

He Escaped the Dark Web's Biggest Bust. Now He's Back

Andy Greenberg : 14-18 minutes : 9/23/2021

Just over four years ago, the US Department of Justice announced the [takedown of AlphaBay](#), the biggest dark web market bust in history. Thai police arrested the site's 26-year-old administrator, Alexandre Cazes, in Bangkok, and the FBI seized AlphaBay's central server in Lithuania, wiping out a marketplace that was selling hundreds of millions of dollars a year worth of hard drugs, hacked data, and other contraband to its 400,000-plus registered users. The FBI called the disruption of the site a "landmark operation."

But the fate of one key player in that massive black market scheme was never explained: AlphaBay's former number-two administrator, security specialist, and self-described cofounder, who went by the name DeSnake. Now, four years after his market's demise, DeSnake appears to be back online and has relaunched AlphaBay under his own singular leadership. After four years off the radar, he's not keeping quiet about his return.

In an extended chat interview, DeSnake tells WIRED how he walked away unscathed from the takedown of AlphaBay, why he has resurfaced now, and what his plans are for the resurrected, once-dominant online black market. He communicated with WIRED via encrypted text messages, from a frequently changing series of pseudonymous accounts, after proving his identity by [signing a public message with DeSnake's original PGP key](#), which multiple security researchers verified.

"The biggest reason I am returning is to make the AlphaBay name be remembered as more than the marketplace which got busted and the founder made out to have committed suicide," DeSnake writes. Cazes was [found dead](#) of an apparent suicide in a Thai jail cell a week after his arrest; like many in the dark web community, DeSnake believes Cazes was murdered in prison. He was driven to rebuild AlphaBay, he says, after reading about an FBI [presentation on the circumstances of Cazes' arrest](#) that he deemed disrespectful. "AlphaBay name was put in bad light after the raids. I am here to make amends to that."

A kind of practical paranoia permeated DeSnake's messages to WIRED, both on a personal level and in his plans for AlphaBay's revamped technical protections. (DeSnake says he uses male pronouns.) The revived version of AlphaBay, for instance, allows users to buy and sell only with [the cryptocurrency Monero](#), which is designed to be far more difficult to trace than Bitcoin, whose [blockchain has proven to sometimes allow powerful forms of financial tracking](#). AlphaBay's dark web site is now accessible not only via Tor, like the original AlphaBay, but also I2P, a less popular anonymity system that DeSnake encourages users to switch to. He repeatedly described his wariness that Tor may be vulnerable to surveillance, though he provided no evidence.

DeSnake says his security practices—both the ones he's applying within AlphaBay and on a personal level—go far beyond those of his predecessor, Cazes, who went by the online handle Alpha02. Cazes was caught, in part, through Bitcoin blockchain analysis that confirmed his role as AlphaBay's boss, a trick that would be far more difficult, if not impossible, with Monero. DeSnake argues that new safeguards like these will make AlphaBay that much harder to remove from the dark web this time around. "I had given [Cazes] many 'holy grails' of anonymity, but he chose to use only certain things while he branded other methods/ways as 'overkill,'" DeSnake writes, in his seemingly foreign-inflected and occasionally misspelled English. "In this game there is no overkill."

DeSnake credits his ongoing freedom to an operational security regimen that borders on the extreme. He says his work computers run an "amnesiac" operating system, like the [security-focused Tails distribution of Linux](#), designed to store no data. He claims, in fact, not to store any incriminating data on hard drives or USB drives at all, encrypted or not, and declined to explain further how he pulls off

this apparent magic trick. DeSnake also claims to have prepared a USB-based "kill switch" device designed to wipe his computers' memory and shut them off in seconds if they ever leave his control.

To avoid the risk of his PC being grabbed while he's logged into AlphaBay, DeSnake says he also shuts it down entirely every time he steps away from it, even to take a bathroom break. "Biggest issue in that regard is the human needs ... I would say that is the biggest inconvenience," DeSnake writes. "You make sacrifices. Though once you get used to it, it becomes second nature."

After all, law enforcement seized the laptops of Alexandre Cazes and [Ross Ulbricht](#)—the latter is [serving a life sentence](#) for running the original [dark web drug market known as Silk Road](#)—while they were open, running, and logged into administrator accounts on the dark web sites they oversaw. DeSnake, by contrast, makes the very bold claim that his work PC could not implicate him even if seized.

