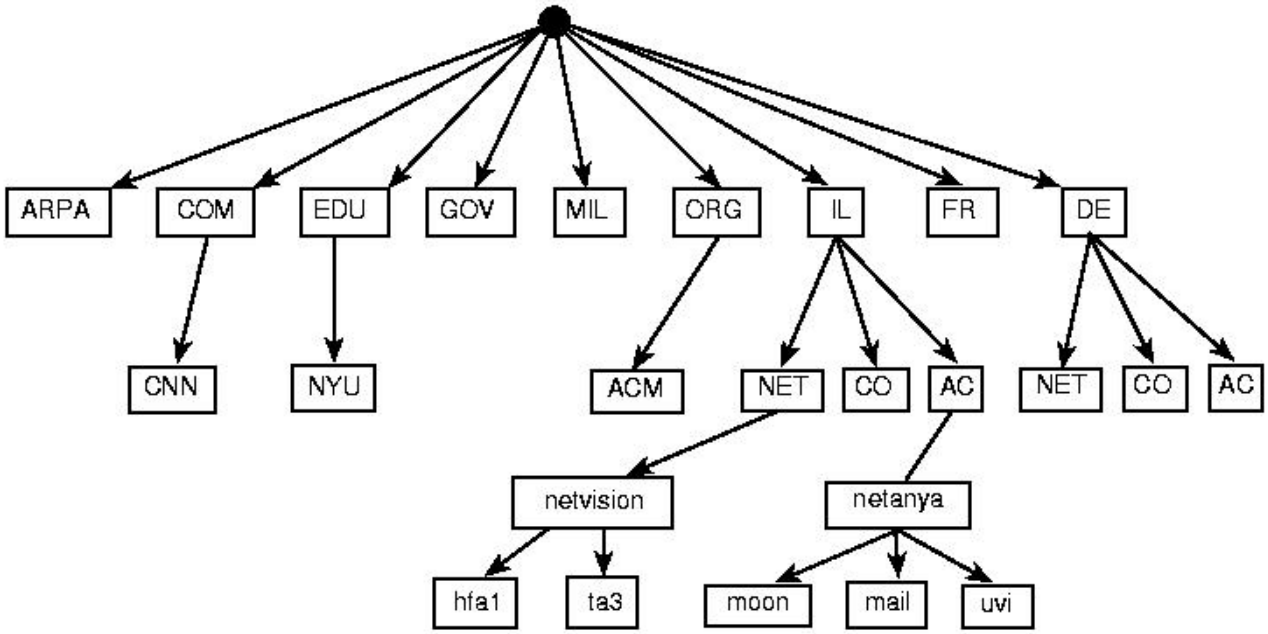
DNS缓存安全

2012-07-02 07:57:16 By admin

关于缓存

缓存中毒攻击者(cache poisoning)给DNS服务器注入非法网络域名地址，如果服务器接受这个非法地址，那说明其缓存就被攻击了，而且以后响应的域名请求将会受黑客所控。当这些非法地址进入服务器缓存，用户的浏览器或者邮件服务器就会自动跳转到DNS指定的地址。例如evilgrade攻击



这种攻击往往被归类为域欺骗攻击(pharming attack)，由此它会导致出现很多严重问题。首先，用户往往会以为登陆的是自己熟悉的网站，而它们却并不是。与钓鱼攻击采用非法URL不同的是，这种攻击使用的是合法的URL地址

另外一个问题是，成百上千的用户会被植入缓存中毒攻击的服务器重定向，引导至黑客设立的圈套站点上。这种问题的严重性，会与使用域名请求的用户多少相关。在这样的情况下，即使没有丰富技术的黑客也可以造成很大的麻烦，让用户稀里糊涂的就把自己网银帐号密码，网游帐号密码告诉给他人。

用这种类似的方法，邮件系统也会受到黑客攻击。只不过不是给Web服务器，而是给邮件服务器非法地址，从而让系统引导至受到控制的邮件服务器中。
那么，黑客究竟是怎么做到使缓存服务器接受非法地址呢?当一个DNS缓存服务器从用户处获得域名请求时，服务器会在缓存中寻找是否有这个地址。如果没有，它就会上级DNS服务器发出请求。
在出现这种漏洞之前，攻击者很难攻击DNS服务器：他们必须通过发送伪造查询响应、获得正确的查询

参数以进入缓存服务器，进而控制合法DNS服务器。这个过程通常持续不到一秒钟，因此黑客攻击很难获得成功。
但是，现在有安全人员找到该漏洞，使得这一过程朝向有利于攻击者转变。这是因为攻击者获悉，对缓存服务器进行持续不断的查询请求，服务器不能给与回应。比如，一个黑客可能会发出类似请求：1q2w3e.google.com，而且他也知道缓存服务器中不可能有这个域名。这就会引起缓存服务器发出更多查询请求，并且会出现很多欺骗应答的机会。
当然，这并不是说攻击者拥有很多机会来猜测查询参数的正确值。事实上，是这种开放源DNS服务器漏洞的公布，会让它在10秒钟内受到危险攻击。
要知道，即使1q2w3e.google.com受到缓存DNS中毒攻击危害也不大，因为没有人会发出这样的域名请求，但是，这正是攻击者发挥威力的地方所在。通过欺骗应答，黑客也可以给缓存服务器指向一个非法的服务器域名地址，该地址一般为黑客所控制。而且通常来说，这两方面的信息缓存服务器都会存储。
由于攻击者现在可以控制域名服务器，每个查询请求都会被重定向到黑客指定的服务器上。这也就意味着，黑客可以控制所有域名下的子域网址：www.bigbank.com，mail.bigbank.com，ftp.bigbank.com等等。这非常强大，任何涉及到子域网址的查询，都可以引导至由黑客指定的任何服务器上。

为了解决这些问题，用于查询的UDP端口不应该再是默认的53，而是应该在UDP端口范围内随机选择（排除预留端口）

如何应对？

但是，很多企业发现他们的DNS服务器远落后于提供网络地址转换（network address translation ，NAT）的各种设备。大部分NAT设备会随机选择NDS服务器使用的UDP端口，这样就会使得新的安全补丁会失去效果。IT经理也不会在防火墙中开放全方位的UDP端口。更严重的是，有安全研究员证明，即使提供64000UDP端口中随机选择的保护，DNS服务器也照样有可能受到中毒攻击。

现在是时候考虑保护DNS的其他方案了。UDP源端口随机化选择是一种比较有用的防护举措，但是这会打破UDP源端口随机化给与DNS服务器的保护，同由此全方位开放端口面临的风险或者降低防火墙性能这两者间的平衡关系。还有一种比较有效的防护措施就是，当检测到面临潜在攻击风险时，让DNS服务器切换到使用TCP连接。

如果攻击者猜测到了必要的参数以欺骗查询响应，那么就需要额外的防御措施了。这意味着DNS服务器需要更智能化，能够准确分析每个查询响应，以便剔除攻击者发送的非法应答中的有害信息。

DNSSnoopy

要利用此漏洞有一个简单的自动化的工具DNSSnoopy ，

作者的介绍运行流程：

- Primero obtiene los servidores DNS del dominio solicitado.
- Comprueba si alguno de ellos es vulnerable al ataque de snooping, para ello se solicita un listado de los dominios más comunes hasta que se encuentra alguno cacheado o se acaba la lista.
- Si se ha obtenido uno o más servidores vulnerables se procede a probar una lista de dominios que se indique para encontrar los cacheados con anterioridad.
- Trata de calcular el tiempo que hace que se cacheó en el servidor vulnerable, para ello compara el TTL obtenido del servidor cacheado con el TTL original.

下载地址 : http://code.google.com/p/dns-snoopy/
作者博客 ： http://blog.buguroo.com/?p=8561
关于攻击的方法稍后放出