Los actores maliciosos detrás del grupo de ransomware BlackByte han sido observados posiblemente explotando una vulnerabilidad de seguridad recientemente corregida que afecta a los hipervisores VMware ESXi, al mismo tiempo que utilizan varios controladores vulnerables para desactivar las protecciones de seguridad.

> *«El grupo de ransomware BlackByte continúa utilizando tácticas, técnicas y procedimientos (TTP) que han sido fundamentales en su metodología desde su inicio, iterando continuamente en el uso de controladores vulnerables para evadir las protecciones de seguridad y desplegando un encriptador de ransomware autorreplicante,»* dijo Cisco Talos en un informe técnico.

La explotación de CVE-2024-37085, una vulnerabilidad de omisión de autenticación en VMware ESXi que también ha sido utilizada por otros grupos de ransomware, indica que el grupo de ciberdelincuencia está cambiando sus métodos tradicionales.

BlackByte apareció por primera vez en la segunda mitad de 2021 y se cree que es una de las variantes de ransomware que surgieron en los meses previos al desmantelamiento del infame grupo de ransomware Conti.

Este grupo de ransomware como servicio (RaaS) tiene un historial de explotación de las vulnerabilidades ProxyShell en Microsoft Exchange Server para obtener acceso inicial, evitando los sistemas que utilizan ruso y varios idiomas de Europa del Este.

Al igual que otros grupos RaaS, también utiliza la doble extorsión como parte de sus ataques, empleando un enfoque de *«nombre y vergüenza»* a través de un sitio de filtración de datos en la dark web para presionar a las víctimas a pagar. Hasta la fecha, se han detectado múltiples variantes del ransomware escritas en C, .NET y Go.

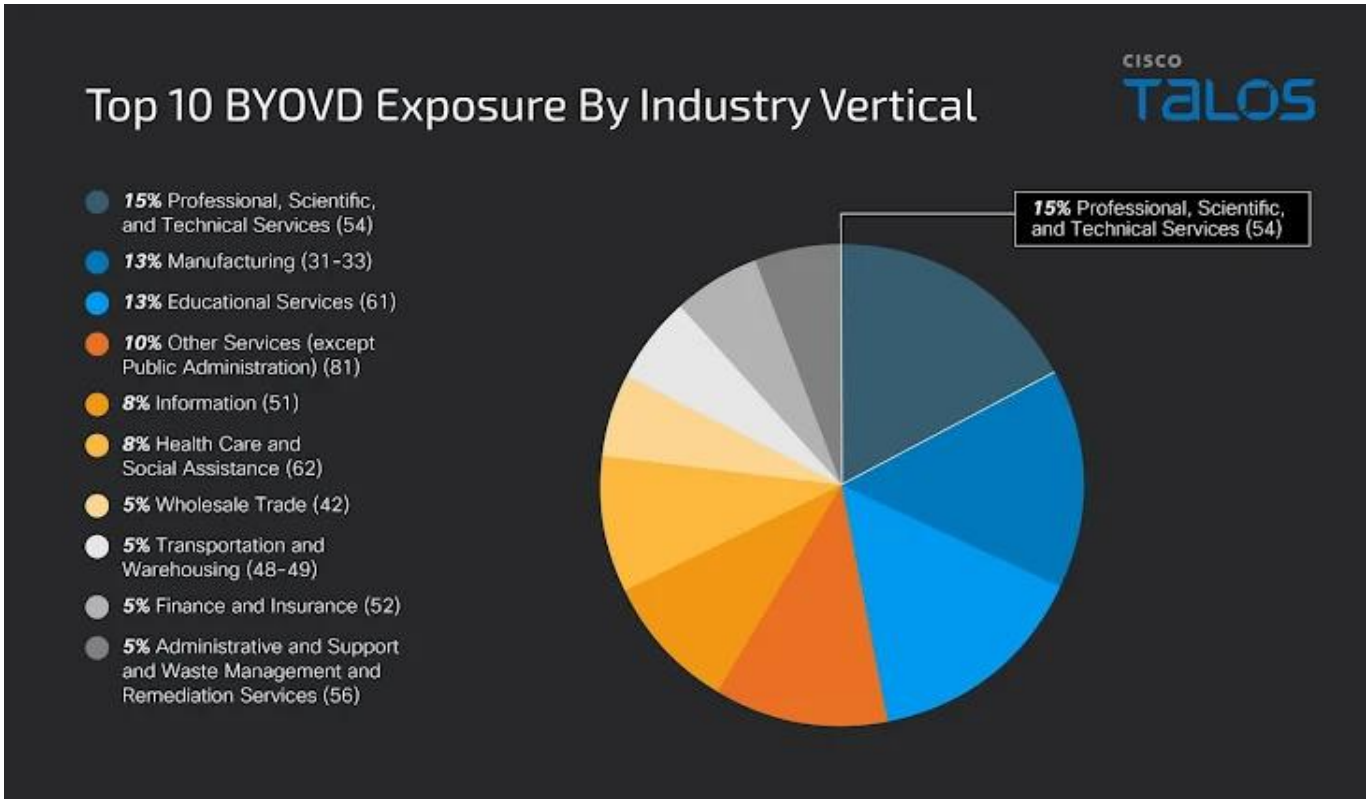
Aunque Trustwave lanzó un descifrador para BlackByte en octubre de 2021, el grupo ha seguido perfeccionando su modus operandi, llegando incluso a utilizar una herramienta personalizada llamada ExByte para exfiltrar datos antes de comenzar el cifrado.

Un aviso emitido por el gobierno de EE. UU. a principios de 2022 atribuyó a este grupo RaaS ataques motivados por ganancias financieras que se dirigían a sectores de infraestructura crítica, incluidos los sectores financiero, alimentario y agrícola, y las instalaciones gubernamentales.

Uno de los aspectos clave de sus ataques es el uso de controladores vulnerables para finalizar procesos de seguridad y evadir controles, una técnica conocida como *«trae tu propio controlador vulnerable»* (BYOVD, por sus siglas en inglés).

Cisco Talos, que investigó un reciente ataque de ransomware de BlackByte, afirmó que la intrusión probablemente se facilitó utilizando credenciales válidas para acceder a la VPN de la organización afectada. Se cree que el acceso inicial se logró a través de un ataque de fuerza bruta.

> *«Dado el historial de BlackByte en la explotación de vulnerabilidades públicas para obtener acceso inicial, el uso de la VPN para el acceso remoto puede representar un ligero cambio en su técnica o simplemente una cuestión de oportunidad. El uso de la VPN de la víctima para el acceso remoto también brinda otras ventajas al adversario, como una menor visibilidad desde el EDR de la organización»*, dijeron los investigadores de seguridad James Nutland, Craig Jackson, Terryn Valikodath y Brennan Evans.



Posteriormente, el actor malicioso logró escalar sus privilegios, utilizando los permisos para acceder al servidor VMware vCenter de la organización y crear nuevas cuentas en un grupo de Active Directory llamado ESX Admins. Talos explicó que esto se logró explotando la vulnerabilidad CVE-2024-37085, que permite a un atacante obtener privilegios de administrador en el hipervisor creando un grupo con ese nombre y agregando cualquier usuario a él.

Este privilegio podría ser explotado para controlar máquinas virtuales (VM), modificar la configuración del servidor host y acceder sin autorización a registros del sistema, herramientas de diagnóstico y monitoreo de rendimiento.

Talos destacó que la explotación de esta vulnerabilidad ocurrió pocos días después de su divulgación pública, lo que subraya la rapidez con la que los actores maliciosos refinan sus tácticas para incorporar nuevas vulnerabilidades divulgadas a su arsenal y avanzar en sus

ataques.

