网络安全信息简报

安博士月刊

2014.04 (Vol.18)

AhnLab MDS,
基于内存分析的漏洞检测技术

AhnLab MDS，装载了基于内存分析的漏洞检测技术

阻断‘迂回行为分析手法’的恶意软件

为检测未知恶意软件(unknown malware)，很多APT响应解决方案提供商强调 signature-less 技术。这些提供商使用的技术是虚拟机(Virtual Machine)或者沙箱(Sandbox)。但是，只依赖基于沙箱的行为分析技术来检测未知恶意软件，预测已不再有效。 最近，攻击者为了迂回自动化的行为分析系统，致力于制作迂回自动化的行为分析系统的 恶意软件。这使得恶意软件变得有史以来最为强大。

通过本文，首先了解一下基于沙箱的行为分析技术的局限性，然后介绍可以代替该技术的AhnLab MDS产品的新的功能。

进化的恶意软件，连沙箱自动分析技术也可以迂回

2012年11月，AhnLab安全响应中心(ASEC, AhnLab Security E-response Center)检测到了有趣的恶意软件样品。该样本通过电子邮件附件传播，电子邮件标题为“对韩国空军的威望评价和诊断”。附件文件详细记述了韩国空军的未来和社会对航空宇宙军的认识等，致使收件人认为是国防重要文件。可以看出，这是一个攻击者针对特定对象智能接近的APT攻击。

在技术方面，该文件在制作得非常巧妙。为了迂回‘堆喷射(Heap Spray)’检测，只发生少量的堆喷射，致使很难判断文件的恶意与否。而且，只在该软件的最新版本下运行恶意软件。

但是，该文件分明执行了恶意行为。那么，该文件的秘密在哪里？

该文件如要执行恶意行为，要具备一些条件。收到该文件的用户因好奇而打开文件。用户使用滚动条读到第二页的‘问题的提出’段落的瞬间，便自动生成名称为‘HncCtrl.exe’的恶意文件并运行。该恶意文件一旦运行，又生成其他恶意文件并运行。而该文件运行后便收集计算机里的个人信息，然后传送到指定的电子邮件地址。最终导致个人信息外泄的结果。总结来看，攻击者设计的恶意文件必须有特定用户的行为才可以发生漏洞(exploit)。这是利用文件攻击的最新APT攻击类型之一，即迂回‘自动化的沙箱分析系统’的典型恶意软件。

基于沙箱的行为分析（Behavior Analysis in Sandbox）技术的局限

目前，很多APT响应解决方案提供商强调为检测未知恶意软件，不依赖于恶意软件特征码的‘signature-less’技术的必要性。特别是，一些提供商主张‘基于行为分析’技术是检测未知恶意软件的唯一‘signature-less’技术。那么，仅仅利用‘基于沙箱的行为分析’技术检测越来越高级化的恶意软件，果真足够？

对该问题的回答是‘不足够’。我们来看一下利用‘基于沙箱的行为分析’技术的APT响应解决方案来检测最新恶意软件的局限性。

沙箱是一种按照安全策略限制程序行为的执行环境。‘基于沙箱的行为分析’技术是将文件或程序在沙箱环境中运行，根据运行所产生的变化来判断恶意与否。

因此，如要利用APT响应解决方案的该技术来检测恶意软件，恶意软件必须要有行为。即，恶意软件必须在沙箱环境中执行它原来所意图的行为，才可以检测到该行为。但是，如前面所提到的，最近的攻击方式有很多利用不发生行为的文件，它们开始了迂回‘自动化的沙箱分析系统’。

迂回基于沙箱的行为分析系统的最近代表性的恶意软件的三种类型如下：

1. 感应‘计算机用户的特定行为(Interaction)’发生恶意行为的恶意软件

比如，用户仅打开恶意PDF文件不会发生恶意行为。但是，利用滚动条移动到特定页时发生恶意行为。

还有一种是，计算机被恶意软件感染的状态下，恶意软件将感应用户执行的‘点击鼠标’或者‘鼠标移动到特定方向’等输入装置的变化，便执行恶意行为。有趣的是，首先弹出被恶意软件感染的警告信息，用户点击弹窗的‘确定’键时才发生恶意行为。

此类恶意软件在用户执行特定行为之前是无可疑行为的恶意软件。因此，利用‘基于沙箱的行为分析’技术的APT响应解决方案无法检测到该恶意软件。

2. 利用自动化的沙箱分析系统无法控制的‘时间限制’的恶意软件

大部分的APT响应解决方案为了自动化的行为分析而使用虚拟机(Virtual Machine)或沙箱(Sandbox)。但是，为了驱动虚拟机或沙箱需要使用硬件有限资源，因此直到样本的行为结束为止无法无限制使用‘一个样本需要的动态分析时间’。恶意软件制作者则瞄准该漏洞，利用在特定时间发生恶意行为的调度(scheduling)法。利用该手法的恶意软件本称为‘定时炸弹恶意软件(Time-bomb Malware)’或者‘特洛伊木马小睡(Trojan Nap)’。

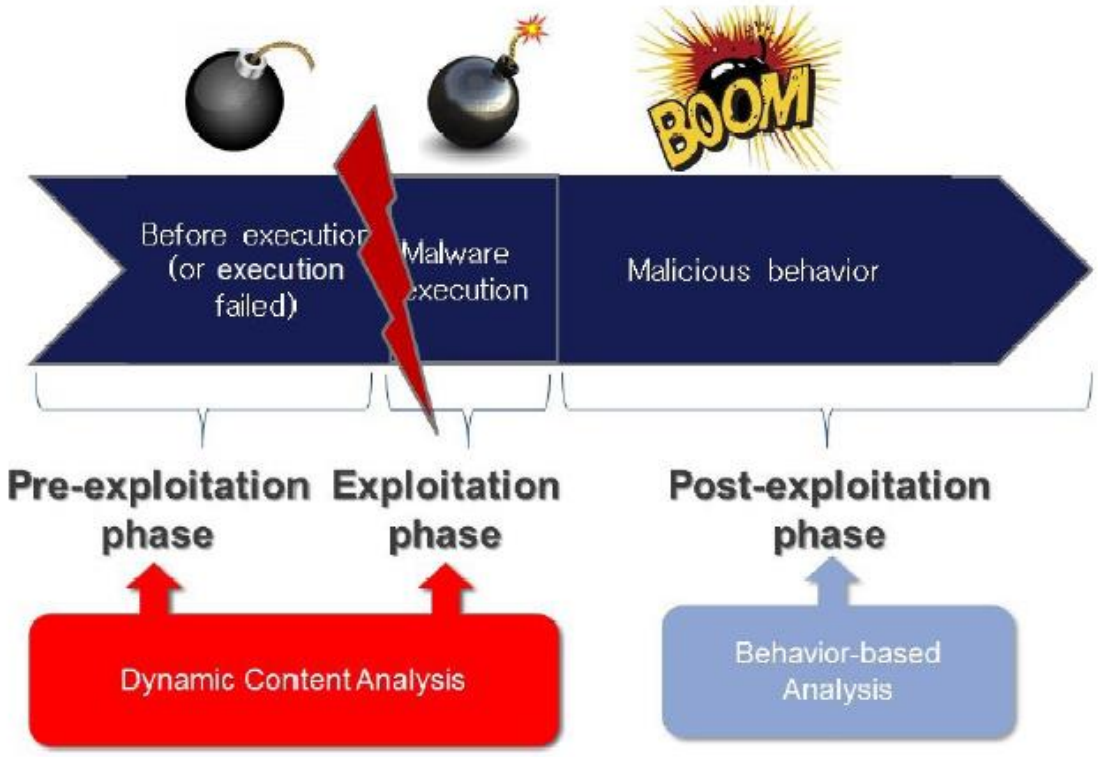
一些APT响应解决方案，如果使用利用在定时炸弹手法的如‘Sleep API’的特定API，毫无疑问地判断为恶意软件。但是，该API也可用在正常的程序，因此如上述的判断会导致增加误诊的问题。

3. 认知虚拟机或沙箱而隐蔽恶意行为的智能型恶意软件

攻击者制作此类恶意软件，不仅是为了迂回APT响应解决方案检测和分析，因为恶意软件分析家在动态分析时也使用虚拟机或沙箱。一些APT响应解决方案检测欲想掌握运行中的进程、注册表密钥或注册表值、虚拟硬件等虚拟机或沙箱中的变化的企图。相反，当有此类的检测时，恶意软件则进化为‘感知此类的检测后不发生恶意行为’的方式。

AhnLab MDS，装载了基于内存分析的漏洞检测技术

AhnLab MDS针对此类迂回行为分析的恶意软件，应用了新的分析技术，即动态内容分析(Dynamic Intelligent Content Analysis)技术。该技术是在内存领域执行基于汇编代码(Assembly Code)的分析的技术，由AhnLab开发的独自技术。利用该技术，可以在应用程序漏洞攻击阶段(Exploitation Phase)检测到恶意软件与否，还可以检测到利用新的零日(Zero-Day)漏洞的恶意软件。



[图 1] 动态内容分析技术的概念

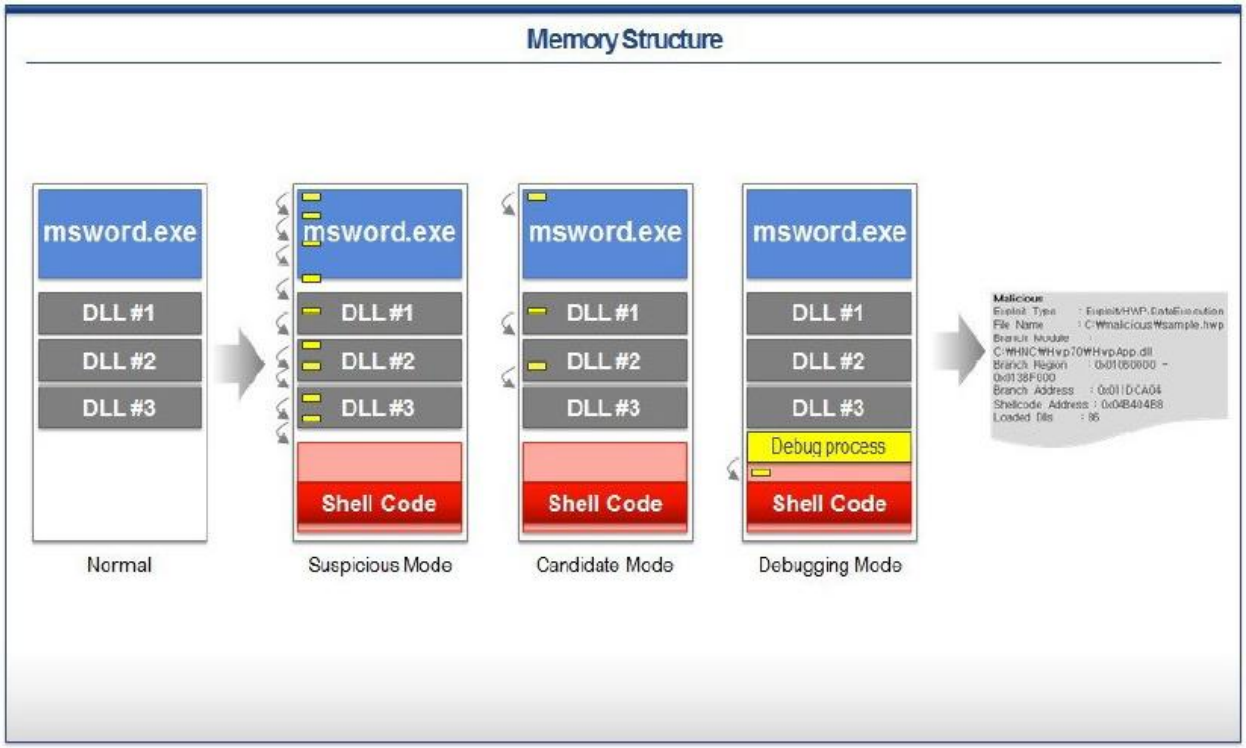
AhnLab MDS的动态内容分析技术的概念如图1所示。

假设一下，如果攻击特定应用程序漏洞的恶意软件正常利用漏洞发生恶意行为，则该恶意软件最终发生恶意行为的过程可以分为‘运行恶意软件的前阶段(Pre-exploitation Phase)’和‘运行恶意软件阶段(Exploitation Phase)’。如果，该恶意软件在运行前阶段没有正常运行或在运行阶段感知到虚拟机或沙箱环境而不发生恶意行为，则‘基于行为的分析’技术便成为无用之物。

因此，需要不管恶意行为的发生与否，在恶意软件运行前阶段或运行阶段可以检测的的方法。

克服‘基于行为的分析’技术的局限性，并在攻击漏洞前阶段就可以检测到恶意软件而开发的技术即是AhnLab MDS的动态内容分析(Dynamic Intelligent Content Analysis)技术。

AhnLab MDS的动态内容分析技术的动作原理



[图 2] 动态内容分析(Dynamic Intelligent content Analysis)动作原理

假设一下，微软公司Word文件存在缓冲区溢位(buffer overflow)攻击漏洞。

运行正常的MS word文档的时，结果是图2的左侧第一个图形所示。当点击正常的word文档，内存将装载主程序msword.exe文件和有关动态程序库文件。如果是正常程序，处理到DLL#3，然后正常打开word文档。

下面看一下，攻击word文档漏洞的时候。起初，如正常情况一样运行程序。但是在某一瞬间，将shell代码保存到保存数据的heap领域。然后，发生缓冲区溢位漏洞。如果是正常的情况，只移动到DLL#3的EIP，但是EIP非正常地跳跃到shell代码领域。之后，便发生被shell代码编码的恶意行为的结果。

如果导入装载动态分析技术的AhnLab MDS，如下检测上述的恶意软件。

在分析对象程序在内存加载的瞬间即插入‘调试线程(Debugging Thread)’，检测非正常移动或跳跃到内存领域的恶意软件。动态内容分析不仅可以检测‘缓冲区溢位’，还可以检测SEH(Structured Exception Handing), RTL(Return-to-Lib), ROP(Return-Oriented Programing), 堆喷射(Heap spray)等恶意软件利用的攻击漏洞的阶段。即，AhnLab MDS的动态内容分析不管‘恶意行为的类型和发生与否’都可以检测到恶意软件。

事前阻断APT是关键

AhnLab MDS动态分析技术是AhnLab研究阵容研发的基于数十个算法完成的独自的技术。具有Non-PE型恶意文件在发生漏洞攻击前阶段通过堆喷射((Heap Spray)保存shell代码的方法、通过栈溢出(Stack Overflow)保存shell代码的方法、包括恶意脚本在内存领域保存shell代码的方法等。

尤其是，AhnLab MDS检测攻击应用程序漏洞的恶意文件的shell代码在内存开始的地点，可视性地显示将shell代码的内存转储和汇编代码。通过内存分析感知shell代码后正确提供shell代码的开始地址，只有AhnLab MDS才可以做到的与众不同的最为出色的技术。

上面所阐述的AhnLab MDS的动态内容分析技术，它本身对于恶意软件分析家或安全专家并不是一个重大的新的概念。但是，该技术转载到自动化的分析系统并分析大量的文件这一点来看，可以称得上是‘恶意软件分析和事前阻断利用高级恶意软件的APT攻击’的领先者。

我们坚信：AhnLab MDS以装载此技术，不管环境和运行条件等潜在的因素检测到恶意软件，在事前阻断APT攻击方面更加发挥出强大的力量。

http://www.ahn.com.cn
http://global.ahnlab.com
http://www.ahnlab.com

关于安博士（AhnLab,Inc.）

安博士的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

安博士已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区酒仙桥甲12号电子城科技大厦1206室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0935 / +86 21 6095 6780 | v3site@ahn.com.cn