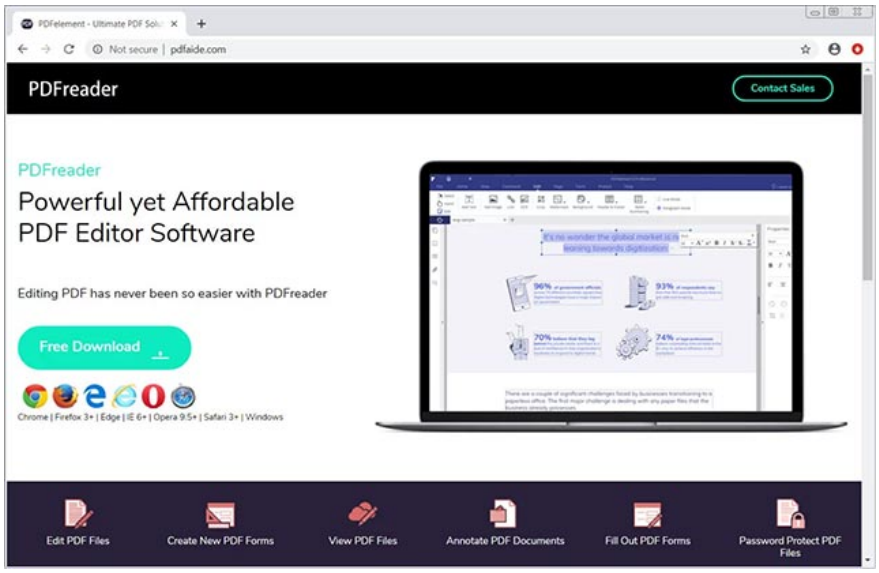
Facebook Ads Manager becomes a victim of Trojan information theft

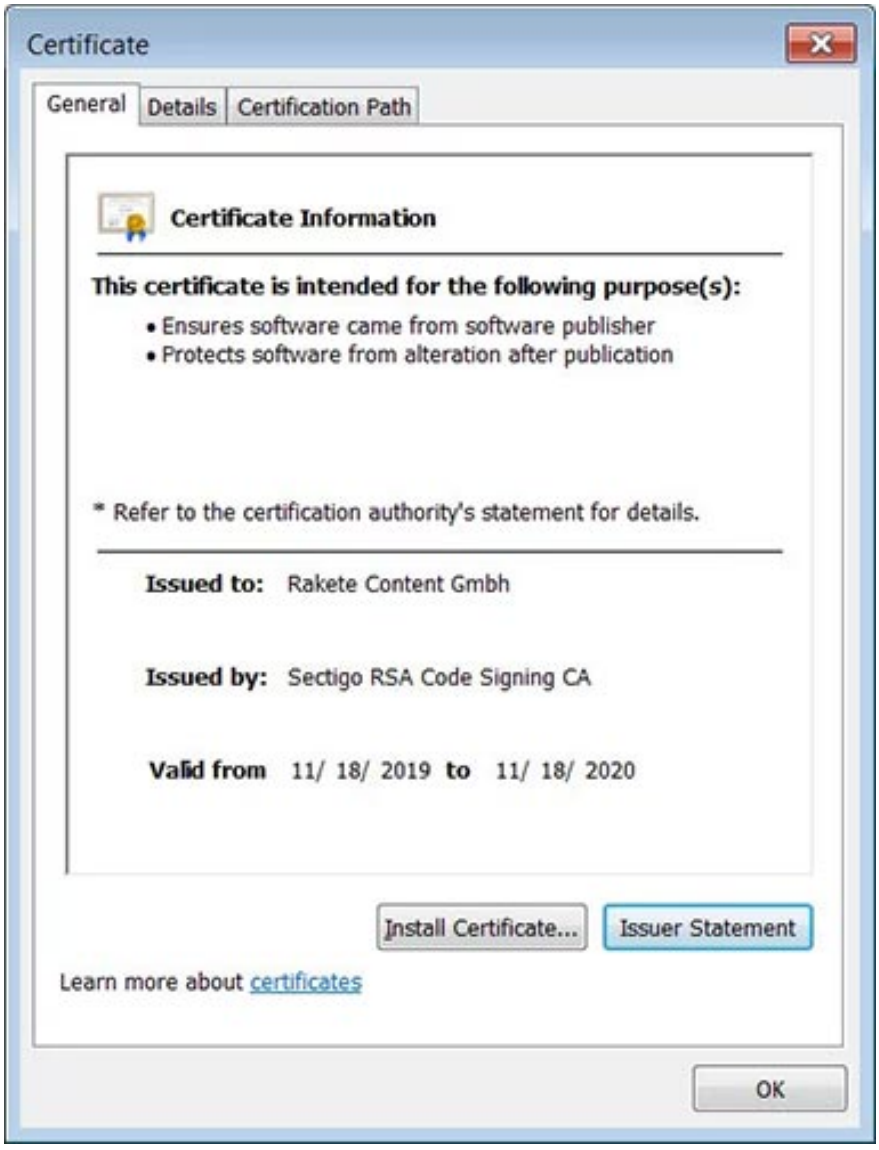
An unknown hacker group is distributing a Trojan stealing information disguised as a PDF reader that can copy Facebook session cookies

An unknown hacker group is distributing a Trojan stealing information disguised as a PDF reader that can copy Facebook session cookies as well as sensitive data from the Facebook Ads Manager. .

In particular, on November 30, MalwareHunterTeam found many websites distributing fake PDF editing program called 'PDFreader'. Executables distributed from this site are signed by a digital certificate issued by Sectigo for "Rakete Contenticineh".



VirusTotal then took over and identified this Trojan as Socelars, however it possessed some similarities with other Trojans, such as AdKoob and Stresspaint, in attempting to extract and steal Facebook data from Many different URLs. However, according to Vitali Kremez, the security expert who is responsible for analyzing this Trojan, there is not much similarity in code between this Socelars and other Trojans, so it can be confirmed that this is a specially developed Trojan. instead of upgrading from known Trojans.



Target Facebook Ads Manager

First, Socelars will attempt to steal Facebook cookie sessions from Chrome and Firefox by accessing the SQLite Cookies database. After the cookie is successfully retrieved, it will be used to connect various Facebook URLs where the information is extracted.

```
https://www.facebook.com/bookmarks/pages?ref_type=logout_gear

https://secure.facebook.com/settings

https://secure.facebook.com/ads/manager/account_settings/account_billing/
```

The account_billing URL will be used to extract the user's account and access_token, which will then be used in the Facebook Graph API call to steal data from the user's Ads Manager settings.

```
add     esp, 4Ch
mov     [ebp+var_17C], eax
mov     byte ptr [ebp+var_4], 13h
push    offset aHttpsGraph_fac ; "https://graph.facebook.com/v4.0/act_"
lea     ecx, [ebp+var_54]
call    sub_49DFE0
mov     [ebp+var_180], eax
mov     byte ptr [ebp+var_4], 14h
lea     ecx, [ebp+var_6C]
push    ecx
lea     ecx, [ebp+var_54]
call    sub_4B3E60
push    offset a?_reqnameAdacc ; "?_reqName=adaccount&_reqSrc=AdsPaymentM"...
lea     ecx, [ebp+var_54]
call    sub_4B3E80
lea     edx, [ebp+var_84]
push    edx
push    offset aAccess_token_0 ; "&access_token="
lea     eax, [ebp+var_28C]
push    eax
call    sub_4B4890
```

The call to the Facebook Graph API is as follows:

```
https://graph.facebook.com/v4.0/act_{account_id}?_reqName=adaccount&_reqSrc=Ads
```

Data that can be stolen includes session cookies, access tokens, account ids, promotional email addresses, related pages, credit card information (numbers, expiration dates), PayPal emails, balances. advertisements, spending limits, etc., are then compiled and sent to the attacker's Command & Control (C2) server.

More seriously, attackers can use these stolen Facebook cookies to access their accounts and use them to create their own malicious advertising campaigns.

This Trojan is silently executed and performs all its actions in the background, so users will not know that they have become victims of malicious code. Facebook has not yet commented on the incident.