kindred

Security Newsletter

8 October 2018

Subscribe to this newsletter

Facebook got hacked: 50 million accounts accessed

On the afternoon of Tuesday, September 25, Facebook engineering team discovered a security issue affecting almost 50 million accounts. Attackers exploited a vulnerability in Facebook's code that impacted "View As" a feature that lets people see what their own profile looks like to someone else. This allowed them to steal Facebook access tokens which they could then use to take over people's accounts. Access tokens are the equivalent of digital keys that keep people logged in to Facebook so they don't need to re-enter their password every time they use the app.

In a conference call with reporters, Facebook vice president of product Guy Rosen shared a few more details of the breach: Facebook Detected Breach After Noticing Unusual Traffic Spike; Hackers Exploited Total 3 Facebook Vulnerabilities; Hackers Stole Secret Access Tokens for 50 Million Accounts but they reseted access tokens for 90 millions accounts to be

safe; Your Facebook Account Password Has Not Been Compromised; Hackers Downloaded Users' Private Information Using Facebook API; Your "Logged in as Facebook" Accounts at 3rd-Party Apps/Websites Are At Risk; You should Check Active Sessions on Facebook to Find If Your Account Have Been Hacked

Warning: Attackers behind the recently revealed Facebook mega-breach may still be able to access victims' accounts at third-party web services and mobile apps, and Facebook has offered no timeline for when that might change. Here's the problem: Whoever hacked Facebook stole single sign-on access tokens - and thus access - to at least 50 million accounts, which also gives them access to the hundreds of third-party services and mobile apps that accept victims' SSO authentication, dubbed Facebook Social Login or Facebook Login. Facebook found no evidence "so far" that proves such claims.

Unfortunately, Facebook now says that while it can reset access tokens, it cannot guarantee that all third-party services that accept Facebook Social Login will honor these token-reset requests. This corporate approach, in fact, appears to mirror precisely what got Facebook into the Cambridge Analytica data scandal mess. Simply put, Facebook wasn't policing how third parties accessed, processed, used or sold Facebook users' data.

Official statements from Facebook

Even More on BankInfoSecurity

10 important updates on TheHackerNews

Phishing Attack Uses Azure storage to Impersonate Microsoft

Even though phishing attacks can be quite convincing, a give away is when diligent users notice that the login form is unsecured, the URL is not right or the SSL certificate is clearly not owned by the company being impersonated. A new Office 365 phishing attack utilizes an interesting method of storing their phishing form hosted on Azure Blob Storage in order to be secured by a Microsoft SSL certificate.

Azure Blob storage is a Microsoft storage solution that can be used to store unstructured data such as images, video, or text. By storing a phishing form in Azure Blob storage, the displayed form will be signed by a SSL certificate from Microsoft. This makes it an ideal method to create phishing forms that target Microsoft services such as Office 365, Azure AD, or other Microsoft logins.

In these attacks, bad actors are sending out spam emails with PDF attachments. These attachments are named "Scanned Document... Please Review.pdf" and simply contain a button to download a supposed PDF of a scanned document. When users click on this link they will be brought to a HTML page pretending to be a Office 365 login form that is stored on the Microsoft Azure Blob storage solution. Notice how the URL, https://onedriveunbound80343.blob.core.windows.net indicates it is a blob. As this page is also being hosted on a Microsoft service, it gets the benefit of being a secured SSL site as well.

While more experienced users may not fall for this attack due to the strange URL, others may be more convinced because the page utilizes a certificate from Microsoft and thus must be safe. To better protect users from these types of evolving threats,Netskope recommends that companies properly educate their users to recognize non-standard web page addresses. "Enterprises should educate their users to recognize AWS, Azure, and GCP object store URLs, so they can discern phishing sites from official sites. "

Read More on BleepingComputer

Original blog post from Netskope

Cutting room floor

- Update now: Adobe fixes 85 serious flaws in Acrobat and Reader
- Security Update for Foxit PDF Reader Fixes 118 Vulnerabilities
- You gave your number to Facebook for security and it used it for ads...
- GhostDNS: New DNS Changer Botnet Hijacked Over 100,000 Routers
- New iOS Passcode Bypass Method Exposes Photos, Contacts on iPhone XS
- Telegram Leaks IP Addresses by Default When Initiating Calls
- Apple forgot to lock Intel Management Engine in laptops, so get patching
- European Cyber Security Month
- Google Adds New Rules To End Malicious Chrome Extensions
- Fortnite gamers targeted by data theft malware
- The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies
- An Innovative Phishing Style
- D-Link Patches Code Execution, XSS Flaws in Management Tool
- Mozilla Releases Critical Security Update For Thunderbird
- The KRACK-en reawakens in updated WPA2 attack

#Tech and #Tools

- Review of Container scanning tools
- Static Analysis of Client-Side JavaScript for pen testers and bug bounty hunters
- Solo: Open Source FIDO2 USB+NFC security key
- Violating Your Personal Space with Webex
- APT37: Final1stspy Reaping the FreeMilk
- APT38: Details on New North Korean Regime-Backed Threat Group
- Threat-Intelligence-Hunter: intelligence tool that helps you in searching for IOCs across multiple openly available security feeds
- Whoisology: Reverse Whois Lookup
- crt.sh: Certificate Transparency search
- CertStreamMonitor: Monitor certificates generated for specific domain strings and associated
- Follow-Up on KRACK attacks
- Twenty years of Escaping the Java Sandbox
- Auditing Bitbucket Server Data for Credentials in AWS
- Draw.io for threat modeling
- BYOB (Build Your Own Botnet)
- PRTG Network Monitor Privilege Escalation
- Convert nmap Scans into Beautiful HTML Pages

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us