Pozor na „vylepšený“ WhatsApp

Škodlivou verzi neoficiálního vylepšení populární komunikační aplikace WhatsApp s názvem FMWhatsapp objevila bezpečnostní společnost Kaspersky. Tato modifikace šíří mobilního trojského koně Triada, který stahuje další trojany a může spouštět reklamy, vnucovat předplatné nebo monitorovat SMS uživatele napadeného zařízení.

WhatsApp je jedna z nejoblíbenějších komunikačních aplikací, avšak ne všichni uživatelé jsou s jejími funkcemi zcela spokojeni. Při hledání uživatelsky nejpřívětivější verze mohou být v pokušení nainstalovat si neoficiální úpravy aplikace WhatsApp, které nabízejí více možností než základní verze (např. výběr dynamických šablon nebo čtení smazaných zpráv).

V takových modifikacích jejich tvůrci často zveřejňují různé reklamy, aby zpeněžili svou práci. Toho však na druhé straně využívají i podvodníci, kteří prostřednictvím reklam mnohdy šíří škodlivý kód. Jedním z příkladů je aplikace FMWhatsapp verze 16.80.0, která obsahuje trojan Triada a jednu z reklamních knihoven.

V nebezpečné verzi modifikace FMWhatsapp působí trojan Triada jako prostředník. Nejprve shromažďuje údaje o napadeném mobilním zařízení a pak do něj na příkaz hackera stáhne další trojské koně. Ty mohou samostatně spouštět reklamy, připojovat majitele zařízení k placeným službám nebo se přihlašovat k jeho účtu WhatsApp. Dokážou i zachytit potvrzovací SMS – oběť je tak bezbranná před nelegálními aktivitami, které jsou realizovány prostřednictvím jejího telefonu.

„U této úpravy je pro uživatele těžké rozpoznat potenciální hrozbu, protože aplikace skutečně dělá to, co nabízí: přidává další funkce. Zjistili jsme však, že kyberzločinci začali v těchto aplikacích šířit škodlivé soubory prostřednictvím reklamních bloků. Doporučujeme proto používat pouze komunikační software stažený z oficiálních obchodů s aplikacemi. Ty sice postrádají některé užitečné funkce, ale zpravidla nenainstalují do chytrého telefonu žádný malware,“ uvedl Igor Golovin, bezpečnostní expert společnosti Kaspersky.

Bezpečnostní experti společnosti Kaspersky radí, jak se obecně vypořádat s potenciálním rizikem při stahování aplikací:

– instalujte aplikace pouze z oficiálních obchodů a spolehlivých zdrojů,
– nezapomínejte kontrolovat, jaká oprávnění instalovaným aplikacím udělujete – některá z nich mohou být velmi nebezpečná,
– nainstalujte si do chytrého telefonu spolehlivé mobilní antivirové řešení, např. Kaspersky Internet Security for Android.

To platí nejen pro WhatsApp, ale i pro další aplikace, včetně těch, které se používají v mobilních zařízeních v automatizační technice, např. pro čtení kódů, rozpoznávání obrazu nebo dálkovou konfiguraci a programování nejrůznějších zařízení.

(*ed*)

Cloudový systém Acronis pro sdílení souborů nově s notarizací a elektronickým podpisem

Společnost Acronis uvedla další nové služby v rámci svého systému Acronis Cyber Protect Cloud, které jsou součástí balíčku Advanced File Sync and Share, určeného pro bezpečné sdílení podnikových souborů. Nové funkce notarizace dat a elektronického podpisu umožňují dodavatelům řízených služeb (MSP – *Managed Service Provider*) posílit jejich nabídku.

S tím, jak v reakci na pandemii 88 % organizací poslalo alespoň částečně své zaměstnance pracovat z domova, za posledních osmnáct měsíců silně vzrostla poptávka po službách sdílení a synchronizace souborů. V důsledku toho 67 % podniků zvýšilo výdaje na nástroje vzdáleného přístupu a pro online konferenční hovory. To se ukázalo jako velká příležitost pro ty MSP, kteří dokázali poskytnout služby sdílení včetně zajištění bezpečné kontroly nad datovým úložištěm, přístupem k datům a nastavením oprávnění jednotlivých uživatelů.

Služba „notarizace souborů“ s podporou blockchainu na platformě Ethereum umožňuje klientům ověřit původnost souboru jakéhokoliv formátu a typu a prokázat, že soubor je originální a nezměněný. V současném světě, kdy je zneužíváno digitální editování a metody deep-fake, zabraňuje notarizační služba neoprávněným úpravám dokumentů, záznamů, videí či obrázků.

Služba „elektronický podpis“ poskytuje několika stranám možnost na dálku podepisovat dokumenty. Jednoduše metodou *drag-and-drop* lze řídit oběh dokumentů od jejich vytvoření přes distribuci až po podpis. K zajištění autenticity podpisu a dokumentu služba generuje blockchainový certifikát.

„Je čím dál jasnější, že práce na dálku zůstane významným trendem a MSP budou muset svým zákazníkům zajistit, aby jejich zaměstnanci využívali firemní data produktivně a přitom bezpečně,“ řekl Jan-Jaap Jager, Chief Revenue Office ve společnosti Acronis. „Na rozdíl od tradičních řešení pro sdílení souborů nabízí inovovaný Advanced File and Sync Share možnosti bezproblémové integrace se službami kybernetické bezpečnosti a ochrany dat z jedné centrální konzole.“

Více informací: https://www.acronis.cz/produkt/cyber-protect-cloud/, https://www.acronis.com/en-us/products/cloud/cyber-protect/file-sync-and-share/.

[Tisková zpráva Acronis, srpen 2021.]

(*ed*)