After a year of intensely investigating password theft, here’s what Google found

Hackers are constantly trying to break into Google accounts, so Google researchers spent a year tracking how hackers steal passwords and expose them on the Internet’s black market.

To gather hard evidence about the tools hackers use to steal passwords, Google collaborated with University of California Berkeley cybersecurity experts to track activity on some of these markets. On Thursday, they published their results.

“Trends in accounts about how accounts are being hacked and we’re providing solid evidence about how this is going on in the wild,” Google anti-abuse researcher Kurt Thomas told Mashable.

SEE ALSO: Google adds stronger security features for hacking targets

Google found that most passwords are obtained in two ways: deceptive e-mail phishing and “third-party breaches,” such as hackers stealing passwords from a massive corporation like Equifax. In the year between March 2016 and 2017, Google found 12 million credentials, which are a combination of both usernames and passwords, obtained from phishing and a whopping 3.3 billion credentials swiped during third-party breaches.

The numbers are staggering because passwords are an attractive commodity — especially a Google account password that allows access to one’s Gmail, Google Docs, Google Drive, and so on.

“It’s the key to the kingdom,” said Thomas. “Accounts are incredibly valuable to hackers. There’s an incredible effort they’re putting into getting access to your email.”

“Passwords are no longer a paradigm that you can really trust in.”

Although the study’s attainable password numbers are massive, it’s important to note that the research team was limited in scope, so these figures could be significantly higher: the team only collected information that was freely available on the web.

“A hijacker that doesn’t hold themselves to that standard can get a lot more,” explained Thomas.

It’s certainly not rare anymore for people to have their e-mail accounts hijacked by the web’s malicious players. Google says that 15 percent of web users report having an account breached by hackers, although that number could certainly be much higher.

If passwords have as many enemies today — either through direct hacking or massive corporate data breaches — how do we battle these constant attempts at password theft?

Thomas emphasized using different passwords across sites, which many people know but simply disregard. Juggling passwords used to be pretty inconvenient, but today there are reusable password managers. “Like a password manager,” said Thomas, while also emphasizing Google’s own security measures, such as Google’s Security Check-up and having a phone number associated with your account — so Google can alert you of suspicious activity.

In short, meaningful password security — for Google accounts — is a collaborative effort between Google’s behind-the-scenes efforts to spot strange account activity and your own vigilance.

Take it from a cybersecurity expert: “Passwords are no longer a paradigm that you can really trust in,” said Thomas.

WATCH: Puerto Rico is recovering cell service… with balloons