www.foolishit.com/vb6-projects/cryptoprevent/

lxquick

About How I Quit Ci

Blog Tech Info Forums Reviews Press Buy Something Now Get Notified

d7

- d7 Free
- d7 Premium
- License
- Revision History (v10+)
- Revision History (-> v9)
- To-Do List
- Online Manual
- Video Tutorials

CryptoPrevent

Current Version: 3.0

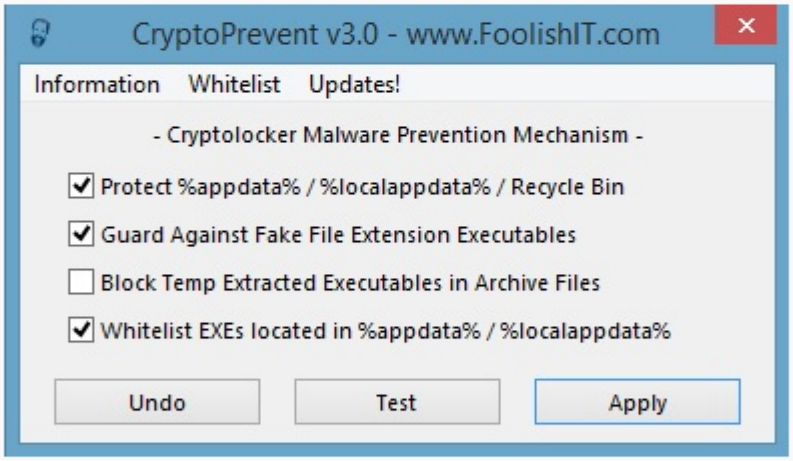
CryptoPrevent is a tiny utility to lock down any Windows OS (XP, Vista, 7, 8, and 8.1) to prevent infection by the Cryptolocker malware or 'ransomware', which encrypts personal files and then offers decryption for a paid ransom.

CryptoPrevent seeks to alleviate these issues in allowing protection on ALL Windows OSes, while being easy enough for the average Joe to do, and optionally providing silent automation options for system admins and those who need to immunize a lot of computers automatically.

CryptoPrevent is a single executable and is fully portable (of course unless you download the installer based version) and will run from anywhere, even a network share.

The User Interface

The User Interface allows you to select to apply the blocks to executable files as listed under Prevention Methodology below. You may also automatically whitelist all EXEs located in %appdata% / %localappdata% and first level subdirectories. There also exists an Undo feature, and a Test feature, a Whitelist Options dialog allowing you to selectively whitelist individual items, and a feature to automatically check for and apply updates to the application itself.



Prevention Methodology

CryptoPrevent artificially implants group policy objects into the registry in order to block certain executables in certain locations from running. The number of rules created by CryptoPrevent is somewhere between 150 and 200 rules depending on the OS and options selected, not including whitelisting! **Note that because the group policy objects are artificially created, they will not display in the Group Policy Editor** on a Professional version of Windows — but rest assured they are still there! Executables now protected against (starting with v2.6) are *.exe *.com *.scr and *.pif, and these executables are blocked in the paths below where * is a wildcard:

Protection does not need to be applied while logged into each user account, it may be applied only once from ANY user account and it will protect all user accounts on the system.

The Test Feature

When using the test feature, you are first presented with a dialog of simple success or failure. What actually happens is a temporary executable is extracted to %appdata% and the test feature attempts to launch it, if the launch fails then the prevention is successful. If the launch succeeds the temporary application silently returns errorlevel 9 back to CryptoPrevent to alert it that the app was successful in launching and the prevention has failed.

NOTE: Versions prior to v1.3 did not alert when the prevention was successful, only if it failed – this is explained in a dialog box which pops up prior to the test in those versions.

Whitelist Options

There are a handful of legitimate executables that developers have poorly decided to put in these locations, and the most popular seems to be 'Spotify' though there also there are a few remote support applications as well that can run from these locations. Due to this CryptoPrevent v2 comes with a whitelist editor and capabilities. From here you can view whitelisted items and add your own manually or via browse button, and also you may choose to automatically whitelist all items currently located in %appdata% / %localappdata% and their first level subdirectories. Note that manually entered whitelist items may NOT contain wildcards.

Undo

You may undo the protection at any time by using the Undo button in the main interface. You are given the option in v2.x to also undo the whitelist policies, selecting no will undo the protection only. Note that actually removing the protection is not consistent behavior. In my testing, when removing the protection sometimes the change is instantaneous, while other times a reboot is required just like applying the policies in the first place, and on rare occasion a group policy update is required, then a reboot. Windows is funny that way and there seems to be no way to predict this behavior. v2.1.1 now runs **gpupdate /force** after the Undo features to ensure group policy is refreshed, and then protection is tested for again to determine if a reboot prompt will be displayed.

License

CryptoPrevent is completely **FREE** for personal **and** commercial usage. If you would like to give a little something for it, consider purchasing the Automatic Updates service for CryptoPrevent!

Download the portable version below:

Download "CryptoPrevent"

CryptoPrevent.zip – Downloaded 30347 times – 402 kB