安博士月刊

星 期 三
2月 20日
2 0 1 3年

Vol.6

【安博士月刊】是综合安全解决方案公司-安博士公司发行的网络安全信息月刊。

您是否已准备好迎接“APT时代”？

当今各种先进的攻击来自多种途径，攻击手段日益复杂且攻击目标日益广泛，这使传统解决方案无力应对。 高级持续性威胁（APT）攻击中使用的恶意软件不是通用的，而是为了侵入目标组织的网络而专门设计的。

Gartner[1] 报告中这样描述当前的安全威胁： “攻击者越来越专注于在电子邮件和 Web 事务中加入恶意内容，以便破坏您的安全系统并突破您现有的安全控制。” [2] 结果就是， “出现了更新型的攻击和有效载荷传输技术，该技术可以绕过这些传统的基于签名的方法，因此必须通过新兴的安全技术加以解决，同时这也扩充了我们对传统安全技术的陈旧思考方式。” [3]

很显然，在当今的环境中，有效的安全战略需要比以往任何时候都更加先进的防护元素。

非常诱人，但却是致命的： 量身定制的攻击结合了电子邮件和社会工程技术

采用社会工程和常见文件类型的攻击是不断增加的众多 APT 类型中的一种。 最近的攻击趋势主要集中于通过电子邮件侵入目标系统并利用 DOC、PDF、XLS 和其他广泛使用的文件格式中的漏洞的威胁。与较早的攻击方式（例如向公众批量发送电子邮件）不同，当今的 APT 专门针对特定组织、机构或公司中的已知个人发动攻击。这些量身定制的电子邮件具有一些共同的特征，都是专门针对目标环境所设计，企图提高成功攻击的可能性：

- 有吸引力或显得很重要的主题行
- 诱人或显得很重要的附件，但其中包含对常见文件类型的攻击
- 电子邮件中有限的正文内容，鼓励攻击目标打开附件

如果有人使用未修补的应用程序打开附件，则会创建恶意文件并且目标系统将被感染。 受害者很少能够注意到他们的系统受到感染，因为他们所做的不过是打开看起来很普通的文件附件而已。 如果缺少额外的保护层，则几乎不可能知道附件是恶意的。 从国防工业观察到的情况来看，当打开这些类型的附件时（例如，使用未修补的 PDF 阅读器），恶意代码随即注入以下路径：

- C:\Documents and Settings\[user]\startmenu\program\start program\ld.exe
- C:\Documents and Settings\[user]\Local Settings\Temp\AdobeARM.dll

1 Gartner (NYSE: IT and ITB)全球最具权威的IT研究与顾问咨询公司，成立于1979年，总部设在美国康涅狄克州斯坦福。其研究范围复盖全部IT产业，就IT的研究、发展、评估、应用、市场等领域，为客户提供客观、公正的论证报告及市场调研报告，协助客户进行市场分析、技术选择、项目论证、投资决策。为决策者在投资风险和管理、营销策略、发展方向等重大问题上提供重要咨询建议，帮助决策者作出正确抉择。（来源：百度百科）

2 Best Practices for Mitigating Advanced Persistent Threats , Gartner Inc. , G00224682 , 2012年 1月 18日

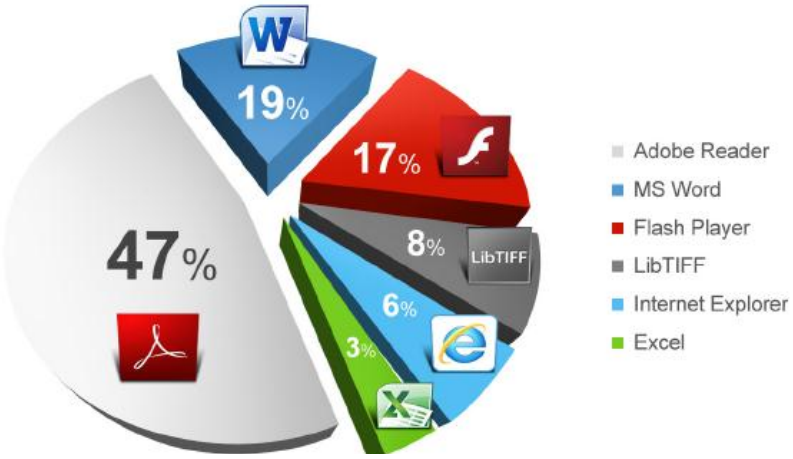
3 Best Practices for Mitigating Advanced Persistent Threats , Gartner Inc. , G00224682 , 2012年 1月 18日

恶意代码被添加到启动例程中，因此每次启动计算机时它都会运行。它还会定期连接到 C&C 服务器，从而实际上将计算机变成由远程攻击者控制的“僵尸”。

例如，在 2011年 3月的 RSA Security®公司违规行为中，一位员工打开了标题为“2011 Recruitment plan.xls”的电子表格，该表格包含嵌入式 Adobe® Flash® 漏洞。该漏洞允许远程攻击者获得该员工计算机的完全控制权，最终访问了 RSA 网络中的其他计算机，然后将敏感数据传输到外部服务器。几个月后，从 RSA 偷走的信息又被用于对国防承包商 Lockheed Martin 发动攻击。

从上述情况可以看出，APT攻击不限于对攻击目标造成损害。利用目标展开更加广泛的攻击，攻击目标反而成为APT攻击的一个关键的垫脚石。

图 1 利用应用程序漏洞的威胁



来源：安博士

基于签名的保护不起作用，因为攻击通常是量身定制的，隐藏在攻击后面的黑客攻击目标应用程序中之前未发现的漏洞。

猫鼠游戏：零时差攻击

许多公司都表示了对 APT的担忧，因为此类攻击利用业务环境中常用应用程序的漏洞。在软件发布者发布安全修补程序之前，用户必须非常谨慎以防止他们的系统受到感染。根据 Gartner 副总裁 Neil MacDonald 和 Gartner 调查部总监 Lawrence Pingree 的观点，“到 2020年，75% 的企业信息安全预算将分配给快速检测和响应方法，而在 2012 年这一比例还不到 10%。”[4]

根据安博士近期对字处理文件中发现的恶意软件示例的分析来看，恶意软件文件从外表看起来和普通文件没什么两样，但是一旦打开，就会发现它包含许多恶意代码。 恶意软件内嵌以下恶意文件，每个文件都具有特定的角色：

- %Systemroot%\system32\rundir.dll
- %Systemroot%\hwprnt.dl
- %Systemroot%\system32\soric.rxc
- %Systemroot%\system32\comirv.dll

在此特定示例中，rundir.dll 文件使用名称“Themas”注册为服务 — 故意将“Themes”稍微拼错以帮助避开检测。该服务在系统启动时自动启动，一旦开始运行，它就会关闭防火墙设置并将 comirv.dll 文件注入 Windows 资源管理器的可执行文件 (explorer.exe)。

4 Security 2020: Technology, Business and Threat Discontinuities That Will Reshape Information Security , Gartner Security & Risk Management Summit , 2012年 6月 11日~6月 14日

