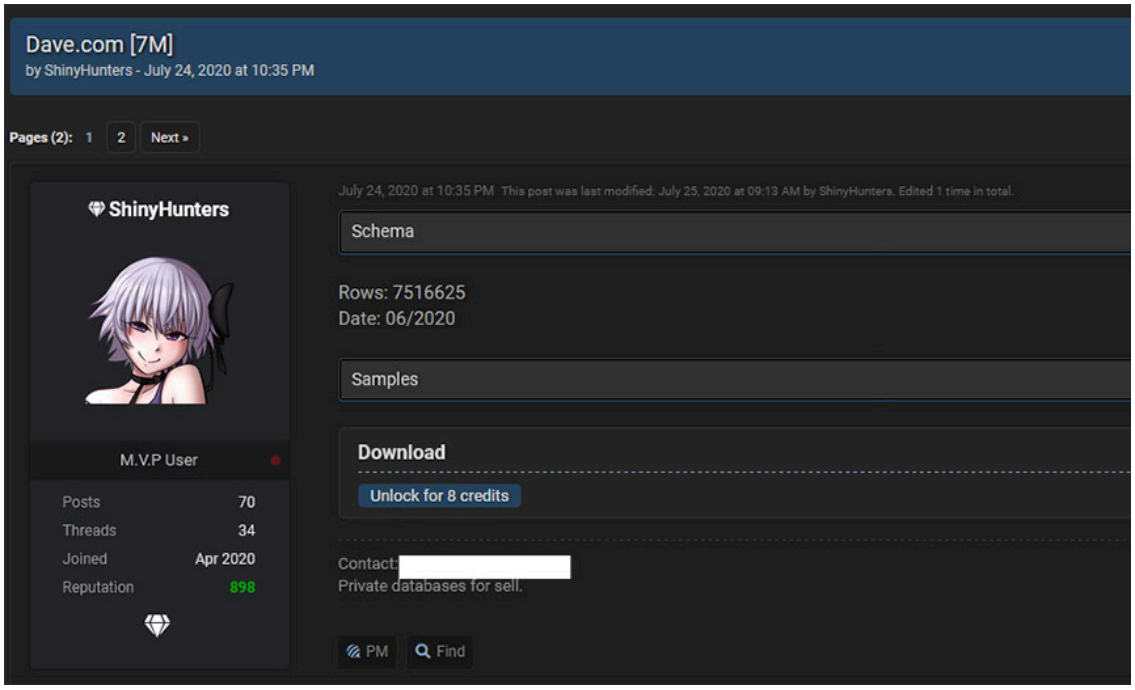
Anatomy of a Breach: Criminal Data Brokers Hit Dave

By Mathew J. Schwartz

Account Takeover Fraud , Application Security , Cybercrime

Evidence Points to 'ShinyHunters' Hacking Team Phishing Employees of Mobile Bank (euroinfosec) • July 28, 2020



Stolen data from Dave for sale on a cybercrime forum (Source: ZeroFox)

The hack of mobile banking startup Dave appears to be just the latest in a long line of breaches tied to data brokers who make money from selling stolen data to fraudsters.

See Also: OnDemand | Transform API Security with Unmatched Discovery and Defense

The mobile-only banking startup - valued at $1 billion - has confirmed the breach. But Dave's first data breach notification, issued Saturday, offers few specifics about how it happened, except to say that attackers were able to access its network "as the result of a breach at Waydev, one of Dave's former third-party service providers." (See: *Dave: Mobile Banking App Breach Exposes 3 Million Accounts*)

Dave says that an unspecified number of its 7 million users' "names, emails, birth dates, physical addresses and phone numbers" were exposed, although no payment card data, bank account numbers or Social Security numbers were stolen. But breach notification site Have I Been Pwned has analyzed a batch of stolen Dave data in circulation and counted 7.5 million rows of data, resolving to information on about 3 million unique users.

Security experts say the individual or group called ShinyHunters appears to have been behind the attack against Dave, as well as the attempt to first sell stolen data, and then simply dumping it online for free, or nearly free.

