Who Is the Network Access Broker ‘Babam’?

krebsonsecurity.com/2021/12/who-is-the-network-access-broker-babam/

Rarely do cybercriminal gangs that deploy ransomware gain the initial access to the target themselves. More commonly, that access is purchased from a cybercriminal broker who specializes in acquiring remote access credentials — such as usernames and passwords needed to remotely connect to the target’s network. In this post we’ll look at the clues left behind by “**Babam**,” the handle chosen by a cybercriminal who has sold such access to ransomware groups on many occasions over the past few years.

Since the beginning of 2020, Babam has set up numerous auctions on the Russian-language cybercrime forum **Exploit**, mainly selling virtual private networking (VPN) credentials stolen from various companies. Babam has authored more than 270 posts since joining Exploit in 2015, including dozens of sales threads. However, none of Babam’s posts on Exploit include any personal information or clues about his identity.

But in February 2016, Babam joined **Verified**, another Russian-language crime forum. Verified was hacked at least twice in the past five years, and its user database posted online. That information shows that Babam joined Verified using the email address "**operns@gmail.com**." The latest Verified leak also exposed private messages exchanged by forum members, including more than 800 private messages that Babam sent or received on the forum over the years.

In early 2017, Babam confided to another Verified user via private message that he is from Lithuania. In virtually all of his forum posts and private messages, Babam can be seen communicating in transliterated Russian rather than by using the Cyrillic alphabet. This is common among cybercriminal actors for whom Russian is not their native tongue.

Cyber intelligence platform Constella Intelligence told KrebsOnSecurity that the operns@gmail.com address was used in 2016 to register an account at **filmai.in**, which is a movie streaming service catering to Lithuanian speakers. The username associated with that account was "**bo3dom**."

A reverse WHOIS search via DomainTools.com says operns@gmail.com was used to register two domain names: bonnjoeder[.]com back in 2011, and sanjulianhotels[.]com (2017). It's unclear whether these domains ever were online, but the street address on both records was "**24 Brondeg St.**" in the United Kingdom. [Full disclosure: DomainTools is a frequent advertiser on this website.]

A reverse search at DomainTools on "24 Brondeg St." reveals one other domain: **wwwecardone[.]com**. The use of domains that begin with "www" is fairly common among phishers, and by passive "typosquatting" sites that seek to siphon credentials from legitimate websites when people mistype a domain, such as accidentally omitting the "." after typing "www".

A banner from the homepage of the Russian language cybercrime forum Verified.

Searching DomainTools for the phone number in the WHOIS records for wwwecardone[.]com — +44.0774829141 — leads to a handful of similar typosquatting domains, including **wwwebuygold[.]com** and **wwwpexpay[.]com**. A different UK phone number in a more recent record for the wwwebuygold[.]com domain — 44.0472882112 — is tied to two more domains – **howtounlockiphonefree[.]com**, and **portalsagepay[.]com**. All of these domains date back to between 2012 and 2013.

The original registration records for the iPhone, Sagepay and Gold domains share an email address: **devrian26@gmail.com**. A search on the username "bo3dom" using Constella's service reveals an account at **ipmart-forum.com**, a now-defunct forum concerned with IT products, such as mobile devices, computers and online gaming. That search shows the user bo3dom registered at ipmart-forum.com with the email address **devrian27@gmail.com**, and from an Internet address in Vilnius, Lithuania.

Devrian27@gmail.com was used to register multiple domains, including **wwwsuperchange.ru** back in 2008 (notice again the suspect "www" as part of the domain name). Gmail's password recovery function says the backup email address for devrian27@gmail.com is **bo3*******@gmail.com**. Gmail accepts the address **bo3domster@gmail.com** as the recovery email for that devrian27 account.

According to Constella, the bo3domster@gmail.com address was exposed in multiple data breaches over the years, and in each case it used one of two passwords: "**lebeda1**" and "**a123456**".

