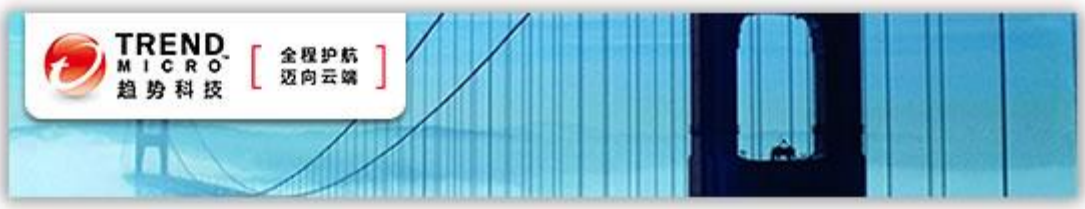

[趋势科技成功案例]

TDA 精准定位威胁源头 趋势科技携手华晨金杯谨防 APT 攻击

近年来，汽车制造行业的信息化建设已成为国内外汽车产业发展的热点，依靠网络平台凝聚整体竞争力正在成为企业战略发展的核心。然而，随着业务与网络的黏合度不断提升，网络安全的重要性也日益突显。在这一背景下，像华晨金杯汽车有限公司（以下简称华晨金杯）这样拥有复杂信息化系统的用户而言，及时发现 IT 环境中的漏洞，第一时间消除威胁已成为了保证网络安全、业务稳定的关键。

安全管理容不得威胁升级

具有自主品牌的国产汽车，坚持走自主研发之路，是华晨金杯立于汽车行业激烈竞争中的制胜武器。随着自主研发的多套信息化系统在采购、研发、财务、销售和物流各个环节的实施，确保业务系统安全稳定的运行，以及千余个企业 PC 端点的网络安全成为了 IT 运维工程师的重要责任。

华晨金杯网络安全负责人孙磊先生认为：“不管是设备层面、系统层面，还是应用层面，企业都需要建立一套有效的防护策略，而华晨金杯正是出于整体安全的考虑，建立与之配套的安全防护体系。但随着病毒黑色产业链的不断发展，恶意 Web 地址链接、钓鱼网站及裹挟着社交工程学的黑客攻击不断增多，单一的基于终端防毒的防护架构已经不能应对上述的威胁。尤其是对于华晨金杯如此庞大的内网终端数量而言，威胁有可能潜伏下来，并且有可能在某一时间点突然爆发。因此，我们在安全防御体系下，最重要的是发现和阻断这些潜在的威胁，只有这样才能将企业的核心数据外泄风险降到最低。”

随着黑客、木马、病毒、垃圾邮件在互联网上的泛滥，华晨金杯依据自身特点，并结合国际上成熟的 IT 安全管理框架，分阶段完成了信息安全管理体系的建设。在这套管理体系中，对 IT 人员的管理提出了非常严格的要求，而在这种要求下，大量终端的“防漏补差”工作消耗了大量的人力成本。尤其是一些普通用户使用的终端，这些终端很有可能受到 Web 木马陷阱的攻击，当无心点击一些被挂马的网站链接后，恶意代码会从浏览器侵蚀进来，伺机

作案。因此，如何进一步完善安全防护体系、如何挖掘防毒软件的作用、如何将威胁消除在萌芽状态？这些问题逐个摆在了华晨金杯 IT 安全管理人员的眼前。

TDA 可发挥防毒系统的联动功能

趋势科技作为服务器安全、虚拟化及云计算安全的领导厂商 ,服务于全球各大汽车制造厂商，而华晨金杯与趋势科技的合作从 2006 年开始至今也从未间断过。在考察了网络安全市场的各种终端威胁防御系统之后，华晨金杯最终还是感觉到趋势科技威胁管理解决方案中的 Threat Discovery Appliance（简称 TDA）最能符合信息安全整体框架的要求。

这是因为在针对威胁的入侵防御方面，TDA 与 IDS、IPS 这些产品有着本质上的区别，并且涵盖了传统安全设备无法实现的多重协议侦测、直接预警分析、零日攻击、未知病毒检测、专门针对内部网络的功能设计，以及最重要的根源分析功能。

孙磊先生表示，除去上述有代表性的功能之外，还有三点最能说明问题："首先，在长期使用趋势科技 OfficeScan 网络版的过程中，产品的防护能力和配套的服务水平都让我们十分满意。其次，从防病毒产品的兼容性和采购管理方面考虑，延续与趋势科技的再度合作存在一定程度的便利性。最后，趋势科技作为防病毒产品领域的国际领军企业，其基于云安全的产品对于最新的威胁攻击能够实现有效的防护，通过 TDA 这样的威胁发现产品，可以与 OfficeScan 网络版对风险形成联动管控。"

据了解，在部署 TDA 之前，在华晨金杯内网中部署的监控系统，对于网络流量的管理主要是依靠 IP 地址或主机名信息为主。而这种手工定位病毒源头的方式，将会失去阻断病毒的最佳时机，而且这些恶意代码可能从一个子网泛滥到另一个子网，让 IT 管理者十分担心引发连锁问题。而在部署 TDA 之后，可以实现对病毒源头的自动定位，在第一时间通知管理员，并启动防毒软件的联动功能。由于和 OfficeScan 一样，TDA 也使用了趋势科技独有的"云安全"技术，两者通过有效的组合，当恶意程序在网络中传播感染其它用户时，它们就会被打上"特殊标记"明确分工，TDA 负责发现和阻断，而 OfficeScan 负责查杀与修补。

精细化管理谨防 APT 攻击

对于 TDA 和 OfficeScan 联动功能的实现 ,华晨金杯表示不但达到了预期的效果 ,并且 TDA 的报表功能也使得安全管理变得更加精细化。孙磊先生表示："对于现在流行的高级持续性威胁（Advanced Persistent Threat，简写 APT)）攻击，华晨金杯网络部门非常重视，但现在市面上没有单独防御此类社交攻击的设备 ,因此最有效的防御手段就是要把管理做到细化。利用 TDA 的流量分析功能，我们迅速找到了隐藏于网络中的高风险节点，并根据趋势

科技整合在 TDA 报告中的解决方案，把这些潜伏下来的恶意代码一一清扫出了网络。”

事实证明，华晨金杯利用 TDA 实现的精细化管理，以及针对 APT 攻击所采取的预防手段，在今天这样一个威胁无处不在的网络中，具有十分显见的借鉴作用。如果企业用户怀疑已经遭遇了 APT 攻击，那么，通过网络流量的细微变化即可发现 APT 的破绽。这是因为，狡猾的黑客为了盗取有价值的商业数据，会在受攻击目标的内部建立更多的立足点，而当其通过企业内部的交换机时，就很容易被趋势科技的威胁发现设备 TDA 揪出来。