



## 网络安全：一场不对称的战争

哈尔滨安天科技集团股份有限公司



Hal Lonas

2017年8月28日

**要想领先于攻击者，安全团队需要像犯罪分子一样思考、利用人工智能（AI）的能力发现恶意威胁，并停止担心机器学习会取代我们的工作。**

在网络安全行业，我们都听过一句古老的格言：“防御者必须时刻警惕，而攻击者只需成功利用一个漏洞就行了。”

虽然这令人生畏，但这正是网络安全行业每天都要面对的现实。我们面临着一场不对称的战争，不幸的是，我们的对手是一大批拥有各种武器的网络犯罪分子。

像其它战场一样，网络空间的不对称战争可以描述为：一方只需要适度投资来实现收益，而另一方则必须投入大量资金来维持足够的防御。在网络安全行业，恶意软件和勒索软件的作者和推广者是前者，而安全行业和潜在受害者是后者。这种投入时间和资源的不平衡导致这场战争是不对称的。

我们以 WannaCry 勒索软件攻击为例。这是一个简单的



恶意软件，令人惊讶的是，它通过窃取的技术进行传播，感染了 40 多万台机器，攻击者几乎是毫不费力地实现了这一切。

网络犯罪分子富有创意，有能力测试新的攻击。同时，安全团队将资源投入到多层安全防御上，如网络分段和网络钓鱼培训。

这就出现了一个可怕的想法：当网络犯罪分子集中精力利用 AI 时会发生什么？

一旦攻击者掌握了 AI 技术，就会大规模渗透网络、窃取数据、传播能够导致设备瘫痪的计算机病毒。这可能会导致大规模军备竞赛，后果无法估量。足够聪明的 AI 能够清除电子邮件或网站被感染的迹象，这实在太可怕了。

虽然多态恶意软件（到达新机器后发生变形）有一些机器能力，但是这种恶意软件并非每日演变的。勒索软件几年前就出现了，到现在也没太大变化。我们经常看到受害者一次又一次地遭受同种类型的攻击。网络犯罪分子仍然可以用靠谱的工具制造混乱。

虽然我们无法预测网络犯罪分子下一步会做什么，但是一些人已经开始利用 AI 和机器学习来保护自己了。机器学



习并非银子弹，但是它正在快速成为领先犯罪分子，或至少快速检测最新的攻击类型的重要、必不可少的工具。它可以通过持续观察网络来提高安全性，并利用威胁研究团队的能力来创建一个整体大于各部分之和的解决方案。它设置一个基准，以帮助检测异常行为。但是想领先于攻击者，安全行业需要采取以下三个措施：

首先，我们要像网络犯罪分子一样思考。他们的主要动机很简单--赚钱。他们不断思考怎样用最小的行动产生最大的收益，因此他们非常喜欢网络钓鱼活动。他们可以轻松地发送数百万封电子邮件，将受害者重定向到伪造的网站并获得巨大的收益。网络犯罪分子可能会调整他们的方法，例如，伪装为技术公司而非金融机构（正如我们的《2017年威胁报告》所述），但是这些机制保持不变。如果我们利用机器学习来追踪和分类常规或日常任务，我们就可以腾出时间来像犯罪分子一样思考，并提出应对下一次攻击的解决方案。

第二，我们需要集成了AI技术的安全产品，利用AI固有的优势来发现恶意威胁。这些解决方案必须包含来自最佳威胁研究人员的情报和分析数据并发现进入企业的威胁的模型。这些解决方案可以是通用或特定的。如果我们可以为更多的公司制定计划，就能在对抗网络犯罪方面获得优势。



# 中国网络安全产业联盟

## China Cybersecurity Industry Alliance

最后，我们不用担心机器学习会取代我们的工作。真正的威胁来自于不利用机器学习，这种回避迫使您最好的研究员疲于应付繁琐的工作，无法创造性地思考问题、预测新的攻击形式并进行防御。机器学习能够为研究员提供帮助，使他们腾出手来处理更重要的问题。由于人类参与对于监控和塑造机器学习模型至关重要，这会导致就业岗位增加。

如果我们想公平竞争，就要利用机器学习创造一个更安全的世界。虽然网络犯罪分子目前可能不会广泛利用机器学习，但是他们迎头赶上也是迟早的事。当那一天到来时，世界各地的安全团队都要做好准备。

