拍拍熊（APT-C-37）：持续针对某武装组织的攻击活动揭露 - 360 核心安全技术博客

blogs.360.cn/post/analysis-of-apt-c-37.html

03月25, 2019

0 comments

拍拍熊（APT-C-37）：持续针对某武装组织的攻击活动揭露

一、 概述

从2015年10月起至今，拍拍熊组织（APT-C-37）针对某武装组织展开了有组织、有计划、针对性的长期不间断攻击。其攻击平台为Windows和Android，截止目前360烽火实验室（360 Beaconlab）一共捕获了Android平台攻击样本32个，Windows平台攻击样本13个，涉及的C&C域名7个。

某武装组织由于其自身的政治、宗教等问题，使其成为了众多黑客及国家的攻击目标。2017年3月，某武装组织Amaq媒体频道发布了一条警告消息，该消息提醒访问者该网站已被渗透，任何访问该网站的人都会被要求下载伪装成Flash安装程序的病毒文件。从消息中我们确定了某武装组织是该行动的攻击目标，其载荷投递方式至少包括水坑式攻击。

通过分析，我们发现拍拍熊组织使用到的一个主要C&C位于中东某国，且和同时期的黄金鼠组织[1]使用的C&C属于同一个网段。进一步分析对比，两个组织有很强的关联性，然两者又包含有各自的特有RAT。

由于拍拍熊组织的攻击目标针对的是某武装组织，支持双平台攻击，另史上曾经出现过唯一一种获有士兵证的中东某国特色动物，结合该组织的一些其它特点以及360对 APT 组织的命名规则，我们将该组织命名为DOTA游戏里的一个角色名----拍拍熊。

图1.1 拍拍熊攻击相关的关键时间事件点

二、 载荷投递

此次拍拍熊组织载荷投递的方式主要为水坑攻击。

水坑攻击

Al Swarm新闻社网站（见图2.1）是一个属于某武装组织的媒体网站，同样的原因，使其也遭受着来自世界各地的各种攻击，曾更换过几次域名，网站目前已经下线。拍拍熊组织除了对上述提到的Amaq媒体网站进行水坑攻击外，我们发现Al Swarm新闻社也同样被该组织用来水坑攻击。

图2.1 Al Swarm新闻社网站（注：采用archive获取）

该水坑攻击方式采用的是把Al Swarm站的正常APP替换成一个插入RAT后的恶意APP， 其RAT具体下载链接和链接对应文件MD5见表1。

恶意下载链接	**https://sawarim.net/apps/Sawarim.apk**
域名状态	失效
下载的APK文件MD5	bb2d1238c8418cde13128e91f1a77ae7

表1 Android端RAT程序具体下载链接和链接对应文件MD5

除了上面两个针对某武装组织新闻媒体网站的水坑攻击外，我们还发现到该组织使用到的一些其它历史水坑攻击见表2，包含了Android端和Windows端RAT程序具体下载链接和链接对应文件MD5。

恶意下载链接	**http://androids-app.com/downloads/Youtube_v3_4.apk**
域名状态	失效
下载的APK文件MD5	dc1ede8e2d3206b04cb95b6ae62f43e0
恶意下载链接	http://androids-app.com/SystemUI.exe
域名状态	失效
下载的PE文件MD5	d2c40e2183cf18855c36ddd14f8e966f
恶意下载链接	http://snapcard.argia.co.id/woocommerce/wp-content/plugins/Adobe_FlashPlayerX86_64.exe
域名状态	失效
下载的PE文件MD5	8c49833f76b17fdaafe5130f249312ca

恶意下载链接	**http://androids-app.com/downloads/Youtube_v3_4.apk**
恶意下载链接	http://snapcard.argia.co.id/woocommerce/wp-content/plugins/Adobe_FlashPlayer_installX86.exe
域名状态	失效
下载的PE文件MD5	e6e676df8250a7b930b2d016458225e2

表2 RAT程序具体下载链接和链接对应文件MD5

三、 诱导方式

拍拍熊组织在这次行动中主要使用以下两种诱导方式：

含有正常APP功能的伪装

为更好的躲避被察觉到，除了对文件图标进行伪装外，还会把RAT插入到正常的APP中，如一款名为“زوجات الرسول”的APP，它运行后展示的是正常时的界面，但当接收到指定的广播时，便在后台进行间谍活动。

image.png

图3.1 带有两种RAT的伪装APP“زوجات الرسول”

文件图标伪装

image.png

图3.2 伪装的应用软件图标

四、 RAT攻击样本分析

截至目前，拍拍熊组织此次攻击活动已使用到数种分别针对Android和Windows的不同RAT。

Android

Android端共使用到三种RAT，其中有两种（DroidJack和SpyNote）是使用较频繁的商业RAT，曾在多个黑客论坛上进行传播，已被多家安全公司查杀和曝光。而另外一种我们认为是专门为此次攻击开发的，我们命为SSLove，其仅出现在该活动中，并历经数个版本的更新。

DroidJack

Droidjack是一个极度流行的RAT，有自己的官网，功能强大，且有便捷的管理工具。该组织在使用Droidjack时除了直接使用外；还会把其插入到正常APP中进行隐藏，有趣的是同时SSLove也会一块插入到该APP中，这意味着该APP会同时带有两种RAT。

image.png

图4.1 Droidjack管理工具界面图

SpyNote

SpyNote类似Droidjack ，虽然拍拍熊组织使用到SpyNote，但该RAT在此次攻击活动中被用到的次数有限。

image.png

图4.2 SpyNote管理工具界面图

SSLove

这是一个之前未被曝光的RAT。根据该RAT包含的特殊字符“runmylove”，结合其是首款被发现到的使用SqlServer实现指令交互的RAT，我们命名为SSLove。最新版本的SSLove具有窃取短信、通讯录、WhatsApp和Telegram数据、使用FTP进行上传文件等多种功能。

该组织在使用SSLove时和Droidjack用法一样，一种是直接使用，其中上述提到的Al Swarm网站被拍拍熊组织用来水坑攻击时使用的伪装APP就属于这种；另一种是插入到正常APP中进行隐藏。

image.png

图4.3 SSLove指令功能相关数据表

Windows

Windows端共使用到三种RAT，都是在中东地区流行了数年的RAT，其中有两种（njRAT和H-worm）曾被多次曝光，但依旧活跃。

njRAT

njRAT[2]又称Bladabindi，通过控制端可以操作受控端的注册表，进程，文件等，还可以对被控端的键盘进行记录。同时njRAT采用了插件机制，可以通过不同的插件来扩展njRAT的功能。

该组织在使用njRAT时大多不是直接使用，而是在njRAT的基础上进行了二次封装，使用C#为njRAT加了一层壳，并对壳的代码进行了大量的混淆。该壳的作用是在内存中加载njRAT运行，防止njRAT被杀毒软件检测，而上述提到的Amaq网站被该组织用来水坑攻击时使用的伪装成Adobe Flash Player就属于这种。

image.png

图4.4 从Amaq水坑活动中伪装的恶意样本提取出来的njRAT

H-Worm

H-Worm是一个基于VBS（Visual Basic Script）的RAT，该RAT情况信息可参阅FireEye之前发表的详细报告《Now You See Me - H-worm by Houdini》[3]。此次攻击使用的是混淆变异后的H-Worm版本，去除混淆后进行分析，我们发现其指令列表并无变化。

图4.5 混淆的H-Worm代码片段

指令	功能
excecute	执行服务端命令
update	更新载荷
uninstall	卸载自身
send	下载文件
site-send	指定网站下载文件
recv	上传数据
enum-driver	枚举驱动
enum-faf	枚举指定目录下的文件
enum-process	枚举进程
cmd-shell	执行shell
delete	删除文件
exit-process	结束进程
sleep	设置脚本休眠时间

表3 H-Worm样本指令与功能对应关系

Fkn0wned

fkn0wned是一款通过VB.NET编写的RAT，此次攻击使用的属于一个早期版本，仅接收“DOWNLOAD”指令，DDoS功能代码并未起作用，该RAT实际是个下载者。

图4.4 fkn0wned配置信息及指令响应代码图

C&C、IP及部分样本对应关系

图4.5 C&C、IP及部分样本对应关系

五、 受攻击地区分布情况

截至目前，360烽火实验室发现此次拍拍熊组织攻击活动影响到的国家共有11个 ，通过查询可以知悉这些国家均存在某武装组织组织人员。显而易见，造成这个分布现象的缘由正是该组织采用的数次针对性的水坑攻击导致。

图5.1 受攻击的地区分布情况

六、 溯源与关联

360烽火实验室通过对此次拍拍熊攻击活动的分析，结合之前对黄金鼠组织的分析，我们发现两个组织除掉攻击目标和各自的专属RAT外，两者在下面几个方面有很强的关联性。

- 均熟悉阿拉伯语，持续数年针对Android和Windows平台，擅长水坑攻击。
- 均使用多种RAT，其中大多数双方都有使用。
- 两个组织在两个时间段内使用了处于同一网段的C&C。

七、 总结

随着地缘政治冲突等问题，各方试图通过网络情报和网络攻击活动占领先机，进一步造成网络空间冲突的加剧。此次拍拍熊组织又是一个基于此而产生的间谍情报活动组织，没有和平的因素，攻击不可能会停止。近期报道称中东某国境内的某武装组织最后据点被攻下且被宣灭亡，这或许意味着拍拍熊组织的攻击活动将会有所变化，最后愿早日长久和平!

附录A：样本MD5

Android攻击样本MD5	Windows攻击样本MD5
12100da4635765f8d69d684f742a47bd	085e195c9b14ef099171805c44ff4914
1d5e36be4b94289f214447964ede688d	1a655affc8d5fffa48915a934f31f95e
1daf7e38d8d918e8e087ad590b299218	291c3f5b9b53381283a044e337899c84
1eb8e8667ed7d2a07076e3d240207613	6d6961ced0e77c28f881db579301a927
249aad5d2722b69aac7ed27c9e669c79	8bb342a3e770717bd8f39ac12a687b54

Android攻击样本MD5	Windows攻击样本MD5
2706be45411ed22ce456b8fe8273b285	8c49833f76b17fdaafe5130f249312ca
31aad6045f403fcd397e19cad4f80d1f	ba1249123e808e744aeb96753bc119d4
3751db0d511305b39601e09959491d8e	bfaf6389cb9fba695daa8552f697d40b
430a0b26cc53f7d39b8192d0b3f79837	d2c40e2183cf18855c36ddd14f8e966f
4333a9e5d6de6e12b368f5a943a30a0e	d52f57b6597e55c40c21b0f8c763cd69
484d74ebd0e3586e2ff694017dcaa9e3	d9153bdf30e0a3ab31601e43d85c9949
51f7d6fec2be62fc29cfb94f52803428	daf7f053cf78690ff0c6ec0384d85bf2
523845736fc92ea80e9880641b768dc1	e6e676df8250a7b930b2d016458225e2
71d0cea1bee13d1e36b5a53788001b85	
7d50a9bd474a7c5878ac8e0e4a183a8b	
80382a7f2eb4f292a28554bc95b57938	
98d584d4d575e31f9f4f70c9be05166f	
a31f1ce49662a60daa46180d02ab6218	
a41c5f227ac2816355ce4cf650993749	
a95d57eaaf7847a07e62c6ea0fecbfb7	
b7d12ab736b41d503e93a0bd6125cf62	
b87f516b2ee0e6df09510f75b16c25ef	
bb2d1238c8418cde13128e91f1a77ae7	
bef2dddd8892a4985879971cf437d79b	
c9e434e780b5bed397c543bb3264deea	
d195511307a2c5ac52bebf8a98b9dfae	
d207a876369681ed476f650d808a25a8	
dc1ede8e2d3206b04cb95b6ae62f43e0	
e92651bb3ad8c5c3acf38dedb2abc2ca	
ea6e187934fc1459d3b04b0898496b2c	

Android攻击样本MD5	Windows攻击样本MD5
eb3310f19720abddc34c4602983e4f3c	
f66d99406819ca96b47d7ff0881a0a1a	

附录B：C&C

66.85.157.86

82.137.255.0

da3da3.duckdns.org

samd1.duckdns.org

samd2.duckdns.org

sorry.duckdns.org

btcaes2.duckdns.org

附录C：参考链接

[1] https://ti.360.net/blog/articles/analysis-of-apt-c-27/

[2] https://en.wikipedia.org/wiki/Njrat

[3]https://www.fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html

本文链接：https://blogs.360.cn/post/analysis-of-apt-c-37.html

-- EOF --