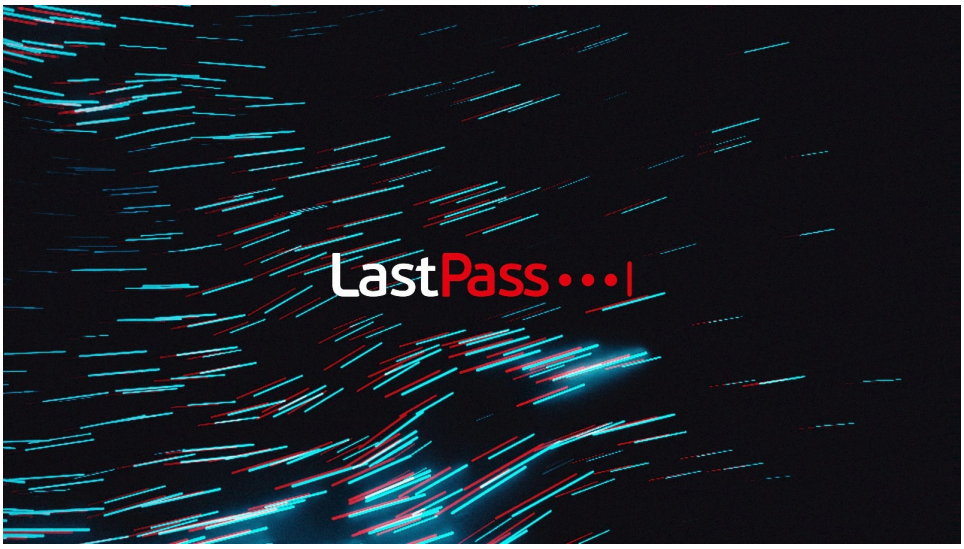
Lastpass says hackers accessed customer data in new breach

By
Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)

November 30, 2022 04:24 PM 9

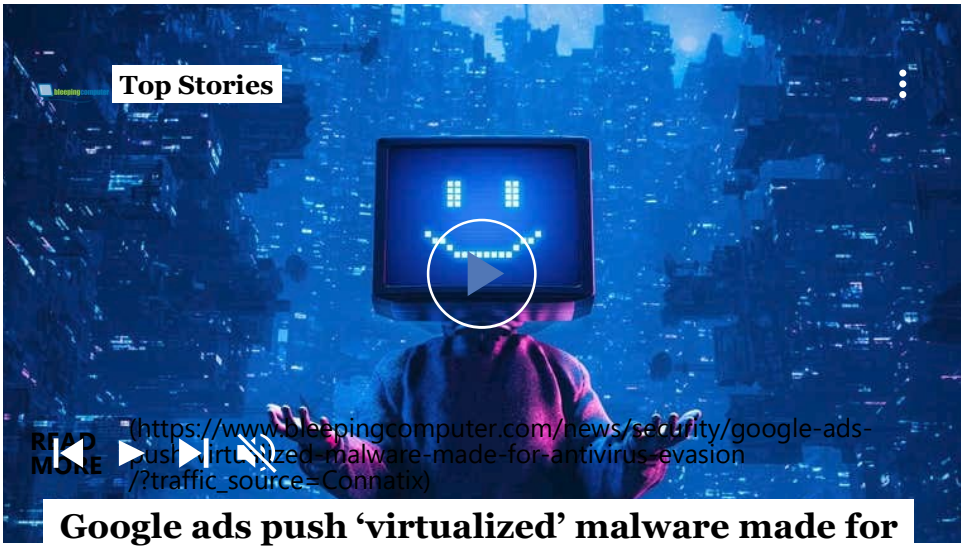


LastPass says unknown attackers breached its cloud storage using information stolen during a previous security incident from August 2022.

The company added that, once in, the threat actors also managed to access customer data stored in the compromised storage service.

"We recently detected unusual activity within a third-party cloud storage

service, which is currently shared by both LastPass and its affiliate, GoTo," the company said (https://blog.lastpass.com/2022/11/notice-of-recent-security-incident/).



"We have determined that an unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers' information."

Lastpass said it hired security firm Mandiant to investigate the incident and notified law enforcement of the attack.

It also noted that customers' passwords have not been compromised and "remain safely encrypted due to LastPass's Zero Knowledge architecture."

"We are working diligently to understand the scope of the incident and identify what specific information has been accessed," Lastpass added.

> *We recently detected unusual activity within a third-party cloud storage service, which is currently shared by both LastPass and its affiliate GoTo. Customer passwords remain safely encrypted due to LastPass's Zero Knowledge architecture. More info: https://t.co/xk2vKa7icq (https://t.co/xk2vKa7icq) pic.twitter.com/ynuGVwiZcK (https://t.co/ynuGVwiZcK)*
>
> *— LastPass (@LastPass) November 30, 2022 (https://twitter.com/LastPass/status/1598047380305104896?ref_src=twsrc%5Etfw)*

Breached twice in one year

This is the second security incident disclosed by Lastpass this year after confirming in August (https://www.bleepingcomputer.com/news/security/lastpass-developer-systems-hacked-to-steal-source-code/) that the company's developer environment was breached via a compromised developer account.

The advisory was published days after BleepingComputer reached out to the company and received no response to questions regarding a possible breach.

In emails sent to customers at the time, Lastpass confirmed the attackers had stolen source code and proprietary technical information from its systems.

In a subsequent update, the company revealed (https://www.bleepingcomputer.com/news/security/lastpass-says-hackers-had-internal-access-for-four-days/) that the attackers behind the August security breach maintained internal access to their systems for four days until they were evicted.

LastPass is behind one of the most popular password management software, claiming that it's being used by more than 33 million people and 100,000 businesses.

Related Articles:

Lastpass: Hackers stole customer vault data in cloud storage breach (https://www.bleepingcomputer.com/news/security/lastpass-hackers-stole-customer-vault-data-in-cloud-storage-breach/)

Riot Games receives ransom demand from hackers, refuses to pay (https://www.bleepingcomputer.com/news/security/riot-games-receives-ransom-demand-from-hackers-refuses-to-pay/)

Chick-fil-A investigates reports of hacked customer accounts (https://www.bleepingcomputer.com/news/security/chick-fil-a-investigates-reports-of-hacked-customer-accounts/)

CloudSEK claims it was hacked by another cybersecurity firm (https://www.bleepingcomputer.com/news/security/cloudsek-claims-it-was-hacked-by-another-cybersecurity-firm/)

U.S. No Fly list shared on a hacking forum, government investigating (https://www.bleepingcomputer.com/news/security/us-no-fly-list-shared-on-a-hacking-forum-government-investigating/)

BREACH (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/BREACH/)

CLOUD STORAGE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CLOUD-STORAGE/)

LASTPASS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/LASTPASS/)

SECURITY BREACH (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SECURITY-BREACH/)

(https://www.bleepingcomputer.com/author/sergiu-gatlan/)

SERGIU GATLAN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/SERGIU-GATLAN/)
(MAILTO:SERGIU@BLEEPINGCOMPUTER.COM) (HTTPS://TWITTER.COM/SERGHEI)

Sergiu Gatlan has covered cybersecurity, technology, and a few other topics for over a decade. Email or Twitter DMs for tips.

PREVIOUS ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/NEW-WINDOWS-MALWARE-ALSO-STEALS-DATA-FROM-VICTIMS-MOBILE-PHONES/)

NEXT ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/CRITICAL-RCE-BUGS-IN-ANDROID-REMOTE-KEYBOARD-APPS-WITH-2M-INSTALLS/)

Comments

Mr.Tom (https://www.bleepingcomputer.com/forums/u/828767/mrtom/)
- 2 months ago

So I take it the attackers got the encrypted customer passwords? Just the main password to access the account, or everything contained in each person's account?

If they grabbed that information anyway, how long do you think it'll take them to decrypt that information? If I had passwords stored in there, I'd be changing every single one of them right now, because, you just never know.

You know they've been compromised, so just assume all your passwords have been compromised too.

ChipBoundary (https://www.bleepingcomputer.com/forums/u/1266810/chipboundary/)
- 2 months ago

Your reading comprehension failed you here. They specifically said the passwords are not compromised. The ONLY thing accessed was customer information.

Passwords are not that.

"It also noted that customers' passwords have not been compromised and "remain safely encrypted due to LastPass's Zero Knowledge architecture.""

bayinfo (https://www.bleepingcomputer.com/forums/u/1266818/bayinfo/) - 2 months ago

Sure, but the 'hackers' only need to work out a single password to gain access to all of that customers other passwords, right?

And the stolen 'user information' will make the process of obtaining that one password much easier, either by 'security questions' or a social engineering/phishing attack.

ChipBoundary (https://www.bleepingcomputer.com/forums/u/1266810/chipboundary/) - 2 months ago

LastPass doesn't use security questions, it uses 2FA. Master passwords aren't accessible to LastPass employees at any level. Not back doors, not recoveries, nothing. They can never access it and have no way to obtain it even with their access. There was no way for the hackers to gain access to any password of any type. Also, if you fall for social engineering, that's on you as an individual and NOBODY else. If you're smart enough to be using an encrypted password manager, you're not dumb enough to fall for social engineering.

On top of that, every single website in existence experiences regular breaches. LastPass is just one of the few with the balls to admit when it happens.

xues (https://www.bleepingcomputer.com/forums/u/1266884/xues/) - 2 months ago

You trust Lastpass a little too much without being able to verify anything via their source code. How do you know they don't have a backdoor have you looked at the source code that was stolen in August

2022 or work there as a dev? They sure aren't on github like BitWarden is => https://github.com /bitwarden/server (https://github.com/bitwarden /server). It's possible they added a backdoor to comply with the PRISM program that Snowden uncovered. Why make the server code closed source, what do they have to hide? With Bitwarden, you can compile and host it yourself anywhere in the world, outside if the 9-eyes if you wish.

JustCallBen (https://www.bleepingcomputer.com /forums/u/986427/justcallben/)
- 2 months ago

Although core data for my previously deleted account was not available to the hackers, I am extremely elated to have left LastPass after the previous breach.

I sleep soundly knowing that I migrated to a more secure platform for encrypted password management. I'll leave to you to figure that out; I'm no shill.

SoftwareEngineer248 (https://www.bleepingcomputer.com /forums/u/1265904 /softwareengineer248/)
- 2 months ago

How do you know that your new password manager is more secure than Last Pass? Unfortunately, all software has security bugs and all computers can be hacked given enough time and effort. The same is true for password managers. Even if you run a password manager locally on your own machine, your machine can be hacked and the passwords can be stolen.

ChipBoundary (https://www.bleepingcomputer.com /forums/u/1266810 /chipboundary/)
- 2 months ago

Yeah, your other password managers aren't any more secure than any other in terms of functionality. All software has security vulnerabilities, ESPECIALLY open source stuff. Putting source code out there is beyond stupid when it comes to security software of any type. It broadens your attack surface exponentially.

This PRISM program you're so paranoid about isn't what you believe it to be. The ONLY way they can collect information is with a specific court order, targeting specific individuals. On top of that, there isn't anything to comply with. That's not how the act PRISM functions under works. It's merely a judge issuing a court order for a company to turn over information regarding a specific user.

They cannot demand encryption keys to the algorithm. This has already been demonstrated in court, that agencies have no authority to request that information. So it's established case law and already specifically addresses this concept.

On top of that, LastPass uses a zero-knowledge architecture, like almost every password manager uses. Meaning their software was designed from the ground up with zero ability for them to obtain customer information. It's like how certain VPN's design their network to not collect logs in the first place, so there's literally nothing to turn over.

LastPass couldn't comply with a court order to turn over customer passwords if they wanted to, as they don't have the ability to.

Wannabetech1 (https://www.bleepingcomputer.com/forums/u/1162770/wannabetech1/)
- 2 months ago

I agree with you about L.P. I've used it for years, though I am not a tech pro. But, concerning PRISM, aren't you trusting the government to do things the "right way"? They certainly have the ability to collect data without permission.

ChipBoundary (https://www.bleepingcomputer.com/forums/u/1266810/chipboundary/)
- 2 months ago

It's not about trusting the government, it's about trusting the civilian company. Encryption can't be just decrypted at will. You either need the encryption key, or there needs to be a security flaw in the

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

encryption algorithm that can be exploited for them to get into the secure password databases. Which is to say, that's the same with ANY encryption. You cannot brute force modern encryption.

PRISM is a big nothingburger, because they have to follow legal standards. If they do something illegal, that's on them and that's no different than hackers hitting you. Also, if they do something illegal, any prosecution they attempt would be null and void.

You may also like:

POPULAR STORIES

New Nevada Ransomware targets Windows and VMware ESXi systems
(https://www.bleepingcomputer.com/news/security/new-nevada-ransomware-targets-windows-and-vmware-esxi-systems/)

Google Fi data breach let hackers carry out SIM swap attacks
(https://www.bleepingcomputer.com/news/security/google-fi-data-breach-let-hackers-carry-out-sim-swap-attacks/)

LATEST DOWNLOADS

Malwarebytes Anti-Malware (https://www.bleepingcomputer.com/download/malwarebytes-anti-malware/)

Version: 4.5.21

4M+
DOWNLOADS

AdwCleaner (https://www.bleepingcomputer.com/download/adwcleaner/)

Version: 8.4.0.0

56M+
DOWNLOADS

Windows Repair (All In One) (https://www.bleepingcomputer.com/download/windows-repair-all-in-one/)

Version: 4.13.1

2M+
DOWNLOADS

Everything Desktop Search (https://www.bleepingcomputer.com/download/everything-desktop-search/)

Version: 1.4.1.1017

22,118
DOWNLOADS

Zemana AntiLogger Free (https://www.bleepingcomputer.com/download/zemana-antilogger-free/)

Version: 1.8.2.320

52,703
DOWNLOADS

FOLLOW US:

(https://www.bleepingcomputer.com/BleepingComputer)

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)

Uninstall Database (https://www.bleepingcomputer.com/uninstall/)

Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)