工业控制系统如何防御高级持续性威胁(APT)的攻击？

很长时间以来，工业控制系统一直被认为不受网络攻击的影响，因为它们大多与互联网隔离。遗憾的是，情况不再如此。如今先进的网络攻击开始针对拥有极为重要信息的那些关键基础设施和组织，从而破坏大量的生产线，造成严重的经济损失和数据泄露。最近的研究表明，有针对性的攻击大都瞄准防御能力较弱的员工计算机或移动存储设备，因此控制可执行文件和防止网络中的未授权活动就显得至关重要。自 2011 年起，信息和网络安全行业已然面临着全新的挑战，即对抗高级持续性威胁（Advanced Persistent Threats，APT）。新型网络犯罪具有前所未有的周密计划、更加一致和更有针对性，主要针对政府机关和社会基础设施、信息通信产业、制造业、金融机关。下面我们将全面了解一下 APT 的真实面目，以及在工业系统中什么样的安全解决方案可以实现有效防范。

工业控制系统如何防御高级持续性威胁(APT)的攻击？

如今高级持续性威胁（Advanced Persistent Threat）已成为人尽皆知的"时髦术语"。自 2011 年起，在行业中已成为最热门的关键字。越来越多的企业开始对其高度关注，不仅是企业就连政府部门也面临着遭受 APT 攻击的危险。

众多企业和机构惨遭 APT 攻击的一个重要原因在于它们没有发现真正的漏洞所在并加以修复。我们要做的是，首先深入了解 APT 的核心要素，然后利用它来完善我们的安全举措。只要充分了解 APT 攻击性的威胁，企业和机构才能做到对症下药的修复漏洞，最终能防范 APT 的攻击。

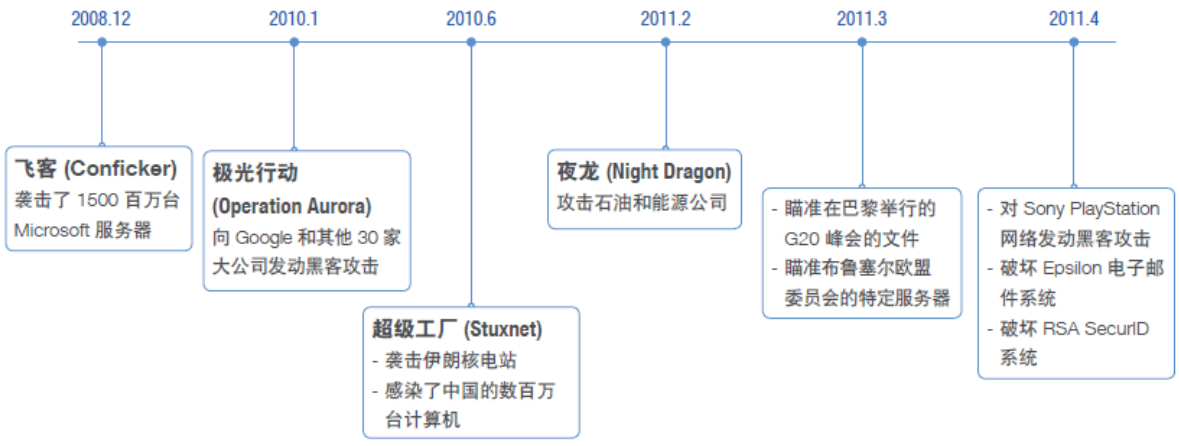
什么是 APT？

市面上出现了无数种有关 APT 的定义。某种程度上，美国国家标准及技术研究所给出的定义应该属于最客观。它是这样描述 APT 的： 它来自一名具备非常先进的专业技术拥有大量资源的对手。利用多种类型的攻击（如网络、物理以及欺诈等）创造出各种机会来完成既定的攻击任务。

顾名思义，这是一项非常高超的技术，它很有耐心地协调识别和利用现有漏洞的工作，从而渗透到目标组织的网络中。

APT 攻击与传统的针对性攻击在目标和目的方面有所不同。这些入侵会在受害者的网络中获得立足之地，有时候长达数年，有时候甚至在公司已经发现并采取补救措施之后，仍然无法将其清除。APT 攻击持续时间极长，许多企业直到安全漏洞和破坏发生之后才会注意到攻击症状。这表明 APT 攻击者很可能非常聪明、有充足的资金来源、有组织、坚持不懈且极有耐心。在当今世界，没有人可以免遭攻击。

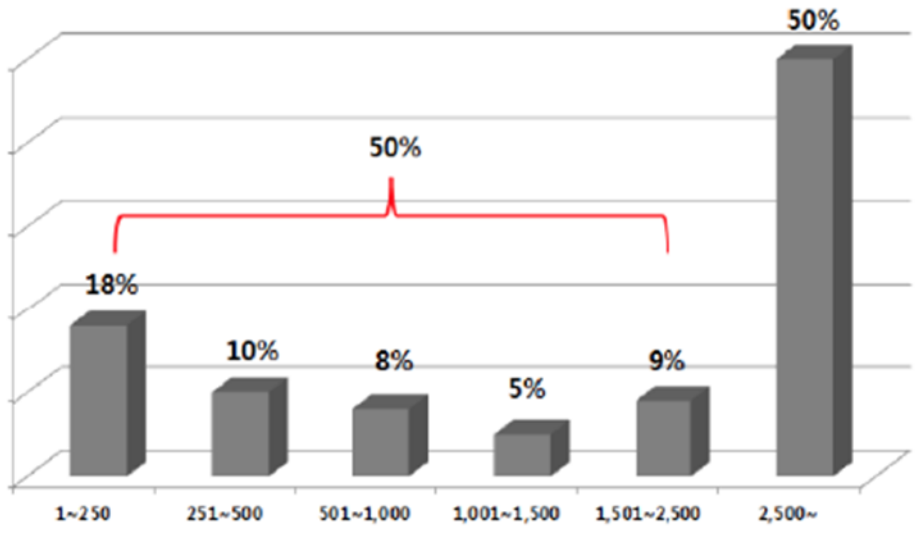
具有代表性的 APT 攻击有超级工厂(Stuxnet)、极光行动(Operation Aurora)、夜龙(Night Dragon)和 EMC/RSA。下面图显示 APT 攻击演变。



APT 攻击的演变

ATP 攻击只针对大企业?

中小企业是否可以躲过 APT 攻击？是否安全？我们可以说“NO”。通常人们认为公共机关或大企业会成为 APT 攻击的主要对象，实际在很多种规模的企业和机关曾报道 APT 攻击事件发生。根据赛门铁克资料显示，APT 攻击事件的百分之五十是在员工数不到 2,500 名的中小企业里发生；百分之二十是在员工数不到 250 名的中小企业里发生。



Internet Security Threat Report(来源：赛门铁克)

安博士发表对 APT 攻击的对策

国际综合安全解决方案公司安博士发表了最近最具有威胁性的 APT 攻击的对应方案。安博士表示为对付 APT 攻击，需要多方位的准备和应对。

1. 为应对APT攻击者收集基础信息，需要建立政策，控制组织内部信息和组织成员的身份信息并持续进行各种安全威胁的内外监控和日志分析。
2. 为应对恶意代码的入侵，必须定期进行有关安全方面的教育并管理和监督客户端计算机里安装的安全软件，以防止在访问P2P、网络硬盘和软件自动更新网站时被恶意代码感染。
3. 以企业内部检讨并授权程序为对象建立白名单（White List），阻止不在白名单里的程序的运行。通过权限设置，阻止未被确认或未授权帐户访问重要系统。而且分离重要系统所在网络带宽和普通职员使用的网络带宽，阻止访问重要系统的源头。
4. 为应对机密信息泄漏，需要定期进行计算机操作系统及应用程序漏洞修补和管理；通过访问控制防止信息泄漏；还要对数据进行加密处理，即使机密信息泄漏也不会恶意引用。

安博士公司强调对于如此高级的安全威胁的模式变化，需要构成全方位的融合安全体系来加强安全。融合安全体系是指，对于外部恶意攻击和内部信息泄漏，可以同时监控及应对的综合的响应对策。

安博士提出的融合安全体系始发于 2009 年开始准备的'ACCESS(AhnLab Cloud Computing E-Service)'战略。ACCESS 是一个技术平台，以智能型技术支援 ASEC(安博士安全中心)的恶意代码收集和分析，CERT(计算机应急响应组)的威胁监控及响应服务。不仅可以实时收集、检测和修复恶意代码和黑客手法，还可以生成恶意代码数据库，实时联系 ASEC、CERT、产品及服务，达到迅速和正确的综合响应。

安博士公司包括 V3(端点 PC 安全解决方案)和 TrusGuard(网络安全解决方案)，结合 TrusWatcher(僵尸 PC 防御解决方案)、TrusLine(基于白名单的工业系统专用安全解决方案)和 TrusZone(网隔离解决方案)等多种产品，提出了应对 APT 攻击的对策。

工业系统面临的安全威胁

很长时间以来，工业控制系统一直被认为不受网络攻击的影响，因为它们大多与互联网隔离。遗憾的是，情况不再如此。如今先进的网络攻击开始针对拥有极为重要信息的那些关键基础设施和组织，从而破坏大量的生产线，造成严重的经济损失和数据泄露。最近的研究表明，有针对性的攻击大都瞄准防御能力较弱的员工计算机或移动存储设备，因此控制可执行文件和防止网络中的未授权活动就显得至关重要。自 2011 年起，信息和网络安全行业已然面临着全新的挑战，即对抗高级持续性威胁(APT)。新型网络犯罪具有前所未有的周密计划、更加一致和更有针对性，主要针对政府机关和社会基础设施、信息通信产业、制造业、金融机关。

