ČESKÁ CZECH
BANKOVNÍ BANKING
ASOCIACE ASSOCIATION

TISKOVÁ ZPRÁVA
22.04.2021

ČBA: Útočníci využívají situace. Krádeže osobních dat a s tím související útoky na klienty bank rapidně narůstají

Praha, 22. dubna 2021 – Koronavirová epidemie a s ní zvýšený pobyt lidí v online prostoru představují pro hackery ideální situaci. Značně se proto navýšil počet útoků na organizace i běžné uživatele. Útoky jsou navíc čím dál sofistikovanější. Zatímco v případě institucí dochází zejména k únikům osobních a obchodních dat, v případě obyčejných lidí se útočníci zaměřují nejčastěji na zcizení finančních prostředků na bankovních účtech nebo citlivých dat, například přihlašovacích údajů. Kromě phishingových útoků se navíc čím dál častěji objevuje i tzv. vishing, kdy se s uživatelem spojí útočník napřímo telefonicky a vydává se za zástupce banky.

Přetrvávající pandemie a přesun do online prostředí s sebou přináší dramatický nárůst kybernetických útoků. S útoky tak čím dále častěji bojují sociální sítě, státní instituce, firmy bez ohledu na velikost, ale i třeba nemocnice. Bezpečnostní situaci zkomplikoval mimo jiné přechod na vzdálenou práci.

„Podle dostupných dat začalo během pandemie nově pracovat z domovů 40 % zaměstnanců, u některých firem pracují v současnosti z domova téměř všichni zaměstnanci. Z technologického hlediska je nutné zpřístupnit na dálku různé interní systémy a data, což umožňuje několik technologií, například VPN (virtuální privátní síť) nebo protokoly pro vzdálenou správu RDP,“* říká Petr Barák, předseda Komise České bankovní asociace (ČBA) pro bankovní a finanční bezpečnost.

Právě na RDP (*Remote Desktop Protocol)* se útočníci zaměřili. Jen v lednu a únoru letošní roku zachytili bezpečnostní analytici společnosti ESET v České republice přes 800 milionů pokusů o prolomení protokolu pro práci na dálku. Celkově se jedná o více než 15 tisíc unikátních počítačů, na kterých se podařilo včas útok detekovat a zastavit jej.

„Meziročně sledujeme jednoznačný nárůst. Pokud srovnáme data za první čtvrtletí loňského a letošního roku, počet uživatelů, kteří byli cílem těchto aktivit, se v České republice meziročně zvýšil o 92 procent, ale počet pokusů o útok se za stejné období zvednul bezmála devětkrát. Svědčí to o výrazném zvýšení intenzity aktivity útočníků na české uživatele,“ doplňuje Ondřej Šafář, manažer PR a komunikace společnosti ESET.

Vydírání jako nový nástroj

Institucím a firmám, jejichž bezpečnostní systémy napadením neodolaly, dávají hackeři často možnost ukradená data odkoupit zpět, a to za velmi vysoké částky. Firmy tak často doplácejí na podcenění zabezpečení a nedostatečnou prevenci při práci s daty a ukradená data z jejich systémů končí na tržištích darkwebu.

„Stejně jako pro každého z nás, i pro firmy platí, že by ve svých zařízeních a systémech měly uchovávat vždy pouze to, co je skutečně nezbytné. Pokud data uchovávat nemusí, je bezpečnější je odstranit. Vše ostatní znamená, že se o data musí důsledně starat, tedy řídit riziko nejen obsahu (citlivosti) dat, ale i způsobu jejich uložení, zabezpečení, přístupu k nim a dalšího nakládání s nimi, za což nesou vzhledem k tomu, že jsou v roli jejich zákonného správce, i právní odpovědnost,“ komentuje Petr Barák z bankovní asociace.

V posledním roce útočníci přišli s řadou dalších metod, jak oběti z řad firem a institucí vydírat a vydělat na nich. Příkladem může být zejména doxing.

„Doxing vznikl jako reakce na menší účinnost kampaní využívajících ransomware, což je zjednodušeně řečeno vyděračský software, který blokuje počítačový systém, dokud oběť nezaplatí výkupné. Pokud uživatel či firma ale správně zálohují, ransomware je neohrozí a útočník o šanci na výkupné za opětovné zpřístupnění zašifrovaných dat přijde. Vydá-li se ale útočník cestou doxingu, oběti de facto vyhrožuje zveřejněním takto získaných dat. Což pro firmu představuje reputační riziko, ale i riziko ztráty dat z výzkumu, interních informací, obchodních tajemství a podobně,“ vysvětluje Robert Šuman, vedoucí pražského výzkumného oddělení společnosti ESET.

*Zdroj: https://www.evropavdatech.cz/clanek/70-prace-behem-pandemie/

Na pozoru by se měl mít každý klient banky

Zvýšenou pozornost ochraně svých dat by měli věnovat i soukromí uživatelé. Ukradená data z firem a institucí, jako jsou telefonní čísla, adresy, jména příbuzných ale i hesla, si pak hackeři a další podvodníci dle potřeby různě přeprodávají a následně je používají pro další útoky. *„Přeprodávané informace útočníci vkládají do propracovaných databází a s využitím nejpokročilejší umělé inteligence si pak vybírají co nejsnazší cíle, což jsou v případě bank klienti,*“ popisuje další práci hackerů s ukradenými daty Petr Barák.

