Snort - Rule Docs 1:26941

Archived: 2026-04-05 20:43:17 UTC

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.PipCreat RAT dropper download

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.PipCreat RAT dropper download was detected. Ease of Attack: Simple. This may be an indication of a malware infestation.

What To Look For

No information provided

Known Usage

No public information

False Positives

No known false positives

Contributors

Cisco Talos

Rule Groups

No rule groups

None

Additional Links

Rule Vulnerability

No information provided

CVE Additional Information

This product uses data from the NVD API but is not endorsed or certified by the NVD.

None
