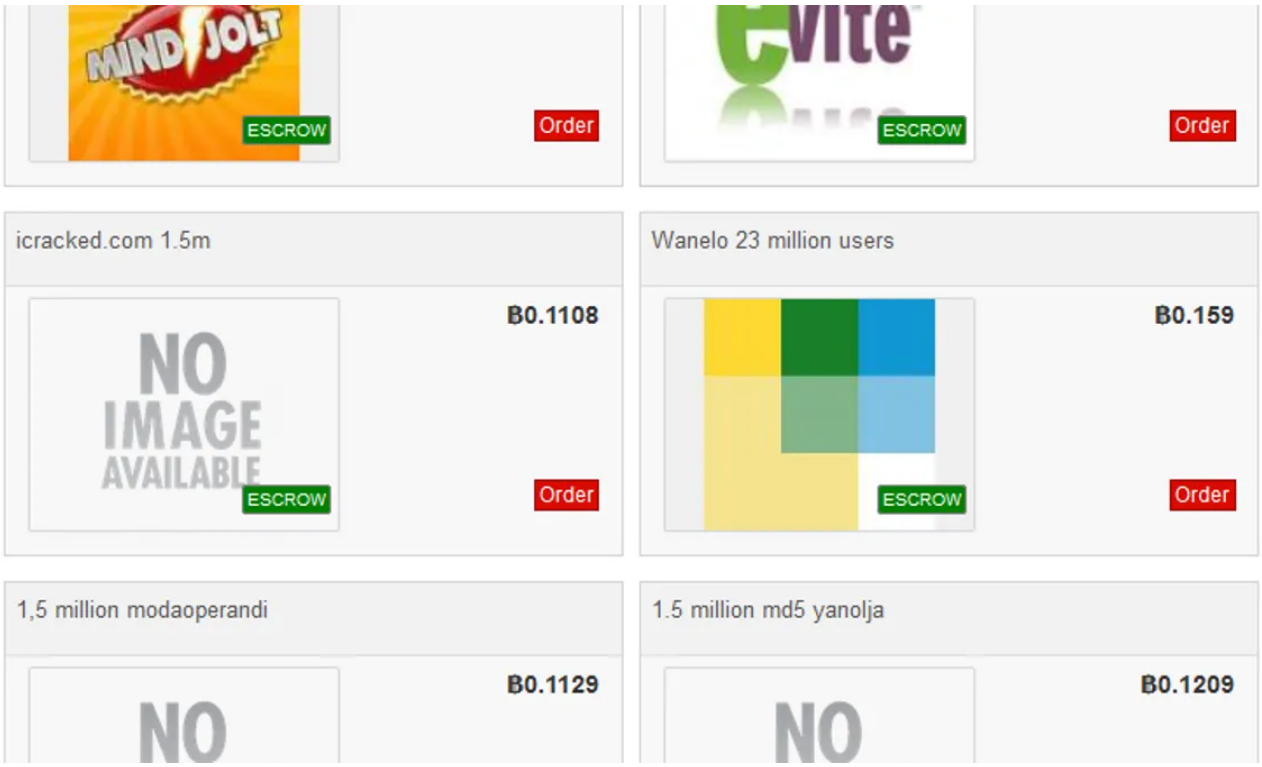
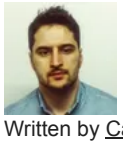
A hacker has dumped nearly one billion user records over the past two months



Home Innovation Security

Hacker Gnosticplayers has stolen over 932 million user records from 44 companies.



Written by Catalin Cimpanu, Contributor on April 15, 2019

-
-
-
-
-

Security

- My Instagram account was hacked, and two-factor authentication didn't help
- The 5 best browsers for privacy: Secure web browsing
- Stop doing these 10 things that let hackers in, says FBI and NSA
- What is a cybersecurity degree?
- How to delete yourself from search results and hide your identity online

A hacker who spoke with *ZDNet* in February about wanting to put up for sale the data of over one billion users is getting dangerously close to his goal after releasing another 65.5 million records last week and reaching a grand total of 932 million records overall.

The hacker's name is Gnosticplayers, and he's responsible for the hacks of 44 companies, including last week's revelations.

Since mid-February, the hacker has been putting batches of hacked data on Dream Market, a dark web marketplace for selling illegal products, such as guns, drugs, and hacking tools.

