CYBER ADVISORY

Technical Analysis of **MegaCortex Version 2** Ransomware

accenturesecurity

SUMMARY

MegaCortex Version 2 is a recently updated ransomware developed in the C++ programming language. Actors weaponized the first version of **MegaCortex** to be self-protecting and required a password in the command-line arguments to run correctly. This feature makes it difficult for security vendors to analyze the sample and will prevent them from being able to reverse engineer it unless those researchers have captured the password during a live infection. The disadvantage of the first version was that actors had to run the ransomware manually or risk of leaking the password. This prevented global distribution of the ransomware. The MegaCortex Version 2 author has updated the ransomware to remove these disadvantages and redesigned the ransomware to self-execute. In addition, the ransomware integrates all of the script features of the first version into the ransomware.

Audience Note

This report is intended to aid security professionals, including security operations center (SOC) staff. Security professionals can use this intelligence to better understand MegaCortex's behavior to identify indicators of compromise (IoCs). SOC analysts may use the IoCs in the Analysis section to hunt for the endpoints that MegaCortex affects. The provided information can also help inform ongoing intelligence analysis and forensic investigations, particularly for compromise discovery, damage assessment and attribution efforts. This report covers the technical details about MegaCortex and provides knowledge of MegaCortex's tactics, techniques and procedures (TTPs) to help better inform detection and response efforts to attacks using this threat.

ANALYSIS

Assessment

MegaCortex Version 2 Ransomware Overview

MegaCortex Version 2 is a recently updated ransomware developed in the C++ programming language. Actors weaponized the first version of **MegaCortex** to be self-protecting and required a password in the command-line arguments to run correctly. This feature makes it difficult for security vendors to analyze the sample and will prevent them from being able to reverse engineer it unless those researchers have captured the password during a live infection. The disadvantage of the first version was that actors had to run the ransomware manually or risk of leaking the password. This prevented global distribution of the ransomware. The MegaCortex Version 2 author has updated the ransomware to remove these disadvantages and redesigned the ransomware to self-execute. In addition, the ransomware integrates all of the script features of the first version into the ransomware. Version 2:

- decrypts the main payload and executes in memory;
- detects and terminates security tools;
- detects and stops various types of software such as backup software, database software and Web server software so there is no update to files related to that software;
- hardcodes the password into the ransomware to allow the ransomware to decrypt the main payload automatically; and

- integrates the loader, main module and worker into a single executable.

Exhibit 1 provides an overview of the ransomware.

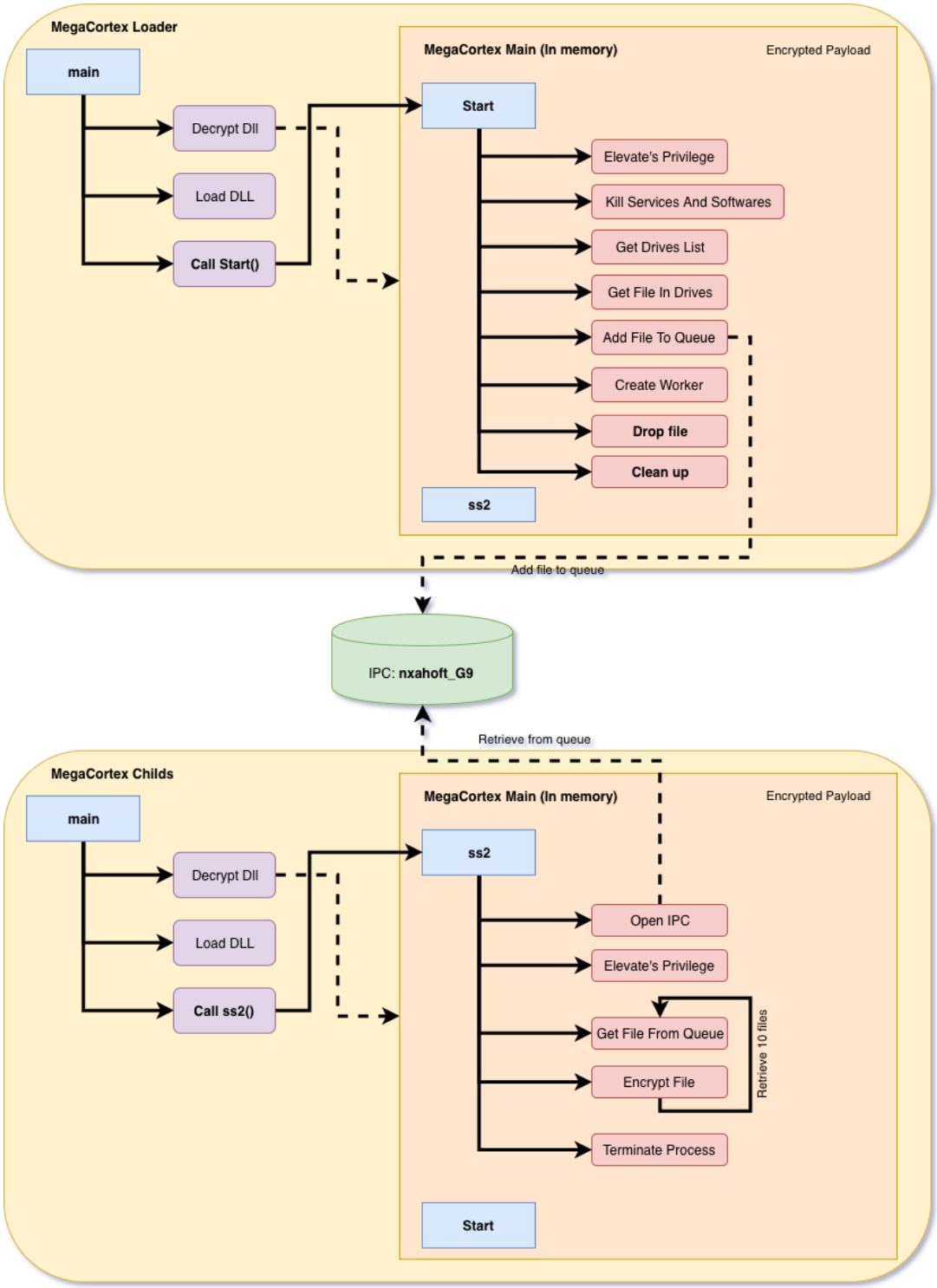

Exhibit 1: MegaCortex Version 2 Overview

MegaCortex File Overview

iDefense analyzed a sample of the MegaCortex Version 2 ransomware with the following properties:

- **MD5:** 65939a4515a59da3697e4a454d6e8378
- **SHA-1:** 470a8189915b01bc4012d7e0bdccba8e97a6a2d6
- **SHA-256:** 86aeea7b383e35d4eec0219f031935648ddcf0b257196d3b60e44091ac4e99c2
- **Size:** 956,416 bytes
- **File Type:** PE32 executable (GUI) Intel 80386, for MS Windows

The executable is digitally signed with a valid signature from ABADAN PIZZA (see Exhibit 2).

