|  |  |
| --- | --- |
|  | SmartFileExtract Forensics and Exfiltration  GNU General Public licensed security utility  Find files by pattern and keyword and extract to a specified location. Optionally stop copy after *n* seconds and / or *n* MBs. Stealthy status windows may be used as necessary.  [saintcrossbow@gmail.com](mailto:saintcrossbow@gmail.com) |

Smart

File

Extract

What is it?

The SmartFileExtract is the copy utility you wished you had when you have had to rely on scripting. Yes, you can find patterns and copy to a location, but you can also use additional features:

Find keywords in any file.

Use “curtains” that either show standard progress, no window, or stealthy windows that are either inconspicuous or look like an Install Window.

Best of all, stop the copy after a specified time or amount of MBs have been copied. If you use for security reasons, you will no longer have to worry if your extract will cause an error by filling up the USB (or unplugging the USB prematurely).

Why would I use it?

The main uses cases include:

* Find files for backup
* Audit PCs for security risk
* Extract using Bash Bunny in security testing
* Acquire forensics data right under hostile party’s noses
* General file management usage

I’m certain there are additional uses that anybody would find.

How do I counter it?

This is not exploiting a vulnerability – if anything this is for post exploitation for pen testing.

So how does it work?

Smart File Extract takes several arguments that are obvious, such as the file pattern to find, the drives to seek, and where to copy the extract. Optionally a keyword may be specified (which will slow down the search). For stealth, *curtains* may be used - mocked up screens that give you the status of the copy without showing what you are doing. To further control your copy:

* Total MBs to act as a threshold past which no other files will be copied
* Total seconds to perform the extract, after which the copy will be killed
* Performance style tuning: a copy may be made intense (possibly making even screen updates not show) or slow-and-low, delaying copies to for a long but stealthy extract

Why would you even create something like this?

I wanted it specifically for use on my Hak5 Bash Bunny. I liked the extract option, but wanted to make something a little stealthier that I could monitor the status, and also feel OK unplugging it if I know the copy is definitely done.

Could I be used for evil?

Sure, but shame on those that do that for two reasons: 1) obviously it’s unethical; and 2) there are more devious tools out there than Smart File Extract that can actually cause significant damage. This is not an exploitation tool for evil usage but for white hat pen testing. If you do use it for evil, just remember karma does find you, and often someone witnesses it happening for additional embarrassment.

How do I run it?

Start the Smart File Extract tool on the command line with /help to see the available options. To run an extract, just specify the options needed (the file pattern, copy to location, and drives to search are required at minimum).

How do I customize it for my use?

Smart File Extract was written in C# and was designed to be extended. The curtains use a common interface – just add a new one as needed.

The code has been documented clearly to show what it is doing and why it is doing it. If you are new to C#, links are included where appropriate, and there are good examples on how to use some C# concepts that some might consider difficult.

Can you add *x* feature or answer *y* question?

The answer is probably yes, but I have done this in my spare time when I am not working, not being a parent, and not having fun in other areas. Email [saintcrossbow@gmail.com](mailto:saintcrossbow@gmail.com) or follow the project on <https://github.com/saintcrossbow/SmartFileExtract/>.

What’s up with the name SaintCrossbow?

Most of it is because it wasn’t taken. Other than that, I’m a big fan of the literary Saint by Leslie Charteris: a vigilante type who very kindly takes on problem people, serves his own justice, and has a great deal of fun doing it. Also, I just can’t help but think that crossbows are cool.