Threat Category: Malware, Backdoor

Threat Description: The rule is designed to detect communication indicative of the CDK backdoor. This detection focuses on identifying TCP traffic containing the specific string "ypi0ca," which is associated with the CDK backdoor. The rule checks for this string within the first 15 bytes of the payload, ignoring case sensitivity.

Indicators of Compromise (IoCs)

Content: "ypi0ca" (case-insensitive)

Detection Mechanism:

The traffic is TCP.

The traffic flow is from the server to the client and the TCP connection must be established (to_server,established).

The destination port is 79.

The rule checks for the presence of the string "ypi0ca" (case-insensitive) within the first 15 bytes of the packet's content.

Possible Attribution & Use Cases:

The detection indicates the possible presence of the CDK backdoor.

CDK is a type of malware that allows unauthorized access and control of the compromised system.

This rule can be used to identify and block CDK backdoor communications.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the presence of the CDK backdoor.

Containment & Mitigation: Isolate the affected system to prevent further spread. Remove the

backdoor and secure the system.

Threat Hunting & Intelligence Sharing: Use this rule to proactively hunt for similar activity. Share information with the security community to improve detection and prevention efforts.

Author & Attribution:

Rule Author: community

Ruleset: community

SID: 185

Revision: 10