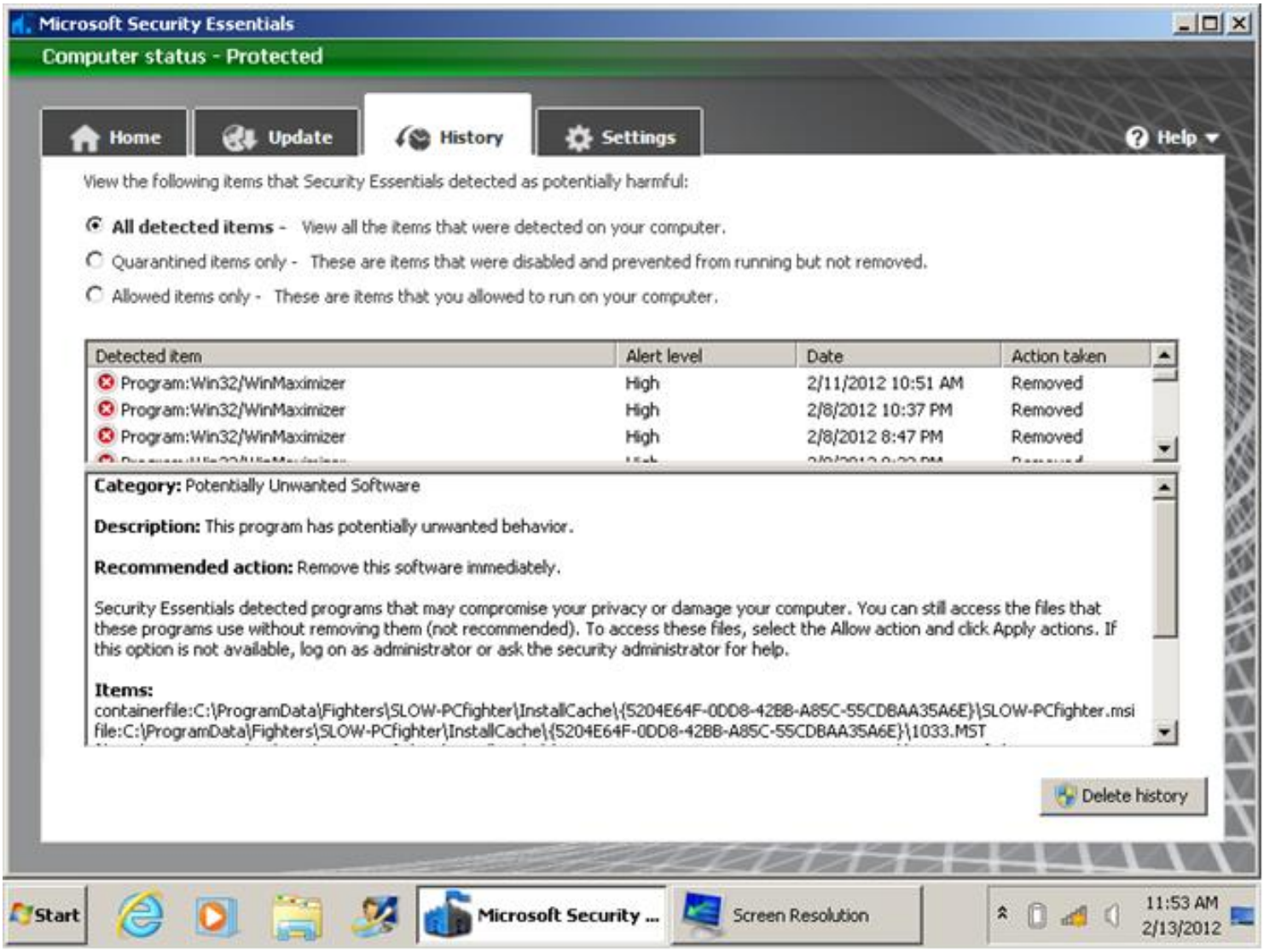
REMOVAL OF "Win32/WinMaximizer" FOR A "WINDOWS 7" COMPUTER

SUMMARY:

A "Windows 7" netbook was infected with "Win32/WinMaximizer" and some discussion group gurus provided us with a fix on February 4, 2012.

A RECALCITRANT MALWARE INFECTION

A computer running "Windows 7 Starter" was running "Microsoft Security Essentials" as its antivirus/antimalware software program. "Microsoft Security Essentials" was up to date. However, it repeatedly stated that the computer was infected with "Win32/WinMaximizer". This notice would pop up in the "Notification Area" within 2 minutes of the bootup of the computer. The notice had a "Clean" button. When the end user clicked on the "Clean" button, "Microsoft Security Essentials" would then claim that the problem was removed. Then it would ask the end-user to reboot the computer. When the computer was rebooted, this sequence of events would repeat itself.



Initially, three computer instructors, Francis, Liz, and Mari, thought that this computer was infected with a rootkit, since many rootkit infections exhibit this level of stubbornness. Mari used forensic software on a USB flash drive to determine that at least one suspicious file resided on the root directory of the netbook's flash drive.

