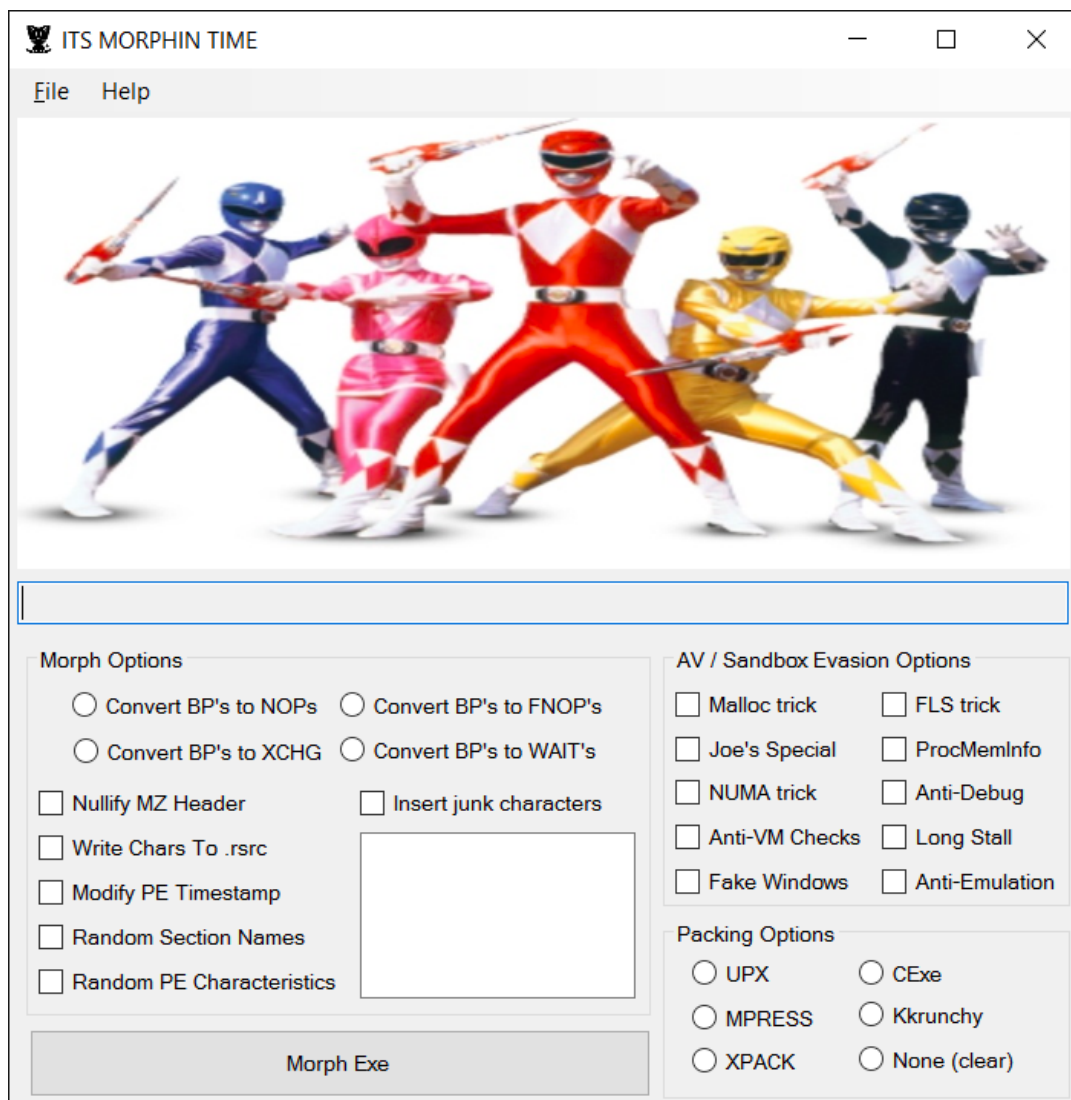


Joe's Security Blog

Dec
22
2015

JoeCrypter finally released

Finally, I'm done with this my crypter. I've written the entire thing in a mish mash of C#, C, and assembly.



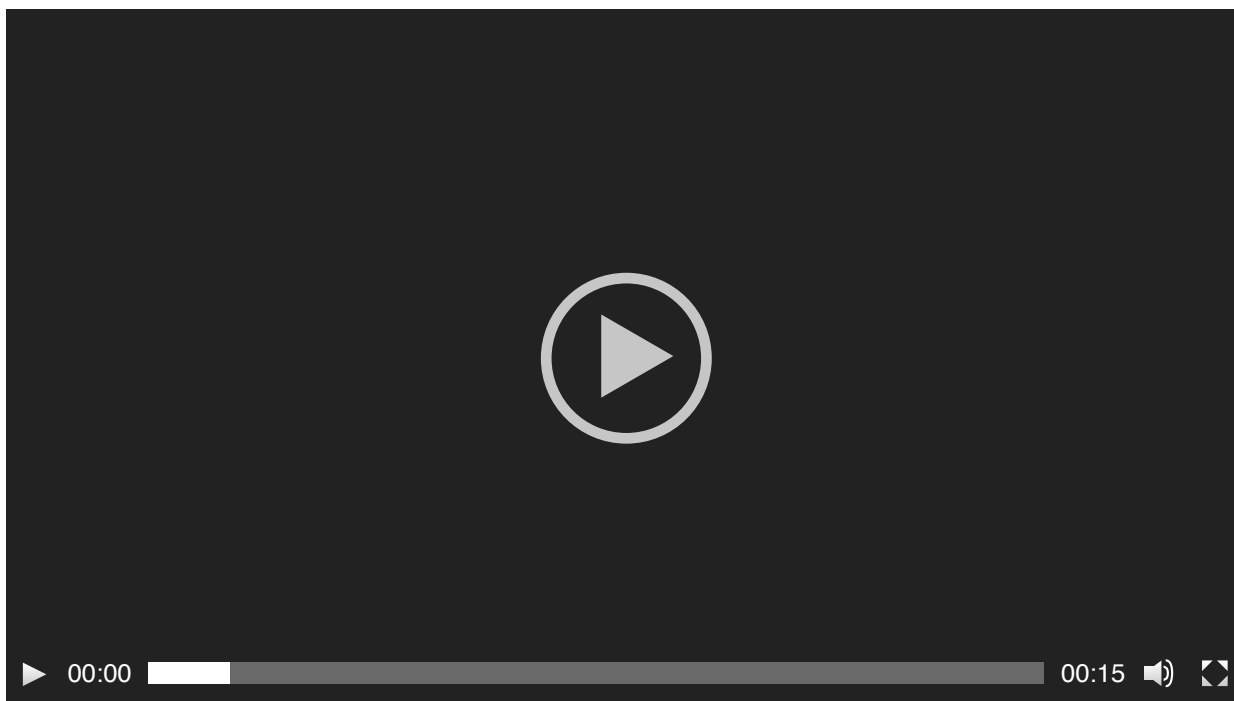
The crypter I made modifies exes, packs them, and adds AV / VM / Sandbox / debugging evasions inside of a wrapper. I'm employing a basic process hollowing technique for the payload that is only run after all evasions are satisfied. The anti-

debug modules include anti-single stepping as well as anti-tracing. I can even detect procmon without checking the process list.

The front end is in C# and that performs the rudimentary exe modifications and packing, however the real meat and potatoes is in the back end. The back-end compiler is [Pelles C compiler](#) and the evasions are coded in C and assembly. The payload is loaded in as a resource and is encrypted (decrypted at run-time).

I got a theme too as well as music that plays in the background.

So what are you waiting for? [Download it now!](#) Btw, the password is 'infected' without quotes.



This entry was posted on Tuesday, December 22nd, 2015 at 7:11 am and is filed under [code](#), [Joe you evil bastard](#), [reversing](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can skip to the end and leave a response. Pinging is currently not allowed.

« [3 stage dot net Trojan](#)

4 Responses to “JoeCrypter finally released”



1. MCKSys says:

[December 23, 2015 at 11:00 pm](#)

12/23/2015: Firefox big red screen:

Reported Unwanted Software Page!


This web page at <http://www.gironsec.com> has been reported to contain unwanted software and has been blocked based on your security preferences.

Unwanted software pages try to install software that can be deceptive and affect your system in unexpected ways.

Just to let you know...


Cheers!!!

[Reply](#)

- o  *averagejoe* says:
[December 24, 2015 at 8:02 pm](#)

lel. That was fast.


[Reply](#)

2.  *NotWorking* says:
[December 28, 2015 at 3:44 pm](#)

<http://www.minerva-labs.com/#!Joe?s-Crypter?-Fixed-and-PREVENTED/c7a5/568129200cf236d40390595f>

As pointed out in this article, I can't "crypt" calc.exe without errors.

[Reply](#)

- o  *averagejoe* says:
[December 28, 2015 at 5:50 pm](#)

I saw on twitter. I'll fix this week 😊

[Reply](#)

Leave a Reply

<input type="text"/>	Name (required)
<input type="text"/>	Mail (will not be published) (required)
<input type="text"/>	Website

- Search for:

• Archives


- o [December 2015](#)
- o [September 2015](#)
- o [July 2015](#)
- o [June 2015](#)
- o [March 2015](#)
- o [February 2015](#)
- o [January 2015](#)

- [November 2014](#)
- [October 2014](#)
- [September 2014](#)
- [August 2014](#)
- [July 2014](#)
- [June 2014](#)
- [May 2014](#)
- [March 2014](#)
- [February 2014](#)
- [January 2014](#)
- [December 2013](#)
- [November 2013](#)
- [October 2013](#)
- [September 2013](#)
- [August 2013](#)
- [June 2013](#)
- [May 2013](#)
- [April 2013](#)
- [March 2013](#)
- [February 2013](#)
- [January 2013](#)
- [December 2012](#)
- [November 2012](#)
- [October 2012](#)
- [September 2012](#)
- [August 2012](#)
- [July 2012](#)
- [June 2012](#)
- [May 2012](#)
- [April 2012](#)
- [March 2012](#)
- [February 2012](#)
- [December 2011](#)
- [October 2011](#)
- [September 2011](#)
- [August 2011](#)

• Categories

- [code](#) (63)
- [cracking](#) (21)
- [Joe you evil bastard](#) (26)
- [reversing](#) (36)
- [Uncategorized](#) (29)

Powered by [WordPress](#) | [Entries \(RSS\)](#) | [Comments \(RSS\)](#) | Template stolen from wordpress theme search

	Has your credit card number been STOLEN on the Internet?	
	<input type="text"/>	<input type="text"/>
	card number	expires
	<input type="button" value="Check It"/>	