

NUEVO RANSOMWARE 'YMIR' CIFRA DATOS DE UNA EMPRESA FINANCIERA EN COLOMBIA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_11_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/11/2024
Es día cero (0 day):	No

RESUMEN

Una empresa del sector financiero en Colombia ha sido víctima de un sofisticado ataque de ciberseguridad en el que se desplegó el nuevo ransomware conocido como 'Ymir'. Este malware encripta datos críticos tras aprovechar infecciones previas del malware RustyStealer, que actúa como herramienta de acceso inicial.

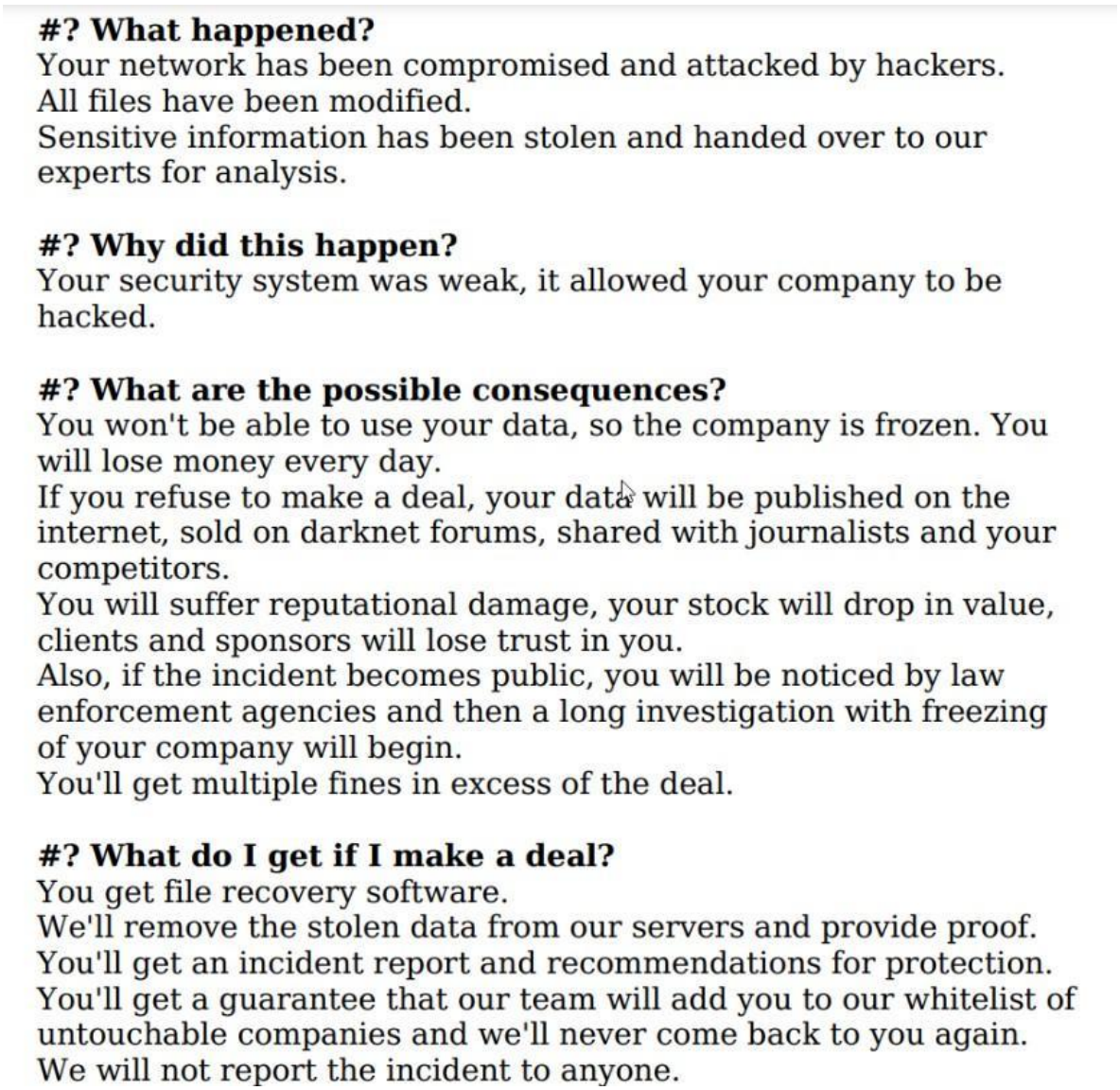
Técnicas avanzadas empleadas en el ataque

