

Null Byte

The aspiring white-hat hacker/security awareness playground

Follow

World Home

How-To

Inspiration

Forum

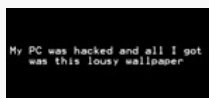
Creators



Is There a VPN That Keeps No Log??



The Ultimate Guide to Upping Tx-Power in Kali Linux 2.0



Zanti: Introduction



Cloning Bootable Live USB to Partition of Hard Disk



Executable in Image



The Food Hacks Guide to Getting Ethnic Flavors Part 2



Security-Oriented C Tutorial 0xFA - Enhancing Our Crypter

Posted By



dontrustme



16 hours ago



KUDOS



Hello again, readers! In our [previous crypter tutorial](#), we looked at how we could obfuscate our malware (or any program) by using a simple one-byte XOR key. In this quick tutorial, we will be looking at how a simple little tweak can create a better means of obfuscation. Let's get right into it!

Multi-Key XOR

With a couple of tests, we saw that the obfuscation method worked however, our real-world test with the RAT, *Dark Comet*, proved that our crypter was not robust enough as it was still detected by common antiviruses such as AVG, Avira and Bitdefender. A very simple way to strengthen our obfuscation method is by modifying our XOR key. All we have to do is to expand our key with more keys and then have it cycle through while encrypting our file. How do we do this? Why, with an array, of course!

```
21 #include <sys/stat.h>
22
23 /*
24  * this is the key we
25  * will use to XOR
26  */
27 //define XOR_KEY 0x6F
28
29 /*
30  * here is our extended
31  * multi-key XOR array
32  */
33 unsigned char key[] = {0x03, 0x12, 0x4d, 0xe3, 0x11, 0x6f};
34
35 /*
36  * definitions for crypting
37  * or decrypting
```

We can see our previous definition of the single-byte XOR key, *XOR_KEY*. We've now defined an array of bytes in an unsigned char array called *key*. Note that it's of type *unsigned char* because we want to use the entire range from 0-255. For our encrypting method in our *xorFile* function, we need to be able to cycle through our array for each byte we read and encrypt. How we can do this is by using the *modulus* operator (%). A brief description of what it does: it is an operator which obtains the *remainder* of a division. Here's a demonstration of how it works in calculating the position inside our *key* array.

1. First character read is XORed with 0x03 (element 0),
2. Second XORed with 0x12 (element 1),
3. ...
4. ...
5. ...
6. Sixth character is XORed with 0x6f (element 5),
7. Our seventh needs to be XORed with 0x03 (element 6?),
8. Eighth with 0x12 (element 7?).

If we take element "6" and divide it by the size of the array, 6, the remainder is 0, so therefore, our seventh character will roll back to the first element, AKA 0x03. Our eighth is element "7" divided by size of the array, 6, we get the remainder 1 which is element 1, i.e. 0x12. It will keep doing this until it finishes the entire encryption. How do we do it in code? Let's check it out:

```
/*
 * this is our single
 * key method using
 * only one byte to
 * XOR the file contents
 */
//fputc (c^XOR_KEY, ofile);

/*
 * this is our multi-
 * key method using
 * multiple bytes to
 * XOR the file contents
 */
fputc (c^key[i % sizeof (key)], ofile);
```

Using our loop incremter, *i*, we can obtain the element of our array starting from 0 and as *i* increases, so does the element number. We also use the *sizeof* operator on our *key* array to obtain the total number of elements (6). With these two together along with our modulus operation from above, it will work perfectly, cycling through the keys as we need.

Here are our [new results](#) with our tweaked crypter with the Dark Comet RAT in VirusTotal.



The screenshot shows the VirusTotal interface for a file named 'encrypted_dc'. The SHA256 hash is 91ae8acc03773b9ae52c00af4b0f50c0ae660756b4ffcc8d99541a9d907aa. The detection ratio is 1 / 53. The analysis date is 2016-01-24 07:03:56 UTC (1 week, 3 days ago). The analysis shows a single detection by CAT-QuickHeal, identifying the file as TrojanPWS.ZBot. The update date for CAT-QuickHeal is 20160123.

Antivirus	Result	Update
CAT-QuickHeal	TrojanPWS.ZBot	20160123

Well then, that is much MUCH better! Look at that, only a single detection by a "CAT-QuickHeal" antivirus. Well I've never heard of that so I'm guessing it's safe to assume that the typical user wouldn't have either. Excellent! In fact, our file didn't even get flagged as a PUA (Possibly Unwanted Application) which is nice!

Conclusion

By using a multi-key method, we were able to deny any form of brute force method that might've revealed the signature of our malware (or any other program) as it would take much more time and resources to decrypt. Of course, any forensics analysis or reverse engineering method would unveil our encryption key, method and ultimately the true face of our file.

That's it for our crypter program. If you'd like to go even further, perhaps you could implement some sort of array which stores the entire encrypted binary file inside the crypter and have it decrypt and write out to a file (also known




as dropping which could be detected by heuristics) on execution so it wouldn't be two separate files and require that dependency.

If you want to go *even* further and try writing your own runtime crypter, you would need to explore and learn how executables are loaded into memory according to their headers and segments (which is pretty advanced).

See you in the next tutorial!

dtm.

See Also

-  [Security-Oriented C Tutorial 0xFB - A Simple Crypter](#)
-  [How to Orient to path in Adobe Flash CS3](#)
-  [How to Orient objects to a curve \(sweep\) in Houdini 9](#)

[Show More...](#)

Start the Discussion

Subscribe











Popular How-To Topics in Computers & Programming

Hack in to another computer th...	Track who views your facebook ...	Create web page using notepad...
Crack facebook password	How to Hack wifi with ps3	How to Hack skype chat
How to Hack skype password	Hack a website password	Write in bold text on facebook w..
Hack another computer on you...	Bypass facebook password	Remove block website
Hack router password	Boost usb modem wireless signal	Install firefox to ps3
Hack another computer from yo...	Hack a website password	Hack laptop password
How to Hack wifi passwords	How to Hack facebook chat	Hack others facebook account
Hack facebook account	Progress bar in visual basic 6.0	Hack in to another computer th...

Trending Across WonderHowTo



	Hack Like a Pro: Digital Forensics for the Aspiring Hacker, Part 13 (Browser Forensics)		4 Ways to Crack a Facebook Password and How to Protect Yourself from Them
	The Hard-Boiled Egg Killer: Perfect Easy-Peel Eggs in Half the Time		Raspberry Pi: Physical Backdoor Part 2
	Keeping Your Hacking Identity Secret: How to Become a Ghost Hacker #3		The Food Hacks Guide to Getting Ethnic Flavors Right, Part 2
	Galaxy S5 Battery Dies Too Fast? Here's Why & How to Fix It		Crack Any Master Combination Lock in 8 Tries or Less Using This Calculator

Arts

Arts & Crafts
Beauty & Style
Dance
Fine Art
Music & Instruments

Science & Tech

Autos, Motorcycles & Planes
Computers & Programming
Disaster Preparation
Education
Electronics
Film & Theater
Software
Weapons

Lifestyle

Alcohol
Business & Money
Dating & Relationships
Diet & Health
Family
Fitness
Food
Home & Garden
Hosting & Entertaining
Language
Motivation & Self Help
Outdoor Recreation
Pets & Animals
Pranks & Cons
Spirituality
Sports
Travel

Gaming

Gambling
Games
Hobbies & Toys
Magic & Parlor Tricks
Video Games