

Forum:[Hack Forums](#)

Thread: [\[Question\] Python - Rat and Cryption](#)

Anymore - May 9, 2016, 6:56 am

I have a question. i'm sure is possible to make a RAT with python, but is possible crypt (i think is the right word :?) i mean crypting the source but on duple click working, like this if i set my ip inside will be hide?

?BORNE? - May 9, 2016, 8:27 am

Everything is possible in python... encryption is possible but a RAT would be more stable on a different language.

Anymore - May 9, 2016, 8:36 am

(May 9, 2016 08:27 AM)OneBongWill Wrote: [\[CITE\]](#) Everything is possible in python... encryption is possible but a RAT would be more stable on a different language.

Got it, now i have two more question:

- 1) Witch language?
- 2) Can you tell me how to work technically, i can't imagine how work this cryption, i mean how is possible the computer can read a script/program if the source is crypted?

?BORNE? - May 9, 2016, 9:40 am

(May 9, 2016 08:36 AM)Anymore Wrote: [\[CITE\]](#) Got it, now i have two more question:

- 1) Witch language?
 - 2) Can you tell me how to work technically, i can't imagine how work this cryption, i mean how is possible the computer can read a script/program if the source is crypted?
- Wait I am confused on what your asking... are you encrypting the source code or a server? (I figured you meant server as you were asking about RAT)

Anymore - May 9, 2016, 9:50 am

(May 9, 2016 09:40 AM)OneBongWill Wrote: [\[CITE\]](#) Wait I am confused on what your asking... are you encrypting the source code or a server? (I figured you meant server as you were asking about RAT)

Both of it

Crynx - May 9, 2016, 9:52 am

(May 9, 2016 08:36 AM)Anymore Wrote: [\[CITE\]](#) Got it, now i have two more question:

- 1) Witch language?
 - 2) Can you tell me how to work technically, i can't imagine how work this cryption, i mean how is possible the computer can read a script/program if the source is crypted?
- C++ can be very stable

TheKojak - May 9, 2016, 12:09 pm

Python can be used to create any sort of stable malware, however, expect to be coding the low level stuff (memory management, hooking, etc..) in a language like C or C++ to actually have it be stable. The problem then is that you'd have to "compile" it using a tool like PyInstaller and from my experience PyInstaller binaries cannot be crypted using the usual RunPE method, so you'd probably

have to code some sort of a custom packer.

Goodies - May 9, 2016, 1:09 pm

If you put your IP in it, it will not be hidden. Ever. Do not make a Python RAT. Also, anyone can run netstat to see your IP anyways...

SIM-1866423 - May 10, 2016, 3:48 am

(May 9, 2016 01:09 PM)Goodies Wrote: [\[CITE\]](#) If you put your IP in it, it will not be hidden. Ever. Do not make a Python RAT. Also, anyone can run netstat to see your IP anyways...

Its not true, with little magic you can avoid your IP from netstat,nmap etc. anything on windows(not working on linux yet).I'm working on it when its complete i will share from here :)

DJSanderrr - May 10, 2016, 3:53 am

(May 9, 2016 01:09 PM)Goodies Wrote: [\[CITE\]](#) If you put your IP in it, it will not be hidden. Ever. Do not make a Python RAT. Also, anyone can run netstat to see your IP anyways...

You sure can hide it as good as C will.

You could encrypt the DNS server to connect to, and decrypt using same key (using aes or something)

And then youcould convert it to .pyc and it would be wayharder to read.

Right?

Anymore - May 10, 2016, 6:34 am

(May 9, 2016 01:09 PM)Goodies Wrote: [\[CITE\]](#) If you put your IP in it, it will not be hidden. Ever. Do not make a Python RAT. Also, anyone can run netstat to see your IP anyways...

I'm not a black/gray hat, for now i'm in learning just at home with my own device, my question was just for curiosity 'cause, everybody tell me " You can do everything in python " and i want know how much is powerful :D however i send you a PM right now

Xutdes. - May 10, 2016, 7:36 am

(May 10, 2016 03:53 AM)DJSanderrr Wrote: [\[CITE\]](#) You sure can hide it as good as C will.

You could encrypt the DNS server to connect to, and decrypt using same key (using aes or something)

And then youcould convert it to .pyc and it would be wayharder to read.

Right?

Correct me if I'm wrong, but encrypting the communications between you and the DNS server won't help with anything. You don't need to actually request anything from a DNS server when connecting to an IP. You just connect to it, simply.

DJSanderrr - May 10, 2016, 7:45 am

(May 10, 2016 07:36 AM)Tenebris Wrote: [\[CITE\]](#) Correct me if I'm wrong, but encrypting the communications between you and the DNS server won't help with anything. You don't need to actually request anything from a DNS server when connecting to an IP. You just connect to it, simply.

Sorry I might was unclear, but I just woke up.

But I actually meant: encrypting the dns-server-link (no-ip kinda link, like i-am-hacker.no-ip.org), as it's a bad thing anyways to use your IP raw in the code.

Is this more clear?

