بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

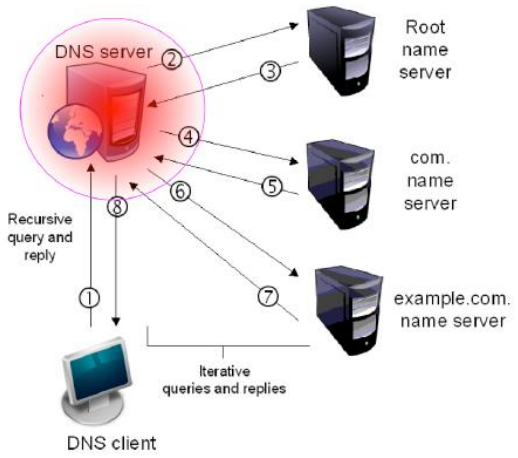
حمله DNS Zone Poisoning و راه کارهای امن سازی

تاریخ نگارش.....۱۵ آبان ۱۳۹۶

شمارهٔ نگارش..... ۱

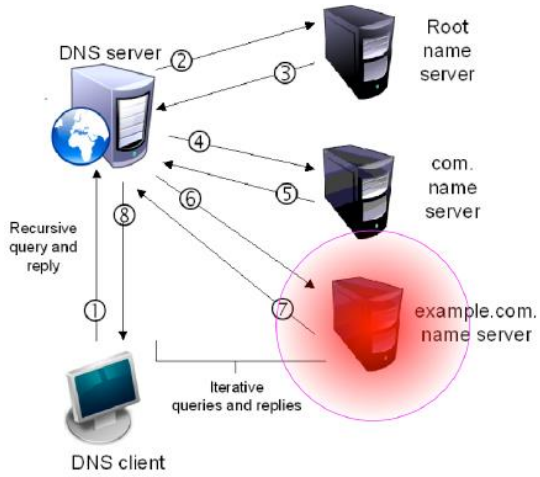
مقدمه

پروتکل DNS یکی از سرویس‌های پایه شبکه اینترنت است. این پروتکل دارای عمر زیادی بوده و در طول سال‌ها، تهدیدات مختلفی برای آن آشکار شده است. دو تهدید قدیمی cache poisoning و malicious name resolution services دو نمونه از این تهدیدات هستند که سعی می‌نمایند در عملکرد صحیح تبدیل نام به آدرس IP اختلال ایجاد نمایند. نقطه اشتراک این دو تهدید آن است که هر دو سعی می‌نمایند تا در جایی میان کاربر و سرویس‌دهنده نام این اختلال را ایجاد نمایند (شکل ۱).



شکل ۱. حمله Cache Poisoning

اما اخیراً حمله‌ی دیگری مورد توجه قرار گرفته که مستقیماً zone fileهای سرویس‌دهنده نام authoritative را هدف قرار می‌دهد. این حمله از آسیب‌پذیری موجود در طراحی افزونه به‌روزرسانی پویای DNS سوءاستفاده می‌کند (شکل ۲).



شکل ۲.حمله Zone Poisoning

افزونه‌ی به‌روزرسانی پویای DNS به‌طور بالقوه به هرکسی که بتواند به سرور نام authoritative دست یابد، امکان به‌روزرسانی محتوای zone fileهایش را می‌دهد. برای سوءاستفاده از این آسیب‌پذیری، فرد مهاجم فقط نیاز به دانستن اسم zone و اسم سرور نام برای آن zone دارد. این حمله را zone poisoning نامیده‌اند. امکان‌پذیری اجرای این حمله برای اولین بار در سال ۱۹۹۷ مطرح شده ولی در پیاده‌سازی‌های جدید DNS هنوز این مشکل وجود دارد.

در ساده‌ترین حالت حمله، فرد مهاجم می‌تواند رکورد A یا MX موجود در Zone file یک سرور authoritative را جایگزین کرده و نام دامنه را به یک آدرس IP تحت کنترل مهاجم ارجاع دهد.

در zone poisoning نیازی به هک ماشین سرویس‌دهنده یا ماشین فرد ثبت کننده نام نیست و این حمله به سادگی ارسال یک پکت استاندارد به‌روزرسانی پویای DNS برای یک سروریس‌دهنده نامی است که به‌درستی پیکربندی نشده است.

قابلیت به‌روزرسانی پویای محتویات DNS

قابلیت به‌روزرسانی پویای DNS در سال ۱۹۹۷ در RFC 2136 معرفی شده است. با استفاده از این قابلیت می‌توان هر یک از انواع A، AAAA، CNAME، NS یا ... را به بانک اطلاعاتی Resource Record افزود یا حذف نمود. پیام UPDATE مورد نیاز، سازگار با فرمت پیام‌های DNS استاندارد است. پس از دریافت پیام به‌روزرسانی، سرویس‌دهنده نامی که از قابلیت به‌روزرسانی خودکار پشتبانی می‌کند، بررسی می‌نماید که:

- آیا تمامی پیش نیازهای تعیین شده توسط درخواست کننده برآورده شده است یا خیر (مثلاً Record خاص مورد نظر موجود است یا خیر).
- آیا فرد متقاضی مجوز ارسال درخواست به‌روزرسانی را دارد یا خیر (اگر هیچ‌گونه محدودیتی اعمال نشده باشد، هر فردی که از نام zone و نام ماشین سرویس‌دهنده مطلع است، می‌تواند پیام به‌روزرسانی ارسال کند).

پیاده‌سازی

در سال ۲۰۱۶، سه محقق از دانشگاه صنعتی دلف هلند و دانشگاه صنعتی کومپین فرانسه اقدام به بررسی پیاده‌سازی‌های مختلف DNS نموده و نتایج آن را در قالب مقاله‌ای منتشر نموده‌اند. در این بررسی، پیکربندی پیش‌فرض پیاده‌سازی‌های زیر مد نظر قرار گرفته است.

- BIND: Berkeley Internet Name Domain (BIND) یک نرم‌افزار DNS متن‌باز بوده که به‌صورت گسترده در سطح شبکه اینترنت استفاده می‌شود. در نسخه‌های ۸ و ۹ از BIND، به‌روزرسانی پویا به‌صورت پیش‌فرض غیرفعال است و راهبر سیستم می‌تواند امکان به‌روزرسانی پویا را در پیکربندی zone اضافه کند

و میزبان‌هایی که مجاز به به‌روزرسانی رکوردها هستند را مشخص کند (از طریق تعریف لیست تطابق آدرس). از BIND 8.2، لیست تطابق آدرس، TSIG[1] را پشتیبانی می‌کند.

- Microsoft DNS: ویندوز ۲۰۰۰ اولین سیستم‌عامل توسعه‌یافته توسط مایکروسافت است که به‌روزرسانی پویای DNS را پشتیبانی می‌کند. سرور را می‌توان به عنوان primary استاندارد یا به‌عنوان zone یکپارچه‌شده‌ی Active Directory مایکروسافت پیکربندی کرد. ویندوز ۲۰۰۰ و جانشینان آن یعنی ویندوز سرور ۲۰۰۳، ۲۰۰۸ و ۲۰۱۲، به‌روزرسانی‌های پویای امن را پشتیبانی می‌کنند. در تمامی این نسخه‌ها، یک الگوریتم TSIG توسعه‌یافته پیاده‌سازی شده است (RFC 3645). زمانی که راهبر سیستم یک zone یکپارچه‌شده‌ی Active Directory را ایجاد می‌کند، به‌طورپیش‌فرض سرور فقط امکان به‌روزرسانی‌های امن را از طریق TSIG توسعه‌یافته می‌دهد. با این‌حال راهبر می‌تواند عدم به‌روزرسانی پویا یا به‌روزرسانی پویا به‌صورت غیرامن را نیز پیکربندی نماید. مهم‌تر از همه اینکه قابلیت به‌روزرسانی امن برای zoneهای اصلی (primary) استاندارد در دسترس نیست و در هر zone اصلی (primary) پیکربندی‌شده برای به‌روزرسانی‌های پویای DNS ، هر فردی می‌تواند zoneها را تغییر دهد.
- سایر پیاده‌سازی‌ها: همان‌گونه که در RFC 2137 اشاره شده است، هر zone file ای که امکان به‌روزرسانی‌های پویا را می‌دهد، از نمونه مشابهی که به‌صورت ایستا پیکربندی شده باشد، امنیت کمتری دارد. بعضی از سرورهای قابل اعتماد متن‌باز مانند Name Server Daemon (NSD) توسعه‌داده‌شده توسط NLnet Labs، DJBDNS یا Unlogic Eagle DNS به‌روزرسانی‌های پویا را پشتیبانی نمی‌کنند. با این‌حال این قابلیت در برخی از موارد توسط ابزارهای خارجی اضافه می‌شود. PowerDNS اخیراً کامپوننت به‌روزرسانی پویا را اضافه کرده است و طبق مستندات، به‌طور پیش‌فرض همه‌ی محدوده‌های IP، برای انجام به‌روزرسانی مجاز هستند.

