Symantec™

Security Response

Comment Crew: Indicators of Compromise

Introduction

This document contains additional Comment Crew indicators of compromise that were seen in the past year. See our accompanying blog for more information.

This document details the following types of indictors:

- Network
- File
- System
- Email

The contents of this document are indicators only and may match legitimate services or applications. Additional verification is required to confirm an actual compromise.

Network indicators

Network based indications of possible compromise by the comment crew attackers.

HTTP POST traffic containing

- name=GeorgeBush&userid=<4 digit number>&other=

HTTP GET traffic to pages with paths:

- aspnet_client/report.asp
- Resource/device_Tr.asp
- images/device_index.asp
- news/media/info.html
- backsangho.jpg
- addCats.asp
- SmartNav.jpg
- nblogo2.jpg

Domains

- GT446.ezua.COM
- aunewsonline.com
- avvmail.com
- cas.ibooks.tk
- cas.m-e.org.ru
- colville.com
- cvba.com
- deebeedesigns.ca
- dev.teamattire.com
- doversolutions.co.in
- download.epac.to
- drgeorges.com
- dril-quip.deltae.com.br
- dsds.co.kr
- [REMOVED].ruok.org
- engineer.lflinkup.org
- exactearth.info.tm
- fbrshop.com
- firebirdonline.com
- forceoptions.net
- freelanceindy.com
- ftp.xmahone.ocry.com
- garyhart.com
- gobroadreach.com
- hint.happyforever.com
- hojutsu.com
- imly.org
- interradiology.com
- jimnaugle.com

- kayauto.net
- keenathomas.com
- ks.utworld.ch
- mast.zyns.com
- media.conci.com.au
- media.finanstalk.ru
- media.metdf.com.au
- meeting.toh.info
- mountainvalley.americanunfinished.com
- mrswehrman.com
- mwa.net
- news.hqrls.com
- odysseus.qs-va.orbcomm.net
- ohb-technology.brgh.de
- omegalogos.org
- pastorsrest.com
- portal.itsaol.com
- progammerli.com
- rbaparts.com
- report.crabdance.com
- [REMOVED].photo-frame.com
- route.cisco.ns01.info
- shunleewest.com
- slowblog.com
- smilecare.com
- software.myftp.info
- soko.com
- tcw.homier.com
- [REMOVED]comminc.us.to
- [REMOVED].arnotex.com
- thecrownsgolf.org
- [REMOVED].alfalcons.com
- twocirclesmusic.com
- un.linuxd.org
- update.sektori.org
- us.gnpes.org
- vwrm.com
- woodagency.com
- worldnews.kickingdruging.toythieves.com

Internet protocol addresses

- 140.116.70.8
- 143.89.35.7
- 143.89.35.7
- 150.176.164.6
- 202.105.39.39
- 202.39.61.136
- 202.6.235.83
- 203.200.205.245
- 204.111.73.150

- 209.124.51.194
- 209.124.51.219
- 209.161.249.125
- 209.208.114.83
- 209.233.16.84
- 209.253.17.229
- 211.232.57.235
- 212.130.19.154
- 218.232.66.12
- 218.233.206.2
- 218.234.17.30
- 24.73.192.154
- 46.149.18.151
- 60.248.52.95
- 61.219.67.1
- 63.192.38.11
- 64.80.153.108
- 65.105.157.228
- 65.110.1.32
- 65.114.195.226
- 65.89.173.68
- 66.151.16.30
- 66.155.114.145
- 66.170.3.43
- 66.228.132.53
- 66.228.132.8
- 68.17.104.162
- 68.96.31.136
- 69.20.5.219
- 69.25.50.10
- 69.28.168.10
- 69.74.43.87
- 69.90.123.6
- 69.90.18.22
- 69.90.18.23
- 70.108.241.36
- 70.62.232.98
- 74.86.197.56
- 74.93.92.50
- 78.95.63.1

File indicators

File based indications of possible compromise by the comment crew attackers.

Filenames and locations:

- %TEMP%\AdobeARM.exe
- %TEMP%\iTunesHelper.exe
- %PROGRAMS%\Startup\AdobeRe.exe
- rouj.exe
- %USERPROFILE%\Local Settings\iexplore.exe
- %USERAPPDATA%\Microsoft\wuauclt.exe
- %PROGRAMS%\Startup\adobeup.exe
- %TEMP%\AdobeUpdater.exe
- NTLMSVC.DLL
- %PROGRAMS%\Startup\adobe_sl.lnk
- %TEMP%\runinfo.exe

File version Info:

Product: SoundMAX service agent

Description: Microsoft NTLM Service Holder

Product & Description: JpgAsp

File MD5 hashes:

```
00b61db083b07a64fb6072b42aa83dc1
0136ab6d2e507d4e63990b196121d41c
017c03ad61f89ee6597ead40cc552aef
019cb1a6776f0e0d353814711e9e171b
02043566d027445374a1f7f0fc35d495
025dc68c8e06d6488e338dcc55b295eb
026c1532db8125fbae0e6aa1f4033f42
02c9a3c3efd52e43dbf53e0995a7a24e
051caf12c36662d946fd0146cd199db5
05269f5236bd89b66f6f4694abef6222
05c63c450d4d2aeb23053a6b6f8275b0
05df8d890eb18614a7d206b41453d306
086e91fa95136ad1d814cac327543bf9
08ac41ce00bf436a3dc23c4639d5f5ed
0925fb0f4c06f8b2df86508745dbacb1
09a6d5b54e8c48ed33189ebf80df750d
09c0f3a3099b6b38ec36d001361edd98
0a98bfa4bef1eb755c9c154963b69dc8
0aa4e635a61038a621d9264e33b4bc3f
0b33a683812124d99de45c8e84dc9013
0b6755e61840378952d69630b5c23e41
0c6f8665dd18d5e86124c7bfbf3207f0
0cdfea216d117cc97845edb9becaa498
0d335de3c082627cd0c5699aa6012b7d
```

```
0f1dd1bef76967a6b06a5e0432ca947b
0f4432d54b28aafc976b5950d5337a5f
1285ff3c3a4089b43c275220d0c54442
1286c678b3a821dec8c8cc1125bd2bc0
12c64a64ae32fd3dff75347dde2aafac
13eb87290affe1360834037d9d400b39
1475f178b6a86d3922b3e2c6fc59512d
14d17aaa3016a618a3ede92511fdd339
16710c96d5ee6554bae6b881d9e136bd
17173efe0062114d2f993c7584520c1a
18575542dc4e9aa5aa8eeda14c26e46a
18a3bf5d8336f075ba503622880b5025
19bc509f31f33a8f473ef9d671c1828b
1b517ea2aae0ed0a71f6e74e34e860e1
1bc363e4ad9fc3be4953dd3eaa2bdb76
1d1e2c7bb5a9fa546a6b0ae3c308db61
1d69504a3d3ac32275fa4df8af25d1f7
1ee30f7ecaf25af38cf684ca56b75cf2
1f9cf9f1b5738198674a58a378b0d7e1
218bbd007898e6b6fc754fe5c76668fc
21ed762e867cdabbb194aba878530c88
22e10cbe46f406f5f1be0d613db4c2c3
241e8465fd4d99a3f446d7f75957522b
24be0dd53bb43bb6cd08044b21a6aaaa
2500494616f4e7e1fa14fb3a46f468a7
255b1aaff69668ac19906219d36c607c
271dad1471efd9bfc1a9dc05d6c30a24
27fb01f7b3137921126ba086da4e6a2c
280531bb85998ff3dc7eb8d057525ffe
2997ec540932ea6b1fe0cab555b939d8
299ca1f787d2340d34407ef084845260
2a3aca1b002c6894c5edcc5e25a8f970
2b3faf2856c220aa8b87632ac8bbd1a5
2c4cabb4ca19ddf87c7f11bad44bdf05
2cf5b5a9333d159b664725811465d1a3
2d0318507bc4c1958913b31009de37f8
2dbbadc147f11f2a856a648cdc332c0e
2e7a8e7e9d8d62c94d011e86de9cb12a
2f37912e7cb6e5c478e6dc3d0e381a24
2f6c8da1c5f397bea7b300d28b3ad4ba
2f7918548b0aa59f23a1c16aa98e058b
30e81a30471c8f63b4688533252b56fa
320b4bd876004c1f0455f6f48b07e164
32e474b21555d3946970c73648d88b36
33a03ca462cec85e33dba0a1dcb9aee0
356e11813fed7623a77610e836bcab65
3599a78c7e99b451c00d3490f17f842f
35ae79bbe9f560b9634ce28b6569bd0f
35ed31733fbd7eeb4bfcc29e28a8496f
36ca00585d13d6911f086f0d2d496f96
370947e6c802d21a732ac0cc024c4fcf
37b1e5809dd5a92a1d73f0e36af6791e
399c41047abd99b6e86d04b7dd444509
3b266b165468b810cd456cdf88ca8619
3b6a1f6ad4b8141b1aed8644d789706f
```

