Miniduke: Indicators

v1.00 (Feb 27, 2013)

Technical Report

by

Laboratory of Cryptography and System Security (CrySyS Lab)

http://www.crysys.hu/

Budapest University of Technology and Economics

Department of Networked Systems and Services

http://www.bme.hu/

Authors:

CrySyS Malware Intelligence Team. Based on joint work with Kaspersky Labs GREAT Team

Document history

27/02/2013 Initial release

Table of contents

1. Introduction

Our malware analysis team in the CrySyS Lab, Budapest worked together with Kaspersky Labs on the analysis of the Miniduke malware. Our participation in this research was justified by a detected Hungarian incident. A detailed report on the results of our joint efforts has been published by Kaspersky Labs Securelist blog site (see link below). The Kaspersky Labs report describes what we currently know about the operation of Miniduke including its stages, and also information on the C&C infrastructure and communications. In this report, we summarize the indicators of a Miniduke infection, and give specific hints on its detection.

The Kaspersky Labs report is available at

> https://www.securelist.com/en/blog/208194129/The_MiniDuke_Mystery_PDF_0_day_Government_Spy_Assembler_Micro_Backdoor

2. Known malware samples

The available malware samples are highly obfuscated, and compiled by a polymorphic compiler. The attackers were able to produce new variants with only a few minutes difference between compile times. Therefore the number of distinct samples could be very large.

bg_<sthg>.gif and bg_<sthg>.gif_dec refers to pieces of stage 2 of the malware, which are downloaded from the C&C server by the stage 1 code. bg_<sthg>.gif is a gif file that contains encrypted code, bg_<sthg>.gif is the corresponding decrypted file. bg_<sthg>.gif is generally 24484 bytes long, while bg_<sthg>.gif_dec is 22784 bytes long.

```
3e71a9f492101bde28cf9f024d87b496 bg_aefk.gif
a4ad6b55b1bc9e16123de1388f6ef9bf bg_aefk.gif.dec
92a2c993b7a1849f11e8a95defacd2f7 bg_afvd.gif
297ef5bf99b5e4fd413f3755ba6aad79 bg_afvd.gif.dec
06def6c642dcbd58d0291ac110a57274 bg_dafd.gif
2679e112f908fbf4ac96d87f7fdc46ca bg_dafd.gif.dec
afe0190820b3edc296daefe6d1611051 bg_dasfs.gif
e196fa056d1a728d9ba9654fbc482777 bg_dasfs.gif.dec
7049aa581874752093bb98850ff45dac bg_dfdsh.gif
441ee6a307e672c24d334d66cd7b2e1a bg_dfdsh.gif.dec
e975e87bec844c882bf6d60604fc996b bg_dfell.gif
a58e8e935341b6f5cc1369c616de3765 bg_dfell.gif.dec
0a2da3c2c6b94c925459bc5e32bbb03c bg_dfesik.gif
d2f39019bfa05c7e71748d0624be9a94 bg_dfesik.gif.dec
0a5c9055c2b35bee78c911dfc29fe1a4 bg_dfeu.gif
ecd349138a6ef7d7ca40b9ce70dbb575 bg_dfeu.gif.dec
21f16767e53da7fef8a1b5d4159256a9 bg_dfew.gif
935892bb70d954efdc5ee1b0c5f97184 bg_dfew.gif.dec
bba6b0d31553cd8df0c45b85c0495816 bg_dfews.gif
48bbce47e4d2d51811ea99d5a771cd1a bg_dfews.gif.dec
b47b36484cfb0ab38ef481e23275fafb bg_dflj.gif
b68677e04fcc9103560bb0a5e5c7303f bg_dflj.gif.dec
5e757aa35087ca7c479c82d0d5502f51 bg_dfoiu.gif
27212d5e5d40a5e5c1742aac58dc59a8 bg_dfoiu.gif.dec
4193796cffa19e2e5cace58e9f10c599 bg_dfrio.gif
aab06d4ab78336b7315201637d9f1b0e bg_dfrio.gif.dec
474fa3c28d867f7113c060020b3e268b bg_dfwe.gif
05d10323111f02233163a6742556c974 bg_dfwe.gif.dec
f0b327565c25128ad15f9c378bc4ea60 bg_dsaf.gif
d9b68522053396644bcb72448d6cf327 bg_dsaf.gif.dec
af906032917674f1f39a260b2b9fe0fb bg_dsaffe.gif
6507f6b1e2ce05dccf329b8cab078071 bg_dsaffe.gif.dec
633b59e7b97ef4574804ca35669fbf95 bg_dsef.gif
b100d530d67cfbe76394bb0160567382 bg_dsef.gif.dec
203a6ff36ee2cd58daf5680b5a6890ec bg_dsert.gif
2d552b20e8164f3d4250fd8871b11b0f bg_dsert.gif.dec
877a34931b087d04d387633824d9c813 bg_dwed.gif
e990e0d1ee90cd10c4be7bfde6cc3e5a bg_dwed.gif.dec
c8373db89be0a155673e0cd414442fc1 bg_edf.gif
8233c532bfcc4ccf2831765eae084409 bg_edf.gif.dec
```

```
d39f2202b421561cfc36a8802184685c bg_edf_v2.gif
2d87ab160291664d62445548a2164c60 bg_edf_v2.gif.dec
e37d7cc17070df4917f194968073e14b bg_edfsa.gif
fdc96d77af6fdae487002e32d61df123 bg_edfsa.gif.dec
f80af1246744f8eedae152dc44ebfc51 bg_edse.gif
2dcd049c591644e35102921a48799975 bg_edse.gif.dec
7aef3a8776c7a58ef01542ff7d4c83e8 bg_eefds.gif
b540a9f81f538f4f324db422e7bb4559 bg_eefds.gif.dec
ed67c4aca1d25d1083bb8ba65573a4a9 bg_efd.gif
1528567b1a2f1da31d602ce1ddfd8918 bg_efd.gif.dec
bedb8231a7b0d8b13a53e7e1fdff04dd bg_efdse.gif
7056df132f448d45b4781c2ddc27b113 bg_efdse.gif.dec
d469a7d7750c964419c0aaa0347c7a9c bg_efed.gif
d27c2cce5ceb8a62c766a2ae4d50730e bg_efed.gif.dec
5add9bb805c8956931739308369b2c45 bg_efwe.gif
1e0c1f4271c5cadcad7b66bef5863b83 bg_efwe.gif.dec
4c3664dce0b336f4262b5ec1374f9690 bg_ekjf.gif
ab2d8a0d5b03d40f148f2f907b55f9f1 bg_ekjf.gif.dec
113e5ab47e1efae97fd7641276055984 bg_ekks.gif
2f3fd599020fa857d28fe3e2bb26c6ca bg_ekks.gif.dec
55b25ccb549df610c34072556abf88fa bg_elfj.gif
fd85ca2a0da6b7b7c93e1ad0efa25c4c bg_elfj.gif.dec
b248d1b0ee26cb4393efe4ffab0c8c91 bg_elj.gif
1667a3a01b906b1e47328ad601d68d1e bg_elj.gif.dec
f7ed059147802b503f1792694a167e74 bg_esd.gif
c92252487615d5379317febc22dba7d4 bg_esd.gif.dec
34f62a12bc36fd119734a322ef666f14 bg_ewfed.gif
efb1246ee89798a2d9182ad9bbcbb41a bg_ewfed.gif.dec
85388d2adf7b8608f1d3468b4e07920d bg_ewwe.gif
7829cb4ca55fcda8928e0f63ee86c6c2 bg_ewwe.gif.dec
882957f0845d54d83cd0389264d9ba8f bg_fdfe.gif
c519eef57001ad3ae60cdcb0009bf778 bg_fdfe.gif.dec
5935bc0845e6b192c163fc77ee3c00bf bg_fed.gif
381691b297f7f5694709e21ad61ec645 bg_fed.gif.dec
cfb4e25bd9dbf5afef6a56d468de91a1 bg_fefsf.gif
c8d75ed7835fdb543200298216d1d0f4 bg_fefsf.gif.dec
cde0900f94c4c360540735028d6be71c bg_fked.gif
aa48cb8e26ecdf16f22b0585a5fd96bf bg_fked.gif.dec
e498ef07eba70804e90aa303cbd4c20b bg_fwds.gif
798bea2f1e2e6fc8edcedea548877aa2 bg_fwds.gif.dec
78cca6a7d4aed656c9683aeb18732e95 bg_kefs.gif
241363e7641cfa7d9063013ed44bf87b bg_kefs.gif.dec
7f77c4839d09cdf930b021cbdd89410e bg_kei.gif
b8e89f9908262b5385623c0e39d6b940 bg_kei.gif.dec
e2019b16e587ef1d3e05df164a01101c bg_keio.gif
3649fc6e3222721826485131142846b4 bg_keio.gif.dec
4fbe44c36d6c1a2b74733c1cd0d34cbf bg_kje.gif
1051aeace46a4bd33d0167cacd42b12b bg_kje.gif.dec
0e02b78673a9cf2db7a0cc5b00e306e9 bg_kkf.gif
3c188004c98934beaafa7a52ee397f90 bg_kkf.gif.dec
2bd1572913eed832451b768c6c4c610c bg_koe.gif
089b3f42a96f4f74b05e858cdf8db3fc bg_koe.gif.dec
58cf3b1adb7981938848c018d2e52ecb bg_ldfe.gif
014030329695cabdb9966a3006eae07a bg_ldfe.gif.dec
7ae8ac5de85b0777868281f64237197c bg_leo.gif
b8088f6594dd8cba31b4f52a2d91f40e bg_leo.gif.dec
b24f414809671328ced9cec73ff5ca3a bg_lfe.gif
6dca5669aad4933b0629571ce6c99998 bg_lfe.gif.dec
cf1e3f0b0d3a9e009bea821b4bffa387 bg_lkje.gif
```

```
22036375458057994e5fa81474393465 bg_lkje.gif.dec
cffd063dacff1830de63c833e89facc1 bg_lkjkef.gif
168f3d5a88f695c157446549e4770dd9 bg_lkjkef.gif.dec
ffd8ab9d37519ffa15a86157422a6517 bg_oef.gif
8282eb6d6f20c5de6e7f4ae3a42438d2 bg_oef.gif.dec
fed5e99509537e0f46a6e7ab4f9f3587 bg_ojlro.gif
aaa1633a0b8108763334bbcd590848d1 bg_ojlro.gif.dec
5b0f68e23817494f52c84e8e38c6a30d bg_qdf.gif
ffefe16d581340c1e49f585a576a1fd8 bg_qdf.gif.dec
492134baaf2059bdb799c9c7483d1926 bg_qrg.gif
a67ad3e2a020f690d892b727102a759b bg_qrg.gif.dec
b664ce0888cdf5180813be0cfcfcf8ee bg_rie.gif
687a596db9031b38f23064d45c0a4ddb bg_rie.gif.dec
8e4505e28766ab08db27ca91e5ecc839 bg_ruie.gif
04d5e76049db2c1e799e70231107339a bg_ruie.gif.dec
00457691525bf21484827bcd8a01828b bg_sasd.gif
e1a659473ae1e828508309b77da13783 bg_sasd.gif.dec
1a1afc3d26c82c4b0facf5ca8a5dcb36 bg_sdef.gif
f648bd9d68bd016739988bb71bf5486b bg_sdef.gif.dec
42ccad0b47cb1836e7e09869b41ebdb2 bg_sdefk.gif
8ee3cf5e37480ee1324146feef30de02 bg_sdefk.gif.dec
796f0698644f61fdcd7da04bf590544e bg_sfef.gif
2ab25d33d61cf4cfbac92c26c7c0598e bg_sfef.gif.dec
0b02262772b8c2c5e54dae99bdb07029 bg_ureio.gif
728f9c1d9dd0635a4b205f2d4d68a887 bg_ureio.gif.dec
95694878bba2e099ea9ca1b5deeedb7a bg_wdf.gif
f19345e0e5aecc0da45b4c110591bdd9 bg_wdf.gif.dec
```

