Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

8BASE RANSOMWARE AUMENTA SU ACTIVIDAD

25/Agosto/2023

CONTENIDO

INTRODUCCIÓN

Una investigación conducida por el equipo de VMware Carbon Black ha observado un reciente aumento en la actividad del grupo de ransomware denominado 8Base, la actividad del grupo se vería en aumento en junio y se ha podido observar la incursión del grupo en ataques de doble extorción, teniendo como objetivo, organizaciones a nivel mundial.

8BASE RANSOMWARE AUMENTA SU ACTIVIDAD

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_08_25_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	25/08/2023
Es día cero (0 day):	Si

RESUMEN

Una investigación conducida por el equipo de VMware Carbon Black ha observado un reciente aumento en la actividad del grupo de ransomware denominado 8Base, la actividad del grupo se vería en aumento en junio y se ha podido observar la incursión del grupo en ataques de doble extorción, teniendo como objetivo, organizaciones a nivel mundial.

8Base es un grupo de actores maliciosos que ha estado activo desde 2022 y cuya actividad se ha visto limitada a unos pocos ataques sobresalientes. Sin embargo, recientemente se ha podido observar un aumento en las actividades del grupo, siendo el pico más alto, el mes de junio.

Los objetivos principales del grupo de ransomware incluyen, pero no se limitan, a: servicios a empresas, organizaciones financieras, industria manufacturera e industria de tecnología

Recientemente se ha podido observar, desde el sitio de filtraciones del grupo de ransomware una gran actividad contra estas industrias, listándose hasta ahora 35 víctimas en el sitio alojado en la dark web, la actividad del grupo se ha visto reflejado en la añadidura de hasta 6 víctimas al mismo tiempo, en dicha lista. Como se puede observar a continuación.

Según se puede observar en el sitio de 8Base, estos se ven a sí mismos como un grupo “honesto y simple” de pentesters, quienes ofrecen a las compañías las más leales condiciones para el retorno de la información cifrada, concluyendo con que, las compañías que encuentran en su lista son solamente aquellas que han descuidado la privacidad e importancia de la información de sus clientes y empleados.

ASOCIADOS Y SIMILITUDES

El grupo de ransomware 8Base, utiliza técnicas de encriptación y de denuncia para obligar a sus víctimas a pagar los rescates. Este tipo de tácticas, sumado a varias similitudes que se abordaran a continuación, permite suponer que 8Base podría ser, o bien, un renombre de algún grupo de ransomware ya establecido, potencialmente Ransomhouse, o la colaboración de miembros de grupos anteriores.

Entre las primeras observaciones referentes a similitudes entre distintos grupos de ransomware, se tiene la nota de ransomware provista por los grupos con una coincidencia del 99% en la lingüística, estructura y contenido de estos, donde inclusive las páginas de FAQ parecieran ser un simple copy-paste, como se puede observar a continuación (8Base derecha y Ransomhouse izquierda).

Sin embargo, la evidencia expuesta resulta no ser suficiente a la hora de confirmar si 8Base es, de hecho, un descendiente de Ransomhouse o bien, solo un grupo de ransomware copiando las plantillas utilizadas por otro grupo de ransomware ya establecido, lo que resulta ser normal en este tipo de entornos de grupos maliciosos.

Otra de las similitudes compartidas con 8Base y otras organizaciones, es la utilización de la extensión “.8base” de Phobos, en archivos cifrados. 8Base hace uso de una versión personalizada de ransomware de Phobos v2.0.1 la cual se carga mediante SmokeLoader. Ya que Phobos es una operación de Ransomware-as-a-Service (RaaS), cualquier actor malicioso es capas de utilizar partes especialmente personalizadas a sus preferencias, como es el caso de 8Base.

Aunque 8Base añadió su propia personalización de marca añadiendo “.8base” a sus archivos cifrados, el formato de toda la parte añadida era el mismo que el de Phobos, que incluía una sección de identificación, una dirección de correo electrónico y, a continuación, la extensión del archivo.

Otro hallazgo notable en la investigación es que 8Base utiliza el dominio “admlogs25[.]xyz” para el alojamiento de la carga útil, que está asociado con SystemBC, un malware proxy utilizado por varios grupos de ransomware para la ofuscación C2.

Según las similitudes antes descritas, sería correcto suponer que 8Base es una rama de RansomeHouse o Phobos, sin embargo, al toparse con algunas otras diferencias, este hecho es algo que no se puede confirmar en un 100%. Lo que sí es cierto es la gran actividad reciente de 8Base, como lo ha demostrado en su sitio de filtraciones. 8Base apenas está empezando a recibir la atención de los analistas, por lo que muchos aspectos de su naturaleza técnica siguen siendo desconocidos o poco claros.

Se registra actividad del grupo de Ransomware 8Base en la zona donde el grupo asegura haber cargado en sus servidores

Se cargaron en los servidores:

- Recibos de facturas
- Documentos contables
- Datos personales
- Certificados
- Contratos de trabajo
- Otros

IOC

Tipo	Indicador
Hash	518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c
Hash	5BA74A5693F4810A8EB9B9EEB1D69D943CF5BBC46F319A32802C23C7654194B0
Hash	e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0
Hash	C6BD5B8E14551EB899BBE4DECB6942581D28B2A42B159146BBC28316E6E14A64
Hash	518544E56E8CCEE401FFA1B0A01A10CE23E49EC21EC441C6C7C3951B01C1B19C
Hash	AFDDEC37CDC1D196A1136E2252E925C0DCFE587963069D78775E0F174AE9CFE3
Hash	3D2B088A397E9C7E9AD130E178F885FEEBD9688B
Hash	5d0f447f4ccc89d7d79c0565372195240cdfa25f
Hash	9769c181ecef69544bbb2f974b8c0e10
Hash	20110FF550A2290C5992A5BB6BB44056
Hash	9769C181ECEF69544BBB2F974B8C0E10
Hash	5D0F447F4CCC89D7D79C0565372195240CDFA25F
Hash	E142F4E8EB3FB4323FB377138F53DB66E3E6EC9E82930F4B23DD91A5F7BD45D0
URL	hxxp[:]//dexblog45[.]xyz/statweb255/
URL	hxxp[:]//sentrex219[.]xyz/777/mtx5sfN.exe
URL	hxxp[:]//sentrex219[.]xyz/777/skx2auB.exe
IP	45.131.66[.]120
IP	45.89.125[.]136
Data POST a URL	wlaexfpxrs[.]org
Data POST a URL	serverlogs37[.]xyz
Petición GET de datos a URL	admhexlogs25[.]xyz
Petición GET de datos a URL	admlogs25[.]xyz
Petición GET de datos a URL	admlog2[.]xyz
Petición GET de datos a URL	dnm777[.]xyz
Petición GET de datos a URL	dexblog[.]xyz
Petición GET de datos a URL	blogstat355[.]xyz
Petición GET de datos a URL	blogstatserv25[.]xyz
Nombre del archivo	9f1a.exe
Nombre del archivo	d6ff.exe
Nombre del archivo	3c1e.exe
Nombre del archivo	8A26.exe
Nombre del archivo	8B7F.exe

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos
- confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión.
- Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red

NOTICIA COMPLETA

https://devel.group/blog/8base-ransomware-aumenta-su-actividad-2/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente