



Malicious Application Targets MapInfo Professional

MapInfo Corporation has confirmed the existence of a malicious application written in MapInfo MapBasic[®] language that targets MapInfo Professional[®] versions 5.5 or higher and MapInfo Professional-based applications. This application has the potential to corrupt data used in MapInfo and spread to other MapInfo Professional users who share that data. It does not harm operating systems or other non-MapInfo/MapBasic-based programs.

This document provides information about the program and its potential effects on your system and data. It also provides information about how you can detect if your system has been infected and recommended courses of action to remove it. This document covers the following key areas:

- [How can I receive this malicious program?](#)
- [How does my MapInfo Professional and data become infected?](#)
- [How does this program spread?](#)
- [What is the potential impact of this program?](#)
- [How can you tell if your system is infected?](#)
- [How to clean/remove the application](#)
- [How to avoid becoming infected](#)
- [What is MapInfo doing about this issue?](#)

How can I receive this malicious program?

MapInfo Professional users can get this application in one of the following ways:

1. ***Downloading and executing*** MapBasic applications inside MapInfo Professional that come from ***questionable sources***.
2. ***Downloading and opening*** altered TAB files from unknown or ***questionable sources***.

Applications written in the MapBasic language can only run inside of MapInfo Professional or in an application built on MapInfo Runtime technology. Systems that are not running these programs cannot be affected.

How does my MapInfo Professional and data become infected?

A MapBasic application runs inside of MapInfo Professional via a "Run Application" statement. This statement is executed by the menu option "Run MapBasic Program." The same statement can be embedded in another MapBasic program or MapInfo Professional workspace. In the case of this infecting application, the creator used standard MapInfo functionality by altering a MapInfo .TAB file and MapInfo WOR file that are capable of executing MapBasic commands.

A MapBasic application can also be run by double clicking the file in Windows Explorer. In order for your system to be infected, either you or someone in your organization must have either been sent the application or the set of files that make up a MapInfo TAB set with the program masking itself as a .MIF file.

How does this program spread?

This program tries to guarantee its effectiveness by writing the "Run Application" statement into the "Startup.WOR" file. This file is an optional standard workspace file that MapInfo Professional will look for and execute automatically when MapInfo Professional starts.

When the program runs, it copies itself to the MapInfo Professional program directory under the name "0gPiSs1.dll." Note that this file is not a Windows DLL. It is the malicious program. It then creates a Startup.WOR file with the statement **Run Application "0gPiSs1.dll."** so that every time you start MapInfo Professional, the malicious program runs.

Once the program is running inside MapInfo Professional, it will attempt to replicate itself by writing the "Run Application" statement to other open TAB files. If these files are shared among users, the program can spread to their installations of MapInfo Professional. This can also happen when the files that are infected and shared are opened in MapInfo Professional.

At times the program may attempt to copy itself to the same directory of any open TAB file, disguising itself as a .MIF file with the same base name as the .TAB file. For example: If you had a file called my_customers.TAB open during the session, the program will copy itself to the my_customers.TAB directory and will name itself my_customers.MIF.

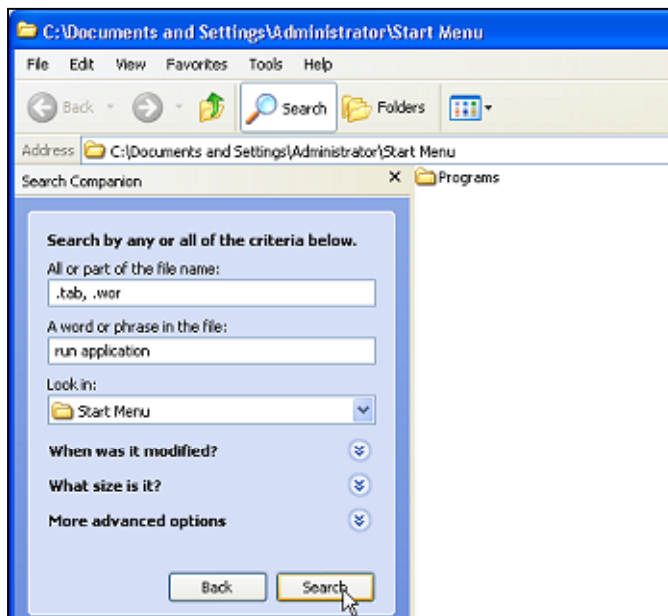
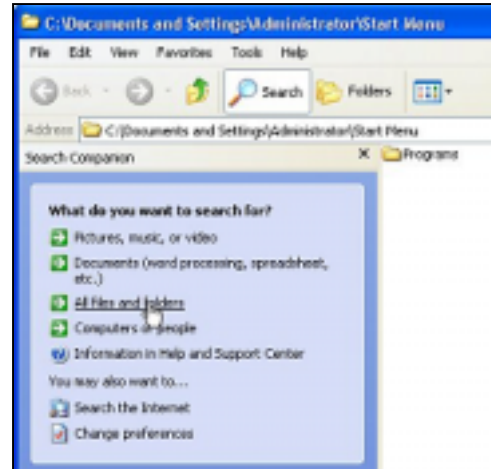
What is the potential impact of this program?

The program's most destructive potential is its occasional attempt to delete .MAP files, which hold the geographic data in a MapInfo table, and also certain raster image files associated with MapInfo TAB files. It attempts to do this on Mondays and on Friday the 13th, but only when a random number function returns certain values. Thus the destructive behavior is somewhat hard to predict.

How can you tell if your system is infected?

The following simple test will reveal if your files/application has been infected with this application.

1. Open Windows Explorer and click the search icon.
2. Click on All Files and Folders.
3. Search for all .TAB and .WOR files that contain the phrase “run application” in all drives where you store MapInfo Professional programs and data.
4. If no results are found, your computer is safe from this program.
5. If the search returns results, carefully examine the content of the files, specifically the “run application” statement. If the application statement is followed by *somefile.MIF* or a *somefile.DLL*, there is a high likelihood that it is the malicious application.



How to clean/remove the application

If you positively confirm the existence of the malicious MapBasic application, we recommend the following process to remove it from your system:

1. **Identify all infected locations and files.** Make sure you search all your possible locations including network drives and other MapInfo Professional users and their systems. If you have backup tapes of .TAB and .WOR files check them as well.
2. **Remove the "Run Application *somefile.MIF* or *somefile.DLL*" statements** from .TAB files.
3. **The malicious program may be hiding as a .MIF file** in the same directory under the name that is referenced in the run application statement. That file should be deleted.
4. **Remove Run Application statement from Startup.WOR**
Find Startup.WOR and remove "Run Application 0gPiSs1.dll." If this is the only statement in startup.wor, delete Startup.WOR from your system. Delete 0gPiSs1.dll from the MapInfo Professional program directory, as it is not a true .DLL, but a renamed infecting MapBasic application.

How to avoid becoming infected

As with any other programs, we strongly recommend that you avoid downloading and executing applications and data from unknown origins. MapInfo Professional is a feature rich and highly customizable environment offering great flexibility and customizability to our customers. With great flexibility, however, comes the possibility of users developing programs that leverage this capability for destructive purposes.

What is MapInfo doing about this issue?

MapInfo Corporation has taken several proactive steps to ensure the safety and security of MapInfo Professional and MapInfo Professional Runtime:

- MapInfo has contacted our partners and passed along this information.
- MapInfo has contacted key anti-virus product providers, such as McAfee, and passed this information to them as well. We anticipate that future versions of their products will contain detection information for this malicious program.
- MapInfo Corporation will be looking into enhancement possibilities of future versions of MapInfo Professional to alert users when programs are being run automatically, and possibly without their knowledge.

Should you have any questions, please contact MapInfo Support at techsupport@mapinfo.com