Threat Name: APT_Dropper_Win_MATRYOSHKA

Threat Category: Malware Dropper, Advanced Persistent Threat (APT)

Threat Description: The YARA rule APT_Dropper_Win_MATRYOSHKA_1 detects Matryoshka, a sophisticated multi-layered malware dropper. It embeds multiple payloads within itself, executing them sequentially to evade detection.

Indicators of Compromise (IoCs):

Strings related to execution errors and process spawning:

"matryoshka.exe", "Unable to write data", "NTStatus: \n", "failed to execute process"

MD5 Hash: edcd58ba5b1b87705e95089002312281

Detection Mechanism:

Identifies PE files that execute multiple embedded payloads in layered fashion.

Possible Attribution & Use Cases:

Used in stealthy malware deployment operations.

Strings:

"\x00matryoshka.exe\x00"

"\x00Unable to write data\x00"

"\x00Error while spawning process. NTStatus: \x0a\x00"

"\x00.execmdstart/Cfailed to execute process\x00"

Recommended Actions:

Monitor execution of unknown binaries with multi-stage behaviors.

Author & Attribution:

Rule Author: FireEye