

<https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/new-golang-ransomware-agenda-customizes-attacks/IOCs-blog-New%20Golang%20Ransomware%20Agenda%20Customizes%20Attacks.txt>

Archived: 2026-04-05 21:30:02 UTC

File name	SHA-256	Detection
N/A	117fc30c25b1f28cd923b530ab9f91a0a818925b0b89b8bc9a7f820a9e630464	Ransom.Win64.AGENDACR'
N/A	93d0cc8492511c663f17544b3bf14eab8ccb492909536e79ef652921d809bb1a	Ransom.Win64.AGENDACR'
N/A	e4a319f7afafbbd710ff2dbe8d0883ef332afcb0363efd4e919ed3c3faba0342	Ransom.Win64.AGENDACR'
pwndll.dll	28aeb2d6576b2437ecab535c0a1bf41713ee9864611965bf1d498a87cbdd2fab	Trojan.Win64.AGENDA.S'

Tor communication

- ygo44wtbprhx2kvibtgjj3rrjo3f4fccuahuavy6vvnvtrvihpruqduad[.]onion
 - pmbvfcoawmpkqptrcv3fmtqyvufbpiidrseseyvpxrmlbh727aoqmyd[.]onion
 - ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd[.]onion
-

Services that Agenda terminates:

acronis vss provider
acronisagent
acronisagentd
acrsch2svc
acrsch2svcd
adobearmservice
adobearmserviced
alerter
alerterd
arism
arsmd
aswbcc
aswbccd
avbackup
avbackupd
backup
backupexecagentaccelerator
backupexecagentaccelerator
backupexecagentbrowser
backupexecagentbrowserd
backupexecdevicemediaservice
backupexecdevicemediaserviced

backuexecjobengine
backuexecjobengine.d
backuexecmanagementservice
backuexecmanagementservice.d
backupexecrpcservice
backupexecrpcservice.d
backupexecvssprovider
backupexecvssprovider.d
bcbservice
bcbservice.d
bedbg
bedbg.d
bits
bits.d
bluestripecollector
bluestripecollectord
brokerinfrastructure
brokerinfrastructure.d
ccevtmgr
ccevtmgr.d
ccsetmgr
ccsetmgr.d
cissesrv
cissesrv.d
cpqrcmc3
cpqrcmc3.d
csadmin
csadmin.d
csauth
csauth.d
csdbsync
csdbsync.d
cslog
cslog.d
csmom
csmom.d
csradius
csradius.d
cstacacs
cstacacs.d
db2
db2-0
db2-0d
db2d
db2das00
db2das00d
db2governor_db2copy1
db2governor_db2copy1d
db2inst2
db2inst2d
db2licd_db2copy1
db2licd_db2copy1d
db2mgmtsvc_db2copy1
db2mgmtsvc_db2copy1d
db2remotecmd_db2copy1
db2remotecmd_db2copy1d

ehhttpsv
ehhttpsvd
ekrn
ekrnd
erasersvc11710
erasersvc11710d
ersvc
ersvcd
esgshkernel
esgshkerneld
eshasrv
eshasrvd
eventlog
eventlogd
fa_scheduler
fa_schedulerd
googlechromelevationservice
googlechromelevation serviced
gupdate
gupdated
gupdatem
gupdatemd
healthservice
healthserviced
ibmdataservertmgr
ibmdataservertmgrd
ibmdsserver41
ibmdsserver41d
idrivot
idrivotd
imapiservice
imapiserviced
klnagent
klnagentd
logprocessorservice
logprocessorserviced
lrsdrvx
lrsdrvxd
macmnsvc
macmnsvcd
masvc
masvcd
mbamservice
mbamserviced
mbendpointagent
mbendpointagentd
mcshield
mcshieldd
mentas
mepocs
mfefire
mfefired
mfemms
mfemmsd
mfevtp
mfevtpd

