

BlackCatは、以下のディレクトリを回避します。

system volume information	default
intel	all users
\$windows.~ws	tor browser
application data	programdata
\$recycle.bin	boot
mozilla	config.msi
\$windows.~bt	google
public	perflogs
msocache	appdata
windows	windows.old

ファイル名に文字列を含む以下のファイルの暗号化を回避します。

desktop.ini	boot.ini
autorun.inf	ntuser.dat
ntldr	iconcache.db
bootsect.bak	bootfont.bin
thumbs.db	ntuser.ini
	ntuser.dat.log

以下の拡張子を持つファイルの暗号化を防止します。

themepack	ocx	386
nls	diagcab	lock
diagpkg	diagcfg	cur
msi	pdb	idx
lnk	wpx	sys
exe	hlp	com
cab	icns	deskthemepack
scr	rom	shs
bat	dll	ldf
drv	msstyles	theme
rtp	mod	mpa
msp	ps1	nomedia
prf	ics	spl
msc	hta	cpl
ico	bin	adv
key	cmd	icl
	ani	msu

BlackCatは以下のプロセスやサービスを終了させます。

プロセス:

agntsvc	sql	QBDBMgrN
dbeng50	steam	QBFCFMonitorSe
dbsnmp	synctime	SAP
encsvc	tbirdconfig	TeamViewer_Service
excel	thebat	TeamViewer
firefox	thunderbird	tv_w32
infopath	visio	tv_x64
isqlplussvc	winword	CVMountd
msaccess	wordpad	cvd
msspub	xfssvcon	cvfwd

mydesktopq	*sql*	CVODS
mydesktopservic	bedbh	saphostexe
notepad	vxmon	saposcol
ocautoupds	benetns	sapstartsrv
ocomm	bengien	avagent
ocssd	pvlsvr	avsc
onenote	beserver	DellSystem
oracle	raw_agent_svc	EnterpriseClient
outlook	vsnapvss	VeeamNFSSvc
powerpnt	CagService	VeeamTransportSvc
sqbcoreservic	QBIDPService	VeeamDeploymentSvc

サービス:

mepocs	BackupExecVSSProvider	SAP
memtas	BackupExecAgentAccelerator	SAP\$
veeam	BackupExecAgentBrowser	SAPD\$
svc\$	BackupExecDiveciMediaService	SAPHostControl
backup	BackupExecJobEngine	SAPHostExec
sql	BackupExecManagementService	QBCFMonitorService
vss	BackupExecRPCService	QBDBMgrN
msexchange	GxBlr	QBIDPService
sql\$	GxVss	AcronisAgent
mysql	GxCIMgrS	VeeamNFSSvc
mysql\$	GxCVD	VeeamDeploymentService
sophos	GxCIMgr	VeeamTransportSvc
MSExchange	GXMMM	MVArmor
MSExchange\$	GxVssHWProv	MVarmor64
WSBExchange	GxFWD	VSNAPVSS
PDFSService	SAPService	AcrSch2Svc