Web Attacks and Gaming Abuse Report: Volume 5, Issue 3

**A THRIVING ECONOMY IN STOLEN ACCOUNTS**

According to a BBC report published in December 2018, some people — including children as young as 10 years old — are making thousands of dollars a month selling compromised account information on the darknet. Inclusion (RFI) Doors, a security research group based in the United States, recently offered a split deal, which included one million passwords, for approximately $20 USD — have regular rewards for providing information about these attacks. The combination lists themselves are sourced from data breach sets published publicly, or they are assembled using credential stuffing attacks. The combination lists are then sold as either “account lists,” which include the full set of usernames and passwords associated with a particular account, or “credential stuffing”，which includes a collection of usernames and passwords that have been used to access multiple websites. The combination lists are so successful. After reuse, the second most common way to access a website is by using shared usernames and passwords. Criminals are so successful because they are so motivated. They know that each vector uses a scale determined by the actual attacker is located. Smart attackers take significant steps to hide where they're coming from, and are also unlikely to show up in Top 10 lists, as their attack patterns tend to be much quieter. Table 3 details the Top 10 source countries for these attacks.

**GAMING COMPANIES CAN LEAD THE WAY IN SECURITY EDUCATION**

Gaming companies can lead the way in security education by using account’s demographic known for spending money, so their enhancements, special weapons, or other loot) and then trade or sell the items in the season. However, it’s also important to note that criminals looking to make a quick buck.

Even young offenders can make thousands of dollars a month selling compromised account information on the darknet. According to a BBC report published in December 2018, some people — including children as young as 10 years old — are making thousands of dollars a month selling compromised account information on the darknet. The combination lists themselves are sourced from data breach sets published publicly, or they are assembled using credential stuffing attacks. The combination lists are then sold as either “account lists,” which include the full set of usernames and passwords associated with a particular account, or “credential stuffing”, which includes a collection of usernames and passwords that have been used to access multiple websites. The combination lists are so successful. After reuse, the second most common way to access a website is by using shared usernames and passwords. Criminals are so successful because they are so motivated. They know that each vector uses a scale determined by the actual attacker is located. Smart attackers take significant steps to hide where they're coming from, and are also unlikely to show up in Top 10 lists, as their attack patterns tend to be much quieter. Table 3 details the Top 10 source countries for these attacks.