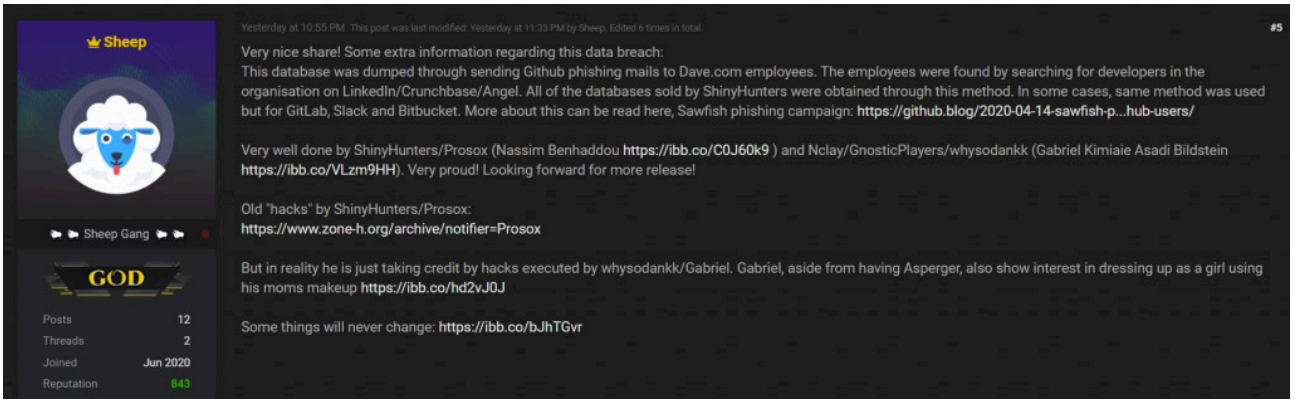
"The database was initially on an auction by the alias ‘hasway’ at the hacking forum 'exploit,' and later was removed [from] auction. Cyble believes the alias belongs to ShinyHunters," the security firm says in a blog post. "On July 24, things took an interesting turn when ‘ShinyHunters’ leaked the database of Dave.com and others. The leaked user records have been put up for free."

Cyble says it spotted the data circulating on an underground forum on June 28 and gave Dave a heads-up on July 2.

Dave hasn't yet responded to questions about how it learned of the breach, when the breach began or exactly how attackers stole the data.

How Did Dave's Database Get Dumped?

At the moment, however, some evidence points to ShinyHunters having phished Dave employees. The group has previously advertised - and has been suspected of being behind - the sale of millions of stolen records obtained from Indonesian e-commerce firm Tokopedia, Indian online learning platform Unacademy, Chicago-based meal delivery outfit HomeChef, online printing and photo store ChatBooks, university news site Chronicle.com, as well as Microsoft's private GitHub repositories, according to Baltimore-based security firm ZeroFox.



Post to a cybercrime forum by "Sheep" (Source: Cyble)

How does ShinyHunters steal so much data? Cyble says that in a post to a hacking forum, a user called "Sheep" says of the Dave breach: "This database was dumped through sending GitHub phishing emails to Dave.com employees. The employees were found by searching for developers in the organization on LinkedIn/Crunchbase/Angel. All of the databases sold by ShinyHunters were obtained through this method. In some cases, [the] same method was used but for GitLab, Slack and Bitbucket."

Source: Cyble

As an example, Sheep references an April blog post by GitHub's security incident and response team describing a Sawfish phishing campaign targeting GitHub users.

That phishing campaign used fake messages that said something suspicious may have been happening with a user's account and presented them with a link to "check your activity." Unfortunately, if users click the link, they can fall for an attack that's designed to compromise not just their credentials, but also time-based one-time passwords.

"Clicking the link takes the user to a phishing site mimicking the GitHub login page, which steals any credentials entered," according to the GitHub blog post. "For users with TOTP-based two-factor authentication enabled, the site also relays any TOTP codes to the attacker and GitHub in real-time, allowing the attacker to break into accounts protected by TOTP-based two-factor authentication. Accounts protected by hardware security keys are not vulnerable to this attack."

It's not clear if Sheep might be part of ShinyHunters or somehow privy to its operations, but as described, the MO would seem to be a fit, Cyble says. "While the identities of the group are unconfirmed, based on the interviews Cyble conducted, along with the references made by the alias 'Sheep' (as above), there is a similarity - ShinyHunters group is known to target GitHub accounts and use that to steal access tokens and so forth."

Dave, however, has suggested that it was compromised via a hack of Waydev, a third-party analytics tool for software engineers that it formerly used. Dave didn't immediately respond to a request for comment about when it stopped working with Waydev.

San Francisco-based, Waydev first warned on July 2 that its service may have been breached and users' GitHub OAuth tokens obtained. Waydev says its investigation into the breach found that from June 10 to July 3, attackers may have "cloned repositories from the users who connected via GitHub OAuth."

Not ShinyHunters' First Rodeo

However ShinyHunters hit Dave, this isn't the first time the hacking group has been tied to large databases of stolen user data being sold on cybercrime forums.

In May, for example, the group advertised a massive amount of breached data (see: *Hacking Group Offers Another 27 Million Records for Sale*). As ZeroFox said in a May blog post: "ShinyHunters is taking a page out of the book of gnosticplayers, the breach data broker who in 2018-2019 pilfered billions of records from dozens of companies and sold them online."

Recently, ShinyHunters also advertised 22 million records stolen from promotional video creation site Promo.com, which has confirmed the breach, saying it began on July 21.

Since then, ShinyHunters has advertised more than 20 million additional records for sale. On Monday, ShinyHunters "made a number of posts on a known hacking and cybercriminal forum advertising additional breaches," including a count of stolen records, ZeroFox says. Here's the list:

- Appen.com: 5.8 million records;
- Scentbird.com: 5.8 million;
- Vakina.com.br: 4.8 million;
- Drizly.com: 2.4 million;
- Havenly.com: 1.3 million;
- Truefire.com: 600,000;
- Proctoru.com: 444,000.

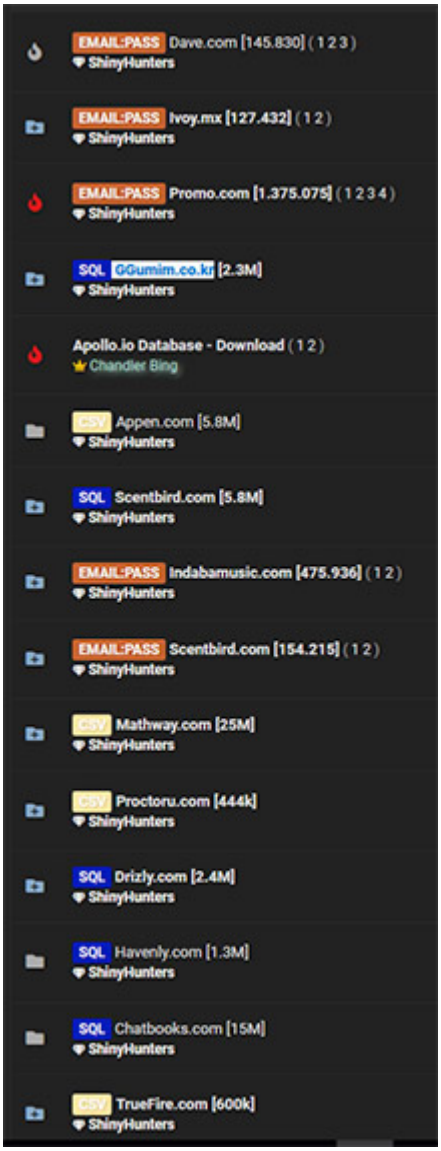
It's not clear when all of those breaches occurred, although the Appen breach happened in 2017, according to ZeroFox. It says each of the above breached record sets are now being sold for 8 credits, or the equivalent of about $2.30, on a cybercrime forum.

"ShinyHunters also posted the Chatbooks breach, previously for sale on Empire Market for $2,000, now [with] a steep discount of 99.9%," ZeroFox told Information Security Media Group on Monday.

The buyers of this stolen data would typically be fraudsters or anyone else who might be able to turn a profit using personally identifiable information. "The type of fraud people can use this for include: account takeovers and credential stuffing, PII harvesting, as well as email harvesting for target lists for phishing, malware and spam," Zack Allen, director of threat intelligence at ZeroFox, tells ISMG.

But the sale prices are notable. Typically, when ShinyHunters would first advertise breach information, it would price it between $1,500 and $2,500, ZeroFox says. "These are 'higher' priced dumps, that are typically traded around by larger brokers," Allen says. "Many of these dumps then get sold for lower and lower prices, until eventually they are released for these cheap prices."

The Economics of Fire Sales



Stolen data being sold by ShinyHunters (Source: ZeroFox)

How can hackers who make money from peddling stolen data afford to sell it for so little, as with the above dumps?

"A fire sale of a dump can usually be traced back to it losing its exclusivity, and the supply rises with the demand; or the dumps aren't worth as much due to strong cryptographic hashing of the passwords," Allen says. "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. This could be the case in [the Dave] dump."

Marketing the name of the group also appears to be a consideration. "ShinyHunters has a playbook that is similar to gnosticplayers," Allen says. "They will breach a company, sell the data privately, then once that breach becomes more available, they will leak it to still build hype."

Those similarities have led cybercrime watchers to ask if there might be a crossover in the membership between the two groups. But in May, ShinyHunters claimed to Wired that there was no connection between the groups, saying instead simply that they'd been inspired by gnosticplayers.