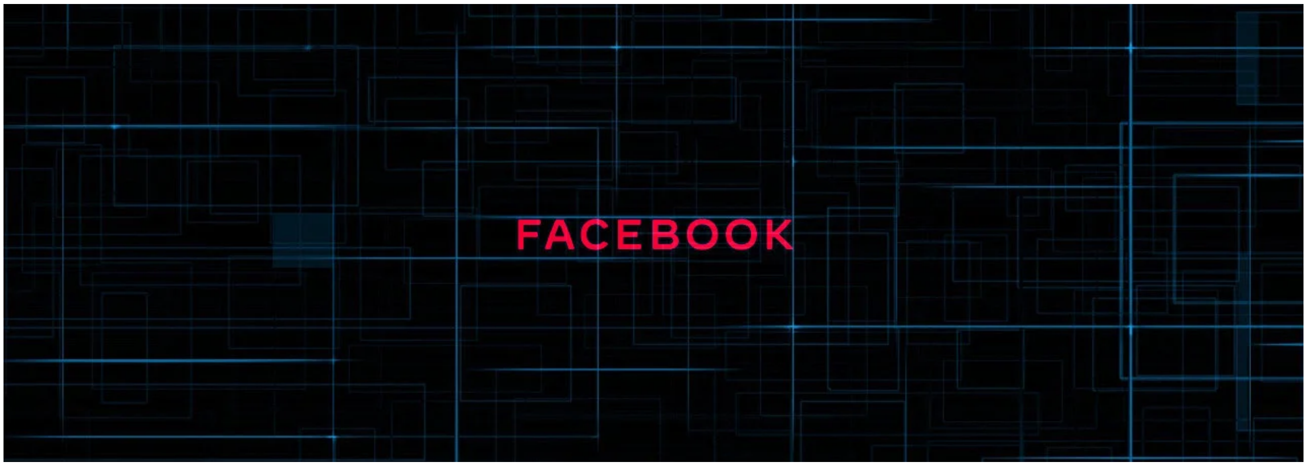
Facebook Ads Manager Targeted by New Info-Stealing Trojan

Lawrence Abrams

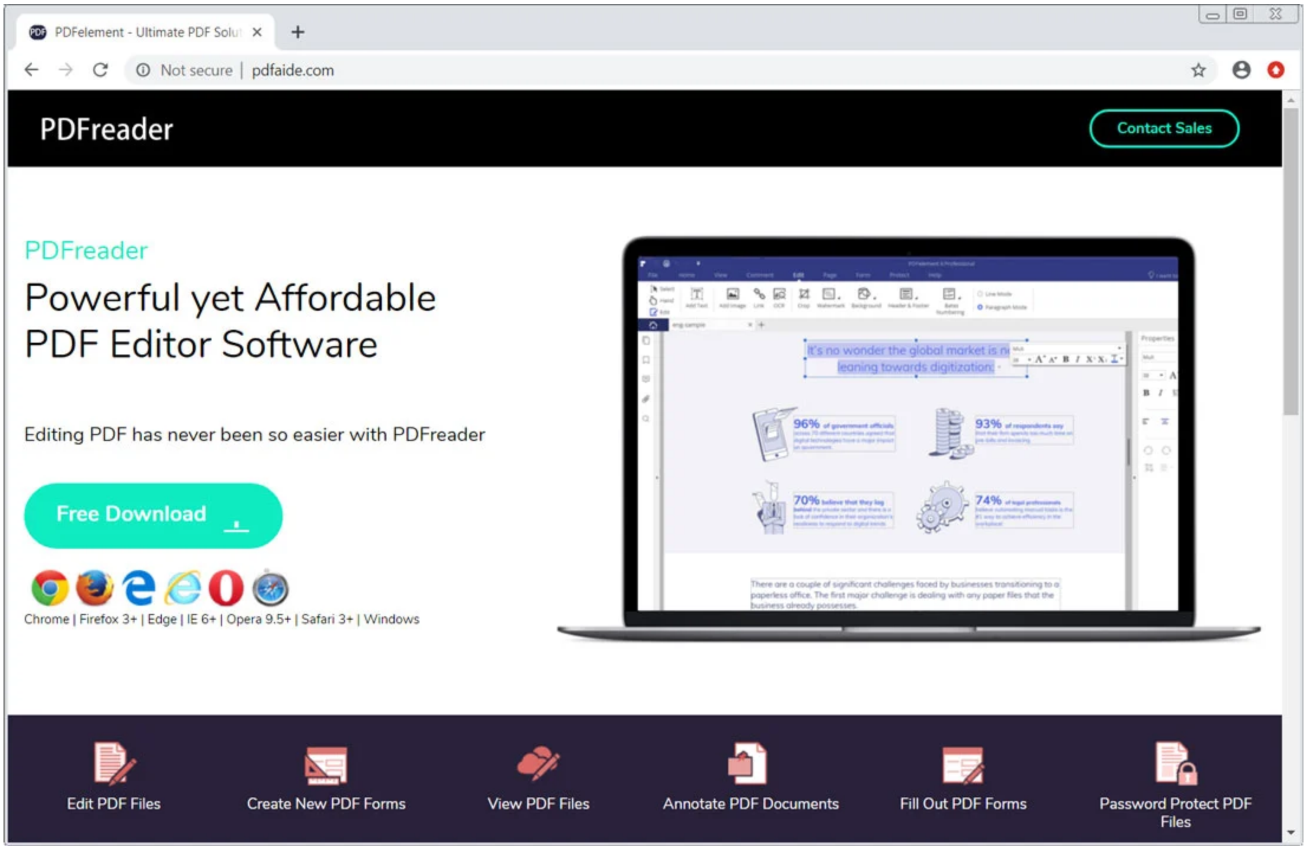
By
Lawrence Abrams

- December 2, 2019
- 05:24 PM
- 4



Attackers are distributing an information-stealing Trojan disguised as a PDF reader that steals Facebook and Amazon session cookies as well as sensitive data from the Facebook Ads Manager.

Over the weekend, MalwareHunterTeam found numerous sites distributing a fake PDF editing program called 'PDFreader'.



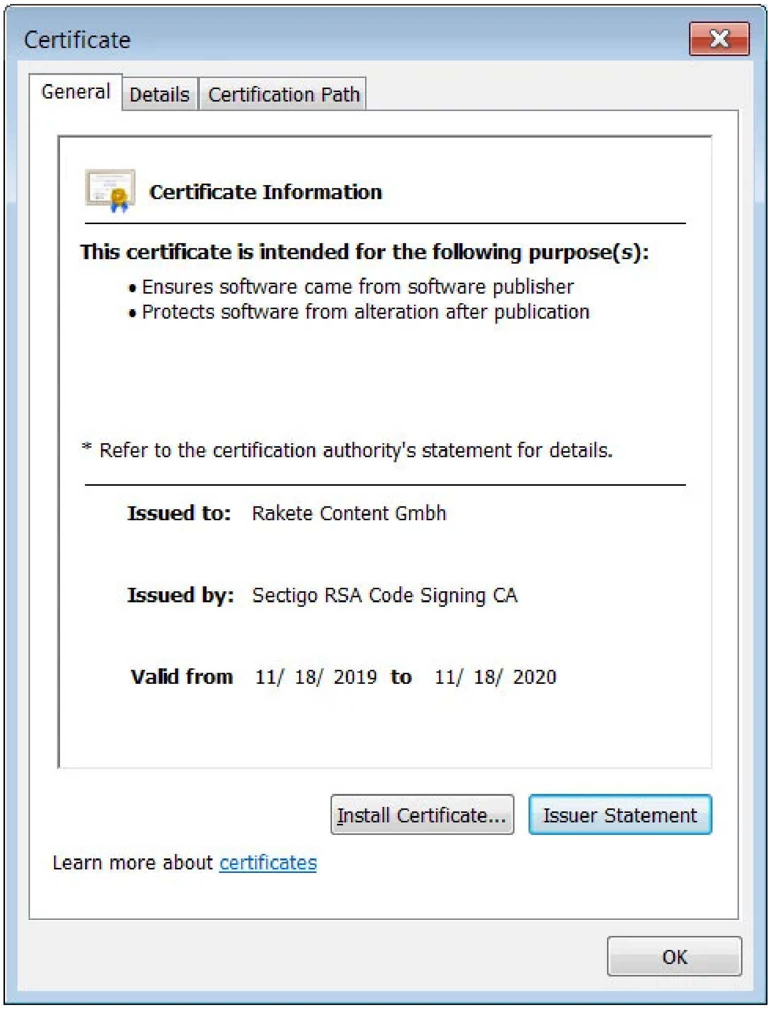
PDFreader

Powerful yet Affordable PDF Editor Software

Editing PDF has never been so easier with PDFreader

Site promoting PDFreader

The executables distributed from this site are signed by a digital certificate issued by Sectigo to "Rakete Content Gmbh".



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Rakete Content Gmbh

Issued by: Sectigo RSA Code Signing CA

Valid from 11/ 18/ 2019 **to** 11/ 18/ 2020

Digital signature

VirusTotal detects this Trojan as Socelars, but it also shares characteristics with other Trojans, such as AdKoob and Stresspaint, that also attempt to extract and steal Facebook data from various URLs.

According to Vitali Kremez, who analyzed this Trojan, there is not much code similarity between this Trojan and the others, so it may be inspired rather than evolved from previous infections.

"That tells it must be a newer (maybe inspired) variant or significantly improved one over the previous generation. I assess this might be only the beginning of the evolution of this type of malware targeting ad and social media providers," Kremez told BleepingCOmputer.com

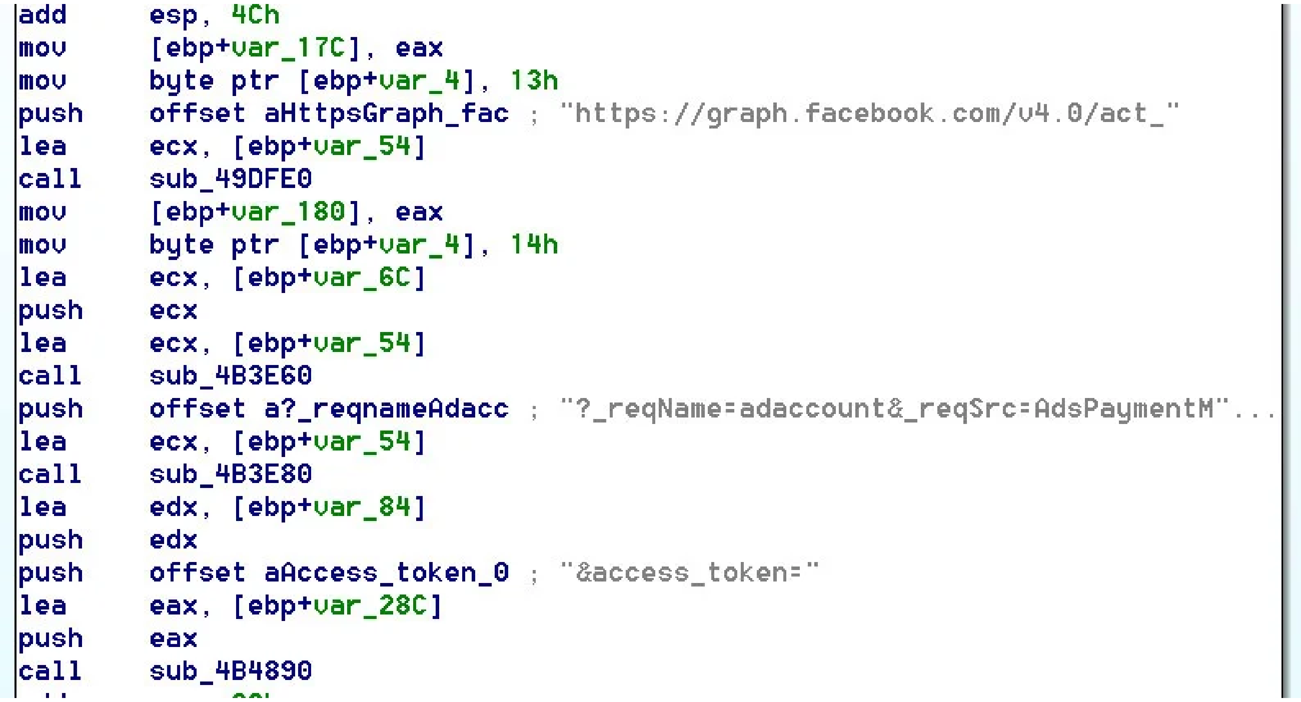
Targets Facebook Ads Manager

When launched, Kremez told BleepingComputer that the Trojan will first attempt to steal Facebook sessions cookies from Chrome and Firefox by accessing the Cookies SQLite database.