Figure 1 – MD5 checksum list of pieces of stage 2 of the known versions

```
8d7e8b7871b634ad67b13e55aebb7fb7a954ff90 bg_aefk.gif
1e6b9414fce4277207aab2aa12e4f0842a23f9c1 bg_aefk.gif.dec
ed64fba3195f52192c65cad491a28bf18f6f67a3 bg_afvd.gif
28a43eac3be1b96c68a1e7463ae91367434a2ac4 bg_afvd.gif.dec
cc492d4b188f4cf5003f8b6954f6dd071a8066c2 bg_dafd.gif
97a374bac7572d44ca8c73c49d3d6ddeade90e34 bg_dafd.gif.dec
81612fc09cfae280cc35b1331c832a5a87c2edff bg_dasfs.gif
b32b675699a59b4272a956dbd81738d02d4ca8a4 bg_dasfs.gif.dec
352a2cf4bb2c9e300ce9a51740f238c9282ca6e4 bg_dfdsh.gif
2ceae0f5f3efe366ebded0a413e5ea264fbf2a33 bg_dfdsh.gif.dec
05c539ca5dfbfab8e61ffab4b7b13ba2a5e7154c bg_dfell.gif
ad9734b05973a0a0f1d34a32cd1936e66898c034 bg_dfell.gif.dec
f3c6c0c73dcccbf44521763985bbf1ad6e3317eb bg_dfesik.gif
a9e529c7b04a99019dd31c3c0d7f576e1bbd0970 bg_dfesik.gif.dec
5e33dd2fcf0c32d3fc458b2d99a0033461c3a6ea bg_dfeu.gif
69d95479d520e016ce733541ec815aafe16ead04 bg_dfeu.gif.dec
b995e16fc3a981d693778e370e5ba19861412db6 bg_dfew.gif
efcb9be7bf162980187237bcb50f4da2d55430c2 bg_dfew.gif.dec
39952ab95453de127a6a61f4e67c3109ca8ff93e bg_dfews.gif
1ba5bcd62abcbff517a4adb2609f721dd7f609df bg_dfews.gif.dec
a9e9cd4b2b1ec4efcdbce79b582f874cebe3ebd1 bg_dflj.gif
a6c18fcbe6b25c370e1305d523b5de662172875b bg_dflj.gif.dec
5cb2d1005caccbe451f2bd2c6314283ba04a7401 bg_dfoiu.gif
d99ddb6c4fc13f97c6a77f84ba31533ca2e1d9e0 bg_dfoiu.gif.dec
d4c10e9248392936cf94a168a792d4b9942398a8 bg_dfrio.gif
832d80c16886a7529aa22c962a00a7bb3fe1ff77 bg_dfrio.gif.dec
78e20444a96f4405aae2a26e1a013634c81d7328 bg_dfwe.gif
```

```
4ec769c15a9e318d41fd4a1997ec13c029976fc2 bg_dfwe.gif.dec
1f07d80b16a539cc6d7fccd2bb37ddaaf734352e bg_dsaf.gif
f762ff3801d1e4ad1360d50e54f2894211cd8958 bg_dsaf.gif.dec
be9aa1776fbd5b05fea230ff77654e8a9d29a802 bg_dsaffe.gif
8da1aca62c3a19ac0f9b85fb48b711e6b946bc77 bg_dsaffe.gif.dec
b524a190d74a1b8824a049936e17aee714f5bd23 bg_dsef.gif
43fa0d5a30b4cd72bb7e156c00c1611bb4f4bd0a bg_dsef.gif.dec
4213387b4e4cf0bb2499b06b4fecd90af7d7257a bg_dsert.gif
92465134302755552eb82bb39bb3327a08112e02 bg_dsert.gif.dec
0e924796517cbb62f3a30740eb60ac1a9829b24d bg_dwed.gif
53140342b8fe2dd7661fce0d0e88d909f55099db bg_dwed.gif.dec
f8c6f1cc3b937e0d7501c098776945bdc7c83856 bg_edf.gif
582dbde44753e0af4996ddb63ab088221b2e49a2 bg_edf.gif.dec
109e1e387f8b2bb8d92f45e79881809384e9ae54 bg_edf_v2.gif
c39d0b12bb1c25cf46a5ae6b197a59f8ea90caa0 bg_edf_v2.gif.dec
6b1dd4fa0f9570760c02bbcf44acf74d752aa8f8 bg_edfsa.gif
5551408323086f31d9bc3358ab5b2ed4dde86c5d bg_edfsa.gif.dec
d3a1b7d35b314139ab87bf4cd3e7ce752b37e56a bg_edse.gif
30b377e7dc2418607d8cf5d01ae1f925eab2f037 bg_edse.gif.dec
280aadae40cb340894f17ce1ca00f7dda3eb4425 bg_eefds.gif
6b56ff806ee0b094b4846f494257e84b62bee35f bg_eefds.gif.dec
00da3d559f36e842d2411b8c47ee377650722da0 bg_efd.gif
a32817e9ff07bc69974221d9b7a9b980fa80b677 bg_efd.gif.dec
0e5a4768d7020b336f58ea4d521756401c24efd4 bg_efdse.gif
939ac22e8425654a57753bd4083e8cd16d337ee0 bg_efdse.gif.dec
f7932b0a5b710d4e7e698d3c990a875771698fce bg_efed.gif
c9cedca208049c7bf08cba544ef32bb7a3ebe37a bg_efed.gif.dec
25a7c6b0f48e68f4ca135ecec46d3ad190d518d9 bg_efwe.gif
9689ebbeeb544b9d1c00b71f3b886aeebcb92138 bg_efwe.gif.dec
95ad87fd28d7367fd5323d5281c044238dd4c303 bg_ekjf.gif
36b969c1b3c46953077e4aabb75be8cc6aa6a327 bg_ekjf.gif.dec
b9d576a47cfebb2c3ff0ecc8cd7c352e6ce32b23 bg_ekks.gif
366b41bcac6259c77ed5792becae75670a74c4c1 bg_ekks.gif.dec
8e3e6ea2c79c9994ded4922358898814efd2cbe0 bg_elfj.gif
367030d5cf3ce7e9ef7770367f04c7dd88332374 bg_elfj.gif.dec
