Threat Category: Malware, Backdoor

Threat Description:The SNORT rule "rule10_m" is designed to detect attempts to use the Back Construction 2.1 backdoor to initiate an FTP connection. This rule focuses on traffic from an external network to an internal network on TCP port 666. The detection mechanism involves checking for the presence of the string "FTPON" within the TCP packet payload. This string is a command used by the Back Construction 2.1 backdoor to request an FTP connection. [cite: 10]

Indicators of Compromise (IoCs):

TCP Port: 666

Content Pattern: "FTPON"

Detection Mechanism:

The network protocol must be TCP.

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

The destination port must be 666.

The TCP connection must be established.

The payload must contain the string "FTPON".

Recommended Actions:

Containment: Isolate any potentially infected systems to prevent further unauthorized access or activity.

Remediation: Remove the Back Construction 2.1 backdoor from infected systems.

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

Classtype: misc-activity

Rule SID: 157

Rule Revision: 9