El ataque fue caracterizado por el uso de tácticas avanzadas que permitieron el acceso, movimiento lateral y la posterior cifrado de información en la red de la empresa:

Técnica MITRE ATT&CK	Descripción
Servicios remotos (T1021.006)	Los atacantes utilizaron Windows Remote Management (WinRM) para acceder a sistemas clave de manera remota, empleando credenciales comprometidas.
Cuentas válidas (T1078)	Se aprovecharon credenciales obtenidas previamente para infiltrarse en la red y acceder a sistemas críticos.
Captura de credenciales Kerberos (T1558)	RustyStealer fue desplegado para extraer información confidencial y credenciales.
Intérprete de comandos y scripts: PowerShell (T1059.001)	Se ejecutaron comandos maliciosos y scripts para el despliegue del ransomware.
Transferencia lateral de herramientas (T1570)	Herramientas como Advanced IP Scanner facilitaron el movimiento lateral dentro de la red.
Desactivación de defensas (T1562)	Los atacantes desactivaron herramientas de seguridad, abriendo el camino para el despliegue del ransomware.
Modificación de procesos del sistema (T1547.001)	Se utilizaron herramientas como Process Hacker para reconocimiento y persistencia.
Cifrado de datos para impacto (T1486)	Se aplicó el algoritmo de cifrado ChaCha20 para bloquear los archivos de las víctimas.
Inyección de procesos (T1055)	Funciones como malloc, memmove y memcmp fueron empleadas para tareas en memoria, evadiendo detección.
Exfiltración a través de canales de comando y control (T1041)	Datos específicos fueron transferidos a direcciones remotas mediante canales encubiertos.
Descubrimiento de sistemas remotos (T1018)	Advanced IP Scanner permitió mapear dispositivos y servicios en la red.
Eliminación de indicadores en el host (T1070)	Se borraron registros y trazas para dificultar la investigación.

Cómo operó 'Ymir'

El ransomware Ymir, que opera exclusivamente desde la memoria del sistema, desplegó técnicas avanzadas para evadir detección. Durante su ejecución, el malware realizó reconocimiento del sistema, identificó procesos en ejecución y verificó el entorno para evitar sandboxes.
El cifrado de archivos se realizó utilizando extensiones generadas aleatoriamente, como ".6C5oy2dVr6", y se generó una nota de rescate en formato PDF titulada "INCIDENT_REPORT.pdf". Además, el ransomware modificó valores en el registro de Windows para mostrar mensajes de extorsión antes de que el usuario iniciara sesión.



#? What happened?
Your network has been compromised and attacked by hackers.
All files have been modified.
Sensitive information has been stolen and handed over to our experts for analysis.

#? Why did this happen?
Your security system was weak, it allowed your company to be hacked.

#? What are the possible consequences?
You won't be able to use your data, so the company is frozen. You will lose money every day.
If you refuse to make a deal, your data will be published on the internet, sold on darknet forums, shared with journalists and your competitors.
You will suffer reputational damage, your stock will drop in value, clients and sponsors will lose trust in you.
Also, if the incident becomes public, you will be noticed by law enforcement agencies and then a long investigation with freezing of your company will begin.
You'll get multiple fines in excess of the deal.

#? What do I get if I make a deal?
You get file recovery software.
We'll remove the stolen data from our servers and provide proof.
You'll get an incident report and recommendations for protection.
You'll get a guarantee that our team will add you to our whitelist of untouchable companies and we'll never come back to you again.
We will not report the incident to anyone.

¿Qué podemos esperar de 'Ymir'?
Aunque aún no se ha identificado un sitio de filtración de datos asociado con Ymir, este nuevo ransomware plantea una seria amenaza al combinar herramientas de acceso inicial como RustyStealer con avanzadas técnicas de persistencia, movimiento lateral y cifrado.

Es crucial que las empresas implementen medidas proactivas, como la supervisión de cuentas privilegiadas, el uso de autenticación multifactor y la actualización constante de sus herramientas de seguridad, para mitigar ataques similares.
Mantener una vigilancia activa y contar con protocolos de respuesta rápida será clave para enfrentar esta nueva amenaza.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20241113_Ymir

NOTICIA COMPLETA

https://devel.group/blog/nuevo-ransomware-ymir-cifra-datos-de-una-empresa-financiera-en-colombia-utilizando-avanzadas-tecnicas-de-ataque/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente