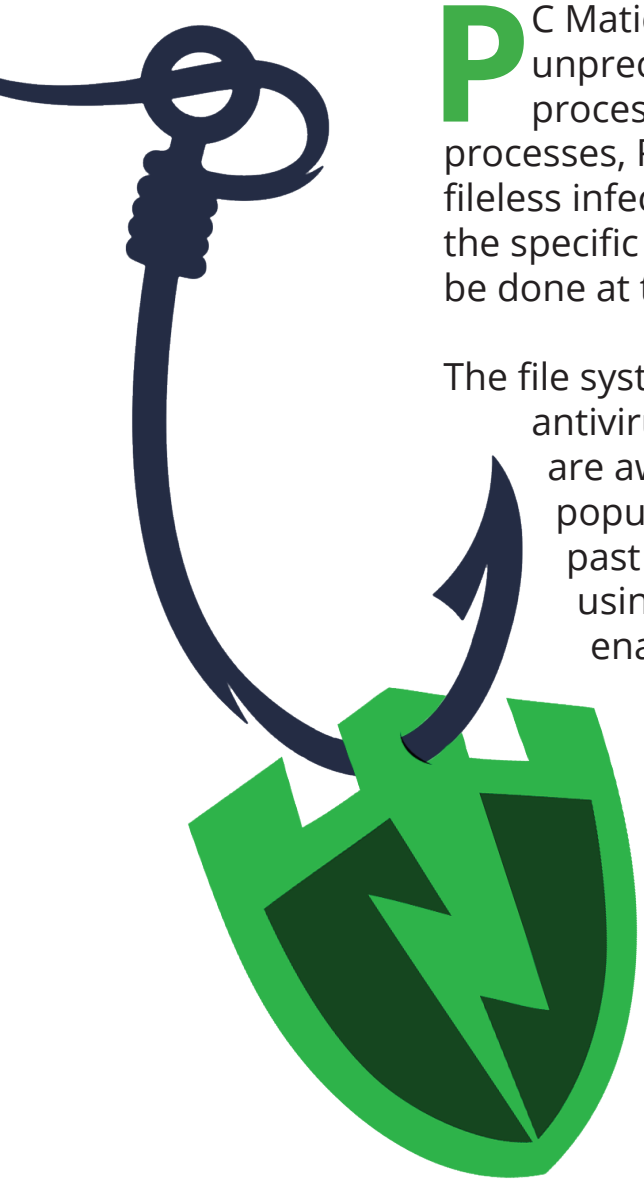
PC Matic PRO DEEP INTEGRATION

PC Matic's Process Hooking Provides Unprecedented Protection



PC Matic hooks into each process permitting unprecedented control over how, what and when each process executes. Listening to communications between processes, PC Matic works to thwart suspicious activity such as fileless infections using advanced heuristics to block or invoke the specific scripting engine. Stopping a scripting attack must be done at the engine level to prevent it from happening.

The file system driver approach employed by mainstream antivirus is becoming obsolete and cyber criminals are aware of it. Fileless ransomware is increasing in popularity every day, allowing criminals a way to slip past many security solutions and increase profits using new technology. PC Matic's hooking technology enables unprecedented command and control which blocks scripting attacks before they enter the scripting engine, continuing our crusade in the war on ransomware

Choosing between a solution that protects you from malware and a solution that is lightweight is no longer necessary. PC Matic's default-deny protection has been proven to be far ahead of our competition, while providing new advanced heuristics to stop scripting attacks without consuming all of your endpoints resources.

How Hooking Works

PC Matic hooks into parent processes to determine if the parent has been whitelisted and allowed to run.

PC Matic monitors communication from the parent to Windows and other processes.

PC Matic traps commands sent to scripting engines. such as: Powershell, Cscript, Wscript, MSHTA

PC Matic's advanced heuristics determine whether the scripting engine should be invoked or blocked.