安博士月刊

星 期 三
10月 30日
2 0 1 3年
Vol.13

【安博士月刊】是综合安全解决方案公司-安博士公司发行的网络安全信息月刊。

AhnLab MDS，下一代主动型安全技术

市场研究公司 Gartner 推出预测报告，如要应对 APT，不仅具备基本的安全响应体系，还要具备高级的防御技术。Gartner 还预测，未来将需要“取证分析(Forensic)”和“沙箱(Sandboxing)”等安全响应技术。为了响应越来越高级化的安全威胁，AhnLab 已在 APT 解决方案“AhnLab MDS”就体现了沙箱技术。AhnLab MDS 不仅具备了 Gartner 强调的下一代安全技术“沙箱技术”基础的卓越的分析能力，还具备了自己研发的动态内容分析技术“DICA（Dynamic Intelligence Content Analysis）”。同时，AhnLab MDS 还装载了最根本的响应方案且可以实际应对（修复和响应)的 Agent 技术。

AhnLab MDS 结合了包括沙箱技术的下一代主动型安全技术后变得更强大，本刊将详细介绍 AhnLab MDS 的 APT 响应技术 。

沙箱技术概要

在介绍沙箱技术之前，首先来了解以下恶意软件分析方法。

恶意软件分析方法可以分为静态分析和动态分析。动态分析通过运行分析对象样本后分析其行为，当发现可疑行为和明确的恶意行为，即诊断为恶意软件。这种动态分析过程存在着危险，这里危险是指黑客通过某种恶意行为对分析系统和周边网络引起致命的打击，如发生系统破坏、攻击相同网络的其他系统和网络超载等。

与此相反，静态分析为了最小化这种危险，通过AV扫描诊断已知恶意软件(known malware)或者利用分析文件头及二进制字符串等方式。更专业点，通过调试器分析 API 调用关系等方法诊断恶意软件与否。

沙箱技术是在沙箱环境下进行基于动态分析的恶意软件分析的技术。沙箱环境是指如虚拟机(Virtual Machine)的虚拟的受限制的操作系统环境，重要的一点是，由动态分析结果发生的损害不会传播到分析系统外部。沙箱技术根据技术供应商不同，用“VM(Virtual machine)”、“VM emulator”、“Hypervisor”和“沙箱”等表现。

那么，为什么选择沙箱技术？

在回答此问题之前，让我们来先了解一下为什么需要基于动态分析的恶意软件分析。

随着网络攻击越来越复杂且恶意软件变得越来越强大，仅依赖于传统防病毒软件的启发式(heuristic)功能检测未知恶意软件，或者提取PE头或样品字符串诊断恶意与否已越来越无效。尤其是，恶意软件制作者利用多样的常用加壳(packer)或者定制加壳(customized packer)妨碍静态分析。

如此，仅利用静态分析是很难诊断实际恶意软件，再加上分析对象样品的数量也显示急增的趋势。因此，比起投入专家并通过复杂过程的静态分析，简单运行分析对象样品即可诊断的动态分析方法更受到偏好。

动态分析可以在实际计算机执行，但是效率低。因此除了取证分析之类的特别的情况，大部分都是在如虚拟机的沙箱环境下执行。举个例来讲，恶意软件分析专家对于多样的分析环境(操作系统等)各拥有物理计算机，每次分析结束都要重新安装操作系统，这就需要2~3小时的作业时间。结果来讲，在实际计算机分析是效率低且没有现实性。

为什么需要自己专用的沙箱解决方案？

那么，顾客可以选择的沙箱技术有哪些？

第一，在线收费/免费沙箱服务。如果企业想使用沙箱技术，则可以利用在线服务并上传分析对象文件即可执行动态分析。但是，免费服务需要把分析对象文件对外公开。黑客就通过这种公开的免费服务，了解自己制作的恶意软件是否可以委托分析。如果委托分析成功，为了不被追踪立即格式化受感染系统或者删除表等极端的行为带来致命的损害。

在线收费/免费沙箱服务有“GFI 沙箱(GFI Sandbox)”、“Noman 沙箱分析仪(Norman Sandbox Analyzer)”和“Joe沙箱(Joe Sandbox)”等。

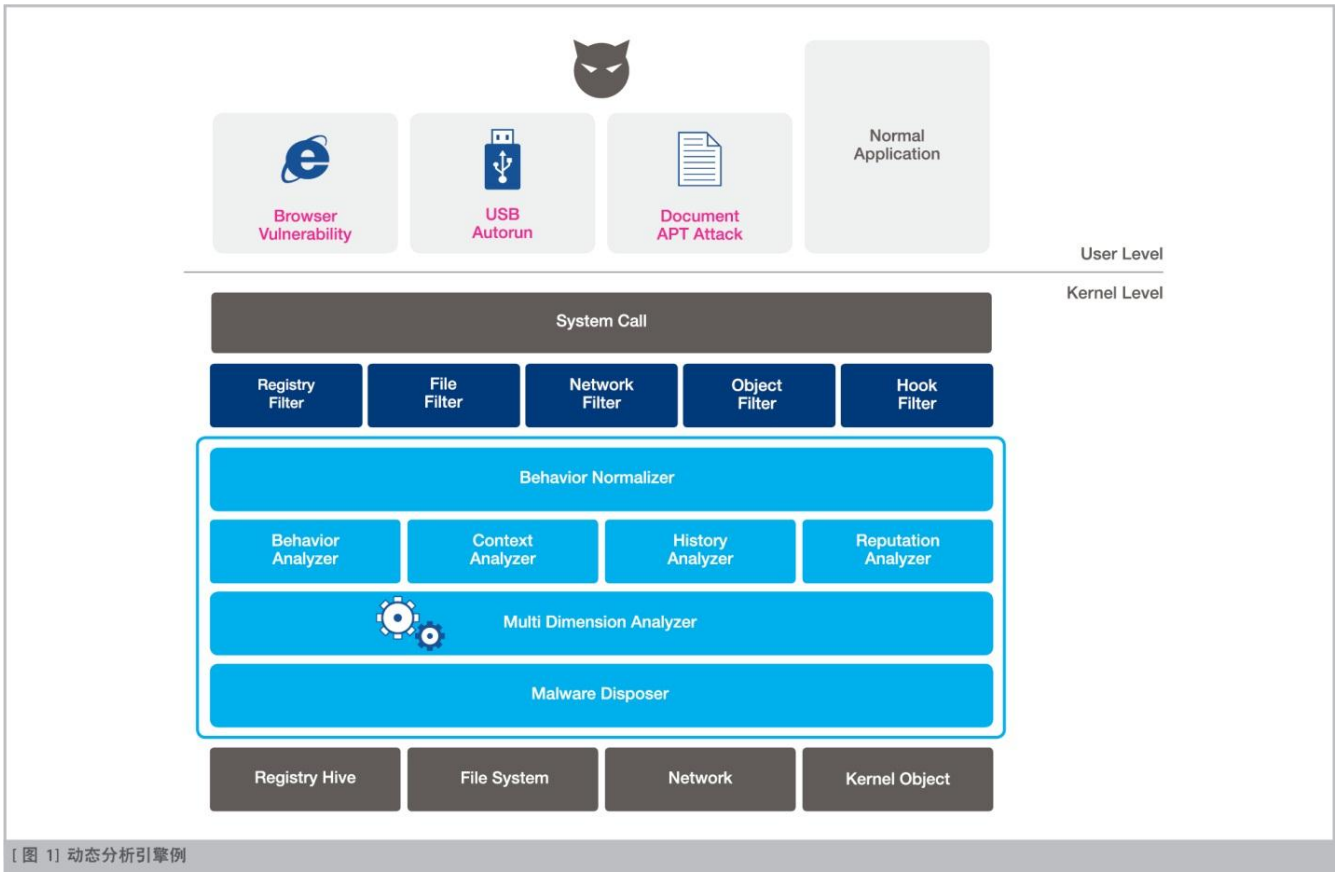
第二，公开源代码恶意软件动态分析。目前，有很多基于公开源代码的动态分析已被商用化。但是这种恶意软件分析也被恶意软件制作者容易构筑并分析源代码，最终被利用在判断自己制作的恶意软件是否被检测或如何避开检测。这种工具有 ZeroWine 和 Cuckoo 沙箱等。

如此，基于在线沙箱服务或公开源代码沙箱服务的动态分析对于暴露在APT(高级持续威胁)的顾客无法给与帮助。对此，有必要构筑应用沙箱技术的专用安全解决方案(in-house sandboxing)。

基于沙箱的动态分析技术

动态分析是将分析对象即样本文件在受控的分析环境下运行，并对发生的行为进行监控和分析，是目前最为广泛使用的分析方式。动态分析是在虚拟机形式的受限制的环境下进行分析，在分析环境下运行样品文件的同时可以检查网络行为、伪造注册表和伪造文件系统等多样的操作系统的变化。

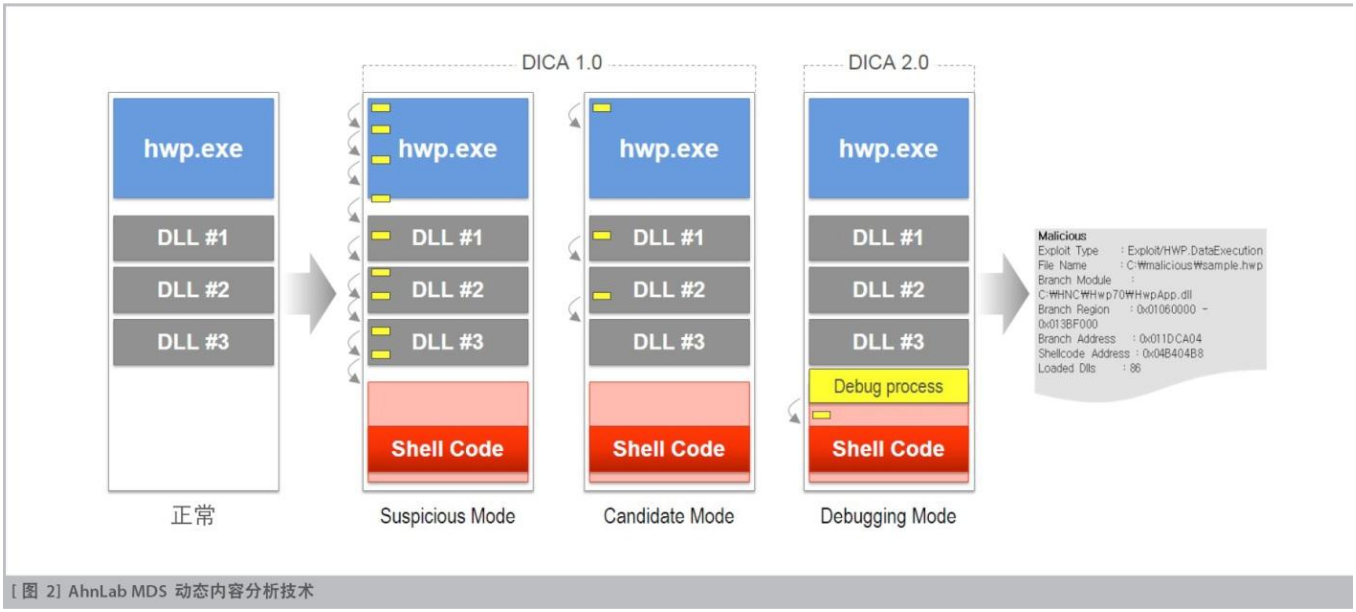
为了感知操作系统发生的变化，分析环境下使用两种方式。一是，在用户模式(User Mode)和内核模式(Kernel Mode)下挂钩(hooking)API 函数的方式；二是，监控在发生特别的事件时系统自动呼出的通知例程(Notification Routine)。



