Threat Category: Malware / Backdoor

Threat Description: The SNORT rule is designed to detect network traffic associated with the Infector 1.x backdoor. This rule focuses on traffic from an internal network to an external network. The detection mechanism involves checking for the presence of the string "WHATISIT" within the TCP packet payload at a depth of 9 bytes. This string is a characteristic marker used by the Infector 1.x backdoor.

Indicators of Compromise (IoCs):

Content Pattern: "WHATISIT" (at depth 9)

Detection Mechanism:

This rule identifies potential Infector 1.x backdoor activity using the following conditions:

The network protocol must be TCP.

The traffic direction must be from $HOME_NET to $EXTERNAL_NET.

The TCP connection must be established.

The payload must contain the string "WHATISIT" at a depth of 9 bytes.

Possible Attribution & Use Cases:

The detection can be used to identify systems infected with the Infector 1.x backdoor.

Recommended Actions:

Remediation: Remove the Infector 1.x backdoor from infected systems and restore any affected files.

Network Security: Implement intrusion detection and prevention systems to block known backdoor traffic.

Vulnerability Management: Ensure that systems are patched and up-to-date to prevent exploitation

of vulnerabilities that could lead to backdoor infections.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 117

Rule Revision: 17

Reference: Nessus, 11157