企业远程接入配置　不宜贪小失大

几个月前发生的“灰鸽子事件”，表明黑客行为及行为者已然发展成一条产业链，并且是一个赚钱快速成长的产业。数以百万的网民，为了方便从互联网下载方便实用的的软件，但很可能会在无意间外泄电脑中所有的信息，甚至成为攻击第三者的跳板。以前的黑客，大多的是出于技术炫耀，或是好奇而采取黑客行为；随着时代的发展，现在黑客行为却常常和金钱与利益挂勾，并且大批用户被黑的事件更是频频爆发。可以想象，未来黑客行为会更加趋向于以窃取网民用户的利益为出发点，并且手段会更加高明。

Qno 侠诺的技术人员在最近的交流中，也谈论到这个事件。由于 Qno 侠诺在全国各个城市都有技术人员，因此对于用户应用互联网的情况也有全面性的了解。在“灰鸽子事件”的讨论中发现，很多企业用户由于观念不正确或者专业知识不足，常常因此而导致在网络配置上留下很大的漏洞，未来可能成为企业信息外泄的重要渠道。

一、ERP 远程接入配置

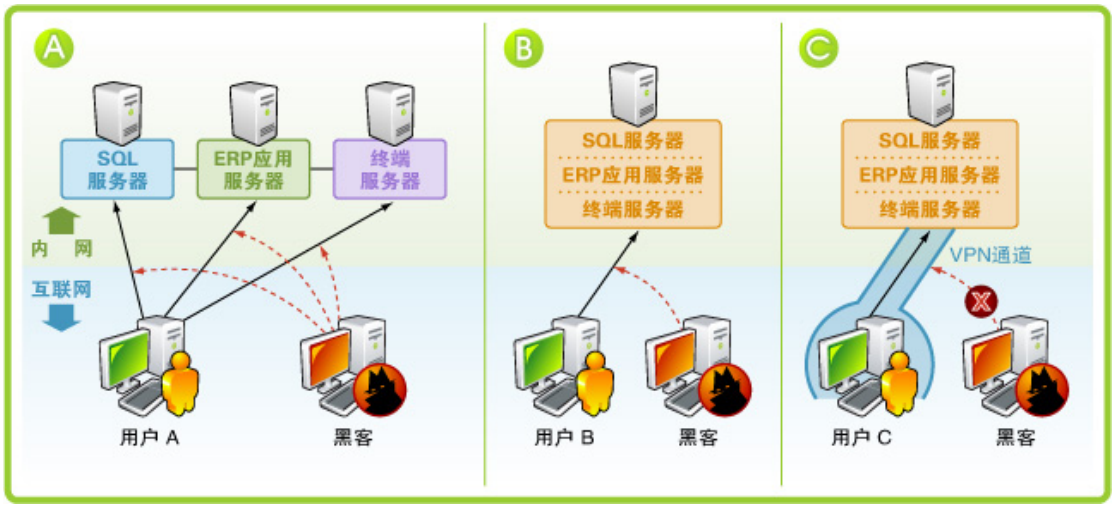
随着企业信息化国家发展政策出台，很多中小企业也建置了像 ERP、财务管理、CRM 等方面的软件系统，作为企业运作的核心。近一两年，据 Qno 侠诺工程师调查发现，更多的中小企业又更进一步地建置了远程接入的系统。这也许是因为经营扩张的需要，或者是因为经营者希望能更迅速地掌握企业现状，希望随时可登陆相关系统。

但是，由于企业希望最大程度地节省成本，因此有些软件商、SI 或者是项目公司会根据客户的需求，采取直接开放内网资源的方式，让互联网用户可以直接使用路由器的虚拟路由功能，直接登陆企业内部服务器。常见的作法包括：第一，直接开放数据库端口给公网；第二，通过应用服务器开放一个端口对公网，再把此端口传来的请求，通过应用服务器转成标准的数据库请求后，交给数据库服务器处理；第三，通过终端服务、Citrix 等软件，让用户直接使用中心的应用系统。

对于这些作法，大多数用户不会感到任何不同，因此也可以达到终端接入的目的。但是由于大部分企业 SQL 服务器和应用服务器放在一台 PC 机上，因此给攻击者一个很好的机会和渠道。例如，早期做法是直接把 SQL 服务器的 TCP1433 端口开放给外部用户，这样就相当于给所有用户都开放了此端口；即使现在大量的软件都是做一个应用服务器中转一下，也是

开放了应用服务器的计算机；而 B/S 的应用，同样要对外开放 SQL 服务器或者其它端口。由于计算机的端口开放，黑客只要使用类似 Portscan 的软件，就可以很快的查到企业服务器。

这样的情况，在台湾、香港或外企公司，由于已经具备很强的安全意识，所以基本上都是用 VPN 来做远程，没有人愿意冒风险以直接开放的方式进行配置。但是在国内，一般项目实施的供应商在项目洽谈的时候，可能考虑控制成本或者是迎合客户决策者的低成本暗示，一般会掩盖此问题，只有在出了安全问题的时候才有可能暴露。所以，企业用户使用路由器虚拟服务的方式，会容易被竞争对手或黑客入侵，导致报价信息、商业机会外泄、投标输掉等情况都有可能发生。



图：企业用户应用情况分析

用户 A：不论是存取终端服务器、ERP 应用服务器，或是 SQL 服务器，都极有可能被黑客侵入；

用户 B：服务器都配置于同一硬件计算器上，风险更大；

用户 C：采用 VPN，使用 VPN 隧道隔离对外联系，黑客无从进入。

二、方便的黑客工具

由于信息交流的方便，再加上有很多像“灰鸽子”这样的服务厂商，利用以上漏洞攻击企业并不困难。

早期应用软件一般采取直接开放 TCP 的 1433 （SQL 常用端口）或 3389（开放终端服务）端口，因此只要知道服务器域名，很容易就可以发动攻击。即使不知道，网络上许多免费工

具软件都可以帮助找到，非常简单，初级黑客即可实现。例如，先用 IPSCAN 扫公网上已经开机的 IP，再用 PortScan 扫已经开机的 IP 的开放端口，同时目前还有很多免费软件直接可以帮你一次性把 IP 和端口都扫出来。

由于服务器的对应端口开放给用户，这样做也同时开放给了互联的所有人，包括黑客。一旦找到服务器及端口，用户如果不强制断开，IP 一般是不会变，在相对的时间内就是一个固定的 IP，此时的黑客就有足够的时间来进行入侵服务器。之后，再用工具软件去猜测 SQL 的密码，一旦 SQL 密码被猜中，所有用户的数据都会被看到。并且，SQL 一般默认密码为空，所以很多时候不用猜测，或者密码很简单，1234，abcd 等，会更容易造成信息外漏。

即使无法入侵，容易造成被网络攻击的风险，例如以 DDoS 进行攻击，导致 1433 端口繁忙，无法回应正常的请求，或者是服务器直接被攻死掉。这都是因为开启端口，所可能引发的问题！

三、中小企业宜防范未然

Qno 侠诺技术服务人员发现，大多数中小企业大量采用路由器的虚拟服务作为远程接入，主要原因是成本问题。但是一半以上的业主，并不了解以上的风险，也无法了解“灰鸽子事件”和自身的网络安全相关连。由于对于网络知识的不足，即使受到攻击，也常常意识不到。

事实上，由于现在很多黑客个人或是工作室，都通过收费的方式提供攻击服务，只不过之前攻击对象主要以网吧和大型企业为主。这是由于网吧对于网络知识比较了解，有些业主会以这种方式打击邻近的网吧，把客人抢过来。随着网吧设备对于攻击的防御能力越来越高，不肖的黑户难免会把主意打到中小企业上来。对于企业而言，招标数据或商业秘密的取得，利益价值是很高的。这样买卖相合，未来针对特定客户的攻击或是盗取资料事件，肯定会更多。

对于中小企业而言，现在的 VPN 产品价格已经不再高不可攀。只要适当地配置，也可用以很省钱的方式建置 VPN 联机，例如 Qno 侠诺的 QVM330 产品，同时支持 IPSec、PPTP 及 SmartLink VPN 协议，中小企业若是只要移动用户或是几台电脑要上线，只要采用 PPTP 即可，建置成本也只在几千元之间。相较于把企业重要的资料，以虚拟服务器的作法开放在互联网上，再采用加密的 VPN 的作法，可达到预防的效果。