Na uživatele internetu v tuto chvíli míří nejen phishingové útoky v podobě masových kampaní s infikovanými e-maily či v podobě falešných stránek, lačnících po přihlašovacích údajích k bankovním účtům a samozřejmě finančních prostředcích na nich, ale čím dál častěji se objevuje i tzv. vishing, což je podvodná technika založená na vyvolání strachu a zpanikaření oběti. Klientovi volá v neobvyklý čas útočník vydávající se za bankéře a s pomocí osobních údajů o klientovi, které získal například z ukradených databází či sociálních sítí, si získá jeho důvěru. Ten pak snadno uvěří, že je jeho účet byl napaden a jediné, co jeho prostředky „zachrání“, je jejich odeslání na účet, který mu falešný bankéř sdělí.

„Tato podvodná technika není tak častá jako phishing, ale vede ke značným škodám – klient může přijít o veškeré prostředky a než si svou chybu uvědomí a kontaktuje banku či policii, jsou již peníze nenávratně pryč,“ komentuje Petr Barák.

„V současné době jsou *útoky sofistikovanou kombinací analýzy ukradených dat, psychologických triků a vhodného načasování. Je to sázka na pravděpodobnost. Čím více o vás útočník ví, tím větší šanci má vás zaskočit ve slabý okamžik a vymámit z vás přístupové údaje,“* vysvětluje Petr Barák a dodává, že základem je nezpanikařit a uvažovat racionálně: *„Banky přihlašovací údaje, PINy ani údaje z platebních karet od klientů nikdy nevyžadují. Stejně tak neposílají v mailech, SMS ani jinak odkazy na stránky, kam mají klienti tyto údaje zadávat. Údaje nikomu na vyzvání neposkytujte a urychleně kontaktujte svou banku – můžete tak pomoci někomu, kdo již tak obezřetný jako vy nebude.“*

Riziko se skrývá v mobilu

Od počátku roku taktéž narůstá objem bankovního malware v mobilních telefonech, jedná se zejména o bankovní trojský kůň Cerberus. V únoru analytici zachytili 40% nárůst detekcí. Tento škodlivý kód dokáže pomocí vysokých oprávnění udělených uživatelem odcizit přihlašovací údaje do internetového bankovnictví a také obejít dvoufázové ověření přihlášení. Proto je důležité dbát také na bezpečnost našich telefonů. Infikované aplikace pocházejí z neoficiálních zdrojů.

„Doporučuji aplikace stahovat výhradně z oficiálních obchodů jako jsou Google Play či App Store a používat renomovaný bezpečnostní software, který potenciální riziko včas odhalí. Uživateli to nepřidělává žádné starosti, ale je to skutečně nejspolehlivější prevence,“ radí Martin Jirkal, vedoucí analytického týmu v české pobočce společnosti ESET. *„Cerberus navíc ohrožuje jen internetové bankovnictví, nikoli aplikace bank. Osobně bych upřednostnil požívání oficiálních bankovních aplikací a ověřování plateb přímo v nich pomocí otisků prstů či FaceID,“* uzavírá.

Pro bezpečný pobyt v kyberprostoru přitom stačí dodržet jen pár základních zásad, viz tzv. DESATERO BEZPEČNOSTI ČBA:

1. **Starejte se o bezpečí svého počítače**
   Nainstalujte a pravidelně aktualizujte antiviry a firewally na svém počítači na nejnovější verzi.
2. **Zabezpečte si mobilní telefon**
   V každém mobilním obchodě s aplikacemi najdete mnoho bezpečnostních aplikací, buď za malý poplatek nebo zdarma.
3. **Ověřujte si původ instalovaných programů a aplikací**
   Jakékoli programy stahujte a instalujte pouze z důvěryhodných a ověřených zdrojů, aplikace jen
4. **Chraňte své přihlašovací údaje**
   Nikomu je nesdělujte, neukládejte je na počítačích ani v prohlížečích a zadávejte je jen na bezpečných serverech.
5. **PIN chraňte jako oko v hlavě**
   PIN by neměl být jednoduchý na uhodnutí. Zároveň ho nikomu nesdělujte, nenechávejte ho poblíž platební karty a střežte ho jako oko v hlavě.
6. **Mějte bezpečné heslo**
   Heslo by mělo být neodhadnutelné, silné (kombinace velkých, malých písmen a znaků), nezjistitelné (př. hackerský program zkouší slova ze slovníku) a především unikátní – nikdy nepoužívejte stejné heslo pro různé služby (př. sociální sítě, e-mail a bankovní účet)! Hesla s nikým nesdílejte a neukládejte je do prohlížeče. Pokud je to možné, zvolte k účtům dvoufaktorové ověřování. Více o tom, jak na silné heslo, zde.
7. **Pozor na neznámé přílohy**
   Neotvírejte e-maily ani přílohy od neznámých a podezřelých odesílatelů, neklikejte ani na žádné odkazy v těle těchto e-mailů.
8. **Nakupujte u prověřených online prodejců**
   Přes internet nakupujte jen u prověřených a důvěryhodných prodejců. Vždy raději zkontrolujte adresu e-shopu, orientujte se také podle bezpečnostního certifikátu.
9. **Čtěte upozornění**
   A to platí nejen pro upozornění vaší banky, ale také pro upozornění vašeho počítače.
10. **Informujte vaši banku**
    Pokud máte, byť jen podezření, že se s vaším účtem děje něco podivného či špatného, kontaktujte svou banku.

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 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:

Monika Petrásková,
manažerka PR a komunikace ČBA
monika.petraskova@cbaonline.cz
tel: + 420 733 130 282

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