3b8ada8eda04f204164449a0fec0c296
3b9cc9e174ad19380efef2744b7ff046
3c058ca758f97cd2ae56df8a08f6a5a3
3c9aa6dc8c4501ffa2798f044df53438
3ce55c6994101faec00b5b7c2fee494f
3d41375ee362f4265ea2e90b9a08f0dd
3f637c1477442d92962be4ed427bb1cd
3f9e63ee4ae254778c69369fedf0d999
3fb6039a572369d8d23fb99987ea21a9
3fc2aa493492e6d7560ac8a5d69d7cbd
3fecd601404abda8f793ff5cc7ecf973
41998b32ab11e474b167edf9dbb59b12
4248d33b4273a80d11d6b3b6297851eb
4287353240e4e473e940a9289a48a333
42acd0ed699d94602a0494f65a328615
431f635eb68b936182d73bf6db06fc97
43e128cfd0080a644e4ce98f84e29e8e
43f3a0a82397400a181c080992d35a5b
4602735e4a8754ff7f5a8785f9fd336a
467b90773754e35e1535a164140be005
46b3b305530fb68f7a88b8453e4866ea
4890bf4c2d68657969e1cd11e0ae2648
4899aa64923115886dd7cff5fff5ea1c
491db327f479a1a34898229811fa8a5d
49cc5f649e9098530ceeb2ea45346a9d
4b03db464b22536f700c99c3bd36e9e2
4c136f1fbd9d7010369ae5644a8af4b0
4cd5a29a7fc904aaaccbca9e30e0a865
4cdfb56105b07f463d046fb425567cb0
4ce22cee6abcb37db757e3fd60970090
4dc2bcad31fb36f0913e441deeda8121
4e5ed120295d9937de106fc703e64732
4f13bd1db43e54d2cd2427a87ddb8e22
507fa8a735417219d6b881834f660cb2
5084ddfb90791516015c02c68d58fe5d
5106b19a9a29f0228782e0cafcd1cc2e
516c2981f3506ede7608ef2f273c6aed
534b3650b350b503e0f0f3bb6dd7598c
53d1e354104d5fc028d83aa519c1d1c6
551aa0ab2b40fa7d891664caf0da879b
5621ed9c3b844654141c1a5ea7ca8c0d
578dbadaa5086e24d576328b7d4fedba
57bc1531a12179c5794d5c99b8442eba
582207d1f939f80bacc36a7790f40dc8
582e827a539b6243f1c90b720fc143a4
5aea3a20553a07fa50c4e815cf9ba7ff
5afdb5db234a1a13f5449be25f114999
5ba8c4ef080e61310943fcb3c68bf002
5bdb1b2313541f4cdc967391a4d150f4
5c43e4ac0a6ad74844b2a310f1abc1c7
5ca21c7986db58d44306e94f1ea6ae5c
5d1d18c697eefb03e120d9ef3f53dd28
5e8d1334238dfaf5f11d7f2186989095
5fee0adbac53eee82626daa5c5f99aba
607b46c73adb9a8bf03f5cd038871347

```
628e4933864d3f712670658a93d11113
62ccc75782d657850b85456ab48f2277
633d92d13c2e8330cb4a3bc5130ab84f
640a64136516298ca80490d75a365695
640fbb5f8938ea45204de6496240f82a
6414217bafb6f4c058773b0134e56e99
64b865afdc34091a9c02700adeea5853
655d1322795ed9532390ccf2e8f726f8
659300af2f7c9e76f55464b21784a7f6
659fb07c70034571de7a1b4b5ac86b01
66060b82f299c14e18b65d21d277a49e
668731574fa9ad7567fb4854805a3fb2
66e4538702381035dc62247080d4593f
6757128a636e2c509861d4f75ff128f1
67a8b964857fe499b62442308a767e94
6827e494a230a1483e19c205c532df17
685e10f1393eaee470224b7fe1359202
688ba2b3739ad54dee4139a727e457cc
6981364b6f1142363c151b11da66cc98
6993ed604acd3e17a7bafcfdc2b27898