Once the cookie is retrieved, it will be used to connect a variety of Facebook URLs where 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_id and access_token, which will then be used in a 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
```

Facebook Graph API call
The graph API call used is below:

```
https://graph.facebook.com/v4.0/act_{account_id}?
_reqName=adaccount&_reqSrc=AdsPaymentMethodsDataLoader&fields=%5B%22all_payment_metho
```

The stolen data, which consists of session cookies, access tokens, account ids, advertising email address, associated pages, credit card info (number, expiration date), PayPal email, ad balances, spending limits, etc, is then compiled and sent to the attacker's Command & Control server.

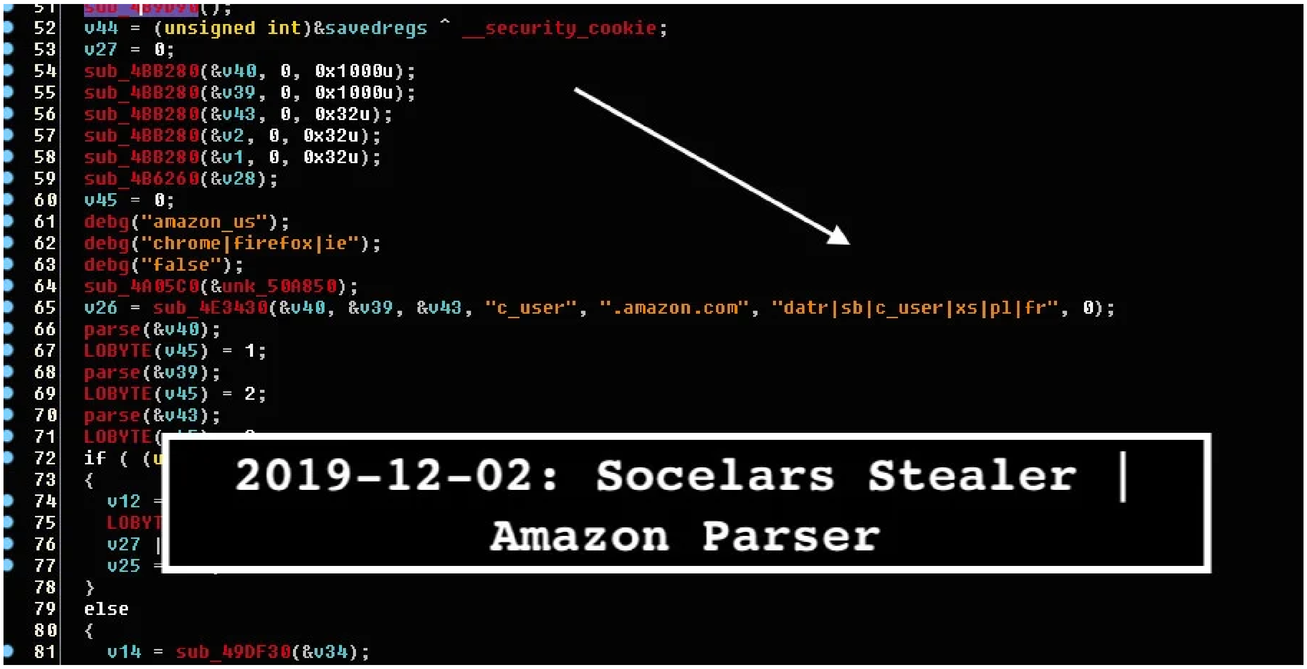
With the USA election season looming and state-sponsored actors abusing Facebook ads in the past, it is important for anyone running political campaigns to know that malware is targeting Facebook's ad infrastructure.

"Also, I think in light of the upcoming elections and intensified FB campaigns running political messages, this tool is almost like an espionage malware looking for possible political narratives (and grabbing account information)," Kremez told BleepingComputer.com.

To make matters worse, with the information stolen by the attackers, they could potentially use these stolen Facebook cookies to access accounts and use them to create their own ad campaigns.

Steals Amazon session cookies

While the main focus of this Trojan is to steal data from Facebook, the malware will also attempt to steal session cookies for Amazon.com and Amazon.co.uk.