95d8b5e4bff4c35a7ef32f1cbb7e385a331c6138 bg_elj.gif
b42ab1b2b257f65ad18823ecb2f284c8fc118c26 bg_elj.gif.dec
b72df8e1f24c4e05699fc892cfd536053d762065 bg_esd.gif
73366c1eb26b92886531586728be4975d56f7ca5 bg_esd.gif.dec
554cd374591ee8bf0f062567c17beae54f9055ff bg_ewfed.gif
6956a776f3395d1aee8a3c27e9db5eb2d38db32b bg_ewfed.gif.dec
40f8ee78fb9969c8ec9a795cb827dfb427c19036 bg_ewwe.gif
1ddcd6b1475f016d04d8a43ccb03abeb83371eda bg_ewwe.gif.dec
0cd54a0c3f7fdaf7a83e6a1ff818daf514e81e7a bg_fdfe.gif
5acaea49540635670036dc626503431b5a783b56 bg_fdfe.gif.dec
fef95bdb9f984bcbb89f3a29928263dfc01aef72 bg_fed.gif
f62600984c5086f2da3d70bc1f5042cf464f928d bg_fed.gif.dec
1747a7a74a6fac25bc4315b8d3a8311ce8a082e2 bg_fefsf.gif
501452d2c21bb8248e068932920554db6204a7f2 bg_fefsf.gif.dec
4bba1d30c971fdd23131e8ec1d768066b400f0a1 bg_fked.gif
49889f3db0d70b716aa3cb2ab571f0b4a56a6f99 bg_fked.gif.dec
551bf2d2268dba5d22e91fdd7ca9832bc8874bcc bg_fwds.gif
824d383bb5093e3a6c232afca3293779a297c0ad bg_fwds.gif.dec
95760332c76b32919d4c053b3360ecad4811256a bg_kefs.gif
f484d874097ca95e5a86f43a15ef184bec1e972a bg_kefs.gif.dec
b1dec7f17381cf41699184ec4bc591ff20b451b3 bg_kei.gif
296fd4c5b4bf8ea288f45b4801512d7dec7c497b bg_kei.gif.dec
e6429ea40864e36dd6a25cab00b416ff207825a7 bg_keio.gif
df64ac1bb4ca177539e3fa669dcc471d3093ff2f bg_keio.gif.dec
```

```
c20ba675d5df997623c7da4c79ca9be5c995eb3c bg_kje.gif
4a88e007bbd9a729fde016de1c9709cd06818ef7 bg_kje.gif.dec
ff2319abaeded930feb0ddbcb47fdfc2d57e182c bg_kkf.gif
a4445f1ae3e2d5196eb4292121e6cf0d1cc5dad2 bg_kkf.gif.dec
7419bfc9d393b2a9fbd09c18ea4a31ce98d60342 bg_koe.gif
7e57c80574fdebf5f3fedce5a2ebb62d49de1345 bg_koe.gif.dec
5316a02c1e120885a2382e95a3eb0c1f8fd69551 bg_ldfe.gif
60efd28c07d07d10d50b5ad00c243e17e7f1707e bg_ldfe.gif.dec
862305dedb93100aee6ef07c858c3a0b6878620e bg_leo.gif
634a1649995309b9c7d163af627f7e39f42d5968 bg_leo.gif.dec
997d5765e4cc7475fa2cf64233af9b51ddf219f2 bg_lfe.gif
81c99d19ea8065cfff6dc76a950b9d1b25a5f7a9 bg_lfe.gif.dec
c6fd105437e9ddd914721f3ba7fcbc6bef39067a bg_lkje.gif
6f530edc584a18df98ee7fade2dd03b610955e23 bg_lkje.gif.dec
8802cbff6f2b39932e9b699d89a6f3a407cd39a7 bg_lkjkef.gif
c0c26060b4f003322f3cda9dee294fd6221b85da bg_lkjkef.gif.dec
1160010b1df2601fe176353be76ba1a922425dc6 bg_oef.gif
edf74413a6e2763147184b5e1b8732537a854365 bg_oef.gif.dec
49989446d542b1face2c031a205a702178dc2496 bg_ojlro.gif
ebe78cc14bb8e13374da4264c41df24dc0ceeaa7 bg_ojlro.gif.dec
071b67b2645e574f6fc5ba889c041bb2ee85f6d8 bg_qdf.gif
31ab6830f4e39c2c520ae55d4c4bffe0b347c947 bg_qdf.gif.dec
53d1c812510c51d0b6eec767d15f740ea54135b5 bg_qrg.gif
223c7eb7b9dde08ee028bba6552409ee144db54a bg_qrg.gif.dec
be1a53afaab89f47a91a21b0d65415af1b5d1bff bg_rie.gif
3171957cfeb7b415f21b04f9a587b0c339b5c0e3 bg_rie.gif.dec
898a3e5e34eeb3349aa6f291c31195dc02bb9530 bg_ruie.gif
f0f7d755add2305bceaacfe6840d61ccd5f03b0f bg_ruie.gif.dec
0b1e28ecd5b4eb14519470775dce965c63579640 bg_sasd.gif
683104d28bd5c52c53d2e6c710a7bd19676c28b8 bg_sasd.gif.dec
ba884173e98a4f2b6af6acc7f702ead14b146960 bg_sdef.gif
f30ba7eeebd97843f0bcf9c3930741fa29c132cd bg_sdef.gif.dec
6c889228219012b25387bf3e063136b994d2dcac bg_sdefk.gif
e804f3bf72bfda867fd3725a82da6212e29dbfc4 bg_sdefk.gif.dec
07e26464e17a750bb60665c377b41efd23c440b6 bg_sfef.gif
827de388e0feabd92fe7bd433138aa35142bd01a bg_sfef.gif.dec
28ec7eb49f7af3ca7787e4566b144d8ea544a78d bg_ureio.gif
08a4baa154dc41d7dee9bd424c2679253c743ee3 bg_ureio.gif.dec
84fa36acb51a0569ed931f1db5d44ec907dcb624 bg_wdf.gif
d81b0705d26390eb82188c03644786dd6f1a2a9e bg_wdf.gif.dec
```

