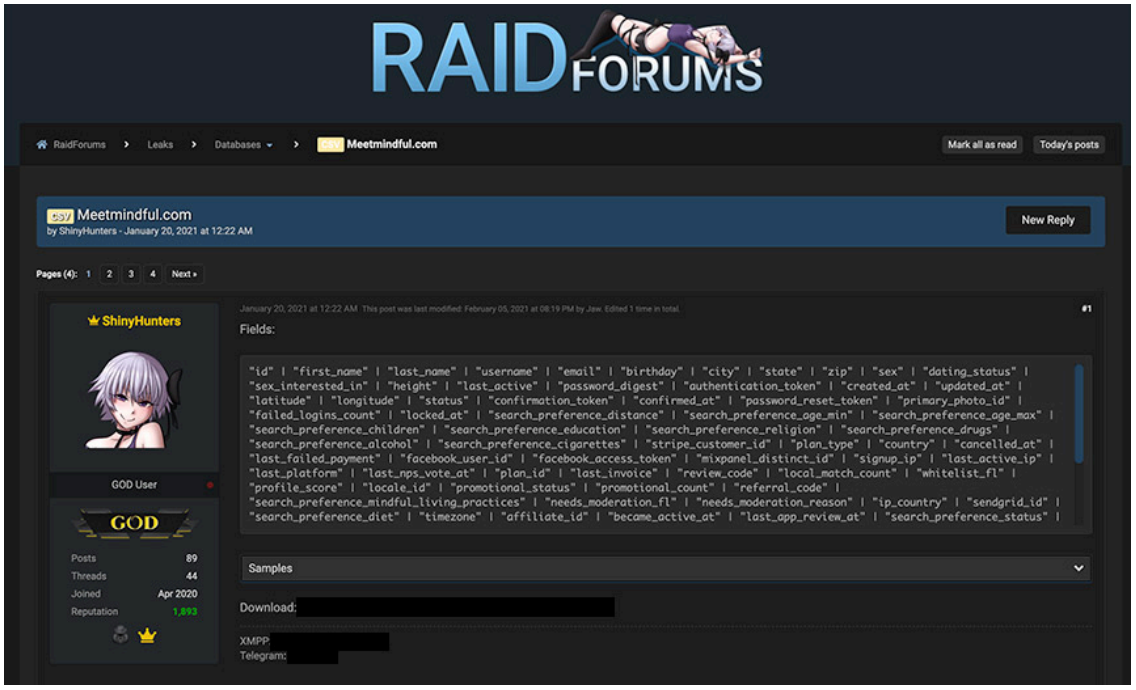
Data Breaches: ShinyHunters' Dominance Continues

By Mathew J. Schwartz

Cybercrime , Fraud Management & Cybercrime , Fraud Risk Management

Prolific Cybercrime Group Recently Tied to Breaches of E-Commerce and Dating Sites (euroinfosec) • February 18, 2021



ShinyHunters disclosed its breach of dating site MeetMindful.com by dumping stolen data on the cybercrime forum RaidForums.

The ShinyHunters cybercrime operation runs a data exfiltration and sales business that appears to be off to a roaring start again this year, following on the heels of its data breach spree last year.

See Also: Gen AI Stalls, Shadow AI Rises: A CISO Concern

"ShinyHunters released a tsunami of sensitive data in 2020," says cybersecurity firm Risk Based Security, noting that the group had been tied to "data dumps that ultimately exposed over 550 million user records."

After nearly 50 data breaches in 2020, so far this year, the gang has already taken credit for recent data breaches at e-commerce site Bonobo and dating site MeetMindful.

Known Breaches Have Declined

To give the group's activities some context, in 2020, the overall count of breached organizations and records declined slightly compared to 2019, according to the Identity Theft Resource Center, a nonprofit organization

based in San Diego, California, that provides no-cost assistance to U.S. identity theft victims to help resolve their cases.

While that trend is good news, the bad news is the decline can be traced to many criminals having found more lucrative outlets. Indeed, James E. Lee, COO of ITRC, says many cybercrime gangs have retooled to run ransomware and phishing attacks - especially those leading to business email compromise schemes. These attacks don't require much stolen data to be successful.

"We really only need two data elements to commit those kinds of crimes - you need a login and a password," Lee says. "If you have a login and a password, you can commit ransomware. If you run a phishing attack, what are you trying to get? A login and a password."

Of course, many ransomware-wielding gangs have then been grabbing customer records before leaving systems crypto-locked, and posting the stolen data to dedicated data-leak sites to pressure more victims into paying. But unlike historical breaches, oftentimes ransomware gangs don't necessarily seem to aim for valuable customer data, but rather just any corporate records they can get their hands on.

Hackers Sell Stolen Data

Some non-ransomware-wielding cybercrime gangs, however, continue to wage data breach campaigns, attempting to steal large amounts of data and sell it to others who might use it for payment card fraud, credential-stuffing attacks or extortion efforts.

Based on breach notification reports issued by U.S. firms, last year, 1,108 organizations suffered a breach - 676 of which included ransomware as an element of the attack - which collectively exposed information on more than 300 million individuals, ITRC reports. Note that not all organizations that report they were breached specify what was exposed or how many individuals might have been affected.

Compared to 2019 - when 1,362 organizations collectively reported 887 million individuals' personal details getting exposed - the overall number of breaches declined by 19% in 2020.

Reported U.S. data breaches and inadvertent data exposure in 2020 (Source: ITRC)

Risk Based Security, in its tally of publicly reported data breaches around the world in 2020, counted 3,932 breaches, which was a 48% decline compared to 2019. Last year, the most affected industry globally was healthcare, which accounted for 12% of all breached organizations, the security firm says.

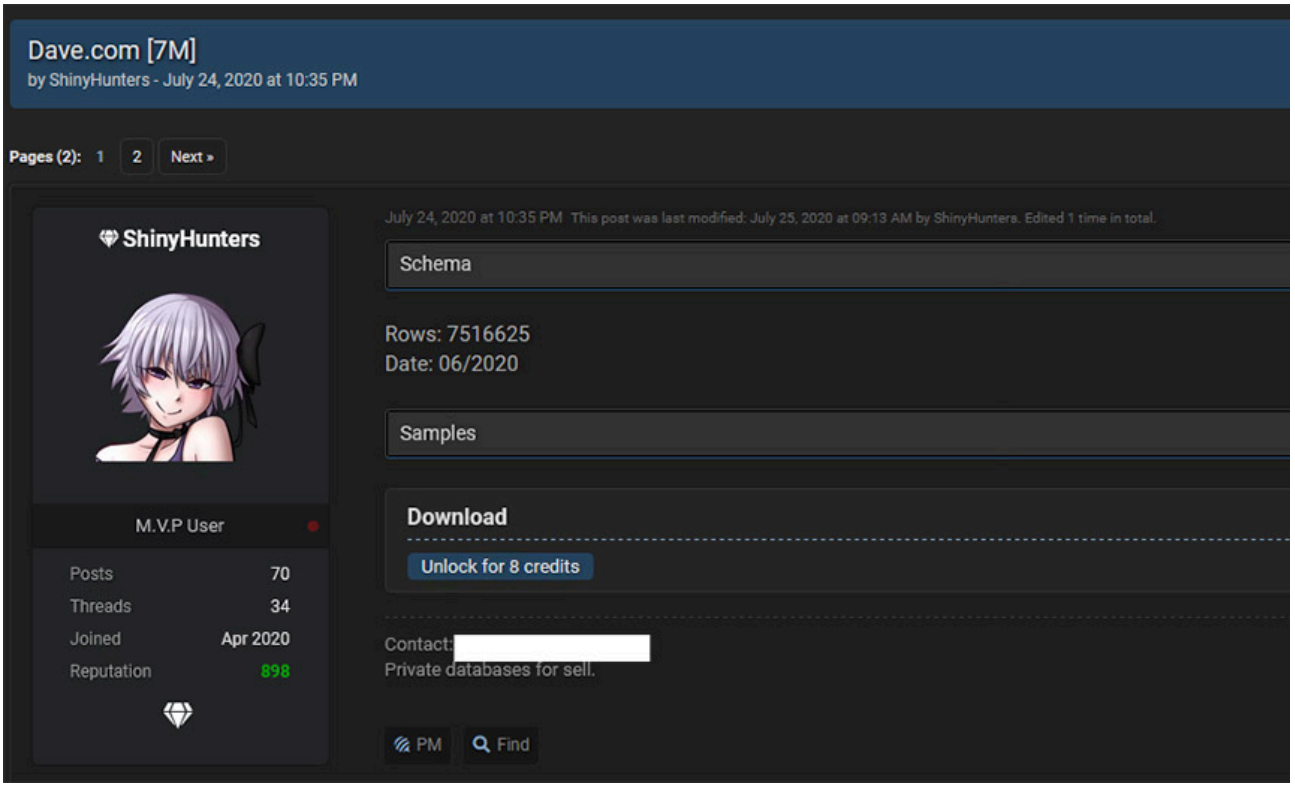
ShinyHunters' Big Year

Many of last year's biggest hits apparently trace back to one gang: ShinyHunters.

"ShinyHunters first rose to prominence in May 2020 by attempting to sell a number of valuable databases on the dark web," Risk Based Security says. "Dubbed 'stage 1' by the threat actor, they promised more databases in the future. While the dark web marketplace listings caught the attention of the media, ShinyHunters had already begun to leak databases on dark web hacking forums."

More attacks soon followed last year: Risk Based Security says ShinyHunters was ultimately connected to six attacks from April to May, 25 attacks in July and 16 attacks from October to November.

Last July, for example, the group hit Dave, a mobile-only banking startup with a valuation of more than $1 billion, exposing 3 million accounts. Dave blamed the intrusion on "a breach at Waydev, one of Dave's former third-party service providers."



Stolen data from Dave for sale on RaidForums (Source: ZeroFOX)

Another example: Last November, ShinyHunters hit India's online grocery delivery service BigBasket, posting purported details of 20 million customers online.

Big January Breaches

ShinyHunters already looks set to dominate this year's data breach charts.

The gang's operations have continued with a hit against e-commerce store Bonobo, owned by Walmart, which sells men's clothing. Last month, ShinyHunters posted stolen Bonobo data to cybercrime forum RaidForums, including account information for nearly 2 million registered users, Bleeping Computer reported.

Also last month, the group disclosed a hit against dating site MeetMindful.com. In a Jan. 20 post to RaidForums, ShinyHunters posted a link to a 320MB "mindful.7z" archive, containing details on 1.4 million accounts and exposing information for 2.3 million users of the service.

MeetMindful confirmed the breach on Jan. 24 and recommended all users change their passwords. It said some users' names, email addresses, Bcrypt-hashed passwords, Facebook access tokens and geolocation information, among other details, had been exposed.

Historical Breaches Surface

More ShinyHunters hits from 2020 are also coming to light.

In January, for example, a RaidForums user called "Spiral" posted what they said was the set of data exposed in the September 2020 breach of Australian PDF-creation service Nitro, which the user said had been "dumped by

ShinyHunters." That data dump contained 70 million unique email addresses, as described by free breach notification site Have I Been Pwned, run by security expert Troy Hunt, who received the information from a security researcher.

"This is the same database that Troy Hunt has, including all the users, contacts, filenames and so on," Spiral claimed of the dump.

In October 2020, cybersecurity intelligence firm Cyble told Bleeping Computer that the stolen information was being privately auctioned with a start price of $80,000. But ShinyHunters later offered it for free.

On Feb. 5, another RaidForums user named "sl4ckto" posted what the user said was all of the records stolen from the Sept. 4, 2020, breach of Singapore-based hotel booking and management platform RedDoorz. That breach reportedly resulted in the theft of a database with 5.8 million user records. And sl4ckto said ShinyHunters was responsible, again offering the data for free.

Stolen Data: For Sale, Then Free

"ShinyHunters has made a number of posts about being frustrated that people were reselling their data, so they release it for free or dirt cheap," Zack Allen, director of threat intelligence at ZeroFOX, told me last year.

But marketing savvy is a more likely explanation for why the group releases data for which it has already been paid, and which has gone into wide circulation - at least via cybercrime forums. "They will breach a company, sell the data privately, then once that breach becomes more available, they will leak it to still build hype," Allen said.

While it's the early days for breaches in 2021, so far, ShinyHunters appears to be continuing to run with that data breach playbook.
