



# Flashback OS X Malware

Broderick Ian Aquilino – September 27, 2012

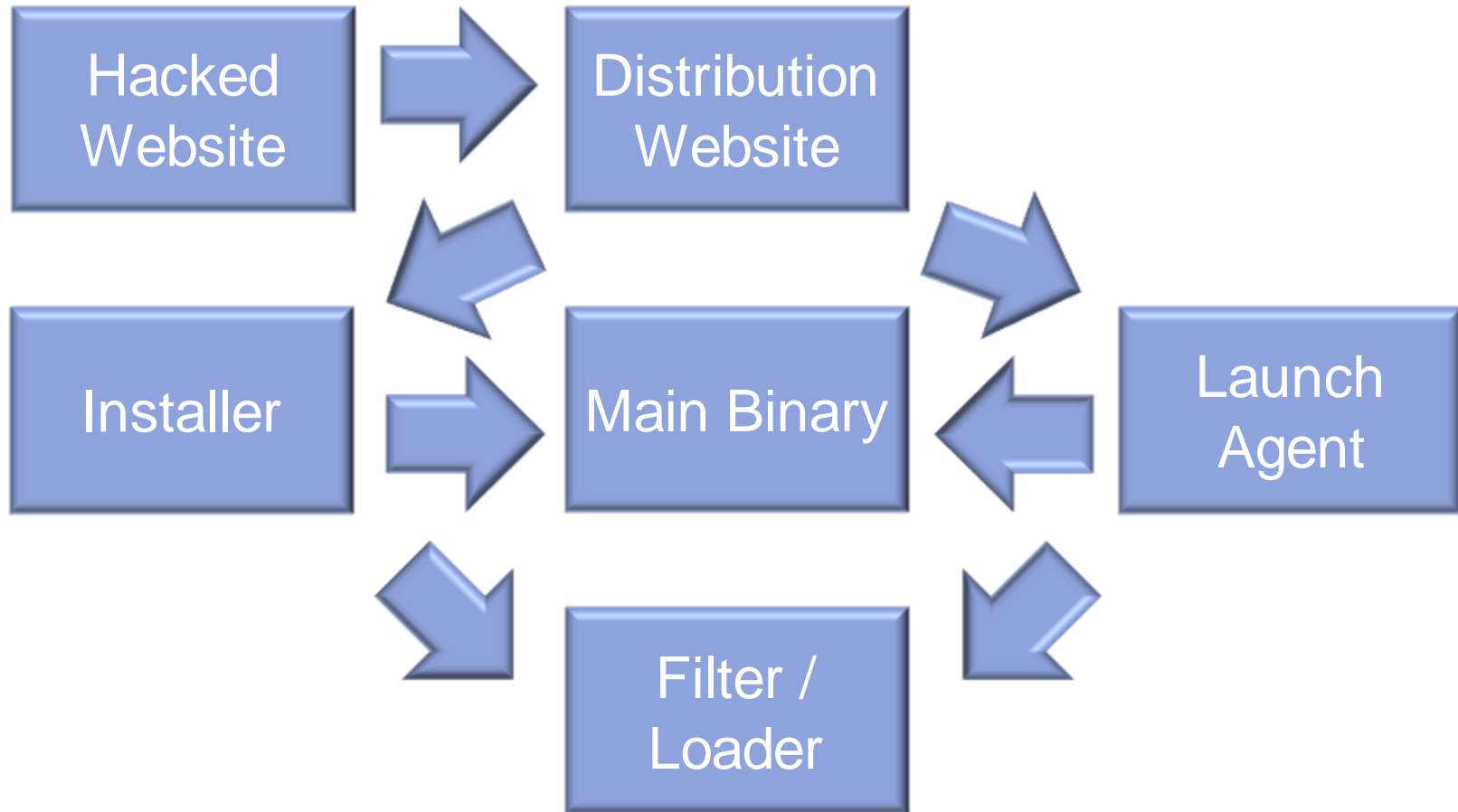
# Agenda

---

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

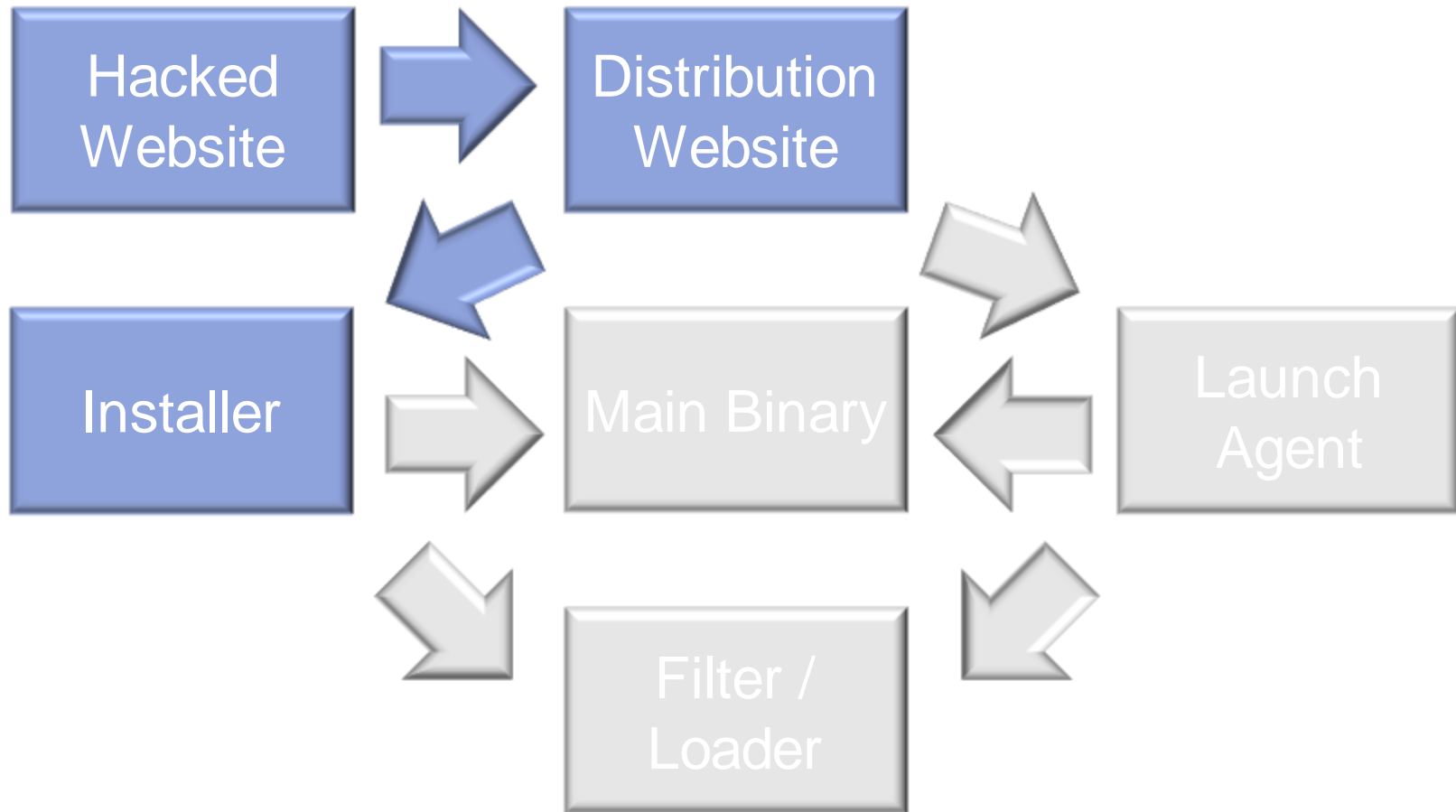
# Infection Summary

---



# Infection Vector

---





# Infection Vector



# Infection Vector



# Infection Vector

---

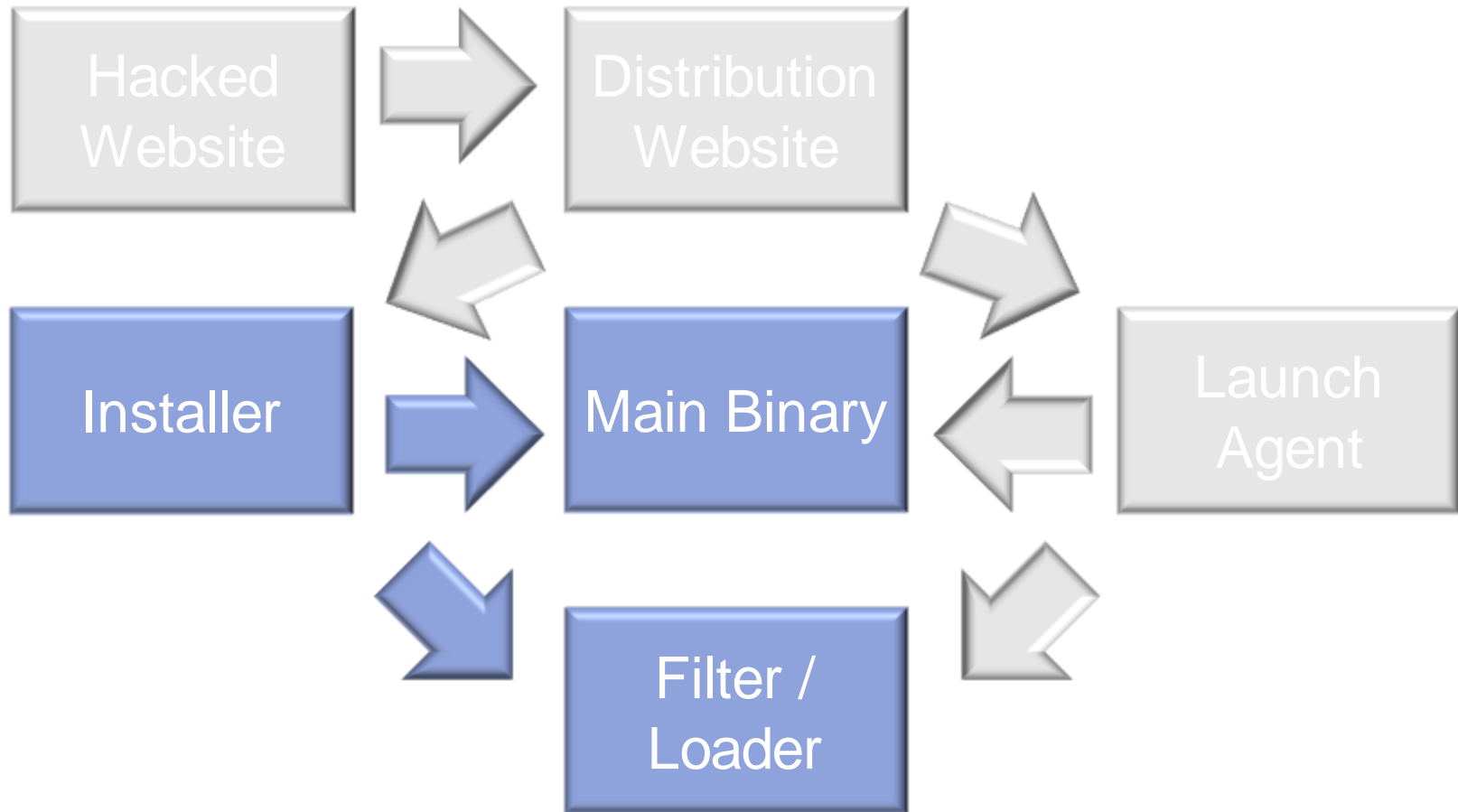
- CVE-2008-5353
- CVE-2011-3544
- **CVE-2012-0507**





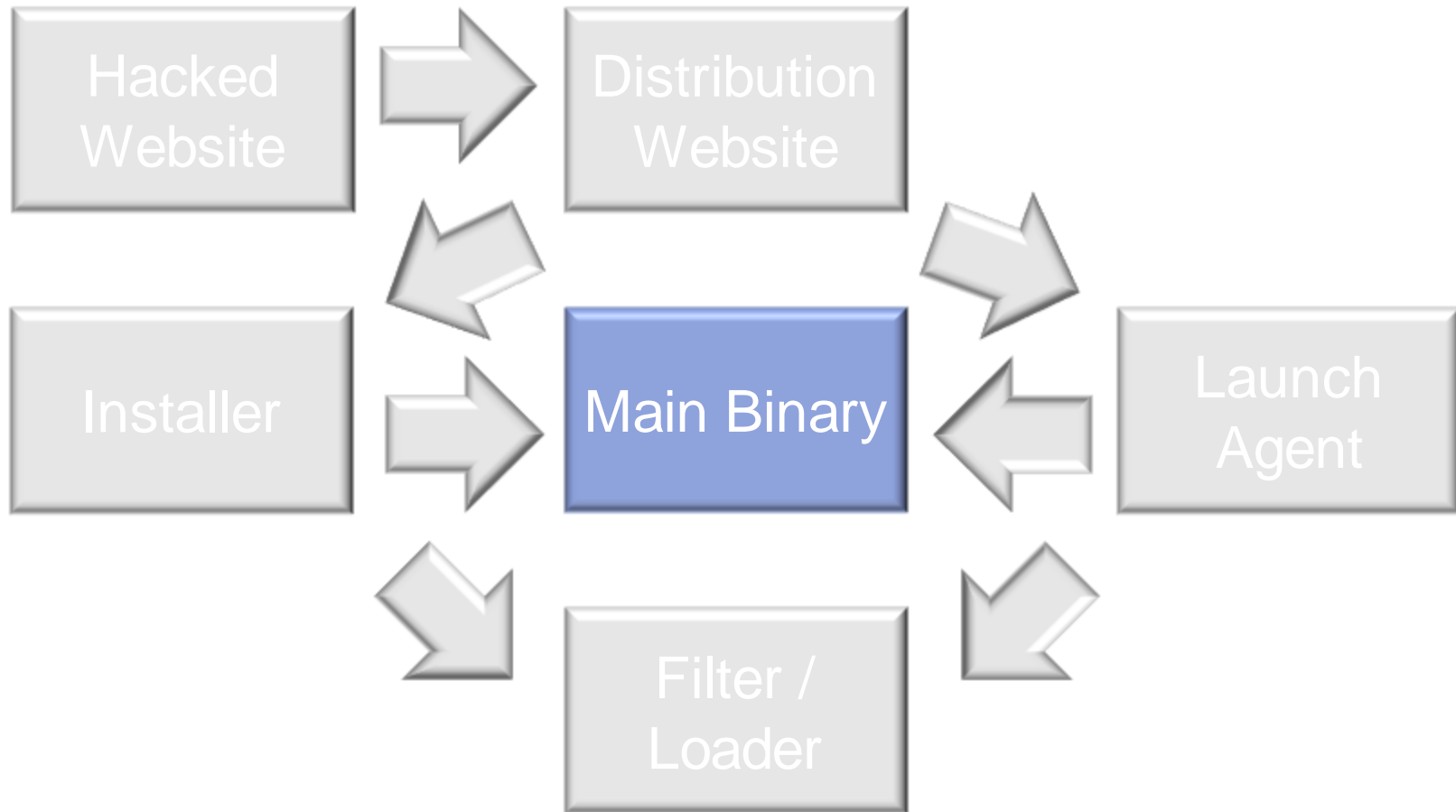
# Installation

---



# 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)



# Main Binary: Update Program

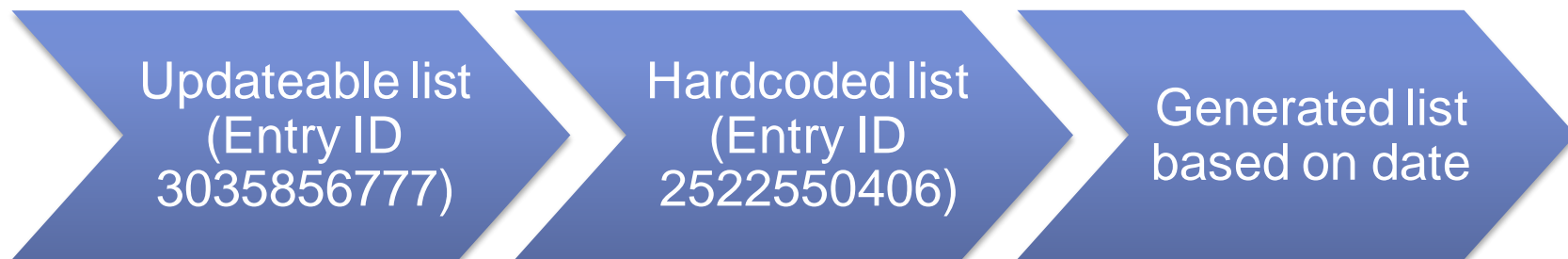
---

- 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)

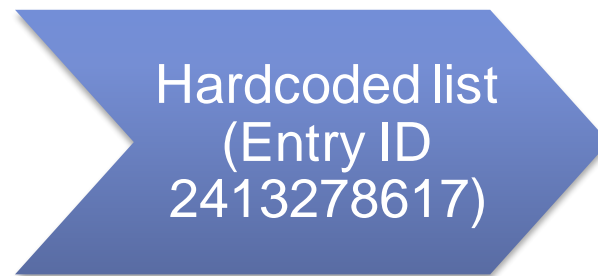
---

- Same thread will also connect to another set of C&C servers
- This time to select a server for executing the payload



# Main Binary: Payload C&C (Old Variants)

---



- Selected only once - when binary is loaded

# Main Binary: Payload C&C Validation

---

- Response
  - %SHA1\_string\_of\_server\_name% | %MD5\_RSA\_signature%
- Use (2<sup>nd</sup> – old variant / 1<sup>st</sup> – new variant) host in hardcoded list as default server
  - Use “localhost” if configuration entry does not exist (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

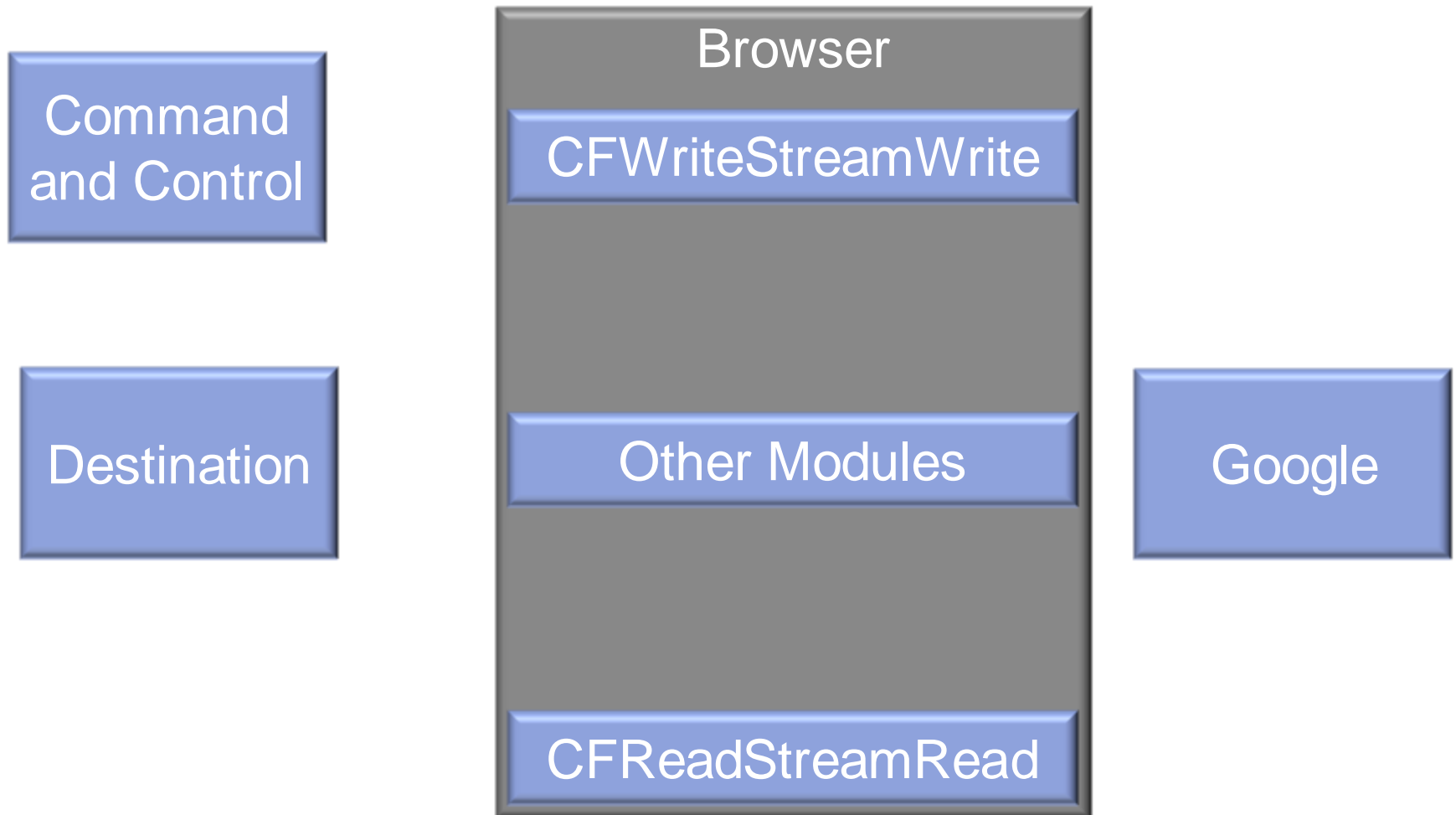
Contains target  
string?

Inject content

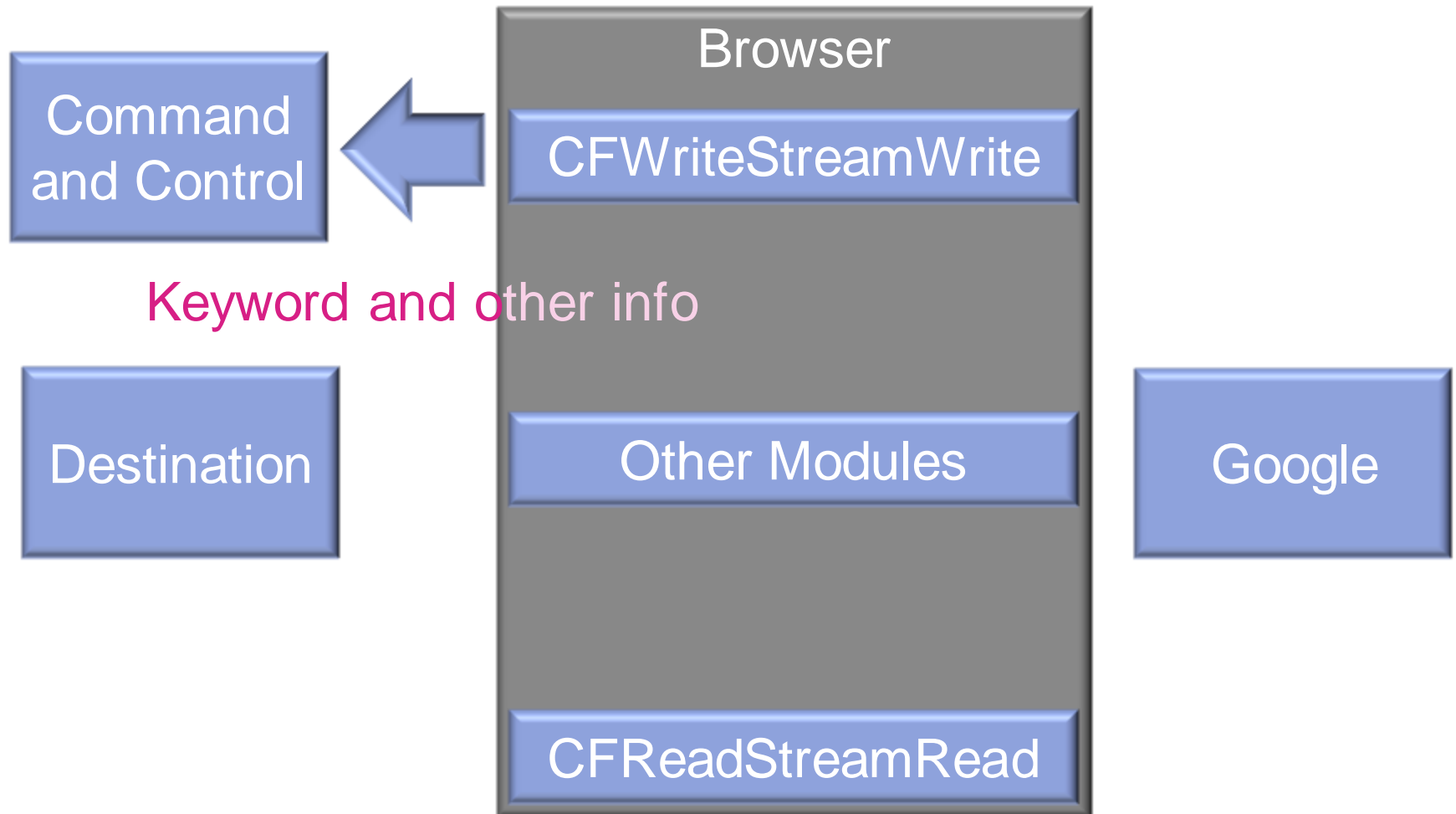
# Demo

# Main Binary: Payload (Newer Variants)

