

Threat Name: APT\_Dropper\_Win64\_MATRYOSHKA

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

Threat Description: The YARA rule APT\_Dropper\_Win64\_MATRYOSHKA\_1 detects Matryoshka, a layered malware dropper used for stealthy payload delivery.

Indicators of Compromise (IoCs):

Assembly instruction sequences matching dropper logic.

MD5 Hash: edcd58ba5b1b87705e95089002312281

Strings:

{ 8D 8D [4] E8 [4] 49 89 D0 C6 [2-6] 01 C6 [2-6] 01 [0-8] C7 44 24 ?? 0E 00 00 00 4C 8D 0D [4] 48 8D 8D [4] 48 89 C2 E8 [4] C6 [2-6] 01 C6 [2-6] 01 48 89 E9 48 8D 95 [4] E8 [4] 83 [2] 01 0F 8? [4] 48 01 F3 48 29 F7 48 [2] 08 48 89 85 [4] C6 [2-6] 01 C6 [2-6] 01 C6 [2-6] 01 48 8D 8D [4] 48 89 DA 49 89 F8 E8 }

{ 0F 29 45 ?? 48 C7 45 ?? 00 00 00 00 0F 29 45 ?? 0F 29 45 ?? 0F 29 45 ?? 0F 29 45 ?? 0F 29 45 ?? 0F 29 45 ?? 00 00 00 00 C7 45 ?? 68 00 00 00 48 8B [2] 48 8D [2] 48 89 [3] 48 89 [3] 0F 11 44 24 ?? C7 44 24 ?? 08 00 00 0C C7 44 24 ?? 00 00 00 00 31 ?? 48 89 ?? 31 ?? 45 31 ?? 45 31 ?? E8 [4] 83 F8 01 }

Detection Mechanism:

Detects multi-layer malware unpacking techniques.

Possible Attribution & Use Cases:

Used to deploy secondary-stage malware.

#### Recommended Actions:

Monitor for multi-stage payload delivery events.

#### Author & Attribution:

Rule Author: FireEye