```
rule ransomware_exPetr

{

meta:


copyright = “Kaspersky Lab”

description = “Rule to detect PetrWrap ransomware samples”

last_modified = “2017-06-27”

author = “Kaspersky Lab”

hash = “71B6A493388E7D0B40C83CE903BC6B04”

version = “1.0”


strings:


$a1 =
“MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2Jm
URWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEF
LCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEU
w6o3pt5pNOskfOJbMan2TZu” fullword wide

$a2 =
“.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.
gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sq
l.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls” fullword wide

$a3 = “DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED”
fullword ascii

$a4 = “1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX” fullword ascii

$a5 = “wowsmith123456@posteo.net.” fullword wide


condition:


(uint16(0) == 0x5A4D) and

(filesize<1000000) and

(any of them)

}
```