Security Newsletter

28 January 2019

Subscribe to this newsletter

Online casino group leaks information on 108 million bets, including user details

An online casino group has leaked information on over 108 million bets, including details about customers' personal information, deposits, and withdrawals, ZDNet has learned. The data leaked from an ElasticSearch server that was left exposed online without a password.

ElasticSearch is a portable, high-grade search engine that companies install to improve their web apps' data indexing and search capabilities. Such servers are usually installed on internal networks and are not meant to be left exposed online, as they usually handle a company's most sensitive information.

Despite being one server, the ElasticSearch instance handled a huge swathe of information that was aggregated from multiple web domains, most likely from some sort of affiliate scheme, or a larger company operating multiple betting portals. Some of the domains that Paine spotted in the leaky server are from Mountberg Limited, including kahunacasino.com, azur-casino.com, easybet.com, and viproomcasino.net, just to name a few.

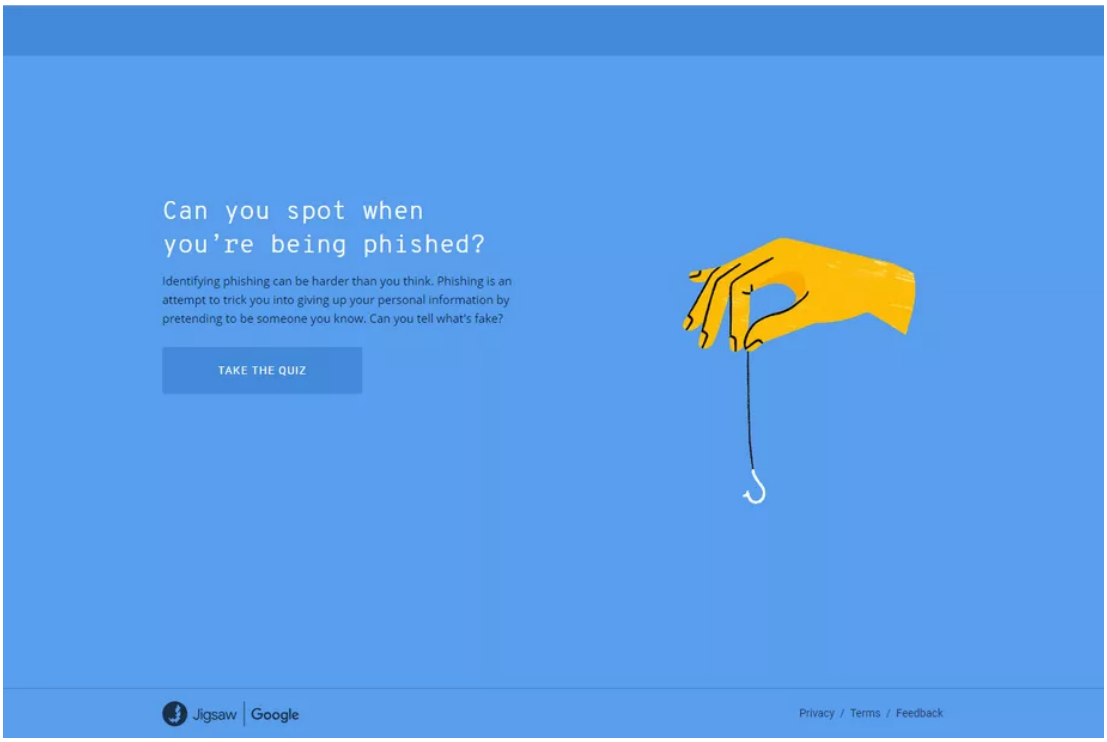
The user data that leaked from this common ElasticSearch server included a lot of sensitive information, such as real names, home addresses, phone numbers, email addresses, birth dates, site usernames, account balances, IP addresses, browser and OS details, last login information, and a list of played games. Furthermore, Paine also found roughly 108 million records containing information on current bets, wins, deposits, and withdrawals. Data on deposits and withdrawals also included payment card details.

