KASPERSKY lab

THE PROJECTSAURON APT. INDICATORS OF COMPROMISE

Global Research and Analysis Team

GREAT

C2

185.78.64[.]121
rapidcomments[.]com
81.4.108[.]168
bikessport[.]com
178.211.40[.]117
176.9.242[.]188
www.myhomemusic[.]com
flowershop22[.]110mb[.]com
wildhorses[.]awardspace[.]info
sx4-ws42*.yi[.]org *(mask)*
217.160.176[.]157
asrgd-uz%d.weedns[.]com (*mask)*
we%d.q.tcow[.]eu *(mask)*
5.196.206[.]166

Filenames

Most of the ProjectSauron DLL filenames seem to have been generated automatically by multiplication of several prefixes, roots and suffixes in a random order.

%System%\rpchlpr.exe
%System%\symnet32.dll
%System%\rdiskman.dll
%System%\rseceng.dll
%System%\msprtssp.dll
%System%\ncompc.dll
%System%\rdeskm.dll
%System%\dpsf.dll
%System%\nsecf.dll
%System%\rdesk.dll
%System%\dpsloc.dll
%System%\ddeskm.dll
%System%\rdisksup.dll
%System%\rcompf.dll
%System%\ncompsup.dll
%System%\rdiskf.dll
%System%\iseceng.dll
%System%\msasspc.dll
%System%\wpsloc.dll
%System%\wpackpwf.dll
%System%\rcnfm.dll
%Temp%\kavupdate.exe
%Temp%\kavupd.exe

%Temp%\klnupd.exe
%System%\hptcpprnt.dll
%System%\rdeskf.dll
%System%\ncnfloc.dll
%System%\msaosspc.dll
%System%\ndiskloc.dll
%System%\mperfcl.dll
%System%\polsec.dll
%System%\sxsmgrkbd.dll
%System%\cfgbaseprt.dll
%System%\seccertapi.dll
%System%\krbsec.dll
%System%\prnpapi.dll
%System%\ndisk.dll
%System%\ndisksup.dll
%System%\rdiskloc.dll
%System%\pngmon.dll
%System%\kavsec64.dll
%System%\wlseccomm.dll
%System%\rcnfsys.dll
%System%\wpackshim.dll
%System%\ncnfsys.dll
%System%\sxsapifeed.dll
%System%\wmupdsvc.dll
%System%\dpsf.dll
%System%\compc.dll
%System%\rdiskf.dll
%System%\compman.dll
%System%\cnfsys.dll
%System%\isecf.dll
%System%\klsec.dll
%System%\nagent.exe
%System%\rpsf.dll
%System%\tv_prntx64.dll
%System%\wdesksys.dll
%System%\dsecc.dll
%System%\dcompf.dll
%System%\dsecman.dll
%System%\isecc.dll
%System%\rcompc.dll
%System%\rcnfloc.dll
%System%\rdisk.dll
%System%\dcompman.dll
%System%\npsloc.dll
%System%\nsecc.dll
%System%\wcprts32.dll
%System%\rpsloc.dll

%System%\rsecman.dll
%System%\mstimed.dll
%System%\dcompsup.dll
%System%\compsup.dll
%System%\ncompman.dll
%System%\rsecloc.dll
%System%\rdeskman.dll
%System%\mfc64d.dll
%System%\sceclid.dll
%System%\ddesksys.dll
%System%\isecman.dll
%System%\scsvc32.exe
%System%\polcfg.dll
%System%\cnfloc.dll
%System%\nseci.dll
%System%\eapproxycrypt.dll

In-memory string

EFEB0A9C6ABA4CF5958F41DB6A31929776C643DEDC65CC9B67AB8B0066FF2492

MD5

Pipe backdoor / rpc helper

46a676ab7f179e511e30dd2dc41bd388
9f81f59bc58452127884ce513865ed20
e710f28d59aa529d6792ca6ff0ca1b34