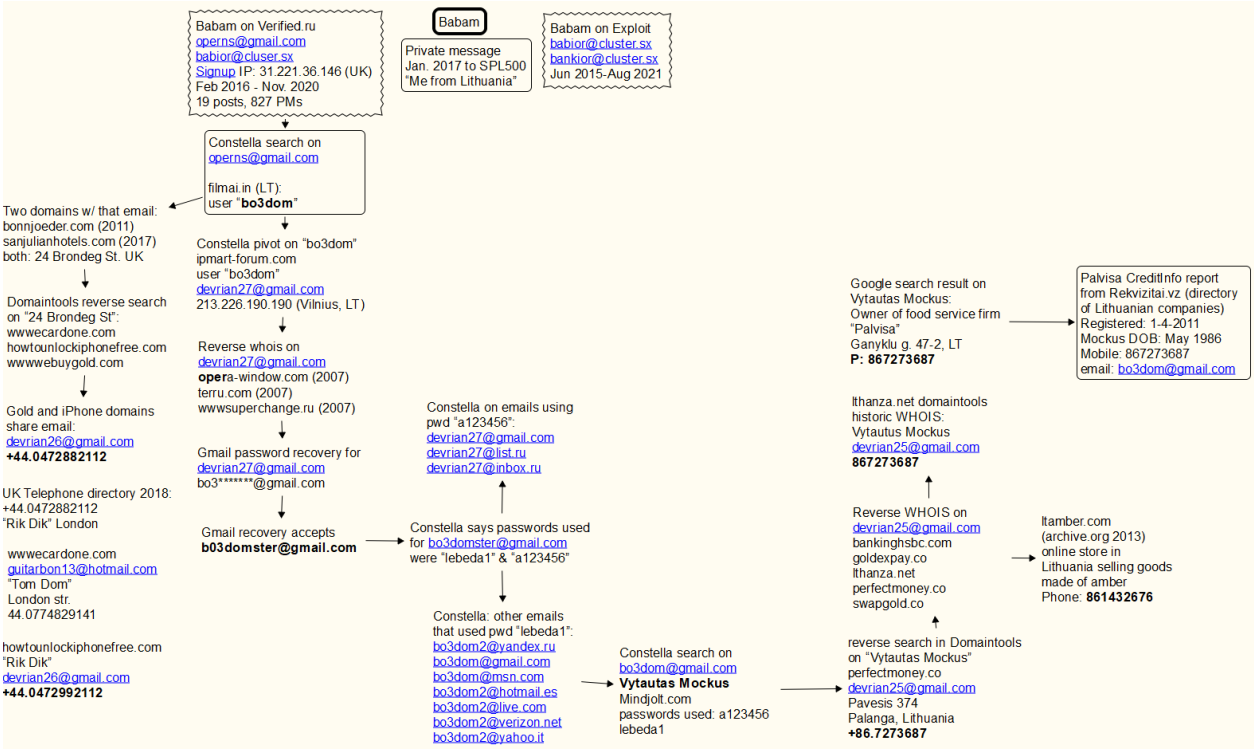
Searching in Constella for accounts using those passwords reveals a slew of additional "bo3dom" email addresses, including **bo3dom@gmail.com**. Pivoting on that address in Constella reveals that someone with the name **Vytautas Mockus** used it to register an account at mindjolt.com, a site featuring dozens of simple puzzle games that visitors can play online.

At some point, mindjolt.com apparently also was hacked, because a copy of its database at Constella says the bo3dom@gmail.com used two passwords at that site: **lebeda1** and **a123456.**

A reverse WHOIS search on "Vytautas Mockus" at DomainTools shows the email address **devrian25@gmail.com** was used in 2010 to register the domain name **perfectmoney[.]co**. This is one character off of perfectmoney[.]com, which is an early virtual currency that was quite popular with cybercriminals at the time. The phone number tied to that domain registration was "**86.7273687**".

A Google search for "Vytautas Mockus" says there's a person by that name who runs a mobile food service company in Lithuania called "**Palvisa**." A report on Palvisa (PDF) purchased from **Rekvizitai.vz** — an official online directory of Lithuanian companies — says Palvisa was established in 2011 by a Vytautaus Mockus, using the phone number **86.7273687**, and the email address bo3dom@gmail.com. The report states that Palvisa is active, but has had no employees other than its founder.

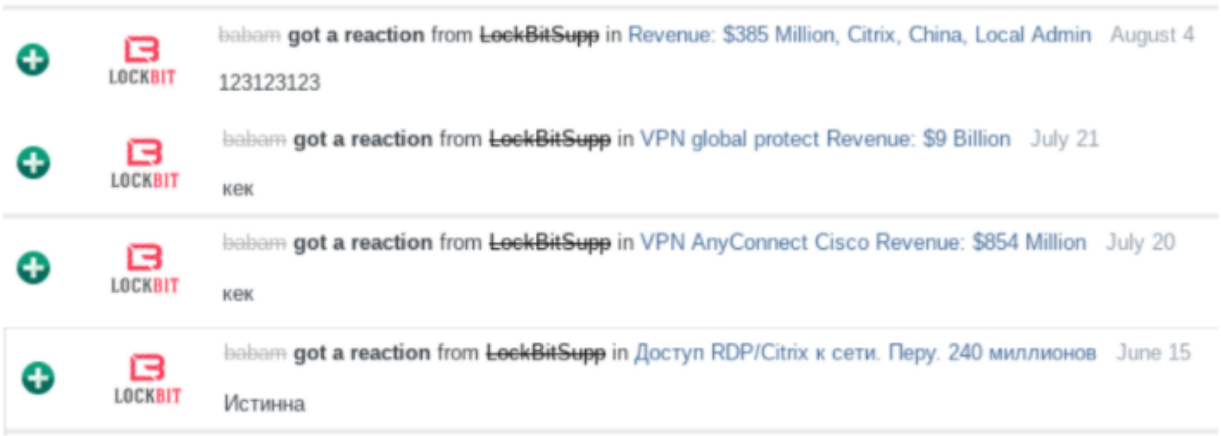
Reached via the bo3dom@gmail.com address, the 36-year-old Mr. Mockus expressed mystification as to how his personal information wound up in so many records. "I am not involved in any crime," Mockus wrote in reply.



A rough mind map of the connections mentioned in this story.

The domains apparently registered by Babam over nearly 10 years suggest he started off mainly stealing from other cybercrooks. By 2015, Babam was heavily into "carding," the sale and use of stolen payment card data. By 2020, he'd shifted his focus almost entirely to selling access to companies.

A profile produced by threat intelligence firm Flashpoint says Babam has received at least four positive feedback reviews on the Exploit cybercrime forum from crooks associated with the LockBit ransomware gang.



The ransomware collective LockBit giving Babam positive feedback for selling access to different victim organizations. Image: Flashpoint

According to Flashpoint, in April 2021 Babam advertised the sale of Citrix credentials for an international company that is active in the field of laboratory testing, inspection and certification, and that has more than $5 billion in annual revenues and more than 78,000 employees.

Flashpoint says Babam initially announced he'd sold the access, but later reopened the auction because the prospective buyer backed out of the deal. Several days later, Babam reposted the auction, adding more information about the depth of the illicit access and lowering his asking price. The access sold less than 24 hours later.

"Based on the provided statistics and sensitive source reporting, Flashpoint analysts assess with high confidence that the compromised organization was likely **Bureau Veritas**, an organization headquartered in France that operates in a variety of sectors," the company concluded.

In November, Bureau Veritas acknowledged that it shut down its network in response to a cyber attack. The company hasn't said whether the incident involved ransomware and if so what strain of ransomware, but its response to the incident is straight out of the playbook for responding to ransomware attacks. Bureau Veritas has not yet responded to requests for comment; its latest public statement on Dec. 2 provides no additional details about the cause of the incident.

Flashpoint notes that Babam's use of transliterated Russian persists on both Exploit and Verified until around March 2020, when he switches over to using mostly Cyrillc in his forum comments and sales threads. Flashpoint said this could be an indication that a different person started using the Babam account since then, or more likely that Babam had only a tenuous grasp of Russian to begin with and that his language skills and confidence improved over time.

Lending credence to the latter theory is that Babam still makes linguistic errors in his postings that suggest Russian is not his original language, Flashpoint found.

"The use of double "n" in such words as "проданно" (correct – продано) and "сделанны" (correct – сделаны) by the threat actor proves that this style of writing is not possible when using machine translation since this would not be the correct spelling of the word," Flashpoint analysts wrote.

"These types of grammatical errors are often found among people who did not receive sufficient education at school or if Russian is their second language," the analysis continues. "In such cases, when someone tries to spell a word correctly, then by accident or unknowingly, they overdo the spelling and make these types of mistakes. At the same time, colloquial speech can be fluent or even native. This is often typical for a person who comes from the former Soviet Union states."