More Insights On The APT

Title: More Insights On The Advanced Persistent Threat
Author: Cryin#insight-labs.org
Link: http://insight-labs.org

概述

APT 高级持续性威胁(Advanced Persistent Threat) APT 攻击从收集情报开始，一直到成功窃取机密资料或者达到其攻击目的为止。这可能会持续几天、几周、几个月，甚至更长时间。自 2010 年 Google 承认遭受严重黑客攻击之后，APT 高级持续性威胁便成为信息安全圈炙手可热的名词，是噱头还是真实的威胁？作为安全厂商或许需要的就是噱头。

APT 本身是一个抽象的概括性的概念，并不像 XSS、SQL 注入、BOF、Trojan 这些名词定义的比较鲜明。但对于像 Google、NASA、Comodo 等深受其害的公司而言 APT 无疑是真实的威胁，个人认为 APT 其本质也是平常所见的网络攻击和入侵行为。但与一般网络攻击而言其本身又有自身的特点:

- 长期持续的攻击、控制、潜伏
- 有组织、有计划、有目的的攻击、入侵、窃取数据
- 针对特定目标、组织、企业的定向攻击

简而言之，APT 攻击即是针对特定目标有组织、有计划的进行持续的定向攻击、入侵并以达到获取机密数据的目的。因为 APT 攻击整个过程复杂、持久，涉及技术面比较广，所以 APT 真正的威胁是其实施攻击的人员。

APT 高级持续性威胁攻击过程从收集情报开始,攻击者通过搜索引擎或者一些公开社工库搜集特定目标的信息加以研究并实施攻击； 通常是通过电子邮件、即时通讯、文件下载等方式(当然，黑客也可以通过攻击 Web 网站，控制并进一步入侵网络)，向目标用户系统植入木马、后门等恶意软件，一旦攻击者控制用户系统就可以将其作为跳板进一步入侵更多计算机来搜集信息。并进行后续渗透、发掘有价值的数据所在的服务器并收集机密资料打包外传。

