Threat Category: Malware / Backdoor

Threat Description: The SNORT rule2_h detects malicious network activity associated with the QAZ Worm, a backdoor that allows attackers to control infected machines remotely. The rule specifically identifies login attempts by detecting the string "qazwsx.hsq", a unique identifier used by the worm during its communication with the command-and-control (C2) server.

Indicators of Compromise (IoCs)

Targeted Port: 7597

Signature Pattern: "qazwsx.hsq"

Rule SID: 108

Revision: 12

Detection Mechanism: The rule looks for TCP traffic from $EXTERNAL_NET to $HOME_NET on port 7597. It checks for the presence of the unique string "qazwsx.hsq", which signifies an infected system communicating with a QAZ Worm C2. The connection must be established for the rule to trigger.

Recommended Actions:

Monitor and Investigate: Look for suspicious connections to port 7597.

Containment & Mitigation: Isolate infected hosts and remove the QAZ Worm from the network.

Threat Hunting & Intelligence Sharing: Share intelligence with cybersecurity communities.