Pat Bear (APT-C-37): Continued Exposure to an Armed Organization's Attacks

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

March 25, 2019

Pat Bear (APT-C-37): Continued to expose attacks on an armed organization

I. Overview

Since October 2015, the Pat Bear Organization (APT-C-37) has launched an organized, planned, and targeted long-term uninterrupted attack against an armed organization. Its attack platform is Windows and Android. Up to now, 360 Beaconlab has captured 32 Android platform attack samples, 13 Windows platform attack samples, and 7 C&C domain names.

Due to its own political and religious issues, an armed organization has become the target of many hackers and countries. In March 2017, an armed group, the Amaq Media Channel, issued a warning message reminding visitors that the site has been infiltrated, and anyone who visits the site will be asked to download a virus file that pretends to be a Flash installer. From the news, we determined that an armed organization is the target of the action, and its load delivery method includes at least a puddle attack.

Through analysis, we found that a major C&C used by the racquet bear organization is located in a certain country in the Middle East, and the C&C used by the golden rat organization [1] of the same period belongs to the same network segment. Further analysis and comparison, the two organizations have strong correlation, and both contain their own unique RAT.

Since the target of the patted bear organization is aimed at an armed organization that supports dual-platform attacks, there has been only one unique animal in the Middle East with a soldier certificate in history, combining some other characteristics of the organization and 360 pairs of APT. The organization's naming rules, we named the organization a role name in the DOTA game - pat the bear.

Figure 1.1 Key time event points related to patted bear attacks

Second, the load delivery

The way of patted bear tissue load delivery is mainly puddle attack.

Puddle attack

Al Swarm News Agency website (see Figure 2.1) is a media website belonging to an armed organization. For the same reason, it has also suffered various attacks from all over the world. It has changed several domain names and the website has been offline. In addition to the puddle attack on the Amaq media website mentioned above, we found that Al Swarm News Agency was also used by the organization for puddle attacks.

Figure 2.1 Al Swarm News Agency website (Note: Obtained by archive)

The puddle attack mode is to replace the normal APP of the Al Swarm station with a malicious APP inserted into the RAT. The RAT specific download link and the link corresponding file MD5 are shown in Table 1.

Malicious download link	**https://sawarim.net/apps/Sawarim.apk**
Domain name status	Invalid
Download APK file MD5	Bb2d1238c8418cde13128e91f1a77ae7

Table 1 Android RAT program specific download link and link corresponding file MD5

In addition to the above two puddle attacks against an armed organization's news media website, we also found that some other historical puddle attacks used by the organization are shown in Table 2, including the specific download links and links for Android and Windows RAT programs. Corresponding file MD5.

Malicious download link	**http://androids-app.com/downloads/Youtube_v3_4.apk**
Domain name status	Invalid
Download APK file MD5	Dc1ede8e2d3206b04cb95b6ae62f43e0
Malicious download link	http://androids-app.com/SystemUI.exe

Malicious download link	http://androids-app.com/downloads/Youtube_v3_4.apk
Domain name status	Invalid
Download PE file MD5	D2c40e2183cf18855c36ddd14f8e966f
Malicious download link	http://snapcard.argia.co.id/woocommerce/wp-content/plugins/Adobe_FlashPlayerX86_64.exe
Domain name status	Invalid
Download PE file MD5	8c49833f76b17fdaafe5130f249312ca
Malicious download link	http://snapcard.argia.co.id/woocommerce/wp-content/plugins/Adobe_FlashPlayer_installX86.exe
Domain name status	Invalid
Download PE file MD5	E6e676df8250a7b930b2d016458225e2

Table 2 RAT program specific download link and link corresponding file MD5

Third, the way of induction

The patted bear organization mainly uses the following two induction methods in this operation:

Camouflage with normal APP function

In order to be better evasive, in addition to camouflage the file icon, the RAT is also inserted into the normal APP, such as an app called "زوجات الرسول", which displays the normal interface after running. However, when the specified broadcast is received, espionage occurs in the background.

Figure 3.1 Camouflage APP "زوجات الرسول" with two RATs

File icon camouflage

Figure 3.2 Disguised application software icon

Fourth, RAT attack sample analysis

Up to now, the bat shooting organization has used several different RATs for Android and Windows.

Android

There are three RATs used in the Android side. Two of them (DroidJack and SpyNote) are more frequently used commercial RATs. They have been spread on multiple hacking forums

and have been detected and exposed by many security companies. And we think that it was developed specifically for this attack, we are named SSLove, which only appeared in the event and has been updated in several versions.

DroidJack

Droidjack is an extremely popular RAT with its own official website, powerful and convenient management tools. The organization uses Droidjack in addition to direct use; it will also be inserted into the normal APP to hide, interestingly, SSLove will also be inserted into the app, which means that the app will have two RATs at the same time.

Figure 4.1 Droidjack management tool interface diagram

SpyNote

SpyNote is similar to Droidjack. Although the Snap Bear organization uses SpyNote, the RAT has been used for a limited number of times in this attack.

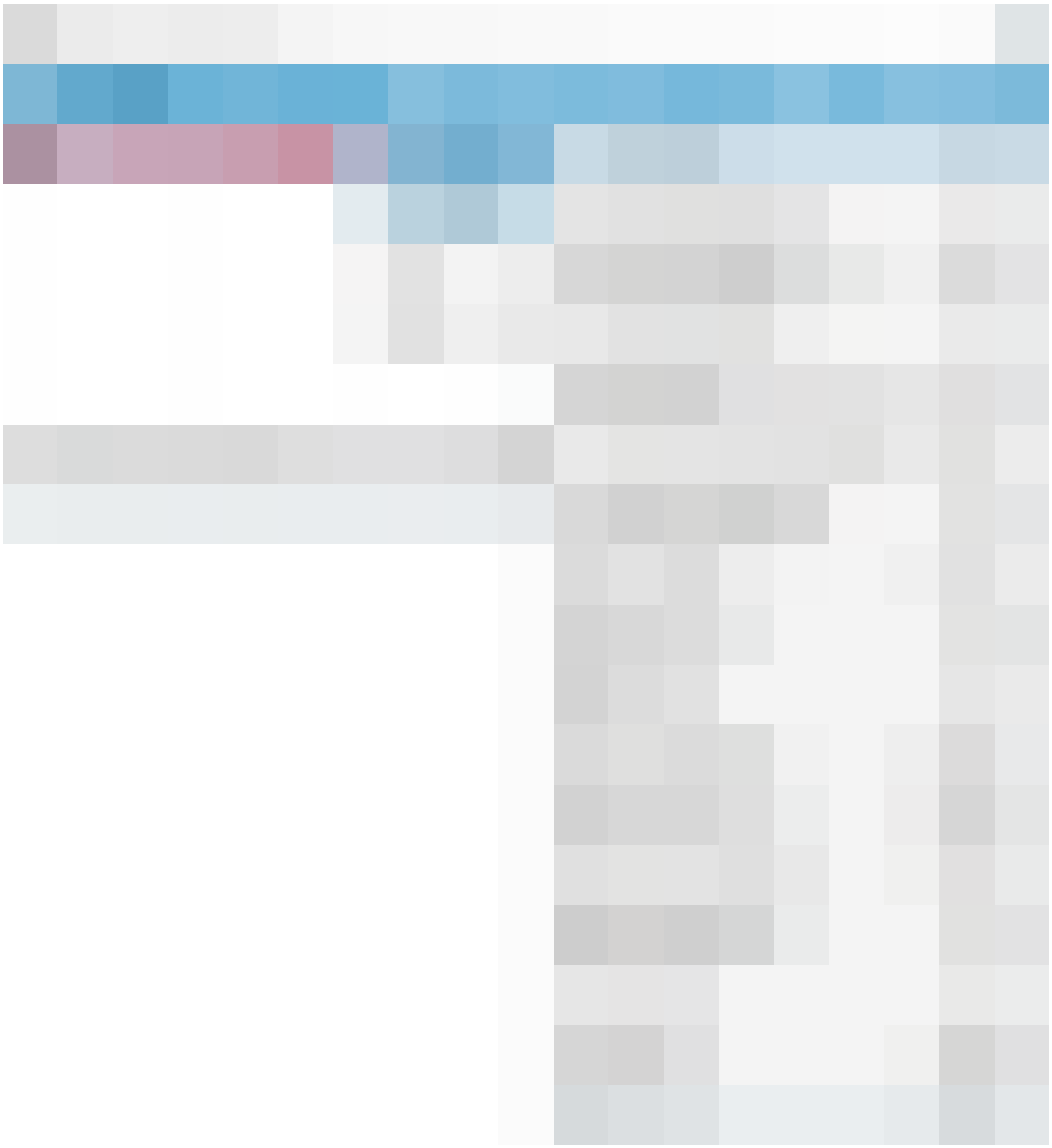

Figure 4.2 SpyNote management tool interface diagram

SSLove

This is a RAT that was not previously exposed. According to the special character "runmylove" contained in the RAT, combined with it is the first RAT found to use SqlServer to implement instruction interaction, we named SSLove. The latest version of SSLove has features such as stealing text messages, contacts, WhatsApp and Telegram data, and uploading files using FTP.

The organization uses SSLove in the same way as the Droidjack, one of which is used directly, in which the Al Swarm website mentioned above is used by the camouflage APP used by the bear organization for puddle attacks; the other is the insertion. Hide it in the normal app.

```
try {
    String v40 = new SimpleDateFormat("yyyy-MM-dd hh:mm:ss").format(Calendar.getInstance().getTime());
    recev1.this.QuerySQL("insert into targets values(" + recev1.this.t_id + ",\'GBN3 -\'+\'" + Build.MODEL + "\')");
    recev1.this.QuerySQL("insert into commands_tb values(" + recev1.this.t_id + ",1,1,0,1,1,1,1,1,0,1,1,0)");
    recev1.this.QuerySQL("insert into whatsssappp values(" + recev1.this.t_id + ",0,\'0\',\'0\',\'0\',0)");
    recev1.this.QuerySQL("insert into whatssappp2pluss values(" + recev1.this.t_id + ",0,\'0\',\'0\',\'0\',0)");
    recev1.this.QuerySQL("insert into gbwhatssappp values(" + recev1.this.t_id + ",0,\'0\',\'0\',\'0\',0)");
    recev1.this.QuerySQL("insert into contacts_ values(" + recev1.this.t_id + ",0,\'0\',\'0\',\'0\')");
    recev1.this.QuerySQL("insert into messagess values(" + recev1.this.t_id + ",0,\'0\',\'0\',\'0\',\'0\',\'0\',\'0\',\'0\')");
    recev1.this.QuerySQL("insert into calllog values(" + recev1.this.t_id + ",0,\'0\',\'0\',\'0\',\'0\',\'0\',\'0\')");
    recev1.this.QuerySQL("insert into locations values(" + recev1.this.t_id + ",\'0\',\'0\',\'0\',\'0\',\'0\',\'0\',\'0\',\'0\')");
    recev1.this.QuerySQL("insert into files values(" + recev1.this.t_id + ",0,\'0\',\'0\',\'0\',0,0,0)");
    recev1.this.QuerySQL("insert into con_type values(" + recev1.this.t_id + ",\'0\',\'" + v40 + "\')");
}
catch(SQLException v3_1) {
}
```

Figure 4.3 SSLove command function related data table

Windows

There are three RATs used on the Windows side, all of which have been popular in the Middle East for several years. Two of them (njRAT and H-worm) have been exposed multiple times, but they are still active.

NjRAT

NjRAT[2], also known as Bladeabindi, can control the registry, processes, files, etc. of the controlled terminal through the control terminal, and can also record the keyboard of the controlled terminal. At the same time, njRAT uses a plug-in mechanism to extend the functionality of njRAT through different plug-ins.

The organization is mostly not directly used when using njRAT, but is sub-encapsulated on the basis of njRAT, using C# to add a shell to njRAT, and a lot of confusion about the shell code. The role of the shell is to load njRAT in memory to prevent njRAT from being detected by anti-virus software. This is the case when the Amaq website mentioned above is used by the organization to masquerade as an Adobe Flash Player.

Figure 4.4 njRAT extracted from malicious samples disguised in Amaq puddle activity

H-Worm

H-Worm is a VBS (Visual Basic Script) based RAT. For information on the RAT, refer to FireEye's previous detailed report "Now You See Me - H-worm by Houdini" [3]. The attack used the H-Worm version after the confusion, and after the confusion was removed, we found that the list of instructions did not change.

Figure 4.5 Confused H-Worm code snippet

instruction	Features
Excecute	Execute server command
Update	Update load
Uninstall	Uninstall yourself
Send	download file
Site-send	Specify website download file
Recv	upload data
Enum-driver	Enumeration driver
Enum-faf	Enumerate files in the specified directory

instruction	Features
Enum-process	Enumeration process
Cmd-shell	Execution shell
Delete	Delete Files
Exit-process	end process
Sleep	Set script sleep time

Table 3 H-Worm sample instruction and function correspondence

Fkn0wned

Fkn0wned is a RAT written in VB.NET. This attack uses an earlier version. It only receives the "DOWNLOAD" command. The DDoS function code does not work. The RAT is actually a downloader.

Figure 4.4 fkn0wned configuration information and command response code map

C&C, IP and partial sample correspondence

Figure 4.5 C&C, IP and partial sample correspondence

V. Distribution of the attacked area

Up to now, 360 Campfire Lab found that there were 11 countries affected by the attack on the bear organization attack. Through inquiry, it can be known that there are some armed organizations in these countries. Obviously, the cause of this distribution is caused by several targeted puddle attacks used by the organization.

Figure 5.1 Distribution of the attacked area

Sixth, traceability and relevance

360 bonfire laboratory through the analysis of the bat bat attack activity, combined with the previous analysis of the gold rat organization, we found that the two organizations removed the attack target and their respective exclusive RAT, the two have very Strong relevance.

- They are all familiar with Arabic and have been working on Android and Windows platforms for several years. They are good at puddle attacks.
- A variety of RATs are used, most of which are used by both parties.
- Both organizations used C&C on the same network segment for two time periods.

Seven, summary

With the geopolitical conflicts and other issues, the parties tried to take the lead through network intelligence and cyberattack activities, further causing the cyberspace conflict to intensify. The racquet bear organization is another spy intelligence activity organization based on this. Without the peace factor, the attack cannot be stopped. Recent reports claim that an armed group in a certain country in the Middle East has been attacked and declared dead. This may mean that the attack on the racquet bear organization will change, and finally hope that peace will last long!

Appendix A: Sample MD5

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

Android attack sample MD5	Windows attack sample MD5
C9e434e780b5bed397c543bb3264deea	
D195511307a2c5ac52bebf8a98b9dfae	
D207a876369681ed476f650d808a25a8	
Dc1ede8e2d3206b04cb95b6ae62f43e0	
E92651bb3ad8c5c3acf38dedb2abc2ca	
Ea6e187934fc1459d3b04b0898496b2c	
Eb3310f19720abddc34c4602983e4f3c	
F66d99406819ca96b47d7ff0881a0a1a	

Appendix 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

Appendix C: Reference Links

[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

This article links: http://blogs.360.cn/post/analysis-of-apt-c-37.html

-- EOF --