



近期 E-Jihad 威胁评估

IntelliSIGHT 典型报告

2007 年 11 月 5 日

目录

综述	3
分析	3
Al-Jinan.net 和其前身Al-Jinan.org对比	3
主页格式和主机.....	3
竞赛和攻击程序依旧提供.....	4
使命	4
时间	4
目标	5
Al-Jinan.net 网站的附加信息.....	5
结论	5

综述

最近的一份报告表明，一批自称“奥萨姆·本·拉登的追随者”呼吁在 2007 年 11 月 11 日发动针对西方世界、犹太人、以色列、穆斯林和什叶派穆斯林叛教网站的电子圣战（即：网络攻击或 e-圣战）。埃赛特伙伴公司的分析专家定位了发布号召电子圣战的网站，并发现了 2006 年 10 月的另一个类似的号召网站。这份报告讨论了“Al-jinan”组织者过去一年的动向，并且确定了我们的评估方向。

分析

埃赛特伙伴公司的分析专家认为：“Al-Jinan group”成功实施攻击的威胁较低。以前从“Al-jinan”发起的电子圣战并没有成功过，主要原因是攻击者没有被恰当的安排攻击时间，拥有太少的攻击者和太多的攻击目标。另外，过去声称被“Al-jinan”成功关闭的网站至今仍未得到证实。因此，尽管该组织内攻击者的技术水平和组织能力得到提高，埃赛特伙伴公司的分析专家仍然认为这种威胁处于较低的等级。

从表面上看，该组织改进了他们的拒绝服务（DoS）自动攻击程序，而且被组织者赋予了更多的控制时机和目标网站。因此，攻击目标范围的缩小使得攻击者参加电子圣战更加容易，然而参与攻击者仍缺乏必要的技术知识。虽然组织者选择攻击时间、攻击目标和工具易用性等问题得到了解决，但攻击手段仍在使用 ping 之类对目标仅有较小影响的攻击形式，导致这种状况的主要原因是由于缺乏参与者。此外，该组织从未以金融机构或西方政府网站为目标，而是主要集中于以色列和基督教网站。由于从 Al-jinan 传出的信息主要讨论误报和攻击以色列，穆斯林叛教者和什叶派的网站，针对金融机构和西方政府网站的攻击可能非常低。

Al-Jinan.net 和其前身 Al-Jinan.org 对比

主页格式和主机

Al-jinan.net 网站被设计成几乎完全与以前的 Al-Jinan.org 网站一样，两者均采用阿拉伯文。虽然一些图片有所变化，但是网站内容基本上是相同的。



Al-jinan.org 的网页标题，上面的阿拉伯语是“电子圣战”

Al-Jinan.net 的主页上面讨论了当他们的服务被终止后其网络恢复的可能性。Al-Jinan.org 以前的主机位于德克萨斯州休斯顿的一家美国公司，是非常有名的网站。但是新的 Al-Jinan.net 位于马

来西亚，由于马来西亚的法律对网站托管的控制不严格，因此能为组织者提供更稳定的服务。其组织者甚至声称新的服务器是受“阿拉真主保护”，并且永远不会消失。



Al-jinan.net 的标题，右边的阿拉伯语是“电子圣战”

网站主页还讨论了名为“黎明前的一个新圣战”的主题，Al-Jinan 组织者声称用来阻止成员接受新闻和电子圣战攻击日期的电子邮件问题已经解决。主页还包含其他到各种网页的网站链接，详细的内容在本报告后面有介绍。

竞赛和攻击程序依旧提供

Al-Jinan 组织者今年初改进了他们的电子攻击方法，其中包括参加基于小时数的攻击竞赛。和之前的攻击一样，多数成功的攻击者的名字将被列在网站上面而且将获得荣誉勋章奖励。这些特征被认为是一个升级的自动 DoS 攻击程序的圣战 2.0 版本。Al-Jinan 现在提供的圣战 3.0，非常类似于圣战 2.0（一个自动 ping 类型的拒绝服务攻击程序）。两者的区别在于 3.0 版本提供自动更新目标功能。为了方便组织者监视攻击者攻击的持续时间，网站需要用户注册一个用户名和密码并登录。一旦注册并登录，攻击者每一小时的攻击将获得 1 分。此外，Al-Jinan 组织者提供给注册的攻击者每人 24 分。分数最高的攻击者将获得直接接触高级首脑的资格并被赋予特殊任务。

使命

Al-Jinan 组织者宣称其使命是攻击有限的网站使其超负载并崩溃。组织者希望他们的这种攻击会增加目标公司的运营成本并最终危害其业务发展。组织者还声称，他们的这种攻击策略将导致目标公司最终无法负担其自身的网站的开销。

时间

Al-Jinan 的组织者似乎吸取了以前 e-jihad 的教训。当他们尝试于 2006 年 10 月和 2007 年 6 月发动攻击时，攻击时间没有明确规定而且实际攻击参与者处于不同的时区的问题也被忽略了。此次攻击将从 2007 年 11 月 11 日开始，每天 24 个小时连续不断的进行攻击，将持续一周的时间或者直到目标网站被强制关闭为止，这样做不需要同步所有攻击者的攻击时间。然而，这种做法在很大程度上需要有大量的参与攻击者和较长攻击时间才能完成。

目标

过去的攻击中，所有的攻击目标都被列举在网站的首页上面，而且都配上了诸如“以色列和伊斯兰教的敌人”的简单描述。攻击者可以选择其中列出的目标，但是对于 Jihad3.0 版，组织者声称程序将会自动更新攻击目标列表（埃赛特伙伴公司还没有核实）。组织者还声称攻击目标列表将在开始攻击前的 15 分钟有效。虽然此情况仍然未知，但是攻击目标很有可能仍然遵循过去的标准，即以以色列或基督教网站为主。组织者指出这次袭击是针对西方、犹太人、以色列、穆斯林和什叶派穆斯林叛教网站。

Al-Jinan.net 网站的附加信息

网站主页上面提供的可用链接包含了各种各样有关电子攻击的信息，以供参与攻击者浏览。这些信息包括专用术语，如：常用术语“jihad”、Jihad3.0 可执行文件的下载、攻击程序的使用说明书、一个“关于我们”和“联系我们”页面。“联系我们”页面包含一份完整的用户表，直接供 Al-Jinan 组织者使用。同时，也为攻击者提供了各种信息的链接。这些信息讨论关于穆斯林、穆斯林游击队、黑客、高速互联网连接的所有者、圣战组织和敌人等。更多有关 Al-Jinan.net 的信息将被列入埃赛特伙伴公司每月威胁报告。

网站主页上的 Jihad 3.0 截图如下所示：



Al-Jinan.net 上 Jihad 3.0 的屏幕截图

结论

埃赛特伙伴公司将继续关注和评估 Al-Jinan，因为他们可能通过提高攻击者的能力，进而攻击银行类金融机构和西方政府网站。此外，随着其预计的攻击日期（2007 年 11 月 11 日）的临近，埃赛特伙伴公司将继续关注 Al-Jinan 组织。更多有关此网站和参与攻击者的详细信息及潜在的攻击目标将在下个月的威胁报告中讨论。