All of these exposed databases were found by independent researchers using tools anyone, including cybercriminals, can access. That is the important point – the problem of exposed Elasticsearch data is out of the bag and people are now looking for it.

Read More on ZDNet

Even More on NakedSecurity

Can you spot when you're being phished?



Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

On Tuesday, Google's Jigsaw unit published a quiz that tests users' abilities to identify phishing emails. The quiz tests you on a series of emails to see if you can distinguish telltale signs of phishing.

"Phishing is, by far, the most common form of cyberattack," Jigsaw explains in a blog post. "One percent of emails sent today are phishing attempts." According to the post, the quiz is based on trainings Jigsaw held with "10,000 journalists, activists, and political leaders."

In total, there are eight examples that Google tests you on, some representing legitimate emails and others phishing scams. Many of the examples are actually based on real events, such as the massive phishing attempt that hit Google Doc users in 2017 or an email that Russian hackers sent to Hillary Clinton's campaign manager in 2016.

Take the Quiz!

Read More on TheVerge

More #News

- Google is hit With the Highest GDPR Fine of 50 Million Euros
- Critical RCE Flaw in Linux APT Allows Remote Attackers to Hack Systems

- The Fact and Fiction of Homomorphic Encryption
- Chrome Extension Manifest V3 May Break uBlock Origin Content Blocker
- White-listing Azure cloud connections to grease your Office 365 wheels? About that...
- Compare data protection laws around the world
- This is the first truly great Amazon Alexa and Google Home hack
- PCI Council Releases New Software Framework for DevOps Era
- 265 Researchers Take Down 100,000 Malware Distribution Websites
- Center for Internet Security releases Microsoft 365 benchmarks
- Security flaws found in 26 low-end cryptocurrencies
- Data Collected from Old Breaches Is Not a New Data Breach
- VLC Responds to Criticism Over Lack of HTTPS for Updates
- Google Chrome Adding Malicious Drive-By-Downloads Protection
- Microsoft Exchange zero-day and exploit
- Concerns raised about WordPress' new 'White Screen Of Death' protection feature
- Millions of financial records leaked from server not protected by password
- The Swedish Data Protection Authority (Datainspektionen) announced investigation on Google

#Patch Time!

- Two more Windows zero-days get temporary patches
- Cisco Released Security Updates & Fixed Several Vulnerabilities that Affected Cisco Products
- Check Point Fixes Privilege Escalation Bug in ZoneAlarm Free
- Ghostscript PDF interpreter needs patching
- NumPy Is Awaiting Fix for Critical Remote Code Execution Bug
- Running Sysmon 8.0.0? Update to 8.0.4 to Avoid a Memory Leak
- Upgrade to Nagios XI 5.5.8 or above

#Tech and #Tools

- Let's Encrypt gives admins until February 13 to switch off TLS-SNI-01
- Contextualizing Attacker Activity within Sessions in Exchange Online
- Hardening MacOS X Mojave
- Turbinia: Automation and Scaling of Digital Forensics Tools
- Confiant & Malwarebytes Uncover Steganography Based Ad Payload That Drops Shlayer Trojan On Mac Users
- MongoDB will not prevent NoSQL injections in your Node.js app
- DynamoDB Injection
- URLhaus: Malicious URLs that are being used for malware distribution.
- Security Practitioner's Guide to Email Spoofing and Risk Reduction
- Abusing Exchange: One API call away from Domain Admin
- Local Admin Access and Group Policy don't mix
- Application Security Weekly Review, Week 4 2019
- How I abused 2FA to maintain persistence after a password change
- Electronegativity: identifying misconfigurations and security anti-patterns in Electron-based applications

based applications.

- Magento – RCE & Local File Read with low privilege admin rights
- Github: Maintaining access to repos after they kick you out
- SSHtranger Things Exploit POC (CVE-2019-6111, CVE-2019-6110)
- Rooting Nagios Via Outdated Libraries
- PortPush: pivoting into internal networks upon compromising a public-facing host.

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