

## Forum:[Hack Forums](#)

Thread: [Trick to make a Runtime Crypter work without a RunPe](#)

**pr0t0typ3** - March 25, 2011, 10:43 am

Hey guys,

Basically I found a "exploit" which does allow something cool and I want your opinion:  
You have a Scantime Crypter which does drop the crypted malware.

This Crypter does write one Registry Key before dropping the file.

The Scantime Crypter does drop the file and execute it.

No Anti-Virus Guard will pick it up until the victim does directly scan the file because of the Registry Key.

I tested it on Avira Anti-Vir and Kaspersky and I'm currently checking if it does work with the heuristic engines of the AVs, but yeah what do you think. Should I sell it ? It would make all RunPEs unnecessary.

**hxkd** - March 25, 2011, 10:44 am

A trick like that would not last very long, and you just more or less told us how to do it (well, I guess we would need the location) but hell yeah, don't share stuff, sell it, too many leechers.

hxkd

**pr0t0typ3** - March 25, 2011, 10:55 am

(Mar 25, 2011 10:44 AM)hxkd Wrote: [\[CITE\]](#) A trick like that would not last very long, and you just more or less told us how to do it (well, I guess we would need the location) but hell yeah, don't share stuff, sell it, too many leechers.

hxkdThe Registry is big and you would need the location to make it work but yeah I don't think I'll share it

**hxkd** - March 25, 2011, 11:05 am

How on Earth did you find this though? :O

hxkd

(Mar 25, 2011 10:55 AM)pr0t0typ3 Wrote: [\[CITE\]](#) The Registry is big and you would need the location to make it work but yeah I don't think I'll share it

**Xenon** - March 25, 2011, 12:08 pm

If you sell it, I will buy it in a heartbeat.

**New Age Griefing** - March 25, 2011, 1:25 pm

I definitely recommend that u sell it

**D??M!** - March 25, 2011, 1:35 pm

Keep it for yourself and sell a crypter here, but keep sales limited.

**Kill?Muvz** - April 16, 2011, 2:08 am

Packers? :3 IF it is what I think you'll understand what I just said <3

**Supreme Kai** - April 16, 2011, 2:18 am

Sell it you will get alot of customers.

**narutorine** - April 16, 2011, 9:27 am

sell it but limited customers that's my opinion nice work :)

**wacked3** - April 16, 2011, 9:36 am

(Mar 25, 2011 10:43 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Hey guys,  
Basically I found a "exploit" which does allow something cool and I want your opinion:  
You have a Scantime Cryter which does drop the crypted malware.

This Crypter does write one Registry Key before dropping the file.

The Scantime Crypter does drop the file and execute it.

No Anti-Virus Guard will pick it up until the slave does directly scan the file because of the Registry Key.

I tested it on Avira Anti-Vir and Kaspersky and I'm currently checking if it does work with the heuristic engines of the AVs, but yeah what do you think. Should I sell it ? It would make all RunPEs unnecessary. This trick isn't new and will not work! Avirar for example checks all files and immadently ditches files that don't start with "MZ" (marking a Portable Executable)

Also it will make no effect to any AV with behaviour blocking (which could be considered a form of heuristics)

The registry key (HKEY\_CLASSES\_ROOT\ ) has been known for years.

**Mater™** - April 17, 2011, 6:03 pm

Loll ! i need a crypter for 64bit i give 50\$ :O quessy95@hotmail.com

**Taserz** - April 17, 2011, 6:21 pm

once one av see a reg write it will then associate it as malware.

**pr0t0typ3** - April 17, 2011, 9:37 pm

(Apr 17, 2011 06:21 PM)Taserz Wrote: [\[CITE\]](#) once one av see a reg write it will then associate it as malware.

Uhm no ?! 90 % of all applications do write to the registry which does not mean they are maleware

-.-