Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CL0P RANSOMWARE

12 / julio /2023

CONTENIDO

INTRODUCCIÓN

El grupo de actores maliciosos auto-denominado Cl0p ranwomware surgió alrededor del año 2019, considerado por varios investigadores de ciber seguridad como el sucesor de CryptoMix. Cl0p se ha caracterizado por ser uno de los grupos de ransomware que incorpora miembros de grandes habilidades técnicas y la utilización de métodos sofisticados a la hora de irrumpir en alguna organización.

Cl0p se auto denomina como un Ransomware-as-a-Service (RaaS), modelo que le ha servido muy bien hasta ahora, apuntando a objetivos de gran perfil, organizaciones grandes con ingresos promedios de 5 millones de dólares anuales. Cl0p también tiene como objetivo sectores de salud, educación e inclusive sectores de gobierno.

Una de las más amplias campañas, llevadas a cabo por Cl0p ransomware es la que tuviera lugar en mayo de 2023 contra el software de gestión de transferencias de archivos MOVEit de Progress, mediante la explotación de una vulnerabilidad Zero-day (ahora rastreada como CVE-2023-34362) estos comprometieron el software en antes mencionado y así conducir una campaña masiva contra todo tipo de organizaciones, las cuales suman hasta el día de hoy, más de 150.

CL0P RANSOMWARE

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

ID de alerta:	DSOC-CERT_2023_07_12_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/07/2023
Es día cero (0 day):	No

RESUMEN

Cl0p es un grupo de actores maliciosos con motivaciones financieras que operan desde regiones de habla rusa. Se ha establecido como un grupo de Ransomware-as-a-Service, o RaaS cuyo principal objetivo son organizaciones grandes, que presenten ingresos de al menos 5 millones de dólares anuales, o mayor. Este grupo de actores maliciosos se ha visto vinculadas a los grupos identificados como TA505 y FIN11. Se estima que Cl0p es el sucesor directo del grupo de ransomware CryptoMix.

Históricamente, el grupo de actores maliciosos ha tenido a organizaciones de Estados Unidos, Canadá y América Latina como principal objetivo, teniendo presencia también en Asía y la mayor parte de Europa. Entre otras de las características más sobresalientes del grupo Cl0p es la implementación de técnicas avanzadas e innovadoras.

Imagen 1. Distribución geográfica de las víctimas de Cl0p.

El grupo de Cl0p fue observado por primera vez en el 2019, mediante ataques de phishing, ataques de fuerza bruta y la explotación de vulnerabilidades conocidas. El grupo es conocido por implementar la estrategia de doble extorción, en la cual el actor malicioso roba información sensible de los usuarios para ser cifrados posteriormente. De esta manera el actor malicioso cobra un monto por descifrar los datos de los dispositivos comprometidos, y un segundo monto por no exponer los datos filtrados de los sistemas. Si por algún motivo, la víctima se niega a pagar el monto exigido, los atacantes, aparte de no descifrar los documentos, procede a hacerlos públicos mediante su plataforma de filtraciones 'CL0P^_- LEAKS' el cual es accesible mediante enlace Tor.

Entre los objetivos más recurrentes de Cl0p ransomware, se pueden observar organizaciones e industrias de distinta índole, pues el grupo tiene un amplio listado de objetivos, entre los cuales se encuentran

universidades, agencias de gobierno, y compañías privadas, también se pueden observar víctimas en IT & ITES, entidades centradas en BFSI, proveedores de salud, servicios profesionales.

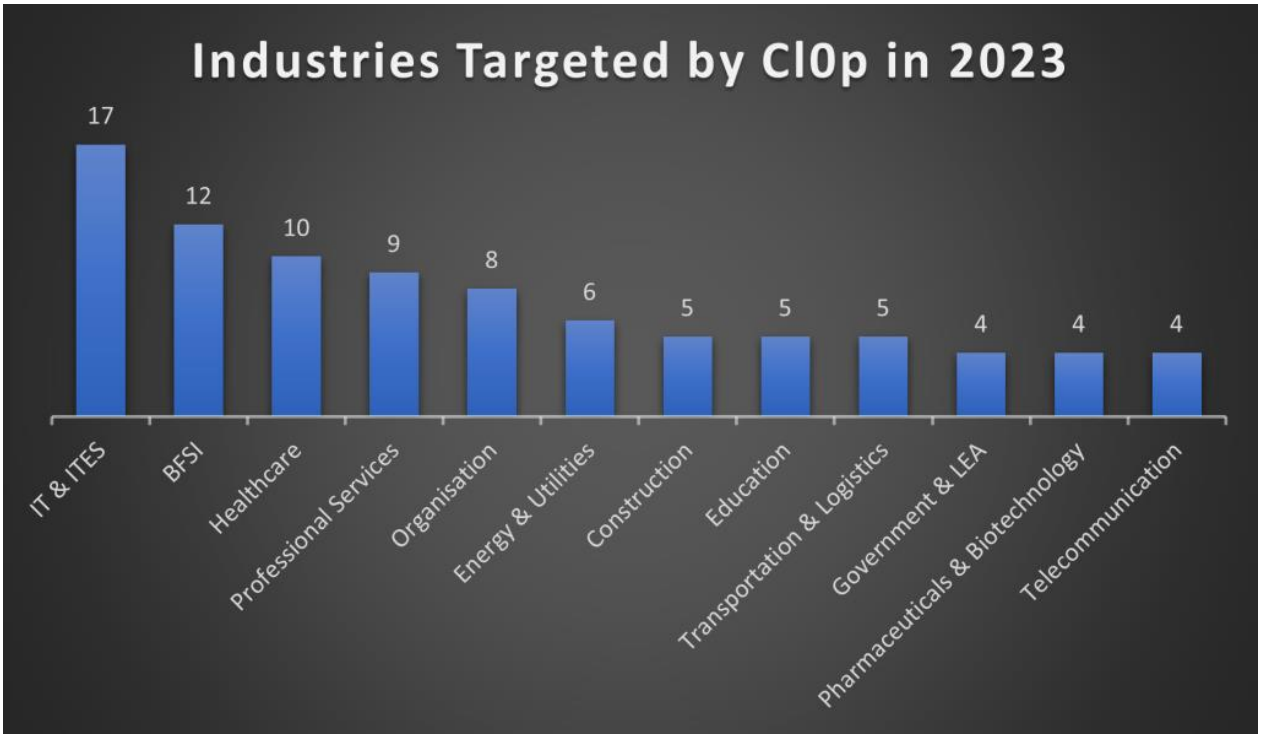

Imagen 2. Sectores de la industria, objetivos de Cl0p.

ACCESO INICIAL

El grupo de actores maliciosos Cl0p ransomware, hace uso de una amplia gama de métodos y tácticas con la finalidad de maximizar el impacto en la organización objetivo, para la brecha inicial de un ataque contra la víctima, Cl0p utiliza tácticas como correos de phishing con archivos maliciosos adjuntos, protocolo de escritorio remoto (RDP) desprotegido y kits de explotación. Tan pronto como Cl0p tiene acceso a los sistemas, este comienza el proceso de cifrado de archivos y presentando la nota de rescate con el monto a pagar para obtener la clave de descifrado.

PERSISTENCIA

La persistencia en los dispositivos comprometidos se da de múltiples maneras, según observaciones recientes a un ataque conducido por Cl0p, el grupo de actores malicioso hizo uso de una baliza de Cobalt Strike para establecer la persistencia. Lo anterior, mediante la creación de un nuevo servicio.

```
<Channel>Microsoft-Windows-PowerShell/Operational</Channel>
    <Computer><redacted></Computer>
    <Security UserID="S-1-5-21-3791960067-4030423757-2836428764-2179"
/>
  </System>
  <EventData>
    <Data Name="MessageNumber">1</Data>
    <Data Name="MessageTotal">12</Data>
    <Data Name="ScriptBlockText">$s=New-Object IO.MemoryStream(
[Convert]::FromBase64String("H4sIAAAAAAAA/+y9W6/ySLIg+tz9K+phS1UlajcGgz
EjbWnA3GxsczEXQ0+rBTYYG7DxDZOe....[SNIP]....WDNHk2KN6Mxg5x8wfbYFvvA9vFc
1DMF8FGOzap+FfIoYe5TjEznFHO6XQ94fQGRcAL</Data>
    <Data Name="ScriptBlockId">8730204e-7b5d-42e5-8e67-
3076424eddd9</Data>
    <Data Name="Path" />
  </EventData>
```

```
"[7045 / 0x1b85] Source Name: Service Control Manager Message string: A
service was installed in the system.

Service Name:  <redacted string #1>\nService File Name:
\\127.0.0[.]1\ADMIN$\<redacted string #1>[,]exe\nService Type:  user
mode service\nService Start Type:  demand start\nService Account:
LocalSystem Strings: ['<redacted string #1>'
'\\127.0.0[.]1\ADMIN$\<redacted string #1>[.]exe'  'user mode service'
'demand start'  'LocalSystem'] Computer Name: <redacted>.local Record
Number: 122100 Event Level: 4"
```


Imagen 3. Creación de nuevo servicio mediante baliza de Cobalt Strike.