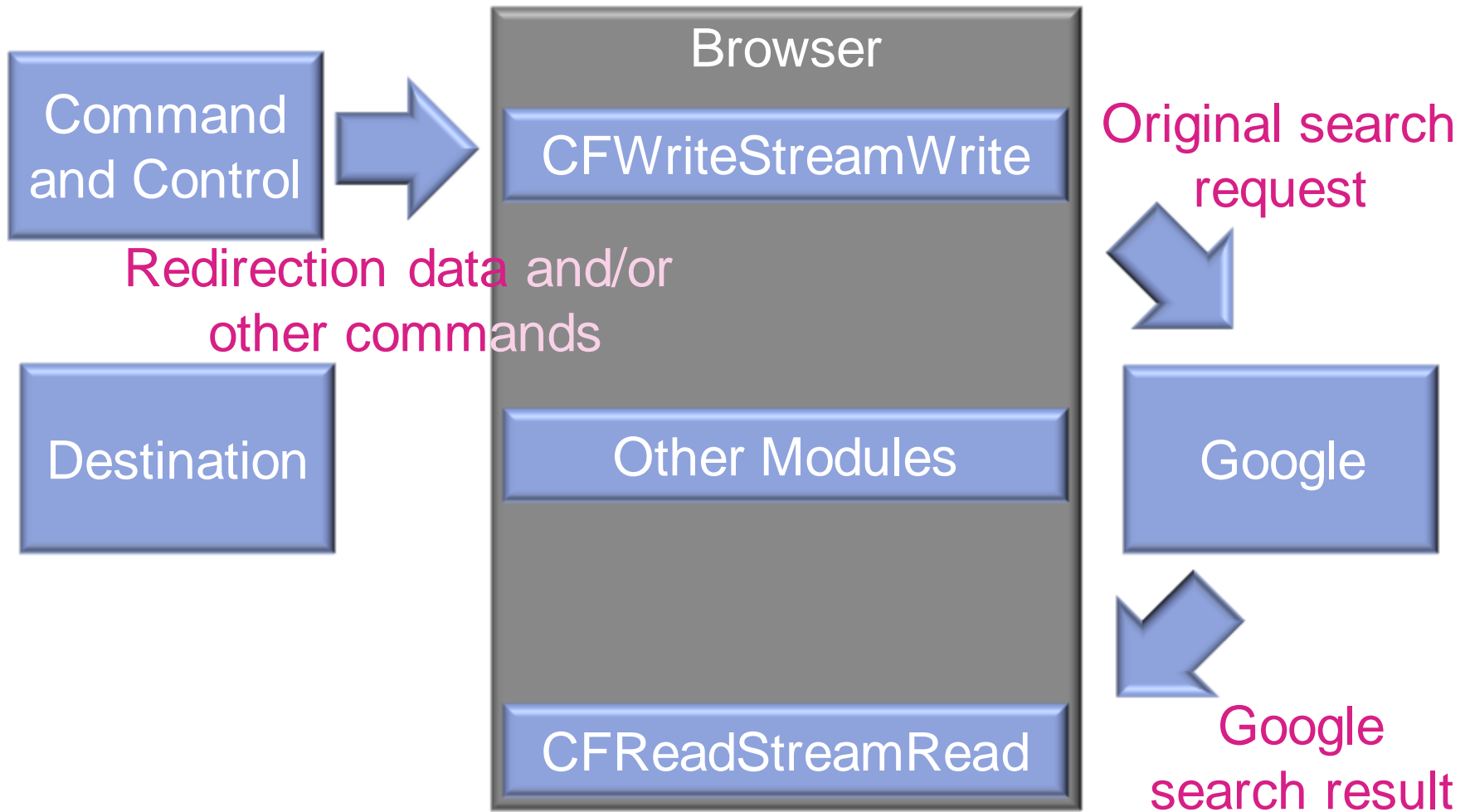
---



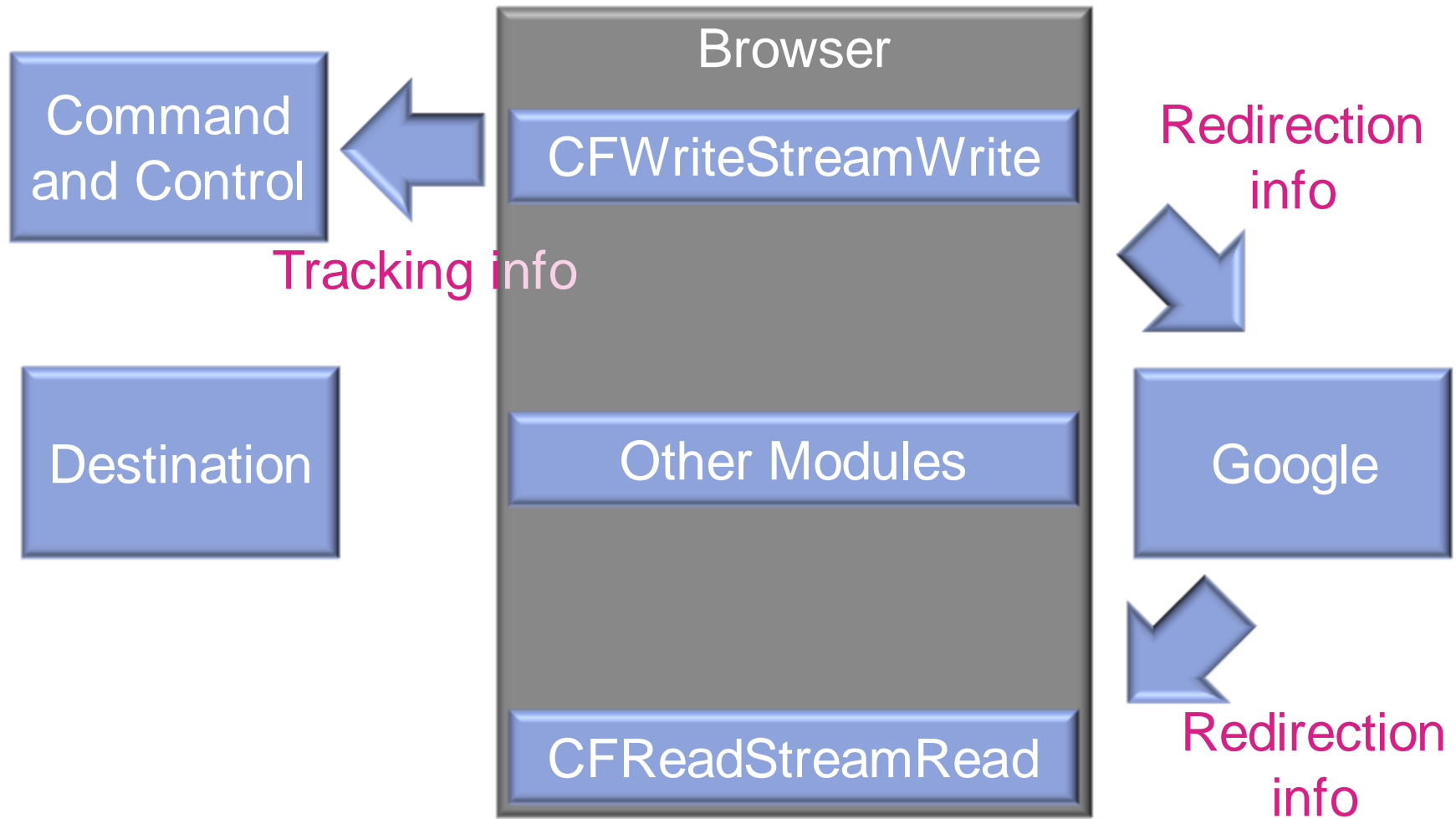
# Main Binary: Payload (Newer) -> Search



# Main Binary: Payload (Newer) -> Search

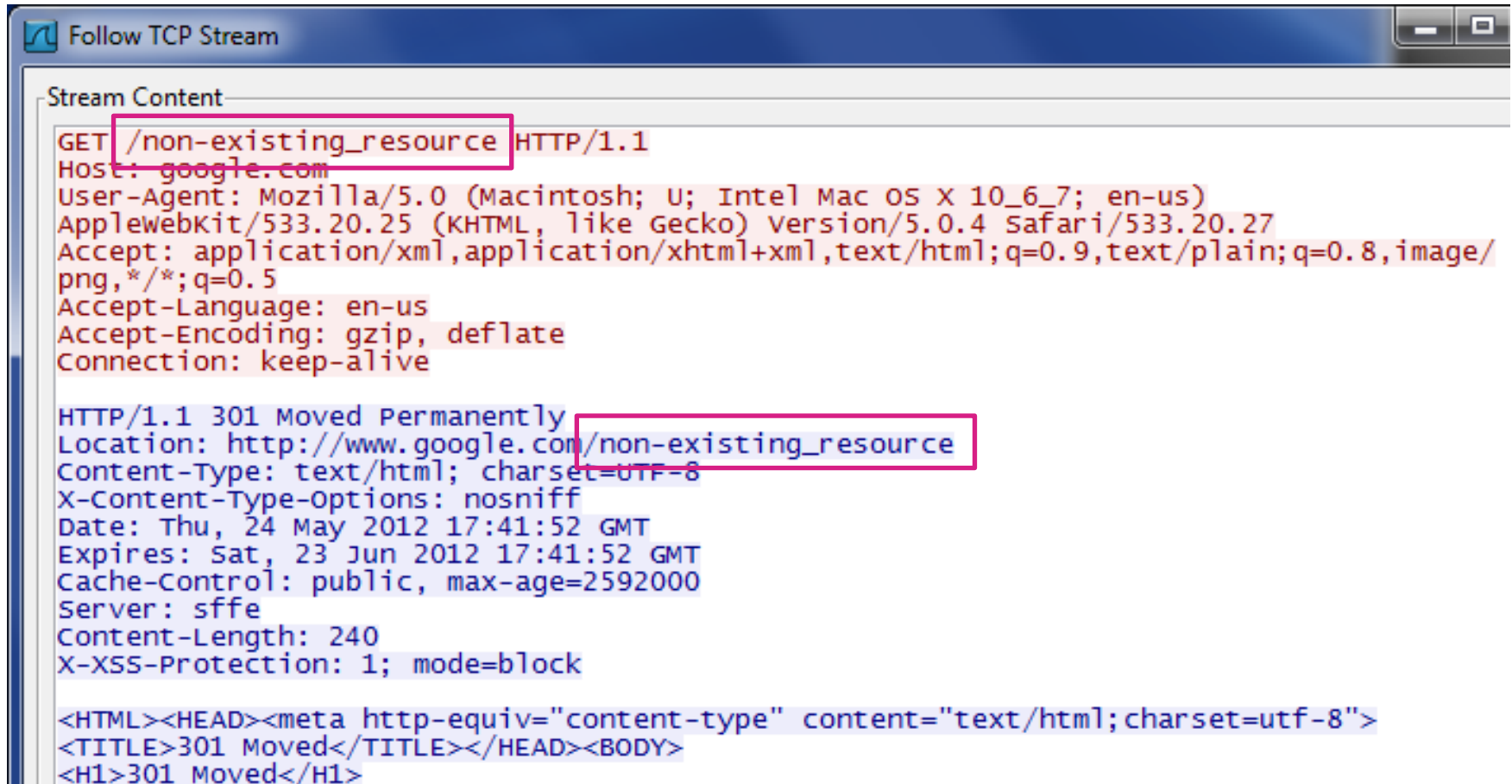


# Main Binary: Payload (Newer) -> Click



# Main Binary: Payload (Newer) -> Click

- Google return the request in the response



```
Follow TCP Stream

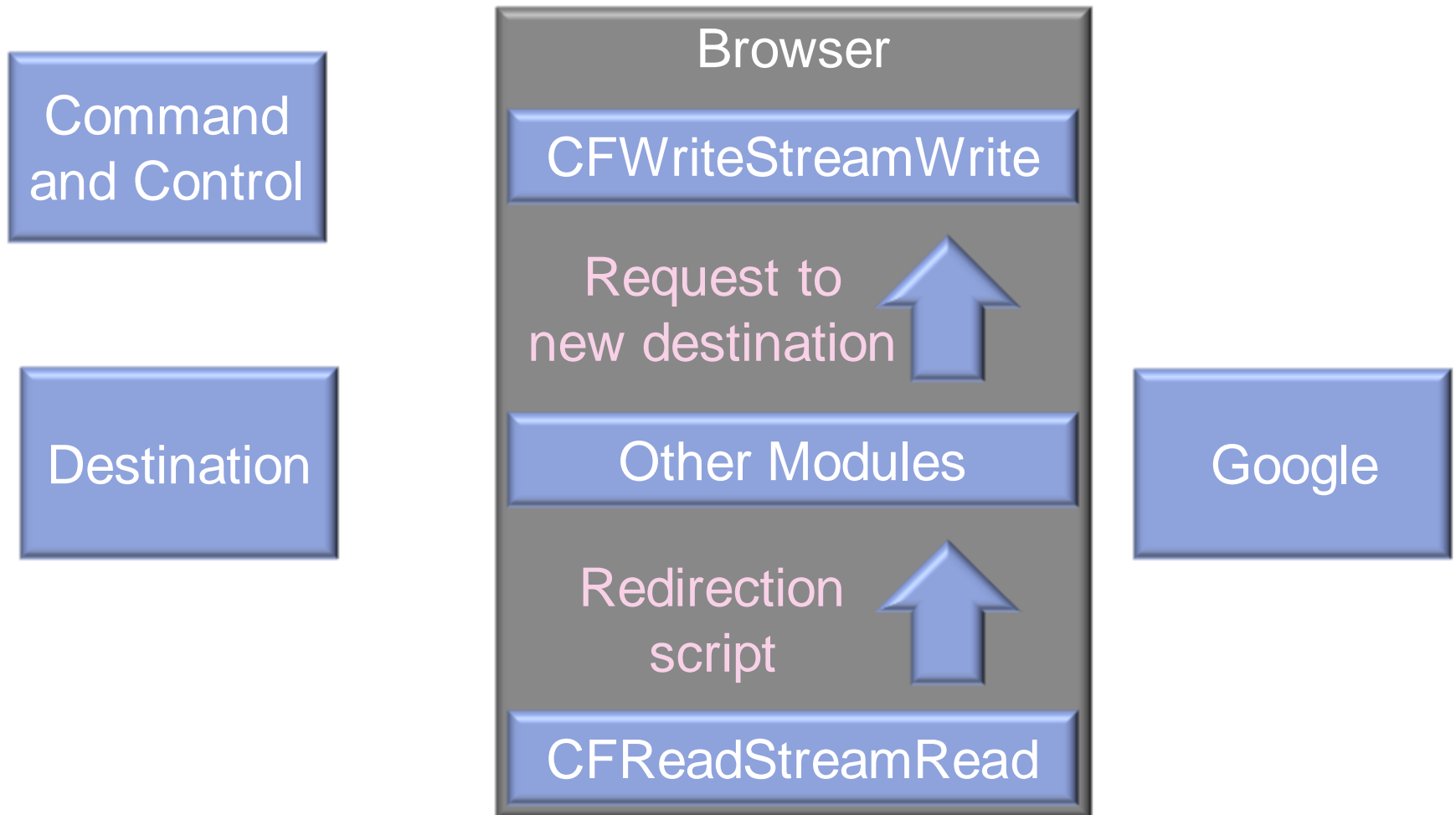
Stream Content

GET /non-existing_resource HTTP/1.1
Host: google.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_7; en-us)
AppleWebKit/533.20.25 (KHTML, like Gecko) version/5.0.4 Safari/533.20.27
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/
png,*/*;q=0.5
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/non-existing_resource
Content-Type: text/html; charset=UTF-8
X-Content-Type-Options: nosniff
Date: Thu, 24 May 2012 17:41:52 GMT
Expires: Sat, 23 Jun 2012 17:41:52 GMT
Cache-Control: public, max-age=2592000
Server: sffe
Content-Length: 240
X-XSS-Protection: 1; mode=block

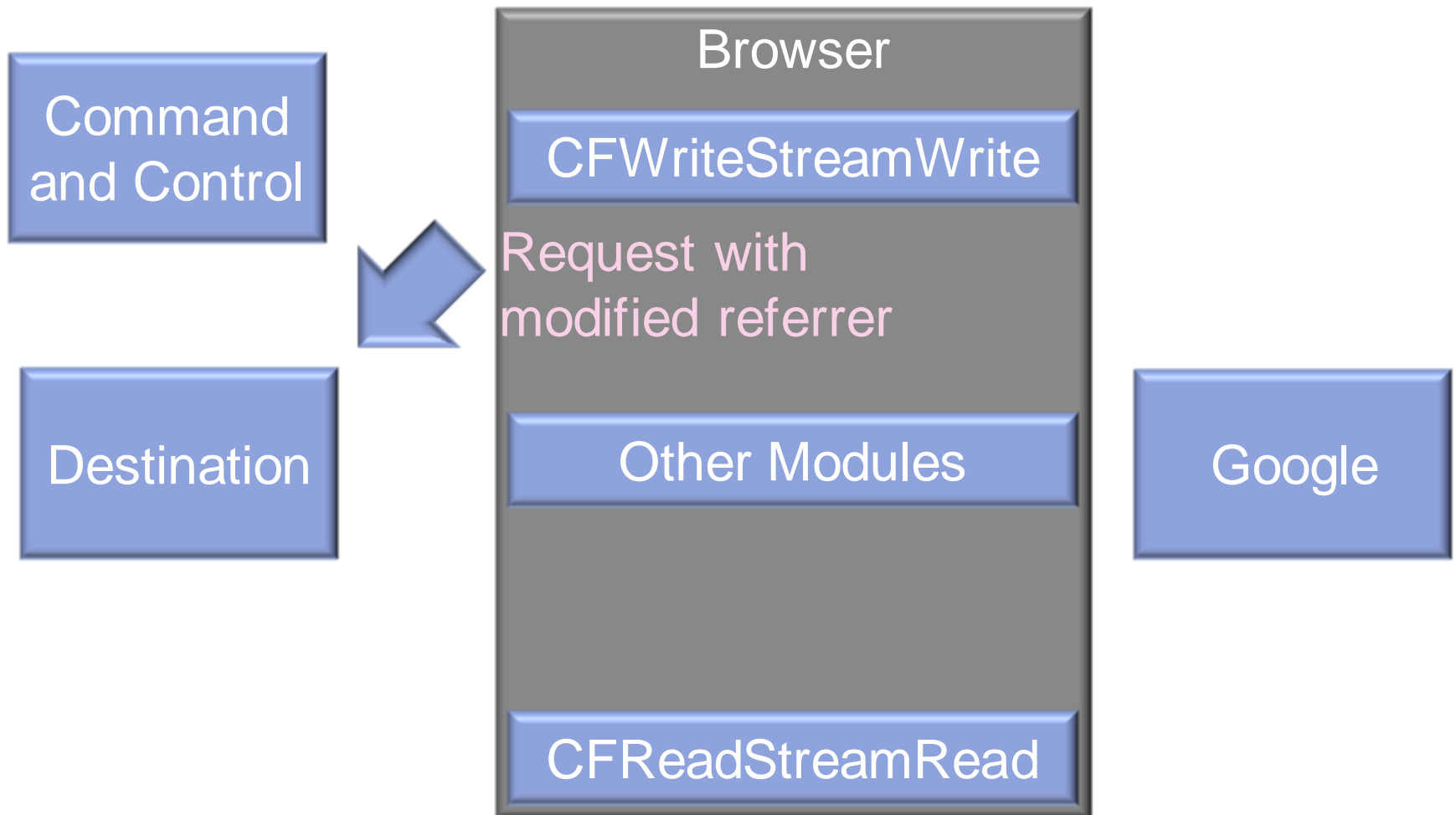
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
```

