

C&C-as-a-Service

Abusing third-party web services as C&C channels

Artturi Lehtiö (@lehtior2)

Researcher, F-Secure

Network-level detection & blocking for the win!

Detect & block C&C traffic!

Hide the C&C traffic!

“Only 2.6% of active malware families used encrypted C&C protocols and most of those could be detected by inspecting the traffic.”

Source: <http://resources.alcatel-lucent.com/asset/189669> Motive Security Labs malware report H1 2015

“OPM officials **did not know** they had a problem until April 15, 2015, when the agency **discovered ‘anomalous SSL traffic with [a] decryption tool’**”

Source: <https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx>

“Malware that uses standard cryptography such as **SSL is more difficult** [to detect, but] we can **often accurately identify** the malware using **IP or DNS blacklists**.”

Source: <http://resources.alcatel-lucent.com/asset/189669> Motive Security Labs malware report H1 2015

What's the fuss?

**Does the Kremlin Have a New
Way of Hacking the West?**

Hackers found an ingenious way to embarrass Microsoft

**Russia's cyberwarriors use Twitter to hide
intrusion**

'World's most sophisticated cyber weapon'



TechNet



tumblr.



“Employing legitimate web services [...] makes it harder for network defenders to discern between malicious and legitimate traffic.”

Source: <https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf>

Challenge 1: No network-level detection & blocking

Challenge 2:

No netflow, traffic logs, PCAPs, etc. for incident response

Challenge(?) 3: Takedowns?

Challenge(?) 4: Sinkholing?

Simplicity for the win!

Backdoor.Makadocs

<https://docs.google.com/viewer?url=https%3A%2F%2Fwww.virusbtn.com%2F>

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head xmlns:atom="http://www.w3.org/2005/Atom" xmlns:georss="http://www.georss.org/georss">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="stylesheet" href="/library/css/fullscreen.css" type="text/css">
<link rel="stylesheet" href="/library/css/vbstyle.css" type="text/css">
<!--[if IE]>
  <style type="text/css" media="screen">
    body { behavior: url(/library/javascript/csshover.htc); }
    .dropdown ul li {float: left; width: 100%;}
    .dropdown ul li a {height: 1%;}
    #center {overflow-x:auto;}
    fieldset legend {margin-left:-6px;}
  </style>
<![endif]--><title>Virus Bulletin : Covering the global threat landscape</title>
```


3rd party services for primary C&C channel establishment

Janicab/DuCK

ALL COMMENTS (2)

Share your thoughts

Top comments ▾

 **Jasper Warmerdam** 1 week ago
our 50380702789658th psy anniversary
Reply · 1  

 **Jasper Warmerdam** 1 week ago
our 50380702789658th psy anniversary
Reply · 1  

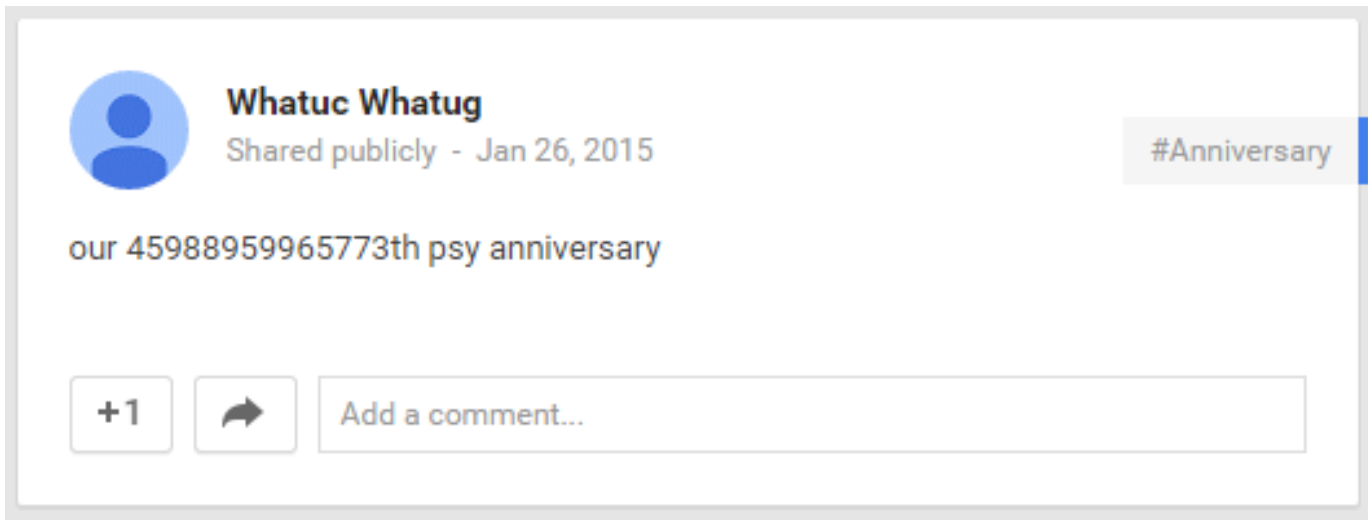
Janicab/DuCK


MONDAY, 17 DECEMBER 2001

our 45988959746414th psy anniversary

posted by 0x00000016 @ 02:28


Janicab/DuCK

A screenshot of a Facebook post. The post is from a user named 'Whatuc Whatug' who shared it publicly on January 26, 2015. The post content is 'our 45988959965773th psy anniversary'. There is a '#Anniversary' hashtag in the top right corner. At the bottom, there are buttons for '+1', a share icon, and a text input field with the placeholder 'Add a comment...'.

 **Whatuc Whatug**
Shared publicly - Jan 26, 2015

#Anniversary

our 45988959965773th psy anniversary

