Threat Category: Malware, Backdoor

Threat Description: The rule is designed to detect activity indicative of a WinCrash 1.0 server. This detection focuses on identifying TCP traffic with specific flags and content that are characteristic of the WinCrash 1.0 backdoor. The rule specifically looks for the ACK and SYN flags set (AS, 12) and the content "|B4 B4|".

Indicators of Compromise (IoCs)

Flags: AS, 12 (ACK and SYN)

Content: "|B4 B4|" (hexadecimal representation)

Detection Mechanism:

The traffic is TCP.

The traffic flow is stateless.

The destination port is 5714.

The TCP flags are ACK and SYN (AS, 12).

The rule checks for the presence of the hexadecimal string "|B4 B4|" in the packet's content.

Possible Attribution & Use Cases:

The detection indicates the possible presence of a WinCrash 1.0 backdoor server.

WinCrash 1.0 is a type of malware that allows unauthorized access and control of the compromised system.

This rule can be used to identify and block WinCrash 1.0 backdoor activity.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the presence of the WinCrash 1.0 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: 163

Revision: 14