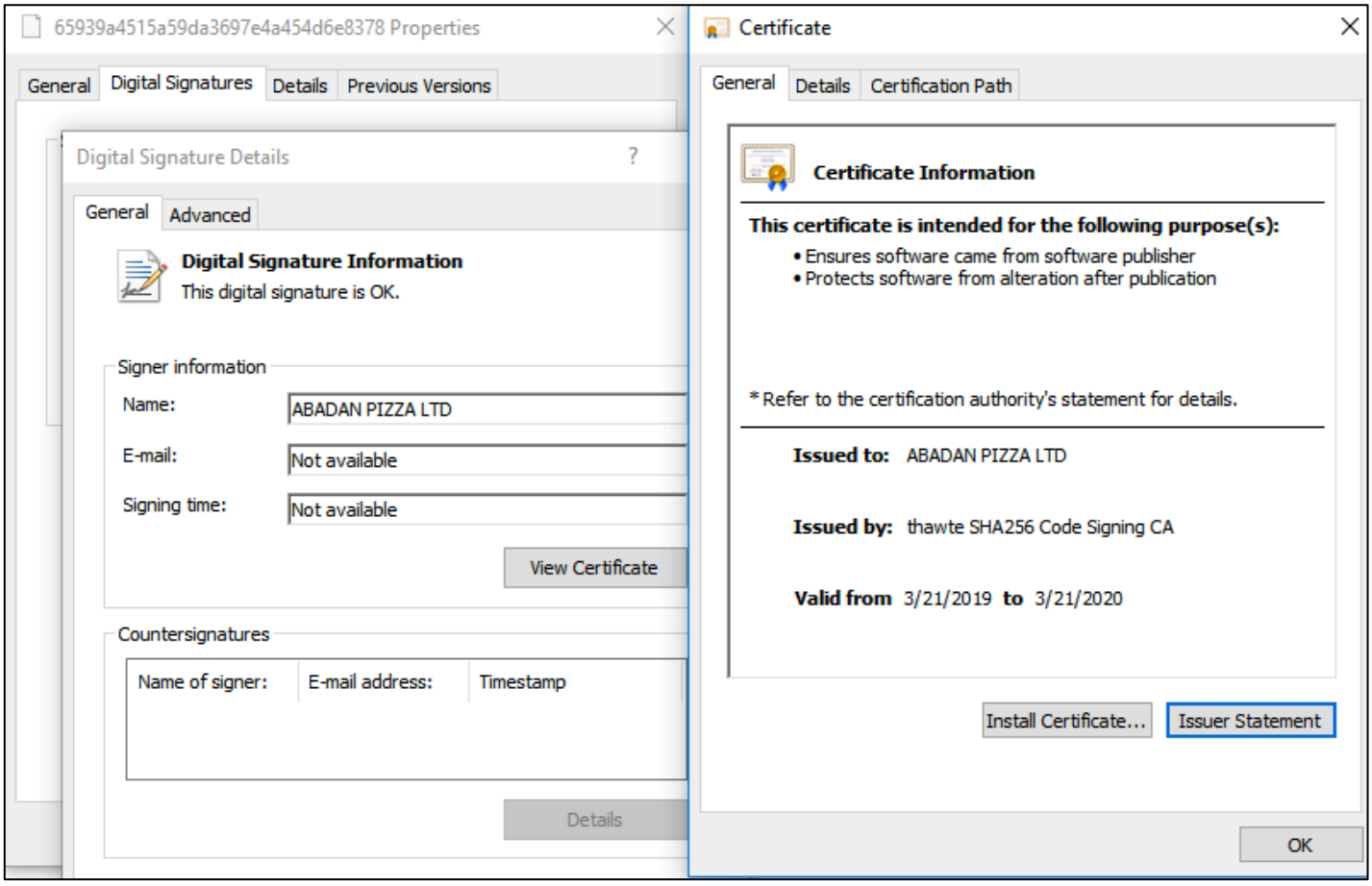

Exhibit 2: Digital Signature

Command Option

In the first version of the ransomware, the ransomware requires a password to be able to run successfully. The loader uses this password to decrypt the main module. In version 2, the ransomware can be executed with and without the password. When the ransomware executes without the password, it decrypts the payload with the hardcoded password. The password provided in the command line also specifies to the loader which module to load. Exhibit 3 shows the decompiled code of the hardcoded password and the type of module to load.

Exhibit 3: MegaCortex Version 2 Hardcoded Password

Loader

Similar to version 1, the version 2 loader is responsible for decrypting the main module and executing the ransomware. While the first version only decrypts the payload if the password is available in the command argument, the password in version 2 is hardcoded into the ransomware, as shown in Exhibit 3. In addition, the loader decides which module to execute in memory based on the command argument. If the ransomware process does not have a command argument, the ransomware decrypts and loads the controller module. When the ransomware is executed with a password, the ransomware decrypts and executes the worker's code. The controller created the following command line:

```
C:\Users\[user]\Desktop\mega.exe" E9Ql0G9gSiXqlyWa7sdT6LX2O//TIQq9msLQUuBsLcg=
```

MegaCortex Main Module File Overview

The MegaCortex decrypted module is a Microsoft Corp. Windows DLL file. The DLL file contains two exported functions, Start and ss2. The Start function is the controller; it is responsible for killing analysis software, terminating services, adding tasks to the inter-process communication (IPC) queue and starting the worker. The ss2 function is the worker; it is responsible for retrieving 10 tasks and encrypting files. The main payload has the following properties:

- **MD5**: 53dddbb304c79ae293f98e0b151c6b28
- **SHA-1**: 2632529b0fb7ed46461c406f733c047a6cd4c591
- **SHA-256**: 873aa376573288fcf56711b5689f9d2cf457b76bbc93d4e40ef9d7a27b7be466
- **Size**: 745,408 bytes
- **File** Type: PE32 executable (DLL) (console) Intel 80386, for MS Windows

Controller Module

The Controller module is responsible for searching files on the victim system and creating the worker process to start encryption. The ransomware uses an IPC queue to add tasks to the worker. The module performs the following actions:

- Detects and terminates anti-analysis software
- Detects and shuts down software
- Retrieves a list of drives
- Searches files in every directory and adds them to the queue for each drive
- Creates a worker process to encrypt files
- Drops !!!README!!!.txt and nxahoft_G9.log into the c:\ directory

- Deletes shadow files and unused data
- Drops a ransom message in the C:\ directory

Controller Module: Anti-Analysis and Services

Upon execution, the controller gathers all services and processes and compares them with a list of filenames. If the processes filename and the filename from the list match, the ransomware executes **taskkill.exe** to terminate the process. If the services match, the ransomware executes **net.exe** stop to stop the services. This feature is an integration of the scripts in version 1. Exhibit 4 shows the decompiled code of the anti-analysis software.

