Stuxnet 0.5：破坏纳坦兹铀浓缩过程

非官方中文译本•安天技术公益翻译组 译注

文档信息			
原文名称	Stuxnet 0.5: Disrupting Uranium Processing at Natanz		
原文作者	Symantec Security Response	发布日期	2013 年 2 月 26 日
作者简介	Symantec 是一家总部设于美国加利福尼亚州库比蒂诺的互联网安全技术厂商，在全球有 40 个国家设有分公司。 http://en.wikipedia.org/wiki/Symantec		
原文发布单位	Symantec		
原文出处	http://www.symantec.com/connect/blogs/stuxnet-05-disrupting-uranium-processing-natanz		
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。		

当我们首次揭示关于 Stuxnet 病毒攻击伊朗用于铀处理的可编程逻辑控制器(PLC)时，我们记录了两次攻击所用的策略。同时，我们还注意到针对 417 PLC 设备的策略已被禁用。目前，我们得到 Stuxnet 病毒的早期版本，该版本包括运行 417 PLC 设备的全部攻击代码。

经过仔细分析，我们确定 417 PLC 设备的攻击代码可以修改浓缩铀离心机提供六氟化铀气体的阀门的状态。这样可以关闭输铀阀门导致铀流量受阻并破坏离心机及其相关系统。此外，该病毒会用快照记录系统正常运行的状态，然后在攻击过程中回放这些正常的操作参数，这样就可以避免机器操作者察觉系统存在的异常。它还会阻止机器操作者修改阀门状态，以免攻击过程中出现离心机设置被修改的情况。

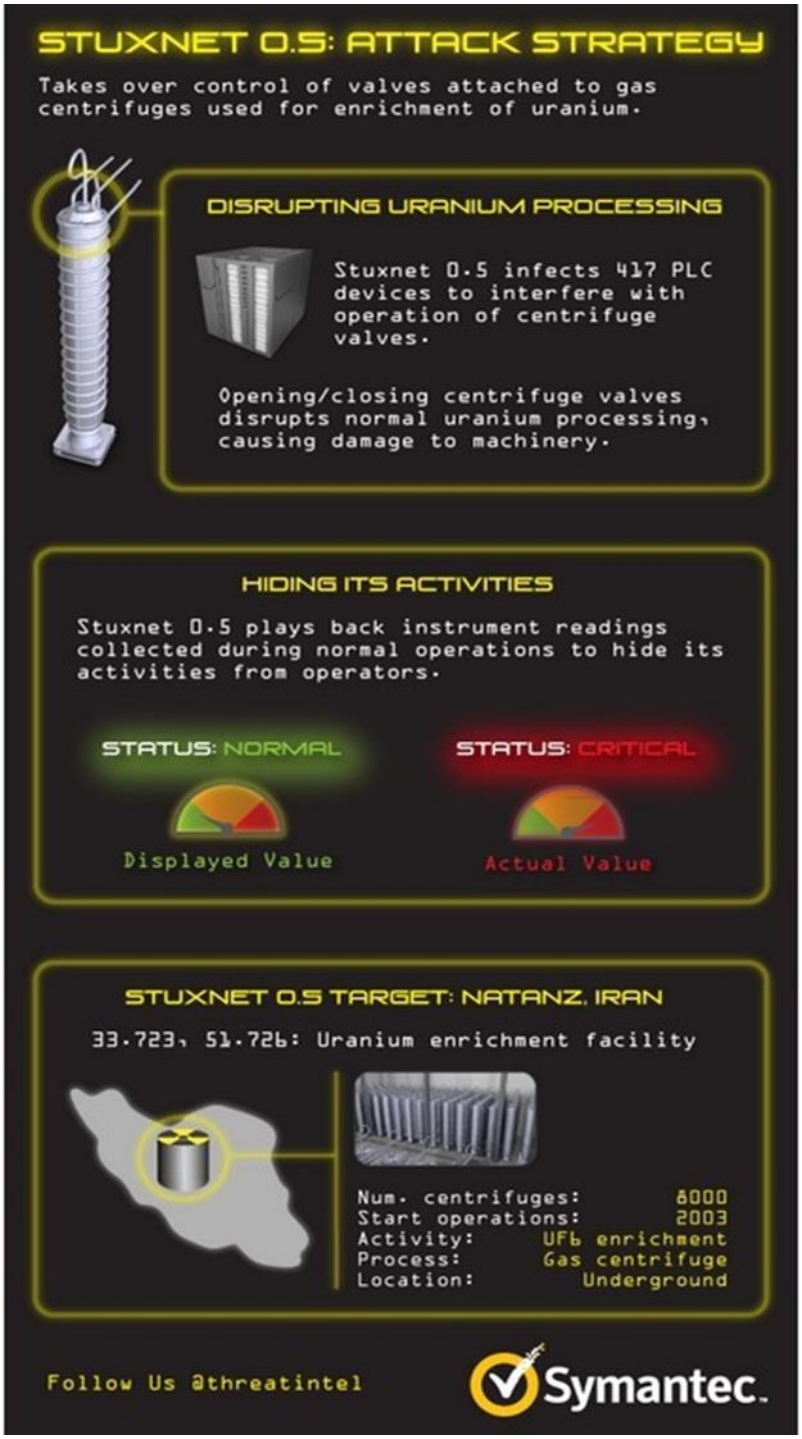

图 1 Stuxnet0.5 攻击策略概要

Stuxnet0.5 是 Stuxnet 病毒的早期版本，它所使用的攻击策略——“417PLC”也被后来 Stuxnet1.x 版本所用的“改变离心机速度”所取代。

Stuxnet1.x 存在代码缺失的情况，而这些缺失的代码恰好出现在 Stuxnet0.5 里。这些代码可以在 417PLC 策略部署前，对目标系统进行必要的指纹识别，并创建一个重要的 PLC 数据块（DB8061）。接下来，我们将全面解析 417PLC 攻击策略。

指纹识别目标系统

Stuxnet0.5 在激活有效载荷之前，通过指纹识别判断目标系统是否处在正确的位置。为确保判断准确，该病毒首先检测受感染系统是否运行 Step7 软件，并解析目标系统中符号表。这些符号表包含目标系统中每一个物理设备的识别标签，例如，每一个阀门、油泵和传感器都有唯一的识别符。这些符号表大致遵循 ANSI/ISA-5.1 仪表符号及识别标准，该标准应用于管道仪表流程图（P&ID）。

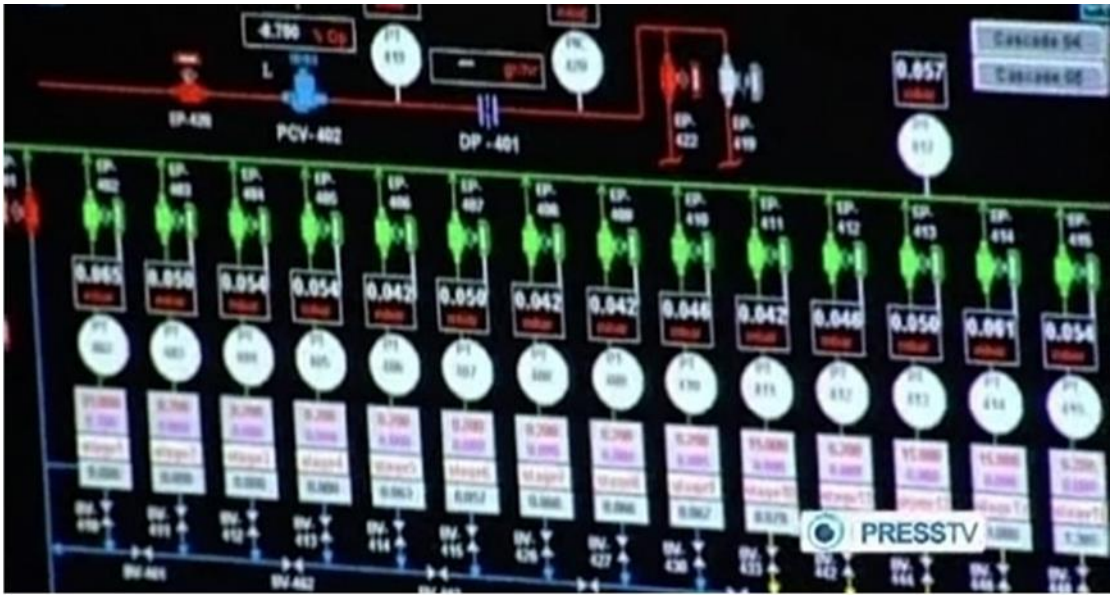

图 2 伊朗铀浓缩设施 P&ID

下表总结了 Stuxnet 病毒在上述符号表中所要查询的设备名称及其识别标签。

设备类型	P&ID 功能识别符	控制设备范围
辅助阀门	{HS,HV,PV,EP},{ZLO,ZO},{ZLC,ZC}	2-25
离心机阀门	{NVS,RVS,VS},{MV,RV,SV,YV}	163-164
阶段压力传感器	PT,PCV,PIA#,PIT,PIC,PI,PS	3-30
离心机压力传感器	PT,PCV,PIA#,PIT,PIC,PI,PS	0-164
流速传感器	{FIA},{FIT},{FITC},{FIC,FT,MFC,MFM}	0-30

表 1 Stuxnet 攻击的设备类型及其识别标签

这些设备的识别标签遵循下列特殊格式：

<Function Identifier><Cascade Module>Cascade Number<Device Number>

例如，一阀门为“module A21, in cascade eight, associated with centrifuge 160, the label would be PV-A21-8-160”。

用于解析这些字符串的逻辑为我们提供了额外有趣的线索。例如，级联模块必须在 A21 到 A28 之间，这样才能与位于伊朗纳坦兹的级联模块的配置信息匹配。Stuxnet 病毒的每一个模块最多有 18 套级联，每套级联有 165 个离心机（分为 15 个等级），这些与纳坦兹公布的配置信息相匹配。

如下所示，这些离心机被分布在铀浓缩过程的不同阶段。

阶段	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
离心机数量	2	2	4	6	8	10	12	16	20	24	20	16	12	8	4

表 2 离心机和阶段配置信息

每一阶段内，离心机会被进一步划分为 4 个一组的子集。

在指纹识别过程中，Stuxnet 为每一个设备配置一个与其配置信息相符的计时器。一旦这个计时器的数值超过某个特定的阀值，Stuxnet 病毒则认为该系统正在通过指纹识别与目标系统进行匹配，并向系统中注入 PLC 攻击代码。Stuxnet 病毒还能判断出 18 个级联中 6 最具攻击价值的目标，并将这些信息连同设备地址及其配置信息一起存储在数据块 DB8061 里。

攻击过程

与 Stuxnet1.x 相似，417PLC 设备攻击代码包含一个可能具有 8 种状态的状态机。各个状态通过关闭位于 18 套级联中的 6 个级联内的阀门来达到攻击目的。

