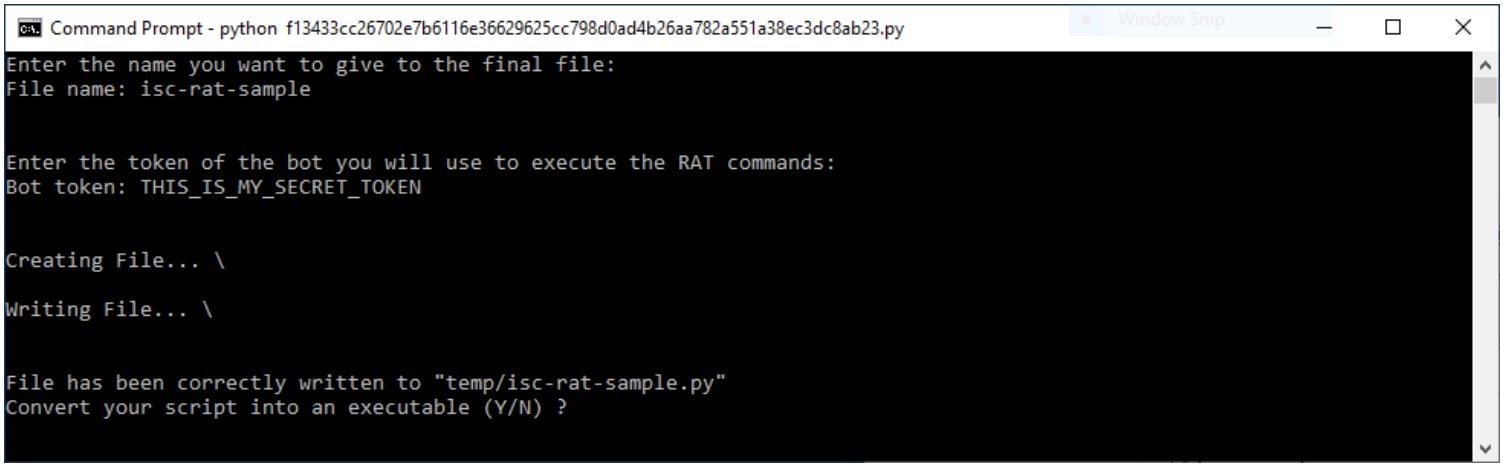
Custom Python RAT Builder

isc.sans.edu/diary/28224

Published: 2022-01-07
Last Updated: 2022-01-07 10:22:05 UTC
by Xavier Mertens (Version: 1)

This week I already wrote a diary about "code reuse" in the malware landscape[1] but attackers also have plenty of tools to generate new samples on the fly. When you received a malicious Word documents, it has not been prepared by hand, it has been for sure automatically generated. Except if you're a "nice" target for attackers and victim of some kind of "APT". The keyword here is "automation". If defenders try to automate as much as possible, attackers too!

Today, Discord is often used by attackers as a nice C2 server[2] and we can find plenty of Python malware that interact with Discord. Most of them are info stealers. I already found plenty of such scripts but today I spotted something else. A script to generate your own RAT ("Remote Access Tool"). The script has a VT score of 7/56[3] (SHA256:f13433cc26702e7b6116e36629625cc798d0ad4b26aa782a551a38ec3dc8ab23). I had to fine tune a bit the script to make it work in my sandbox but the usage is pretty simple:



The script is very simple, it contains the RAT standard code and the provided token is injected into it:

```
file.write("""import winreg
import ctypes
import sys
import os
import ssl
import random
import threading
import time
import cv2
import subprocess
import discord
from comtypes import CLSCTX_ALL
from discord.ext import commands
from ctypes import *
import asyncio
import discord
from discord import utils
token = '~~TOKENHERE~~'
global appdata
appdata = os.getenv('APPDATA')
client = discord.Client()
bot = commands.Bot(command_prefix='!')
...
...
""".replace("~~TOKENHERE~~", tokenbot))
```

You can see that the script asks if the script must be compiled. This is achieved using the pyinstaller[4] module.Once completed, you will have a fully standalone PE file ready to be sent to your victims. I uploaded my sample to VT and it got a score of 10/67, not so bad from an attacker's point of view.

Here is a quick overview of the supported bot commands:

!kill	Kill the bot (disconnect from Discord)
!dumpkeylogger	Dump captured keys to the Discoard channel
!exit	Exit the bot (process)
!windowstart	Start Window logging
!windowstop	Stop Window logging
!screenshot	Take a screenshot
!webcampic	Take picture with the webcam
!message	Display a message on the desktop (via MessageBoxW())
!wallpaper	Change the desktop background
!upload	Upload a file
!shell	Remote command execution
!download	Download a file

!cd	Change current directory
!help	Because attackers need some help too :-)
!write	Write something (like on the keyboard)
!clipboard	Get clipboard data
!sysinfo	Collect system information
!geolocate	Collect GeoIP details about the victim
!admincheck	Check if bot is running with admin privileges
!uacbypass	Try UAC privileges escalation
!startkeylogger	Start the keylogger
!stopkeylogger	Stop the keylogger
!blockinput	Annoy the user[5]
!unblockinput	Release the user
!streamwebcam	Start webcam recording
!stopwebcam	Stop webcal recording
!getdiscordinfo	What about the Discord session?
!streamscreen	Record multiple screenshots
!stopscreen	Stop screen streaming
!shutdown	Stop the victim's computer
!restart	Reboot the victim's computer
!logoff	Logoff the current user
!bluescreen	Generate a BSOD (!)
!currentdir	Print current directory
!displaydir	List files in the direcotry
!dateandtime	Return the victim's computer date & time
!listprocess	Return the list of running processes
!prockill	Try to kill a process
!recscreen	Record a video from screen
!reccam	Record a video from webcam

!recaudio	Record a wav from the internal mic
!delete	Delete a file
!disableantivirus	Try to disable the AV
!disablefirewall	Try to disable the firewall
!audio	Play a record file
!selfdestruct	Try to wipe the computer
!windowspass	Try to collect system credentials
!displayoff	Turn off display
!displayon	Turn on display
!hide	Try to hide a file ("attrib +h")
!unhide	Try to unhide a file
!decode	Decode Base64
!ejectcd	Open CD tray
!retractcd	Close CD tray
!critproc	Set process as critical
!website	Visit a webpage
!distaskmgr	Try to disable the task manager
!enbtaskmgr	Try to re-enable the task manager
!getwifipass	Exfiltrate Wifi passwords

[1] https://isc.sans.edu/forums/diary/Code+Reuse+In+the+Malware+Landscape/28216/
[2] https://crawl3r.github.io/2020-01-25/DaaC2
[3] https://www.virustotal.com/gui/file/f13433cc26702e7b6116e36629625cc798d0ad4b26aa782a551a38ec3dc8ab23/details
[4] https://pypi.org/project/pyinstaller/
[5] https://isc.sans.edu/forums/diary/A+Simple+Batch+File+That+Blocks+People/28212/

Xavier Mertens (@xme)
Xameco
Senior ISC Handler - Freelance Cyber Security Consultant
PGP Key