Rule

alert udp any any -> any 1434 (msg: “Slammer Worm Detected”; content:”|04 01|”; sid:1000019; rev:1;)

Description

This Snort rule is designed to detect traffic associated with the Slammer Worm, one of the best-known worms that spread explosively in early 2003, after the examination we have made using wireshark. It checks for the UDP packets generated from any source to any destination on port number 1434 (Microsoft SQL Server port), which has been utilized by inspecting the pcap file. This rule generates an alert when the payload contains the binary pattern |04 01|. This pattern was the signature for Slammer Worm's payload.

It generates an event upon detecting and then logs an alert with the message "Slammer Worm Detected" along with the unique identifier of sid:1000019 with revision 1 being the first rule revision for it. But like all signature-based approaches, this rule will only find the particular Slammer Worm variant that it was designed to match and will not catch modified or obfuscated versions of the worm.

Screenshot of alert

