行动纲要

GNSO Fast Flux Hosting 工作组初步报告

本文档的来由状况

本文档是 Fast Flux Hosting 工作组《初步报告》的“行动纲要”部分。

翻译注释

本文档由相应的英文文档翻译而来，目的是方便更多读者阅读。 虽然互联网名称与数字地址分配机构（ICANN）已尽力确保译本的准确性，但英语是 ICANN 的工作语言，因此，本文档的英文原件是唯一有效力的官方文本。 请注意，本行动纲要只是报告全文中的一章。报告全文只提供英文版本，可从 http://gnso.icann.org/ 网站获取。

目录

1 行动纲要

1.1. 背景信息

- 在 2008 年 1 月发布《SSAC 关于 Fast Flux Hosting 和 DNS 的咨询报告》(SAC 025) 之后，GNSO 委员会于 2008 年 3 月 6 日指示 ICANN 相关人员着手准备《问题报告》，该报告应考虑 SAC 咨询报告 [SAC 025] 并概述 GNSO 政策制定方面可能会采取的后续步骤，旨在削弱犯罪分子当前通过更改“Fast Flux”IP 或名称服务器来攻击 DNS 的能力。
- 该《问题报告》于 2008 年 3 月 31 日发布，报告中建议“在考虑是否启动正式的政策制定流程之前，GNSO 组织应就最佳行业做法的指导原则做进一步的事实调查和研究工作。
- 在 2008 年 5 月 8 日的会议上，GNSO 委员会启动了正式的政策制定流程 (PDP)，并呼吁成立 Fast Flux 工作组。 工作组章程于 2008 年 5 月 29 日通过批准，章程要求工作组要考虑以下问题：
  - 谁是 Fast Flux 的受益者和受害者？
  - 谁将从停止 Fast Flux 活动中受益，谁会因此受到损害？
  - 注册运营商是否涉嫌或者可能涉嫌 Fast Flux Hosting 活动？ 如果是，如何处理？
  - 注册商是否涉嫌 Fast Flux Hosting 活动？ 如果是，如何处理？
  - Fast Flux Hosting 如何影响注册人？
  - Fast Flux Hosting 如何影响互联网用户？
  - 注册管理机构和注册商可以采取哪些技术措施（例如，更改 DNS 更新的操作方式）和政策措施（例如，更改注册管理机构/注册商协议或者更改注册人许可行为的监管规则）来减少 Fast Flux 的负面影响？
  - 对注册人、注册商和/或注册管理机构开放或促进使用 Fast Flux Hosting 技术的行为建立相应的限制、准则或约束，会有哪些正面或负面影响？
  - 这些限制、准则或约束会对产品和服务创新产生什么样的影响？
  - 在防范 Fast Flux 方面有哪些最佳做法可以使用？

  工作组还受命在合适的情况下，就 GNSO 的政策制定应涵盖哪些 Fast Flux 领域和不应涉及哪些 Fast Flux 领域听取专家意见。

1.2. 工作组采取的措施

- Fast Flux 工作组于 2008 年 6 月 26 日开始其审议工作，并决定着手解决章程中提出的问题，同时准备该主题的群体组织意见书。 为了方便各群体组织反馈，工作组制作了一个用于反馈的模板（请参见“附件 I”）。 除了每周举行电话会议之外，工作组还通过 Fast Flux 邮件列表展开广泛的对话，目前发送的邮件已超过 800 封。
- 除了特别注明，本文档中表述的立场均为工作组所认同的立场。 对于工作组内部未达成广泛共识的立场观点，文档中使用下列标签文字来注明相应的支持度：
  - 支持 – 收集到了一些正面支持意见，但可能存在反面意见，并且尚未达成广泛共识。
  - 多种观点 – 成员表达了不同观点，任何观点在工作组内部均未获得足够的认同，无法形成“支持”或“认同”意见。 应该注意的是，在达成广泛共识以及支持意见的情况下，也可以存在不同观点的表达。

