AhnLab

安全月刊

2020.09 Vol.94

AhnLab MDS

AhnLab MDS，误诊率为0%的高级威胁响应解决方案

AhnLab MDS，通过集成和链接有效防御高级威胁

我们经常听到勒索软件、新种和变种恶意代码、网络钓鱼邮件以及针对性攻击等熟悉而不受欢迎的威胁导致的安全事件的消息。 黑客随时随地进行各种类型的攻击，只要他们可以窃取金钱利益或可以产生收益的信息即可。组织的安全负责人也非常清楚这一点。因此，根据需要引入了各种解决方案并运营，并且为了保护组织的资产做好了一切准备。

尽管如此，安全事件持续发生。虽然安全解决方案都在各自发挥着应有的作用，但问题在于，黑客也已经知道这一点，并不断开发新的迂回攻击的方法。根据AhnLab的数据，所有攻击的5%左右是迂回已构筑好的解决方案而成功实现了攻击。那么，如何才能有效响应这5%的“高级”威胁，并在不断与黑客进行的对抗中占据优势呢?

在本文中，我们重点介绍了高级威胁的主要目标、攻击方法、对安全解决方案的要求以及组织为有效响应威胁应采取的观点。

首先，高级威胁的主要目标是电子邮件、网络和端点。

攻击目标 1：电子邮件

攻击电子邮件最为频繁发生，因为任何人都可以通过电子邮件的地址轻松尝试攻击。尽管内部邮件通常被视为攻击目标，但通过 Web 或 Outlook 查阅外部邮件时也经常发生安全事件。与黑客付出的努力相比，由于针对电子邮件的攻击成功率很高，预计今后此类攻击将持续增加。

在电子邮件攻击中，一种常用的方式是通过附件进行攻击。可执行文件、文档文件和压缩文件占据大部分，其中 Hangul、MS Office 和 PDF 等文件的比重最高。当收件人运行附加到电子邮件的恶意文档文件时就会感染恶意代码，而这种攻击事件经常的攻击事例经常发生。

以就近的事例，8 月份，AhnLab 发现了伪装成“原产地调查自律检验表”的恶意 Hangul 文档（hwp），并提醒用户要注意。该文档包含了实际法律的格式内容，因此很难识别该文档是恶意文档，而且电子邮件攻击中使用的其他附加文件也进行了巧妙的伪装，以使收件人无法轻易识别。

最近，由于电子邮件附件受到限制，利用电子邮件正文链接的攻击也在增加。不是直接附加文件，而是插入外部的大容量下载链接，或者是诱导用户访问钓鱼网站来攫取帐户。或者，还会发起传送隐藏漏洞的网站链接的攻击。

还有一些攻击仅使用电子邮件正文而不包含附件或链接，其主要目的是窃取金钱。攻击者声称已感染了 PC，并威胁将用户的互联网访问记录和视频播放列表发送到地址簿中的所有邮件帐户，以此索要金钱；还或者欺骗说要筹集事业相关投资金等。另外，通过回复与客户往来的电子邮件，谎称收取货款的银行账号已更改并要求向其他帐号汇款。据悉，很多企业会因此类攻击遭受了大大小小的财务损失。另外，由于此类攻击都会经过彻底的事前调查，因此成功率很高。

攻击目标 2：网络

针对网络的攻击需要比电子邮件更先进的技术。这是因为要诱导已被指定为目标的用户直接访问恶意网站。

网络攻击基本上使用文件形式的恶意代码。利用 Web 浏览器漏洞或博客或 SNS 分发伪装成正常程序的恶意可执行文件。还使用包包宏和漏洞的文档文件、图像和视频。以上攻击大多分都是通过 Web 进行的，有些还使用 FTP。最近，随着物联网（IoT）基础设施的扩散，通过它的攻击也逐渐增加。

还经常执行不使用恶意代码的网络攻击。在外部网络中，经常发生针对主要内部服务器的漏洞攻击、IP/Port 扫描和 Webshell 攻击。从内部到外部的恶意流量也被认为是危险因素。通过用户的疏忽而访问的恶意网站或已感染的 PC 泄漏个人信息或机密密信息到外部属于上述情况。

在网络安全方面，需要注意的一点是，尽管很多组织使用的网分离是很好的一种安全措施，但这并不是万能的解决方法。如果通过网连接解决方案在业务网络上浏览了伪装成业务相关内容的恶意电子邮件或文

