赛门铁克互联网安全威胁报告

在过去的六个月中，计算机攻击、IT 产品漏洞以及新形式恶意代码的易感染性所造成的总体威胁仍然切实存在且不断发展。对于没有采取相应防范措施的公司来说，这些威胁增加了他们遭受攻击的风险程度。本报告着重介绍了支持上述结论的具体调查结果，包括以下主题：计算机攻击趋势、漏洞趋势和恶意代码趋势。

计算机攻击趋势

除了蠕虫和混合型威胁活动之外，过去六个月中计算机攻击活动的总数比此前六个月低 6%。平均每个公司每周遭受到大约 30 次攻击，而在此前六个月中每个公司每周遭受到 32 次攻击。尽管此数据有所下降，但过去六个月的攻击活动总数仍比 2001 年同期高出 20%。就攻击类型而言，85% 的攻击都属于攻击前的侦察活动，这类攻击不一定会立即对组织产生威胁。其余 15% 的攻击是由未遂或得逞的漏洞利用尝试所组成。

过去六个月中，公司经历严重事件的可能性比此前六个月稍有下降，至少经历过一次严重事件的公司占 21%，而在此前六个月中占 23%。严重事件发生率远远低于 2001 年同期所记录的 43%。

在过去的六个月中，组织在周末遭受的攻击数量和攻击严重程度明显较低。与互联网连接的所有组织遭受攻击次数的波动情况在很大程度上取决于攻击方系统所在地区的当地时间，而与受害方的当地时间无关。无论受害方位于何处，攻击者活动始终在格林尼治时间(GMT) 12:00 到 21:00 之间处于高峰期。

在过去的六个月中，接受安全监视服务的时间少于 12 个月的客户中大约有 29% 至少经历了一次严重事件，而超过 12 个月的客户中只有 17% 至少经历了一次严重事件。公司接受安全监视服务的时间越长，其经历严重事件的可能性越低。

能源与电力行业的攻击数量和严重事件发生率依然最高，大约有 60% 的电力与能源公司都至少经历过一次严重事件。金融服务行业的严重事件发生率有显著增长。非盈利的公司在攻击数量方面增长显著，而在严重事件发生率增长幅度为中等。电信公司的攻击数量和严重事件发生率都很高。

员工人数较多的大公司遭受攻击的次数和严重程度始终较高。

在过去的 18 个月中，来自明显的攻击源国家/地区的总体攻击活动保持相对稳定。在前六个月中，来自排名前十位的攻击源国家/地区的攻击数量占检测到的攻击总数的 80%；来自美国的攻击仍保持最多，占攻击总数的 35.4%。值得注意的是：在过去六个月中，从韩国发起的攻击总数比此前六个月增加了 62%，从而使该国成为第二大攻击源。

有几个东欧国家/地区无论在攻击总数方面还是在按互联网用户平均计算的攻击数量方面都有所增长。

在过去六个月中，赛门铁克未检测到可证实的计算机恐怖活动。计算机恐怖分子监视名单中的国家/地区发起的攻击不到过去六个月中检测到的攻击总数的 1%。

在过去几年中，在赛门铁克所调查的全部安全事故中，50% 以上都与员工误用或滥用公司资源有关。这些事故造成的财务损失大大超过由外部破坏所导致的损失。

漏洞趋势

2002 年，赛门铁克记录了 2,524 个漏洞，漏洞总数比在 2001 年增加了 81.5%。

比新漏洞的总数增加更加令人担心的是，增加的几乎都是严重程度中等或较高的漏洞。在 2002 年，严重程度为中等和较高的漏洞增加了 84.7%，而严重程度较低的漏洞只增加了 24.0%。

在过去的一年中，攻击者利用新漏洞的相对容易程度仍未改变。在所有的新漏洞中，大约有 60% 的漏洞可以很容易地被利用。

已知的混合型威胁仅仅利用了当前记载漏洞的一小部分。由于以前的混合型威胁能够成功利用数月前发现的漏洞，看起来最近发现的许多漏洞仍极有可能为未来的威胁所利用。

恶意代码趋势

混合型威胁是对互联网团体影响最大的威胁之一。Klez、Opaserv 和 Bugbear 这三种混合型威胁将近占提交的所有恶意代码的 80%。此外，混合型威胁的提交量几乎是 2001 年同期的两倍。

通过自己的 SMTP 引擎进行传播的自我复制群发邮件蠕虫的数量急剧增长。在过去的六个月中，报告的前 50 种威胁中有八种都属于自我复制的群发邮件蠕虫。

在过去的六个月中，通过网络共享传播的恶意代码在增加。W32.Opaserv 蠕虫变种就是这类蠕虫的典型实例。

在过去的一年中，窃取用户机密信息的恶意代码显著增加。由于存在泄漏商业机密、敏感金融信息以及其他形式的私人数据的潜在危险，极容易带来成几何级数增加的潜在破坏力。

即时消息和对等 (P2P) 应用程序强大的市场渗透能力以及日益增长的未授权使用状况，使得这些程序成为对未来混合型威胁充满吸引力的感染媒介。

预计在 2003 和 2004 年移动设备将具有更强的市场渗透能力。由于这些设备的安全防护配置相对较弱，因此是对未来恶意代码极具吸引力的感染媒介。软

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net