```
v44 = (unsigned int)&savedregs ^ __security_cookie;
v27 = 0;
sub_4BB280(&v40, 0, 0x1000u);
sub_4BB280(&v39, 0, 0x1000u);
sub_4BB280(&v43, 0, 0x32u);
sub_4BB280(&v2, 0, 0x32u);
sub_4BB280(&v1, 0, 0x32u);
sub_4B6260(&v28);
v45 = 0;
debg("amazon_us");
debg("chrome|firefox|ie");
debg("false");
sub_4A05C0(&unk_50A850);
v26 = sub_4E3430(&v40, &v39, &v43, "c_user", ".amazon.com", "datr|sb|c_user|xs|pl|fr", 0);
parse(&v40);
LOBYTE(v45) = 1;
parse(&v39);
LOBYTE(v45) = 2;
parse(&v43);
LOBYTE(
if ( (u
{
  v12 =
  LOBYT
  v27 |
  v25 =
}
else
{
  v14 = sub_49DF30(&v34);
```

2019-12-02: Socelars Stealer | Amazon Parser

Stealing Amazon session cookie

Unlike the Facebook routine, this cookie will simply be sent back to the attacker and will not be used by the Trojan to extract any other information. Once again, if the attacker gains access to a user's Amazon session cookie they will be able to log in as that user.

Distributed via adware bundles

As the sites promoting the 'PDFreader' program do not have active links that allow a user to download the program, BleepingComputer investigated how this malware may be distributed.

After following trail of other malware that communicated with one of the PDFreader domains, we found that many of the requests to the PDFreader domains came from adware bundles installing unwanted programs such as YeaDesktop or pretending to be copyrighted software.

As this Trojan is silently executed and performs all its tasks in the background, users will not be aware that anything was installed and will just see whatever adware or copyrighted software was downloaded.

Related Articles:

Pixiv, DeviantArt artists hit by NFT job offers pushing malware

New powerful Prynt Stealer malware sells for just $100 per month

New Meta information stealer distributed in malspam campaign

New BlackGuard password-stealing malware sold on hacker forums

Fake Binance NFT Mystery Box bots steal victim's crypto wallets

- Adware
- Amazon
- Facebook
- Info Stealer
- Password Stealing Trojan
- Trojan

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-

  buddy215 - 2 years ago

  Likely Russia....since Mueller outed it spreading propaganda...is behind this. Facebook users will once again be bombarded with pro-Trump Russian propaganda. Facebook has refused to ban political ads like Twitter has done. That's assuming the Senate will not vote to impeach Trump out of fear of losing their jobs. Trump is going all out in rallies across the country with his lies about Ukraine...not Russia...interfering in the last election. Voters should think about why Russia wanted Trump elected.

-
  herbman - 2 years ago
  -
  -

You cannot be serious LOL. Are you really this ridiculously clueless ?

Everything you said is completely bogus , it was democrats who colluded with Russia and Ukraine helped the democrats in the 2016 election.

You got to stop watching fake news , see official list of fake news below.

Cnn, Msnbc,Abc,Cbs, Nbc, HuffPost, NYT, WashPost, The AP, BuzzFeed, Politico, NewsWeek, The Hill, Rolling Stone, Sky News, USA Today, Time, LA Times, Reuters, BBC, Boston Globe, Vox, The Miami Herald, Mother Jones, HLN Yahoo, MSN, NY Daily News, Vice, Univision, People, PBS, NPR, New Yorker, Wall Street Journal, Daily Beast, Bloomberg, Aurn, National Journal, BI ,

"Politicians And Their Families Are Playing in The Corrupt Ukrainian Sandbox"

http://newswithviews.com/politicians-and-their-families-are-playing-in-the-corrupt-ukrainian-sandbox/

"The impeachment investigation into President Donald J. Trump’s alleged quid pro quo conversation with Ukrainian President Volodymyr Zelensky is beyond the theatre of the absurd. The continued harassment and ongoing defamation against the 45th president of the United States are acts of harassment, obstruction, and treason. Democrats and the liberal mainstream fake news media have been on a perpetual witch hunt to overthrow the duly elected POTUS and their credibility has reached new lows. If the United States is to remain a republic, the Democrat Party and their liberal propaganda media puppets must be stopped."

President Trump has the moral high ground and he has always been a fighter. He will not sit idly by and allow a socialist-communist coup d’etat overthrow of his presidency to occur. As President Trump has said, “They’re not really after me, they’re after you. I’m just in their way.”

http://newswithviews.com/impeach-the-enemy-within-for-treason/

-

  Whalley_World - 2 years ago

  -
  -

  I thought this was a site for technical information, not political bickering. We certainly need relevant FACTS (verifiable) to protect ourselves from this cyber-security threat, but political finger-pointing and competing conspiracy theories will not help us here.

-

  Lawrence Abrams - 2 years ago

  -
  -

  On topic political comments are allowed, but let's not stray from the content of the article.

  If it continues, I will disable comments for this article.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: