DRIDEX's New Tricks Lead to Global Spam Outbreak

Appendix

TrendLabs Security Intelligence Blog
Michael Casayuran, Rhena Inocencio, and Jay Yaneza
May 2016

Indicators of Compromise

SHA1	Detection
1a5179c9b72fdb4b606cb63037c91de413a49db1	W2KM_DRIDEX.YVD
7ea297d29023a7ea7a3d01df618c0166c559bdf5	
19cc50c25f6135f73852f06c9a0722deff76a3a3	
22a7d69955fbafd0d5e090295e367a409731ba90	
93ec6482f36639578784a61f6bc1ed4b0fa14912	
133a1fffc46903061d8ea2d12b80deb89636dbb4	
268f374b0fcc7fab399c64311dfac2e9f97a4da1	
707ad2ab4f9735b51e5da503178d7763198cc4d7	
885b48c5a644caf92ce62e70b90197c6f30b225c	
4611e4824587231d7dc6fbe271d18b14bb3aed3f	
84342db658af50c34dd75c792bf4ff726d6e02d9	
94046ddd538b5831e9e3ba7548e84da645ad4bb8	
96197dc35306c827f3891c1fdf807624b071972d	
406059fe3ddf8ef42bfcc99441871efd2fa8fb07	
603135d21d691797969fd1e330e285c173815ab4	
a1a5c7a55e14481a93b1e2a836a4ffaf1242b301	
a14b2b9626549b34737ffb55a5caff71cdb3d714	
a3606a848a40c554ee60add2eb53ba44778aca46	
aea29b594274eeabf954415a347fbca802d057e3	
b9afbd6054d4c512b0e4e048e2eec518acc95b0a	
b99d8c6e0ad54728cb93eb22a1ae9115a2cfc750	

SHA1	Detection
befa9acb077f8c8c75e3892a811c5bfd08e3e7fe	
d775706af618112ad7e8defe3a77ec9724b97a8a	
de238864f60e34b6fc6d4d26590692141ad9ca32	
ea83c4f39ce54f09359f09f14ae8e05e055ab6c5	
f9d17572fdf3e891f03e23ea0b1bfef276405b49	
f778982a989c54f800aac913e0e9afa7d6c6a8f2	
0699fb11acea5906e4f5d6c97164812c51b579d2	
0b70c4376e74700bb4df6882c28a71ace417d2c9	
2859eaf08f5da8752b2da399cc583d5030ac7e9f	
350d537414ddc7db6c545e1d2a25406161615693	
4d3f50def97ab7eab86771d1bf2f2710c8af48d0	
594d87c767f776ca610636b601a9cc9faf0fd1e0	
5ae28c8f5ff3e35c708ef76e40c9672651ec6fc9	
845b1d71ffec59322f688a21221e5817475d2da9	
89fe9b77ea0e9ec6dc5ded8d9812b4dfab612512	
9f227611e68ef2128bdd7a9f03483f7f8e275920	
a136f9ff047767fe4d603c96c6c57d759a211c2c	
b0c100374dd7142edf97a9d233b3c68bcf77a07e	
b3b07b038834a8b3eb8527f2990a1b8d89e82602	
bb9bed40b9b8eef3132e6c0844a88744c61fe219	
dce40b0833f241b6027633ff4481a3ea910766c3	
def75ed1591517947f094b02cb3627a2e852e637	

SHA1	Detection
e34f5dd4d8b8d40c49afef563055baeee9d0c755	
faccbbc8160e27d7c625d0be6b974825c68dc58c	
b94f0b460cf620a77120bbe76dd378146116ed25	TSPY_DRIDEX.YVD

Related URLs:

- 101[.]187[.]28[.]8:8443
- 12[.]109[.]210[.]112:8443
- 12[.]227[.]176[.]187:8443
- 135.26.29.213:8443
- 14[.]97[.]18[.]93:8443
- 14[.]99[.]8[.]219:8443
- 165[.]255[.]60[.]173:8443
- 197[.]96[.]139[.]253:443
- 203[.]45[.]13[.]29:8443
- 206[.]223[.]199[.]159:8443
- 222[.]255[.]121[.]202:443
- 24[.]8[.]213[.]200:8443
- 5[.]2[.]145[.]23:8443
- 64[.]203[.]222[.]43:8443
- 67[.]22[.]207[.]161:8443
- 68[.]200[.]154[.]229:8443
- 70[.]164[.]35[.]105:8443