6a0280f169d233a0bdc81ee6a70ef817
6b8585ffbdf90c9b120ac1a79fa4dc51
6bc6bacbbbacf369fea145d9044bd863
6c5b2712a66db42b960aef5b87590033
6e67fc27a49769f5218824d405d8fce5
6f1c70d77e2571fe8a402aa1a8b7e8cd
6fd6aa2a4038903ed6d8e5771689f7c1
700941e4fa44941b18844c9bfb3474dc
70320b5c719c70c860a55cec7ef173e8
709d6eff31854fad212f83a91a900920
70fef3c8073e97980b60b4ad8388ab5d
716978305d76e1e458c480d80f24caca
718179479dd9bd93beae66665e452c87
718fcf2a80348110f519a000854e9e0e
71de04a952f8c09243c15a7fa5371073
71fd3ea6c3e7e2f1eba9d7e911b1cffe
7228ac8f341f6ecaff45c8163f421f14
76000c77ea9a214f5b2ae8cc387809db
7715864443576c824cdc9f39ffacd9dc
7b81fa4334cf0e520269f5484fef9fca
7bcdd0e5996e849d1068fcffdec81371
7bee4b7d948433a58b18d2189d480a29
7cd15bb31ff889e81f370d0535e02493
7d00ea1262125b2b0469dd639b810823
7d101cc3b87ac51c0c1ca8a4371bc84a
7d21e2b1b293f4176ba1d8abc2460328
7e75928b5ce3dd41c9b9b1e67cff16d6
7f7cc1a8d7a6bbe6a52c94bb7f41f727
7f90942ace185ca1ba5610f6eddf3376
8027234685f88f3b74c45b245c841843
802a3965e42e75cc3dcd5f5523929859
80ba5a336a4044c1406774d56e130e7e
80c58de2dbd1571228b538c9556cd29d
824bee27f10d5c81879657c8a2af9f0c
82c598abdf848c6fef03c63f5cf7feaf
```

```
834a274599aed64959b3b2bfe931af4c
83cdbc9aa1907d55dda3e28149e897cc
83d45d80682afa9b2526029b2bc2fb33
850ac92dfa39f2391addc2d888c62ef8
8548dd501aaf132b134aa3849e15d2aa
85873c12599490a0f7db691b0c5179ae
860d5840c3b1a750d8c4e6bc68ecfbab
867d80bc1c369ca7ee429c727d2c5fea
875cb4844bc03f6da7a60553632c7678
888eadff6982de01c60891ce185473b7
88c0e5a4ca408ac12acaaf7a9ef9eb49
894ef915af830f38499d498342fdd8db
8a413af90665ca7909bcdcf19cd566ed
8ac64b904c188ef6b73dbc5073cee1a9
8b69f0a948c32288f3fab4ed2845cb1b
8ba366ef5ecd802c82289dcea22b2146
8c148fe80ae705af284b92f1c283013a
8c3a791ce682e3c5da5bcfbce261eeaa
8c76de0a8ac79536b96619613960681c
8d3a6b78118b647a7f31f06a46c27fd4
8dc7eb49fe1fbf490f90c153a71c60a5
8e2e709c01ccb286c51ac9e592eea48a
8e53ad954f05d2c3f57b19b1ecb0fea0
8f8e948a2f9afd7ece6dc6603cfbd56a
8fbbf38c053dbb0da3dd2fd6af4869d2
905d5cd372fb22dd5f9804adb2d2787b
9157d078effa4b727180c40bedb74ef6
920dffe40787f1f3fdb24548b4a210db
92785f445f366ed548388b1af6b01f9c
9327f1eefb18fde7f622fc2efbbbdb4b
939e07685fec28a15f88786b097bb14b
9400950fa381ba1750c914fa9e6fd85e
942b1ca8c3c64be1e4c40e26c9e39ad8
962c52436706b5c226894de0436b860e
96ee5acbe155f37ff1604b4fd259e55f
96f31d6fda587b43887e846876e5c399
975c718bf93ca5d0693bb0d4c7e42d1e
99b58e416c5e8e0bcdcd39ba417a08ed
9a58902740c5b73eb6a68a126ac6ac55
