Sid 1-34217

snort.org/rule_docs/1-34217

Rule Category

MALWARE-CNC -- Snort has detected a Comand and Control (CNC) rule violation, most likely for commands and calls for files or other stages from the control server. The alert indicates a host has been infiltrated by an attacker, who is using the host to make calls for files, as a call-home vector for other malware-infected networks, for shuttling traffic back to bot owners, etc.

Alert Message

MALWARE-CNC Win.Trojan.Aytoke variant outbound connection

Rule Explanation

This event is generated when activity relating to malware is detected. Impact: Serious. Possible existance of malware on the target host. Details: This activity is indicative of malware activity on a host. In this case the MALWARE-CNC Win.Trojan.Aytoke variant outbound connection was detected. Ease of Attack: Simple. This may be an indication of a malware infestation.

What To Look For

Known Usage

No public information

False Positives

No known false positives

Contributors

Cisco Talos

MITRE ATT&CK Framework

Tactic:

Technique:

For reference, see the MITRE ATT&CK vulnerability types here: https://attack.mitre.org

Additional Links

www.virustotal.com/en/file/0e0a7056024c00f95470a4e56ee8a2f67c717414ad38c28f30476c0462822e4f/analysis/

Rule Vulnerability

CVE Additional Information