LastPass říká, že domácí počítač zaměstnance byl napaden hackery a podnikový trezor

arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault

Dan Goodin

Zvětšit

Leon Neal | Getty Images

LastPass, který se již dostal z narušení, které dalo částečně zašifrovaná přihlašovací data do rukou aktéra hrozby, v pondělí uvedl, že stejný útočník hacknul domácí počítač zaměstnance a získal dešifrovaný trezor dostupný pouze hrstce vývojářů společnosti.

Ačkoli počáteční vniknutí do LastPass skončilo 12. srpna, úředníci s předním správcem hesel uvedli , že aktér hrozby „byl aktivně zapojen do nové série průzkumných, výčtových a exfiltračních aktivit“ od 12. srpna do 26. srpna. neznámému aktérovi hrozeb se podařilo ukrást platná pověření staršímu inženýrovi DevOps a získat přístup k obsahu datového trezoru LastPass. Úložiště mimo jiné umožnilo

přístup ke sdílenému prostředí cloudového úložiště, které obsahovalo šifrovací klíče pro zálohy zákaznických trezorů uložené v kbelících Amazon S3 .

Padne další bomba

„Toho bylo dosaženo zaměřením na domácí počítač inženýra DevOps a využitím zranitelného mediálního softwarového balíčku třetí strany, který umožnil vzdálené spuštění kódu a umožnil aktérovi hrozby implantovat malware keylogger," napsali představitelé LastPass. „Aktor hrozby dokázal zachytit hlavní heslo zaměstnance tak, jak bylo zadáno, poté, co se zaměstnanec autentizoval pomocí MFA, a získat přístup do podnikového trezoru LastPass inženýra DevOps."

Napadený inženýr DevOps byl jedním z pouhých čtyř zaměstnanců LastPass s přístupem do podnikového trezoru. Poté, co se aktér hrozby dostal k dešifrovanému trezoru, exportoval záznamy, včetně „dešifrovacích klíčů potřebných pro přístup k produkčním zálohám AWS S3 LastPass, dalším cloudovým úložným zdrojům a některým souvisejícím kritickým zálohám databází".

Pondělní aktualizace přichází dva měsíce poté, co LastPass vydal předchozí bombovou aktualizaci , která poprvé uvedla, že v rozporu s předchozími tvrzeními útočníci získali data z trezoru zákazníků obsahující jak zašifrovaná data, tak data v prostém textu. LastPass poté uvedl, že aktér hrozby také získal přístupový klíč ke cloudovému úložišti a dešifrovací klíče pro duální úložný kontejner, což umožňuje kopírování zálohovaných dat zákaznického trezoru ze zašifrovaného úložného kontejneru.
Zálohovaná data obsahovala jak nešifrovaná data, jako jsou adresy URL webových stránek, tak uživatelská jména a hesla webových stránek, bezpečné poznámky a data vyplněná formuláři, která měla další vrstvu šifrování pomocí 256bitového AES. Nové podrobnosti vysvětlují, jak aktér hrozby získal šifrovací klíče S3.

Pondělní aktualizace uvedla, že taktika, techniky a postupy použité v prvním incidentu byly odlišné od těch, které byly použity v druhém incidentu, a v důsledku toho nebylo zpočátku vyšetřovatelům jasné, že tyto dva spolu přímo souvisí. Během druhého incidentu použil aktér hrozby informace získané během prvního incidentu k výčtu a exfiltraci dat uložených v segmentech S3.

„Upozorňování a protokolování bylo během těchto událostí povoleno, ale neindikovalo to okamžitě anomální chování, které se při zpětném pohledu během vyšetřování vyjasnilo," napsali představitelé LastPass. "Konkrétně byl aktér hrozby schopen využít platná pověření ukradená staršímu inženýrovi DevOps pro přístup ke sdílenému prostředí cloudového úložiště, což zpočátku ztěžovalo vyšetřovatelům rozlišení mezi aktivitou aktéra hrozby a probíhající legitimní aktivitou."

LastPass se o druhém incidentu dozvěděl z varování Amazonu o anomálním chování, když se aktér hrozby pokusil použít role Cloud Identity and Access Management (IAM) k provedení neoprávněné činnosti.

Další čtení

Plex zavádí reset hesla poté, co hackeři ukradnou data více než 15 milionům uživatelů

Podle osoby informované o soukromé zprávě od LastPass, která hovořila pod podmínkou anonymity, byl mediální softwarový balík, který byl zneužit na domácím počítači zaměstnance, Plex. Zajímavé je, že Plex ohlásil vlastní narušení sítě 24. srpna, pouhých 12 dní po zahájení druhého incidentu. Toto narušení umožnilo aktérovi hrozby přístup k proprietární databázi a odjezd s hesly, uživatelskými jmény a e-maily patřícími některým z jeho 30 milionů zákazníků. Plex je významným poskytovatelem služeb streamování médií, které uživatelům umožňují streamovat filmy a zvuk, hrát hry a přistupovat k jejich vlastnímu obsahu hostovanému na domácích nebo místních mediálních serverech.

Není jasné, zda má narušení Plex nějaké spojení s průniky LastPass. Zástupci LastPass a Plex neodpověděli na e-maily s žádostí o komentář k tomuto příběhu.

Hrozba, která stojí za porušením LastPass, se ukázala jako obzvláště vynalézavá a odhalení, že úspěšně zneužil zranitelnost softwaru na domácím počítači zaměstnance, tento názor dále posiluje. Jak Ars v prosinci doporučil, všichni uživatelé LastPass by si měli změnit svá hlavní hesla a všechna hesla uložená v jejich trezorech. I když není jasné, zda má aktér hrozby přístup k jednomu z nich, opatření jsou oprávněná.

Aktualizace středa 1. března 9:06: Den poté, co byl tento příspěvek zveřejněn, zástupce Plex napsal v e-mailu: „Nebyli jsme kontaktováni společností LastPass, takže nemůžeme mluvit o podrobnostech jejich incidentu. Bezpečnostní problémy bereme velmi vážně a často spolupracujeme s externími stranami, které hlásí velké nebo malé problémy pomocí našich pokynů a programu odměn za chyby. Když jsou po zodpovědném zveřejnění nahlášeny zranitelnosti, řešíme je rychle a důkladně a nikdy jsme nezveřejnili kritickou zranitelnost, pro kterou by ještě nebyla vydána opravená verze. A když jsme měli vlastní incidenty, vždy jsme se rozhodli je rychle sdělit. Nejsme si vědomi žádných neopravených zranitelností a jako vždy vyzýváme lidi, aby nám sdělili problémy podle výše uvedených pokynů. Vzhledem k nedávným článkům o incidentu LastPass,