Figure 2 – SHA1 checksum list of pieces of stage 2 of the known samples

<id>.gif files are pieces of stage 3 codes prepared for specific victims with <id> used as an ID. These are typically 334093 byte long files with a 13-byte long gif header. Below, we list the hashes of these files; in case of the decrypted files with .gif_dec extension, we list the hashes for the internal decrypted PE file.

```
07a9975d7d96ff3b56de024ab2017582 *1109821546.gif
43cd449e3b0c1ecde8136eeb710de233 *174239657.gif
85a645c42e2fcf718c211ebc6cbc71b8 *2334309658.gif
a9315dc0ff95809839af3b95e7de329d *2618653991.gif
92ff4df1d079a003ae2a8ac47dd5e81b *2627081433.gif
bf0253ee830b498bd442c3b97aec1270 *3100425864.gif
c48d0822eedd75c9c56f688fb8a05259 *3198217296.gif
44ee71de720fc1a50c919bc5a01c592d *3946889701.gif
626489f8cafacb1b24fe6ecf0db52f23 *3979106736.gif
```

```
03f8485cacb0458194d2bbef9f33cc06 *626088424.gif
738c60fff066934b6f33e368cfe9a88c *1109821546.gif_dec
cf59ed2b5473281cc2e083eba3f4b662 *174239657.gif_dec
b8d1d74a0ad4985adaf9afe4c868ae0b *2334309658.gif_dec
c79a35313238e71a17d19de979a0d63a *2618653991.gif_dec
18e64b8e5ce5bdd33ce8bd9e00af672c *2627081433.gif_dec
86ef8f5f62ae8590d6edf45e04806515 *3100425864.gif_dec
4c6608203e751cf27f627220269d6835 *3198217296.gif_dec
78e51be60eab2c6e952c9538a46ab521 *3946889701.gif_dec
b798c968cbfd53f878e13c7698610d9c *3979106736.gif_dec
f5f84c0c7ae871c2aa3cfe25199da628 *626088424.gif_dec
738c60fff066934b6f33e368cfe9a88c *1109821546.gif_dec
07a9975d7d96ff3b56de024ab2017582 *1109821546.gif
f78454d4ac3e4fe9ef5cac69b1ec43d7 *4137794344.gif
811f66d6dd2c713073c0b0aebbe74ce8 *4137794344.gif_dec
```

Figure 3 – MD5 checksums of pieces of stage 3 code

```
31a31f6be9c31cb2d02c04176eb500f1aba14dd0 *174239657.gif
804701959a1dbfbbfc6d8142de850db9fce9a611 *1109821546.gif
ac4642885ca779e7b66b8bb6aa21d3c0396f7a1d *2334309658.gif
d8c6d3e6988516595399003d1db0abd7df334d87 *2618653991.gif
6cf8ca847ee317255a9084bb44ae3f38ef61e5c3 *2627081433.gif
0fc29adc3aca39f32763096e090a6a69e50a716f *3100425864.gif
1df9b4dc693ce7250f51cbc7ced53ad0a6e1c587 *3198217296.gif
9d716d2f8f1c2841a2707eba2ebadd01ed830030 *3946889701.gif
497f9c688ed142ae91e354b3d9c9e13243a268b0 *3979106736.gif
b464fc5cab7a93e5607b2abb49f343e81f4fa2f1 *626088424.gif
15c75472f160f082f6905d57a98de94c026e2c56 *1109821546.gif_dec
00852745cb40730dc333124549a768b471dff4bc *174239657.gif_dec
8cce571ca74e4b0074c09acb814541a0192ea9a8 *2334309658.gif_dec
781d0b12bbe0a862d4a5527cd85489551cfe5d31 *2618653991.gif_dec
e4add0b118113b2627143c7ef1d5b1327de395f1 *2627081433.gif_dec
493d0660c9cf738be08209bfd56351d4cf075877 *3100425864.gif_dec
118114446847ead7a2fe87ecb4943fdbdd2bbd1e *3198217296.gif_dec
0e263d80c46d5a538115f71e077a6175168abc5c *3946889701.gif_dec
d22d80da6f042c4da3392a69c713ee4d64be8bc8 *3979106736.gif_dec
71d059edb81acb6b65213386bda3e2bdc724fa0f *626088424.gif_dec
15c75472f160f082f6905d57a98de94c026e2c56 *1109821546.gif_dec
804701959a1dbfbbfc6d8142de850db9fce9a611 *1109821546.gif
e17d004cd57f5f5eaa3652c926793d57ef88f1ec *4137794344.gif
416d1035168b99cc8ba7227d4c7c3c6bc1ce169a *4137794344.gif_dec
```

