A Detailed Examination of the Siesta Campaign

fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html

Threat Research Blog

March 12, 2014 | by Ned Moran, Mike Oppenheim

Executive Summary

FireEye recently looked deeper into the activity discussed in TrendMicro's blog and dubbed the "Siesta" campaign. The tools, modus operandi, and infrastructure used in the campaign present two possibilities: either the Chinese cyber-espionage unit APT1 is perpetrating this activity, or another group is using the same tactics and tools as the legacy APT1.

The Siesta campaign reinforces the fact that analysts and network defenders should remain on the lookout for known, public indicators and for shared attributes that allow security experts to detect multiple actors with one signature.

Overview

On March 6, 2014 TrendMicro reported on the Siesta Campaign. Though not explicitly stated in this report, the tactics, techniques and procedures (TTPs) described in this report share a number of characteristics with historical activity we've attributed to APT1 (also known as the

“Comment Crew”).

We witnessed this same campaign targeting a customer in the telecommunications sector on Feb. 20, 2014, using a spear-phishing message with a link to ifuedit[.]net/Healthcare_Questionnaire.zip. This zip file contained a malicious executable with the following properties:

MD5	61249bf64fa270931570b8a5eba06afa
Compile Time	2014-02-20 02:28:21
.text	39e9e4eac77a09b915626f315b963a4f
.rdata	a126c8c7c50bf034f2d3ba4aa5bcab28
.data	bb95154b5aeb13a4ff937afa2e7e4560
.rsrc	edf3a1e142fc212da11dc72698184ad5
Import Hash	20ff5087740eabff5bdbdf99d9fb6853

This sample initiated a callback to www[.]microsofthomes[.]com/index.html.

This same import hash was seen in the following samples:

MD5	Compile Time	Command-and-Control (CnC) server
68f73d81c814ab2f70eed02c0be3b67d 68f73d81c814ab2f70eed02c0be3b67d	2014-02-20 02:26:24 2014-02-20 02:26:24	www[.]microsofthomes[.]com www[.]microsofthomes[.]com
20b124baaaec1e8cbc3cd52e8e5ceebd 20b124baaaec1e8cbc3cd52e8e5ceebd	2014-02-20 02:26:24 2014-02-20 02:26:24	www[.]microsofthomes[.]com www[.]microsofthomes[.]com

Techniques, tactics, and procedures analysis

The TTPs described above are consistent with APT1. This group previously relied on establishing a foothold in targeted networks with following methods:

- Spear-phishing emails with links to archives
- Callback traffic to a legitimate-looking webpage

Analysis of Related Samples

A related dropper listed in the TrendMicro report on the Siesta campaign is MD5 0f3031412d255336a102bbc1dcd43812. This sample had the following properties:

MD5	0f3031412d255336a102bbc1dcd43812
Compile Time	2014-02-19 09:29:04
.text	a2e11e9c8b07888345d6cdf7d995b832
.rdata	0203cc3bb607e9cfa296fa857b243468
.data	7d281bd27bc1279428bd1798671eb57b
.rsrc	caa869fa01ddfee26156166a10c42944
Import Hash	0fefba40443edd57f816502035077e3e

The import hash of 0fefba40443edd57f816502035077e3e is in other samples linked to the Siesta campaign including:

MD5	Compile Time	CnC
643654975b63a9bb6f597502e5cd8f49 643654975b63a9bb6f597502e5cd8f49	2014-01-14 04:38:30 2014-01-14 04:38:30	www[.]cloudcominc[.]com www[.]cloudcominc[.]com
0f3031412d255336a102bbc1dcd43812 0f3031412d255336a102bbc1dcd43812	2014-02-19 09:29:04 2014-02-19 09:29:04	www[.]skyslisten[.]com www[.]skyslisten[.]com

The import hash from this dropper was also seen in a number of previous APT1 samples dating as far back as 2011 — well before the release of the APT1 report. We previously discussed the value of tracking via import hashing here. Other APT1 samples with this same import hash include (but are not limited to):

MD5	Compile Time	CnC
719453b4da6d3814604c84a28d4d1f4c 719453b4da6d3814604c84a28d4d1f4c	2011-06-16 12:54:20 2011-06-16 12:54:20	www[.]stapharrest[.]com www[.]stapharrest[.]com
93a6e9a26924a5cdab8ed47cadbe88d5 93a6e9a26924a5cdab8ed47cadbe88d5	2012-01-18 13:35:54 2012-01-18 13:35:54	www[.]offerdahls[.]com www[.]offerdahls[.]com
c2aadd6a69a775602d984af64eaeda96 c2aadd6a69a775602d984af64eaeda96	2012-05-15 09:02:25 2012-05-15 09:02:25	www[.]bluecoate[.]com www[.]bluecoate[.]com
1df0b937239473df0187063392dae028 1df0b937239473df0187063392dae028	2012-06-20 09:25:31 2012-06-20 09:25:31	www[.]billyjoebobshow[.]com www[.]billyjoebobshow[.]com

