Threat Category: Malware, APT30, Backspace Malware

Threat Description: The YARA rule is designed to detect Backspace Malware, specifically a sample mentioned in the FireEye APT30 report.

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

The file size must be less than 100KB.

The file must be a valid Portable Executable (PE) file, indicated by the MZ header (0x5A4D).

The file must contain all of the following strings:

$s0 = "ForZRLnkWordDlg.EXE" fullword wide

$s1 = "ForZRLnkWordDlg Microsoft " fullword wide

$s9 = "ForZRLnkWordDlg 1.0 " fullword wide

$s11 = "ForZRLnkWordDlg" fullword wide

$s12 = " (C) 2011" fullword wide

Indicators of Compromise (IoCs):

File size: < 100KB

MZ Header: 0x5A4D

MD5 Hash: 0359ffbef6a752ee1a54447b26e272f4a5a35167

Possible Attribution & Use Cases:

The rule detects a sample of Backspace Malware.

Backspace Malware is associated with the APT30 group.

APT30 is known for conducting cyber espionage activities.

Recommended Actions:

Investigation: If this rule is triggered, investigate the affected system for signs of APT30 activity and related malware.

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

Network Monitoring: Monitor network traffic for suspicious connections and command and control activity.

Intelligence Sharing: Share information about the APT30 activity with relevant security communities.

Author & Attribution:

Rule Author: Florian Roth

Rule Reference: https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Rule Date: 2015/04/13

Rule Identifier: 821a2de9-48c4-58d8-acc4-1e25025ab5cf