9a847c1f54359ffd3c335e97600f6f5d
9aca099f7cd3b3b29551b67af48467d1
9be590614e2407dc144ad6c100a2873a
9bf4683c09a2d60294ff79ce026f4e64
9cc15358d6ce18150dbee6be3281151d
9cd1e3b67540bdc2fc4a3835e170bc65
9e6b8b265f05302eca455ce8ea10a3aa
9fcb233ee18df6c19b1ad3922dd41a2a
9fd0e94fce1543b75b44414a61b252b0
a01ea69e4c10721ec088676cef67d8bd
a19e68e72084d867a39776faaa6f5fce
a1fa946523928c16340cf40daa2ffb53
a26a85c33ddf57d720040629931be174
a4847e655c817e3c5112e888a2877f4d
a4d476fb7b084bd01a847ab7e0d839b5
a55f6c8b795ccdc469b9b67b22ddc88b
```

```
a637ea307380ba21a355c3cffd37639a
a6cba31fcca49ff9ed6fd9894644de9e
a76f0fada1602e9c119cba24306442b4
a98d2c90b9494fc885c7cd35d43666ea
a9c20499d43f9674cc37dbfa81381203
a9d2caa6ebbfd5be071748e59e754cf4
a9e0a604e5b8ed5f4f286c3355d7a0fb
aaa01f776acabdf9f07ea3eaff1695d6
ac2b219ede57f9d14cdce38e987862aa
ac9e0b2af215821f7223b6eaeaea03db
ad95f613fc4b644bd5e3230eb0b5dbcc
adb97252b05a6e82697bf93c347bdf25
aea5dc22e706c836d056f4ba1f13dea3
af285fa9a141f422b8ccbfb4e9a00054
b18cabead7248e8156230c71399b79c9
b19ef1134f54b4021f99cc45ae1bc270
b1c540b4b9c8a87a1e87a76ed289f18d
b2784e4dc6e602d9d6bf09325bba8c4e
b29556856203049b9e7b05e01f5ae73f
b3056919871fc01a1ed3294e2014e0c4
b41c02eb41070e0a2e459abf2fc39b69
b44cd1fa5d8beb08519bbe0c1d796b0f
b457372a87597b746ce69e05c4a7d3fa
b653012d2bfa4e3419d97eb9f2e5ed4a
b665ea35f8f7954657eed1e54517843d
b68eadb2a8069c7e88535e1ebfb4be0a
b8c83b3549ebb24b3e00dd23c2aa050a
b8f77674d292d205f8f5cf6c3f3c34df
b8fdf06f78341581870477574e2b08c3
b921e0d11127af9613804c63cddd86ca
b9367aba4f267b82a838223df016bd6b
b96b79f4f1b4306ac2c63fc988305fb0
ba700e3a83fec3cc984e1fb572aa0add
bbb4bdd1d7e8589d145163f1efd458f5
bbbf285e8344f7df330f93c7c3baf27f
bbccf8643368c80dd083fb92d67d00be
bbdce1e1991f292d366097a743da3724
bcc6addece28265390b2d535d65c49b8
bd6481ed6dfe67ba9f2f8f26e2cee722
bdf512d5eef853d07c0db345345e3db7
be3799da210edb81143d609e66e5b7ff
be54e3660bf928b8b5f764f5cdfdc4da
bf18ef997b7d589f031f47799a33f27b
bf65727accaa53d65c31ed5b582053c5
bf778439895829ff986207900bfcfe02
c1438390098e4dc7bb8b52efcf1d2465
c1919e6f2e05feb9dc9b6ab9f81dcb2f
c243a7c1cf23b91f73100bb9e947439e
c32696b255bac4b849fc249e56944a91
c376aecf43bf021b6408ca99cd31da01
c5062bbbb15911a63de77a66773874d9
c63cc0a8b0b3a70f7b835a3fff9f02a5
c8607553e37cc1fc870572670c1910f5
c89d4d40e4b68a9952121b62b0dda920
c9570396c897e02ec8aa195c6241f945
```

```
c9a32616f89dc953486bd1b5d83359ec
c9b4c4d65298dc10be6784d0f0ad8519
c9f19071bac9d4eb3b08b4017c0d9c4d
cac3bc3039cd73935051ad8df2e53d34