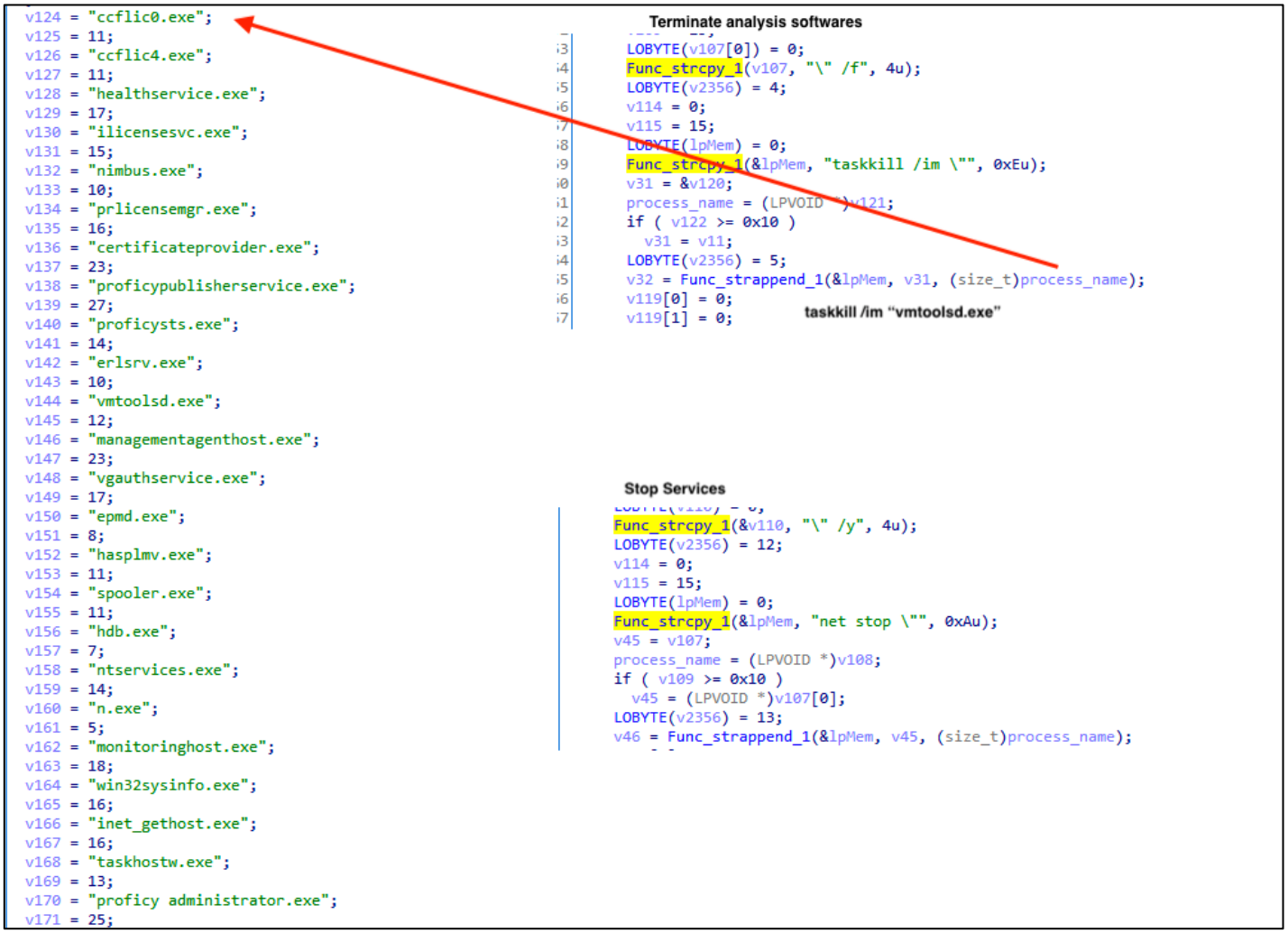

Exhibit 4: Decompiled Anti-Analysis Software and Services Code

The following is a list of process names and service names for which the ransomware scans:

ccflic0.exe	ccenter.exe
ccflic4.exe	ravxp.exe

healthservice.exe	rfwproxy.exe
ilicensesvc.exe	rfwstub.exe
nimbus.exe	knownsvr.exe
prlicensemgr.exe	ras.exe
certificateprovider.exe	rasupd.exe
proficypublisherservice.exe	upfile.exe
proficysts.exe	rstray.exe
erlsrv.exe	ravalert.exe
vmtoolsd.exe	rav.exe
managementagenthost.exe	ravmond.exe
vgauthservice.exe	ravmon.exe
epmd.exe	ravservice.exe
hasplmv.exe	ravstub.exe
spooler.exe	ravtask.exe
hdb.exe	ravtray.exe
ntservices.exe	ravupdate.exe
n.exe	rnreport.exe
monitoringhost.exe	rsnetsvr.exe
win32sysinfo.exe	scanfrm.exe
inet_gethost.exe	rfwmain.exe
taskhostw.exe	rfwsrv.exe
proficy administrator.exe	winlog.exe
ntevl.exe	omslogmanager.exe
prproficymgr.exe	snhwsrv.exe
prrds.exe	snicheckadm.exe
prrouter.exe	snichecksrv.exe
prconfigmgr.exe	snicon.exe
prgateway.exe	snsrv.exe
premailengine.exe	smsx.exe
pralarmmgr.exe	svcharge.exe
prftpengine.exe	svdealer.exe
prcalculationmgr.exe	svframe.exe

prprintserver.exe	svtray.exe
prdatabasemgr.exe	sschk.exe
preventmgr.exe	trjscan.exe
prreader.exe	trupd.exe
prwriter.exe	ssecuritymanager.exe
prsummarymgr.exe	dltray.exe
prstubber.exe	dlservice.exe
prschedulemgr.exe	almon.exe
cdm.exe	lmon.exe
musnotificationux.exe	savadminservice.exe
npmdagent.exe	savservice.exe
client64.exe	sweepsrv.sys
keysvc.exe	swnetsup.exe
server_eventlog.exe	alsvc.exe
proficyserver.exe	alupdate.exe
server_runtime.exe	savmain.exe
config_api_service.exe	sav32cli.exe
fnplicensingservice.exe	certificationmanagerservicent.exe
workflowresttest.exe	emlibupdateagentnt.exe
proficyclient.exe	managementagentnt.exe
vmacthlp.exe	mgntsvc.exe
msdtssrvr.exe	routernt.exe
sqlservr.exe	schdsrvc.exe
msmdsrv.exe	scfmanager.exe
reportingservicesservice.exe	scfservice.exe
dsmcsvc.exe	scftray.exe
winvnc4.exe	op_viewer.exe
client.exe	sgbhp.exe
collwrap.exe	pctsauxs.exe
bluestripecollector.exe	pctsgui.exe
sqlbrowser.exe	pctssvc.exe
dsmcad.exe	pctstray.exe

nimcluster.exe	regmech.exe
googleupdate.exe	sdtrayapp.exe
smc.exe	svcntaux.exe
bcrservice.exe	swdsvc.exe
dbsrv9.exe	swnxt.exe
rtvscan.exe	execstat.exe
bcreporter.exe	seestat.exe
csadmin.exe	swserver.exe
csdbsync.exe	slee81.exe
csmon.exe	kpf4gui.exe
csauth.exe	kpf4ss.exe
cslog.exe	wrspysetup.exe
csradius.exe	acctmgr.exe
cstacacs.exe	alertsvc.exe
url_response.exe	alunotify.exe
vmware-converter-a.exe	aluschedulersvc.exe
vmware-converter.exe	appsvc32.exe
avagent.exe	ccap.exe
paxton.net2.clientservice.exe	ccapp.exe
paxton.net2.commsserverservice.exe	ccevtmgr.exe
avscc.exe	ccproxy.exe
prunsrv.exe	ccpxysvc.exe
googlecrashhandler.exe	ccsetmgr.exe
googlecrashhandler64.exe	checkup.exe
vmwaretray.exe	cka.exe
nd2svc.exe	comhost.exe
tnslsnr.exe	cpdclnt.exe
omtsreco.exe	csinject.exe
oracle.exe	csinsm32.exe
patrolagent.exe	csinsmnt.exe
scfagent_64.exe	dbserv.exe
patrolperf.exe	defwatch.exe

rscdsvc.exe	defwatch
rscd.exe	diskmon.exe
pmgreader.exe	djsnetcn.exe
firefox.exe	doscan.exe
chrome.exe	dwhwizrd.exe
netsession_win.exe	fwcfg.exe
pcsws.exe	ghost_2.exe
pcscm.exe	ghosttray.exe
cwbunnav.exe	icepack.exe
rdrcef.exe	idsinst.exe
ndrvx.exe	ispwdsvc.exe
ndrvs.exe	issvc.exe
dr_serviceengine.exe	isuac.exe
teamviewer_service.exe	luall.exe
sqlagent.exe	lucallbackproxy.exe
dwrcst.exe	lucoms~1.exe
ccm messaging.exe	lucoms.exe
zoolz.exe	mcui32.exe
agntsvc.exe	navapsvc.exe
dbeng50.exe	navapw32.exe
dbsnmp.exe	navectrl.exe
encsvc.exe	navelog.exe
excel.exe	navesp.exe
firefoxconfig.exe	navshcom.exe
infopath.exe	navw32.exe
isqlplussvc.exe	navwnt.exe
msaccess.exe	ndetect.exe
msftesql.exe	ngctw32.exe
mspub.exe	ngserver.exe
mydesktopqos.exe	nisoptui.exe
mydesktopservice.exe	nisserv.exe
mysqld.exe	nisum.exe

mysqld-nt.exe	nmain.exe
mysqld-opt.exe	npfmntor.exe
ocautoupds.exe	nprotect.exe
ocomm.exe	npscheck.exe
ocssd.exe	npssvc.exe
onenote.exe	nscsrvce.exe
outlook.exe	nsctop.exe
powerpnt.exe	nsmdtr.exe
sqbcoreservice.exe	olfsnt40.exe
sqlwriter.exe	opscan.exe
steam.exe	poproxy.exe
synctime.exe	pqibrowser.exe
tbirdconfig.exe	pqv2isvc.exe
thebat.exe	pxeservice.exe
thebat64.exe	qdcsfs.exe
thunderbird.exe	qserver.exe
visio.exe	reportersvc.exe
winword.exe	rnav.exe
wordpad.exe	savfmsesp.exe
xfssvccon.exe	savroam.exe
tmlisten.exe	savscan.exe
pccntmon.exe	savui.exe
cntaosmgr.exe	sbserv.exe
ntrtscan.exe	scanexplicit.exe
mbamtray.exe	semsvc.exe
qhactivedefense.exe	sesclu.exe
qhwatchdog.exe	sevinst.exe
qhsafetray.exe	smsectrl.exe
avgsvc.exe	smselog.exe
avgui.exe	smsesjm.exe
v3lite.exe	smsesp.exe
v3main.exe	smsesrv.exe

v3sp.exe	smsetask.exe
avastui.exe	smseui.exe
avastsvc.exe	sms.exe
avguard.exe	sndmon.exe
avshadow.exe	sndsrvc.exe
avgnt.exe	spbbcsvc.exe
avira.servicehost.exe	symlcsvc.exe
avira.systray.exe	symproxysvc.exe
bdagent.exe	symsport.exe
bdredline.exe	symtray.exe
bdss.exe	symwsc.exe
bullguardbhvscanner.exe	sysdoc32.exe
bullguardscanner.exe	ucservice.exe
bullguardtray.exe	updtnv28.exe
bullguardupdate.exe	urllstck.exe
bullguard.exe	usrprmpt.exe
cmdagent.exe	v2iconsole.exe
cistray.exe	vpc32.exe
cis.exe	vpdn_lu.exe
spideragent.exe	vprosvc.exe
dwengine.exe	wfxctl32.exe
dwarkdaemon.exe	wfxmod32.exe
dwnetfilter.exe	wfxsnt40.exe
a2service.exe	lucomserver.exe
a2guard.exe.a2start.exe	savfmselog.exe
egui.exe	savfmsesjm.exe
ekrn.exe	savfmsectrl.exe
fshoster32.exe	savfmsespamstatsmanager.exe
fshoster64.exe	savfmsesrv.exe
fortisslvpndaemon.exe	savfmsetask.exe
fortiesnac.exe	savfmseui.exe
fortiwf.exe	snac.exe

fortitray.exe	ssm.exe
fchelper64.exe	reportsvc.exe
fortiproxy.exe	vptray.exe
fcappdb.exe	procexp.exe
fcdblog.exe	tdimon.exe
avp.exe	tfun.exe
avpui.exe	tfgui.exe
mbamservice.exe	tfservice.exe
mcsacore.exe	tftray.exe
mcapexe.exe	tiaspn~1.exe
mcshield.exe	traflnsp.exe
mcsvhost.exe	asupport.exe
nortonsecurity.exe	isntsmtp.exe
psuaservice.exe	nsmdemf.exe
psuamain.exe	nsmdmon.exe
psanhost.exe	nsmdreal.exe
sdrservice.exe	nsmdsch.exe
swc_service.exe	ofcdog.exe
swi_service.exe	pccnt.exe
ssp.exe	pccntupd.exe
ccsvchst.exe	pcctlcom.exe
smcgui.exe	pcscnsrv.exe
coreserviceshell.exe	schupd.exe
coreframeworkhost.exe	tmntsrv.exe
uiwatchdog.exe	tmpfw.exe
uiseagnt.exe	tmproxy.exe
paamsrv.exe	tmas.exe
psh_svc.exe	entitymain.exe
aupdrun.exe	aphost.exe
acaas.exe	lwdmserver.exe
acaegmgr.exe	mrf.exe
acaif.exe	isntsysmonitor

acais.exe	ofcpfwsvc.exe
ahnsd.exe	dwwin.exe
ahnsdsv.exe	patch.exe
autoup.exe	pccclient.exe
v3clnsrv.exe	pccguide.exe
v3medic.exe	pcclient.exe
v3svc.exe	pccpfw.exe
aflogvw.exe	pcscan.exe
ahnrpt.exe	pntiomon.exe
atwsctsk.exe	pop3pack.exe
v3exec.exe	pop3trap.exe
v3imscn.exe	scanmailoutlook.exe
monsvcnt.exe	smoutlookpack.exe
monsysnt.exe	webtrapnt.exe
aexnsrcvsvc.exe	euqmonitor.exe
aexsvc.exe	smex_activeupda
atrshost.exe	smex_master.exe
ctdataload.exe	smex_remoteconf
aexagentuihost.exe	smex_systemwatc
aexnsagent.exe	svcgenerichost
aclntusr.exe	spntsvc.exe
aexswdusr.exe	stopp.exe
pxemtftp.exe	stwatchdog.exe
aclient.exe	usbguard.exe
securitycenter.exe	uploadrecord.exe
starta.exe	sbamsvc.exe
stopa.exe	vrvmail.exe
anvir.exe	vrvmon.exe
csrss_tc.exe	vrvnet.exe
ashavast.exe	vrv.exe
ashbug.exe	wrsa.exe
ashchest.exe	networkagent.exe

ashcmd.exe	websensecontrolservice.exe
ashdisp.exe	mpcmdrun.exe
ashenhcd.exe	msascui.exe
ashlogv.exe	msmpeng.exe
ashmaisv.exe	mspmspsv.exe
ashpopwz.exe	kb891711.exe
ashquick.exe	zavaux.exe
ashserv.exe	zavcore.exe
ashsimp2.exe	zillya.exe
ashsimpl.exe	zlclient.exe
ashskpcc.exe	vsmon.exe
ashskpck.exe	forcefield.exe
ashupd.exe	iswmgr.exe
ashwebsv.exe	zapro.exe
aswdisp.exe	zonealarm.exe
aswregsvr.exe	mantispm.exe
aswserv.exe	Acronis VSS Provider
aswupdsv.exe	Enterprise Client Service
aswwebsv.exe	Sophos Agent
avengine.exe	Sophos AutoUpdate Service
afwserv.exe	Sophos Clean Service
avastemupdate.exe	Sophos Device Control Service
unsecapp.exe	Sophos File Scanner Service
avgamsvr.exe	Sophos Health Service
avgas.exe	Sophos MCS Agent
avgcc32.exe	Sophos MCS Client
avgcc.exe	Sophos Message Router
avgctrl.exe	Sophos Safestore Service
avgdiag.exe	Sophos System Protection Service
avgemc.exe	Sophos Web Control Service
avgfws8.exe	SQLsafe Backup Service
avgfwsrv.exe	SQLsafe Filter Service