[图 1] 动态分析引擎例

混合码分析

混合码分析是混合静态分析和动态分析的方式，又称基于动态内容的分析(Dynamic content-based analysis)。恶意软件若保存到硬盘，以计算机语言级别的二进制形式存在。在反汇编过程中恶意软件二进制用于输入值， 汇编语言代码导出为输出值。这种过程中，判断应用程序运行时是否在内存领域发生异常代码的运行是基于动态内容的分析的核心。

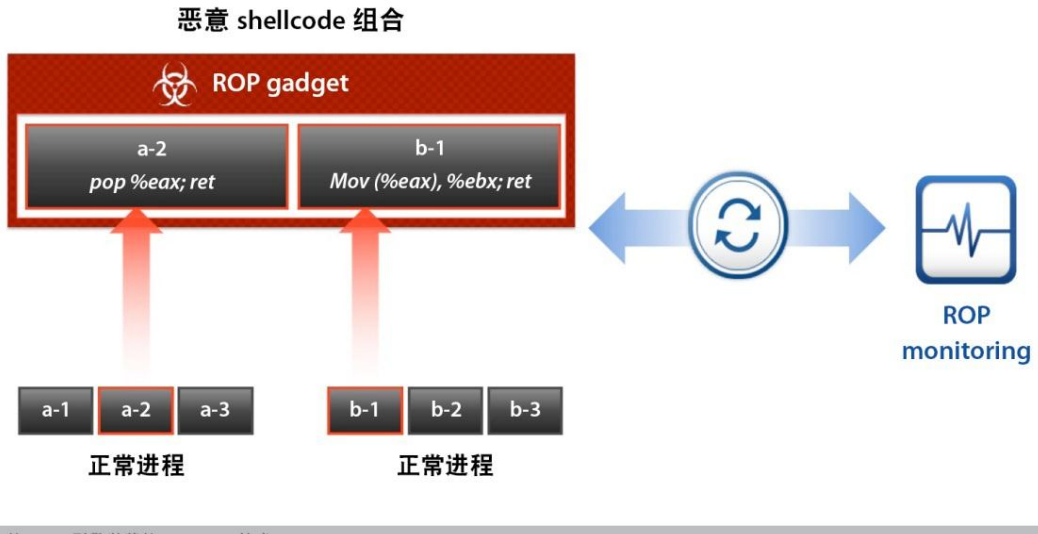


[图 2] AhnLab MDS 动态内容分析技术

AhnLab MDS 的动态内容分析技术 "DICA(Dynamic Intelligent Content Analysis)" 使用了 Suspicious Mode 和 Candidate Mode。 Suspicious Mode 是分析可以派生为 shellcode 的所有命令的每个地址是否 EIP(Extended Instruction Pointer, 下次运行的命令位置的内存地址) 包含在正常内存领域；而 Candidate Mode 只在漏洞攻击实际利用的的命令地址里分析 EIP。但是，每样品分析仍然需要几秒钟的分析时间，因此在大量恶意软件分析时有可能成为问题。

有关此问题，AhnLab 最近研发的 DICA 2.x 版本，只在检验对象应用程序运行并移动到 Non-PE 属性的内存地址领域时发生事件的瞬间监控 EIP，从而可以实时分析 Non-PE 恶意软件。

另外，AhnLab MDS 提供的动态内容分析技术还可以检测到像 DEP(Data Execution Prevention) 和 ASLR(Address Space Layout Randomization) 等迂回 Windows 本身的内存保护功能的使用 ROP(Return-Oriented Programming) 手段的恶意代码。



[图 3] AhnLab MDS 的 DICA 引擎装载的 Anti-ROP 技术

ROP 是将已存在的命令按顺序排列后根据黑客的需要使用一系列的命令集合，称为 ROP gadget。DICA 通过下面的方式来判断恶意 shellcode。

① 监控 ROP gadget 有可能引起的所有行动
② 检查内存领域，该内存判断为利用 ROP 方式运行 shellcode
③ 检查内存领域是否是恶意 shellcode

通过如上述的 "拦截 DICA 内的 ROP" 技术，不仅可以检测到利用 ROP gadget 的 Non-PE 型 APT 恶意代码，还可以检测到利用迂回 Windows 操作系统提供的自我内存保护功能的 ROP gadget 的 exploit。另外，按阶层构成多样的启发式的诊断方法，发展为源泉封锁 ROP gadget 运行的响应技术。

端点安全技术

前面所述的沙箱技术是专用安全设备在网络流量中提取的文件，从而可以检测到高级的针对性攻击。但是，下面的情况在基于网络的安全解决方案分析存在明显的界限。

- 以多数正常文件模块化的程序包形式的恶意软件
- 在像沙箱的受限制的虚拟分析环境下无法正常运行的恶意软件
- 因为是不经常使用的文件格式，所以无法提取或动态分析的恶意软件
- 通过U盘或公司内网传播的恶意软件的时候，通过基于网络的安全解决方案分析

为了克服网络安全解决方案的界限，越来越强调端点的多层次的分析。只有正确分析，才可以主动的防御。

在端点的行为分析可以分为两种：一是分析安装的恶意软件的最终目的是什么，即可判断为恶意软件的可疑行为分析；二是安装到计算机以后避开检测而持续活动的隐蔽行为的分析。
第一种分析方法与动态码分析方式相同，除了分析文件和进程的生成•更改•删除履历、注册表项的更改及网络连接状态变化等，还通过事件日志的监控可以如下分类主要的恶意代码。

- Downloader：运行时，从互联网下载其他恶意代码。
- Launcher(或 loader)：即刻运行自己或者其他恶意代码，或在未来隐秘地运行。
- Backdoor：提供使黑客可以远程访问感染计算机的通道。
- Credential Stealer：截取重要的认证信息。

有关隐匿行为的主要分析的例子如下：

- 注册表分析：需要分析有关自动重启的注册表项。
- 检测特洛伊木马化的系统文件：感染 DLL 等系统文件后加载该文件时可以运行恶意代码。需要分析系统文件的哈希值被伪造的状态。

在这种端点的行为分析过程中逐步被强调的部分就是内存领域的取证分析。即多样的内核层隐匿功能的恶意软件可以伪造端点的行为内容，隐藏实际运行的应用程序或伪造访问该应用程序的文件内容，还可以隐藏访问外部网络的内容。为内存取证，分析技术发展为以下两种，一是内存转储后事后分析；二是实时分析内存领域。

AhnLab MDS 的竞争产品大部分没有 Agent 就通过网络层的分析设备提供网络拦截方式的响应技术。但在此过程中最初使用在分析的恶意代码早已流入到内部网络引起更多损害。像这样仅仅通过网络拦截是无法对已下载的恶意代码采取任何的措施，这是该方式的界限。

AhnLab MDS 从产品企划开始就已超越了单纯的网络级别的检测，强调通过端点的 Agent 做出积极响应的技术。部分竞争产品刚开始强调没有 Agent 而给用户带来的方便，但是现在逐步发展为推进与第三方 Agent 安全提供商的融合产品，或研发自身的 Agent 技术的趋势。

AhnLab MDS 将网络层检测到的未知恶意软件的删除指令传达给 Agent，不仅可以简单响应，还提供运行保留(execution holding)功能，对未确认的可执行文件保留运行，直到分析结束为止。

总结上述的内容，AhnLab MDS 是通过“基于沙箱技术的动态分析技术”、“检测 Non-PE 型恶意软件的技术 DICA”和“利用 Agent 的端点安全技术”等，重新武装成为专门响应 APT 的下一代主动型安全技术。

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。

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
http://www.ahn.com.cn / v3site@ahn.com.cn