XForceIR / SideLoadHunter Public

forked from TactiKoolSec/SideLoadHunter

Files

cc7ef2e

Go to file

- PS-SideLoadHunter
- SideLoads
  - DridexSideLoads
  - README.md
- Sysmon-SideLoadHunter
- LICENSE
- README.md

SideLoadHunter / SideLoads / README.md

John Dwyer and John Dwyer first commit cc7ef2e · 2 years ago History

Preview Code Blame 273 lines (271 loc) · 23.5 KB Raw

SideLoad Targets

Executables and associated DLL filenames that are susceptible to sideloading

Bin	DLL
bthudtask.exe	DEVOBJ.dll
computerdefaults.exe	CRYPTBASE.DLL
computerdefaults.exe	edputil.dll
computerdefaults.exe	MLANG.dll
computerdefaults.exe	PROPSYS.dll
computerdefaults.exe	Secur32.dll
computerdefaults.exe	SSPICLI.DLL
computerdefaults.exe	WININET.dll
dccw.exe	ColorAdapterClient.dll
dccw.exe	dxva2.dll
dccw.exe	mscms.dll
dccw.exe	USERENV.dll
easinvoker.exe	AUTHZ.dll
easinvoker.exe	netutils.dll
easinvoker.exe	samcli.dll
easinvoker.exe	SAMLIB.dll
easpolicymanagerbrokerhost.exe	InprocLogger.dll
easpolicymanagerbrokerhost.exe	policymanager.dll
fodhelper.exe	CRYPTBASE.DLL
fodhelper.exe	edputil.dll
fodhelper.exe	MLANG.dll
fodhelper.exe	PROPSYS.dll
fodhelper.exe	Secur32.dll
fodhelper.exe	SSPICLI.DLL
fodhelper.exe	WININET.dll

fsavailux.exe	DEVOBJ.dll
fxsunatd.exe	FXSAPI.dll
fxsunatd.exe	IPHLPAPI.DLL
fxsunatd.exe	PROPSYS.dll
immersivetpmvscmgrsvr.exe	DEVOBJ.dll
iscsicli.exe	ISCSIDSC.dll
iscsicli.exe	ISCSIUM.dll
iscsicli.exe	WMICLNT.dll
mdsched.exe	bcd.dll
mschedexe.exe	MaintenanceUI.dll
msconfig.exe	ATL.DLL
msconfig.exe	bcd.dll
msdt.exe	ATL.DLL
msdt.exe	Cabinet.dll
msdt.exe	SSPICLI.DLL
msdt.exe	UxTheme.dll
msdt.exe	wer.dll
msdt.exe	WINHTTP.dll
multidigimon.exe	NInput.dll
netplwiz.exe	CRYPTBASE.dll
netplwiz.exe	DSROLE.dll
netplwiz.exe	NETPLWIZ.dll
netplwiz.exe	netutils.dll
netplwiz.exe	
netplwiz.exe	PROPSYS.dll
netplwiz.exe	samcli.dll
netplwiz.exe	SAMLIB.dll
optionalfeatures.exe	DUI70.dll
optionalfeatures.exe	msi.dll
optionalfeatures.exe	OLEACC.dll
optionalfeatures.exe	osbaseln.dll
optionalfeatures.exe	PROPSYS.dll
perfmon.exe	ATL.DLL
perfmon.exe	credui.dll
perfmon.exe	SspiCli.dll
printui.exe	IPHLPAPI.DLL
printui.exe	printui.dll
printui.exe	PROPSYS.dll
printui.exe	puiapi.dll
recdisc.exe	bcd.dll

