CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Ciberataques a la Cadena de Suministros

Fecha: **08/09/2022**

Problemática: **Grupo APT Lazarus ejecuta ciberataques contra proveedores de energía de EE.UU, Japón y Canadá**

Correlativo: **AA-0023**

Institución / Sector: **Instituciones Públicas y Privadas**

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

CONTEXTO

De acuerdo al informe emitido por Cisco Talos Intelligence Group el grupo norcoreano APT Lazarus (APT38) está explotando los servidores VMWare Horizon para acceder a las redes corporativas de proveedores de energía en los Estados Unidos, Canadá y Japón. La campaña está destinada a infiltrarse en organizaciones de todo el mundo para establecer acceso a largo plazo y, posteriormente, filtrar datos de interés para el estado-nación del adversario. Talos ha descubierto el uso de dos familias conocidas de malware en estas intrusiones: siendo estas; "VSingle" y "YamaBot" y un troyano de acceso remoto (RAT) previamente desconocido llamado MagicRAT respectivamente.

SITUACIÓN

La información recabada por el Centro Estratégico de Monitoreo-CEM, Lazarus se dirigió a las organizaciones de energía entre febrero y julio de 2022, aprovechando los exploits públicos de VMWare Horizon para obtener el acceso inicial de las maquinas afectadas. A partir de ahí, utilizaron diversas familias de malware personalizadas como «VSingle» y «YamaBot» y un troyano de acceso remoto (RAT) previamente desconocido llamado MagicRAT, que se utiliza para buscar y robar datos de dispositivos infectados. La investigación de Cisco Talos presenta varias estrategias de ataque que ilustran las últimas técnicas, tácticas y procedimientos (TTP) de Lazarus y destacan la versatilidad del sofisticado grupo de ciberdelincuentes.

RECOMENDACIONES

Verificar la versión del firmware instalado en el dispositivo, si la misma es anterior a la 210628. Instale las actualizaciones de inmediato.

Información de versiones afectadas y versiones resueltas: https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/security-notification-command-injection-vulnerability-in-some-hikvision-products/

ÁREA PARA DEFINICIONES

DICCIONARIO DE DATOS

1. **Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.**
2. **Código Arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.**
3. **Troyano: Malware diseñado para tener múltiples utilidades, la más común es crear una puerta trasera en el equipo infectado, para poder descargar actualizaciones y nuevas funcionalidades.**
4. **Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.**
5. **RAT: Troyano de acceso remoto**
6. **Internet de las cosas (IoT): Abreviación del término en inglés Internet of Things; en español, Internet de las cosas, es un concepto que se refiere a la interconexión digital de objetos cotidianos, como relojes, cámaras de grabación, electrodomésticos, etc. mediante Internet.**

REFERENCIAS

1. **Alerta https://www.cronup.com/el-grupo-apt-lazarus-estaria-llevando-ataques-contra-los-proveedores-de-energia-de-ee-uu-japon-y-canada/**
2. **Informe Talos Network https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html**

ÁREA PARA DEFINICIONES