Threat Category: Malware, Dropper

Threat Description: The YARA rule rule7_h is designed to detect a specific dropper that originates from a CAB file, as mentioned in a Kaspersky report. This rule identifies files that contain specific strings indicating the presence of the dropper.

The detection mechanism focuses on identifying files that meet the following criteria:
The file must be a valid Portable Executable (PE) file, indicated by the MZ header (0x5A4D).
The file size must be less than 1000KB.
The file must contain both of the following ASCII strings:
"029.Hdl" (fullword ascii)
"http.exe" (fullword ascii)

Indicators of Compromise (IoCs):
MZ Header: 0x5A4D
File size: < 1000KB
Specific strings: (See Threat Description)
MD5 Hash: 9e7e5f70c4b32a4d5e8c798c26671843e76bb4bd5967056a822e982ed36e047b

Possible Attribution & Use Cases:
The rule detects a dropper associated with threats involving CVE-2015-2545, as reported by Kaspersky.
Droppers are used to install other malware, indicating a potential for further infection.
Detection of this dropper suggests an attempt to exploit vulnerabilities and install additional malicious payloads.

Recommended Actions:

Investigation: If this rule is triggered, investigate the system for the presence of other malware and the exploit used to deliver the dropper.

Removal: Remove the identified dropper and any associated malicious files.

Patching: Apply patches to address the vulnerabilities that may have been exploited.

Enhanced Security: Implement enhanced security measures to prevent future dropper attacks, such as email filtering and web security.

Intelligence Sharing: Share information about the dropper and associated activity with relevant security communities.

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Reference: https://goo.gl/13Wgy1

Rule Date: 2016-05-25

Rule Identifier: f67c13e9-67e7-56aa-8ced-55e9bb814971