kindred

Security Newsletter

9 July 2018

Subscribe to this newsletter

Facebook Admits Sharing Users' Data With 61 Tech Companies

Facebook has admitted that the company gave dozens of tech companies and app developers special access to its users' data after publicly saying it had restricted outside companies to access such data back in 2015.

During the Cambridge Analytica scandal revealed March this year, Facebook stated that it already cut off third-party access to its users' data and their friends in May 2015 only. However, in a 747-page long document [PDF] delivered to Congress late Friday, the social networking giant admitted that it continued sharing data with 61 hardware and software makers, as well as app developers after 2015 as well.

The documents also acknowledged that Facebook partnered with 52 domestic and international companies, including U.S. tech giants Apple, Microsoft, Spotify, Amazon, Sony, Acer, China-based Huawei and Alibaba, and device-makers Samsung and BlackBerry. The document comes months after it revealed that personal data of 87 million Facebook users were harvested by Cambridge Analytica, a political consultancy firm, who reportedly helped Donald Trump win the US presidency in 2016.

Read More

Another Facebook Quiz App Left 120 Million Users' Data Exposed

Cutting room floor

- Typeform Suffers Data Breach, More than 20,000 User's Personal Data Was Compromised
- Two Zero-Day Exploits Found After Someone Uploaded 'Unarmed' PoC to VirusTotal #OpSec
- Beware! Fortnite Cheat Hijacks Gamers' PCs to Intercept HTTPS Traffic
- Data Security Startup Enveil Unveils Homomorphic Encryption Platform
- Newer Diameter Telephony Protocol Just As Vulnerable As SS7
- NHS data breach exposed sensitive health data of 150,000 patients
- My experience of vulnerability disclosure - Jolokia
- WordPress Update 4.9.7 – Critical Security Update
- Your smartphone can watch you if it wants to, study finds
- Weak Admin Password Enabled Gentoo GitHub Breach
- Polar fitness app exposed locations, names and addresses of soldiers and spies
- Google Released Security Updates for More than 40 Android Security vulnerabilities
- Hackers Compromised the Gas Station Fuel Pump and Steal 600 Gallons of Gas using Remote Device

#Tech and #Tools

- Exfiltrating credentials via PAM backdoors & DNS requests
- Bypassing Web-Application Firewalls by abusing SSL/TLS
- Exposing the Secret Office 365 Forensics Tool
- Compiler-assisted Code Randomization
- LAZY: script for Kali Linux that automates many procedures about wifi penetration and hacking.
- lookyloo: Scrape a website and then displays a tree of domains calling each other.
- How to drop 10 million packets per second
- Categorizing and Enriching Security Events in an ELK with the Help of Sysmon and ATT&CK
- How to search for Open Amazon s3 Buckets and their contents
- Five Easy Steps to Bypass Antivirus using manipulated MIME
- Hackability: Rendering Engine Hackability Probe
- Hackability inspector
- Enumerid: Enumerate RIDs using pure Python
- Apfell: A macOS, post-exploit, red teaming framework

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