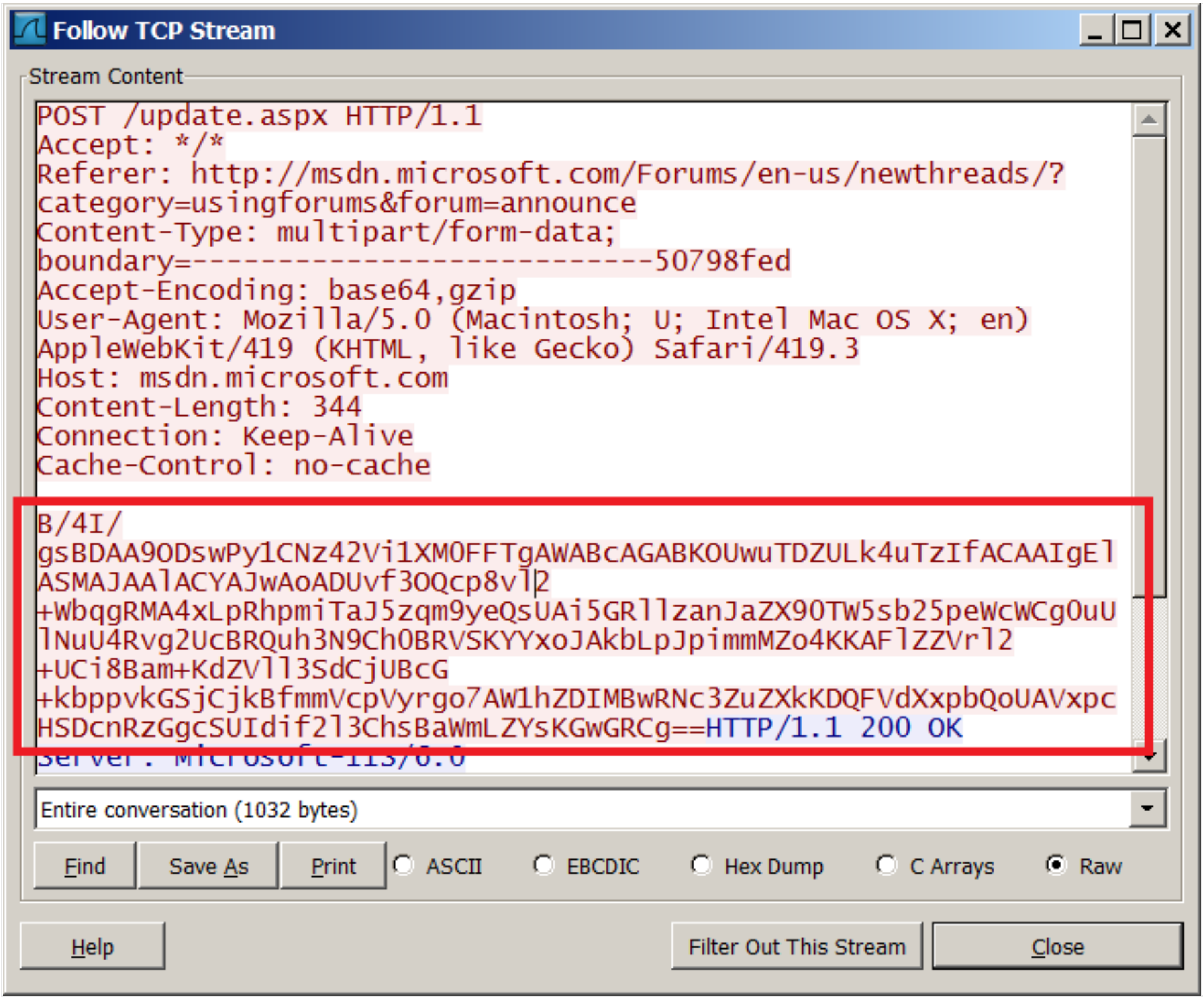
New Version of OSX.SabPub & Confirmed Mac APT attacks

Late last week, we found evidence of a possible link between a Mac OS X backdoor trojan and an APT attack known as LuckyCat. The IP address of the C&C to which this bot connects (199.192.152.*) was also used in other Windows malware samples during 2011, which made us believe we were looking at the same entity behind these attacks.

For the past two days, we have been monitoring a "fake" infected system - which is a typical procedure we do for APT bots. We were extremely surprised when during the weekend, the APT controllers took over our "goat" infected machine and started exploring it.

