Stuxnet 0.5：如何演变

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: How It Evolved		
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-how-it-evolved		
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：如何演变

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 19 秒格林威治时间

介绍

在 Stuxnet 的代码中存储有它的版本号。对该段代码的分析揭示了对 Stuxnet 0.5 的最新发现。依据网站域名注册的详细信息，Stuxnet 0.5 可能早在 2005 年就已经处于运转中了。该版本在世界范围内开始传播的确切日期还尚不清楚。我们所知道的是，这个早期变种入侵计算机的日期是是在 2009 年 7 月 4 日，这仅仅是在 V1.x 被创建的 12 天后。

时间	版本	描述
2005 年 11 月 3 日	0.500	C&C 服务器注册
2007 年 11 月 15 日	0.500	提交数据至一个公共扫描服务器
2009 年 7 月 4 日	0.500	感染终止日期
2010 年 3 月 1 日	1.001	主要的二进制文件编译时间戳
2010 年 4 月 14 日	1.100	主要的二进制文件编译时间戳
2012 年 6 月 24 日	1.x	感染终止日期

***表 1.** 已知 Stuxnet 变种，基于主模块 PE 时间戳*

本博文主要讲述 Stuxnet 发展演变的时间轴。Stuxnet 0.5 是如何与攻击事件时间表相契合的，以及他是如何演变到 Stuxnet 1.x 版本的。

演变

Stuxnet 0.5 是迄今为止分析的、最古老的已知 Stuxnet 变种。该变种在 2009 年 7 月 4 日停止了对计算机的攻击，并且于同年的 1 月 11 日停止了与它的命令和控制（C&C）服务器的通信。在大多数代码中发现的编译时间戳看起来不可信，并且通常是在 2001 年左右。

Stuxnet 0.5 与之后的版本的主要区别如下：

1. 后期版本显著增加了他们的传播能力和对漏洞的利用。
2. 用 Tilded 平台代码替换 Flamer 平台代码
3. 后期版本采取了另一种攻击策略，从铀浓缩阀破坏对离心机速度的修改

1. 显著增加了传播能力和对漏洞的利用

通过引入多个漏洞，Stuxnet 显著增加了它的传播能力和攻击性。在 Stuxnet 0.5 中辨识到的、唯一的复制方法是利用对西门子 Step 7 项目文件的感染。不同于 Stuxnet 1.x，Stuxnet 0.5 并不利用任何微软漏洞来从一台计算机移动到另一台计算机。

表 2 和表 3 显示了在漏洞利用和传播机制方面的不同。

漏洞	0.500	1.001	1.100	1.101	描述
CVE-2010-3888			X	X	任务调度程序 EOP
CVE-2010-2743			X	X	加载键盘布局 EOP
CVE-2010-2729		X	X	X	PrintSpooler RCE
CVE-2008-4520		X	X	X	Windows 服务器服务 RPC RCE
CVE-2012-3015	X	X	X	X	Step7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC 缺省密码
CVE-2010-2568			X	X	Shortcut.lnk RCE
MS09-025		X			NtUserRegisterClassExWow /NtUserMessagerCall EOP

表 2. *Stuxnet 漏洞利用的演变*

复制技术	0.500	1.001	1.100	1.101
Step 7 项目文件	X	X	X	X
利用 Step 7 项目文件的 USB	X			
利用自动运行的 USB		X		
利用 CVE-2010-2568 的 USB			X	X
网络共享		X	X	X
Windows 服务器 RPC		X	X	X
Printer Spooler		X	X	X
WinCC 服务器		X	X	X
利用 mailslots 进行 P to P 更新	X			
利用 RPC 进行 P to P 更新		X	X	X

表 3. *Stuxnet 复制机制的演变*

2. 从 Flamer 迁移到 Tilded

迄今为止，Stuxnet 被认为是由一个能够访问 Flamer 组件的人开发的项目，并且不需要全部的 Flamer 平台源代码。Stuxnet 0.5 中的发现显示 Stuxnet 的开发者已经可以使用 Flamer 平台的全部源代码。

Stuxnet 0.5 是部分基于 Flamer 平台的， 然而 Stuxnet 1.x 是主要基于 Tilded 平台的。随着时间的推移，开发者似乎将更多的代码向 Tilded 平台迁移。在新近的版本中，开发者实际上使用 Tilded 平台重新实现了 Flamer 平台的组件。

Flamer 和 Tilded 平台代码库的不同足以表明涉及的开发人员是不同。

3. 采取另一种攻击策略

Stuxnet 1.x 版包含针对西门子 315 PLCs 的代码。315 PLCs 控制旋转离心机的速度。Stuxnet 1.x 版还包含一个不完整的，针对西门子 417PLCs 的代码序列，我们并不清楚其所能造成的后果。