件，则存在感染恶意代码的风险。另外，仅通过网络分离还无法响应各种威胁，因为黑客会通过迂回网络并直接对端点进行攻击。

攻击目标 3：端点

组织的重要数据都聚集在端点，因此端点可以视为攻击者的最终攻击目标。如果组织遭受攻击并允许访问敏感数据或公司机密，则公司将会遭受无法估量的损失。

当前的端点攻击的主要针对公司内部的办公电脑、移动设备、服务器、生产设备及可在公司外部使用的笔记本电脑。攻击者主要选择一种方法，该方法通过将损失从一个端点传播到多个终端设备来最大化攻击效果。普遍的手法是，用恶意代码感染 USB 并将其传播到连接的电脑、笔记本电脑及生产设备，还可以通过利用 OS 的漏洞将感染传播到连接在同一网络的电脑。另外，还有一种无文件（fileless）攻击，它不使用恶意代码，利用在电脑上运行的正常程序来导致恶意行为（例如勒索软件）。

未来，针对端点的攻击将变得更加复杂，安全复杂性也会进一步深化。市场调查机构弗若斯特沙利文在今年 7 月发行的《5G 和 5G 网络安全对企业的影响（5G and its Cybersecurity Implications for Enterprises）》报告中指出，在 5G 时代，企业要面对的安全挑战课题之一就是攻击点的扩大。这意味着使用 5G 网络的企业将跨越传统的端点，使用 OT 环境等新领域的设备和应用程序，攻击点也不可避免地会随之扩大。

对安全解决方案有哪些要求?

现在，来了解一下安全解决方案需要满足哪些要求才能有效响应这些高级威胁。

首先，在以电子邮件为目标的攻击中，应该尽快分析和处理文档文件以尽量减少电子邮件的延迟。从电子邮件中包含的链接下载并分析文件，并利用信誉信息迅速过滤是否存在恶意代码。如果没有信誉信息，解决方案还应具备自行分析链接的能力。通过分析电子邮件正文关键词，还可以检测到欺诈（Scam）邮件。此外，还应支持针对韩国分发的 ALZip 扩展名压缩文件和加密压缩文件的响应方案。以上内容均适用于公司内部及外部电子邮件。

网络安全解决方案必须通过彻底检查用户通过网络下载或上传的文件来确保“可见性”。该解决方案的分析引擎还必须针对文件类型进行优化的分析逻辑，以分析防病毒软件无法检测到的新种和变种恶意代码，并对多种文件进行分析。此外，必须监控进出网络的内部和外部流量，以检测外部攻击和从内部到外部的恶意数据包。

最后，在端点层，需要对各设备进行实时监控。公司外部的电脑也有可能在外部受感染的状态下访问内部系统，因此安全级别也要保持与内部相同水准。另外，必须同时执行 USB 扫描，并且必须确保漏洞拦截和实时检测无文件攻击的功能。

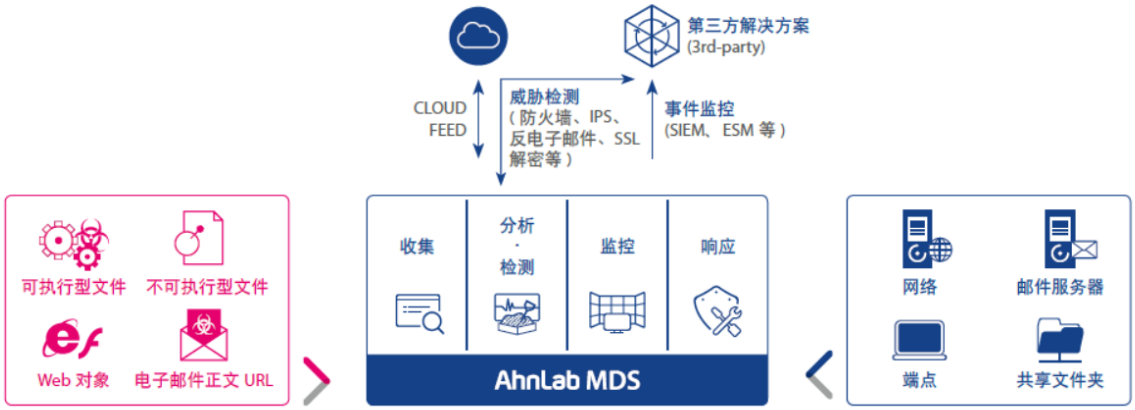
考虑到这一切都会遇到一个难题。“是否可能满足所有这些要求？”另外，如果引入按区域分布的解决方案来建立安全体系，则很可能难以确保可见性和提高管理效率。

“有机”响应高级威胁的 AhnLab MDS

为了有效响应高级威胁，需要有将各领域的安全功能连接起来的集成解决方案。由于一个解决方案很难独自保护所有分支机构，因此考虑到多种攻击的特性，确保与现有的安全解决方案有机连接的“网络杀伤链（Cyber Kill Chain）”至关重要。

AhnLab MDS（以下简称为 MDS）建立了直观而全面的威胁可见性，以及“收集 → 分析和检测 → 监控 → 响应”的响应流程。在此基础上，提供网络与端点之间的有机响应能力，有效拦截来自各种渠道入的高级威胁。MDS 的主要能力摘要如下：

1.多引擎分析
2.基于沙箱的动态分析
3.网络流量分析
4.电子邮件分析
5.响应 PC 攻击
6.V3 + MDS 统一 Agent



1.多引擎分析

MDS 基于多引擎，能够精确有效地检测及分析已知威胁到未知的新种/变种威胁。在所有威胁中约占 90%的已知威胁可以通过检测有害网站和 C&C(Command and Control)流量的特征码引擎，通过实时与云端连接迅速过滤恶意文件的信誉引擎，以及 YARA、Hash 和 IP/域等管理员预先定义的规则，可以迅速完成分析。

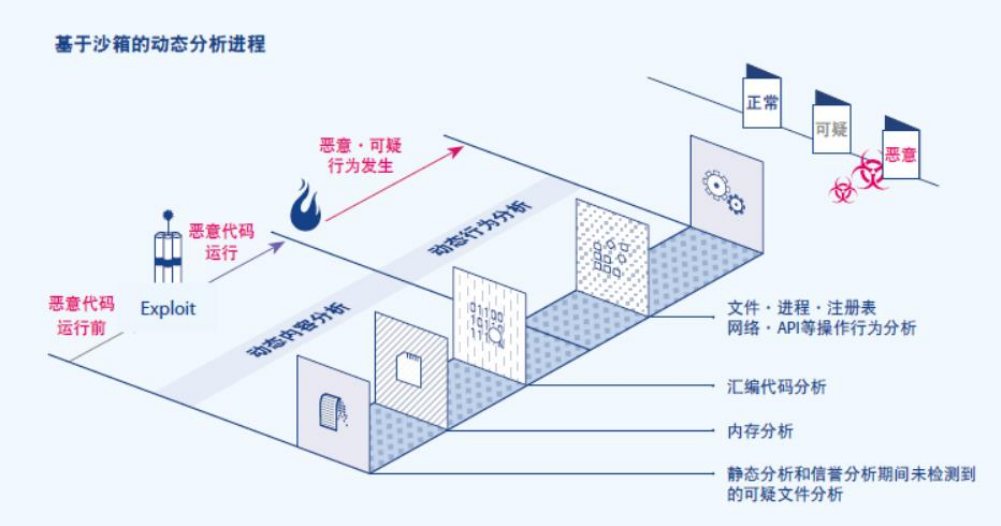
其余 10%的未知威胁通过机器学习和沙箱（非特征码）引擎进行详细分析。机器学习引擎分析文档类型文件的数据以检测恶意与否，沙箱引擎在虚拟机环境中，根据对象文件的种类运行专门的分析引擎。

2.基于沙箱的动态分析

基于沙箱的 MDS 动态分析分为行为分析和内容分析。

动态行为分析引擎在虚拟机中分析可执行文件。实时监控文件、进程、注册表和网络的变更，记录所有相关文件的行为、信誉和其他信息，并对其进行全面分析以判断是否是恶意。它可以最大程度地减少误诊，因为它可以分析前后行为，并使用云端上的信誉信息，实时诊断试图通信的 IP、URL、进程和文件的恶意/正常与否，因此可以将误诊程度降到最低。

动态内容分析引擎将分析不可执行文件，即文档文件和脚本文件，例如 js、vbs 和 wsf。它通过分离文档中包含的宏、注入对象和漏洞代码并进行分析，与行为分析相比，能迅速判断是否是恶意。在电子邮件的附件及网连接传送文件较多的环境中，易于使用。



3.网络流量分析

MDS 在网络层拦截来自 C&C 服务器和恶意代码分发网站等在异常点的恶意流量。为此，将实时检查所有数据包以分析网络流量，并将流量的源和目的地、IP、URL 等信息传送至云端，并使用信誉信息快速过滤。另外，对外部攻击者试图进行的攻击进行分类，并检测从内部受感染 PC 传送到外部的恶意数据包。MDS 会立即拦截检测到的恶意流量，从而阻止其他的连接。

4.电子邮件分析

MDS 不仅可以对传入的电子邮件的附件进行动态分析，而且还可以对正文中的恶意 URL 和脚本进行基于黑/白名单及信誉信息等的多维度分析。

对于附件，使用前面提到的多引擎进行迅速而准确的分析。其中，占据大部分的文档文件可以通过沙箱动态内容分析引擎在短时间内分析大量文件。

对于电子邮件正文中包含的链接，也可进行多角度的分析。直接从下载链接下载文件，检查是否存在异常，并使用云分析网络钓鱼网站，以及通过可疑 URL 访问分析攻击漏洞网站。此外，可以通过分析电子邮件正文及标题关键词来检测欺诈（Scam）邮件。

通过以上多种引擎进行分析确定为恶意的电子邮件将通过 MDS 解决方案被隔离。

5.响应PC攻击

MDS 通过专用 Agent 提供▲运行保留、▲漏洞检测和拦截功能，以响应 PC 攻击。

首先，MDS Agent 的运行保留（Execution Holding, EH）功能可防止运行未确认恶意与否的文件，提前预防感染带来的损失。在通过 USB 或其他路径流入 PC 的文件运行时，将对文件的恶意与否进行分析，并根据确认结果允许其运行，因此可在感染之前主动响应被检测到的恶意代码。

此外，还提供了针对利用漏洞的各种攻击的检测和响应功能。基本上，对攻击进行实时监控，并在检测到恶意行时预先拦截，使用户可以享受与运行保留功能相似的效果。另外，MDS Agent 细分的例外处理功能最大程度地减少了误诊和用户可能遇到的各种不便。

6.V3 + MDS统一Agent

MDS Agent 根据用户环境与 V3 连接，并可以作为统一 Agent 运行。通过 V3 检测已知的恶意代码和恶意行为，并通过 MDS 检测和响应未知的新种和变种恶意代码，建立了有机的防御体系。在使用其他防病毒软件的环境中，它还具有灵活去，可以支持单独安装 MDS Agent。

威胁检测率为 99.1%...AhnLab MDS 值得关注的理由

可以说 MDS 解决方案的成功或失败取决于是否检测到新种和变种威胁。具有各种功能并有效响应现有攻击固然重要，但如果不能正确检测到越来越高度化的新种威胁，其价值必然会下降。

在全球安全评估机构 ICSA Labs 于 2019 年第三季度进行的高级威胁响应（Advanced Threat Defense, ATD）测试中，MDS 记录的未知威胁检测率为 99.1%，误诊率为 0%，在所有评估项目中均获得高分，最终获得了认证。AhnLab 一直在开发新的功能以有效响应各种攻击，同时努力客观地证明它们。

此外，AhnLab MDS 值得关注的差别化优势如下：

● **管理资源优化**：MDS 提供对在各区间检测到的所有威胁的自动响应功能。即，用户只需在响应结束后确认误诊信息，并仅对误诊信息采取纠正措施。

● **成本效益**：MDS 通过一体化（All-in-one）设备，支持在不同的区间的监控、分析及响应。另外，还提供了 Pinpoint 检查功能，使管理员可以直接分析可疑文件或恶意 IP/URL，并支持可以与其他解决方案联动的标准化 API。

● **定制的策略分离**：MDS 可以按照组织分类来分别应用策略。根据组织的特性，可以应用适当的策略强度，还可以考虑各地区网络带宽来管理分析文件的大小。

● **专门服务**：MDS 不仅提供解决方案，而且通过与 AhnLab 专家的服务连接来响应攻击。服务主要分为三种： “恶意代码专家分析服务” （ 专家直接详细分析恶意代码并提供报告）， “可疑系统诊断服务” （分析疑似感染对象的入侵历史记录并提供诊断报告）， “数据分析服务” （分析检测日志并共享各领域危险级别及策略优化指南。

集成和连接，日趋复杂的业务环境以及新出现的威胁使安全负责人的责任更加沉重。如前所述，由于许多解决方案的运用导致的可见性和管理效率低下认为是亟待解决的课题。

解决这一问题的核心关键词是“集成”和“连接”。现在，在网络、端点和电子邮件等所有区间分别安装安全解决方案来进行彻底保护已几乎不可能。因此，需要通过集成的安全解决方案链接现有的分数的解决方案，并构筑迅速而全面的安全流程。在此过程中，必须先明确了解组织的安全需求，然后再选择适当的安全解决方案和策略。

如果能够成功实现这些事项，那么您将可以向为组织建立安全的环境迈出一步。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab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。
AhnLab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

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502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 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com