avginet.exe	Symantec System Recovery
avgmsvr.exe	Veeam Backup Catalog Data Service
avgrssvc.exe	AcronisAgent
avgscanx.exe	AcrSch2Svc
avgserv9.exe	Antivirus
avgserv.exe	ARSM
avgupd.exe	BackupExecAgentAccelerator
avgupdln.exe	BackupExecAgentBrowser
avgupsvc.exe	BackupExecDeviceMediaService
avgvv.exe	BackupExecJobEngine
avgwb.dat	BackupExecManagementService
avgw.exe	BackupExecRPCService
avgwizfw.exe	BackupExecVSSProvider
guard.exe	bedbg
avgcsrvx.exe	DCAgent
avgidsagent.exe	EPSecurityService
avgidsmonitor.exe	EPUpdateService
avgidsui.exe	EraserSvc11710
avgidswatcher.exe	EsgShKernel
avgam.exe	FA_Scheduler
avgnsx.exe	IISAdmin
avgfws9.exe	IMAP4Svc
avgrsx.exe	macmnsvc
avgtray.exe	masvc
avgwdsvc.exe	MBAMService
sidebar.exe	MBEndpointAgent
avgchsvx.exe	McAfeeEngineService
avgcmgr.exe	McAfeeFramework
avgemcx.exe	McAfeeFrameworkMcAfeeFramework
avgfws.exe	McShield
avgmfapx.exe	McTaskManager
avgcefrend.exe	mfemms

avgcsrva.exe	mfevtp
avgemca.exe	MMS
avgnsa.exe	mozyprobackup
avgrsa.exe	MsDtsServer
loggingserver.exe	MsDtsServer100
toolbarupdater.exe	MsDtsServer110
wtusystemsuport.exe	MSExchangeES
avgregcl.exe	MSExchangeIS
avgsystx.exe	MSExchangeMGMT
vprot.exe	MSExchangeMTA
avcenter.exe	MSExchangeSA
avconfig.exe	MSExchangeSRS
avesvc.exe	MSOLAP$SQL_2008
avmailc.exe	MSOLAP$SYSTEM_BGC
avmcdlg.exe	MSOLAP$TPS
avnotify.exe	MSOLAP$TPSAMA
avscan.exe	MSSQL$BKUPEXEC
guardgui.exe	MSSQL$ECWDB2
avadmin.exe	MSSQL$PRACTICEMGT
avfwsvc.exe	MSSQL$PRACTTICEBGC
avwebgrd.exe	MSSQL$PROFXENGAGEMENT
fwinst.exe	MSSQL$SBSMONITORING
sysoptenginesvc.exe	MSSQL$SHAREPOINT
bavtray.exe	MSSQL$SQL_2008
bhipssvc.exe	MSSQL$SYSTEM_BGC
bmrt.exe	MSSQL$TPS
seccenter.exe	MSSQL$TPSAMA
gziface.exe	MSSQL$VEEAMSQL2008R2
gzserv.exe	MSSQL$VEEAMSQL2012
bdc.exe	MSSQLFDLauncher
bdlite.exe	MSSQLFDLauncher$PROFXENGAGEMENT
bdmcon.exe	MSSQLFDLauncher$SBSMONITORING

bdsubmit.exe	MSSQLFDLauncher$SHAREPOINT
deloeminfs.exe	MSSQLFDLauncher$SQL_2008
livesrv.exe	MSSQLFDLauncher$SYSTEM_BGC
setloadorder.exe	MSSQLFDLauncher$TPS
vsserv.exe	MSSQLFDLauncher$TPSAMA
xcommsvr.exe	MSSQLSERVER
bka.exe	MSSQLServerADHelper100
bkavsystemserver.exe	MSSQLServerOLAPService
blupro.exe	MySQL57
blackd.exe	ntrtscan
blackice.exe	OracleClientCache80
proutil.exe	PDVFSService
rapapp.exe	POP3Svc
basfipm.exe	ReportServer
isafe.exe	ReportServer$SQL_2008
cavrid.exe	ReportServer$SYSTEM_BGC
vetmsg.exe	ReportServer$TPS
amswmagt	ReportServer$TPSAMA
caf.exe	RESvc
capmuamagt.exe	sacsvr
ccnfagent.exe	SamSs
ccsmagtd.exe	SAVAdminService
cfftplugin.exe	SAVService
cfnotsrvd.exe	SDRSVC
cfsmsmd.exe	SepMasterService
alert.exe	ShMonitor
igateway.exe	Smcinst
inotask.exe	SmcService
caantispyware.exe	SMTPSvc
caavcmdscan.exe	SNAC
caav.exe	SntpService
caavguiscan.exe	sophossps

cafw.exe	SQLAgent$BKUPEXEC
calogdump.exe	SQLAgent$ECWDB2
capfaem.exe	SQLAgent$PRACTTICEBGC
capfsem.exe	SQLAgent$PRACTTICEMGT
cappactiveprotection.exe	SQLAgent$PROFXENGAGEMENT
casecuritycenter.exe	SQLAgent$SBSMONITORING
caunst.exe	SQLAgent$SHAREPOINT
cavrep.exe	SQLAgent$SQL_2008
cctray.exe	SQLAgent$SYSTEM_BGC
ccupdate.exe	SQLAgent$TPS
isafinst.exe	SQLAgent$TPSAMA
itmrt_supportdiagnostics.exe	SQLAgent$VEEAMSQL2008R2
itmrtsvc.exe	SQLAgent$VEEAMSQL2012
itmrt_trace.exe	SQLBrowser
ppclean.exe	SQLSafeOLRService
umxagent.exe	SQLSERVERAGENT
umxcfg.exe	SQLTELEMETRY
umxfwhlp.exe	SQLTELEMETRY$ECWDB2
umxpol.exe	SQLWriter
unvet32.exe	SstpSvc
capfasem.exe	svcGenericHost
ccprovsp.exe	swi_filter
ppctlpriv.exe	swi_service
casc.exe	swi_update_64
ccschedulersvc.exe	TmCCSF
ccsystemreport.exe	tmlisten
inonmsrv.exe	TrueKey
inoweb.exe	TrueKeyScheduler
auth8021x.exe	TrueKeyServiceHelper
krbcc32s.exe	UI0Detect
pep.exe	VeeamBackupSvc
realmon.exe	VeeamBrokerSvc

repmgr64.exe	VeeamCatalogSvc
csacontrol.exe	VeeamCloudSvc
leventmgr.exe	VeeamDeploymentService
okclient.exe	VeeamDeploySvc
clamscan.exe	VeeamEnterpriseManagerSvc
clamtray.exe	VeeamMountSvc
clamwin.exe	VeeamNFSSvc
ccemflsv.exe	VeeamRESTSvc
cssauth.exe	VeeamTransportSvc
cavscan.exe	W3Svc
clps.exe	wbengine
clpsla.exe	WRSVC
clpsls.exe	VeeamHvIntegrationSvc
cmdinstall.exe	swi_update
cfpconfig.exe	SQLAgent$CXDB
cfp.exe	SQLAgent$CITRIX_METAFRAME
cfplogvw.exe	SQL Backups
cfpsbmit.exe	MSSQL$PROD
cfpupdat.exe	Zoolz 2 Service
crashrep.exe	MSSQLServerADHelper
cpf.exe	SQLAgent$PROD
cfpconfg.exe	msftesql$PROD
csfalconservice.exe	NetMsmqActivator
cylanceui.exe	EhttpSrv
cylancesvc.exe	ekrn
cramtray.exe	ESHASRV
crssvc.exe	MSSQL$SOPHOS
amsvc.exe	SQLAgent$SOPHOS
frzstate2k.exe	AVP
drwagnui.exe	klnagent
drweb32.exe	MSSQL$SQLEXPRESS
drweb32w.exe	SQLAgent$SQLEXPRESS

drweb386.exe	kavfsslp
drwebcgp.exe	KAVFSGT
drwebdc.exe	KAVFS
drweb.exe	mfefire
drwebmng.exe	avast! Antivirus
drwebscd.exe	aswBcc
drwebupw.exe	Avast Business Console Client Antivirus Service
drwebwcl.exe	mfewc
drwebwin.exe	Telemetryserver
drwinst.exe	WdNisSvc
spiderml.exe	WinDefend
spidernt.exe	MCAFEETOMCATSRV530
spiderui.exe	MCAFEEEVENTPARSERSRV
drwagntd.exe	MSSQLFDLauncher$ITRIS
drwupgrade.exe	MSSQL$EPOSERVER
drwebcom.exe	MSSQL$ITRIS
eeyeevnt.exe	SQLAgent$EPOSERVER
retinaengine.exe	SQLAgent$ITRIS
a2guard.exe	SQLTELEMETRY$ITRIS
a2start.exe	MsDtsServer130
administrator.exe	SSISTELEMETRY130
control_panel.exe	MSSQLLaunchpad$ITRIS
usergate.exe	BITS
esmagent.exe	BrokerInfrastructure
era.exe	epag
ppmcativedetection.exe	EPIntegrationService
vettray.exe	EPProtectedService
cavtray.exe	epredline
inorpc.exe	TmPfw
inort.exe	SentinelAgent
ca.exe	SentinelHelperService
caissdt.exe	LogProcessorService

etagent.exe	SentinelStaticEngine
etloganalyzer.exe	DB2
etrssfeeds.exe	DB2GOVERNOR_DB2COPY1
evtarmgr.exe	DB2LICD_DB2COPY1
evtmgr.exe	DB2MGMTSVC_DB2COPY1
etreporter.exe	DB2REMOTECMD_DB2COPY1
etconsole3.exe	DB2DAS00
etwcontrolpanel.exe	DB2-0
useranalysis.exe	DB2INST2
etcorrel.exe	IBMDataServerMgr
evtprocessecfile.exe	IBMDSServer41
etscheduler.exe	MSSQL$CITRIX_METAFRAME
useractivity.exe	RumorServer
traptrackermgr.exe	myAgtSvc
ewidoctrl.exe	SentinelAgent
ewidoguard.exe	SentinelHelperService
nslocollectorservice.exe	LogProcessorService
fmon.exe	SentinelStaticEngine
fortifw.exe	TmPfw
update_task.exe	EPSecurityService
fpavserver.exe	EPUpdateService
fprottray.exe	epredline
fameh32.exe	EPProtectedService
fspex.exe	EPIntegrationService
fsaa.exe	epag
bwgo0000	BITS
fch32.exe	BrokerInfrastructure
fih32.exe	EPSecurityService
fsaua.exe	EPUpdateService
fsav32.exe	MSSQLLaunchpad$ITRIS
fscuif.exe	SSISTELEMETRY130
fsdfwd.exe	MsDtsServer130

fsgk32.exe	SQLTELEMETRY$ITRIS
fsgk32st.exe	SQLAgent$ITRIS
fsguidll.exe	SQLAgent$EPOSERVER
fsguiexe.exe	MSSQL$ITRIS
fshdll32.exe	MSSQL$EPOSERVER
fsm32.exe	MSSQLFDLauncher$ITRIS
fsma32.exe	MCAFEEEVENTPARSERSRV
fsmb32.exe	MCAFEETOMCATSRV530
fsorsp.exe	WdNisSvc
fspc.exe	WinDefend
fsqh.exe	Telemetryserver
fssm32.exe	mfewc
setupguimngr.exe	Avast Business Console Client Antivirus Service
tnbutil.exe	aswBcc
fsavgui.exe	avast! Antivirus
gdscan.exe	mfefire
avkproxy.exe	KAVFS
avkservice.exe	KAVFSGT
avktray.exe	kavfsslp
avkwctl.exe	wbengine
gdfirewalltray.exe	SQLAgent$SQLEXPRESS
gdfwsvc.exe	MSSQL$SQLEXPRESS
endpointsecurity.exe	klnagent
esecservice.exe	AVP
gfireporterservice.exe	SQLAgent$SOPHOS
esecagntservice.exe	MSSQL$SOPHOS
rcsvcmon.exe	EhttpSrv
dolphincharge.e	ekrn
dolphincharge.exe	ESHASRV
loggetor.exe	NetMsmqActivator
netalertclient.exe	msftesql$PROD
printdevice.exe	SQLAgent$PROD

pwdfilthelp.exe	MSSQLServerADHelper
pthosttr.exe	Zoolz 2 Service
hpqwmiex.exe	MSSQL$PROD
ntcaagent.exe	SQL Backups
ntcadaemon.exe	SQLAgent$CITRIX_METAFRAME
ntcaservice.exe	Acronis VSS Provider
privacyiconclient.exe	Enterprise Client Service
rapuisvc.exe	Sophos Agent
vpatch.exe	Sophos AutoUpdate Service
tclproc.exe	Sophos Clean Service
isscsf.exe	Sophos Device Control Service
issdaemon.exe	Sophos File Scanner Service
kvdetech.exe	Sophos Health Service
kvmonxp_2.kxp	Sophos MCS Agent
kvmonxp.kxp	Sophos MCS Client
kvolself.exe	Sophos Message Router
kvsrvxp_1.exe	Sophos Safestore Service
kvsrvxp.exe	Sophos System Protection Service
kvxp.kxp	Sophos Web Control Service
ppppwallrun.exe	SQLsafe Backup Service
avpcc.exe	SQLsafe Filter Service
avpexec.exe	Symantec System Recovery
avpm.exe	Veeam Backup Catalog Data Service
avpncc.exe	AcronisAgent
avps.exe	AcrSch2Svc
avpupd.exe	Antivirus
kav.exe	ARSM
kavisarv.exe	BackupExecAgentAccelerator
kavmm.exe	BackupExecAgentBrowser
kavss.exe	BackupExecDeviceMediaService
kavsvc.exe	BackupExecJobEngine
kis.exe	BackupExecManagementService

klnagent.exe	BackupExecRPCService
klswd.exe	BackupExecVSSProvider
klwtblfs.exe	bedbg
kwsprod.exe	DCAgent
up2date.exe	EPSecurityService
klserver.exe	EPUpdateService
oespamtest.exe	EraserSvc11710
kavadapterexe.exe	EsgShKernel
kavlotsingleton.exe	FA_Scheduler
kavfsgt.exe	IISAdmin
kavfsrcn.exe	IMAP4Svc
kavfs.exe	macmnsvc
kavfswp.exe	masvc
kavshell.exe	MBAMService
klnacserver.exe	MBEndpointAgent
avpdtagt.exe	McAfeeEngineService
netcfg.exe	McAfeeFramework
kavfsscs.exe	McAfeeFrameworkMcAfeeFramework
kavtray.exe	McShield
persfw.exe	McTaskManager
avserver.exe	mfemms
winroute.exe	mfevtp
wrctrl.exe	MMS
kabackreport.exe	mozyprobackup
kaccore.exe	MsDtsServer
kanmcmain.exe	MsDtsServer100
kastray.exe	MsDtsServer110
kislive.exe	MSExchangeES
kmailmon.exe	MSExchangeIS
knupdatemain.exe	MSExchangeMGMT
kswebshield.exe	MSExchangeMTA
kxeserv.exe	MSExchangeSA