Figure 4 – SHA1 checksums of pieces of stage 3 code

```
3668b018b4bb080d1875aee346e3650a action_plan.pdf (Country: Belgium)
88292d7181514fda5390292d73da28d4 ASEM_seminar.pdf (Country: Hungary)
3f301758aa3d5d123a9ddbad1890853b EUAG_report.pdf (Country: Luxembourg)
0cdf55626e56ffbf1b198beb4f6ed559 report.pdf (Country: Spain)
cf5a5239ada9b43592757c0d7bf66169 EUAG_report.pdf (Country: Belgium)
c03bcb0cde62b3f45b4d772ab635e2b0 The 2013 Armenian Economic Association.pdf
(Country: Belgium)
```

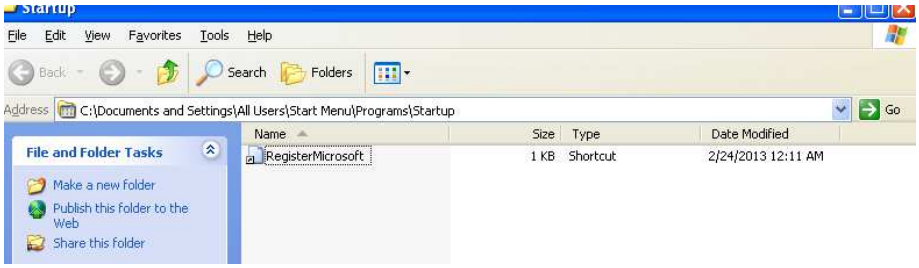
Figure 5 – MD5 checksums for known malicious documents (droppers)

3. Detection of the running malware

Due to a large number of compiled samples, there is a high chance that the current version is difficult to detect by signatures. Yet, there are common features in the samples that can be used to identify the malware components.

In every sample we checked, the “Program Files/Startup” contains a file with “.lnk” extension after installation. This is used to start up the malware after the computer is rebooted.

An example of the lnk file created by the malware:



The contents of the .lnk files are similar to the below described path and file, but random names are used. The extension of the dll called is generally “.tmp” or “.cat” or “.db” (not sure about full list) and the export function called has a random name.

"C:\WINDOWS\system32\rundll32.exe"
C:\DOCUME~1\ALLUSE~1\APPLIC~1\base.cat,JorNgoq

The running process of the malware can be pinpointed, e.g., by using ProcessExplorer. The running copies of stage 1 and 2 appear as separated rundll.exe processes. It is very useful to create a memory dump from these running processes, e.g., by using SysInternals ProcessExplorer.

On the picture below, the export function name they use is GqOlls. The names seem to follow a pattern: 6 chars long with two upper case letters.

A not fully cross-checked information is that during installation the malware will be copied in two copies to the system and the two executables differ. This might mean that the executable modifies itself.

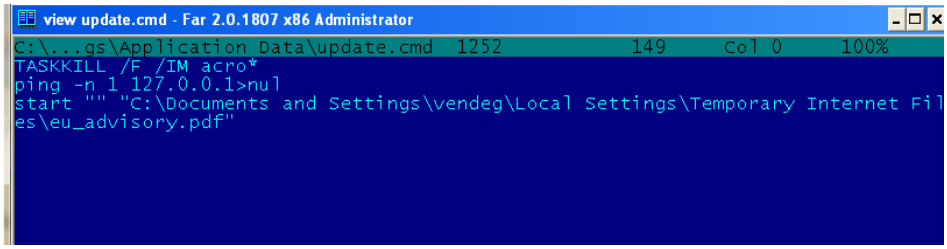
For example, we recovered the following two files:

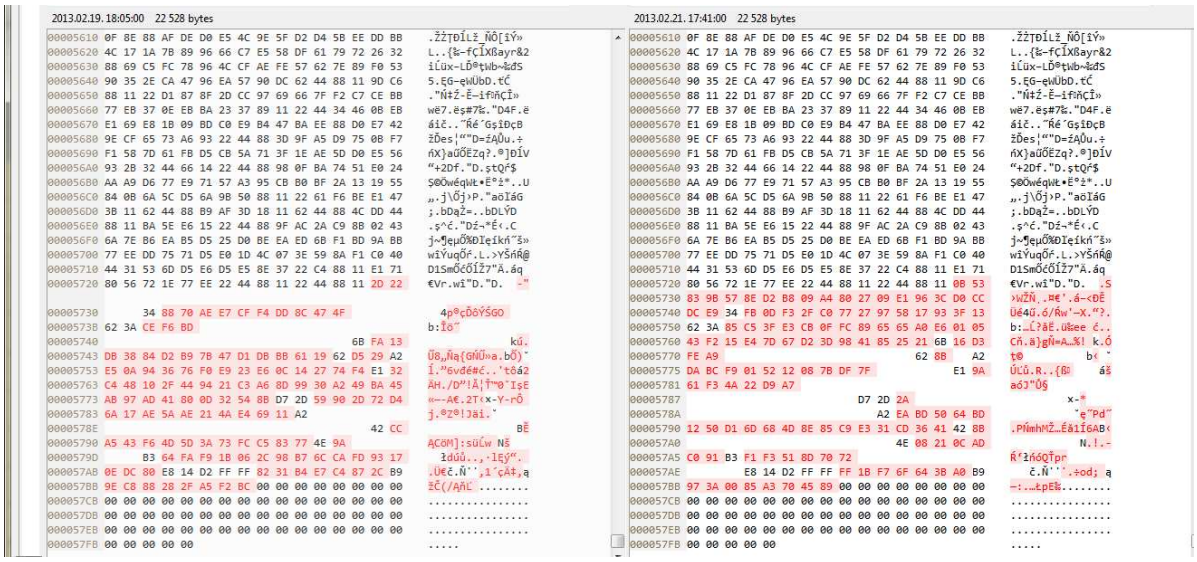
md5sum base.cat :113e6fc85317fdd135e3f5f19e6c7a58 *base.cat

md5sum ~6rld.tmp : c786a4cdfe08dbe7c64972a14669c4d1 *~6rld.tmp

where base.cat is the startup file, which is created based on ~6lrd.tmp. base.cat is stored in the “All users” directory, whereas ~6lrd.tmp is stored in a user’s directory, e.g., in the guest user directory as “C:\Documents and Settings\guest\Local Settings\Application Data\~6rld.tmp”

This user directory contains at least one more file, update.cmd with a specific content that could be used for detection. E.g., a search for any *.cmd files with content “TASKKILL /f /IM acro*” might be a a detection tool of this stage.





As for stage 3 of the attack, it is important to note that it is not yet analyzed deeply. So once a victim downloads the ~300k long piece of code, we don't know what happens with the previous stages, and we have no information about detections once this stage is reached, except the usage of the C&C server news.grouptumbler.com.

4. C&C communication

There are multiple layers of C&C communications in the malware. First the malware uses Google search to receive information from its master. Then, it uses the Twitter messaging service looking for the twits of a specific Twitter user. Commands received via this channel trigger the download of stage 2 and stage 3 code from the C&C server.

We identified the following C&C servers delivering stage 2 and stage 3 codes:

Attack location	C&C server	C&C IP / location	path on C&C
Hungary	arabooks.ch	194.38.160.153 / Switzerland	/lib/index.php /srch/index.php /forumengine/index.php /events/index.php /groups/[different]
Luxembourg	artas.org	95.128.72.24 / France	/engine/index.php /web/index.php
Belgium	tsoftonline.com	72.34.47.186 / United States	/views/index.php
(Multiple)	www.eamtm.com	188.40.99.143 / Germany	/piwik/web/index.php

The C&C server used by stage 3 of the malware is news.grouptumbler.com and it is located in Panama. At the time of this writing, port 80 seems to be closed on this server. Address and open port information is below:

```
news.grouptumbler.com/news/feed.php
IP: 200.63.46.23

Interesting ports on 200.63.46.23:
Not shown: 65524 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
111/tcp   open     rpcbind
920/tcp   open     unknown
1437/tcp  open     tabula
46436/tcp open     unknown
```

Figure 6 – Stage 3 C&C server information

4.1. Detection of C&C communications

Basic detection can be based on 3 queries that are initiated by the victim computers within seconds.

```
www.google.com – port TCP/80 - HTTP
twitter.com –port TCP/443 - SSL
www.geoiptool.com –port TCP/80 - HTTP
```

Figure 7 – Initial web page – and possibly DNS queries issued by the malware

Known search strings in Google search (see below) can also be used to detect the malware. Unfortunately, these strings are most likely unique to each C&C server or victim, thus unknown samples might use other strings, but possibly with the same length.

```
lUFEfiHKljfLKWPR
HkyeiIDKiroLaKYr
lUFEfiHKDroLaKYr
```

Figure 8 – Google search strings used by the malware

The malware also sends a query to the geoiptool. An example is shown below:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 6.0; en-US; Trident/5.0)
Host: www.geoiptool.com
```

Figure 9 – Geoip lookup query sample – Agent string might be different for each query!

4.2. Initial C&C communication

Initial communications with the stage 2/3 delivery C&C servers (such as arabooks.ch) can be used to develop detection signatures as follows:

The malware retrieves the URL using a Twitter query as described earlier. Then, we can observe the first query from the victim towards the stage 2/3 delivery C&C server. This query contains pure HTTP traffic on port 80 to the server following the template below.

GET /original/path/shortname/index.php?e=aaaaaaaaa

where:

- shortname can be a number of strings, generally human readable (e.g. lib, engine, forum, forumengine etc.)
- "e=" is not constant, can be anything, but generally 1-2 letters long
- aaaaaaaaa stands for some Base64-like text (see details below)
- the servers used are assumed to be legitimate sites, just hacked by the attackers.

Based on this format, we can detect a valid query as follows:

- The name of the 1st GET parameter should be discarded
- this means "e=" is not important
- we saw only one GET parameter, queries with multiple parameters are likely not used

For detection, the Base64-like string "aaa…" should be first modified as follows:

- "-" should be replaced by "+"
- "_" should be replaced by "/"

This results in correct Base64 encoding, which can be decoded with library functions such as base64_decode. After decoding, a string of data, partially binary will be available. Parts are separated by the delimiter character "|". The format and a numerical example are below:

<binary data (~100 bytes)>|<numerical ID (~10 digits)>|<version number>

e.g.,

<binary data>|5551115551|1.13

As the binary data itself may contain the ”|” character, parsing should start from the end (i.e., the numerical ID starts from the second “|” character from the end). In additional, the ID length may vary (not fully confirmed), but it seems to be around 10 digits. Finally, the version number always follows the pattern <1digit><dot><two digits>, e.g., 1.1X 3.1X.

The correct decoding of the HTTP query information should be enough to quickly develop possible IDS-based detections. As we have seen, detection is complicated, but not impossible. The following is the summary of potential detection steps:

- Check if there is only one GET parameter
- (check if path is not empty and contains index.php)(possible, but not confirmed)
- convert the Base64-like GET parameter string into real Base64 encoding, and check if it decodes correctly
- check if the decoded string has at least two delimieter character "|" in it
- check if after the last but first "|" character, there are digits only
- check if the version part of the string follows the format "1.11" or similar

The header sent is fairly standard, but we include one example nonetheless:

```
0x00d0:  2e31 0d0a 4163 6365 7074 3a20 2a2f 2a0d  .1..Accept:.*/*.
0x00e0:  0a41 6363 6570 742d 456e 636f 6469 6e67  .Accept-Encoding
0x00f0:  3a20 677a 6970 2c20 6465 666c 6174 650d  :.gzip,.deflate.
0x0100:  0a55 7365 722d 4167 656e 743a 204d 6f7a  .User-Agent:.Moz
0x0110:  696c 6c61 2f34 2e30 2028 636f 6d70 6174  illa/4.0.(compat
0x0120:  6962 6c65 3b20 4d53 4945 2037 2e30 3b20  ible;.MSIE.7.0;.
0x0130:  5769 6e64 6f77 7320 4e54 2035 2e31 3b20  Windows.NT.5.1;.
0x0140:  5472 6964 656e 742f 342e 303b 2049 6e66  Trident/4.0;.Inf
0x0150:  6f50 6174 682e 3129 0d0a 486f 7374 3a20  oPath.1)..Host:.
0x0160:  XXXX XXXX XXXX XXXX XXXX XX0d 0a43 6f6e  XXXXXXXXXXX..Con
0x0170:  6e65 6374 696f 6e3a 204b 6565 702d 416c  nection:.Keep-Al
0x0180:  6976 650d 0a0d 0a                        ive....
```

Figure 10 – Other HTTP header values in a C&C query

The used Agent strings vary significantly across queries, therefore they cannot be really used for detection:

```
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+InfoPath.2)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+Trident/4.0;+.NET+CLR+1.1.4322;+
.NET+CLR+2.0.50727;+.NET+CLR+3.0.4506.2152;+.NET+CLR+3.5.30729;+InfoPath.2)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+Trident/4.0;+.NET+CLR+2.0.50727;
+.NET+CLR+3.0.4506.2152;+.NET+CLR+3.5.30729;+InfoPath.2)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+Trident/4.0;+.NET4.0C;+.NET+CLR+
1.1.4322;+.NET+CLR+2.0.50727;+.NET+CLR+3.0.4506.2152;+.NET+CLR+3.5.30729;+.NET4.0E;
+InfoPath.3)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+Trident/4.0;+GTB7.4;+InfoPath.1;
+.NET+CLR+3.0.4506.2152;+.NET+CLR+3.5.30729;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322;+
.NET4.0E;+.NET4.0C;+.NET+CLR+2.0.50727)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+Trident/4.0;+InfoPath.2)
```

