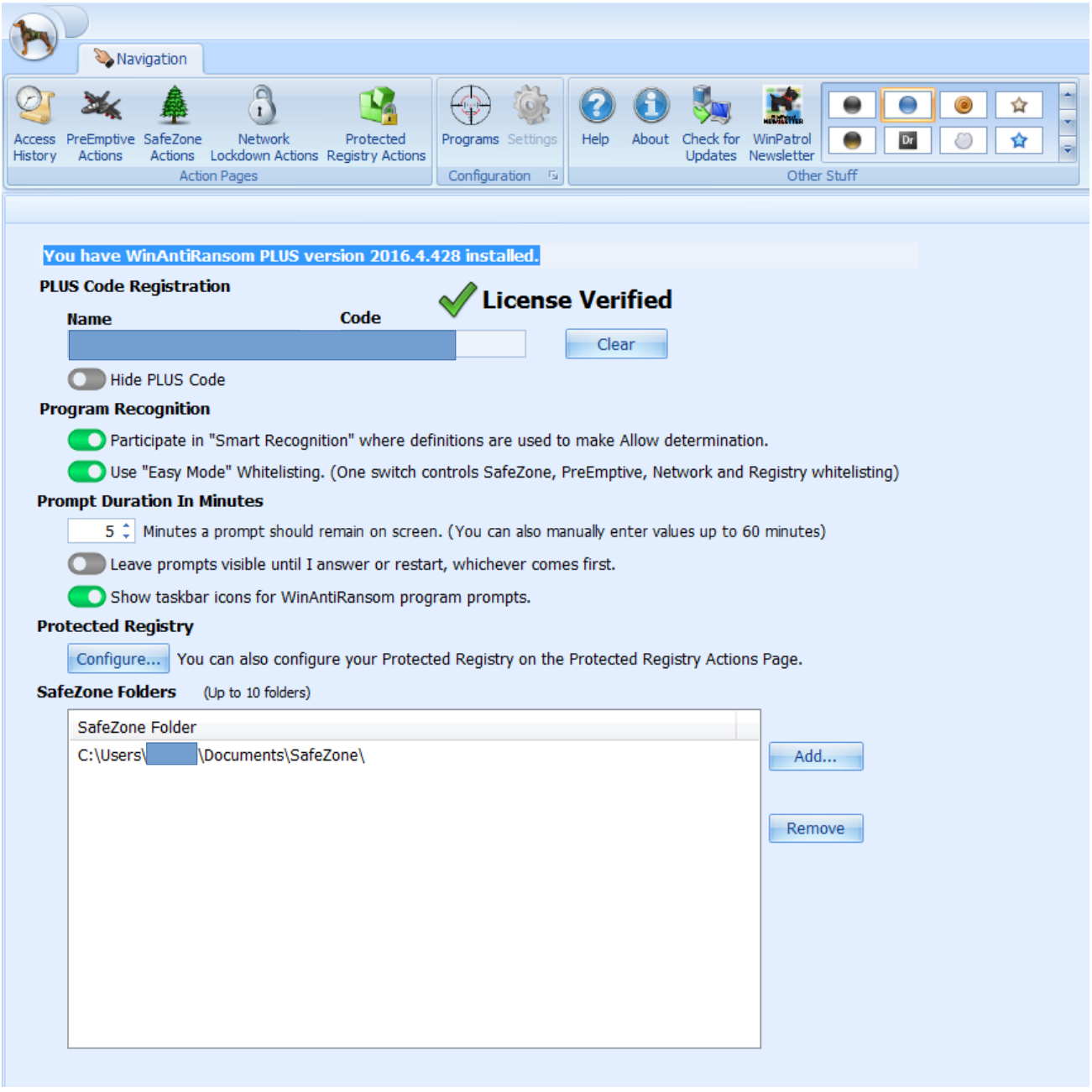
Review Of WinAntiRansom Plus (WAR) - reviewed by Nathan Stokes (Natronics)

During this last week and a half I have been carrying out testing on WinAntiRansom Plus software, starting with version 2016.4.418 and moving to the current version 2016.4.428. The company who produces this software has been working since last year on a solution to the ransomware threats. This software is meant to supplement a good virus/malware suite by using a combination of white-listing, intelligent behaviour analysis, registry key protection, and safe zone for data files

The software install is very quick approx. 1 minute and takes up only 250KB when running. The main components run as a service on Windows load. There was a problem with these services loading properly in Win10 but this has been corrected in this latest version.

My testing mainly was carried out on a Win7 and XP environment.



After installing, the program automatically scans the PC for known good programs which are white-listed, this process took 90 seconds to complete on my test system with 53 programs installed.

You do have the choice to forgo the ‘easy mode’ automatic white-listing scan and smart recognition and may white-list your own programs manually. In the case of some unknown good software on first execution and subsequent alert it can easily be accepted and therefore also white-listed.

For instance in my case on my test it was MYOB Premiere accounting. What was particularly good to see was the retention of this amended white list log after complete unistall and reinstall of a new version, saving the inconvenience of re training.

The top panel gives you a file access history, List of all Pre-emptive Actions – files that are stopped from execution – they can be white-listed from here if a mistake in identification is made.
The Programs icon lists all running files – these can be analysed or stopped from this window.

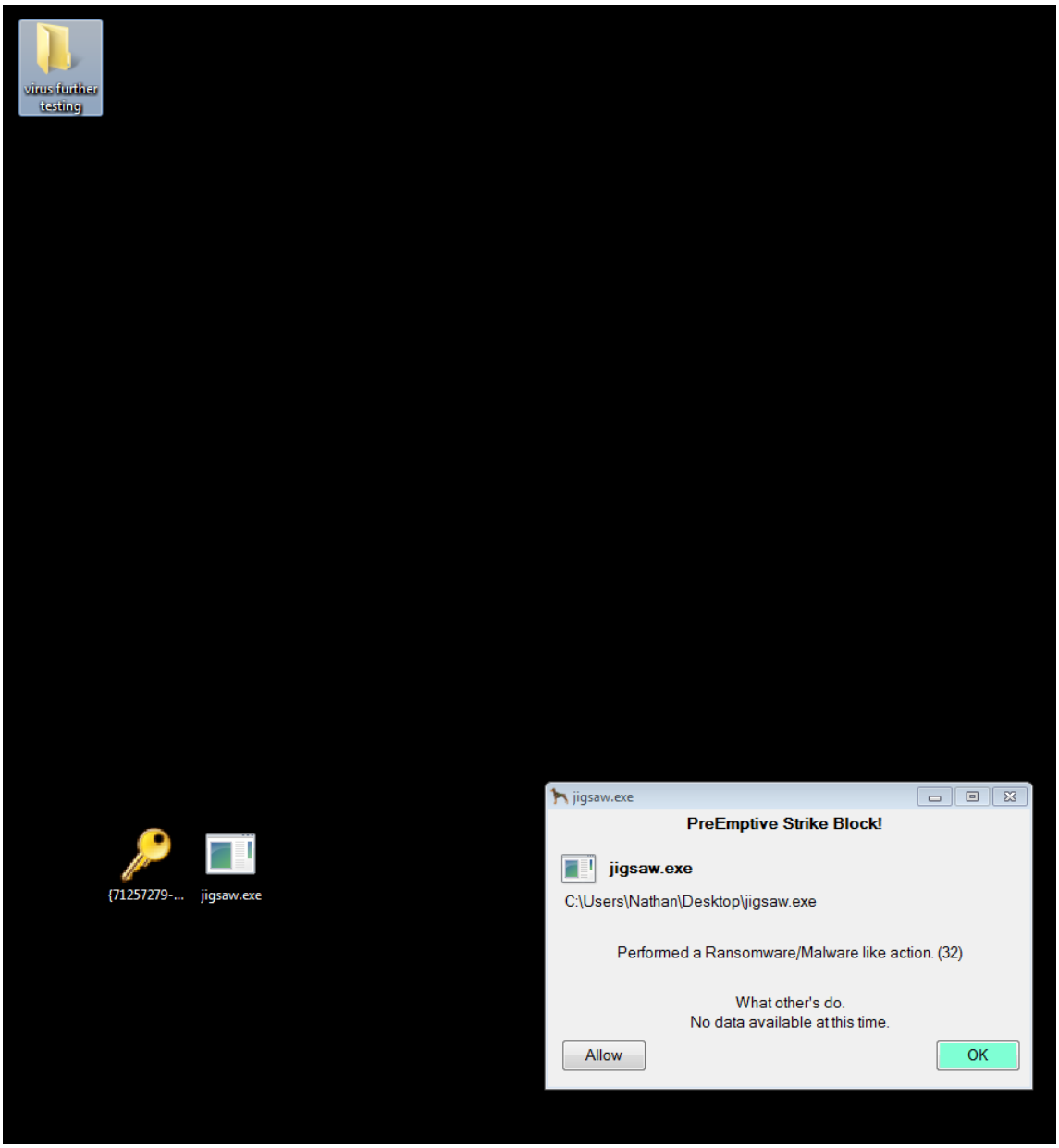
In the new version 4.4.428 the update function has been made much more streamlined and the number of known white-listed software has been increased – including MYOB now being white-listed.

WinAntiRanson Plus automatically protects hundreds of system critical registry keys, in addition to that you can further enhance this protection by selecting individual registry keys to block changes in, block other known bad programs and utilising special designated folder/s (up to 10) which are protected from change (can only be used for data – no programs and cannot be a system designated folder i.e. My Documents). During testing of malware samples I did not add any extra settings just left it standard in easy mode.

The automatic mode of running the software is very effective as the following detection results show:

Malware Name	**Result**
Teslacrypt	32
Locky	65
Jigsaw	32
Zerolocker	71
Matsnu	19
Petya	71
Radament1	82,83
Radament2	82,83
Vipsana	5,81
Vipsana2	5.81
Cryptolocker1	18
Cryptolocker2	18
Cryptolocker3	71 71
Cryptolocker4	71
Backdoor.Win32.Tyuokin/Backdoor.MSIL	65
Spyeye	5
Trojen.Dropper.Gen	61
Stuxnet	100
Zero Access	1

Zero Locker	71
Zeus Banking Version	1
Cerber.B	71
Files not detectable by direct scan or resident protection Eset Smart Protection v9	
shylock	100
Win32.Boaxxe.BB	68
Trojan.Win32.Bechiro.BCD	13
KRBanker	84
Artemis	68



The screen capture above is indicative of the normal pop-up occurring when malware/ransomware files are attempted to be run. Only the number in brackets change depending on why it was stopped. I did note that on a few of the samples multiple pop-ups occurred – no extra processes were spawned from these instances.

While executing the ransomware tests the CPU usage rose to a maximum of 60 percent for a few seconds and only when responding to a threat.

I experimented with changing the names of the ransomware file to white-listed one's like mbam.exe and still the file was blocked from executing.

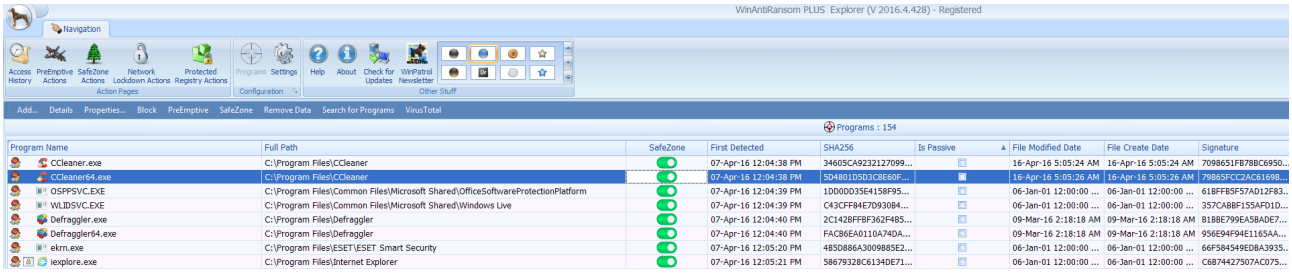
Of particular interest were 5 malware samples which eset smart did not detect after scanning the folder. These items were stopped from executing by WAR.

Network Lockdown

After my initial testing I became aware of another very powerful feature of WinAntiRansom Plus. WAR has a default behavior of restricting network access to programs which are whitelisted. Any new network shares or network storage can not be accessed by unknown programs thus reducing the ability of malware to make changes such as encryption of these areas.

If you deactivate Easy Mode you will see a column for each layer of security (shown below).

By default, in easy mode, if you whitelist a program all 4 settings are set. If you de-whitelist the program all 4 settings are unset. It is possible to remove any network access to any file from here.



As this protection covers any new shares, be it via wifi or wired **without intervention by the user** I consider it is another very powerful layer of protection especially where network storage is part of a backup routine.

Summary

With regard to blocking ransomware the software has proven itself to be one of the best products available in its effectiveness – not only by my tests but in comparison tests carried out by others. Whilst you definitely need to use a good antivirus package in conjunction with this layer of protection, doing so gives you far more coverage against the running of malicious files be they ‘ordinary malware‘ or more importantly ransomware.

Just as a side note with regard to support. During the initial version installation I requested help in solving an issue and was responded via email within 24 hours. Taking into account that I live in Australia that’s a great turn around.