uplive.exe	MSExchangeSRS
kansgui.exe	MSOLAP$SQL_2008
kansvr.exe	MSOLAP$SYSTEM_BGC
kavstart.exe	MSOLAP$TPS
kpfwsvc.exe	MSOLAP$TPSAMA
kwatch.exe	MSSQL$BKUPEXEC
kav32.exe	MSSQL$ECWDB2
kissvc.exe	MSSQL$PRACTICEMGT
kpfw32.exe	MSSQL$PRACTTICEBGC
system.exe	MSSQL$PROFXENGAGEMENT
wssfcmai.exe	MSSQL$SBSMONITORING
aawservice.exe	MSSQL$SHAREPOINT
ad-aware2007.exe	MSSQL$SQL_2008
nlsvc.exe	MSSQL$SYSTEM_BGC
engineserver.exe	MSSQL$TPS
eventparser.exe	MSSQL$TPSAMA
log_qtine.exe	MSSQL$VEEAMSQL2008R2
mfeann.exe	MSSQL$VEEAMSQL2012
nailgpip.exe	MSSQLFDLauncher
rpcserv.exe	MSSQLFDLauncher$PROFXENGAGEMENT
srvmon.exe	MSSQLFDLauncher$SBSMONITORING
mcagent.exe	MSSQLFDLauncher$SHAREPOINT
mfemactl.exe	MSSQLFDLauncher$SQL_2008
macmnsvc.exe	MSSQLFDLauncher$SYSTEM_BGC
masvc.exe	MSSQLFDLauncher$TPS
masalert.exe	MSSQLFDLauncher$TPSAMA
msssrv.exe	MSSQLSERVER
massrv.exe	MSSQLServerADHelper100
msscli.exe	MSSQLServerOLAPService
mcshld9x.exe	MySQL57
mgavrtcl.exe	ntrtscan
mcappins.exe	OracleClientCache80

mfecanary.exe	PDVFSService
macompatsvc.exe	POP3Svc
mcvsrte.exe	ReportServer
mfefire.exe	ReportServer$SQL_2008
dao_log.exe	ReportServer$SYSTEM_BGC
firesvc.exe	ReportServer$TPS
firetray.exe	ReportServer$TPSAMA
mfeesp.exe	RESvc
naprdmgr.exe	sacsvr
cpd.exe	SamSs
mfefw.exe	SAVAdminService
frameworkservic	SAVService
cmgrdian.exe	SDRSVC
mcshell.exe	SepMasterService
mfehcs.exe	ShMonitor
mcinfo.exe	Smcinst
hwapi.exe	SmcService
mcafeedatabackup.exe	SMTPSvc
mcmscsvc.exe	SNAC
mcnasvc.exe	SntpService
mcods.exe	sophossps
mcpromgr.exe	SQLAgent$BKUPEXEC
mcproxy.exe	SQLAgent$ECWDB2
mcuimgr.exe	SQLAgent$PRACTTICEBGC
mpfsrv.exe	SQLAgent$PRACTTICEMGT
mpsevh.exe	SQLAgent$PROFXENGAGEMENT
mps.exe	SQLAgent$SBSMONITORING
msksrver.exe	SQLAgent$SHAREPOINT
redirsvc.exe	SQLAgent$SQL_2008
saservice.exe	SQLAgent$SYSTEM_BGC
siteadv.exe	SQLAgent$TPS
mfemms.exe	SQLAgent$TPSAMA

neotrace.exe	SQLAgent$VEEAMSQL2008R2
vshwin32.exe	SQLAgent$VEEAMSQL2012
mpfagent.exe	SQLBrowser
mpfconsole.exe	SQLSafeOLRService
mpf.exe	SQLSERVERAGENT
mpfservice.exe	SQLTELEMETRY
mpftray.exe	SQLTELEMETRY$ECWDB2
mscifapp.exe	SQLWriter
mfevtps.exe	SstpSvc
qclean.exe	svcGenericHost
mcregwiz.exe	swi_filter
rssensor.exe	swi_service
safeservice.exe	swi_update_64
ncdaemon.exe	TmCCSF
mcdash.exe	tmlisten
mcdetect.exe	TrueKey
ssscheduler.exe	TrueKeyScheduler
sahookmain.exe	TrueKeyServiceHelper
mskdetct.exe	UIODetect
msksrvr.exe	VeeamBackupSvc
mskagent.exe	VeeamBrokerSvc
stinger.exe	VeeamCatalogSvc
mcsysmon.exe	VeeamCloudSvc
mctskshd.exe	VeeamDeploymentService
mfetp.exe	VeeamDeploySvc
myagttry.exe	VeeamEnterpriseManagerSvc
mcupdmgr.exe	VeeamMountSvc
rulaunch.exe	VeeamNFSSvc
mcvsshld.exe	VeeamRESTSvc
tbmon.exe	VeeamTransportSvc
alogserv.exe	W3Svc
mcmnhdlr.exe	WRSVC

mghtml.exe	VeeamHvIntegrationSvc
edisk.exe	swi_update
scan32.exe	SQLAgent$CXDB
frameworkservice.exe	McAfee SiteAdvisor Enterprise Service
mcconsol.exe	MSSQL$CITRIX_METAFRAME
mcscript_inuse.exe	IBMDSServer41
mctray.exe	IBMDataServerMgr
mcupdate.exe	DB2INST2
shstat.exe	DB2-0
udaterui.exe	DB2DAS00
updaterui.exe	DB2REMOTECMD_DB2COPY1
mcepoc.exe	DB2MGMTSVC_DB2COPY1
mcepocfg.exe	DB2LICD_DB2COPY1
mcpalmcfg.exe	DB2GOVERNOR_DB2COPY1
mcwcecfg.exe	DB2
mcwce.exe	Alerter
frameworkservic.exe	ERSvc
vsmain.exe	Eventlog
oasclnt.exe	ImapiService
vsstat.exe	NetDDE
mcvsftsn.exe	NtLmSsp
avconsol.exe	NtmsSvc
avsynmgr.exe	odserv
vstskmgr.exe	ose
webscanx.exe	SnowInventoryClient
mfewc.exe	TlntSvr
mfewch.exe	TSM
giantantispywaremain.exe	VMTools
giantantispywareupdater.exe	VMware
gcasservalert.exe	WebClient
gcascleaner.exe	WinVNC4
gcasinstallhelper.exe	BlueStripeCollector

gcasnotice.exe	Cissesrv
gcasdtserv.exe	CpqRcmc3
gcasserv.exe	gupdate
gcasswupdater.exe	gupdatem
fcsms.exe	HealthService
fcssas.exe	NimbusWatcherService
nissrv.exe	ProLiantMonitor
dpmra.exe	SDD_Service
msseces.exe	sysdown
wscntfy.exe	System
securitymanager.exe	GoogleChromeElevationService
aesecurityservice.exe	bcrservice
deteqt.agent.exe	ccEvtMgr
omniagent.exe	ccSetMgr
nerosvc.exe	CSAdmin
seanalyzertool.exe	CSAuth
spyemergency.exe	CSDbSync
spyemergencysrv.exe	CSLog
nlclient.exe	CSMon
crdm.exe	CSRadius
nmagent.exe	CSTacacs
ehttpsrv.exe	Symantec
nod32.exe	VGAuthService
nod32krn.exe	SepMasterServiceMig
nod32kui.exe	vmware-converter-agent
nod32view.exe	vmware-converter-server
cclaw.exe	vmware-converter-worker
elogsvc.exe	avbackup
nip.exe	MSSQL$NET2
nipsvc.exe	Net2ClientSvc
njeeves.exe	NetSvc
npfmsg2.exe	SQLAgent$NET2

npfmsg.exe	tpautoconnsvc
npfsvice.exe	TPVCGateway
nrmenctb.exe	VMwareCAFCommAmqpListener
nvcoas.exe	VMwareCAFManagementAgentHost
nvcsched.exe	TPAutoConnSvc
nymse.exe	AdobeARMservice
zanda.exe	RSCDsvc
zlh.exe	LRSDRVX
ixaptsvc.exe	msvsmon90
ixavsvc.exe	IDriverT
ixfwsvc.exe	MSMQ
emlproui.exe	Alerter
emlproxy.exe	ERSvc
mpsvc.exe	Eventlog
onlinent.exe	ImapiService
onlnsvc.exe	NetDDE
scanmsg.exe	NtLmSsp
scanwscs.exe	NtmsSvc
tsansrf.exe	odserv
tsatisy.exe	ose
tscutynt.exe	SnowInventoryClient
tsmpnt.exe	TlntSvr
upschd.exe	TSM
xfilter.exe	VMTools
aps.exe	VMware
aus.exe	WebClient
outpost.exe	WinVNC4
adminserver.exe	BlueStripeCollector
avtask.exe	Cissesrv
clshield.exe	CpqRcmc3
console.exe	gupdate
cpntsrv.exe	gupdatem

padfsvr.exe	HealthService
pasystemtray.exe	NimbusWatcherService
pavfnsvr.exe	ProLiantMonitor
pavkre.exe	SDD_Service
pavprot.exe	sysdown
pavreport.exe	System
pnmsrv.exe	GoogleChromeElevationService
psimsvc.exe	bcrservice
pavupg.exe	ccEvtMgr
remupd.exe	ccSetMgr
iface.exe	CSAdmin
pavfires.exe	CSAuth
pavmail.exe	CSDbSync
pavprsrv.exe	CSLog
pavsched.exe	CSMon
pavsrv50.exe	CSRadius
pavsrv51.exe	CSTacacs
pavsrv52.exe	Symantec
prevsrv.exe	VGAuthService
tpsrv.exe	SepMasterServiceMig
pagent.exe	vmware-converter-agent
pagentwd.exe	vmware-converter-server
psctris.exe	vmware-converter-worker
apvxdwin.exe	avbackup
inicio.exe	MSSQL$NET2
pavbckpt.exe	Net2ClientSvc
pavjobs.exe	NetSvc
psctrls.exe	SQLAgent$NET2
pshost.exe	tpautoconnsvc
psimreal.exe	TPVCGateway
pskmssvc.exe	VMwareCAFCommAmqpListener
srvload.exe	VMwareCAFManagementAgentHost

webproxy.exe	TPAutoConnSvc
avltmain.exe	AdobeARMservice
firewallgui.exe	RSCDsvc
pviewer.exe	LRSDRVX
pview.exe	msvsmon90
pmon.exe	IDriverT
qoeloader.exe	MSMQ
fws.exe	

Worker Module

The worker is responsible for retrieving files from the IPC queue and encrypting them. The ransomware uses an RSA public key, which is hardcoded into the malware, to encrypt files.

Ransom Notes

The ransomware drops the following ransom note onto the C drive.

If you are reading this text, it means, we've hacked your corporate network.

Now all your data is encrypted with very serious and powerful algorithms (AES256 and RSA-4,096).

These algorithms now in use in military intelligence, NSA and CIA .

No one can help you to restore your data without our special decipherer.

Don't even waste your time.

But there are good news for you.

We don't want to do any damage to your business.

We are working for profit.

The core of this criminal business is to give back your valuable data in the original form (for ransom of course).

In order to prove that we can restore all your data, we'll decrypt 3 of your files for free.

Please, attach 2-3 encrypted files to your first letter.

Each file must be less than 5 Mb, non-archived and your files should not contain valuable information

(databases, backups, large word files or excel sheets, etc.).

You will receive decrypted samples and our conditions how to get the decipherer.

For the fastest solution of the problem, please, write immediately in your first letter:

the name of your company,

the domain name of your corporate network and

the URL of your corporate website

It is important !

And please do not start your first letter to us with the words:

"It's a mistake !! Our company is just trimming and grooming little dogs. We don't have money at all."

"There is a big mistake on our site !

We are not leaders in our industry and all our competitors don't suck our huge dick.

We're just a small company, and we are dying because of hard competition."

"We are not the Super Mega International Corporation ltd., we are just a nursery etc."

We see it 5 times a day. This shit doesn't work at all !!!

Don't waste our and your time.

Remember ! We don't work for food.

You have to pay for decryption in Bitcoins (BTC).

If you think you pay $500 and you'll get the decryptor, you are 50 million light years away from reality :)

The ransom begins from 2-3 BTC up to 600 BTC.

If you don't have money don't even write to us.

We don't do charity !

One more time :

1.(In first letter) write the name of your company, the domain name of your corporate network and the URL of your corporate website

2. Attach 2-3 encrypted files (we'll show you some magic)

3. Use Google in order to find out how to buy bitcoins fast

As soon as we get bitcoins you'll get all your decrypted data back.

Contact emails:

ShianeUrabe1991@mail.com

or

MelodeySprague89@mail.com

Man is the master of everything and decides everything.

Conclusion

MegaCortex is a recently deployed ransomware that is making a few headlines due to its ability to infect various organizations. The developer of this ransomware designed to be self-protective and anti-forensic, therefore making capturing the main component difficult. However, these features are also the major disadvantage of the ransomware due to a lack ability to deploy globally and quickly. Version 2 is the latest version of MegaCortex in which the author traded security for ease of use. With a hardcoded password and anti-analysis software, parties can deliver the ransomware without an actor-supplied the password for that ransomware. Therefore, there could potentially be an increase in the number of MegaCortex files delivered through e-mail campaigns or dropped by a malware downloader.

MITIGATION

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
	Command-Line Interface		Access Token Manipulation	Access Token Manipulation						
				Disabling Security Tools						

For threat hunting, iDefense recommends leveraging the YARA rule below:

```
rule MegaCortex_v2_DLL
{
   meta:
      description = “Detects MegaCortex DLL samples from version 2”
```

```
        hash = “53dddbb304c79ae293f98e0b151c6b28”
        author = “iDefense”
        date = "2019-07-29"
    strings:
        $ = "If you are reading this text, it means, we've hacked your corporate network" nocase wide ascii
        $ = "No one can help you to restore your data without our special decipherer" nocase wide ascii
        $ = "You will receive decrypted samples and our conditions how to get the decipherer" nocase wide ascii
        $ = "Man is the master of everything and decides everything" nocase wide asci
        $ = "@mail.com" nocase wide ascii
            $ = ".log" nocase wide ascii
           $ = "MEGA-" nocase wide ascii
          $ = "elevate" nocase wide ascii
        $ = "fail:" nocase wide ascii
          $ = "scaning" nocase wide ascii
          $ = "taskkill" nocase wide ascii
          $ = "payload.dll" nocase wide ascii
      condition:
          all of them
}
```

iDefense also recommends searching for the following:

- **System**: Presence of the following artifacts:
    - **On-disk Artifacts**:*
        - c:\nxahoft_G9.log
        - c:\!!!_READ-ME_!!!.txt
        - C:\x5gj5_gmG8.log
    - **Any of the Following File Hashes**:
        - c965e59627b1fed12e8bb049480f55d9
        - e69f84e15dec9e49eb56031962d26854
        - 582a604682e44330a9ab549a94226545

LEGAL NOTICE AND DISCLAIMER: *This document is produced by consultants at Accenture as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact your Accenture representative.*

Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. You should independently assess your specific needs in deciding to use any of the tools mentioned.

As such, all information and content set out is provided on an "as-is" basis without representation or warranty and the reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion. Accenture accepts no liability for any action or failure to act in response to the information contained or referenced in this alert.