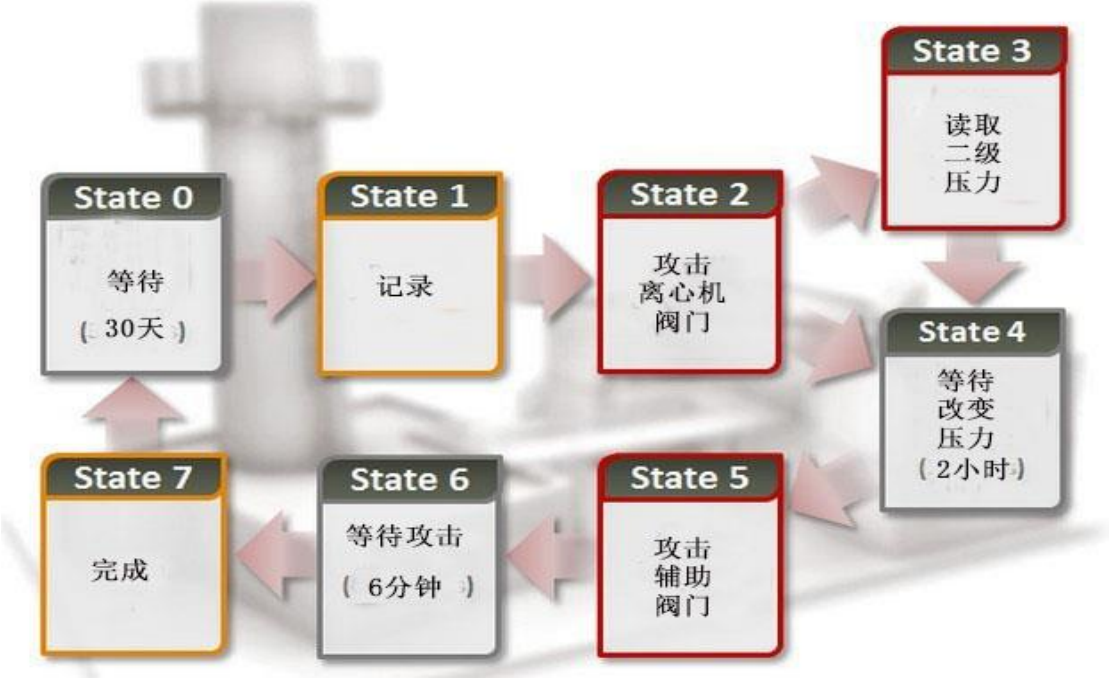

表 3 417PLC 攻击代码状态流程图

- 状态 0-等待：完成系统识别，等待铀浓缩过程达到稳定状态，之后进行攻击（大约 30 天）。
- 状态 1-记录：进行快照和创建虚假输入信息数据块，以备后续使用。
- 状态 2-攻击离心机阀门：开始回放虚假输入信息，关闭大部分离心机上的阀门（最初阶段离心机的阀门除外）。
- 装态 3-读取二级压力：打开处于最后阶段级联的阀门，获取较低压力读数。
- 状态 4-等待改变压力：等待所需的压力变化或时间限制。这一阶段大概需要 2 小时。
- 状态 5-攻击辅助阀门：打开除了接近阶段 1（或阶段 10）的所有阀门，此过程需要持续 3 分钟。
- 状态 6-等待实施攻击：等待 6 分钟，同时阻止任何状态的变化。
- 状态 7-攻击完成：重启回至状态 0。

通过关闭除了位于初始阶段的阀门，UF6（六氟化铀）可继续在系统内流动。仅是这一行为就可引起离心机的严重破坏，然而，攻击的目的是使这一压力达到正常压力的 5 倍。在此压力下，铀浓缩系统可能会被严重损坏，UF6 甚至可能凝华为固体。

这种攻击方法是否取得成功，我们无从考证。即使这种方式是成功的，攻击者还是转换了攻击策略——将“改变离心机速率”的技术应用于 Stuxnet1.x。

对于科学与国际安全研究所（ISIS）在分析铀浓缩离心机系统所提供的帮助，我们表示非常感谢。

我们会将接下来的博客、视频及技术白皮书里分享更多关于 Stuxnet 0.5 组件的细节信息，如：

- Stuxnet 0.5: 缺少的环节
- Stuxnet 0.5: 演变过程
- Stuxnet 0.5: C&C 能力
- 视频: Stuxnet 时间线和攻击策略

想了解更多关于 Stuxnet 0.5 的细节，请下载我们的技术白皮书。