55065f1b341e5b095b6d453923d5654d 55065f1b341e5b095b6d453923d5654d	2012-07-12 09:21:17 2012-07-12 09:21:17	184.82.164.104 184.82.164.104
65502e91e3676cf30778a7078f1061de 65502e91e3676cf30778a7078f1061de	2012-07-19 09:31:42 2012-07-19 09:31:42	www[.]billyjoebobshow[.]com www[.]billyjoebobshow[.]com
287113e4423813efd242af8e6255f680 287113e4423813efd242af8e6255f680	2012-07-24 05:53:22 2012-07-24 05:53:22	thales[.]myftp[.]info thales[.]myftp[.]info
d613d40d5402f58d8952da2c24d1a769 d613d40d5402f58d8952da2c24d1a769	2012-09-27 12:46:20 2012-09-27 12:46:20	www[.]billyjoebobshow[www[.]billyjoebobshow[
57a4c6236b4ecf96d31258e5cc6f0ae4 57a4c6236b4ecf96d31258e5cc6f0ae4	2013-01-07 07:43:14 2013-01-07 07:43:14	manslist[.]loopback[.]nu manslist[.]loopback[.]nu
e5a4ec0519c471b5be093aee5c33b1ee e5a4ec0519c471b5be093aee5c33b1ee	2013-01-08 07:34:59 2013-01-08 07:34:59	www[.]whackcard[.]com www[.]whackcard[.]com
f822a9e08b51c19a154dfb63ee9b8367 f822a9e08b51c19a154dfb63ee9b8367	2013-01-10 07:50:58 2013-01-10 07:50:58	technology[.]acmetoy[.]com technology[.]acmetoy[.]com

Further, the 0f3031412d255336a102bbc1dcd43812 sample dropped a backdoor with the MD5 hash 185e930a19ad1a99c226d59ef563e28c. This implant was stored as a resource within the dropper, and it contained a custom base64 alphabet of oWXYZabcdefghijkl123456789ABCDEFGHIJKL+/MNOPQRSTUVmn0pqrstuvwxyz. This custom alphabet was used by the malware to decode commands issued by the attacker to the victim machine and to Base64 encode the reverse shell from the victims back to the CnC server.This same custom alphabet has been used in previous APT1 samples including (but not limited to):

MD5	**Compile Time**	**CnC**
736ebc9b8ece410aaf4e8b60615f065f 736ebc9b8ece410aaf4e8b60615f065f	2003-05-15 08:58:48 2003-05-15 08:58:48	www[.]comtoway[.]com www[.]comtoway[.]com
ac87816b9a371e72512d8fd82f61c737 ac87816b9a371e72512d8fd82f61c737	2006-09-14 02:28:46 2006-09-14 02:28:46	www[.]mwa[.]net www[.]mwa[.]net

173cd315008897e56fa812f2b2843f83 173cd315008897e56fa812f2b2843f83	2006-09-14 02:28:46 2006-09-14 02:28:46	www[.]deebeedesigns[.]ca www[.]deebeedesigns[.]ca
513644c57688b70860d0b9aa1b6cd0d7 513644c57688b70860d0b9aa1b6cd0d7	2010-12-17 03:24:13 2010-12-17 03:24:13	69.90.65.240 69.90.65.240
fdf6bf1973af8ab130fbcaa0914b4b06 fdf6bf1973af8ab130fbcaa0914b4b06	2012-05-10 08:41:35 2012-05-10 08:41:35	www[.]woodagency[.]com www[.]woodagency[.]com
682bfed6332e210b4f3a91e5e8a1410b 682bfed6332e210b4f3a91e5e8a1410b	2012-05-15 03:17:04 2012-05-15 03:17:04	www[.]oewarehouse[.]com www[.]oewarehouse[.]com
fb7a74a88eead4d39a58cc7b6eede4ce fb7a74a88eead4d39a58cc7b6eede4ce	2013-08-01 18:23:07 2013-08-01 18:23:07	www[.]mwa[.]net www[.]mwa[.]net

Executable (PE) resource with PDF icon Table

MD5	Compile Time	CnC
719453b4da6d3814604c84a28d4d1f4c 719453b4da6d3814604c84a28d4d1f4c	2011-06-16 12:54:20 2011-06-16 12:54:20	www[.]drgeorges[.]com www[.]drgeorges[.]com
854cb8ba3b2d3058239a7ba6a427944a 854cb8ba3b2d3058239a7ba6a427944a	2011-08-17 00:31:27 2011-08-17 00:31:27	meeting[.]toh[.]info meeting[.]toh[.]info
a049b8ec51c0255dec734c7ba5641af3 a049b8ec51c0255dec734c7ba5641af3	2011-08-17 00:31:27 2011-08-17 00:31:27	meeting[.]toh[.]info meeting[.]toh[.]info
0725a1819a58e988b939f06e53990254 0725a1819a58e988b939f06e53990254	2011-08-17 00:31:27 2011-08-17 00:31:27	google.ninth.biz google.ninth.biz
0fdffd4f5730bdd37f2f082bf396064a 0fdffd4f5730bdd37f2f082bf396064a	2011-08-11 09:35:24 2011-08-11 09:35:24	homepage[.]longmusic[.]com homepage[.]longmusic[.]com
e476e4a24f8b4ff4c8a0b260aa35fc9f e476e4a24f8b4ff4c8a0b260aa35fc9f	2012-06-09 13:19:49 2012-06-09 13:19:49	www[.]heliospartners[.]com www[.]heliospartners[.]com

d613d40d5402f58d8952da2c24d1a769 d613d40d5402f58d8952da2c24d1a769	2012-09-27 12:46:20 2012-09-27 12:46:20	www[.]billyjoebobshow[.]com www[.]billyjoebobshow[.]com
f822a9e08b51c19a154dfb63ee9b8367 f822a9e08b51c19a154dfb63ee9b8367	2013-01-10 07:50:58 2013-01-10 07:50:58	technology[.]acmetoy[.]com technology[.]acmetoy[.]com

Both 61249bf64fa270931570b8a5eba06afa and 0f3031412d255336a102bbc1dcd43812 droppers also had a portable executable (PE) resource with the SHA256 of fb080cef60846528c409f60400f334100a16a5bd77b953c864b23a945fcf26fd. This PE resource contained the PDF icon used by the dropper to make the executable appear as though it was a PDF document rather than an executable. Previous APT1 samples also used this sample PE resource including (but not limited to):

MD5	Compile Time	CnC
1aab2040ed4f918e1823e2caf645a81d 1aab2040ed4f918e1823e2caf645a81d	2009-09-28 22:08:38 2009-09-28 22:08:38	www[.]olmusic100[.]com www[.]olmusic100[.]com
8ee2cf05746bb0a009981fdb90f1343e 8ee2cf05746bb0a009981fdb90f1343e	2010-03-15 11:46:31 2010-03-15 11:46:31	gogotrade[.]apple.org[.]ru tradeproject[.]rlogin[.]org gogotrade[.]apple.org[.]ru tradeproject[.]rlogin[.]org
9c4617793984c4b08d75b00f1562cbda 9c4617793984c4b08d75b00f1562cbda	2010-08-31 03:27:55 2010-08-31 03:27:55	freetrade[.]allowed[.]org worldwide[.]chickenkiller[.]com freetrade[.]allowed[.]org worldwide[.]chickenkiller[.]com
b584b48d401e98f404584c330489895c b584b48d401e98f404584c330489895c	2010-08-31 07:52:17 2010-08-31 07:52:17	worldwide[.]chickenkiller[.]com freetrade[.]allowed[.]org worldwide[.]chickenkiller[.]com freetrade[.]allowed[.]org
b92a53fc409d175c768581978f1d3331 b92a53fc409d175c768581978f1d3331	2010-09-16 09:57:09 2010-09-16 09:57:09	www[.]rbaparts[.]com www[.]rbaparts[.]com
d6c19be4e9e1ae347ee269d15cb96a51 d6c19be4e9e1ae347ee269d15cb96a51	2010-10-25 01:59:00 2010-10-25 01:59:00	www[.]kayauto[.]net www[.]kayauto[.]net
d0a7cd5cd7da9024fb8bd594d37d7594 d0a7cd5cd7da9024fb8bd594d37d7594	2011-04-20 07:39:01 2011-04-20 07:39:01	www[.]kayauto[.]net www[.]kayauto[.]net

b19ef1134f54b4021f99cc45ae1bc270 b19ef1134f54b4021f99cc45ae1bc270	2011-06-13 06:56:04 2011-06-13 06:56:04	www[.]kayauto[.]net www[.]kayauto[.]net
b0a95c47d170baad8a5594e0f755e0c1 b0a95c47d170baad8a5594e0f755e0c1	2012-03-26 06:50:10 2012-03-26 06:50:10	www[.]coachmotor[.]com www[.]coachmotor[.]com
894ef915af830f38499d498342fdd8db 894ef915af830f38499d498342fdd8db	2012-03-26 07:13:36 2012-03-26 07:13:36	www[.]rightnowautoparts[.]com www[.]rightnowautoparts[.]com
c2aadd6a69a775602d984af64eaeda96 c2aadd6a69a775602d984af64eaeda96	2012-05-15 09:02:25 2012-05-15 09:02:25	www[.]bluecoate[.]com www[.]bluecoate[.]com

Links to other Activity

This same PE resource was also used in a number of other samples deployed by the "Menupass" group, which we have detailed in our Poison Ivy report. Previous Menupass samples with this same PE resource include (but are not limited to):

MD5	Compile Time	CnC
392f15c431c00f049bb1282847d8967f 392f15c431c00f049bb1282847d8967f	2012-05-16 06:48:02 2012-05-16 06:48:02	army.xxuz.com army.xxuz.com
21567cce2c26e7543b977a205845ba77 21567cce2c26e7543b977a205845ba77	2012 06 26 05:17:52 2012 06 26 05:17:52	nasa.xxuz.com nasa.xxuz.com
d4b7f99669a3efc94006e5fe9d84eb65 d4b7f99669a3efc94006e5fe9d84eb65	2012-07-03 09:33:46 2012-07-03 09:33:46	tw.2012yearleft.com tw.2012yearleft.com
df5bd411f080b55c578aeb9001a4287d df5bd411f080b55c578aeb9001a4287d	2012-07-04 04:07:36 2012-07-04 04:07:36	apple.cmdnetview.com apple.cmdnetview.com
001b8f696b6576798517168cd0a0fb44 001b8f696b6576798517168cd0a0fb44	2012 11 13 07:19:03 2012 11 13 07:19:03	google.macforlinux.net google.macforlinux.net
6a3b8d24c125f3a3c7cff526e63297f3 6a3b8d24c125f3a3c7cff526e63297f3	2013-02-25 05:31:41 2013-02-25 05:31:41	cvnx.zyns.com cvnx.zyns.com
a02610e760fa15c064931cfafb90a9e8 a02610e760fa15c064931cfafb90a9e8	2013-08-01 18:23:04 2013-08-01 18:23:04	cvnx.zyns.com cvnx.zyns.com
78a4fee0e7b471f733f00c6e7bca3d90 78a4fee0e7b471f733f00c6e7bca3d90	2013-08-01 18:23:05 2013-08-01 18:23:05	fbi.sexxxy.biz fbi.sexxxy.biz
6f3d15cf788e28ca504a6370c4ff6a1e 6f3d15cf788e28ca504a6370c4ff6a1e	2013-09-10 06:40:28 2013-09-10 06:40:28	scrlk.exprenum.com scrlk.exprenum.com

Shared Tools

This shared PE resource between what is believed to be two distinct groups (likely APT1, and Menupass) can be explained by either of the following:

- APT1 and Menupass are actually one and the same
- APT1 and Menupass share “binder” tools

It is unlikely that APT1 and Menupass represent the same group. We have observed no other overlaps in infrastructure or tools between these two groups. A more likely possibility is that the shared resource between APT1 and the Menupass group is a binder tool.

A binder tool enables a malicious actor to add an innocuous-looking icon, such as a PDF document icon, to a malicious dropper. This technique facilitates social engineering, presenting the end user with a file that looks like a PDF document rather than an executable. Figure 1 shows a builder that enables actors to bind a JPG image icon to a malicious executable.

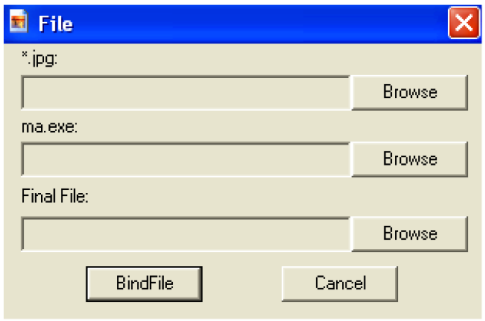

Figure 1: Binder tool for disguising executable files as JPGs

Attribution

Based on the evidence provided, the following are possibilities:

- The Siesta campaign was executed by APT1
- An unknown group using tools and tactics shared by APT1 executed the Siesta campaign

Although we are not certain that APT1 is responsible for the Siesta activity, this current campaign shares a number of distinct characteristics with previous activity attributed to APT1.

So What?

Regardless of which group is responsible for this campaign, our analysis highlights the importance of monitoring for known indicators. As shown above, monitoring for previously disclosed indicators of compromise (IOCs), even IOCs that are years old, can yield value.

Additionally, monitoring for IOCs and attributes of malware that are shared by multiple groups may also improve the effectiveness of your network defense operations. In this example, implementing detection for executables with a PE resource with a SHA256 hash of fb080cef60846528c409f60400f334100a16a5bd77b953c864b23a945fcf26fd would detect both Menupass and APT1 samples.