2013 年关于针对性攻击的三個预测

作者： *Nart Villeneuve*（趋势科技资深安全研究员）

当前 ,关于针对性攻击 ,包括APT 高级持续性威胁(Advanced Persistent Threat, APT) 知识，已成为了安全界的主流。我预测到了 2013 年，我们的认知将会面临挑战。在过去几年，我们看到了一些所谓“技术上并不复杂”的攻击被成功运用，我预测这种状况仍然会继续，针对性攻击将尽可能的利用人为因素，从人的方面突破，不足之处再用技术手段弥补。

趋势科技 CTO *Raminud Genes* 在 2013 年安全威胁预测中认为，恶意软件的攻击将会变得越来越复杂。这并不一定是指恶意软件本身的技术复杂度，而是指恶意软件在攻击中的运用。此外，他认为这类攻击将更具有破坏力，并难以定性。基于这些观点，对于 2013 年的趋势预测如下：

1. **更多的特异性 APT 攻击。**随着一些 APT 攻击案例陆续被公开，其中所使用的技术和手法被更多人知晓和了解，从而我们预测这将导致更多的特异性目标攻击。我们预计区域性攻击将会增长，例如一些恶意软件将只会在一些特定条件满足的情况下才会执行，比如语言设置或者水坑式攻击。这些区域性攻击针对的都是特定的地理区域或特定的网段。

2. **更多据有破坏性的攻击。**当我们已经习惯性认为当前的针对性攻击的目的是为了进行间谍活动时，2013 年我们将看到更多更具有破坏能力的攻击。无论是攻击的主要目的还是为了销毁入侵证据。针对性攻击中所使用的恶意软件将更多的具有破坏性

质。这种破坏性的功能很可能被用在对时间敏感，例如具有军事或者政治目的的攻击中。

3. **更多具有迷惑性的攻击。**过去我们经常用一些简单的技术指标来判断针对性攻击的目的以及攻击源。但是在 2013 年我们应该更加深刻的认识到必须将社会，政治，经济指标与技术指标相关联。才能够更加充分与全面地对攻击进行评估和分析。但是能够做到这点，需要经过艰苦的努力，正如我预测的那样我们可能将会看到一些错误判定的案例。除了攻击者利用技术指标的知识，进行“假标签”操作，嫁祸其他目标。直接从经常对被攻击目标单位或以其名义发起欺骗操作（或疑似攻击）的增加，也会让攻击的属性模糊变更加难以判断。

增加对针对性攻击的知识，也是保护自己的最好的方式。不过攻击者也会去不断了解哪些手段已成为已知，并会利用这些信息。这些是否会改变攻防方式仍然有待观察。但是这些发展也将会是对我们关于针对性攻击的认识的挑战。

原文地址：
http://blog.trendmicro.com/trendlabs-security-intelligence/what-kind-of-targeted-attacks-will-we-see-in-2013/