Cring, el ransomware que se aprovecha de software antiguo para lanzar su ataque

CIUDAD DE MÉXICO. 6 de octubre de 2021.- Sophos, líder mundial en ciberseguridad de última generación, publicó una investigación llamada **"**Cring Ransomware exploits Ancient ColdFusion Server**"**, que describe un ataque sofisticado que los operadores de *ransomware* Cring lanzaron luego de intervenir un servidor ejecutando una versión de hace 11 años, sin parches, del software ColdFusion 9 de Adobe.

Los atacantes, describe Sophos, usaron el servidor para recopilar los datos contables para la nómina de la empresa y violaron el servidor de acceso a Internet en minutos, para ejecutar el *ransomware* 79 horas después.

"*Los dispositivos que ejecutan software vulnerable y obsoleto son un fruto fácil para los ciberatacantes que buscan una forma fácil de llegar a un objetivo"*, **dijo Andrew Brandt, investigador principal de Sophos.** "*Cring ransomware no es nuevo, pero es poco común. En el incidente que investigamos, el objetivo era una empresa de servicios, y todo lo que se necesitó para entrar fue una máquina conectada a Internet que ejecutaba un software antiguo, desactualizado y sin parches. Lo sorprendente es que este servidor estaba en uso diario activo. A menudo, los dispositivos más vulnerables son máquinas inactivas o fantasmas, ya sea olvidadas o pasadas por alto cuando se trata de parches y actualizaciones*".

El análisis de Sophos muestra que los atacantes comenzaron escaneando el sitio web del objetivo utilizando herramientas automatizadas y pudieron ingresar, en minutos, una vez que identificaron que estaba ejecutando ColdFusion sin parches en un servidor.

Sophos descubrió que después de la infracción inicial, los atacantes utilizaron técnicas bastante sofisticadas para ocultar sus archivos, inyectar código en la memoria y cubrir sus huellas sobrescribiendo archivos con datos confusos, así como eliminando registros y otros artefactos que los cazadores de amenazas podrían usar en una investigación. Los atacantes también pudieron desactivar los productos de seguridad porque la función de protección contra manipulaciones estaba desactivada.

Los atacantes publicaron una nota de rescate que indicaba que también robaron datos que estaban "listos para filtrarse en caso de no llegar a un buen trato".

Sophos recomienda las siguientes prácticas para ayudar a defenderse contra Cring y otros tipos de ransomware y ciberataques relacionados:

A nivel estratégico:

- **Implementar protección en capas**. A medida que más ataques de ransomware comienzan a utilizar la extorsión, las copias de seguridad siguen siendo necesarias, pero insuficientes. Es más importante que nunca mantener alejados a los adversarios

en primer lugar, o detectarlos rápidamente, antes de que causen daño. Las empresas deben utilizar protección en capas para bloquear y detectar atacantes en tantos puntos como sea posible.

- **Combinar expertos humanos y tecnología anti-ransomware.** La clave para detener el ransomware es la defensa en profundidad que combina tecnología y la búsqueda de amenazas dirigida por humanos. La tecnología proporciona la escala y la automatización que necesita una organización, mientras que los expertos humanos son capaces de detectar las tácticas y procedimientos que indican que un atacante está intentando ingresar al entorno.

A nivel táctico del día a día:

- **Monitorear y responder a alertas.** Los atacantes de ransomware a menudo programan su ataque durante las horas de menor actividad, los fines de semana o durante las vacaciones, en el supuesto de que poco o ningún personal está mirando.
- **Establecer y hacer cumplir contraseñas seguras.** Las contraseñas seguras sirven como una de las primeras líneas de defensa. Las contraseñas deben ser únicas o complejas y nunca reutilizarse. Esto es más fácil de lograr con un administrador de contraseñas que puede almacenar las credenciales del personal.
- **Utilizar la autenticación multifactor (MFA).** Incluso las contraseñas seguras pueden verse comprometidas. Cualquier forma de autenticación multifactorial es mejor para asegurar el acceso a recursos críticos como correo electrónico, herramientas de administración remota y activos de red.
- **Bloquear los servicios accesibles.** Realizar escaneos de red desde el exterior e identificar los puertos comúnmente utilizados por herramientas de acceso remoto es fundamental. Si una máquina necesita ser accesible mediante una herramienta de administración remota, ésta se debe colocar detrás de una VPN o una solución de acceso a la red de confianza cero que use MFA como parte de su inicio de sesión.
- **Segmentación y confianza cero.** Se deben separar los servidores críticos entre sí y de las estaciones de trabajo colocándolos en VLAN independientes mientras trabajan hacia un modelo de red de confianza cero.
- **Realizar copias de seguridad de la información y las aplicaciones sin conexión.** Las empresas deben mantener las copias de seguridad actualizadas, garantice su recuperabilidad y mantenga una copia fuera de línea
- **Hacer un inventario de sus activos y cuentas.** Los dispositivos desconocidos, desprotegidos y sin parches en la red aumentan el riesgo y crean una situación en la que las actividades maliciosas podrían pasar desapercibidas. Es fundamental tener un inventario actualizado de todas las instancias informáticas conectadas. Se deben hacer escaneos de red y comprobaciones físicas para localizarlos y catalogarlos, e instalar software de protección de endpoints en cualquier máquina que carezca de protección.
- **Configuración correcta.** Los sistemas y dispositivos subprotegidos también son vulnerables. Es importante que las soluciones de seguridad estén configuradas correctamente y actualizar las políticas de seguridad con regularidad. Las nuevas funciones de seguridad no siempre se habilitan automáticamente.

- **Auditar Active Directory (AD).** Es importante realizar auditorías periódicas en todas las cuentas en AD, asegurándose de que ninguna tenga más acceso del necesario para su propósito. Además, deshabilita las cuentas para los empleados que se van tan pronto como dejen la empresa.
- **Parcha todo.** Windows, y otros sistemas operativos, siempre deben estar actualizados. Esto también significa verificar dos veces que los parches se hayan instalado correctamente y estén en su lugar para sistemas críticos como máquinas conectadas a Internet o controladores de dominio. En el incidente investigado por Sophos, la empresa había detenido el soporte para el software Adobe ColdFusion 9 del servidor, así como el sistema operativo Windows 2008, lo que significa que ya no estaban recibiendo actualizaciones de software.

Sobre Sophos

Sophos es la empresa líder mundial en ciberseguridad de última generación, que protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología para la detección de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de gestión integral basada en la nube llamada Sophos Central, el eje de un ecosistema de ciberseguridad adaptable que cuenta con un 'lago de datos' centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/