به‌طور خلاصه، پیاده‌سازی‌های رایج نه‌تنها پیکربندی آسیب‌پذیر مانند پذیرش درخواست‌ها از همه‌ی میزبانها را پشتیبانی می‌کنند، بلکه برخی از آن‌ها به‌طور پیش‌فرض آسیب‌پذیر هستند. از دو مکانیزم امنیتی رایج یعنی انواع TSIG و لیست‌های تطابق آدرس، فقط اولی می‌تواند یک دفاع قابل اعتماد را در برابر به‌روزرسانی‌های مخرب فراهم کند. از آن‌جایی که اجرای حمله فقط شامل ارسال یک پکت UDP است، فرد مهاجم می‌تواند آدرس‌های IP مبدا

[1] کلید محرمانه‌ی تایید اعتبار تراکنش برای DNS

بسته را جعل کند. این تهدید می‌تواند با محدود کردن به‌روزرسانی‌های پویا صرفاً از طریق پروتکل TCP کاهش یابد.

راه‌کارهای امن‌سازی قابلیت به‌روزرسانی پویای DNS

به‌طور خلاصه، دو راه‌کار اصلی مقابله با حمله Zone Poisoning عبارتند از:

- سرویس‌دهنده authoritative به‌گونه‌ای پیکربندی گردد که پیام‌های به‌روزرسانی را تنها از آدرس‌های IP مجاز یا از سرویس‌دهنده DHCP دریافت نماید.
- در مستند RFC 2137، دونالد ایستلیک در مورد چگونگی استفاده از افزونه‌های امنیت DNS (DNSSEC) برای محدود کردن دریافت پیام‌های به‌روزرسانی پویا از سوی موجودیت‌های مجاز براساس کلیدهای رمزنگاری توضیح می‌دهد. اما استفاده از مکانیزم کلید عمومی، کارآمدی کمتر و مدیریت سخت‌تری را درپی دارد. سه سال پس از معرفی قابلیت به‌روزرسانی پویای DNS ، جایگزین کارآمد و مؤثری برای تایید اعتبار به‌روزرسانی‌های پویا پیشنهاد شد: کلید محرمانه‌ی تائید اعتبار تراکنش برای DNS (TSIG) که براساس کلیدهای مخفی مشترک و کد تایید هویت پیام (MAC[۲]) می‌باشد.

راهنمای امن‌سازی BIND

Berkeley Internet Name Domain (BIND) یک نرم‌افزار DNS متن‌باز بوده که به‌صورت گسترده در سطح شبکه اینترنت استفاده می‌شود. در نسخه‌های ۸ و ۹ از BIND، به‌روزرسانی پویا به‌صورت پیش‌فرض غیرفعال است و راهبر سیستم می‌تواند امکان به‌روزرسانی پویا را در پیکربندی zone اضافه کند و میزبان‌هایی که مجاز به به‌روزرسانی رکوردها هستند را مشخص کند (از طریق تعریف لیست تطابق آدرس). نرم‌افزار BIND از نسخه 8.2 به بعد، از لیست تطابق آدرس، TSIG[۳]پشتیبانی می‌کند.

[۲] Message Authentication Code

[۳] کلید محرمانه‌ی تایید اعتبار تراکنش برای DNS

در Bind 9 برای تعریف لیست تطابق آدرس لازم است که یک address_match_list از میزبان‌هایی تعریف شود که اجازه‌ی به‌روزرسانی پویا برای master zoneها دارند. با استفاده از گزینه allow-update می‌توان یک address_match_list از میزبان‌هایی را که اجازه‌ی ثبت به‌روزرسانی‌های پویا را دارند را تعریف کرد.

```
allow-update { address_match_list };
allow-update { !172.22.0.0/16;};
```

همان‌گونه که پیش‌تر بیان شد، در این نسخه به‌صورت پیش‌فرض دریافت به‌روزرسانی از سوی همه‌ی میزبان‌ها غیرفعال است (در واقع DDNS به‌صورت پیش‌فرض غیرفعال است) ولی تعریف لیست فوق موجب فعال شدن این قابلیت می‌گردد. این موضوع منحصر به update_policy بوده و فقط به master zoneها اعمال می‌شود.

در صورت تمایل به استفاده از TSIG برای امن‌سازی پیام‌های به‌روزرسانی DNS در BIND می‌توان از دستور ddns-confgen استفاده نمود. گزینه a- نوع الگوریتم مورد استفاده TSIG را مشخص می‌کند. الگوریتم‌های موجود، hmac-md5، hmac-sha1، hmac-sha224، hmac-sha256، hmac-sha384 و hmac-sha512 هستند (درصورت عدم تعیین، مقدار پیش فرض hmac-sha256 انتخاب خواهد شد). گزینه k- نام کلید احراز اصالت DDNS را مشخص می‌کند. نام پیش فرض ddns-key است. گزینه z- نیز zone را مشخص می‌نماید. در مثال زیر از الگوریتم hmac_sha256 و نام dynamic-update-key استفاده شده است.

```
sara@ubuntu:/etc/bind/zones/master$ ddns-confgen -a hmac-sha256 -k dynamic-update-key -z example.com
# To activate this key, place the following in named.conf, and
# in a separate keyfile on the system or systems from which nsupdate
# will be run:
key "dynamic-update-key" {
        algorithm hmac-sha256;
        secret "76kSggpyQG1OovgWg2ju9N5Nq3ZR4yT8JOtrf+65Jjw=";
};

# Then, in the "zone" definition statement for "example.com",
# place an "update-policy" statement like this one, adjusted as
# needed for your preferred permissions:
update-policy {
          grant dynamic-update-key zonesub ANY;
};

# After the keyfile has been placed, the following command will
# execute nsupdate using this key:
nsupdate -k <keyfile>
```

در گام بعد بایستی کلید فوق را در named.conf قرار داد:

```
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
key "dynamic-update-key" {
        algorithm hmac-sha256;
        secret "76kSggpyQG1OovgwgZju9N5Nq32R4yyT8JOtrrf+65Jw="
};
```

همچنین بایستی در Zone مربوط به دامنه مورد نظر، مقدار update_policy را بنا به نیاز مشخص نمود. به عنوان مثال:

```
update_policy {
        grant dynamic-update-key zonesub ANY;
};
```

برای فعال کردن به‌روزرسانی با استفاده از کلید، بایستی در قسمتی که zone تعریف شده است، امکان به‌روزرسانی با کلید را فعال کرد.

```
zone "example.com" in {
        type master;
        allow-update { key "dynamic-update-key";};
};
```

همان‌گونه که قبلاً اشاره شد، برای تعریف لیست مبتنی بر IP می‌توان از روش زیر استفاده نمود:

```
zone "example.com" in{
        type master;
        allow-update {10.0.1.2;};
};
```

تبصره: به‌صورت پیش‌فرض به‌روزرسانی پویا غیرفعال است اما می‌توان آن را به‌صورت زیر نیز غیرفعال کرد:

```
zone "example.com" in {
        type master;
        allow-update {none;};
};
```

