APT-C-56（透明部落）近期最新攻击分析与关联疑似Gorgon Group攻击事件分析预警

By 高级威胁研究院

Archived: 2026-04-05 18:09:04 UTC

APT-C-56
透明部落

透明部落（Transparent Tribe）别名APT36、ProjectM、C-Major，是一个具有南亚背景的APT组织，其长期针对周边国家和地区（特别是印度）的政治、军事进行定向攻击活动，其开发有自己的专属木马CrimsonRAT，还曾被发现广泛传播USB蠕虫。TransparentTribe也曾经对Donot的恶意文档宏代码进行模仿，两者高度相似。之前透明部落也曾经模仿响尾蛇组织进行攻击。其一直针对印度的政府、公共部门、各行各业包括但不限于医疗、电力、金融、制造业等进行攻击和信息窥探。

近日360高级威胁研究分析中心在日常情报挖掘中发现并捕获到了透明部落攻击印度的文档，恶意文档最终释放CrimsonRAT。

Gorgon Group
攻击事件

与此同时，我们还监控到了疑似Gorgon Group利用Netwire对印度的攻击行动，该组织由疑似巴基斯坦或与巴基斯坦有其他联系的成员组成。该组织一直有针对性的攻击英国、西班牙、俄罗斯和美国。Gorgon也曾经被怀疑与Transparent Tribe有关联，并可能负责Aggah活动。

一. 透明部落近期最新攻击分析

恶意文档

此次捕获到的恶意文档被打开的时候，其内部的宏代码就应该开始自动运行。在ALLUSERSPROFILE目录下伪装成HDM Media相关程序，从恶意文档的指定结构中读取隐藏的数据并写入文件中，可以看出APT36利用简单的字符串拼接技术，对exe字符进行拆解，以躲避杀毒引擎的静态查杀。

```
file_shoby_name = "davivthain"

folder_shoby_name = Environ$("ALLUSERSPROFILE") & "\HDM Media\"

If Dir(folder_shoby_name, vbDirectory) = "" Then
    MkDir (folder_shoby_name)
End If

path_shoby_file = folder_shoby_name & file_shoby_name


Dim awr1shoby_s() As String

If Dir(path_shoby_file & ".ex" & "e") = "" Then

    Dim shoby_bweyt(123903) As Byte


    awr1shoby_s = Split(ActiveDocument.Pages(1).Shapes(1).TextFrame.Story.TextRange

    Dim i As Double
    For i = 0 To UBound(awr1shoby_s) - LBound(awr1shoby_s)
        shoby_bweyt(i) = awr1shoby_s(i)
    Next
```

启动释放的恶意PE程序，同时进一步读取内部隐藏的正常文本文档数据，释放到wordxdoc.docx，最后打开这个文档伪装迷惑用户。

Dropper

释放的PE文件是一个.Net的Dropper程序。首先判断Templates目录下是否存在zip文件，如果不存在将读取资源节并将其中的数据写入文件，如果存在则删除后重新写入。

判断目录下是否有以.ford为后缀的文件，如果有，直接创建进行启动文件。没有指定后缀文件则直接进入后续释放流程。

随后在ProgramData目录下，判断系统版本并释放下一阶段RAT后门。

RAT

释放的RAT后门是透明部落一直维护和使用的CrimsonRAT。最后创建进程启动RAT。

控制码与命令如下：

指令	控制码
枚举进程	getavs
上传gif	thumb
枚举进程	procl
设置自启动	putsrt
下载文件	dowf
设置截屏	scrsz
获取文件属性	filsz
查看截图	cdcrgn
	cscrgn
	csdcrgn
停止截屏	stops
桌面截图	scren
获取磁盘信息	dirs

参数初始化	cnls
删除文件	delt
获取文件信息	afile
删除用户	udlt
搜索文件	listf
获取用户信息	info
执行文件	runf
移动文件	file

二. 关联Shoot行动分析

近期我们捕获了一批针对印度的样本，其最终释放NetwireRAT，NetwireRAT是开源的商业RAT软件，但是也已经被一些APT组织使用，例如 APT33 和 Gorgon，Gorgon Group 是一个由疑似巴基斯坦或与巴基斯坦有其他联系的成员组成。该组织实施了犯罪和有针对性的攻击，包括针对英国、西班牙、俄罗斯和美国的政府组织的活动。Gorgon也曾经被怀疑与Transparent Tribe、APT36有关联，并可能负责Aggah活动。

疑似挂马网页

捕获的样本下载链接是：hxxp://lms.apsdigicamp【.】com/webapps/uploads/acc/cctv-footages/student-termination-and-proof.zip

这个网页可能已经被恶意挂马：

印度陆军公立学校的网站

压缩包

下载后的压缩包释放出一张色情图片，一个恶意文档与一个可疑pe文件。

恶意文档

我们首先分析恶意文档，文档打开后是假装文档被密码保护从而诱使用户运行宏代码的图片，一旦用户没有足够的网络安全防护意识，按照说明操作后，隐藏的恶意宏代码就开始在用户后台运行。

- 当文档打开的时候，会自动显示文档内容。
- 当文档更新时候，会从指定CC下载文件并存放到C:\\Users\\Public\\Adobe.exe。
- 当文档关闭时候，利用shell命令运行下载的二进制文件。

Dropper

释放出来的二进制文件图标伪装成Adobe PDF，利用student-cctv-video(private)的文件名称刺激不明真相的人群点击打开，最终运行Dropper。

我们捕获到的版本还可以看到Dropper的PDB信息。

运行后首先弹出对话框，让用户以为自己的组件损坏需要升级，企图以假乱真，此时代码已经开始偷偷运行，这里不知道是否存在bug。这个对话框是不能被关闭的。

首先加载AmsiScanBuffer并企图通过修改内存关闭。

注册自启动。

隐式加载API函数，躲避杀毒引擎的静态查杀。

创建一个新的自身进程。

远程线程注入写入隐藏在PE内部的二进制文件。

RAT

重新写入覆盖的样本是NetwireRAT，其是开源的商业RAT软件，但是也已经被一些APT组织使用，例如APT33 和 Gorgon。

总结

印巴冲突因为边境、文化、种族、历史等原因一直存在，地缘冲突导致的军事、政治刺探始终是该区域的主旋律，印度有专门APT组织如肚脑虫（APT-C-35）主要针对巴基斯坦相关政府、国防军工的重点目标发起攻击。巴基斯坦的透明部落也始终对印度的政治、军事行动频频。
混乱的局势往往代表着各国之间经济、军事、网络安全能力的较量，通过网络攻击活动占领情报先机，维护国家安全也显示越发重要。

附录 IOC

cb3adae7ac07bfe8e366e0f3197811c8

74fa8961827639d1b481a4eea50863e5

e59bf2ce3fe67ff394023a4fd7ed3968

dbd37b8c044a27ec8008c6489231075f

66.154.103.106:13377

hxxp://lms[.]apsdigicamp[.]com/webapps/uploads/acc/cctv-footages/student-termination-and-proof.zip

77C29D464EFCAE961424AE050453EF11

3C2B45A6D878CC9F30A5DC10ABF400A1

7F1F7C5C4B6B486E5BA9340944036285

360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。
