Změňte si hesla a prchejte. Po půl roce LastPass přiznal, co jim ukradli

SZ | seznamzpravy.cz/clanek/tech-technologie-internet-zmente-si-hesla-a-prchejte-po-pul-roce-lastpass-priznal-co-jim-ukradli-227282

Správce hesel představuje pro mnohé uživatele vysvobození z nepřehledného a složitého světa internetového zabezpečení. Kdo si ostatně má ta silná a jedinečná hesla pamatovat? Aplikace hesla uloží a zašifruje, takže pak člověku stačí jen jedno hlavní heslo zvané master password.

Pro pohodlnější používání napříč zařízeními pak program pro správu hesel ukládá vaše zašifrovaná hesla v cloudu. A právě tuto zašifrovanou zálohu neznámí útočníci ukradli firmě LastPass, která provozuje zřejmě nejznámější správce hesel.

Své uživatele (kterých je přes 33 milionů) LastPass počátkem března informoval, že došlo k odcizení řady důležitých a citlivých údajů. Firma radí změnit si nejen hlavní heslo, ale raději i všechna hesla, která mají uživatelé uložená v trezoru.

Nejdůležitější informace pro uživatele LastPass

Pokud patříte mezi uživatele LastPass, měli byste v zájmu své bezpečnosti provést následující:

1. Změnit své hlavní heslo
2. U všech svých důležitých účtů zapnout dvoufázové ověření
3. Změnit všechna hesla uložená ve vašem trezoru, počínaje důležitými službami
4. Projít všechna data uložená v trezoru a posoudit, co jejich únik znamená
5. Zvážit přechod na jinou službu, které budete důvěřovat

Seznam Native

Muži po tisíce let pečovali o své vousy různě. Jak si vousy upravujete vy?

Námi oslovení odborníci jdou ve svém doporučení ještě o něco dále: uživatelé LastPass by nejspíše měli změnit i nástroj, který ke správě hesel používají. Pojďme se podívat podrobněji, co se vlastně stalo, jaké riziko hrozí, co mohla firma LastPass udělat lépe a co si z toho mohou odnést běžní uživatelé.

Jak útok začal?

Služba LastPass byla coby správce hesel pochopitelným a častým cílem hackerů. Tomu měly odpovídat i její bezpečnostní postupy. Když tedy v srpnu 2022 na firmu zaútočil neznámý hacker, LastPass využil služeb externí bezpečnostní firmy Mandiant a pokusil se zmapovat, co všechno hackeři odcizili.

Hackerovi se podařilo proklouznout do firemního vývojového prostředí, odcizit části zdrojového kódu a dokumentace.

„Útočník exfiltroval 14 z přibližně 200 repozitářů zdrojového kódu různých součástí služby LastPass," uvádí LastPass. Nedošlo k narušení ani odcizení uživatelských dat.

„Incident jsme prohlásili za uzavřený a začali jsme se soustředit na další nápravná opatření, abychom posílili bezpečnostní pozici našeho prostředí," uvedla firma. Jenže z pohledu útočníka to byl teprve začátek.

Jak se hacker dostal ke „korunovačním klenotům"?

Útočník nebo útočníci využili informace získané během prvního útoku a vytipovali si konkrétního klíčového vývojáře firmy LastPass. Zaútočili na jeho domácí síť prostřednictvím tři roky neaktualizovaného přehrávače Plex. To hackerovi umožnilo přístup na jeho domácí síť.

„K útoku došlo na domácím počítači a k získání přístupu byla použita zranitelnost v multimediálním softwaru Plex," uvedl Michal Cebk, bezpečnostní analytik společnosti ESET. „Z praxe a minulosti lze odhadovat, že motivem k takovému útoku může být krádež dat s cílem finančního zisku z jejich následného prodeje."

Něco takového by se nemělo pokročilému uživateli stát, ale je velmi těžké zabezpečit se 100% proti dlouhodobému a cílenému útoku. Problém však byl, že tento zaměstnanec byl jedním ze čtyři lidí, kteří měli přístup ke všem zálohám LastPass. A navzdory obvyklým zásadám pro zabezpečení tento přístup využíval i z domova.

Když tedy útočník na jeho domácí počítač na dálku nainstaloval keylogger (nástroj na odposlech stisků klávesy), získal postupně přístup k zašifrovaným zálohám. A začal si je stahovat.

„Skutečnost, že k průniku došlo pomocí keyloggeru, který umožnil získat přístup k hlavnímu heslu firemního trezoru z jiného než firemního počítače, poukazuje na problémy s firemní kulturou a s přístupem k zabezpečení ," Chris Cowling, etický hacker, který se ve firmě Unicorn Systems zabývá testováním zabezpečení.

Možnost zaměstnance přistupovat z domácí sítě k nejdůležitějším zálohám, označuje řada expertů za hlavní prohřešek firmy LastPass. Je to svým způsobem podobné, jako kdyby byla bezpečnostní firma pověřena hlídáním korunovačních klenotů, a členové ochranky si je vzali na víkend domů a položili si je v obýváku na stolek.

Co všechno hackeři ukradli?

Protože není přesně jasné, jak velkou část záloh hackeři odcizili, je nutné vycházet z toho, k čemu měli přístup. A ten seznam není krátký. Pro běžné uživatele je ale nejdůležitější, že útočníci měli k dispozici zálohy uživatelských trezorů a uživatelských informací.

