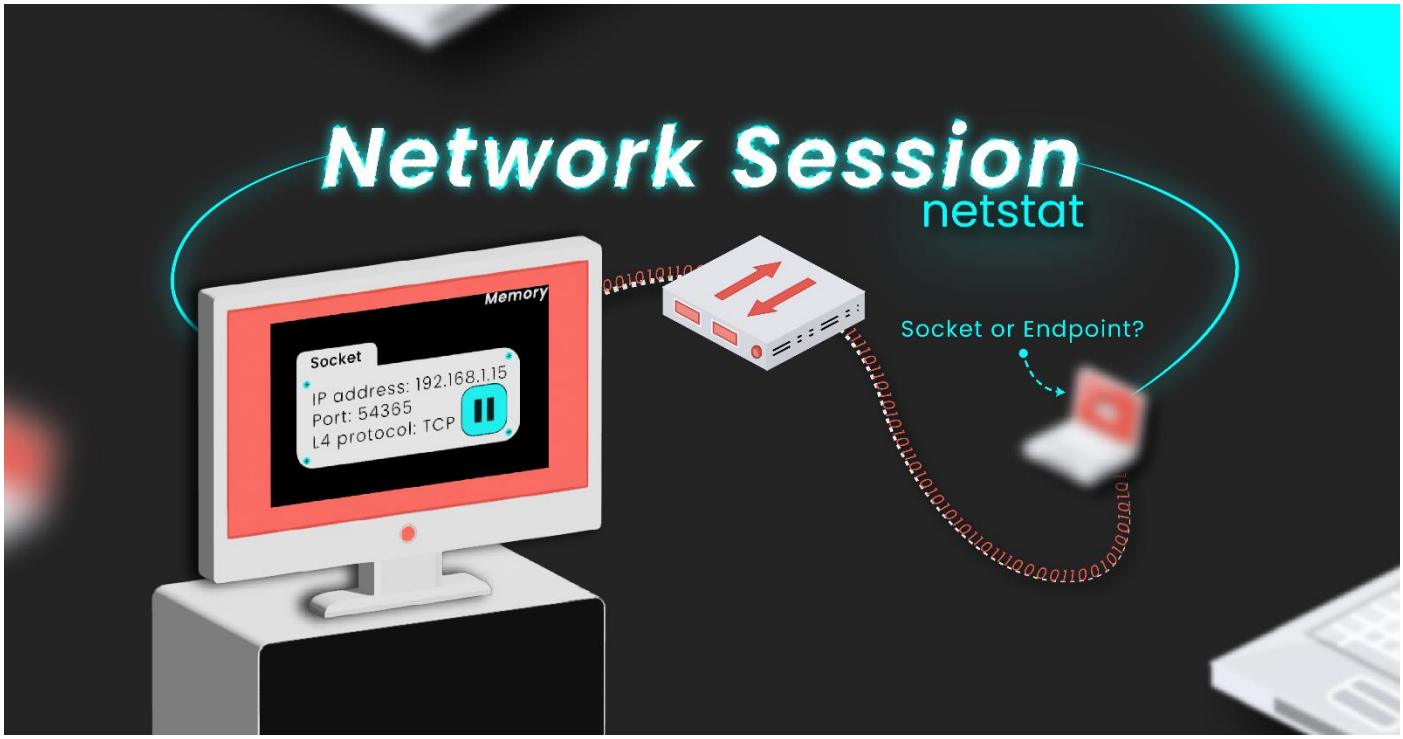
See Your Malicious Network Sessions | Revealing With netstat



Blog post summary:

- **Key networking terms:**
  - **A session** refers to the connection between two hosts.
  - **A socket**, or **endpoint**, refers to the session information stored in memory on one host.
  - **A socket pair**, or **endpoints**, refers to the session information stored in memory on two hosts about the same connection.
- **With netstat,** you can know a lot about active connections, listening ports, and protocol statistics on your computer.

- **To distinguish between legitimate and malicious connections,** monitor active connections and track them by Process ID and name. Research any unfamiliar process names to verify their legitimacy. If you identify malicious processes, take steps to remove them.
- **Most netstat options summary:**

Most netstat Options	
No switches	Active TCP sessions
-a	All active sessions & listening ports
-n	IP addresses & port numbers numerically
-o	Process ID (PID)
-f	Fully Qualified Domain Name (FQDN)
-b	Process Name
-p	specify protocol, -p *protocol*
-r	Network Interfaces, their MAC addresses, IPv4 and IPv6 routing tables
-s	Protocol statistics: IPv4, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, UDPv6
-e	Ethernet statistics