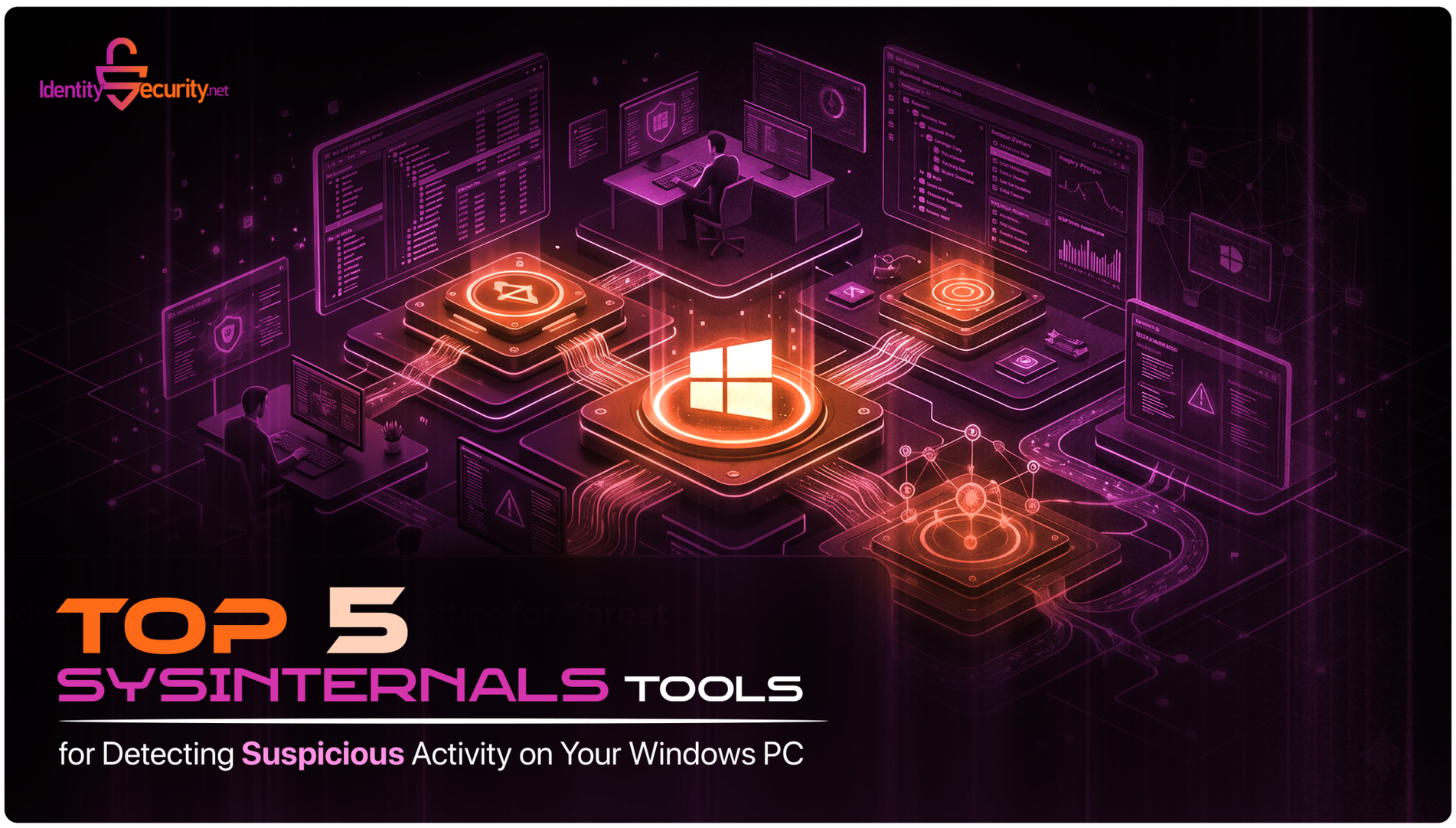
Top 5 Sysinternals Tools for Detecting Suspicious Activity on Your Windows PC



When we think of malware, we often imagine it as a dramatic event: a ransomware warning flashing on the screen or a sudden blue screen of death. In reality, the most dangerous forms of malware are much subtler. It could be a sneaky process draining your CPU resources to mine cryptocurrency, a seemingly helpful app silently sending data to an unknown IP address, or a persistent script that reinstalls itself every time the system reboots.

Windows Task Manager is often insufficient to detect these hidden threats. That's when I turn to the Windows Sysinternals Suite. Developed by Mark Russinovich, now Microsoft's Chief Technology Officer (CTO) and Technical Fellow at Azure, Sysinternals tools are considered the gold standard for deep system analysis. Lightweight, portable, and precise, these tools help me detect even the most stealthy issues in my system.

Here are five Sysinternals tools I personally use to identify anomalies and secure my system.

1. Process Explorer: Task Manager's Smarter Sibling

If Windows Task Manager is a blunt tool, Process Explorer is a sharp scalpel. I use it as my first line of defense whenever I notice system slowdowns or unusual behavior. Although it may look similar to Task Manager, Process Explorer offers far greater depth. It provides a complete family tree of running processes, revealing which processes are linked to others.

01

One of my main uses for Process Explorer is spotting disguised malware. Often, malware tries to masquerade as essential system processes like svchost.exe or chrome.exe, hoping you won't dig too deep. Process Explorer shows exactly where each process originated from. For example, if I see a svchost.exe process initiated by explorer.exe instead of the expected services.exe, I immediately get suspicious.

For more content like and follow me:  **@bertblevins**

02

Another feature I love is its integration with VirusTotal. With a simple toggle in the options menu, Process Explorer checks each running executable against VirusTotal, displaying a detection score. A score of 0 means the file is safe; anything higher gets my immediate attention.

2. TCPView: Tracking Suspicious Network Activity

Malware is often helpless without an internet connection, whether it's a remote access Trojan (RAT) waiting for commands or a keylogger stealing passwords. That's where TCPView comes in handy. Unlike the command-line netstat utility, TCPView presents network connections in an easy-to-read list that updates in real time. I use it to monitor incoming and outgoing connections and identify suspicious activity.

If I notice a process like Notepad or Calculator connected to an unknown IP, I know something is wrong. TCPView allows me to sort active connections by state, which helps me quickly identify open TCP/IP ports. I can also look up IP addresses through a Whois query to see if they're associated with unexpected locations or services. If I spot a shady connection, I don't hesitate to shut it down.

3. Autoruns: Preventing Malware from Reappearing

Malware often ensures its persistence by inserting itself into startup locations, so it reappears every time you restart your computer. While Task Manager's Startup tab only shows a limited number of startup processes, Autoruns digs much deeper. It scans the Registry, Task Scheduler, WMI, and other hidden areas of Windows to provide a comprehensive list of programs set to run at startup.

My preferred method for using Autoruns is to filter out legitimate Microsoft entries, leaving me with a concise list of third-party software. I focus on any entries marked in pink, indicating unsigned code, which is a big red flag. If I find any unsigned program running from a temporary location like AppData\Local\Temp, I immediately suspect malware is at work.

4. Process Monitor: Granular Tracking for Advanced Threats

For dealing with especially persistent infections, Process Monitor (ProcMon) is my go-to tool. Unlike the other Sysinternals tools, ProcMon records every activity in real-time, including file system changes, registry edits, and running processes. It's incredibly detailed—sometimes too detailed—but it's perfect for tracking down malware that refuses to stay dead.

I typically use ProcMon when I need to pinpoint specific actions, like identifying which file is recreating a suspicious registry key after I delete it. After pausing the initial flood of data, I drag the tool's target icon onto the suspicious process to filter the log and focus on that particular activity.

For more content like and follow me:  **@bertblevins**

5. Sysmon: The Long-Term Surveillance Tool

While the tools above are great for catching malware in the act, Sysmon (System Monitor) is ideal for ongoing surveillance. Sysmon runs quietly in the background and logs everything it detects to the Windows Event Log. It records every process that starts, every network connection, and every file loaded—providing a detailed history of your system's activity.

What I rely on most is Sysmon's Event ID 1, which logs process creation. This allows me to track back through time and uncover exactly what caused a mysterious file to appear on my desktop. It's like having a digital trail that helps me piece together the puzzle of what happened when I wasn't looking.

Conclusion: Empowering Your System with Sysinternals

Using these five Sysinternals tools has given me far more control over my Windows PC's security than traditional antivirus software ever could. They allow me to uncover and address issues that might otherwise fly under the radar. The best part? These tools are free and portable, so I can run them on any Windows machine without worrying about compatibility.

If you're looking to level up your ability to detect suspicious behavior on your PC, I highly recommend exploring these tools. Not only will you learn a lot about how Windows works under the hood, but you'll also gain valuable skills in system troubleshooting and security.
Happy hunting!

For more content like and follow me:  **@bertblevins**