Stuxnet 0.5：命令和控制能力

非官方中文译本•安天实验室 译注

文档信息			
原文名称	Stuxnet 0.5: Command-and-Control Capabilities		
原文作者	赛门铁克	**原文发布日期**	2013 年 2 月 26 日
作者简介	赛门铁克是一家总部位于美国加州山景城的计算机安全、备份和可用性解决方案的软件公司，是一家全球 500 强公司和 S&P 500 股票指数的成员。http://en.wikipedia.org/wiki/Symantec		
原文发布单位	赛门铁克		
原文出处	http://www.symantec.com/connect/blogs/stuxnet-05-command-and-control-capabilities		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技		

	术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

Stuxnet 0.5：命令和控制能力

发布：2013 年 2 月 26 日 17 点 40 分 格林威治时间
更新：2014 年 1 月 23 日 18 点 09 分 21 秒格林威治时间

与 Stuxnet 1.x 版相似，Stuxnet 0.5 有有限的命令和控制（C&C）能力。特别的是，Stuxnet 0.5 不向它的作者提供细粒度的控制。相反的，Stuxnet 0.5 只能下载新代码和自我更新。Stuxnet 需要在孤立的网络中传播，因此它被设计为自治，减少了对强健的、细粒度的 C&C 能力的需求。Stuxnet 0.5 还采用二次点对点机制，以便将代码更新传播到从广域互联网无法访问到的网络节点上。

Stuxnet 0.5 有四个 C&C 服务器。目前，所有这些服务器要么是已经不可用，要么是已被不相关人士注册。

有趣的是，Stuxnet 0.5 被设定为在 2009 年 1 月 11 日后停止联络 C&C 服务器，而该威胁被设定为在 2009 年 7 月 4 日的数月后停止传播。

该 C&C 服务器的域名创建于 2005 年。所有服务器都显示同样的首页。首页标注为一个叫做 Media Suffix 的互联网广告公司，采用“相信心灵中的梦想。”作为广告标语。

***图 1.** Stuxnet C&C 服务器首页*

该服务器被托管给位于美国、加拿大、法国和泰国的商业主机提供商。

Stuxnet 0.5 最终的目标网络十有八九是孤立于互联网的网络。为了使更新到达这些计算机，Stuxnet 0.5 利用一个点对点机制。如果威胁的一个更新版本被引入网络（例如，通过 U 盘），网络上所有其它被攻陷的计算机可以接收更新或新的代码模块。

Stuxnet 0.5 利用 Windows 的 mailslots 来进行点对点通信。Mailslots 允许一个进程传递消息给另一个远程计算机上的进程。该威胁枚举网络上的所有计算机，并试图利用下面的名字连接到一个 mailslot：

```
\\\mailslot\svchost
```

该威胁则提供如下的回调的 mailslot 名字：

```
\\\mailslot\imnotify
```

Stuxnet 0.5 使用这些 mailslots 来提供点对点的通信，并且将更新分发到威胁的其他版本上。此外，Stuxnet 0.5 可能将系统配置为允许登陆并开启四个文件共享（temp$, msagent$, SYSADMIN$, and WebFiles$），通过 peer infections 来共享一组文件以供检索。

Stuxnet 1.x 版本还包含一个点对点的更新机制，但是是利用一个远程过程调用实现的。

有关 Stuxnet 0.5 各种组件的更多信息，请参见如下的博客，视频和技术白皮书：

- Stuxnet 0.5：缺失的环节
- Stuxnet 0.5：扰乱 Natanz 的铀处理
- Stuxnet 0.5：命令和控制功能
- Video：Stuxnet 时间表和攻击策略

有关 Stuxnet 0.5 的详情，请下载 Symantec 的白皮书。