1.3. 章程问题讨论

- 从工作组的角度看，Fast Flux 攻击网络具有以下特征：
  - 一些（不一定是所有）网络节点通过被胁持的主机来运行（即，使用安装在主机上的软件进行活动，而没有通知或取得系统操作人员/所有者的同意）；
  - 某种意义上具有“易变性”，即网络的活跃节点会不断变化，目的是延长攻击网络存在的时间，便于网络软件组件扩展活动范围和执行其他攻击；以及
  - 使用各种技术来达到不断变换身份的目的，包括：
    - 从一组宿主主机中快速重复选择系统，这些主机用于提供恶意内容，用作名称服务器，以及用于其他目的，所有这些活动都通过较短存留时间 (TTL) 的 DNS 条目来进行；
    - 在广泛的多个用户自治系统之间分散网络节点；
    - 监控成员节点以确定/确认主机恶意活动是否已被识别并关闭；以及
    - 时间或其他针对网络节点、名称服务器、代理目标或者其他组件的可测量的拓扑变化。

    其他结合或共同用于区分或“鉴定”Fast Flux Hosting 攻击的特征包括：
    - 单个 NS 有多个 IP，跨越多个 ASN；
    - NS 频繁变化；
    - 用户带宽分配块内存在 in-addr、arpa 或 IP 欺骗；
    - 域名存在时间；
    - WHOIS 信息不完整；

  - 确认指定地址的机器上是否正在运行 nginx 代理： nginx 通常用于隐藏/代理非法网络服务器；
  - 用于恶意活动的域名可能是域管理帐户被胁持的注册人名下的多个可能存在的域名之一，攻击者未经授权而修改了域名信息。
- 未通知或取得主机系统操作员/所有者的同意，即利用该系统分发软件和使用安装在其上的软件进行活动，这是 Fast Flux 攻击网络极为重要的特征；特别是，还存在可将 Fast Flux 攻击网络同应用程序利用 Fast Flux 技术进行正常运营活动（如内容分发网络、高可用性和应急恢复网络等等）区分开来的其他一些特征。
- 犯罪分子利用 Fast-flux Hosting 技术的主要目的是延长攻击的有效持续时间。 这种技术本身并不构成攻击 – 它是攻击者用于躲避侦测以及使反攻击措施失效的一种方式。
- 工作组根据初步工作结果，对于章程中的问题提出了以下解决措施，不过工作组强调，这些解决措施方面的相关工作还需要继续开展下去：
  - 有关“Fast Flux”完善的技术和流程定义；
  - 用于检测 Fast Flux 网络的可靠技术，能保持可接受的误检率；
  - 有关 Fast Flux 网络的范围和渗透情况的可靠信息；
  - 有关 Fast Flux 网络在金融和非金融方面影响的可靠信息；
- 章程中提出的问题：

1. 谁是 Fast Flux 的受益者和受害者？

谁从 Fast Flux 受益？

- 高度目标化网络的运营机构
- 内容分发网络
- 自由言论/倡议组织

谁是 Fast Flux 活动的受害者？

- 工作组注意到，无论是合法还是恶意使用 Fast Flux 技术，都有可能造成他方损害。讨论期间，工作组成员发现，对于由该技术自身直接引发的损害，和利用 Fast Flux 技术作为反侦测手段之一的“邪恶操纵者”的恶意行为所引发的损害，在二者之间很难划清界限。
- 对于恶意行为引发的损害，工作组关于可独立识别的 Fast Flux Hosting 应受处罚行为没有达成共识，但成员对于攻击者利用 Fast Flux 技术延长攻击时间的方式表示认同。

2. 谁将从停止 Fast Flux 活动中受益，谁会因此受到损害？

因停止该活动而受益的相关方，也就是 Fast Flux 用于支持 Fast Flux 攻击网络时的受损方。 因此，工作组将工作重点放在确认这些受损者方面。

- 计算机被攻击者感染并在 Fast Flux 攻击网络中用来承载攻击工具的个人用户。
- 计算机受感染并随后在 Fast Flux 攻击网络中用来承载攻击工具的公司和组织。
- 收到网络钓鱼电子邮件并被引诱到 Fast Flux 攻击网络上的网络钓鱼诈骗网站的个人用户，他们的身份信息可能会被盗用，或者由于信用卡、有价证券或银行账户诈骗而遭受财产损失。
- 互联网服务提供商（ISP）的 IP 地址块和域名如果与 Fast Flux 攻击网络有关联，也会遭受损失。 ISP 还可能由于调派人员和资源用于监控和解决 IP 和域名滥用问题而增加成本。
- 如果注册商的注册和 DNS 托管服务被利用来实施采用“Double Flux”技术的 Fast Flux 攻击，其声誉也可能会受到损害。 注册商也可能由于调派人员和资源用于监控和解决 IP 和域名滥用问题而增加成本。
- 遭受驻留在 Fast Flux 攻击网络上的假冒网站网络钓鱼诈骗行为的公司和组织。
- 生活或日常运营受到通过 Fast Flux 攻击网络实施的非法活动影响的个人或公司。
- 注册机构可能由于分出人员和资源用于监控和解决 IP 和域名滥用问题而增加成本。