šifrovaná data v trezoru (chráněná hlavním heslem uživatele)	uživatelská jména, uživatelská hesla, uložené dokumenty, uložené poznámky, čísla kreditních karet apod.
nešifrovaná data v trezoru	URL uložených stránek, alternativní URL, duplicitní URL, jméno aplikace, jméno a e-mail uživatele, který provedl poslední změnu daného uloženého hesla
další data spojená s uživatelem	uživatelské jméno, uživatelův e-mail, fakturační adresa u platících uživatelů, IP adresa zařízení, která uživatelé používali, telefonní číslo, identifikátor mobilního zařízení a síla šifrování (PBKDF2 iterace),

Zašifrované informace – tedy především hesla – jsou chráněné hlavním heslem (master password) a útočníci k nim nemají okamžitý přístup. Mohou se ale pokusit hesla prolomit.

Bohužel mají útočníci díky nešifrovaným informacím o uživateli ohromné množství informací a mohou si tak vybrat, koho se pokusí „rozlousknout“ dříve.

Dokážou hackeři rozšifrovat moje data?

Na tuto nejpalčivější otázku zatím není odpověď. Firma LastPass radí, aby si uživatelé odpověděli na čtyři otázky:

- je moje hlavní heslo silné a unikátní?
- je moje hlavní heslo šifrované alespoň 600 tisíckrát (tzv. PBKDF2 iterace, lze nalézt v nastavení programu)
- jsou všechna hesla v mém trezoru silná a unikátní?
- používám dvoufázové ověření u LastPass i všech důležitých účtů?

„Odpověděli jste na některou z těchto otázek záporně nebo si nejste jistí?“ ptá se bezpečnostní bulletin. „Pokud ano, podnikněte doporučené kroky, dokud nebudou všechny odpovědi kladné.“

Obecně lze říci, že LastPass používá silnou metodu šifrování hesel. Neplatí to ale pro všechna hesla. Pokud jste si své hlavní heslo delší dobu neměnili, je možné, že byl váš trezor šifrovaný menším počtem iterací. To by útočníkovi mohlo prolamování usnadnit. A počet iterací bohužel vidí, je to součást těch nezašifrovaných dat, ke kterým měl přístup.

Foto: LastPass
Počet iterací při šifrování by měl být dle nového doporučení nastaven alespoň na 600 000.

„A nezapomeňte, že změna hesla nebo počtu iterací dodatečně sama o sobě nepomůže,“ připomíná bezpečnostní expert Michal Špaček. Pokud útočník disponuje zálohou vašeho trezoru, může si zkoušet různá hesla na této záloze, jak dlouho bude chtít.

„Pokud vaše hlavní heslo nebylo v okamžiku pořízení záloh dostatečně silné nebo je na seznamu dříve zneužitých hesel, mohou útočníci získat přístup k archivovanému trezoru a přihlašovacím údajům, které jste v něm uložili,“ vyjmenovává Cowling. „Doporučuji proto resetovat všechna hesla, která máte v trezoru uložena, abyste minimalizovali riziko. Může to být dobrá příležitost vyhodnotit, které účty ještě potřebujete nebo můžete migrovat z ověřování pomocí hesla.“

Zůstat, nebo odejít?

A to nebude jediná věc, kterou budou naštvaní uživatelé přehodnocovat. Otázka se sama nabízí: když už stejně musím resetovat všechna hesla, neměl bych rovnou odejít někam jinam?

Námi oslovení odborníci zdůraznili, že takové rozhodnutí je samozřejmě na daném uživateli. „Jako soukromý uživatel bych po tomto incidentu pravděpodobně ztratil důvěru," říká Michal Čábela, odborník na kyberbezpečnost ze společnosti Deloitte Advisory.

„Z pohledu technického je pravděpodobné, že po takto masivním incidentu došlo k detailnímu vyšetření a zajištění bezinfekčnosti aktuálního prostředí. Zároveň byly pravděpodobně aplikována všechna potřebná bezpečnostní opatření. Nicméně budoucí útok na tuto nebo jinou podobnou službu není možné vyloučit," dodal.

Michal Špaček byl přísnější. „Doporučil bych uživatelům používat správce hesel, který s případnou krádeží trezoru lépe počítá." Jako příklad uvádí nástroj 1Password.

„Tam je k dešifrování hesel v trezoru potřeba nejen hlavní heslo, ale i náhodně vytvořený tajný klíč. Ten je vždy silný. Na rozdíl od hlavního hesla, které uživatel může zadávat častěji a tak si ho zvolí o něco jednodušší," vysvětluje Špaček.

Tajný klíč je uložen na zařízení a uživatel jej zadává pouze jednou, při instalaci na nový počítač nebo mobil.

Přehled některých často doporučovaných správců hesel:

Nástroj	Cena od:	Doporučují
1Password	cca 68 Kč měsíčně	Wirecutter, Tom's Guide, PC Mag
Bitwarden	zdarma, open-source	Wirecutter, Tom's Guide, PC Mag
Dashlane	zdarma	Tom's Guide, PC Mag
Keeper	cca 52 Kč měsíčně	Tom's Guide, PC Mag
KeePassXC	zdarma, open-source	EFF

Rozhodně by uživatelé neměli rezignovat na správce hesel obecně. „Hlavně by se uživatelé neměli vracet k opakování slabých hesel, psaní na lístečky u počítače a podobným metodám," zdůraznil

Čábela. „Pravděpodobnost zneužití slabého hesla je významně vyšší, než že bude někdo přímo ovlivněn útokem podobným tomu, který prožil LastPass.“