# Main Binary: Payload (Newer) -> Click





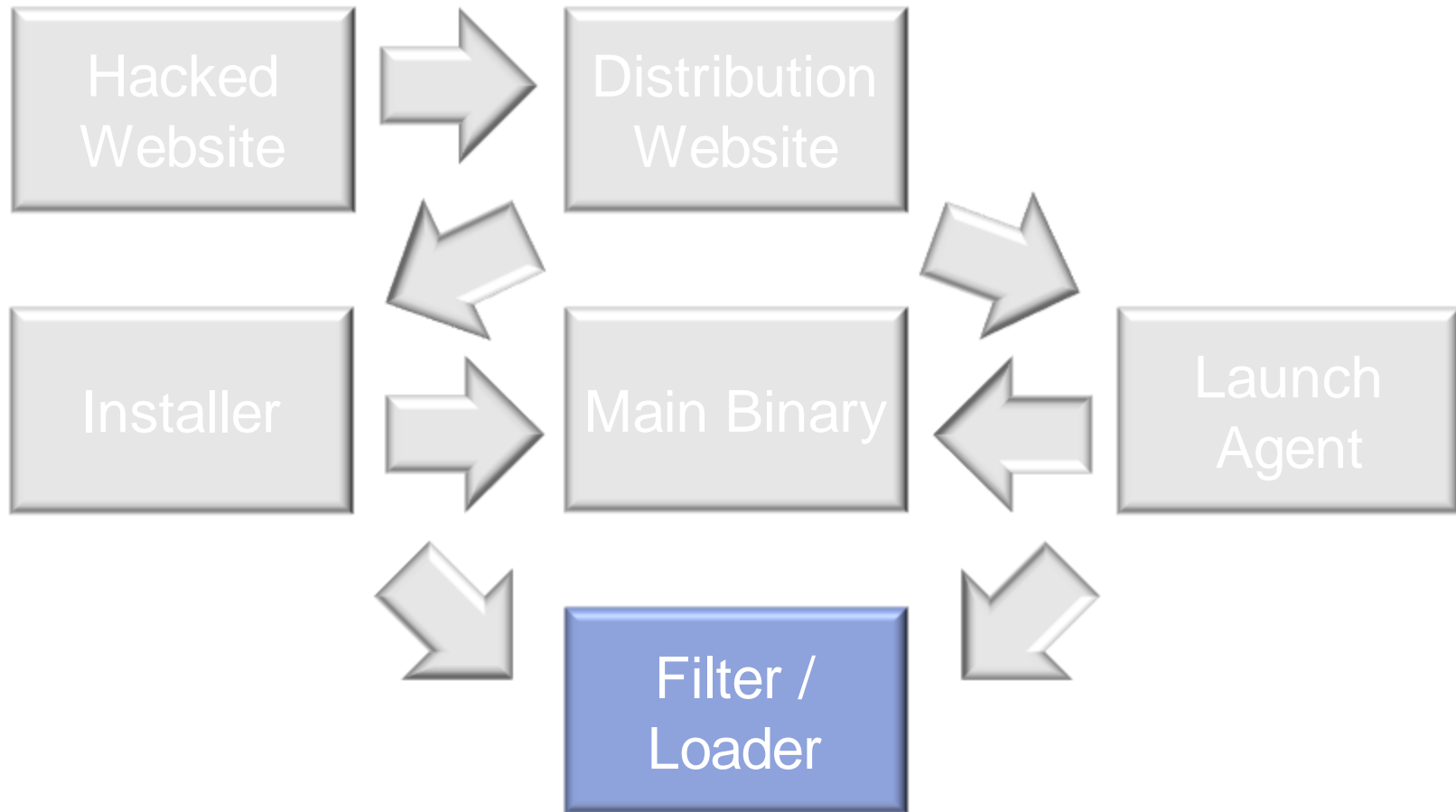
# Main Binary: Payload (Newer) -> Click



# Demo

# Filter/Loader Binary

---



# 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 righprocess_check
cmp      byte ptr [rbx+2], 66h ; 'f'
jnz      short righprocess_check
cmp      byte ptr [rbx+3], 61h ; 'a'
jnz      short righprocess_check
cmp      byte ptr [rbx+4], 72h ; 'r'
jnz      short righprocess_check
mov      cs:_rightProcess, 0FFDAFEh
jmp      short righprocess_check
```

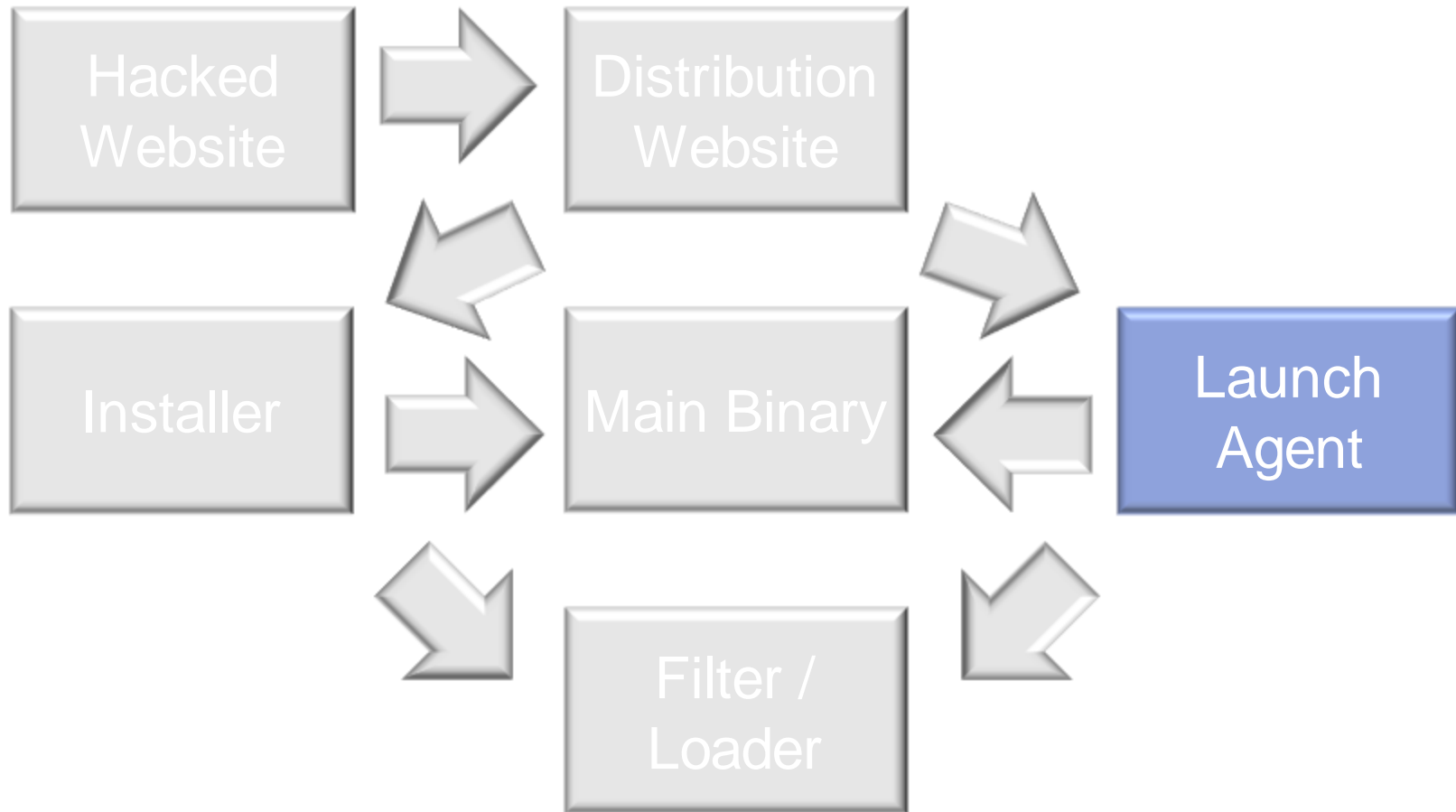
# Filter/Loader Binary

---

