Igigi - novodobý hrdina nebo bad boy?

Vložil/a RubberDuck [1], 25 Prosinec, 2009 - 14:44

6. prosinec 2009 - Česko-slovenská filmová databáze neustála první výpad do té doby neznámého útočníka vystupujícího pod nickem Igigi a na jeho blogu http://www.igigi.baywords.com/ [2] se objevují první výpisy z databáze, včetně hashů hesel.

Tento incident pořádně otřásl komunitou kolem CSFD, ale větší medializace se mu nedostalo. V té době jsem si pomyslel, že dotyčný měl štěstí a jak se rychle ukázal, tak rychle zapadne.

9. prosinec 2009 - Během tří dnů padlo pár dalších méně významných webů a e-shopů. Vždy se stejným výsledkem: Igigi vystavuje strukturu databáze na svém blogu a připojuje některé zajímavé záznamy v ní. Ovšem další zářez má opět zvučné jméno v končinách CZ/SK internetu - rozzlobenimuzi.com

V tomto okamžiku jsem přemýšlel, zda má Igigi takové štěstí na cíle. A poprvé se objevila myšlenka, že používá nějaký kvalitní scanner. Frekvence útoků je přecijen relativně vysoká a dva cíle zvučného jména ve třech dnech je vážně k zamyšlení.

15. prosinec 2009 - Po menší odmlce přichází celkem zneklidňující zpráva: rockyou.com - 32 miliónů hesel v plain-textu! A opět stejný scénář: struktura databáze + zajímavé záznamy.

Pomalu jsem se začínal plácat po rameni: Zase jsi měl jednou odhad na lidi :) V zápětí přichází šok! To už není náhoda. Necelých 10 dnů a tři velké portály. Myšlenku o kvalitním scanneru rozšiřuji o teorii, že dotyčný využívá nějaký 0day exploit, případně má vytvořen kvalitní dotaz na odhalování Full Blind SQL injection. Poprvé si pohrávám s myšlenkou, že Igigi není jedinec.

19. prosinec 2009 - Orange.sk - slovenský mobilní operátor padl a Igigi přeje adminům Šťastné vánoce.

Z výpisu je patrné, jací lidé se dnes vydávají za adminy. Ač zveřejnění loginů a hesel/hashů neschvaluji, do jisté míry jsem rád za to, že konečně někdo ukáže nabubřelým a radobynedotknutelným společnostem, koho že to zaměstnávají. Stále více sílí názory lidí, že by měli být hackeři perzekuováni. Těmto lidem vzkazuju: Až vám někdo vyluxuje bankovní účet, protože je admin pi*us a neumí si systém pohlídat, až vám blízký člověk zemře, protože rádoby-programátoří webových palikací "pracují pod tlakem a nemají šanci všechno kontrolovat" (výsměch největší, protože to jsou alibistické kecy) nechali v kódu chybu, která se projeví náhodně, až budete dlužit statisíce kvůli chybnému zaokrouhlování v účetním programu, pak si vzpomeňte na lidi, pro které je hrabání se v kódu a hledání potenciálních chyb a bezpečnostních mezer zábava a třeba i práce. Pak se vám snad konečně rozsvítí ve vašich konzumních palicích prošpikovaných bulvárem a konečně vystoupíte ze stáda oveček a začnete přemýšlet sami.

21. prosinec 2009 - Igigi zveřejňuje dumpy obsahující hesla ze serveru rockyou.com

Igigi, tak tohle byla vážně blbost!! A pokud jsem s tebou do té doby sympatizoval, teď jsi mé sympatie ztratil. Začínám si vážně myslet, že to děláš jen kvůli slávě. Pokud se pletu, neměj mi to za zlé, ale tohle se vážně nedělá.

23. prosinec 2009 - Union.sk - Igigi začíná hrát nebezpečnou hru. Je jen otázkou času, kdy dojde k podání trestního oznámení na neznámého pachatele.

Banky nebo pojišťovny. Všichni z nás ždímou nemalý peněžní obnost za každou blbost, za každou kravinku, o kterou ani nemáme zájem. Chyba z jejich strany není chybou, ale chyba ze strany zákazníka je neodpustitelná. Neuvědomují si, že bez nás, lidí, by neexistovaly. Copak chci tak moc, pokud žádám vysokou míru bezpečnostního opatření pro mé peníze a mé osobní údaje? Styďte se!!

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

24. prosinec 2009 - atlas.sk - Igigi stupňuje intenzitu útoků a zásadně si vybíra pouze vysoce populární weby a portály.

Již není pochyb, že dotyčný opravdu něco umět musí. Jinak by to snad ani nebylo možné. Ovšem vzhledem k formátování výstupů si stále myslím, že využívá nějaký kvalitní scanner. Konečně někdo, kdo nemá strach postavit se autoritám a ukázat, jak to u nás vypadá s bezpečnostní. A věřme tomu, že Igigi je pouze vrcholkem ledovce. Ve skutečnosti je situace mnohem žalostnější. S vidinou snadného zisku se u nás velkou módou stalo zakládání webhostingů, stejně jako tvorba webových aplikací. Jenže tvůrci nemají ani základní znalosti správy a vývoje, natož aby byli schopní dostatečně vyřešit zabezpečení. V neposlední řadě všechno dotváří média, která tak v lidech uměle živí strach. Ne! Opravdu ne každý, kdo se zajímá o bezpečnost, musí být nutně zlý. Někteří z nás mají i snahu pomoci, pokud vidí zájem, snahu a vděčnost ze strany adminů.

To, zda je Igigi je chvástal nebo je to novodobý hrdina, nechám na posouzení vám. U mě hodně ztratil uveřejněním hesel. Pokud to ale povede k alespoň minimální nápravě žalostné situace na CZ/SK internetu, pak to svůj význam mělo.
Na závěr přikládám pár mediálních zpráv:

http://redaktori.blog.zive.cz/2009/12/23/igigi-napadl-atlassk-muj-obdiv-... [3]
http://www.lupa.cz/clanky/miliony-hacknutych-uctu-v-ohrozeni-i-v-cesku/n... [4]
http://pocitace.sme.sk/c/5164719/hacker-igigi-dalej-utoci-najnovsimi-obe... [5]

URL článku: https://security-portal.cz/blog/igigi-novodob%C3%BD-hrdina-nebo-bad-boy

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] http://www.igigi.baywords.com/
[3] http://redaktori.blog.zive.cz/2009/12/23/igigi-napadl-atlassk-muj-obdiv-ale-nema/
[4] http://www.lupa.cz/clanky/miliony-hacknutych-uctu-v-ohrozeni-i-v-cesku/nazory/283892/
[5] http://pocitace.sme.sk/c/5164719/hacker-igigi-dalej-utoci-najnovsimi-obetami-su-union-denikcz-a-atlassk.html

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn