kindred

Security Newsletter

13 January 2020

Subscribe to this newsletter

The Difficulty of Disclosure, Surebet247 and the Streisand Effect

SureBet247, a popular sport betting company based in Nigeria was victim of an incident related to the data protection of its users that would have put thousands of records stored by the company at risk. An anonymous user discovered the information exposed on the public Internet, who reported the find to Troy Hunt, a security researcher and founder of the Have I Been Pwned platform. After attempting to contact SureBet247 without success, the researcher decided to share the find with the cybersecurity community.

This incident has been particularly frustrating for both Hunt and the anonymous informant, who have repeatedly tried to contact the company; on the other hand, SureBet247 has not commented on the incident in any way, so investigators ignore whether the company was even aware of this serious breach of the data protection of its users. Based on Hunt's reporting, the International Institute of Cyber Security (IICS) finds it unlikely that the company will implement an appropriate security incident management process or even notify all potentially exposed users. Given the company's irresponsibility, customers are advised to reset their access passwords to the SureBet247 platform, in addition to monitoring their bank accounts for any suspicious activity.

"This is a blog post about disclosure, specifically the difficulty with doing it in a responsible fashion as the reporter whilst also ensuring the impacted organisation behaves responsibly themselves. It's not a discussion we should be having in 2020, a time of unprecedented regulatory provisions designed to prevent precisely the sort of behaviour I'm going to describe in this post. Here you're going to see - blow by blow - just how hard it is for those of us with the best of intentions to deal with organisations who have a very different set of priorities. This is a post about how hard disclosure remains and how Surebet247's behaviour now has them experiencing the full blown Streisand effect."

Read More on Troy Hunt's blog

Even More on SecurityNewspaper

More #News

More #News

- TikTok Flaws Allowed Hackers to Delete Videos, Steal User Info
- MageCart Attackers Steal Card Info from Focus Camera Shoppers
- Google suspends Xiaomi from Home Hub over camera privacy glitch
- Only 9.27% of all npm developers use 2FA
- Google's Project Zero highlights patch quality with policy tweak
- InfoTrax Gets Slap on The Wrist After Being Breached 20+ Times
- Introducing Cloudflare for Teams
- IT Executive Steals $6 Million, Busted by Word Doc Metadata
- Ransomware Attackers Offer Holiday Discounts and Greetings
- Starbucks Devs Leave API Key in GitHub Public Repo
- Chinese hacker group caught bypassing 2FA
- Google Removed Over 1.7K Joker Malware Infected Apps from Play Store
- Unremovable malware found preinstalled on low-end smartphone sold in the US
- PayPal Patches Vulnerability That Exposed User Passwords
- Hackers use system weakness to rattle doors on Citrix systems
- UK Fines Dixons Carphone for Massive Breach

#Patch Time!

- Critical Firefox 0-Day Under Active Attacks – Update Your Browser Now!
- Critical Citrix Flaw May Expose Thousands of Firms to Attacks
- New Magellan 2.0 SQLite Vulnerabilities Affect Many Programs

#Tech and #Tools

- Extract credentials from lsass remotely
- New SHA-1 Attack
- Kali Linux to Default to Non-Root User With 2020.1 Release
- Promiscuous Cookies and Their Impending Death via the SameSite Policy
- How to install and use git-secret
- Resurrected PowerShell Empire Framework Converted to Python 3
- The Bug That Exposed Your PayPal Password
- The Basics of Packed Malware: Manually Unpacking UPX Executables
- SSH Client Auditing & Hardening
- Account takeover via HTTP Request Smuggling
- Alert Alarm SMS exploit - English version
- Endlessh: SSH tarpit that slowly sends an endless banner
- git-vuln-finder: Finding potential software vulnerabilities from git commit messages
- Catalog of supply chain compromises
- Artillery: combination of a honeypot, monitoring tool, and alerting system.
- Spray-AD: Cobalt Strike tool to audit Active Directory user accounts for well known or easy guessable passwords.
- What I've Learned in Over a Decade of "Red Teaming"
- Lesser-known Tools for Android Application PenTesting

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

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