+1  Add a comment...

Other examples:

- APT17
 - Microsoft TechNet
- Operation Poisoned Hurricane
 - Google Code
- Shadows in the Cloud
 - Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com
- GeminiDuke
 - Twitter
- Trojan.Whitewell
 - Facebook
- Trojan-downloader f0xy
 - VKontakte

New Botnet controlled via Twitter

Resolution

New Botnet controlled via Twitter (Aug 18, 2009)

SonicWALL UTM Research team observed a new Botnet family that uses social networking services like Twitter, Jaiku, Tumblr as its Command & Control (C&C) server mechanism.

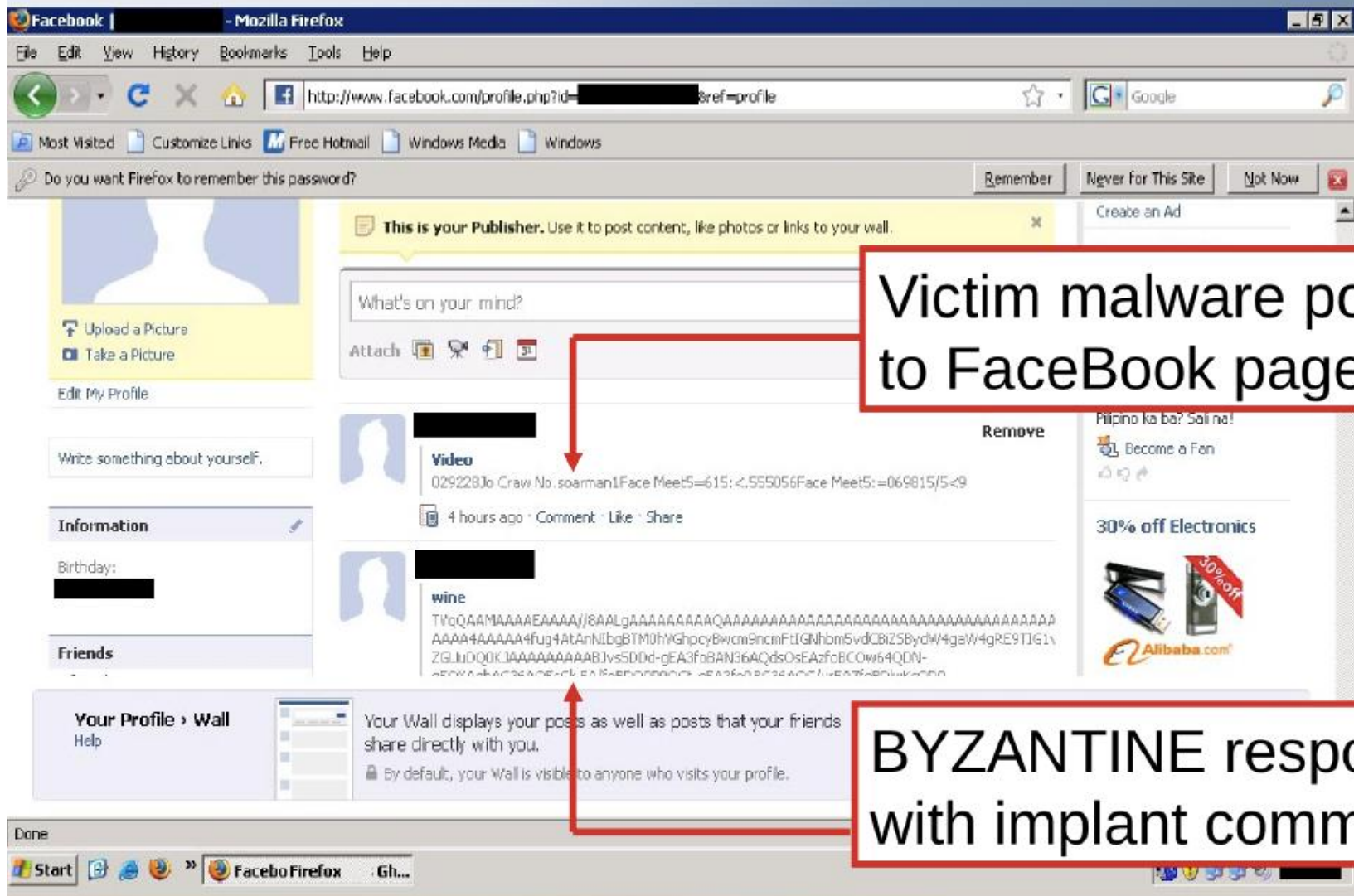
The status messages on the social blogging sites serve as the C&C commands that contain links to download malicious payload. The status messages are Base-64 encoded.

<https://support.software.dell.com/kb/sw7146>

3rd party services as primary C&C channels



(S)Command and Control over FaceBook



Victim malware posts to FaceBook page

BYZANTINE responds with implant commands

Other examples:

- Inception/CloudAtlas
 - CloudMe
- CloudDuke
 - Microsoft OneDrive
- IcoScript
 - Yahoo Mail
- APT1: GLOOXMAIL, MACROMAIL & CALENDAR
 - Google Talk, MSN Messenger & Google Calendar
- BlackEnergy
 - Google+ module
- Lots of academic papers on using Twitter!

Also mobile

- Android.Cajino uses Baidu Cloud Push
- Various Android malware use Google Cloud Messaging
 - Trojan-SMS.AndroidOS.FakeInst.a
 - Trojan-SMS.AndroidOS.Agent.ao
 - Trojan-SMS.AndroidOS.Agent.az
 - Trojan-SMS.AndroidOS.OpFake.a
 - Backdoor.AndroidOS.Maxit.a



3rd party services as backup C&C channels


OnionDuke





TWEETS

1

Tweets Tweets & replies

  · Sep 16

What a nice picture  [images/nature....](#) take a look

OnionDuke



OnionDuke

