Threat Category: Malware/Backdoor, Trojan

Threat Description: This rule is designed to detect the presence of the GateCrasher backdoor. This rule focuses on traffic from an internal network to an external network on TCP port 6969. The detection mechanism involves checking for specific strings within the TCP packet payload. Specifically, it checks for "GateCrasher" at a depth of 11 (case-insensitive), "Server" (case-insensitive) with a distance of 0, "On-Line..." (case-insensitive) with a distance of 0, and uses a PCRE to match the pattern /^GateCrasher\s+v\d+\x2E\d+\x2C\s+Server\s+On-Line\x2E\x2E\x2E/ims. These patterns are indicative of communication from a system infected with the GateCrasher backdoor.

Indicators of Compromise (IoCs):

TCP Port: 6969

Content Pattern 1: "GateCrasher" (depth 11, case-insensitive)

Content Pattern 2: "Server" (distance 0, case-insensitive)

Content Pattern 3: "On-Line..." (distance 0, case-insensitive)

PCRE Pattern: ?/^GateCrasher\s+v\d+\x2E\d+\x2C\s+Server\s+On-Line\x2E\x2E\x2E/ims?

Detection Mechanism:This rule identifies potential GateCrasher backdoor activity using the following conditions:

The network protocol must be TCP.

The traffic direction must be from $HOME_NET to $EXTERNAL_NET.

The source port must be 6969.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the affected systems to confirm the presence of the GateCrasher backdoor.

Containment: Isolate any infected systems to prevent further spread of the malware.

Remediation: Remove the GateCrasher backdoor from infected systems.

Network Analysis: Analyze network traffic to identify the source of the infection and any additional compromised systems.

Prevention: Implement security measures to prevent future infections, such as updating antivirus software, patching vulnerabilities, and enforcing strong access controls.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Metadata: policy max-detect-ips drop, ruleset community

Reference: url,www.spywareguide.com/product_show.php?id=973

Classtype: trojan-activity

Rule SID: 147

Rule Revision: 12