On Friday Apri 13, port 80 on the C&C server located at rt*****.onedumb.com and hosted on a VPS in Fremont, U.S. was closed. Saturday, the port was opened and bot started communicating with the C&C server. For the entire day, the traffic was just basic handshakes and exchanges, nothing more.

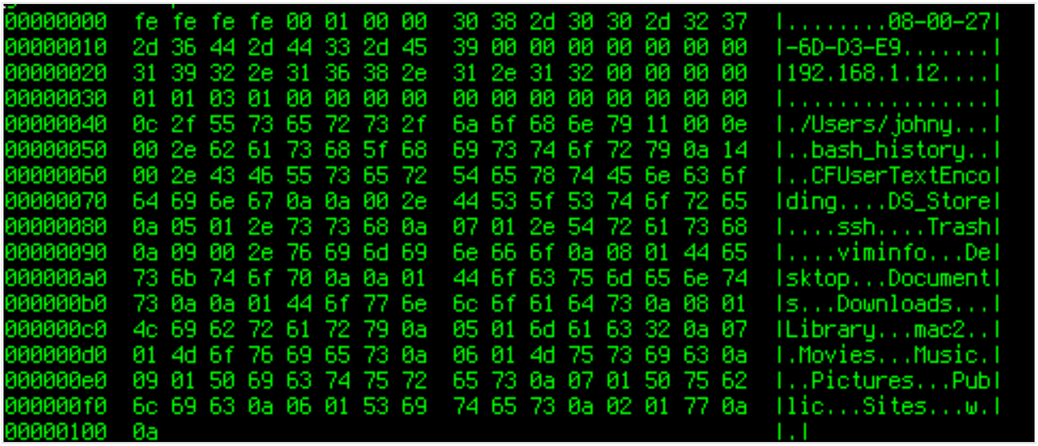
On the morning of Sunday April 15, the traffic generated by the C&C changed. The attackers took over the connection and started analysing our fake victim machine. They listed the contents of the root and home folders and even stole some of the goat documents we put in there!



```
POST /update.aspx HTTP/1.1
Accept: */*
Referer: http://msdn.microsoft.com/Forums/en-us/newthreads/?
category=usingforums&forum=announce
Content-Type: multipart/form-data;
boundary=---------------------------50798fed
Accept-Encoding: base64,gzip
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en)
AppleWebKit/419 (KHTML, like Gecko) Safari/419.3
Host: msdn.microsoft.com
Content-Length: 344
Connection: Keep-Alive
Cache-Control: no-cache

B/4I/
gsBDAA9ODswPy1CNz42Vi1XM0FFTgAWABcAGABKOUwuTDZULk4uTzIfACAAIgEl
ASMAJAAlACYAJwAoADUvf3OQcp8vl2
+WbqgRMA4xLpRhpmiTaJ5zqm9yeQsUAi5GRllzanJaZX90TW5sb25peWcWCg0uU
lNuU4Rvg2UcBRQuh3N9Ch0BRVSKYYxoJAkbLpJpimmMZo4KKAFlZZVrl2
+UCi8Bam+KdZVll3SdCjUBcG
+kbppvkGSjCjkBfmmVcpVyrgo7AW1hZDIMBwRNc3ZuZXkKDQFVdXxpbQoUAVxpc
HSDcnRzGgcSUIdif2l3ChsBaWmLZYsKGwGRCg==HTTP/1.1 200 OK
Server: Microsoft-IIS/6.0
```

Encoded communication between C&C and our fake victim



```
00000000  fe fe fe fe 00 01 00 00  30 38 2d 30 30 2d 32 37  |........08-00-27|
00000010  2d 36 44 2d 44 33 2d 45  39 00 00 00 00 00 00 00  |-6D-D3-E9.......|
00000020  31 39 32 2e 31 36 38 2e  31 2e 31 32 00 00 00 00  |192.168.1.12....|
00000030  01 01 03 01 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000040  0c 2f 55 73 65 72 73 2f  6a 6f 68 6e 79 11 00 0e  |./Users/johny...|
00000050  00 2e 62 61 73 68 5f 68  69 73 74 6f 72 79 0a 14  |..bash_history..|
00000060  00 2e 43 46 55 73 65 72  54 65 78 74 45 6e 63 6f  |..CFUserTextEnco|
00000070  64 69 6e 67 0a 0a 00 2e  44 53 5f 53 74 6f 72 65  |ding....DS_Store|
00000080  0a 05 01 2e 73 73 68 0a  07 01 2e 54 72 61 73 68  |....ssh....Trash|
00000090  0a 09 00 2e 76 69 6d 69  6e 66 6f 0a 08 01 44 65  |....viminfo...De|
000000a0  73 6b 74 6f 70 0a 0a 01  44 6f 63 75 6d 65 6e 74  |sktop...Document|
000000b0  73 0a 0a 01 44 6f 77 6e  6c 6f 61 64 73 0a 08 01  |s...Downloads...|
000000c0  4c 69 62 72 61 72 79 0a  05 01 6d 61 63 32 0a 07  |Library...mac2..|
000000d0  01 4d 6f 76 69 65 73 0a  06 01 4d 75 73 69 63 0a  |.Movies...Music.|
000000e0  09 01 50 69 63 74 75 72  65 73 0a 07 01 50 75 62  |..Pictures...Pub|
000000f0  6c 69 63 0a 06 01 53 69  74 65 73 0a 02 01 77 0a  |lic...Sites...w.|
00000100  0a                                                |.|
```