我们已经发现一个 0.5 版下的、完整的工作版本，该版本可以对西门子 417 PLCs 进行攻击。它的目的是在铀浓缩过程中修改阀门操作。

Stuxnet 0.5 只包含 417 的攻击代码，不包含 315 的攻击代码。

有关 417 的攻击代码的详细信息请参见博文 Stuxnet 0.5：扰乱 Natanz 的铀处理。

总结

Stuxnet 0.5 的发现进一步明确了 Stuxnet 的演变。联系当下的背景，我们已经将 Stuxnet 发展的关键日期与 Natanz 的低浓缩铀的生产水平相映射起来。有趣的事情是供料或产出产品数量的跳水，以及在同样数量或更大数量的供料情况下更低水平的产出产品数量。（两条线之间的差距）。

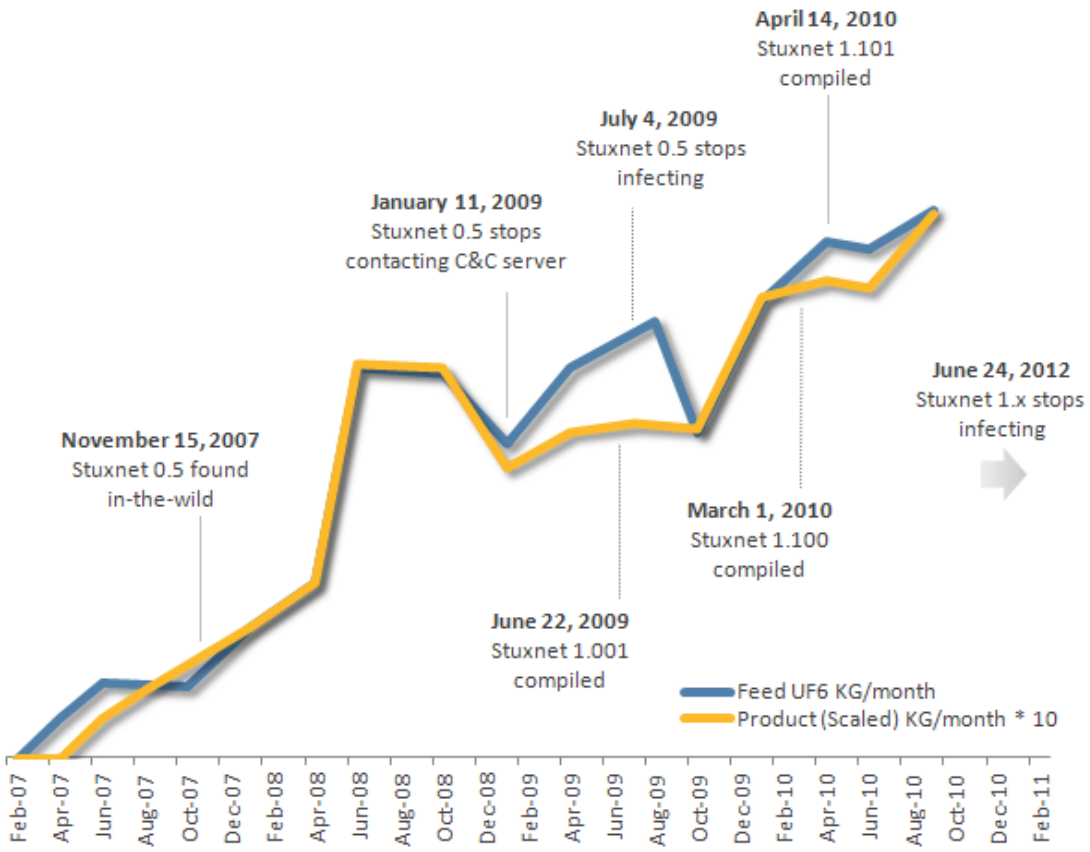

***图 1.** LEU 生产过程（来源：ISIS）*

在 Stuxnet 0.5 以前，尤其是 Stuxnet 0.5 和 Stuxnet 1.001 之前可能存在没发现的 Stuxnet 版本。在 2010 年发现的 Stuxnet 的部分组件依旧与已知的 Stuxnet 版本不匹配。

表 4 为已知版本间的主要差异列表。

版本	0.500	1.001	1.100	1.101
资源	5	10	13	13
漏洞	1	5	7	7
零日漏洞	1	4	6	6
目标 PLC	417	315	315	315
MITM DLL	2	1	1	1

***表 4.** Stuxnet 版本间的比较*

有关 Stuxnet 0.5 关键方面的更多的信息，请参见如下的博客，视频，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：