recdisc.exe	Cabinet.dll
recdisc.exe	ReAgent.dll
rstrui.exe	bcd.dll
rstrui.exe	ktmw32.dll
rstrui.exe	SPP.dll
rstrui.exe	SRCORE.dll
rstrui.exe	VSSAPI.DLL
rstrui.exe	VssTrace.DLL
rstrui.exe	wer.dll
sdclt.exe	bcd.dll
sdclt.exe	Cabinet.dll
sdclt.exe	CLDAPI.dll
sdclt.exe	CRYPTBASE.DLL
sdclt.exe	edputil.dll
sdclt.exe	FLTLIB.DLL
sdclt.exe	PROPSYS.dll
sdclt.exe	ReAgent.dll
sdclt.exe	SPP.dll
sdclt.exe	SspiCli.dll
sdclt.exe	UxTheme.dll
sdclt.exe	VSSAPI.DLL
sdclt.exe	VssTrace.DLL
sdclt.exe	wer.dll
sdclt.exe	WTSAPI32.dll
systempropertiesadvanced.exe	bcd.dll
systempropertiesadvanced.exe	credui.dll
systempropertiesadvanced.exe	DNSAPI.dll
systempropertiesadvanced.exe	DSROLE.DLL
systempropertiesadvanced.exe	LOGONCLI.DLL
systempropertiesadvanced.exe	netid.dll
systempropertiesadvanced.exe	NETUTILS.DLL
systempropertiesadvanced.exe	SRVCLI.DLL
systempropertiesadvanced.exe	WINBRAND.dll
systempropertiesadvanced.exe	WINSTA.dll
systempropertiesadvanced.exe	WKSCLI.DLL
systempropertiescomputername.exe	bcd.dll
systempropertiescomputername.exe	WINSTA.dll
systempropertiesdataexecutionprevention.exe	bcd.dll
systempropertiesdataexecutionprevention.exe	WINSTA.dll
systempropertieshardware.exe	bcd.dll

systempropertieshardware.exe	WINSTA.dll
systempropertiesprotection.exe	bcd.dll
systempropertiesprotection.exe	WINSTA.dll
systempropertiesremote.exe	bcd.dll
systempropertiesremote.exe	WINSTA.dll
systemreset.exe	bcd.dll
systemreset.exe	Cabinet.dll
systemreset.exe	d3d10warp.dll
systemreset.exe	
systemreset.exe	d3d11.dll
systemreset.exe	dbgcore.DLL
systemreset.exe	DismApi.DLL
systemreset.exe	dxgi.dll
systemreset.exe	FVEAPI.dll
systemreset.exe	ReAgent.dll
systemreset.exe	ResetEngine.dll
systemreset.exe	tbs.dll
systemreset.exe	VSSAPI.DLL
systemreset.exe	VssTrace.DLL
systemreset.exe	WDSCORE.dll
systemreset.exe	WIMGAPI.DLL
systemreset.exe	WINHTTP.dll
systemreset.exe	WOFUTIL.dll
systemreset.exe	XmlLite.dll
systemsettingsadminflows.exe	AppXDeploymentClient.dll
systemsettingsadminflows.exe	Bcp47Langs.dll
systemsettingsadminflows.exe	DEVRTL.dll
systemsettingsadminflows.exe	DismApi.DLL
systemsettingsadminflows.exe	DNSAPI.dll
systemsettingsadminflows.exe	FirewallAPI.dll
systemsettingsadminflows.exe	fwbase.dll
systemsettingsadminflows.exe	logoncli.dll
systemsettingsadminflows.exe	netutils.dll
systemsettingsadminflows.exe	newdev.dll
systemsettingsadminflows.exe	PROPSYS.dll
systemsettingsadminflows.exe	samcli.dll
systemsettingsadminflows.exe	SspiCli.dll
systemsettingsadminflows.exe	StateRepository.Core.dll
systemsettingsadminflows.exe	SystemSettingsThresholdAdminFlowUI.c
systemsettingsadminflows.exe	timesync.dll

systemsettingsadminflows.exe	USERENV.dll
systemsettingsadminflows.exe	WINBRAND.dll
systemsettingsadminflows.exe	wkscli.dll
systemsettingsadminflows.exe	Wldp.dll
systemsettingsadminflows.exe	WTSAPI32.dll
taskmgr.exe	credui.dll
taskmgr.exe	d3d11.dll
taskmgr.exe	d3d12.dll
taskmgr.exe	dxgi.dll
taskmgr.exe	pdh.dll
taskmgr.exe	UxTheme.dll
tcmsetup.exe	TAPI32.dll
winsat.exe	d3d10_1.dll
winsat.exe	d3d10_1core.dll
winsat.exe	d3d10.dll
winsat.exe	d3d10core.dll
winsat.exe	d3d11.dll
winsat.exe	dxgi.dll
winsat.exe	winmm.dll
wsreset.exe	licensemanagerapi.dll
wsreset.exe	wevtapi.dll
wusa.exe	dpx.dll
wusa.exe	WTSAPI32.dll
AppVStreamingUX.exe	DWMAPI.dll
AppVStreamingUX.exe	d3d9.dll
AppVStreamingUX.exe	igdumdim64.dll
calc.exe	PROPSYS.dll
calc.exe	Secur32.dll
calc.exe	MLANG.dll
calc.exe	WININET.dll
certreq.exe	rdpendp.dll
change.exe	utildll.dll
charmap.exe	MSFTEDIT.DLL
chglogon.exe	utildll.dll
DeviceCensus.exe	dcntel.dll
DeviceCensus.exe	rdpendp.dll
DeviceCensus.exe	igd10iumd64.dll
DeviceCensus.exe	igd12umd64.dll
DeviceCensus.exe	igdusc64.dll
DeviceCensus.exe	dxilconv.dll