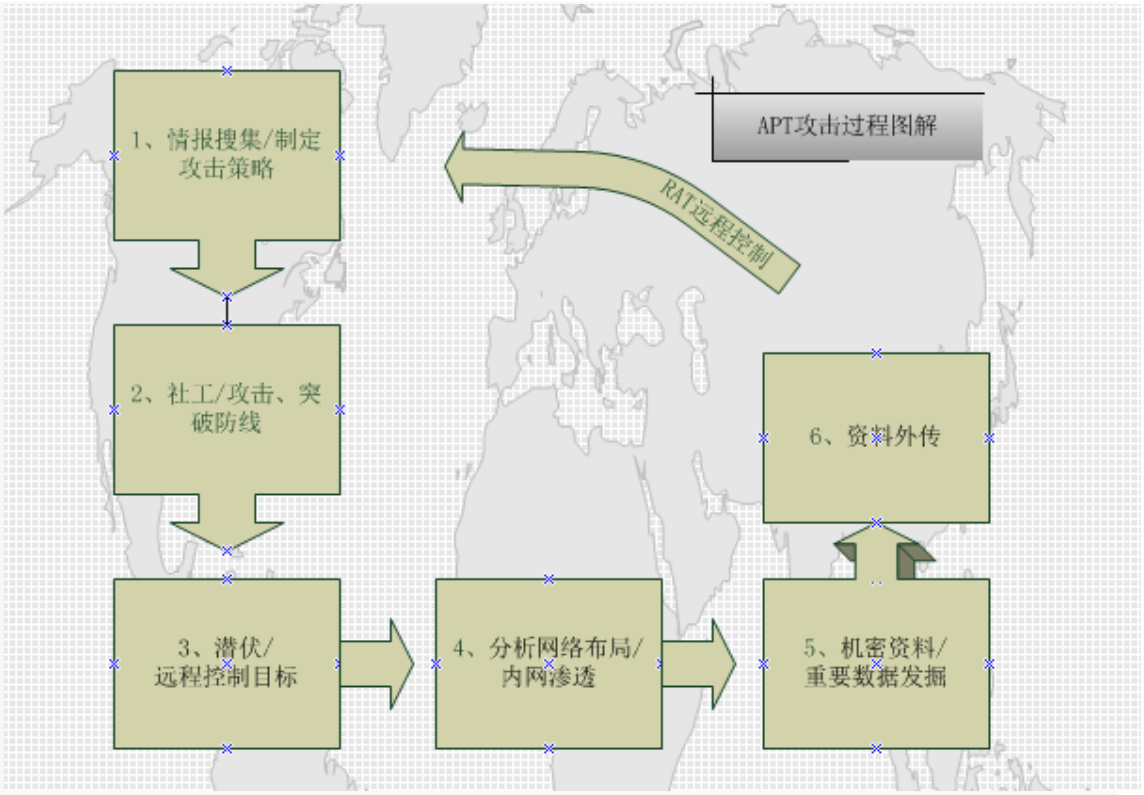


图: APT 攻击过程

APT 攻击简单概括为以下过程:

- 情报搜集/制定攻击策略
- 社工/攻击、突破防线
- 潜伏/远程控制目标
- 分析网络布局/内网渗透
- 机密资料/重要数据发掘
- 资料外传

攻击策略

在网络上看到关于 APT 攻击的文章大多是利用电子邮件作为突破口，攻击者通过发送精心构造好的 Office、PDF 等 Exploit 利用文档诱使用户打开并触发漏洞执行恶意代码并植入 RAT 等恶意软件。但个人认为 APT 攻击并不只是局限于此，通常攻击者有很多方法可以打开突破口，比如钓鱼、攻击 Web 服务器、利用 IE 等浏览器漏洞挂马，甚至是结合社会工程学利用即时通信软件直接给目标用户发送可执行的 RAT 恶意程序等。
APT 高级持续性威胁目前来看更多的是利用 Office、PDF 等文档型漏洞，结合社会工程学通过电子邮件、即时通讯、文件下载的形式发送给目标用户，诱使其打开文档。从而植入后门程序。本文着重以电子邮件形式为主进行探讨，如下图 APT 攻击邮件截图:

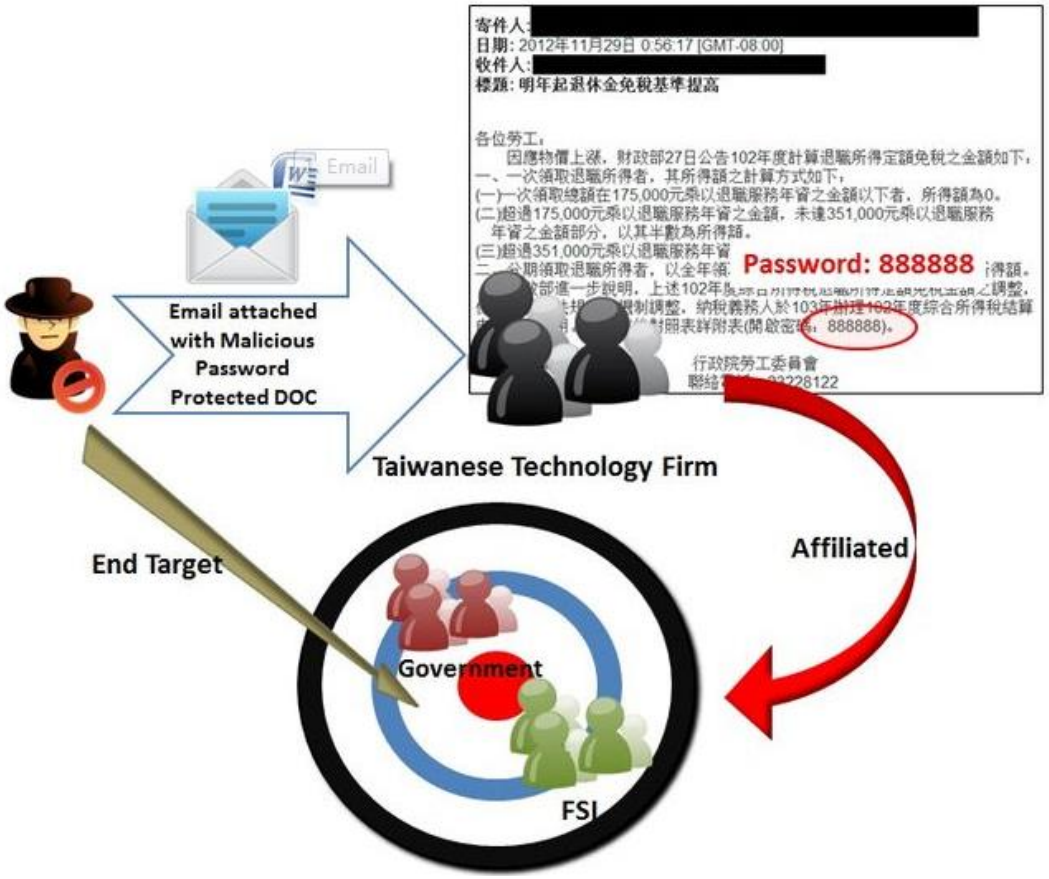


图:APT 攻击邮件

而邮件内容正是根据目标所处地最新的时政热点新闻编写，目标用户如果看过这则新闻又对此感兴趣的话就很容易信任并打开附件文档.

图:新闻内容

· 关于邮件

APT 攻击之前的信息搜集阶段，利用 Google 等搜索引擎和公开的社工库或者目标用户公开的联系方式，很容易获取到目标的电子邮件地址。为了诱使用户信任并打开附件文档。攻击者可以利用钓鱼、邮箱跨站来获取和目标用户或目标用户相关的联系人的邮箱，并利用获取到的邮箱发送攻击邮件，也可以利用相关技术伪装发信人地址诱使目标用户信任并打开邮件查看附件内容。

在邮件内容编写上，可以结合特定目标的信息进行分析发送用户感兴趣的内容，并结合社会工程学编写增加真实性。

· 关于附件

在利用电子邮件进行 APT 攻击中,攻击者通常借助文档型漏洞制作捆绑等利用文件发送附件以达到不被用户发觉的隐藏的目的，其中利用最多的文档类型有:
• 微软 Office 文档: Windows 操作系统广泛普及，Office 文档自然是 APT 攻击人员的首选，其中 Word 的漏洞(包含 RTF)最多，也是 APT 攻击中使用最广泛的；还有 Excel、PPT 等，甚至借助 flash 的漏洞也可以构造出 Word、Excel 等文件的漏洞利用 Exploit

· Adobe PDF 文档:作为漏洞大户，Adobe PDF Reader 的漏洞也为 APT 攻击提供了不少资源。

其它还有 zip、rar、rm、swf、甚至 html 文件类型、chm 以及 rtf 等文件类型，均可以利用其漏洞构造捆绑或者其它恶意文件进行 APT 攻击。近年来，被利用 APT 攻击较多的文件类型及漏洞信息(仅部分漏洞)如下:

· CVE-2010-3333:Microsoft Word RTF 文件解析栈溢出漏洞(MS10-087)

· CVE-2012-0158:Microsoft Windows Common Controls ActiveX 控件远程代码执行漏洞(MS12-027)

· CVE-2009-3129:Microsoft Excel FEATHEADER 记录内存破坏漏洞（MS09-067）

· CVE-2010-0821:Excel SxView 记录解析远程代码执行漏洞（MS10-038）

· CVE-2010-2883:Adobe Reader CoolType.dll 库 TTF 字体解析栈溢出漏洞

· CVE-2010-2884:Adobe Flash Player Unspecified Remote Code Execution Vulnerability

· CVE-2010-3654:Adobe Flash Player authplay.dll 库 PDF 文件解析远程代码执行漏洞

实例分析

这里主要以利用电子邮件进行 APT 攻击的实例进行分析和介绍，上面说了攻击者通常借助文档型漏洞制作捆绑等 Exploit 进行攻击。其中漏洞比较多并且利用也比较广泛的就是

Word 和 PDF 两种文件类型，对于 APT 攻击实例应用中两种类型并无本质区别，这里以 Word 文档类型实例分析。
文件型 Exploit 一般利用文件自身的漏洞，目标用户打开攻击者精心构造的恶意文档的同时触发漏洞，攻击者控制并接管程序执行流程，跳转至预先构造好的 Shellcode。
Shellcode 是攻击者构造好并放在文件中的恶意代码。其本身能实现几乎任何一个编程语言能实现的所有功能，但在真实的攻击中一般常见的是下载执行类 Shellcode 以及 Bindfile Shellcode。下载执行类 Shellcode 的功能是在特定的 URL 或者 FTP 等链接下载恶意程序到用户系统本地并执行。Bindfile Shellcode 的功能是将捆绑在文档中的恶意程序释放在本地并执行，一般也会释放一个正常的文档并打开给用户。当然还有一些 DLL 劫持的漏洞就不需要负载 Shellcode，只需降将 DLL 文件一同传输并放在同个目录即可触发并执行恶意代码。比较常见的是捆绑类型，所以这里分析 Bindfile 类型攻击实例。捆绑型恶意文档由四部分组成，此类恶意文档一般组成结构如下图:

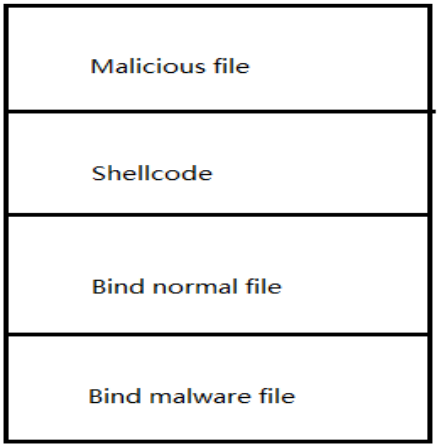
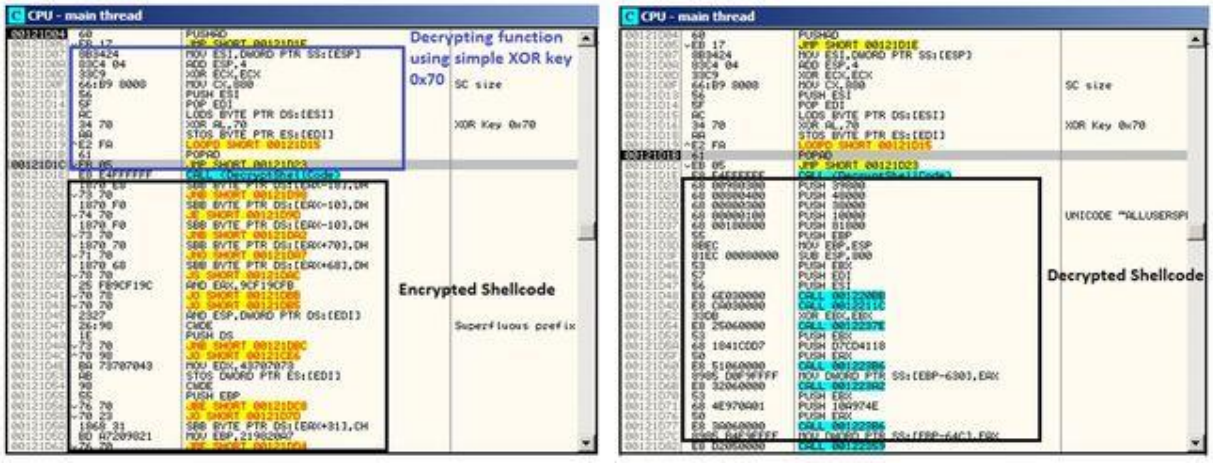