But all of those technical and operational protections may matter less than a simple geographic one. DeSnake claims to be located in a non-extradition country, beyond the reach of US law enforcement. In messages to WIRED, AlphaBay's new boss describes having lived in the former USSR, and he previously wrote Russian-language messages to users on the original AlphaBay's forums.

AlphaBay has long been rumored to have some sort of connections to Russia or Russians. Its rules have always banned the sale of data stolen from victims in former USSR countries, a common prohibition among Russian hackers intended to shield them from Russian law enforcement scrutiny. And when Alexandre Cazes wrote under the Alpha02 moniker on the site, he sometimes signed off with a Russian phrase for "stay safe." But when Cazes was later tracked down in Thailand, many assumed AlphaBay's Russian fingerprints had been designed to mislead investigators.

DeSnake now claims, however, that he and others involved in the original AlphaBay do in fact remain beyond the reach of Western law enforcement. "You do not shit where you sleep," he writes of AlphaBay's rule against selling the stolen data of ex-Soviet citizens. "We did that for security of other staff members. [Cazes] decided to embrace it as a way to secure himself."

Regardless, DeSnake claims that he has traveled to "several continents within the last 4 years" and "had zero problems," leading him to believe that his years of freedom have been a result not only of his location but of having technically outmaneuvered the law enforcement agencies tracking him. Of course, everything DeSnake told WIRED may itself be misdirection designed to help him further evade those agencies.

When WIRED reached out to Justice Department officials, including one who participated in the original investigation of AlphaBay that resulted in its 2017 takedown, they either didn't respond or declined to comment.

While few of DeSnake's claims can be confirmed, he has at least enjoyed unusual longevity for a dark web market operator. Security firm Flashpoint says it has seen evidence and descriptions of DeSnake operating under the same pseudonym—first as a credit-card-focused cybercriminal on sites like Evolution and Tor Carder Forum before becoming a market administrator himself—since at least 2013.

DeSnake first appeared on the original AlphaBay's forums in the fall of 2014, a vendor of credit card fraud—also known as "carding"—tools and guides, looking for a new home after the administrators of Evolution absconded with their users' money in a so-called "exit scam." He says he quickly befriended Alpha02 by an unorthodox method: He claims he "popped a shell" on AlphaBay, hacking the website and gaining a foothold to run his own commands on its server. Rather than exploit that breach, he says, he helped the administrator fix it and soon became the site's number-two admin and security lead. "I took care of the security and certain admin stuff," DeSnake says. "He took care of the rest."

Nearly three years later, Cazes was arrested and the site torn offline, thanks in part to a trail of evidence that began when the AlphaBay founder leaked a personal email address in the metadata of a welcome message to new users on its forums, a problem DeSnake says he had fixed early on by

switching the site's forum software. "I am still in disbelief to this day that he had put his personal email on there," DeSnake says. "He was a good carder and he knew better opsec."

Dark web buyers and vendors haven't exactly flocked back to AlphaBay's since its return. A few weeks into the relaunch, it has just under 500 listings, compared to more than 350,000 at AlphaBay's 2017 peak. Those low numbers likely stem from DeSnake's insistence on accepting only Monero, from skeptical dark web users waiting to see if the new AlphaBay is legitimate, and from a barrage of distributed denial-of-service attacks that have knocked the site offline since its launch. But DeSnake argues that dark web markets typically gain an influx of new users only when another popular market shuts down or is busted by law enforcement; neither has happened since AlphaBay came back.

In the meantime, DeSnake wants to attract users with promises of a still-unproven system he calls AlphaGuard, designed to let users withdraw their funds even if authorities once again seize the servers that run AlphaBay's infrastructure.

As DeSnake describes it, AlphaGuard will automatically rent and set up new servers if it detects that AlphaBay's are being taken offline. He even claims that AlphaGuard will automatically hack other websites and plant data on their servers to give users "withdrawal codes" they can use to save the cryptocurrency they've stored on AlphaBay in case of a takedown. "It is a system to ensure users can withdraw funds, settle disputes, and generally go without a cent lost if raids happen," DeSnake writes, "even if it happens on all servers at the same time. It is unstoppable."

