Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NACIONAL DE ADUANAS DE CHILE BAJO ATAQUE

17/10/2023

CONTENIDO

INTRODUCCIÓN

El Servicio Nacional de Aduanas informó que durante esta jornada se registró un ciberataque a sus equipos informáticos, pero que, pese a la emergencia, el servicio no dejará de atender al público.

NACIONAL DE ADUANAS DE CHILE BAJO ATAQUE

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

ID de alerta:	DSOC-CERT_2023_10_17_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	17/10/2023
Es día cero (0 day):	No

RESUMEN

El Servicio Nacional de Aduanas informó que durante esta jornada se registró un ciberataque a sus equipos informáticos, pero que, pese a la emergencia, el servicio no dejará de atender al público.

La información fue confirmada luego de que se registraran denuncias por parte de usuarios importadores y exportadores en Chile, que vieron dificultado la interacción con el servicio aduanero.

“Hoy detectamos un incidente de seguridad en nuestros equipos informáticos y, de acuerdo, al protocolo establecido por CSIRT, el Servicio Nacional de Aduanas adoptó medidas preventivas, justamente, para no exponer los equipos computacionales a eventuales ataques”, aseguraron a Radio Bío Bío desde Aduanas.

El grupo al que se le acredita este ataque es Black Basta.

Black Basta (también conocido como BlackBasta) es un operador de ransomware y una empresa criminal de ransomware como servicio (RaaS) que surgió por primera vez a principios de 2022 e inmediatamente se convirtió en uno de los actores de amenazas RaaS más activos del mundo, acumulando 19 víctimas empresariales destacadas y más de 100 víctimas confirmadas en sus primeros meses de funcionamiento. Black Basta se dirige a organizaciones en los EE. UU., Japón, Canadá, el Reino Unido, Australia y Nueva

Zelanda en ataques altamente dirigidos en lugar de emplear un enfoque de rociar y rezar. Las tácticas de rescate del grupo utilizan una doble táctica de extorsión, encriptando los datos críticos y los servidores vitales de sus víctimas y amenazando con publicar datos confidenciales en el sitio público de filtraciones del grupo.

Se cree que la membresía principal de Black Basta se generó a partir del extinto grupo de actores de amenazas Conti debido a las similitudes en su enfoque del desarrollo de malware, los sitios de fugas y las comunicaciones para la negociación, el pago y la recuperación de datos. Black Basta también se ha relacionado con el actor de amenazas FIN7 (también conocido como Carbanak) a través de similitudes en sus módulos personalizados de evasión de detección y respuesta de endpoints (EDR) y el uso superpuesto de direcciones IP para operaciones de comando y control (C2).

En las primeras campañas, los ataques de Black Basta comenzaron con campañas de spear-phishing muy específicas para obtener acceso inicial. En abril de 2022, el grupo comenzó a anunciar su intención de comprar acceso a la red corporativa y compartir las ganancias con corredores de acceso inicial (IAB) afiliados. Después de obtener acceso inicial, Black Basta despliega una variedad de tácticas de segunda etapa para adquirir credenciales de dominio de Windows y penetrar lateralmente en la red de un objetivo, robar datos confidenciales e implementar ransomware.

Para lograr los objetivos de la segunda etapa, Black Basta usa un conjunto diverso de tácticas, incluido el uso del ladrón **QakBot** (también conocido como QBot o Pinkslipbot), MimiKatz y la explotación de la API nativa de Instrumental de administración de Windows (WMI) para la recolección de credenciales, luego use los comandos de Powershell y PsExec para obtener acceso a los puntos de conexión de red adyacentes mediante las credenciales extraídas. Black Basta también puede explotar las vulnerabilidades ZeroLogon, NoPac e PrintNightmare para la escalada de privilegios locales y de Windows Active Domain. Para el control remoto C2 de los sistemas infectados, Black Basta instala Cobalt Strike Beacons, utiliza SystemBC para el proxy C2 y la herramienta Rclone para la exfiltración de datos.

La etapa de cifrado de un ataque Black Basta comienza deshabilitando los productos antivirus, ejecutando una carga útil de cifrado de forma remota a través de PowerShell y eliminando instantáneas del sistema mediante el programa vssadmin.exe. A partir de ahí, Black Basta ejecuta una carga útil de ransomware personalizada que ha pasado por al menos un cambio de versión significativo desde que se observó por primera vez. La primera versión del módulo de cifrado de Black Basta era similar al ransomware Conti. Por el contrario, la segunda versión mejorada utiliza una fuerte ofuscación y nombres de archivo aleatorios para evadir los productos EDR y ha reemplazado su uso de los algoritmos de la Biblioteca Aritmética de Precisión Múltiple (GMP) de GNU con la biblioteca de cifrado Crypto++. El módulo de cifrado Black Basta 2.0 utiliza el algoritmo XChaCha20 para el cifrado simétrico, un par de claves de criptografía de curva elíptica (ECC) único para cifrar y anteponer la clave simétrica junto con la clave pública ECC para descifrarla y con un nonce a los datos del archivo cifrado.

Black Basta también ha utilizado otras técnicas distintas en sus ataques, como la desactivación de los servicios DNS del sistema comprometido para complicar el proceso de recuperación impidiendo que acceda a Internet y la implementación de una variante de ransomware que se dirige a las máquinas virtuales (VM) VMware ESXi basadas en Linux.

En vista de esta situación El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior y Seguridad Pública, recomienda encarecidamente a todos los organismos tomar las siguientes medidas preventivas:

- Asegurarse de que las copias de seguridad estén resguardadas y almacenadas en ubicaciones distintas.
- Supervisar los Active Directory, incluyendo la auditoría de cuentas de administración, la reducción de usuarios con privilegios de administración y la comprobación de lo siguiente:
    - Creación de cuentas con privilegios.
    - Elevación de permisos no autorizados.
    - Detección de herramientas sospechosas, como Netcat, PsExec, PowerShell y Rclone.
- Revisar los registros de antivirus o sistemas de protección durante al menos 15 días hacia atrás para identificar y analizar las amenazas bloqueadas.
- Investigar qué aplicaciones se ejecutaron en los servidores y estaciones de trabajo durante el mismo período de tiempo.
- Realizar un escaneo completo de los sistemas, desactivando la opción de solo analizar archivos nuevos.
- Comprobar si se están realizando conexiones a través de torrents y auditar el tráfico de red.
- Mantener un registro actualizado de los sistemas para garantizar una supervisión efectiva.
- Revisar la actividad de eventos de Microsoft Windows (Active Directory) con los siguientes ID relacionados con:
    - Tareas programadas.
    - Servicios.
    - Administración de cuentas.
    - Inicio de sesión y cierre de sesión.
    - Red.

Estas acciones preventivas son esenciales para proteger la infraestructura digital y mantener la seguridad en la administración pública frente a la amenaza del ransomware Black Basta. CSIRT

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.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/blob/main/20231017_01_BlackBasta

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