Threat Category: Malware, Backdoor, Trojan

Threat Description: The rule is designed to detect activity indicative of a PhaseZero server. This detection focuses on identifying TCP traffic containing the specific string "phAse zero server," which is a characteristic response from the PhaseZero backdoor server. The rule checks for this string within the first 17 bytes of the payload, ignoring case sensitivity.

Indicators of Compromise (IoCs)

Content: "phAse zero server" (case-insensitive)

Detection Mechanism:

The traffic is TCP.

The traffic flow is from the server to the client and the TCP connection must be established (to_client,established).

The source port is 555.

The rule checks for the presence of the string "phAse zero server" (case-insensitive) within the first 17 bytes of the packet's content.

Possible Attribution & Use Cases:

The detection indicates the possible presence of a PhaseZero backdoor server.

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

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

Recommended Actions:

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

Metadata: policy max-detect-ips drop

Reference: url,www.megasecurity.org/trojans/p/phasezero/PhaseZero1.0b.html

Reference: url,www3.ca.com/securityadvisor/pest/pest.aspx?id=4539

SID: 208

Revision: 13