```
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/4.0;+GTB7.4;+SLCC2;+.NET
+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+InfoPa
th.3;+.NET4.0C;+.NET4.0E)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/5.0;+SLCC2;+.NET+CLR+2.0
.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/5.0;+SLCC2;+.NET+CLR+2.0
.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+InfoPath.3;+Media+Center+PC+6.0;+.N
ET4.0C;+.NET4.0E)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/5.0;+SLCC2;+.NET+CLR+2.0
.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+.NET4.0C;+.NET
4.0E)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/5.0;+SLCC2;+.NET+CLR+2.0
.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+.NET4.0C;+Info
Path.2;+.NET4.0E)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/5.0;+SLCC2;+.NET+CLR+2.0
.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+CMDTDF;+.NET4.
0C;+InfoPath.3)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/5.0;+SLCC2;+.NET+CLR+2.0
.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+InfoPath.2)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/5.0;+SLCC2;+.NET+
CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+.NET4.0
C;+.NET4.0E)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/5.0;+SLCC2;+.NET+
CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+.NET4.0
C;+.NET4.0E;+BRI/2;+InfoPath.3)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/5.0;+SLCC2;+.NET+
CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+.NET4.0
C;+.NET4.0E;+InfoPath.2)
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+WOW64;+Trident/5.0;+SLCC2;+.NET+
CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+Media+Center+PC+6.0;+.NET4.0
C;+.NET4.0E;+InfoPath.3)
Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Trident/4.0;+.NET+CLR+2.0.50727;
+.NET+CLR+3.0.04506.648;+.NET+CLR+3.5.21022;+.NET+CLR+3.0.4506.2152;+.NET+CLR+3.5.3
0729;+InfoPath.2)
Mozilla/5.0+(Windows+NT+5.1;+rv:19.0)+Gecko/20100101+Firefox/19.0
Mozilla/5.0+(Windows+NT+6.1;+rv:10.0)+Gecko/20100101+Firefox/10.
```

Figure 11 – Agent strings used in C&C comms – might be partial or wrong – not useful for detection

4.3. Other indicators of C&C communication: Google and Twitter queries

The Google search step also uses different agent strings:

```
„GET /search/?q=lUFEfiHKDroLaKYr HTTP/1.1" 304 211 "-" "Opera/7.0 (compatible; MSIE
7.0; Windows NT 6.0; en-US; WOW64)"
„GET /search?q=lUFEfiHKDroLaKYr HTTP/1.1" 301 588 "-" "Opera/5.0 (Windows; U;
Windows NT 5.2; en-US; Trident/4.0)"
„GET /search?q=lUFEfiHKDroLaKYr HTTP/1.1" 301 588 "-" "Opera/4.0 (Windows NT 5.1;
en-GB; Trident/4.0)"
```

Figure 12 – Some Google search agent strings

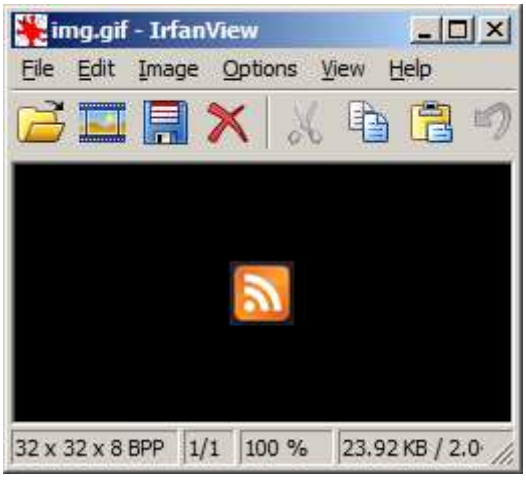
```
"GET /EdithAlbert11 HTTP/1.1" 404 1229 "-" "Mozilla/6.0 (X11; Linux x86_64; en-GB;
Trident/5.0)"
 "GET /ifsWcj9a HTTP/1.1" 404 529 "-" "Mozilla/5.0 (compatible; MSIE 6.0; Windows
NT 5.0; en-GB; WOW64; Trident/5.0)"
 "GET /EdithAlbert11 HTTP/1.1" 404 644 "-" "Mozilla/5.0 (Windows NT 5.1; en-GB;
Trident/4.0)"
 "GET /ifsWcj9a HTTP/1.1" 404 529 "-" "Mozilla/5.0 (compatible; MSIE 6.0; Windows
NT 5.0; en; WOW64; Trident/5.0)"
 "GET /EdithAlbert11 HTTP/1.1" 404 1229 "-" "Mozilla/7.0 (compatible; MSIE 7.0;
Windows NT 6.0; en-GB; WOW64)"
] "GET /ifsWcj9a HTTP/1.1" 404 510 "-" "Opera/5.0 (compatible; MSIE 9.0; Windows NT
6.1; en-GB; SV1)"
```

Figure 13 – Twitter search samples – 443/SSL

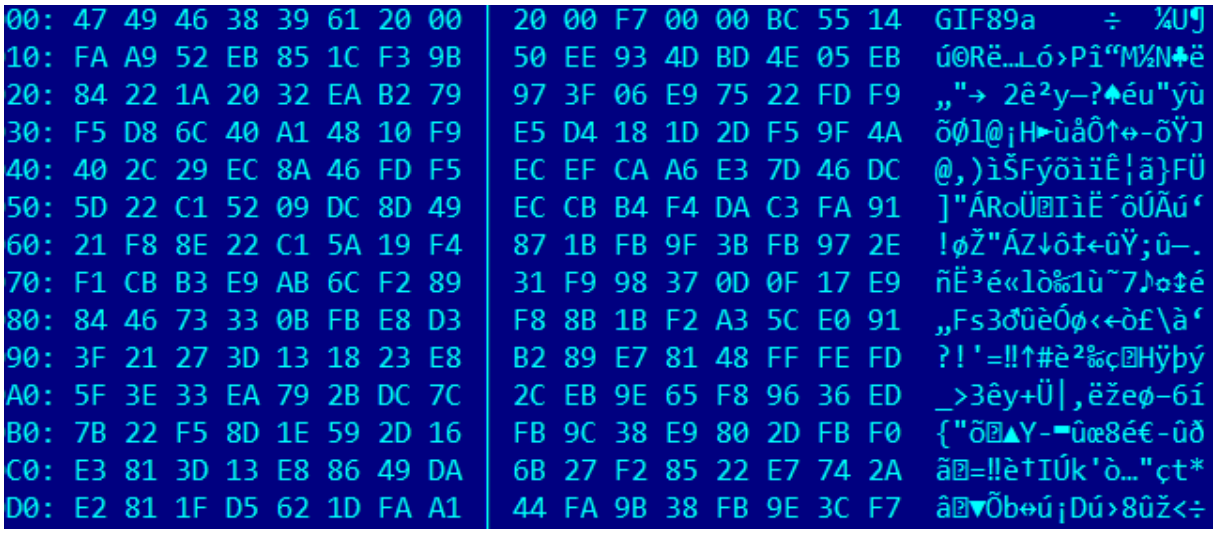
The C&C server's response – if it sends encrypted files – is a GIF file containing a small icon, and after that, the malware:

```
0x0020:  XXXX XXXX XXXX XXXX 4749 4638 3961 2000  XXXXXXXXGIF89a..
0x0030:  2000 f700 00bc 5514 faa9 52eb 851c f39b  ......U...R.....
0x0040:  50ee 934d bd4e 05eb 8422 1a20 32ea b279  P..M.N..."..2..y
0x0050:  973f 06e9 7522 fdf9 f5d8 6c40 a148 10f9  .?..u"....l@.H..
0x0060:  e5d4 181d 2df5 9f4a 402c 29ec 8a46 fdf5  ....-..J@,)..F..
0x0070:  ecef caa6 e37d 46dc 5d22 c152 09dc 8d49  .....}F.]".R...I
0x0080:  eccb b4f4 dac3 fa91 21f8 8e22 c15a 19f4  ........!.."Z..
0x0090:  871b fb9f 3bfb 972e f1cb b3e9 ab6c f289  ....;........l..
0x00a0:  31f9 9837 0d0f 17e9 8446 7333 0bfb e8d3  1..7.....Fs3....
```

Figure 14 – GIF File header sent back by the C&C server



For stage 3 (i.e., <id>.gif files), the file downloaded has a larger size (~300KB). It also begins with a GIF header, but that header is only 13 bytes long, and then starts the encrypted executable, as shown below:

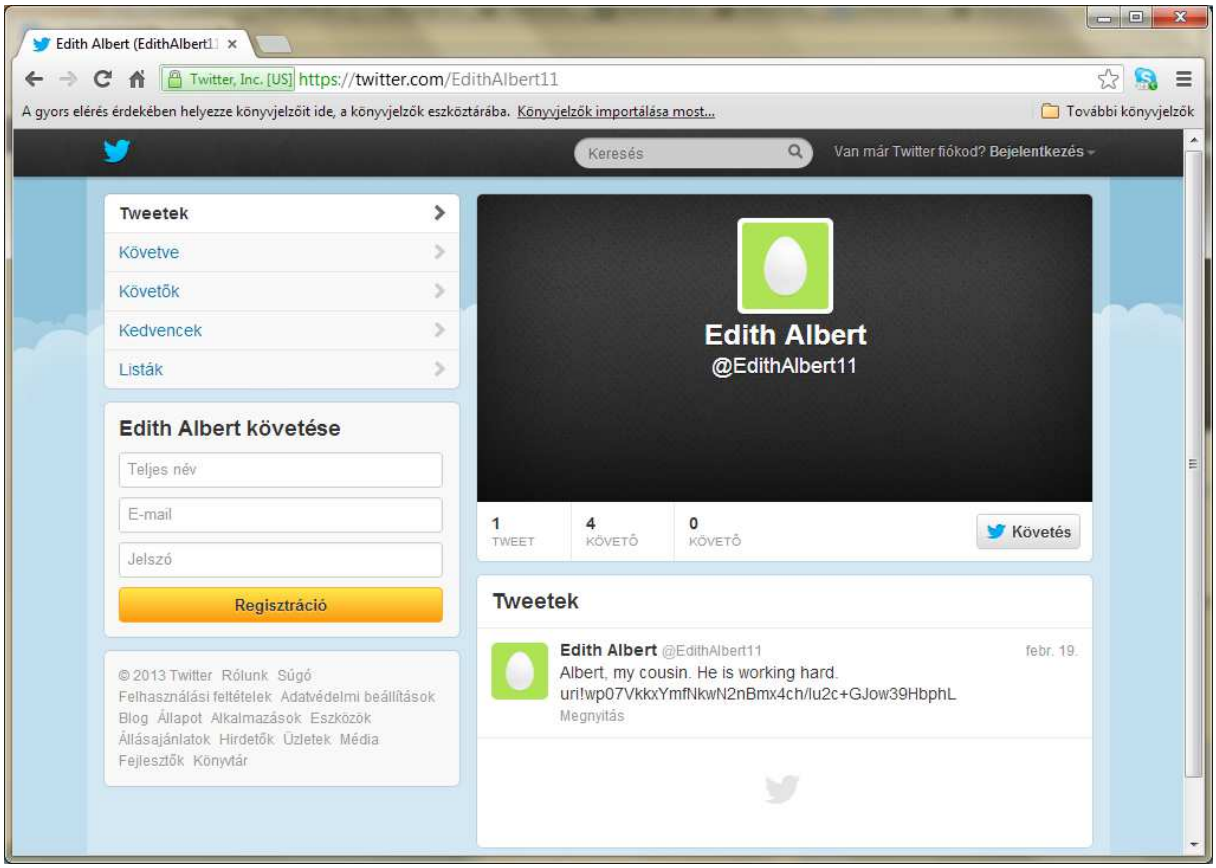


Examples for twits containing the URL of the C&C server are shown below:

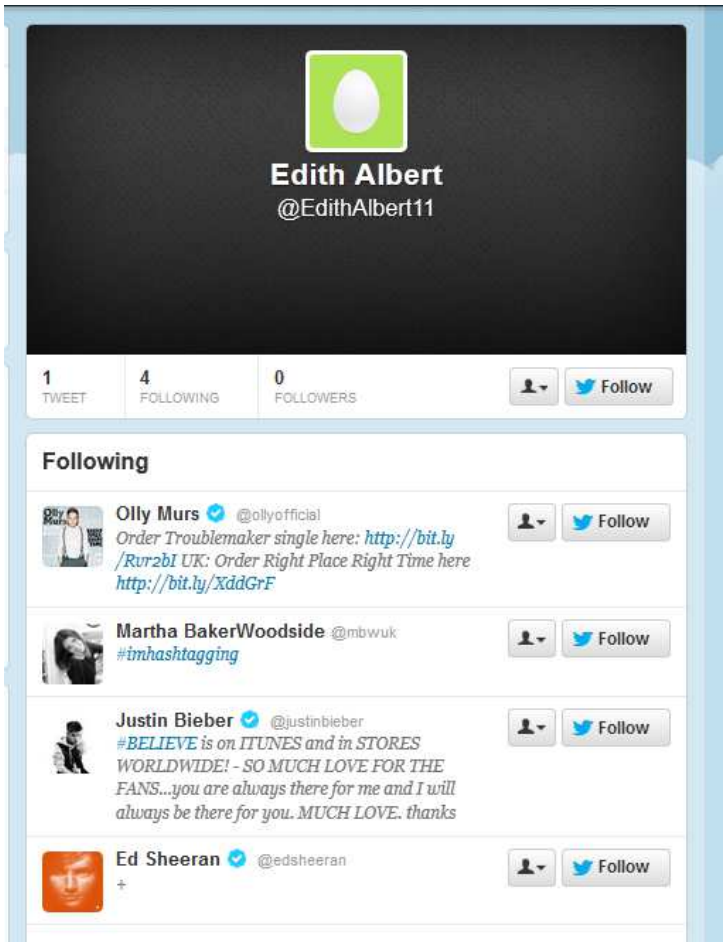
```
The weather is good today. Sunny! uri!wp07VkkxYt3Mne5uiDkz4Il/Iw48Ge/EWg==

Albert, my cousin. He is working hard. uri!wp07VkkxYmfNkwN2nBmx4ch/Iu2c+GJow39HbphL

My native town was ruined by tornado. uri!wp07VkkxYt3Md/JOnLhzRL2FJjY8l2It
```

Figure 15 – Known twitter answers for C&C discovery

The twitter information is currently not very useful for content based detection, as it is downloaded through SSL connection, and therefore, IDS rules can only be applied if some SSL proxy is used.



An interesting observation is that this user follows 4 partners, most likely for deception.


Edith Albert
@EdithAlbert11
1
TWEET
4
FOLLOWING
0
FOLLOWERS
Follow
Following
Olly Murs @ollyofficial
Order Troublemaker single here: http://bit.ly/Rvr2bI UK: Order Right Place Right Time here http://bit.ly/XddGrF
Follow
Martha BakerWoodside @mbwuk
#imhashtagging
Follow
Justin Bieber @justinbieber
#BELIEVE is on ITUNES and in STORES WORLDWIDE! - SO MUCH LOVE FOR THE FANS...you are always there for me and I will always be there for you. MUCH LOVE. thanks
Follow
Ed Sheeran @edsheeran
+
Follow