Packet above, decoded - attacker is listing folders content

We are pretty confident the operation of the bot was done manually -- which means a real attacker, who manually checks the infected machines and extracts data from them.

We can therefore confirm SabPub as APT in active stage.

On Sunday midday, the C&C domain was shutdown and the bot lost connection to it; this appears to be an initiative from the free DNS service onedumb.com and it was no doubt triggered by the media attention. Interestingly, the VPS used as the C&C is still active.

While analysing SabPub, we discovered another version of the backdoor which seems to have been created earlier. This version differs from the original one only slightly -- the hardcoded C&C address is different -- instead of the onedumb.com subdomain used by the original sample (hardcoded in the bot as "**e3SCNUA2Om97ZXJ1fGI+Y4Bt**"), this one simply contains the IP address of the VPS (hardcoded as "**OjlDLjw5Pi4+NUAuQDBA**"), meaning, it should still be operational. Its size is 42556 bytes vs 42580 for the original one.

One of the biggest mysteries is the infection vector of these attacks. Given the highly targeted nature of the attack, there are very few traces. Nevertheless, we found an important detail which is the missing link: Six Microsoft Word documents, which we detect as **Exploit.MSWord.CVE-2009-0563.a**. In total we have six relevant Word .docs with this verdict -- with four dropping the MaControl bot. **The remaining two drop SabPub**.

The most interesting thing here is the history of the second SabPub variant. In our virus collection, it is named "8958.doc". This suggests iit was extracted from a Word document or was distributed as a Doc-file.