MOVIMIENTO LATERAL

Una vez dentro de la red, los actores maliciosos proceden realizan movimiento lateral en los sistemas, buscando e infectando sistemas conectados. Mediante el movimiento lateral, el ransomware tiene la capacidad de desplegarse rápidamente por toda la red con la finalidad de infectar la infraestructura completa de la organización, encriptar todos los archivos posibles y así maximizar el impacto de la operación. Observaciones de ataques revelan como el grupo aprovecho conexiones SMB antes de realizar las transacciones a secciones interactivas de RPD.

```
<Channel>Microsoft-Windows-SmbClient/Connectivity</Channel>
<Computer><redacted></Computer>
<Security UserID="S-1-5-18" />
</System>
<EventData>
<Data Name="Reason">4</Data>
<Data Name="Status">3221226038</Data>
<Data Name="ServerNameLength">12</Data>
<Data Name="ServerName">192.168.8[.]47</Data>
<Data Name="AddressLength">16</Data>
<Data Name="RemoteAddress">020001BDC0A8082F0000000000000000</Data>
<Data Name="LocalAddress">00000000000000000000000000000000</Data>
<Data Name="InstanceNameLength">24</Data>
<Data Name="InstanceName">\Device\LanmanRedirector</Data>
<Data Name="ConnectionType">1</Data>

Event 131 - Remote Desktop Services - RDPCoreTS
<Channel>Microsoft-Windows-RemoteDesktopServices-
RdpCoreTS/Operational</Channel>
    <Computer><redacted>[.]local</Computer>
    <Security UserID="S-1-5-20" />
  </System>
  <EventData>
    <Data Name="ConnType">TCP</Data>
    <Data Name="ClientIP">192.168.8[.]57[:]57851</Data>
  </EventData>
```

Imagen 4. aprovechar las conexiones SMB.

ANÁLISIS

Según las muestras observadas del malware de Cl0p, esta muestra una interfaz gráfica, la cual ha sido compilada mediante Visual C/C++. Tras un análisis inicial, se pudo observar que Cl0p ransomware puede ser lanzado mediante la utilización de tres métodos distintos:

- Parámetro runrun: Sólo cifra las unidades de red.
- Parámetro temp.ocx: El cual cifra folders específicos mencionados en el archivo temp.
- Ejecutándolo sin ningún parámetro, lo que cifraría todas las unidades locales y de red.

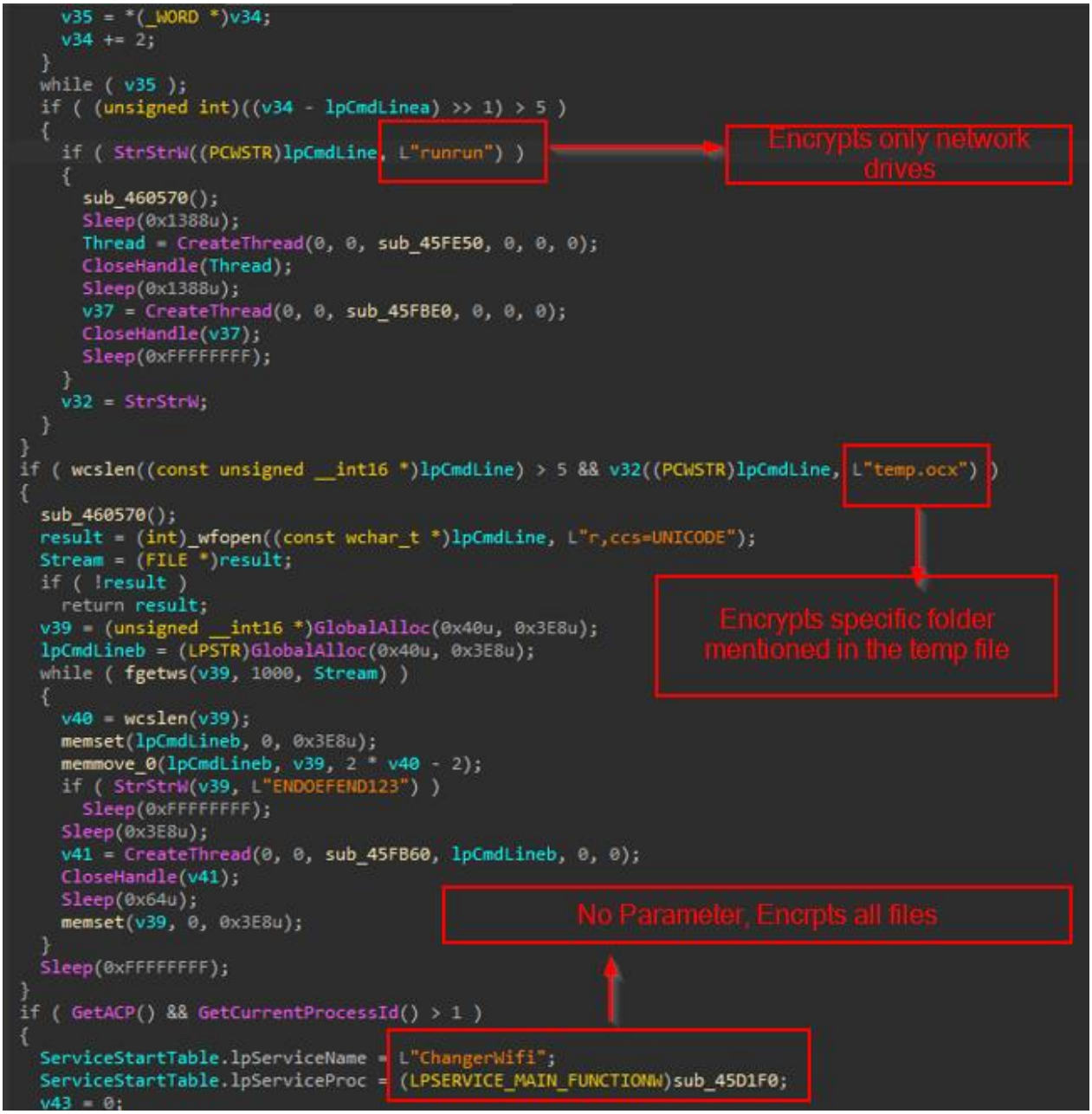

Imagen 5. Métodos para la ejecución del ransmware.

RUNRUN

Cuando el ransomware de Cl0p se inicia con el parámetro “runrun”, este crea dos procesos subsecuentes, el primero se encarga de escanear todos los recursos compartidos de la red como gestores de archivos de red, aplicaciones de backup o bien, herramientas de gestión de impresión para posteriormente cifrar archivos de estos. Esto lo realiza mediante el uso del módulo “MPR.DLL”: WNetOpenEnumW, WNetEnumResourceW y WNetCloseEnum.

Si por algún motivo, el malware es incapaz de enumerar los recursos compartidos de red, este cierra el proceso y comienza un segundo proceso, el cual tiene como propósito principal el recuperar las rutas a los folders de Outlook, Word u Office, de los usuarios mediante la función “SHGetSpecialFolderPathW()”. Esta ruta se somete a un proceso de cifrado luego de terminado su propósito.

```
hEnum = 0;
if ( !WNetOpenEnumW(2u, 0, 0, 0, &hEnum) )
{
  cCount = 1000;
  BufferSize = 32000;
  v3 = (char *)v1(0x40u, 0x7D00u);
  v11 = v3;
  if ( !WNetEnumResourceW(hEnum, &cCount, v3, &BufferSize) )
  {
    WNetCloseEnum(hEnum);
    hEnum = 0;
    v4 = v1(0x40u, 0x400u);
    v5 = cCount;
    v6 = 0;
    v10 = v4;
    v14 = 0;
```

Imagen 6. Enumeración de recursos compartidos de red.

Temp.ocx

Si el ransomware se ejecuta mediante el parámetro “temp.ocx”, inicialmente este verificara la existencia del argumento que contiene el string “temp.ocx”, de encontrarlo el código intenta abrir el archivo mencionado en el argumento de la línea de comandos en el modo UNICODE para lectura. Si este archivo es abierto de manera exitosa, el malware crea un nuevo hilo para el cifrado de los archivos especificados en “temp.ocx”.

```
if ( wcslen((const unsigned __int16 *)lpCmdLine) > 5 && v32((PCWSTR)lpCmdLine, L"temp.ocx") )
{
  sub_460570();
  result = (int)_wfopen((const wchar_t *)lpCmdLine, L"r,ccs=UNICODE");
  Stream = (FILE *)result;
  if ( !result )
    return result;
  v39 = (unsigned __int16 *)GlobalAlloc(0x40u, 0x3E8u);
  lpCmdLineb = (LPSTR)GlobalAlloc(0x40u, 0x3E8u);
  while ( fgetws(v39, 1000, Stream) )
  {
    v40 = wcslen(v39);
    memset(lpCmdLineb, 0, 0x3E8u);
    memmove_0(lpCmdLineb, v39, 2 * v40 - 2);
    if ( StrStrW(v39, L"ENDOEFEND123") )
      Sleep(0xFFFFFFFF);
    Sleep(0x3E8u);
    v41 = CreateThread(0, 0, sub_45F360, lpCmdLineb, 0, 0);
    CloseHandle(v41);
    Sleep(0x64u);
    memset(v39, 0, 0x3E8u);
  }
  Sleep(0xFFFFFFFF);
}
```

Imagen 7. El ransomware utilizando el párametro temp.ocx para ejecución.

En el caso de que el ransmoware se inicie sin parámetro alguno, el código primeramente buscara si puede instalarse como servicio, si esta instalación falla, el código se terminara a sí mismo. Si se determina que este puede ejecutarse como servicio, el malware genera un mutex, el cual se utiliza para bloquear y evitar que múltiples sub-procesos se escriban en la memoria compartida al mismo tiempo.

Posteriormente, el malware realiza tareas múltiples en el sistema comprometido, como primer punto, genera una lista completa de todos los procesos que se encuentran activos en el sistema y procede a cambiar el nombre a mayúsculas, seguidamente compara los procesos con el nombre “EXPLORER.EXE”, si se encuentra que estos coinciden, este utiliza la función “OpenProcess” para obtener un handle del token de acceso para ese proceso.

Mediante el handle del token, el malware recupera el nombre de usuario asociado a este. Seguidamente, crea un nuevo proceso y un proceso inicial bajo el contexto de seguridad del usuario, utilizando el argumento de línea de comandos, “runrun”. En el transcurso de este proceso, el malware se asegura de que los drivers de red también se cifran.

```
  result = CreateToolhelp32Snapshot(2u, 0);
  v1 = result;
  if ( result == (HANDLE)-1 || (pe.dwSize = 556, (result = (HANDLE)Process32FirstW(result, &pe)) == 0) )
  {
LABEL_5:
    if ( v1 )
      return (HANDLE)CloseHandle(v1);
  }
  else
  {
    while ( 1 )
    {
      lstrcpyW(String1, pe.szExeFile);
      v2 = lstrlenW(String1);
      CharUpperBuffW(String1, v2);
      if ( StrStrW(String1, L"EXPLORER.EXE") )
        break;
      result = (HANDLE)Process32NextW(v1, &pe);
      if ( !result )
        goto LABEL_5;
    }
    CloseHandle(v1);
    return (HANDLE)pe.th32ProcessID;
  }
  return result;
}
```

Imagen 8. Validación de nombre.

Seguidamente el malware procede a importar una clave privada desde una representación de cadena a un proveedor de servicios criptográficos (CSP) con fines de cifrado. Desde aquí, el ransomware procede a escanear todas las letras en la unidad disponibles en el sistema, mediante la utilización de la función GetDriveTypeW()este determina el tipo de drive asociado con cada letra, como es el caso de “Fixed”, “Removable”, o “Network drivers”.

Una vez identificados, el malware procede a crear un nuevo hilo mediante la API CreateThread, la cual transfiere las letras del drive como parámetro, para el proceso de infección. Entre las extensiones que el ransomware excluye a la hora de cifrar archivos, se encuentran las siguientes:

BAT	CMD	TTF
LNG	HLF	CHM
MSI	INI	ICO
LNK	SYS	EXE
DLL	OCX	CI_0P
NTUSER.DAT		

Tabla 1. Extensiones excluidas.

Posterior a cifrar los archivos, la nota de ransomware es liberada en cada uno de los ficheros, esta nota se encuentra de igual manera, cifrada, y es descifrada por el algoritmo XOR.

Otra funcionalidad destacable, es que el ransomware de Cl0p utiliza una aproximación asada en el tamaño del archivo, con la finalidad de elegir la mejor manera de proceder en relación al método a utilizar para el cifrado de los archivos. Los archivos pequeños no se cifran, los medianos se cifran mediante la función de API “ReadFile” y “WriteFile”. Mientras que los archivos más grandes se cifran mediante las funciones “CreateFileMappingW”, “MapViewOfFile”, “WriteFile”, y “UnmapViewOfFile”.

Imagen 9. Lógica de cifrado.

Por último, el ransomware cifra la clave RC4 mediante la clave publica RSA, y lo almacena en un archivo con el formato “filename.extension.C_I_0P”. Una vez se ha establecido la lógica del proceso, el ransomware comienza a cifrar los archivos en la maquina comprometida, mediante el algoritmo RC4, por último, la nota de rescate se establece en todos los archivos cifrados. El cuerpo de la nota presenta la demanda como tal, así como una URL onion a la página de filtraciones del grupo malicioso.

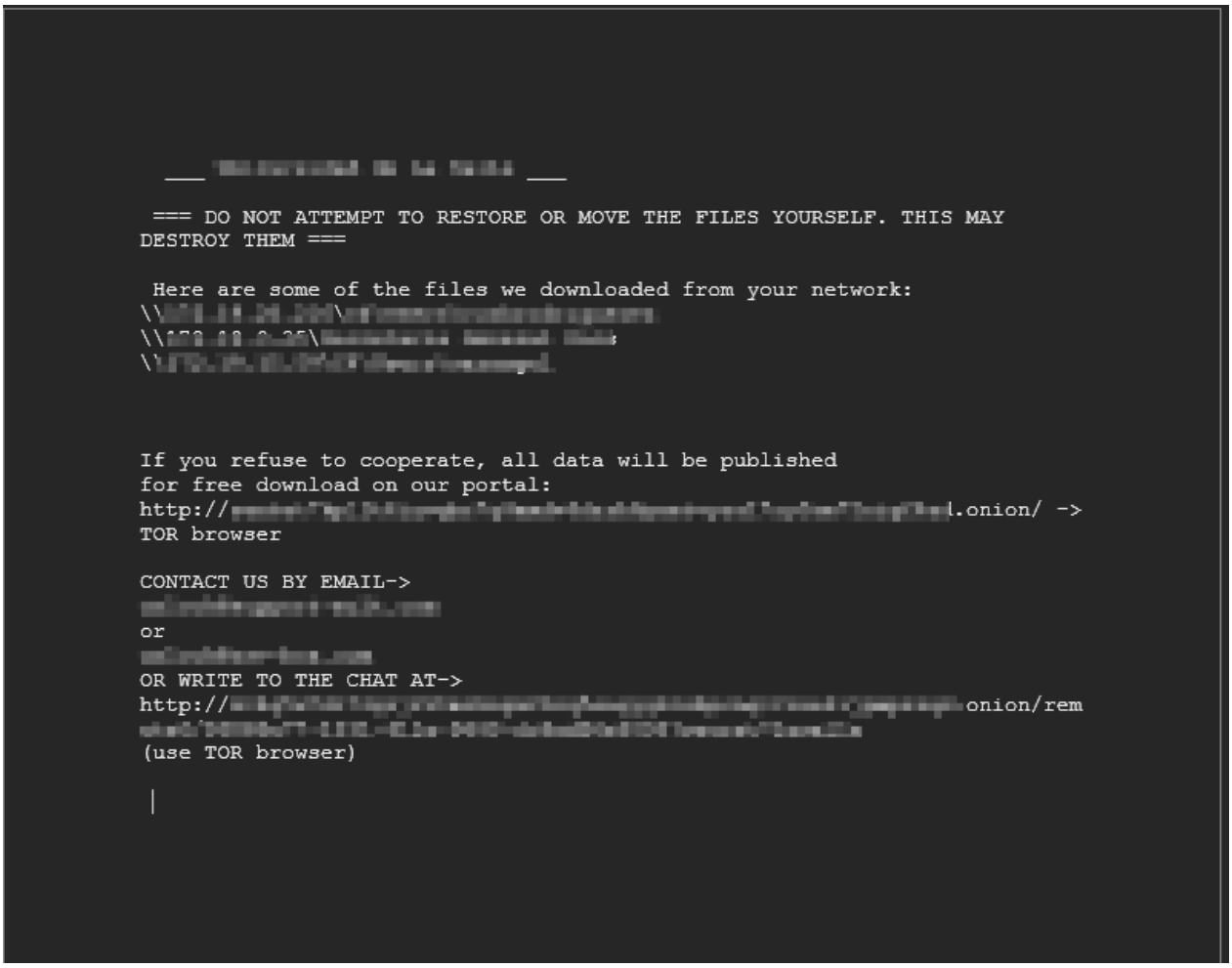

Imagen 10. Nota de rescate.

TECNICAS DEL FRAMEWORK DE MITRE ATT&CK

Táctica	ID de técnica	Nombre de la técnica
Acceso inicial	T1133 T1566	Servicios remotos externos. Phishing.
Ejecución	T1059 T1204	Intérprete de comandos y secuencias de comandos. Ejecución de usuario.
Persistencia	T1505.003 T1546.011	Componente de software de servidor: Shell Web. Ejecución activada por eventos: Ajuste de aplicaciones.
Escalación de privilegios	T1068	Explotación para la escalada de privilegios.
Descubrimiento	T1082 T1135 T1083	Descubrimiento de información del sistema. Descubrimiento de recursos compartidos de red. Descubrimiento de archivos y directorios.
Movimiento lateral	T1021.002 T1563.002	Servicios remotos: SMB/Windows Admin Shares. Secuestro de Sesión de Servicio Remoto: Secuestro RDP
Comando y Control	T1071 T1105	Protocolo de la capa de aplicación. Transferencia de herramientas de entrada.
Impacto	T1486	Cifrado de datos.

MOVEIT

En mayo de 2023, el grupo de actores maliciosos lanzó una campaña aprovechando una vulnerabilidad Zero-day en los sistemas de transferencia de archivos MOVEit de Progress, el cual admite motores de base de datos MYSQL, Microsoft SQL, y Azure SQL. Posteriormente la vulnerabilidad se rastreó como CVE-2023-34362, y fue utilizada por los actores maliciosos para la instalación del Web Shel denominado LEMURLOOT en la aplicación web de MOVEit Transfer.

Dentro de los sistemas comprometidos, LEMURLOOT se utilizó como método de persistencia, recolector de información y ladrón de información, a su vez, el webshell importó múltiples bibliotecas, incluyendo “MOVEit.DMZ.ClassLib”, “MOVEit.DMZ.Application.Files,” y “MOVEit.DMZ.Application.Users”, con la finalidad de interactuar con el software de gestión de transferencia de archivos de MOVEit.
Tras la instalación, el shell web crea una contraseña aleatoria de 36 caracteres que se utilizará para la autenticación. El webshell interactúa con sus operadores esperando peticiones HTTP que contengan un campo de cabecera denominado X-siLock-Comment, que debe tener un valor asignado igual a la contraseña establecida al instalar el shell web. Después de autenticarse con el shell web, los operadores pasan comandos al shell web que pueden:

- Recupere la configuración del sistema Microsoft Azure, Azure Blob Storage, la cuenta Azure Blob Storage, la clave Azure Blob y Azure Blob Container mediante la siguiente consulta:

    - "select f.id, f.instid, f.folderid, filesize, f.Name as Name, u.LoginName as uploader, fr.FolderPath , fr.name as fname from folders fr, files f left join users u on f.UploadUsername = u.Username where f.FolderID = fr.ID" (Figura 2).

- Enumera la base de datos SQL subyacente.
- Almacenar una cadena enviada por el operador y luego recuperar un archivo con un nombre que coincida con la cadena desde el sistema MOVEit Transfer.
- Store a string sent by the operator and then retrieve a file with a name matching the string from the MOVEit Transfer system.
- Cree una nueva cuenta privilegiada de administrador con un nombre de usuario generado aleatoriamente y los valores LoginName y RealName establecidos en "Health Check Service".
- Eliminar una cuenta con los valores LoginName y RealName establecidos en 'Health Check Service'.

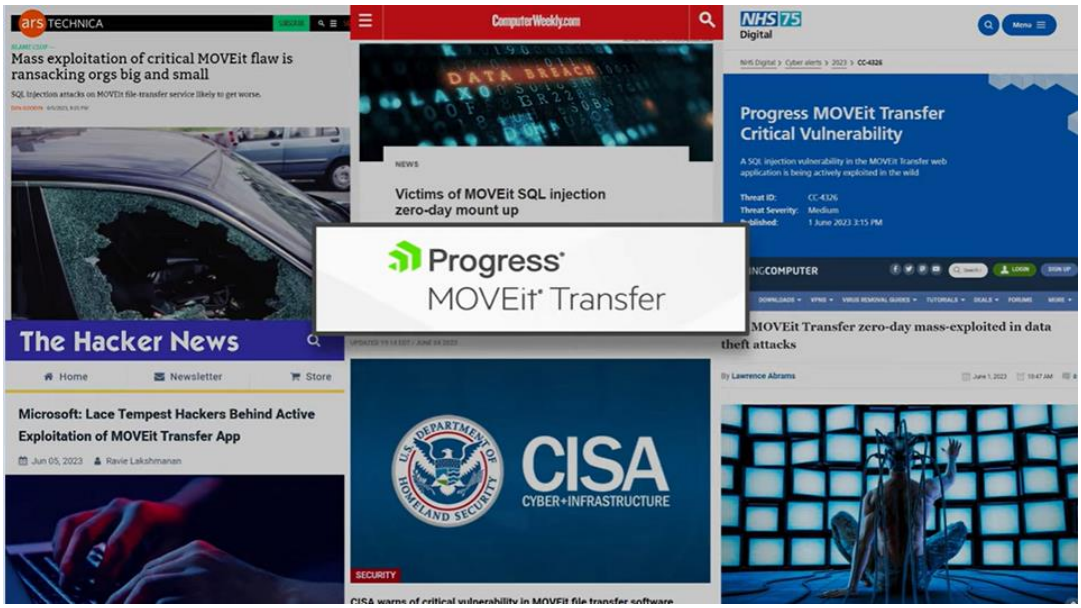

Imagen 11. Campaña masiva de MOVEit.

Desde la brecha inicial hasta el día de hoy, la campaña de Cl0p mediante la explotación de CVE-2023-34462, ha ido agregando una gran cantidad de víctimas a su lista, se estima que, a día de hoy los afectados en esta campaña superan las 150 organizaciones a nivel mundial. Entre las organizaciones afectadas, más conocidas se encuentran las siguientes.

- SHELL
- Genworth
- Departamento de Energía de EE.UU.
- Departamento de Educación de Minnesota
- Ofcom, regulador de las telecomunicaciones en el Reino Unido
- Autoridad sanitaria de la provincia canadiense de Nueva Escocia
- British Airways
- BBC
- Cadena de farmacias Boots
- Universidad Johns Hopkins
- Sistema sanitario Johns Hopkins
- Banco Tesco
- Seguros de vida Delaware
- Aer Lingus
- 1st Source
- First National Bankers Bank
- Inversiones Putnam
- Landal GreenParks
- Shell, el gigante energético británico
- Datasite
- Centro Nacional de Información Estudiantil
- Recursos para estudiantes de United Healthcare
- Leggett & Platt
- ÖKK
- Sistema Universitario de Georgia (USG)
- Heidelberg
- Gobierno de Nueva Escocia
- Ernst and Young
- Gobierno del Estado de Illinois
- Gobierno del Estado de Minnesota
- Gobierno del Estado de Missouri
- Zellis
- Universidad Técnica de Hennepin
- Distrito escolar de Perham
- Departamento de Innovación y Tecnología de Illinois (DoIT)

La gravedad y amplitud de estos ataques ha puesto en alerta a varias instituciones tanto privadas como gubernamentales. El 16 de junio, a través de su cuenta oficial de Twitter, el programa de Recompensas por la Justicia del Departamento de Recompensas por la Justicia del Departamento de Estado de los Estados Unidos, anuncio que se estaría recompensando con la suma de 10 millones de dólares a aquellos

que pudieran proporcionar información verificable, que vincule los ataques de Cl0p con un gobierno extranjero, así como información de cualquiera de los integrantes de este.

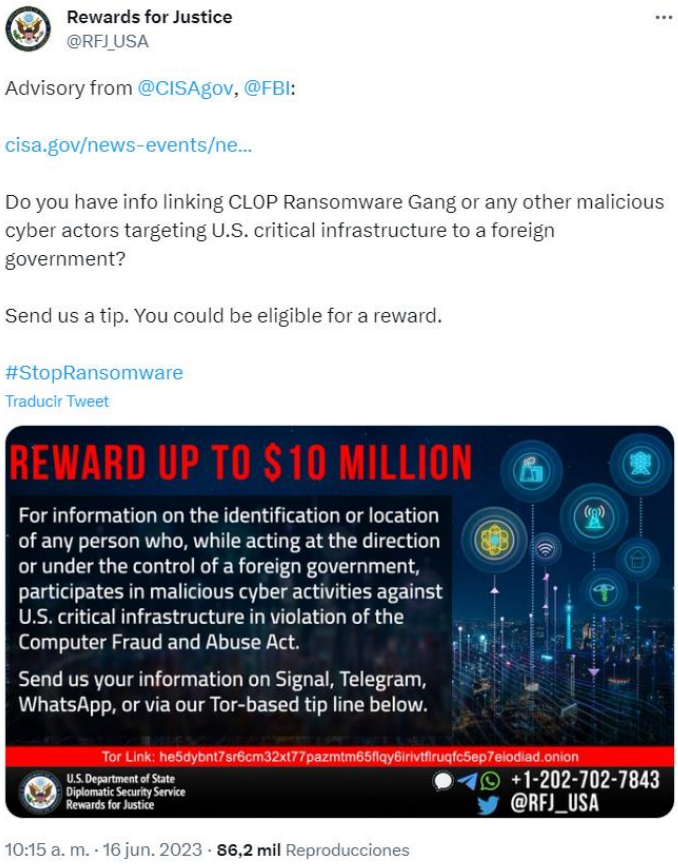

Imagen 12. Recompensa ofrecida por información que conduzca a Cl0p.

CONCLUSION

El grupo de actores maliciosos “Clop ransomware” ha demostrado ser un grupo muy capaz, sumamente experimentado y sofisticado, la variedad en la versión de su ransomware demuestra la capacidad de estos de afectar no solo operaciones que corren sobre Windows, si no también, aquellos sistemas operativos basados en Linux.

El servicio que ofrece Cl0p como un Ransomware-as-a-Service (RaaS) ha demostrado ser un modelo viable para este tipo de actores maliciosos. abonado a la selectividad de objetivos, como aquellos de América Latina, donde la concientización sobre ciber seguridad, no se encuentra arraigada en las organizaciones, de manera que se vea como una prioridad en toda organización.

Campañas a gran escala contra software de gestión de transferencia de archivos, como el caso de MOVEit ha demostrado la gran vialidad para comprometer organizaciones enteras por parte de los actores maliciosos, y resalta, nuevamente, la importancia de tener un gran un plan robusto de contingencia. La estimación por parte de la comunidad de ciber seguridad, es que se veo un aumento en ataques contra este tipo de software, por lo que se insta a implementar las medidas necesarias.

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.
- Implementar sistemas de detección de intrusión (IDS) y así detectar actividad de mando y control, así como cualquier otra actividad de red potencialmente maliciosa.
- Realizar análisis de malware periódicos en los sistemas para detectar y eliminar posibles amenazas.
- Utilizar técnicas de sandboxing para ejecutar archivos sospechosos de forma aislada y proteger los sistemas principales.
- Implementar MFA resistente a phishing, especialmente en email, VPNs, y cuentas con acceso a sistemas críticos.
- 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.
- No utilizar cuentas de acceso raíz en las operaciones del día a día. Crear usuarios, grupos y roles para llevar a cabo tareas.
- Realice copias de seguridad periódicas y manténgalas fuera de línea o en una red separada.
- Activa la función de actualización automática de software en tu ordenador, móvil y otros dispositivos conectados siempre que sea posible y pragmático.
- 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/tree/26fc2b5c5e44aaab6a40e7fae79ae743c65c132b/20230712_01_Cl0p

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