安博士月刊

星 期 三
7月 31日
2 0 1 3年

Vol.11

【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。

多层次的分析平台
恶意代码防御迎来新的局势

恶意代码变得越来越高级化且多样化，事后防御为主的应对方式面临了局限。包括 Zero-day 攻击，最近 APT 攻击利用新•变种恶意代码的事件增加，这足以说明仅仅依靠传统的“基于特征码”的恶意代码检测技术已经无法有效应对最近的安全威胁。

对此，AhnLab 独自开发了“多层次分析平台”。该技术首先应用在 V3 产品群，然后计划依次应用在 APT 解决方案“AhnLab TrusWatcher(国际市场被称为 AhnLab MDS)”和网络安全解决方案“AhnLab TrusGuard”产品系列等几乎所有的产品。

构筑以“主动防御”为主干的创新的防御体系是 AhnLab 推出的新的战略。下面我们来看一下 AhnLab 即将推出的新的防御威胁结构，即恶意代码防御技术“多层次分析”技术。

每天有大量的恶意代码被制作并发布，这已不是新鲜的事情。根据 AhnLab ASEC（AhnLab 安全响应中心）的统计，4月份被报告的恶意代码共有550万8895件。3月份被报告的恶意代码大约760万件。就韩国国内每月平均发生500~700万件的恶意代码感染事件。

不仅如此，全世界未知（unknown）的新•变种恶意代码的发布速度与日俱增。还有，出现了逃过防病毒检测的恶意代码等，恶意代码已变得更加周密和高级。

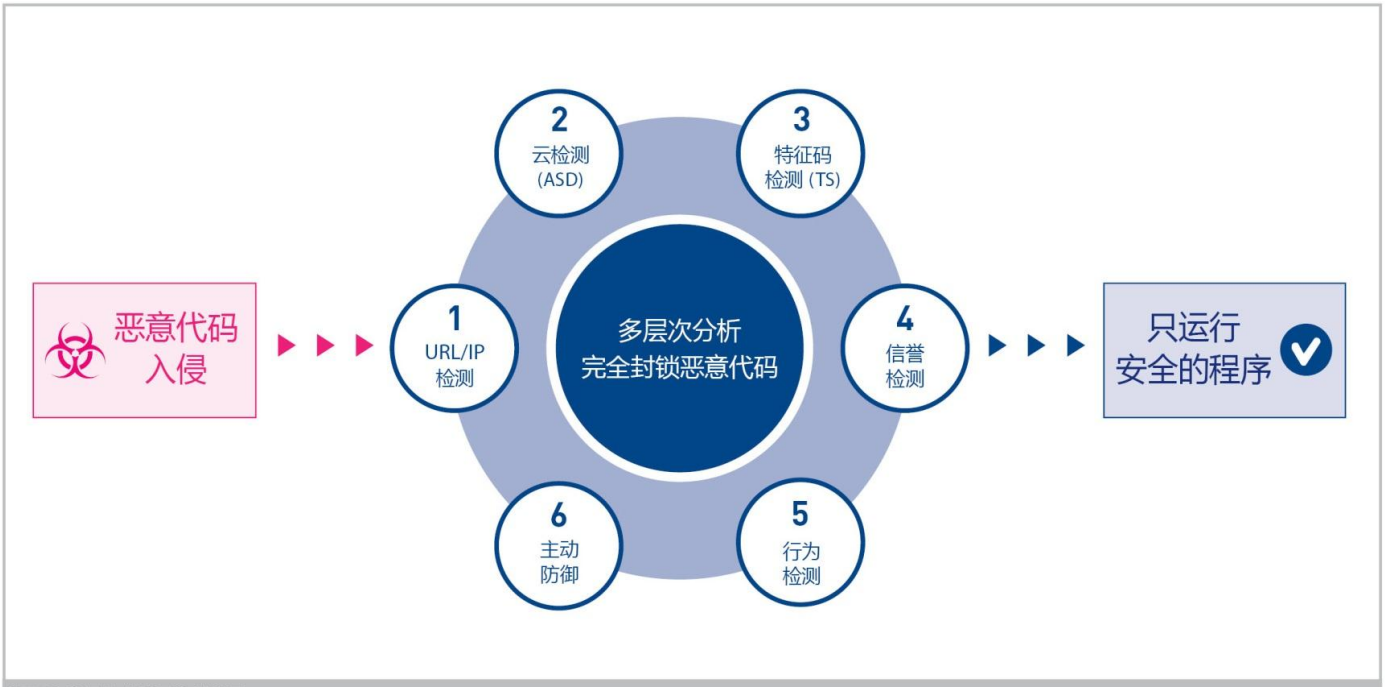
同时，最近还出现了与 APT 相似的“定制型恶意代码”。它主要是针对企业、机关或特定地区。先选择攻击目标，然后找到该目标经常使用的应用程序的漏洞并利用该漏洞进行攻击。因此，防御这些周密且高级的恶意代码可以比喻成“海底捞针”。随之，传统的“特征码技术”的局限也渐渐显露出来。

多层次的分析才是最佳解决方式

很多安全提供商纷纷研究和开发可以代替“特征码技术”局限的恶意代码防御技术。AhnLab 也进行了多角度分析威胁，谋求多维防御的方案。结果，今年就开发了“多层次分析平台”并计划应用在公司大部分的产品。

“多层次分析”技术是引进了“主动防御(Active Defense)”的概念，但是与传统的“主动防御”技术不同。传统的“主动防御”是指通过对计算机病毒的行为进行分析来实现检测的技术。而“多层次分析”综合应用了“基于行为”的分析技术和“基于信誉”的分析技术等多样的分析技术，在威胁入侵阶段就开始主动防御，是一个新概念的综合威胁防御技术。

“多层次分析”技术不仅可以实时应对威胁，还可以能动地应对威胁。共有6个主要检测及分析技术构成。
▲URL/IP 检测技术 ▲基于云的检测 ▲基于特征码的检测 ▲基于信誉的检测 ▲基于行为的检测 ▲主动防御



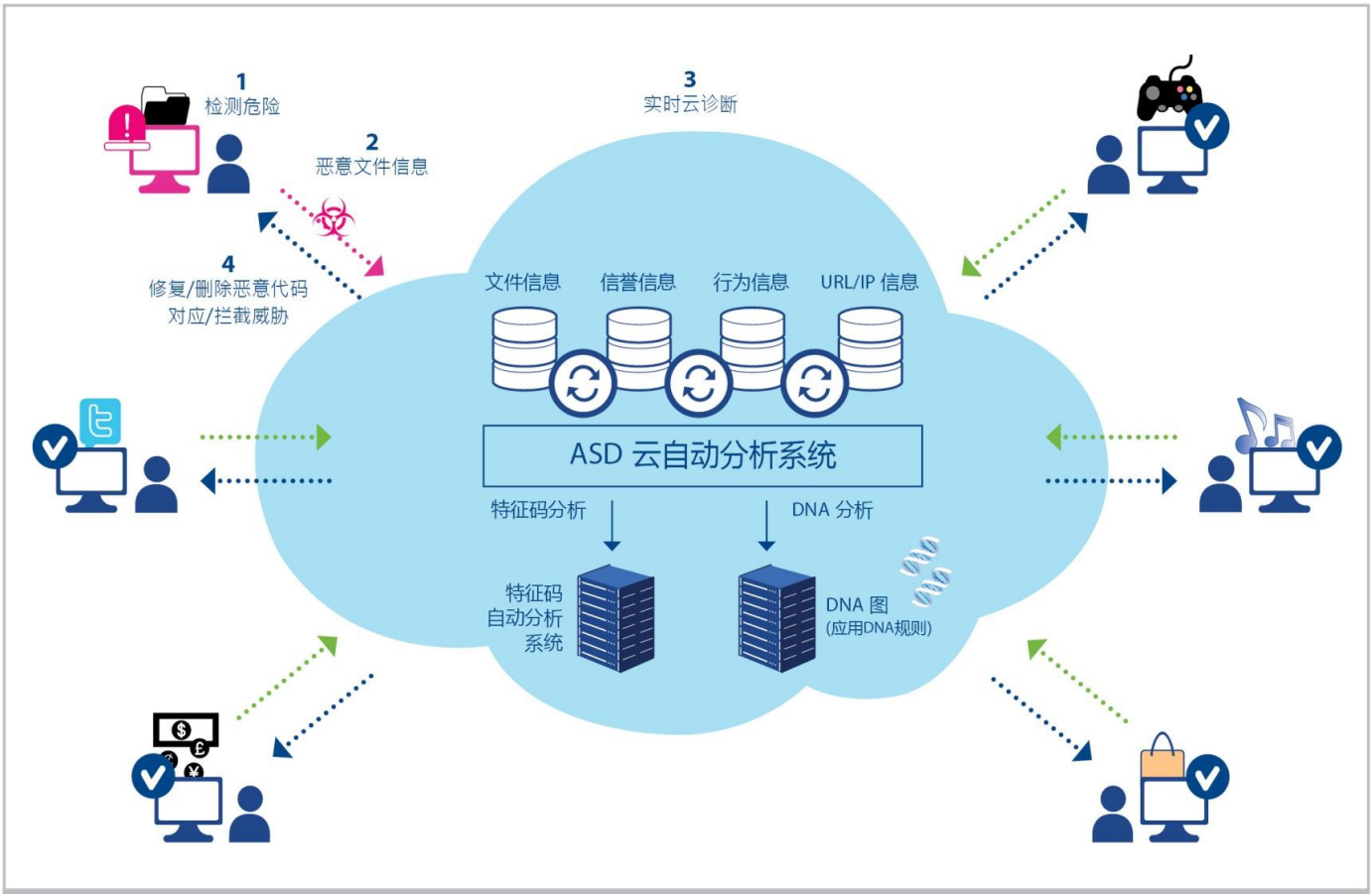
[图 1] 多层次分析平台概念图

1. URL/IP 检测 – 阻止访问恶意网站、阻止连接 C&C 服务器等外部网络

最近大部分的恶意代码通过互联网入侵到内部。神不知鬼不觉地伪装成正常的文件，传播恶意代码。这种巧妙伪装的网站如洪水般增加，而且只要访问该网站就被感染恶意代码的事例也频繁发生。

因此，为了防止恶意代码通过网络流入，根据多数人使用的经验，对于具有传播恶意代码履历的或者判断为具有危险的 URL 提前阻止。这就是 URL 及 IP 检测技术的核心。基于 URL/IP 检测技术是在恶意代码流入阶段开始阻止并完全封锁恶意代码的技术，在“主动防御”的观点来讲，具有非常重要的价值。

特别是，检测或拦截与 C&C 服务器通信等恶意的外部网络连接，可以预防重要信息被盗或根据攻击者命令的附加攻击。不用另外的“特征码技术”就可以实时检测并应对危险 URL 或者 IP，这一点被认定是应对最近威胁的有效技术。



[图 2] ASD 网络概念图

2. 云检测 – 实时应对威胁，主动防御

基于云的检测技术是利用 AhnLab 的云计算基础的 AhnLab Smart Defense（以下简称为 ASD）技术，多角度实时分析和诊断文件的恶意与否的技术。中央服务器管理大容量文件信息数据库，当计算机（或系统）安装的 ASD 引擎向 ASD 中心询问文件的恶意与否时，ASD 中心则对该文件进行多角度分析后告知 ASD 引擎该文件是恶意的还是正常的。 这种技术是特征码引擎还未更新就可以实现防御威胁的，主动防御观点的诊断技术，特别对新•变种恶意代码诊断很有效。

AhnLab 的基于云的检测技术由2000万名以上的ASD网络构成。迅速收集实际发生或发布的威胁，在威胁发生的同时实时应对。通过 ASD 网络收集的样本，进行及时分析后，将该威胁信息共享到包括 V3 产品的 AhnLab 的所有产品，防止恶意代码的进一步扩散。

3. 特征码检测 – 误诊最少化、改善诊断速度及引擎轻量化

应用到“多层次分析”技术的“特征码技术”也经过了反复的技术革新，与传统的“特征码技术”相当的不同。首先，AhnLab 的基于特征码的检测技术中心具有 7 亿多个的 ASD 数据库。ASD 数据库不仅积累了恶意文件信息，还积累了正常文件信息。这就可以更加迅速有效地诊断恶意与否，几乎没有误诊。