cb40ff3b3ed8c1966defbe1dafdd1326
cca75af9786d7364866f40b80dddcc5c
cd5f3dbea197dc5afb673e42f0e9c3fe
cdc0c4fdc649dec017ace0f2898068d0
cec766518fa5b607157e92e9c24c0d03
cf5356cdf42d264d5213cce4cd415f0b
cf96139290c09963a32506cd85825ed3
d3174652816010a7f6d8f4523ee3a077
d4036f03c760084cc677edf4ee6c4a39
d46d261ec92daf703cd584f10037198c
d5027d35c8bd9e867113bd4a1edb931f
d58323fb222b9ff681c0982ba286a296
d6b1989d9c271b8575326e4fca159ae8
d6b198eda724e2b3367502a6a2232939
d6b467c92256094f720e9fc75f149737
d6d5aeb79899485f5734bf8847782266
d6e98d062d7900c6fe9a6d7f0b1d7fec
d6ff4333eb1a2305d5b6cf4705213393
d795292ea23217480ad92939daf6dd22
d83055efe66377067ce99d99c706f19a
d8f7aaad3677fac1cde911c7362c2b69
d910d21bd54b63ef61b3f250fe73dcc6
da451674bb68804b390bd7413691c91e
dab17bcceae6f32eae5d800d0d3f9e46
db6ae6da64f14168b3624e26191277cf
db7d3724e5f004168a1a56f6b9de3cd5
dd5aad5d66bc96e5ac60cbe5d132c2ec
de5eeb9847a5fbc1a6cbb4cfb8bb6aa0
df53ce3797932d9e62ceaa760a3f0e3e
dfaa6250dc947602d5dc200e503f23a5
dff3a274e5fa35013601c7985bf13d56
dff7ac111e48115e208c2649b94b1115
e0b3a0fd042ff50e0de22725864775b8
e1117ec1ea73b6da7f2c051464ad9197
e2494eba419891c0c101af74eb8c029c
e2620e1cf89830e8de1e8c4530829a15
e27f0975fd3278e7303102783767c508
e2a557b39231ee91724c150e3ec4b493
e2be37df12f7b98b2b73197d77773263
e4255f51a871a95baa10b6b2c4ed2470
e62bb947d72d12311890f2e07eb6ac8b
e6446d52e9f4b5c2c5a9ac850281cae8
e649b8b9e541406446da47d8d0a91385
e6ffb1c6e1508f474a69f091435454ce
e85863b1de035814b4b01a2b6c477dd1
e90b037f1cbc79796fd8b1f6382c8483
e93a4f4872bf6cd8c3f0eed6017a8d41
ea823850b777993d636e4a565568f734
ead35eab94820d5a34f185d0b26b7930
ebe291e968eb5a86b4963d27352bc525
eced29c71867e375aed0da408d6b07f4
```

```
ed665cf8a48f08f8b4fed8bbf9d2d998
ee998128e20971ca4296a8a73ed79f43
eea7ae4eb726c3e05f187110090adb18
ef10f4f11032d48f7e82c0a788c0f489
efaadcfa4271c50927ab817e0c4a0bc3
f0a00cfd891059b70af96b807e9f9ab8
f15cff24d8a3a9ffce590cc8e69baec9
f1c4b919fdf008a8400189562f5e2fba
f29cb80bde4af21c226596e9d125795d
f2f2cad79dcfb356db7b2485c7a27f03
f643fa851203e9159c9dc50e4ab8d81e
f74ec871c77e4b5e5b2ae0917b1f0f21
f7820d429d3185ad00e6758c343e29ce
f82d3b270b16780044817978f4f3fe1a
f9d2c3e8f81b9c44a1837478b2a98e5e
fb0b900de6d286321fd6d20c6c4f5679
fbb0c14cacc60fdd393fb5889d5a0b57
fc97b89541b149e0dd9937ba876b3ee1
fd130b2bce93caf18bc23f1526daae99
fd31f952637370a30d74c2a65ba8d2cd
fd9b5c35c042a6c462187067fb869aac
fde5e109bfab33964564f387f8940030
fe568a370aa3d2c78125ab37c16484d1
```

