**Task 2: Malicious Package Analysis**

Daniel Dalal

Heres my analysis of two suspicious packages I was given.

This is what I found so far.

Behavioral Analysis:

1. **colors-dev (NPM)**

* I noticed the code in colors.js file (JS Package/package/lib/colors.js) is really hard to read (lots of weird names and encodings).
* I investigated together with AI what it does and the findings are:

1. Finds installed Discord versions on your coputer
2. Injects malicious JS into Discords core files
3. Downloads and runs remote code from an external server
4. Steals users data, possibly including Discord tokens.
5. Restars Discord to make sure the injected code runs
6. Silently avoids detection by using techniques like hiding logs and changing file contents

How i knew it was malicious:

It uses things like require('fs'), child\_process, and axios to access the file system, run commands, and talk to external servers.

It writes into paths like discord\_desktop\_core and replaces index.js — this is the core logic file for the Discord client.

There's a hardcoded URL (https://kaue...) where it downloads remote code to inject.

it restarts Discord using commands like Update.exe –processStart.

In short:

This is a token grabber malware targeting Discord. It gets into the user’s local app data, overwrites files, and silently sends back stolen info.

1. **Typing-unions-3.10.0.0 (PyPI)**

* At first I noticed setup.py file is huge (933kb) which is very odd.
* Went straight away and opened the code, the file is full of Base64 data. (recognized this from CTF’s I did)
* I decoded the Base64 data using online decorder and found out some python code, I investigated together with AI what it does and the findings are:

1. It runs antivirus program to list antivirus programs on the system.
2. It looks for names like BitDefender, Sophos, McAfee, Avira, etc. If it finds one, it stops running.
3. If no antivirus found then it creates a random filename ending in .exe in the temp folder and takes a very long Base64 string (which is hidden binary code), decodes it, and writes it into that .exe file.
4. Now there’s a new executable file on the system that came from the script.

How i knew it was malicious:

The script detects antivirus software by running a Windows command silently (wmic). If it finds antivirus, it stops and does nothing — this is a sign that it’s trying to avoid getting caught.

If no antivirus is found, it creates a random .exe file and writes a decoded Base64 payload into it — this is classic dropper behavior.

The Base64 data starts with "TVqQ...", which I learned is how Windows executable files start — confirming it’s actually an .exe hidden inside the code.

In short:

It’s a malicious script that only runs its evil code if there’s no antivirus. It drops a hidden .exe on the system using Base64 and a random filename.

Operational Research:

I checked what each package says it should do vs what it actually does:

* colors-dev claims to add colors to console text but it also injects code in Discord.
* typing-unions claims to bring newer typing features to older python versions. But it actually installs malware on windows.

Comprehensive Documentation:

Summary:

-Both packages turned out to be malware hiding in normal looking libraries.

-colors-dev steaks Discord tokens and typing0unions plants a windows exe.

How I did it:  
1. I read through the code to see weird stuff and looked for big files

2. When found weird code I investigated it with AI.

Reccomendations:

-Don’t install these packages.

-Report them to the npm and PyPI security teams.