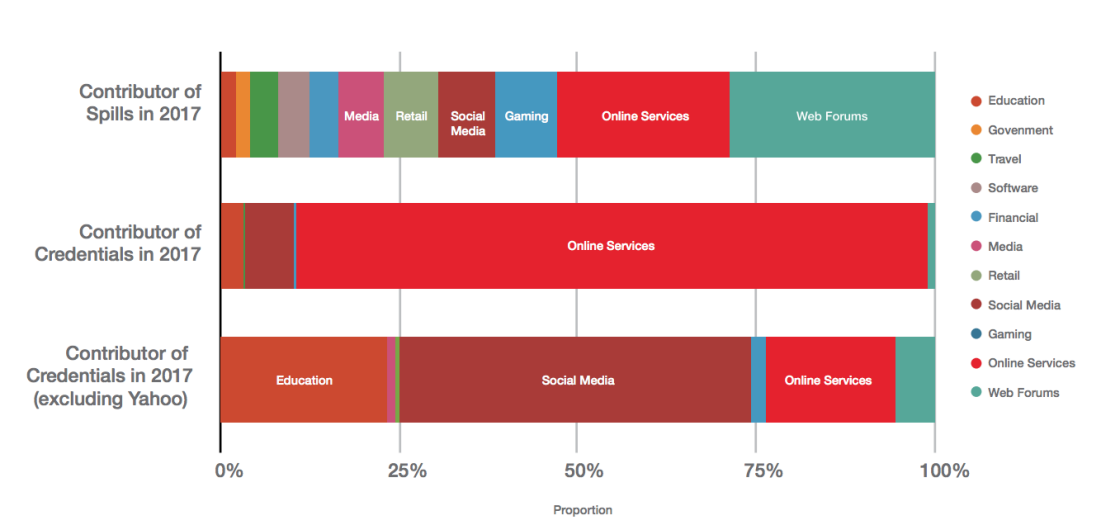
kindred

Security Newsletter

23 July 2018

Subscribe to this newsletter

2.3B credentials were stolen in 2017



In 2017, some 2.3 billion account credentials were stolen because of 51 independent credential spill incidents, according to Shape Security's second annual Credential Spill Report. The main industries affected were consumer banking, retail, airline, and hospitality, which were primarily attacked via credential stuffing and account takeovers, according to Shape Security's press release.

Credential stuffing are large scale cyberattacks where criminals use stolen credentials over a mass amount of logins. These attacks are often successful because of users reusing passwords, which is no surprise, as 25% of employees use the same passwords for every account. Attackers then use the information to commit various fraudulent actions, from unauthorized bank transfers to online purchases.

"What most people don't realize is the domino effect of damage that a single breach is capable of producing. To fight back, organizations have started banding together to build a collective defense to be alerted when credentials stolen from one breach are being used to log in to another, effectively blocking attackers attempting to access their platforms with compromised credentials."

An average of 15 months passed between the day credentials were stolen and the day the incident was realized and reported by an organization, said the release. With this substantial amount of time, cybercriminals can carry out a slew of attacks. Roughly 1 million credentials were exposed to criminals every day in 2017, said the report.

Read More

2018 Credential Spill report

Cutting room floor

- Researchers Mount Successful GPS Spoofing Attack Against Road Navigation Systems
- PayPal's Venmo App Exposes Most Transactions via Its API
- This $39 Device Can Defeat iOS USB Restricted Mode
- Droppers Is How Android Malware Keeps Sneaking Into the Play Store
- Oracle Patches Record 334 Vulnerabilities in July 2018
- Telefonica Spain Exposed the Personal Details of Millions of Customers
- NIST to Withdraw 11 Outdated Cybersecurity Publications
- Hackers hold 80,000 healthcare records to ransom
- Singapore's Largest Healthcare Group Hacked, 1.5 Million Patient Records Stolen
- A new security header: Feature Policy
- 5 tips for getting started with DevSecOps

#Tech and #Tools

- KeyFinder: Find and analyze private (and public) key files, support Android APK.
- Reversing JS Malware From marveloptics.com #Magecart
- This Week in OSINT — #2018–28
- Instrumenting Electron Apps for Security Testing
- SSL/TLS for dummies part 4 – Understanding the TLS Handshake Protocol
- Bypassing Memory Scanners with Cobalt Strike and Gargoyle
- Evading CSP with DOM-based dangling markup
- Exploiting a SAML Implementation
- Hunting for Bad Apples — Part 2 (Part 1)
- Mitre ATT&CK and the Mueller GRU Indictment: Lessons for Organizations
- What is single sign-on? How SSO improves security and the user experience
- Hackers Breach Russian Bank and Steal $1 Million Due to Outdated Router
- Microsoft Says Russia Tried to Hack Three 2018 Midterm Election Candidates
- Riot's approach to anti-cheat

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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