10-BankInfoSecurity-Facebook

Get Permission

Photo: Facebook

In the wake of a massive breach that hacked Facebook's single sign-on program, the time seems right for single sign-off.

See Also: Live Webinar | Making the Case for Managed Endpoint Detection and Response

On Friday, Facebook warned that on Sept. 25 it discovered that it had fallen victim to an attack that breached 50 million user accounts . Facebook has invalidated its SSO access tokens for all of those accounts, as well as 40 million more that had used the "View As" feature exploited by attackers. *[Rebuild]* As a result, those 90 million users must log in again, which will generate a new SSO access token (see Facebook Breach: Attackers Exploited Privacy Feature).

"Due to the proliferation of single sign-on, user accounts in identity providers are now keys to the kingdom and pose a massive security risk. *[Worry]*"

Here's how Facebook explains the feature: "Our site, like many others, uses a mechanism called access tokens. This is not your password; it is kind of a digital key that keeps you logged into Facebook so that you don't need to re-enter your password every time you use the app," Guy Rosen, Facebook's vice president of product management, said in a Friday press briefing.

"And parts of our site use a mechanism called single sign-on - or SSO - to create new access tokens," he added. "The example is if I'm logged into the Facebook mobile app and it wants to open another part of Facebook inside a browser window, it can use SSO to generate an access token for that browser, which means you don't have to enter your password again."

Easy Access for All

To be clear: Facebook's SSO system, dubbed Facebook Social Login, allows users to access compatible third-party website services or mobile apps without having to log in again. Such capabilities have obvious ease-of-use upsides for legitimate users.

Unfortunately, the same can be said for any attacker who comes to possess stolen access tokens, because they too can use them to easily gain access to users' accounts on compatible sites and apps.

Using phishing or WiFi sniffing, attackers can intercept access tokens created by popular identity providers (IdPs) such as Facebook to access other, compatible web services or mobile apps - referred to as relying parties, or RPs. (Source: "O Single Sign-Off, Where Art Thou?")

In fact, in the wake of the recent Facebook breach, researchers have warned that attackers may have accessed any third-party site that accepts Facebook SSO, even if the victim had never previously visited that third-party site.

Percentage of websites from the top 1 million (per Alexa) that support each identity provider, aka IdP (Source: "O Single Sign-Off, Where Art Thou?")

Single Point of Failure

Warnings about the risk posed by web services that offer SSO - including not just Facebook's SSO, but also offerings from Google and Twitter, among many others - are not new *[Disappointment]*.

Most, but not all, services comply with OpenID Connect, which is an extension to OAuth 2.0. But if attackers can steal a user's OAuth token, they can use it to authenticate, as the user, to any site for which they've enabled it.

Cue ongoing phishing campaigns that are designed to separate users from their OAuth tokens (see Phishing Defense: Block OAuth Token Attacks).

“Due to the proliferation of SSO, user accounts in identity providers are now keys to the kingdom and pose a massive security risk. If such an account is compromised, attackers can gain control of the user’s accounts in numerous other web services,” according to “O Single Sign-Off, Where Art Thou?,” a recently published report into “single sign-on account hijacking and session management on the web” authored by five researchers at the University of Illinois at Chicago.

In the case of the Facebook breach, for example, its SSO system could have been used for a range of other sites, including its own Instagram, as well as Tinder, Spotify and others.

“Our study on the top 1 million websites according to Alexa found that 6.3 percent of websites support SSO. This highlights the scale of the threat, as attackers can gain access to a massive number of web services,” the researchers say.

Access Not Always Logged

Any illicit SSO activity may never even get logged by whomever manages the SSO access tokens or cookies.

“An unexpected finding during our experiments was that when attackers use hijacked FB tokens (i.e., cookies) to access the user’s FB account, the attacker’s session didn’t show up in the list of active sessions if the attacker stayed connected for less than 60 [minutes],” Jason Polakis , an assistant professor of computer science at the University of Illinois at Chicago, says on Twitter.

“Another very critical yet overlooked problem is that the stolen tokens can be used to obtain access to a user’s account on other websites that support Facebook SSO even if the user doesn’t use Facebook SSO to access them,” he adds. “This depends on third-party implementations.”

To make matters worse, we found that the majority of popular sites that we audited, don’t offer session management options for terminating active sessions and invalidating cookies. Users currently lack ways to recover from their accounts being hijacked on many 3rd parties. (11/n)

��� jason polakis (@jpolakis) September 29, 2018

Following the breach at Facebook, the social network giant says it invalidated the tokens for 50 million users whose accounts were attacked, as well as 40 million more accounts for which a vulnerable feature was used - even if it might not have been illegitimate. *[Rebuild]* This will break attackers' ability to use the tokens to access victims' account on Facebook or via any SSO services that allow Facebook to authenticate them.

Current Outlook for Most Victims: 'Bleak'

Unfortunately, however, aside from these types of mass resets, it's often very difficult for anyone whose access token gets stolen to revoke the token, the University of Illinois at Chicago researchers say.

"Out of the 95 RPs we evaluated, only 10 (six web, four iOS) offer some form of session management; for those RPs the user can lock the attacker out by changing the IdP password and invalidating all active sessions in the RP and IdP," the researchers note.

Of the 95 web services and mobile apps studied by the researchers, only these "can somehow affect the attacker's ability to maintain access to the account. (Source: "O Single Sign-Off, Where Art Thou?")

In some cases, when users log out, unexpected behavior may result. For Goodreads, for example, revoking RP access and logging out from all active sessions would kick a web attacker out, but leave them with app access. In the case of Kayak, meanwhile, no matter what a user does to revoke access, "the attacker retains partial read access to the account no matter what actions are taken," the researchers say.

And for the other 71 web services and mobile apps studied by the researchers, unfortunately, "the user does not have any course of action to revoke attacker access to the accounts," they say. Logging out and logging back in does not kick out an attacker, except if the RP cookie expires, although they note that only five apps have short expiration dates.

Remedy: Single Sign-Off

As that suggests, too many victims of access token hijacking attacks have no way to protect themselves by revoking not only tokens, but potentially unauthorized access.

“To remedy this, we propose single sign-off, an extension to OpenID Connect for universally revoking access to all the accounts associated with the hijacked identity provider account,” the researchers say. Such a single sign-off would enable users “to initiate a chain reaction of access-revocation operations that propagate across all associated accounts.”

Websites and social networks remain keen to ensure that they present as frictionless a user experience as possible, in part by facilitating single sign-on across numerous sites, service and apps. But the recently discovered Facebook breach once again highlights the dangers posed by this interconnectedness.

The more users can automatically connect to numerous accounts and services, the more they must be able to easily and automatically revoke access to them as well.