

Forum:[Hack Forums](#)

Thread: [What malicious tools did you write in Python?](#)

chaozu - January 7, 2020, 6:50 am

I'd love to hear what you guys managed to archive with some Python code.

I am still a beginner at programming, so I started small, but my first two projects were the following:

Code snippet for other Python scripts, which injects an auto downloader of any file (e.g. your RAT), which then executes the downloaded file and deletes it afterwards. Also available as a standalone .exe

Chrome logins and history stealer that injects its into the users startup folder. the encrypted data is then uploaded to a cloud service and then deleted from the victims pc.

The good thing about these is, that they are FUD without the need of any crypter. Unfortunately the file sizes a little big, when compiled to an executable. But that's the downside of Python I guess..

h0lyl337 - January 7, 2020, 10:31 am

just keep in mind if you post malicious code, the feds will keep it, and use it against you in the futures lol.

Joel - January 7, 2020, 11:52 pm

Taking the malicious route with coding isn't that smart. Maybe focus on training some marketable skills so you can get hired.

chaozu - January 8, 2020, 1:40 pm

(Jan 8, 2020 12:52 AM)Joel Wrote: [\[CITE\]](#) Taking the malicious route with coding isn't that smart. Maybe focus on training some marketable skills so you can get hired.

Thank you Joel for your feedback. I really appreciate it. However, no need to assume I am taking any route here. These are just some little side projects I worked on, because they were a lot of fun and I learned a lot. Am I am going to post them on my Github? Most likely not. But these are not the only projects I am working on and I am absolutely not focusing on a malicious route here.

Shisho - January 9, 2020, 7:34 pm

(Jan 8, 2020 12:52 AM)Joel Wrote: [\[CITE\]](#) Taking the malicious route with coding isn't that smart. Maybe focus on training some marketable skills so you can get hired.

Regardless of what he decides to code he is training his programming knowledge which is a marketable skill. I'm sure, like he said, "malicious code" isn't the only things he has limited himself to write.

By the way, something is only considered malicious if it is actually used for a malicious purpose. Until that moment it is just a proof of concept.

dracx - January 9, 2020, 10:19 pm

(Jan 7, 2020 11:31 AM)h0lyl337 Wrote: [\[CITE\]](#) just keep in mind if you post malicious code, the feds will keep it, and use it against you in the futures lol.

LoL. Depends on the code tho if the feds even wanna try and use it againsts you, or even steal it from you.

JordanClutch - January 10, 2020, 11:29 am

The most "malicious" thing I've done using Python is web scraping...which technically some websites forbid you from doing and is a rude practice.

TheBrokenWasp - January 13, 2020, 12:57 pm

I took a reverse multi-shell someone made in python from github and added as much shit to it as I could, including a password grabber. Never used it but it was a fun project

I was also fascinated with videos on Cobalt Strike for a while, and Raphael Mudge (the creator) was basically the only person who did videos on the tool so I would watch those and he would always get his initial shell from a Powershell one-liner, so I made a download&execute one-liner maker in python. It has a UI from Tkinter I believe, and you simply give it the direct link and an exe output name and it would give you a base64 encoded Powershell one-liner that worked in CMD. It assumed you had a newer version of Powershell though, as I couldn't find a universal Powershell download command. If anyone wants either of these projects for some reason hit me up, I don't mind giving out the sources to these old projects.

ThisBearScat - January 22, 2020, 12:27 am

What's this, a confession page for the feds ?

On a serious note I have never made anything malicious but they could be used for malicious intent.

I believe it's the user that's malicious not the program, tool or script ?

VIXV - January 22, 2020, 3:13 am

Never written a malicious script in python, I don't see the point. Only useful ones, I guess.

vorticalbox - January 22, 2020, 3:30 am

(Jan 10, 2020 12:29 PM)JordanClutch Wrote: [\[CITE\]](#) The most "malicious" thing I've done using Python is web scraping...which technically some websites forbid you from doing and is a rude practice.

how is it "rude practice" if you're not hitting a site with 100s of requests p/s then what's the problem?