谁从使用 Fast Flux 技术中受益？

- 高度目标化网络的运营机构
- 内容分发网络
- 为自由言论、少数派倡议和革命思想提供网络渠道的组织
- 犯罪分子、恐怖分子以及通常意义上使用 Fast Flux 攻击网络的任何组织

工作组承认，这项技术的使用未来还会有新的发展变化，因此，无法列出所有可能通过这一技术受益的相关方面。

3. 注册运营商是否涉嫌或者可能涉嫌 Fast Flux Hosting 活动？ 如果是，如何处理？

注册机构群体在其群体组织声明书中对注册运营商就 Fast Flux Hosting 可以采用的技术和政策措施给出了详细说明（请参见“附录 III”）。

4. 注册商是否涉嫌 Fast Flux Hosting 活动？ 如果是，如何处理？

- 大部分注册商未涉及 Fast Flux 或 Double Flux 活动
- 在存在有恶意者注册 Fast Flux 域的注册商中，大部分对于这种恶意阴谋都不知情
- 某些注册商（更多的是注册商服务分销商）有为 Fast Flux 域攻击提供便利的迹象
- 虽然尚没有注册商由于为与 Fast Flux 域相关的犯罪活动提供便利而受到起诉，但是，已有报告将一家 ICANN 认可的注册商与包含 Fast Flux 域的大量诈骗域联系在一起。

此外，问题报告中还描述了许多已知的攻击手段以及应对措施。

5. Fast Flux Hosting 如何影响注册人？

注册人是寻找域名用于实施 Double Flux 攻击的 Fast Flux 攻击者的目标。 由于域的存在时间和历史记录已成为调查人员确定一个域是否与 Fast Flux 攻击有关的考虑因素，在新近注册的域中声誉良好的已有域会吸引攻击者。

6. Fast Flux Hosting 如何影响互联网用户？

互联网用户既提供了 Fast Flux Hosting 运行所需的基本工具（恶意软件控制的带宽 – 联网的用户计算机），同时还是利用 Fast Flux 技术实现的垃圾电子邮件发送网站的目标邮件读者。

7. 注册管理机构和注册商可以采取哪些技术措施（例如更改 DNS 更新的操作方法）和政策措施（例如更改注册管理机构/注册商协议或者更改注册人许可行为的监管规则）来减少 Fast Flux 的负面影响？

工作组希望强调的是，Fast Flux 需要更好地进行界定和深入研究。 此处的观点作为草案，记录了研究中逐渐累积的一些成果。 按照对 ICANN 及其合同方或认可方（gTLD 注册机构和注册商）所期望的参与形式，将解决方案分为两类： 只要求可以获得更多或更准确的信息的方案，这些信息可能会（也可能不会）由参与反诈骗和相关活动的其他方在合适情况下使用（信息收集）；以及要求或至少在某种程度上受益于 ICANN 和/或注册机构/注册商的积极参与的方案，以识别和威慑诈骗行为或其他“恶意”行为（积极参与）。

- 信息收集 – 所讨论的信息共享方面的建议包括以下几个观点：
  - 可以通过基于 DNS 的查询来获取关于注册域的更多非隐私性信息；
  - 由注册商、TLD 和名称服务器发布特别投诉卷宗摘要；
  - 鼓励 ISP 武装自己的网络；
  - 社群合作性举措，旨在方便数据共享和识别可疑域名。
- 积极参与 – 关于积极参与的讨论观点包括：
  - 与经过认证的调查机构/应急服务机构合作，采取快速的域暂停处理机制；
  - 建立特定技术（如非常慢的 TTL 值）的使用准则；
  - 在注册人进行域名注册时确认名称服务器是静态服务器还是动态服务器；
  - 对静态名称服务器 IP 地址变更收取少许费用；
  - 允许互联网社区通过采取解决其他滥用问题的类似方式来抑制 Fast Flux Hosting 行为；
  - 加强注册人验证过程。