System indicators

System based indications of possible compromise by the comment crew attackers.

Registry entries:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Acroread"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Adobe Update"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCheck"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCom"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"IMSCMig"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"McUpdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Register"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"SysTray"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"systemupdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"wininstaller"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"APVSVC"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"AdobeUpdate"

Service names:

- aec
- elpmasym
- Net CLR

Email indicators

Email based indications of possible compromise by the comment crew attackers.

Subject lines

- Capt [REMOVED] update
- Fw: LES Request
- Libya crisis
- Five Simple Questions for Democrats on Spending Cuts
- Behind the Easing of Israeli-Palestinian Tensions
- Business Exec Urges Broad Trade Agenda To Curb China Role In Latin America
- President Chavezs Comments About President Obama and the United States on Sundays "Alo,Presidente"
- FW: New Standdard Operational Procedures (SOPs) between the
- AGENDA
- [REMOVED] Help You Save Enough for Retirement
- Human right of north Afica under war
- Spreading Civil Unrest in the Middle East and North Africa
- The latest analysis on Syria
- International Atomic Energy Agency invite you to attend Atomic Energy Summit
- GAC Monthly Report
- Emergency notification
- Meeting information of [REMOVED]
- Meeting information of [REMOVED]
- Meeting notice from [REMOVED]
- Meeting notice from [REMOVED]
- FY12 Government Opportunities
- Yemen para for SC briefing
- Fighting Protectionism and Promoting Trade and Investment
- Weekly Security Report
- Agenda of [REMOVED] Visit in July 2011
- Agenda of [REMOVED] Visit in July 2011
- Obituary Notice
- Updated Roster 20110712
- 2011 project budget
- [REMOVED] National Security Seminar
- Current internatinal situation surrounding Syria
- New Update of Health & Medical force
- FW:How to Get Free Airline Tickets
- Nuclear Security and Summit Diplomacy
- Fw: [REMOVED] Defence & Security Industry Mission to [REMOVED] 201
- [REMOVED] heriketlik pilani
- 2012 Global aerospace and defense industry outlook

Email attachment names

- update.exe
- CTF 2011 (MF).xls
- BBC Monitoring reports..xls

- Five Simple Questions for Democrats on Spending Cuts.doc
- Behind the Easing of Israeli-Palestinian Tensions.doc
- Business Exec Urges Broad Trade AgendaTo Curb China Role In Latin America.doc
- PatriotLMSR2009Fin .doc
- New SOPs for HEC Coord with NATO.pdf
- agenda201005.pdf
- Human right report of noth Afica under the war.scr
- Middle_East_Civil_Unrest.pdf
- Protests Spread in Syria.pdf
- Cybersecurity and Cyber War.pdf
- The Meeting intivation of International Atomic Energy Agency 06-05-2011.scr
- meeting invitation of British Council 2011.scr
- Meeting information details of [REMOVED].exe
- Meeting information details of [REMOVED].exe
- Meeting detail information from [REMOVED].scr
- Meeting detail information from [REMOVED].scr
- FY12 Government Opportunities.pdf
- China's Jasmine protests.pdf
- Yemen para for SC briefing.doc
- DECLARATION- COMMENTS.Netherlands.pdf
- weekly_security_report-06-20-2011__-__06-26-2011.pdf
- 2011.xls
- Obituary.xls
- Updated_roster.xls
- 2011 project budget.xls
- Participant_Contacts.xls
- Current international situation surrounding Syria.doc
- Update of Health & Medical force.xls
- How to Get Free Airline Tickets.pdf
- REPLY_ FORM.doc
- Global A&D outlook 2012.pdf
- Global_A&D_outlook_2012.pdf

References

Mandiant Indicators of Compromise

http://intelreport.mandiant.com/Mandiant_APT1_Report_Appendix.zip

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at *www.symantec.com*

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.