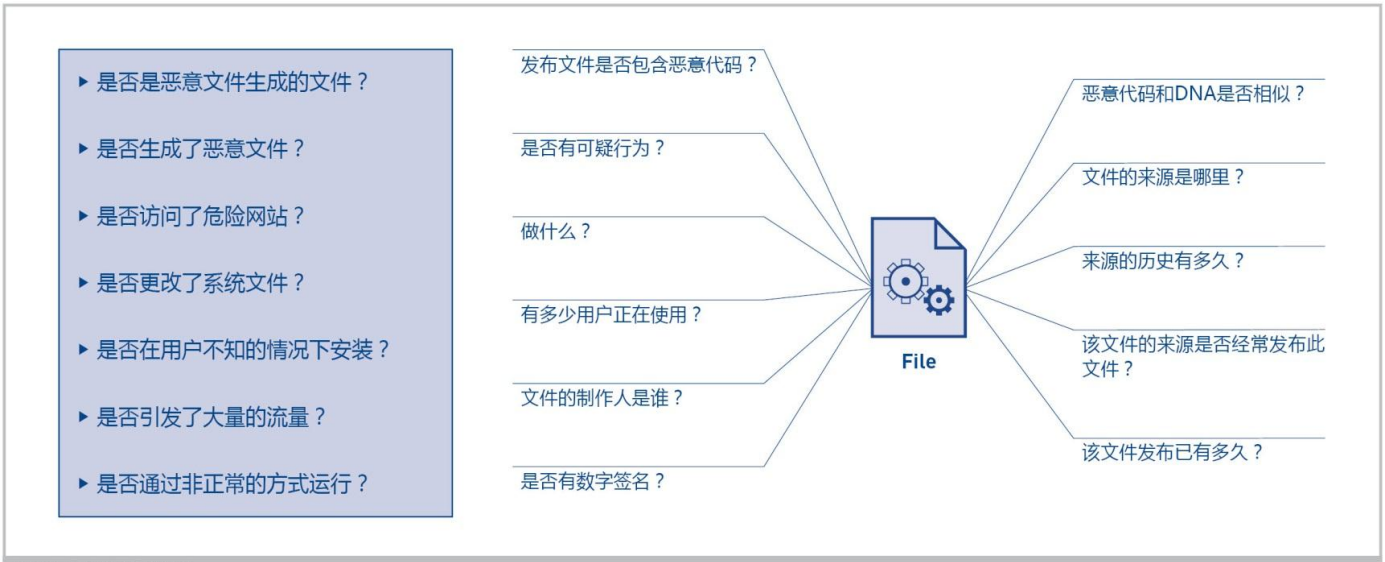
然后，它应用了 AhnLab 独自开发的 DNA 扫描技术，再加了一层技术革新。DNA 扫描是利用恶意文件的 DNA 信息检测的技术。提取恶意代码具有的固有的特征和文件的 DNA 信息，将其利用在恶意代码诊断。与传统方式不同的是，传统方式利用文件特征码诊断恶意与否，而 AhnLab 的“特征码技术”利用文件 DNA 特征来诊断恶意与否。这种方法克服了传统的“特征码技术”的局限性，提供高效且主动的解决方案，从而可以防止恶意代码，几乎不需其他硬件资源就能大大减少了误诊率。

不断积累多种多样的恶意代码特征码来应对安全威胁的方式目前来讲不符合现实，并且效果不大。随着特征码数量的增加，引擎大小也会增加。相反，如果应用通过庞大的样本数据库和分析专门技术压缩重编的 DNA 规则，比起不断积累特征码的方式大幅减少引擎大小，可以带来“主动防御”和“用户方便”的两大效果。

4. 基于信誉的检测 – 应对迂回攻击及潜在的威胁

AhnLab的“多层次分析平台”的核心可以说是“信誉检测”和“行为检测”。前面所述的“基于云的检测技术”和“基于特征码的检测技术”是原有技术的革新的改善，而“基于信誉的技术”和“基于行为的技术”是对恶意代码应对模版的革新。

“基于信誉的检测技术”是对于未知文件，即“未诊断”文件及应用程序的潜在威胁提前防御的技术。该技术对于最近的高级化的攻击技巧很是有效，可以检测到逃避防病毒软件的恶意代码。最近，恶意代码制作者在传播恶意代码前先测试被防病毒软件的检测与否。这点也被认为是“特征码技术”的局限。与此相关，AhnLab 的“多层次分析技术”把用户数、评价、来源和与其他文件的关系等多样的信誉要素添加到诊断基准，克服了“基于特征码的检测技术”的局限，彻底实现了预防性提前对应。根据通过云收集到的多样的信誉信息，还参考了其他用户的评价，让用户实际判断并对应。



[图 3] 信誉信息的例子

即使是未知文件(或程序)，但是可以根据多数用户分类的信息(恶意或正常)或实际用户数，并考虑用户环境等多种要素判断为恶意或正常。这意味着，用户可以根据多数用户的“评价”信息，自己可以设置实际安全级别并防御威胁。

5. 行为检测 – 防御零日攻击，Exploit(漏洞利用)

不亚于“基于信誉的检测技术”的有效技术即是“基于行为的检测技术”。“基于行为的检测技术”是诊断文件行为是否恶意与否的技术，防御对于逃避检测的高级恶意代码、利用零日攻击的恶意代码很有效。与前面所述的“基于信誉的检测技术”一样，根据 AhnLab 多年积累的专门知识和基础设施实现了“基于行为的技术”。该技术对恶意文件最终执行的行为详细区分为100多个模式，以此为根据进行诊断恶意与否。例如，根据没有用户同意下载并运行恶意代码的行为，可以判断恶意与否，然后对应。以此，不仅是零日攻击，就连非正常的漏洞利用也可以完全封锁。

6. 主动防御 – 详细分析报告，实现能动地防御

结合基于云、特征码、信誉和行为的技术，对于目前的大部分恶意代码都可以对应。但是，恶意代码及攻击技巧进化的速度超出想象，且方向也很难预料。这意味着，不能完全排除逃过高级分析技术的威胁的存在。

预备此类情况而诞生的技术就是“主动防御(Active Defense)”。该技术也是 AhnLab 独自研发，提供了主动防御系统内部威胁的可视性的技术及功能。如果当前系统内部存有异常行为的文件，则对该文件具体有何种行为等信息，通过实时详细分析提供，确保可视性的同时用户可以预先对应。用户可以利用各种分析信息，能动地对应恶意代码威胁，可以提高安全级别。

多层次分析技术的期待效果

如此，多样的高级技术有机结合的 AhnLab “多层次分析技术”，应用在今年 6月上市的个人用户版防病毒软件“V3 Lite”和“V3 365 Clinic”，并应用在即将上市的“V3 Internet Security 9.0”等 V3 产品群。接着，还计划将应用在 TrusGuard 等网络产品，移动产品，APT 解决方案，TrusWatcher（AhnLab MDS）和生产系统专用安全及控制解决方案“AhnLab EPS”等产品。

[图 4] 多层次分析技术最初应用在 V3 IS 9.0

结尾

那么，通过这种“多层次分析技术”应用的产品，我们可以期待怎样的效果呢？

首先，最终可以期待正确诊断威胁。利用“多层次分析技术”可以最少化未诊•误诊，利用“基于行为”和“基于信誉”的检测技术，诊断新•变中恶意代码，从而达到更加精确的诊断。

然后，特别是实现了“主动防御”观点的安全，克服了“特征码技术”的局限，这一点就很值得瞩目，且具有很大的意义。考虑到随着针对特定企业/机关的目标攻击的增加陆续出现了“定制型”恶意代码的当前情况，通过提供提前防御技术，期待着可以有效防御多样的安全威胁。

最后，当今复杂多变的威胁环境中，单纯一个产品、一个技术很难全面解决安全问题。未来时代是一个融合安全的时代，各种安全技术需要融合，我们期待重新开启一个新安全、大安全的时代。但是，有机融合技术并取得效果并非易事。正是这一点，AhnLab 充分显示了 AhnLab 的专门技术和基础设施价值。根据 AhnLab 积累的20多年的专门技术和基础设施，体现了各种高级分析技术并取得了协同效果。

www.ahn.com.cn / v3site@ahn.com.cn / 电话：010-8260-0935
北京市朝阳区酒仙桥甲 12 号电子城科技大厦 1206 室