Duqu 2.0

Yara rules

```
rule apt_duqu2_loaders {

meta:

        copyright = "Kaspersky Lab"
        description = "Rule to detect Duqu 2.0 samples"
        last_modified = "2015-06-09"
        version = "1.0"


strings:

        $a1="{AAFFC4F0-E04B-4C7C-B40A-B45DE971E81E}" wide
        $a2="\\\\.\\pipe\\{AAFFC4F0-E04B-4C7C-B40A-B45DE971E81E}" wide
        $a4="\\\\.\\pipe\\{AB6172ED-8105-4996-9D2A-597B5F827501}" wide
        $a5="Global\\{B54E3268-DE1E-4c1e-A667-2596751403AD}" wide
        $a8="SELECT `Data` FROM `Binary` WHERE `Name`='%s%i'" wide
        $a9="SELECT `Data` FROM `Binary` WHERE `Name`='CryptHash%i'" wide
        $a7="SELECT `%s` FROM `%s` WHERE `%s`='CAData%i'" wide

        $b1="MSI.dll"
        $b2="msi.dll"
        $b3="StartAction"

        $c1="msisvc_32@" wide
        $c2="PROP=" wide
        $c3="-Embedding" wide
        $c4="S:(ML;;NW;;;LW)" wide

        $d1 =
"NameTypeBinaryDataCustomActionActionSourceTargetInstallExecuteSequenceConditionSequenceProp
ertyValueMicrosoftManufacturer" nocase
        $d2 = {2E 3F 41 56 3F 24 5F 42 69 6E 64 40 24 30 30 58 55 3F 24 5F 50 6D 66 5F 77 72 61 70 40
50 38 43 4C 52 ?? 40 40 41 45 58 58 5A 58 56 31 40 24 24 24 56 40 73 74 64 40 40 51 41 56 43 4C 52 ??
40 40 40 73 74 64 40 40}

condition:

        ( (uint16(0) == 0x5a4d) and ( (any of ($a*)) or (all of ($b*)) or (all of ($c*)) ) and filesize < 100000
)
```

```
        or

        ( (uint32(0) == 0xe011cfd0) and ( (any of ($a*)) or (all of ($b*)) or (all of ($c*)) or (any of ($d*)) )
and filesize < 20000000 )


}



rule apt_duqu2_drivers {

meta:

        copyright = "Kaspersky Lab"
        description = "Rule to detect Duqu 2.0 drivers"
        last_modified = "2015-06-09"
        version = "1.0"

strings:


        $a1="\\DosDevices\\port_optimizer" wide nocase
        $a2="romanian.antihacker"
        $a3="PortOptimizerTermSrv" wide
        $a4="ugly.gorilla1"

        $b1="NdisIMCopySendCompletePerPacketInfo"
        $b2="NdisReEnumerateProtocolBindings"
        $b3="NdisOpenProtocolConfiguration"

condition:

        uint16(0) == 0x5A4D and (any of ($a*) ) and (2 of ($b*)) and filesize < 100000

}
```