```
000428d0 1c c2 16 25 26 f4 03 6f-4a e9 2f b8 48 ce 28 8e | ???%&??oJ?/?H?(?  
000428e0 a2 8e 61 c6 6d 51 5c 4c-a7 48 20 8f 61 40 6d 96 | ??a?mQ\L?H ?a@m?  
000428f0 c5 45 75 01 0b 24 af b1-15 6e e4 b7 61 97 56 37 | ?Eu??$???n??a?V?  
00042900 00 13 81 4c b2 a8 23 13-2e ca d5 48 89 37 44 15 | ??L??#?.??H?7D?  
00042910 3a 57 b7 20 77 c0 f5 aa-0d a7 6b 89 24 65 27 b8 | :W? w?????k?$e'?  
00042920 a6 9b 54 e4 41 82 f3 ef-36 87 d2 ac e5 27 bf 34 | ??T?A????6?????'?4  
00042930 b6 f3 a0 c9 2e 6d d8 14-72 05 3a 0f 42 33 59 e3 | ?????.m??r?:?B3Y?  
00042940 13 ff d9 3c 3c 3c 2d 2d-2d 20 33 62 37 38 39 35 | ???<<<--- 3b7895  
00042950 30 61 30 35 30 34 30 34-30 34 30 34 30 34 30 34 | 0a05040404040404  
00042960 30 34 37 31 30 34 34 39-35 65 39 34 30 34 30 37 | 047104495e940407  
00042970 30 34 30 34 30 34 30 30-30 34 30 34 30 34 66 62 | 04040400040404fb  
00042980 66 62 30 34 30 34 62 63-30 34 30 34 30 34 30 34 | fb0404bc04040404  
00042990 30 34 30 34 30 34 34 34-30 34 30 34 30 34 30 34 | 0404044404040404  
000429a0 30 34 30 34 30 34 30 34-30 34 30 34 30 34 30 34 | 0404040404040404  
000429b0 30 34 30 34 30 34 30 34-30 34 30 34 30 34 30 34 | 0404040404040404  
000429c0 30 34 30 34 30 34 30 34-30 34 30 34 30 34 30 34 | 0404040404040404  
000429d0 30 34 30 34 30 34 30 34-30 34 30 34 30 34 65 63 | 04040404040404ec  
000429e0 30 34 30 34 30 34 30 61-31 62 62 65 30 61 30 34 | 0404040a1bbe0a04  
000429f0 62 30 30 64 63 39 32 35-62 63 30 35 34 38 63 39 | b00dc925bc0548c9  
00042a00 32 35 35 30 36 63 36 64-37 37 32 34 37 34 37 36 | 25506c6d77247476  
00042a10 36 62 36 33 37 36 36 35-36 39 32 34 36 37 36 35 | 6b63766569246765  
00042a20 36 61 36 61 36 62 37 30-32 34 36 36 36 31 32 34 | 6a6a6b7024666124  
00042a30 37 36 37 31 36 61 32 34-36 64 36 61 32 34 34 30 | 76716a246d6a2440
```

Other examples:

- CozyDuke
 - Twitter
- OSX.Flashback
 - Twitter
- Downloader.Sninfs
 - Tumblr

3rd party services as exfiltration channels

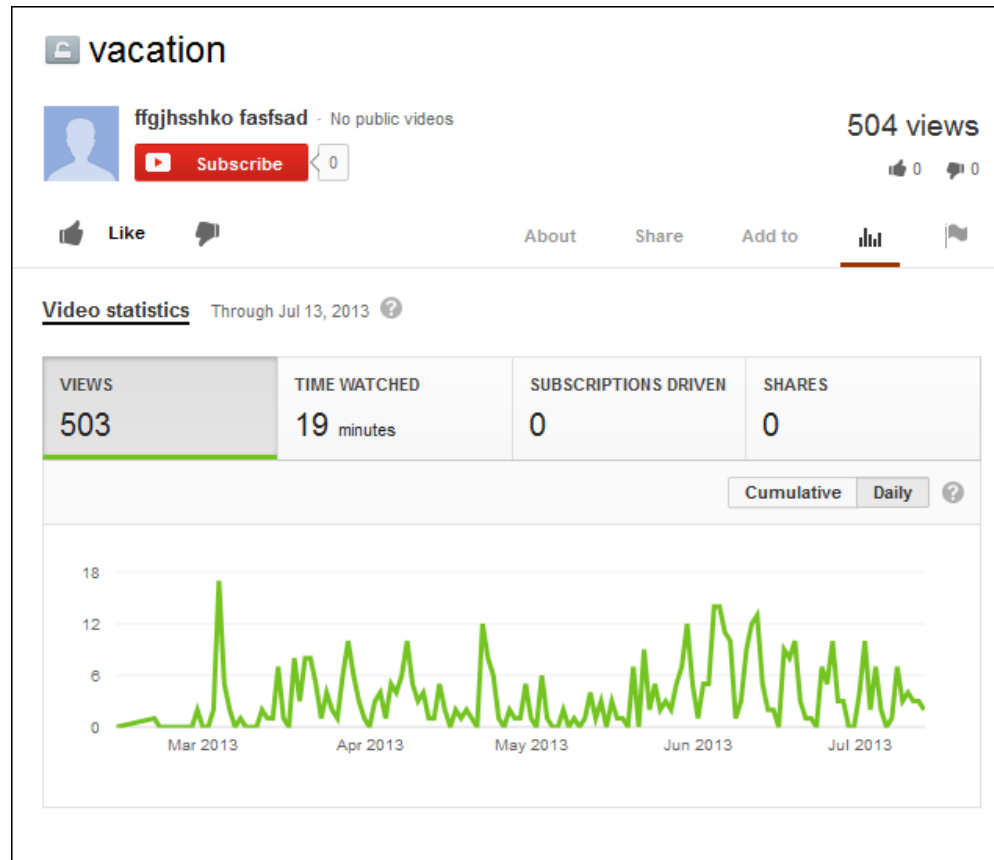
- CozyDuke uses HTTP(S) for C&C but often Microsoft OneDrive for exfiltration
- HammerDuke uses Twitter for C&C but often Microsoft OneDrive for exfiltration

Recap

- Use cases:
 - For proxying
 - For establishing a primary C&C channel
 - As a primary C&C channel
 - As a backup C&C channel
 - As an exfiltration channel
 - Combinations of the above
- Examples & references in the paper!

Opportunity 1:
**Don't monitor the victims,
monitor the attackers!**

Opportunity 2: Statistics!



Opportunity 3: History!

“Since every response is stored as a posting in the newsgroup, it was possible for Symantec to track the activity of the Trojan in detail. An even more useful feature of the newsgroup is the version control incorporated into pages.”

<http://www.symantec.com/connect/blogs/google-groups-trojan>

Opportunity 4: Service provider God-mode!

“CloudMe has shared a great deal of log information related to this attack. These indicate that there are many other accounts (over 100) likely related to this attack system.”

http://dc.bluecoat.com/Inception_Framework

Recap

- Challenges
 - No network-level detection & blocking
 - No netflow, PCAPs, logs
 - Takedowns?
 - Sinkholing?
- Opportunities
 - Monitor the attackers!
 - Statistics!
 - History!
 - God-mode!

Conclusions

- Not a new thing – but we've had it easy so far
- New challenges but also new opportunities
- Something to take into account when designing defenses
- Deserves more attention & research

C&C-as-a-Service

Abusing third-party web services as C&C channels

@lehtior2