

Threat Category: Malware, Backdoor, Trojan

Threat Description: This rule is designed to detect responses from a DeepThroat 3.1 server. This detection focuses on identifying UDP traffic containing the specific string "Ahhhh My Mouth Is Open," which is a characteristic response from the DeepThroat 3.1 backdoor server.

Indicators of Compromise (IoCs)

Content: "Ahhhh My Mouth Is Open"

Detection Mechanism:

This rule identifies potential DeepThroat 3.1 server activity using the following conditions:

The traffic is UDP.

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

The source port is 2140.

The rule checks for the presence of the string "Ahhhh My Mouth Is Open" in the packet's content.

Possible Attribution & Use Cases:

The detection indicates the possible presence of a DeepThroat 3.1 backdoor server.

DeepThroat 3.1 is a type of malware that allows unauthorized access and control of the compromised system.

This rule can be used to identify and block DeepThroat 3.1 backdoor communications.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the presence of the DeepThroat 3.1 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

Reference: nessus,10053

SID: 195

Revision: 15