Kaspersky odhalil, jak phishing obchází dvoufaktorové ověřování

14.6.2024 - Darko Natalic | PROTEXT

Dvoufaktorové ověřování (2FA) je bezpečnostní funkce, která se stala standardní metodou pro online zabezpečení. Vyžaduje, aby uživatelé kromě obvyklého přihlášení jménem a heslem potvrdili svoji totožnost ještě dalším způsobem.

Dvoufaktorové ověřování (2FA) je bezpečnostní funkce, která se stala standardní metodou pro online zabezpečení. Vyžaduje, aby uživatelé kromě obvyklého přihlášení jménem a heslem potvrdili svoji totožnost ještě dalším způsobem, například jednorázovým heslem (OTP) zaslaným prostřednictvím textové zprávy, e-mailu nebo ověřovací aplikace. Tato dodatečná úroveň zabezpečení má chránit účty uživatelů i v případě, že dojde k odhalení jejich hesla. Podvodníci nyní našli způsoby, jak uživatele přimět k prozrazení těchto OTP a tím ochranu pomocí 2FA obejít.

Kyberzločinci postupují tak, že se nejprve snaží získat přihlašovací údaje oběti a její telefonní číslo prostřednictvím phishingu nebo úniku dat. Často používají podvodné webové stránky, které vypadají jako legitimní přihlašovací rozhraní do bank, e-mailových služeb nebo jiných online účtů. Pokud oběť zadá svoje uživatelské jméno a heslo, útočníci tyto informace zachytí v reálném čase. Pomocí získaných údajů se pak sami přihlásí k účtu oběti, čímž spustí odeslání OTP na její telefon.

V tomto okamžiku vstupuje do hry tzv. OTP bot, což je nástroj, který podvodníci používají k vyzvídání OTP pomocí technik sociálního inženýrství. OTP bot zavolá oběti, předstírá, že je zástupcem důvěryhodné organizace, a pomocí připraveného dialogu se ji snaží přesvědčit, aby mu OTP sdělila. Pokud je OTP bot úspěšný, útočník se kontrolní jednorázové heslo dozví a použije ho pro přístup k účtu oběti.

Podvodníci dávají přednost telefonátům před textovými zprávami, protože telefonáty zvyšují šanci, že oběť zareaguje rychle. Bot dokáže napodobit tón a naléhavost legitimního hovoru, takže bývá přesvědčivější než člověk.

Podvodníci si mohou OTP boty pronajmout a ovládají je prostřednictvím speciálních online panelů nebo platforem pro zasílání zpráv, jako je Telegram. Tito boti mají různé funkce a plány předplatného. Lze je přizpůsobit tak, aby se vydávali za různé organizace, používali více jazyků nebo mluvili mužským či ženským hlasem. Mezi pokročilé možnosti patří podvržení telefonního čísla (spoofing), takže identifikace volajícího vypadá jako od legitimní organizace.

Výzkum společnosti Kaspersky ukazuje významný dopad útoků s využitím phishingu a OTP botů. Od 1. března do 31. května 2024 zabránily produkty společnosti 653.088 pokusům o návštěvu stránek generovaných phishingovými nástroji zaměřenými na bankovní sektor. Údaje získané prostřednictvím těchto falešných stránek jsou často využívány při útocích pomocí OTP botů. Ve stejném období technologie společnosti Kaspersky odhalila 4721 phishingových stránek vytvořených nástroji, jejichž cílem je obejít dvoufaktorové ověřování v reálném čase.

Metoda dvoufaktorového ověřování je důležitým bezpečnostním opatřením, nemusí být však zcela spolehlivá. Na ochranu před výše uvedenými podvody Kaspersky doporučuje:

• Neotevírejte odkazy v podezřelých e-mailových zprávách. Pokud se potřebujete přihlásit ke svému účtu, zadejte adresu stránky ručně nebo použijte odkaz v záložce.

• Před zadáním přihlašovacích údajů se ujistěte, že je webová adresa správná a neobsahuje překlepy. Pomocí služby Whois zkontrolujte webové stránky: pokud byly zaregistrovány teprve nedávno, je pravděpodobné, že se jedná o podvod.

• Jednorázová hesla během telefonování nevyslovujte ani nevyťukávejte, ať už volající zní jakkoli přesvědčivě. Skutečné banky a jiné organizace tuto metodu k ověření totožnosti svých klientů nikdy nepoužívají.

• K ochraně organizací všech typů a velikostí před širokou škálou hrozeb použijte EDR a XDR řešení společnosti Kaspersky, zajistí ochranu v reálném čase, přehled o hrozbách, jejich vyšetřování a příslušné reakce na ně. V závislosti na aktuálních potřebách a dostupných zdrojích si můžete vybrat nejvhodnější úroveň produktu a snadno přejít na jinou, pokud se vaše požadavky na kybernetickou bezpečnost změní.

• Investujte do kurzů kybernetické bezpečnosti pro vaše zaměstnance, aby byli informováni o nejnovějších poznatcích. Odborníci na informační bezpečnost si mohou pomocí školení Kaspersky Expert training, prohloubit svoje praktické dovednosti, aby dokázali lépe bránit firmy před sofistikovanými útoky. Můžete si vybrat vhodný formát a věnovat se samostudiu v online kurzech nebo se vzdělávat pod vedením lektora v kurzech pořádaných naživo.

Kontakt pro média

Darko Natalic

Corporate Communications Manager Eastern Europe & Israel at Kaspersky

E-mail: Darko.Natalic@kaspersky.com

ČTK Connect ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.