Threat Category: Malware, Backdoor

Threat Description: The SNORT rule is designed to detect initial connection attempts to a Matrix 2.0 backdoor server. This detection focuses on identifying client traffic containing the specific content "activate," which is indicative of a Matrix 2.0 client attempting to connect and activate the backdoor.

Indicators of Compromise (IoCs)

Content: "activate"

Detection Mechanism:

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

The traffic is UDP.

The source port is 3344 and the destination port is 3345.

The rule checks for the presence of the string "activate" in the packet's content.

Possible Attribution & Use Cases:

The detection indicates a possible Matrix 2.0 client attempting to connect to a Matrix 2.0 backdoor server.

Matrix 2.0 is a type of malware that allows unauthorized access and control of the compromised system.

This rule can be used to identify and block initial connection attempts to the Matrix 2.0 backdoor.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the presence of the Matrix 2.0 backdoor.

Containment & Mitigation: Isolate the affected system to prevent further spread. Identify and block the source of the malicious traffic.

Author & Attribution:

Rule Author: community

Ruleset: community

SID: 161

Revision: 10