# Security Newsletter

12 April 2021

Subscribe to this newsletter

# Pwn2Own 2021: Zoom, Teams, Exchange, Chrome and Edge "fully owned"



The annual Pwn2Own contest features live hacking where top cybersecurity researchers duke it out under time pressure for huge cash prizes.

Their quest: to prove that the exploits they claim to have discovered really do work under real-life conditions.

The competitors are faced with a standardised, patched, vanilla configuration of the system they're targeting, set up for them on hardware they didn't choose theselves, and they have just 20 minutes in which to complete their attack during the competition.

Read More on Naked Security

Even More on Zero Day Initiative blog

# 533 Million Facebook Users' Phone Numbers and Personal Data Leaked Online



In what's likely to be a goldmine for bad actors, personal information associated with approximately 533 million Facebook users worldwide has been leaked on a popular cybercrime forum for free—which was harvested by hackers in 2019 using a Facebook vulnerability.

The leaked data includes full names, Facebook IDs, mobile numbers, locations, email addresses, gender, occupation, city, country, marital status broken, account creation date, and other profile details broken down by country, with over 32 million records belonging to users in the U.S., 11 million users the U.K., and six million users in India, among others.

In total, the data being offered includes user information from 106 countries. Additionally, the data seems to have been obtained by exploiting a vulnerability that enabled automated scripts to scrape Facebook users' public profiles and associated private phone numbers en masse. The flaw has since been fixed by Facebook.

Read More on The Hacker News

# More #News

- New Wormable Android Malware Spreads by Creating Auto-Replies to Messages in WhatsApp
- Booking.com fined for not reporting data breach fast enough
- Ubiquiti All But Confirms Breach Response Iniquity
- GitHub Actions being actively abused to mine cryptocurrency on GitHub servers
- Attackers deliver legal threats, IcedID malware via contact forms

# #Breach Log

- PHP's Git server hacked to add backdoors to PHP source code
- The Facebook Phone Numbers Are Now Searchable in Have I Been Pwned
- Gigaset smartphones infected with malware due to compromised update server
- Threat actor offers to sell 8 TB of MobiKwik's personal and financial data on almost 100M consumers
- Leading cosmetics group Pierre Fabre hit with $25 million ransomware attack
- World's largest pathologists association discloses credit card incident
- Over 600,000 stolen credit cards leaked after Swarmshop hack
- Joker malware infects over 500,000 Huawei Android devices
- Hacker sells $38M worth of gift cards from thousands of shops
- Ransomware hits TU Dublin and National College of Ireland
- No password required: Mobile carrier exposes data for millions of accounts

# #Patch Time!

- Cisco fixes bug allowing remote code execution with root privileges
- VMware fixes authentication bypass in data center security software
- Android Security Bulletin—April 2021

# #Tech and #Tools

- BleedingTooth: Linux Bluetooth Zero-Click Remote Code Execution
- SAML XML Injection
- Breaking GitHub Private Pages for $35k
- Remote Method Guesser
- Kubesploit: a cross-platform post-exploitation C&C server focused on containerized environments

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 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 is an innovation driven company that builds on trust.

You can access the previous newsletters at [https://news.infosecgur.us](https://news.infosecgur.us)