Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

I. DATOS GENERALES

Clase de alerta: Malware
Tipo de incidente: Ransomware
Nivel de riesgo: Medio

II. ALERTA

Durante marzo y abril de 2022, empresas ecuatorianas, de los sectores de comercialización de materiales de construcción y prestadores de servicios de logística y transportación, fueron víctimas de un ciberataque de tipo Ransomware LockBit 2.0.

Figura 1. Arriba: empresa ecuatoriana#1 datos publicados en marzo 25 de 2022
Abajo: empresa ecuatoriana#2 datos por publicarse en abril 10 de 2022
Fuente: Sitio Web en la red Tor Ransomware LockBit 2.0

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

Figura 2. Pantalla de información Ransomware LokBit 2.0.
Fuente: Chuongdong

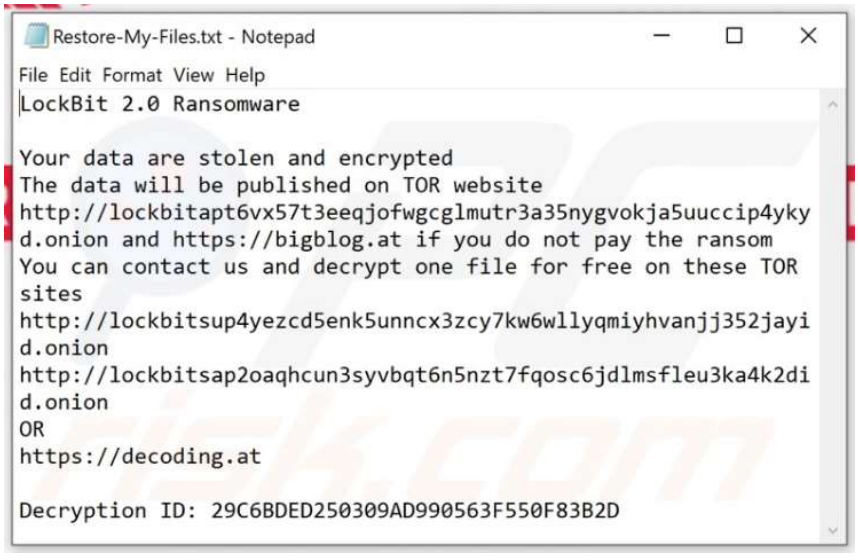

Figura 3. Nota de rescate de información Ransomware LokBit 2.0.
Fuente: PCrisk

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

III. INTRODUCCIÓN

LockBit 2.0 es una variante del ransomware Lockbit, también conocido como Bitwise Spider o LockBitSupp, perteneciente a la familia de malware "LockerGoga & MegaCortex"; LockBit apareció en septiembre de 2019 como un RaaS (Ransomware as a Service); entre las características de este ransomwarese menciona:

- Autopropagación
- Eliminación de instantánea
- Eludir el Control de cuentas de usuario (UAC)
- Compatibilidad con ESXi
- Impresión de notas de rescate a través de impresoras detectadas en la red de la víctima.

LockBit 2.0 actúa creando nuevas políticas de grupo en el controlador de dominio que luego se enviarán a todos los dispositivos de la red; deshabilitando la protección en tiempo real de Microsoft Defender, utiliza un esquema de criptografía híbrida de XSalsa20-Poly1305-Blake2b-Curve25519 y AES-128-CBC de Libsodium para cifrar archivos

IV. VECTOR DE ATAQUE

Red, Phishing.

V. IMPACTO

LockBit 2.0 sigue el modelo de Ransomware como Servicio (RaaS); es decir, proporciona a sus clientes la infraestructura y el malware a cambio de una comisión del rescate; siendo responsabilidad del contratista, el ingreso a la red de la víctima. Cabe señalar que, los ciberdelincuentes utilizan técnicas de ingeniería social y correo electrónico con phishing para obtener el acceso inicial. El nombre de archivo de la nota de rescate es Restore-My-Files.txt

A. Etapas de ataque:

LockBit 2.0, presenta tres etapas para desarrollar su ataque.

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:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

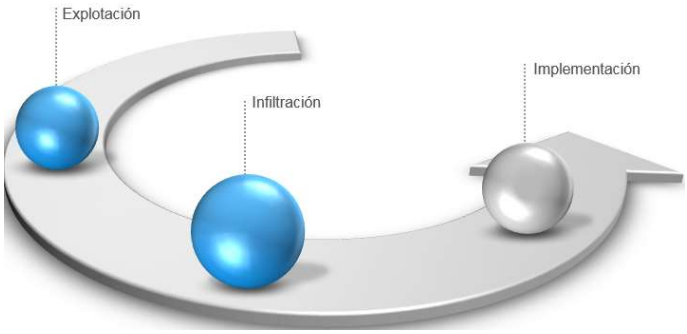

Figura 4. Etapas ransomware LockBit 2.0
Fuente: Kaspersky

- La **Explotación** puede originarse a través de técnicas de Ingeniería Social como el phishing; sin embargo, no se descarta el uso de fuerza bruta contra los servidores de la intranet y los sistemas de red de una organización.

- En la etapa de **Infiltración,** LockBit 2.0 realiza todas las actividades por sí mismo; es decir, siguiendo la ejecución de comandos, su objetivo principal es imposibilitar la recuperación de la información de la víctima.

  Este ransomware está programado para utilizar herramientas de pos explotación para obtener privilegios escalonados y lograr el nivel de acceso necesario para lanzar los ataques.

- En la fase de **implementación** se busca que LockBit 2.0 empiece a propagarse a través de las máquinas a las que puede acceder; cabe señalar que una sola unidad de sistema con alto nivel de acceso puede emitir comandos a otras unidades de la red para descargar LockBit 2.0 y ejecutarlo.

  En esta sección ocurre el **cifrado** que consiste en bloquear el acceso a los archivos del sistema; en este caso, las víctimas solo podrán desbloquear sus sistemas con una clave personalizada creada por LockBit 2.0. Los diferentes archivos comprometidos tienen la extensión: **.lockbit**

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

B. Análisis del funcionamiento:

Un análisis realizado al funcionamiento de LockBit 2.0, destaca lo siguiente:

1. **Comprobación del Lenguaje Informático**
   LockBit 2.0 verifica si el idioma de la interfaz de usuario predeterminado del sistema o del usuario está en ruso o en países cercanos, en el caso de que el equipo este en dichos países, se ejecuta **ExitProcess** y se termina de inmediato; para la verificación resuelve **GetSystemDefaultUILanguage** y **GetUserDefaultUILanguage**, como se indica en la siguiente figura:

```
  GetSystemDefaultUILanguage = (v0 + *(v97[7] + 4 * *(v97[9] + 2 * v105 + v0) + v0));
LABEL_28:
  GetSystemDefaultUILanguage_1 = GetSystemDefaultUILanguage;
LABEL_29:
  sys_def_UI_lang = GetSystemDefaultUILanguage();
  if ( sys_def_UI_lang != 0x82C                 // Azerbaijani (Cyrillic, Azerbaijan)
    && sys_def_UI_lang != 0x42C                 // Azerbaijani (Latin, Azerbaijan)
    && sys_def_UI_lang != 0x42B                 // Armenian (Armenia)
    && sys_def_UI_lang != 0x423                 // Belarusian (Belarus)
    && sys_def_UI_lang != 0x437                 // Georgian (Georgia)
    && sys_def_UI_lang != 0x43F                 // Kazakh (Kazakhstan)
    && sys_def_UI_lang != 0x440                 // Kyrgyz (Kyrgyzstan)
    && sys_def_UI_lang != 0x819                 // Russian (Moldova)
    && sys_def_UI_lang != 0x419                 // Russian (Russia)
    && sys_def_UI_lang != 0x428                 // Tajik (Cyrillic, Tajikistan)
    && sys_def_UI_lang != 0x442                 // Turkmen (Turkmenistan)
    && sys_def_UI_lang != 0x843                 // Uzbek (Cyrillic, Uzbekistan)
    && sys_def_UI_lang != 0x443                 // Uzbek (Latin, Uzbekistan)
    && sys_def_UI_lang != 0x422 )               // Ukrainian (Ukraine)
  {
    goto LABEL_72;
  }
```

Figura 5. Comprobación de Idioma por parte de LockBit
Fuente: Chuongdong

2. **Configuración predeterminada de errores y privilegios**

   Con el objetivo de que el aplicativo no pueda ser cerrado, LockBit emplea la función **NtSetInformationProcess.** Esta función externa del sistema operativo no documentada, le indica al sistema operativo que configure el proceso actual como "crítico" sin que pueda cerrarse el proceso y desencadenaría un BSOD cuando se cierra a la fuerza.

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:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

```
default_hard_error_mode = 7;                    // SEM_FAILCRITICALERRORS |
                                                // SEM_NOGPFAULTERRORBOX | SEM_NOALIGNMENTFAULTEXCEPT
NtSetInformationProcess = get_NtSetInformationProcess();
NtSetInformationProcess(0xFFFFFFFF, ProcessDefaultHardErrorMode, &default_hard_error_mode, 4);
RtlAdjustPrivilege = get_RtlAdjustPrivilege();
RtlAdjustPrivilege(SE_TAKE_OWNERSHIP_PRIVILEGE, TRUE, 0, &Enabled_flag);
```

Figura 6. Configuración predeterminada de errores y privilegios
Fuente: Chuongdong

- **SEM_FAILCRITICALERRORS:** el sistema no muestra el cuadro de mensaje del controlador de errores críticos y envía el error al proceso de llamada.
- **SEM_NOGPFAULTERRORBOX** : el sistema no muestra el cuadro de diálogo Informe de errores de Windows.
- **SEM_NOALIGNMENTFAULTEXCEPT**: el sistema corrige automáticamente las fallas de alineación.
- También llama a **RtlAdjustPrivilege** para habilitar el privilegio **SE_TAKE_OWNERSHIP_PRIVILEGE** para poder luego tomar posesión de los archivos durante el cifrado.

3. Configuración de LockBit 2.0

- Se codifica y almacena estáticamente en el ejecutable, conteniendo los siguientes campos:

```
decrypt_config(0x1B25u, byte_4E7F10, &EMF_ALL_YOUR_FILES_ARE_ENCRYPTED, &EMF_RESOURCE_LEN);
decrypt_config(0xC78u, byte_4EAF10, &EMF_LOCKBIT_2_0, &EMF_RESOURCE_2_LEN);
decrypt_config(0x2839u, byte_4E5220, &BLENDER_PRO_MED_FONT, &FONT_RESOURCE_LEN);
decrypt_config(0x40F1u, byte_4EBB90, &PROXIMA_NOVA_FONT, &FONT_RESOURCE_2_LEN);
decrypt_config(0x11BFu, byte_4E9A40, &LOCKBIT_TEXT_PNG, &LOCKBIT_WALLPAPER_LEN);
decrypt_config(0x228u, byte_4EFC90, &LOCKBIT_ICON_PNG, &LOCKBIT_WALLPAPER_ICON_LEN);
decrypt_config(0x73Bu, byte_4EFEC0, &LOCKBIT_ICON_LARGE_PNG, &LOCKBIT_WALLPAPER_ICON_LARGE_LEN);
decrypt_config(0x4A5u, byte_4E7A60, &PROCESSES_NAME_LIST, &PROCESSES_NAME_LIST_LEN);
decrypt_config(0x30Fu, byte_4EAC00, &SERVICES_NAME_LIST, &SERVICES_NAME_LIST_LEN);
```

Figura 7. Datos de configuración
Fuente: Chuongdong

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

A continuación, se describen los datos que se observan en la figura 9:

- Archivo EMF 1: contiene el gráfico vectorial para el texto "TODOS SUS ARCHIVOS IMPORTANTES SON ROBADOS Y ENCRIPTADOS"
- Archivo EMF 2: contiene el gráfico vectorial para el texto "LOCKBIT 2.0"
- Archivo Blender Pro Medio TTF
- Archivo Próxima Nova TTF
- Texto de LockBit PNG
- Icono de LockBit PNG
- Icono de LockBit PNG grande
- Lista de procesos: lista de procesos para terminar, cada uno separado por una coma
- Lista de servicios: lista de servicios para detener, cada uno separado por una coma

- La configuración de banderas “flags”, se almacena en una matriz de bytes. Cada byte corresponde a un indicador de ejecución específico que comprueba LockBit 2.0.
  - La bandera está habilitada si el byte correspondiente es 0xFF.
  - Está deshabilitada si el byte correspondiente es 0xAA.

```
.data:004F05FC CONFIG_FLAGS     db 0FFh
.data:004F05FD                  db 0FFh
.data:004F05FE                  db 0FFh
.data:004F05FF                  db 0FFh
.data:004F0600                  db 0AAh
.data:004F0601                  db 0AAh
.data:004F0602                  db 0FFh
.data:004F0603                  db 0FFh
.data:004F0604                  db 0FFh
.data:004F0605                  db 0AAh
```

Figura 8. Banderas de configuración
Fuente: Chuongdong

Considerando la figura 9, en la siguiente tabla se muestran las banderas y su orden en la matriz.

Índice	Detalle
Índice 0	Deshabilitar la derivación de UAC.
Índice 1	Habilitar la eliminación automática.
Índice 2	Habilitar registro.
Índice 3	Habilitar el cruce de red para el cifrado de archivos.
Índice 4	Si los 3 están configurados, configure las políticas de grupo para Active Directory.
Índice 5	
Índice 6	
Índice 7	Establecer registro para el icono predeterminado de la extensión de LockBit.
Índice 8	Imprimir nota de rescate en la impresora de red.

Tabla 1. Banderas de LockBit 2.0.
Fuente: Chuongdong

4. **Escalada de privilegios.**
Dentro de escalada de privilegios, LockBit 2.0 considera dos escenarios:
   a) Si el usuario ejecuta el ransomware en cuentas de servicio.
   b) Si el usuario ejecuta el ransomware en otro tipo de cuentas: administrador, administrador de dominio.

5. **Inicio de sesión**
El malware configura automáticamente la interfaz de usuario; por tal razón llama a **GetModuleHandleW** para recuperar el identificador del ejecutable en ejecución. A continuación, el malware completa una estructura **WNDCLASSEXW** utilizando este identificador como instancia de la ventana de registro.

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

```
  GetModuleHandleW = (v0 + *(v0 + v174[7] + 4 * *(v0 + v174[9] + 2 * v160)));
LABEL_28:
  GetModuleHandleW_1 = GetModuleHandleW;
LABEL_29:
  curr_mod_handle = GetModuleHandleW(0);
  v23 = USER32_DLL;
  curr_mod_handle_1 = curr_mod_handle;
  memset(&class_struct, 0, sizeof(class_struct));
  class_struct.cbSize = 0x30;
  class_struct.style = 3;
  class_struct.lpfnWndProc = log_window_procedure;
  class_struct.hInstance = curr_mod_handle;
  if ( USER32_DLL )                                  // pointer to an application-defined
                                                     // function called the window procedure.
                                                     // The window procedure defines most
                                                     // of the behavior of the window.
```

Figura 9. Configuración Ventana de Registro LockBit 2.0.
Fuente: Chuongdong

Cada vez que LockBit 2.0 muestra un mensaje de registro, llama a la función **SendMesageA;** siendo esta función la que envía el mensaje a la ventana de registro. En la siguiente gráfica, se indica la interfaz de usuario (IU) de la ventana de registro.

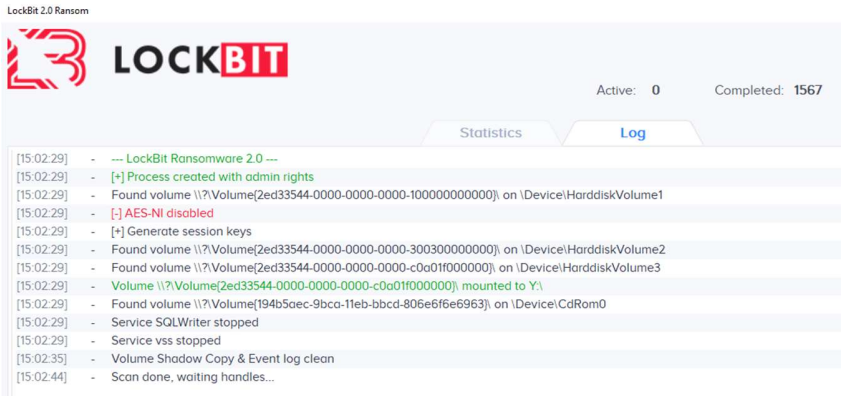

Figura 10. IU ventana de registro.
Fuente: Chuongdong

Cabe recalcar que LockBit 2.0 evita que se ejecuten varias instancias de ransomware al mismo tiempo.

6. Configuración de política de grupo.

A través de la función **GetComputerNameW,** LockBit 2.0 verifica si se está ejecutando en un controlador de dominio principal, posteriormente a través de **NetGetDCName** obtiene el nombre del controlador de dominio.

Para obtener el identificador del token del proceso emplea **NtOpenProcessToken.** En la siguiente gráfica se muestran los códigos asociados a estas funciones.

```
 GetComputerNameW = (v2 + *(v2 + *(v102 + 0x1C) + 4 * *(v2 + *(v102 + 0x24) + 2 * v104)));
LABEL_29:
 GetComputerNameW_1 = GetComputerNameW;
LABEL_30:
 if ( !GetComputerNameW(computer_name_buffer_1, computer_name_len) )
```

```
if ( NetGetDCName(0, 0, DC_name_buffer) )     // retrieve primary domain controller name
  goto LABEL_126;
DC_name_buffer_2 = *DC_name_buffer_1;
if...
v73 = KERNEL32_DLL;
if...
v74 = NtCurrentPeb()->Ldr->InLoadOrderModuleList.Flink->Flink;
v102 = v74;
v75 = v74;
v104 = v74;
while...
do...
if...
v73 = v104[3].Flink;
LABEL_110:
KERNEL32_DLL = v73;
LABEL_111:
lstrcmpiW = lstrcmpiW_1;
if...
if...
v87 = (v73 + *(v85 + 0x20));
v101 = v87;
while...
do...
v86 = v104;
if...
lstrcmpiW = (v73 + *(*(v102 + 0x1C) + 4 * *(*(v102 + 0x24) + 2 * v104 + v73) + v73));
LABEL_124:
lstrcmpiW_1 = lstrcmpiW;
LABEL_125:
v99 = lstrcmpiW(computer_name_buffer_1, *DC_name_buffer) == 0;// Compare PC name to PDC name
```

Figura 11. Política de Grupo
Fuente: Chuongdong

En el caso de que el usuario tenga privilegios de adminsitrador; LockBit 2.0 llama a la función **GetComputerNameExW** para recuperar el nombre del dominio DNS de la computadora local.

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

7. Establecer icono predeterminado de LockBit 2.0

Los archivos cifrados tienen la extensión **.lockbit**; para configurar el ícono premeditado, el malware tiene privilegios de administrador y se establece en el índice 7 (tabla Nro. 2) de las banderas de LockBit 2.0: "*Establecer registro para el icono predeterminado de la extensión de LockBit.*"

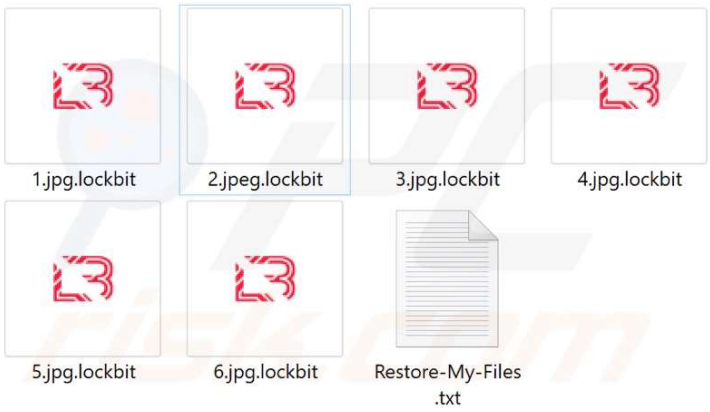

Figura 12. Íconos LockBit 2.0
Fuente: PCrisk

8. Limpieza del sistema de cifrado previo

La sección de limpieza del sistema de cifrado empleado por LockBit 2.0 está compuesta por tres secciones:

a) Servicios de detención.
b) Procesos de Terminación.
c) Eliminación de copias de seguridad.

En las siguientes gráficas, se observan las diferentes acciones realizadas por LockBit 2.0 para la ejecución de servicios de detención y procesos de terminación.

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

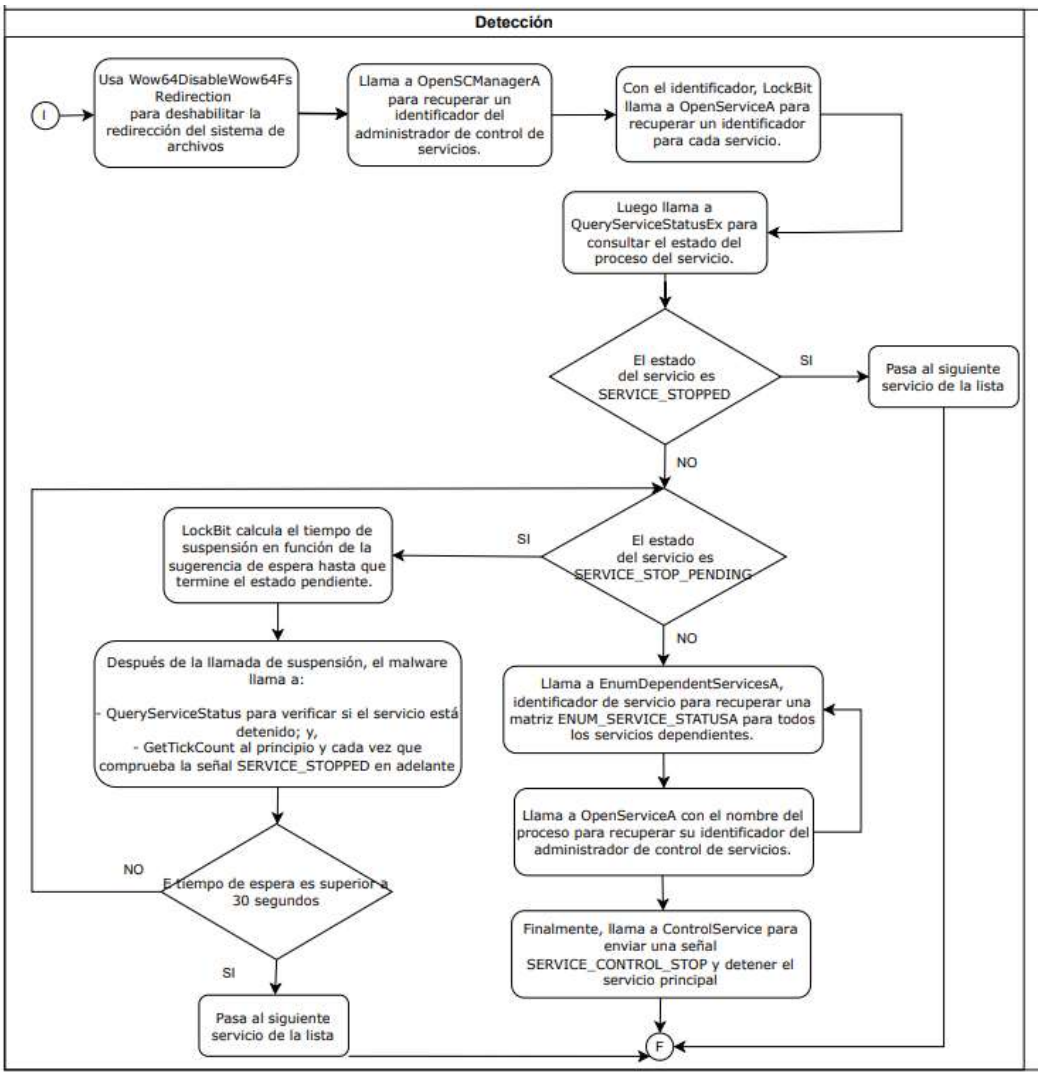

Figura 13. Diagrama de flujo Servicios de Detención
Fuente: Chuongdong

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

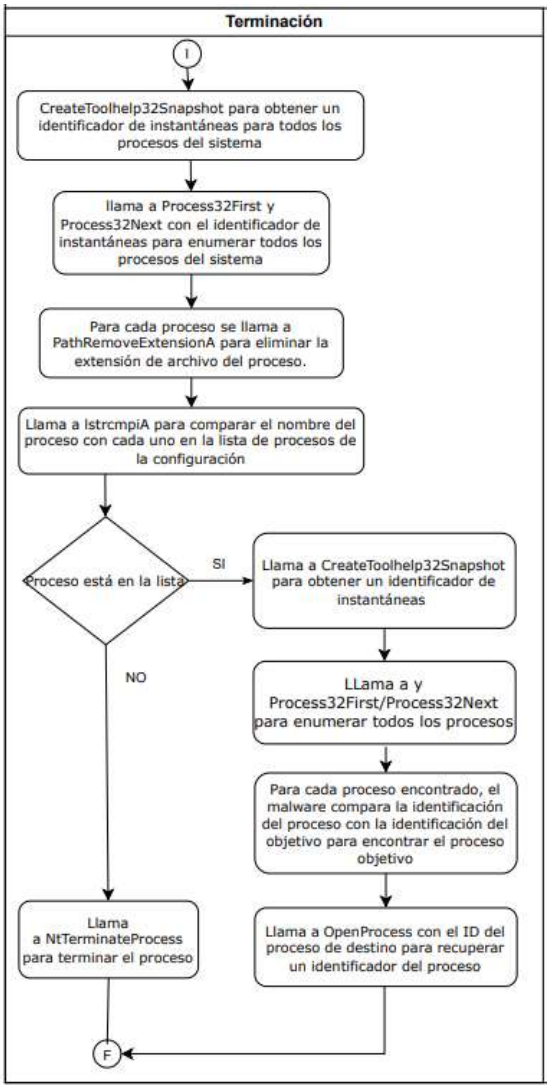

Figura 14. Diagrama de flujo Procesos de Terminación ejecutado por LockBit 2.0
Fuente: Chuongdong

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

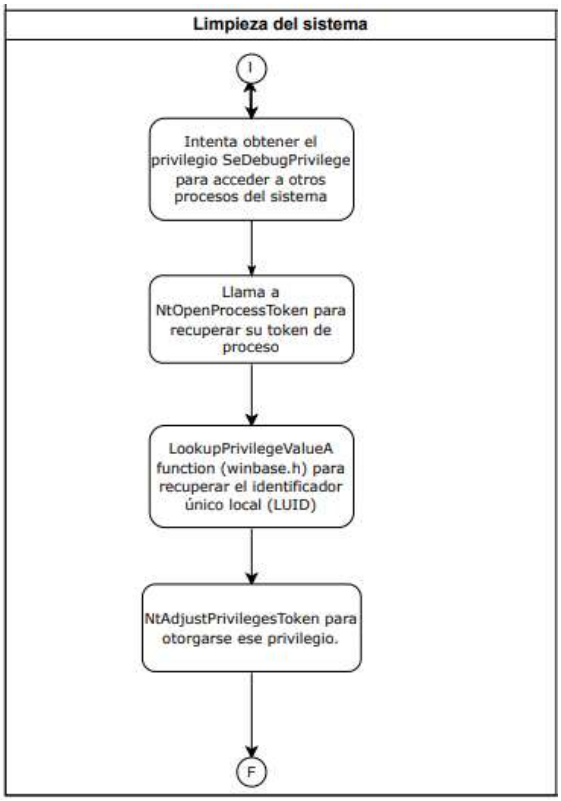

Figura 15. Diagrama de flujo Procesos de Limpieza ejecutado por LockBit 2.0
Fuente: Chuongdong

En referencia a la Eliminación de copias de seguridad; **LockBit 2.0**¸ analiza el siguiente parámetro:

```
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
```

Figura 16. Cadena de comparación verificado por LockBit 2.0
Fuente: Chuongdong

De la cadena anterior, selecciona los campos apropiados y envía a la función **ShellExecuteA** y ejecuta con el comando **cmd.exe.**

9. Impresión de una nota de rescate en las impresoras.

LockBit 2.0, al igual que otras muestras de ransomware, imprime las notas de rescate en todas las impresoras de red que estén conectadas. Para imprimir la nota de rescate en impresoras físicas, LockBit 2.0 llama a la función **EnumPrintersW.**

```
v45 = printer_enum_info;
if ( EnumPrintersW_1(enum_printer_flags, 0, 1, printer_enum_info, pcbNeeded, &pcbNeeded, &pcReturned) )
{
  v46 = 0;
  if ( pcReturned )
  {
    printer_name = &printer_enum_info->pName;
    do
    {
      ++v46;
      v50 = printer_print(FULL_RANSOM_NOTE_BUFFER, *printer_name, RANSOM_NOTE_LEN); // enum each printer and print ransom note
      printer_name += 4;
    }
    while ( v46 < pcReturned );
    v45 = printer_enum_info;
  }
}
```

Figura 17. Líneas de código de LockBit 2.0 para impresión de nota de rescate
Fuente: Chuongdong

LockBit 2.0 resuelve las dos cadenas "**Microsoft Print to PDF**" y "**Microsoft XPS Document Writer**", llama a **lstrcmpiW** para compararlas con el nombre de la impresora. Si el nombre de la impresora es uno de esos dos, la función sale y la nota de rescate no se imprime. Esto es para evitar imprimir la nota de rescate en un archivo en el sistema y solo imprimir la nota en las impresoras físicas a las que está conectada la máquina.

En la siguiente gráfica se observa las notas de rescate ejecutadas por LockBit 2.0.

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

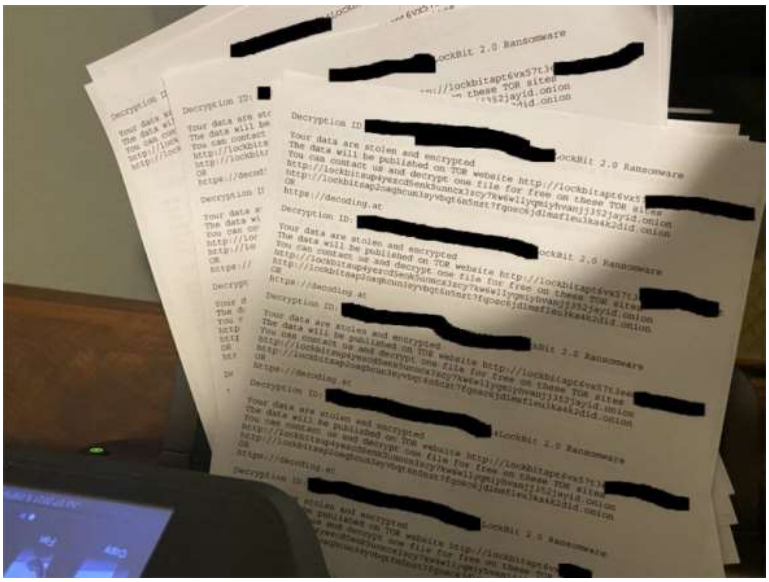

Figura 18. Impresiones de notas de rescate de LockBit 2.0
Fuente: ESET

C. Resumen de la amenaza:

Considerando que LockBit 2.0 es un ransomware con consecuencias significativas para las víctimas y, teniendo como referencia que el mismo ya ha sido detectado en Ecuador; un paso clave para mitigar su accionar; es la detección de LockBit 2.0. En la siguiente tabla, se indican las características de este ransomware:

Resumen de la Amenaza:	
Nombre	Virus "LockBit 2.0"
Tipo de Amenaza	Ransomware, Crypto Virus, Files locker

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:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

Resumen de la Amenaza:	
Extensión de Archivos Encriptados	.lockbit
Mensaje Demandate de Rescate	Texto presentado en LockBit_Ransomware.hta, Restore-My-Files.txt y fondo de escritorio
Contacto del Cibercriminal	Sitios web en la red Tor
Nombres de Detección	Avast (Win32:LockBit-A [Ransom]), Combo Cleaner (Gen:Variant.Ransom.Lockbit2.9), ESET-NOD32 (una variante de Win32/Filecoder.Lockbit.E), Kaspersky (HEUR:Trojan-Ransom.Win32.Lockbit.gen), Microsoft (Ransom:Win32/Lockbit.STA), Lista Completa de Detecciones (VirusTotal)
Síntomas	No se pueden abrir archivos almacenados en su computadora, los archivos previamente funcionales ahora tienen una extensión diferente (por ejemplo, my.docx.locked). Se muestra un mensaje de solicitud de rescate en su escritorio. Los ciberdelincuentes exigen el pago de un rescate (generalmente en bitcoins) para desbloquear sus archivos.
Métodos de Distribución	Archivos adjuntos de email infectados (macros), sitios web de torrents, anuncios maliciosos.
Daño	Todos los archivos están encriptados y no se pueden abrir sin pagar un rescate. Se pueden instalar troyanos adicionales que roban contraseñas e infecciones de malware junto con una infección de ransomware.

Tabla 1. Parámetros de LockBit 2.0. **Fuente:** PCrisk

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

D. Cadena de ataque del ransomware Lockbit 2.0:

La cadena de ataque del ransomware LockBit 2.0, se resume de la siguiente forma:

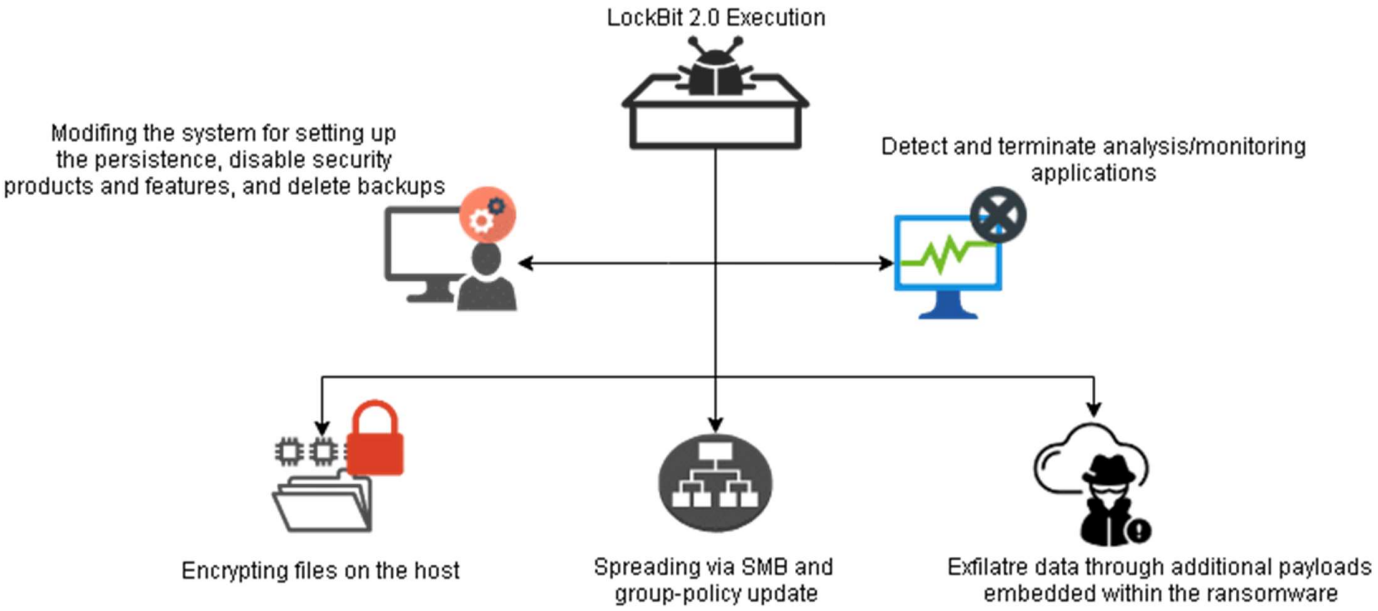

Figura 19. Cadena de ataque LockBit 2.0
Fuente: Cynet

E. Características de comportamiento del ransomware Lockbit 2.0 Mitre ATT&C:

De acuerdo a MITRE, LockBit 2.0 presenta las siguientes características generales de comportamiento de tácticas y técnicas:

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

Táctica ATT y CK	Técnica ATT y CK
Reconocimiento	• Escaneo activo - Escaneo de bloques de IP - T1595.001
Desarrollo de recursos	• Infraestructura comprometida – Dominios – T1584.001
Acceso inicial	• Aprovechar la aplicación orientada al público – T1190 • Servicios Remotos Externos – T1133
Ejecución	• Intérprete de comandos y secuencias de comandos – PowerShell – T1059.001 • Consola de comandos de Windows – T1059.003 • Instrumentación de gestión de Windows – T1047
Persistencia	• Ejecución de inicio automático de inicio o inicio de sesión: clave de ejecución del registro: T1547.001
Movimiento lateral	• Servicios remotos - Protocolo de escritorio remoto - T1021.002 • Transferencia lateral de herramientas – T1570
Impacto	• Datos cifrados para impacto: T1486 • Recuperación del sistema Habitar – T1490 • Parada de servicio – T1489

Figura 20. Características LockBit 2.0 MITRE
Fuente: Cynet

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

VI. INDICADORES DE COMPROMISO

Comandos Registrados en el Sistema
cmd.exe /c vssadmin Delete Shadows /All /Quiet Description: Deletes Shadow Copies
cmd.exe /c bcdedit /set {default} recoveryenabled No Description: Disables Win 10 recovery
cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures Description: Ignore boot failures
cmd.exe /c wmic SHADOWCOPY /nointeractive Description: This command has an invalid syntax and errors out
cmd.exe /c wevtutil cl security Description: Deletes security log
cmd.exe /c wevtutil cl system Description: Deletes system log
cmd.exe /c wevtutil cl application Description: Deletes application log
cmd.exe "C:\Windows\System32\cmd.exe" /C ping 127.0.0.7 -n 3 >Nul&fsutil file setZeroData offset=0 length=524288 "C:\Users\fred\Desktop\Lsystem-234-bit.exe" & Del /f /q "C:\Users\fred\Desktop\Lsystem-234-bit.exe" Description: Wipes and deletes itself
cmd.exe "C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no Description: Lockbit 2.0 deletes all shadow copies on disc to prevent data recovery

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:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

Registro de llaves de sistema
Creción - UAC Bypass
Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\ICM\Calibration
Value: Display Calibrator
Data: <LockBit 2.0 Ransomware path>
Creación - LockBit 2.0 Wallpaper Change
Key: HKEY_CLASSES_ROOT\Lockbit\shell\Open\Command
Data: "C:\Windows\system32\mshta.exe" "C:\Users\<username>\Desktop\LockBit_Ransomware.hta"
Key: HKEY_CLASSES_ROOT\Lockbit\DefaultIcon
Data: C:\Windows\<First 6 characters of LockBit 2.0 Decryption ID>.ico
Creación - Persistencia
Key: HKEY_CURENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{GUID}
Data: C:\Users\<Username>\Desktop\LockBit_Ransomware.hta
Data: <LockBit 2.0 Ransomware path>
Creción - Encriptación
Key: HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Private
Key: HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Public
Created - LockBit 2.0 Icon Location
Key: HKEY_LOCAL_MACHINE\Software\Classes\.lockbit\DefaultIcon
Creción / Modificación - LockBit 2.0 Escritorio
KEY: HKEY_CURRENT_USER\Control Panel\Desktop
String Value: %APPDATA%\Local\Temp\<LockBit 2.0 wallpaper>.tmp.bmp
String Value: TitleWallpaper=0
String Value: WallpaperStyle = 2

Archivos Creados
C:\Users\<Username>\Desktop\LockBit_Ransomware.hta - LockBit 2.0 hta File

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:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

C:\Windows\SysWOW64\<First 6 characters of Decryption ID>.ico - LockBit 2.0 Icon
C:\Users\<username>\AppData\Local\Temp\<LockBit 2.0 wallpaper> .tmp.bmp - LockBit 2.0 Wallpaper

Actualización de Políticas – Desactivación de Windows Defender
[General]
Version=%s
displayName=%s
[Software\Policies\Microsoft\Windows Defender;DisableAntiSpyware]
[Software\Policies\Microsoft\Windows Defender\Real-Time Protection;DisableRealtimeMonitoring]
[Software\Policies\Microsoft\Windows Defender\Spynet;SubmitSamplesConsent]
[Software\Policies\Microsoft\Windows Defender\Threats;Threats_ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\UX Configuration;Notification_Suppress]
Comando PowerShell – Forzar Políticas de GPO
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"

Comando de auto recuperación
C:\Windows\System32\cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no

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:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

Indicadores de Red
After a host establishes a connection to one of the command and control servers, a HTTP PUT request with hexadecimal value and a length of 32 or 33 characters is sent to the command and control server.
For example, PUT /06599379103BD9028AB56AE0EBED457D0 HTTP/1.1.

Ejemplo de URL Usurpada
hxxp://185[.]182[.]193[.]120/06599379103BD9028AB56AE0EBED457D

Comando de autoeliminación
ping 127.0.0.7 –n 7 > Nul & fsutil file setZeroData offset=0 length=<Stealbit file size>< Stealbit file path > & Del /f /q <Stealbit executable>

Direcciones IP involucradas			
139[.]60[.]160[.]200	93[.]190[.]139[.]223	45.227[.]255[.]190	193[.]162[.]143[.]218
168[.]100[.]11[.]72	93[.]190[.]143[.]101	88[.]80[.]147[.]102	193[.]38[.]235. [.]234
174[.]138[.]62[.]35	185[.]215[.]113[.]39	185[.]182[.]193[.]120	

Características de muestra analizada en punto: V. IMPACTO
Nombre de la muestra
9feed0c7fa8c1d32390e1c168051267df61f11b048ec62aa5b8e66f60e8083af.7z
MD5
63131241d8bbe4f64593f8f93af70a72
SHA-256
910f1c631274bac3e033b5172e12e9c007d832c8308450c6eba78eacba707377

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

VII. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es NO PAGAR el rescate.
- En el caso de sufrir un ataque de ransomware, informe el incidente a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional y al EcuCERT.
- Aislar el dispositivo infectado.
- Identificar la infección del ransomware
- Buscar herramientas de desencriptado de ransomware
- Restaurar archivos con herramientas de recuperación de datos
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de

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

toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.

- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de que la Organización/Institución se vea afectada por un ransomware, visita los siguientes enlaces; a fin de establecer un panorama de la situación: https://www.nomoreransom.org/es/decryption-tools.html#LockFile (herramientas de des encriptado en el caso de existir) / https://id-ransomware.malwarehunterteam.com/ (identificación de tipo de Ransomware y herramienta de des encriptado en el caso de existir una)
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. REFERENCIAS:

Abrams, L. (27 de 07 de 2021). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/

Alboros, J. (08 de 07 de 2021). *Protegerse*. Obtenido de Protegerse: https://blogs.protegerse.com/2021/07/28/blackmatter-y-lockbit-2-0-nuevos-actores-y-cambios-en-el-mundo-del-ransomware/

Aver, H. (03 de 08 de 2021). *KASPERSKY DAILY*. Obtenido de KASPERSKY DAILY: https://www.kaspersky.es/blog/ransomware-group-policies/25745/

DONG, C. (19 de 03 de 2022). *CHUONG DONG*. Obtenido de CHUONG DONG: https://chuongdong.com/reverse%20engineering/2022/03/19/LockbitRansomware/#anti-analysis-stack-string

Kaspersky. (s.f.). *Kaspersky*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware

Ofir, G. (s.f.). *AppSec*. Obtenido de AppSec: https://appsec-labs.com/portal/protecting-a-windows-application-from-premature-termination/

Nro. Alerta:	EC-2022-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	5-abril-2022	**Campaña de Ransomware LockBit 2.0 presente en Ecuador**	V 1.5

Total, V. (22 de 03 de 2022). *Virus Total*. Obtenido de Virus Total: https://www.virustotal.com/gui/file/910f1c631274bac3e033b5172e12e9c007d832c8308450c6eba78eacba707377/detection

VX-Underground. (22 de 02 de 2022). *VX-Underground*. Obtenido de VX-Underground: https://samples.vx-underground.org/samples/Families/LockBitRansomware/Samples/

Matan Haim Guez. (01 de 02 de 2022). *Cynet*. Obtenido de Cynet: https://www.cynet.com/attack-techniques-hands-on/malware-evolution-analyzing-lockbit-2-0/

Tomas Meskauskas. (30 de 03 de 2022). *PCrisk*. Obtenido de PCrisk: https://www.pcrisk.es/guias-de-desinfeccion/10926-lockbit-2-0-ransomware

Ciber División FBI. (04 de 02 de 2022). *Ciber División FBI*. Obtenido de Ciber División FBI: https://www.ic3.gov/Media/News/2022/220204.pdf

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