|  |  |
| --- | --- |
|  | SmartFileExtract Forensics and Exfiltration  GNU General Public licensed security utility  Find files by pattern and keyword, then extract them to a specific location. Optionally stop copy after *n* seconds and / or *n* MBs. Stealthy status windows included for covert extraction.  [saintcrossbow@gmail.com](mailto:saintcrossbow@gmail.com) |

Smart

File

Extract

What is it?

SmartFileExtract is a find-and-copy utility written specifically for the Hak5 BashBunny but also is usable as a standalone utility. Files are found by standard patterns (including wildcards) and then copied to any valid path. Additional features:

* Find by seeking keywords in any file.
* Use “curtains” that show standard progress, no window, or stealthy windows that are either inconspicuous or look just like a regular install window.
* Best of all, stop the copy after a specified time or amount in MBs has been copied. If you use the utility for security reasons, you will no longer have to worry if your extract will cause an error by filling up the BashBunny or USB (or unplugging the device prematurely).

Why would I use it?

The main uses cases include:

* Extract using the Hak5 Bash Bunny for security testing.
* Find files for backup.
* Audit PCs for security risks.
* Acquire forensics data right under hostile party’s noses.
* General file management usage.

How do I counter it?

SmartFileExtract is not exploiting a vulnerability – if anything, this is for the post exploitation phase during pen testing.

So how does it work?

SmartFileExtract runs from the command line using three mandatory parameters: the file pattern to find (/file), the drives to seek (/drive), and where to copy the found files (/copyto). Optionally a keyword may be specified – but be aware it will slow down the search (/keyword). For stealth, *curtains* may be used - mocked up screens that give you the status of the copy without showing what you are truly doing (/curtain). To further control your copy, additional optional parameters include:

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

What kind of curtains are included?

For the first iteration of this utility, I have created four:

1. Progress (option 0): a standard progress window that just shows the status of the copy. Phases are displayed as *Initialize, Discovery,* and *Extract* – so even those not familiar with security procedures might get suspicious if they see it in progress. Press the **Kill** button to stop the copy.
2. Quiet (option 1): show no form and only stop the copy after it is complete or if a threshold has been met.
3. Stealthy (option 2): show a transparent form on the top right that shows the status in dots:

* 1 dot = Initialize
* 2 dots = Finding targets
* 3 dots = Copying

Abort the extract by double-clicking the dots.

1. Fake install window (option 4): a window will display indicating that new hardware has been found. Status is reported by:

* *New hardware found* = Initialize
* *Finding compatible drivers…* = Finding targets
* *Installing driver…* = Copying files

Click **Cancel** to stop the copy.

Can you give me some examples of usage?

Absolutely.

* Find all instances of a file named password or secret on the d drive and copy it to a shared network location:

smartfileextract /drive d /file password\*.\*;secret\*.\* /copyto n:\secretnetworklocation

* Find secret.doc on c: and copy to current directory while looking like an install window:

smartfileextract /drive c /file secret.doc /copyto . /curtain 3

* Find all pictures on c: and copy to a USB on e: and kill the copy after extracting 500MBs:

smartfileextract /drive c /file \*.jpg;\*.jpeg /copyto e:\loot /maxmbs 500

The BashBunny script that I use is the one included on the distribution – look at the e.cmd file which will show it finding all documents and any filename with the word “secret” or “pass” in it and copy it to the Bash Bunny’s loot file. It will kill the extract after 90 seconds or after 500 MBs are copied.

Why would you even create something like this?

I wanted it specifically for use on my Hak5 Bash Bunny. I liked the extract options people had made, but wanted something a little stealthier that I could monitor the status of the extract.

Could it 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 SmartFileExtract 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 SmartFileExtract 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?

SmartFileExtract 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 do 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.