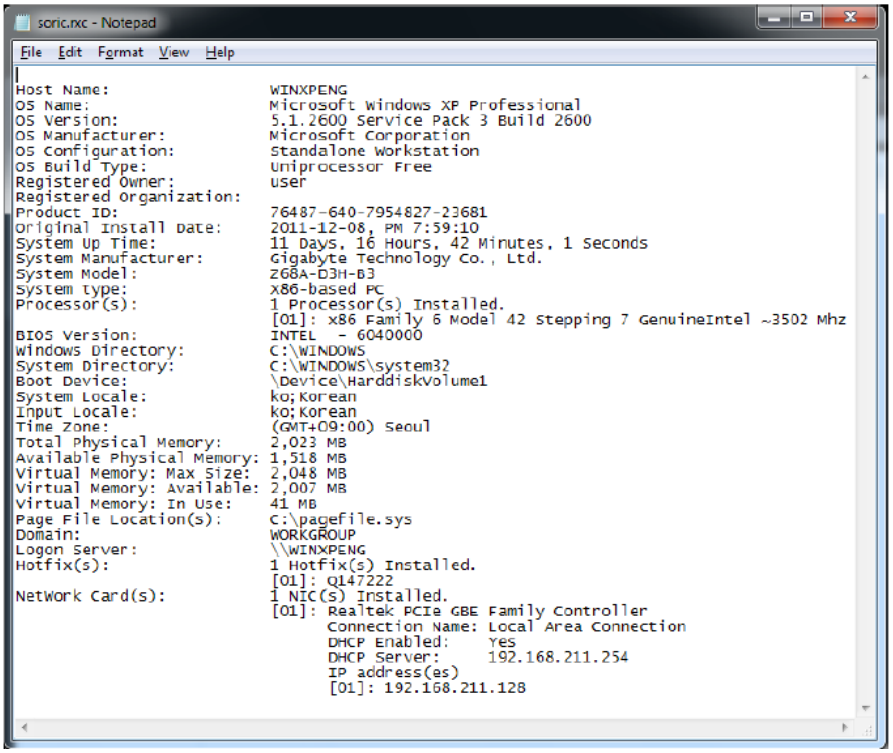
了解您的敌人： 安博士的新一代 APT 防御战略

新一代的威胁防御要求分四个阶段来防范先进的、有针对性的攻击： (1) 检测新兴的恶意软件、(2) 识别未知的恶意软件、(3) 完全删除发现的威胁，以及 (4) 持续监控可疑活动。

云智能的强大功能

威胁当今 IT 世界的先进的网络攻击势头要求更深入的洞察力、更全面的知识以及更及时的威胁防范行动。配合安博士云计算应急安全服务 (ACCESS)，可以从世界各地的数百万部传感器收集最新的网络威胁数据。这种有关网络威胁的全球智能使安博士能够利用广泛的新兴威胁数据库，并更准确地识别合法文件，减少误报和漏报。另外，无需浪费时间分析已知恶意软件和合法文件。

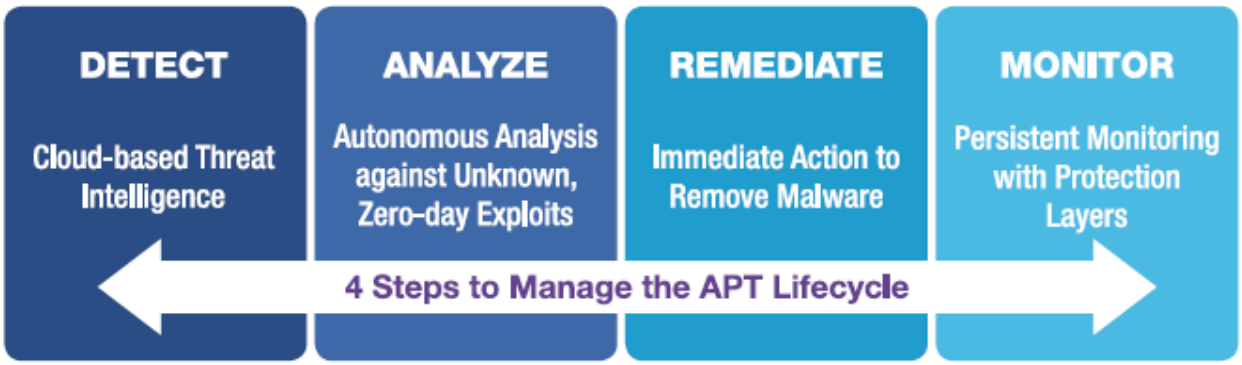
图 2 soric.rxc 文件的内容



来源：安博士

安博士的威胁防御策略充分利用这一重要资源。 正如安博士安全应急响应中心 (ASEC) 总监 Luke Lee 先生所言，“进入公司网络的超过 80% 的恶意软件都会被我们基于云的智能功能及时挡在门外。”

图 3 新一代威胁防御的生命周期



来源：安博士

多个自主诊断引擎

当今 APT 中使用的恶意软件都是为了侵入目标组织的网络而专门设计的。这些类型的有针对性的攻击需要及时且自动化的应对措施。

安博士提供了自主诊断功能，可实时动态识别未知的恶意软件。这种保护技术基于多个分层的分析引擎，可检测与有害网站的连接、C&C 通信通道流量和 DDoS 流量，以及机箱内的虚拟机上的 OS更改。这种不依赖于签名的方法可快速发现之前未遇到过的恶意软件的可疑行为，并使网络管理员快速采取行动保护公司网络。

"进入公司网络的超过 80% 的恶意软件都会被我们基于云的智能功能及时挡在门外。"

- Luke Lee 先生，ASEC 总监

"通过对多个保护机制进行分层，安博士的防御策略可以将恶意软件挡在门外，防止您的敏感数据受到影响。"

- Sangln Yoon 先生，安博士产品经理

动态内容分析以防御零时差攻击

随着结合网络钓鱼活动和文档漏洞的攻击方法的不断增多，市场上推出了许多解决方案来检测利用常见应用程序中的漏洞的恶意软件。根据 Gartner 分析师 Peter Firstbrook 的观点，"检测先进的、有针对性的附件恶意软件的方法可分为两大类：

- 静态代码分析： 读取文件以检测并删除可疑命令或代码块。大多数供应商都至少执行一定程度的静态分析，这使在不测试解决方案的情况下很难比较这些解决方案。
- 动态代码分析： 在沙盒环境中执行代码以检测恶意行为。"[5]

由于各应用程序版本具有不同的功能和特性，因此只通过静态代码分析不足以检测所有的恶意软件，包括利用零时差漏洞的变体。这就是为什么安博士提供的检测方法胜过许多其他安全供应商提供的传统检测方法，从而推动行业发展的原因所在。

正在申请专利的动态智能内容分析 (DICA) 技术通过采用安博士独特的 Shell 代码检测技术显著缩短了分析时间。通常，Shell 代码会注入格式错误的文档或多媒体文件，以运行攻击者可以从中控制受感染计算机的命令 Shell。如果在打开文件时检测到 Shell 代码，则可以将其归类为可疑文件，因为正常文件不应包含 Shell 代码。DICA 技术实时捕获注入的 Shell 代码，而不考虑应用程序版本。

应对长期威胁的智能端点控制

一旦发现威胁，您肯定不愿意让风险多停留一秒钟。 由于 APT 可能很长时间都检测不出来，同时暗地里提升权限以获得对关键系统的访问权限，因此一次修复可能不足以解决威胁。 为了克服这一难题，安博士使用其修复和监控功能，甚至可以在端点已经受到攻击的情况下保护网络。

安装在端点上的代理直接与防 APT 系统通信，并执行命令以搜索和删除恶意软件。 管理员可以使用高级端点控制功能密切监控感染情况。 任何可疑活动都能得到收集、传输和分析，就像它第一次进入网络一样。 这种智能控制意味着恶意软件无法在您的网络中立足。

在应对来自多方面的威胁的同时控制成本

恶意软件通过多种途径持续威胁着网络，例如网络流量、电子邮件、ftp、即时消息等等。 为了解决这些威胁，公司 IT 预算必须不断增加以便针对各个途径提供专门的检测。这一负担导致大量的 IT 行政和管理开销，如 Deloitte 2011 年的报表所述。他们对各个行业和组织规模的 CIO 开展的一项在线调查显示，降低 IT 成本是 CIO 的首要任务之一。[6]

