Threat Category: Advanced Persistent Threat (APT) ? Rootkit/Driver-Level Implants

Threat Name: Duqu 2.0 ? Driver Component

Threat Description: Duqu 2.0 is a highly sophisticated malware linked to the same threat actor behind the original Duqu and Stuxnet attacks. It uses advanced driver-level implants for stealth and persistence. This YARA rule targets driver files associated with Duqu 2.0, as identified by Kaspersky Lab during their incident response investigation.

Indicators of Compromise (IoCs):

Wide and ASCII strings indicative of Duqu 2.0 driver behavior:

$a1 = "\\DosDevices\\port_optimizer" (wide, nocase)

$a2 = "romanian.antihacker" (ascii)

$a3 = "PortOptimizerTermSrv" (wide)

$a4 = "ugly.gorilla1" (ascii)

$b1 = "NdisIMCopySendCompletePerPacketInfo" (ascii)

$b2 = "NdisReEnumerateProtocolBindings" (ascii)

$b3 = "NdisOpenProtocolConfiguration" (ascii)

Detection Mechanism:

File must start with the 'MZ' magic number: uint16(0) == 0x5A4D

File size must be less than 100KB.

Must match:

At least one string from group $a*

At least two strings from group $b*

Rule Name: APT_apt_duqu2_drivers

Rule Metadata:

author: Mixed (Kaspersky Lab & Florian Roth)

copyright: Kaspersky Lab

description: Rule to detect Duqu 2.0 drivers

last_modified: 2015-06-09

version: 1.0

id: 714d5151-9f80-582e-a628-1de9d83a072d

Date Published: 2015-06-10