\

技术白皮书

天阗高级持续性威胁检测与管理系统 V2.0

APT 检测系列

未知威胁有效检测

目录

一. 前言 4

二. 为什么需要 APT 检测 6

2.1 专业级黑客攻击不断浮出水面 6

2.2 高级持续威胁攻击的主要特征 8

2.3 专业黑客攻击不断挑战传统安全设备 9

三. 如何评价 APT 检测系统 11

四. 天阗 APT 检测解决的主要问题 12

4.1 系统的目标和定位 12

4.2 弥补网络安全设备检测深度不够的问题 12

4.3 识别未知漏洞利用或逃逸触发的攻击 13

4.4 识别利用已知和未知漏洞的文件攻击行为 14

4.5 记录高级持续威胁的攻击行为还原真相 15

五. 天阗 APT 检测系统主要功能特性 16

5.1 天阗 APT 检测系统的架构 16

5.2 支持两种待检测文件接收方式 16

5.3 全面支持已知威胁检测 17

5.4 对恶意文件的静态检测 17

5.5 对恶意文件的动态检测 19

5.6 对多种文件格式的检测 20

5.7 支持 SPAN/TAP 部署模式 20

5.8 对加密协议进行检测 21

5.9 YARA 规则检测 21

5.10 对 PCAP 文件回溯检测 21

5.11 基于邮件钓鱼场景检测 21

5.12 基于 WEB 水坑攻击场景检测.....21

六. 系统主要优势.....22

6.1 集成已知检测，精确检测网络威胁.....22

6.2 动态静态检测，让恶意代码无处遁形.....22

6.3 威胁情报应用，快速精准发现攻击威胁.....24

6.4 紧跟安全趋势，全面支持 ATT&CK 模型.....25

6.5 系统环境构造，提高检测粒度和精度.....27

6.6 独有反沙箱检测技术，让恶意威胁无处逃逸.....28

6.7 隐秘通道感知，让信息外泄有效避免.....28

6.8 简洁报告设计，让复杂问题简单易懂.....30

6.9 检测调度智能，检测性能计算效率提升.....33

6.10 跨界设备联动，抵御未知威胁和攻击.....33

七. 部署和解决方案.....34

八. 结论.....35

一. 前言

2017 年，各个有针对性的 APT 组织尤为活跃，这或许与今年被频繁曝光的各类高危漏洞有关。在 APT 组织攻击目标中，政府部门最受青睐，其次为金融行业。“海莲花”，“白象”，“蔓灵花” 等 APT 组织持续对我国政府机构进行攻击， 经济发达地区成为 APT 攻击的重灾区。国内部分厂商已提供基于动态沙箱检测技术的产品，其主要技术路线为：

- 代码仿真分析技术

在恶意代码运行时追踪恶意代码的行为，能够高效的捕捉到异常行为。这种方法允许在真实环境中运行，但是一旦恶意代码失控，将会感染真实主机，造成不必要的损失。因此，使用代码仿真分析技术模拟真实环境，将是一个非常好的选择。

- 行为监控分析技术

行为监控分析技术是通过监控、记录目标程序的各种类型的行为，根据其对系统产生的负面影响的程度来判定其是否为恶意代码。 行为监控分析技术按照分析的行为类型可以分为网络行为分析和主机行为分析。

网络行为分析是通过分析目标程序在网络中的通信行为来判定其恶意性的。传统的网络通信行为分析的方法是深度包检测技术，即从网络层和传输层两个层面分析恶意代码行为，并提取能够有效描述恶意代码行为的四个特征，用正则表达式匹配攻击模式检测木马程序，从而识别出恶意代码，但是当网络流量数据巨大的时候，无法及时分析出结果。

主机行为分析是依据恶意程序的恶意行为，如 API 调用序列、参数的依赖轮廓等，来对目标程序进行判断。运用的比较好的模型，是通过组合对应权限下用户可能的操作构建的攻击树模型，在基础的攻击树模型上增加危害权值、攻击树文本图等元素，并结合代码仿真技术中的虚拟机运行技术，解决了传统攻击树模型行为差异性描述不准确、危害量化不合理等问题，从而提供更为高效的恶意代码分析结果。

- 可执行路径分析技术

基于可行路径的分析技术有两种应用思路：一种是结合静态分析中的完整性校验技术，对内核级恶意代码在内存中的执行路径进行完整性校验；另一种是为了对恶意代码进行更为完整的功能分析，遍历恶意代码所有可能的执行路径。

内核级恶意代码实现静默修改系统的执行路径，一般是通过修改系统库函数的返回值、修改系统库函数表的转向等手法来实现。一旦内核级恶意代码拿到了系统内核的控制权，那么对于应用层上的任何用户软件，包括应用层的杀毒软件都将会造成巨大的威胁，此时的杀毒软件将形同虚设。通过分析发现，恶意代码不管使用何种隐藏手法，其最终必将运行于内存中。其中，系统库函数在内存中执行的指令顺序、指令数都是固定的，通过计算正常的系统库函数内存指令的哈希值，并与被测系统库函数内存指令哈希值进行比对，一旦发现两者不同，就可以立即判定系统被恶意代码修改了，应当及时采取措施。

国家互联网应急中心已进行了恶意代码动静态检测系统的部署。各厂商由于技术积累和路线不同，各有特点，主要关注点如下：

- 静态分析能力和动态分析能力的均衡性
- 动态分析行为标签的类别和细致度；
- 误报和漏报
- 沙箱的种类
- 性能
- 自动分析报告的可读性
- 自动分析报告提取对应样本的网络特征
- 与其它安全设备的联动能力
- 机器学习算法
- 沙箱防逃逸技术

二. 为什么需要 APT 检测

2.1 专业级黑客攻击不断浮出水面

在刚刚过去的这几年间，被媒体披露出来的知名黑客攻击不胜枚举，一些专业级黑客组织还在不断对我国的各级政府部门、行业组织和企业单位发起攻势，这些攻击有一部分就是是 APT 攻击。APT 攻击的杀伤力，不仅通过网络跳转窃取网络内部的敏感信息，而且这类攻击难以被发现，甚至控制或破坏整个网络，它的破坏性无疑是强悍的。

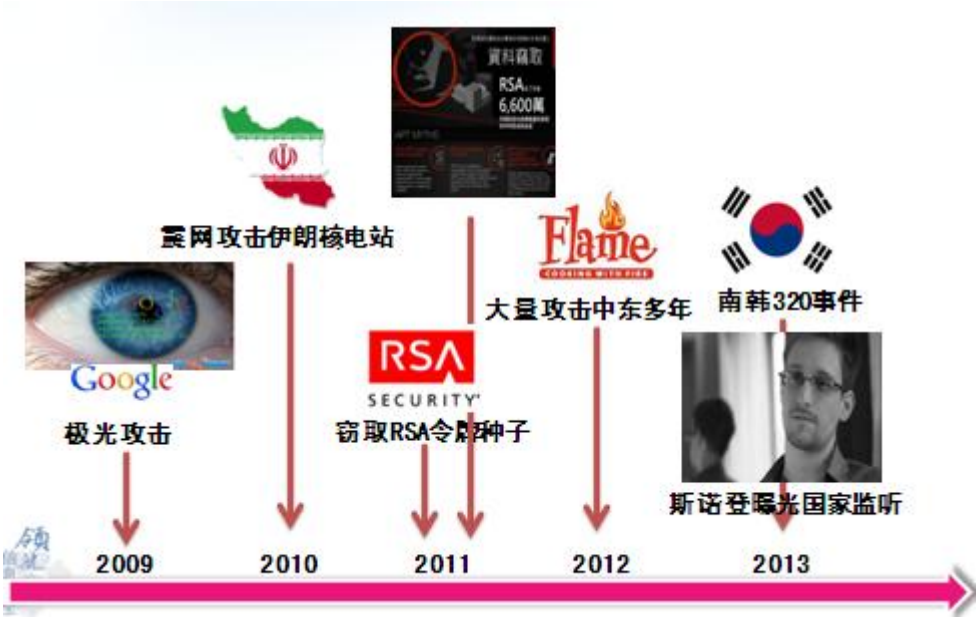


图 2.1 更频繁的 APT 攻击

所谓 APT 是 Advanced Persistent Threat “高级持续性威胁”的英文简称。这类攻击的特殊性属于攻击的潜伏时间长，驻留在隐秘的网络中发现困难，爆发后的破坏力很大。这些重大的 APT 安全事件，从震网到微软 office 逻辑漏洞，都是在被媒体披露后才浮出水面：

- 2015 年 6 月 11 日，启明星辰成功截获一起针对中国政府机构的 APT 攻击事件，利用 BlackFox 黑狐木马直接下载成功，实现 C&C 攻击，篡改 svchost.exe 进程等系列手法，详细可以参看《一起针对中国政府机构的 APT 攻击事件详细分析报告报告》。
- 2014 年 10 月 14 日凌晨，启明星辰 APT 研究团队获取到利用微软最新漏洞（CVE-2014-4114）的攻击样本 SandWorm（以下简称：沙虫）。经过样本分

析发现，该漏洞影响 windows vista、windows7 等以上操作系统，属于 WindowsOLE Package 逻辑漏洞。由于是逻辑漏洞，该漏洞传播的文件载体无需任何 shellcode，导致基于传统可疑代码扫描检测的检测设备无能为力。另一方面由于是逻辑漏洞，具有易被利用、易被改造的特点，如被黑客二次利用后扩散范围更广。启明星辰 APT 研究团队对此做出产品级应急响应，并进行了详细的《漏洞深入分析》。

- 2011 年 3 月——RSA：通过社会工程邮件打开了世界著名信息安全厂商 RSA 的门户，攻击者发动零日攻击获取了 RSA SecurID 种子，导致 SecurID 令牌无法保护 RSA 的客户。
- 2009 年 12 月——Operation Aurora：Google、Adobe 等公司被高度专业、目标明确的组织利用了 IE 零日攻击，导致了大量知识产权失窃。这次攻击也使得 Google、Adobe 两家公司的源代码泄露。
- 2009 年 7 月——Stuxnet：是世界上首个专门针对工业控制系统编写的破坏性病毒，能够利用对 windows 系统和西门子 SIMATIC WinCC 系统的零日(0day)漏洞进行攻击。特别是针对西门子公司的 SIMATIC WinCC 监控与数据采集(SCADA) 系统进行攻击，导致数千台离心机的核设施完全瘫痪。


超级工厂病毒全球肆虐 已入侵中国恐将迅速传播

来源：千龙网　2010年09月26日05:55

我来说两句(3787)　复制链接　打印　大 中 小

【提要】一个席卷全球工业界的病毒已入侵我国，这种名为Stuxnet的蠕虫病毒已造成伊朗核电站推迟发电，目前国内有近500万网民及多个行业的领军企业遭其攻击。专家表示，这个破坏性病毒专门针对西门子公司的SIMATIC WinCC监控与数据采集系统，可能造成钢铁、电力、能源、化工等重要行业运行异常，甚至造成商业资料失窃、停工停产等严重事故…[我来说两句]

可能遭袭的伊朗核电站

图 2.2　伊朗核电站遭到攻击的媒体报道

当信息化与日常生活工作的结合愈发紧密的时刻，安全边界已经从传统的网关、桌面终端延续到网络中的每一项应用、每一项业务等每一个节点中，专业级的黑客正利用了应用或业务逻辑中存在的漏洞，发起了 APT 攻击。

2.2 高级持续威胁攻击的主要特征

APT 利用没有补丁的漏洞程序，发起针对网络的深层次攻击，攻击形式多样。

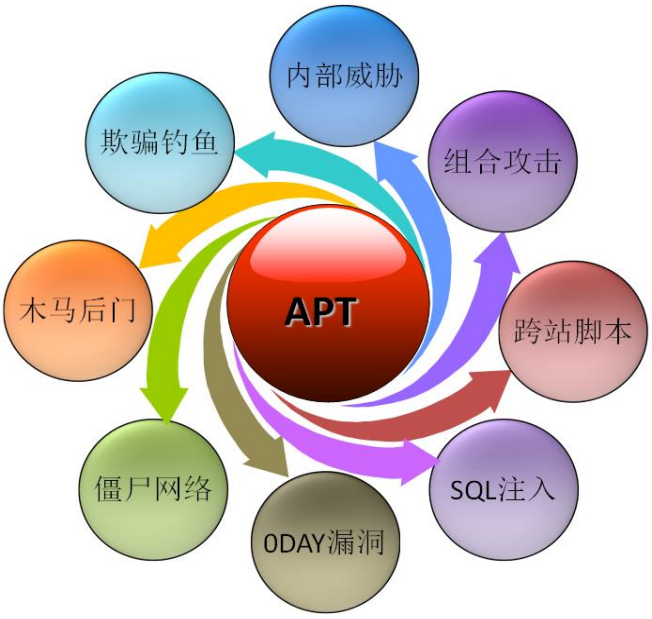


图 2.3 攻击手段多样化

APT 攻击之所以称之为高级持续威胁，是因为攻击本身复杂多维度，手段变化多样，且让传统的网络安全设备诸如防火墙、入侵检测、入侵防御、上网行为管理等设备难以招架的特点，它们典型的特征有：

- 持续性：攻击者针对重要的目标长时间持续攻击，直到攻破为止。甚至攻击成功用上一年到三年，攻击成功后持续潜伏五年到十年的案例。这种持续性攻击下，让攻击完全处于动态发展之中，而当前我们的防护体系都是强调静态对抗能力很少有防护者有动态对抗能力，因此防护者或许能挡住一时的攻击，但随时间的发展，系统不断有新的漏洞被发现，防御体系也会存在一定的空窗期：比如设备升级、应用需要的兼容性测试环境等，最终导致系统的失守。
- 终端性：攻击者虽然最终针对的是重要的资产目标，但是入手点是从终端入手，因为，他们十分清楚，任何针对核心网络和服务器等重要的资产，都是由终端的行为人来发起的。人在一个大型组织里，是难以保证所有人的安全能力与安全意识都处于一个很高水准之上的，因为要做好终端防护要比服务器端防护要困难很多。譬如，通过 SQL 注射攻击到 WEB 服务器上，一般都是利用终端用户的脆弱性，通过发起对终端的攻击作为跳板，渗透进网络中来，实现诸如 WEB 服务器等核心资产的攻陷。

- 广谱信息收集性：攻击者会花上很长的时间和资源，依靠互联网搜集，主动扫描，甚至真实物理访问方式，收集被攻击目标的信息，主要包括：组织架构，人际关系，常用软件，常用防御策略与产品，内部网络部署等信息。
- 针对性：攻击者会针对收集到的常用软件，常用防御策略与产品，内部网络部署等信息，搭建专门的环境，用于寻找有针对性安全漏洞，测试特定的木马是否能饶过检测，并通过邮件针对性地发送攻击代码到指定被攻击目标中。
- 未知性：攻击者依据找到的针对性安全漏洞，特别是 0-DAY，根据应用本身构造专门的触发攻击的代码，并编写符合自己攻击目标，且能绕过现有防护者检测体系的特种木马。触发的方式往往可以通过邮件附件中或者恶意网址的点击等，这些 0-DAY 漏洞和特种木马，都是防护者或现有防御体系无法检测到的的。
- 渗透性社工：攻击者为了让被攻击者目标更容易信任，往往会先从被攻击者目标容易信任的对象着手，比如攻击一个被攻击者目标的好友或家人，也可以是那些能够让被攻击者轻易信任的某些内部论坛，通过第三方的身份再对组织内的被攻击者目标发起 0-DAY 攻击，成功几率也很高。假如，再利用组织内的已被攻击成功的身份再去渗透攻击他的上级，逐步拿到对核心资产有访问权限的目标，破坏性就更大。
- 合法隐蔽性：攻击者访问到重要资产后，往往通过控制的客户端，分布使用合法加密的数据通道，将信息传输出来，以饶过我们的审计和异常检测的防护。
- 长期潜伏与控制：攻击者长期控制重要目标获取的利益更大，一般都会长期潜伏下来，控制和窃取重要目标，有的时候，也会采用在某个“敏感时刻”或者“关键时候”，引发破坏型的爆发。

2.3 专业黑客攻击不断挑战传统安全设备

值得引起重视的是，国内已经出现“0-Day”的地下交易市场，并且发展较为成熟。对“0-Day”有需求的包括大型的网络安全公司、黑客组织、特殊团体等，比如较为知名的 iDefence 的职业黑客，或者其他一些漏洞研究爱好者，或是比较松散的网络安全组织存在，我们也可以经常从一些国外研究 0-Day 的网站，找到一些线索，这些黑客组织或个人，不断对传统安全设备发起挑战。

在上述那么多 APT 攻击案例中，我们不难发现，传统安全设备在应对 APT 攻击方面存在很多局限性：

- 边界防护的防火墙（Firewall）和入侵防御系统（NIPS）应对 APT 攻击的局限性：这两类安全设备主要采用访问控制手段，针对网络中数据包进行过滤，当

发现符合特征的可疑数据包时及时拦截报警，但在 APT 攻击中，主要采用的是复合文档类文件结合行为嵌套，是介于 2 到 7 层的威胁，因此，这类边界防护的设备存在一定的劣势。即便我们在市场上能看到需要运用了防病毒功能、应用控制功能、流量控制功能等在内容层上做检测的安全设备，依然对嵌套式攻击的防护能力捉襟见肘。

- 基于网络检测的入侵检测（NIDS）应对 APT 攻击的局限性：入侵检测系统是基于已知特征码进行数据包检测的，但对于漏洞利用无法检测，尤其当 APT 攻击中用到的各种未知 0-Day 攻击时，存在“未知检测”的一块短板，加上 Office 文件、PDF 文件等文档类文件均需要采用内容还原的措施，存在“还原有效性”和耗费系统资源过多的难题，加上这类文件往往都有自己特有的格式，或采用加密格式、压缩格式，这使得检测有效性上大为降低。攻击代码又往往在解密或解压缩之后的数据里，入侵检测系统在扫描网络数据包的时候不对这些特定格式的文件进行一一解析，也就无法检测出 APT 攻击。
- 专业防病毒网关（AV）针对 APT 攻击的局限性：专业防病毒网关（AV）的确对文件格式识别、文件预处理等技术手段有内容解析的效果，他们发现病毒后，主要采用特征匹配（包括已知精确特征、家族特征、启发式特征）的处置手段也是典型的处理模式。但就 APT 攻击的特点而言，恶意样本很容易则将他们一一击破或者绕过。仍以最近出现的 CVE-2014-4114 漏洞样本为例，从第三方杀毒软件集合引擎扫描结果中可以看到，主流防病毒厂商的杀毒软件和防病毒

网关报警情况，在针对 0-Day 漏洞样本面前基本无能为力。

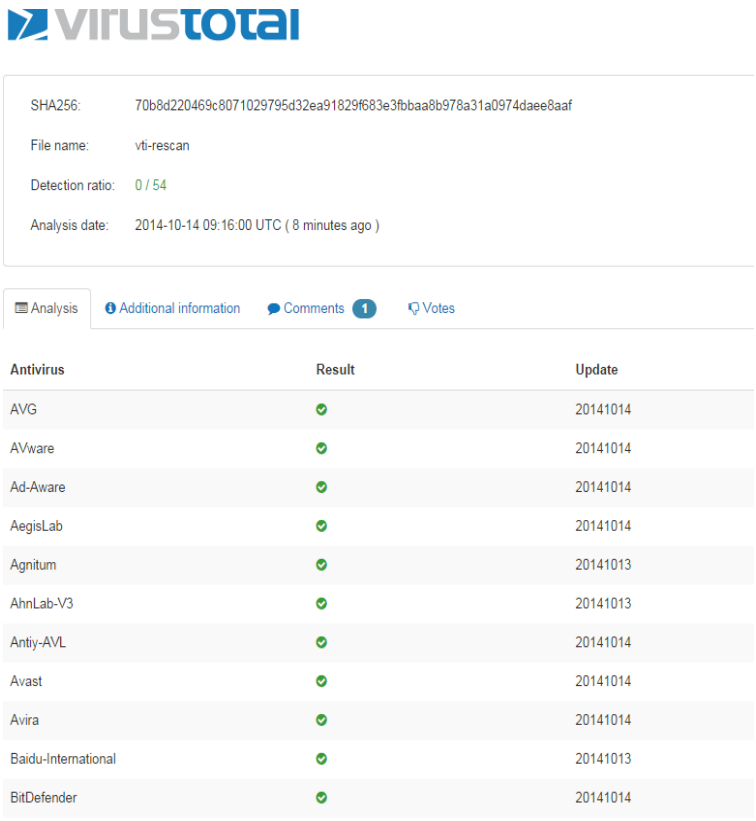


图 2.4　病毒分析报告

三. 如何评价 APT 检测系统

APT 检测像入侵检测系统一样，具有实时检测、报警和动态响应等功能，还能够很好地帮助网络管理员对特定威胁、未知威胁、恶意代码、隐秘通道、嵌套攻击等进行深度识别，找到网络中可能存在的隐患。所以，APT 检测应该从以下几个方面来做选型考虑：

- 是否能够准确地检测出 APT 的入侵行为，即检测精度。
- 针对 APT 的检测性能如何。
- 检测所采用的技术手段是否完善。
- 管理能力是否做到易管理、易配置，操作简单。
- 检测设备是否采用了专业的硬件设备。
- 检测设备是否具有良好的自身安全性，不易遭受攻击。

- 检测设备是否具有丰富的响应能力，报警的准确率高，误报和漏报率低。
- 检测设备是否具有能够满足不同网络规模的检测需求。
- 检测设备是否具有与其他网络安全设备联动的能力。

四. 天阗 APT 检测解决的主要问题

4.1 系统的目标和定位

天阗 APT 检测系列，是一款针对恶意代码等未知威胁具有细粒度检测效果的专业安全产品，可实现包括对：未知恶意代码检查、嵌套式攻击检测、木马蠕虫病毒识别、隐秘通道检测等多类型未知漏洞（0-day）利用行为的检测，由启明星辰集团独立自主研发。

天阗 APT 检测系列，采用国内领先的双重检测方法（静态检测和动态检测），多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shell code 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤，同时，产品可结合人工服务，有效发现 APT 攻击。

4.2 弥补网络安全设备检测深度不够的问题

我们的网络可能已经部署了一些安全防护设备，但当我们网络遭受了未知威胁和零日攻击、APT 攻击时，并且部署的网络安全设备依然没有报警，重要信息资产正在流失，我们却浑然不知，有这样的场景出现是，无疑给我们的网络安全风险管理带来极大的挑战。

事实上，现有网络安全设备普遍不具备对 APT 类型的攻击的检测能力，尤其是建立单独的未知威胁检测特征库。以防火墙为例，防火墙在 APT 攻击中需要解决的问题主要是检测恶意样本的 C&C 非法连接行为，即是基于已知特征来进行包数据匹配，显然，这种检测手段对于一个新的 0-day 攻击是无法奏效的。因此，天阗 APT 检测系列，很好地弥补了传统的基于特征库的被动防御体系的检测缺陷，能自动识别 APT 攻击，并可与防火墙、入侵防御、网闸等串行网络安全设备联动，提升防护 APT 攻击的能力。

4.3 识别未知漏洞利用或逃逸触发的攻击

APT 攻击大多使用了攻击者自行挖掘发现的 0DAY 安全漏洞，现有的安全防御体系很难检测基于未知安全漏洞的攻击，而且即使针对已知安全漏洞的攻击，攻击者也有一定的能力变异逃逸检测。

以市场上常见的防病毒网关为例，首先，当前的反病毒引擎都是以文件格式为先导，假如在 PDF 格式溢出情况出现之前，反病毒软件一般不会识别文件格式，当扫描到恶意 PDF 文件时，反病毒软件甚至可能直接将其视为无毒文件跳过处理，只有当反病毒软件添加了 PDF 文件格式解析后，才能对该类文件进行处理。而即便反病毒软件已经对某种复合文档进行了解析，顺利通过了第一步。

但由于复合文档格式的复杂性以及某些文档格式的不完全公开性，反病毒软件在处理这些文件的时候也都是仅仅解析当前已知漏洞的某些需要的字段和数据，无法做到面面俱到，当该格式的其他字段或数据出现漏洞的时候则需要再次重新添加解析代码，这使得反病毒软件处理文件的第二步被轻易绕过。

第三步，特征匹配就更显而易见了，从广义上说目前反病毒软件的检测仍然是基于特征匹配，只不过有些特征是一对一提取的，即精确特征；而有些特征则是针对恶意代码聚集的群体样本集合的检测规则，即家族特征或启发式特征。而因为复合式文档中出现漏洞位置的不确定性，今天可能是其中某个数据区的某个整数字段经过一系列复杂运算导致溢出漏洞，明天又可能是文档中嵌入的图片文件，字体文件等出现了漏洞，所有这些都使得原有的简单特征匹配不再奏效。

因此我们看到，对于每次出现的新的针对复合文档的漏洞，反病毒软件厂商不得不在文件格式解析和各种复杂逻辑的检测算法中疲于奔命。当然，近年来，反病毒软件也在一直演进，延伸出了诸如云查杀，程序信誉度，URL 信誉度，主动防御等一系列主机防御的新技术。云查杀是将海量的病毒特征库置于云端，解放了终端上宝贵的内存和计算资源，同时也解决了实时响应和误报的快速修补等问题。后来逐渐出现的程序信誉和 URL 信誉同样也是如此。而这几种基于云计算的技术从根本上来说仍然存在明显的滞后性，仍然逃脱不了前端捕获样本－后端分析样本－将结果再下发到前端这样的模式，无法有效对抗 APT 攻击。

另外这几种检测方法基本都是基于 PE 文件或 URL 的检测技术，APT 攻击常常采用的是复合文档，因此这几种技术在 APT 攻击检测中明显显得力不从心。另外一个在 APT 攻击

中比较有用的技术是主动防御技术，这类技术通过对主机上各程序的异常行为进行判断并拦截。由于主动防御技术并非是专门为 APT 攻击开发的，因此他要避免主机上的各种误报情况的发生，于是就会对一些具有合法数字签名的文件进行放过处理。而我们看到近年来的很多 APT 攻击中最终释放的恶意后门都是有合法数字签名的，比如 Stuxnex 程序的数字签名是 Realtek 的，Duqu 使用的是 C-Media 的。拥有了合法的数字签名就相当于拥有了合法的通行证，杀毒软件的主动防御技术便将其完全放过。

以上是从杀毒软件自身探讨的在防御 APT 攻击中的弱点，另外，攻击者在进行攻击之前往往会进行大量时间的“踩点”，这也使得攻击者能提前对被攻击者安装的杀毒软件进行较深层次的分析和测试，使得攻击样本能够绕过这些杀毒软件，正是由于反病毒软件易于获得，所以其易于被进行先导测试，导致其成了反病毒软件不能拦截 APT 攻击的根本软肋。天阗 APT 检测就针对防病毒类安全设备在未知漏洞利用或逃逸触发的不足，定向精准检测 APT 攻击。

4.4 识别利用已知和未知漏洞的文件攻击行为

我们发现 APT 攻击的特点，是经常利用第三方软件比如 Adobe、Office 等的漏洞构造的恶意文件，其攻击方式通常都是诱使用户下载该文件，当用户运行该文件后，攻击过程在本地后台悄悄执行，通常会在用户不知情的情况下进行启动或下载后门程序等攻击行为。

由于攻击的过程发生在本地，攻击发生时网络报文中没有攻击特征，因此传统的 IDS、IPS 等安全防护产品无法在攻击过程中对该类恶意文件进行检测。而且此类恶意文件构造相对复杂，理论上可以有无数种变形，单纯通过对文件传输过程中的网络报文进行特征匹配很容易造成漏报、误报。要精确检测该恶意文件的特征需要对各种文档类型比如“.pdf”、“.doc”等等进行精确的解析，同时要掌握各种漏洞的详细原理，在 IDS 等设备上实现成本太高。因此，天阗 APT 检测系统充分弥补了传统的 IDS、IPS 等安全防护产品对该类型攻击的检测能力较弱的问题。

另外，APT 攻击大多使用了专门的特殊木马，这些木马可以绕过防御者主机杀毒软件的检测，可在受限的小范围内传播。火焰病毒在中东地区的大量主机上存活了四年以上，而且无一主机安全防护软件能发现其危害性，就是典型的案例。

天阗 APT 检测系统通过动态沙箱检测技术，使用多种虚拟机环境运行被检测文件，监测文件打开后的系统环境、内存状态以及文件的各种行为等以确定文件是否为恶意文件。由

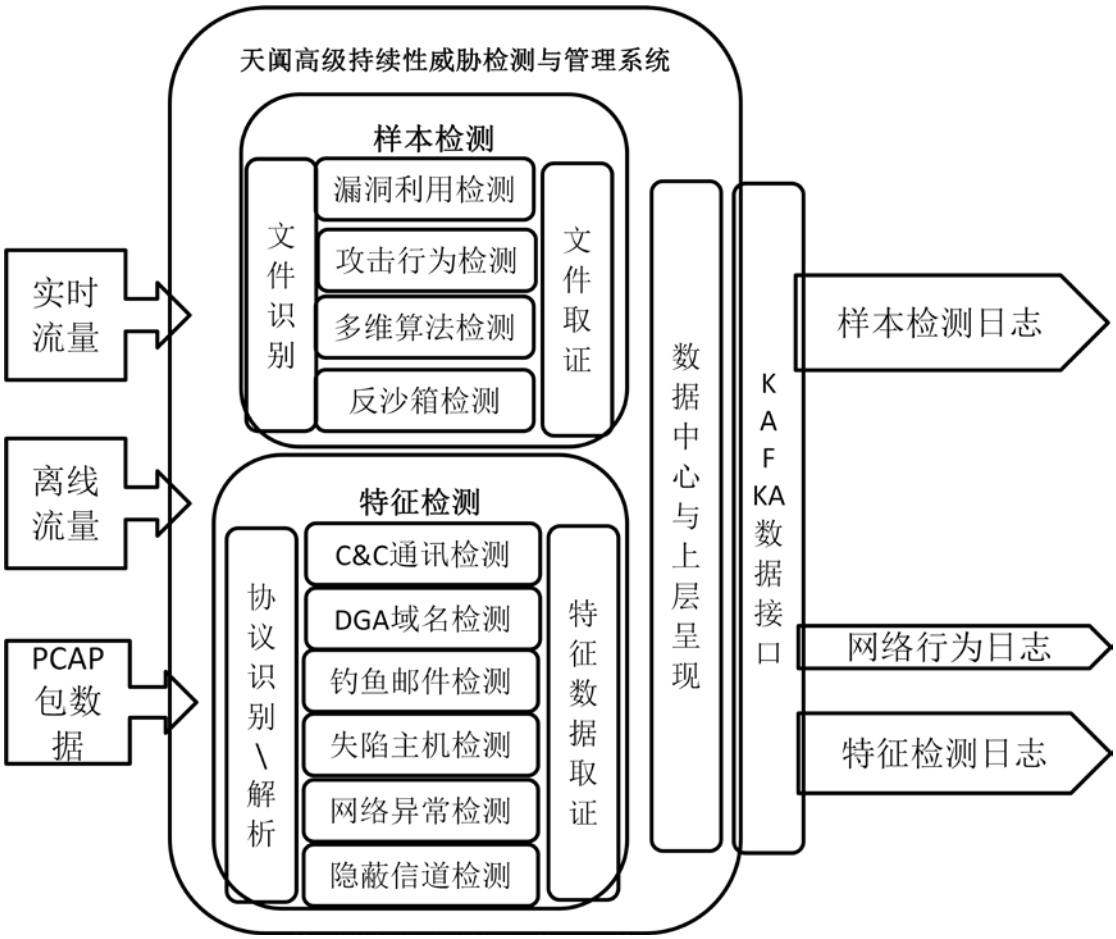
于系统是直接检测文件的具体行为，而恶意文档不论利用何种漏洞，也不论利用的是已知还是未知漏洞，它们要做的一些恶意操作总是具有一定相似性和特征模式。因此，天阗 APT 检测系统不但可以检测多种 Nday 攻击，同样可以检测未知的 0day 攻击，是已知威胁和未知威胁紧密结合的一款新一代网络安全检测设备。检测系统可以检测 windows 系统下可执行文件、pdf、doc、xls、rtf、docx、xlsx、ppt、pptx、ppsx 等大多数常用文档文件格式。

4.5 记录高级持续威胁的攻击行为还原真相

本系统动态沙箱检测引擎具有多种虚拟机环境，可以充分模拟应用程序的执行以及恶意文件中攻击代码的执行，恶意文件的一举一动都能够被监视记录下来。从而可以知道该攻击事件的内容和意图。记录的行为包括注册表操作、文件操作、漏洞利用方式、API 调用序列、网络行为、进程线程操作、其它危害系统的行为、恶意文件所含 PE 文件的详细行为报告。

五. 天阗 APT 检测系统主要功能特性

5.1 天阗 APT 检测系统的架构



天阗 APT 检测软件架构全透析

5.2 支持两种待检测文件接收方式

系统支持两种待检测文件上传方式：

- Web 接口手工上传文件：系统内置 web 服务器，用户可通过 HTTP 方式上传需要检测的文件。
- 调用 API 函数，自动上传：系统提供一套标准的文件上传 API 函数，IDS、IPS、WAF、防火墙等产品可以调用这些 API 自动上传需要检测的文件，以实现与本系统的联动。

5.3 全面支持已知威胁检测

当前发布的天阗 APT 检测系列，只需要添加入侵检测与管理系统功能模块，就可以实现已知威胁加未知威胁的全面检测，包括但不限于：病毒、蠕虫、木马、DDoS、扫描、SQL 注入、XSS、缓冲区溢出、欺骗劫持等攻击行为以及网络资源滥用行为（如 P2P 上传/下载、网络游戏、视频/音频、网络炒股）、网络流量异常等威胁具有高精度的检测能力，产品对已知威胁事件库完美融合。

5.4 对恶意文件的静态检测

静态检测是指通过一定的特征比对或算法对被检测文件的二进制内容进行匹配或计算的检测方法，静态检测并不真实的运行被检测文件。静态检测的方法有很多种，天阗 APT 检测系统针对未知 PE 文件特别设计了专用检测方法，主要包含通用检测方案和非通用检测方案。通用检测方案针对非 PE 文件内嵌恶意代码的特点进行检测，主要包含内嵌脚本检测、内嵌 PE 检测、内嵌 shellcode 检测三种检测方案。

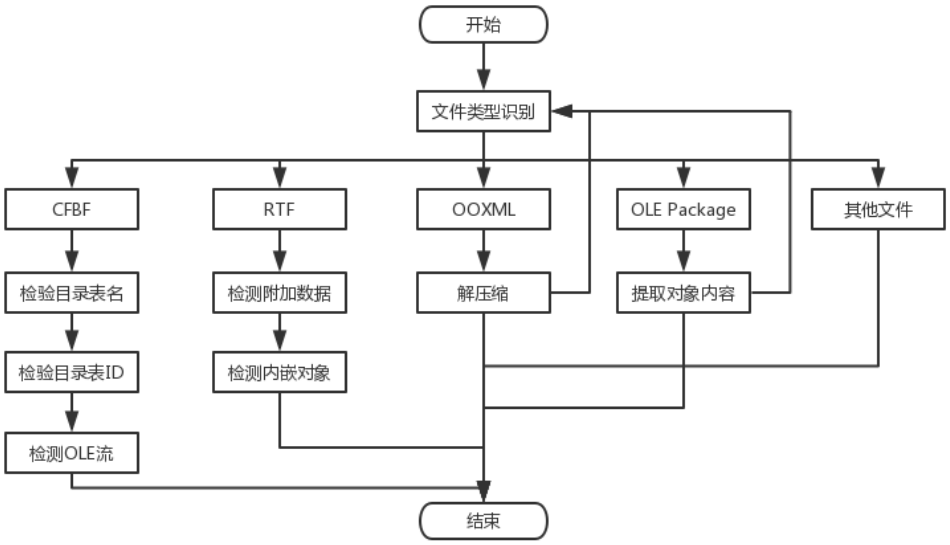
内嵌 shellcode 检测：虚拟 shellcode[1]执行是在 APT 攻击常用的文档类文件中搜索可能存在的可执行代码（shellcode），一旦找到疑似代码后则将这段二进制内容送入到虚拟执行引擎中当做代码进行虚拟执行。如果这段二进制内容恰好能够在虚拟引擎中得到顺利的执行，则说明该文档中含有可执行的 shellcode 代码。由于正常的文档文件中的二进制内容几乎不可能恰好可以作为代码得以执行，所以该方法可以有效判定文档文件是否为恶意。

[1]Shellcode：Shellcode 是一段代码或填充数据，是利用程序或复合文档作为载体，通过特定漏洞可以在目标主机上非法触发执行的代码，该代码执行后一般可以用来获取权限、执行或下载木马病毒等。

内嵌 PE 检测：APT 攻击的最主要目的是获得对目标对象的长时间控制，因此在目标对象中种植后门就成了 APT 攻击的最终目标。而后门的主要载体就是可执行的 PE 文件，这些 PE 文件通常会被提前嵌入到恶意文档中。当漏洞成功触发后 shellcode 会从恶意文档中释放出该 PE 文件（一般为木马），进行进一步的攻击。PE 文件有明显的特征格式，为了避免被查杀，攻击者会通过一些算法来对该 PE 文件进行变形，以达到隐藏自己的目的。暴力搜索隐藏 PE 文件就是通过已知的一些常用变形算法逐一对整个目标文件进行逆向解码，然后在解码后的文件中查找其是否含有 PE 文件。如果搜索到了就证明该文件是故意嵌入了隐藏的 PE 文件。由于正常的文档中不可能故意编码嵌入 PE 文件，因此该方法的误报率几乎为 0。

内嵌脚本检测方案主要针对各种非 PE 文件中内嵌的宏、Action Script，JavaScript 脚本代码进行检测。以 office 宏机器学习检测方案为例，首先需要对 office 进行结构化解析，从中提取出相应的宏代码。对宏代码提取名称的特征、恶意行为的特征、数据加密特征。其中提取宏代码中名称的特征，采用的是马尔科夫链算法。通过对大量的英文文章进行训练，统计每个单词中相邻两个字母组合的分布情况，然后计算出每种组合的概率分布。对于一个单词而言，将其拆分成相邻两个字母的若干组合，然后将所有组合之间的概率相乘，从而求出总概率值。先设置一个初始阈值，然后对阈值进行迭代，使得对 99%以上的正常单词的判断为正常。然后在测试阶段中，对新单词通过上述的方法进行计算，通过相乘计算出单词的总概率，通过将该概率与训练阶段的阈值进行比较，从而判断它是正常或者异常字符串。

非通用检测方案主要是针对特定类型的非 PE 文件进行深度结构解析，基于解析出的元数据发现异常文件的检测方案。以 Office 文档检测为例，主要流程如下：



5.5 对恶意文件的动态检测

系统使用多种虚拟机环境运行被检测文件，检测文件打开后的各种行为和系统环境等以确定文件是否具有恶意行为。动态检测的优点是检测率高、误报率低。

动态检测能在很大程度上克服静态检测的通过代码混淆，压缩加密等方式便被绕过的特点，直接把样本放到真实环境中模拟运行，并观察样本的恶意行为。当样本存在可疑漏洞利用行为、可疑文件动作行为以及可疑网络行为时则报警提示给用户。经过启明星辰研发团队对于漏洞攻击多年的研究经验，我们将漏洞样本的行为分为了上述三种，并针对上述三种行为设计了漏洞利用检测引擎，文件行为分析检测引擎和隐匿通道检测引擎。

漏洞利用检测引擎是专门针对 APT 攻击常见的漏洞攻击行为设计的专用检测引擎。该检测引擎通过对常见漏洞攻击的系统脆弱点进行监控，在监控到对应脆弱点被攻击后则报警提示用户。具体地，以栈溢出[2]漏洞利用来说，在此类漏洞成功利用后会覆盖其后面的重要数据

[2]堆、栈溢出：计算机操作系统在执行一段程序的时候，需要划分一块内存区域用于存放用户输入的数据。如果编程人员没有对输入数据的大小做检查，当用户输入的数据超过事先分配的内存大小时，就有可能覆盖到相邻程序或函数的数据区。通过精心

-返回地址，返回地址指向程序接下来要执行的代码，当返回地址被覆盖后，程序的执行逻辑就可能被篡改，甚至执行用户输入的数据。漏洞利用检测引擎就是用来监控类似的漏洞攻击行为的。漏洞利用检测引擎是天阗 APT 检测系统的最大亮点也是甄别各种未知漏洞攻击行为的不二法眼。

5.6 对多种文件格式的检测

本系统可以对不少于 120 种文件格式进行静态动态检测，涵盖 Windows、Linux、Android 多种操作系统格式文件。

图 5.1 多种文件格式支持

5.7 支持 SPAN/TAP 部署模式

系统支持旁路模式的 SPAN/TAP 部署方式。

SPAN，全称为 Switched Port Analyzer，直译为交换端口分析器。是一种交换机的端口镜像技术。作用主要是为了给天阗 APT 检测系列产品提供网络数据流，SPAN 并不会影响源端口的数据交换，它只是将源端口发送或接收的数据包副本发送到监控端口。

利用 SPAN 技术我们可以把交换机上某些想要被监控端口（以下简称受控端口）的数据流 COPY 或 MIRROR 一份给天阗 APT 检测系列产品。

构造输入的数据，可能会使之覆盖到当相邻数据区的重要数据，则有可能造成程序崩溃甚至篡改程序执行流程，达到攻击的目的。

TAP（Test Access Port）又称网路分流器（Network Tap），也叫做测试接入端口 TAP，天阗 APT 检测设备直接插入到网络中，TAP 设备发送一份网络通信给天阗 APT 检测设备，从而实现 APT 攻击的检测。

5.8 对加密协议进行检测

支持 SSL 证书导入功能，可对 HTTPS 等加密流量进行协议识别、协议解析、文件还原及攻击威胁检测。

5.9 YARA 规则检测

支持 yara 规则检测，可自定义规则进行文件检测，同时支持导入 yara 规则，提升恶意样本检测的灵活性。

5.10 对 PCAP 文件回溯检测

支持手工导入 pcap 文件，进行离线流量检测。可以根据 pcap 包中的时间戳进行检测，回溯到流量当时发生的时间进行上报攻击。同时支持特征检测、文件还原、文件检测，做到全方位的回溯检测。

5.11 基于邮件钓鱼场景检测

攻击者通过发送一些隐蔽链接，引诱被攻击者点击，跳转到钓鱼网站收集敏感信息或者通过 url 直接下载恶意文件，以实现对内部人员的攻击；APT 产品能够完整还原出邮件的正文信息，并提取出邮件中的 URL 链接进行检测，能够快速发现针对内部网络的钓鱼邮件。

5.12 基于 WEB 水坑攻击场景检测

很多时候在用户不知不觉中恶意代码就已经“潜入”了我们的计算机，这正是因为攻击者使用了水坑攻击的手段，通过收集内部人员的上网习惯，在被攻击常用的网站“埋下”木马病毒，使被攻击以为自己下载的是正常文件。木马病毒就很轻易的被植入进了目标主机，被攻击者却完全不知情。APT 产品能够还原出常见的支持文件传输的协议的文件，并进行深度检测，对内部人员下载的敏感文件进行报警。

六. 系统主要优势

6.1 集成已知检测，精确检测网络威胁

天阗 APT 检测系统，集成已知威胁检测能力，在特征库的质量上不断更新，并且精选出来的 4000 多条代表主流攻击的事件，特征库还覆盖了大量 APT 攻击事件 ，满足用户对于检测产品“全、精、新、准”的述求。事件库覆盖了各种攻击类型包括：病毒、蠕虫、木马、DDoS、扫描、SQL 注入、XSS、缓冲区溢出、欺骗劫持等攻击行为等同时涵盖了各种攻击过程：信息收集、社工攻击、木马植入、漏洞利用、横向攻击、远程控制等。通过准确的原始报文取证功能提供高可用的研发分析能力。

6.2 动态静态检测，让恶意代码无处遁形

天阗 APT 检测系统，针对 APT 攻击常常采用复合文档攻击的特点，本系统的动态检测系统创造性的采用了两大检测系统进行 APT 攻击检测：基于二进制的漏洞利用检测系统和针对 PE 文件的传统行为分析系统。之所以采用双系统检测 APT 攻击，是因为传统的行为分析系统在分析利用漏洞的复合文档时存在明显缺陷。

首先简要介绍下漏洞触发的一些过程。漏洞触发后的 Shellcode 基本都会执行或下载一个后门或其他病毒程序（俗称大马），用于对目标主机的更长期控制。大马在 Shellcode 执行该可执行文件之前的过程我们叫做漏洞利用准备期（Pre-exploitiation），Shellcode 执行的过程叫做漏洞利用触发期（Exploitiation），Shellcode 执行完毕后启动的大马所做的恶意行为叫做漏洞触发后期。传统的行为分析系统都只能捕捉最后的大马的可疑行为，由于检测的是复合文档，因此，传统行为分析系统检测的是其所依赖的软件的行为（比如 doc 文档所依赖的 word.exe），而这些软件或多或少都存在一些合法的“越界”行为，容易与真正的 Shellcode 行为混淆发生误报。

此外，由于 shellcode 最终执行的行为还不一定是释放了可执行文件这么容易捕捉的文件系统 I/O 操作，如果 shellcode 最终执行的行为是从网络上下载恶意文件，且黑客服务器已经停止服务，那么传统的行为分析系统很可能就无法完全捕捉到漏洞触发过程。为此，我

们特别针对传统行为分析系统的缺陷设计了专门用于检测二进制文件漏洞的漏洞利用检测系统。该系统通过监控二进制代码流的异常行为，比如针对漏洞准备期的堆喷行为检测，漏洞利用触发期的可疑 API 调用拦截，堆栈执行代码检测，可疑 ROP 行为检测等监控漏洞利用的各种可疑行为。使得漏洞的检测过程更加全面和精准。

以 CVE-2012-0158 漏洞为例，杀毒软件在得到具体的漏洞细节前根本无法查杀该样本，而我们的漏洞利用检测系统成功在不升级的情况下就能成功检测到该样本的攻击行为。通过漏洞检测模块的固定内存地址攻击检测到了样本尝试跳转到 MSCOMCTL.OCX 模块的特定地址以进一步执行下一步 shellcode。

图 6.1　警示用例

在漏洞利用系统检测到可疑漏洞利用行为的文档类文件后，会根据漏洞触发的具体情况将其投入到行为分析检测系统中继续进行检测，从而获得更进一步的行为分析结果，包括具体的文件行为信息和网络行为信息。

而当可执行文件被投入到系统后，将直接进入行为分析系统进行分析。整体的分析流程如下图：

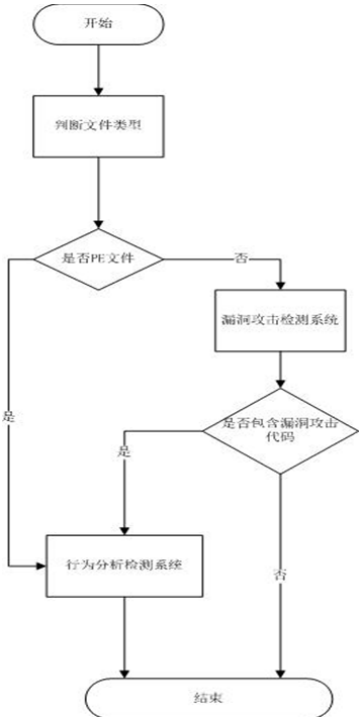


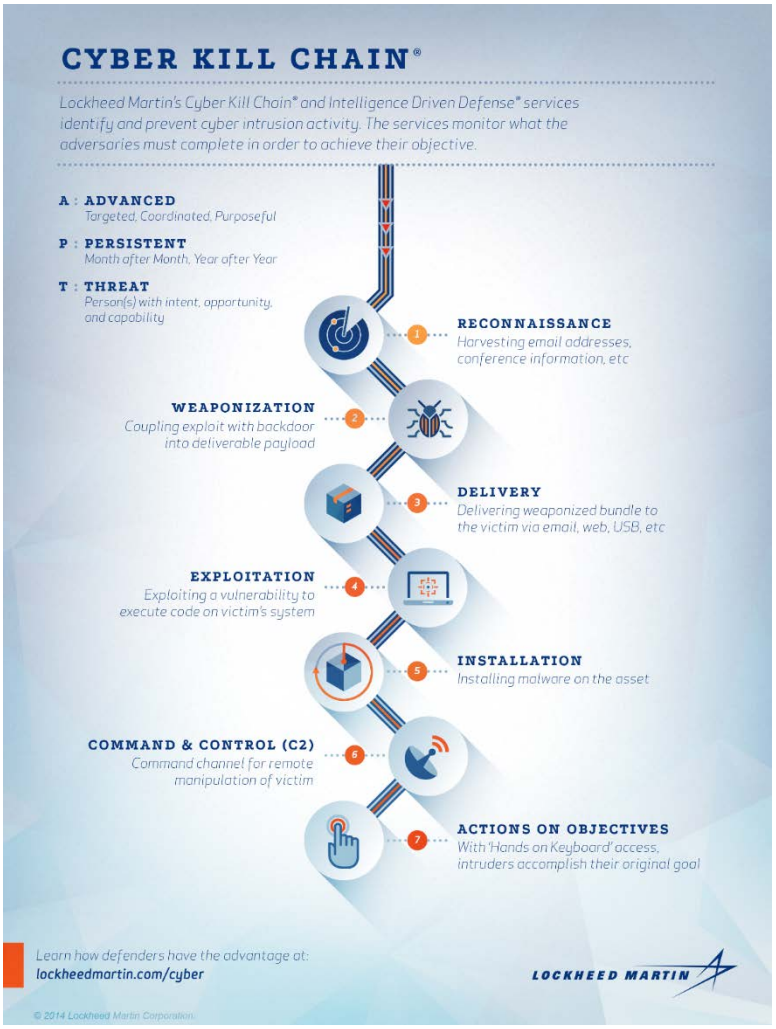
图 6.2　分析过程

6.3 威胁情报应用，快速精准发现攻击威胁

通过内置公司自有的 VenusEye 威胁情报，可通过情报碰撞快速发现攻击威胁。情报种类覆盖 120 个 APT 组织、560 种家族信息、34 种情报大类。根据 IP、域名/URL、MD5 快速判断攻击威胁，提升检测效率。同时通过联网可进行云端威胁情报查询，可以利用情报实时进行云端检测。

6.4 紧跟安全趋势，全面支持 ATT&CK 模型

2013 年洛克马丁公司提出了以军事战争为蓝本的 Kill Chain 模型，以此来描述攻击的各个阶段，根据这个链条，防护者可以针对性地构建纵深防御体系，快速发现外部威胁，精准切断链条的关键节点，阻止甚至反制攻击者的入侵攻击行为。



Kill Chain 模型对于理解高维度的过程和攻击者目标很有帮助，但这类模型无法有效描述对手在单个行动中做了什么，例如：

一次行动与另一次行动之间有什么联系？

连续的行动是如何与敌人的战术目标联系起来的？

这些行动与数据源、防御、配置和其他被用在一个平台/技术域之间的措施间如何具体联系起来？

于是，MITRE 公司在 KillChain 模型的基础上，构建了一套更细粒度、更易共享的知识模型和框架-ATT&CK。

ATT&CK，全称是 Adversarial Tactics, Techniques, and Common Knowledges。A 是 Adversarial，表示攻击者、对手；两个 T 分别是 Tactics 和 Technical，即战术和技术；CK 是 Common knowledge，通用知识库。

ATT&CK 中用途最广泛的模型是 ATT&CK for Enterprise，主要包含 12 种战术，即初始访问、执行、持久化、特权提升、防御绕过、凭证访问、发现、横向移动、收集、命令与控制、泄露、影响。如果把这 12 种战术比喻成为一场真实的战争，初始访问就相当于抢滩登录的过程；执行、持久化、特权提升、防御绕过就是夺取和巩固阵地的过程；凭证访问、发现、横向移动相当于在当前阵地上继续扩大战果，夺取新的高地的过程；收集、命令与控制、泄露、影响则是战争的最终目标达成。

ATT&CK 中的战术和技术将一次生命周期中的攻击者行为定义到了一个能将其更有效映射到防御的程度。高级别的概念(战术)，诸如控制、执行和维持被进一步分解为更具描述性的分类(技术)。而且技术的具体实现过程还可以细分，一项技术可以通过多种方式去进行实现。

可以说，自从有了 ATT＆CK，无论对攻击者还是对防御者来说，都有了一部可以“照章办事”的百科全书。攻击者可以利用 ATT&CK 构建自己的攻击路线，防御方可以利用 ATT&CK 构建自己的纵深防御体系。对于防御方来说，以 ATT&CK 的覆盖度为依据则足以判定出防御方的防御体系成熟度。

天阗 APT 检测系统的告警只是标签输出已全面支持 ATT&CK 模型，可以在报告页面查看到相关规则对应的 ATT&CK 技术信息。

6.5 系统环境构造，提高检测粒度和精度

在我们的检测系统中内置了多种操作系统和软件环境，在检测的时候我们会将样本放进所有环境进行检测，如果某一个环境检测到了恶意行为则报警。目前我们支持的操作系统有 Windowx XP 和 Windows 7；支持检测的 Office 软件有 Office 2003、2007、2010，支持检测的 Adobe 软件有 Adobe 8、9、10、11 以及 WPS 办公软件等。

图 6.3　支持多种格式

以 CVE-2014-4114 漏洞攻击的检测场景为例，该漏洞在 Windows Vista SP2 以上的操作系统和安装 Office2007 以上的软件环境中才能触发。我们的系统在检测的过程中将其放入

了 Windows XP 和 Windows 7 环境中同时检测，结果只在 Windows 7 中检测到了攻击发生。如果没有多系统多环境的同时检测，那么该攻击将被放过。

6.6 独有反沙箱检测技术，让恶意威胁无处逃逸

随着高级可持续攻击威胁对抗技术的不断发展，针对恶意代码进行分析，检测未知恶意代码，经常利用虚拟机技术。攻击者为了逃避这些虚拟机以及病毒分析沙箱，会在恶意程序中加入检测虚拟机及沙箱的代码，以判断程序所处的运行环境。当发现程序处于虚拟机沙箱中时，它就会改变操作行为隐蔽恶意动作，逃避检测。我们称之为沙箱逃逸技术。沙箱逃逸技术通过获取进程，文件，注册表，窗口，MAC 地址，内存，CPU，硬盘，屏幕分辨率，机器名信息，是否有交互行为等信息检测是否运行在虚拟机中，还可能运用延迟运行等方式延缓恶意行为发生时间降低虚拟环境的检出率。越是危害性大的恶意代码，越会采用多种沙箱逃逸手段。威胁情报整编系统在处理和分析这类恶意样本时，针对各种沙箱逃逸手段进行了针对性的反沙箱逃逸技术开发，以防止恶意代码躲避沙箱检查，对用户网络和系统造成影响。

6.7 隐秘通道感知，让信息外泄有效避免

APT 攻击经常会使用看起来合法的加密信道来负载数据并逃过审计检测，天阗 APT 检测系统的可疑行为分析系统在分析样本时，能快速感知其发出的可疑 C&C 连接，并可自动提取 C&C 连接的可疑 IP，端口，URL 等信息并将相关信息发送给 IDS、IPS、Firewall 等

配套安全设备，使得这些本无能力防范 APT 攻击的设备具有拦截 APT 攻击的能力。如下图为我们在检测到海莲花样本时发现的可疑 C&C 连接。

▾ TCP协议

源IP	目的IP	源端口	目的端口	数据长度	数据信息
10.20.14.65	10.20.14.2	49160	80	97	47 45 54 20 2f 6e 63 73 69 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4e 43 53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73 66 74 6e 63 73 69 2e 63 6f 6d 0d 0a 0d 0a
10.20.14.65	10.20.14.2	49161	443	176	16 03 03 00 ab 01 00 00 a7 03 03 5e e1 63 10 07 f4 dc 71 4a b4 e8 15 0c 20 56 3d 34 34 c9 f8 44 47 c6 5a 24 54 00 d5 58 e8 e1 bd 00 00 2a 00 3c 00 2f 00 3d 00 35 00 05 00 0a c0 27 c0 13 c0 14 c0 2b c0 23 c0 2c c0 24 c0 09 c0 0a 00 40 00 32 00 6a 00 38 00 13 00 04 01 00 00 54 00 00 00 1a 00 18 00 00 15 6f 6e 65 64 72 69 76 65 2e 73 65 72 76 65 70 32 70 2e 63 6f 6d 00 05 00 05 01 00 00 00 00 00 0a 00 06 00 04 00 17 00 18 00 0b 00 02 01 00 00 0d 00 10 00 0e 04 01 05 01 02 01 04 03 05 03 02 03 02 02 00 17 00 00 ff 01 00 01 00
10.20.14.65	10.20.14.2	49161	443	198	16 03 01 00 86 10 00 00 82 00 80 04 0f 94 4c b5 7e d7 45 7a 7c d7 de c9 38 ba cb ad b3 9a 06 a0 d6 57 b5 22 27 d4 65 5a be 41 0f 4b b5 a3 19 79 f3 ba 0e ed 78 0d 82 89 0e 72 7c 30 1f 84 d5 10 d5 4a ef 1c ee 0f 17 64 52 cc c6 59 53 75 87 7d 00 4b 6a fa 8a e7 a7 ff 88 c0 35 a0 39 91 4d 50 44 98 95 de 1e 1c 5c 20 0a 70 b5 01 01 9f 6f 06 30 2e 82 c1 47 c0 5a 93 f2 e0 44 9d a1 4b c1 31 f9 91 24 39 6a 0d 9a 82 74 b7 5f 14 03 01 00 01 01 16 03 01 00 30 b4 fd 2a a9 8b 6c 2f 29 b1 2b 4a 06 c4 5d ae db 47 f5 1e 74 28 7e bc 7b 27 2f a9 cb f9 bc 68 32 22 a0 d5 6e e3 c3 b9 6b fd 4c 18 13 1e f2 e4 d3
10.20.14.65	10.20.14.2	49162	80	201	47 45 54 20 2f 6d 73 64 6f 77 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 76 33 2f 73 74 61 74 69 63 2f 74 72 75 73 74 65 64 72 2f 65 6e 2f 64 69 73 61 6c 6c 6f 77 65 64 63 65 72 74 73 74 6c 2e 63 61 62 3f 34 64 61 63 31 37 30 65 64 36 64 36 33 64 66 37 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 70 74 6f 41 50 49 2f 36 2e 31 0d 0a 48 6f 73 74 3a 20 63 74 6c 64 6c 2e 77 69 6e 64 6f 77 73 75 70 64 61 74 65 2e 63 6f 6d 0d 0a 0d 0a
10.20.14.65	10.20.14.2	49163	80	195	47 45 54 20 2f 6d 73 64 6f 77 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 76 33 2f 73 74 61 74 69 63 2f 74 72 75 73 74 65 64 72 2f 65 6e 2f 61 75 74 68 72 6f 6f 74 73 74 6c 2e 63 61 62 3f 32 32 33 39 66 36 39 36 65 39 36 61 35 30 32 61 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 70 74 6f 41 50 49 2f 36 2e 31 0d 0a 48 6f 73 74 3a 20 63 74 6c 64 6c 2e 77 69 6e 64 6f 77 73 75 70 64 61 74 65 2e 63 6f 6d 0d 0a 0d 0a

▾ DNS协议

类型	请求
A	onedrive.servep2p.com

图 6.4　网络连接行为

在 C&C 通道自动感应系统中，我们解决了既避免将可疑样本传到公网上扩散又能有效的抓住其发出的 C&C 连接的问题。我们动态的模拟出了各种协议，从而虚拟出一个假的响

应服务器，同时对虚拟沙箱的网关和 DNS 进行劫持，使得样本在发出网络连接时将所有的数据都发向我们虚假响应服务器。该方法弥补了传统 Hook 各种网络连接函数(connect 等函数)方式甚至是直接将沙箱连接到公网等的方式抓取网络数据包的缺陷。

天阗高级持续性威胁检测与管理系统针对各种木马后门的通讯方式与协议进行了深入研究，总结出了多达 5 种以上的僵木蠕 C&C 通信共性特征，从数据包传输大小，上下行流量，心跳行为，时间分布，行为序列等方面再结合威胁情报综合检测未知僵木蠕的命令控制通道，效果明显。

6.8 简洁报告设计，让复杂问题简单易懂

我们设计出了专业人士和非专业人士都易读懂的报告格式，报告既包括非专业人士需要的威胁简要描述等信息，也包括专业人士需要的详细报告。

下面是漏洞分析系统检测报告。可以看到报告的上方是简要的威胁描述信息。这里用红字表示当前的样本非常危险，强烈建议不要打开。下方的检测具体报告展开后则是我们在每个环境下的运行结果，这里我们看到 Windows XP 环境未能检测出攻击，而 Windows 7 环境则检测出了攻击。

图 6.5 漏洞检测报告

下面是行为分析系统检测报告。同样包含简要的威胁描述信息和具体的报告两项内容。从上方的威胁描述可以看到该样本同时存在文件威胁行为和网络威胁行为，且等级都是最高级别。在文件威胁行为分析报告中我们看到了该样本触发了多种等级的行为规则，并分别用

不同颜色表示；下面的行为分析详细信息则从另一方面佐证了上面的报警规则，是该样本行为规则的报警依据，供专业人士阅读。

文件基本信息　行为分析系统检测报告

文件基本信息

被检测文件名	slide1.gif
文件大小(byte)	108544
文件类型	exe
文件MD5	8a7c30a7a105bd62ee71214d268865e3

行为分析系统检测报告

威胁行为描述

非攻击 低级别 中级别 高级别

该样本极其危险，强烈建议不要打开.

网络威胁行为描述

非攻击 低级别 中级别 高级别

发现可疑HTTP请求

行为分析概要报告

操作系统环境	软件版本	检测程序版本	检测开始时间	检测持续时间(s)	检测结束时间	危险行为	其他行为
Windows 7	Miscrosoft Office 2007	1.1	2014-10-15 13:30:59	220	2014-10-15 13:34:39	• 安装自启动项 • 搜集系统信息	• 尝试查找文件 • 尝试挂接窗口钩子 • 释放PE文件到系统目录 • 尝试创建可执行文件 • 尝试创建HTTP连接

行为分析详细信息

操作系统:Windows 7,软件版本:Miscrosoft Office 2007

释放文件

FONTCACHE.DAT

文件信息

- C:\Documents and Settings\test\Local Settings\Application Data\FONTCACHE.DAT
- C:\Documents and Settings\test\start menu\programs\startup\{6C6C4942-4942-1250-4249-6C6C42496C6C}.lnk
- C:\WINDOWS\system32\rundll32.exe
- C:\DOCUME~1\test\LOCALS~1\Temp\slide1.exe

注册表操作

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ProductOptions
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\DefaultSecurity
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName
- ActiveComputerName
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList
- HKEY_CLASSES_ROOT\CLSID\{59031A47-3F72-44A7-89C5-5595FE6B30EE}\InProcServer32

网络行为

http

URL	Data
/aG91c2VhdHJlaWRlczk0/dirconf/check.php	POST /aG91c2VhdHJlaWRlczk0/dirconf/check.php HTTP/1.1 Accept: */* Accept-Language: zh-cn Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E) Host: 95.143.193.131 Content-Length: 72 Connection: Keep-Alive Cache-Control: no-cache id=4C594BC82A1039516A4467312089C1F111E84BCB&bid=cmhBTlA=&nm=1&cn=2&num=5

图 6.6　行为分析报告

能够预警未知威胁和零日攻击/APT，能够记录攻击行为，能够发现攻击目的，能够追踪攻击源。

系统就是针对未知威胁和零日攻击/APT 的预警平台，它通过清晰直观的视图与表格，帮助管理者发现那些不易发现的零日攻击，并且捕获攻击行为，发现攻击目的以及追踪攻击源。有了系统预警平台就像有了一个未知威胁和零日攻击/APT 的雷达一样，不再是瞎子和聋子，让您能够预警零日攻击，发现攻击目的，追踪攻击源。

系统的产品目标：“预警未知威胁和零日攻击/APT 的先进雷达，让您四能：能够预警零日攻击，能够记录攻击行为，能够发现攻击目的，能够追踪攻击源”。

6.9 检测调度智能，检测性能计算效率提升

我们设计了一套全新的高效智能虚拟机调度引擎，该引擎能根据当前的系统资源占用和自动启动或关闭相应的虚拟环境，保证样本的实时检测性。另外当样本数量突发时虚拟机调度引擎亦能智能调节虚拟机任务的分发。

图 6.7　智能调度

6.10 跨界设备联动，抵御未知威胁和攻击

天阗 APT 检测系统可通过联动接口与传统 IDS、IPS、WAF、防火墙、网闸等安全防护产品进行联动。联动产品将监测到的可疑文件通过联动接口传送至本系统，由本系统进行动

态沙箱检测。系统检测的结果也可以通过联动接口传送回联动设备等设备，以作为传统安全防护产品对于恶意文件类型的攻击无法准确检测的补充，做到全方位的防护。

天阗 APT 检测系统使用了大量的技术专利，为检测系统提供强有力的技术保障。

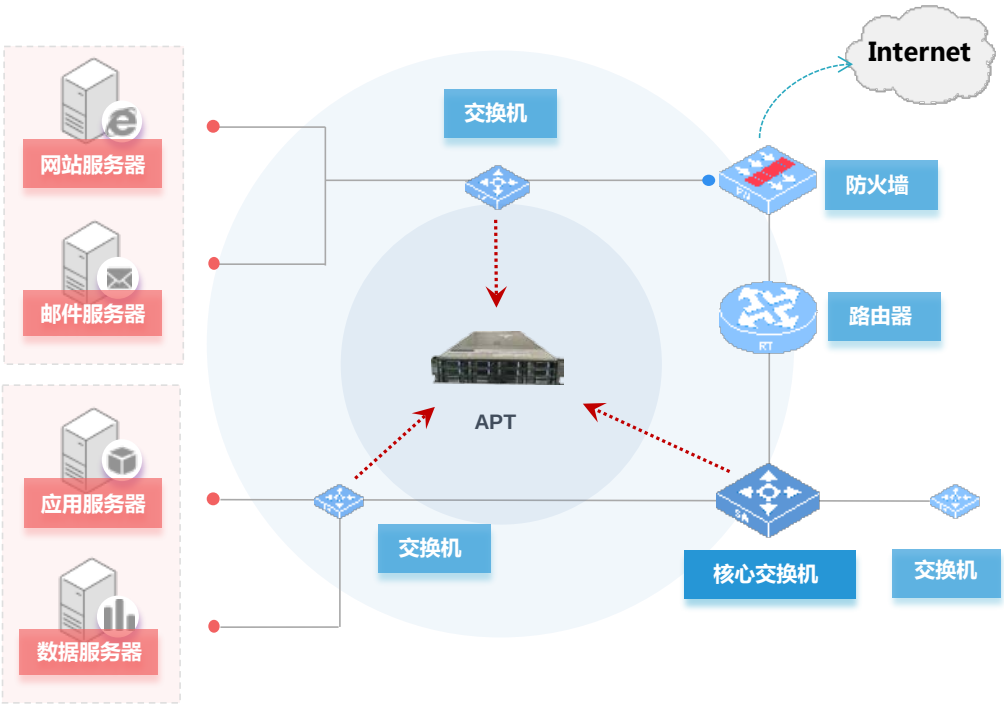
图 6.8　多项国内专利和国际专利

七. 部署和解决方案

天阗 APT 检测系统可支持单级或多级部署，通过 SPAN/TAP 部署方式，将设备并联到网络当中。普遍认知是把所有检测设备部署在边界，认为如果攻击进入内部则为时已晚。从攻击者的角度思考，突破边界进入内部必要进行横向移动，来寻找核心资产。此时部署在交换节点，可以检测从内部发起高级威胁攻击。一旦发现此类攻击则证明边界已被突破，但发现攻击并及时制止可以“挽回损失”。

作为面向 APT 检测的专业安全检测设备，在企业内网、党政专网等网络中可发挥如下作用：发现基于应用层的攻击、发现通过网络协议传输的恶意代码等；如部署在互联网出口处可发挥如下作用：基于用户的恶意代码攻击等。

天阗 APT 检测系统根据用户需求，提供多级部署方案，保证用户网络安全，也可提供与其他网络完全设备提供联动接口。



八. 结论

随着安全漏洞不断被发现，黑客组织的攻击技巧和破坏能力不断提高，手段多样，入侵的成功几率高。这些威胁，还在不断挑战我们的政府部门、行业组织、企业单位等组织的网络安全，启明星辰深刻理解用户需求趋势，在此基础上推出了契合用户使用习惯的天阗 APT 检测系统。

为了弥补防火墙等边界防护设备对高级威胁的检测能力不足，我们需要利用基于静态动态结合的检测技术，实时网络已知和未知风险的监控，减少由此带来的损失。

天阗 APT 检测系统产品优势明显和功能完备，是客户在检测下一代威胁“已知和未知”网络威胁的最佳选择。