图:恶意文档一般组成结构

其中 Malicious filee 是用来触发漏洞的文件头或者文件，漏洞出发后程序执行流程交给 Shellcode 继续往下执行，Shellcode 功能主要负责解密 Bind normal file、Bind malware file 并将两个文件释放到用户本地系统然后分别执行 malware file，之后再打开正常的捆绑 normal file 并展示给用户。这样用户看到的只是打开的 normal file。而其它流程在内部已经悄然执行。当用户打开 Word 文档并且 Office 软件存在有的对应漏洞时，捆绑的 malware file 将成功执行，一般情况下此时攻击者就基本可以控制目标用户的计算机系统。



这里 Shellcode 的本身变化可能比较多，但大体捆绑型漏洞利用原理都基本相同，不过大多数 Shellcode 都会经过简单或者稍微复杂的加密处理，在漏洞触发后并跳转至 Shellcode 时，
未加密的部分 Shellcode 会对其加密部分进行动态解密常见方法有 byte 异或、word 异或、dword 异或，其中也有些对 key 进行递增或者递减的异或加密方法，解密时也是如此。
所以如果出现利用 Office 文件类型的攻击时如何分析该类恶意文档及攻击细节？根据上述对恶意文档一般组成结构，结合虚拟机中动态调试，很容易分析该类攻击，当然有些 Word 漏洞利用对其文档进行了加密，此类恶意文档分析稍微困难一些。一般恶意文档网上类似分析很多，这里不再赘述！可以参考 fireeye 的分析文章
<Hackers Targeting Taiwanese Technology Firm>见参考链接。

检测思路

安全研究人员的天性是出现一个新型攻击技术时，我们会去研究它如何攻击，攻击原理，技术细节，及成功复现或者成功实验利用等，在过去几年本人也一直是如此。但如何行成有价值的产品这可能是程序员或者产品经理会想到的。前面说了 APT 攻击到底是噱头还是真实的威胁？作为客户期待厂商提供一个可以解决问题的产品，这是最重要的。目前国内外一般的 APT 防护产品已经比较成熟，比如 fireeye 的 MPS 等。

我心中的 APT 防护产品包括三个方面:

· 安全设备

部署网络入口，基于七层协议识别、解码，并识别、提取文件，基于签名库、引擎事件及关联事件检测方法两种检测机制对已知和为止的漏洞攻击进行检测，并对高危攻击进行阻断。

• 沙箱虚拟机

将可疑恶意文件引入虚拟机或沙箱，通过对沙箱的文件系统、进程、注册表、网络行为实施监控，判断流量中是否包含恶意代码。将可以文档上传云端处理分析。这里难点在于模拟的客户端类型是否全面，如果缺乏合适的运行环境，会导致流量中的恶意代码在检测环境中无法触发，造成漏报。

- 云端管理

海量云集恶意文件样本资源库，专业的应急响应团队，逆向分析可疑攻击样本。攻击事件处理、分析及溯源！专业的安全意识及安全知识课程培训、指导！

上面所述完全个人想法，关于更多的下一代 APT 防护产品可参考 Definitive Guide to Next-Generation Threat Protection!

结束语

关于 APT 攻击的具体分析没有在本文中展现，为在互联网上很容易找到类似的分析文章，关于 CVE-2010-3333、CVE-2012-0158 等 office 漏洞，附件中会给出其漏洞利用工具以供分析。
在这里只是介绍笔者这几年的个人经验和想法，肯定会有不足甚至错误之处。总之希望这篇文章能够对大家带来些许帮助，如果对这篇文章有什么疑问或建议请联系我！

参考

[1]http://www.fireeye.com/blog/technical/cyber-exploits/2010/01/pdf-obfuscation-using-getannots.html
[2]http://www.fireeye.com/resources/pdfs/fireeye-definitive-guide-next-gen-threat-protection.pdf
[3]http://cn.trendmicro.com/imperia/md/content/cn/license/tda10000-2-20120626.pdf
[4]http://blog.trendmicro.com.tw/?p=3178
[5]http://www.fireeye.com/blog/technical/malware-research/2013/02/hackers-targeting-taiwanese-technology-firm.html
[6]http://www.fireeye.com/blog/technical/targeted-attack/2012/12/to-russia-with-apt.html