- 72[.]27[.]189[.]56:8443
- 72[.]35[.]204[.]239:8443
- 74[.]207[.]137[.]87:8443
- 75[.]67[.]214[.]42:8443
- 78[.]146[.]221.200:8443
- 82[.]140[.]160[.]54:8443
- 82[.]152[.]47[.]41:8443
- 86[.]175[.]137[.]132:8443
- 89[.]230[.]226[.]187:8443
- 96[.]93[.]247[.]161:8443
- 174[.]34[.]164[.]106:11443/2/natwest_62y7rKX8yF819Lg3/
- 174[.]34[.]164[.]106:11443/2/halifaxpers_62y7rKX8yF819Lg3/
- 174[.]34[.]164[.]106:11443/2/lloydspers_62y7rKX8yF819Lg3/
- 174[.]34[.]164[.]106:11443/2/tsbpers_62y7rKX8yF819Lg3/
- 174[.]34[.]164[.]106:11443/2/ulster_ie_62y7rKX8yF819Lg3/
- 174[.]34[.]164[.]106:11443/2/ulster_uk_62y7rKX8yF819Lg3/
- 174[.]34[.]164[.]106:11443/2/bospers_62y7rKX8yF819Lg3/
- 174[.]34[.]164[.]106:11443/2/rbs_62y7rKX8yF819Lg3/

Spam-sending IP addresses:

- 91[.]126[.]113[.]98
- 81[.]135[.]163[.]170
- 92[.]53[.]8[.]33
- 89[.]161[.]7[.]29

- 189[.]201[.]241[.]39
- 191[.]6[.]166[.]125
- 200[.]218[.]244[.]205
- 179[.]105[.]223[.]6
- 92[.]114[.]80[.]90
- 202[.]158[.]6[.]57
- 187[.]210[.]229[.]13
- 190[.]111[.]75[.]30
- 45[.]64[.]166[.]26
- 196[.]44[.]165[.]42
- 101[.]96[.]114[.]66
- 179[.]38[.]90[.]245
- 201[.]6[.]240[.]190
- 31[.]11[.]93[.]53
- 191[.]242[.]27[.]96
- 188[.]241[.]121[.]168
- 60[.]243[.]207[.]59
- 223[.]31[.]109[.]82
- 51[.]179[.]25[.]170
- 5[.]149[.]90[.]113
- 114[.]110[.]23[.]217
- 129[.]208[.]209[.]32
- 191[.]241[.]229[.]22

- 109[.]233[.]23[.]122
- 46[.]136[.]220[.]202
- 198[.]23[.]143[.]113
- 185[.]108[.]99[.]144
- 109[.]177[.]147[.]168
- 193[.]188[.]199[.]5
- 185[.]89[.]245[.]180
- 5[.]160[.]89[.]195
- 186[.]170[.]23[.]98
- 150[.]107[.]239[.]145
- 91[.]112[.]149[.]50
- 86[.]104[.]215[.]16
- 41[.]215[.]244[.]83
- 36[.]73[.]200[.]237
- 125[.]99[.]72[.]50
- 175[.]214[.]99[.]120
- 185[.]97[.]118[.]216
- 51[.]39[.]254[.]233
- 41[.]180[.]4[.]210
- 213[.]243[.]4[.]132
- 197[.]231[.]159[.]154
- 197[.]159[.]214[.]14
- 185[.]117[.]48[.]154

- 139[.]192[.]147[.]54
- 80[.]120[.]67[.]90
- 197[.]248[.]222[.]70
- 41[.]218[.]102[.]82
- 185[.]76[.]248[.]253
- 103[.]59[.]202[.]131
- 41[.]76[.]8[.]51
- 103[.]207[.]56[.]230
- 43[.]239[.]144[.]71
- 103[.]225[.]221[.]162
- 117[.]247[.]232[.]133
- 115[.]124[.]70[.]250
- 180[.]93[.]100[.]4
- 49[.]143[.]187[.]227
- 201[.]130[.]1[.]118
- 109[.]177[.]100[.]208
- 197[.]210[.]186[.]133
- 177[.]36[.]184[.]144
- 92[.]58[.]155[.]253
- 89[.]108[.]145[.]100
- 103[.]18[.]180[.]10
- 177[.]39[.]155[.]115

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003