از BIND 9.1 به بعد، سرورهای slave، مجاز به انتقال به‌روزرسانی‌های پویا به سرورهای اصلی شدند. اگر سرویس‌دهنده نام دریافت کننده پیام به‌روزرسانی، سرور master نباشد، می‌تواند پیام به‌روزرسانی را به سوی سرور upstream خود هدایت نماید. به این عمل update forwarding گویند. اگر سرور upstream سرور master نباشد، مجدداً آن را به سرور بالادستی خود هدایت می‌کند تا نهایتاً به سرور mater برسد. پس از به‌روزرسانی رکورد master، تمامی سرورهای slave از طریق Zone Transfer با سرور master سنکرون می‌شوند. برای فعال‌سازی هدایت پیام‌های به‌روزرسانی می‌توان از گزینه allow-update-forwarding استفاده نمود:

```
allow-update-forwarding { address_match_list };
```

در مثال فوق، یک لیست تطابق برای آن دسته از آدرس‌های IP تعریف شده است که مجاز به هدایت پیام‌های به‌روزرسانی هستند (از سوی سرور slave به سوی سرور master). فعال‌سازی نا امن این قابلیت، یک راه جدید نفوذ پیش پای نفوذگران می‌گذارد.

راهنمای امن‌سازی Microsoft DNS

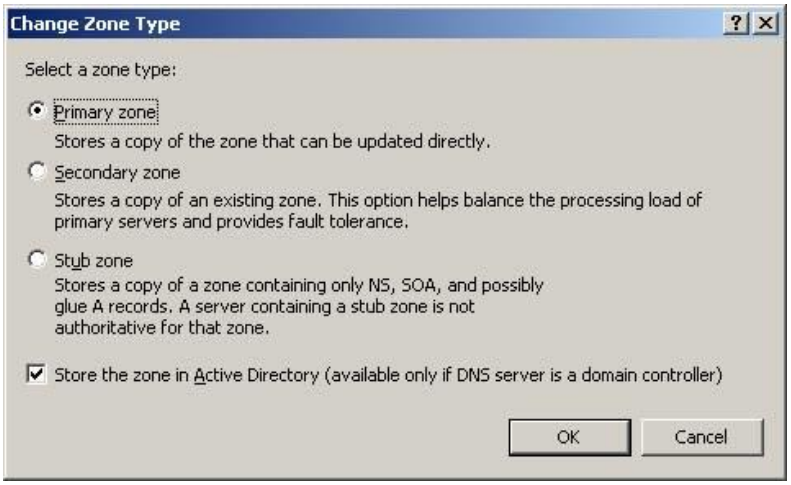
ویندوز ۲۰۰۰ اولین سیستم‌عامل توسعه‌یافته توسط مایکروسافت است که به‌روزرسانی پویای DNS را پشتیبانی می‌کند. سرور را می‌توان به عنوان primary استاندارد یا به‌عنوان zone یکپارچه‌شده‌ی Active Directory مایکروسافت پیکربندی کرد. ویندوز ۲۰۰۰ و جانشینان آن یعنی ویندوز سرور ۲۰۰۳، ۲۰۰۸ و ۲۰۱۲، به‌روزرسانی‌های پویای امن را پشتیبانی می‌کنند. در تمامی این نسخه‌ها، یک الگوریتم TSIG توسعه‌یافته پیاده‌سازی شده است (RFC 3645). زمانی که راهبر سیستم یک zone یکپارچه‌شده‌ی Active Directory را ایجاد می‌کند، به‌طورپیش‌فرض سرور فقط امکان به‌روزرسانی‌های امن را از طریق TSIG توسعه‌یافته می‌دهد. با این‌حال راهبر می‌تواند عدم به‌روزرسانی پویا یا به‌روزرسانی پویا به‌صورت غیرامن را نیز پیکربندی نماید. مهم‌تر از همه اینکه قابلیت به‌روزرسانی امن برای zoneهای اصلی (primary) استاندارد در دسترس نیست و در هر zone اصلی (primary) پیکربندی‌شده برای به‌روزرسانی‌های پویای DNS ، هر فردی می‌تواند zoneها را تغییر دهد.

امنیت به روزرسانی فقط برای zoneهایی در دسترس است که با سرویس‌های دامنه‌ی active directory (AD DS) یکپارچه شده‌اند. بعد از یکپارچه‌سازی zone با دایرکتوری، ویژگی ویرایش لیست کنترل دسترسی در دسترس

خواهد بود و از این پس می‌توان کاربران یا گروه‌هایی را از لیست دسترسی برای یک zone مشخص یا رکورد مشخص حذف یا اضافه کرد.

