This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

反信息滥用工作组（MAAWG）有关采用宽带花园（Walled Garden）的最佳做法

退出、登录、修复和用户教育的标准

引言

源自用户的网络滥用现象的日益增长，需要互联网业务提供商（ISP）更主动地采取措施，保护其网络以及网络生成的业务。僵尸程序（Bot）和僵尸网络（botnets）越来越成为垃圾邮件制造者和黑客的得力工具，通过传播垃圾邮件、病毒和其它形式的恶意软件达到滥用网络的目的。在用户浑然无知的情况下，这种恶意软件被悄然植入用户的个人电脑，结果无辜的最终用户被锁定为这些恶意网络的头号帮凶。

为强化 MAAWG 保护电子信息免受在线利用或滥用的职能，MAAWG Botnet/Zombie（僵尸主机）分委员会就部署宽带花园提出了以下最佳做法。宽带花园是指一种可对用户获准使用的信息和服务以及获得的网络访问权加以控制的环境。这些做法的首要目标是帮助最终用户了解并清除其个人电脑中存在的无用程序或恶意软件，并制止对网络的滥用。除非另有规定，ISP 将负责所有建议的实施工作。

关于本文通篇可见的“必须”（MUST）、“应该”（SHOULD）和“可以”（MAY）等关键词的用法和定义，请见 RFC 2119 中的说明。

一、退出和登录进入/退出宽带花园的标准必须简明扼要

使用户了解受恶意软件感染的个人电脑面临的风险和问题，ISP“可以”为新的用户帐户或任何他们认为有风险或生成可疑业务流的帐户设置宽带花园。宽带花园的进入和退出标准必须清晰扼要，便于终端用户理解。

建议综述：

a) **“必须”对可疑问题发出了明确通知，如使用可接受使用策略（AUP）范围以外的网络。 AUP 还“必须”对通知做出解释，并概要介绍建议对含有恶意软件的电脑采用的纠正或清除措施。**

b) **“可以”将 HTTP [80]分别转往隔离网址或网站。**

c) “可以”将 botnet 命令和控制业务转发至蜂罐网络（honey network）进行分析。

d) “应该”将所有出局的 SMTP [25]控制在一个隔离区或蜜罐程序信息传送代理（MTA）内部。

e) “应该”允许基于信任的快速取消。可通过说明一台个人电脑清洁无毒的动作或在一可配置的时间段内“原封不动”地使用网络的请求加入信任。

f) “可以”在下载与安装经 ISP 批准的清除或安全软件后提供退出。

g) ISP“可以”使用内部用户信誉衡量标准（利用内容过滤器、深度包检测技术和行为使用模式等探测技术加以确定），启动进入或退出宽带花园的事件。

h) 正如已安装和受信任的用户客户端软件宣传的那样，ISP“可以”利用技术自动确定用户的安全态势。

二、恢复体验必须做到方便最终用户

在为保护其网络和用户免受恶意滥用而做出不懈努力的过程中，ISP 的做法决不能给最终用户带来过多不便。为收回投资，ISP 也“可以”自行决定有偿地向最终用户提供恢复工具。提供这类工具的方式“必须”适应 ISP 特有的支持环境。此外，宽带花园“必须”提供网站接入，使最终用户能够通过直接接入或间接代理连接机制，下载重要和适用的软件更新和补丁程序。（这给提供商和签约的 ASP 通过单一门户网站提供恢复服务提供了可能，这种方式似于微软代您启动 Windows 更新和多种新驱动程序的下载。）

建议综述：

a) “必须”能够提供免费和/或有偿的恢复可选方案（或与现有在线工具的链接）。

b) “必须”提供可识读的信息，将上述体验作为正式的 ISP 通知或恢复程序予以正式批准。例如，这一信息包括账号或私密问题答案等数据。

c) “必须”提供关于为寻求帮助而联系客户支持部门的详细信息。

d) 不“应该”为追求恢复体验而要求重启最终用户的个人电脑。

e) “必须”提供 URL 和域的链接，以（酌情）解决 OS 补丁程序和安全更新的非理想状况。

f) “应该”提供“点击与客户支持交谈”服务或代表 ISP 提供客户服务的第三方。

g) “应该”提供 ISP 支持或滥用联系信息（如电话号码）。

h) “应该”通知发出恶意 SMTP [25]业务的客户重新配置其邮件用户代理（MUA），并经端口 587 发送出局电子邮件业务流。

i) “应该”根据非理想条件或以往的用户动作提供独特的恢复体验，例如用户“应该”亲眼看到对症下药地解决问题或可疑类型恶意软件的过程。

j) “应该”提供侵入性最小的客户端，其下载迅速、安装方便，不会与已配置的安全客户端的其它应用软件发生冲突，无需重新启动，也不需要为监测和清除恶意软件而对电脑进行整体扫描。

k) “必须”能够转发例外情况，使用户能够使用应急在线服务。

三、应把最终用户教育作为头等大事

由于最终用户通常是安全链条中的薄弱环节，ISP“应该”为通过其网站提供文件资料做出适当努力，让最终用户未雨绸缪、自我教育，了解怎样缓解受恶意软件感染的风险。为此，“应该”以“常见问题解答”、支持服务音像片、辅导课和可查询知识库的形式，向最终用户提供文件资料。而且向他们提供资料的方式，“必须”与 ISP 客户服务界面的外观和感受相一致。除此之外，提供的资料“应该”具有广泛性，能够涵盖多种互联网技术和不同电脑操作系统（如 Windows、MacOS、Linux）的应用。

建议综述：

a) “必须”提供可识读的信息，将上述体验作为正式的 ISP 通知或恢复程序予以正
式批准。例如，这一信息将包括账号或私密问题答案等数据。

b) “应该”以“常见问题解答”和辅导课的形式提供直观的用户教育。

c) “应该”提供诸如简单的音频问候语和知识查询中心等可选的学习中心工具。

d) “应该”提供针对电子邮件（POP3/SMTP）和浏览（HTTP）等多类应用的教育
信息。