Flashback OS X Malware

Broderick Ian Aquilino – September 27, 2012
Agenda

• Infection Vector
• Installation
• Main Binary
  • C&C Servers
  • **Payload**
• Remaining Binaries
  • Filter/Loader Binary
  • LaunchAgent Binary

September 27, 2012
Infection Summary

Hacked Website → Distribution Website

Installer → Main Binary

Filter / Loader → Launch Agent
Infection Vector

- Hacked Website
- Distribution Website
- Installer
- Main Binary
- Launch Agent
- Filter / Loader
Infection Vector
Infection Vector
Infection Vector

Do you want content signed by “Apple Inc.” to have access to your computer?

The digital signature of this certificate could not be verified. Do not trust this certificate if you do not know who issued it.

Always trust “Apple Inc.”

Apple Inc.

Self-signed root certificate
Expires: Monday, May 7, 2012 2:02:02 AM Singapore Time

This root certificate is not trusted

Details
Infection Vector

- CVE-2008-5353
- CVE-2011-3544
- CVE-2012-0507
Main Binary

- Hacked Website
- Distribution Website
- Installer
- Launch Agent
- Filter / Loader

Main Binary
Main Binary: Update Server

- Creates a thread that connects to a set of C&C servers to download updates every 3670 secs (>1hr)

- Hardcoded list
- Returned by a third party server
- Generated list based on date (*new variants only*)
Main Binary: Update Program

• Response:
  • %marker1%encoded_VM_program%marker2%
    %encoded_MD5_RSA_signature%marker3%

• Log SHA1 of VM program
  • {HOME}/Library/Logs/swlog
  • {HOME}/Library/Logs/vmLog
Main Binary: Payload C&C (Newer Variants)

• Same thread will also connect to another set of C&C servers

• This time to select a server for executing the payload

Updateable list (Entry ID 3035856777)  Hardcoded list (Entry ID 2522550406)  Generated list based on date
• Selected only once - when binary is loaded
Main Binary: Payload C&C Validation

- Response
  - `%SHA1_string_of_server_name% | %MD5_RSA_signature%

- Use (2nd – old variant / 1st – new variant) host in hardcoded list as default server
- Use “localhost” if configuration entry does not exists (new variant only)
Main Binary: Payload (Old Variants)

Outbound
- CFWriteStreamWrite
- send

Inbound
- CFReadStreamRead
- recv
Main Binary: Payload (Old Variants)

Outbound

To Google?

Pls reply in a format that is parseable

Inbound

Contains target string?

Inject content
Demo
Main Binary: Payload (Newer Variants)

- Command and Control
- Destination
- Other Modules
- Browser
  - CFWriteStreamWrite
  - CFReadStreamRead
- Google
Main Binary: Payload (Newer) -> Search

- Command and Control
- CFReadStreamRead
- CFWriteStreamWrite
- Other Modules
- CFReadStreamRead
- Google
- Destination

Keyword and other info
Main Binary: Payload (Newer) -> Search

Browser

CFWriteStreamWrite

CFReadStreamRead

Other Modules

Command and Control

Redirection data and/or other commands

Destination

Google

Original search request

Google search result
Main Binary: Payload (Newer) -> Click

Command and Control

CFWriteStreamWrite

Browser

Other Modules

CFReadStreamRead

Tracking info

Redirection info

Destination

Google

Redirection info
Main Binary: Payload (Newer) -> Click

- Google return the request in the response
Main Binary: Payload (Newer) -> Click

Command and Control

Destination

Browser
  CFWriteStreamWrite
  Request to new destination

Other Modules
  Redirection script
  CFReadStreamReadStream

Google

September 27, 2012
Main Binary: Payload (Newer) -> Click

Command and Control

Destination

Browser
CFWriteStreamWrite
Request with modified referrer

Other Modules

CFReadStreamRead

Google
Demo
Filter/Loader Binary

- Hacked Website
- Distribution Website
- Installer
- Main Binary
- Launch Agent
- Filter / Loader
Filter/Loader Binary

safari_check:

    movzx    eax, byte ptr [rbx]
    cmp      al, 53h    ; 'S'
    jnz      short webpo_check
    cmp      byte ptr [rbx+1], 61h    ; 'a'
    jnz      short rightprocess_check
    cmp      byte ptr [rbx+2], 66h    ; 'f'
    jnz      short rightprocess_check
    cmp      byte ptr [rbx+3], 61h    ; 'a'
    jnz      short rightprocess_check
    cmp      byte ptr [rbx+4], 72h    ; 'r'
    jnz      short rightprocess_check
    mov      cs:_rightProcess, OFFDABEh
    jmp      short rightprocess_check
Filter/Loader Binary

```assembly
webpo_check:
    cmp    al, 57h ; 'W'
    jnz    short righprocess_check
    cmp    byte ptr [rbx+1], 65h ; 'e'
    jnz    short righprocess_check
    cmp    byte ptr [rbx+2], 62h ; 'b'
    jnz    short righprocess_check
    cmp    byte ptr [rbx+3], 50h ; 'P'
    jnz    short righprocess_check
    cmp    byte ptr [rbx+4], 6FH ; 'o'
    jnz    short righprocess_check
    mov    cs:_rightProcess, 0FFDAFEh
    jmp    short loc_BBB
```
LaunchAgent Binary

- Hacked Website
- Distribution Website
- Installer
- Main Binary
- Filter / Loader
- Launch Agent
LaunchAgent Binary

- Stand-alone light version of the updater module found in the main binary
- Uses different set of C&C servers
- Similar server validation process
- Logs CRC32 of the update/installation program
  - /tmp/.%crc32_of_VM_program%
- Have it’s own instruction set
LaunchAgent Binary - Recent Variant
LaunchAgent Binary - Recent Variant

- Taken over the responsibility of installing the malware

September 27, 2012
Thank you! Please check out the conference paper for more details.

broderick.aquilino@f-secure.com