ScanPro File Scanner – Project Overview

ScanPro is a Python-based graphical application designed to enhance basic endpoint security by monitoring a user's Downloads folder and scanning newly added files for potential security risks. The project was created as a learning-focused security tool and demonstrates practical concepts in file system monitoring, risk classification, and user-facing security design.

Project Purpose

The primary goal of ScanPro is to act as a simple first line of defense against potentially dangerous files commonly downloaded from the internet. Rather than performing deep malware analysis, ScanPro focuses on identifying risky file types and alerting users before they open them. This approach emphasizes prevention, awareness, and transparency.

How ScanPro Works

ScanPro continuously monitors the user's Downloads folder using the Python watchdog library. Watchdog enables the application to detect file system events such as file creation, modification, movement, and deletion. When a new file appears in the monitored directory, ScanPro automatically initiates a scan.

During a scan, the application compares the file's extension (for example, .exe, .js, or .bat) against a predefined list of extensions commonly associated with executable or potentially dangerous files. If the extension matches a known risky type, the file is flagged as high risk.

ScanPro also uses Python's built-in mimetypes module to infer the file's MIME type. While this method does not analyze the file's internal contents, it provides an additional validation layer by checking whether the file's apparent type matches its extension. Based on these checks, the application assigns a risk level and provides a recommendation to the user.

Risk Classification

ScanPro categorizes files into two primary risk levels:

- HIGH – Files with extensions commonly associated with executables or scripts that could pose a security risk.
- LOW – Files that do not match known risky extension patterns.

Each scan result includes a clear recommendation indicating whether the file is likely safe to open or should be treated with caution.

Key Features

- Real-time monitoring of the Downloads folder
- Automatic scanning of newly downloaded files
- Manual file scanning capability
- File analysis based on size, extension, and MIME type

• Clear, user-friendly graphical interface
• Simple risk-level output with safety recommendations

Installation and Usage

ScanPro is distributed as a standalone executable for ease of use. No additional setup or Python installation is required when using the prebuilt application.

For Windows users, ScanPro can be launched by downloading and double-clicking the ScanPro.exe file. For macOS users, ScanPro is available as a ScanPro.app package. Due to macOS security protections, users may need to explicitly allow the application to run via System Settings if prompted.

Developer Requirements (Running from Source)

Developers who wish to run ScanPro from source code will need:
• Python version 3.8 or later (developed using Python 3.12.2)
• The watchdog library

The watchdog dependency can be installed using pip prior to running the application.

Security Considerations and Limitations

ScanPro is intentionally designed as a basic scanner. It does not perform signature-based malware detection, heuristic analysis, or sandbox execution. As a result, it cannot determine whether a file is truly malicious at a binary or behavioral level.

Advanced malware scanners typically analyze file contents, compare signatures against known malware databases, or execute files in isolated environments. ScanPro does not attempt to replicate these capabilities and should not be considered a replacement for full antivirus or endpoint detection solutions.

Security Philosophy

ScanPro was built with transparency and responsible security practices in mind. Users are strongly encouraged not to run unfamiliar software blindly, including ScanPro itself. The project's source code is available for review, allowing anyone to verify its behavior and confirm that it performs only the actions described.

Conclusion

ScanPro serves as an educational and practical demonstration of file monitoring and basic risk assessment in cybersecurity. While intentionally limited in scope, it highlights the importance of cautious file handling and proactive security awareness. The project provides a foundation that could be expanded in the future to include deeper analysis techniques and integration with more advanced security tooling.