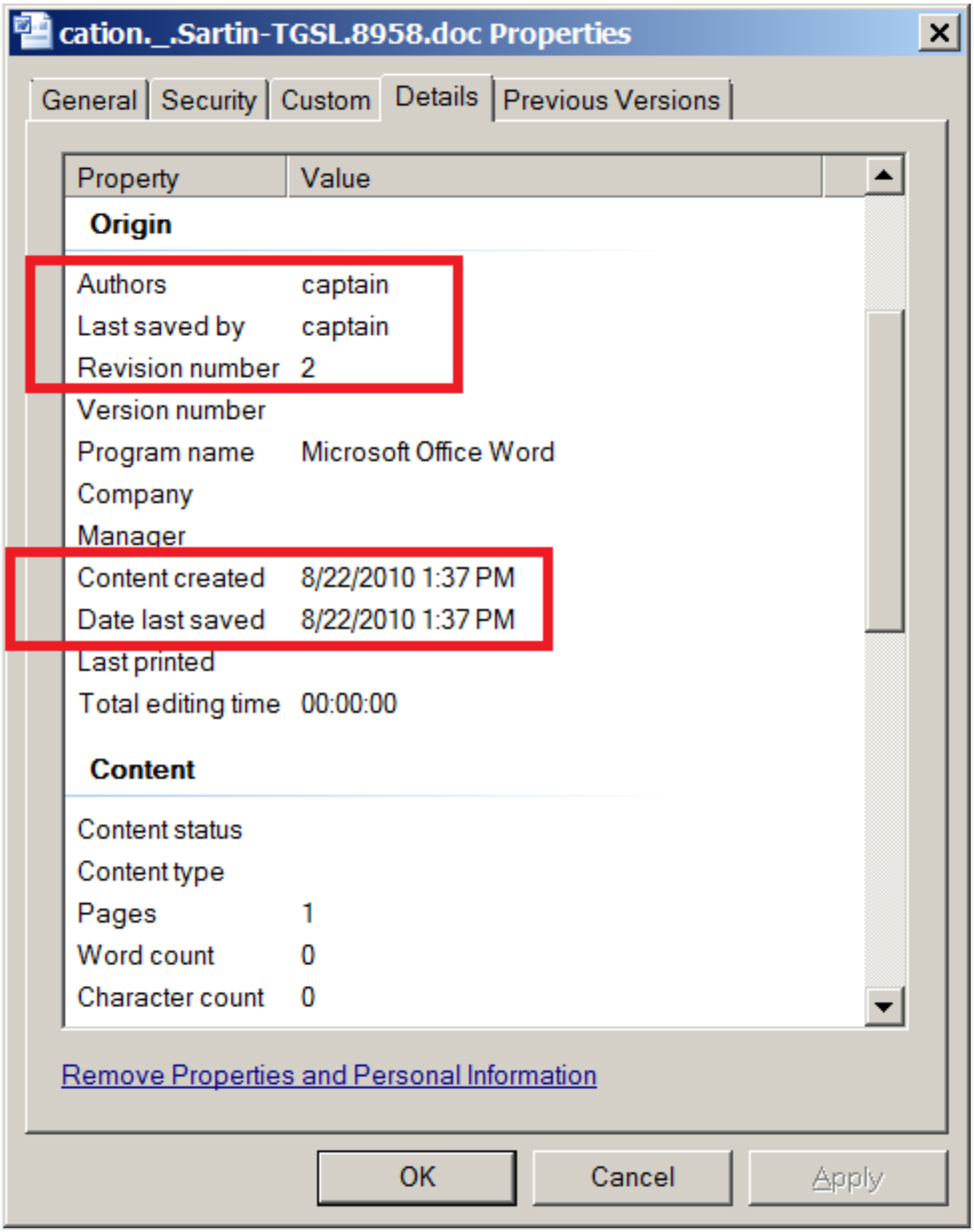
We performed an analysis of the same and traced its origin by the MD5 (*40C8786A4887A763D8F3E5243724D1C9*). The results were fascinating:

- The sample was uploaded to VirusTotal on February 25, 2012 – from two sources in the U.S.

- In both cases, the original file name was "10th March Statemnet" (yes, with the typo and without extension)

- Zero detections on VirusTotal at that time (0/40)

In case you are wondering, the name of the file ("10th March Statemnet") is directly linked with the Dalai-Lama and Tibetan community. On March 10, 2011, the Dalai-Lama released a special statement related to Anniversary of the Tibetan People's National Uprising Day -- hence the name.


cation._.Sartin-TGSL.8958.doc Properties
General
Security
Custom
Details
Previous Versions
Remove Properties and Personal Information
OK
Cancel
Apply

Property	Value
Origin	
Authors	captain
Last saved by	captain
Revision number	2
Version number	
Program name	Microsoft Office Word
Company	
Manager	
Content created	8/22/2010 1:37 PM
Date last saved	8/22/2010 1:37 PM
Last printed	
Total editing time	00:00:00
Content	
Content status	
Content type	
Pages	1
Word count	0
Character count	0

Properties field of a document used to spread SabPub

Unfortunately there is little information in the doc files, but the Author field and the creation date are interesting. In particular, if we trust the creation date, this means the container DOC was created in August 2010 and it was updated in 2012 with the SabPub sample. This is quite normal for such attacks and we have seen it in other cases, for instance, Duqu.

We think the above facts show a direct connection between the SabPub and Luckycat APT attacks. We are pretty sure the SabPub backdoor was created as far back as February 2012 and was distributed via spear-phishing emails.

It is also important to point that SabPub isn't backdoor MaControl (the case was described here) but still uses the same topics to trick victims into opening it. SabPub was the more effective attack because it remained undetected for almost two months!

The second variant of SabPub was created in March and the attackers are using Java exploits to infect target Mac OS X machines.

SabPub is still an active attack and we expect the attackers will release new variants of the bot with new C2s over the next days/weeks.

To summarize:

- At least two variants of the SabPub bot exist today.

- The earliest version of the bot appears to have been created and used in February 2012.

- The malware is being spread through Word documents that exploit the CVE-2009-0563 vulnerability.

- SabPub is different from MaControl, another bot used in APT attacks in February 2012; SabPub was more effective because it stayed undetected for more than 1.5 months.

- the APT behind SabPub is active at the time of writing.

* *Thanks to Aleks Gostev and Igor Soumenkov for the analysis*.