mfewc
mfewcd
mms
mmsd
mozyprobackup
mozyprobackupd
msexchange
msexchangees
msexchangeesd
msexchangeis
msexchangeisd
msexchangemgmt
msexchangemgtd
msexchangemta
msexchangemtad
msexchangesa
msexchangesad
msexchangesrs
msexchangesrsd
msftesql\$prod
msftesql\$prodd
msmq
msmqd
msolap\$sql_2008
msolap\$sql_2008d
msolap\$system_bgc
msolap\$system_bgcd
msolap\$tps
msolap\$tpsama
msolap\$tpsamad
msolap\$tpsd
mssql\$bkupexec
mssql\$bkupexecd
mssql\$citrix_metaframe
mssql\$citrix_metaframed
mssql\$ecwdb2
mssql\$ecwdb2d
mssql\$eposerver
mssql\$eposerverd
mssql\$itris
mssql\$itrisd
mssql\$net2
mssql\$net2d
mssql\$practicemgt
mssql\$practicemgtd
mssql\$practticebgc
mssql\$practticebgcd
mssql\$prod
mssql\$prodd
mssql\$profxengagement
mssql\$profxengagementd
mssql\$sbsmonitoring
mssql\$sbsmonitoringd
mssql\$sharepoint
mssql\$sharepointd
mssql\$sql_2008

mssql\$sql_2008d
mssql\$sqlexpress
mssql\$sqlexpressd
mssql\$system_bgc
mssql\$system_bgcd
mssql\$tps
mssql\$tpsama
mssql\$tpsamad
mssql\$tpsd
mssql\$veeamsql2008r2
mssql\$veeamsql2008r2d
mssql\$veeamsql2012
mssql\$veeamsql2012d
mssqlfdlauncher
mssqlfdlauncher\$itrisk
mssqlfdlauncher\$itriskd
mssqlfdlauncher\$profxengagement
mssqlfdlauncher\$profxengagementd
mssqlfdlauncher\$sbsmonitoring
mssqlfdlauncher\$sbsmonitoringd
mssqlfdlauncher\$sharepoint
mssqlfdlauncher\$sharepointd
mssqlfdlauncher\$sql_2008
mssqlfdlauncher\$sql_2008d
mssqlfdlauncher\$system_bgc
mssqlfdlauncher\$system_bgcd
mssqlfdlauncher\$tps
mssqlfdlauncher\$tpsama
mssqlfdlauncher\$tpsamad
mssqlfdlauncher\$tpsd
mssqlfdlauncherd
mssqllaunchpad\$itrisk
mssqllaunchpad\$itriskd
mssqlserver
mssqlserveradhelper
mssqlserveradhelper100
mssqlserveradhelper100d
mssqlserveradhelperd
mssqlserverd
mssqlserverolapservice
mssqlserverolapserviced
msvsmon90
msvsmon90d
mysql57
mysql57d
net2clientsvc
net2clientsvcd
nimbuswatcherservice
nimbuswatcherserviced
ntlmsp
ntlmspd
ntmssvc
ntmssvcd
ntrtscan
ntrtscand
odserv

odservd
oracleclientcache80
oracleclientcache80d
ose
osed
pdvfsservice
pdvfsserviced
pop3svc
pop3svcd
proliantmonitor
proliantmonitord
reportserver
reportserver\$sql_2008
reportserver\$sql_2008d
reportserver\$system_bgc
reportserver\$system_bgcd
reportserver\$tps
reportserver\$tpsama
reportserver\$tpsamad
reportserver\$tpsd
reportserverd
rscdsvc
rscdsvcd
rumorserver
sacsvr
sacsvrd
samss
samssd
savservice
savserviced
sdd_service
sdd_serviced
sdrsvc
sdrsvcd
sentinelagent
sentinelagentd
sentinelhelperservice
sentinelhelperserviced
sentinelstaticengine
sentinelstaticengine
sepmasterservice
sepmasterserviced
sepmasterservicemig
sepmasterservicemigd
shmonitor
shmonitord
smcinst
smcinstd
smcservice
smcserviced
smtpsvc
smtpsvcd
snac
snacd
snowinventoryclient
snowinventoryclientd

sntpservice
sntpserviced
sql
sql backups
sqlagent\$bkupexec
sqlagent\$bkupexecd
sqlagent\$citrix_metaframe
sqlagent\$citrix_metaframed
sqlagent\$cxdb
sqlagent\$cxdbd
sqlagent\$ecwdb2
sqlagent\$ecwdb2d
sqlagent\$eposerver
sqlagent\$eposerverd
sqlagent\$itris
sqlagent\$itrisd
sqlagent\$net2
sqlagent\$net2d
sqlagent\$practticebgc
sqlagent\$practticebgcd
sqlagent\$practicemgt
sqlagent\$practicemgtd
sqlagent\$prod
sqlagent\$prodd
sqlagent\$profxengagement
sqlagent\$profxengagementd
sqlagent\$sbsmonitoring
sqlagent\$sbsmonitoringd
sqlagent\$sharepoint
sqlagent\$sharepointd
sqlagent\$sql_2008
sqlagent\$sql_2008d
sqlagent\$sqlexpress
sqlagent\$sqlexpressd
sqlagent\$system_bgc
sqlagent\$system_bgcd
sqlagent\$tps
sqlagent\$tpsama
sqlagent\$tpsamad
sqlagent\$tpsd
sqlagent\$veeamsql2008r2
sqlagent\$veeamsql2008r2d
sqlagent\$veeamsql2012
sqlagent\$veeamsql2012d
sqlbrowser
sqlbrowserd
sqlsafe backup service
sqlsafe filter service
sqlsafeolrservice
sqlsafeolrserviced
sqlserveragent
sqlserveragentd
sqltelemetry
sqltelemetry\$ecwdb2
sqltelemetry\$ecwdb2d
sqltelemetry\$itris

sqltelemetry\$itrisd
sqltelemetryd
sqlwriter
sqlwriterd
ssistelemetry130
ssistelemetry130d
sstpsvc
sstpsvcd
svc\$
svcgenerichost
svcgenerichostd
swi_filter
swi_filterd
swi_service
swi_serviced
swi_update
swi_update_64
swi_update_64d
swi_updated
symantec
symantec system recovery
symantecd
sysdown
sysdownd
telemetryserver
telemetryserverd
tmccsf
tmccsfd
tmlisten
tmlistend
tpautoconnsvc
tpautoconnsvcd
tpvcgateway
tpvcgatewayd
truekey
truekeyd
truekeyscheduler
truekeyschedulerd
truekeyservicehelper
truekeyservicehelperd
tsm
tsmd
ui0detect
ui0detectd
veeam
veeam backup catalog data service
veeambackupsvc
veeambackupsvcd
veeambrokersvc
veeambrokersvcd
veeamcatalogsvc
veeamcatalogsvcd
veeamcloudsvc
veeamcloudsvcd
veeamdeploymentsservice
veeamdeploymentsserviced

```
veeamdeploysvc
veeamdeploysvcd
veeamenterprisemanagersvc
veeamenterprisemanagersvcd
veeamhvintegrationsvc
veeamhvintegrationsvcd
veeammountsvc
veeammountsvcd
veeamnfssvc
veeamnfssvcd
veeamrestsvc
veeamrestsvcd
veeamtransportsvc
veeamtransportsvcd
vgauthservice
vgauthserviced
vmtools
vmtoolsd
vmware
vmwarecafcommamqplistener
vmwarecafcommamqplistenerd
vmwarecafmanagementagenthost
vmwarecafmanagementagenthostd
vmware-converter-agent
vmware-converter-agentd
vmware-converter-server
vmware-converter-serverd
vmware-converter-worker
vmware-converter-workerd
vmwared
vss
w3svc
w3svcd
wbengine
wbengine.d
wdnissvc
wdnissvcd
windefend
windefendd
winvnc4
winvnc4d
wrsvc
wrsvcd
zoolz
```

Processes that Agenda terminates:

```
a2service.exe
a2start.exe
aawservice.exe
acaas.exe
acaegmgr.exe
acaif.exe
acais.exe
```

acctmgr.exe
aclient.exe
acIntusr.exe
ad-aware2007.exe
administrator.exe
adminserver.exe
aesecurityservice.exe
aexagentuihost.exe
aexnsagent.exe
aexnsrcvsvc.exe
aexsvc.exe
aexswdusr.exe
aflogvw.exe
afwserv.exe
agntsvc
agntsvc.exe
ahnrpt.exe
ahnsd.exe
ahnsdsv.exe
alert.exe
alertsvc.exe
almon.exe
alogserv.exe
alsvc.exe
alunotify.exe
alupdate.exe
aluschedulersvc.exe
amsvc.exe
amswmagt
aphost.exe
appsvc32.exe
aps.exe
apvxdwin.exe
ashbug.exe
ashchest.exe
ashcmd.exe
ashdisp.exe
ashenhcd.exe
ashlogv.exe
ashmaisv.exe
ashpopwz.exe
ashquick.exe
ashserv.exe
ashsimp2.exe
ashsimpl.exe
ashskpcc.exe
ashskpck.exe
ashupd.exe
ashwebsv.exe
asupport.exe
aswdisp.exe
aswregsvr.exe
aswserv.exe
aswupdsv.exe
aswwbsv.exe
atrshost.exe

atwsctsk.exe
aupdrun.exe
aus.exe
auth8021x.exe
autoup.exe
avcenter.exe
avconfig.exe
avconsol.exe
avengine.exe
avesvc.exe
avfwsvc.exe
avkproxy.exe
avkservice.exe
avktray.exe
avkwctl.exe
avltmain.exe
avmailc.exe
avmcdlg.exe
avnotify.exe
avscan.exe
avsc.exe
avserver.exe
avshadow.exe
avsynmgr.exe
avtask.exe
avwebgrd.exe
basfipm.exe
bavtray.exe
bcreporter.exe
bcbservice.exe
bdagent.exe
bdc.exe
bdlite.exe
bdmcon.exe
bdredline.exe
bdss.exe
bdsubmit.exe
bhipssvc.exe
bka.exe
blackd.exe
blackice.exe
bluestripecollector.exe
blupro.exe
bmrt.exe
bwgo0000
ca.exe
caantispyware.exe
caav.exe
caavcmdscan.exe
caavguiscan.exe
caf.exe
caf.w.exe
caissdt.exe
calogdump.exe
capfaem.exe
capfasem.exe

capfsem.exe
capmuamagt.exe
cappactiveprotection.exe
casc.exe
casecuritycenter.exe
caunst.exe
cavrep.exe
cavrid.exe
cavscan.exe
cavtray.exe
ccap.exe
ccapp.exe
ccemflsv.exe
ccenter.exe
ccevtmgr.exe
ccflic0.exe
ccflic4.exe
cclaw.exe
ccmmessaging.exe
ccnfagent.exe
ccprovsp.exe
ccproxy.exe
ccpxysvc.exe
ccschedulersvc.exe
ccsetmgr.exe
ccsmagtd.exe
ccsvchst.exe
ccsystemreport.exe
cctray.exe
ccupdate.exe
cdm.exe
certificateprovider.exe
certificationmanagerservicent.exe
cfftplugin.exe
cfnotsrvd.exe
cfp.exe
cfpconfig.exe
cfpconfig.exe
cfplogvw.exe
cfpsbmit.exe
cfpupdat.exe
cfsmsmd.exe
checkup.exe
chrome.exe
cis.exe
cistray.exe
cka.exe
clamscan.exe
clamtray.exe
clamwin.exe
client.exe
client64.exe
clps.exe
clpsla.exe
clpsls.exe
clshield.exe

cmdagent.exe
cmdinstall.exe
cmgrdian.exe
cntaosmgr.exe
collwrap.exe
comhost.exe
config_api_service.exe
console.exe
control_panel.exe
coreframeworkhost.exe
coreserviceshell.exe
cpd.exe
cpdclnt.exe
cpf.exe
cpntsrv.exe
cramtray.exe
crashrep.exe
crdm.exe
crssvc.exe
csacontrol.exe
csadmin.exe
csauth.exe
csdbsync.exe
csfalconservice.exe
csinject.exe
csinsm32.exe
csinsmnt.exe
cslog.exe
csmo.exe
csradius.exe
csrss_tc.exe
cssauth.exe
cstacacs.exe
ctdataload.exe
cwbunnav.exe
cylancesvc.exe
cylanceui.exe
dao_log.exe
dbeng50
dbeng50.exe
dbserv.exe
dbsnmp
dbsnmp.exe
dbsrv9.exe
defwatch
defwatch.exe
deloeminfo.exe
deteqt.agent.exe
diskmon.exe
djsnetcn.exe
dlservice.exe
dltray.exe
dolphinscharge.e
dolphinscharge.exe
doscan.exe
dpmra.exe

dr_serviceengine.exe
drwagntd.exe
drwagnui.exe
drweb.exe
drweb32.exe
drweb32w.exe
drweb386.exe
drwebcgp.exe
drwebcom.exe
drwebdc.exe
drwebmng.exe
drwebscd.exe
drwebupw.exe
drwebwcl.exe
drwebwin.exe
drwinst.exe
drwupgrade.exe
dsmcad.exe
dsmcsvc.exe
dwarkdaemon.exe
dwengine.exe
dwhwizrd.exe
dwnetfilter.exe
dwrcst.exe
dwwin.exe
edisk.exe
eeyeevnt.exe
egui.exe
ehhttpsrv.exe
ekrn.exe
elogsvc.exe
emlibupdateagentnt.exe
emlproui.exe
emlproxy.exe
encsvc
encsvc.exe
endpointsecurity.exe
engineserver.exe
entitymain.exe
epmd.exe
era.exe
erlsrv.exe
esecagntservice.exe
esecservice.exe
esmagent.exe
etagent.exe
etconsole3.exe
etcorrel.exe
etlogalyzer.exe
etreporter.exe
etrssfeeds.exe
etscheduler.exe
etwcontrolpanel.exe
euqmonitor.exe
eventparser.exe
evtarmgr.exe

evtmgr.exe
evtprocessecfile.exe
ewidoctrl.exe
excel
excel.exe
execstat.exe
fameh32.exe
fcappdb.exe
fcdblog.exe
fch32.exe
fchelper64.exe
fcsms.exe
fcssas.exe
fih32.exe
firefox
firefox.exe
firefoxconfig.exe
firesvc.exe
firetray.exe
firewallgui.exe
fmon.exe
fnplicensingsservice.exe
forcefield.exe
fpavserver.exe
fprottray.exe
frameworkservic
frameworkservic.exe
frameworkservice.exe
frzstate2k.exe
fsaa.exe
fsaua.exe
fsav32.exe
fsavgui.exe
fscuif.exe
fsdfwd.exe
fsgk32.exe
fsgk32st.exe
fsguidll.exe
fsguiexe.exe
fshdll32.exe
fshoster32.exe
fshoster64.exe
fsm32.exe
fsma32.exe
fsmb32.exe
fsorsp.exe
fspc.exe
fspex.exe
fsqh.exe
fssm32.exe
fwcfg.exe
fwinst.exe
fws.exe
gcascleaner.exe
gcasdtserv.exe
gcasinstallhelper.exe

gcasnotice.exe
gcasserv.exe
gcasservalert.exe
gcasswupdater.exe
gdfirewalltray.exe
gdfwsvc.exe
gdscan.exe
gfireporterservice.exe
ghost_2.exe
ghosttray.exe
giantantispwaremain.exe
giantantispwareupdater.exe
googlecrashhandler.exe
googlecrashhandler64.exe
googleupdate.exe
gziface.exe
gzserv.exe
hasplmv.exe
hdb.exe
healthservice.exe
hpqwmix.exe
hwapi.exe
icepack.exe
idsinst.exe
iface.exe
igateway.exe
ilicensescv.exe
inet_gethost.exe
infopath
infopath.exe
inicio.exe
inonmsrv.exe
inorpc.exe
inort.exe
inotask.exe
inoweb.exe
isafe.exe
isafinst.exe
isntsmtp.exe
isntsysmonitor
ispwdsvc.exe
isqlplussvc
isqlplussvc.exe
isscsf.exe
issdaemon.exe
issvc.exe
isuac.exe
ismmgr.exe
itmrt_supportdiagnostics.exe
itmrt_trace.exe
itmrtsvc.exe
ixaptsvc.exe
ixavsvc.exe
ixfwsvc.exe
kabackreport.exe
kaccore.exe

kanmcmmain.exe
kansgui.exe
kansvr.exe
kb891711.exe
keysvc.exe
kis.exe
kislive.exe
kissvc.exe
klnacserver.exe
klnagent.exe
klserver.exe
klswd.exe
klwtblfs.exe
kmailmon.exe
knownsvr.exe
knupdatemain.exe
kpf4gui.exe
kpf4ss.exe
kpfw32.exe
kpfwsvc.exe
krbcc32s.exe
kwebshield.exe
kvdetect.exe
kvmoxp.kxp
kvmoxp_2.kxp
kvolself.exe
kvsrvxp.exe
kvsrvxp_1.exe
kvxp.kxp
kwatch.exe
kwsprod.exe
kxeserv.exe
leventmgr.exe
livesrv.exe
lmon.exe
log_qtine.exe
loggetor.exe
loggingserver.exe
luall.exe
lucallbackproxy.exe
luoms.exe
luoms~1.exe
luomsrv.exe
lwdmsrv.exe
macmnsvc.exe
macmpatsvc.exe
managementagenthost.exe
managementagentnt.exe
mantispm.exe
masalert.exe
massrv.exe
masvc.exe
mbamservice.exe
mbamtray.exe
mcagent.exe
mcapexe.exe