```
webpo_check:                                     ; CODE XREF:
        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

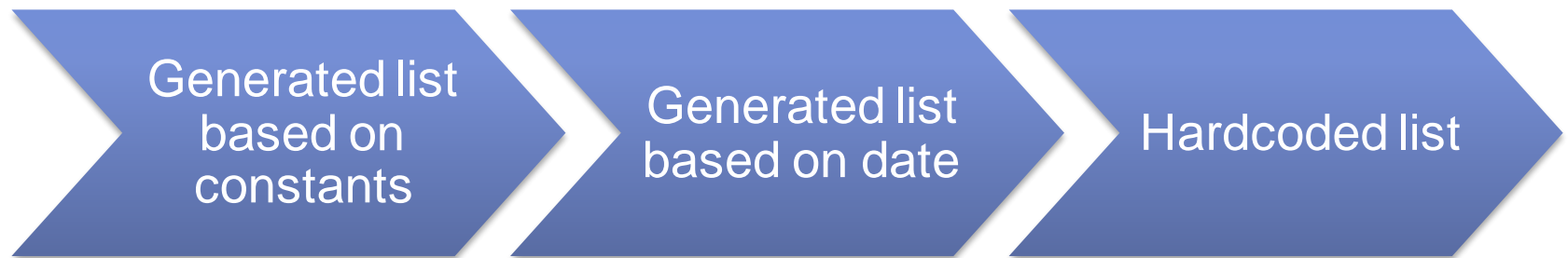
---



# LaunchAgent Binary

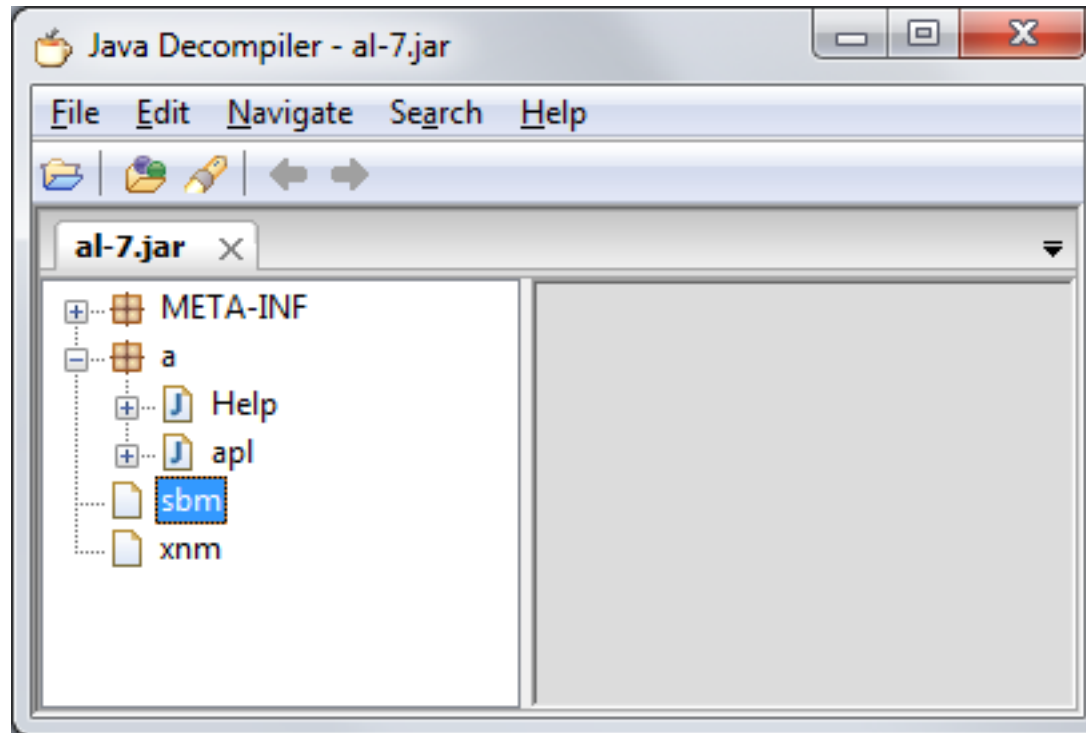
---

- Stand-alone light version of the updater module found in the main binary
- Uses different set of C&C servers



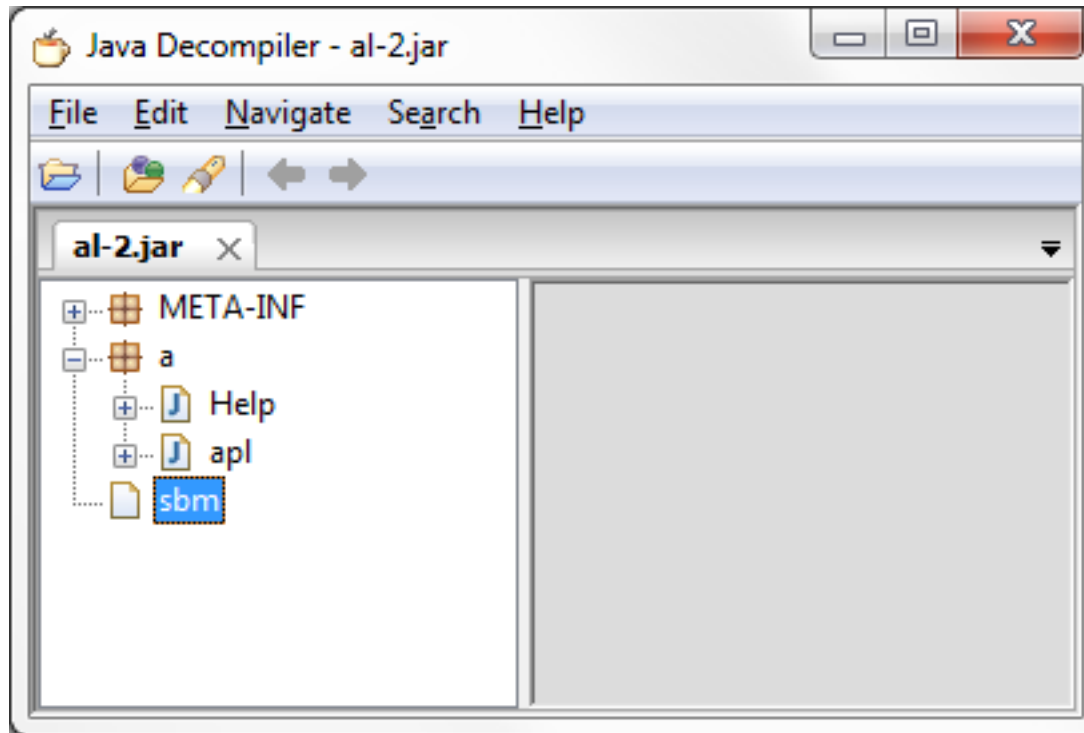
- Similar server validation process
- Logs CRC32 of the update/installation program
  - /tmp/.%crc32\_of\_VM\_program%
- Have it's own instruction set

# LaunchAgent Binary - Recent Variant





# LaunchAgent Binary - Recent Variant



- Taken over the responsibility of installing the malware

**Thank you! Please check out the conference paper for more details.**

broderick.aquilino@f-secure.com

