TISKOVÁ ZPRÁVA

Útoky na klienty bank rapidně narůstají a jsou čím dál sofistikovanější. ČBA, Policie ČR a ESET proto spouští „Kyberkampaň“

Praha, 13. července 2021 – Pandemická situace a s ní spojený přesun lidí do online světa vytvořily ideální podmínky pro hackery a online podvodníky. Z dat České bankovní asociace (ČBA) získaných od jejích členských bank vyplývá, že útoky na klienty bank, kteří z pohledu kybernetické bezpečnosti představují „zranitelný“ článek, rapidně narůstají. Již nyní v červnu dorovnal počet phishingových útoků loňský rok, počet vishingových útoků, kdy se útočníci během telefonického hovoru například vydávají za bankéře či policisty, se dokonce šestinásobně zvýšil. A vyvíjejí se i metody útočníků. Bohužel kvůli nízké informovanosti veřejnosti se ne všem útokům daří systémově zabránit. To je mj. důvodem, proč bankovní asociace spojila síly s Policií ČR a společností ESET a spouští osvětovou „Kyberkampaň“.

Bankovnictví se díky současným technickým možnostem i kvůli aktuální pandemii koronaviru přesouvá z kamenných poboček bank do mobilních telefonů a počítačů. Rozvoj bankovních služeb však bohužel není spojen se stejně rychlým rozvojem klientských znalostí v oblasti kybernetické bezpečnosti. Ta je ze strany řady klientů stále podceňována. V posledních letech tak banky i Policie ČR evidují rapidní nárůst počtu kybernetických útoků směřujících nikoliv na technické zabezpečení bank, ale vůči „nejzranitelnějšímu článku v řetězci“, kterým jsou právě klienti.

„V současné době je zabezpečení bankovních systémů na velmi vysoké úrovni. Z toho důvodu sledujeme dlouhodobě trend zaměření aktivit útočníků na nejzranitelnější článek v celém řetězci – uživatele. Dlouhodobě představují vysoké riziko phishingové emaily a SMS zprávy, podvodné aplikace a různé druhy škodlivých kódů, které cílí jak na osobní počítač, tak chytrý telefon uživatele. Samostatnou a mimořádně nebezpečnou kapitolu představuje tzv. vishing, který z logiky věci obchází veškeré bezpečnostní mechanismy. Klíčová je proto neustálá edukace veřejnosti. Jen v takovém případě můžeme riziko bezpečnostního incidentu minimalizovat,“ říká Robert Šuman, vedoucí pražského výzkumného oddělení společnosti ESET.

Pandemie přinesla nárůst útoků

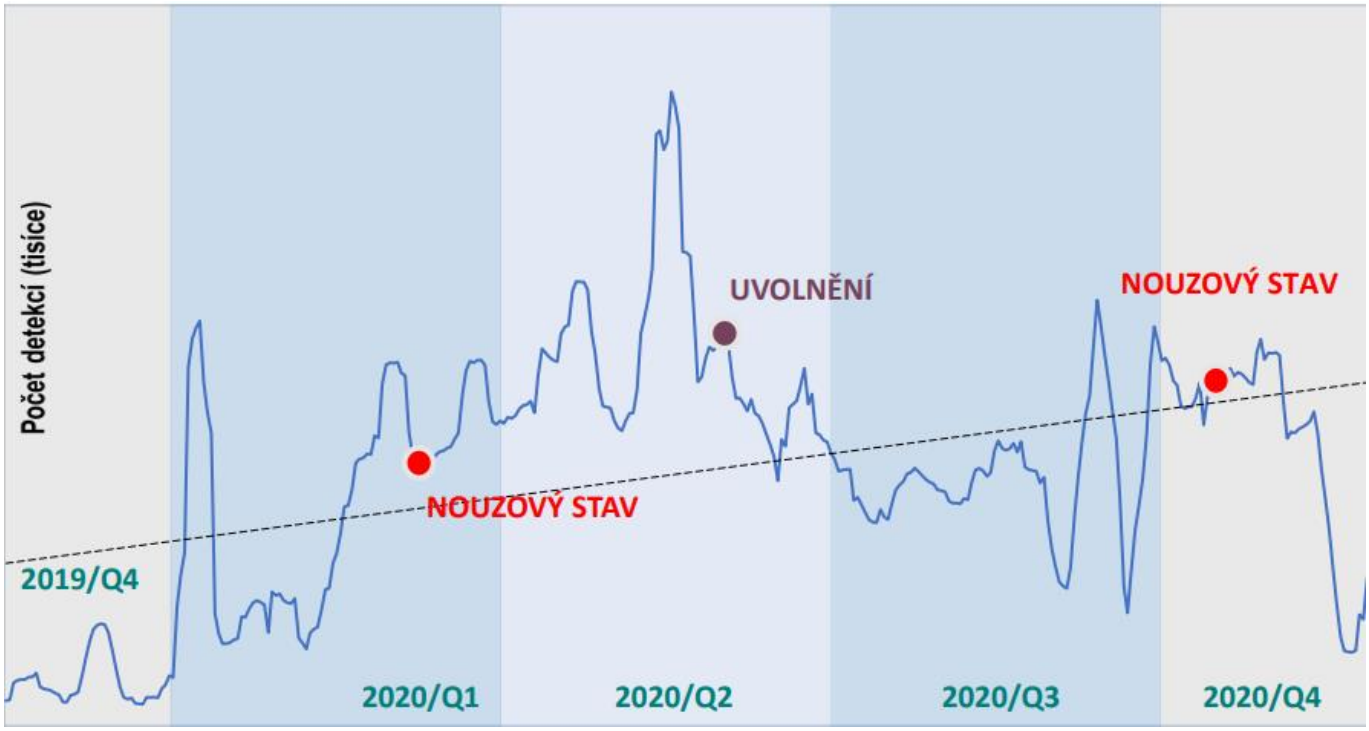
Z průzkumu ČBA mezi jejími členskými bankami vyplynulo, že na jejich klienty v roce 2020 mířilo na tisíce phishingových útoků, což je několikrát více než v roce 2019. Počet útoků v tomto roce, ačkoli jsme zatím v jeho polovině, již celková loňská čísla prakticky dorovnal.

„Pod pojmem phishingový útok na klienta banky se skrývá velké množství typů útoků lišících se svým cílem, nástrojem či technikou. Banky navíc tyto útoky sice evidují, každá ale za použití různé metodiky. Vzhledem k tomu, že o přesnější data má zájem i Policie ČR, zahájili jsme na půdě ČBA konzultace, jejichž cílem bude mimo jiné právě i sladění metodiky vykazování útoků na klienty,“ komentuje Petr Barák, předseda Komise ČBA pro bankovní a finanční bezpečnost, proč celkové počty útoků v tuto chvíli nelze vykázat v přesnějších číslech.

V uvedeném průzkumu banky udávaly počty klientů, kteří se setkali s útokem, při kterém od nich útočníci chtěli získat údaje o platební kartě, či přístupové údaje do internetového bankovnictví skrze podvodné stránky, aplikace, sociální sítě, e-maily apod. a banky se o útocích dozvěděly – buď je samy odhalily dřív, než byly dokončeny, nebo jim byly nahlášeny klienty. Nicméně ve statistice nejsou zahrnuty případy skimmingu, úniky dat ze strany třetích stran, tedy e-shopů apod.

Nicméně masivní nárůst útoků na klienty v posledních letech je i tak z průzkumu zřejmý: *„Nárůst útoků, který banky zaznamenaly v posledním roce, lze přisuzovat zejména kovidové situaci, kdy si útočníci byli dobře vědomi nervozity a zmatečnosti panující ve společnosti, posílené strachem o zdraví či práci – jednoduše řečeno o budoucnost, s níž samozřejmě úzce souvisí i ta finanční,“* komentuje Petr Barák.

Podle společnosti ESET došlo v roce 2020 vlivem celospolečenské situace k přibližně 100% meziročnímu nárůstu detekcí phishingu. *„Phishing nás ohrožuje dlouhodobě. Objem detekovaných hrozeb se liší s ohledem na specifické události během celého roku. V loňském roce útočníci reagovali v České republice například na vyhlašování nouzového stavu a rozvolnění. V návaznosti na tyto události jsme sledovali výrazné nárůsty phishingu. Pokud nás podobné mimořádné události postihnou i v tomto roce, dá se čekat podobný scénář,"* vysvětluje Robert Šuman ze společnosti ESET.



Zdroj: ESET

Díky aktivitě bank a obezřetnosti klientů se daří zastavit naprostou většinu útoků (86 %). Zbývající – dokonané – útoky, při nichž dojde k odčerpání peněz klientovi z účtu, a vznikne tedy klientovi škoda, se často řeší ve spolupráci s Policií ČR. Podle Petra Baráka se útočníkům daří „úspěšně" dokončit zejména útoky mířící na karetní údaje, které jim oběti „prozradí" při online nakupování na stránkách, kde platební brána není odpovídajícím způsobem zabezpečena. *„Současně si je třeba uvědomit, že útoků, respektive pokusů o útok, je ve skutečnosti daleko více, než vykazují dostupná čísla, a banky se o některých vůbec nemusí dozvědět. Například v případě phishingových e-mailů postupují útočníci metodou „kobercového náletu" a jeden phishingový mail tak mohou poslat až na statisíce mailových adres svých potenciálních obětí. Nicméně mají-li klienti svá zařízení dobře zabezpečena, skončí tyto útoky v mailové schránce klienta mezi spamy,"* dodává Petr Barák.

Úspěšné útoky řeší banky se svými klienty individuálně a v maximální možné míře se jim snaží pomoci. V případech, kdy ale prokazatelně dojde na straně klienta k hrubému porušení bezpečnostních pravidel – např. mají uvedený PIN na kartě, stahují programy a aplikace z nedůvěryhodných zdrojů – nelze očekávat, že by banky škodu klientům uhradily. V takových případech je klient se svým požadavkem na náhradu škody odkázán na orgány činné v trestním řízení s tím, že škodu je třeba vymáhat na pachateli trestného činu.

Metody útočníků se vyvíjí, nejzákeřnější je vishing

Kromě zintenzivnění útoků s pomocí tradičních phishingových metod, například podvodné e-maily zneužívající vizuální identitu legitimní bankovní instituce, začali podvodníci v loňském roce používat také tzv. vishing.

Počet vishingových útoků na klienty českých bank se v roce 2020 pohyboval v nízkých stovkách, přičemž úspěšní byli útočníci zhruba v 25 %. Letos úspěšnost těchto útoků poklesla na zhruba 14 %, nicméně prudce narostl jejich počet – jen do konce května bylo útočníky uskutečněno zhruba 6x více útoků než za celý loňský rok.

Vishingové útoky sice nejsou co do počtu tak masivní jako ty phishingové, nicméně finanční ztráty klientů jsou často velmi vysoké. Současně se jedná o metodu, o které mezi veřejností ještě není tak široké povědomí, navíc velmi zákeřnou, neboť útočníci používají různé manipulační techniky, které navíc neustále vylepšují.

„Vishing je technika založená na vyvolání strachu a zpanikaření oběti. Klientovi útočník často volá v neobvyklý čas a vydává se za bankéře, případně policistu. S pomocí osobních údajů o klientovi, které získal například v internetovém prostředí, mnohdy ze sociálních sítí, si získá jeho důvěru. Ten pak snadno uvěří, že jeho účet byl napaden a jediné, co jeho prostředky „zachrání", je jejich odeslání na účet, který mu falešný bankéř sdělí. Útočník klienta následně instruuje, jak transakci autorizovat," přibližuje plk. Mgr. Bc. Luděk Fiala, ředitel úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky. Policie ČR doplňuje, že praktiky útočníků se mohou lišit: *„Útočníci někdy cílí na údaje k platební kartě, jindy na přihlašovací údaje do internetového bankovnictví. Objevují se i případy, kdy útočník svou oběť přesvědčí, aby ze svého účtu vybrala hotovost a vložila ji vkladomatem na bitcoiny."*

„Největší nebezpečí vishingu spočívá v tom, že útočník pomocí zmíněných technik sociálního inženýrství v podstatě oběť přiměje k tomu, aby sama překonala veškeré bezpečnostní bariéry. Pod vlivem strachu, stresu a časové tísně máme bohužel přirozenou tendenci vyhovět hlasu na druhé straně. Alespoň základní povědomí o existenci tohoto typu útoku je nejúčinnější formou obrany proti němu," vysvětluje Robert Šuman z ESETu.

Obzvláště zákeřné pak je, když útočníci při hovorech užívají tzv. spoofing telefonního čísla, při kterém dokážou napodobit jakékoliv telefonní číslo, včetně infolinek bank, takže má-li oběť v telefonu uložené číslo na call centrum své banky, objeví se jí na displeji příchozí hovor její jeho banky. *„Služba změny telefonního čísla, nabízená operátory, je velice nešťastná a často kriminálníky zneužívaná. Ve Velké Británii takto například volali obětem vyděrači pod „spoofovanými" čísly jejich potomků, které fiktivně unesli, a žádali po obětích okamžitě výkupné, samozřejmě pod pohrůžkou, že pokud oběť kontaktuje policii, dítěti ublíží. Rodič pak výkupné rychle zaplatil, ačkoli jeho dítě tou dobou sedělo v pořádku ve škole s mobilním telefonem v aktovce,"* popisuje Petr Barák, proč Česká bankovní asociace zahájila jednání s operátory a Českým telekomunikačním úřadem s cílem zrušit tuto službu, případně ji omezit, či zabezpečit ji proti zneužívání podvodníky. V tomto případě banky totiž nemají možnost, jak klienta ochránit.

Osvěta veřejnosti je nezbytná, spouští se Kyberkampaň

Je zřejmé, že kriminalita se přesouvá z ulic na internet, přičemž toto nebezpečí je ze strany veřejnosti stále značně podceňováno. Z těchto důvodů aktuálně navázala bankovní asociace v oblasti kyberbezpečnosti úzkou spolupráci s Policií ČR a společností ESET. Společně startují preventivní „Kyberkampaní" s hlavním heslem „Cílem útočníka můžete být i vy!". Jejím stěžejním prvkem je webová aplikace Kybertest.cz.

„Tuto aplikaci jsme s ČBA začali vyvíjet v loňském roce, abychom zjistili, nakolik se liší naše domnělá odolnost vůči kybernetickým hrozbám a realita," říká Robert Šuman ze společnosti ESET a upřesňuje: *„Jedná se o speciálně připravený online interaktivní kvíz, ve kterém si může uživatel otestovat, zda při reálně vypadajících simulacích zvládne rozpoznat podezřelé prvky naznačující, že se stal terčem online podvodníků. Kvíz mu v závěru nabídne porovnání s ostatními účastníky, případně více informací k problematice."*

Kampaň bude vedena zejména formou edukativních videí či bannerů na sociálních sítích, upozornění na bankomatech a obrazovkách na pobočkách bank. Osvěta o problematice bude veřejnosti přibližována i prostřednictvím plakátů a letáčků, které distribuují do vybraných míst regionální preventisté Policie ČR. Do kampaně se kromě ČBA, Policie ČR a společnosti ESET zapojí i členské banky ČBA, společnost Zásilkovna, Hospodářská komora ČR a další.

„Útočníky je ve chvíli, kdy jsou útoky dokonány, velmi obtížné odhalit a sankcionovat, natož od nich získat zpět zcizené finanční prostředky jejich obětí. Věříme, že s pomocí této kampaně a další preventivní činností se nám podaří rozšířit povědomí o nebezpečích, která číhají na internetu, a předejít tak škodám a nepříjemnostem, které podvodné vishingové a phishingové útoky způsobují," shodují se zástupci asociace, policie a společnosti ESET.

Není to jen o phishingu a vishingu, na webu Kybertest.cz najdete více o dalších častých metodách útočníků!

Pro bezpečný pobyt v kyberprostoru platí těchto 5 základních zásad:

1. Nikdy nikomu nesdělujte své přihlašovací údaje do internetového bankovnictví ani čísla ze své platební karty. Banky se na ně opravdu NIKDY neptají, a to ani telefonicky, ani e-mailem, ani SMS či jinými zprávami. Zároveň nikdy neposílají odkazy na weby, kde jsou údaje vyžadovány! Ani Policie ČR nikdy občany nevyzývá k provádění bankovních transakcí nebo poskytování osobních údajů dalším osobám!
2. Nereagujte na telefonní hovory, e-maily ani zprávy, kde se vás někdo pokouší vmanipulovat do situace, že jsou vaše finanční prostředky v ohrožení a vy musíte udělat další kroky pro jejich záchranu. Kdyby byly vaše peníze skutečně v ohrožení, banka by již zareagovala dávno a bez vaší pomoci.
3. Nezadávejte a ani v žádné aplikaci nepotvrzujte platby, které vám někdo bude diktovat po telefonu. Stejně tak nedávejte nikomu vzdálený přístup do vašeho počítače.
4. Mějte aktualizovaný software a antivirus v PC i telefonu. Aplikace stahujte jen z oficiálních zdrojů a nedávejte jim více oprávnění, než potřebují.
5. Buďte vždy v pozoru, nenechte se zviklat ani nalákat. V případě pochybností vždy kontaktujte svou banku či volejte Policii (158).

O České bankovní asociaci

Česká bankovní asociace vznikla v roce 1990 a je dobrovolným sdružením právnických osob podnikajících v oblasti peněžnictví. V současné době sdružuje 37 členů. Rolí asociace je především zastupovat a prosazovat společné zájmy členů, prezentovat roli a zájmy bankovnictví vůči veřejnosti, podílet se na standardizaci postupů v bankovnictví a na vytváření odborných zvyklostí, podporovat harmonizaci bankovní legislativy s legislativou Evropské unie a vyvíjet aktivitu v informativní a školící oblasti. ČBA je členem Evropské bankovní federace a EMMI. Více informací na www.cbaonline.cz

O Policii ČR

Policie České republiky je jednotný ozbrojený bezpečnostní sbor zřízený zákonem České národní rady ze dne 21. června 1991. Slouží veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku, chránit veřejný pořádek a předcházet trestné činnosti. Plní rovněž úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, předpisy Evropských společenství a mezinárodními smlouvami, které jsou součástí právního řádu České republiky. Předcházení kriminalitě realizací preventivních aktivit je důležitou součástí činnosti Policie České republiky.

O společnosti ESET

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

Další informace obdržíte na adrese:

Andrea Trudičová
PR a komunikace ČBA
andrea.trudicova@cbaonline.cz
tel: + 420 734 638 103

plk. Zuzana Pidrmanová
vedoucí oddělení prevence
Policejní prezidium ČR
zuzana.pidrmanova@pcr.cz
tel: + 420 974 834 375

Ondřej Šafář
manažer PR a komunikace ESET
ondrej.safar@eset.cz
tel: + 420 776 234 218