mcappins.exe
mcconsol.exe
mcdash.exe
mcdetect.exe
mcepoc.exe
mcepocfg.exe
mcinfo.exe
mcmnhdlr.exe
mcmscsvc.exe
mcnasvc.exe
mcods.exe
mcpalcmfg.exe
mcpromgr.exe
mcproxy.exe
mcregwiz.exe
mcsacore.exe
mcscript_inuse.exe
mcshell.exe
mcshield.exe
mcshld9x.exe
mcsvhost.exe
mcsysmon.exe
mctray.exe
mctskshd.exe
mcui32.exe
mcuimgr.exe
mcupdate.exe
mcupdmgr.exe
mcvsftsn.exe
mcvsrte.exe
mcvsshld.exe
mcwce.exe
mcwcecfg.exe
mfeann.exe
mfecanary.exe
mfeesp.exe
mfefire.exe
mfefw.exe
mfehcs.exe
mfemactl.exe
mfemms.exe
mfetp.exe
mfevtps.exe
mfewc.exe
mfewch.exe
mgavrtcl.exe
mghtml.exe
mgntsvc.exe
monitoringhost.exe
monsvcnt.exe
monsysnt.exe
mpcmdrun.exe
mpf.exe
mpfagent.exe
mpfconsole.exe
mpfservice.exe

mpfsrv.exe
mpftray.exe
mps.exe
mpsevh.exe
mpsvc.exe
mrf.exe
msaccess
msaccess.exe
msascui.exe
mscifapp.exe
msdtssrvr.exe
msftesql.exe
mskagent.exe
mskdetct.exe
msksrver.exe
msksrvr.exe
msmdsrv.exe
msmpeng.exe
mspmpsv.exe
mspub
mspub.exe
msscli.exe
msseces.exe
msssrv.exe
musnotificationux.exe
mvdesktopservice
myagttry.exe
mydesktopqos
mydesktopqos.exe
mydesktopservice.exe
mysqld.exe
mysqld-nt.exe
mysqld-opt.exe
nailgpip.exe
naprdmgr.exe
navectl.exe
navelog.exe
navesp.exe
navshcom.exe
navw32.exe
navwnt.exe
ncdaemon.exe
nd2svc.exe
ndetect.exe
ndrvs.exe
ndrvx.exe
neotrace.exe
nerosvc.exe
netalertclient.exe
netcfg.exe
netsession_win.exe
networkagent.exe
nexe
ngctw32.exe
ngserver.exe
nimbus.exe

nimcluster.exe
nip.exe
nipsvc.exe
nisopty.exe
nisserv.exe
nissrv.exe
nisum.exe
njeeves.exe
nlclient.exe
nlsvc.exe
nmagent.exe
nmain.exe
nortonsecurity.exe
notepad
npfmontor.exe
npfmsg.exe
npfmsg2.exe
npfsvce.exe
npsdagent.exe
nprotect.exe
npscheck.exe
npssvc.exe
nrmenctb.exe
nscsrvc.exe
nsctop.exe
nscollector.service.exe
nsmdef.exe
nsmdmon.exe
nsmdreal.exe
nsmdsch.exe
nsmdtr.exe
ntcaagent.exe
ntcadaemon.exe
ntcaservice.exe
ntevl.exe
ntrtsan.exe
ntservices.exe
nvcoas.exe
nvcsched.exe
nymse.exe
oasclnt.exe
ocautoupds
ocautoupds.exe
ocomm
ocomm.exe
ocssd
ocssd.exe
oespamtest.exe
ofcdog.exe
ofcpfwsvc.exe
okclient.exe
olfsnt40.exe
omniagent.exe
omslogmanager.exe
omtsreco.exe
onenote