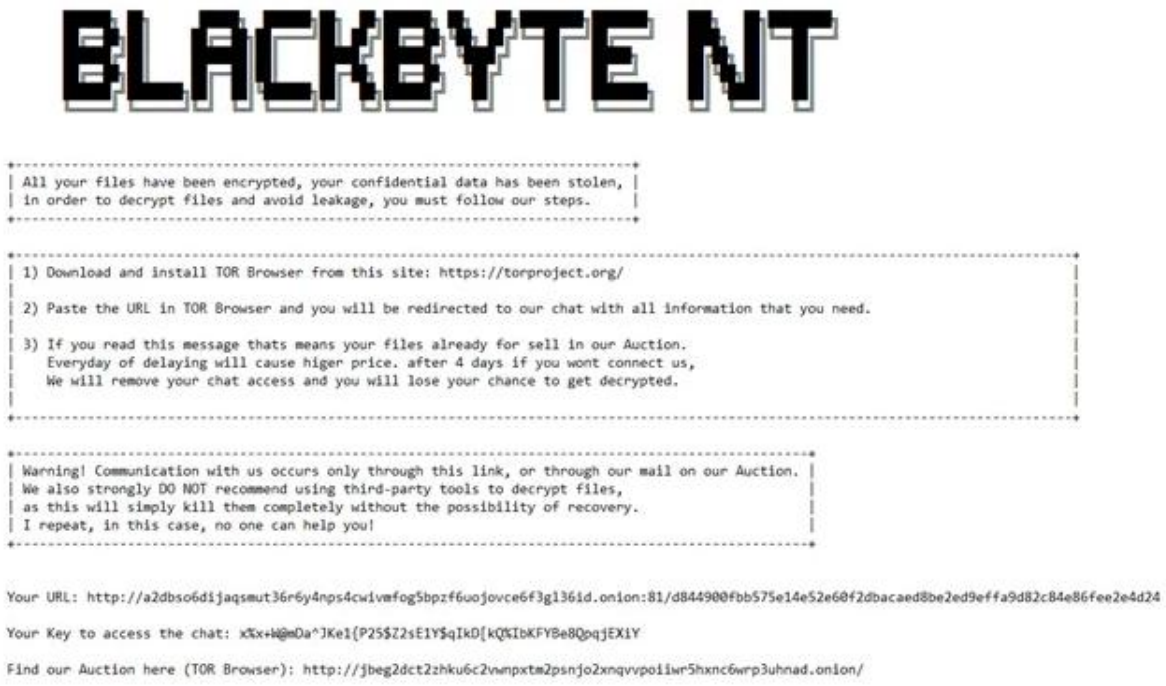
Además, los recientes ataques de BlackByte terminan con los archivos encriptados siendo renombrados con la extensión «blackbytent_h», y el encriptador también despliega cuatro controladores vulnerables como parte del ataque BYOVD. Los cuatro controladores siguen una convención de nomenclatura similar: Ocho caracteres alfanuméricos aleatorios seguidos de un guion bajo y un número incremental:

- AM35W2PH (RtCore64.sys)
- AM35W2PH_1 (DBUtil_2_3.sys)
- AM35W2PH_2 (zamguard64.sys, también conocido como Terminator)
- AM35W2PH_3 (gdrv.sys)

Los sectores de servicios profesionales, científicos y técnicos son los más expuestos a los controladores vulnerables observados, representando el 15% del total, seguidos por el sector manufacturero (13%) y los servicios educativos (13%). Talos también evaluó que es probable que el grupo de amenazas sea más activo de lo que parece, y que solo entre el 20% y el 30% de las víctimas se hacen públicas, aunque la razón exacta de esta disparidad aún no está clara.

> *«El avance de BlackByte en los lenguajes de programación, pasando de C# a Go y luego a C/C++ en la última versión de su cifrador – BlackByteNT – muestra un esfuerzo consciente por aumentar la capacidad del malware para evadir detección y análisis,»* indicaron los investigadores.
>
> *«Lenguajes complejos como C/C++ permiten la implementación de técnicas avanzadas para evitar el análisis y la depuración, que han sido observadas en las herramientas de BlackByte durante un análisis exhaustivo realizado por otros expertos en seguridad.»*

Esta información se da a conocer mientras Group-IB revela las tácticas asociadas con otras dos cepas de ransomware denominadas Brain Cipher y RansomHub, destacando las posibles conexiones de Brain Cipher con grupos de ransomware como EstateRansomware, SenSayQ y RebornRansomware.



> *«Se han encontrado similitudes en el estilo y contenido de la nota de rescate de Brain Cipher con las del ransomware SenSayQ. Los sitios web en TOR del grupo de ransomware Brain Cipher y el grupo de ransomware SenSayQ emplean tecnologías y scripts semejantes.»*, señaló la empresa de ciberseguridad de Singapur.

En contraste, se ha observado que RansomHub ha comenzado a reclutar antiguos miembros de Scattered Spider, una información que se hizo pública el mes pasado. La mayoría de los ataques han afectado a los sectores de salud, finanzas y gobierno en Estados Unidos, Brasil, Italia, España y el Reino Unido.

«Para obtener acceso inicial, los afiliados suelen adquirir cuentas de dominio comprometidas y válidas a través de Intermediarios de Acceso Inicial (IABs) y servicios remotos externos,» indicó Group-IB, añadiendo que *«las cuentas se han obtenido mediante LummaC2 stealer.»*

> *«Las tácticas de RansomHub incluyen el uso de cuentas de dominio comprometidas y VPN públicas para el acceso inicial, seguido de la extracción de datos y procesos extensivos de cifrado. Su reciente introducción de un programa de afiliados RaaS y el uso de pagos de rescate de alta demanda demuestran su enfoque en evolución y agresivo.»*