kindred

Security Newsletter

26 April 2021

Subscribe to this newsletter

Facebook has a new mega-leak on its hands

Still smarting from last month's dump of phone numbers belonging to 500 million Facebook users, the social media giant has a new privacy crisis to contend with: a tool that, on a massive scale, links Facebook accounts with their associated email addresses, even when users choose settings to keep them from being public.

A video circulating on Tuesday showed a researcher demonstrating a tool named Facebook Email Search v1.0, which he said could link Facebook accounts to as many as 5 million email addresses per day.

The researcher—who said he went public after Facebook said it didn't think the weakness he found was "important" enough to be fixed—fed the tool a list of 65,000 email addresses and watched what happened next.

Read More on Ars Technica

Hackers are exploiting a Pulse Secure 0-day to breach orgs around the world

Hackers backed by nation-states are exploiting critical vulnerabilities in the Pulse Secure VPN to bypass two-factor authentication protections and gain stealthy access to networks belonging to a raft of organizations in the US Defense industry and elsewhere, researchers said.

At least one of the security flaws is a zero-day, meaning it was unknown to Pulse Secure developers and most of the research world when hackers began actively exploiting it, security firm Mandiant said in a blog post published Tuesday.

Mandiant said that it has uncovered “limited evidence” that tied one of the hacker groups to the Chinese government.

Read More on Ars Technica

Even More on Mandiant's blog

More #News

- Easy-to-guess default device passwords are a step closer to being banned
- Nightmare week for security vendors: Now a Trend Micro bug is being exploited in the wild
- Nation-State Actor Linked to Pulse Secure Attacks

- Linux bans University of Minnesota for committing malicious code
- Attackers can hide 'external sender' email warnings with HTML and CSS
- Hacking Startup 'Azimuth Security' Unlocked the San Bernardino iPhone
- Cost of Account Unlocks, and Password Resets Add Up
- Researchers Find Additional Infrastructure Used By SolarWinds Hackers
- Remote code execution vulnerabilities uncovered in smart air fryer
- Bugs Allowed Hackers to Dox John Deere Tractor Owners
- 120 Compromised Ad Servers Target Millions of Internet Users
- Rapid7 acquires open-source project Velociraptor
- Facebook uncovers Palestinian government officials targeted with malware

#Breach Log

- Supply chain attack on the password manager Clickstudios - PASSWORDSTATE
- Logins for 1.3 million Windows RDP servers collected from hacker market
- Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices
- Botnet backdoors Microsoft Exchange servers, mines cryptocurrency
- Hackers threaten to leak stolen Apple blueprints if $50 million ransom isn't paid
- HashiCorp is the latest victim of Codecov supply-chain attack

#Patch Time!

- 3 Zero-Day Exploits Hit SonicWall Enterprise Email Security Appliances
- Google Patched Two New Zero-Day Bugs
- Microsoft partially fixes Windows 7, Server 2008 vulnerability
- Exploitation of Pulse Connect Secure Vulnerabilities

#Tech and #Tools

- Uncovering and Disclosing a Signature Spoofing Vulnerability in Windows Installer
- Remote code execution in Homebrew by compromising the official Cask repository
- Breaking ABUS Secvest internet-connected alarm systems
- Hacking 3,000,000 apps at once through CocoaPods
- Duo Two-factor Authentication Bypass
- Leaky John Deere API's
- Attacking Xerox Multi Function Printers
- Exploiting vulnerabilities in Cellebrite UFED

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