onenote.exe
onlinent.exe
onlnsvc.exe
op_viewer.exe
opscan.exe
oracle
oracle.exe
outlook
outlook.exe
outpost.exe
paamsrv.exe
padfsvr.exe
pagent.exe
pagentwd.exe
pasystemtray.exe
patch.exe
patrolagent.exe
patrolperf.exe
pavbckpt.exe
pavfires.exe
pavfnsvr.exe
pavjobs.exe
pavkre.exe
pavmail.exe
pavreport.exe
pavsched.exe
pavsrv50.exe
pavsrv51.exe
pavsrv52.exe
pavupg.exe
paxton.net2.clientservice.exe
paxton.net2.commserverservice.exe
pccclient.exe
pccguide.exe
pcclient.exe
pccnt.exe
pccntmon.exe
pccntupd.exe
pccpfw.exe
pcctlcom.exe
pcscan.exe
pcscm.exe
pcscnsrv.exe
pcsws.exe
pctsauxs.exe
pctsgui.exe
pctssvc.exe
pctstray.exe
pep.exe
persfw.exe
pmgreader.exe
pmon.exe
pnmsrv.exe
pntiomon.exe
pop3pack.exe
pop3trap.exe

poproxy.exe
powerpnt
powerpnt.exe
ppclean.exe
ppctlpriv.exe
ppmcatedetection.exe
ppppwallrun.exe
pqibrowser.exe
pqv2isvc.exe
pralarmmgr.exe
prcalculationmgr.exe
prconfigmgr.exe
prdatasemgr.exe
premailengine.exe
preventmgr.exe
prevsrv.exe
prfttengine.exe
prgateway.exe
printdevice.exe
privacyiconclient.exe
prlicensemgr.exe
procexp.exe
proficyadministrator.exe
proficyclient.exe4
proficypublisherservice.exe
proficyserver.exe
proficysts.exe
proutil.exe
prprintserver.exe
prproficymgr.exe
prrds.exe
prreader.exe
prrouter.exe
prschedulemgr.exe
prstubber.exe
prsummarymgr.exe
prunsrv.exe
prwriter.exe
psanhost.exe
psctris.exe
psctrls.exe
psh_svc.exe
pshost.exe
psimreal.exe
psimsvc.exe
pskmssvc.exe
psuamain.exe
psuaservice.exe
pthosttr.exe
pview.exe
pviewer.exe
pwdfilthelp.exe
pxemtftp.exe
pxeservice.exe
qclean.exe
qdcfs.exe

qoel loader.exe
qserver.exe
rapapp.exe
rapuisvc.exe
ras.exe
rasupd.exe
rav.exe
ravmon.exe
ravmond.exe
ravservice.exe
ravstub.exe
ravtask.exe
ravtray.exe
ravupdate.exe
ravxp.exe
rcsvcm on.exe
rdrcef.exe
realmon.exe
redirsvc.exe
regmech.exe
remupd.exe
repmgr64.exe
reportersvc.exe
reportingservicesservice.exe
reportsvc.exe
retinaengine.exe
rfwmain.exe
rfwproxy.exe
rfwsrv.exe
rfwstub.exe
rnav.exe
rnreport.exe
routernt.exe
rpcserv.exe
rscd.exe
rscdsvc.exe
rsnet svr.exe
rssensor.exe
rstray.exe
rtvscan.exe
ru launch.exe
safeservice.exe
sahookmain.exe
saservice.exe
sav32cli.exe
savfmsectrl.exe
savfmse log.exe
savfmsesjm.exe
savfmsesp.exe
savfmsespamstatsmanager.exe
savfmsesrv.exe
savfmsetask.exe
savfmseui.exe
savmain.exe
savroam.exe
savscan.exe

savservice.exe
savui.exe
sbamsvc.exe
sbserv.exe
scan32.exe
scanexplicit.exe
scanfrm.exe
scanmailoutlook.exe
scanmsg.exe
scanwscs.exe
scfagent_64.exe
scfmanager.exe
scfservice.exe
scftray.exe
schdsrv.exe
schupd.exe
sdrs-service.exe
sdtrayapp.exe
seanalyzertool.exe
seccenter.exe
securitycenter.exe
securitymanager.exe
seestat.exe
semsvc.exe
server_eventlog.exe
server_runtime.exe
sesclu.exe
setloadorder.exe
setupguimngr.exe
sevinst.exe
sgbhp.exe
shstat.exe
sidebar.exe
siteadv.exe
slee81.exe
smc.exe
smcgui.exe
smex_activeupda
smex_master.exe
smex_remoteconf
smex_systemwatc
smoutlookpack.exe
sms.exe
smsectrl.exe
smselog.exe
smsesjm.exe
smsesp.exe
smsesrv.exe
smsetask.exe
smseui.exe
smsx.exe
snac.exe
sndmon.exe
sndsrv.exe
snhwsrv.exe
snicheckadm.exe

snichecksrv.exe
snicon.exe
snsrv.exe
spbbcsvc.exe
spideragent.exe
spiderml.exe
spidernt.exe
spiderui.exe
spntsvc.exe
spooler.exe
spyemergency.exe
spyemergency.exe
sqbcoreservice
sqbcoreservice.exe
sql
sqlagent.exe
sqlbrowser.exe
sqlservr.exe
sqlwriter.exe
srvload.exe
srvmon.exe
sschk.exe
ssecuritymanager.exe
ssm.exe
ssp.exe
ssscheduler.exe
starta.exe
steam
steam.exe
stinger.exe
stopa.exe
stopp.exe
stwatchdog.exe
svcgenerichost
svcharge.exe
svcntaux.exe
svdealer.exe
svframe.exe
svtray.exe
swc_service.exe
swdsvc.exe
sweepsrv.sys
swi_service.exe
swnetsup.exe
swnxt.exe
swserver.exe
symlcsvc.exe
symproxysvc.exe
symSPORT.exe
symtray.exe
symWSC.exe
synctime
synctime.exe
sysdoc32.exe
sysoptenginesvc.exe
taskhostw.exe

tbirdconfig
tbirdconfig.exe
tbmon.exe
tclproc.exe
tdimon.exe
teamviewer_service.exe
tfgui.exe
tfservice.exe
tftray.exe
tfun.exe
thebat
thebat.exe
thebat64.exe
thunder_bird
thunderbird.exe
tiaspn~1.exe
tmas.exe
tmlisten.exe
tmntsrv.exe
tmpfw.exe
tmproxy.exe
tnbutil.exe
tnslsnr.exe
toolbarupdater.exe
tpsrv.exe
traflnsp.exe
traptrackermgr.exe
trjscan.exe
trupd.exe
tsansrf.exe
tsatisfy.exe
tscutynt.exe
tsmpnt.exe
ucservice.exe
udaterui.exe
uiseagnt.exe
uiwatchdog.exe
umxagent.exe
umxcfg.exe
umxfwhlp.exe
umxpol.exe
unsecapp.exe
unvet32.exe
up2date.exe
update_task.exe
updaterui.exe
updtv28.exe
upfile.exe
uplive.exe
uploadrecord.exe
upschd.exe
url_response.exe
urllstck.exe
useractivity.exe
useranalysis.exe
usergate.exe

usrprmt.exe
v2iconsole.exe
v3clnsrv.exe
v3exec.exe
v3imscn.exe
v3lite.exe
v3main.exe
v3medic.exe
v3sp.exe
v3svc.exe
vetmsg.exe
vettray.exe
vgauthservice.exe
visio.exe
vmacthlp.exe
vmtoolsd.exe
vmware-converter.exe
vmware-converter-a.exe
vmwaretray.exe
vpatch.exe
vpc32.exe
vpdn_lu.exe
vprosvc.exe
vprot.exe
vptray.exe
vrv.exe
vrvmail.exe
vrvmon.exe
vrvnet.exe
vshwin32.exe
vsmain.exe
vsmon.exe
vsserv.exe
vsstat.exe
vstskmgr.exe
webproxy.exe
webscanx.exe
websensecontrolservice.exe
webtrapnt.exe
wfxctl32.exe
wfxmod32.exe
wfxsnt40.exe
win32sysinfo.exe
winlog.exe
winroute.exe
winvnc4.exe
winword
winword.exe
wordpad
wordpad.exe
workflowresttest.exe
wrctrl.exe
wrsa.exe
wrspyssetup.exe
wscntfy.exe
wssfcmmai.exe

```
wtusystemsupt.exe  
xcommsvr.exe  
xfilter.exe  
xfssvcon  
xfssvcon.exe  
zanda.exe  
zapro.exe  
zavcore.exe  
zillya.exe  
zlclient.exe  
zlh.exe  
zonealarm.exe  
zoolz.exe
```

Source: <https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/new-golang-ransomware-agenda-customizes-attacks/IOCs-blog-New%20Golang%20Ransomware%20Agenda%20Customizes%20Attacks.txt>