برای یکپارچه‌سازی باید مراحل زیر طی شوند:

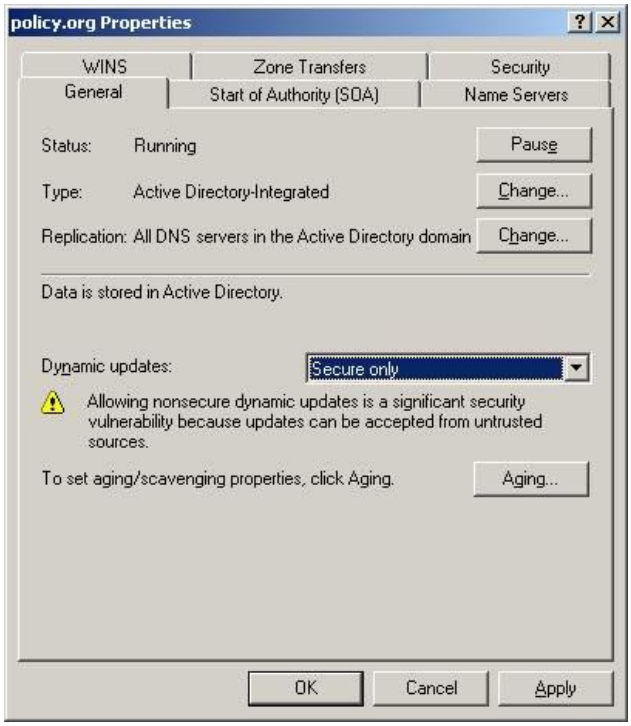
ابتدا بایستی بر روی zone مورد نظر کلیک راست نمود و گزینه‌ی properties را انتخاب کرد و سپس در تب General دکمه‌ی change مقابل type را زد. در این قسمت بایستی تیک Store the Zone Active Directory (available only if DNS server is a domain controller) را فعال نمود و OK را برای ذخیره‌ی تغییرات فشار داد. یک DNS server یکپارچه شده با Active Directory مزایای امنیتی زیادی دارد.



با فعال‌سازی به روزرسانی پویای DNS، راه نفوذ بالقوه جدیدی به سیستم اضافه می‌شود. تمهید فوق باعث می‌گردد تا فقط کامپیوترهایی که به دامنه ی active directory پیوسته باشند بتوانند پایگاه داده‌ی DNS را به‌صورت پویا به روزرسانی کنند.

فعال‌سازی امکان به‌روزرسانی پویای امن

بر روی zone کلیک راست کرده و گزینه ی peroperties را انتخاب کنید. در تب General مطمئن شوید که نوع zone، AciveDirecoty-integrated است. سپس در Dynamic Updates گزینه‌ی secure only را کلیک کنید.



اگر zone با active Directory ادغام شود، لیست کنترل دسترسی می‌تواند برای zoneها و برای مجوزهای کاربران و گروه‌هایی که می‌خواهند داده‌های DNS zone را تغییر دهند استفاده شود.

در جدول زیر لیست مجوزهای پیش فرض گروه‌ها و کاربران برای Dns zoneهای ادغام شده با Active Direcory آمده است.

کاربر یا گروه	مجوز
administrators	امکان خواندن-نوشتن- ساختن همه‌ی شیئ‌ها و مجوزهای ویژه
Authenticated Users	امکان ساختن شیئ
Creator owner	امکان مجوزهای ویژه
DnsAdmins	کنترل کامل-خواندن – نوشتن-ساختن و حذف ChildObjects- مجوزهای ویژه
Domain Admins	کنترل کامل- خواندن – نوشتن-ساختن و حذف child object
Enterprise Admin	کنترل کامل- خواندن – نوشتن- ساختن و حذف child objects- مجوزهای ویژه
Everyone	خواندن- مجوزهای ویژه
Pre-Windows2000	دسترسی سازگار مجوزهای ویژه

System	کنترل کامل- خواندن – نوشتن- ساخت و حذف child objects

البته می‌توان این مقادیر پیش‌فرض را براساس نیازهای خاص خود اصلاح نمود.