Threat Category: Malware, Dropper

Threat Description: The YARA rule is designed to detect the Casper French Espionage Malware, specifically the Win32/ProxyBot.B dropper.

The detection mechanism focuses on identifying files that contain at least seven of the following strings:

"<Command>" (fullword ascii)

"</Command>" (fullword ascii)

"" /d "" (fullword ascii)

"'%s' %s" (fullword ascii)

"nKERNEL32.DLL" (fullword wide)

"@ReturnValue" (fullword wide)

"ID: 0x%x" (fullword ascii)

"Name: %S" (fullword ascii)

Indicators of Compromise (IoCs):

Specific strings: (See Threat Description)

MD5 Hash: e4cc35792a48123e71a2c7b6aa904006343a157a

Possible Attribution & Use Cases:

The rule detects a dropper associated with the Casper French Espionage Malware.

This malware is also known as Win32/ProxyBot.B.

Droppers are used to install other malware, indicating a potential for further infection.

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.

Enhanced Security: Implement enhanced security measures to prevent future dropper attacks.

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

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Reference: http://goo.gl/VRJNLo

Rule Date: 2015/03/05

Rule Identifier: a901d045-6f9b-57e8-8347-6f78178b7231