He's released data from companies like 500px, UnderArmor, ShareThis, GfyCat, and MyHeritage, just to name the bigger names. Releases have been grouped in four rounds --Round 1 (620 million user records), Round 2 (127 million user records), Round 3 (93 million user records), and Round 4 (26.5 million user records).

Hacker releases Round 5

Last week, the hacker notified *ZDNet* about his latest release --Round 5-- containing the data of 65.5 million users, which the hacker claims to have taken from six companies: gaming platform Mindjolt, digital mall Wanelo, e-invitations and RSVP platform Evite, South Korean travel company Yanolja, women's fashion store Moda Operandi, and Apple repair center iCracked.

While *ZDNet* has reached out for comment to each of the named businesses, most of the hacker's previous 38 victims have confirmed hacks, so this new batch of stolen data is also very likely to be authentic as well.

Image: ZDNet

Company	DB size	Price	Content
Mindjolt (gaming platform)	28 Mil	฿0.1008	email, full name, birth date, register date, gaming details, no password
Wanelo (digital mall)	23 Mil	฿0.159	email, username, password (3 million MD5 & the rest bcrypt)
Evite (e-invitations platform)	10 Mil	฿0.2419	full name, country, email, IP address, password (cleartext)
Yanolja (South Korean hotel and travel)	1.5 Mil	฿0.1209	email, password (MD5)
Moda Operandi (women's fashion store)	1.5 Mil	฿0.1129	email, name, password (SHA1), user-agent, IP address, and more
iCracked (Apple device repair center)	1.5 Mil	฿0.1108	name, physical address, geo-location details, email, password, and more

Dream Market admins decided last month to shut down their marketplace on April 30, and transition users to a competing site after being bombarded by nearly non-stop DDoS attacks and ransom demands.

In an email to *ZDNet*, the hacker said he decided to put this data up for sale (for 0.8463 Bitcoin/~$4,350), regardless of the market's impending closure.

The quest for one billion

But while many will believe the hacker is putting all this data on sale for selfish, and obvious monetary reasons, there is more to Gnosticplayers' actions than most people are aware.

In an interview with *ZDNet* after the release of Round 3 in February, the hacker was very candid about the reasons behind his sudden appearance in the public's eye.

Hackers like Gnosticplayers are part of small underground communities of hackers and data hoarders. They hack companies, steal their data, and then sell it to vetted partners.

This data is filtered and organized in various categories. Stolen email addresses are sold to spam botnets. Financial details are sold to groups specialized in online fraud or tax scams. Usernames and cracked passwords are sold to botnet operators specialized in credentials stuffing attacks.

This is a lucrative business, and many of these hackers don't have to sell their data on public marketplaces like Dream Market.

We say "public" because despite being hosted on the dark web, Dream Market is a very very public space, littered with law enforcement, journalists, and employees of many cyber-security firms.

Anyone selling data in such a public space is, without a doubt, looking for trouble and putting a bullseye on his back.

But according to Gnosticplayers, his foray into a public marketplace like Dream has two goals --besides the first and obvious one being money.

See als

10 dangerous app vulnerabilities to watch out for (free PDF)

Peace's long shadow

It's about reputation, the hacker told us in February. Gnosticplayers wants to be remembered in the same way hackers like Peace_of_Mind (or Peace) are remembered today.

Throughout 2016, Peace has grabbed headlines all over the world by putting for sale over 800 million user records on the now-defunct TheRealDeal marketplace, and other places. He's known for selling data from companies such as LinkedIn (167 million), MySpace (360 million), Tumblr (68 million), VK.com (100 million), Twitter (71 million), and many others.

The data that Peace was selling in 2016 was eventually released in the public domain and is now available in many places. Peace's original leaks are what made credentials stuffing attacks such dangerous threat today. His initial leaks are what have powered credential stuffing botnets for the past few years.

With over 932 million records already available for sale on Dream, Gnosticplayers' data hovers dangerously above all our heads, as it could greatly increase the capabilities of existing credentials stuffing botnets with new login combinations.

Furthermore, while it was initially pretty well contained, many of the databases that Gnosticplayers has advertised on Dream are now slowly entering the public domain, similar to how Peace's original data eventually leaked as well.

Some have ridiculed Gnosticplayers for selling data from small-time sites, with very few high-profile names when compared to Peace's list of hacked sites, but Gnostic's data should not be ignored, mainly due to its sheer size and everyone's penchant for reusing passwords.

Data leaks: The most common sources

More data breach coverage: