

Folders created by the malware

- ☐ I
- ☐ I
- ☐ I

Malicious attachments

K I O O	

OK O	
O	

Malware modules installed in the system

O I	
O I	
II O OK I	
II O OK I	
O I	
O I	
O I	

Legitimate objects used by the malware

O I	
O I	
O I	
O I	
O I D D	
O I D D	

O I	

O I

00 0 0	0 1 0 1
00 0 0 0	
00 0 0	
00 0 0	
00 0 0	
00 0 0 k	
00 0 0	

Typical characteristics of the network activity of legitimate software used by the attackers

Servers used by the attackers

```
rule RMS_winspooldrv_dllhijack {
meta:
    description = "winspool.drv malicious file used in RMS RAT"
    hash = "5a6efa2921d3174bb9808fa3a3400d13"
    hash = "bb188e1e92e2be8a1ff009fe22f58f7f"
    version = "1.1"
strings:
    $a1= "Password.rcfg" fullword
    $a2 = "Password.rcfg" wide fullword
    $b1= "winspool.drv" fullword
    $b2= "killrms" wide fullword
condition:
    uint16(0) == 0x5A4D
    and any of ($a*)
    and all of ($b*)
    and filesize < 100000
}

rule TeamViewer_msimg32_dllhijack {
meta:
    description = "msimg32.dll malicious file used in TeamViewer"
    hash = "16b4ebfdf74db8f730f2fb4d03e86d27"
    hash = "8c4e9016b9b4db809dd312f971a275b1"
    version = "1.1"

strings:
    $a1="msimg32.dll" fullword

condition:
    uint16(0) == 0x5A4D
    and any of ($a*)
    and pe.exports("SvcMain")
}
```