Phishing

„Drahoušek Zákazník, Tato is tvuj funkcionár oznámení dle Ceská Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostrední. Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridelil až k tato úcet. Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být deactivated a odstranit. Obnovit se Ted tvuj SERVIS 24 Internetbanking.“

Oslovení Drahoušek Zákazník se stalo téměř ikonickým a s oblibou ho používají všichni, kdo se v oblasti počítačové bezpečnosti pohybují. Výše uvedený e-mail byl v roce 2008 rozeslán z adresy CeskaSporitelna@seznam.cz a vedl na podvodné internetové stránky, kde měl uživatel vyplnit své údaje s přihlášením do internetového bankovnictví a číslo platební karty. V českém prostředí šlo o první velký phishingový útok, který se současně dostal do zájmu veřejnosti.

To na jednu stranu vytvořilo téměř všeobecně známou informaci, že **phishing** je druh útoku, kdy někdo formou e-mailu (dnes stále častěji skrze sociální sítě) láká po uživatelích jejich přihlašovací nebo platební údaje. Jde o velice rozšířený druh útoku a jistě každý ve svém e-mailu najde desítky takových zpráv. Problémem ale je, že druhou rozšířenou informací bylo, že phishing poznáte podle špatné angličtiny nebo češtiny. To ale může i nemusí být pravda, protože dnes jsou útoky mnohem sofistikovanější.

Cílem phishingu je, aby si uživatel otevřel nějaký nebezpečný odkaz (nebo přílohu) nebo se dostal na stránku, kde něco vyplní. To něco mohou být přihlašovací údaje, informace o platební kartě, pin atp. Aby byl takový útok úspěšný, je možné využít dvě základní strategie – kobercový nálet spočívající v tom, že vsadíte na jednoduchý e-mail a někdo se prostě chytí, nebo budete využívat podstatně sofistikovanějších nástrojů.

Například: „Group 74 (známá také jako Sofact, APT28, Fancy Bear) se zaměřila na profesionály v oblasti počítačové bezpečnosti pomocí e-mailu, který předstíral souvislost s americkou konferencí Cyber Conflict, již společně pořádali Vojenský kybernetický institut Vojenské akademie USA, Společná vojenská kybernetická akademie NATO a Centrum excelence společné kybernetické obrany NATO. Přestože je CyCon skutečnou konferencí, byla příloha dokumentem obsahujícím škodlivé makro jazyka Visual Basic for Applications (VBA), který by stáhl a spustil průzkumný malware nazývaný Seduploader.“

Často se používají e-maily, které mají vypadat jako od nadřízených nebo učitelů, případně se pracuje s odkazy, které se jen nepatrně liší od něčeho známého a slavného. **Phishingová stránka** pak vypadá téměř k nerozeznání od té běžné (jedinou šancí je kontrolovat si adresní řádek) a láká k zadání potřebných údajů. A jak je z příkladů patrné, nemusíte být úplní hlupáci, abyste se do nějakého takového útoku namočili, respektive, abyste se nechali ulovit.

Text phishingové zprávy často vypadá jako informace o neodeslané nebo nedoručené zprávě, vyzývá k aktualizaci, zvětšení místa v e-mailu, informace o změně hesla, změně podmínek, výzkum, pozvánka atp. Nejčastějšími diferenčními znaky jsou jednak e-mail odesílatele (třeba ČS asi nebude mít e-mail u Seznamu) a jednak odkaz, který se často liší jen v maličkosti (třeba .cz zaměněné za .com), případně použití zkracovače odkazu (např. bitly).

Jaká základní pravidla tedy dodržet, pokud chcete minimalizovat riziko phishingu?

1. Na odkazy v e-mailu nebo na messengeru neklikejte, pokud nevíte kdo a proč vám je posílá. Buďte velice obezřetní k přílohám.
2. Pokud chcete vstoupit do internetového bankovnictví, běžte do něj přímo. Totéž platí o všech službách.
3. Používejte aktualizovaný software (hlavně prohlížeč a pluginy v něm) a antivir. Nepoužívejte flash.
4. Nevěřte nikomu, pokud vás někdo oslovuje, že vás zná, ale vy jste o něm nikdy neslyšeli.
5. Kontrolujte drobné překlepy v adresách – ať již webových nebo e-mailových.
6. Nikdy neklikejte na URL z e-mailu uváděné skrze zkracovače adres, stejně tak se vyhýbejte QR kódům od osob či institucí, kterým skutečně nedůvěřujete.
7. Pokud se děje cokoli neobvyklého, hlavně v bankovnictví nebo třeba v přihlašování k e-mailu, zbystřete.
8. Přemýšlejte!