基于动态分析的 APT 检测技术研究

安天实验室

文档信息			
作者	安天实验室反病毒引擎研发中心	发布日期	2012/11
背景介绍	本报告介绍了安天在 APT 检测方面的经验及近年来在对抗 APT 方面的工作。		
版权说明	本文版权属于安天实验室所有。本着开放共同进步的原则，允许以非商业用途使用自由转载。转载时需注明文章版权、出处及链接，并保证文章完整性。以商业用途使用本文的，请联系安天实验室另做授权。联系邮箱：resource@antiy.cn 。		

基于动态分析的 APT 检测技术研究

安天实验室安天实验室反病毒引擎研发中心 Andy&CuteK

编者按：*2012 年 11 月 12 日至 14 日，第十五届 AVAR 国际反病毒安全会议在杭州举行。安天实验室研发负责人在大会上做了题为《基于动态分析的 APT 检测技术研究》的英文报告，报告中介绍了安天在 APT 检测方面的经验及近年来在对抗 APT 方面的工作。报告中指出基于动态分析系统可以判定网络中传输的文件是否利用了已知或未知的漏洞，从而发现可能的 APT 攻击中搜集信息和渗透行为。本文根据大会报告整理形成的论文，并在技术文章汇编（十）中首次公开。*

关键词：

APT：高级持续性威胁(Advanced Persistent Threat, APT)

C&C：命令与控制(Command and Control)

1 摘要

在信息化高速发展的今天，网络安全正面临着全新的挑战。高级持续性威胁（APT）不断发展升级，也许就在我们认为一切正常时，APT 攻击正在发生或已然完成。攻击者不再是原有意义上的恶意代码作者或黑客，通过宽泛的大面积攻击以获取部分利益；而是有组织团队、具有极强目的性的持续性攻击。

由于上述的特点 APT 攻击的对象必然是有所选择的，为了利益的最大化，他们选择的目标开始转为企业甚至是政府。也正是上述的这些特点导致了企业防御成本的增加，防范难度的加大。APT 攻击组织会通过各种手段收集目标的信息，不断的利用最新的漏洞甚至是已知漏洞对目标进行定点的攻击。

自 2010 年 1 月 Google 在其官方微博承认自己遭受到网络攻击后，APT 就成为信息安全界的一个热门话题。这两年随着 Stuxnet 事件、Duqu 事件以及 Flame 事件的接连发生，如何发现和应对 APT 成为一个新的挑战。

第一，简介

APT(Advanced Persistent Threat)即高级持续性威胁，通常是指在某个组织(如国家或财团)的支持下针对一个特定的目标使用比较高级的技术进行持续的攻击。这种攻击通常具有很强的破坏性，手段比较隐蔽，持续时间较长，这种攻击造成的后果也是极其严重的。

APT 并不是一个新的技术，其主要采用的是最新的漏洞利用溢出攻击目标并进行远程控制。对于溢出和远程控制的检测传统上杀毒软件通过特征码技术以及及时的升级。但由于杀毒软件的特征码以及简单的启发检测受到资源和时间的限制，对于变化的新的样本难以及时发现。针对恶意代码的动态分析技术也有很多包括类似 CWSandbox 为代表的 Ring3 级别的监控程序，主要运行在虚拟机或者冰点还原系统内部，可以对恶意代码的进程相关的 API 调用做记录。但由于该分析系统只是停留在简单的监控，对于分析的结果缺乏进一步的提炼挖掘和识别，所以在恶意检测上还需要更进一步；另一个自动分析恶意代码的系统是 Threatexpert，该自动化分析的主要技术方案是通过快照对比方式发现恶意代码运行前后的对系统的修改，同时也使用 Hook 的方法对系统进行监控，模拟一定的网络应答，触发一些网络行为。由于其是全封闭状态，所以很多网络行为无法捕获，只能捕获模拟开始的几个包。Anubis 系统主要采用对 QEMU 的修改这种方式的好处是比较底层，但是解析指令比较复杂，特别是一些上层的 API 调度，到了系统底层就变化为基本的操作，所以 Anubis 系统的记录的行为多是以对系统修改为主。由于 APT 可能采用多种格式入侵，特别是文档类型的格式，一些反 APT 产品如 FireEye 的设备中已经出现支持文档类型、PDF 等恶意代码的动态分析。

本文采取的主要检测方法是依托白名单和动、静态分析技术对一个网络进行立体的防御，达到尽可能的缩短检测时间，尽可能全面的检测 APT 威胁。

第二，攻击技术特点研究

a) 高级可持续攻击介绍

APT 主要是指有组织，有能力且针对特定相关目标所发动功击。APT 是一种攻击类型，其主要针对企业、政府以及军事领域发起有针对性的攻击，具有极高的目的性、阶段性与长其潜伏的特性。为了发起 APT 攻击，攻击者会进行针对性的资料收集，对被攻击的目标进行深入分析。通常来说攻击者具有较强的网络安全相关的技术能力。

i. APT 攻击与传统攻击的区别

- **目标及针对性**

APT 攻击具有极强的针对性，发起攻击时目标明确，通常以企业、政府、军事领域为主要攻击目标。而传统攻击以经济利益的获取为主要目的，其通常不以特定的目标为攻击点，所以对应的攻击目标具有不确定的因素。两者之间希望达到的目的不同，导致了攻击目标不同，其针对性也有较大的差异

- **可控性的区别**

由于所攻击的目标及针对性的区别，导致了两者的传播方式具有较大的不同，传统的攻击为扩大非法获取经济利益，其传播方式以大面积的传播为主。而 APT 攻击由于针对目标明确，一切以接近攻击目标为主要目的，因此传播方式可控(如在 Stuxnet 样本存在针对时间的判定，当计算机的时间大于 2012/04/24 则不进下一步的操作)。甚至对于特定目标进行传播。

- **长期潜伏性区别**

APT 攻击在完成攻击后持续潜伏，直到锁定目标或接收到攻击指令后才发起下一阶段的攻击，而传统的攻击通常在攻击成功后会立即进行后续的操作。甚至被 APT 攻击所入侵“被控主机”仅仅被用来作为跳板，进行下一步的持续搜索，直到锁定目标。而传统攻击往往是攻击成功后会立即或间隔时间较短的情况下进行下一步的操作。

下面简单的将其与传统的攻击手段做一下比较：

	APT	**传统攻击手段**
时间	从确立攻击目标，到开发攻击工具，实施攻击等过程时间很长	通常时间较短
动机	通常窃取攻击者感兴趣的机密，通常是国家或企业的重要机密。也可能是攻击国家机构或企业因此为其带来重大的损失	目的不一，通常是为了经济利益
攻击者	有实力的团体甚至是国家	个人或者较小规模的组织
攻击对象	具有明确的针对性，如政府机构，科技企业等	一般不具有明显的针对性
攻击手法	通常通过社会工程，借助 0Day 实现入侵，然后使用复杂的手段完成后续动作。通常是针对该目标为其开发的	手段单一，持续时间短。使用的工具比较常见

	APT	传统攻击手段
	相关的工具。	

表 错误!文档中没有指定样式的文字。-1 传统攻击手段比较

通过前面的对比，我们可以看到 APT 通常是一个非常复杂的攻击过程，需要精心准备。攻击者需要明确攻击的目标，搜集相关的信息，然后利用一些未公开的手段，十分隐蔽的实现其目的。这个过程需要较大的投入，通常情况下只有政府或财团才能够具备这样的实力。通过对 Stuxnet 和 Duqu 的关联性比较，信息安全产业普遍认为 APT 存在着一个产业链，并且其开发平台已经成熟。

ii. APT 的攻击的特点

- **混合的攻击手法**

APT 攻击往往采用混合式攻击的手法，包括通过社交工程发送恶意的 URL、利用格式溢出的漏洞发送含有恶意程序的邮件附件，然后恶意软件释放数据并且通过文件共享、移动储存介质横向扩散，在攻击目标成功后收集高价值的数据或进行破坏性攻击。

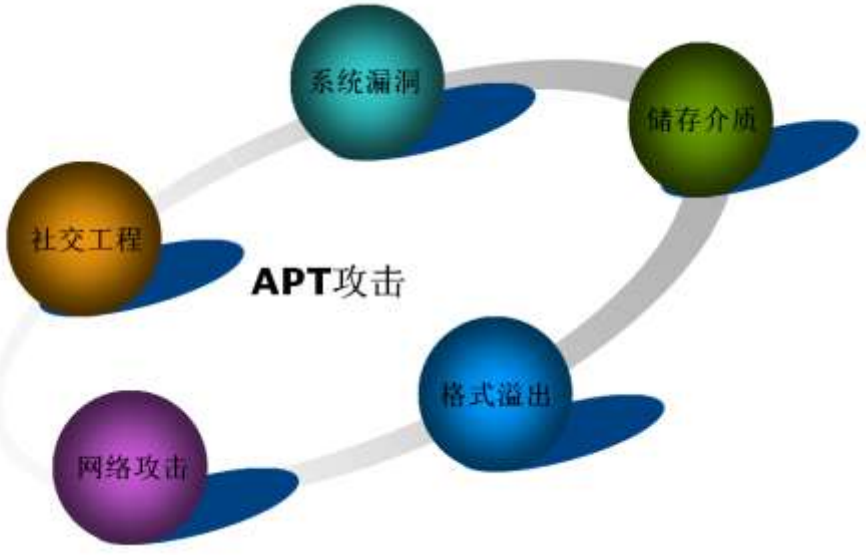

图 3-1 APT 的攻击手法

- **持续的攻击活动**

APT 攻击通常是一个持续的攻击活动，而非单一的攻击事件。在攻击的过程中会利用各种攻击手法不停的尝试，直到达到目的为止。我们可以通过一个事件了解到 APT 攻击的持续性，其实早在 2011 年年底，Kaspersky 实验室已经在报告中提出 Duqu 木马和 Stuxnet 蠕虫的作者是同一个人（或者团队）的观点，并在另一份报告中提出 Duqu 木马可能早在 2007－2008 年之间就已出现，而其主要目的正是收集一系列有关伊朗企业和政府情报机构活动的数据。似乎先有 Duqu 木马后有 Stuxnet 蠕虫的假设，更符合实际情况（即先用木马收集详细数据再用蠕虫实施精确攻击）。

比较项目	Duqu 木马	Stuxnet 蠕虫
功能模块化	是	
Ring0 注入方式	PsSetLoadImageNotifyRoutine	
Ring3 注入方式	Hook ntdll.dll	
注入系统进程	是	
资源嵌入 DLL 模块	一个	多个
利用微软漏洞	是	
使用数字签名	是	
包括 RPC 通讯模块	是	
配置文件价解密密钥	0xae240682	0x01ae0000
注册表解密密钥	0xae240682	
Magic Number	0x90,0x05,0x79,0xae	
运行模式判断代码存在 Bug	是	
注册表操作代码存在 Bug	是	
攻击工业控制系统	否	是
驱动程序编译环境	Microsoft Visual C++ 6.0	Microsoft Visual C++ 7.0

表 错误!文档中没有指定样式的文字。-2 Duqu 木马与 Stuxnet 蠕虫的对比

- **明确的目标**

在 Stuxnet 蠕虫的分析中，我们可以看到 Stuxnet 是专门针对 WinCC 系统进行攻击。那么 WinCC 之后又发生了什么？

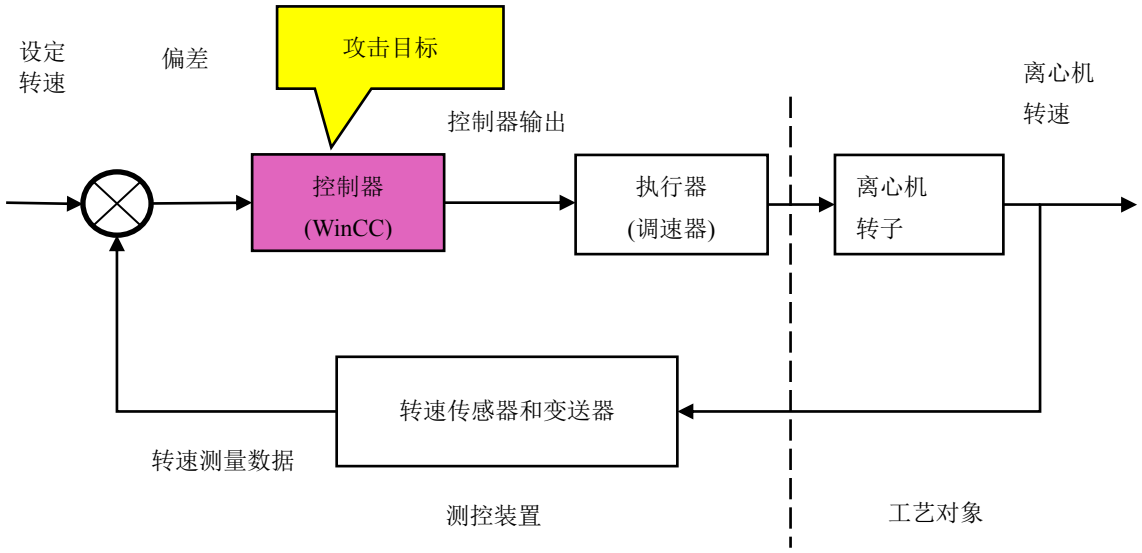

图 3-2 离心机感染示意图

一台伊朗 IR-1 型离心机的转速为 1064 赫兹，当离心机第一次被病毒感染出错时，会持续以 1410 赫兹的转速运转 15 分钟，然后回到正常转速。27 天以后 Stuxnet 蠕虫病毒再次发起攻击，这次让离心机以低于正常转速几百赫兹的速度运转了 50 分钟。离心机出错产生的过度离心力让铝管扩大，提高了离心机部件相互冲撞的危险，最终可能导致离心机的摧毁。

b) APT 攻击过程分析

现有的常规方法很难检测和防御 APT 攻击，因为 APT 是一个复杂的长期的过程，同时还会使用一些比较隐蔽的方法如 0day。通过对 APT 攻击过程的分析，我们可以了解 APT 的相关细节从而做到有效的预防和防御。

我们这里把 APT 攻击的过程分为六个阶段，这六个阶段覆盖了常见的 APT 攻击的过程。这六个过程如下：确立目标，信息搜集和攻击方法的准备，渗透目标，控制目标，扩展攻击目标，窃取机密或破坏目标。下面我们将针对这六个阶段进行详细的分析。

i. 确立目标

由于 APT 的背后往往有巨大资源支持，需要投入大量的人力和财力，所以要攻击的目标往往是对发动攻击者或者支持者有很大的利益。被攻击的对象通常是拥有很高的机密，商业价值，或者影响巨大的结构或组织。这些被攻击的对象往往是政府部门，金融机构，知名公司等。

以震惊世界的“超级武器”Stuxnet 蠕虫为例，它的攻击目标是西门子公司的 SIMATIC WinCC 系统。这是一款数据采集与监视控制（SCADA）系统，被广泛用于钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域，特别是国家基础设施工程；它运行于 Windows 平台，常被部署在与外界隔离的专用局域网中。WinCC 已被广泛应用于很多重要行业，一旦受到攻击，可能造成相关企业的设施运行异常，甚至造成商业资料失窃、停工停产等严重事故。一些专家认为，Stuxnet 病毒是专门设计来攻击伊朗重要工业设施的，包括当时刚刚竣工的布什尔核电站。

从而我们可以看到 APT 的攻击目标很明确，而且具有很强针对性。但是并不是说 APT 对于小企业没有威胁。随着 APT 的发展，小企业也逐渐成为被攻击的对象，甚至也可能会通过小企业作为跳板间接实现其攻击目的。

3.2.2 信息搜集和攻击方法的准备

在攻击目标确立之后，下一步便是开始搜集信息。搜集的方法可以是很简单，但是通常情况下很有效。可以使用搜过引擎搜索与要攻击对象相关的关键词。通常情况下可以搜索到不少信息。同时通过社交网站（如 Facebook、Twitter）搜索与该目标相关的信息（如该目标的雇员的名字，邮件或其他联系方式，甚至他的职务等信息），很多人办公邮件会和其网名或昵称相同，同时有可能他的多个账户使用同一个密码。另外通过社交网站可以轻易的了解一个人的爱好，这也是一个很好的发起攻击的突破点。

在信息搜集的足够可用后，APT 攻击的发起者开始开发对应的攻击工具。通常购买一些 0day 开发对应的攻击方法，同时还会开发渗透成功后，远程控制相关的功能(C&C)。通常 APT 的开发会以团队的形式开发，并且开发的平台通常是专有的。这些平台功能齐全，并且开发的速度很快。这一点可以从 Stuxnet 的分析中找到一些影子。

例如 Stuxnet 使用了影响比较大的漏洞包括 MS10-046、MS10-061、MS08-067 等，同时还用到了两个针对西门子 SIMATIC WinCC 系统的漏洞。

3.2.3 渗透目标

通常情况下，APT 要攻击的目标是被严密保护的。目标所在的网络和外界是隔离的，同时还有各种保护设备。APT 攻击这需要找到恰当的入口，渗透进去。常见的渗透方法如下：

- ✓ 通过 SQL 注入等方式入侵要攻击目标的 web server，然后伺机进入要攻击的目标的内网。
- ✓ 通过发送欺诈邮件或暴力破解等手段获取更高的权限。著名的域名为 rootkit.com 的网站就是由黑客冒充管理员发送邮件，轻易地获取了其他的管理员的账户和密码。
- ✓ 通过向与被攻击对象相关人员发送求职或与政治相关新闻事件等内容的邮件，骗取其点击。通常这些邮件会附带一些附件，这些附件是利用某些漏洞构造的特殊文件，攻击者通过这些附件触发相应的漏洞，然后再继续下一步的动作。

2011 年发生了"RSA Secur ID 被窃取"的事件中，黑客发送了名为"2011 Recruitment plan(2011 年招聘计划)"的邮件给 RSA 员工。截图如下：

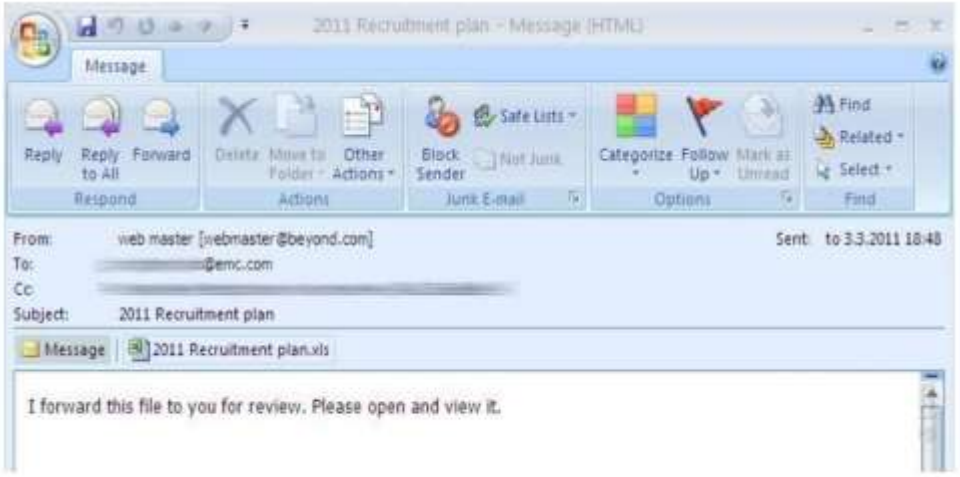

图 3-3 邮件截图

该邮件附带了一个名为“2011 Recruitment plan.xls”的附件，该附件利用了一个 Adobe 解析 Flash 文件格式的漏洞。当它被打开时触发了相应的漏洞，然后执行相应的恶意的代码。

3.2.4 控制目标

在成功的渗透进要攻击的目标后，APT 开始在目标网络中搜集信息找到其感兴趣的目标，然后通过网络协议和 C&C 服务器通讯。APT 攻击者就可以控制该目标实现其进一步的目的，下图是一个 Stuxnet 的一个例子。

```
100197F1 sub_100197F1 proc near
100197F1 push     ebp
100197F2 mov      ebp, esp
100197F4 and      esp, 0FFFFFFF8h
100197F7 push     offset aRpcss    ; "rpcss"
100197FC call     sub_10019819
10019801 push     offset aNetsvcs ; "netsvcs"
10019806 call     sub_10019819
1001980B push     offset aBrowser ; "browser"
10019810 call     sub_10019819
10019815 mov      esp, ebp
10019817 pop      ebp
10019818 retn
10019818 sub_100197F1 endp
```

图 3-4 Sstuxnet 例子

3.2.5 扩展攻击目标

APT 攻击这可以通过网络协议和可控制的对象通讯后，可以从目标的机器上搜集信息。然后提升权限，并将攻击对象扩展到网络内的其他目标为对象。同时在目标机器通过可控制命令安装功能更加强大的工具甚至是更新攻击程序等。这个时候 APT 会借助一些 rootkit 技术将自己隐藏起来，然后长期的“潜伏”。

值得一提的是 2011 年 3 月 RSA 的 RSA SecurID 被窃取后，黑客凭借从 RSA 获得的 SecurID 通过身份认证，侵入武器制造商洛克希德马丁。从这里可以看出一旦一个目标被攻破后后续的影响会有多大。

3.2.6 窃取或破坏目标

APT 攻击的主要目的是窃密或者破坏目标，在这个阶段 APT 基本上已经可以为所欲为了。一旦被攻击的目标的信息被窃取或者目标被破坏将会给受攻击者带来巨大的损失。

3.3 典型案例

下面我们看以下几个 APT 的案例，以更加具体的了解一下 APT 攻击的特点。

3.3.1 极光行动(2009-2010)

极光行动(英语：Operation Aurora)是发生于 2009 年 12 月中旬可能源自中国的一场网络攻击，其名称“Aurora”（意为极光、欧若拉）来自攻击者电脑上恶意文件所在路径的一部分。遭受攻击的除了 Google 外，还有 20 多家公司：其中包括 Adobe Systems、Juniper Networks、Rackspace、雅虎、赛门铁克、诺斯洛普·格鲁门和陶氏化工。

根据网络资料和我们的分析结果，将这个极光行动的攻击过程还原如下：

- ✓ 攻击者网络上搜集 Google 员工的相关信息，伪造一个网站诱使 Google 员工访问。
- ✓ Google 员工访问伪造的网站，该网站的页面中有一段包含利用 IE 漏洞获得执行权的 javascript 代码。漏洞被成功利用后，执行相应的 shellcode。shellcode 远程下载更多的程序并执行。
- ✓ 然后通过 SSL 的方式与攻击发起者进行通讯。然后持续的监听该员工的电脑并且窃取该员工访问 Google 服务器的账户密码信息等。
- ✓ 利用该员工的凭证进入 Google 邮件服务器，进而获取相关的信息。

3.3.2 夜龙行动(Night Dragon 2007-2011)

2011 年 2 月 10 日，知名信息安全公司 McAfee 发布了一份标题为“全球能源网络攻击：(Night Dragon)”的分析报告。McAfee 在报告中称有 5 家西方跨国能源公司遭到了“来自中国的黑客”的“有组织，隐蔽，有针对性”的攻击。超过千兆字节的敏感数据被窃取。这其中包括气油田操作的机密信息，项目融资和投标文件等。

夜龙攻击的过程如下：

- ✓ 通过外网的 web 服务器作为突破口，使用 SQL 注入等方法入侵 web 服务器。
- ✓ 以被攻陷的 web 服务器作为跳板，对内网的服务器或桌面机器进行入侵。
- ✓ 如果内网的服务器或者开发者的电脑被攻破，可能是暴力破解了密码。

- ✓ 被攻陷的机器被植入恶意程序，通常为远程控制工具。然后传回大量的机密信息。
- ✓ 继续持续的攻击内网内的其他的机器，寻找更有价值的目标。

3.3.3 暗鼠行动(Shady Rat 2006-2011)

2011 年 8 月份 McAfee 发布了一份报告，详细的披露了暗鼠行动(Operation Shady Rat)。这次行动被认为是从 2006 年开始持续了 5 年。在这个过程中至少有 72 个机构遭受到了攻击，包括安全部门，商业机构，政府部门以及非营利组织。

暗鼠行动的过程主要如下：

- ✓ 通过社会工程搜集被攻击者目标的信息；
- ✓ 目标被选定后，攻击者构造邮件，然后向这些组织的个人发送接收者可能感兴趣的邮件。如联系人列表，会议通知等内容。这些邮件会附带一个附件(可能是 doc，excel，pdf 等格式)。如果接受者打开这些附件，恶意代码就可能会被执行；
- ✓ 恶意代码执行后会从网络上下载恶意程序。这些恶意程序经过精心伪装，安全产品很难发现；
- ✓ 借助恶意程序，受害者的电脑可以轻松地被攻击者控制。

第三，APT 检测技术

通过前面的分析，我们发现大部分的 APT 攻击事件中，高级持续攻击者更倾向于利用 0day 漏洞，或者利用目标公司基础设施存在的漏洞问题。从 Google 到 RSA，这些单位受到攻击的关键因素都与普通员工遭遇社交工程的恶意邮件有关。从 RSA 受攻击的事件可以发现，黑客刚一开始，就是针对某些特定员工发送钓鱼邮件，这就是该起 RSA 遭到黑客使用 APT 手法进行攻击的所有源头。在今年稍早的时候，美国有另外一家信息安全顾问公司 HBGary 也面临类似的攻击方式，那就是黑客假冒 CEO 发信给 IT 部门同事，IT 人员对于黑客冒名发送的这封信件完全不曾怀疑，IT 人员直接将该公司 IT 系统 Administrator 的账号、密码给被黑客冒名的 CEO 发送回去。因此，HBGary 内部的 IT 系统防护也在一夜之间溃堤。

那么即使通信等文件检测成为检测攻击的关键，在整个需要保护的网络内部的关键位置部署检测设备及检测软件应对 APT 攻击也是非常必要的。

a) 恶意 URL 和邮件检测

通过网页溢出和邮件附件是 APT 攻击的主要渠道，APT 攻击普遍采用通发送精心构造的可溢出的格式文件(如 PDF，DOC，XLS)的邮件附件，其目的有两个：

- 针对普通员工，通常不是每一个员工都是安全专家，这是安全防卸的弱点也是最好突破口。
- 通过网页或邮件发给普通员工，有很好的欺骗性，因为一般情况下对于非可执行格式的数据，我们不会过多的关注。

通过旁路监控检测对网络中访问的 URL 和邮件附件进行提取，并进行检测，对于未知的网址和文件则交给动态分析系统进行未知判别。

b) 白名单战略

除了网络邮件和访问的 URL 外，还有一些威胁可能是由于移动介质、手机等传播进入保护系统，这样通过在关键系统部署终端防护软件收集未知的可执行程序，交由内网的动态分析系统进行判别。自动化分析系统建立起来的私有云识别系统，可以实现快速的识别和判断恶意样本。同时通过巨大的白名单库，在保证检出率的基础上降低误报。

c) 基于动态分析的溢出检测技术

支持 Windows 系统中 exe、dll 的分析，对 PE 文件进行深度的格式解析以及行为监控。对静态溢出文档方面的解析和监控，对包括 pdf、doc、xls、ppt、rtf、swf 等常见格式进行监控，监控恶意格式溢出所产生的系统动作行为。不仅能够监视文档的加载进程，并且能够全面的监视系统中的所有进程的活动，用来发现采用 COM 的 WMI 机制的跨进程的系统威胁。

通过内核级及应用层级等多层次监控包括进程操作、文件操作、注册表操作、网络通信访问、网络数据 URL。通过不同层次的监控，发现不同角度的数据，综合的分析，相互补充，可以更加全面的获得监控样本的行为和数据。通过研究 Ring3 级别监控的信息丰富性，多样性，研究 Ring3 hook 全面监控，包括跨进程、服务、远程注入的追踪监控达到恶意代码样本衍生的子进程、服务，注入的全面监控。

通过内核层的监控可以对驱动的行为进行一定的监控，也可以通过上下层对比，发现一些

穿过 Ring3 的直接调用系统功能的恶意行为。

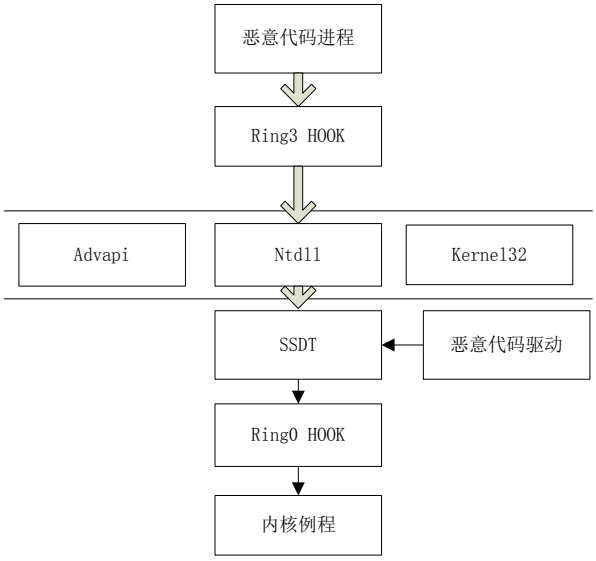

图 4-1 多层监控示意

环境模拟包括对国内常见的软件的安装如 Word、WPS、Adobe Reader 、QQ 等。能够对移动介质模拟，利用文件夹模拟磁盘，并 hook 修改磁盘类型；模拟游戏、杀软进程等用来触发一些对抗和窃取密码等行为；通过环境的模拟，可以更好的对象的行为进行监控，并使系统更加逼真，更加像真实的环境。

隐蔽监控系统的文件、注册表、进程等可能暴露环境的信息；通过 hook 技术以及一些深层的隐蔽手段将监控记录环境的文件、进程隐蔽起来；同时对虚拟机中常见的进程等也可以进行对恶意代码隐蔽。

d) 检测案例

利用邮件发送文档类型附件，比如 doc，xls 等，这些文件具有 0day 漏洞，可以利用操作这些软件的漏洞溢出获得执行权限从而进行网络下载，木马安装等操作。

当邮件监控系统发现附件中包含一个 xls 文件，将会提交给动态分析系统，动态分析系统经过监控分析可以得出该文件是否具有溢出功能，并给出明确的判别。

图 4-2 溢出行为检测

动态分析系统捕获到 xls 的进程 excel.exe 会释放一个动态链接库文件，并将该文件注册为服务，并启动释放一个正常的 xls 文件打开，用以迷惑接收邮件的人。与最新 cve-2012-1535 漏洞，嵌入在 doc 文件的 flash 漏洞一样，都是释放 DLL 文件，并添加启动项。用来达到随机启动的目的。

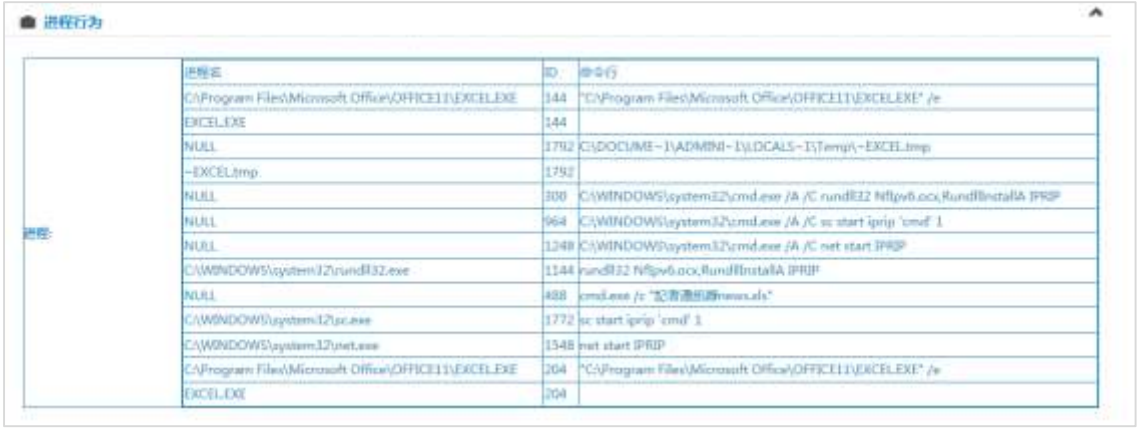

图 4-3 进程创建添加服务

溢出成功后，将会下载执行木马操作，通过其行为可以判断是否具有恶意威胁的样本。对于各种远程控制的木马工具，其基本的行为是具有通用性的，通过动态监控可以发现危险的行为，比如安装，自删除，隐藏文件，添加服务等。

图 4-4 发现危险行为

图 4-5 利用 IE 程序访问网络

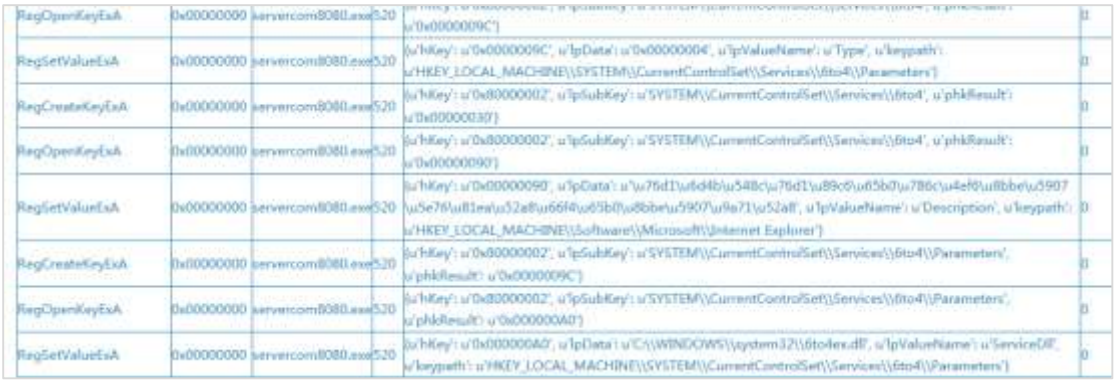

图 4-6 添加到 Svchost 启动的服务列表中

图 4-7 发送主机信息 CPU 信息

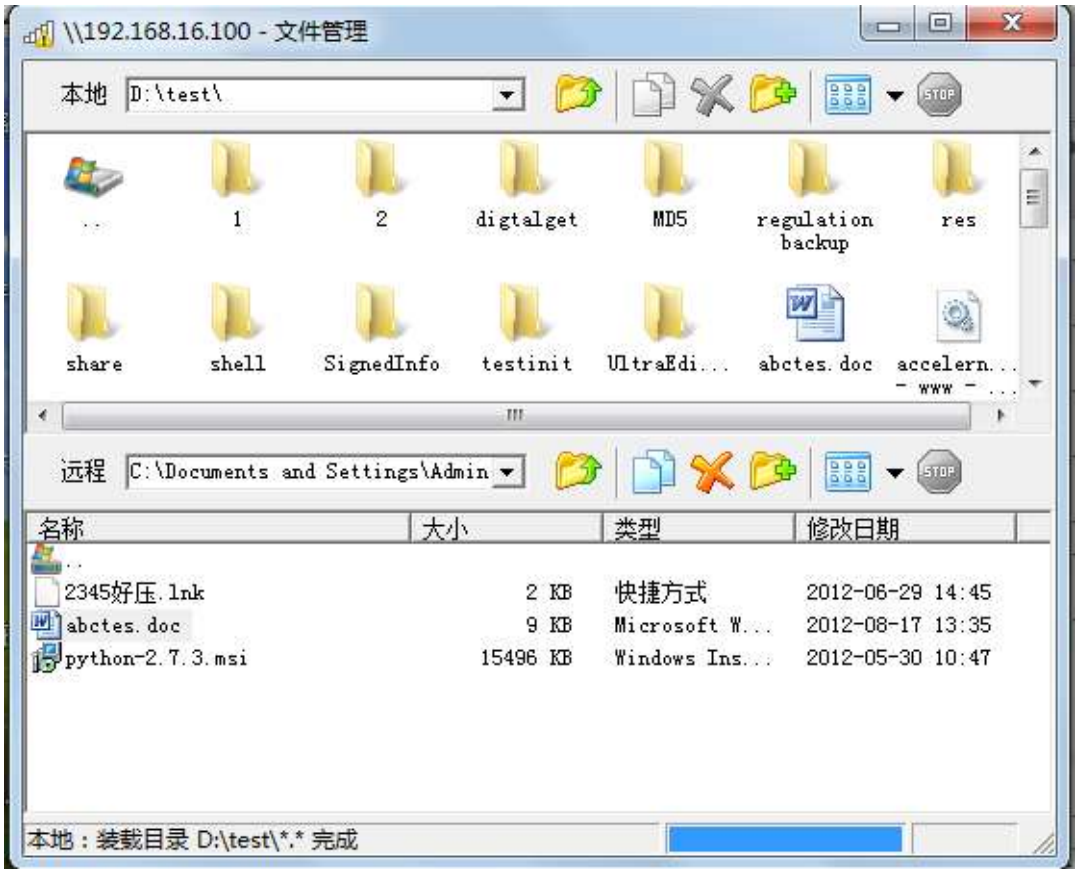

图 4-8 接收查询文件指令

发送文件，读取文件内容，发送到网络，这个序列过程还是很清晰的，有的是加密后发送所以数据很难检测一致。

图 4-9 发送文件序列

第四，总结

本文对 APT 攻击进行了剖析，并提出了相应的防御检测方案，提供了相应的案例和检测案例。通过对 APT 的攻击的过程和案例分析，我们知道 APT 攻击是一个持续性的过程，它的攻击手段也是多样化的，整个过程十分复杂。一旦一个点被突破，可能面临着整个防御系统的崩溃。并通过白名单体系以及未知判别联合动、静态分析达到及时的检测。APT 攻击不是一个单一事件，而是由许多事件的组合而成的。对于每一个可能遭受攻击的对象，都不能够大意。很多时候我们即使发现了攻击，也只是简单的认为是一个“普通的中毒事件”，殊不知后面有十分恐怖的攻击者在窥伺着自己。

但并不是说 APT 完全不可以防范，只要从基础做起也是可以减少遭受 APT 攻击，至少可以减少攻击所造成的损失。防范 APT 攻击要做到如下几点：

- ✓ 加强对员工的安全意识的教育，尤其员工在网络活动中要尽量少的透露在其所在公司的信息，对于不明来源的邮件，文件，网络链接不要轻易接受或打开。
- ✓ 使用安全产品内网进行严格的防护，并不断升级。
- ✓ 制定严格的保密制度和实行严格的保密措施，确保机密信息不会轻易被获取到。
- ✓ 对于一些攻击事件不可以大意，要及时的请专业人员进行分析，避免进一步的损失。

上述方法并不能够完全的避免 APT 攻击，APT 往往会使用一些较高级或未知的技术。这就给传统的检测和防御手段带来了很大挑战。信息安全厂商和研究人员必须不断地研究 APT 的特点并升级检测方法和防御策略，以此来应对 APT 带来的新的威胁。

第五，参考文献

[1] 对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告

http://www.antiy.com/cn/security/2010/Report_On_the_Attacking_of_Worm_Struxnet_by_antiy_labs.htm

[2] 探索 Duqu 木马的身世之谜——Duqu 和 Stuxnet 同源性分析

http://www.antiy.com/cn/security/2012/r120521_001.htm

[3] 对 Flame 病毒攻击事件的分析报告

http://www.antiy.com/cn/security/2012/r120531_001.htm

[4] 蠕虫样本集分析报告

http://www.antiy.com/cn/security/2012/Analysis_Report_on_Flame_Worm_Samples.htm

[5] 2009 姜晓新，段海新，管云涛.恶意代码自动分析技术研究.第六届中国信息和通信安全学术会议(CCICS'2009)， 2009:615-621 Kephart J.O and Arnold W.C. Automatic Extraction of Computer Virus Signatures

[6] http://www.threatexpert.com/

[7] Toward automated dynamic malware analysis using cwsandbox

[8] APT 攻击悄然来袭企业信息面临“精准打击”

http://soft.yesky.com/security/414/30994414.shtml

