AhnLab

安全月刊

2017.02 Vol. 51

Machine Learning

利用“机器学习”的安全威胁检测

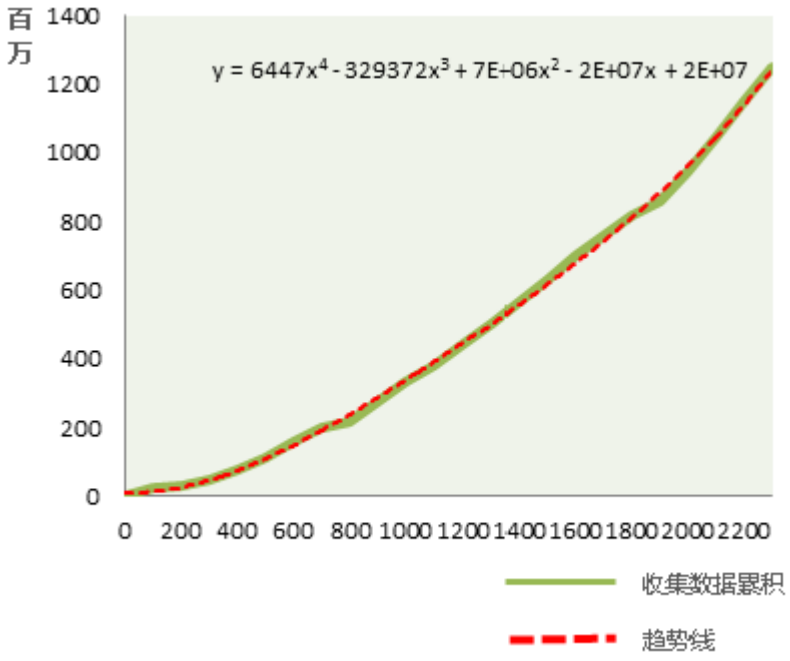
安全领域为什么需要机器学习？

去年Google的AlphaGo和李世石9段的围棋人机大战显示了人工智能并不再是遥远的未来。此外，IT行业的巨头企业正在将“人工智能(Artificial Intelligence)”作为未来的发展动力，并在各个领域展示了应用人工智能的事例。
本刊将分为两次介绍实现人工智能的方法中的一个“机器学习(Machine Learning)”和安全领域为什么需要机器学习。本期将介绍安全领域为什么需要机器学习。

上一期介绍了什么事机器学习，为执行机器学习需要考虑的事项。本期将介绍为什么需要机器学习来防备安全威胁，以及AhnLab是如何将机器学习应用到安全。

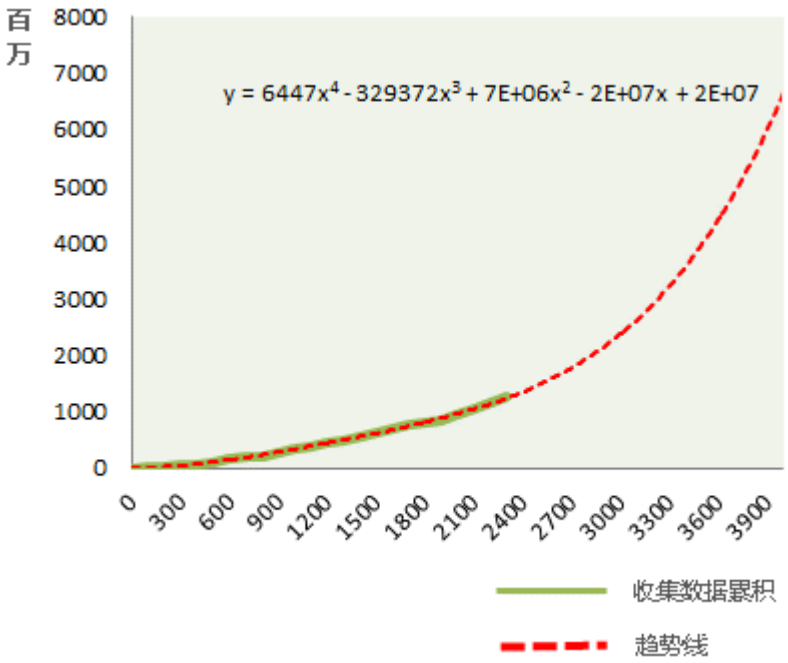
安全系统为什么需要应用机器学习？

【图 1】所示的是ASD(AhnLab Smart Defense)在2300天收集可执行(Portable Executable)文件的数量的累积曲线图。绿线表示累积收集数量，红色虚线表示趋势。



【图 1】ASD收集的可执行文件数量和趋势(X轴：天，Y轴：数量，单位：百万)

