Threat Category: Malware, Command and Control

Threat Description: The YARA rule is designed to detect Cobalt Strike C2 (Command and Control) host artifacts. This rule identifies specific string patterns that are indicative of Cobalt Strike C2 servers.

The detection mechanism focuses on identifying files that meet the following criteria:

The file contains the string "#Host:"

The file does not contain the string "#Host: %s"

The file's first 4 bytes are not equal to 0x0a786564.

The file's first 4 bytes are not equal to 0x0a796564.

Indicators of Compromise (IoCs):

Presence of the string "#Host:"

Absence of the string "#Host: %s"

Specific byte patterns at the beginning of the file (See Threat Description)

Possible Attribution & Use Cases:

The rule detects artifacts associated with Cobalt Strike, a popular penetration testing tool that is also widely used by threat actors for command and control.

Detection of Cobalt Strike C2 indicators suggests potential malicious activity and the presence of an active command and control infrastructure.

Recommended Actions:

Investigation: If this rule is triggered, investigate network traffic and system logs for connections to the detected C2 host.

Network Blocking: Block communication with the identified C2 host to disrupt attacker activity.

Endpoint Analysis: Analyze affected endpoints for signs of compromise and Cobalt Strike beacons.

Threat Hunting: Proactively search for other Cobalt Strike indicators within the network.

Intelligence Sharing: Share information about the detected C2 host with relevant security communities.

Author & Attribution:

Rule Author: yara@s3c.za.net

Rule Date: 2019-08-16

Rule Identifier: 7f15ee30-664e-59b8-9e31-35d88e58a45e