kindred

Security Newsletter

15 April 2019

Subscribe to this newsletter

Featured

WikiLeaks founder Julian Assange has been arrested at the Ecuadorian Embassy in London—that's almost seven years after he took refuge in the embassy to avoid extradition to Sweden over a sexual assault case. According to a short note released by London's Metropolitan Police Service, Assange was arrested immediately after the Ecuadorian government today withdraws his political asylum.

U.S. Department of Justice also confirmed today that Assange would face extradition proceedings for his alleged role in "one of the largest compromises of classified information in the history of the United States." Following his arrest on Thursday, Ecuadorian President Lenín Moreno tweeted, "In a sovereign decision, Ecuador withdrew the asylum status to Julian Assange after his repeated violations to international conventions and daily-life protocols."

However, WikiLeaks said Ecuador had acted illegally in terminating Mr Assange's political asylum "in violation of international law." Assange's arrest comes a day after WikiLeaks editor Kristinn Hrafnsson accused the Ecuadorian government of an extensive spying operation against Julian Assange inside the Ecuadorian embassy. Assange, the 47-year-old Australian hacker, founded WikiLeaks in 2006 and has since made many high-profile revelations through the platform, exposing 'dirty' secrets of several political parties, individuals, and government organizations across the world.

Read More on TheHackerNews

Swedish prosecutor urged to reopen rape investigation into Julian Assange

Assange: A Decade of Stunning Leaks of U.S. Secrets

Two Thirds of Hotel Sites Leak Guest Booking Info to Third-Parties

Third-party services running on most hotel websites have access to guest booking information, including personal data and payment card details. The data they're privy to also allows them to cancel reservations. Multiple websites for over 1,500 hotels in 54 countries fail to protect user information from partner services such as advertisers and analytics companies. In 67% of the studied cases, some level of personal information is leaked via booking reference codes.

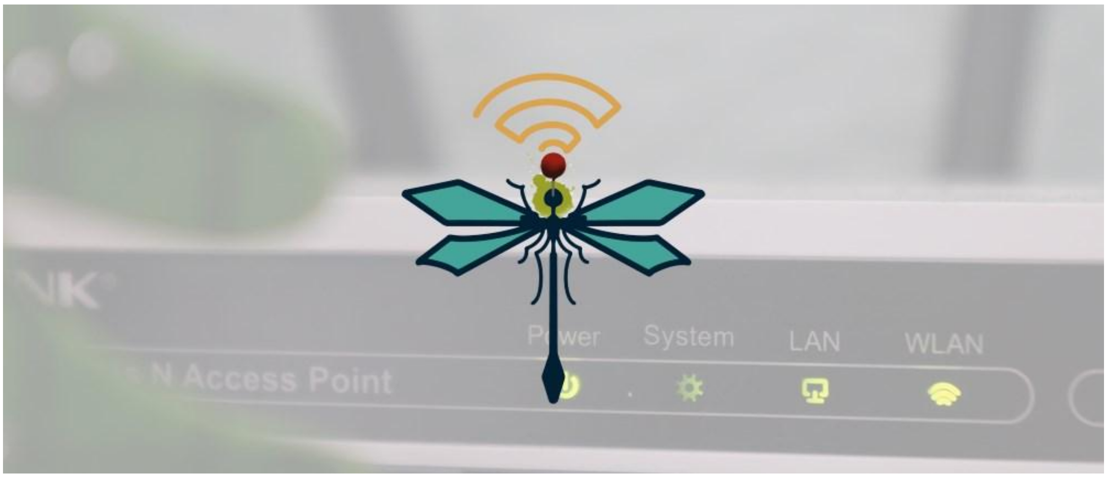
The data exposed this way may include the guest's full name, email and physical address, phone number, the last four digits of the payment card as well as its type and expiration date, and the passport number.

Being in the referrer filed means that the booking reference code is passed along by the browser, potentially reaching over 30 service providers like social networks, search engines, and analytics services. However, bad this may sound, the third-party providers are not to blame for getting more information than they need to operate properly. 25% of the officers did not reply six weeks after being informed of the privacy risks. Those that responded needed an average of 10 days to issue a reply and said they would commit to fixing the problem.

Read More on BleepingComputer

Even More on Symantec Blog

Dragonblood vulnerabilities disclosed in WiFi WPA3 standard



Two security researchers disclosed details today about a group of vulnerabilities collectively referred to as Dragonblood that impact the WiFi Alliance's recently launched WPA3 Wi-Fi security and authentication standard. If ever exploited, the vulnerabilities would allow an attacker within the range of a victim's network to recover the (weak) Wi-Fi password and infiltrate the target's network.

In total, five vulnerabilities are part of the Dragonblood ensemble --a denial of service attack, two downgrade attacks, and two side-channel information leaks. While the denial of service attack is somewhat unimportant as it only leads to crashing WPA3-compatible access points, the other four are the ones that can be used to recover user passwords.

The WiFi Alliance announced today a security update for the WPA3 standard following Vanhoef and Ronen's public disclosure of the Dragonblood flaws. "These issues can all be mitigated through software updates without any impact on devices' ability to work well together," the WiFi Alliance said today in a press release. Vendors of WiFi products will now have to integrate these changes into their products via firmware updates. Vanhoef is the same security researcher who in the fall of 2017 disclosed the KRACK attack on the WiFi WPA2 standard, which was the main reason the WiFi Alliance developed WPA3 in the first place.

Read More on ZDNet

Even More on TheHackerNews

More #News

- Gmail becomes first major email provider to support MTA-STS and TLS Reporting
- Dark Patterns: How Weaponized Usability Hurts Users
- Popular Yuzo WordPress Plugin Exploited to Redirect Users to Scams
- Women in Cybersecurity: A Progress Report
- Threat Group Uses Pastebin, GitHub In SneakyPastes Operation

- Credential Stuffing: Volume 5, Special Media Edition Attacks and Economies (PDF)
- Two teens charged with jamming school Wi-Fi to get out of exams
- Many New Security Features, Services Added to Google Cloud
- New TajMahal Cyberespionage Kit Includes 80 Malicious Modules
- Emotet hijacks email conversation threads to insert links to malware
- 25% of Phishing Emails Bypass Office 365 Default Security
- Airbnb says sorry after man detects hidden camera with network scan
- How to increase your chances of finding a hidden camera
- Mirai Botnet Variants Targeting New Processors and Architectures
- 'Exodus' Surveillance Malware Found Targeting Apple iOS Users
- Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days
- Bootstrap supply chain attack is another attempt to poison the barrel
- Android 7.0+ Phones Can Now Double as Google Security Keys
- Use your Android phone's built-in security key
- Half of organizations don't test their incident response plans
- Amazon employees listen in to your conversations with Alexa

#Patch Time!

- Patch Tuesday Lowdown, April 2019 Edition
- Adobe Releases April 2019 Security Updates for Flash, Shockwave, and More
- Demo Exploit Code Available for Privilege Escalation Bug in Windows (CVE-2019-0841)
- Researcher Reveals Multiple Flaws in Verizon Fios Routers — PoC Released
- Siemens Patches Serious DoS Flaws in Many Industrial Products

#Tech and #Tools

- Folder Actions for Persistence on macOS
- Some enterprise VPN apps store authentication/session cookies insecurely
- A few Ghidra tips for IDA users, part 1 - the decompiler/unreachable code
- The danger of exposing docker.sock
- New BGP hijack attack in the wild
- A Pentester's Guide - Part 3 (OSINT, Breach Dumps, & Password Spraying)
- Verizon Fios Router Authenticated Command Injection
- Why Grubhub uses crypto when generating coupon codes at scale
- CARPE (DIEM): CVE-2019-0211 Apache Root Privilege Escalation PoC
- Funnel: lightweight yara-based feed scraper
- BlueHive: Active Directory Honey User Account Management
- HoneypotBuster: find honeypots and honeytokens in the network or at the host.
- MacOS Red Teaming 201: Introduction (202: Profiles)
- There's Something About Service Accounts
- Running LAPS in the race to security
- Disrupting the Empire: Identifying PowerShell Empire Command and Control Activity (PDF)

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 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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