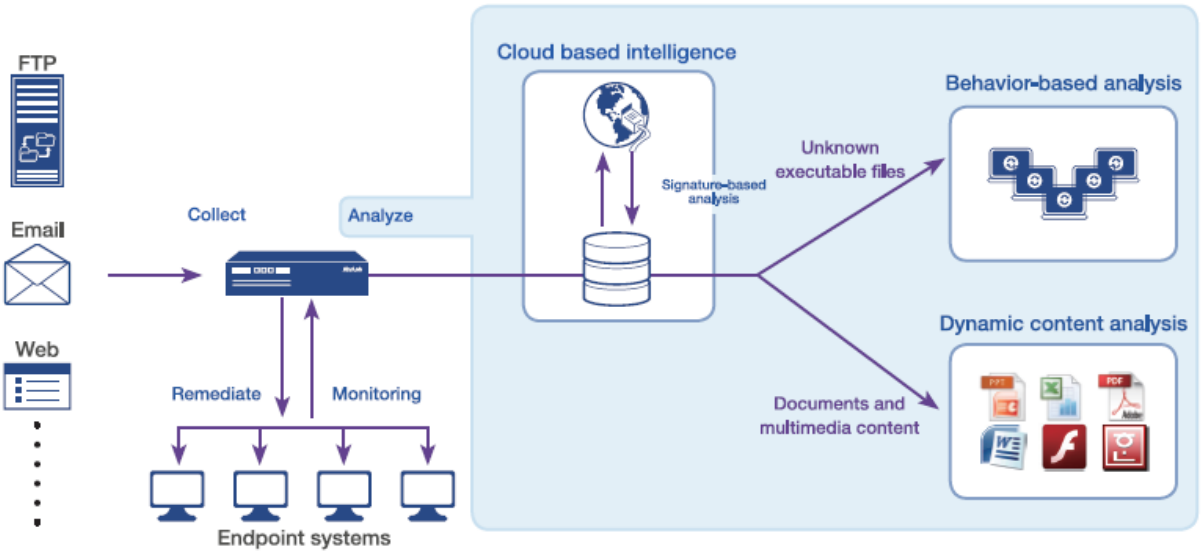
一个有效的网络安全策略必须在确保稳妥地保护公司的宝贵数据免受恶意攻击的同时考虑到效率。 安博士将针对所有协议的监控功能集成到单个平台中，从而真真切切地实现了该目的。 由于它使用单台装置检测 Web 中的 HTTP 流量和电子邮件的 SMTP/POP3/IMAP 流量，因此易于部署和管理，并且降低了总拥有成本，从而通过更快的投资回报 (ROI) 为您的公司带来长期价值。

---

5 Email Security Focus Shifts to Address the Risks of Targeted Attacks and Data Loss，Gartner Inc.，G00232491，2012 年 8 月 29 日

6 "CIO Survey Report 2011" Deloitte, 2011

图 4 安博士专用的 APT 防御系统



来源：安博士

安博士的优势： 更高的可见性，更少的不确定性

在“APT 时代”，需要理解的最重要的事情之一就是“隐匿性”。 这些无声的威胁经常包含巧妙伪装的电子邮件和专门定制的恶意软件，以组织的敏感或机密信息为目标发动攻击。
由于它们通常藏匿于网络中，所以许多组织直到数月甚至数年后才知道自己是受害者。
通过捕获 APT 的任何蛛丝马迹，公司可以采用更佳的对策，防止长期的数据被盗或破坏的毁灭性后果。
防 APT 解决方案的目标是提供安全威胁和恶意通信流的更高可见性，同时保持合理的开销和运营成本。

“凭借我们的安全战略的完整性和敏捷性，我们可以通过更快的投资回报为客户的业务带来长期价值。”

- Vincent Lee 先生，
安博士销售和市场营销经理

通过四阶段的防御生命周期和高级端点控制，安博士可保护您的网络免遭复杂威胁的侵害。
即使您的网络已经受到威胁，我们仍然可以帮助您找出发生感染的时间和位置、恶意软件源自何处，以及它如何侵入您的网络。 最值得一提的是，安博士提供的可见性可以让您确信威胁已经消除。

“我们在防恶意软件行业丰富的经验，加上我们尖端的技术，可帮助组织针对当今先进的威胁保护他们的业务。”

- HongSun Kim 先生，
安博士执行总裁

请记住!
不能只是因为您看不见威胁，就认为不存在威胁。 通过获得可见性掌控局势并准备好迎接“APT 时代”。

来源： 安博士

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。

www.ahn.com.cn / v3site@ahn.com.cn / 电话：010-8260-0935
北京市朝阳区酒仙桥甲 12 号电子城科技大厦 1206 室