生产线上的任何延迟或中断都会导致财务损失。基于这个原因，许多制造商都在生产设施中使用以传统方式管理的封闭式网络。如果不是绝对必要，则避免进行计算机或软件升级。

在这些类型的工业环境中，尽可能减少或阻止封闭式网络外部的连接是防止入侵和攻击的主要方法。但是在 2010 年，Stuxnet 证明了即使是物理隔离的网络也容易受到黑客的攻击。

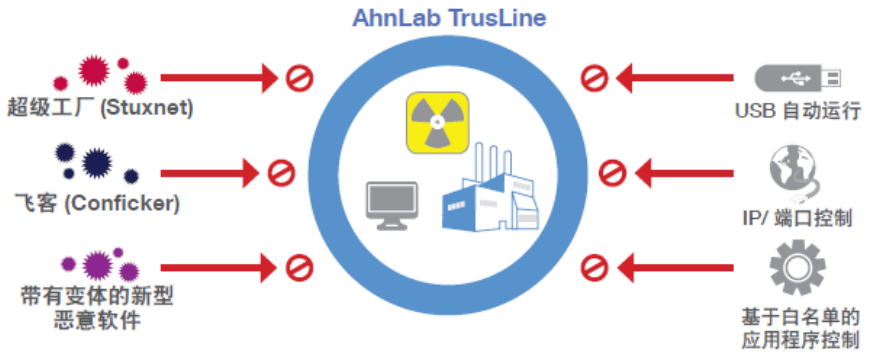
工业系统专用安全解决方案-TrusLine

专门针对工业系统的 TrusLine 采用白名单方式提供对端点的完全控制。它会阻止不在白名单中的所有程序的运行，从而提高系统的全方位安全并减少维护要求，并且不影响系统的正常运行。

TrusLine 可应用于半导体、LCD、汽车等生产线的工业用系统和百货店、购物广场和便利店等销售系统，保障系统的稳定运行。

在安博士于 2010 年 9 月发布 TrusLine 之前，市场上没有专门为工业系统量身定做的安全解决方案。“我们一直都知道我们需要为我们的工业系统采用安全解决方案， 但是苦于找不到这样的解决方案” LG 伊诺特的 GwangYong Cheon 解释说。不只是他们遇到这个问题，他们的下属公司也正在为其生产设施寻找类似的保护措施。

2012 年 4 月 17 日，AhnLab TrusLine 产品的两种新技术在国内（韩国）取得了专利并申请了国际专利。专利技术名称为“拦截恶意代码感染的设备及系统和方法”和“拦截利用可执行文件的恶意代码的设备及其方法”。这两种技术可以在低配置的系统利用较少资源有效拦截恶意代码的感染。



AhnLab TrusLine 的防御

传统的端点安全解决方案依赖于黑名单来检测已知恶意软件，而 TrusLine 通过仅允许白名单中授权的程序运行来保护端点。这种方法提供了最佳的全方位的解决方案，以确保网络的完整性：阻止进入系统内部的攻击，减少潜在的损害金额，最大限度减少操作中断，并防止数据泄露。

AhnLab TrusLine		传统的反恶意软件解决方案
主动防御	响应	被动响应
白名单（仅允许授权应用程序）	应用程序控制	黑名单（已知恶意软件应用程序）
封闭式网络	环境	互联网访问环境
固定不变	引擎大小	不断要求额外的资源
低	资源占用率	高
高	安全等级	低
极少的升级和修补	维护	需要频繁更新

应用程序白名单的优势

结束语

TrusLine 已在韩国多数大企业使用并受到好评。如三星电子和 LG 电子和海力士半导体等，还有它们的协作工厂。近年，TrusLine 产品已打进中国市场。对于前所未有的工业系统专用安全解决方案，中国企业安全负责人很是看好，已在多数大企业构筑了 TrusLine 安全解决方案。为响应中国市场需要，安博士决定打造专为中国市场的 TrusLine 产品，目前已经开始研发，计划明年初可以面向中国市场。

APT 攻击不会减少反而会变得更加精准和复杂。随着 APT 攻击的不断发展，工业系统也不断受到威胁。因此，需要组织实施更好的 IT 策略，以及进行有关网络安全策略的更多培训。除此之外，还需要像 TrusLine 之类的工业系统专用安全解决方案来防御恶意代码的攻击并保护系统。

TrusLine 是适用于 365 天不间断运行的生产及销售环境的最佳安全解决方案。不仅在韩国，在海外也受到了瞩目。我们期待它将引导安博士技术的国际化。

关于安博士（AhnLab, Inc.）

安博士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。

安博士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。

公司主页：www.ahn.com.cn
E-mail：support@ahn.com.cn
电话：86-10-8260-0935
地址：(201103)北京市朝阳区酒仙桥甲12 号电子城科技大厦 1206 室

AhnLab