Un actor del estado-nación, conocido por sus campañas de espionaje cibernético desde 2012, ahora está utilizando técnicas de minería de criptomonedas para permanecer bajo el radar y establecer la persistencia en los sistemas de las víctimas.

El grupo de amenazas identificado como Bismuth por el Equipo de Inteligencia de Amenazas de Microsoft 365 Defender, desplegó mineros de monedas Monero en ataques dirigidos tanto al sector privado como a instituciones gubernamentales en Francia y Vietnam, entre julio y agosto de este año, según la compañía de seguridad.

> *«Los mineros de criptomonedas también permitieron que Bismuth ocultara sus actividades más nefastas detrás de amenazas que pueden percibirse como menos alarmantes porque son malware de mercancía»,* dijeron los investigadores ayer.

Las principales víctimas del ataque se remontan a empresas estatales en Vietnam y entidades vinculadas a una agencia gubernamental vietnamita.

Microsoft comparó Bismuth con OceanLotus (o APT32), vinculándolo con ataques de software espía utilizando conjuntos de herramientas personalizados y de código abierto para apuntar a grandes corporaciones multinacionales, gobiernos, servicios financieros, instituciones educativas y organizaciones de derechos humanos y civiles.

El desarrollo se produce luego de descubrir que OceanLotus aprovechaba una nueva puerta trasera de macOS que permite a los atacantes espiar y robar información confidencial y documentos comerciales confidenciales de las máquinas infectadas.

Aunque las tácticas de espionaje y exfiltración del grupo han permanecido esencialmente iguales, la inclusión de mineros de monedas en su arsenal apunta a una nueva forma de monetizar las redes comprometidas, sin mencionar un medio hábil de mezclarse y evadir la detección durante el mayor tiempo posible.

La idea es ganar tiempo para moverse lateralmente e infectar objetivos de alto valor como

servidores para una mayor propagación.

Para lograr esto, se crearon correos electrónicos de phishing personalizados escritos en vietnamita para destinatarios específicos en una organización objetivo, y en algunos casos, el actor de la amenaza incluso estableció correspondencia con los objetivos en un intento por aumentar las posibilidades de abrir el documento malicioso incrustado en los correos electrónicos y lograr establecer la cadena de infección.

Una técnica separada implicaba el uso de carga lateral de DLL, en la que una biblioteca legítima se reemplaza con una variante maliciosa, utilizando versiones obsoletas de software legítimo como Microsoft Defender Antivirus, Sysinternals DebugView y Microsoft Word 2007 para cargar archivos DLL falsos y establecer un canal de comando y control persistente (C2) al dispositivo comprometido y la red.

El canal recién establecido se usó después para eliminar una serie de cargas útiles de la siguiente etapa, incluidas las herramientas para escaneo de red, robo de credenciales, extracción de Monero y realización de reconocimiento, cuyos resultados se transmitieron al servidor en forma de *«archivo.csv».*

> *«Los ataques de Bismuth ponen un fuerte énfasis en esconderse a plena vista al mezclarse con la actividad normal de la red o las amenazas comunes que los atacantes anticipan recibirán una atención de baja prioridad»,* dijo Microsoft.

> *«La combinación de ingeniería social y el uso de aplicaciones legítimas para descargar archivos DLL maliciosos implica múltiples capas de protección centradas en detener las amenazas en la etapa más temprana posible y mitigar la progresión de los ataques si logran pasar»,* agregó la compañía.