

Forum:[Hack Forums](#)

Thread: [ANSI C Botnet + Crypter \(only targets Raspberry Pi's\)](#)

SIM-3081018 - May 6, 2017, 10:14 am

Hey guys, I brought together some tutorials online and coded some custom functions to make this Raspberry Pi Botnet in C, and a XOR crypter to go with it!

Features include:

- SYN flood on 20 threads.
- Runs at startup in the background (/etc/rc.local).
- Instead of communicating directly with hacker (or P2P) I implemented a simple web request (in cURL) to a hardcoded Pastebin URL for attack instructions.
- 32 byte hardcoded key XOR encryption with crypter

And unfortunately some of the cooler things I didn't have a chance to implement:

- Execute in memory.
- Small script to combine encrypted bytecode with crypter in decrypt mode to create final payload.

The virus code (change the pastebin URL and XOR key to your own, and modify things in the SYN packet if you want)

The crypter code:

Prototype for combining known (hardcoded) encrypted bytecode with the crypter in decrypt mode (unfinished and untested, certainly isn't working as-is):

Thanks

SIM-3081018 - May 12, 2017, 12:58 pm

(May 11, 2017 03:42 AM)Transcendencies Wrote: [\[CITE\]](#) This pastebin idea would fuck you in the ass, unless you implemented it to search/crawl for your new pastes if the main ever goes down, still risky though.

Very true, the idea was to avoid connecting to the hackers dedicated server but the drawback is pretty huge. Hopefully pastebin doesn't monitor their pastes too well lol.

Thanks for the feedback

0xDEAD10CC - May 12, 2017, 8:08 pm

Instead of using the actual characters, why didn't you just do something like:
Code

"\x95\xEF\x24\xF4\xB6\x00\x40\x00\x6F\x00\x00\x00\x00\x20\xF1\xF6\x00\xD6\x00\xF9\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xC7\x00\xF3\x00"

I didn't really have much interest in this so I don't have a comment on the rest at this point. I probably missed some of the real values too above because I copied it into my editor first before a hex editor. Instead of hardcoding that too and making it a non-const pointer you could have used [] instead and sizeof(), but since this is a string, that's actually 33 bytes. If you used an array {} it would prevent that and explicitly sizing it as 32 would prevent you from over or undersizing it from 32 bytes as well.

Simple XOR is pretty ordinary however.

SIM-3081018 - May 12, 2017, 8:11 pm

(May 12, 2017 08:08 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Instead of using the actual characters, why didn't you just do something like:

Code

"\x95\xEF\x24\xF4\xB6\x00\x40\x00\x6F\x00\x00\x00\x00\x20\xF1\xF6\x00\xD6\x00\xF9\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xC7\x00\xF3\x00"

I didn't really have much interest in this so I don't have a comment on the rest at this point.

You mean for the byte code array? at first I had it as just the hex string without the \x but i found it easier to iterate through an array. My prototype code there in the end is bunk, it just shows how you might bring the crypter and bytecode together.

0xDEAD10CC - May 13, 2017, 11:55 am

(May 12, 2017 08:11 PM)Cody8295_ Wrote: [\[CITE\]](#) You mean for the byte code array? at first I had it as just the hex string without the \x but i found it easier to iterate through an array. My prototype code there in the end is bunk, it just shows how you might bring the crypter and bytecode together.

That doesn't really make sense. And no I mean the key X_K.

"at first I had it as just the hex string without the \x but i found it easier to iterate through an array."

The \x##\x##... version I gave you would be the exact same as what you already have except you would see the byte values instead of their ASCII representation. If you had it as a hex string you would have to manually calculate the hex->decimal value.

i.e. "\0" -> "\x00"

REDRIFLE - May 19, 2017, 7:30 pm

Some of the worst C I seen in a long time xD

HFDone - May 20, 2017, 1:33 pm

(May 19, 2017 07:30 PM)REDRIFLE Wrote: [\[CITE\]](#) Some of the worst C I seen in a long time xD
"I brought together some tutorials online ..."

SIM-3081018 - May 21, 2017, 11:37 am

(May 20, 2017 01:33 PM)HFDone Wrote: [\[CITE\]](#) "I brought together some tutorials online ..."

I tried to give credit where ever I did use tutorial code, and the rest was done very hastily as it was for a class project, so a lot of it is not well written