Threat Category: Malware, Backdoor

Threat Description: This rule is designed to detect responses from a BackConstruction 2.1 server indicating an open FTP port. This detection focuses on identifying specific server replies that suggest the presence of the BackConstruction backdoor, which is known to open FTP services for unauthorized access. The rule specifically looks for the string "FTP Port open" in the server's response to a client.

Indicators of Compromise (IoCs)

Content: "FTP Port open"

Detection Mechanism:

The traffic flow must be from the server to the client (to_client).

The TCP connection must be established (established).

The destination port is 666.

The rule checks for the presence of the string "FTP Port open" in the packet's content.

Possible Attribution & Use Cases:

The detection indicates the possible presence of a BackConstruction 2.1 backdoor on the server.

BackConstruction is a type of malware that allows unauthorized access and control of the compromised system.

This rule can be used to identify and block attempts to use the BackConstruction backdoor for malicious activities, such as data exfiltration or further malware deployment.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the presence of the BackConstruction backdoor.

Containment & Mitigation: Isolate the affected system to prevent further spread. Remove the backdoor and secure the system.

Author & Attribution:

Rule Author: community

Ruleset: community

SID: 158

Revision: 10