Seven 'no log' VPN providers accused of leaking – yup, you guessed it – 1.2TB of user logs onto the internet

theregister.com/2020/07/17/ufo_vpn_database

A string of "zero logging" VPN providers have some explaining to do after more than a terabyte of user logs were found on their servers unprotected and facing the public internet.

This data, we are told, included in at least some cases clear-text passwords, personal information, and lists of websites visited, all for anyone to stumble upon.

It all came to light this week after Comparitech's Bob Diachenko spotted 894GB of records in an unsecured Elasticsearch cluster that belonged to UFO VPN.

The silo contained streams of log entries as netizens connected to UFO's service: this information included what appeared to be account passwords in plain text, VPN session secrets and tokens, IP addresses of users' devices and the VPN servers they connected to, connection timestamps, location information, device characteristics and OS versions, and web domains from which ads were injected into the browsers of UFO's free-tier users.

UFO stated in bold in its privacy policy: "We do not track user activities outside of our site, nor do we track the website browsing or connection activities of users who are using our Services." Yet it appears it was at least logging connections to its service – and in a system anyone could access if they could find it.

More than 20 million entries were added a day to the logs, according to Comparitech, and UFO happens to boast on its website it has 20 million users. Diachenko said he alerted the provider to the misconfiguration on July 1, the day he found the unprotected database, and heard nothing back.

Oh, it gets worse

A few days later, on July 5, the data silo was separately discovered by Noam Rotem's team at VPNmentor, and it became clear the security blunder went well beyond UFO. It appears seven Hong-Kong-based VPN providers – UFO VPN, FAST VPN, Free VPN, Super VPN, Flash VPN, Secure VPN, and Rabbit VPN – all share a common entity, which provides a white-labelled VPN service.

And they were all leaking data onto the internet from that unsecured Elasticsearch cluster, VPNmentor reported. Altogether, some 1.2TB of data was sitting out in the open, totaling 1,083,997,361 log entries, many featuring highly sensitive information, it is said.

This exposed cluster contained, we're told, at least some records of websites visited, connection logs, people's names, subscribers' email and home addresses, plain-text passwords, Bitcoin and Paypal payment information, messages to support desks, device specifications, and account info.

"Each of these VPNs claims that their services are 'no-log' VPNs, which means that they don’t record any user activity on their respective apps," Rotem's team said. "However, we found multiple instances of internet activity logs on their shared server. This was in addition to the personally identifiable information, which included email addresses, clear text passwords, IP addresses, home addresses, phone models, device ID, and other technical details."

Using a free VPN? Why not skip the middleman and just send your data to President Xi?

READ MORE

VPNmentor created an account with one of the providers, and spotted that new account in the logs, specifically "an email address, location, IP address, device, and the servers we connected to." VPNmentor alerted the providers involved to get the cluster removed from public view, as well as HK-CERT, though it seems no action was taken to immediately rectify the situation.

On July 14, Diachenko, we're told, warned UFO VPN's hosting provider that the database was unsecured, and the next day, it all disappeared from sight, some 18 days after the system appeared in search engine Shodan.io.

UFO VPN, for one, blamed the coronavirus for preventing its staff from securing the database's networking. "Due to personnel changes caused by COVID-19, we’ve not found bugs in server firewall rules immediately, which will lead to the potential risk of being hacked," it said in a statement. "And now it has been fixed."

UFO also claimed its logs were kept for traffic-performance monitoring only, and were anonymized even though some of the log entries seemingly contained people's IP addresses, and account tokens and secrets. So that's going from "no logs" to "OK, some logs," we note.

The provider also insisted there were no clear-text account passwords in the logs, so that

data must be something else, such as a session token, and that "some feedback sent by users themselves contain email addresses, however, the number is very small, less than one per cent of our users."

Comparitech and VPNmentor disagreed, with the latter saying UFO's statement was "incorrect." "Based on some sample data, we do not believe this data to be anonymous," Comparitech's Paul Bischoff added. "We recommend UFO VPN users change their passwords immediately, and the same goes for any other accounts that share the same password."

Finally, it's worth mentioning UFO's software is developed by Dreamfii HK Limited, which receives all the aforementioned VPN providers' sales transactions, and appears to ultimately control those VPN brands. Dreamfii could not be reached for comment.

'Widespread'

Kenneth White, a security researcher, told us the misconfiguration revealed just how dishonest some VPN providers can be, and that netizens should dose up on more than a bit of skepticism, and not fall for the marketing hype, when selecting an organization through which they'll tunnel their internet traffic.

"It's disappointing but honestly not terribly surprising to see yet another breach from a popular commercial VPN service," White, who is also security principal at MongoDB, told *The Reg* in a personal capacity.

"In this case, the effects are even more widespread because of a common industry practice called white labeling, in which smaller VPN providers rebrand a larger service and piggy back on their network, infrastructure, and software. In this case, there seem to be at least seven VPN providers whose customer data was leaked, completely contrary to their marketing claims of 'no logging.'"

"The vast majority of companies that operate these services use patently false marketing, have very murky corporate provenance, and in some cases are literally run by convicted financial crime felons, so of course they will claim 'strong privacy and security' protections when in fact they offer neither," he continued.

"The few providers that have undergone some sort of third-party audit are at best able to show a narrow point-in-time snapshot of some portion of their technology. It's well known in the industry that highly placed search-engine ad campaigns for VPN services routinely fetch upwards of seven figures. The average consumer is simply outmatched, and these companies prey on people's fears. It's a disgrace."

White was also scathing on Twitter:

> not even that in many cases. As @notdan & others have demonstrated, some of the most popular providers can't even get split tunneling correct and literally dual home your internal interface. You connect and suddenly your entire home LAN allows ingress from _any_ other VPN user.
>
> — Kenn White (@kennwhite) July 17, 2020

The Register suggests savvy readers wishing to encapsulate at least part of their traffic may want to roll their own VPNs using Trail of Bits' Algo, Google's Outline, or WireGuard, all of which are open source.

Or use a VPN provider, and build into your threat model the fact it can see everything your ISP would otherwise be able to see. ®