Phishing (2)

Vložil/a czokl [1], 14 Listopad, 2005 - 23:25

- Anonymita [2]
- Hacking [3]
- Hacking method [4]
- Phishing & Pharming [5]

Dneska ve druhém a konečném dílu se podíváme na technickou stránku věci.

Technická stránka, aneb phishing není jen o sociotechnice

Veškeré přemlouvání by bylo k ničemu, kdyby útočník založil např.: free ftp účet ve tvaru pavel.vorisek.borec.cz a žádal tam zadání přihlašovacích údajů k homebankingu např.: české spořitelny. Proto se rhybholovníci pokouší udělat vše proto, aby jste se domnívali, že se skutečně nacházíte na správné stránce. Některé hojně používané technické metody si představíme:

Zfalšování hlavičky mailu

- snad každý rhybholovník umí zfalšovat hlavičku e-mailu tak, aby běžný uživatel nepoznal, že políčko "od:" není pravdivé. Jednak na internetu najdete množství nástrojů na poslání takového mailu, jednak se to dá nastavit pomocí PHP, dokonce se to dá provést pomocí telnetu.
Obrana: Stačí si pozorně přečíst hlavičku e-mailu, hlavně dejte pozor na pole recevied:, kde byste měli nalézt razítka všech smtp serverů a tak se dovíte, odkud mail skutečně pochází. Horší je když útočník odesílá mail pomocí smtp serveru, ze kterého Vám může přijít mail i od skutečného poskytovatele (např.: příjde mail od administrator@seznam.cz [6] přes smtp seznamu s phishingovym obsahem). Naštěstí takovéto servery většinou vkládají do hlavičky IP adresu člověka, který daný mail odesílá, řádky s těmito informacemi by měli začínat písmenem X. Bohužel hlubší rozbor hlavičky je nad rámec tohoto článku, možná se k tomu dostanu v některém z dalších článků.

Podobnost

- v tomto případě útočník využívá nepozornost uživatelů. Například si zaregistruje doménu hodně podobnou doméně nějaké instituce/služby a za ní se pak vypadá. V praxi to pak vypadá tak, že např.: stránka www.k-banka.cz [7] je kopie stránky www.kb.cz [8] s tím rozdílem, že jí nespravuje Komereční Banka, ale nějaký vykutálený strejda, který Vám právě krade peníze z účtu :) Nejhorší na tom je, že si toho nemusíte všimnout hned, protože stránka může odkazovat na stránku pravou a tak např.: po zadání přihlašovacích údajů se můžete ocitnout na stránce pravé s se svým účtem normálně pracovat.
Obrana: v tomto případě pomůže asi nejlépe být pozorný a pečlivě si všechno ověřovat. Na takovou stránku se dostanete pravděbodobně z odkazu v e-mailu. Teď jsou minimálně dvě možnosti:
a) mail informuje o nové doméně - v tomto případě je dobré projet doménu databází whois(viz. článek o službách na webu), podívat se na starou doménu, kdyby se přecházelo na jinou, bude tam o tom určitě zpráva nebo přímo kontaktovat administrátory/helpdesk/zákaznickou podporu.
b) neinformuje - v tomto případě si zkontrolujte, jestli daná adresa souhlasí přesně s adresou, kterou normálně k přístupu na službu používáte.

IDN - je zkratka slova International Domain Name a znamená to, že v doménovém jméně se mohou objevovat také národní znaky(kdyby to měla cz doména, mohli byste mít url třeba žluťoučkýkůň.cz), což je na jednu stranu sice fajn, ale horší je, že tento systém je nevychytaný z hlediska převádění znaků na ASCII hodnoty a tak dvě různé domény může browser vyhodnotit jako jednu a tu samou,

což pro rhybholovníky je jako dělané. Více o chybě a test odolnosti Vašeho prohlížeče naleznete Multiple Browsers IDN Spoofing Test">zde [9].

Obrana

jediné řešení, na které tvůrci browseru přišli je pouze vypnutí podpory IDN, což sice není ideální, ale ochrání Vás. Pokud přecejen chcete mít IDN zaplé, musíte pečlivě kontrolovat targety odkazů.

Přihlašování se z jiných stránek

- další věc, kterou se můžete nechat lehce zlákat a dokonce ani nemusíte poznat, že jde o podvod, jsou nabídky přihlásit se ke svému účtu z jiné stránky. Autor stránek se může tvářit jako že Vám prokazuje službu, že zbytečně nemusíte přecházet na další stránku, že se můžete přihlásit přímo přes něj ke své oblíbené službě, dokonce to i povětšinou funguje tak jak má, akorát že autor mimochodem ukládá někam do souboru nebo databáze všechny hesla a uživ.jména, které jeho stránkou projdou.

Chyby, exploity

- Už jsem se tady o něčem zmiňoval (chyba v IDN), oblíbené chyby jsou adres nebo status bar spoofingy, to je když v adres baru (tam kde píšete url) nebo v status baru (lišta dole) se objevují jiné url adresy než na jaké skutečně klikáte(právě případ IDN) nebo nainkludování jiných url do špatně napsaných scriptů, např.: www.domena.tld/script.cgi?redirect=www.jinadomena.tld [10], mimochodem na tuto chybu byl nedávno náchylný obchodní dům e-bay. toto inkludování může být taky ve formě popup oken - pamatujte: do popup oken důvoěrné informace nikdy nevyplňovat, téměř vždy se jedná o podvod. Obrana: Sledovat bezpečnostní servery, které o chybách prohlížečů informují a aktualizovat, i když občas (zvlášť v případě ie) se aktualizace dostavují poněkud pozdě.

Změna DNS

- pokud jde o cílený útok, může útočník využít složitějších metod. Například dns spoofignu, změny DNS serveru na Vašem počítači apod. Jedná se o to, že když zadáte url do prohlížeče, tak prohlížeč žádá DNS server o IP adresu a na tu se potom připojuje. A pokud Vám útočník nějakým způsobem podstrčí tento záznam falešný dostanete se na stránku úplně jinou než ste chtěli a zase nic nemusíte poznat. Obrana: myslím, že s takovým útokem toho moc nenaděláte. Ale můžete být v klidu. Tento způsob útoku je hodně náročný na čas i na technickou úroveň a vybavenost útočníka, proto k nim dochází spíše náhodou.

Informujte o podvodu skutečnou společnost

Jestli budete dodržovat těchto pár zásad nemělo by se Vám stát, že naletíte. A pokud na takovéto řádění přijdete, upozorněte prosím i společnost, za kterou se útočník vydává. Pomůžete tak dalším zákazníkům i službě samotné. A vlastně celé společnosti. Protože se může stát, že na základě Vašeho echa se podaří útočníka najít a potrestat. Což je určitě dobře. Průměr přežívání jednoho podvodu je v průměru šest dní a když to bude za rok doba poloviční, zlobit se nikdo nebude (krom podovodníků ovšem:))

Jeden případ za všechny

Následující příběh se stal někdy vloni, možná předloni. Dva týpci se jednoho dne rozhodli, že si zjistí pár hesel na hostingy na serveru webzdarma.cz. Jentak, for fun, z nudy. Založili tedy na wz účet ve tvaru servis.webzdarma.cz a přes smtp webzdarma poslali asi 50 e-mailů informujících o možnosti se přihlášení přes stránku servis.webzdarma.cz . Získali tak asi 15 přístupů k cizím hostingům. A to vše

je stálo tak zhruba 20 minut práce. Až po týdnu admini wz stránku smazali, ale nové vytvoření účtu s tímto názvem je povolen dál. Jak snadné, že ano :)

Budoucnost

Budoucnost ale nevypadá dobře. Tento článek píšu hlavně v důsledku toho, že se o phishingu začalo mluvit jako o vážné hrozbě a že počet útoků neustále roste. Dokonce se na začátku roku začlo mluvit, že letošní rok, bude právě rok phishingu (berte s rezervou). Problém je v tom, že hodně lidí je náchylné a utočník dostane, jak se říká za málo peněz hodně muziky. A s tím musíme něco dělat! Nebo snad chceme aby se phishing rozmohl do takových rozměrů jako třeba spam?

URL článku: https://security-portal.cz/clanky/phishing-2

Odkazy:
[1] https://security-portal.cz/users/czokl
[2] https://security-portal.cz/category/tagy/anonymita
[3] https://security-portal.cz/category/tagy/hacking
[4] https://security-portal.cz/category/tagy/hacking-method
[5] https://security-portal.cz/category/tagy/phishing-pharming
[6] mailto:administrator@seznam.cz
[7] http://www.k-banka.cz
[8] http://www.kb.cz
[9] http://secunia.com/multiple_browsers_idn_spoofing_test/
[10] http://www.domena.tld/script.cgi?redirect=www.jinadomena.tld