【图 1】所示，利用n次多项式可以创建误差极小的趋势线。即，通过n次多项式可以知道今天的流入增加量大于昨天的流入增加量。这意味着，在已构筑恶意软件分析人力和物力系统的前提下，今天至少需要比昨天更多的资源，其增加量随着时间越来越增加。如果在上述图预测4,000天的趋势，其结果如【图 2】所示。



【图 2】预测4,000天的趋势图

从【图 2】中可以看出，由n次多项式表现的趋势线在某一时刻爆炸性地增加。表示实际累积数量的绿线和表示趋势的红线之间存在间隔，使得实际曲线与预测的趋势线不完全重叠。然而，重要的是，总会有一天发生实际数据如趋势线的数据相同。我们将这一天叫做“命运之日”，而这一天正等待着我们。

如此，对于“昨天的流入量大于今天的流入量”的问题，以当前的模式构成的恶意软件分析系统可以持续多久呢？为了解决这个问题，更有效的方法是最大投入物理系统来支援人力资源。物理系统，即机械方式可以当作是通过人的经验构成的启发式的一个例子，但这种方式也不适合来防备“命运之日”。

为解决这个问题的几个选项之一就是“机器学习”。机器学习是一个具有弹性的系统，仅利用机械产生的规则，并对于机械很难完成的高水准的分析工作，先由人研究后再转达“机器学习”相关的知识。

总之，对于“为何需要机器学习来应对安全威胁？”的回答如【表 1】所示。即，机器学习作为能满足下列要求的几个选项之一，可以选择的。

- 需要应对“命运之日”。
- 人类对安全威胁分析的处理量有限，需要机械手段。
- 除了基于特征码来识别恶意软件，还需要基于规则来防御新的恶意软件。
- 安全公司可以更积极地收集样品，以应对安全威胁。
- 可以弹性应对新的和变种恶意软件的攻击。
- 提交客户的报告中包含的信息有必要更加多样。

[表 1] 为应对安全威胁，需要引进机器学习的理由

如果已经了解到机器学习的必要性，现在让我们来看看AhnLab是如何应用机器学习技术，并简单介绍其应用结果。

AhnLab机器学习系统

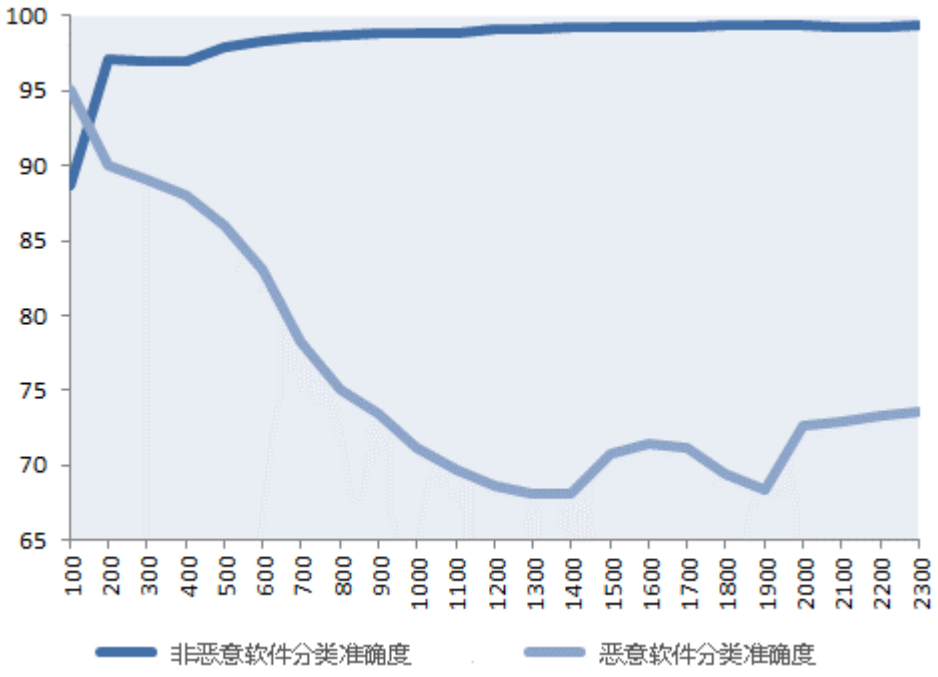
AhnLab花了两年的时间独自研发机器学习系统并已在运行中。该系统的整体运行过程如【表 2】所示。

1) 机器学习开始于将保存在ASD系统的PE文件作为学习对象。
2) 扫描PE文件中的学习信息后，生成数据。
3) 根据提取的信息，并利用下面的算法持续进行学习。
   A. 主算法使用“决策树(Decision Tree)”。
   B. 使用辅助算法“PLANT”来执行增量学习(Incremental learning)。
   C. 部分更新以前的学习结果模型。

【表 2】AhnLab机器学习系统运行流程

首先，扫描ASD系统收集的PE文件以获得机器学习信息，然后生成学习数据。根据该数据执行机器学习，即反复执行【表 2】中的A、B、C。

通常的机器学习算法需要一定的内存空间和CPU(最近还包括GPU)，还有磁盘I/O资源。由于这些资源是有限的而不是无限，所以执行算法总是会存在约束，其中之一就是学习数据的大小。目前，AhnLab机器学习系统已经完成对于保存在ASD系统的约13.4亿个PE文件的学习。如果要一次学习13.4亿个学习数据，一般的系统是无法实现的(内存不足)。无论最近处理大数据的分布式系统(例如：Hadoop)有多先进，一次学习13.4亿数据是不容易的。因此，研发了一种算法。即，不是学习一次而是以一天单位对于流入的数据逐日学习，并自我更新模型的增量学习算法-PLANT，并且已成功完成实际运行。通过以此，超越了当前机器学习存在的局限，并能够减少对未来可预期的学习设备的向上扩张和向外扩展的忧虑。支持这些增量学习的决策数算法在机器学习领域的学术领域也是一个具有挑战性的主题，而AhnLab已成功地研发和应用。



【图 3】按日期的AhnLab机器学习系统的恶意文件分类累积准确度变化

【图 3】表示按日期的AhnLab机器学习系统的学习分类累积准确度变化。y轴表示分类准确度，以百分比(%)表示，x轴表示累积日期。当x轴为1,500时，恶意文件分类准确度显示70%左右。这意味着，经过对1,500天流入的PE文件的学习后，根据导出的模型对所有数据进行测试的结果，其准确度为70%。2,300天的准确度值是指对所有的PE文件(共13.4亿个)进行学习的结果，其恶意文件分类准确度为75%。即，在13.4亿个文件中，恶意文件大约有2.7亿个，约占所有文件的20%，其中70%的恶意文件可以正确分类。

该过程是根据分类成“恶意文件”和“非恶意文件”的数据执行机器学习的结果。“非恶意文件”规定为诊断结果不是恶意的正常文件和当前无法明确判断恶意与否的文件，还有目前正在确认中的无法知道其诊断结果的未知文件(Unknown File)。

一旦分明的是，除了恶意文件之外的分类随着时间的推移逐渐提高，几乎显示接近100%的分类准确度。而恶意文件分类准确度随着时间的推移逐渐下降，停留在70%的水准。【图 3】中，x轴为1,900时，可以看到恶意文件分类准确度稍微下降的部分。其原因之一可以看作是数据的突然趋势变化。换句话说，可以预测大概从1,900天开始出现了未被分类为现有学习模型的新型恶意软件。通常，在这种情况下，如果不支持增量学习，则分类准确度将随着时间的推移而降低。然而，在AhnLab机器学习系统根据自主研发的PLANT算法容纳并接受变化趋势，并成功克服了问题，并证实准确度再次恢复。

通过这种AhnLab机器学习系统完成的引擎目前被应用于智能威胁响应系统“AhnLab MDS”的Agent，并且被用于收集可疑文件功能。此外，AhnLab将应用范围扩大到MDS分析设备，并将继续扩大机器学习的应用技术。

总结

“机器学习”，已成为了当今IT行业的一个重要课题。因此，令人担忧的是，企业争先恐后地盲目地进入该行业，华而不实的机器学习项目如雨后春笋般地生起来。因为，终于浮出水面上的“人工智能”由于泡沫的崩溃再次出现“人工智能已经永远死亡”之说。

与此不同，AhnLab机器学习系统不是贸然制作的产物，而是从两年前开始AhnLab根据需要进行研究的结果。尤其，它并没有利用已知的有名的开放源码来设计，而是直接设计和创造人工智能算法，并且实现了人工智能研究成果，最终通过令人满意的结果应用到实际产品。

最后，抛出一个这样的问题。“人工智能可以抢夺人的饭碗？”笔者的想法是“或多或少是的”。但是，人所做的工作和机器所做的工作分明是不一样的，而我们必须积极地去接受这个事实。

即使一个天才创造了令人瞩目的“机器学习”算法，但是该系统看到“苹果落地”也绝对不可能导出“万有引力定律”。换句话说，具有直觉能力的终究还是只有人。机器也只是进行规则归纳的计算。所以，我们要做的是找出机器无法做的部分，将专注于那部分。

AhnLab

安全月刊

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