Jak to bylo s defacem SP doopravdy

Vložil/a cm3l1k1 [1], 9 Květen, 2007 - 12:00

- SP News [2]

Na Internetu se šíří spousta dezinformací. Lidé se chlubí cizím peřím a jen málo z nich opravdu ví, jak to vše bylo. Chtěl bych zde věc uvést na pravou míru.

Security Portál nebyl doslova defacnut, protože nebyly modifikovány jeho stránky. Nikdo se nedostal do redakčního systému, ke zdrojovým kódům SP a jeho subdomén, ani k databázím (za což jsem rád).
Nicméně výsledek vypadal stejně, proto by se o defacu mohlo mluvit.

O co tedy šlo?
Byly změněny DNS záznamy. Pokud se tedy někdo snažil přistupovat na stránky SP, byl přesměrován na jiný server (88.208.78.122). Když jsem se připojil na FTP(S) Security Portálu, porovnal jsem index.php a nenašel žádnou změnu. Prohlédl jsem .htaccess a opět bez výsledku. To mě v daný okamžik trochu zmátlo. Kdy jsem na FTP přistupoval z jiného PC, všiml jsem si, že resolv vyhodil špatnou IP.

V zájmu mé paranoi totiž přistupuji na mém PC přímo na IP FTP a neresolvuji si název. Teď už mi bylo vše jasné. Doména je stále napsána na kamaráda (clusk), jehož účet u registrátora domén byl napaden. Abych byl přesnější: Někdo se dostal na cluskův mail. Tam se posílaly autorizace změn na doméně (seznam.cz - :o(). Na www.nic.cz [3] jsem zjistil, že proběhly změny den před tím, než jsem "deface" SP zjistil.

Patrně se jednalo o odvetu za deface webu soom.cz. Ten byl defacnut par dní před SP. Mě na tom jen štve, že s defacem soomu jsem neměl nic společného. Ten člověk to udělal sám za sebe, protože ho některá idividua ze soomu zřejmě nějak naštvala(urazila etc.). Nicméně: Protiútok byl veden proti SP. Je důležité rozlišovat SP a komunitu lidí okolo SP. SP jakožto portál, kterému jsem věnoval 3 roky svého volného času, primárně spravuji já. Takže "deface" SP beru spíš osobně, ne jako útok proti jeho komunitě nebo člověku z SP.

Deface soomu se mi líbil. Byl pěkně udělaný. Ale hlavně: Nebyl urážející, což se nedá říct o hnusu na fakenutém serveru SP. Člověk, který materiál dodal (curly_boi?) je... jak to říct ... úchyl? Ano, když budu slušný.

Člověk, který útok provedl mě kontaktoval na ICQ. Psali jsme si spolu celý den. Trvalo mu než mu došlo, že mě soom nezajímá a že s jeho defacem SP, jakožto portál, nemá co dělat. To už je ale jedno. Nevím, jak moc je spojen se soomem, vím jen, že provedl útok. Za umístěním webu a jeho tvorbou však stoji lidé ze soomu (nevím konkrétně kdo). Deface by mi ani tak moc nevadil. Líbilo se mi, že útok přišel odjinud. Útočník prostě našel nejslabší článek v řetězci (cluskův mail) a povedlo se mu ho plnohodnotně využít. Co dokázal jeden přístup k mailovému účtu je zdrcující. Clusk neměl jednoduché heslo. Ani krátké. Řekl mi, že mu ho clusk sám prozradil, nebo že se někde zaregistroval se stejným heslem, což je ale hloupost. Ten email měl totiž jen jako forward a heslo už zapomněl. Doteď vlastně nevím, jak se dostal na ten email na Seznam.cz. Třeba nějaká chybka [4]? :)

Víc mi vadil ten obsah. Dost hnus!! Ten index nedělal on, předal ho někdo ze soomu. Bylo to dost ubohé a dětinské. Obrázky, index atd. byly umístěny na fake IP 88.208.78.122, což je nějaký server curly_boie (to byla jediná jeho role). Stačilo upravit vhosty a mohlo se to spustit. I to stačilo pro velké pobavení osazenstva chanu soom a k enormnímu nárustu ega a testosteronu. lol? Ale beru to v klidu. Né nadarmo má náš BANlist na chanu SP 60 položek. Lidé z IRCa soomu a SP se navzájem napadají, šíří dezinformace a lži. U nás plníme BANlist, ale na soomu by některé velkohubé členy měli srovnat.

Jde totiž o to, že i když se tam na chvíli zavřou (invited only), tak se stále plní log jejich komunikace, vyvěšený na Internetu a lidé, kteří si hledají důvod, si to čtou, že ano.

Takže zpět. Díky přístupu na mail si resetoval heslo do administrace registrátora a thatz all folks. Když jsem nad tím tak přemýlel, mohl útok dovést k dokonalosti. Clusk na ten mail nepřistupoval, měl tam forward, takže by na jeho zcizení nepřišel. Kdyby útočník modifikoval DNS záznamy tak, že by šly na jeho server, ten by je forwardoval dál na skutečný host SP, mohl takhle odposlouchávat hesla při nešifrovaném (SSLv3/TLSv1, změny certifikátu by si snad všiml každý) přístupu (SP, fórum, webmail, admin), přístupy na FTP. A pokud by modifikoval i MXka, tak by mohl číst i poštu. Dostal by se tak kompletně na celý portál (pokud bych na to já, nebo někdo jiný včas nepřišel). Nice :) A to pořád jde o získání jednoho mailu. Naštestí už je v řešení převod domény a až ji budu mít plně pod kontrolou já, už by se nemělo nikdy stát nic podobného. Nikdy se na nikoho moc nespoléhejte...

Přístupy mi (resp. cluskovi) útočník vrátil a tím to haslo. Nebudu podávat trestní oznámení, nebo jiné hlouposti, i když kromě nicku útočníka jsem poté vypátral i jeho skutečné jméno, adresu apod. :)

Nojo, prostě další epizoda našich serverů. Útočník nemusel hledat chybu v redakčním systému díky své vynalézavosti. Je vidět, že i když si někdo myslí, jak bezpečný má systém, dírka se vždycky najde. A když ne, jde se na to jinou cestou a výsledek je +- stejný. Kdyby deface SP byl podobný tomu ze soomu (tedy bez zcizení dat, myslel jsem po stránce obsahu), jen bych se tomu zasmál. Ale pokud tam ty děti vyvěsily nechutné obrázky, nepoškodilo to ani tak pověst SP, ale spíš to naštvalo mě.

URL článku: https://www.security-portal.cz/clanky/jak-bylo-s-defacem-sp-doopravdy

Odkazy:
[1] https://www.security-portal.cz/users/cm3l1k1
[2] https://www.security-portal.cz/category/tagy/sp-news
[3] http://www.nic.cz
[4] http://sysel.security-portal.cz/index.php?article=4