8. 对注册人、注册商和/或注册管理机构开放或促进使用 Fast Flux Hosting 技术的行为建立相应的限制、准则或约束，有哪些正面或负面影响？

工作组为解决这一问题的任何行动，都要等待工作组收到下一轮群体组织声明书和公众意见（特别是关于这些要点而请求反馈的意见）并进行讨论研究之后再行开展。

9. 这些限制、准则或约束会对产品和服务创新产生什么样的影响？

工作组为解决这一问题的任何行动，都要等待工作组收到下一轮群体组织声明书和公众意见（特别是关于这些要点而请求反馈的意见）并进行讨论研究之后再行开展。

10. 在防范 Fast Flux 方面有哪些最佳做法可以使用？

针对 Fast Flux 实施保护的最佳做法的一个来源就是网络钓鱼群体。 反网络钓鱼工作组最近发布了一个关于域注册商如何处理网络钓鱼者注册域名的最佳做法文档（《Anti-Phishing Best Practices Recommendations for Registrars》［注册商反网络钓鱼最佳做法建议］http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf）。 该文档列出的几个做法适用于直接或间接处理 Fast Flux 域名的情况。
此外，SAC 035 说明了当前为用户域提供 DNS 服务的某些注册商所采取的应急缓解办法。

11. 合适情况下，就 GNSO 的政策制定应涵盖哪些 Fast Flux 领域和不应涉及哪些 Fast Flux 领域听取专家意见

工作组的一些成员认为，解决 Fast Flux 问题的政策制定工作不属于 ICANN 的事务处理范围，并且给出了原因，但其他成员持不同看法。 工作组的事实调查和界定工作记录了 Fast Flux 如何涉及到域名使用问题（而不是域名注册问题）。

1.4. 挑战

尽管工作组以极大的热情和专注来开展工作，但也遇到了第六章所提到的许多难题，如对于 Fast Flux 的定义缺乏一致意见以及缺乏支持数据，关于 PDP 的范围和 ICANN 的事务处理范围存在误解，等等。

1.5. 暂时性结论

- 就 Fast Flux 或适应性网络技术实施的背后动机，要获得一致的认识和广泛的了解，对于工作组是一个特别棘手的问题。 尝试将 Fast Flux 行为与犯罪意图而不是犯罪本身联系在一起，以及认定 Fast Flux 行为合法还是非法，是好的行为还是坏的行为，这些都引发了大量的争论。
- 工作组成员的研究表明，准确来说，Fast Flux Hosting 必备的特征是“Fast Flux”，但从更普遍的意义来讲，Fast Flux Hosting 技术包括事件敏感性、响应性或易变性网络技术的几个变体和修改版本。
- 工作组承认，Fast Flux 和类似技术仅是更大的互联网诈骗和滥用问题的一个方面。 本报告中所提到的技术也只是攻击者数量庞大且不断演化的工具套件的一部分： 抑制任何一项技术的作用都不会根除互联网诈骗和滥用问题。
- 在可能进行的政策制定和/或后续措施中，必须全面考虑所有这些高度相关的各种问题。对于 ICANN 在这一过程中可以和应该承担的角色，需要认真加以考虑。

1.6. 可能的后续步骤

说明： 在征求公众意见期间，工作组愿意提出以下观点供讨论和反馈。 请注意，在这一阶段，工作组对于下述任何观点均未达成一致意见。 工作组的目标是，研究在公众意见征求期间所收集的建议和反馈信息，并确定工作组支持将哪些建议（如果有）纳入最终报告。

- 编写新一章内容，或者在编写之前开展深入的研究和事实调查，以重新界定问题和范围。
- 研究在 Fast Flux 政策制定过程中吸纳其他利益相关方参与的可能性。
- 研究解决问题（而非政策制定流程）的其他方法。
- 强调说明哪些解决方案/建议可在政策制定、最佳做法和/或行业解决方案中得以体现。

- 考虑注册滥用方面的政策条款是否可以通过授权注册机构/注册商取消涉及 Fast Flux 行为的域名来解决 Fast Flux 问题。
- 研究开发 Fast Flux 数据报告系统 (FFDRS) 的可能性。