ESET software spol. s r.o.
Classic 7 Business Park
Jankovcova 1037/49, Praha 7
www.eset.cz

ESET varuje před nebezpečnou aplikací QRecorder, cílí na české uživatele a jejich internetové bankovnictví

Praha 25. září 2018 – Bezpečnostní analytici společnosti ESET upozorňují na na rizikovou aplikaci, která je ke stažení v oficiálním obchodě Google Play. Nástroj pro nahrávání hovorů QRecorder se po některé z posledních aktualizací stal pro uživatele hrozbou, která umožňuje útočníkům vzdálený přístup do bankovního účtu napadeného uživatele. Tuto hrozbu ESET detekuje již při instalaci aplikace jako Android/Spy.Banker.AIX. Nástroj QRecorder určený pro mobilní zařízení na platformě Android může mít jen v České republice na desítky tisíc uživatelů.

„Podařilo se nám zachytit nástroj na nahrávání hovorů QRecorder. Na základě naší interní analýzy můžeme říci, že původně legitimní aplikace byla tzv. ztrojanizovaná. To znamená, že po jedné z posledních aktualizací se z QRecorderu stal tzv. trojský kůň. Ten umožňuje útočníkům stáhnout do chytrého telefonu s operačním systémem Android nebezpečný obsah, což se také děje," říká Miroslav Dvořák, technický ředitel české pobočky společnosti ESET.

Z analýzy bezpečnostních specialistů společnosti ESET, která stále probíhá, prozatím vyplynulo, že malware v telefonu čeká na zašifrovaný příkaz z tzv. C&C serveru útočníka, na základě kterého vykoná požadovanou aktivitu. V první fázi škodlivý kód zjišťuje, zda jsou v telefonu aplikace, které mohou být pro útočníky zpeněžitelné a nemusí se jednat pouze o bankovní aplikace. Následně je do telefonu stažen modul, který vytvoří neviditelnou vrstvu nad cílovou aplikací, například internetovým bankovnictvím, a snímá přihlašovací údaje uživatele. Útočníci dále mají přístup do sms zpráv, které jsou nejčastějším druhým ověřovacím faktorem při převodech peněz. Útočníkům tedy nic nebrání, aby si vzdáleně posílali peníze z účtu napadeného uživatele na cizí bankovní účty bez jeho vědomí.

„Útočníci pomocí tohoto malware cílí primárně na uživatele z České republiky, Polska a německy mluvících zemí. Respektive cílí na každého, kdo má přednastavenou českou, polskou či německou jazykovou lokalizaci operačního systému Android. Cílení na české uživatele je přitom výjimečné," dodává Dvořák.

Způsob, jak se uživatel může bránit, není v tomto případě jednoznačný. Aplikace byla stažena z legitimního zdroje Google Play a dříve nepředstavovala žádné riziko. Kromě instalace bezpečnostního softwaru proto představuje jedinou cestu důsledná kontrola požadovaných oprávnění aplikace s ohledem na její primární a legitimní účel.

O společnosti ESET

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Ten drží rekordní počet ocenění a díky němu může více než 100 milionů uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy včetně mobilních a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích. ESET se stal první společností, která díky dlouhodobě vysoké úrovni ochrany získala 100 ocenění prestižního magazínu Virus Bulletin VB100. Za těmito úspěchy stojí zejména dlouhodobé investice do vývoje. Jen v České republice nalezneme tři vývojová centra a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

ESET software spol. s r.o.
Classic 7 Business Park
Jankovcova 1037/49, Praha 7
www.eset.cz

Kontakt pro média:

Ondřej Šafář
PR manažer
ESET software
tel: +420 233 090 264
tel: +420 702 206 705
ondrej.safar@eset.cz

Jan Potůček
Account Manager
TAKTIQ COMMUNICATIONS
Tel: +420 606 222 928
jan.potucek@taktiq.com