Passive sniffer backdoor

1F7DDB6752461615EBF0D76BDCC6AB1A
227EA8F8281B75C5CD5F10370997D801
2F704CB6C080024624FC3267F9FDF30E
34284B62456995CA0001BC3BA6709A8A
501FE625D15B91899CC9F29FDFC19C40
6296851190E685498955A5B37D277582
6B114168FB117BD870C28C5557F60EFE
7B6FDBD3839642D6AD7786182765D897
7B8A3BF6FD266593DB96EDDAA3FAE6F9
C0DFB68A5DE80B3434B04B38A61DBB61
B6273B3D45F48E9531A65D0F44DFEE13

BB6AEC0CF17839A6BEDFB9DDB05A0A6F
C074710482023CD73DA9F83438C3839F
C3F8F39009C583E2EA0ABE2710316D2A
CF6C049BD7CD9E04CC365B73F3F6098E
40F751F2B22208433A1A363550C73C6B
1D9D7D05AB7C68BDC257AFB1C086FB88

Generic pipe backdoors

181c84e45abf1b03af0322f571848c2d
2e460fd574e4e4cce518f9bc8fc25547
1f6ba85c62d30a69208fe9fb69d601fa

Null session pipes backdoor

F3B9C454B799E2FE6F09B6170C81FF5C
0C12E834187203FBB87D0286DE903DAB
72B03ABB87F25E4D5A5C0E31877A3077
76DB7E3AF9BE2DFAA491EC1142599075
5D41719EB355FDF06277140DA14AF03E
A277F018C2BB7C0051E15A00E214BBF2

Pipe and internet backdoor

0C4A971E028DC2AE91789E08B424A265
44C2FA487A1C01F7839B4898CC54495E
F01DC49FCE3A2FF22B18457B1BF098F8
F59813AC7E30A1B0630621E865E3538C
CA05D537B46D87EA700860573DD8A093
01AC1CD4064B44CDFA24BF4EB40290E7
1511F3C455128042F1F6DB0C3D13F1AB
57C48B6F6CF410002503A670F1337A4B
EDB9E045B8DC7BB0B549BDF28E55F3B5

Core platform (LUA VFS)

71EB97FF9BF70EA8BB1157D54608F8BB
2F49544325E80437B709C3F10E01CB2D
7261230A43A40BB29227A169C2C8E1BE
FC77B80755F7189DEE1BD74760E62A72
A5588746A057F4B990E215B415D2D441

0209541DEAD744715E359B6C6CB069A2
FCA102A0B39E2E3EDDD0FE0A42807417
5373C62D99AFF7135A26B2D38870D277
91BB599CBBA4FB1F72E30C09823E35F7
914C669DBAAA27041A0BE44F88D9A6BD
C58A90ACCC1200A7F1E98F7F7AA1B1AE
63780A1690B922045625EAD794696482
8D02E1EB86B7D1280446628F039C1964
6CA97B89AF29D7EFF94A3A60FA7EFE0A
93C9C50AC339219EE442EC53D31C11A2
F7434B5C52426041CC87AA7045F04EC7
F936B1C068749FE37ED4A92C9B4CFAB6
2054D07AE841FCFF6158C7CCF5F14BF2
6CD8311D11DC973E970237E10ED04AD7

MyTrampoline

5DDD5294655E9EB3B9B2071DC2E503B1

Bus manager

5DDD5294655E9EB3B9B2071DC2E503B1
2A8785BF45F4F03C10CD929BB0685C2D
F0E0CBF1498DBF9B8321D11D21C49811
AC8072DFDA27F9EA068DCAD5712DD893
2382A79F9764389ACFB4CB4692AA044D
85EA0D79FF015D0B1E09256A880A13CE
4728A97E720C564F6E76D0E22C76BAE5
B98227F8116133DC8060F2ADA986631C
D2065603EA3538D17B6CE276F64AA7A2
FCD1A80575F503A5C4C05D4489D78FF9
EB8D5F44924B4DF2CE4A70305DC4BD59
17DEB723A16856E72DD5C1BA0DAE0CC7
B6FE14091359399C4EA572EBF645D2C5
C8C30989A25C0B2918A5BB9FD6025A7A
814CA3A31122D821CD1E582ABF958E8F

Network Sniffer

951EBE1EE17F61CD2398D8BC0E00B099

Contact us at: intelligence@kaspersky.com

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy