东巽科技 2046Lab 团队 APT 报告：“丰收行动”

admin 2016-08-08 原创技术文章 阅读(36) 评论(0)

披露声明

本报告由东巽科技 2046Lab 团队编写。

考虑到相关信息的敏感性和特殊性，本报告中和受害者相关的姓名、邮箱、照片、文档等个人信息我们将做模糊处理；涉及到的具体的方位，我们将做放大模糊处理；同时为预防攻击者利用公开信息进行反情报，本报告涉及到的 IP、Domain、URL、HASH 等一系列 IOC（Indicators of Compromise，攻陷指标）我们将做模糊处理。所有 IOC 已经整合到东巽的铁穹产品和东巽威胁情报中心，您可访问以下网址进行查询：https://ti.dongxuntech.com

1 概述

2016 年 7 月，东巽科技 2046Lab 捕获到一例疑似木马的样本，该木马样本伪装成 Word 文档，实为包含 CVE-2015-1641（Word 类型混淆漏洞）漏洞利用的 RTF 格式文档，以邮件附件的形式发给攻击目标，发动鱼叉式攻击。将文件提交到多引擎杀毒平台，发现 54 款杀毒软件仅 8 款可以检出威胁，说明攻击者对木马做了大量的免杀处理。随后，2046Lab 研究人员对样本进行了深入的人工分析，发现其 C&C 服务器依然存活，于是对其进行了跟踪溯源和样本同源分析，又发现了其他两处 C&C 服务器和更多样本。

从溯源和关联分析来看，种种迹象表明，该样本源于南亚某国隐匿组织的 APT 攻击，目标以巴基斯坦、中国等国家的科研院所、军事院校和外交官员为主，通过窃取文件的方式获取与军事相关情报。由于样本的通信密码含有“January14”关键词，这一天正好是南亚某国盛行的“丰收节”，故把该 APT 事件命名为“丰收行动”。

2 时间线分析

2.1 从样本进行分析

通过对所有捕获样本的分析，发现较为早期的两个样本最后修改时间为 2015 年 3 月 9 日（..exe）和 2015 年 5 月 5 日(update_microsoft.exe)，而其他样本的最后修改时间多数在 2016 年 3 月、4 月、5 月，表明攻击的时间至少可追溯到 2015 年 3 月甚至更早，而从 2016 年频繁修改多个样本可以看出，今年的攻击活动尤其频繁。

2.2 从 C&C 进行分析

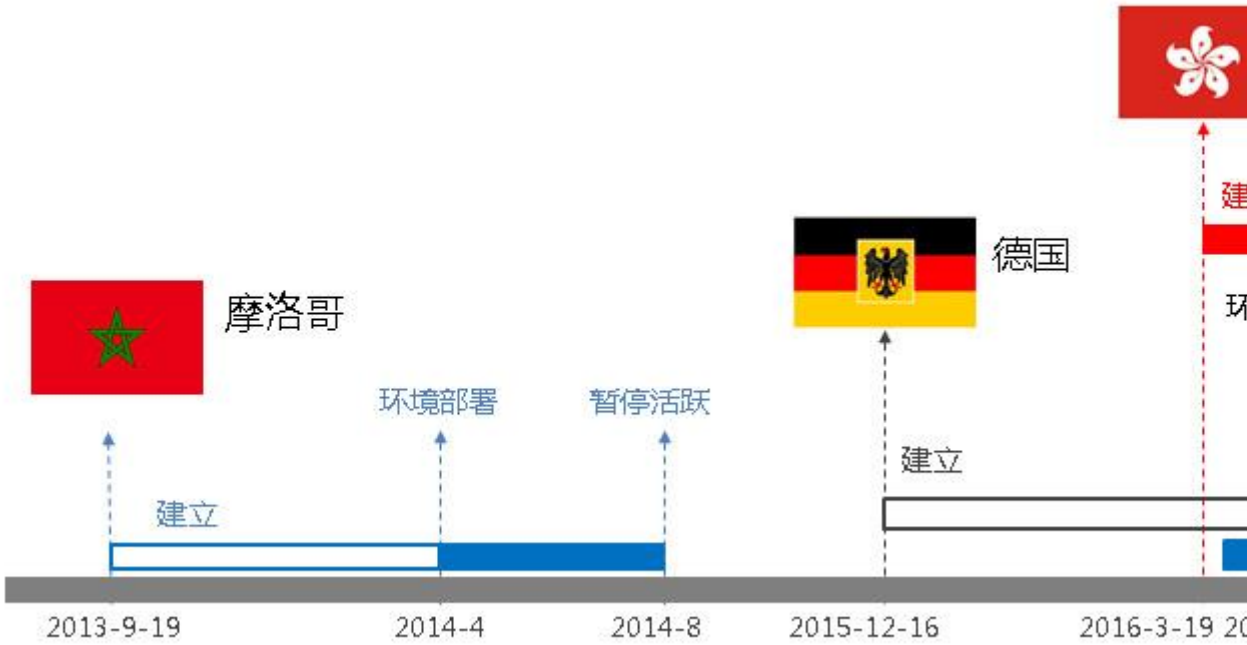


图 1 C&C 建立时间分析

通过对其位于摩洛哥、德国、香港的三个 C&C 服务器的跟踪和溯源，发现其三个据点分阶段建立。其中：

摩洛哥为最早的据点，系统初始化时间可追溯到 2013 年 9 月 19 日，但其真正投入使用部署 C&C 环境为 2014 年 4 月，推测攻击者在这段时间内进行准备工作。随后开始活跃了近 4 个月，然后蛰伏，今年 3 月开始频繁活跃。

德国的据点建立在 2015 年 12 月，但在今年 3 月才开始部署 C&C 环境，然后一直保持活跃至今。

香港是最近时间建立的据点，和前两个据点不同，该据点在 2016 年 3 月开始，短时间内便完成了系统初始化和 C&C 环境部署，然后立即投入使用。后续跟踪过程中发现其 7 月底已失效。

通过对受害者的主机上线时间和 DNS 解析记录分析，我们推测出其主要活跃期为 2014 年 4 月至 8 月和 2016 年 3 月至今。**值得关注的是，与样本分析得到结论一致，今年 3 月至今攻击者尤其活跃,三个 C&C 同时运行。**

1 受害者分析

1.1 区域分析

图 2 受害者区域分布

通过对已知的近 800 名受害者的互联网 IP 进行 Geo 分类统计，得到的统计结论如下：

- 巴基斯坦 77%
- 中国 7%
- 美国 5%
- 英国 0.02%
- 奥地利 0.02%

根据统计结果，推测攻击者主要目标以巴基斯坦为主，中国次之，其中中国以北京区域为主，零星有江苏、内蒙、河北区域。

1.1 领域和群体分析

通过对受害者邮箱、所在单位进行分类统计，我们基本确定攻击者攻击的主要目标领域为：

- 科研院所
- 军事院校
- 外交官员

在这些领域中的又以对外联系人、教授、官员为主要目标。比如***@gmail.com 为某国空军将军相关邮箱，***@***.edu.**为某国防大学官方邮箱。通过对跟踪获得的信息分析，发现被窃取的文件包含部分大使馆通讯录和军事外交相关的文件，与分类统计中以科研院所、军事院校和外交官员为目标的分析结果相吻合。

1.1 领域和群体分析

通过对受害者邮箱、所在单位进行分类统计，我们基本确定攻击者攻击的主要目标领域为：

- 科研院所
- 军事院校
- 外交官员

在这些领域中的又以对外联系人、教授、官员为主要目标。比如***@gmail.com 为某国空军将军相关邮箱，***@***.edu.**为某国防大学官方邮箱。通过对跟踪获得的信息分析，发现被窃取的文件包含部分大使馆通讯录和军事外交相关的文件，与分类统计中以科研院所、军事院校和外交官员为目标的分析结果相吻合。

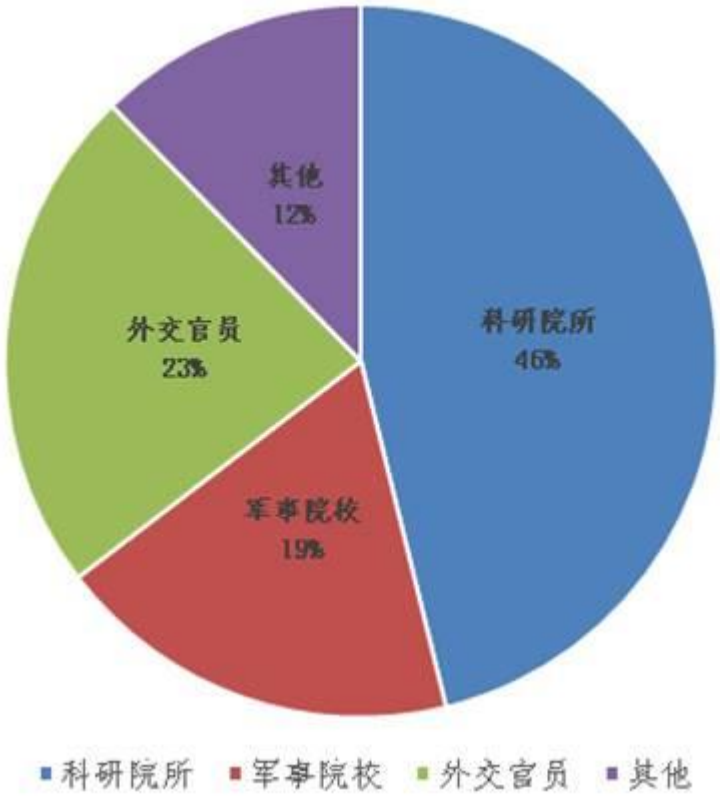


图 3　受害者群体、领域分析

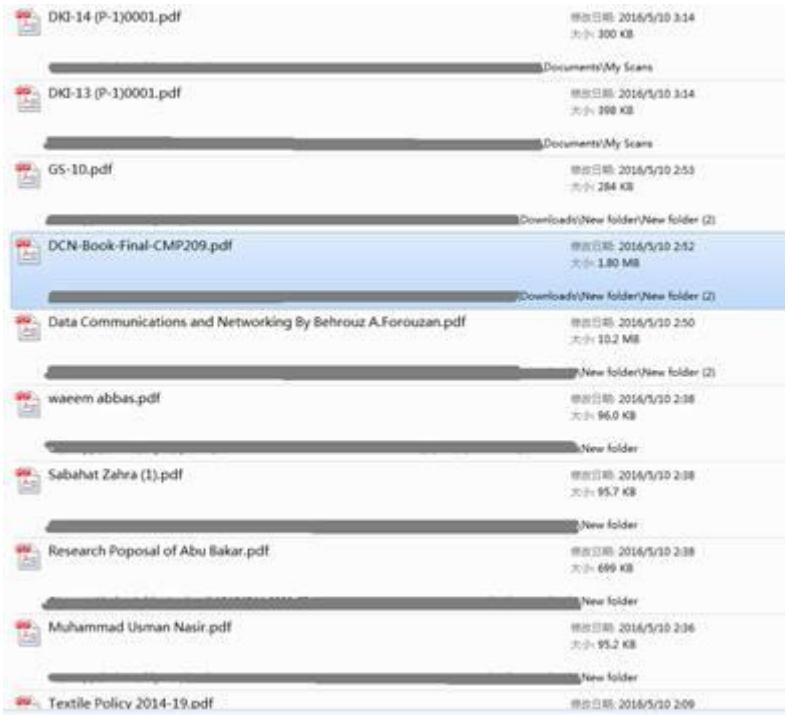
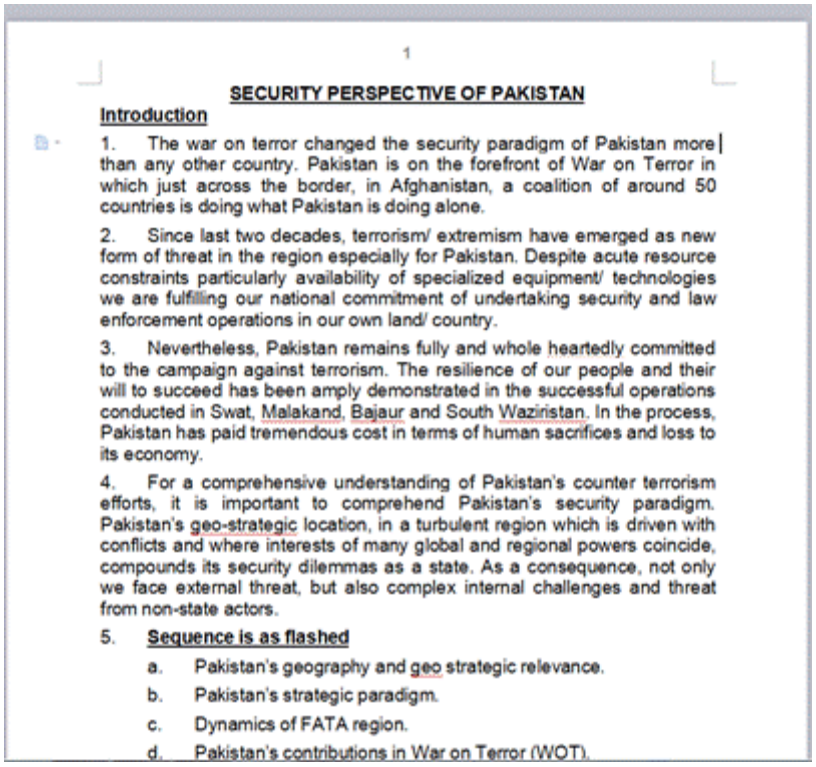


图 4　失窃文件截图



1

SECURITY PERSPECTIVE OF PAKISTAN

Introduction

1. The war on terror changed the security paradigm of Pakistan more than any other country. Pakistan is on the forefront of War on Terror in which just across the border, in Afghanistan, a coalition of around 50 countries is doing what Pakistan is doing alone.

2. Since last two decades, terrorism/ extremism have emerged as new form of threat in the region especially for Pakistan. Despite acute resource constraints particularly availability of specialized equipment/ technologies we are fulfilling our national commitment of undertaking security and law enforcement operations in our own land/ country.

3. Nevertheless, Pakistan remains fully and whole heartedly committed to the campaign against terrorism. The resilience of our people and their will to succeed has been amply demonstrated in the successful operations conducted in Swat, Malakand, Bajaur and South Waziristan. In the process, Pakistan has paid tremendous cost in terms of human sacrifices and loss to its economy.

4. For a comprehensive understanding of Pakistan's counter terrorism efforts, it is important to comprehend Pakistan's security paradigm. Pakistan's geo-strategic location, in a turbulent region which is driven with conflicts and where interests of many global and regional powers coincide, compounds its security dilemmas as a state. As a consequence, not only we face external threat, but also complex internal challenges and threat from non-state actors.

5. **Sequence is as flashed**

   a. Pakistan's geography and geo strategic relevance.

   b. Pakistan's strategic paradigm.

   c. Dynamics of FATA region.

   d. Pakistan's contributions in War on Terror (WOT).

图 5　失窃数据截图

1.2　　和中国相关受害者

我们将中国境内的受害者互联网 IP 做了 Geo 区域统计，得到图 6 结论：

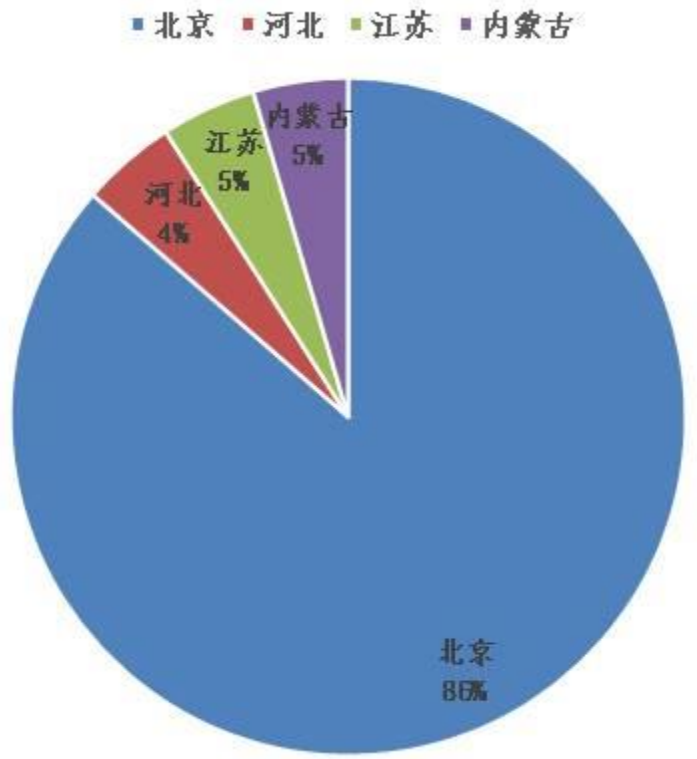


图 6　中国相关受害者区域分布

北京为主要被攻击区域，占到了 86%，其中又以东城区、朝阳区区域为主，考虑到攻击者的目标群体有外交官员，所以推测原因与大使馆多分布在北京的东城和朝阳有关。

对以上受害者被窃取的数据分析，我们发现部分受害者为他国驻华大使馆相关人员，正好与上述 IP 区域分布相符。虽无直接证据证明攻击者的目标直指中国军事情报，但在被窃数据中发现多例受害者间接暴露了中国某些军工单位以及和军队相关的敏感信息。

2 攻击者画像

三个 C&C 服务器，分阶段建立；以科研院所、军事院校、外交官员为目标；近三年持续采用鱼叉、水坑方式进行攻击。其幕后的组织是谁？来自哪里？在研究人员的追踪和分析后，发现了一些端倪。

2.1 他们是谁？

2.1.1 从攻击工具分析

在本次“丰收行动”中，攻击者使用了三套远程控制工具，其中两套远程控制工具与已知的 Darkcomet-RAT[1]有关，作者为法国的 Jean-Pierre Lesueur(通过 LinkedIN 了解)，该作者以 darkcoderSC 为昵称开设了 Facebook、Twitter、G+等社交网络账号，我们推测其与该事件关联性较小，只是远程控制工具的售卖者。

同时，我们还发现在这两款远程控制工具的版权中注释了部分 darkcoderSC 的版权，而以“Green HAT Group/Team”字样出现，我们暂未发现 darkcoderSC 隶属于“Green HAT Group/Team”的线索，所以推测该组织被雇佣对远程控制工具进行过二次修改，或者事件背后组织的名字就叫“Green HAT”，不幸的是在搜索引擎和社交网络中暂未能搜索到与之相关的信息，所幸的是这个名字与中国传统文化习惯完全相悖，加之报告后面的一些重要线索，国外厂商的某些言论是站不住脚的。

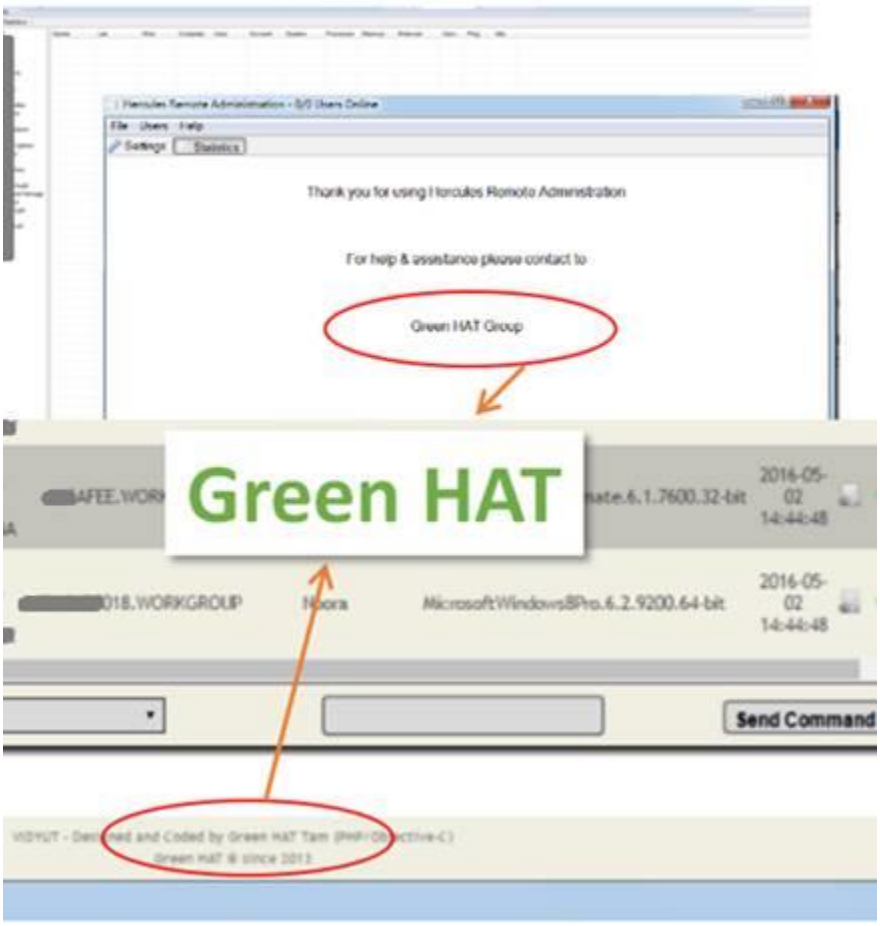


图 7　远程控制工具中的版权关键词“Green HAT”

两套远程控制工具中残留了部分历史部署信息，从中我们发现“sitar”、“Avatar”两个 ID 频繁出现在部署或调试的数据中，而且出现时间是 2015 年 6 月，说明很早就在准备此次攻击。

图 8　调试/部署 bots 信息

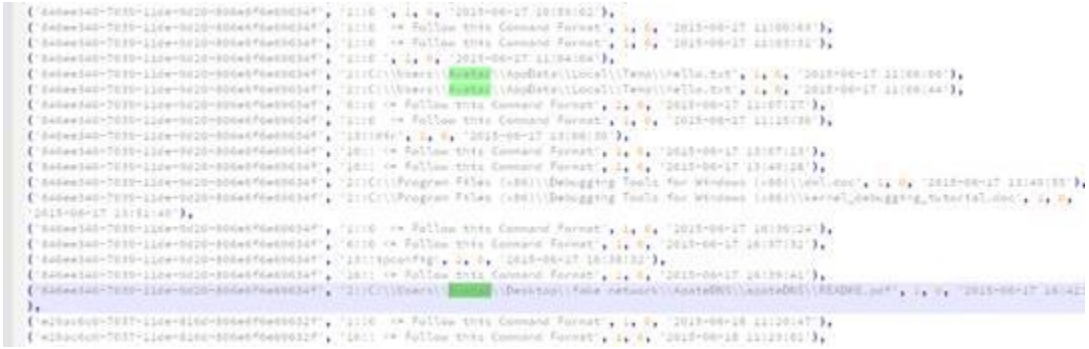


图 9　调试/部署信息，Avatar 为帐户的计算机

图 10　调试/部署信息，sistar 为帐户的计算机

据此，我们推测其组织成员中有“sitar”、“Avatar”为昵称的两个成员。

2.1.2 从关联事件分析

本次攻击者使用的域名多为免费的二级动态域名，所以无法从 Whois 信息中分析注册人和注册组织，但是通过将域名和解析的 IP 与业界报告进行关联分析，我们发现本次攻击者使用的域名和业界报告的某些 APT 事件有重合，如下：

The Dropping Elephant - aggressive cyber-espionage in the Asian region[[2]]

同时，我们发现其域名命名习惯和某些 APT 报告中的域名相似，都以 mico***.***.com 来命名，比如：

https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf[[3]]

所以，如果排除攻击者为了反情报而故意模仿其他攻击组织之嫌，我们推测多起 APT 事件幕后为同一组织。

2.2 来自哪里？

2.2.1 线索一：控制源 IP

攻击者具备很强的反侦察能力，C&C 域名使用了从 freedns.afraid.org 申请的动态二级域名，同时利用了多层跳板来访问和控制 C&C 服务器，这些跳板的来源 IP 包括南亚某国、美国、德国、英国、荷兰等，其中南亚某国的访问最多。

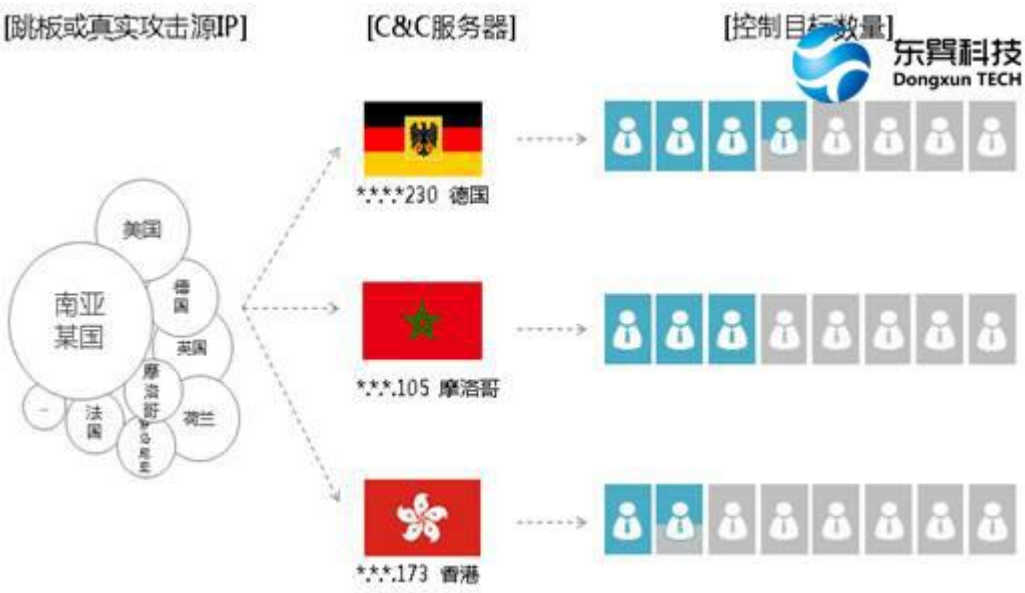


图 11　攻击者来源 IP 的地理区域分布

研究人员对这些 IP 进行了逐个排查，最后锁定了三个方位的 IP：

- 美国：*.*.*.64 和*.*.*.53
- 沙特阿拉伯：*.*.*.68
- 南亚某国：*.*.*.138

随后的深入分析阶段对这三个 IP 进行了研判：

- 美国方位的 IP 段属于 VPS 的 IP 段区，可在 pivateinternetaccess.com 租用，且 IP 对外开放 1723 端口,提供 VPN 服务，确认其为一个跳板；
- 沙特阿拉伯 IP 段出现的频率较少且后续很少出现，未排除其为攻击者真实 IP 的可能性，但推测为被控端可能性较大；
- 在对南亚某国 IP 段分析时，发现其为 Sophos UTM 设备,表明其挂载的至少是一个局域网，故而攻击者来自此区域可能性较大。

2.2.2 线索二：语言文化

在对样本和 C&C 远程控制工具进行分析时，我们发现攻击者将远程控制系统后台通信密码默认设置为“January14”，而这个时间节点是南亚某国盛行的“丰收节”，表明攻击者可能受此风俗习惯影响，有一定的可能性自南亚某国。

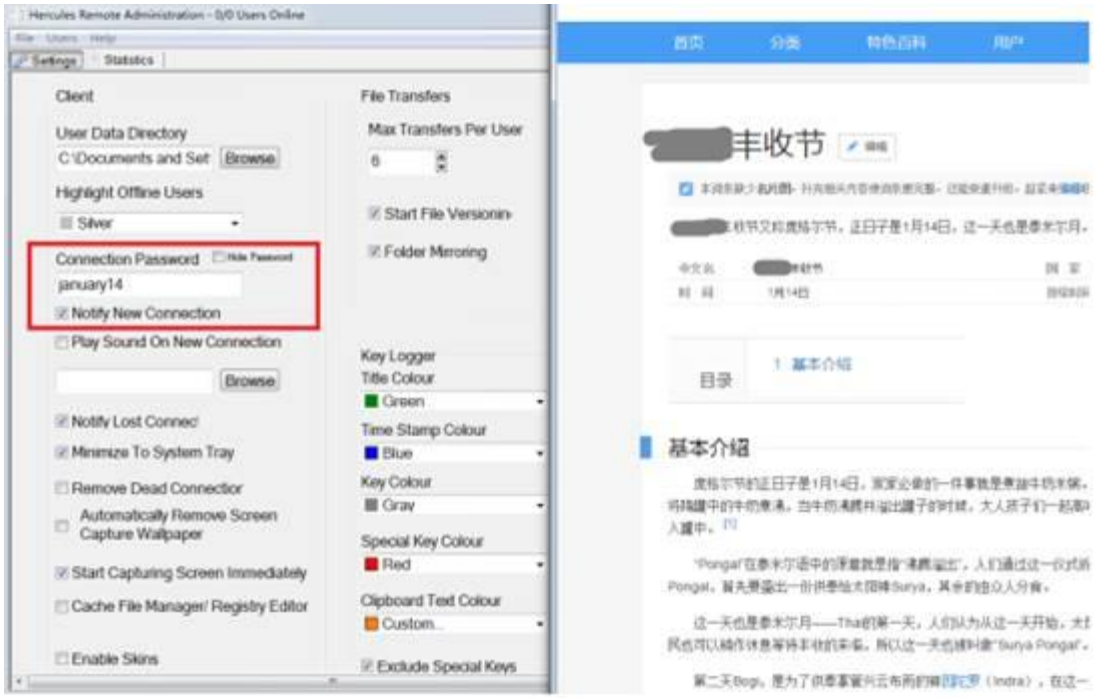


图 12　木马通讯密码配置

除了密码，我们也把上述推测的组织成员昵称放入搜索引擎进行搜索，得到了一些有趣的结果：

v　sitar：南亚某国的一种古老的乐器[[4]]。

v　avatar:大家最熟悉的是《阿凡达》电影，但其同时又是佛教里的一位神[[5]]。

结合密码和昵称的语言文化，我们认为这些信息进一步印证了控制源 IP 来源于南亚某国的分析推断。

2.2.3 线索三：遗留数据

研究人员在跟踪溯源采集的数据中，发现了攻击者调试免杀木马时遗留的证据，免杀针对的杀毒软件包含但不限于：

v AVAST

v Trendmicro

v Bitdefender

v Panda

v GDATA

v NOD32

v AVIRA

v NIS 诺顿

攻击者把每个杀毒软件部署在一个或者多个独立的 WIN7 或者 WIN8 系统上，已知约 10 个系统，逐个测试样本免杀情况。并且，这些杀毒软件同属 10.*.*.* 子网，考虑到终端的数量和部署环境，推测该子网为攻击者真实的工作环境，而非被控端。

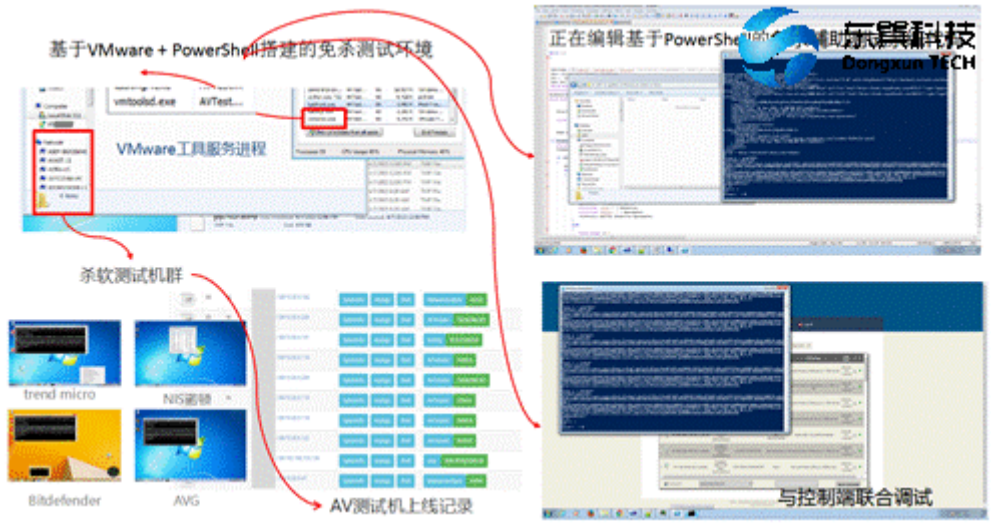


图 13　免杀测试环境和对外链接 IP

最重要的是，这个子网对外的出口 IP 正好是上述南亚某国 IP 段的*.*.*.138，也就是说这个 IP 是跳板或另一个受害者的可能性非常低，再次证实了攻击者来源于此 IP。

基于相关性分析，推测该组织可能与近期友商公布的一些事件存在关联，或许原本是同一组织活跃在不同时期的不同工作。后续研究人员将持续跟进做进一步的确认。

3 攻击工具分析

我们对攻击工具深度分析后发现，攻击者这次发起的“丰收行动”是精心准备的、有组织的一次网络间谍攻击。其使用了 APT 攻击中最为典型和常用的攻击方式，有效的绕过了传统防护手段。为预防攻击者利用公开信息进行反溯源，以下仅阐述攻击工具的部分分析结果。

3.1 载荷投递

在本次行动中，我们捕获了伪装成 Word 文档的 RTF 格式邮件附件样本，所以可以确定攻击者使用了鱼叉攻击。此外，我们发现攻击者囤积了多个浏览器挂马脚本，脚本的最后修改时间为 2016 年 4 月，据此推测攻击者还可能使用了挂马或水坑攻击方式。

3.1.1 鱼叉攻击

利用邮件实施“鱼叉式钓鱼攻击”是典型 APT 攻击方式之一，将恶意代码作为电子邮件的附件，并命名为一个极具诱惑力的名称，发送给攻击目标，诱使目标打开附件，从而感染并控制目标计算机。我们在《利用邮件实施 APT 攻击的演示》[[6]]一文进行了视频演示，读者可以参考印证。

3.1.2 水坑攻击

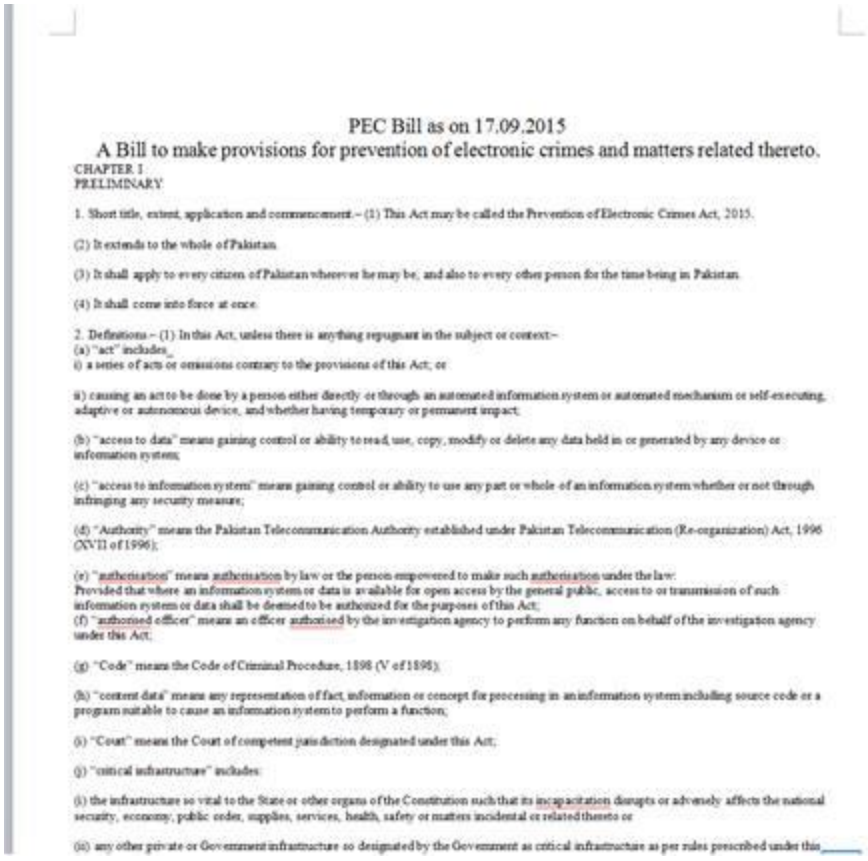
“水坑攻击”，是指黑客通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待被攻击者来访时

实施攻击。这种攻击行为类似《动物世界》纪录片中的一种情节：捕食者埋伏在水里或者水坑周围，等其他动物前来喝水时发起攻击猎取食物。[[7]]

3.2 漏洞利用

3.2.1 鱼叉攻击使用的漏洞

“丰收行动”中，攻击者以邮件形式发送了一份捆绑了漏洞利用代码和远程控制工具的 Word 文档给受害者。附件文档被点击后会显示一份以乌尔都语描述的网络犯罪法案诱饵文档《PEC Bill as on 17.09.2015》，用以迷惑受害者，如下所示：



PEC Bill as on 17.09.2015

A Bill to make provisions for prevention of electronic crimes and matters related thereto.

CHAPTER I
PRELIMINARY

1. Short title, extent, application and commencement.– (1) This Act may be called the Prevention of Electronic Crimes Act, 2015.

(2) It extends to the whole of Pakistan.

(3) It shall apply to every citizen of Pakistan wherever he may be, and also to every other person for the time being in Pakistan.

(4) It shall come into force at once.

2. Definitions.– (1) In this Act, unless there is anything repugnant in the subject or context:–
(a) "act" includes,
i) a series of acts or omissions contrary to the provisions of this Act; or

ii) causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device, and whether having temporary or permanent impact;

(b) "access to data" means gaining control or ability to read, use, copy, modify or delete any data held in or generated by any device or information system;

(c) "access to information system" means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;

(d) "Authority" means the Pakistan Telecommunication Authority established under Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);

(e) "authorisation" means authorisation by law or the person empowered to make such authorisation under the law:
Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;
(f) "authorised officer" means an officer authorised by the investigation agency to perform any function on behalf of the investigation agency under this Act;

(g) "Code" means the Code of Criminal Procedure, 1898 (V of 1898);

(h) "content data" means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;

(i) "Court" means the Court of competent jurisdiction designated under this Act;

(j) "critical infrastructure" includes

(i) the infrastructure so vital to the State or other organs of the Constitution such that its incapacitation disrupts or adversely affects the national security, economy, public order, supplies, services, health, safety or matters incidental or related thereto or

(ii) any other private or Government infrastructure so designated by the Government as critical infrastructure as per rules prescribed under this

图 14　诱饵文档内容

但该附件文档实质是包含 CVE-2015-1641（Word 类型混淆漏洞）漏洞利用的 RTF 格式文档，用户在打开的同时除了用诱饵文档显示迷惑性文档内容外，还会利用该漏洞释放恶意程序，从而感染并控制用户主机。

该附件文档样本的 MD5 为******e0b4a6b6a5b11dd7e35013d13a，样本捕获后不久交由 54 款杀毒引擎检测，仅 8 款能够查杀。用二进制编辑工具打开该文件，由开头的几个字符为{\rtf1\adeflang1025\ansi\，可确定文件是一个 RTF 文件。同时，该样本文件中包含以下内容：

{\object\objemb{*\objclass None}{*\oleclsid \'7bA08A033D-1A75-4AB6-A166-EAD02F547959\'7d}

在注册表查询此 olecsid，发现是 Office 的 otkload.dll 组件，该组件依赖 msvcr71.dll 动态库，可见此 RTF 文档打开时会加载 msvcr71.dll，而 msvcr71.dll 文件不支持 ASRL，所以判断样本加载该库是借此构建 ROP 来绕过 ASRL&DEP。漏洞利用相关代码如下：

```
7c341dfa 5e                    pop          esi

7c341dfb c3                    ret



7c341cca 8b06                  mov          eax,dWord ptr [esi]    ds:0023:7c3
t (76c62341)}

7c341ccc 85c0                  test           eax,eax

7c341cce 74f1                  je               MSVCR71!initterm+0x7 (7c3
0]

7c341cd0 ffd0                  call             eax {kernel32!VirtualProt

7c341cd2 ebed                  jmp            MSVCR71!initterm+0x7 (7c341c



7c341cc1 83c604                  add            esi,4

7c341cc4 3b74240c              cmp          esi,dWord ptr [esp+0Ch] ss:0023:06
```

```
7c341cc8 730a                    jae             MSVCR71!initterm+0x1a (7c34
7c341cca 8b06                    mov           eax,dWord ptr [esi]    ds:002
7c341ccc 85c0                    test            eax,eax
7c341cce 74f1                    je                MSVCR71!initterm+0x7 (7c3
0]
7c341cd0 ffd0                    call              eax {09c908bc}
```

表 1　漏洞利用相关代码片段

主要目的是要调用 VirtualProtect 函数绕过 DEP，接着跳到栈上的代码。Shellcode 部分的代码如下：

```
09c908bc 49                      dec         ecx
09c908bd 49                      dec         ecx
09c908be 49                      dec         ecx
09c908bf 49                      dec         ecx
09c908c0 49                      dec         ecx
09c908c1 49                      dec         ecx
09c908c2 49                      dec         ecx
09c908c3 49                      dec         ecx
09c908c4 49                      dec         ecx
09c908c5 49                      dec         ecx
09c908c6 49                      dec         ecx
```

```
09c908c7 49                    dec         ecx

09c908c8 49                    dec         ecx

09c908c9 49                    dec         ecx

09c908ca 49                    dec         ecx

09c908cb 49                    dec         ecx

09c908cc 49                    dec         ecx

09c908cd 49                    dec         ecx

09c908ce 49                    dec         ecx

09c908cf 49                    dec         ecx

09c908d0 49                    dec         ecx

09c908d1 49                    dec         ecx

09c908d2 49                    dec         ecx

09c908d3 49                    dec         ecx

09c908d4 49                    dec         ecx

09c908d5 49                    dec         ecx

09c908d6 49                    dec         ecx

09c908d7 49                    dec         ecx

09c908d8 eb1c                  jmp         09c908f6



09c908f6 e8e2ffffff            call        09c908dd
```

```
09c908dd 58                              pop          eax

09c908de e9c8000000              jmp          09c909ab

09c909ab e833ffffff                  call         09c908e3
```

表 2 ShellCode 代码片段

前面很长的一段“dec ecx”作为空指令，覆盖更多的地址来提高漏洞利用的适应能力。该 shellcode 的主要功能为释放~$Norm~1.dat 和 Normal.domx 两个文件，~$Norm~1.dat 是恶意文件的载体，Normal.domx 是一个 VBE 文件，并通过修改注册表来设置多个版本 Office 的禁止项目，其目标版本为 Office 10.0 至 Office 16.0。

Normal.domx 执行后会释放诱饵文档，释放并运行 MicroS~1.exe、jli.dll、msvcr71.dll，这三个文件正是攻击者远程控制程序的投放端植入程序。

3.2.2 水坑攻击使用的漏洞

我们在对攻击者所使用的各种资源跟踪过程中，发现攻击者搭建了一套挂马漏洞集成攻击平台。该平台文件最后修改时间为 2016 年 4 月，但未配套挂载欲植入的后门程序，故判断该攻击平台处于预备状态。

平台集成的攻击漏洞有针对 IE、FireFox 浏览器的，也有针对 SWF、PDF 浏览器插件，已知 CVE 漏洞如表 3 所示。

漏洞编号	所属应用
CVE-2010-0806	Internet Explorer
CVE-2010-3962	Internet Explorer
CVE-2006-0003	mdac 组件
CVE-2009-2496	Microsoft Office

CVE-2010-3653	Adobe Shockwave Player
CVE-2010-0188	Adobe Reader
CVE-2008-2992	Adobe Reader
CVE-2009-0927	Adobe Reader
CVE-2009-4324	Adobe Reader
CVE-2007-5659	Adobe Reader

表 3　已知 CVE 漏洞

另外，攻击者还赫然将针对 AOL 9.5 的漏洞利用代码输出函数命名定义为“IE_0Day”，说明该组织对美国在线的用户群也非常感兴趣。

漏洞编号	无，AOL 9.5 - ActiveX Exploit (Heap Spray)
说明	AOL 9.5 Phobos.Playlist ‘Import()’函数存在栈缓冲区溢出，导致远程 Script 方法执行任意代码。
公布时间	尚无官方公开发布，exploit-db　公开时间 2010-01-20
参考链接	https://www.exploit-db.com/exploits/11204/

表 4 IE_0Day 漏洞

漏洞利用执行的 Shellcode 是通过进程的 PEB 结构来查找自己需要的 Dll，继而能够在 Dll 中查找自己需要的函数。

```
seg000:00000000                         xor         eax, eax

seg000:00000002                         mov         eax, fs:[eax+30h] ; PEB
```

```
seg000:00000006                         js          short loc_14
seg000:00000008                         mov         eax, [eax+0Ch]    ; DllList
seg000:0000000B                         mov         esi, [eax+1Ch]    ; DllList[7]
seg000:0000000E                         lodsd
seg000:0000000F                         mov         ebx, [eax+8]        ; DllList[2] kernel32.dll
seg000:00000012                         jmp         short loc_1D
seg000:00000014 ;
```

表 5 ShellCode 代码片段

通过一系列的函数调用完成对新脚本的加载，从而进行后续的恶意行为。

3.3 后门分析

3.3.1 功能分析

“丰收行动”的攻击者使用了三套远程控制工具，这三套工具均以文件和数据窃取为主要目的，其中一款的具体功能主要包括：

v 与远程 C&C 服务器通信接收控制命令，具备文件遍历、文件上传下载、命令无回显执行、屏幕截图等功能；

v 设置自身为随系统启动，收集用户名、计算机名、样本版本信息，并加密上传；

v 全盘搜索各类文档（主要包括：“pdf、doc、docx、ppt、pptx、txt”），并在形成索引文件后加密上传；

v 能够对 U 盘的使用进行监控，对 U 盘上各类文档进行截获；

其中以“MicroS~1.exe、jli.dll、msvcr71.dll”三个文件为投放端植入程序的后门已经在友商的分析报告[[8]]有过相应的描述，我们不再赘述。

从 HTTP 通信协议请求的相似性分析，另外一款远程控制工具应是该套后门的高级版本，且对关联到的组件样本进行分析后发现其还具备非驱动型的文件隐藏功能。

3.3.1.1 反沙箱检测技术

样本分析时发现，样本调用了 QueryPerformanceFrequency 和 QueryPerformanceCounter 两个系统函数来计算系统运行时长，以此来区分真实系统和虚拟系统，从而实现绕过虚拟机的检测，可见其使用了典型的反沙箱检测技术。

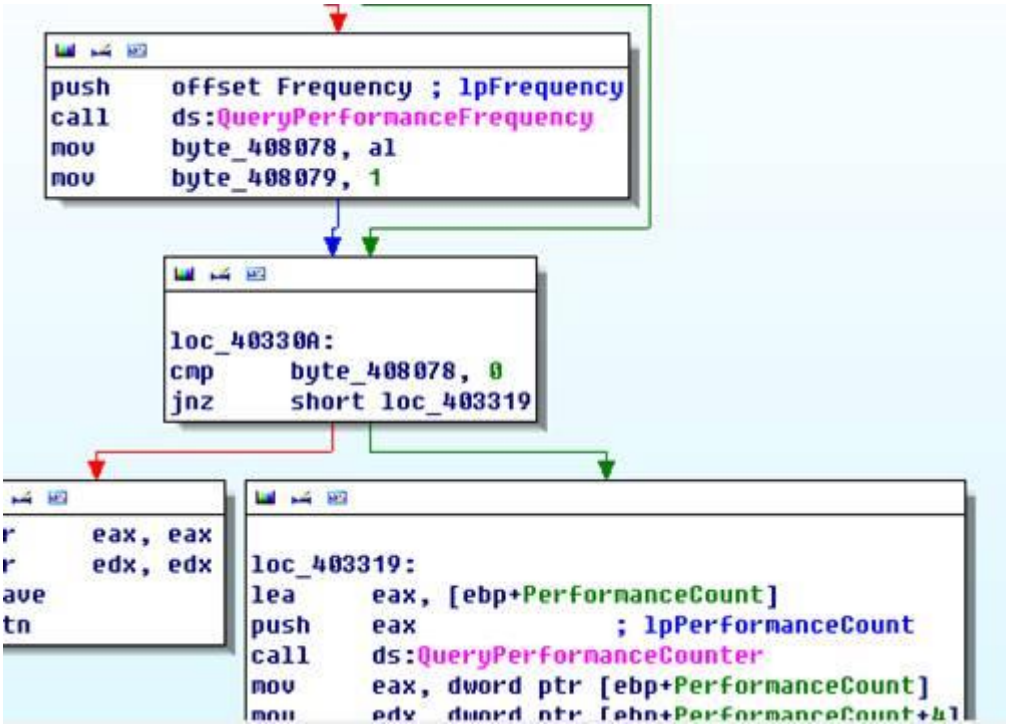


图 15 绕过虚拟检测

3.3.1.2 非驱动型的高级隐藏技术

在对投放端样本进行关联时，找到其疑似组件。该组件样本先通过 SetWindowsHook 挂载到所有进程中，然后 inline Hook 应用层 ntdll!ZWQueryDiectoryFile 函数，该函数是系统用于查询遍历文件目录的函数。图 16 为 jmp 跳转到的 Hook 函数，先平衡堆栈，然后调用原

ZWQueryDiectoryFile 函数来获取系统真实返回数据，最后再对返回的结果数据进行相应的处理。

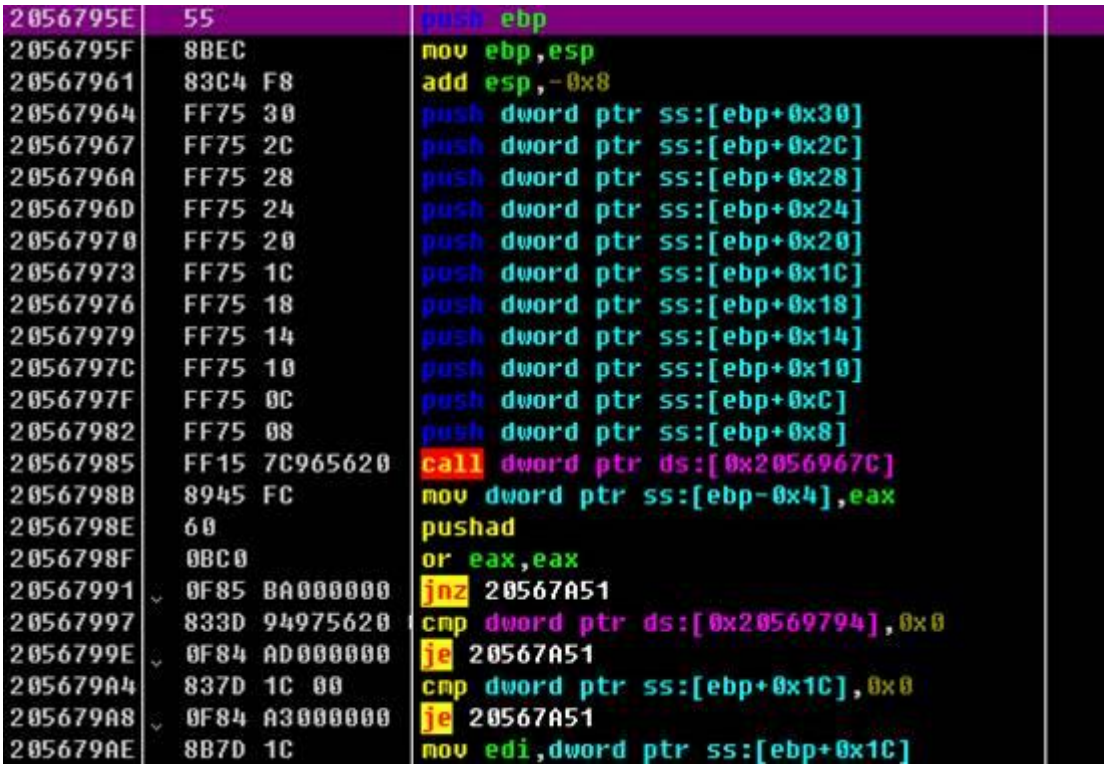


图 16 Hook 跳转后的执行代码

后续对数据的处理，Hook 函数会对原函数的返回结果进行过滤，查询是否包含其指定的文件名称，如果存在则从返回结果里面移除该文件名相关信息。

这样当“我的电脑”对应的 explorer.exe 进程在查询某目录（例如开始菜单启动项）时，就无法查看到指定的文件，达到不加载驱动也能对文件进行隐藏的目的，避免防御软件对驱动加载这一高危行为的拦截和防御。

3.3.2 基于 PowerShell 的恶意代码

攻击者使用 PowerShell 脚本配合程序实现 Agent 代理端，利用 Web 服务器统一接受各 Agent 在杀毒软件测试虚拟机搜集的数据。免杀辅助系统 Agent 代理端具备系统信息搜集、截屏录屏、键盘记录、数据回传等功能，涉及的组件包括：

样本组件	功能作用
connection	连接指定 URL
copy_NOT_for use	复制文件到共享
Get-Keystrokes	获取键盘记录
Get-TimedScreenshot	周期间隔截屏到文件
info	获取硬件信息
screenshort	加密发送截屏数据
screenshot	截屏保存到文件
service	获取所有进程和服务
start	调度程序
systeminfo	获取系统信息

表 6　组件说明

3.4　C&C 分析

从我们直接获取到的样本来看，“丰收行动”的三个 C&C 服务器一共可对应出 8 个域名地址，均为免费的二级动态域名，没有办法直接从注册域名信息进行详细分析。

从一些关联到的数据来看，攻击者有攻击其他正常服务器来放置临时数据，以期在漏洞利用植入阶段提供远程下载恶意模块的行为习惯。

4 TTPs 分析

TTPs（Tactics, Techniques and Procedures），是指攻击者用到的战术、技术和步骤[[9]]。我们把“丰收行动”涉及到的一些相关信息汇总如下：

关键项	本次攻击事件情况说明
主要攻击目标	科研院所、军事院校、外交官员
目标国家	以巴基斯坦为主，中国、美国、英国、奥地利等
关键作用点	个人办公用机
目标人群	高级岗位人员，例如对外联系人、军事院校教授、政府官员、使馆人
攻击手法	鱼叉式钓鱼->VBS 脚本->控制端->信息窃取
攻击目的	窃取信息数据
漏洞使用情况	使用影响 Office 系列的 CVE-2015-1641 漏洞为主 兼用 CVE-2012-0507、CVE-2013-0640 等浏览器漏洞
免杀技术	攻击者搭建免杀测试环境包括：AVAST、NIS 诺顿、Mcafee、AVG、Bi
活跃程度	长期在线操作，且控制系统每天都有新增的被控目标上线
反追踪能力	非常小心谨慎，使用多层跳板代理控制 C&C 服务器，上传文件均加密

工程化能力	C&C 控制系统环境搭建流程标准化，系统加固、支持库安装、控制模
攻击源	从二级跳板 IP 的网络活动痕迹等线索判断，攻击者来自南亚某国的

表 7　　“丰收行动”总览

本次行动涉及到 TTPs，我们希望能通过图 17 来进行简要说明：

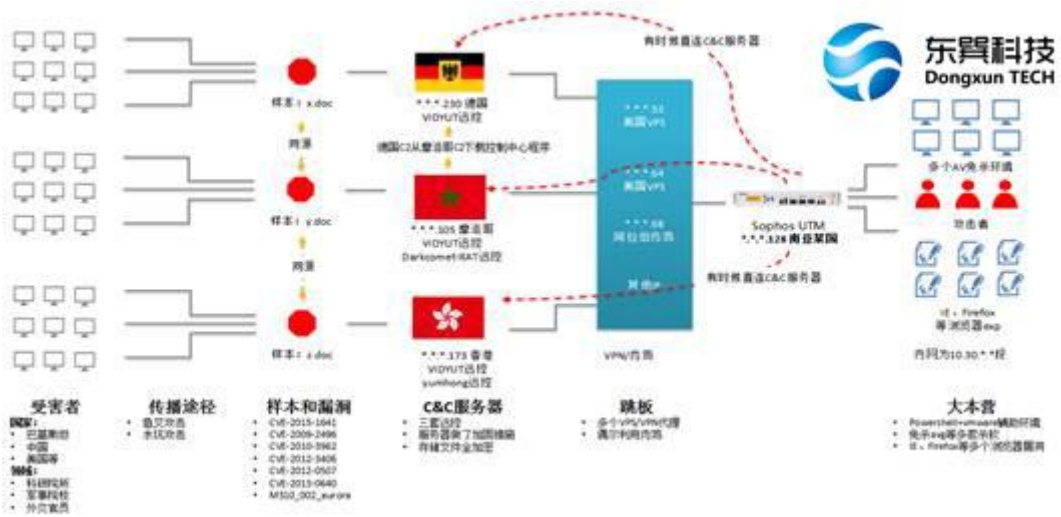


图 17　一张图展示丰收行动

1．确定目标，并搜集个人信息。“丰收行动”针对的目标主要是巴基斯坦、中国等国家的科研院所、军事院校、外交官员为主，攻击者通过搜索引擎、Facebook 等社交网络，获取受害者的电子邮箱地址和个人信息，在后续攻陷受害人，还会从受害人的文档里搜集电子邮箱和个人信息。

2．搭建 C&C 服务器。攻击者分阶段搭建了三个 C&C 服务器，该过程可能与步骤 1 同步进行。跟踪发现，该组织的 C&C 服务器之间有相互的关联，比如德国的 C&C 服务器的远程控制工具是从摩洛哥 C&C 服务器下载部署。同时，这些 C&C 服务器的建设都采用了标准化流程操作，进行了系统加固、支持库安装、控制模块、监控模块部署等，说明对此已经非常熟练。

3．木马免杀。针对目标使用的系统和杀毒软件，搭建环境进行木马免杀工作。在本次跟踪过程中我们发现，攻击者利用了 Powershell+VMware 搭建半自动化免杀平台来提高效率，足见其成员非新手。跟踪到的数据显示，其中一次免杀工作是在 2016 年 5 月 2 日和 3 日进行的。此外，攻击者还制作了多个浏览器挂马漏洞库（参考漏洞利用），最后修改时间为 2016 年 4 月 18 日，搭配三套远程控制工具使用。

4．投放诱饵。攻击者将已免杀的木马捆入带有利用程序的 RTF 文档中，伪装成 Word 文档，通过电子邮件附件方式发送给受害人，诱使其点击。用户点击后会弹出一个真实的 Word 文档，迷惑受害者。此外，推测攻击者也会采取发送浏览器挂马网页，发动水坑攻击。

5．加密回传数据。受害者计算机感染木马后，木马会搜索敏感的电子文档、记录键盘操作等，并加密打包为.enc 后缀发回到 C&C 服务器。加解密工具非通用 zip 等压缩工具，而是攻击者自己编写的私有工具。

6．长期控制。本次行动中攻击者会长期控制受害者计算机，监控其浏览的网页、读取的邮件、新生成的文档，同时根据需要装载新的模块。通过对远程控制工具分析，其包含文件管理、关键词搜索、摄像头监控、键盘记录、U 盘监控等功能模块，以窃取文档为主。此外，攻击者会根据从受害者获取到的个人信息和其他联系人电子邮件，做进一步的扩大攻击。

5 结语

与友商用大量样本统计来分析 APT 方式不同，2046Lab 针对“丰收行动”的分析虽也利用了样本分析手法，但更多是利用跟踪溯源的方式。这种跟踪溯源和分析过程，给了我们一种逐渐拨开迷雾见彩虹的感觉。从一个样本到一个 C&C 服务器，再到另一个样本，到另一个 C&C 服务器，每跟踪溯源一次，我们对攻击者的了解就加深一些，包括攻击者的目标对象、使用工具、C&C 服务器据点、惯用手法，最后云开雾散，发现攻击者的具体 IP，定位到其在南亚某国的幕后大本营。这一过程不免让我们感叹，东巽科技倡导的“人与人”的对抗确实是 APT 防护对抗的本质所在。

本次“丰收行动”，再一次证明了 APT 攻击的存在和长期活跃，而导致攻击成功的主要因素是：防守在明、攻击在暗，受害者的防御措施与攻击者攻击手段存在能力差距，尤其是未知威胁的检测和预警能力。

本次的揭露只是全球 APT 攻击事件的冰山一角,中国也是 APT 攻击的受害者之一。我们预测和以往同行的报告一样，攻击者并不会因为本次的揭露而销声匿迹，至多是偃旗息鼓一段时间，然后以更隐蔽的方式卷土重来，并用上新的免杀技术、新的漏洞或者新的攻击方式。所以，本报告希望能给用户，尤其是可能遭受 APT 攻击的重要机构一些提醒和建议，落实习总书记 4.19 讲话精神，树立正确的网络安全观，充分认识自己的防御措施和攻击技术之间的差距，加快构建安全保障体系，提前部署防御措施，尤其是未知威胁的检测和识别方面的能力建设，增强网络安全防御能力和威慑能力，防患于未然。

东巽科技介绍

东巽科技是中国新兴的网络安全公司，由国内顶尖的白帽子技术团队组成。公司成立于北京，南京设有子公司，北京、南京、成都三地设有研发中心，专业从事高级持续性威胁（APT）相关技术研究、安全产品研发及服务，致力于打造基于大数据思想的 APT 安全云平台，为中高端客户所面临的高级持续性威胁提供高级安全保障服务。

欢迎访问东巽科技官网：www.dongxuntech.com

[[1]] https://en.wikipedia.org/wiki/DarkComet

[[2]] The Dropping Elephant, https://securelist.com/blog/research/75328/the-dropping-elephant-actor/

[[3]] DarkHotel, https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

[[4]] sitar, https://en.wikipedia.org/wiki/Sitar

[[5]] avatar, https://en.wikipedia.org/wiki/Avatar

[[6]] 利用邮件实施 APT 攻击，
http://mp.weixin.qq.com/s?src=3&timestamp=1470618506&ver=1&signature=iL9QskvxpmXKHy7hy*xFENSwn-2xRDA1-DruyOtDkd4Fe3kCfU5olgBs3RgSaH2mn6KoxyKY78LXeZeJWu3mXXBe2H8PiEE2SbugOtv4jzW4F*Z7W56qwPoPJzCdfUHhtswfNhc96UcyBK9rKJdlvxt13iXpPbGKV6KWeYv0szU=

[[7]] 水坑攻击，http://baike.baidu.com/link?url=b_-FXNCFcKDWuph7v-ViUhyQStOWmqT_EtVNqQkiWRn8NMEtd2Zh6TIsLTQkWrhILjeKeKgRa95isIb-6DVnhF7DeKcQ6bA2-7itMpwkjwM1wzjxCMOU2AWQXbtrCVEx

[[8]] 360 追日团队 APT 报告：摩诃草组织（APT-C-09），
http://bobao.360.cn/learning/detail/2935.html

[[9]] TTPs,
https://en.wikipedia.org/wiki/Terrorist_Tactics,_Techniques,_and_Procedures