Threat Category: Malware / Backdoor

Threat Description: The YARA rule rule1_h is designed to detect network traffic associated with the Dagger 1.4.0 backdoor. This rule identifies TCP communication on port 2589, specifically targeting established connections where certain hexadecimal content patterns indicate the presence of malicious activity.

Targeted Port: 2589

Content Pattern: "2|00 00 00 06 00 00 00|Drives|24 00|"

Rule SID: 105

Detection Mechanism: The rule monitors outbound traffic from $HOME_NET to $EXTERNAL_NET on TCP port 2589. It checks for the presence of the specific content pattern associated with Dagger 1.4.0 malware. Only triggers if the connection is to_client and established.

Recommended Actions: Monitor and Investigate: Examine logs for unauthorized outbound connections on port 2589.

Containment & Mitigation: Block outbound traffic on port 2589 if suspicious activity is detected.

Threat Hunting & Intelligence Sharing: Share findings with security teams to enhance detection strategies.