Researchers have found over 23 million stolen credit and debit cards up for sale on the dark web, with US consumers by far the biggest hit.

Nearly two out of every three stolen cards on the sites trawled by Sixgill were issued in the US, amounting to more than 15 million. The next biggest hit country was the UK, which accounted for over 7%.

Tellingly, just 316 stolen cards out of the total 23 million were Russian issued. This isn’t just because many hackers are of Russian origin, but also because of the relatively low GDP of the country, making its citizens less attractive targets, the report claimed.

Although the figures are small in comparison to the five billion cards issued globally by Visa, Mastercard and American Express, fraud on these is estimated to cost US businesses and consumers around $12bn by 2020, according to separate predictions from The Nilson Report.

Threat actors are increasingly moving away from traditional dark web marketplaces to Instant Relay Chat (IRC) channels and encrypted Telegram chats, making it harder for researchers to monitor them, according to Sixgill.

"Fraudsters have a number of illicit methods they use to steal card data. They place ‘skimmers’ over the card readers on gas pumps and ATM machines. Retail workers and restaurant employees use devices to copy the swipes when they take a card for payment,” the firm continued in a blog post.

“They infect computers and other devices with malware to record payment information when their owners buy from e-commerce sites. Hackers infiltrate the networks of large companies..."
and simply steal millions of records at a time.”

Credit card information sells for as little as $5 and comes in two main types: one including all the card details plus CVV for fraudsters to use easily online, and dumps containing magstripe data which enable cyber-criminals to create counterfeit cards.

The former is more popular as it’s easier to commit fraud online, said Sixgill. Dumps of magstripe data will likely get less popular as more retailers and consumers adopt EMV in the US.

Recommended for you

What’s Hot on Infosecurity Magazine?

1. **Flaws Allow Hacker to Bypass Card Limits**
   - 29 JUL 2019
   - NEWS

2. **Malware Cited As Exploit Most Seen By SOC Teams**
   - 29 JUL 2019
   - NEWS

3. **UK Abused Access to EU Database For Years: Report**
   - 29 JUL 2019
   - NEWS

4. **Uptick in Ransomware, Mobile Banking Malware**
   - 29 JUL 2019
   - NEWS

5. **WannaCry Hero Hutchins Spared Jail Time**
   - 29 JUL 2019
   - NEWS

6. **Russian Fake News Targeted Ukraine Elections**
   - 29 JUL 2019
   - NEWS
As a career cyber security professional for 25 years, I had seen more than my fair share of this over the years. After spending this amount of time in the trenches and in the twilight of my professional career, 4 years ago I moved to the SE world and unfortunately continue to see this as a HUGE problem. Far too often they still continue to just peddle snake oil and unfortunately the never seem to realize that is only hurting them professionally, regardless of who they are employed by. Salespeople you need to start thinking about this, not only are you blacklisting your company, but more importantly you are tarnishing your own integrity/trustworthiness. Stand up for what is right as your customers trusted advisor by walking the walk instead of talking the talk (that unfortunately far too many do not). If you work for a snake oil or arrogant vendor then think real hard about your own longevity either there or in your location. It is understood that in many cases you work for a senior Sales VP/Dir/Mgr (who are a far cry from being a leader, like many I have seen in just a short span) who employ the same type, if not worse tactics on you (like threatening your job if quota fails) so do what is best for your customer and career instead, else be added to the pile.