Threat Category: Malware, APT30, Backspace Malware

Threat Description: The YARA rule rule1_h is designed to detect Backspace Malware, specifically a generic 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:

"\Temp1020.txt" (ascii)

"Xmd.Txe" (fullword ascii)

"\Internet Exp1orer" (ascii)

Indicators of Compromise (IoCs):

File size: < 100KB

MZ Header: 0x5A4D

Hashes:

2a4c8752f3e7fde0139421b8d5713b29c720685d

4350e906d590dca5fcc90ed3215467524e0a4e3d