If that AlphaGuard feature doesn't sound aspirational enough, DeSnake says he's also in the early stages of a long-term plan to implement a fully decentralized marketplace system, essentially a BitTorrent to the current dark web markets' Napster. In that hyper-ambitious plan, open source programmers and server operators who independently run hundreds or thousands of servers would be paid a portion of profits for hosting markets that would form a vast dark web network with no single point of failure. AlphaBay, DeSnake says, would be one of the "brands" hosted on that network, but any vendor or market could choose to set up their own, with encryption features that would keep each market or store under that administrator's control even as its code is duplicated across a vast array of machines.

DeSnake has discussed that decentralization project since his earliest posts to the AlphaBay forums, and he acknowledges that it's still years away. But he sees it as a way to both make AlphaBay invulnerable to future law enforcement takedowns and to pay back the dark web's users for the millions they lost when the original AlphaBay server was seized. "When it comes to the money making this is investment in the future of AlphaBay," DeSnake writes. "When it comes to ideology I think that is pretty clear. The reason is to make good to the AlphaBay name ... this is our way to reimburse the darknet scene for what has happened."

But all of the defensive wizardry that DeSnake describes—both AlphaGuard and the decentralization project—remain largely unproven talk, says Flashpoint analyst Ian Gray, who closely monitors dark web markets. The decentralization plan, for instance, would require collective buy-in from a large number of developers and network operators for what would likely be seen as an essentially illegal project. Gray points out that DeSnake hasn't published any code for either that system or AlphaGuard, and questions why he would relaunch AlphaBay four years after its takedown without any real progress toward his decentralization dream. "He hasn't really demonstrated anything besides launching a marketplace," Gray says. "I'm distrustful of DeSnake, and I think across the communities there's a general distrust."

Gray points to a thread on the largely Russian cybercrime forum XSS, where many commenters expressed their skepticism about DeSnake's return, some implying that he's being controlled by law enforcement. "Lol, how many honest comrades will DeSnake have to turn in now to leave the punishment cell?" one commenter asked in Russian. "It's fake and 99.9% sure and feds opening it again," another wrote.

One former US law enforcement official involved in the original AlphaBay investigation, who asked not to be named, also expressed doubts. "If I were a vendor or user on this site, I would be very concerned with it being either set up for an exit scam or some type of honeypot operation," the former

official said, noting that they're not aware of any ongoing law enforcement operations that may be targeting the site.

Nicolas Christin, a dark-web-focused computer scientist at Carnegie Mellon University, verified DeSnake's PGP key against a copy found in his own archive of messages. But that key, he says, could be in the control of law enforcement agencies, or DeSnake himself could have become a law enforcement cooperator. After all, at the same time as AlphaBay's 2017 takedown, the [Dutch police took over and controlled Hansa](#), the second-largest dark web market at the time. "It's unlikely," Christin says of theories that DeSnake is compromised, "but not impossible."





DeSnake counters that if law enforcement had gotten to him and launched the new AlphaBay as a honeypot, they would have simply reused the original AlphaBay's code. Instead, he says, he rewrote it from scratch. And he points out that the Monero-only restriction for the site would make it far less effective for trapping unsuspecting dark web buyers than a site that simply accepts Bitcoin.

"With all of that said you decide for yourself whether you ride the wave with us to the top and beyond," he wrote in a message to users on the dark web market forum Dread. "I understand if you decide not to but over time you will be proven that we are the original AB and we have never been 'compromised' in any way shape or form."

If DeSnake and his revitalized AlphaBay are in fact legit, they may prove to be the opposite of a honeypot: A highly motivated digital black market seemingly beyond the grasp of US law enforcement. And that might well mean that the long track record of one of the dark web's oldest players still has no clear end in sight.

Updated 9-23-2021, 1:10 pm EDT: This story was updated to correct the timing of when Alexandre Cazes was found dead.

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- Can robots evolve into [machines of loving grace?](#)
- 3D printing helps [ultracold quantum experiments](#) go small
- How community [pharmacies stepped up during Covid](#)
- [The Artful Escape](#) is psychedelic perfection
- How to send [messages that automatically disappear](#)
-  Explore AI like never before with [our new database](#)
-  WIRED Games: Get the latest [tips, reviews, and more](#)
-  Torn between the latest phones? Never fear—check out our [iPhone buying guide](#) and [favorite Android phones](#)