Xutdes. - May 10, 2016, 7:46 am

(May 10, 2016 06:34 AM)Anymore Wrote: [\[CITE\]](#) I'm not a black/gray hat, for now i'm in learning just

at home with my own device, my question was just for curiosity 'cause, everybody tell me " You can do everything in python " and i want know how much is powerful :D however i send you a PM right now

You have to understand how the internet works before going any step further. You have been illuded into thinking that everything is possible. There are things that are possible, and there are things which are not. Hiding you IP - the very thing that enables computers to communicate across the internet - is impossible. You almost always have to give your IP whenever you're requesting something from a machine. Now some kid might hurry and say "Oh really sucker? Tor can!". Well, using Tor does hide YOUR IP from the machine you're communicating with, but in the end all the other nodes that your packets had passed through have your IP and everything can be traced back to you, assuming log files were untouched.

So your best bet would be to use a VPN that allows port forwarding, or you could just pay for a VPS or an RDP.

(May 10, 2016 07:45 AM)DJSanderrr Wrote: [\[CITE\]](#) Sorry I might was unclear, but I just woke up.

But I actually meant: encrypting the dns-server-link (no-ip kinda link, like i-am-hacker.no-ip.org), as it's a bad thing anyways to use your IP raw in the code.

Is this more clear?

I can still know the IP by just having the domain. I might not be getting you, if not I really hope you could explain your idea to me more clearly and less vaguely.

DJSanderrr - May 10, 2016, 8:53 am

(May 10, 2016 07:46 AM)Tenebris Wrote: [\[CITE\]](#) You have to understand how the internet works before going any step further. You have been illuded into thinking that everything is possible. There are things that are possible, and there are things which are not. Hiding you IP - the very thing that enables computers to communicate across the internet - is impossible. You almost always have to give your IP whenever you're requesting something from a machine. Now some kid might hurry and say "Oh really sucker? Tor can!". Well, using Tor does hide YOUR IP from the machine you're communicating with, but in the end all the other nodes that your packets had passed through have your IP and everything can be traced back to you, assuming log files were untouched.

So your best bet would be to use a VPN that allows port forwarding, or you could just pay for a VPS or an RDP.

I can still know the IP by just having the domain. I might not be getting you, if not I really hope you could explain your idea to me more clearly and less vaguely.

(May 10, 2016 07:46 AM)Tenebris Wrote: [\[CITE\]](#) I can still know the IP by just having the domain. I might not be getting you, if not I really hope you could explain your idea to me more clearly and less vaguely.

Spoiler ([Click to View](#))

Btw, I'm not saying that what I say is correct, I'm just thinkin

Ok, let me explain in a language we both speak: python.

This code is pretty much way not really readable to the naked eye:

Code from Crypto.Cipher import AES

```
# domain, in this case i-am-hacker.no-ip.net
k =
'\x11\x00\x4a\x16\x5b\xc1\xb5\xf0\x84\xb2\x1d\xed\x6e\xef\x36\xda\x96\x7b\x03\xf3\xf3\xaa\x00\x0d
\x80\xaa\x36\x12\xf4\xe7\x10\xea'

# md5 of i-am-hacker.no-ip.net
c = AES.new('\xb2\x36\xbc\x2e\x38\x3f\xb2\xf2\x0b\x43\xd0\xd4\xf0\xa7\x9f\xdf');

# encrypt and decrypt
b = 16
p = '\x00'
_p = lambda s: s + (b - len(s) % b) * p
_e = lambda s: c.encrypt(_p(s)) # encrypt
_d = lambda s: c.decrypt(s).rstrip(p) #decrypt

print 'Your DNS serv is: ', _d(k)
And after compiling to .pyc:
```

Code sander@sec:~\$ xxd test.pyc

```
00000000: 03f3 0d0a e301 3257 6300 0000 0000 0000 .....2Wc.....
00000100: 0002 0000 0040 0000 0073 5f00 0000 6400 .....@...s...d.
00000200: 0064 0100 6c00 006d 0100 5a01 0001 6402 .d..l..m..Z...d.
00000300: 005a 0200 6501 006a 0300 6403 0083 0100 .Z..e..j..d....
00000400: 5a04 0064 0400 5a05 0064 0500 5a06 0064 Z..d..Z..d..Z..d
00000500: 0600 8400 005a 0700 6407 0084 0000 5a08 .....Z..d.....Z.
00000600: 0064 0800 8400 005a 0900 6409 0047 6509 .d.....Z..d..Ge.
00000700: 0065 0200 8301 0047 4864 0a00 5328 0b00 .e.....GHd..S(..
00000800: 0000 69ff ffff ff28 0100 0000 7403 0000 ..i....(...t...
00000900: 0041 4553 7320 0000 0011 004a 165b c1b5 .AESs .....J.[..
00000a00: f084 b21d ed6e ef36 da96 7b03 f33f aa00 .....n..6..{..?..
00000b00: 0d80 aa36 12f4 e710 ea73 1000 0000 b236 ...6.....s.....6
00000c00: bc2e 383f b2f2 0b43 d0d4 f0a7 9fdf 6910 ..8?...C.....i.
00000d00: 0000 0074 0100 0000 0063 0100 0000 0100 ...t.....c.....
00000e00: 0000 0400 0000 4300 0000 731a 0000 007c .....C...s....|
00000f00: 0000 7400 0074 0100 7c00 0083 0100 7400 ..t..t..|.....t.
00001000: 0016 1874 0200 1417 5328 0100 0000 4e28 ...t...S(...N(
00001100: 0300 0000 7401 0000 0062 7403 0000 006c ....t....bt....l
00001200: 656e 7401 0000 0070 2801 0000 0074 0100 ent....p(...t..
00001300: 0000 7328 0000 0000 2800 0000 0073 0700 ..s(...(...s..
00001400: 0000 7465 7374 2e70 7974 0800 0000 3c6c ..test.pyt....<l
00001500: 616d 6264 613e 0e00 0000 7300 0000 0063 ambda>....s....c
00001600: 0100 0000 0100 0000 0300 0000 4300 0000 .....C...
00001700: 7313 0000 0074 0000 6a01 0074 0200 7c00 s....t..j..t..|.
00001800: 0083 0100 8301 0053 2801 0000 004e 2803 .....S(...N(.
00001900: 0000 0074 0100 0000 6374 0700 0000 656e ...t....ct....en
00001a00: 6372 7970 7474 0200 0000 5f70 2801 0000 cryptt...._p(...
00001b00: 0052 0500 0000 2800 0000 0028 0000 0000 .R....(...(...
00001c00: 7307 0000 0074 6573 742e 7079 5206 0000 s....test.pyR...
00001d00: 000f 0000 0073 0000 0000 6301 0000 0001 .....s....c.....
00001e00: 0000 0002 0000 0043 0000 0073 1600 0000 .....C...s....
00001f00: 7400 006a 0100 7c00 0083 0100 6a02 0074 t..j..|.....j..t
00002000: 0300 8301 0053 2801 0000 004e 2804 0000 .....S(...N(...
00002100: 0052 0700 0000 7407 0000 0064 6563 7279 .R....t....decry
```

```
0000220: 7074 7406 0000 0072 7374 7269 7052 0400 ptt....rstripR..
0000230: 0000 2801 0000 0052 0500 0000 2800 0000 ..(....R....(...
0000240: 0028 0000 0000 7307 0000 0074 6573 742e .(....s....test.
0000250: 7079 5206 0000 0010 0000 0073 0000 0000 pyR.....s....
0000260: 7312 0000 0059 6f75 7220 444e 5320 7365 s....Your DNS se
0000270: 7276 2069 733a 204e 280a 0000 0074 0d00 rv is: N(....t..
0000280: 0000 4372 7970 746f 2e43 6970 6865 7252 ..Crypto.CipherR
0000290: 0000 0000 7401 0000 006b 7403 0000 006e ....t....kt....n
00002a0: 6577 5207 0000 0052 0200 0000 5204 0000 ewR....R....R...
00002b0: 0052 0900 0000 7402 0000 005f 6574 0200 .R....t...._et..
00002c0: 0000 5f64 2800 0000 0028 0000 0000 2800 .._d(....(....(
00002d0: 0000 0073 0700 0000 7465 7374 2e70 7974 ...s....test.pyt
00002e0: 0800 0000 3c6d 6f64 756c 653e 0100 0000 ....<module>....
00002f0: 7310 0000 0010 0506 030f 0306 0106 0109 s.....
0000300: 0109 0109 02          .....
```

That's basically what I meant, and what I thought the OP meant.

Xutdes. - May 10, 2016, 8:59 am

(May 10, 2016 08:53 AM)DJSanderrr Wrote: [\[CITE\]](#)

Spoiler ([Click to View](#))

Btw, I'm not saying that what I say is correct, I'm just thinkin

Ok, let me explain in a language we both speak: python.

This code is pretty much way not really readable to the naked eye:

-snip -

That's basically what I meant, and what I thought the OP meant.

Oh okay, sorry for not getting you the first time. I didn't take into account using the compiled version of the script. I guess you're right, you can hide your IP address from the code. But still, the request to actual server is being made and anyone with the right tools can find the IP.

Thanks for explaining though!

DJSanderrr - May 10, 2016, 9:02 am

(May 10, 2016 08:59 AM)Tenebris Wrote: [\[CITE\]](#) Oh okay, sorry for not getting you the first time. I didn't take into account using the compiled version of the script. I guess you're right, you can hide your IP address from the code. But still, the request to actual server is being made and anyone with the right tools can find the IP.

Thanks for explaining though!

That's true for sure, but perhaps you could route it through TOR or something? That's something I've always wondered to do. Would be cool if that worked.

Xutdes. - May 10, 2016, 9:15 am

(May 10, 2016 09:02 AM)DJSanderrr Wrote: [\[CITE\]](#) That's true for sure, but perhaps you could route it through TOR or something? That's something I've always wondered to do. Would be cool if that worked.

Yeah, that's an interesting thing actually. I haven't really thought of using Tor in python. Let me look it up I guess!

But in all honesty, python wouldn't be a good program to create RATs in. Not that it can't, it's just that a majority of internet users don't have python installed on their machines. Some might think of bundling it with the RAT, but think of it, the file size would be relatively huge.