DETAILS ABOUT "Win32/WinMaximer"

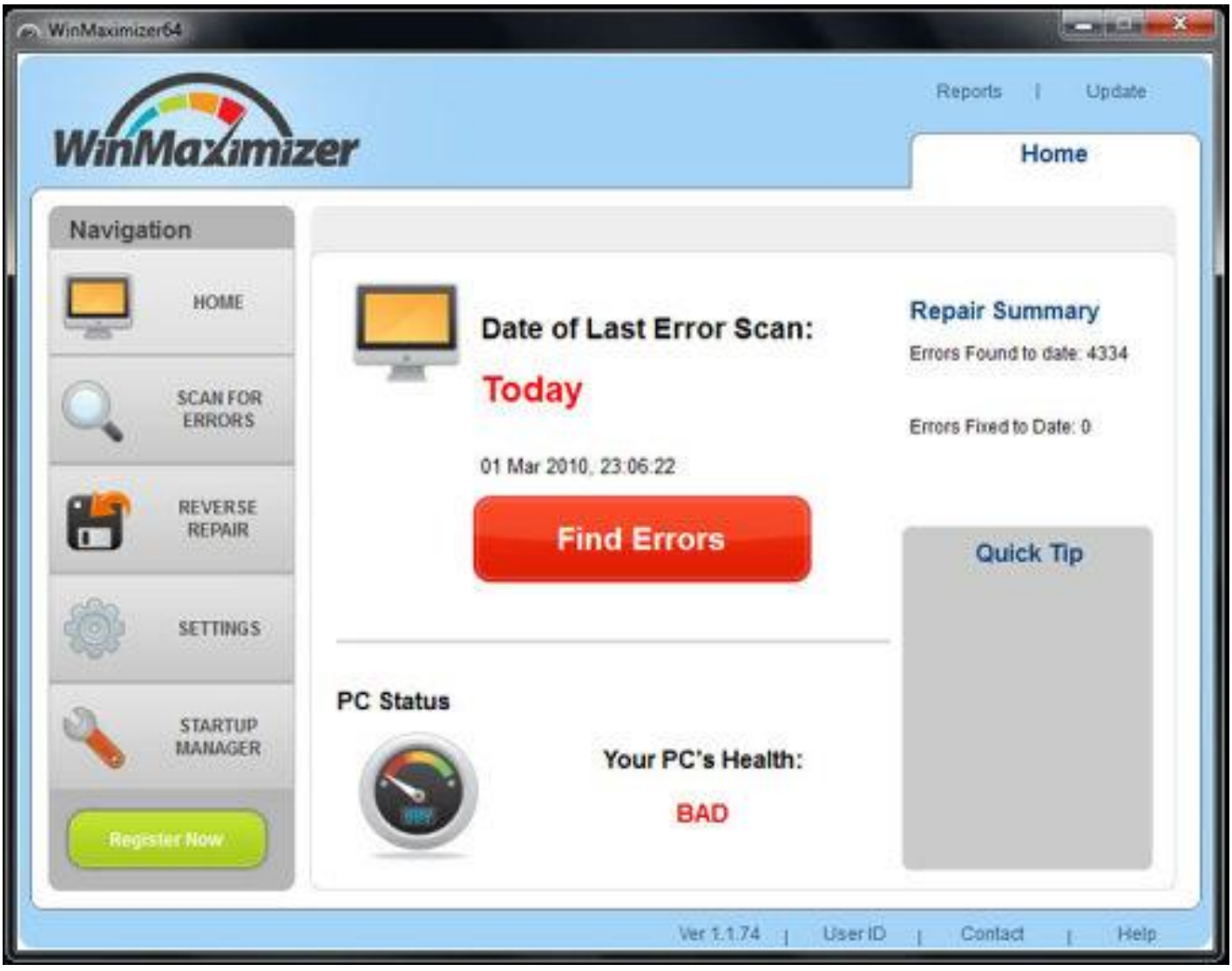
The best description of this malware can be found at

http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Program:Win32/WinMaximizer&ThreatID=167852
In this Web page, Microsoft erroneously claims that "Microsoft Security Essentials" can expunge the malware.

The information at
http://virusremovalhelps.com/help-win32winmaximizer-virus-removal/
was not helpful and there is a possibility that this page is an attempt to sell some "extortionware" rogue software to panicked, gullible end-users.

The information at
http://blog.teesupport.com/permanently-remove-win32winmaximizer-manual-removal/
was informative but the suggested steps for removal failed to work.

When the "payload" action of "Win32/WinMaximizer" triggers, it looks like this:



We never saw this so we surmise that it triggers at a date after the initial infection of a Windows computer.

CLEANUP ATTEMPTS

The end user ran unsuccessful scans with the following antivirus/antimalware tools:

Microsoft Security Essentials
MalwareBytes AntiSpyware Free
SuperAntiSpyware Free Edition
Rootkit Revealer
Sophos Anti-Rootkit
GMER

We ran the above software tools in Safe Mode also.
We also ran
ESET's Free Online Scanner-.
These scans were also unsuccessful in removing Win32/WinMaximizer.

GETTING GOOD ADVICE FROM THE INTERNET

We went to Google.com and search on
remove Win32/WinMaximizer
The following "hit" was on the first page of results:

http://answers.yahoo.com/question/index?qid=20120205093001AAcixFo
At this page, an anonymous discussion group participant with the handle of "AnyDayAnyTime" stated that the solution is to remove two folders, both named "Fighters".

We found and deleted two folders named
Fighters.

One was located in
C:\ProgramData

and the other was located in
C:\Program Files.

Both folders contained some strange-named files inside them.

We ran
regedit
and deleted two registry keys that contained "Fighters" in them.

We rebooted the computer and re-ran all of the above-mentioned antivirus/antimalware software utilities. The computer received a clean bill of health from all of these utilities.