DeviceCensus.exe	utcutil.dll
DeviceCensus.exe	appraiser.dll
DeviceCensus.exe	updatepolicy.dll
dispdiag.exe	DXVA2.dll
djoin.exe	wdscore.dll
dnscacheugc.exe	wdscore.dll
dxdiag.exe	dsound.dll
dxdiag.exe	rdpendp.dll
dxdiag.exe	DispBroker.dll
dxdiag.exe	MSFTEDIT.DLL
fixmapi.exe	mapistub.dll
FXSCOVER.exe	FXSRESM.DLL
licensingdiag.exe	cryptnet.dll
logman.exe	pdh.dll
mcbuilder.exe	mrmcoreR.dll
msdtc.exe	COMRES.DLL
msdtc.exe	msdtcVSp1res.dll
mspaint.exe	MSFTEDIT.DLL
MuiUnattend.exe	wdscore.dll
netbtugc.exe	wdscore.dll
netsh.exe	IFMON.DLL
netsh.exe	RASMONTR.DLL
netsh.exe	AUTHFWCFG.DLL
netsh.exe	DHCPCMONITOR.DLL
netsh.exe	DOT3CFG.DLL
netsh.exe	FWCFG.DLL
netsh.exe	HNETMON.DLL
netsh.exe	NETIOHLP.DLL
netsh.exe	NETTRACE.DLL
netsh.exe	NSHHTTP.DLL
netsh.exe	NSHIPSEC.DLL
netsh.exe	NSHWFP.DLL
netsh.exe	P2PNETSH.DLL
netsh.exe	PEERDISTSH.DLL
netsh.exe	RPCNSH.DLL
netsh.exe	WCNNETSH.DLL
netsh.exe	WHHELPER.DLL
netsh.exe	WLANCFG.DLL
netsh.exe	WSHELPER.DLL
netsh.exe	WWANCFG.DLL

netsh.exe	userenv.dll
netsh.exe	wcmapi.dll
oobeldr.exe	wdscore.dll
phoneactivate.exe	igdusc64.dll
PnPUnattend.exe	wdscore.dll
powershell.exe	amsi.dll
powershell.exe	USERENV.dll
powershell_ise.exe	DWMAPI.dll
powershell_ise.exe	igdumdim64.dll
powershell_ise.exe	amsi.dll
powershell_ise.exe	USERENV.dll
powershell_ise.exe	avrt.dll
PrintIsolationHost.exe	PrintIsolationProxy.dll
de	cscapi.dll
query.exe	utildll.dll
ReAgentc.exe	wdscore.dll
RMActivate.exe	msdrm.dll
RMActivate_isv.exe	msdrm.dll
RMActivate_ssp.exe	msdrm.dll
RMActivate_ssp_isv.exe	msdrm.dll
RpcPing.exe	rpchttp.dll
rwinsta.exe	utildll.dll
SlideToShutDown.exe	igd10iumd64.dll
SlideToShutDown.exe	igdusc64.dll
stordiag.exe	wldp.dll
stordiag.exe	amsi.dll
stordiag.exe	USERENV.dll
stordiag.exe	storageusage.dll
tscon.exe	utildll.dll
tskill.exe	utildll.dll
UNPUXHost.exe	PROPSYS.dll
UNPUXHost.exe	MLANG.dll
UNPUXHost.exe	WININET.dll
WFS.exe	WfsR.dll
WFS.exe	mapistub.dll
WFS.exe	MSI.DLL
WFS.exe	srpapi.dll
WFS.exe	FxsCompose.dll
WFS.exe	scansetting.dll
WFS.exe	WindowsCodecs.dll

wsqmcons.exe	KtmW32.dll
wermgr.exe	wer.dll