Los perpetradores responsables de la operación de ransomware LockBit han vuelto a surgir en la dark web utilizando una nueva infraestructura, días después de que un ejercicio de aplicación de la ley a nivel internacional tomara el control de sus servidores.

En consecuencia, el grupo conocido ha trasladado su portal de filtración de datos a una dirección .onion diferente en la red TOR, mostrando 12 nuevas víctimas hasta el momento de esta redacción.

El administrador detrás de LockBit, en un extenso mensaje de seguimiento, admitió que algunos de sus sitios web fueron confiscados, probablemente explotando una vulnerabilidad crítica en PHP identificada como CVE-2023-3824, reconociendo que no actualizaron PHP debido a *«negligencia personal e irresponsabilidad».*

> *«Comprendo que tal vez no haya sido esta CVE, sino algo similar como un 0-day para PHP, pero no puedo estar al 100% seguro, ya que la versión instalada en mis servidores ya tenía una vulnerabilidad conocida, por lo que es muy probable que así fue como accedieron a los servidores del panel de administración y chat de las víctimas, así como al servidor del blog»,* señalaron.

También afirmaron que el Buró Federal de Investigaciones de EE. UU. (FBI) «hackeó» su infraestructura debido a un ataque de ransomware en el condado de Fulton en enero y que *«los documentos robados contienen mucha información interesante y casos judiciales de Donald Trump que podrían afectar a las próximas elecciones en EE. UU.»*

Además de instar a atacar con mayor frecuencia al sector «.gov», declararon que el servidor del cual las autoridades obtuvieron más de 1,000 claves de descifrado contenía casi 20,000 descifradores, la mayoría de los cuales estaban protegidos y representaban alrededor de la mitad del número total de descifradores generados desde 2019.

El grupo también intentó desacreditar a las agencias de aplicación de la ley, alegando que el verdadero «Bassterlord» no ha sido identificado y que las acciones del FBI están *«dirigidas a*

destruir la reputación de mi programa de afiliados».

> *«¿Por qué tardaron 4 días en recuperarse? Porque tuve que editar el código fuente para la última versión de PHP, ya que había incompatibilidad»,* expresaron.
>
> > *«No seré perezoso y aseguraré que cada versión de LockBit tenga la máxima protección; ahora no habrá descifrado de prueba automático, todos los descifrados de prueba y la emisión de descifradores se realizarán solo en modo manual. De esta manera, en el posible próximo ataque, el FBI no podrá obtener ni un solo descifrador de forma gratuita.»*

Arresto de Tres Integrantes de SugarLocker en Rusia

Esto coincide con la noticia de que las autoridades rusas han detenido a tres individuos, incluido Aleksandr Nenadkevichite Ermakov (también conocido como blade_runner, GustaveDore o JimJones), en relación con el grupo de ransomware SugarLocker.

«Los atacantes operaban bajo la apariencia de una firma de TI legítima llamada Shtazi-IT, que ofrece servicios para el desarrollo de páginas de destino, aplicaciones móviles, scripts, parsers y tiendas en línea», informó la firma de ciberseguridad rusa F.A.C.C.T. *«La empresa publicaba abiertamente anuncios para contratar nuevos empleados».*

A los operadores también se les acusa de desarrollar malware personalizado, crear sitios de phishing para tiendas en línea y dirigir el tráfico de usuarios hacia esquemas fraudulentos populares en Rusia y en las naciones de la Comunidad de Estados Independientes (CEI).

SugarLocker surgió por primera vez a principios de 2021 y más tarde comenzó a ofrecerse bajo el modelo de ransomware como servicio (RaaS), alquilando su malware a otros socios bajo un programa de afiliados para violar objetivos e implementar la carga útil del ransomware.

Cerca del 75% de los ingresos obtenidos por el rescate se destinan a los afiliados, una cifra que aumenta al 90% si el pago supera los $5 millones. La conexión de la banda de ciberdelincuentes con Shtazi-IT fue previamente revelada por Intel 471 el mes pasado.

El arresto de Ermakov es destacado, ya que se produce después de que Australia, el Reino Unido y los Estados Unidos impusieran sanciones financieras en su contra por su presunto papel en el ataque de ransomware de 2022 contra el proveedor de seguros de salud Medibank.

El ataque de ransomware, que ocurrió a finales de octubre de 2022 y se atribuye al ahora desaparecido grupo de ransomware REvil, resultó en el acceso no autorizado a aproximadamente 9.7 millones de sus clientes actuales y anteriores.

La información robada incluyó nombres, fechas de nacimiento, números de Medicare e información médica delicada, que abarcaba registros sobre salud mental, salud sexual y consumo de drogas. Algunos de estos registros también fueron publicados en la dark web.

Esto también sigue a un informe de la agencia de noticias TASS, que reveló que un ciudadano ruso de 49 años enfrentará juicio por cargos relacionados con un ciberataque a los sistemas de control tecnológico que dejó sin energía a 38 asentamientos en la región de Vologda.

Cronología de Eventos de LockBit

20 DE FEBRERO DE 2024

LockBit Desmantelado – Autoridades Confiscan Dominios en la Darknet
Una operación internacional de aplicación de la ley, que involucra a 11 países y Europol, logró confiscar dominios en la darknet vinculados al grupo de ransomware LockBit, que ha extorsionado más de $91 millones desde 2019. La operación, llamada Cronos, utilizó una vulnerabilidad de seguridad en PHP para interrumpir los sitios web de LockBit, marcando un golpe significativo a las actividades del grupo.

21 DE FEBRERO DE 2024

Arresto de Hackers de LockBit – Lanzamiento de Herramienta de Descifrado

La NCA del Reino Unido cierra LockBit ransomware, arresta a 2 en Polonia/Ucrania, congela más de 200 cuentas de criptomonedas, acusa a 2 rusos en EE. UU. Incauta el código de LockBit, inteligencia, desmantela 34 servidores, recupera 1,000 claves de descifrado. LockBit afectó a 2.5k víctimas a nivel mundial, ganando $120 millones. Herramienta de descifrado disponible para las víctimas.

22 DE FEBRERO DE 2024

Recompensa de $15 millones por los Líderes de LockBit Ransomware

El Departamento de Estado de EE. UU. ofrece una recompensa de $15 millones por información sobre los líderes del ransomware LockBit, involucrados en más de 2,000 ataques globales desde 2020, causando $144 millones en daños. Las fuerzas del orden interrumpieron LockBit, arrestaron a afiliados y confiscaron activos. LockBit, conocido por el ransomware como servicio, una extensa red de afiliados y tácticas innovadoras como un programa de recompensas por errores, sigue siendo una amenaza cibernética significativa a pesar de los contratiempos.

25 DE FEBRERO DE 2024

El Cerebro detrás de LockBit Ransomware ‘Colabora’ con la Policía

El individuo o individuos detrás del servicio de ransomware LockBit, conocido como LockBitSupp, al parecer ha colaborado con las fuerzas del orden tras un importante golpe internacional contra la operación de ransomware como servicio llamada Operación Cronos.

26 DE FEBRERO DE 2024

LockBit Está de Regreso – Llamados a Atacar al Gobierno de EE. UU.

El grupo de ransomware LockBit ha vuelto a aparecer en la dark web con una nueva infraestructura poco después de que las fuerzas del orden tomaran el control de sus servidores. El grupo ha enumerado 12 nuevas víctimas en su portal de filtración de datos y ha discutido la incautación de sus sitios web, atribuyéndolo a una posible explotación de una vulnerabilidad en PHP.