CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Pharming

CCERT-PUBDOC-2008-03-223

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Pharming je oblik udaljenog napada kod kojega se promet usmjeren prema ranjivoj web stranici preusmjerava prema zlonamjerno oblikovanoj web stranici. Ovaj napad moguće je izvesti izmjenama datoteke s informacijama o položaju računala unutar mreže (eng. hosts file) na napadnutom računalu ili iskorištavanjem sigurnosnih nedostataka DNS (eng. Domain Name System) poslužitelja. Zadaća DNS poslužitelja je povezivanje imena sa stvarnim adresama na Internetu, a za kompromitirani DNS poslužitelj kaže se da je „zatrovan“ (eng. poisoned).

Naziv ove vrste napada nastao je igrom riječi iz engleskih izraza farm, što znači farma, i phishing (eng. password fishing), izraza koji označava vrstu napada iz skupine napada socijalnog inženjeringa, a cilj mu je stjecanje korisničkih vjerodostojnica kao što su zaporke i korisnička imena. Obje vrste napada, pharming i phishing, koriste se za krađu identiteta pri čemu su pharming napadi prije svega usmjereni na elektroničko poslovanje (eng. ecommerce) i bankovne web stranice. Složene tehnike pharming napada nije moguće spriječiti uobičajenim antivirusnim alatima, već zahtijevaju primjenu posebnih anti-pharming mjera.

U ovom dokumentu dan je uvod u metode razlučivanja imena, čije poznavanje je nužno za razumijevanje različitih metoda pharming napada. Nakon toga, opisani su najčešći vektori pharming napada te metode odgovarajuće obrane.

2. Pharming i razlučivanje imena

Pharming je naziv za tehnike koje kriminalci koriste za krađu identiteta i izvođenje prijevara, a temelje se na iskorištavanju ranjivosti u postupku lociranja i povezivanja korisnika na različite usluge na Internetu. Phishing i pharming napadi za cilj imaju navođenje korisnika na posjećivanje zlonamjerno oblikovane web stranice, a razlikuju se u korištenim tehnikama. Phishing napadi koriste obmanjivanje korisnika dok se pharming napadi temelje na manipuliranju različitim komponentama sustava za imenovanje računala na Internetu. Zbog izvođenja pharming napada na tako niskoj razini nije ih moguće uočiti niti spriječiti uobičajenim tehnikama zaštite od phishinga.

Zbog toga što pharming napadi zloupotrebljavaju mehanizme povezivanja imena usluga, koja korisnici svakodnevno koriste, sa stvarnim adresama tih usluga, za razumijevanje pharming napada potrebno je poznavanje tih mehanizama. Zajednički naziv takvih tehnika je razlučivanje imena (eng. host ili name resolution).

2.1. Klasični DNS sustav

DNS sustav predstavlja jedan od osnovnih mehanizama koji omogućuju svestrano korištenje Interneta. Moglo bi se reći da ovaj sustav djeluje slično telefonskom imeniku, povezujući imena mrežnih uređaja (eng. hostname), npr. ime www.primjer.hr, s IP (eng. Internet Protocol) adresama, npr. 208.77.188.166.

2.1.1. Povezivanje računala

Većina protokola, koji dvama računalima omogućuju komunikaciju putem Interneta, za razlikovanje dostupnih mrežnih uređaja oslanja se na numeričke IP adrese. Ove adrese vrlo su efikasne za komunikaciju među uređajima, ali ljudski korisnici prednost daju lakše pamtljivim pseudonimima. Tako je, na primjer, prikladnije poslužitelju u obližnjoj knjižnici pristupati preko imena „Slovojed“, nego preko adrese 192.168.20.12.

U početcima Interneta, i prije naglog porasta njegove popularnosti, svako računalo imalo je vlastiti popis IP adresa i pridruženih im pseudonima. Pseudonimi upisani u web pregledniku tada bi lokalno bili prevedeni u IP adrese kojima se potom pristupalo.

Opisani način pristupanja računalima dobro funkcionira unutar manjih mreža, ali posjeduje značajne nedostatke vezane uz održavanje i skalabilnost. DNS sustav osmišljen je s ciljem uklanjanja spomenutih nedostataka. Implementiran je diljem Interneta te različitim regulatornim i komercijalnim tijelima omogućuje upravljanje prevođenjem imena u adrese na globalnoj razini.

2.1.2. Hijerarhija DNS sustava

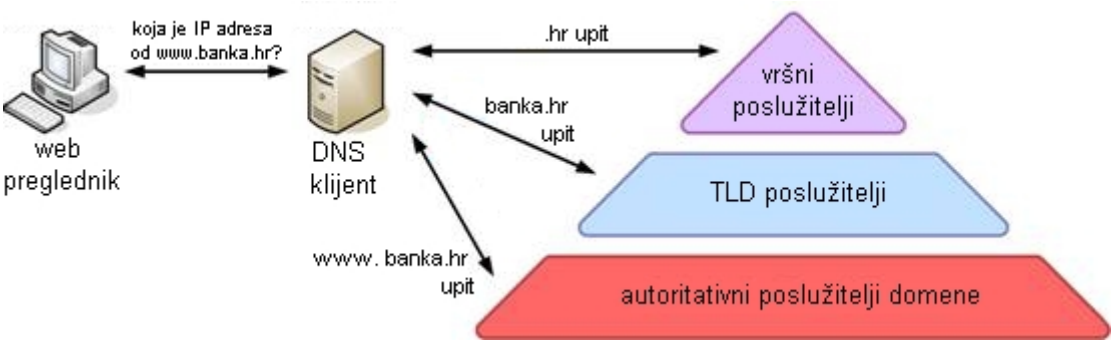
Osnova DNS sustava je hijerarhijska struktura poslužitelja. Preko poslužitelja više razine moguće je pristupiti poslužiteljima na nižim razinama koji pružaju detaljnije informacije. Ovo je moguće ilustrirati piramidom kod koje se podaci kreću od vršnih (eng. root) poslužitelja, preko TLD (eng. Top Level Domain) poslužitelja sve do autoritativnih poslužitelja domena (eng. authoritative domain server - AD), kao na slici Slika 1.

Slika 1. Pojednostavljena DNS hijerarhija

Takvom strukturom korisnicima se omogućuje pristup uslugama bilo gdje u svijetu uz istovremeno lokalno upravljanje imenima računala.

Zbog toga je prije pristupanja pojedinim uslugama potrebno pristupiti DSN poslužitelju koji sadrži podatke o njihovim IP adresama, a samo pristupanje ovom poslužitelju provodi se u više koraka i uz pomoć različitih drugih poslužitelja. Na primjer, ako korisnik želi posjetiti stranicu www.banka.hr, čija IP adresa je pohranjena na DNS poslužitelju pod kontrolom banke, potrebno je prvo pristupiti tom poslužitelju.

U prvom koraku korisnikovo računalo pomoću DNS klijenta (eng. resolver) zahtijeva vezu na neki od poznatih vršnih poslužitelja s kojega se dohvaćaju podaci o poslužitelju koji posjeduje više informacija o zatraženoj TLD domeni. TLD domena je posljednji dio web adrese, slova koja se nalaza iza posljednje točke, u navedenom primjeru to je hr. Vršni poslužitelj pruža DNS klijentu podatke o odgovarajućem TLD poslužitelju kojemu klijent tada šalje upit o autoritativnoj adresi, npr. .banka.hr. U posljednjem koraku DNS poslužitelj od autoritativnog poslužitelja organizacije pribavlja IP adresu željene usluge. Postupak je prikazan na slici Slika 2.



Slika 2. DNS razlučivanje

Kako bi se ubrzao pristup pojedinim često posjećivanim stranicama korisničko računalo može pohraniti njihove IP adrese u priručnu memoriju (eng. cache) na određeno vrijeme.

Trenutno je aktivan određen broj strateški raspoređenih vršnih poslužitelja koji su okupljeni pod 13 imena: A.ROOT-SERVERS.NET, B.ROOT-SERVERS.NET, ..., M.ROOT-SERVERS.NET. DNS klijenti koriste tablice s IP adresama za pristup ovim poslužiteljima. Potrebno je istaknuti kako se iza svakog od navedenih imena ne krije jedan poslužitelj, već grozd (eng. cluster) poslužitelja s raspodjeljivanjem zadataka (eng. load balancing). Njihova jedina uloga je usmjeravanje DNS klijenata ka odgovarajućim TLD poslužiteljima.

Sloj TLD poslužitelja unutar piramide DNS hijerarhije podijeljen je u dva dijela, kao na slici Slika 3.

- gTLD (eng. Generic TLD) poslužitelji DNS klijentu pružaju informacije o općim .com, .net, .org, .gov, .mil i .gov domenama.
- ccTLD (eng. *Country-coded TLD*) poslužitelji pružaju informacije o domenama specifičnim za pojedine zemlje, npr. *.uk* za Veliku Britaniju (eng. *United Kingdom*). U mnogim slučajevima ccTLD poslužitelji dozvoljavaju poddomene, kao što je *.ac.uk* poddomena za akademske institucije unutar Velike Britanije.

Slika 3. Dijelovi TLD sloja DNS hijerarhije

AD poslužitelji, poznati i pod nazivom imenski poslužitelji (eng. name server), pružaju same IP adrese ili preusmjeravaju upite ka drugim AD poslužiteljima. Ovi poslužitelji dijele se na:

- primarne (eng. *Primary Master*) poslužitelje, na kojima se nalaze sami podaci o imenima i IP adresama računala, te
- sekundarne (eng. *Secondary Master*) poslužitelje koji te informacije dohvaćaju s primarnih.

2.1.3. Prevođenje IP adresa

Iako je moguće provođenje potpune DNS pretrage od strane svakog računala prisutnog na Internetu prilikom svakog posjećivanje neke stranice ili korištenja usluge, postoje metode kojima se postupak prevođenja IP adresa ubrzava uz istovremeno smanjenje potrošnje mrežnih resursa.

Unutar većih organizacija, kao što su korporacije ili svi korisnici koji Internetu pristupaju preko istog davatelja usluga (eng. Internet Service Provider - ISP), moguće je preusmjeravati DNS upite prema DNS poslužitelju te organizacije, umjesto prema vršnim poslužiteljima. Takvi poslužitelju provode DNS pretrage za sve pridružene im klijente, a moguće je i pohranjivanje prethodno zatraženih imena domena u priručnoj memoriji.

Ovisno o postavkama korporativnog ili ISP DNS poslužitelja, umjesto provođenja potpune DNS pretrage moguće je informacije o imenu domene zatražiti od većeg ili bolje pozicioniranog poslužitelja. U slučaju da takav poslužitelj već posjeduje zatražene podatke u vlastitoj priručnoj memoriji, vrijeme prevođenja značajno se smanjuje. Posljednji u nizu poslužitelja, ako zatražene informacije nisu pronađene, šalje upit odgovarajućem vršnom poslužitelju te se provodi potpuna DNS pretraga. Rezultate ove pretrage moguće je potom privremeno pohraniti, u trajanju koje je najčešće određeno TTL (eng. Time To Live) parametrom od strane vlasnika domene.

DNS poslužitelji koji provode privremenu pohranu podataka prikupljenih od drugih DNS poslužitelja nazivaju se priručni DNS poslužitelji (eng. DNS Cache Server). Razlike između običnih i priručnih DNS poslužitelja dane su u tablici Tablica 1.

	DNS poslužitelji	**priručni DNS poslužitelji**
dostupnost	treba odgovarati na upite svih računala na Internetu	odgovara samo na „lokalne“ upite
tip upita na koje treba odgovarati	nerekurzivni	rekurzivni
podaci koje pruža	pruža samo podatke za koje je autoritativan	treba pokušati odgovoriti na svaki valjani upit

Tablica 1. Razlike običnih i priručnih DNS poslužitelja

2.2. Ostale usluge za razlučivanje imena

Klasične metode za prevođenje imena osim DNS sustava obuhvaćaju i druge metode, od kojih su neke navedene u nastavku. Pored njih na raspolaganju su usluge koje korisniku omogućuju posjećivanje web stranica čak i kada ne znaju njihova imena, kao što su automatsko dovršavanje unosa (eng. *autocompleters*) i pretraživači (eng. *search engines*).

2.2.1. Ostale metode prevođenja IP adresa

Tijekom povijesti pojavljivale su se različite metode prevođenja IP adresa, a brojni operacijski sustavi još uvijek podržavaju neke od njih kako bi ostvarili unazadnu kompatibilnost. Redoslijed kojim operacijski sustavi iskušavaju metode za prevođenje IP adresa može imati utjecaja na njegovu sigurnost.

Unix i Linux operacijski sustavi redoslijed korištene usluga prevođenja čitaju iz datoteke hosts.conf, a to su najčešće redom:

1. DNS,
2. *etc/hosts* - provjera tablice IP adresa u lokalno pohranjenoj datoteci,

3. NIS (eng. *Network Information Service*) - Unix imenička usluga (eng. *directory service*) koja se danas rijetko koristi.

Windows operacijski sustavi koriste veći broj metoda. To su najčešće:

1. provjera radi li se o imenu računala s kojeg se šalje upit,
2. *%Systemroot%\System32\Drivers\Etc\hosts* - provjera tablice IP adresa u lokalno pohranjenoj datoteci,
3. DNS,
4. WINS (eng. *Windows Internet Naming Service*) - protokol za prevođenje imena tvrtke Microsoft,
5. tzv. Network Broadcast metoda,
6. LMHOSTS (eng. *LAN Manager Hosts*) - datoteka povezana s *LAN Manager* imeničkom uslugom.

2.2.2. Automatsko dovršavanje unosa

Većina web preglednika i Internet aplikacija prilikom upisa adrese pokušat će ju automatski nadopuniti nekom od sljedećih metoda:

- traženjem sličnih imena u priručnoj memoriji,
- dodavanjem niza „http://“ ispred upisanog imena uz pokušaj povezivanja prema HTTP protokolu,
- dodavanjem niza „www.“ ispred i niza „.com“ iza upisane nepotpune adrese,
- traženjem sličnih imena u bazi podataka proizvođača aplikacije idr.

Iako ove metode korisnika spajaju na neku od usluga, nema garancije da će kod sljedećeg pokušaja biti usmjeren na istu IP adresu.

2.2.3. Pretraživači

Korisnici koji ne znaju punu adresu željene usluge do nje dolaze upisom određenih ključnih riječi u nekom od pretraživača. Ovu metodu korisnici često zbog brzine i praktičnosti upotrebljavaju čak i ako im je poznata adresa. Rezultati pretrage rangiraju se prema različitim kriterijima kao što su broj pojavljivanja ključnih riječi, broj veza na stranicu s drugih web stranica, učestalost posjećivanja idr.

3. Vektori napada

Zbog složenosti postupka prevođenja IP adresa postoje brojni načini njegova kompromitiranja, odnosno provođenja pharming napada.

3.1. Ljudski faktor

Sustave za prevođenje IP adresa potrebno je redovno održavati i podešavati, tako da njihov integritet i sigurnost uvelike ovise o administratorima. Složenost ovih sustava zlonamjernom korisniku, koji im ima pristup, omogućuje provođenje izmjena koje može biti teško, ako ne i nemoguće, otkriti.

Pri napadu na DNS poslužitelje napadačima su obično zanimljive slijedeće kategorije:

- DNS poslužitelji unutar lokalne mreže - sustavski administrator može lagano i neprimjetno izmijeniti ili dodati zapise u priručnu memoriju čime utječe samo na DNS pretrage korisnika unutar mreže.
- ISP DNS poslužitelji - kratkotrajne izmjene DNS unosa na ovoj razini mogu, zbog velike količine prometa, rezultirati velikim brojem „žrtava“. Raslojenost i složenost DNS sustava većine pružatelja Internet usluga čine izmjene jednog unosa teško uočljivom.
- Korporativni DNS poslužitelji - izmjenama DNS unosa na ovoj razini napadač osigurava preusmjeravanje svog prometa prema alternativnoj IP adresi uz povećan rizik otkrivanja. Ako na poslužitelju nije na odgovarajući način implementirano stvaranje dnevničkih zapisa, kratkotrajne izmjene, npr. nekoliko sati svakog dana, mogu proći neopaženo.
- Globalni DNS poslužitelji - ukoliko napadač na neki način uspije izmijeniti postupak DNS pretrage na globalnoj razini veliki su izgledi razmjerno brzog otkrivanja prevare.

3.2. Napadi na razini lokalne mreže

3.2.1. Izmjene postupka prevođenja

Ukoliko napadač uspije izmijeniti lokalne postupke prevođenja IP adresa ili datoteke na kojima se oni temelje, moguće je izvođenje pharming napada. Zbog popularnosti Windows operacijskih sustava, brojni ovakvi napadi provode se izmjenama HOSTS datoteka. Ako zlonamjerni korisnik neovlašteno ostvari pristup spomenutoj datoteci, može dodavanjem odgovarajućih unosa preusmjeriti promet s vjerodostojne web stranice ka proizvoljnoj IP adresi. Na primjer, iskorištavanjem ranjivost web preglednika korisnika koji je posjetio zlonamjerno oblikovanu web stranicu napadač može prepisati HOSTS datoteku na ranjivom računalu.

Druga vrsta pharming napada na lokalnu mrežu svodi se na preusmjeravanje svih DNS upita s ranjivog računala ili mreže prema DNS poslužitelju pod kontrolom napadača.

3.2.2. Nadgledanje i izmjene prometa

Zlonamjerni korisnik koji ima pristup lokalnoj mreži može izravno nadgledati podatkovni promet (eng. sniffing) te ga po volji mijenjati, uključujući i preusmjeravanje prometa. Pharming napade je pored toga moguće izvoditi stvaranjem posebno oblikovanog posrednog (eng. proxy) ili DHCP (eng. Dynamic Host Configuration Protocol) poslužitelja te WPAD (eng. Web Proxy Automatic Discovery) usluge.

DHCP protokol se često koristi za dinamičko dodjeljivanje IP adresa te podataka potrebnih za usmjeravanje pojedinim računalima na mreži. Napadač može postaviti zlonamjerno oblikovan DHCP poslužitelj u mrežnom segmentu, kako bi naveo računala iz tog segmenta da, zbog povećanja brzine, koriste spomenuti poslužitelj umjesto udaljenijeg centraliziranog poslužitelja. Kako je DHCP postavkama računala moguće kontrolirati korištenje DNS poslužitelja, zlonamjerni korisnik u opisanom slučaju može DNS upite iz ranjive LAN mreže usmjeriti prema vlastitom ili prethodno kompromitiranom DNS poslužitelju. DHCP postavkama se kod Windows operacijskih sustava također određuje i korišteni WPAD poslužitelj.

WPAD usluga web pretraživačima, i srodnim aplikacijama, omogućuje korištenje različitih metoda za automatski odabir posrednog poslužitelja. Posebno oblikovani WPAD poslužitelj može promet ranjive lokalne mreže usmjeriti prema kompromitiranom posrednom poslužitelju te tako zlonamjernom korisniku omogućiti izvođenje napada preusmjeravanjem prometa (eng. Man-In-The-Middle - MITM). MITM napadi predstavljaju ključnu komponentu brojnih sofisticiranih phishing i pharming napada.

3.3. Napadi registriranjem domene

Posebna skupina phishing napada provodi se zloupotrebom načina registriranja domene.

3.3.1. Otimanje domene

Organizacija koja želi koristiti neku domenu prethodno ju treba registrirati, najčešće plaćanjem određene pristojbe nadležnom tijelu. Registracija domene plaća se na neki vremenski rok, npr. 1 do 3 godine. Pod pojmom otimanja domene podrazumijeva se kupovina domene, čija registracija je istekla, od strane zlonamjernog korisnika.

Prednost ovakvog napada pred stvaranjem nove domene su postojeće veze na otetu domenu, čime si napadač osigurava značajan broj posjeta. Nakon stjecanja domene zlonamjerni korisnik može stvoriti web stranicu i ostale usluge, npr. usluge elektroničke pošte, koje imitiraju izvornu stranicu i usluge te tako zavarati korisnike.

3.3.2. Registracija slične domene

Registracija slične domene najjednostavniji je vektor napada, a svodi se na registraciju domena s imenom sličnim imenu domene s koje se promet želi preusmjeriti. Slična imena obuhvaćaju imena nastala pogrešnim upisom izvornog imena domene, zamjenom pojedinih slova u imenu ili istovremenim pritiskom više tipki, npr. googkle.com umjesto google.com ili masmn.com umjesto msn.com. Ako korisnik pogreškom umjesto željene adrese upiše ime

neke od takvih domena, može biti usmjeren na zlonamjerno oblikovanu stranicu te naveden na odavanje povjerljivih osobnih podataka.

3.3.3. Pharming napadi pomoću botnet aplikacija

Botnet je zajednički naziv za sve tzv. programske robote, odnosno bot aplikacije. To su zlonamjerno oblikovani programski paketi koje se autonomno i automatski izvode na napadnutim računalima, tzv. zombi računalima. Napadač ih može tijekom izvođenje pharming napada koristiti za održavanje krivotvorenih web stranica (eng. hosting) na različitim IP adresama. Kako pružatelj Internet usluga onemogućuje pojedine IP adrese napadač može jednostavnim izmjenama DNS unosa preusmjeravati promet prema nekoj od drugih IP adresa kontroliranih od strane bot aplikacija.

3.4. Napadi podešavanjem domene

3.4.1. DNS višeznačnici

DNS višeznačnici su oznake koje omogućuju preusmjeravanje svih sličnih upita prema istoj IP adresi. Na primjer, autoritativni DNS poslužitelj za domenu *banka.hr* može biti podešen na sljedeći način:

```
www.banka.hr      IN    A          150.10.1.21
mail.banka.hr     IN    A          150.10.1.20
banka.hr          IN    A          150.10.1.21
banka.hr          IN    MX    10   mail.mybank.com
*.banka.hr        IN    MX    10   mail.mybank.com
*.zg.banka.hr     IN    A          150.10.1.21
```

U navedenom primjeru oznake '*' imaju zadaću:

- preusmjeriti sve poruke elektroničke pošte usmjerene ka *[bilo_što]@banka.hr* prema poslužitelju elektroničke pošte *mail.banka.hr*
- preusmjeriti sve upite koji završavaju na *zg.banka.hr* prema IP adresi 150.10.1.21.

Zlonamjerni korisnik koji provodi pharming napad može korištenjem DNS višeznačnika preusmjeriti promet prema domeni pod njegovom kontrolom.

3.4.2. Loše održavani DNS poslužitelji

Usporedno s otkrivanjem sigurnosnih nedostataka DNS sustava objavljuju se zakrpe koje te propuste uklanjaju. Dobro održavan sustav ažurno je nadograđivan kako bi se minimiziralo vrijeme izloženosti na novootkrivene ranjivosti. Nezakrpani DNS poslužitelj često je laka meta zlonamjernom korisniku koji namjerava izvršiti pharming napad.

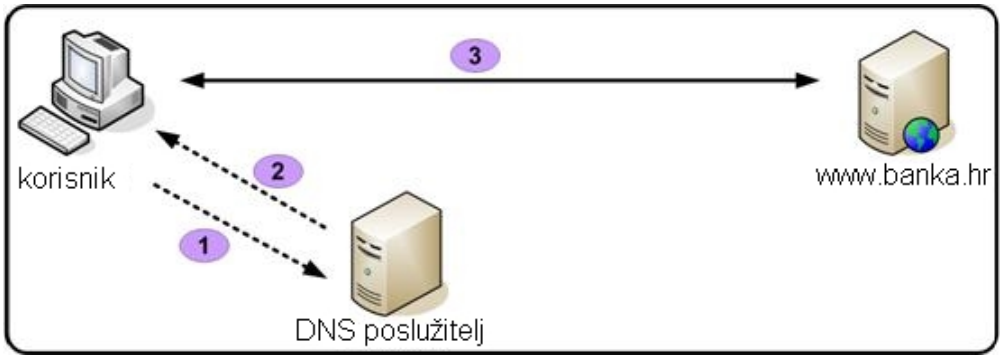
3.5. DNS krivotvorenje

Pharming napad moguće je izvesti i neovlaštenim umetanjem krivotvorenih podataka u postupak prevođenja IP adresa (eng. DNS spoofing) korištenjem različitih tehnika, od socijalnog inženjeringa do iskorištavanja sigurnosnih nedostataka DNS sustava.

U normalnim okolnostima DNS pretraga provodi se u sljedećim koracima:

1. korisnik šalje DNS poslužitelju upit o IP adresi domene, npr. www.banka.hr,
2. DNS poslužitelj odgovara IP adresom zatražene domene, npr. 150.10.1.21
3. korisnik se spaja na dobivenu IP adresu.

Opisani postupak prikazan je slikom Slika 4.

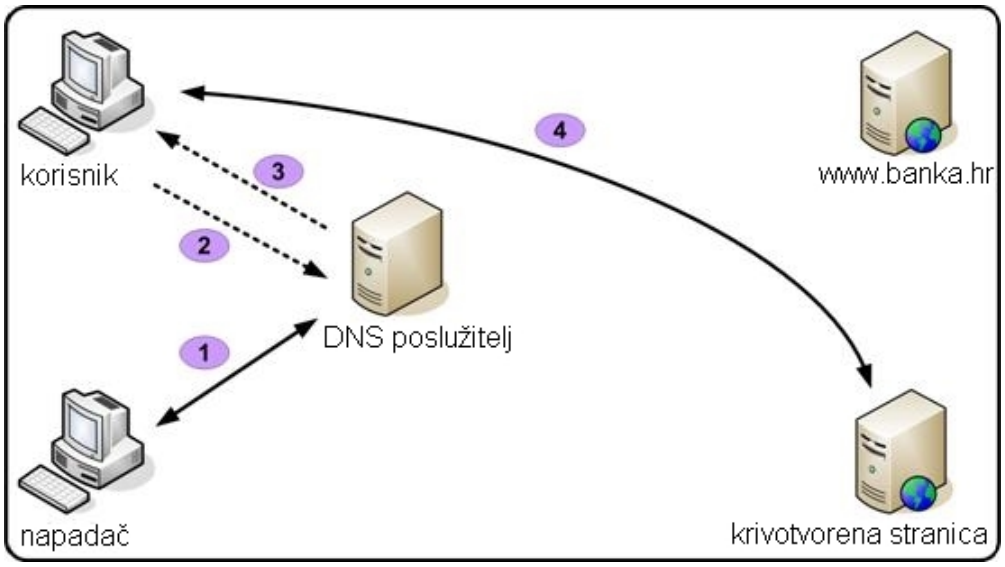


Slika 4. Uobičajena DNS pretraga

DNS krivotvorenje, s druge strane, provodi se na sljedeći način:

1. napadač dodaje ili izmjenjuje unos za domenu *www.banka.hr* na DNS poslužitelju, npr. zamjenjujući stvarnu IP adresu domene 150.10.1.21 IP adresom krivotvorene stranica 200.1.1.10,
2. korisnik šalje DNS poslužitelju upit o IP adresi domene *www.banka.hr*,
3. DNS poslužitelj odgovara IP adresom lažne domene, npr. 200.1.1.10,
4. korisnik se spaja na krivotvorenu stranicu u uvjerenju da se nalazi na *www.banka.hr*.

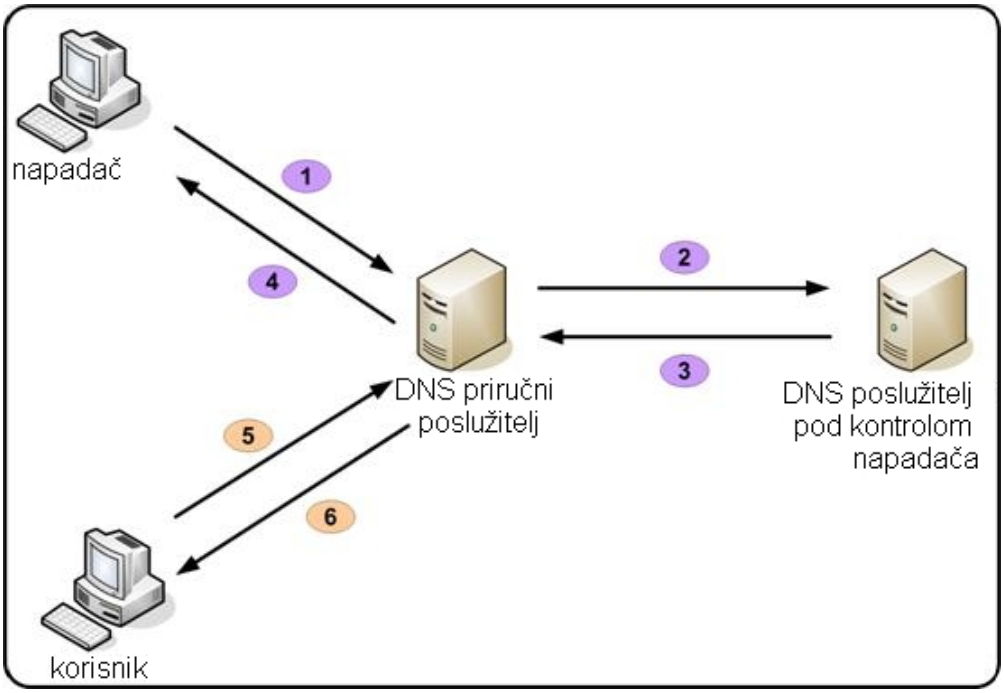
Ovakav napad ilustriran je slikom Slika 5.



Slika 5. DNS krivotvorenje

3.5.1. Umetanje unosa u DNS priručnu memoriju

Zlonamjerni korisnik može DNS krivotvorenje izvesti iskorištavanjem ranjivosti postupka privremene pohrane podataka potrebnih za razlučivanje imena domena (eng. cache poisoning).



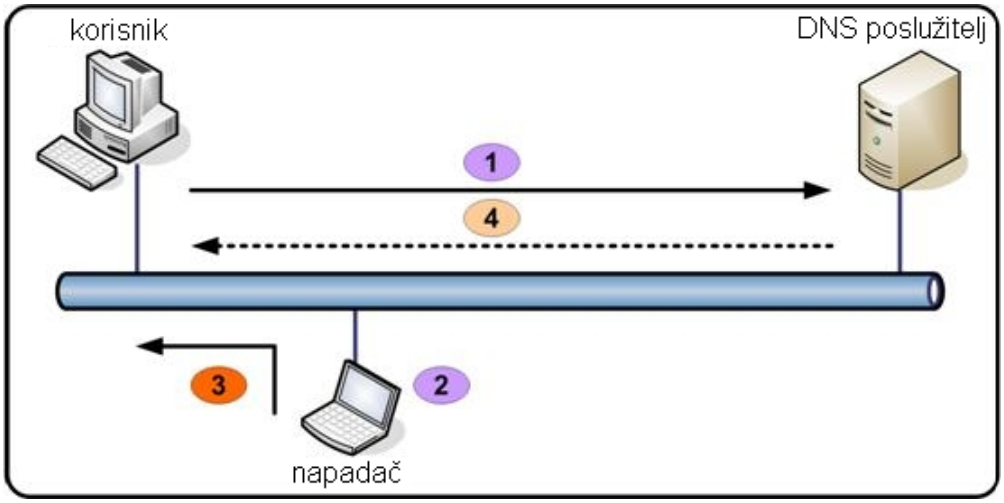
Slika 6. Umetanje unosa u DNS priručnu memoriju

Postupak je prikazan slikom *Slika 6*, a provodi se u sljedećim koracima:

1. napadač šalje DNS poslužitelju upit o domeni pod njegovom kontrolom, npr. *www.napadaceva.hr*,
2. DNS priručni poslužitelj nema podataka o zatraženoj domeni pa šalje upit autoritativnom DNS poslužitelju za tu domenu, a koji je također pod kontrolom zlonamjernog korisnika,
3. napadačev DNS poslužitelj obavještava priručni poslužitelj o IP adresi zatražene domene, npr. 200.1.1.10 za *www.napadaceva.hr*, ali u odgovor umeće dodatne podatke, npr:
4. IP adresa od *www.banka.hr* je 200.1.1.11,
5. IP adresa od *mail.banka.hr* je 200.1.1.11,
6. priručni poslužitelj odgovara napadaču na izvorni upit, npr. adresom 200.1.1.10, te ove podatke, zajedno s dodatno umetnutim informacijama, pohranjuje u priručnu memoriju u trajanju određenom TTL parametrom napadačevog DNS poslužitelja,
7. korisnik kompromitiranom priručnom DNS poslužitelju šalje upit o domeni *www.banka.hr*,
8. priručni poslužitelj na zahtjev odgovara lažnom IP adresom, npr. 200.1.1.11.

3.5.2. Krivotvorenje DNS oznake uz prisluškivanje

Prilikom slanja svakog DNS upita korisnik mu dodjeljuje jedinstvenu identifikacijsku oznaku. Odgovor DNS poslužitelja treba sadržavati istu oznaku, inače ga se ignorira. Zlonamjerni korisnik koji presretanjem i analizom podatkovnog prometa stekne ovu oznaku može pokušati odgovoriti na upit prije pristizanja odgovora DNS poslužitelja.



Slika 7. Krivotvorenje DNS oznake uz prisluškivanje

Ovakav napad prikazan je slikom Slika 7, a provodi se u sljedećim koracima:

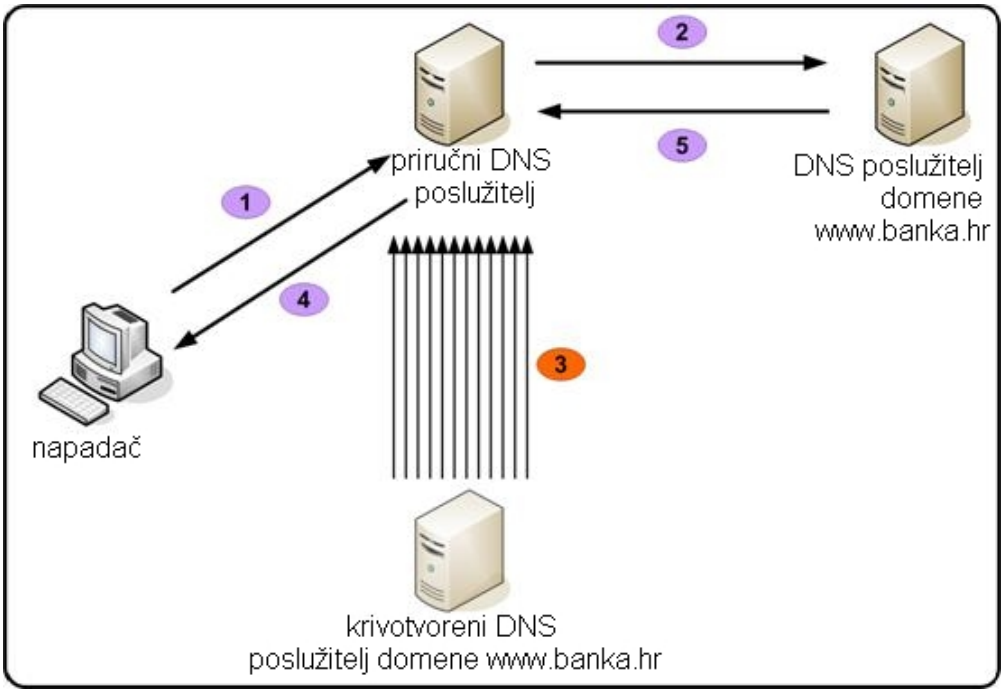
1. korisnik šalje DNS poslužitelju upit o IP adresi domene, npr. *www.banka.hr*,
2. napadač je postavio prijenosno računalo na mrežu te presreće sve DNS upite i odgovara na njih,
3. nakon uočavanja DNS upita o domeni *www.banka.hr* s određenom identifikacijskom oznakom, prijenosnik automatski odgovara lažnom IP adresom uz potpisivanje odgovora spomenutom oznakom,
4. ubrzo nakon toga korisniku stiže valjani odgovor DNS poslužitelja, ali ga korisnikovo računalo odbacuje.

3.5.3. Pogađanje DNS oznake

Kod prethodno opisanog napada zlonamjerni korisnik ograničen je na mreže kojima ima fizički pristup. Za mreže kojima nema pristupa napadač može pokušati pogoditi identifikacijsku oznaku za što postoji realna mogućnost jer je ona duga dva okteta pa postoji samo 65535 mogućih kombinacija.

Napad, prikazan slikom, moguće je izvesti na sljedeći način:

1. napadač šalje DNS poslužitelju upit o domeni, npr. *www.banka.hr*,
2. priručni DNS poslužitelj nema tražene podatke pa šalje upit autoritativnom poslužitelju za zatraženu domenu,
3. dok priručni poslužitelj čeka na odgovor napadač šalje velik broj krivotvorenih odgovora s lažnom IP adresom i svaki puta drugačijom identifikacijskom oznakom,
4. ako je napad uspio, odnosno ako je ispravna DNS oznaka pogođena prije pristizanja odgovora vjerodostojnog DNS poslužitelja, napadač će primiti odgovor od priručnog poslužitelja s krivotvorenom IP adresom koja će biti pohranjena u priručnoj memoriji tog poslužitelja,
5. odgovor vjerodostojnog DNS poslužitelja pristiže prekasno i biva zanemaren.



Slika 8. Napad pogađanjem DNS oznake

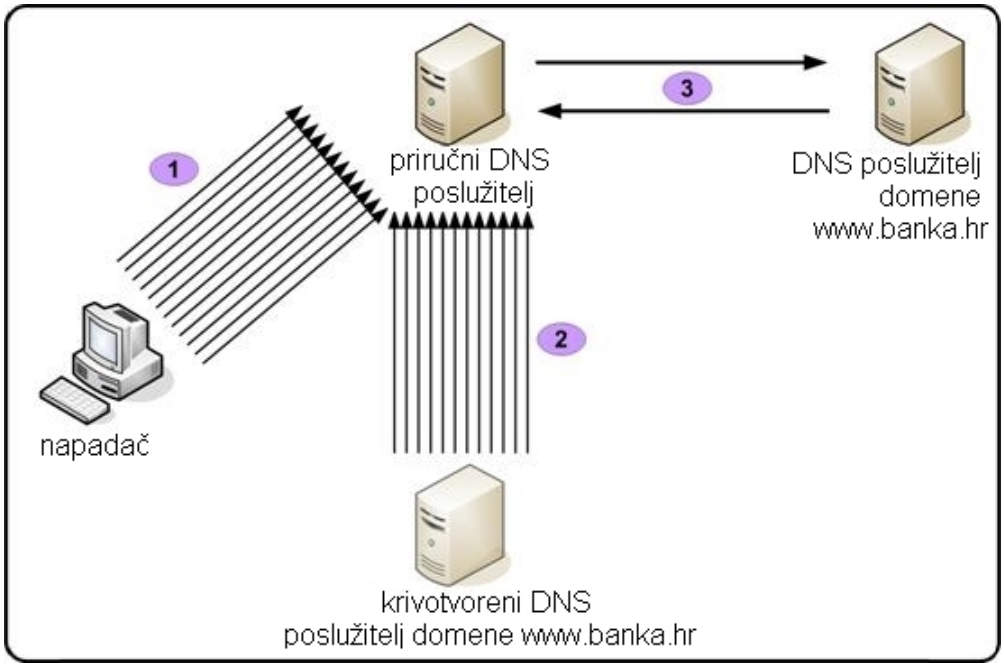
3.5.4. Rođendanski napad

Vjerojatnost pogađanja identifikacijske DNS oznake moguće je povećati iskorištavanjem tzv. rođendanskog paradoksa. Napad se provodi kao na slici Slika 9:

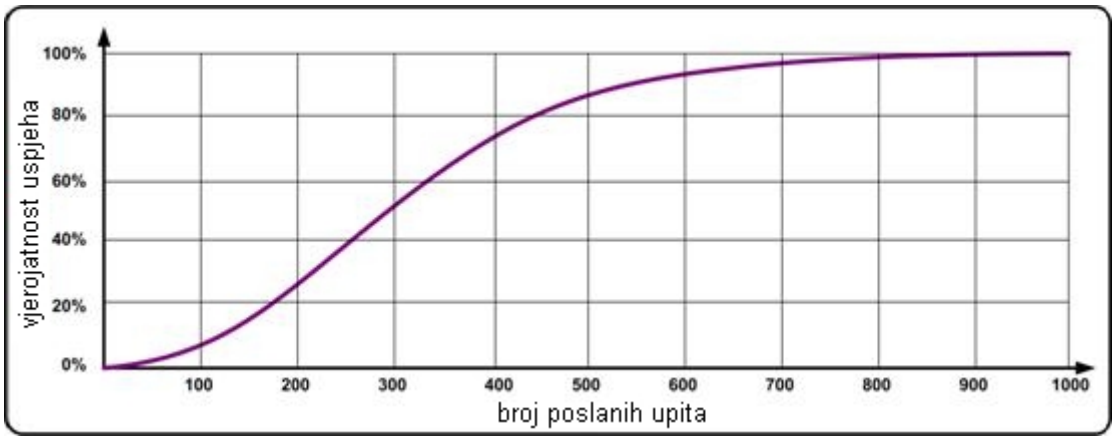
1. napadač šalje opetovane upite o domeni, npr. *www.banka.hr*,
2. istovremeno, napadač šalje velik broj krivotvorenih odgovora s lažnom IP adresom i svaki puta drugačijom identifikacijskom oznakom,
3. za svaki napadačev upit priručni poslužitelj pokušava od odgovarajućeg autoritativnog poslužitelja saznati IP adresu zatražene domene, svaku puta koristeći novu identifikacijsku oznaku.

Kako bi povećao vjerojatnost uspješnog izvođenja napada zlonamjerni korisnik može na autoritativni poslužitelj izvestii napad uskraćivanja usluga.

Spomenuti rođendanski paradoks je matematički pojam, a vezan je uz promatranje grupe koju sačinjavaju dvadeset i tri slučajno odabrane osobe. Matematičari su pokazali kako je u toj skupini vjerojatnost da su dvije ili više osoba rođene na isti datum veća od 50%. Ovaj rezultat moguće je primijeniti na stvaranje pseudonasumičnih brojeva, kao što je slučaj kod DNS rođendanskog napada. Tijekom konvencionalnog napada pogađanjem DNS oznake zlonamjerni korisnik pošalje n krivotvorenih odgovora na DNS upit s vjerojatnošću pogađanja oznake od n/65535 dok je kod rođendanskog napada, uz n pokušaja, vjerojatnost uspjeha prikazana slikom Slika 10. Iz spomenutog grafa vidljivo je kako je vjerojatnost uspjeha ove vrste napada jednaka 50% uz samo 300 poslanih upita, dok se za 800 upita vjerojatnost uspjeha penje do visokih 99%. Konvencionalni napad pogađanjem DNS oznake ima vjerojatnost uspjeha od samo 0.5% uz 300 pokušaja.



Slika 9. DNS rođendanski napad



Slika 10. Vjerojatnost uspjeha rođendanskog DNS napada u ovisnosti o broju poslanih upita

3.6. Ostali napadi

Za izvođenje pharming napada zlonamjerni korisnici mogu koristiti različite usluge koje im olakšavaju pronalaženje domena. Tako napadač, na primjer, može kod tvrtke koja održava pretraživač kupiti tzv. sponzoriranu vezu (eng. sponsored link) i tako osigurati da se njegova domena nađe na vrhu pretrage s određenim ključnim riječima. Zlouporabom načina na koji pretraživači rangiraju rezultate pretrage zlonamjerni korisnik može osigurati visoko mjesto svoje krivotvorene stranice.

Uspješna manipulacija rezultatima web pretraga odlična je polazišna točka za izvođenje pharming napada jer je prijevaru moguće usmjeriti na korisnike unutar određene regije. Pretraživači, naime, rezultate pretraga prilagođavaju korisnikovoj lokaciji tako da je organizaciji žrtvi ovakvog napada izrazito teško uočiti ga i onemogućiti.

4. Kako se braniti

Od pharming napada općenito se puno teže zaštititi nego od tradicionalnih phishing napada zbog njihove distribuirane prirode i zbog korištenja resursa koji nisu pod kontrolom napadnute organizacije. Dodatna poteškoća leži u tome što se napadi uglavnom izvode vrlo nisko na razini DNS prevođenja pa postoji relativno malo metoda koje mogu pouzdano otkriti zlonamjerne izmjene.

4.1. Zaštita od phishing napada

Mnoge od tehnika zaštite od phishing napada moguće je primijeniti i na pharming napade. Na strani klijenta ove metode obuhvaćaju:

- korištenje uobičajenih alata za zaštitu sigurnosti osobnih računala,
- korištenje prikladnih, manje sofisticiranih, komunikacijskih postavki,
- korištenje alata za nadzor na razini korisničkih aplikacija,
- zaključavanje web preglednika (eng. *browser lock-down*) i
- digitalno potpisivanje i provjera valjanosti elektroničkih pisama.

Na strani poslužitelja preporuča se:

- omogućavanje i korištenje tehnologija za provjeru valjanosti,
- razvoj sigurnih web aplikacija koje ne sadrže lako iskoristive sigurnosne nedostatke,
- korištenje strogih sustava autentikacije temeljenih na oznakama (eng. *token-based*),
- održavanje jednostavnih i razumljivih sustava imena domena.

Metode koje otežavaju phishing i pharming napade na razini organizacije su:

- utomatska provjera poslužitelja elektroničke pošte primljenih poruka,
- digitalno potpisivanje elektroničkih pisama,
- nadzor korporativnih domena i uočavanje registracija sličnih domena,
- zaštita pristupnika (eng. *gateway*).

4.2. Specifične tehnike zaštite od pharming napada

4.2.1. Upravljanje i nadzor nad DNS sustavom

Zbog velike opasnosti zlonamjernih izmjena unutar DSN sustava od strane zaposlenika, savjetuje se:

- kod potrebnih izmjena DNS sustava pristup konfiguracijskim datotekama i priručnoj memoriji omogućiti samo ovlaštenim zaposlenicima,
- provoditinadzora svih promjena postavki DNS sustava i bilježiti ih u dnevničkim zapisima,
- nadzor zapisa o izmjenama postavki DNS sustava treba provoditi tim koji je odvojen od zaposlenika koji održavaju sustav,
- redovan nadzor i komparativna analiza sekundarnih i priručnih DNS poslužitelja.

4.2.2. Neovisna provjera prijevoda IP adresa

Zaštitu od pharming napada moguće je implementirati instalacijom posebnih dodataka web preglednicima koji provode provjeru vjerodostojnosti domene. Pojedini ovakvi alati prikazuju IP adresu posjećene domene te potpune podatke o njezinom imenu kako bi korisnik mogao uočiti krivotvorenu web stranicu. Drugi programski paketi provjeru obavljaju uspoređivanjem URL (eng. Uniform Resource Locator) oznake posjećene stranice s listom poznatih pharming stranica, a čiji sadržaj se osvježava u stvarnom vremenu.

Neki od raspoloživih dodataka za otkrivanje pharming napada stvaraju vlastitu listu IP adresa i pridruženih imena domena. Kod ponovne posjete domene provjerava se je li IP adresa jednaka onoj zabilježenoj tijekom posljednjeg posjeta. Ukoliko se uči razlika, korisniku se šalje upozorenje. Problemi se mogu javiti ako vlasnik domene promijeni IP adresu te kod domena kojima je pridijeljen veći broj IP adresa.

Na raspolaganju su i alati koji omogućuju određivanje zemljopisnog položaja domene na temelju IP adrese čime se olakšava otkrivanje krivotvorenih pharming stranica, npr. kod posjete stranici koja se nalazi u Poljskoj, a predstavlja se kao Australska banka.

Dodatnu razinu zaštite predstavljaju certifikati poslužitelja kojima oni dokazuju svoj identitet. Većina web preglednika omogućuje čitanje i provjeru spomenutih certifikata. Za implementaciju takvog sustava zašite organizacija u vlasništvu domene treba zatražiti i dobiti certifikat ovlaštenog tijela za dodjelu certifikata (eng. certificate authority).

4.2.3. Održavanje DNS sustava

Kao i kod svih Internet usluga, tako su i kod DNS sustava nužni sigurno podešavanje svih postavki i pravovremena nadogradnja. Pored toga, savjetuje se korištenje aktualnih inačica programskih paketa jer one u većini slučajeva sadrže najpotpuniju zaštitu od novih vektora napada.

DNS poslužitelji organizacijama koje ih koriste, odnosno administratorima koji ih održavaju, pružaju mnoštvo konfiguracijskih mogućnosti. Zbog toga je potrebno posebnu pažnju posvetiti njihovom sigurnom postavljanju, u skladu s preporukama:

- DNS poslužitelji često su ranjivi ukoliko su podešeni da odgovaraju na rekurzivne upite. Napadač naime može poslati upit o adresi iz domene koja je pridružena DNS poslužitelju pod njegovom kontrolom i tako provesti neki od opisanih napada. Kako bi se ovo spriječilo preporuča se:
- onemogućavanje rekurzivnih upita, ukoliko je to moguće,
- ograničavanje adresa na koje će poslužitelj slati odgovore na upite, te
- ograničavanje adresa na koje će poslužitelj slati odgovore na rekurzivne upite.
- Kad je na poslužitelju onemogućena rekurzija on djeluje u pasivnom načinu rada, tj. ne šalje DNS upite drugim poslužiteljima. Zbog toga ne pohranjuje podatke u priručnu memoriju pa je otežano umetanje krivotvorenih unosa.
- Ukoliko onemogućavanje rekurzivnih upita nije moguće savjetuje se ograničavanje upita na koje poslužitelj treba odgovarati. Ono se, primjerice, može provesti zadavanjem određenog raspona dozvoljenih adresa.
- *Glue Fetching* je naziv postupka kod kojeg poslužitelj pokušava dohvatiti A zapis (eng. *Address record*) povezan s upitom o NS zapisu (eng. *Authoritative Name Server*). Ovaj postupak ranjiv je na umetanje lažnih unosa pa se savjetuje njegovo onemogućavanje.

5. Zaključak

Napadi temeljeni na zlouporabi postupaka prevođenja imena s ciljem ostvarivanja financijske koristi ili krađe identiteta u budućnosti će vjerojatno postajati sve učestaliji. Nedostatak razumijevanja pozadinskih postupka, koji se provode prilikom povezivanja IP adresa s imenima računala ili usluga, od strane korisnika, ali i brojnih organizacija, često rezultira neotkrivanjem napada temeljenih na izmjenama DSN sustava.

Opisani vektori napada zlonamjernom korisniku omogućuju relativno lagano izvođenje pharming napada nad širokom populacijom korisnika uz malenu vjerojatnost otkrivanja. Krađa identiteta provedena na ovaj način za posljedicu može imati ne samo značajne financijske posljedice već i ozbiljno narušavanje ugleda organizacije žrtve napada.

U borbi protiv pharming napada ključno je razumijevanje globalnih DSN usluga razlučivanja imena te mogućih načina njihove zloupotrebe. S takvim znanjima organizacije mogu implementirati bolje metode nadzora i ranog uočavanja.

6. Reference

[1] Pharming, http://en.wikipedia.org/wiki/Pharming, ožujak 2008.

[2] Gunter Ollmann: The Pharming Guide (Part 1), http://www.technicalinfo.net/papers/Pharming.html, ožujak 2008.

[3] Gunter Ollmann: The Pharming Guide (Part 2), http://www.technicalinfo.net/papers/Pharming2.html, ožujak 2008.