SAC 025
SSAC 关于快速通量宿主和 DNS 的公告

ICANN | SSAC
安全和稳定咨询委员会

ICANN 安全与稳定
咨询委员会 (SSAC)
公告
2008 年 1 月

简介

“快速通量”(Fast flux) 是一项躲避技术，网络罪犯和互联网破坏者使用该技术来躲避身份验证，并阻挠旨在找到和取缔非法网站的执法和反犯罪工作。快速通量宿主 (Fast flux hosting) 支持多种多样的网络犯罪活动（欺诈、身份窃取、在线诈骗），被视为当今针对在线活动的一种最为严重的威胁。“双层通量”(double flux) 是快速通量宿主的一种变体，它利用了域名注册和名称解析服务。

本公告从技术的角度，描述了快速通量宿主和快速通量服务网络。本公告阐释了域名系统 (DNS) 如何被快速通量宿主用来从事犯罪活动，确定了快速通量宿主造成的影响，并且针对此类攻击运用这些快速通量技术来延长其执行非法活动的恶意或有利可图的生存期，呼吁应当为此引起特别关注。本公告介绍了当前在互联网的不同阶段缓解快速通量宿主不良影响的可行方法。本公告探讨了这些缓解方法的优缺点，确定了安全与稳定咨询委员会 (SSAC) 认为行之有效的一些方法，并建议有关机构应考虑出台相关政策，以便让注册人、互联网服务提供商 (ISP)、注册服务机构和注册管理机构（如果适用）能够普遍受惠于这些实际可行的缓解方法。

背景

安全专家、反网络犯罪社群，以及执法机构已经对快速通量宿主研究了一段时间。快速通量宿主可以操控由遍布全球的被盗用系统组成的大型分布式网络。随着地下业务日益猖獗，导致互联网破坏者可以租赁到数十个乃至上千个被盗用系统构成的快速通量服务网络[1]。这些服务网络运营商使用分层的隐蔽（加密）信道和代理技术。他们通过例行查询被盗用系统的状态来“精心”管理这些网络，并根据有无响应来向网络添加和从网络中删除被盗用的系统。域名社群应当特别关注这些运营商自动更新域名服务的方式，通过这种方式，这些运营商隐藏了执行以下非法活动的网站位置 – 盗用 IP（音乐、视频、游戏）、作为儿童色情网站、钓鱼系统、销售非法药品的宿主，以及执行身份盗用和欺诈。

有一种快速通量宿主的变体，它通过快速更新 DNS 信息来伪装托管非法活动的网站和其他互联网服务的宿住位置。此外，还有一种叫作“双层通量”的变体，互联网破坏者利用另一个托管 DNS 服务器的服务网络，来补充这个托管非法网站的服务网络。本公告的后续部分对这些服务网络的具体操作进行了详细介绍。

[1] 安全组织在其文献和发布的资料中描述快速通量宿主时，会使用各种不同的术语。在本公告中，我们应用了 Honeynets 项目报告“*Know Your Enemy: Fast Flux Service Networks*”（了解您的敌人：快速通量服务网络）上的术语，请参阅 http://www.honeynet.org/papers/ff/

术语

当前，为了尽可能描述这种复杂、多面性的快速通量技术，SSAC 首先确定了互联网安全社群中与快速通量宿主关联的一些术语：

僵尸网络。僵尸网络是指因为运行软件僵尸程序而被感染的第三方计算机组成的网络。在从事任意数量的未经授权或非法的活动时，这些僵尸程序可接受远程控制，一开始由真正的攻击者控制，随后由那些向攻击者付费以使用僵尸网络的一方控制。这些攻击者通常与有组织的犯罪分子关系密切。攻击者通过间谍软件下载或附带于电子邮件中的病毒，在不通知也不经过授权的情况下，将“僵尸软件”安装在 PC 上；而更为普遍的做法是，通过浏览器或其他客户端攻击（如受到感染的横幅广告）进行安装。一旦执行了僵尸程序，就会建立一个反向通道，通往由攻击者设立的控制基础设施。传统的僵尸网络设计采用集中化模式，且所有反向通道均连接到攻击者的命令和控制中心 (C&C)。近期，僵尸网络运营商采取对等模式来执行反向通道操作，以阻止通过流量分析来检测 C&C。

僵尸牧人。僵尸牧人设计并使用分布式攻击来创建、维护和利用僵尸网络，以获取经济或其他（政治）利益。僵尸网络建立后，僵尸牧人会将其僵尸网络的使用权租赁出去，为**快速通量服务运营商**提供便利

快速通量。这个术语用来表示将网络、电子邮件、DNS 或通常任何互联网或分布式服务的位置从一台或多台连接到互联网的计算机快速移动到另一组计算机，以延迟或躲避检测。

快速通量设施。在本文中，术语 *设施*是指未经同意就安装到整个互联网中大量计算机上的软件代理。

快速通量服务网络。在本文中，服务网络指的是僵尸程序的子集，僵尸牧人将这些僵尸程序分配给指定的快速通量服务运营商，该服务运营商转而为其客户提供用于快速通量宿主或域名服务的设施。请注意，此服务网络经常由“中间人”操作，而不是由客户亲自操作。

剖析快速通量宿主

接下来的描述代表了快速通量宿主的特征。其他表现形式和变体与之类似，攻击者将来可能还会更改快速通量宿主，以躲避此处所述的可检测到快速通量宿主的方法，或者添加其他层次结构或抽象层。

在大量关注快速通量技术层面的同时，也需要对存在的一系列相关“业务”活动进行说明。我们来看一个破坏者打算进行网络钓鱼攻击的案例。

快速通量宿主的业务层面应当从恶意软件编写者说起。一些恶意软件编写者开发了可定制的网络钓鱼工具包、软件包，其目的在于向一组收件人发送网络钓鱼电子邮件，并托管那些向受害者发送网络钓鱼电子邮件的相关非法网站。其他编写者则出租电子邮件地址，并销售可用于发送垃圾邮件的地址列表。还有一些人在开发僵尸软件。僵尸软件是一种灵活的、可远程控制的代理，它在接到指令后可代表相应的**命令和控制中心** (C&C) 软件来执行任意功能：一旦隐蔽地安装在受感染的系统上，僵尸软件则会为后续的下载以及远程执行其他针对特定软件的攻击提供便利。尽管现在使用最多的是客户端破坏（例如，基于浏览器的攻击），但是僵尸牧人经常使用电子邮件承载的蠕虫来感染并破坏成千上万个系统。

在网络犯罪团体中，恶意软件编写者和僵尸牧人是*物品供应商*。物品供应商使用加密、专用/安全的互联网中继聊天 (iRC) 渠道或类似的地下会议场所发布广告，寻找犯罪物品的买主[2]。僵尸牧人的犯罪物品基本上都是可以出售或租赁的工具。僵尸牧人将协商好数量的受损系统的命令和控制权租赁给客户，客户既可以直接使用，也可以代表其他破坏者进行管理；在后一种情况下，僵尸牧人的客户就是作为快速通量宿主服务的提供商。在这种复杂而隐蔽的经济活动中，想要从事犯罪活动的一方可以与若干其他方进行协商，以获得垃圾邮件（网络钓鱼）列表，部署网络钓鱼系统或其他攻击工具包以及僵尸网络，并亲自进行攻击；也可以与某一方（快速通量服务网络运营商）进行协商，根据自身利益指导网络钓鱼攻击。

在快速通量宿主中，快速通量服务网络主要用于以下两种目的：

1) **托管引荐网站**。此服务网络中的僵尸程序通常并不托管快速通量客户的内容，但是会将网络流量重定向到网络服务器，快速通量客户将在该服务器上托管未经授权的或非法活动。如果这是唯一进行快速通量宿主操作的网络，则适用的术语是*单层通量*。

2) **托管域名服务器**。此服务网络中的僵尸程序为快速通量客户运行域名服务器引用网站。这些域名服务器将 DNS 请求转发给隐藏的域名服务器，后者托管了包含一组引荐网站的 DNS A 资源记录的区域。与通过引用域名服务器并以中继的方式返回响应不同，隐藏的域名服务器直接回复给查询主机。如果将第二种网络与 (1) 结合运作以增强欺诈性，则适用的术语是*双层通量*。

[2] 请参阅 *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*（互联网破坏者财富的性质和原因探究）中描述的“Market Activity”（市场活动），*网址为 http://*www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

图 1 对上述关系进行了说明。

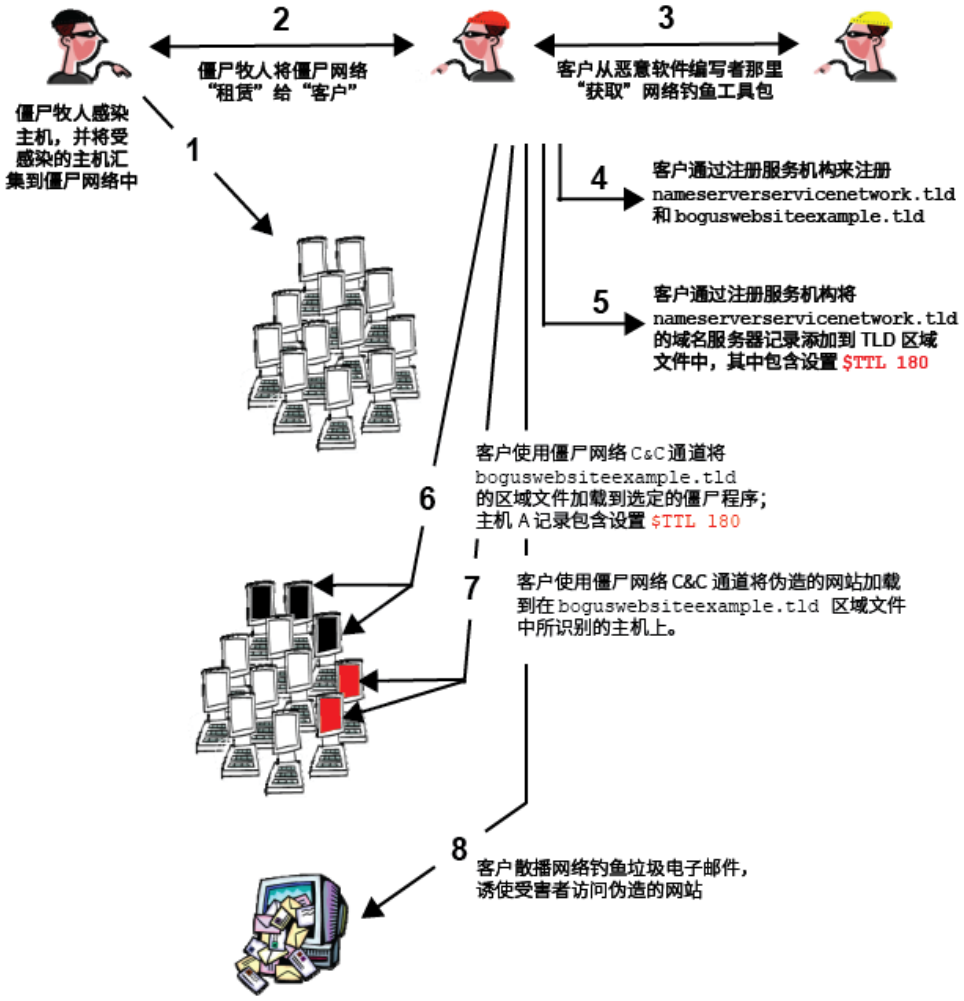

图 1.“双层通量”托管攻击的要素

利用名称服务：双层通量宿主

快速通量客户往往通过认可的注册服务机构或分销商来注册域名，然后从事非法活动。作为攻击的一种形式，快速通量客户会注册一个通量服务网络的域名来托管非法网站 (`boguswebsitesexample.tld`)，并注册第二个或多个通量服务网络的域名来提供名称解析服务 (`nameserverservicenetwork.tld`)。快速通量客户认为这些域名归其快速通量服务网络的运营商所有。快速通量服务网络运营商会使用

自动化技术来快速更改注册服务机构为这些域维护的注册记录中的域名服务器信息，尤其是快速通量服务网络运营商

- 会更改域名服务器的 IP 地址，进而指向域 nameserverservicenetwork.tld 中的其他主机，并
- 将这些域名服务器的地址记录生存时间 (TTL) 设置为极小的值（通常为 1-3 分钟）。

快速通量宿主使用的域名服务器域的相关资源记录可能会出现在顶级域 (TLD) 区域文件中，如下所示：

```
$TTL 180
boguswebsitesexample.tld.       NS  NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.       NS  NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.    A  10.0.0.1
NS2.nameserverservicenetwork.tld.    A  10.0.0.2
```

请注意，资源记录的生存时间 (TTL) 值设置得非常低（上述示例中为 180 秒）。TTL 过期时，快速通量服务网络运营商的自动化功能将确保使用域名服务器的新 A 记录集替换现有的记录集：

```
$TTL 180
boguswebsitesexample.tld.       NS  NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.       NS  NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.    A  192.168.0.123
NS2.nameserverservicenetwork.tld.    A  10.10.10.233
```

因此，用于识别并关闭支持此类快速通量攻击的域名服务器的时间也非常短。

nameserverservicenetwork.tld 中的资源记录指向代理或引用主机，而非提供 boguswebsitesexample.tld 名称解析的僵尸程序。引用主机会侦听端口 53，并将 DNS 查询转发给托管 boguswebsitesexample.tld 区域文件的“DNS”僵尸程序。“DNS”僵尸程序将欺诈网站的域名解析为 Web 通量服务网络中主机的 IP 地址，并直接将响应消息返回到发出查询的解析器。此时，只有非常大的引用主机池可以识别 DNS 僵尸程序的 IP 地址，并且引用网络的 IP 地址每 180 秒更改一次。

引荐 Web 通量宿主

在上一部分，我们阐述了双层通量宿主如何通过利用 nameserverservicenetwork.tld 网络中的僵尸程序并迅速更改 boguswebsitesexample.tld 网络中引荐 Web 服务器主机的 A 记录来提高躲避水平。引荐 Web 服务器的 A 资源记录的 TTL 也配置得很短。如果 Web 服务器主机的 TTL 过期，快速通量服务网络运营商的自动化功能会再次确

保使用 Web 服务器的新 A 记录集替换现有的记录集。因此，用以识别并关闭支持此类快速通量攻击的引荐 Web 服务器的窗口期也非常短。

与非法网站相关的记录会出现在 nameserverservicenetwork.tld 网络中 DNS 僵尸程序所托管的区域文件中，如下所示：

```
boguswebsitesexample.tld.   180      IN     A      192.168.0.1
boguswebsitesexample.tld.   180      IN     A      172.16.0.99
boguswebsitesexample.tld.   180      IN     A      10.0.10.200
boguswebsitesexample.tld.   180      IN     A      192.168.140.
                                                   11
```

再次提醒您注意，各条 A 资源记录的生存时间 (TTL) 值设置得非常低（上述示例中为 180 秒）。TTL 过期时，资源记录会自动修改，以指向托管此非法网站的其他僵尸程序。仅仅在数分钟之后，区域文件就会显示以下内容：

```
boguswebsitesexample.tld.   180      IN     A      192.168.168.
                                                   14
boguswebsitesexample.tld.   180      IN     A      172.17.0.199
boguswebsitesexample.tld.   180      IN     A      10.10.10.2
boguswebsitesexample.tld.   180      IN     A      192.168.0.11
                                                   1
```

迅速更新 boguswebsitesexample.tld 区域中的 A 记录以及 TLD 区域中的域名服务器 A 记录的综合效果是，极其有效地让非法网站（相对于没有使用快速通量的网站）具有更长时间的操作状态。

快速通量宿主：与域名品尝（Domain Name Tasting）有关？

在某种程度上，域名品尝和网络钓鱼属于相互关联的活动[3]。反网络钓鱼工作组 (APWG) 所发布的报告讲述了品尝域名和网络钓鱼攻击之间的关系。该报告对两种研究的调查结果进行了概括总结，这两种研究尝试确定品尝域名的团体是否也使用这些域名来推动网络钓鱼攻击。其中一位 APWG 成员以一组用于网络钓鱼攻击的域名开始研究，并尝试确定这些域名是否在新注宽限期已取消使用。另外一位 APWG 成员将网络钓鱼攻击所使用的域名与三百万左右的域名列表进行比较，这三百万左右的域名在一周之内经过品尝。这两种研究的结果表明，“极少情况下执行网络钓鱼的破坏者会执行域名品尝，并且还有一些情况可以解释网络钓鱼与品尝无关”[4]。

网络钓鱼攻击越来越多地使用快速通量宿主（尤其是对主要财务机构进行攻击）；因此，SSAC 得出的结论是，域名品尝与快速通量宿主之间无针对性的关系。另外，SSAC 还发现，快速通量宿主与域名品尝的目标不尽相同。快速通量宿主的主要目标是，延长托管非法活动的站点的生存时间；根据以往的经验，这些非法活动可以获取利润，并涉及财务信息和信用卡窃取行为。被盗的信用卡用

[3] 请参阅 CADNA 背景，网址为http://www.cadna.org/en/index.html
[4] APWG：网络钓鱼与域名品尝之间的关系，
http://www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

于支付钓鱼网站域名注册费用，因此没有动机来注册域名并使用该域名。比较看来，域名品尝者只在乎支付域名的注册费用，经过证实，这些域名可以在几天内的试用期内获取利润。

当前可用的缓解方法

可以实施几种缓解方法，以减少由快速通量宿主造成的威胁。

关闭托管快速通量设施的僵尸程序

僵尸牧人会危及到商业和居民社区网络中的计算机安全。不过，僵尸牧人通常会攻击那些连接到居民社区宽带接入电路（电缆调制解调器和 DSL）的安全保护较差的计算机，因为这样找到可攻击主机的可能性要大一些，而攻击那些由经验丰富的 IT 员工管理的网络，可能性就要小一些。教育、政府或企业领域的主机容易遭到系统破坏，但是一般来讲，这些主机很少会受到攻击，而且如果尝试对其进行攻击，网络管理员会很容易检测到。

目前可以采用几种缓解方法来降低用于托管僵尸软件的 PC 数量，这些方法可以进行广泛实施，具体如下（当然不仅限于此）：

a) 在专用和公用（如居民社区宽带访问服务）网络中的主机上，采用改进的桌面安全措施（防病毒、反间谍、个人防火墙软件、主机入侵检测软件）。
b) 部署反恶意软件网关。居民社区宽带访问客户由 ISP 为其部署；商业网络由托管安全服务提供商或内部安全管理员为其部署；专用网络的安全管理员也越来越多地采用反恶意软件网关。
c) 教育、认知和培训。将重点特别放在了解和应用严格的输出流量实施政策上。

其他可以考虑的缓解方法包括：

d) 将流程和可执行文件列入白名单。
e) 网络访问/许可控制。
f) 分析已知的僵尸网络行为、开发可用于在“威胁管理”安全网关中阻止该活动的检测技术（如签名）。这种做法是对上述 (b) 项合理的延伸。

虽然 (a) 项和 (b) 项看起来可行性最强，但这两种方法对缓解恶意软件威胁的有效性并未得到验证。Storm[5] 和类似设计的恶意软件，其创建者可通过使用尚未检测到的僵尸网络定期进行更改和分发[6]，并且基于签名的反恶意软件措施对于清除

[5] Storm Worm DDoS 攻击，网址为 http://www.secureworks.com/research/threats/view.html?threat=storm-worm
[6] *Imperfect Storm aids spammers (不完美的 Storm 蠕虫病毒为垃圾邮件发送者推波助澜)，网址为* http://www.securityfocus.com/news/11442

Storm 木马程序之类的恶意软件并没有什么效果[7]。受这些恶意软件感染的 PC 数量在社群中迅速增长，导致社群根本来不及确定受损的 PC 并对其进行杀毒。教育和认知 (c) 是一个费力且进展缓慢的过程。据《CSI/FBI 计算机犯罪和安全调查》报告，97% 的 PC 运行了防病毒软件，79% 运行了反间谍软件，然而僵尸程序感染率仍然居高不下。2007 年 6 月，美国 FBI 公布，通过其持续开展的打击僵尸网络犯罪活动发现，仅在 FBI 美国管辖范围内，就有超过一百万台 PC 遭受僵尸软件的侵害[8]。该数据只涉及企业/商业网络。而在居民社区宽带用户中，使用防病毒和反间谍软件的比例并不高，安全和网络配置更容易忽视，并且对反恶意软件定义更新的订阅通常也不及时。

将流程和可执行文件列入白名单是一种预防恶意软件的技术，该技术可强制实施可执行的政策，具体来说，除受信任的一系列应用程序和相关流程外，所有程序在 PC 上的运行都将受到阻止。将可执行文件列入白名单的技术并没有得到广泛实施，特别是在消费者/居民社区互联网用户中间。应用程序的多样性、新应用程序的不断引进、缺乏消费者友好的商业产品和可以对白名单提供服务的受信任权威机构（如果这种模式还可以跟踪的话），这些都会妨碍白名单技术的采用。

如今，制定网络接入/许可控制解决方案的目的在于，防止不安全的终端连接到局域网 (LAN) 和无线局域网 (WLAN)。允许计算机连接到互联网之前会对计算机执行安全评估，以确认该计算机是否不包含恶意可执行文件。如果计算机受损，则会将其隔离，并且在安全违规问题得到纠正后才可重新连接。这是因为居民社区宽带并未广泛实施 (e) 项，并且可能还要求遵循其他标准和开发软件。ISP 和居民社区宽带访问提供商表明，他们无法承担昂贵的费用来实施并管理网络接入及输入流量筛选。

关闭快速通量主机

很多受此类攻击影响的主机都是连接到居民社区宽带服务的 PC。这些 PC 通常会托管引用网络和域名服务器僵尸软件。

目前最常用的缓解程序包括事件检测、隔离和响应。首先，确定或报告托管非法活动的系统。在快速通量宿主场景下，这可能是引用 Web、域名服务器或托管非法网站的系统，反犯罪投诉人会收集有关该网站的信息：托管系统的位置和管辖权范围；域所有者，网站管理员和 ISP；以及非法活动的类型。投诉人使用 WHOIS 服务

[7] 常见的恶意软件枚举 CME-711木马下载程序。http://cme.mitre.org/data/list.html

[8] *僵尸网络犯罪潜在受害者数量超过 100 万，网址为* http://www.fbi.gov/page2/june07/botnet061307.htm

和其他方法来识别并与多方联系（以并行和重复的方式），直至他们在关闭非法活动方面获得帮助[9]：

- 如果非法活动托管于受损系统上（如，托管于执行合法业务的 Web 服务器上，但管理员并不知道该服务器还托管了非法网站），则应当联系相关域的所有者，以提供关闭主机的帮助。
- 与 ISP 或托管提供商取得联系，以要求终止主机上的相关服务。
- 如果投诉人需要获得当地帮助（语言解释、证实投诉人值得信任，或帮助获得更多信息），则应与当地计算机紧急事件响应小组或突发事件响应小组 (CERT/CIRT) 联系。（在某些国家/地区，CERT 鼓励投诉人尽可能在该流程的早期与其联系）。
- 如果僵尸程序位于 PC 主机的域名服务器上，则应与注册服务机构或注册管理机构联系，以删除 TLD 区域文件中的 NS 记录或暂停域的使用。

非法网站本身可能会通过合法域中受感染的服务器、共享托管的网站提供商或（准）合法、“牢不可破”的网络托管设施进行运作[10]。如果无法进行合作，原因可能是运营商和地方当局不认可或不信任投诉人，或不愿意根据投诉人和 CERT 提供的信息采取行动，投诉人则应当向执法机构 (LEA) 寻求帮助或获取法院指令以迫使运营商关闭网站。这通常是最后才会采取的行动，因为要了解 LEA、与其协作以及获得相应权限的法院指令往往需花费数天或数周的时间，而投诉人寻求在几小时内关闭非法网站。

迅速修改 A 资源记录（解析变动的引用 Web 服务器）会阻止检测，并妨碍采取措施关闭快速通量宿主网站。在很多情况下，托管快速通量的非法网站的生存时间会远远超过 4 天左右的平均天数[11]。

改进这种缓解方式的措施包括：

[9] 这个方案（涉及与投诉人的个人通信往来）是在快速通量宿主的情况较为严重时，用来投诉网络钓鱼攻击的典型方法。

[10] “牢不可破”的托管指的是，那些对托管在他们服务器上的内容和活动很少或几乎不进行治理的 Web 和批量电子邮件托管提供商。使用“牢不可破”这个词是为了强调托管于此类提供商的服务将不会被取缔。很多“牢不可破”的托管提供商并没有与执法机构和反犯罪组织真诚合作，地方当局和互联网法律在对其业务运营实施司法管辖权的同时，也为非法活动提供了相对安全的隐蔽所。

[11] APWG 自 2006 年 12 月至 2007 年 8 月的月度统计中报告，网络钓鱼网站的平均在线时间为 3.3 至 4.5 天，请参阅 http://www.apwg.org/phishReportsArchive.html，但是在计算这个平均天数时，并没有区分按照惯例托管网络钓鱼的网站与使用快速通量的网站。由于快速通量主机的 IP 变化迅速，因此快速通量托管方式会*降低*此数据。

1) 采取可促进域名暂停的程序，避免产生非法网站在关闭后又很快通过其他 ISP 在其他服务器上重新托管的问题。
2) 加强投诉人、LEA 和 CERT 之间的协作和信息共享。建立一个或多个包含以下内容的数据库：联系人信息（使用的语言）、有关司法管辖权要求、惯例的信息，以及其他有助于一般性暂停活动的信息。

从服务中删除快速通量托管使用的域名

在一些实施取缔措施的情况中，反犯罪投诉人员首先会确定快速通量攻击所利用的域名，然后找到该域名注册时选用的注册服务机构或注册管理机构，阐明问题的性质，并说服注册服务机构取消对该域名提供服务。

从政策上讲，并没有约束注册管理机构和注册服务机构以特定的方式响应与快速通量宿主有关的投诉，而且快速通量宿主技术本身并不是非法活动，除非它确实与非法活动（计算机滥用和欺诈、身份盗用）关联。注册管理机构和注册服务机构可以针对滥用情况设定自己的政策，并且独立地实施响应程序。不过，也存在着一些通用的做法。注册管理机构要求对方提供足够的信息，以清楚地表明域名遭到滥用或导致犯罪行为，并且通常会自行进行调查。如果注册管理机构通过自行调查证实了投诉人员或索赔者提供的数据，注册管理机构则会将该证据提供给所记录的注册服务机构，注册服务机构通常会迅速采取行动来解决报告的问题。注册服务机构自身的政策以及 ICANN RAA（如果适用，指的是所注册域名的 TLD）会影响注册服务机构的响应，他们可能会暂停相关域名的使用（例如，使用“挂起”状态来阻止 DNS 解析其名称）；暂停相关域名的使用并更改注册记录以反映该域名存在争议或注册政策遭到滥用，或者暂停相关域名的使用并将其从区域中删除。注册管理机构通常会对来自执法、传票和法院指令的请求迅速做出响应。许多注册管理机构和注册服务机构设有常规的滥用处理部门，而且通过网络通常也可以访问常见问题解答 (FAQ) 和联系人表单。注册管理机构和注册服务机构可能会提供类似的 FAQ 和表单，这会有助于促进并加快与 LEA 和反犯罪投诉人员的沟通。

对 A 资源记录（解析变动的引荐域名服务器）迅速修改会阻止检测，并妨碍采取措施关闭快速通量宿主站点。

如今，人们采用了形式多样的缓解方法，其中包括：

- 在允许更改域名服务器配置之前，验证联系人的身份。
- 采取各种措施以防止对域名服务器配置自动（执行脚本）更改。
- 设置生存时间 (TTL) 的最小允许值（例如 30 分钟），以便让该时间长度足以阻挡快速通量宿主的双层能量元素。

- 实施或扩展滥用监控系统，以便针对过度更改 DNS 配置的情况进行报告。
- 发布并执行通用服务条款协议，禁止使用支持非法或争议活动（如协议中所列）的已注册域名和托管服务（DNS、网络和邮件）。

另外，建议执行其他检测和缓解方法。具体包括：

- **对域名进行隔离（及蜜罐）处理。**基于一套待定标准，要求注册服务机构对于那些涉嫌被快速通量攻击的域名，暂停更新其域名服务器。在暂停期内，观察并记录所有注册人帐户活动，同时记录企图更新的操作。这种方法可延长事件分析时间，给予调查人员追踪更新来源和识别僵尸程序的机会。

- **限制与某个注册域名相关的域名服务器的更改速率（限制每小时/天/周的更改次数）。**注册管理机构和注册服务机构已经将速率限制技术应用于基于查询的 WHOIS 服务，以达到阻止滥用的目的。确定更改速率可以：(a) 满足 TLD 区域文件中 NS 记录较短的 TTL 的合法应用；(b) 给予调查人员时间，让其有机会追踪更新来源并识别僵尸网络；以及
(c) 削弱短 TTL 对快速通量攻击者的用处。

- **将“较短的 TTL 更新”从常规注册更改流程中分离开来。**将把 TTL 设置为低于某种限制的请求视为特殊请求，需要对其进行某种验证。

- **通过暂停域名为消费者提供指导。**不立即返回已证实被非法使用的域名，而是建立着陆页并重新引导访问者进入该着陆页，在页面上解释该域名由于被非法或争议活动所利用而遭到暂停，并告知用户如何检测网络钓鱼和其他犯罪活动，以及如何避免遭受损害。

调查结果

SSAC 提供下列调查结果，供社群参考：

1) 快速通量宿主采用极为复杂的攻击启动基础设施，不断利用域名解析和注册服务来支持非法和争议活动。

2) 当前，人们通过检测和摧毁僵尸网络来阻止快速通量宿主，然而效果并不明显。

3) 双层通量会进一步阻止检测，并妨碍实施关闭快速通量宿主网站的措施。

4) 域名注册人对域名服务器 (NS) 记录的频繁修改，以及 TLD 区域文件中域名服务器 A 记录中较短的 TTL 设置都是可以监控的特征，监控这些特征可以识别潜在发生的域名服务滥用。

5) 以下措施似乎有效，但未得到普遍采用：防止自动更改 DNS 信息，以及增大 TLD 区域文件中域名服务器 A 记录的 TTL 最小值。

6) 提出了打击快速通量宿主和有利于进一步研究的其他方法。

建议

快速通量宿主是一个日益严峻的问题，它可能会影响所有 TLD 中的域名服务。SSAC 建议 ICANN、注册管理机构和注册服务机构考虑本公告中提及的做法，以建立缓解快速通量宿主的最佳做法，并考虑是否应在今后的协议中处理此类做法。